การศึกษาช่องโหว่ของบริการเครือข่าย Wi-Fi

Wi-Fi Vulnerability

โดย

นางสาวศิริพร ตั้งศิริประเสริฐ

นางสาวเสาวภา จันทรัตน์

นางสาวอาริสา คงทอง

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

ภาควิชาวิศวกรรมโทรคมนาคม

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2561

การศึกษาช่องโหว่ของบริการเครือข่าย Wi-Fi

Wi-Fi Vulnerability

โดย

นางสาว ศิริพร ตั้งศิริประเสริฐ	58011216
นางสาว เสาวภา จันทรัตน์	58011380
นางสาว อาริสา คงทอง	58011450

อาจารย์ที่ปรึกษา

ผศ. ดร. นภัทร สระเอี่ยม

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

ภาควิชาวิศวกรรมโทรคมนาคม

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2561

ผ่านการตรวจรูปเล่มแล้ว

(.....)

อาจารย์ที่ปรึกษา

23 / 5 / 62

KMITL วิศวกรรมโทรคมนาคม Telecommunications Engineering

ผ่านการตรวจชิ้นงานแล้ว

(.....)

กรรมการผู้ตรวจชิ้นงาน

23 / 5 / 2562

KMITL วิศวกรรมโทรคมนาคม Telecommunications Engineering

ปริญญานิพนธ์ปีการศึกษา 2561

ภาควิชาวิศวกรรมโทรคมนาคม

คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เรื่อง การศึกษาช่องโหว่ของบริการเครือข่าย WI-FI

WI-FI VULNERABILITY

ผู้จัดทำ

1. นางสาว ศิริพร ตั้งศิริประเสริฐ 58011216
2. นางสาว เสาวภา จันทรัตน์ 58011380
3. นางสาว อาริสา คงทอง 58011450

..... **อาจารย์ที่ปรึกษา**

(ผศ. ดร. นภัทร สระเอี่ยม)

กิตติกรรมประกาศ

ปริญญานิพนธ์เรื่อง “การศึกษาช่องโหว่ของบริการเครือข่าย Wi-Fi” สำเร็จลุล่วงได้ด้วยความกรุณาและความช่วยเหลือจาก ผศ.ดร.นภัทร สระเอี่ยม อาจารย์ที่ปรึกษาปริญญานิพนธ์ ผศ.ดร.ธเนศ พัฒนธาดาพงษ์ และ ดร.สมปอง วิเศษพาณิชกิจ ที่ให้คำแนะนำ คำปรึกษา และแนวคิด ตลอดจนการแก้ไขปัญหา ข้อบกพร่องต่าง ๆ มาโดยตลอด เพื่อให้ปริญญานิพนธ์นี้สำเร็จโดยสมบูรณ์ รวมถึงการสนับสนุนเครื่องมือ อุปกรณ์ หนังสือ และบทความต่าง ๆ ที่ใช้ระหว่างการทำปริญญานิพนธ์ ผู้จัดทำขอขอบพระคุณเป็นอย่างสูงสำหรับการดูแลและเอาใจใส่

ขอขอบคุณคณาจารย์ประจำภาควิชาวิศวกรรมโทรคมนาคม คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบังทุกท่าน ที่ได้อบรมสั่งสอนและมอบวิชาความรู้ และประสบการณ์ต่าง ๆ ที่สามารถนำมาใช้ในการดำเนินปริญญานิพนธ์นี้

ขอบคุณเพื่อน ๆ ทุกคนที่คอยให้คำแนะนำ คำปรึกษาและความช่วยเหลือเป็นอย่างดีมาโดยตลอด ซึ่งเป็นประโยชน์ในการดำเนินปริญญานิพนธ์นี้ ตลอดจนขอกราบขอบพระคุณบิดามารดา และผู้ปกครองที่คอยเป็นกำลังใจที่ดีเสมอมา

นางสาวศิริพร ตั้งศิริประเสริฐ
นางสาวเสาวภา จันทรัตน์
นางสาวอาริสา คงทอง
ผู้จัดทำ

การศึกษาช่องโหว่ของบริการเครือข่าย WI-FI

WI-FI VULNERABILITY

โดย นางสาว ศิริพร ตั้งศิริประเสริฐ 58011216

นางสาว เสาวภา จันทรัตน์ 58011380

นางสาว อาริสา คงทอง 58011450

อาจารย์ที่ปรึกษา ผศ.ดร.นภัทร สระเอี่ยม

บทคัดย่อ

ปริญญานิพนธ์นี้ต้องการศึกษาจุดอ่อนหรือช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากบริการเครือข่าย Wi-Fi และหาช่องโหว่ด้านความปลอดภัยของเครือข่าย Wi-Fi โดยทำการค้นหาและตรวจจับสัญญาณ Wi-Fi โดยการใช้เครื่องมือบนระบบปฏิบัติการ Kali Linux เครื่องมือที่ใช้ในการค้นหาช่องโหว่ก็จะแตกต่างกันออกไป ขึ้นอยู่กับประเภทของ Wi-Fi ขั้นตอนการดำเนินงานได้แก่ การจำลองระบบเครือข่าย Wi-Fi เพื่อทำการทดสอบถึงจุดอ่อนหรือช่องโหว่ที่อาจเกิดขึ้นบนเครือข่าย Wi-Fi หลังจากนั้นทำการเขียนโปรแกรมโดยใช้แบช (Bash) เพื่อให้สามารถรันคำสั่งในการหาช่องโหว่หรือจุดอ่อนตามที่ศึกษามาได้อย่างอัตโนมัติ

ABSTRACT

This thesis would like to study about vulnerabilities caused by wireless network and find security vulnerabilities of wireless network. To perform search and detect Wi-Fi and using tools on Kali operating system, the tools use to find vulnerabilities will be different depend on the type of Wi-Fi. The simulations of wireless network for testing security on wireless network. After that do programming by Bash to run commands find vulnerabilities as learn automatically.

สารบัญ

สารบัญ (ต่อ)

สารบัญ (ต่อ)

สารบัญรูป

สารบัญรูป (ต่อ)

สารบัญรูป (ต่อ)

หน้า

รูปที่

สารบัญตาราง

หน้า

ตารางที่

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในปัจจุบันเครือข่ายอินเทอร์เน็ตไร้สาย มีการให้บริการอินเทอร์เน็ตไร้สายในที่สาธารณะอย่างแพร่หลาย โดยบุคคลทั่วไปสามารถใช้บริการเหล่านี้ได้โดยไม่เสียค่าบริการ โดยบริการเหล่านี้มีช่องโหว่ด้านความปลอดภัยของเครือข่าย Wi-Fi ซึ่งอาจนำไปสู่ภัยคุกคามจากการใช้บริการเครือข่ายอินเทอร์เน็ตไร้สายสาธารณะได้ ดังนั้นผู้จัดทำจึงได้ทำการศึกษามาตรฐานการเข้ารหัสสัญญาณเครือข่าย Wi-Fi ในรูปแบบต่าง ๆ และศึกษาช่องโหว่ด้านความปลอดภัยของเครือข่าย Wi-Fi เพื่อทำการเขียนโปรแกรมเพื่อศึกษาจุดอ่อนของบริการเครือข่าย Wi-Fi

1.2 วัตถุประสงค์

1) เพื่อศึกษามาตรฐานการเข้ารหัสสัญญาณเครือข่าย Wi-Fi (WEP, WPA, WPA2, WPA3)

2) เพื่อศึกษาช่องโหว่ด้านความปลอดภัยของเครือข่าย Wi-Fi

3) เพื่อศึกษาภัยคุกคามที่เกิดขึ้นจากบริการเครือข่าย Wi-Fi

1.3 ขอบเขตของปริญญานิพนธ์

1) สามารถหาช่องโหว่ของบริการเครือข่าย Wi-Fi

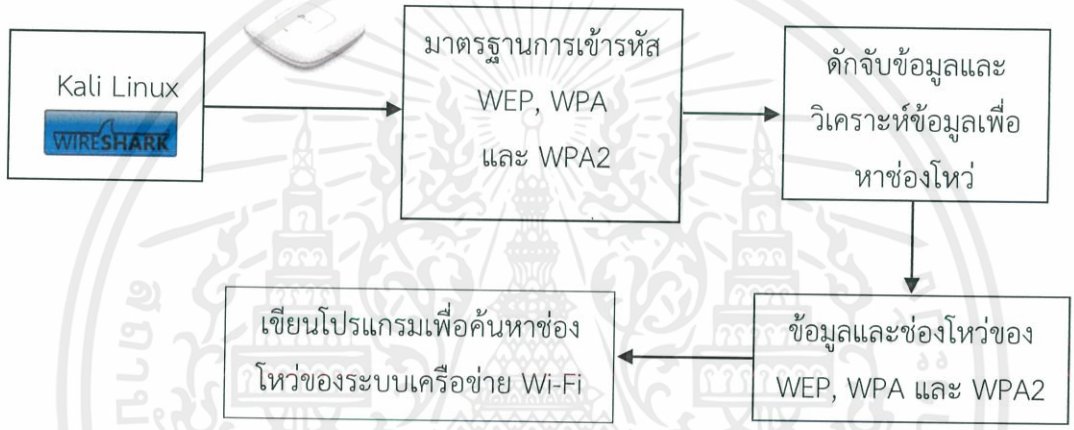
2) โครงงานนี้มุ่งเน้นที่มาตรฐาน WEP, WPA, WPA2, WPA3

3) สามารถเขียนโปรแกรมเพื่อศึกษาจุดอ่อนของบริการเครือข่าย Wi-Fi

บทที่ 2

ทฤษฎีและหลักการที่เกี่ยวข้อง

โครงงานเรื่องการศึกษาช่องโหว่ของบริการเครือข่าย Wi-Fi แบ่งการทำงานออกเป็น 2 ส่วน ได้แก่ การศึกษาช่องโหว่ของบริการเครือข่าย Wi-Fi โดยการใช้เครื่องมือบนระบบปฏิบัติการ Kali Linux และการเขียนโปรแกรมหาช่องโหว่ของบริการเครือข่าย Wi-Fi ดังรูปที่ 2.1



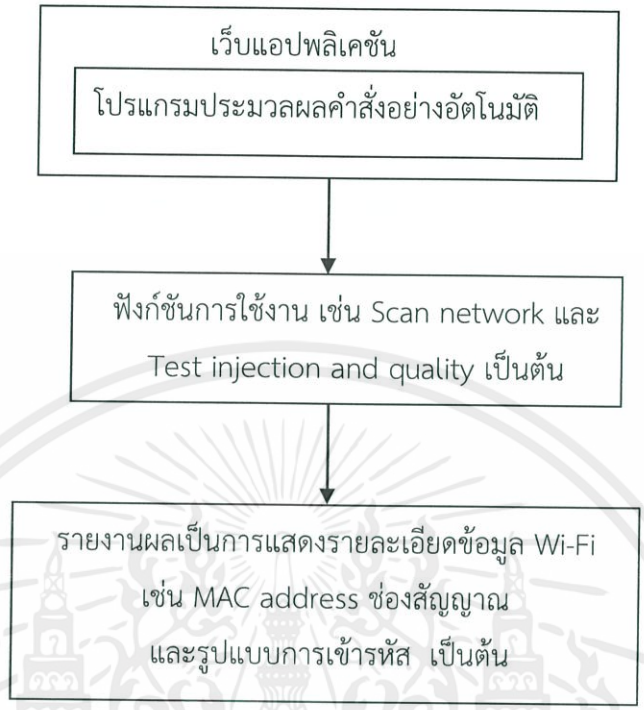
รูปที่ 2.1 บล็อกไดอะแกรมภาพรวมของโครงงาน

ซึ่งภายในบล็อกการเขียนโปรแกรมหาช่องโหว่ของบริการเครือข่าย Wi-Fi จะมีการทำงานในแต่ละส่วนดังรูปที่ 2.2 มีรายละเอียดของแต่ละบล็อกดังนี้

1. เว็บแอปพลิเคชัน (Web Application) เป็นหน้าเว็บสำหรับแสดงผล และรับข้อมูลจากผู้ใช้ ว่าผู้ใช้ต้องการจะดูข้อมูลของ Wi-Fi ตัวใด โดยเนื้อหาที่แสดงหน้าเว็บใช้ภาษาเอชทีเอ็มแอล (Hyper Text Markup Language) เป็นหลัก และใช้ JavaScript ในการสื่อสารระหว่างไคลเอนต์กับเซิร์ฟเวอร์ (Server) จากนั้น CGI (Common Gateway Interfaces) จะรับค่าที่ผู้ใช้กรอกไปทำการประมวลผลต่อไป

2. ในบล็อกของฟังก์ชันการใช้งาน เมื่อ CGI นำข้อมูลจากผู้ใช้ในบล็อกเว็บแอปพลิเคชันมาประมวลผลในโปรแกรมค้นหาช่องโหว่ของบริการเครือข่าย Wi-Fi ที่เขียนขึ้นด้วยแบช (Bash)

3. เป็นการแสดงผลโดยส่งข้อมูลกลับไปแสดงผลให้ผู้ใช้ที่หน้าเว็บแอปพลิเคชัน



รูปที่ 2.2 บล็อกไดอะแกรมการเขียนโปรแกรมเพื่อค้นหาช่องโหว่ของระบบเครือข่าย Wi-Fi

2.1 ระบบเครือข่ายไร้สาย

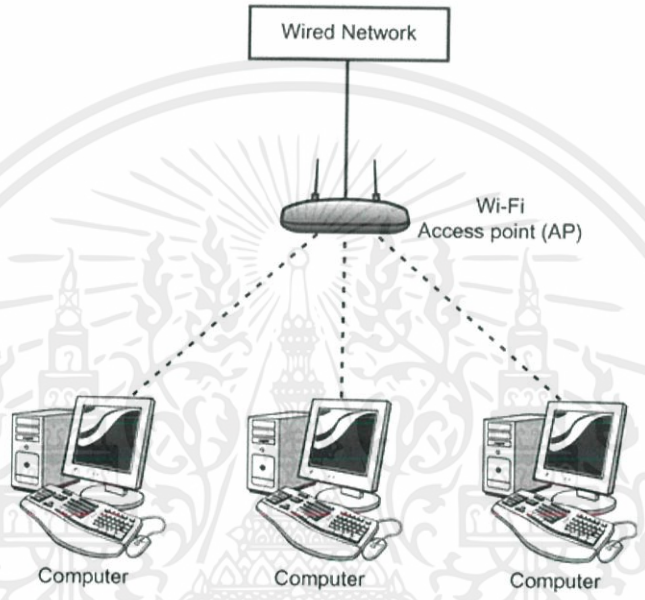
ระบบเครือข่ายไร้สายหรือแลนไร้สาย (Wireless LAN : WLAN) หมายถึง เทคโนโลยีการติดต่อสื่อสารข้อมูลระหว่างอุปกรณ์กับเครื่องคอมพิวเตอร์ตั้งแต่ 2 เครื่องขึ้นไป ให้สามารถสื่อสารกันได้ โดยผ่านคลื่นแม่เหล็กไฟฟ้าเป็นช่องทางการสื่อสารข้อมูล แทนการใช้สายสัญญาณเพื่อรับส่งข้อมูลระหว่างเครื่องคอมพิวเตอร์ และระหว่างเครื่องคอมพิวเตอร์กับแอกเซสพอยต์ (Access Point) โดยคลื่นแม่เหล็กไฟฟ้าอาจเป็นคลื่นความถี่วิทยุ (Radio) หรือคลื่นอินฟราเรด (Infrared)

2.1.1 ลักษณะการเชื่อมต่อของอุปกรณ์

2.1.1.1 โหมด Infrastructure

เป็นโหมดที่อนุญาตให้อุปกรณ์ภายในระบบเครือข่ายไร้สายสามารถเชื่อมต่อกับเครือข่ายอื่นได้ ประกอบด้วยอุปกรณ์ 2 ประเภทได้แก่ ไคลเอนต์ (Client Station) คืออุปกรณ์คอมพิวเตอร์ที่มีอุปกรณ์ไคลเอนต์อะแดปเตอร์ (Client-Adapter) เพื่อใช้รับส่งข้อมูลผ่านบริการเครือข่าย Wi-Fi และแอกเซสพอยต์ ทำหน้าที่เชื่อมต่อไคลเอนต์เข้ากับระบบเครือข่ายอื่น

การทำงานในโหมด Infrastructure มีพื้นฐานมาจากระบบเครือข่ายโทรศัพท์เคลื่อนที่ โดยไคลเอนต์จะสามารถรับส่งข้อมูลโดยตรงกับแอกเซสพอยต์ที่ให้บริการแก่ไคลเอนต์นั้นอยู่เท่านั้น ส่วนแอกเซสพอยต์จะทำหน้าที่ส่งต่อ (Forward) ข้อมูลที่ได้รับจากไคลเอนต์ไปยังจุดหมายปลายทาง หรือส่งต่อข้อมูลที่ได้รับจากเครือข่ายอื่นมายังไคลเอนต์ ดังรูปที่ 2.3

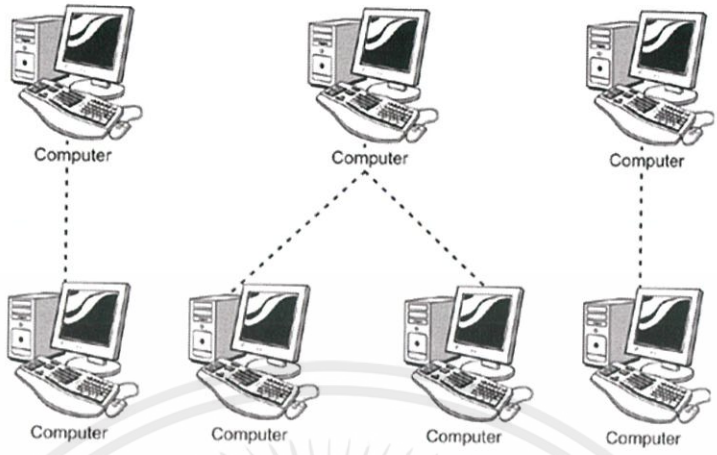


รูปที่ 2.3 การเชื่อมต่อโหมด Infrastructure

(ที่มา : http://etutorials.org/Networking/beginners+guide+to+wi-fi+wireless...)

2.1.1.2 โหมด Ad-Hoc หรือ Peer-to-Peer

เป็นระบบเครือข่ายแบบปิด คือ ไม่มีแอกเซสพอยต์และไม่มีการเชื่อมต่อกับเครือข่ายอื่น บริเวณของเครือข่าย Wi-Fi ในโหมด Ad-Hoc จะถูกเรียกว่า Independent Basic Service Set (IBSS) ซึ่งไคลเอนต์หนึ่งสามารถติดต่อสื่อสารข้อมูลกับไคลเอนต์อื่น ๆ ในเขต IBSS เดียวกันได้โดยตรงโดยไม่ต้องผ่านแอกเซสพอยต์ แต่ไคลเอนต์จะไม่สามารถรับส่งข้อมูลกับเครือข่ายอื่น ๆ ได้ ดังรูปที่ 2.4



รูปที่ 2.4 การเชื่อมต่อโหมด Ad-Hoc หรือ Peer-to-Peer
(ที่มา : http://etutorials.org/Networking/beginners+guide+to+wi-fi+wireless...)

2.1.2 อุปกรณ์ใน WLAN

2.1.2.1 LAN Adapters

ทำหน้าที่เป็นอินเตอร์เฟสระหว่างระบบปฏิบัติการกับสายอากาศของไวเลสการ์ดเพื่อสร้างการเชื่อมต่อไปยังเครือข่ายอื่นต่อไป ซึ่งในโครงงานนี้ใช้แลนการ์ดไร้สายแบบ USB ยี่ห้อ ALFA รุ่น AWUS036AC (AC1200 High Gain) โดยคำนึงถึงปัจจัยเบื้องต้น ดังนี้

- สามารถทำการ packet injection ได้
- สามารถใช้งานกับมาตรฐานการเข้ารหัส WEP, WPA, WPA2 ได้

2.1.2.2 Wireless Access Point

แอกเซสพอยต์เป็นอุปกรณ์กระจายสัญญาณที่ใช้เป็นตัวกลางในการรับส่งข้อมูลระหว่างเครื่องคอมพิวเตอร์ที่ติดตั้งเครือข่ายไร้สายให้สามารถติดต่อสื่อสารกันได้ ลักษณะการทำงานของแอกเซสพอยต์ทำหน้าที่เช่นเดียวกับสวิตช์ในระบบเครือข่ายแบบใช้สาย (LAN) โดยแอก-เซสพอยต์จะมีพอร์ต (Port) RJ-45 สำหรับใช้เชื่อมต่อเข้ากับเครือข่ายแบบใช้สาย อีกทั้งยังกระจายสัญญาณไร้สายออกไปยังไคลเอนต์ที่อยู่ในรัศมีการกระจายสัญญาณ การทำงานของแอกเซสพอยต์ทำงานภายใต้มาตรฐานของ IEEE 802.11ac แสดงดังรูป 2.5

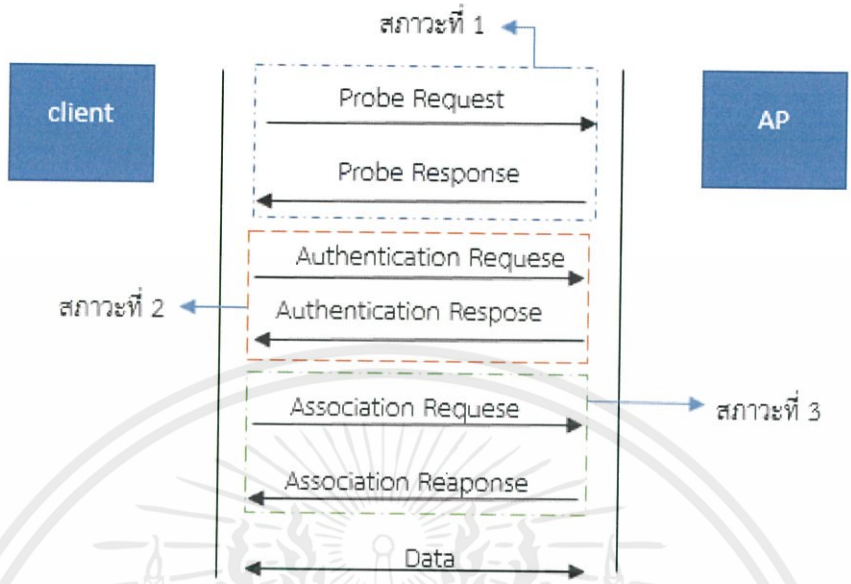
รูปที่ 2.5 แอกเซสพอยต์

2.1.3 กระบวนการสร้างการเชื่อมต่อ (Association Process Explained)

ในการที่จะเชื่อมต่อเพื่อติดต่อสื่อสารกับเครือข่ายไร้สายจะต้องทำการพิสูจน์ตัวตน (Authentication) เพื่อป้องกันการเข้าใช้งานของผู้ที่ไม่ได้รับอนุญาต โดยไคลเอนต์จะทำการร้องขอไปยังแอกเซสพอยต์ด้วยกัน 3 สภาวะ ดังนี้

1. ยังไม่มีการพิสูจน์ตัวตน และยังไม่มีการขอเข้าร่วมเครือข่าย
2. พิสูจน์ตัวตนแล้ว แต่ยังไม่มีการขอเข้าร่วมเครือข่าย
3. ผ่านการพิสูจน์ตัวตนแล้ว และได้รับการตอบรับเข้าร่วมเครือข่าย

แสดงดังรูปที่ 2.6



รูปที่ 2.6 สภาวะการพิสูจน์ตัวตน

โดยแต่ละสภาวะมีรายละเอียดดังนี้

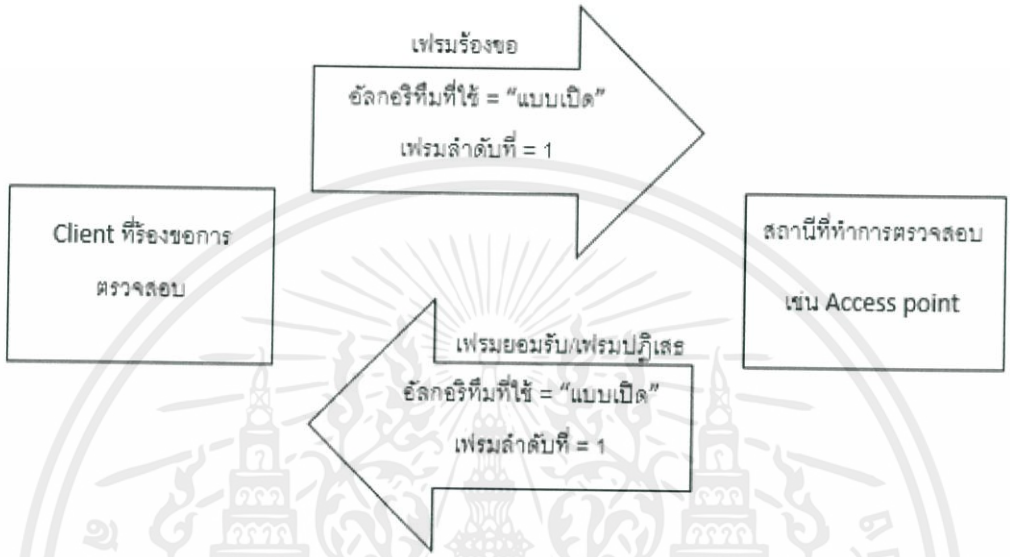
สภาวะที่ 1 ไคลเอนต์จะตรวจหาว่าแอกเซสพอยต์อยู่ในบริเวณใกล้เคียงหรือไม่ การตรวจหาแอกเซสพอยต์ มี 2 แบบ คือ Passive Scanning Mode และ Active Scanning Mode ในส่วนของ Passive Scanning Mode ไคลเอนต์ที่ต้องการเชื่อมต่อจะทำการรอฟังเฟรมบีคอนที่ส่งออกมาโดยแอกเซสพอยต์

แต่ในกรณีของ Active Scanning Mode ไคลเอนต์จะทำการส่งเฟรมที่เรียกว่า เฟรมตรวจสอบ (Probing Frame) ซึ่งจะระบุชื่อของเครือข่ายที่ต้องการเข้าร่วมไว้ในเฟรมที่ส่งไปด้วย จากนั้นก็รอให้มีการตอบกลับมาจากแอกเซสพอยต์ที่มีชื่อเครือข่ายตรงกับที่ร้องขอ ถ้าได้รับการตอบกลับก็จะทำการพิสูจน์ตัวตนต่อไป

สภาวะที่ 2 เป็นสภาวะพิสูจน์ตัวตน ในมาตรฐาน IEEE 802.11 มีการพิสูจน์ตัวตนอยู่ 2 แบบ คือ Open System Authentication และ Share Key Authentication มีรายละเอียดดังนี้

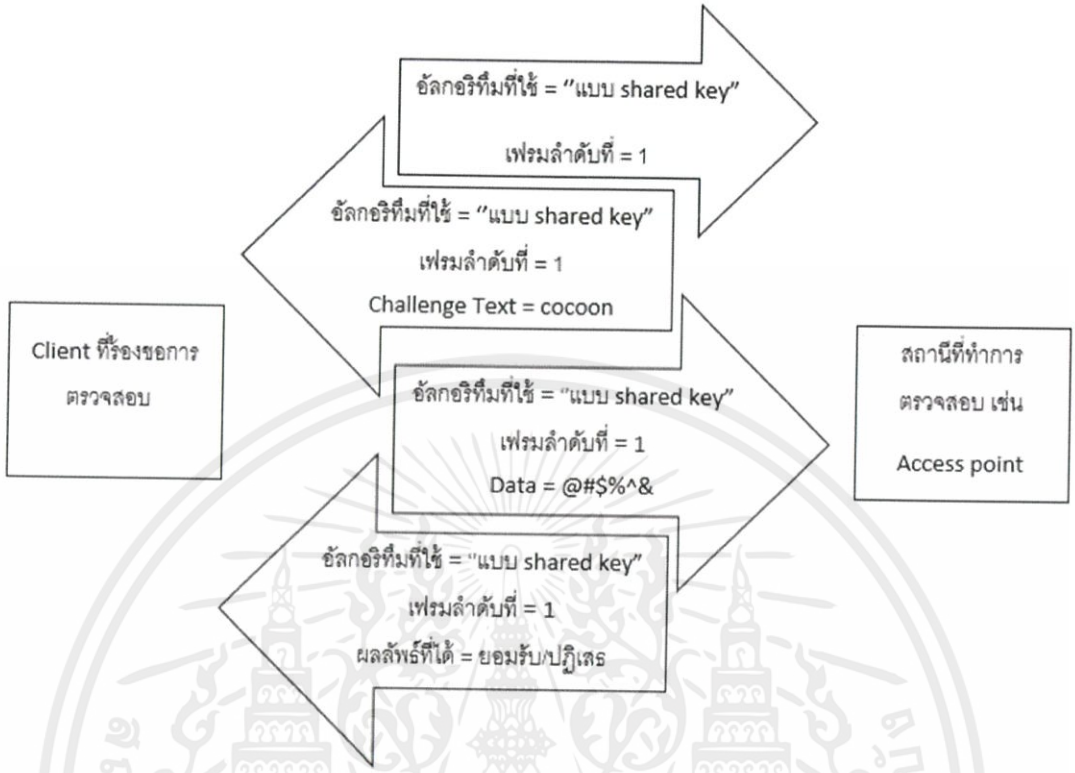
1. Open System Authentication เป็นการพิสูจน์ตัวตนอย่างง่าย โดยไคลเอนต์จะส่งเฟรมร้องขอ (Probe Request) ที่บรรจุประเภทของการพิสูจน์ตัวตน พร้อมด้วยชื่อของเครือข่ายที่ต้องการเข้าร่วม เมื่อแอกเซสพอยต์ได้รับเฟรมร้องขอดังกล่าว ก็จะทำการตรวจสอบชื่อผู้ร้องขอกับ

ฐานข้อมูลที่มี ถ้าพบก็ทำการตอบกลับด้วย Acceptance Frame แต่ถ้าไม่พบก็ตอบกลับด้วย Reject Frame ดังแสดงในรูปที่ 2.7



รูปที่ 2.7 การพิสูจน์ตัวตนแบบเปิด

2. Share Key Authentication เป็นการพิสูจน์ตัวตนแบบใช้คีย์ ไคลเอนต์จะทำการส่งเฟรมร้องขอการตรวจสอบที่บรรจุประเภทของการพิสูจน์ตัวตนไปยังแอกเซสพอยต์ เมื่อแอกเซสพอยต์ได้รับเฟรมร้องขอ แอกเซสพอยต์จะทำการสร้างคีย์ขึ้นมา แล้วบรรจุลงไปในเฟรมแล้วส่งกลับไปหาไคลเอนต์ จากนั้นไคลเอนต์จะนำเอาคีย์ที่ได้ไปทำการเข้ารหัส ด้วยคีย์ที่ทราบระหว่างไคลเอนต์และแอกเซสพอยต์เท่านั้น จากนั้นก็ส่งเฟรมที่ได้กลับไปหาแอกเซสพอยต์ หลังจากนั้นแอกเซสพอยต์จะทำการถอดรหัสข้อความดังกล่าวด้วยคีย์ที่ทราบระหว่างไคลเอนต์และแอกเซสพอยต์เท่านั้น หากได้คีย์เดิมที่สร้างขึ้นอย่างถูกต้องแสดงว่าไคลเอนต์มีสิทธิการเข้าร่วมเครือข่าย แอกเซสพอยต์ก็จะส่งเฟรมตอบรับกลับมา แสดงดังรูปที่ 2.8



รูปที่ 2.8 การพิสูจน์ตัวตนแบบ Shared Key

สภาวะที่ 3 การร้องขอร่วมเครือข่าย เมื่อผ่านกระบวนการพิสูจน์ตัวตนแล้ว ไคลเอนต์ก็จะส่งเฟรมร้องขอร่วมเครือข่าย (Association Request) ไปหาแอกเซสพอยต์ และแอก-เซสพอยต์จะตอบกลับมาด้วยเฟรมตอบรับการเข้าร่วมเครือข่าย (Association Response)

2.1.4 มาตรฐาน IEEE 802.11

Institute of Electrical and Electronics Engineers (IEEE) เป็นองค์กรกำหนดมาตรฐานการสื่อสารข้อมูลบนระบบเครือข่ายคอมพิวเตอร์ ซึ่งได้กำหนดมาตรฐานสำหรับเครือข่ายแลนไร้สายขึ้น คือ มาตรฐาน IEEE 802.11 และกำหนดมาตรฐานย่อยขึ้น คือ a, b, g, n, ac, ax และมาตรฐานอื่น ๆ โดยแต่ละมาตรฐานมีความเร็วและคลื่นความถี่สัญญาณที่แตกต่างกัน มีรายละเอียดดังนี้

2.1.4.1 มาตรฐาน IEEE 802.11a

มาตรฐาน IEEE 802.11a ทำงานที่ย่านความถี่ 5 GHz มีความเร็วในการรับส่งข้อมูล 54 Mbps สามารถทำการแพร่ภาพวิดีโอและข้อมูลที่ต้องการความละเอียดสูงได้ โดยอัตราความเร็วในการรับส่งข้อมูลสามารถปรับระดับให้ช้าลงได้ เพื่อเพิ่มระยะทางการเชื่อมต่อให้มากขึ้น เช่น 54, 48, 36, 24 และ 11 Mbps เป็นต้น

2.1.4.2 มาตรฐาน IEEE 802.11b

มาตรฐาน IEEE 802.11b ทำงานที่ย่านความถี่ 2.4 GHz มีความเร็วในการรับส่งข้อมูล 11 Mbps แลนไร้สายที่มาตรฐาน 802.11b ใช้ในองค์กรธุรกิจ สถาบันการศึกษา สถานที่สาธารณะและที่พักอาศัย มาตรฐานนี้มีระบบเข้ารหัสข้อมูลแบบ WEP ที่ 128 บิต

2.1.4.3 มาตรฐาน IEEE 802.11g

มาตรฐาน IEEE 802.11g ใช้งานที่ย่านความถี่ 2.4 GHz สามารถรับส่งข้อมูลที่ความเร็ว 36-54 Mbps ซึ่งเป็นความเร็วที่สูงกว่ามาตรฐาน 802.11b อยู่ 25-43 Mbps โดยมาตรฐาน 802.11g สามารถปรับระดับความเร็วในการสื่อสารลงเหลือ 2 Mbps ได้ (ตามสภาพแวดล้อมของเครือข่ายที่ใช้งาน)

2.1.4.4 มาตรฐาน IEEE 802.11n

มาตรฐาน IEEE 802.11n ใช้งานที่ย่านความถี่ 2.4 และ 5 GHz ได้รองรับความเร็วตั้งแต่ 300-450 Mbps โดยมีเสาสัญญาณตั้งแต่ 2-3 เสา บนตัวอุปกรณ์กระจายสัญญาณแลนไร้สาย หากผู้ใช้ต้องการใช้งาน เครื่องคอมพิวเตอร์พกพาหรืออุปกรณ์เคลื่อนที่ต้องรองรับมาตรฐาน 802.11n ด้วยเช่นกัน มาตรฐาน 802.11n สามารถทำงานร่วมกับ 802.11b แต่ทำให้ประสิทธิภาพทั้งระบบลดลง

2.1.4.5 มาตรฐาน IEEE 802.11ac

มาตรฐาน IEEE 802.11ac เป็นมาตรฐานที่พัฒนามาจาก 802.11n ซึ่งช่วยให้สามารถรับส่งสัญญาณได้เร็วขึ้น โดยมีคุณสมบัติคือ รองรับจำนวนผู้ใช้ต่อแอกเซสพอยต์ได้มากขึ้น สัญญาณมีความเสถียร และสามารถส่งข้อมูลได้พร้อมกันหลายย่านความถี่บนช่องสัญญาณที่กว้างมากขึ้น

2.1.4.6 มาตรฐาน IEEE 802.11ax

มาตรฐาน IEEE 802.11ax เป็นมาตรฐานที่พัฒนามาจาก 802.11ac ที่รองรับการรับส่งข้อมูลแบบ MIMO (Multiple-input-multiple-output) โดยเพิ่มประสิทธิภาพในการรับส่งข้อมูลบนช่องสัญญาณขนาด 80 MHz ด้วยความเร็ว 1.6 Gbps และช่องสัญญาณขนาด 160 MHz ด้วยความเร็ว 3.5 Gbps ซึ่งมาตรฐาน 802.11ax ยังคงใช้ช่วงคลื่นความถี่ 5 GHz

2.1.5 ระบบรักษาความปลอดภัยบนเครือข่าย Wi-Fi

เครือข่าย Wi-Fi มาตรฐาน IEEE 802.11 มีจุดอ่อนในการรักษาความปลอดภัยในช่วงเริ่มต้น หลังจากนั้นได้มีการพัฒนาระบบรักษาความปลอดภัยเพิ่มขึ้นทำให้ปัจจุบันมีเทคโนโลยีที่รองรับการใช้งานได้อย่างมีประสิทธิภาพ มีรายละเอียดของเทคโนโลยีการรักษาความปลอดภัยสำหรับมาตรฐาน IEEE 802.11 ดังนี้

2.1.5.1 Wired Equivalent Privacy (WEP)

เป็นระบบการเข้ารหัสข้อมูลสำหรับมาตรฐาน IEEE 802.11 ที่ใช้อัลกอริทึมในการเข้ารหัสแบบอาร์ซีโฟร์ (RC4) มีการเข้ารหัส 2 รูปแบบ คือ การเข้ารหัสแบบ 64 บิต และการเข้ารหัสแบบ 128 บิต หลักการของ WEP ได้กำหนดให้ระดับความปลอดภัยของเครือข่ายไร้สายเทียบเท่ากับเครือข่ายแบบใช้สาย การทำงานของ WEP แบ่งเป็น 2 ส่วนหลัก ๆ คือ

1. การเข้ารหัสข้อมูล (Encryption) เพื่อป้องกันไม่ให้ผู้อื่นเข้าใจหรือเปลี่ยนแปลงข้อมูลที่อยู่ในการสื่อสารไร้สายได้

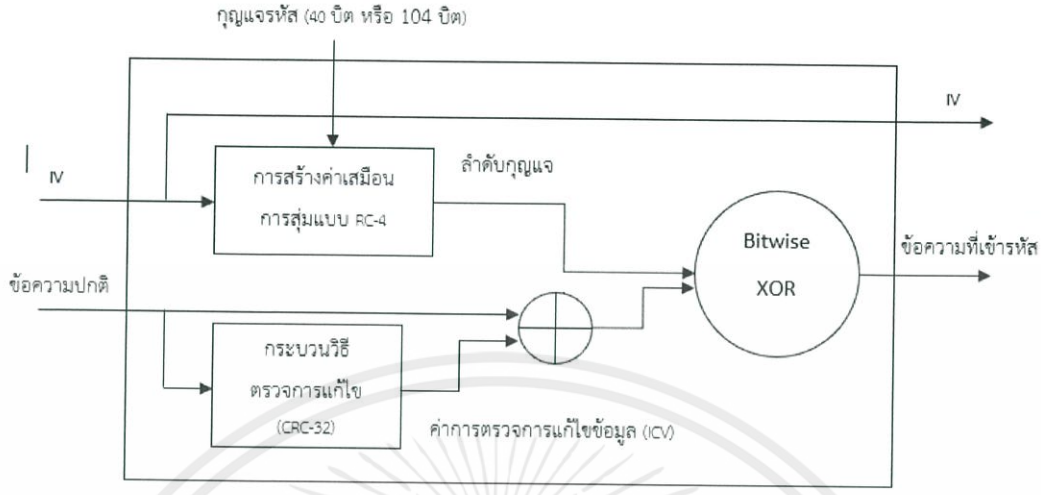
2. การตรวจสอบผู้ใช้ เพื่อป้องกันมิให้ผู้ที่ไม่มีรหัสผ่านสามารถเข้าใช้เครือข่ายได้ มีรายละเอียดดังต่อไปนี้

1) การเข้าและถอดรหัสข้อมูล (WEP Encryption/Decryption)

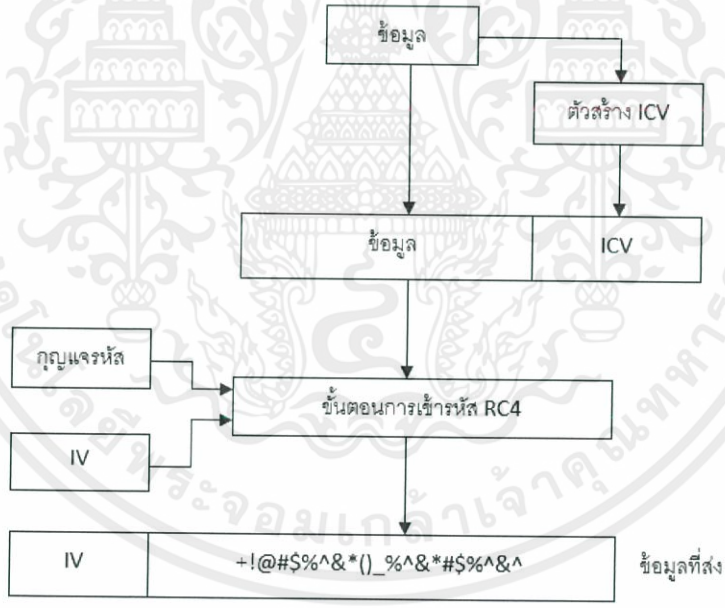
WEP ใช้หลักการในการเข้ารหัสและถอดรหัสข้อมูลที่เป็นแบบ Symmetrical โดยมีหลักการคือ รหัสที่ใช้สำหรับการเข้ารหัสข้อมูลจะเป็นรหัสชุดเดียวกับรหัสที่ใช้สำหรับการถอดรหัสข้อมูล การทำงานของการเข้ารหัสข้อมูลในกลไก WEP เป็นดังนี้

รูปที่ 2.9 แสดงองค์ประกอบของ WEP ฝั่งส่ง รูปที่ 2.10 แสดงขั้นตอนการทำงานของ WEP ฝั่งส่งข้อมูล โดยการทำงานเริ่มจากการนำข้อความปกติมาผ่านกระบวนการวิธีในการสร้างค่าซีอาร์ซี (32-bit Cyclic Redundant Check) ที่ใช้ในการตรวจการแก้ไขข้อมูล ที่เรียกว่า ไอซีวี (ICV : Integrity Check Value) ขนาด 32 บิต จากนั้นนำค่าไอซีวีไปรวมกับข้อความปกติ

ในขณะเดียวกันก็นำค่าเวกเตอร์เริ่มต้นหรือค่าไอวี (IV : Initialization Vector) ขนาด 24 บิต พร้อมกับค่ากุญแจรหัส (40 บิต และ 104 บิต ตามความปลอดภัยที่ผู้ใช้ต้องการ) ป้อนผ่านตัวสร้างค่าเสมือนการสุ่ม (Pseudo-Random Generator) ด้วยการเข้ารหัสแบบอาร์ซีโฟร์ ซึ่งผลลัพธ์ที่ได้คือลำดับกุญแจรหัส (Key Sequence) ที่จะนำไปผ่านกระบวนการ Exclusive-OR แบบทีละบิตกับค่าข้อมูลที่รวมกับไอซีวี ผลลัพธ์จะได้ข้อความที่เข้ารหัสแล้วเป็นค่าที่ใช้ในการสื่อสารโดยการจัดส่งไปพร้อมกันกับค่าเวกเตอร์เริ่มต้น (ซึ่งเป็นส่วนที่ไม่ได้เข้ารหัส)



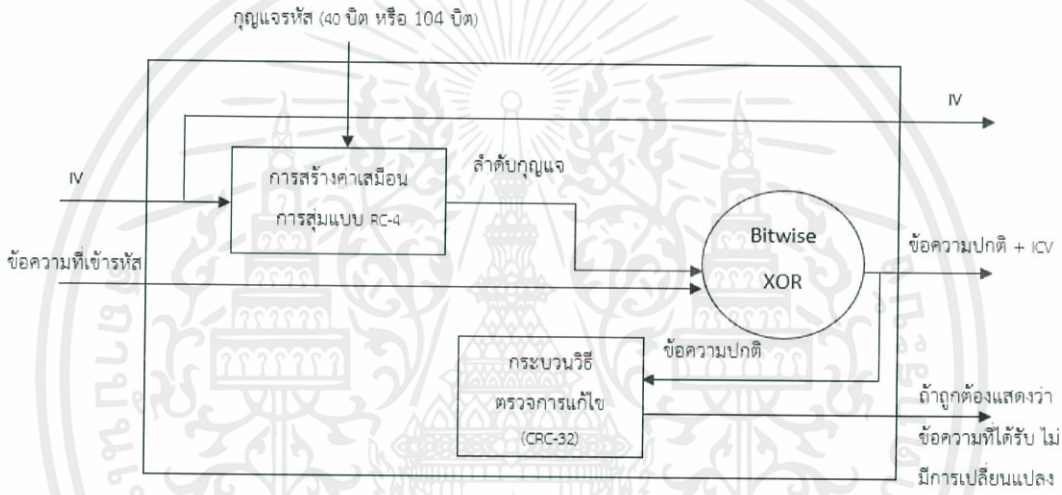
รูปที่ 2.9 แผนภาพองค์ประกอบของ WEP ฝั่งส่งข้อมูล



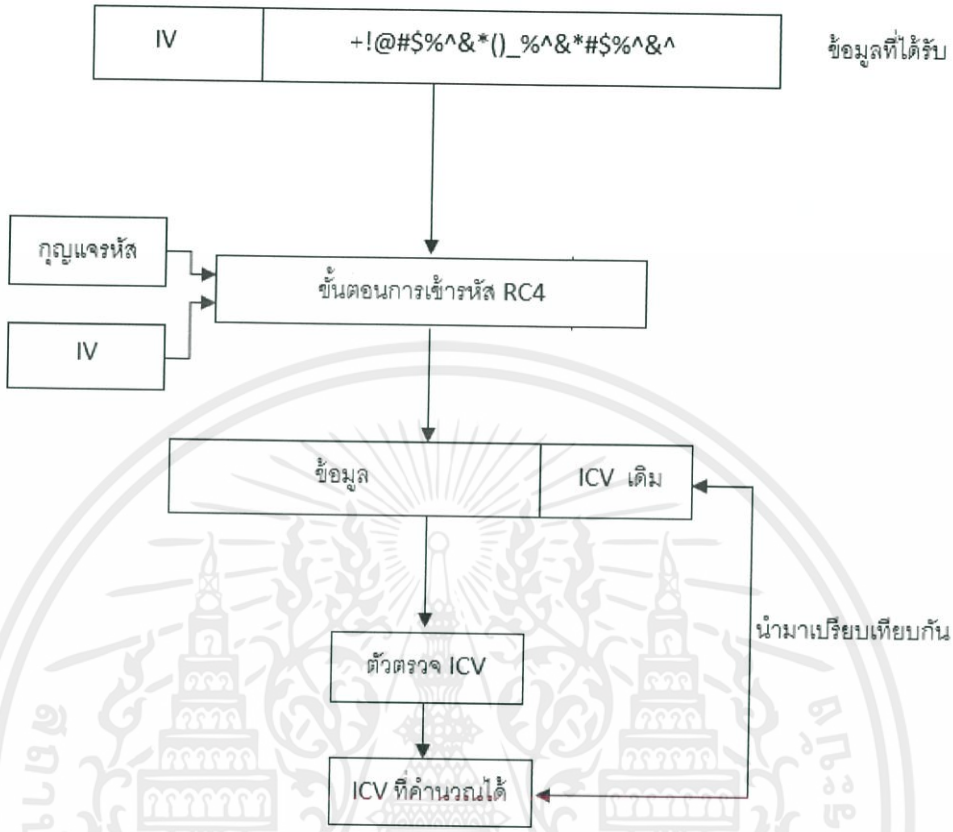
รูปที่ 2.10 แผนภาพขั้นตอนการทำงานของ WEP ฝั่งส่งข้อมูล

ทางฝั่งรับข้อมูลก็อาศัยหลักการเดียวกันในการถอดรหัสข้อมูลที่ได้รับมา โดยหลังจากการนำข้อความที่เข้ารหัสที่ได้รับมา ป้อนเข้ากระบวนการ XOR ก็จะได้ค่าข้อความปกติที่ฝั่งส่งต้องการสื่อสาร จากนั้นจะนำข้อมูลที่ได้รับมาทำการตรวจสอบค่าซีอาร์ซี ถ้าถูกต้องแสดงว่าข้อความที่ได้รับไม่ได้มีการเปลี่ยนแปลงแก้ไขในระหว่างทางก่อนถึงผู้รับ ดังรูปที่ 2.11 แสดงแผนภาพองค์ประกอบของ WEP ฝั่งรับข้อมูล และรูปที่ 2.12 แสดงขั้นตอนการทำงานของ WEP ฝั่งรับข้อมูล

เนื่องจากในมาตรฐาน WEP มีการใช้ค่าเพียง IV 24 บิต และมีการใช้คีย์ชุดเดียวกันในการเข้าและถอดรหัสข้อมูล ทำให้ผู้บุกรุกสามารถคาดการณ์รหัสผ่านได้ ซึ่งเป็นจุดอ่อนของ WEP



รูปที่ 2.11 แผนภาพองค์ประกอบของ WEP ฝั่งรับข้อมูล



รูปที่ 2.12 แผนภาพขั้นตอนการทำงานของ WEP ฝั่งส่งข้อมูล

2.1.5.2 Wi-Fi Protected Access

เป็นวิธีการเข้ารหัสที่มีการพัฒนามาพร้อมกับมาตรฐาน IEEE 802.11b หรือ Wi-Fi มีการพัฒนาอย่างต่อเนื่อง รายละเอียดการทำงานของ Wi-Fi Protected Access มีดังนี้

1) Wi-Fi Protected Access (WPA)

เป็นมาตรฐานความปลอดภัยข้อมูลที่พัฒนาขึ้นมาโดยองค์กร Wi-Fi Alliance (WECA) เพื่อแก้ไขจุดอ่อนของ WEP ในเรื่องการเข้ารหัสข้อมูลและถอดรหัสข้อมูลด้วย WEP Key โดยการนำเอา Dynamic Key Distribution และการตรวจสอบและพิสูจน์สิทธิผู้ใช้งาน IEEE 802.1X มาใช้ร่วมกันในมาตรฐาน WPA โดยจะมีโหมดการทำงานให้เลือก 2 โหมด ดังนี้

- WPA Temporal Key Integrity Protocol (TKIP) คือ เทคนิคการใช้คีย์ชั่วคราวเพื่อเข้ารหัส TKIP เป็นกลไกการเข้ารหัสที่ยังคงใช้เทคนิคอาร์ซีโฟร์เช่นเดียวกับ WEP แต่ได้มีการปรับปรุงการทำงานให้มีประสิทธิภาพที่ดีกว่า WEP ดังนี้

1.) ทุก ๆ แพ็กเก็ตข้อมูลที่สร้างขึ้นจากการสื่อสารระหว่างแอกเซสพอยต์กับเครื่องคอมพิวเตอร์ไร้สายจะถูกเข้ารหัสด้วยคีย์ที่แตกต่างกัน (Dynamic Ciphering Keys) ทำให้ยากแก่การคาดการณ์คีย์ที่ถูกต้อง

2.) ใช้กลไก Message Integrity Checking (MIC) เพื่อทำให้แน่ใจว่าข้อมูลที่อยู่ระหว่างการสื่อสารจะไม่ถูกปลอมแปลงจากผู้บุกรุก

3.) จำนวนบิต IV ขนาด 48 บิต ซึ่งสูงกว่า IV ของ WEP ที่มีจำนวนแค่ 24 บิต (ค่า IV นี้ถูกนำไปรวมกับคีย์ที่ผู้ใช้ต้องใส่เพื่อใช้สำหรับการเข้ารหัสและถอดรหัส) การที่มีจำนวนบิตมากกว่าทำให้การพิจารณาค่านี้ทำได้ยากขึ้น

- WPA Enterprise โหมดการทำงานนี้ใช้อัลกอริทึมการเข้ารหัสและถอดรหัสข้อมูลโดยใช้ RADIUS Server ทำหน้าที่คอยตรวจสอบและพิสูจน์สิทธิผู้ใช้งานก่อนการเชื่อมต่อคอมพิวเตอร์ไร้สายเข้าสู่ระบบ และในระหว่างการสื่อสารข้อมูลของแอกเซสพอยต์กับเครื่องคอมพิวเตอร์ไร้สายข้อมูลจะถูกเข้ารหัสด้วยคีย์ที่แตกต่างกัน และคีย์การเข้ารหัสจะถูกเปลี่ยนไปเรื่อย ๆ โดยอัตโนมัติ

2) Wi-Fi Protected Access version 2 (WPA2)

WPA2 ถูกพัฒนาขึ้นโดยวิธีการเข้ารหัสแบบ AES (Advanced Encryption Standard) ด้วยกุญแจขนาด 128 บิต 192 บิต หรือ 256 บิต เทคโนโลยี AES เป็นรูปแบบของการเข้ารหัสข้อมูลแบบใหม่แทนการใช้อัลกอริทึมอาร์ซีโฟร์ โดย AES ใช้อัลกอริทึม Rijndale ซึ่งกำหนดความยาวของคีย์ในการเข้ารหัสเป็น 3 รูปแบบ คือ การเข้ารหัสแบบ 128 บิต 192 บิต และ 256 บิต ซึ่งอัลกอริทึมของ AES ทำงานโดยมีเซิร์ฟเวอร์เป็นศูนย์กลางที่สามารถส่งคีย์ได้โดยอัตโนมัติเรียกว่า Centralized Encryption Key Server องค์ประกอบอีกส่วนของ AES คือ CCM (Counter mode-CBC MAC) โดย CCM ใช้ Counter เพื่อเปลี่ยนแปลงตัวเลขของข้อมูลหลังการเข้ารหัสในแต่ละครั้งไม่ให้เหมือนกัน เพื่อไม่ให้ได้ Ciphertext ที่เหมือนกัน ดังนั้น AES จึงใช้แทนวิธีเข้ารหัสแบบเดิมที่ใช้อาร์ซีโฟร์และ IV จึงสามารถแก้ปัญหาของ WEP และ WPA ได้

ดังนั้น WPA2 ได้ยกเลิกการใช้อาร์ซีโฟร์ และ IV ที่เป็นพื้นฐานของ WEP และ WPA ทำให้การบุกรุกเข้าระบบทำได้ยากกว่า WEP และ WPA

- WPA2 Personal เป็นการสร้างการพิสูจน์ตัวตนเสมือน ระหว่างผู้ใช้และแอกเซสพอยต์ ด้วย PSK (Pre Share Key) หรือ PMK (Pairwise Master Key) ซึ่ง PMK ที่สร้างขึ้นจะเหมือนกันในทุก ๆ เครื่องลูกข่าย โดยที่ PTK (Pairwise Transient Key) จะถูกสร้างขึ้นต่อ

จาก PMK เพื่อสร้างช่องทางเชื่อมต่อสำหรับส่งรหัสผ่าน โดย WPA2 Personal จะใช้การพิสูจน์ตัวตนที่อ้างอิงอุปกรณ์เป็นหลักระหว่างเครื่องลูกข่ายและแอกเซสพอยต์

- WPA2 Enterprise เป็นการเชื่อมต่อด้วยมาตรฐาน 802.1X บนโปรโตคอลที่ชื่อ RADIUS ใช้การเข้ารหัสด้วยกุญแจขนาด 128 บิต และเข้ารหัสเป็นลักษณะของ fixed-length data block คือจะเข้ารหัสข้อมูลทีละ 128 บิต จนครบทุก data block ทำให้การเข้ารหัสมีความปลอดภัยมากกว่า WPA มีการเข้ารหัสแบบไดนามิค (Dynamic) ซึ่งมีความซับซ้อน มีกระบวนการในการตรวจสอบความถูกต้องในการถอดรหัสข้อมูลที่ปลอดภัยขึ้น

3) Wi-Fi Protected Access version 3 (WPA3)

เนื่องจากมาตรฐานการเข้ารหัส WPA2 มีช่องโหว่ ที่ชื่อว่า KRACK (Key Reinstallation Attacks) เป็นการโจมตีกระบวนการ 4-Way Handshake ของ WPA2 ซึ่งการ KRACK ไม่ได้ช่วยให้ผู้บุกรุกทราบรหัสผ่านของ Wi-Fi แต่ช่วยให้สามารถถอดรหัสข้อมูล Wi-Fi จึงทำให้มีการพัฒนาการเข้ารหัส WPA3 โดยมีวิธีการพิสูจน์ตัวตนและใช้เทคโนโลยีการเข้ารหัสที่ปลอดภัยยิ่งขึ้น โดยการทำงานของ WPA3 จะแบ่งออกเป็น 3 โหมดหลัก ๆ ได้แก่

- WPA3 Personal เป็นการป้องกันการคาดเดารหัสผ่าน ยกตัวอย่างเช่น Dictionary-Attack ที่ผู้บุกรุกใช้คลังคำศัพท์เป็นฐานข้อมูลในการคาดเดารหัสผ่าน โดยใช้การป้องกันใหม่ที่ชื่อว่า Simultaneous Authentication of Equals (SAE)

- WPA3 Enterprise ใช้กับองค์กร หน่วยงานรัฐ สถาบันการเงิน ที่ต้องการความปลอดภัยสูง โดยใช้การเข้ารหัสความปลอดภัยอย่างน้อย 192 บิต อีกทั้งมีการเข้ารหัสที่ดียิ่งขึ้นเพื่อปกป้องข้อมูลที่สำคัญ

- Wi-Fi Easy Connect จับคู่การสื่อสารกับอุปกรณ์ที่ไม่มีหน้าจอแสดงผล ยกตัวอย่างเช่น อุปกรณ์ IoT กับแอกเซสพอยต์ โดยจะนำมาใช้แทนที่ Wi-Fi Protected Setup (WPS) ที่มีช่องโหว่ที่ไม่ปลอดภัย โดยผู้ใช้สแกนโค้ด QR ผ่านโทรศัพท์เคลื่อนที่ก็สามารถเชื่อมต่ออุปกรณ์นั้นได้ทันที

2.2 ระปฏิบัติการ Kali Linux

ระบบปฏิบัติการ Kali Linux เป็นระบบปฏิบัติการที่ถูกสร้างขึ้นมาเพื่อใช้ทดสอบความปลอดภัยของระบบ ซึ่งจะมีเครื่องมือต่าง ๆ ที่จำเป็นต่อการทดสอบความปลอดภัยของระบบ โดยมีเครื่องมือที่ใช้ในปริญญานิพนธ์ ดังนี้

2.2.1 Wireshark

เป็นโปรแกรมจำพวกดักจับข้อมูล (Packet Sniffer) ประกอบไปด้วยส่วนของการดักจับแพ็กเก็ต (Packet Capture) และส่วนการวิเคราะห์แพ็กเก็ต (Packet Analyzer) ซึ่งทำหน้าที่ในการวิเคราะห์ระบบเครือข่าย

2.2.2 Airodump-ng

เป็นเครื่องมือที่ใช้ค้นหาบริการเครือข่าย Wi-Fi และจะแสดงรายละเอียดของบริการเครือข่าย Wi-Fi ที่อยู่ในบริเวณนั้น เช่น ชื่อเครือข่าย และ MAC Address เป็นต้น

2.2.3 Aircrack-ng

เป็นเครื่องมือที่ใช้สำหรับดักจับข้อมูลของบริการเครือข่าย Wi-Fi สามารถใช้ในการถอดรหัส (Crack) ข้อมูลที่เข้ารหัสในรูปแบบของ WEP, WPA และ WPA2

2.2.4 Aireplay-ng

เป็นเครื่องมือที่ใช้ในการส่งเฟรม Deauthentication ให้กับทุกไคลเอนต์ที่เชื่อมต่ออยู่กับแอกเซสพอยต์เป้าหมาย เพื่อให้ไคลเอนต์ทั้งหมดยกเลิกการเชื่อมต่อกับแอกเซสพอยต์

2.2.5 Macchanger

เป็นคำสั่งเปลี่ยน MAC Address ของไวเลสการ์ด

2.3 Web Application

ในการออกแบบหน้าเว็บแอปพลิเคชัน มีการออกแบบโดยใช้ภาษาเอชทีเอ็มแอล และใช้เชลล์สคริปต์ในการเขียนคำสั่ง

2.3.1 เอชทีเอ็มแอล

เอชทีเอ็มแอล คือภาษาคอมพิวเตอร์ที่ใช้ในการแสดงผลของเอกสารบนเว็บไซต์หรือที่เรียกกันว่าเว็บเพจ สำหรับการสร้างเว็บเพจโดยภาษาเอชทีเอ็มแอลสามารถทำโดยใช้โปรแกรม Text Editor ต่าง ๆ หรือโปรแกรมที่เป็นเครื่องมือช่วยสร้างเว็บเพจ เช่น Dreamweaver ส่วนการเรียกใช้งานหรือทดสอบการทำงานของเอกสารเอชทีเอ็มแอล จะใช้โปรแกรม Internet Web Browser เช่น Internet Explorer (IE), Mozilla Firefox และ Google Chrome เป็นต้น

2.3.2 CGI (Common Gateway Interfaces)

CGI เป็นสิ่งที่ใช้กำหนดวิธีการจัดการข้อมูลระหว่างเว็บเซิร์ฟเวอร์และเว็บเบราว์เซอร์ ซึ่ง CGI เป็นวิธีการมาตรฐานสำหรับเว็บเซิร์ฟเวอร์ เพื่อที่จะส่งคำร้องขอจากผู้ใช้ไปยังโปรแกรมบนเว็บเซิร์ฟเวอร์ โดยให้โปรแกรมทำการประมวลผลข้อมูล จากนั้นเว็บเซิร์ฟเวอร์ก็จะรับข้อมูลส่งกลับไปให้ผู้ใช้ โดยส่วนประกอบของ CGI จะประกอบด้วย 2 ส่วน คือ

1. การสร้างแบบฟอร์มการรับข้อมูลจากผู้ใช้ โดยการใช้ Tag ของเอชทีเอ็มแอล สำหรับการสร้างแบบฟอร์มและปุ่มควบคุมการตอบรับ (Submit)

2. การเขียน CGI Script เก็บไว้ที่เครื่องเซิร์ฟเวอร์ ดังนั้นเมื่อผู้ใช้กดปุ่มตอบรับ CGI Script จะเริ่มทำงาน โดยจะทำหน้าที่รวบรวมข้อมูลจากแบบฟอร์มส่งให้กับเซิร์ฟเวอร์ เพื่อทำการประมวลผล รวมไปถึงการแสดงและสร้างผลลัพธ์ที่อยู่ในรูปแบบของไดนามิคเอชทีเอ็มแอลกลับไปยังเว็บเบราว์เซอร์ของผู้ใช้อีกด้วย

2.3.3 เชลล์สคริปต์ (shell script)

เชลล์คือโปรแกรมหนึ่งในระบบยูนิกซ์ (Unix) ที่ทำหน้าที่ติดต่อระหว่างผู้ใช้งานกับระบบปฏิบัติการ ซึ่งผู้ใช้สามารถสั่งงานยูนิกซ์ผ่านเชลล์เท่านั้น นอกจากนี้ยังมีคุณสมบัติของ Shell Programming Language ทำให้ผู้ใช้สามารถนำคำสั่งต่าง ๆ ของเชลล์มาเขียนโปรแกรมเก็บเป็นไฟล์ไว้ได้

บทที่ 3

การออกแบบและการจัดทำปริญญานิพนธ์

ในการจัดทำปริญญานิพนธ์มีวิธีการดังนี้ คือ ทำการทดลองหาช่องโหว่ โดยทดลองดักจับข้อมูล ค้นหา SSID ที่ถูกซ่อนไว้ ปลอมแปลง MAC Address ทดลองโจมตีแอกเซสพอยต์ที่ใช้การเข้ารหัสแบบ WEP และทดลองโจมตีแอกเซสพอยต์ที่ใช้การเข้ารหัสแบบ WPA จากนั้นทำการสร้างเว็บแอปพลิเคชันเพื่อให้สะดวกในการรันคำสั่งต่าง ๆ ตามที่ได้ศึกษามา และนำเว็บแอปพลิเคชันไปทดลองใช้งานจริง

3.1 เครื่องมือที่ใช้ในการทดลอง

3.1.1 อุปกรณ์ที่ใช้ในการทดลอง

3.1.1.1 โน้ตบุ๊กคอมพิวเตอร์

3.1.1.2 แอกเซสพอยต์

3.1.1.3 Wireless USB Adapter ยี่ห้อ ALFA รุ่น AWUS036AC

3.1.2 ระบบปฏิบัติการและโปรแกรมที่ใช้ในการทดลอง

3.1.2.1 ระบบปฏิบัติการ Kali Linux

3.1.2.2 Wireshark

3.1.2.3 Airodump-ng

3.1.2.4 Aircrack-ng

3.1.2.5 Aireplay-ng

3.1.2.6 Macchanger

3.1.3 ภาษาที่ใช้ในการสร้างเว็บแอปพลิเคชัน

3.1.3.1 เอชทีเอ็มแอล

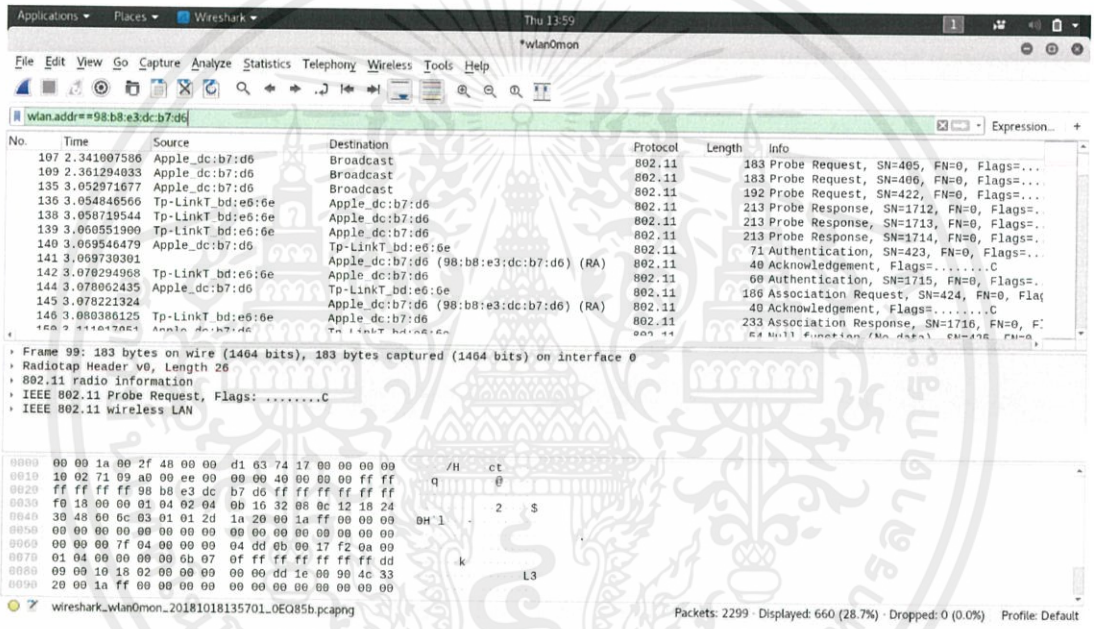
3.1.3.2 แบช

3.2 การออกแบบและการจัดเก็บผลการทดลอง

เป็นการออกแบบและจัดเก็บผลการทดลองในการศึกษาการหาช่องโหว่ของบริการเครือข่าย Wi-Fi โดยมีขั้นตอนต่าง ๆ ดังนี้

3.2.1 การดักจับข้อมูล

ทำการตั้งค่าแอกเซสพอยต์ เพื่อจำลองเป็นแอกเซสพอยต์เป้าหมายที่จะโดนดักจับข้อมูล โดยเปลี่ยน SSID (Service Set Identifier) เป็น wifi_test และตั้งค่า Authentication Type เป็น Disabled ซึ่งเป็นการ Authentication แบบ Open System Authentication จากนั้นตั้งค่าให้ Wireless USB Adapter ที่จะใช้ดักจับข้อมูล ใช้ช่องสัญญาณเดียวกับแอกเซสพอยต์ เพื่อให้สามารถดักจับข้อมูลได้ แล้วใช้ Wireshark ในการดักจับข้อมูล ทำให้เห็นการรับส่งข้อมูลของเครือข่ายทั้งหมดรวมถึงแอกเซสพอยต์ที่ใช้ในการทดลอง ดังแสดงในรูปที่ 3.1



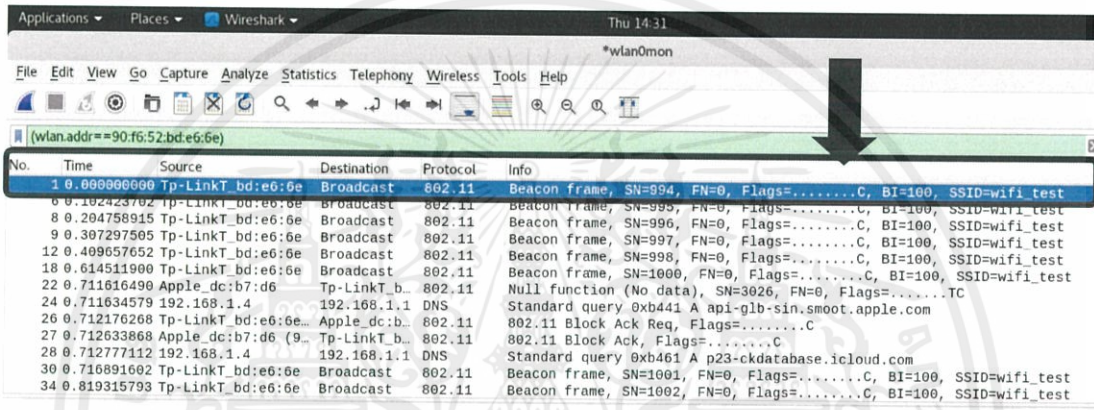
รูปที่ 3.1 แพ็กเก็ตที่ดักจับได้ของแอกเซสพอยต์ที่ทำการทดลอง

จากนั้น ทดลองเปิดเว็บเบราว์เซอร์ (Web browser) และพิมพ์ http://192.168.1.1 ในแถบที่อยู่ (Address Bar) โดย 192.168.1.1 เป็นเลขไอพี (IP) ของแอกเซสพอยต์ แล้วใส่ชื่อผู้ใช้ (Username) คือ admin และรหัสผ่าน คือ admin เพื่อเข้าไปสู่หน้าตั้งค่าของแอกเซสพอยต์ แล้วทดลองดักจับและวิเคราะห์แพ็กเก็ตที่ดักจับได้ ซึ่งจะทำให้ทราบชื่อผู้ใช้และรหัสผ่านที่ใช้สำหรับเข้าใช้งานการตั้งค่าแอกเซสพอยต์

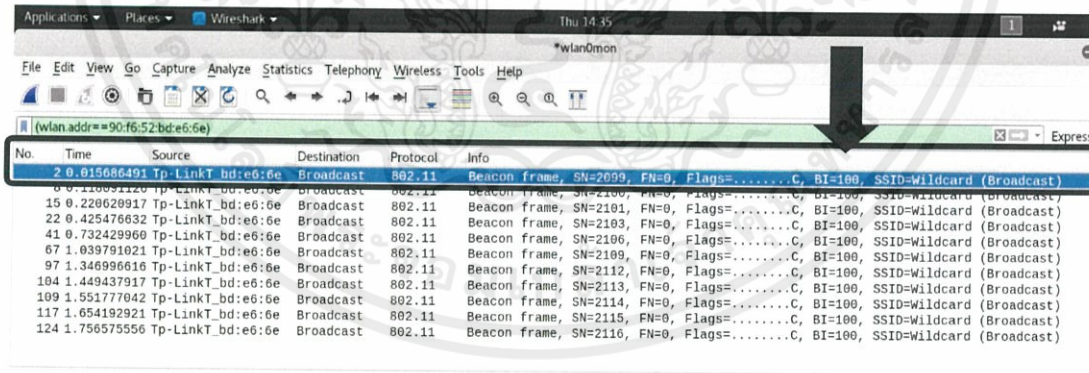
3.2.2 การค้นหา SSID ที่ถูกตั้งค่าให้ซ่อนไว้

ในแอกเซสพอยต์ที่ตั้งค่าให้แสดง SSID ตามปกตินั้น เมื่อใช้ Wireshark ในการดักจับข้อมูล แล้ววิเคราะห์เฟรมบีคอน (Beacon) ที่ถูกปล่อยออกมาจากแอกเซสพอยต์ จะพบ SSID ของแอกเซสพอยต์เป็น wifi_test ซึ่งอยู่ในรูปของเพลนเท็กซ์ (Plain Text) ดังรูปที่ 3.2

จากนั้นทำการตั้งค่าให้แอกเซสพอยต์ซ่อน SSID แล้วดักจับและวิเคราะห์ข้อมูลโดยใช้ Wireshark โดยสังเกตที่เฟรมบีคอน จะพบว่า SSID ได้ถูกซ่อนไว้ดังรูปที่ 3.3



รูปที่ 3.2 เฟรมบีคอนที่ได้จากการดักจับข้อมูลโดยใช้ Wireshark



รูปที่ 3.3 เฟรมบีคอนของแอกเซสพอยต์ที่ถูกตั้งค่าให้ซ่อน SSID

ในการที่จะทราบ SSID ที่ถูกซ่อนไว้นั้นจะต้องรอให้ไคลเอนต์ที่มีสิทธิในการเข้าใช้งานเชื่อมต่อกับแอกเซสพอยต์ ซึ่งในกระบวนการนี้จะมีการส่งเฟรม Probe Request และเฟรม Probe

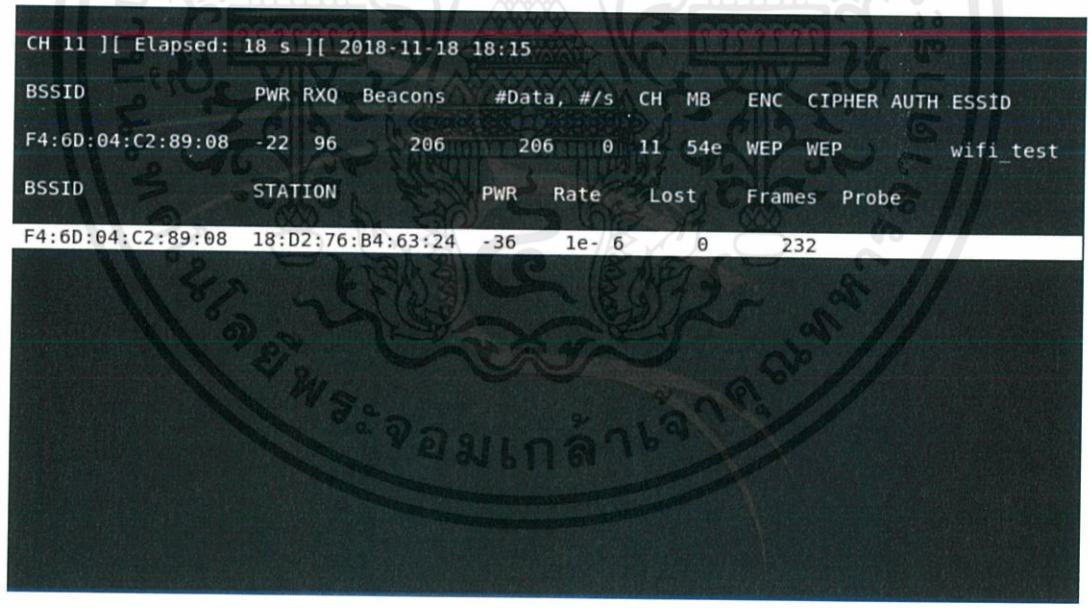
Response ซึ่งในเฟรมเหล่านี้จะมีการระบุ SSID อยู่ด้วย จึงทำให้สามารถทราบได้ว่าแอกเซสพอยต์มี SSID อะไรถึงแม้จะมีการตั้งค่าให้ซ่อนไว้ก็ตาม

อีกวิธีหนึ่งคือใช้ Aireplay-ng ในการส่งเฟรม Deauthentication ให้กับทุกไคลเอนต์ที่เชื่อมต่ออยู่กับแอกเซสพอยต์เป้าหมาย เพื่อบังคับให้ไคลเอนต์ทั้งหมดยกเลิกการเชื่อมต่อกับแอกเซสพอยต์ จากนั้นรอให้ไคลเอนต์เชื่อมต่อกับแอกเซสพอยต์อีกครั้ง ก็จะทำให้สามารถทราบ SSID ได้

3.2.3 Mac Address Filtering

ทำการตั้งค่าแอกเซสพอยต์ให้กรอง MAC Address ของเครื่องอุปกรณ์ โดยเมื่อเปิดใช้งานการกรอง MAC Address แอกเซสพอยต์จะให้เฉพาะ MAC Address ที่อนุญาตเท่านั้นที่จะสามารถเชื่อมต่อกับแอกเซสพอยต์ได้ แต่อุปกรณ์ที่ MAC Address ไม่ตรงกับที่ตั้งค่าไว้ว่าให้สามารถเชื่อมต่อแอกเซสเพอยต์ได้ หากพยายามเชื่อมต่อกับแอกเซสพอยต์ การเชื่อมต่อจะล้มเหลว

เพื่อให้สามารถเชื่อมต่อกับแอกเซสพอยต์ได้ อันดับแรกใช้ Airodump-ng เพื่อค้นหา MAC Address ของอุปกรณ์อื่นที่เชื่อมต่ออยู่กับแอกเซสพอยต์นั้น ดังรูปที่ 3.4



รูปที่ 3.4 MAC Address ของอุปกรณ์อื่นที่เชื่อมต่ออยู่กับแอกเซสพอยต์

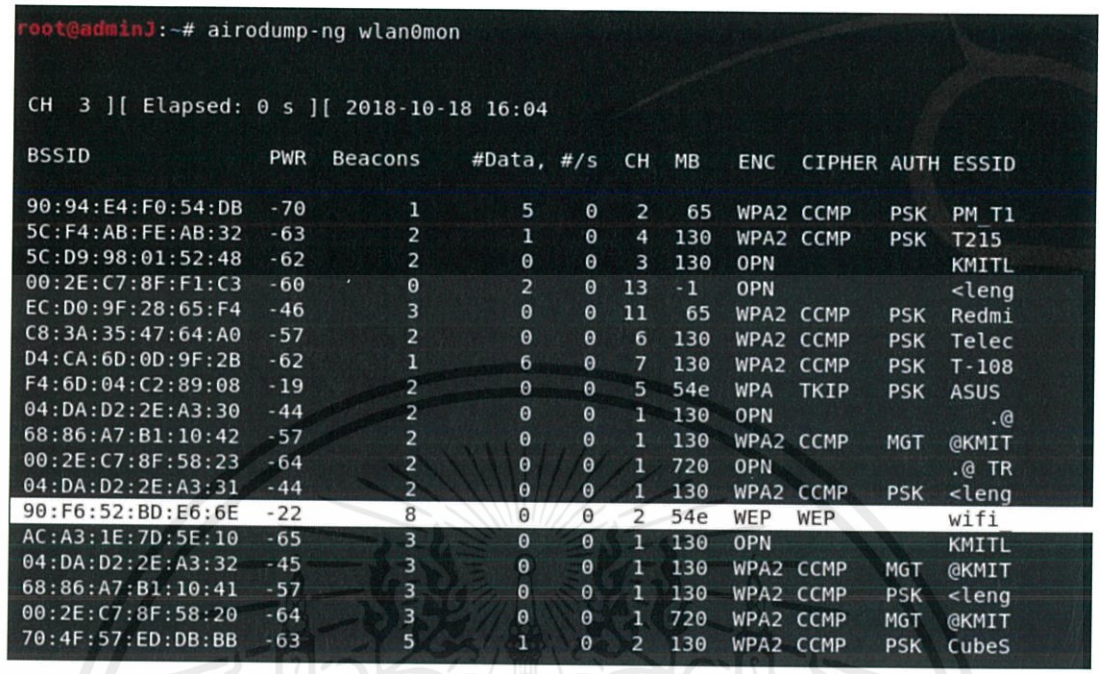
จากรูปที่ 3.4 จะเห็นว่ามีอุปกรณ์หนึ่งตัวที่เชื่อมต่ออยู่กับแอกเซสพอยต์ตัวนี้ ซึ่งอุปกรณ์ตัวนี้มี MAC Address คือ 18:D2:76:B4:63:24 เมื่อเจอ MAC Address ที่แอกเซสพอยต์อนุญาตให้เชื่อมต่อ จากนั้นจึงเปลี่ยน MAC Address ของอุปกรณ์ที่ไม่ได้รับการอนุญาตให้เชื่อมต่อให้เป็น MAC Address ที่แอกเซสพอยต์อนุญาตให้เชื่อมต่อ โดยใช้ Macchanger ดังรูปที่ 3.5

```
root@FAH:~# iwconfig
eth0      no wireless extensions.

wlan0     IEEE 802.11  ESSID:"KMITL-WIFI"
          Mode:Managed  Frequency:2.437 GHz  Access Point: 18:DE:D7:77:EE:21
          Bit Rate=6.5 Mb/s   Tx-Power=15 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=57/70  Signal level=-53 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0

lo        no wireless extensions.

root@FAH:~# ifconfig wlan0 down
root@FAH:~# macchanger -m 18:D2:76:B4:63:24 wlan0
Current MAC:   bc:77:37:73:c1:b2 (Intel Corporate)
Permanent MAC: bc:77:37:73:c1:b2 (Intel Corporate)
New MAC:       18:d2:76:b4:63:24 (unknown)
root@FAH:~# ifconfig wlan0 up
root@FAH:~#
```

รูปที่ 3.5 การปลอม MAC Address ของอุปกรณ์ที่ถูกกรองเป็น MAC Address ของอุปกรณ์ที่แอกเซสพอยต์อนุญาตให้เชื่อมต่อ

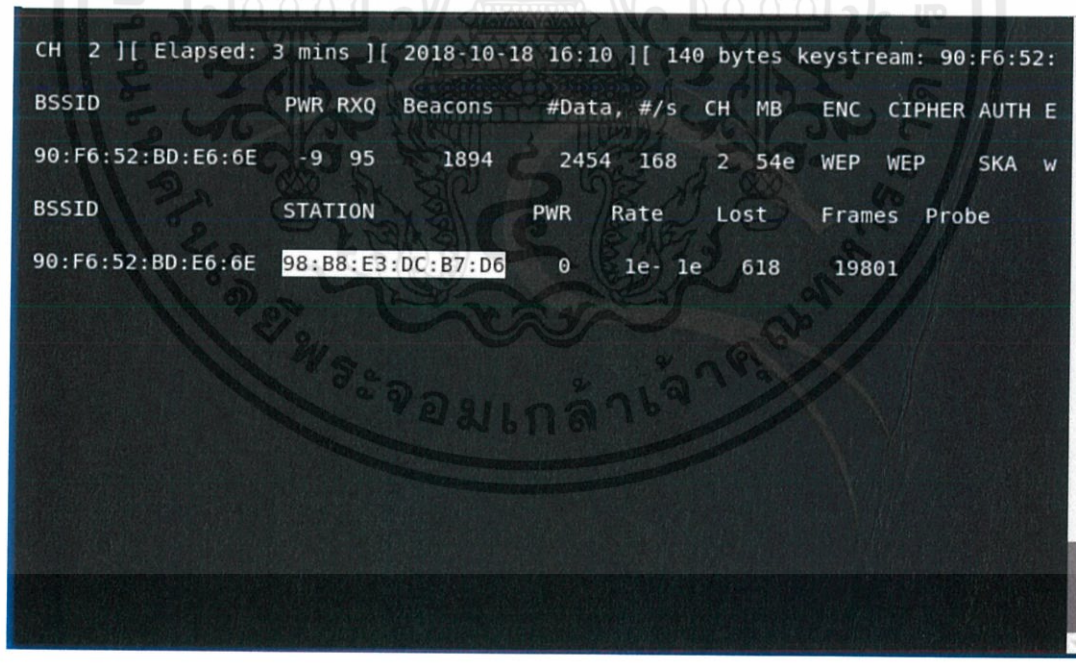
3.2.4 ทดลองโจมตีแอกเซสพอยต์ที่ใช้การเข้ารหัสแบบ WEP

ทำการตั้งค่าแอกเซสพอยต์ โดยตั้ง Authentication Type เป็น WEP-128 Bits และมีรหัสผ่านสำหรับการเชื่อมต่อแอกเซสพอยต์เป็น abcdefabcdefabcdefabcdef12 แล้วใช้ Airodump-ng ในการค้นหาแอกเซสพอยต์ที่ต้องการจะโจมตีและบันทึกข้อมูลแพ็กเก็ตที่ดักจับได้เก็บเป็นไฟล์ไว้ ดังรูปที่ 3.6 และ รูปที่ 3.7 ตามลำดับ จากนั้นใช้ Aircrack-ng ในการคำนวณหารหัสผ่านจากไฟล์ข้อมูลที่ดักจับมาได้



```
root@adminJ:~# airodump-ng wlan0mon

CH  3 ][ Elapsed: 0 s ][ 2018-10-18 16:04

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

90:94:E4:F0:54:DB  -70        1        5    0   2   65  WPA2 CCMP   PSK  PM_T1
5C:F4:AB:FE:AB:32  -63        2        1    0   4  130  WPA2 CCMP   PSK  T215
5C:D9:98:01:52:48  -62        2        0    0   3  130  OPN              KMITL
00:2E:C7:8F:F1:C3  -60        0        2    0  13  -1   OPN              <leng
EC:D0:9F:28:65:F4  -46        3        0    0  11   65  WPA2 CCMP   PSK  Redmi
C8:3A:35:47:64:A0  -57        2        0    0   6  130  WPA2 CCMP   PSK  Telec
D4:CA:6D:0D:9F:2B  -62        1        6    0   7  130  WPA2 CCMP   PSK  T-108
F4:6D:04:C2:89:08  -19        2        0    0   5  54e  WPA  TKIP   PSK  ASUS
04:DA:D2:2E:A3:30  -44        2        0    0   1  130  OPN              .@
68:86:A7:B1:10:42  -57        2        0    0   1  130  WPA2 CCMP   MGT  @KMIT
00:2E:C7:8F:58:23  -64        2        0    0   1  720  OPN              .@ TR
04:DA:D2:2E:A3:31  -44        2        0    0   1  130  WPA2 CCMP   PSK  <leng
90:F6:52:BD:E6:6E  -22        8        0    0   2  54e  WEP  WEP         wifi
AC:A3:1E:7D:5E:10  -65        3        0    0   1  130  OPN              KMITL
04:DA:D2:2E:A3:32  -45        3        0    0   1  130  WPA2 CCMP   MGT  @KMIT
68:86:A7:B1:10:41  -57        3        0    0   1  130  WPA2 CCMP   PSK  <leng
00:2E:C7:8F:58:20  -64        3        0    0   1  720  WPA2 CCMP   MGT  @KMIT
70:4F:57:ED:DB:BB  -63        5        1    0   2  130  WPA2 CCMP   PSK  CubeS
```

รูปที่ 3.6 ผลการค้นหาแอกเซสพอยต์

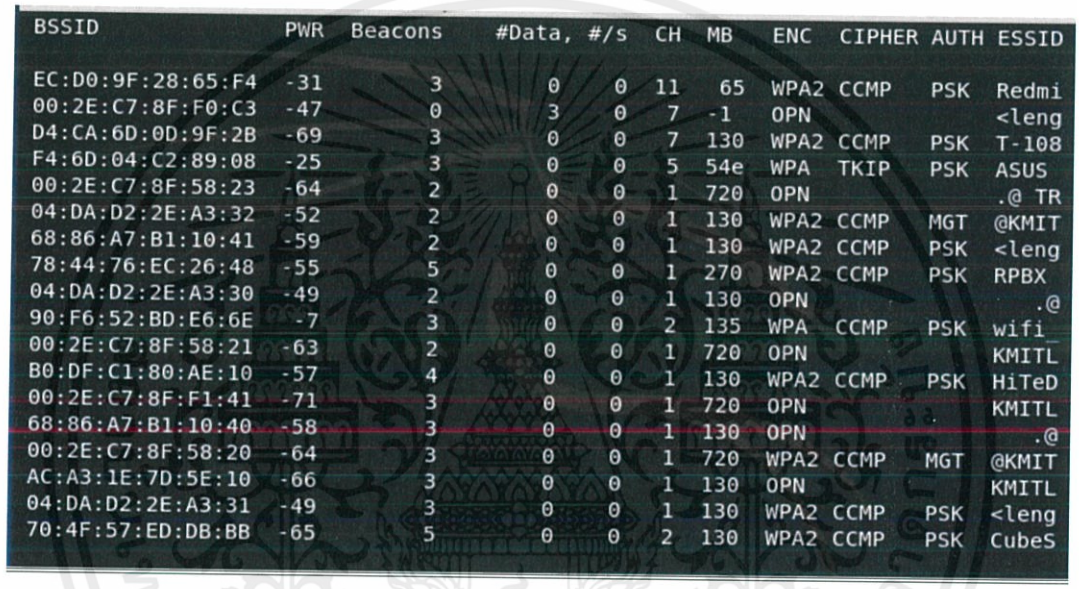


```
CH  2 ][ Elapsed: 3 mins ][ 2018-10-18 16:10 ][ 140 bytes keystream: 90:F6:52:

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH E

90:F6:52:BD:E6:6E   -9  95     1894     2454  168   2  54e  WEP  WEP    SKA  w

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

90:F6:52:BD:E6:6E  98:B8:E3:DC:B7:D6    0    1e- 1e    618     19801
```

รูปที่ 3.7 การดักจับและบันทึกแพ็กเก็ต

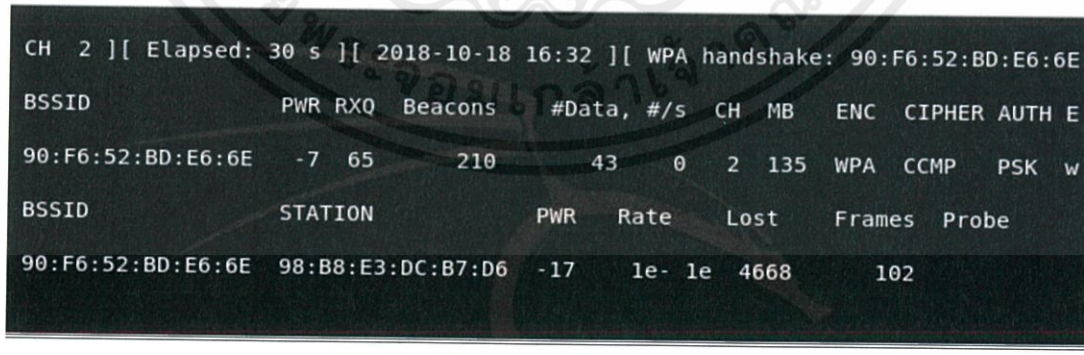
3.2.5 ทดลองโจมตีแอกเซสพอยต์ที่ใช้การเข้ารหัสแบบ WPA

ทำการตั้งค่าแอกเซสพอยต์ โดยตั้ง Authentication Type เป็น WPA-PSK และมีรหัสผ่านสำหรับการเชื่อมต่อแอกเซสพอยต์เป็น abcdefgh แล้วใช้ Airodump-ng ในการค้นหาแอกเซสพอยต์ที่ต้องการจะโจมตีและบันทึกข้อมูลแพ็กเก็ตที่ดักจับได้เก็บเป็นไฟล์ไว้ ดังรูปที่ 3.8 และรูปที่ 3.9 ตามลำดับ จากนั้นใช้ Aircrack-ng ในการสุ่มเดารหัสผ่านจากไฟล์ที่มีการรวมรหัสผ่านต่าง ๆ ไว้



BSSID	PWR	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
EC:D0:9F:28:65:F4	-31	3	0	0	11	65	WPA2	CCMP	PSK	Redmi
00:2E:C7:8F:F0:C3	-47	0	3	0	7	-1	OPN			<leng
D4:CA:6D:0D:9F:2B	-69	3	0	0	7	130	WPA2	CCMP	PSK	T-108
F4:6D:04:C2:89:08	-25	3	0	0	5	54e	WPA	TKIP	PSK	ASUS
00:2E:C7:8F:58:23	-64	2	0	0	1	720	OPN			.@ TR
04:DA:D2:2E:A3:32	-52	2	0	0	1	130	WPA2	CCMP	MGT	@KMIT
68:86:A7:B1:10:41	-59	2	0	0	1	130	WPA2	CCMP	PSK	<leng
78:44:76:EC:26:48	-55	5	0	0	1	270	WPA2	CCMP	PSK	RPBX
04:DA:D2:2E:A3:30	-49	2	0	0	1	130	OPN			.@
90:F6:52:BD:E6:6E	-7	3	0	0	2	135	WPA	CCMP	PSK	wifi_
00:2E:C7:8F:58:21	-63	2	0	0	1	720	OPN			KMITL
B0:DF:C1:80:AE:10	-57	4	0	0	1	130	WPA2	CCMP	PSK	HiTeD
00:2E:C7:8F:F1:41	-71	3	0	0	1	720	OPN			KMITL
68:86:A7:B1:10:40	-58	3	0	0	1	130	OPN			.@
00:2E:C7:8F:58:20	-64	3	0	0	1	720	WPA2	CCMP	MGT	@KMIT
AC:A3:1E:7D:5E:10	-66	3	0	0	1	130	OPN			KMITL
04:DA:D2:2E:A3:31	-49	3	0	0	1	130	WPA2	CCMP	PSK	<leng
70:4F:57:ED:DB:BB	-65	5	0	0	2	130	WPA2	CCMP	PSK	CubeS

รูปที่ 3.8 การค้นหาแอกเซสพอยต์

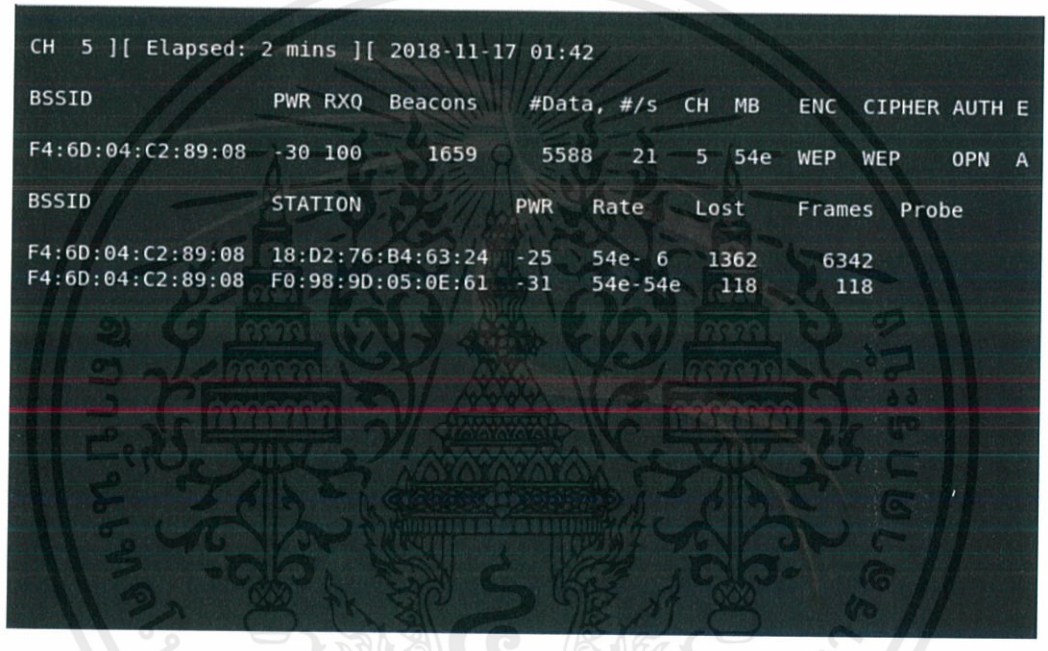


```
CH  2 ][ Elapsed: 30 s ][ 2018-10-18 16:32 ][ WPA handshake: 90:F6:52:BD:E6:6E

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH E

90:F6:52:BD:E6:6E   -7  65      210       43    0   2  135  WPA  CCMP   PSK  w

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

90:F6:52:BD:E6:6E  98:B8:E3:DC:B7:D6  -17    1e- 1e  4668      102
```

รูปที่ 3.9 การดักจับและบันทึกแพ็กเก็ต

3.2.6 การทำ DoS Attack (Denial of Service)

ทำการตั้งค่าแอกเซสพอยต์ โดยตั้งค่า Authentication Type เป็น Enable และเลือกการ Authentication เป็นแบบ Encryption key Authentication แล้วใช้ Airodump-ng เพื่อดูว่าแอกเซสพอยต์มี MAC Address เป็นเบอร์อะไร ใช้งานอยู่ที่ช่องสัญญาณใด จากรูปที่ 3.10 จะเห็นว่าแอกเซสพอยต์ใช้งานอยู่บนช่องสัญญาณที่ 5 มี MAC Address คือ F4:6D:04:C2:89:08 และมีอุปกรณ์สองตัวต่ออยู่กับแอกเซสพอยต์นี้



รูปที่ 3.10 ข้อมูลเบื้องต้นของแอกเซสพอยต์และอุปกรณ์ที่เชื่อมต่ออยู่กับแอกเซสพอยต์

จากนั้นทำการส่งแพ็กเก็ต Deauthentication ไปหาแอกเซสพอยต์และอุปกรณ์ที่ต่ออยู่กับแอกเซสพอยต์ เพื่อขัดขวางหรือก่อกวนระบบเครือข่าย ดังรูปที่ 3.11 ซึ่งจะทำให้อุปกรณ์ที่เชื่อมต่ออยู่กับแอกเซสพอยต์หลุดจากการเชื่อมต่อ

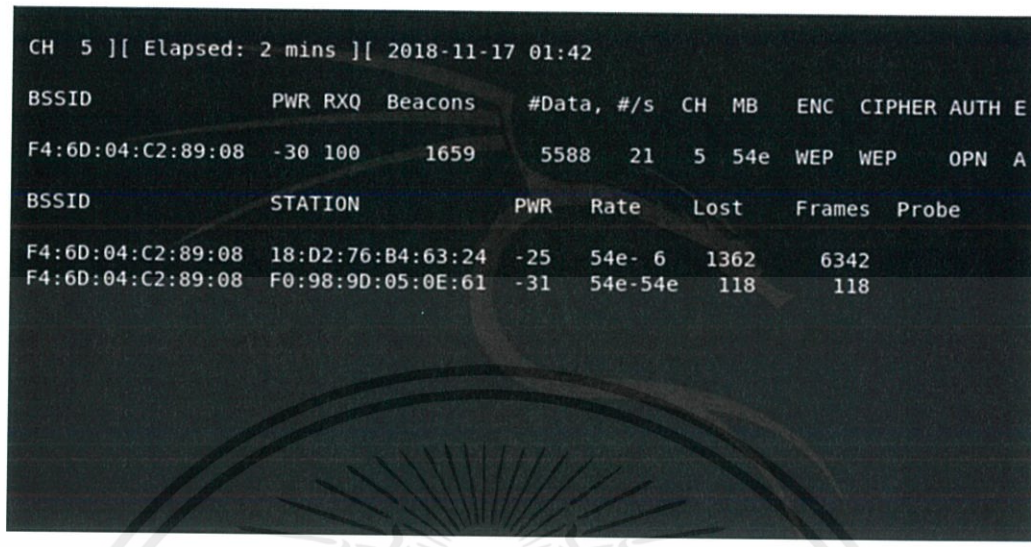
```
root@FAH:~# aireplay-ng -0 0 -a F4:6D:04:C2:89:08 --ignore-negative-one wlan0
02:49:18  Waiting for beacon frame (BSSID: F4:6D:04:C2:89:08) on channel 5
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
02:49:18  Sending DeAuth (code 7) to broadcast -- BSSID: [F4:6D:04:C2:89:08]
02:49:19  Sending DeAuth (code 7) to broadcast -- BSSID: [F4:6D:04:C2:89:08]
02:49:19  Sending DeAuth (code 7) to broadcast -- BSSID: [F4:6D:04:C2:89:08]
02:49:20  Sending DeAuth (code 7) to broadcast -- BSSID: [F4:6D:04:C2:89:08]
02:49:20  Sending DeAuth (code 7) to broadcast -- BSSID: [F4:6D:04:C2:89:08]
02:49:21  Sending DeAuth (code 7) to broadcast -- BSSID: [F4:6D:04:C2:89:08]
02:49:21  Sending DeAuth (code 7) to broadcast -- BSSID: [F4:6D:04:C2:89:08]
02:49:21  Sending DeAuth (code 7) to broadcast -- BSSID: [F4:6D:04:C2:89:08]
02:49:22  Sending DeAuth (code 7) to broadcast -- BSSID: [F4:6D:04:C2:89:08]
02:49:22  Sending DeAuth (code 7) to broadcast -- BSSID: [F4:6D:04:C2:89:08]
02:49:23  Sending DeAuth (code 7) to broadcast -- BSSID: [F4:6D:04:C2:89:08]
02:49:23  Sending DeAuth (code 7) to broadcast -- BSSID: [F4:6D:04:C2:89:08]
02:49:24  Sending DeAuth (code 7) to broadcast -- BSSID: [F4:6D:04:C2:89:08]
02:49:24  Sending DeAuth (code 7) to broadcast -- BSSID: [F4:6D:04:C2:89:08]
02:49:25  Sending DeAuth (code 7) to broadcast -- BSSID: [F4:6D:04:C2:89:08]
02:49:25  Sending DeAuth (code 7) to broadcast -- BSSID: [F4:6D:04:C2:89:08]
02:49:26  Sending DeAuth (code 7) to broadcast -- BSSID: [F4:6D:04:C2:89:08]
02:49:26  Sending DeAuth (code 7) to broadcast -- BSSID: [F4:6D:04:C2:89:08]
02:49:26  Sending DeAuth (code 7) to broadcast -- BSSID: [F4:6D:04:C2:89:08]
```

รูปที่ 3.11 การส่งแพ็กเก็ต Deauthentication หลาย ๆ แพ็กเก็ตไปหาแอกเซสพอยต์

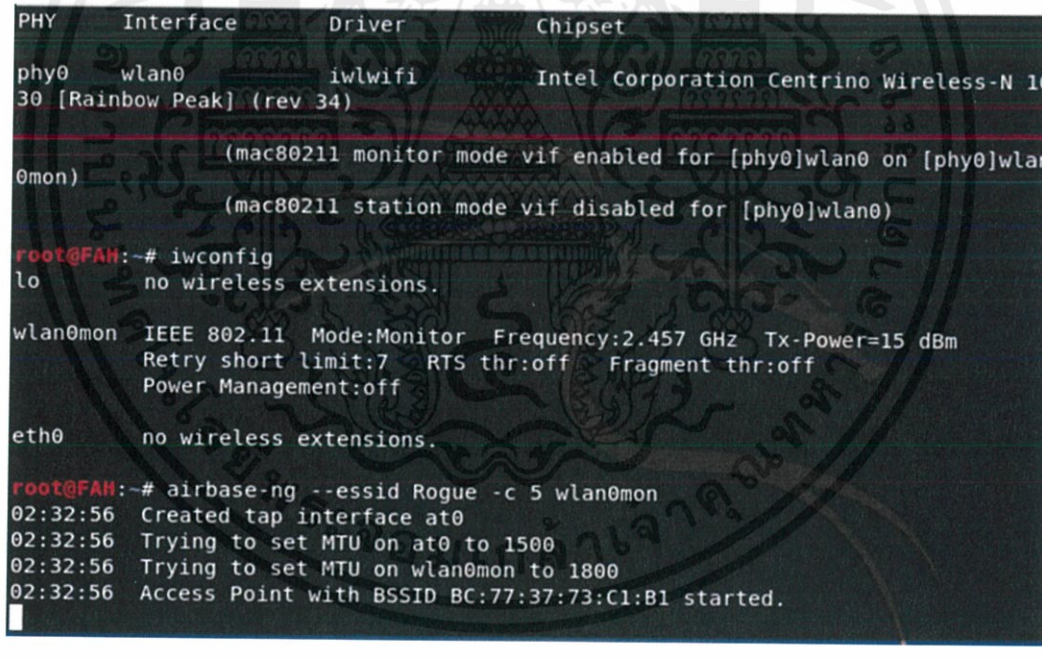
3.2.7 การทำ Evil twin

เป็นการสร้างหรือจำลองแอกเซสพอยต์ขึ้นมา โดยตั้งชื่อ SSID ให้คล้ายคลึงกับ SSID ของ Wi-Fi ที่ให้บริการที่สาธารณะเพื่อที่จะสามารถเข้าถึงชื่อผู้ใช้และรหัสผ่าน

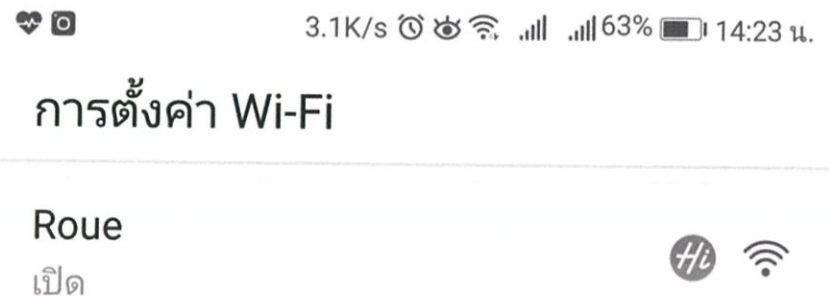
ใช้ Airodump-ng เพื่อค้นหา BSSID และ ESSID ของแอกเซสพอยต์ที่ต้องการจะทำ Evil twin ดังรูปที่ 3.12 จากนั้น สร้างแอกเซสพอยต์ที่มี ESSID คล้ายกับ Wi-Fi สาธารณะ แต่ BSSID แตกต่างกัน ในที่นี้ตั้ง ESSID ชื่อว่า Roue โดยใช้ Airbase-ng ได้ดังรูปที่ 3.13 เมื่อทำการสร้างแอกเซสพอยต์ที่มี ESSID ชื่อ Roue ขึ้นมา จะแสดงได้ดังรูปที่ 3.14 แล้วใช้ Airodump-ng เพื่อค้นหา BSSID และ ESSID ของแอกเซสพอยต์อีกครั้ง จะปรากฏแอกเซสพอยต์ตัวใหม่ที่สร้างขึ้น ดังรูปที่ 3.15



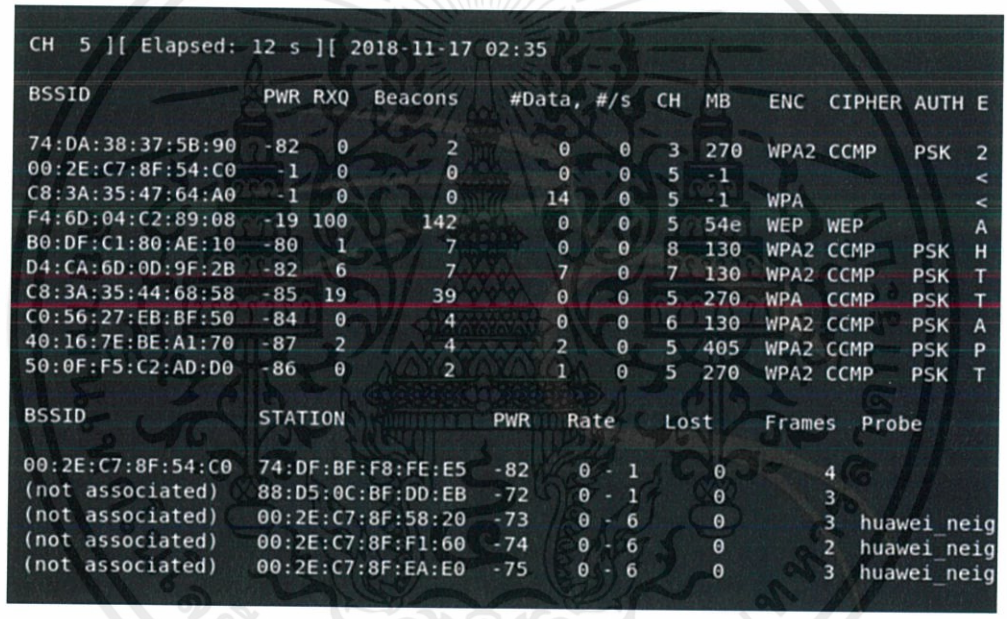
รูปที่ 3.12 BSSID และ ESSID ของแอกเซสพอยต์ที่ดักจับได้



รูปที่ 3.13 การตั้ง ESSID ของแอกเซสพอยต์ที่สร้างขึ้นมาใหม่



รูปที่ 3.14 ผลการค้นหาแอกเซสพอยต์พบ SSID ชื่อ “Roue”

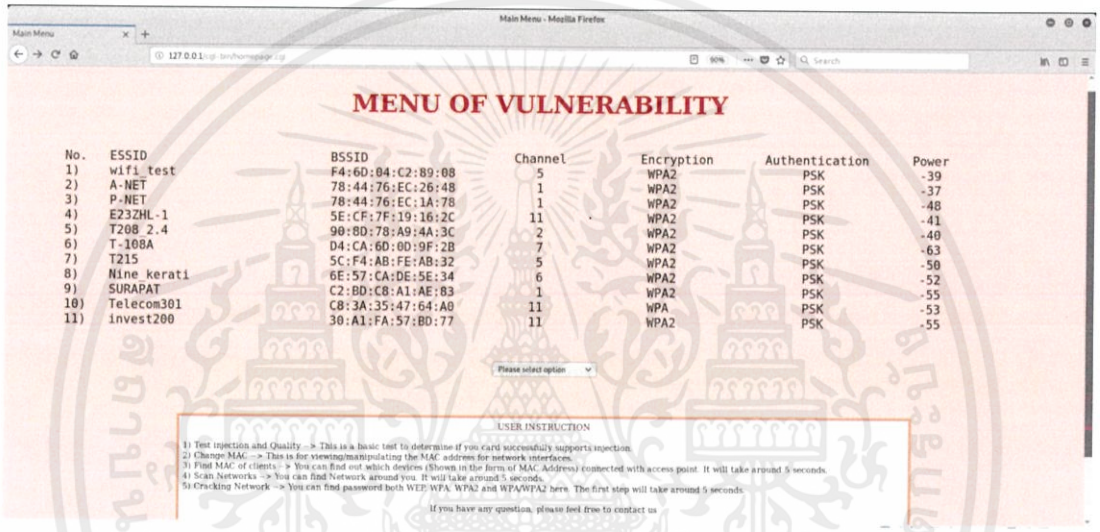


รูปที่ 3.15 ผลการค้นหา BSSID และ ESSID ของแอกเซสพอยต์

หลังจากเสร็จสิ้นขั้นตอน ทำการ DoS Attack เพื่อให้ไคลเอนต์หลุดการเชื่อมต่อกับแอกเซสพอยต์เดิม แล้วมาเชื่อมต่อกับแอกเซสพอยต์ตัวใหม่ที่สร้างขึ้น เมื่อไคลเอนต์ทำการเชื่อมต่อมาที่แอกเซสพอยต์ที่จำลองขึ้นมา ก็จะมีการใส่ชื่อผู้ใช้และรหัสผ่านใหม่อีกครั้ง ก็จะทำให้ทราบชื่อผู้ใช้และรหัสผ่านของไคลเอนต์ได้

3.2.8 การออกแบบเว็บแอปพลิเคชันเพื่อให้สามารถรันคำสั่งในการศึกษาช่องโหว่ที่ศึกษามาได้อย่างอัตโนมัติ

ทำการสร้างเว็บแอปพลิเคชันโดยใช้ภาษาเอชทีเอ็มแอลและแบชโดยใช้หลักการ CGI เพื่อให้สามารถรันคำสั่งในการศึกษาช่องโหว่ตามที่ได้ศึกษามาได้อย่างอัตโนมัติ โดยในเว็บแอปพลิเคชันมีการเรียกใช้โปรแกรมต่าง ๆ ได้แก่ Airmon-ng, Airodump-ng, Aireplay-ng, Macchanger และ Aircrack-ng เว็บแอปพลิเคชันที่สร้างขึ้นมีคุณสมบัติดังนี้



รูปที่ 3.16 หน้าเมนูหลักของโปรแกรม

1) สามารถทดสอบความสามารถการ injection แพ็กเก็ตของ Wireless USB Adapter ที่ใช้ได้

2) สามารถดูและปลอม MAC Address ได้ โดยเลือกได้ 3 แบบ คือ ปลอมแบบสุ่มเลข MAC Address, ปลอมแบบกำหนดเลข MAC Address ที่ต้องการ และรีเซ็ต MAC Address

3) สามารถค้นหาเลข MAC Address ของอุปกรณ์ที่เชื่อมต่ออยู่กับแอกเซสพอยต์ได้

4) สามารถค้นหาสัญญาณ Wi-Fi และบอกรายละเอียดข้อมูลของสัญญาณ Wi-Fi ได้ เช่น MAC Address, ช่องสัญญาณ, กำลังของสัญญาณ และรูปแบบการเข้ารหัส เป็นต้น

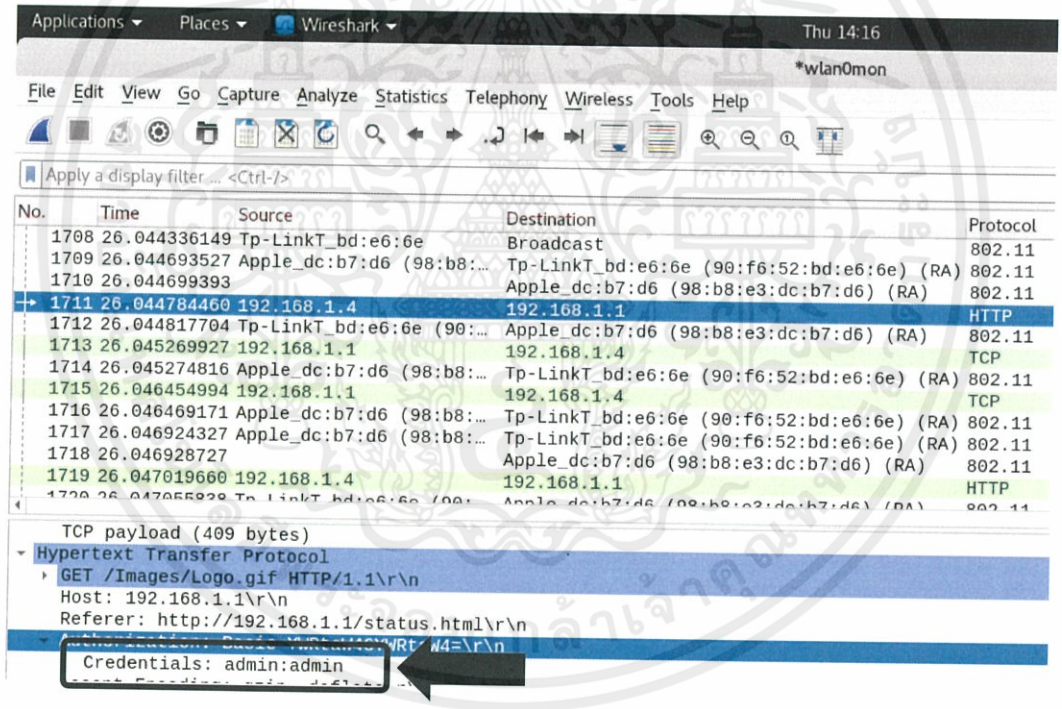
5) สามารถค้นหารหัสผ่านของแอกเซสพอยต์ที่มีการตั้งค่าการเข้ารหัสทั้งแบบ WEP และ WPA/WPA2 ได้

บทที่ 4

ผลการทดลอง

4.1 ผลการทดลองดักจับแพ็กเก็ตข้อมูล

จากการดักจับข้อมูลแล้วนำมาวิเคราะห์พบว่าชื่อผู้ใช้และรหัสผ่านที่ใช้ในการตั้งค่าแอกเซสพอยต์คือ admin และ admin ตามลำดับ ดังรูปที่ 4.1 ซึ่งไม่ได้มีการเข้ารหัสไว้ ดังนั้นจึงเห็นข้อมูลทั้งหมดในรูปแบบของเพลนเท็กซ์ ซึ่งถ้ามีผู้ไม่หวังดีอยู่ในรัศมีการแพร่กระจายของสัญญาณแอกเซสพอยต์ ก็จะสามารถเห็นแพ็กเก็ตทั้งหมดได้โดยการดักจับข้อมูลโดยใช้เครื่องมือที่ดักจับข้อมูลได้ เช่น Wireshark

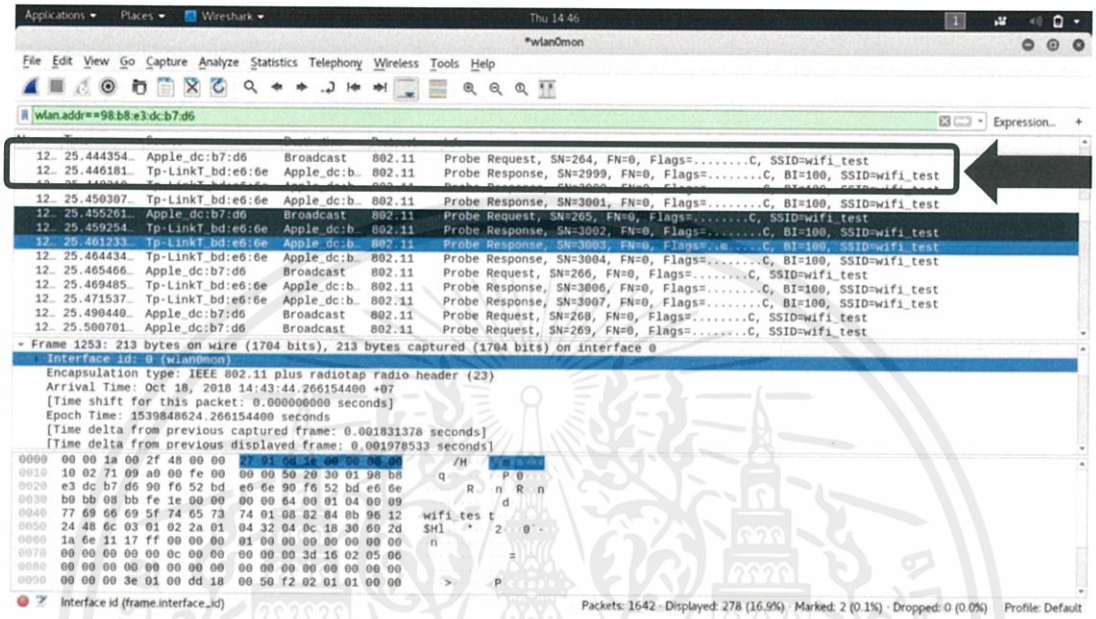


รูปที่ 4.1 ข้อมูลของแพ็กเก็ตที่ดักจับได้

4.2 ผลการค้นหา SSID ที่ถูกตั้งค่าให้ซ่อนไว้

ถึงแม้ว่าแอกเซสพอยต์จะถูกตั้งค่าให้ซ่อน SSID ไว้ แต่ถ้าหากดักจับข้อมูลในขณะที่ไคลเอนต์ที่มีสิทธิ์เข้าใช้งานเชื่อมต่อกับแอกเซสพอยต์ ซึ่งจะมีการส่งเฟรม Probe Request และ

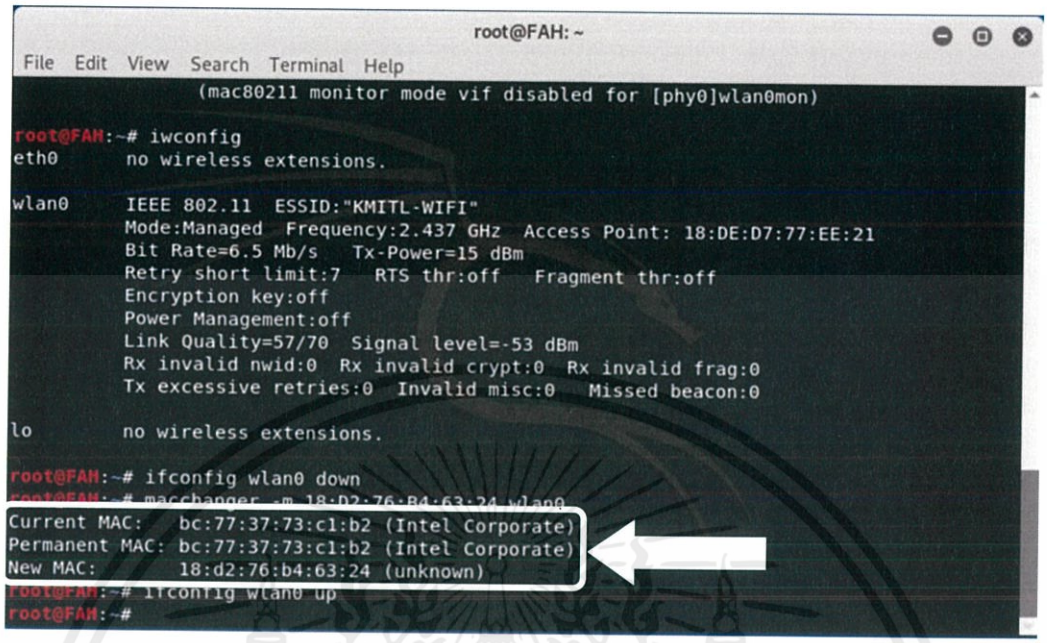
เฟรม Probe Response จะทำให้สามารถทราบ SSID ได้ เนื่องจากในเฟรมเหล่านี้จะมีการระบุ SSID ไว้ ดังรูปที่ 4.2



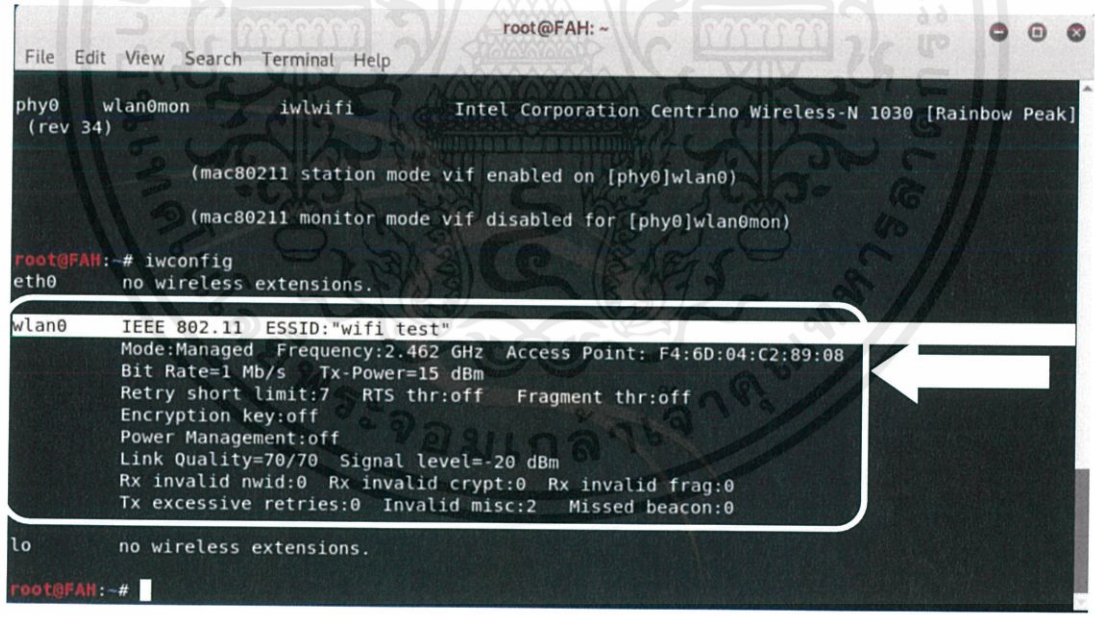
รูปที่ 4.2 ข้อมูลที่ดักจับได้ในขณะที่ไคลเอนต์กำลังเชื่อมต่อแอกเซสพอยต์

4.3 ผลการทดลองปลอม MAC Address เพื่อเชื่อมต่อกับแอกเซสพอยต์ที่ตั้งค่าการกรองไว้

จากรูปที่ 4.3 จะเห็นได้ว่าสามารถปลอม MAC Address จาก bc:77:37:73:c1:b2 เป็น 18:d2:76:b4:63:24 ซึ่งเป็น MAC Address ที่สามารถเชื่อมต่อกับแอกเซสพอยต์ได้โดย หลังจากปลอมเป็น MAC Address นี้แล้ว จึงทำให้สามารถเชื่อมต่อแอกเซสพอยต์ได้ด้วยดังรูปที่ 4.4



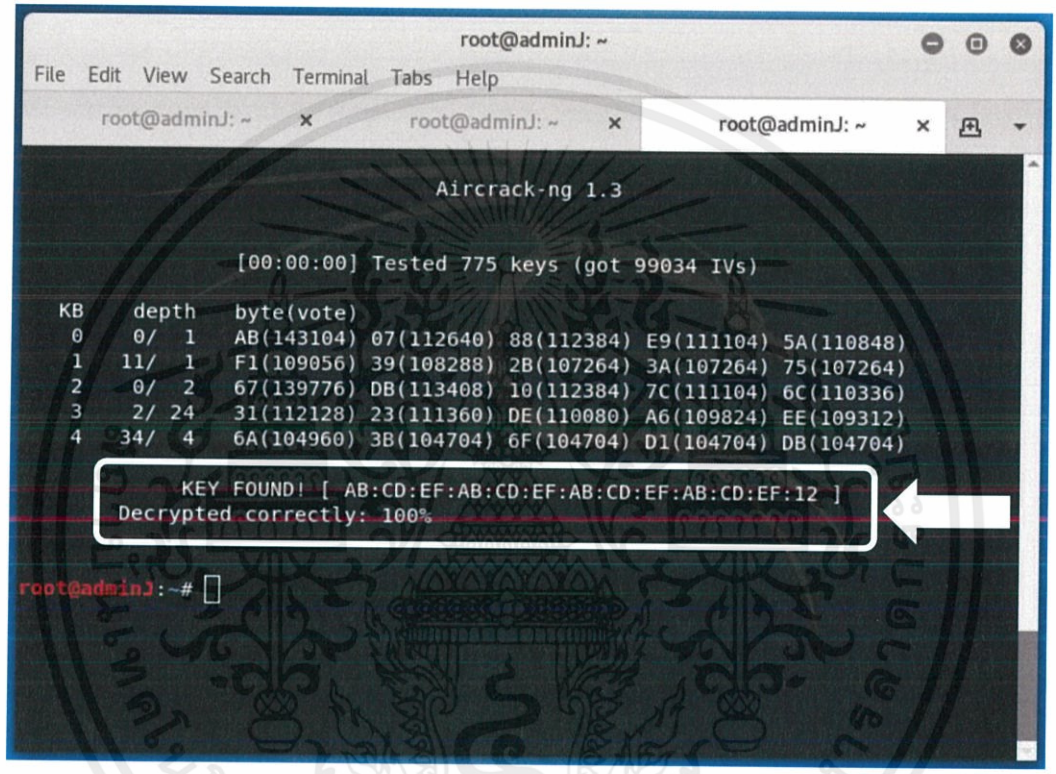
รูปที่ 4.3 ผลการปลอม MAC Address



รูปที่ 4.4 ผลการตรวจสอบสถานะการเชื่อมต่อของอุปกรณ์ Wireless

4.4 ผลการทดลองโจมตีแอกเซสพอยต์ที่ใช้การเข้ารหัสแบบ WEP

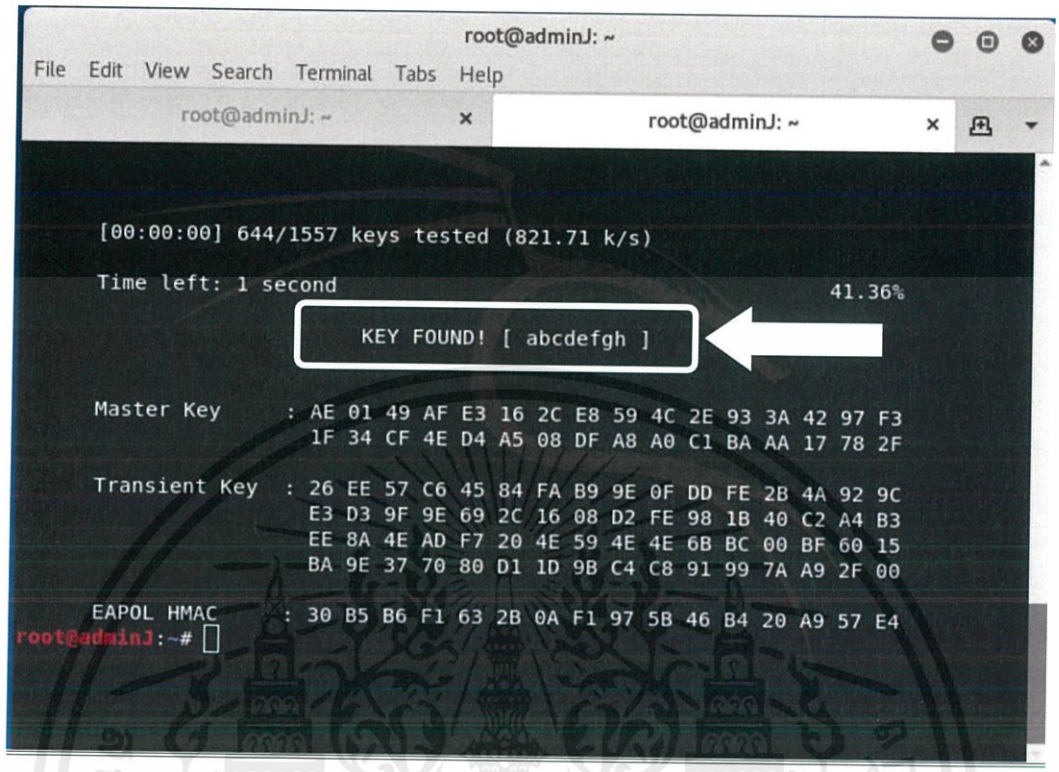
จากการใช้ Aircrack-ng ในการคำนวณหารหัสผ่านจากไฟล์ที่เก็บแพ็กเก็ตที่ดักจับไว้ได้ผลลัพธ์ดังรูปที่ 4.5 จะเห็นได้ว่ารหัสผ่านคือ ABCDEFABCDEFABCDEFABCDEF12 ซึ่งตรงกับรหัสผ่านที่ตั้งค่าไว้ที่แอกเซสพอยต์



รูปที่ 4.5 รหัสผ่านที่ได้จากแอกเซสพอยต์ที่ใช้การเข้ารหัสแบบ WEP

4.5 ผลการทดลองโจมตีแอกเซสพอยต์ที่ใช้การเข้ารหัสแบบ WPA

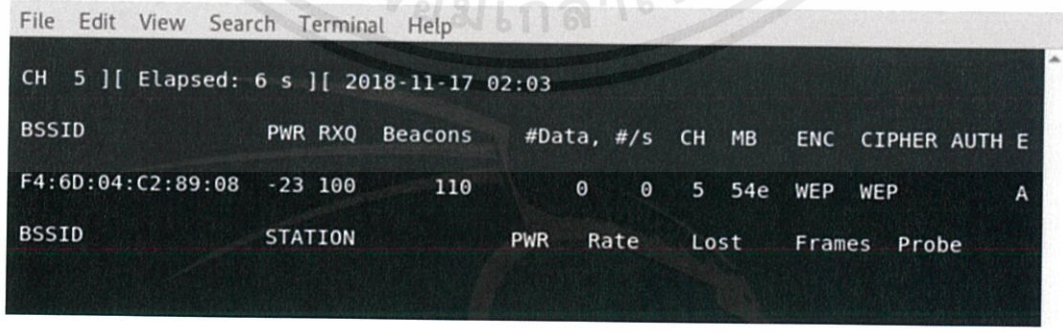
จากการใช้ Aircrack-ng ในการหารหัสผ่าน โดยใช้วิธีการเดารหัสผ่านจากไฟล์คำศัพท์ (Dictionary Attack) จะได้ผลดังรูปที่ 4.6 จะเห็นได้ว่ารหัสผ่านคือ abcdefgh ซึ่งตรงกับรหัสผ่านที่ตั้งค่าไว้ที่แอกเซสพอยต์



รูปที่ 4.6 รหัสผ่านที่ได้จากแอกเซสพอยต์ที่ใช้การเข้ารหัสแบบ WPA

4.6 ผลการทำ DoS Attack (Denial of Service)

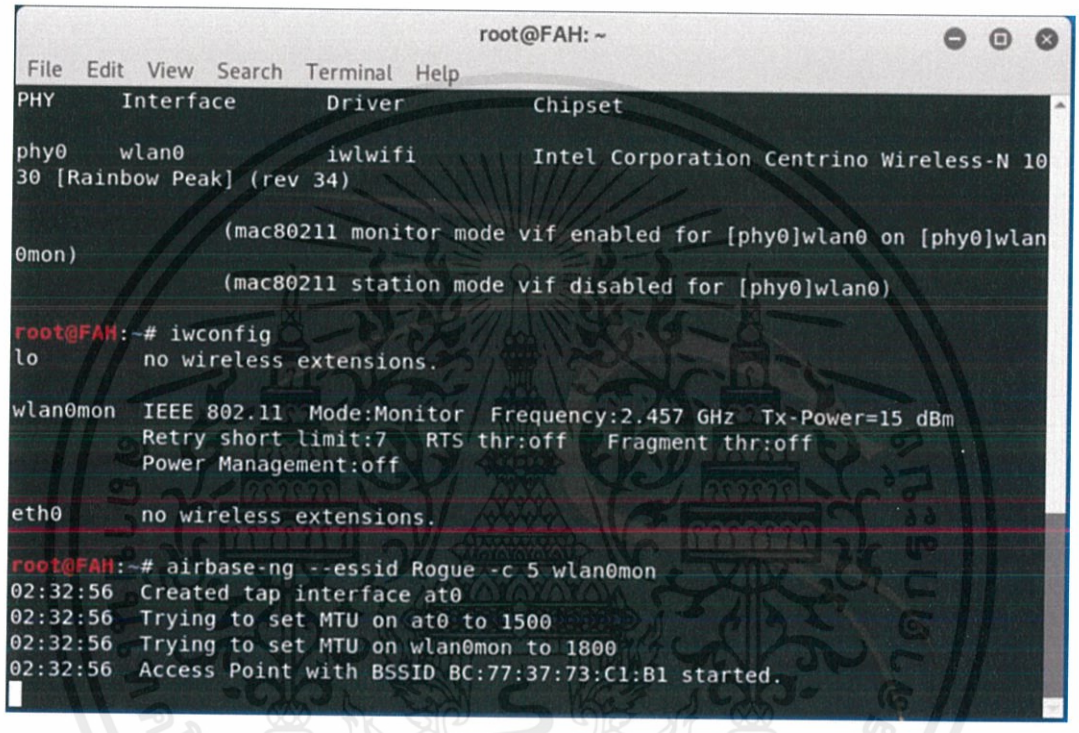
จากการส่งแพ็กเก็ต Deauthentication ไปหาแอกเซสพอยต์ เพื่อขัดขวางหรือก่อกวนระบบเครือข่ายส่งผลให้ไคลเอนต์หลุดจากการเชื่อมต่อกับแอกเซสพอยต์ จากรูปที่ 4.7 จะเห็นได้ว่าไม่มีอุปกรณ์ใดเชื่อมต่อกับแอกเซสพอยต์อยู่เลย



รูปที่ 4.7 ผลการตรวจสอบว่าแอกเซสพอยต์มีอุปกรณ์เชื่อมต่ออยู่หรือไม่

4.7 ผลการการทำ Evil twin

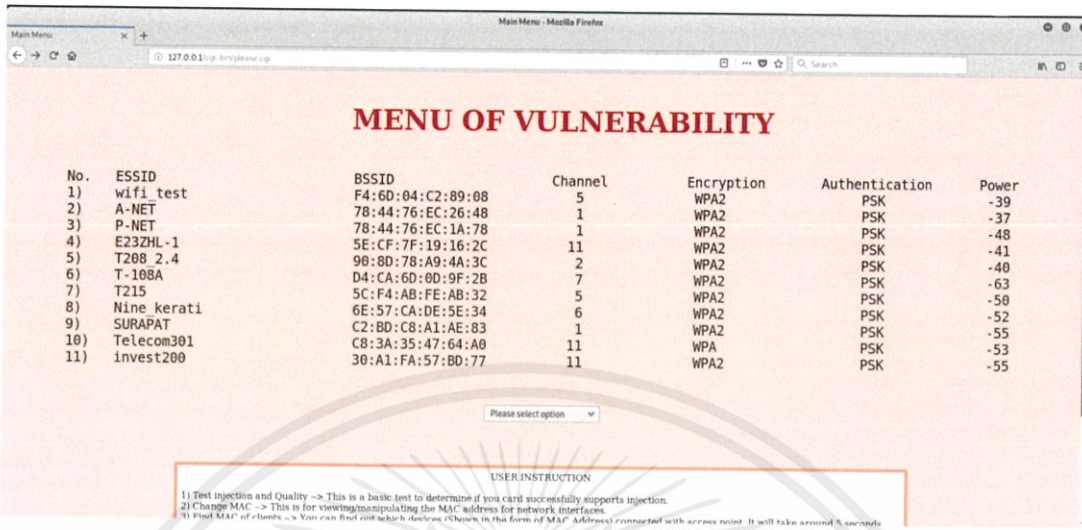
ทำการจำลองแอกเซสพอยต์ขึ้นมา โดยให้มี SSID คล้ายกับ Wi-Fi สาธารณะ ดังรูปที่ 4.8 ซึ่ง Wi-Fi สาธารณะ เป็น Wi-Fi ที่บุคคลทั่วไปสามารถใช้บริการอินเทอร์เน็ตไร้สายได้ เช่น @Kmitl, TrueWifi, 3BBwifi ฯลฯ



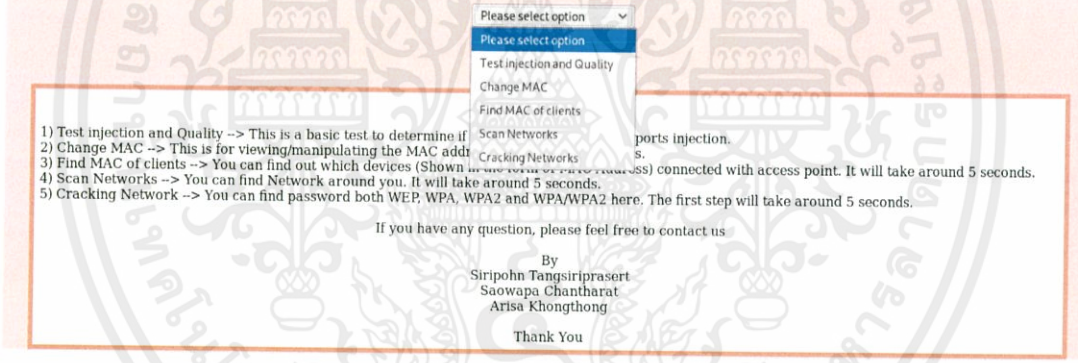
รูปที่ 4.8 การตั้ง SSID ของแอกเซสพอยต์ที่สร้างขึ้นมาใหม่

4.8 ผลการทดลองใช้เว็บแอปพลิเคชันที่สร้างขึ้น

เมื่อเริ่มใช้งานเว็บแอปพลิเคชัน จะแสดงหน้าเมนูหลักของโปรแกรมดังรูปที่ 4.9 โดยให้ผู้ใช้งานเลือกตัวเลือกการทำงานที่ต้องการดังรูปที่ 4.10 ซึ่งในหน้าเมนูหลักจะมีคำอธิบายการทำงานของตัวเลือกต่าง ๆ ด้วย จากนั้นเซิร์ฟเวอร์จะรันค่าตามที่ได้เขียนโปรแกรมไว้ โดยผลทดสอบการทำงานมีดังต่อไปนี้



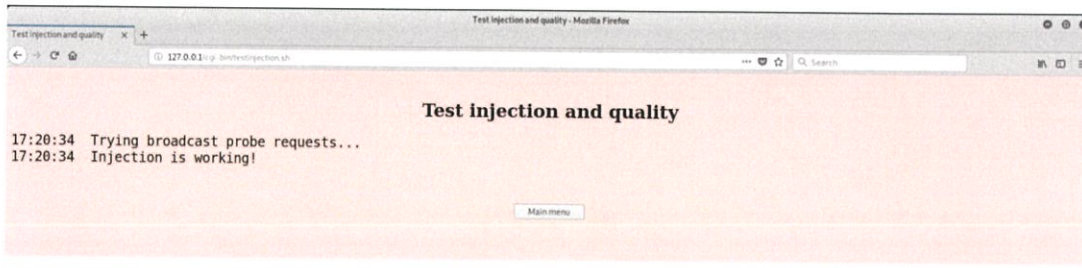
รูปที่ 4.9 เมนูหลักของโปรแกรม



รูปที่ 4.10 ตัวเลือกการทำงานของโปรแกรม

4.8.1 ทดสอบคุณสมบัติการ injection แพ็กเก็ตของ Wireless USB Adapter

เมื่อเลือกเมนู Test injection and quality จะเป็นการทดสอบว่า Wireless USB Adapter สามารถ injection แพ็กเก็ตได้หรือไม่ ซึ่งเป็นคุณสมบัติที่จำเป็นในการศึกษาหาช่องโหว่เครือข่าย Wi-Fi จากรูปที่ 4.11 จะเห็นได้ว่า Wireless USB Adapter มีคุณสมบัติการ injection แพ็กเก็ต



รูปที่ 4.11 ผลการทดลองคุณสมบัติการ injection แพ็กเก็ต

4.8.2 ทดลองปลอมแปลง MAC Address

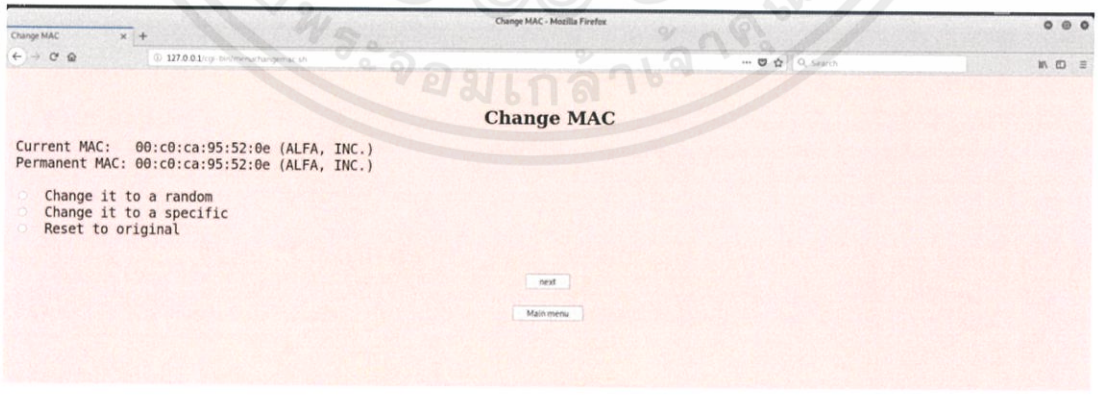
เมื่อเลือกเมนู Change MAC เป็นการปลอม MAC Address จะได้ผลการทดลองดังรูปที่ 4.12 โดยสามารถเลือกการปลอม Mac Address ได้ทั้งหมด 3 แบบดังนี้

4.8.2.1 ผลการทดลองเมื่อเลือก Change it to a random

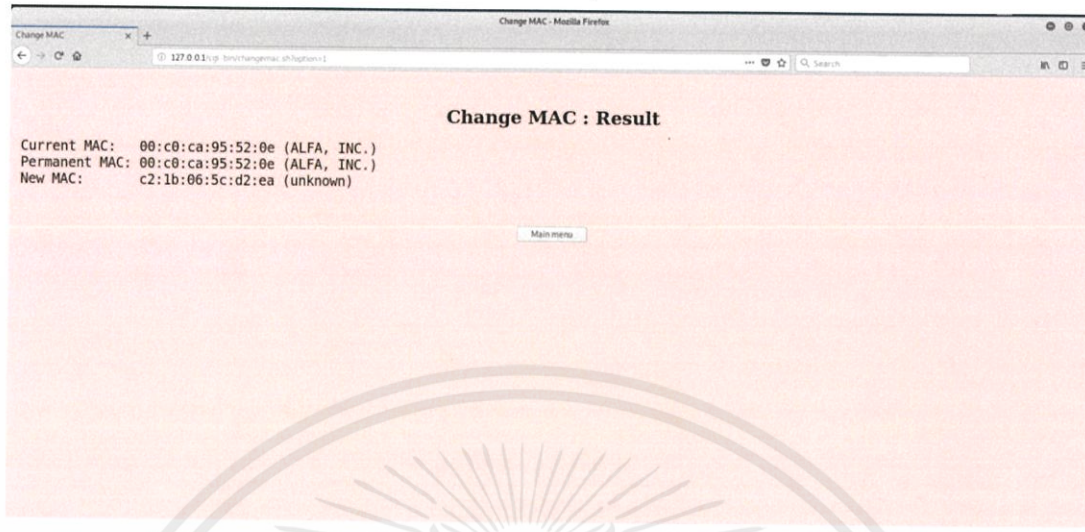
เมื่อเลือก Change it to a random จะเป็นการเปลี่ยน MAC Address เดิมเป็น MAC Address ใหม่ที่มีการสุ่มค่าขึ้นมา โดยมีผลการทดลองดังรูปที่ 4.13 จะเห็นได้ว่า MAC Address ใหม่ที่สุ่มค่ามาคือ c2:1b:06:5c:d2:ea

4.8.2.2 ผลการทดลองเมื่อเลือก Change it to a specific

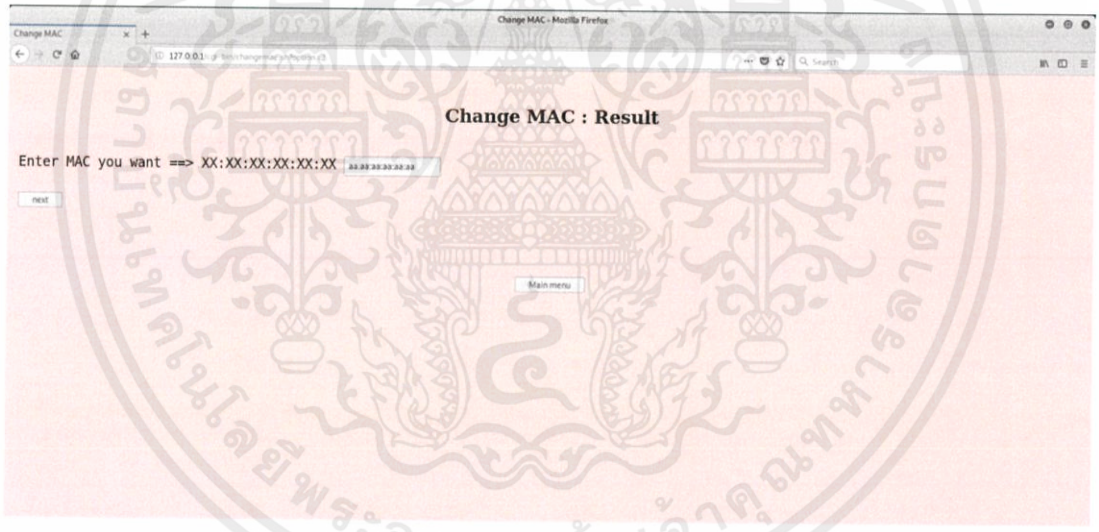
เมื่อเลือก Change it to a specific จะเป็นการเปลี่ยน MAC Address เดิมเป็น MAC Address ใหม่โดยการกำหนด MAC Address เอง จากรูปที่ 4.14 เมื่อใส่ค่า MAC Address ใหม่ที่ต้องการซึ่งคือ aa:aa:aa:aa:aa:aa จะทำให้ได้ผลดังรูปที่ 4.15 ซึ่งพบว่า MAC Address คือ aa:aa:aa:aa:aa:aa



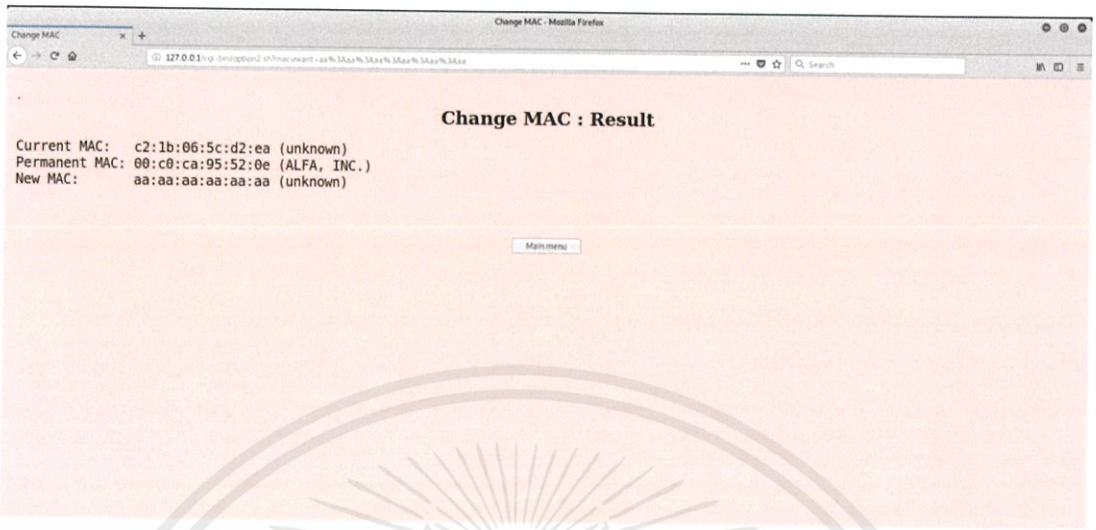
รูปที่ 4.12 ผลการทดลองเมื่อเลือก Change MAC



รูปที่ 4.13 ผลการทดลองเมื่อเลือก Change it to a random



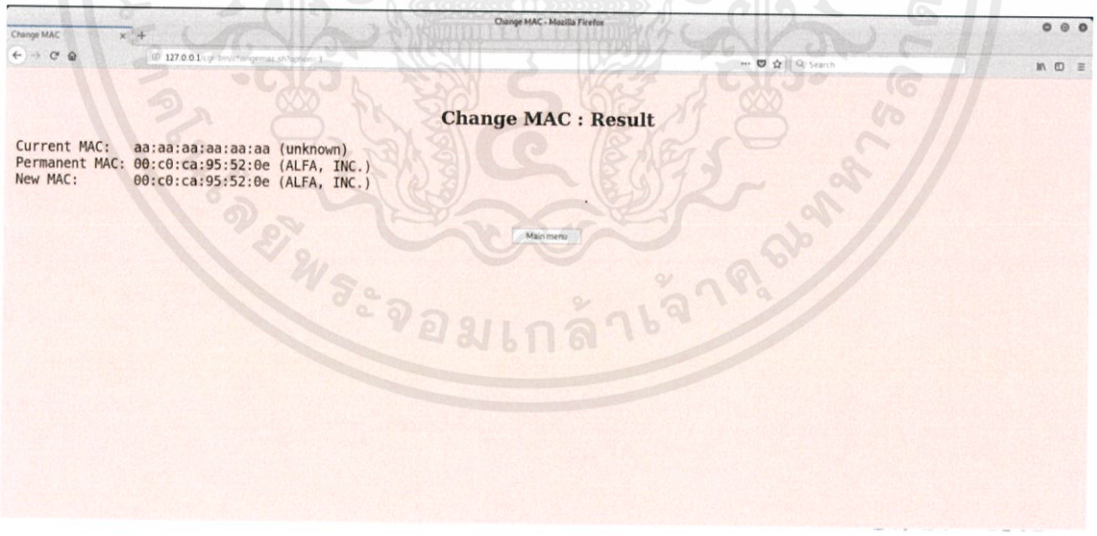
รูปที่ 4.14 การใส่เลข MAC Address ที่ต้องการ



รูปที่ 4.15 ผลการทดลองเมื่อเลือก Change it to a specific

4.8.2.3 ผลการทดลองเมื่อเลือก Reset to original

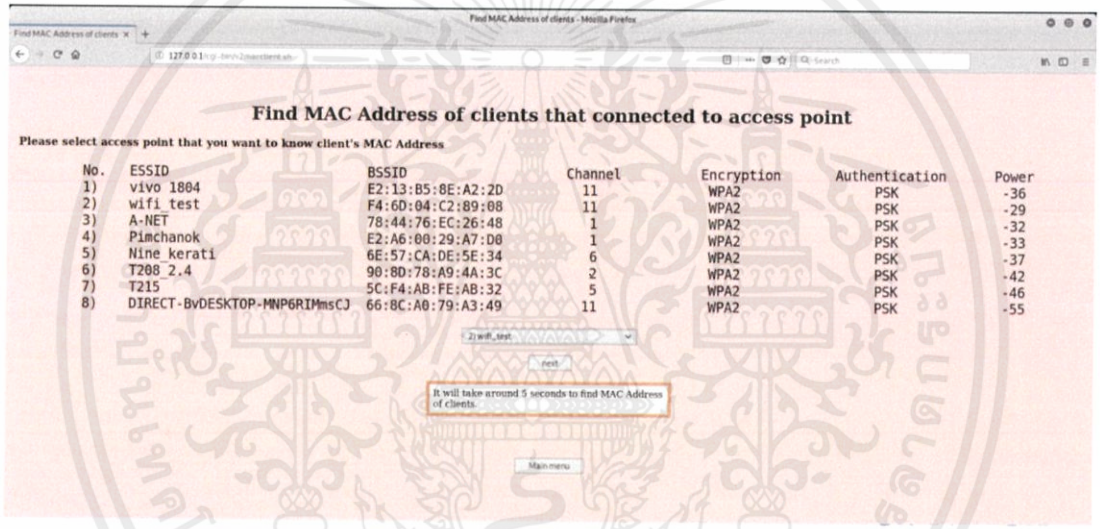
เมื่อเลือก Reset to original เป็นการตั้งค่าให้ MAC Address กลับมาเป็น MAC Address เดิม มีผลการทดลองดังรูปที่ 4.16



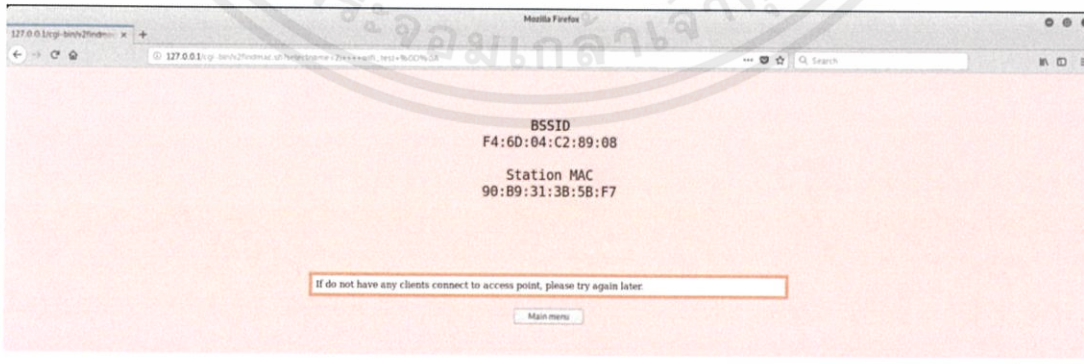
รูปที่ 4.16 ผลการทดลองเมื่อเลือก Reset to original

4.8.3 ทดลองการค้นหา MAC Address ของอุปกรณ์ที่เชื่อมต่อกับแอกเซสพอยต์

เมื่อเลือกเมนู Find MAC of clients จะแสดงแอกเซสพอยต์ที่อยู่โดยรอบ ดังแสดงในรูปที่ 4.17 แล้วให้ผู้ใช้เลือกแอกเซสพอยต์ตัวที่ต้องการทราบว่ามีอุปกรณ์ไหนเชื่อมต่ออยู่บ้าง โดยเมื่อเลือกแอกเซสพอยต์ตัวที่ต้องการแล้ว จะมีการแสดง MAC Address ของอุปกรณ์ที่เชื่อมต่ออยู่กับแอกเซสพอยต์นั้น เพื่อเป็นประโยชน์ในการปลอมแปลง MAC Address โดยมีผลดังรูปที่ 4.18 จากผลการทดลองจะเห็นได้ว่า MAC Address ของแอกเซสพอยต์คือ F4:6D:04:C2:89:08 และมีอุปกรณ์เชื่อมต่ออยู่ 1 ตัว โดย MAC Address ของอุปกรณ์นั้นคือ 90:B9:31:3B:5B:F7



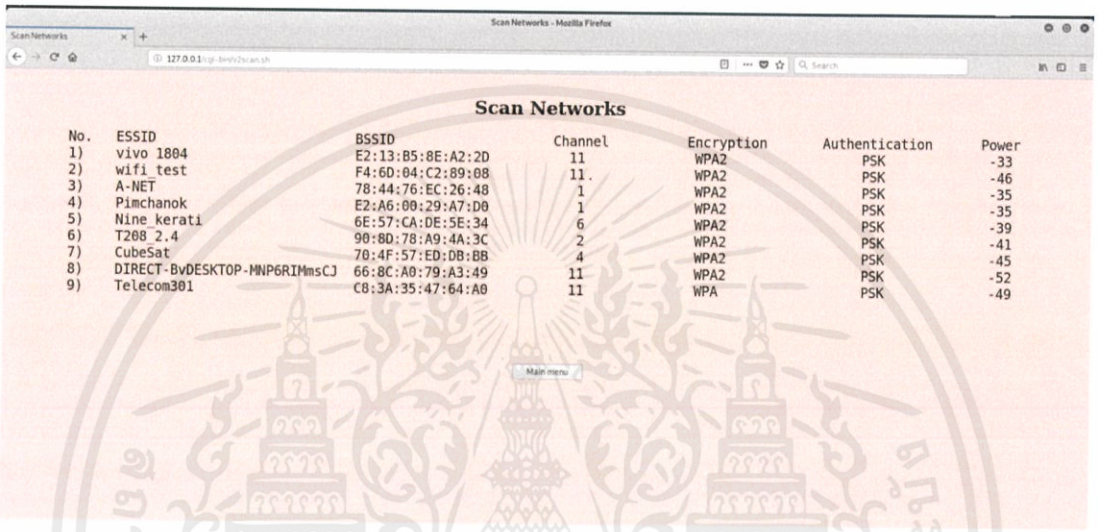
รูปที่ 4.17 ผลการทดลองเมื่อเลือกเมนู Find MAC of clients



รูปที่ 4.18 MAC Address ของอุปกรณ์ที่เชื่อมต่ออยู่กับแอกเซสพอยต์

4.8.4 ทดลองการค้นหาเครือข่าย Wi-Fi

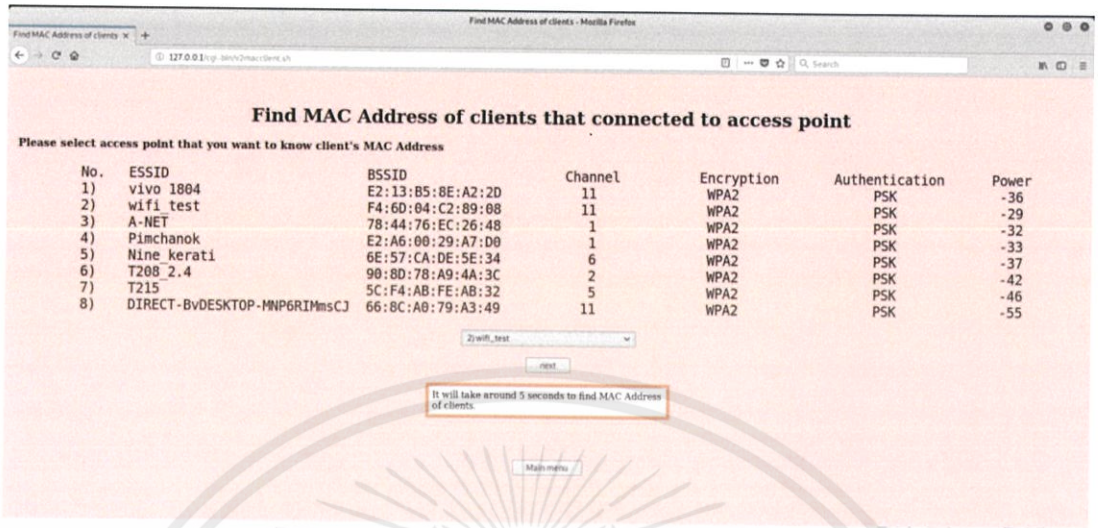
เมื่อเลือกเมนู Scan Networks จะเป็นการค้นหาเครือข่าย Wi-Fi แสดงดังรูปที่ 4.19 จะเห็นได้ว่า มีการบอกรายละเอียดข้อมูลของสัญญาณ Wi-Fi ต่าง ๆ เช่น MAC Address ช่องสัญญาณ กำลังของสัญญาณ และรูปแบบการเข้ารหัส เป็นต้น



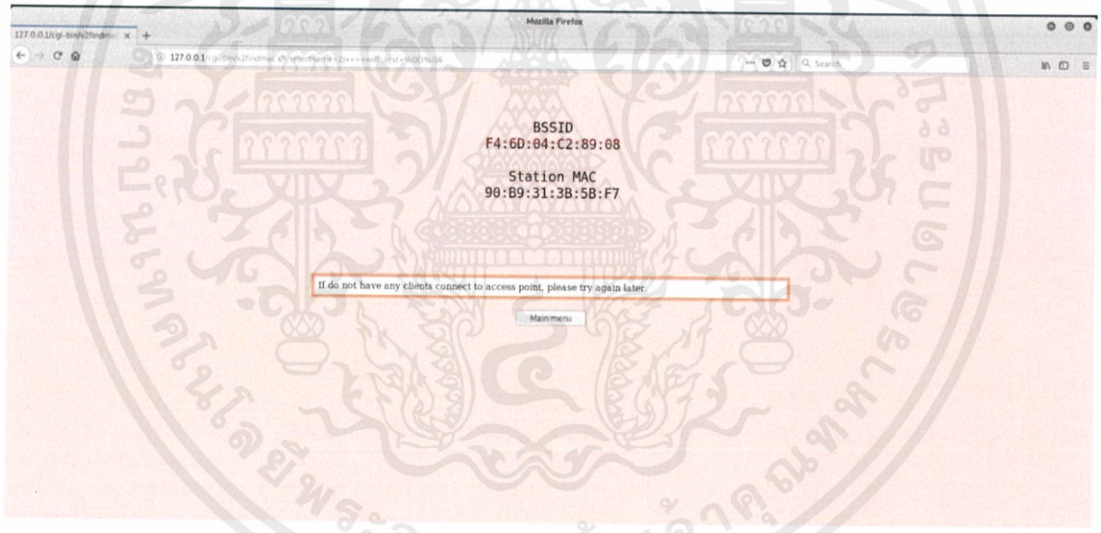
รูปที่ 4.19 ผลการทดลองเมื่อเลือกเมนู Scan Networks

4.8.5 ทดลองการค้นหารหัสผ่านแอกเซสพอยต์ที่ใช้การเข้ารหัสแบบ WEP และ WPA/WPA2

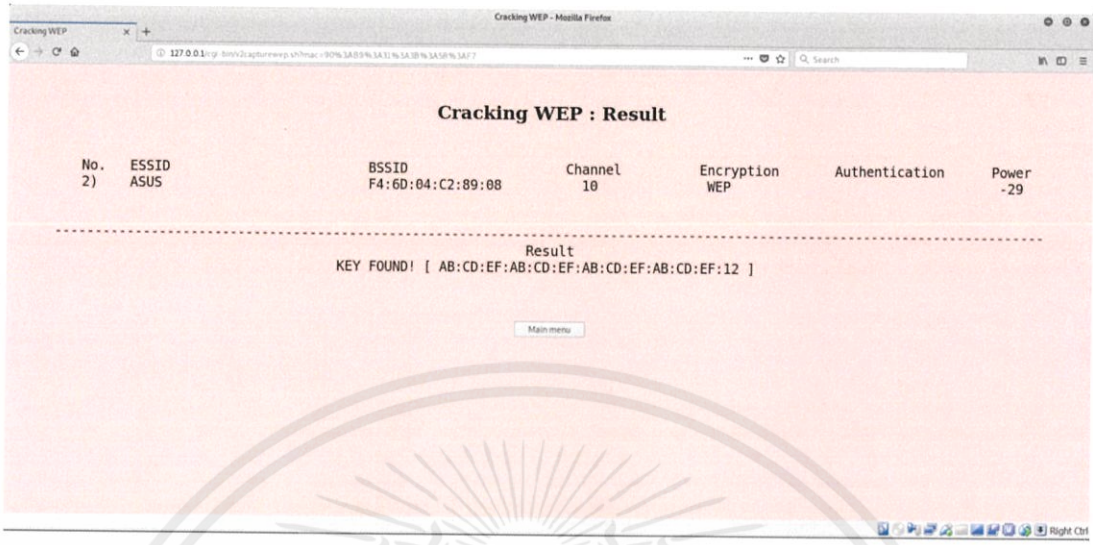
เมื่อเลือกเมนู Cracking Networks จะเป็นการค้นหารหัสผ่านแอกเซสพอยต์ที่ใช้การเข้ารหัสแบบ WEP และ WPA/WPA2 ขั้นตอนแรกโปรแกรมจะทำการค้นหาเครือข่ายอินเทอร์เน็ตและให้ผู้ใช้เลือกเครือข่ายที่ต้องการโจมตีดังรูปที่ 4.20 ถ้าผู้ใช้เลือกเครือข่ายที่ใช้การเข้ารหัสแบบ WEP โปรแกรมจะทำการตรวจสอบว่ามีไคลเอนต์เชื่อมต่อกับแอกเซสพอยต์อยู่หรือไม่ และให้ผู้ใช้เลือกไคลเอนต์ที่ต้องการจะโจมตีดังรูปที่ 4.21 จากนั้นโปรแกรมจะทำการค้นหารหัสผ่านของแอกเซสพอยต์โดยมีผลดังรูปที่ 4.22 จะเห็นได้ว่าแอกเซสพอยต์มีรหัสผ่านคือ abcdefabcdef abcdefabcdef12 แต่ถ้าเลือกเครือข่ายที่ใช้การเข้ารหัสแบบ WPA/WPA2 โปรแกรมจะทำการค้นหารหัสผ่านของแอกเซสพอยต์เลย โดยมีผลดังรูปที่ 4.23 จะเห็นได้ว่าแอก-เซสพอยต์มีรหัสผ่านคือ ilovemymom



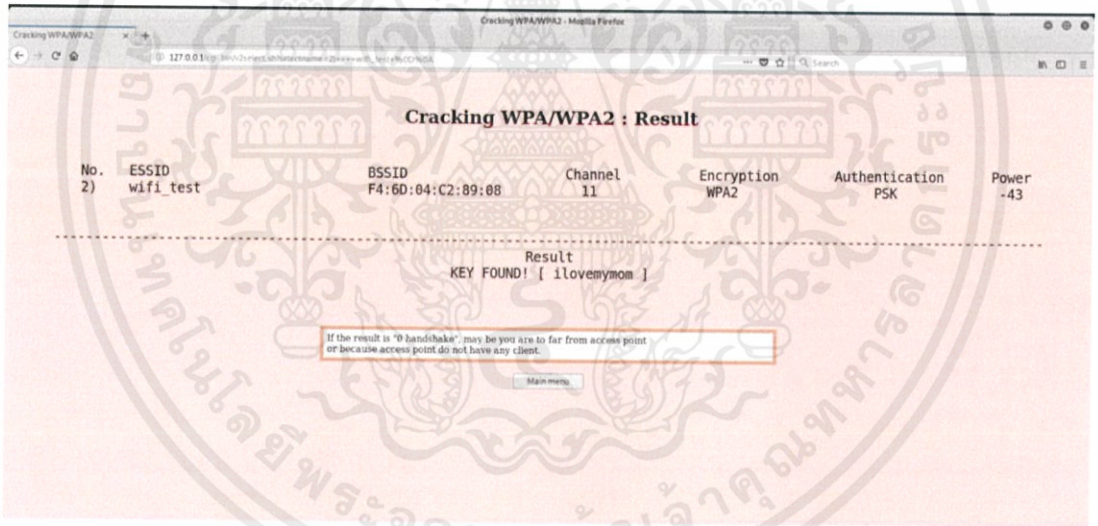
รูปที่ 4.20 ผลการค้นหาเครือข่ายอินเทอร์เน็ต



รูปที่ 4.21 ผลการตรวจสอบว่ามีไคลเอนต์เชื่อมต่อกับแอกเซสพอยต์หรือไม่



รูปที่ 4.22 ผลการค้นหารหัสผ่านแอกเซสพอยต์ที่ใช้การเข้ารหัสแบบ WEP



รูปที่ 4.23 ผลการค้นหารหัสผ่านแอกเซสพอยต์ที่ใช้การเข้ารหัสแบบ WPA/WPA2

4.8.6 ทดลองใช้งานเว็บแอปพลิเคชันกับเครือข่าย Wi-Fi ที่อยู่บริเวณตึกภาควิชาวิศวกรรมโทรคมนาคม

โดยทำการทดลองจำนวน 10 เครือข่าย เพื่อสำรวจการเข้ารหัสของเครือข่าย Wi-Fi และทดลองหารหัสผ่านของเครือข่าย Wi-Fi มีผลการทดลองดังตารางที่ 4.1

ตารางที่ 4.1 ผลการทดลองสำรวจเครือข่าย Wi-Fi และผลลัพธ์ในการหารหัสผ่าน

ชื่อเครือข่าย Wi-Fi	MAC Address ของเครือข่าย Wi-Fi	ช่องสัญญาณ	การเข้ารหัส	การพิสูจน์ตัวตน	รหัสผ่าน	เวลา (วินาที)
wifi_test	F4:6D:04:C2:89:08	5	WEP	-	abcdef abcdef abcdef abcdef12	1
ASUS	D8:50:E6:F4:4B:70	1	WPA/ WPA2	PSK	12345 67890	1
T215	5C:F4:AB:FE:AB:32	2	WPA2	PSK	Key not found	24
@T314	74:D0:2B:39:D8:40	6	WPA2	PSK	Key not found	24
@Telecom301	C8:3A:35:47:64:A0	1	WPA	PSK	Key not found	24
PM_101_	D8:FE:E3:7D:89:44	10	WPA2	PSK	Key not found	24
ASUS550JK_BM	1A:CF:5E:BF:0B:40	11	WPA2	PSK	Key not found	24
Iphone	2A:F0:76:DE:A3:AA	1	WPA2	PSK	mmnn bbvv	1
Tplink	90:F6:52:BD:E6:6E	11	WPA2	PSK	ilove mymom	1
Natta Nilyaporn 's iPhone	7A:67:D7:5A:3E:E6	1	WPA2	PSK	Key not found	24

บทที่ 5

สรุปผลและข้อเสนอแนะ

5.1 สรุปผล

ปริญญานิพนธ์นี้มีวัตถุประสงค์เพื่อศึกษาช่องโหว่ของบริการเครือข่าย Wi-Fi ที่จะนำไปสู่ภัยคุกคามที่เกิดขึ้นจากบริการเครือข่าย Wi-Fi โดยผู้จัดทำได้แบ่งการทำงานออกเป็น 2 ส่วน ได้แก่ การศึกษาช่องโหว่ของบริการเครือข่าย Wi-Fi (WEP, WPA, WPA2, WPA3) โดยการใช้เครื่องมือบนระบบปฏิบัติการ Kali Linux และการเขียนโปรแกรมหาช่องโหว่ของบริการเครือข่าย Wi-Fi

จากการศึกษาช่องโหว่ของบริการเครือข่าย Wi-Fi ได้ทราบถึงการทำงานของระบบบริการเครือข่าย Wi-Fi ได้แก่ WEP, WPA, WPA2 และ WPA3 โดยมาตรฐานการเข้ารหัสแบบ WEP และ WPA มีช่องโหว่ คือ สามารถหาค่า IV ได้ง่าย จึงมีความปลอดภัยในการใช้งานน้อยกว่า WPA และ WPA3 ซึ่งไม่ได้ใช้ค่า IV ในการเข้ารหัส

จากการทดลองในการศึกษาช่องโหว่ของบริการเครือข่าย Wi-Fi พบว่าสามารถดักจับข้อมูลการใช้งานแอกเซสพอยต์ของผู้อื่นได้ โดยวิเคราะห์ ชื่อผู้ใช้และรหัสผ่าน ในบางกรณีที่แอกเซสพอยต์ตั้งค่าไม่ให้แสดง SSID ก็สามารถวิเคราะห์ข้อมูลที่เฟรมบีคอน และในการทดลองโจมตีแอกเซสพอยต์ที่ใช้การเข้ารหัสแบบ WEP ถ้าหากดักจับข้อมูลได้จำนวนมากพอ จะทำให้สามารถทราบรหัสผ่านของแอกเซสพอยต์ได้ ส่วนแอกเซสพอยต์ที่ใช้การเข้ารหัสแบบ WPA จะเป็นการทดลองโจมตีด้วยวิธี Dictionary attack โดยจะสามารถทราบรหัสผ่านได้ถ้ารหัสผ่านนั้นมีอยู่ในไฟล์ Dictionary นอกจากนี้ได้ทำการทดลอง DoS Attack ทำให้สามารถขัดขวางหรือก่อกวนระบบเครือข่ายได้ ทำให้อุปกรณ์ที่เชื่อมต่ออยู่กับแอกเซสพอยต์หลุดการเชื่อมต่อ และได้ศึกษาการทำ Evil twin ทำให้ทราบถึงวิธีการในการเข้าถึงชื่อผู้ใช้และรหัสผ่านได้

นอกจากนี้ได้ทำการสร้างเว็บแอปพลิเคชันเพื่อให้สามารถรันคำสั่งในการศึกษาช่องโหว่ตามที่ได้ศึกษามาได้อย่างอัตโนมัติโดยมีผลการทดลองดังนี้ คือ สามารถทดสอบความสามารถการ injection แพ็กเก็ตของ Wireless USB Adapter ที่ใช้ได้ สามารถดูและปลอม MAC Address ได้ สามารถค้นหาสัญญาณ Wi-Fi และบอกรายละเอียดข้อมูลของสัญญาณ Wi-Fi ได้ และสามารถทำการค้นหารหัสผ่านได้ โดยได้นำเว็บแอปพลิเคชันไปทดลองใช้กับเครือข่าย Wi-Fi ที่อยู่บริเวณตึกภาควิชาวิศวกรรมโทรคมนาคมจำนวน 10 เครือข่าย พบว่ามีแอกเซสพอยต์จำนวน 5 อุปกรณ์ที่

สามารถค้นหารหัสผ่านได้ และมีแอกเซสพอยต์จำนวน 5 อุปกรณ์ที่ไม่สามารถค้นหารหัสผ่านได้ ซึ่งอาจเป็นเพราะไฟล์ Dictionary ที่ใช้เป็นของต่างประเทศ จึงไม่ครอบคลุมการตั้งรหัสผ่านของคนไทย

5.2 ข้อเสนอแนะ

ในการเลือกใช้เครื่องมือบนระบบปฏิบัติการ Kali Linux เพื่อหาช่องโหว่นอกเหนือจาก Wireshark ยังมีเครื่องมืออื่นที่ใช้งานเกี่ยวกับดักจับข้อมูล อ่านข้อมูลแพ็กเก็ตจากไฟล์มาวิเคราะห์ และสามารถอ่านข้อมูลจากจำนวนเครือข่ายประเภทต่างๆรวมทั้ง Ethernet และ IEEE 802.11 เช่น Wifite, Aircrack-ng และ ฯลฯ

บรรณานุกรม

[1] อนันต์ ผลเพิ่ม. *แลนไร้สาย.* กรุงเทพฯ : ซีเอ็ดยูเคชั่น, 2550.

[2] ทศพล กนกนุวัตร์. *เจาะระบบถอดรหัส.* กรุงเทพฯ: ซีเอ็ดยูเคชั่น, 2545.

[3] นนทวัตต์ สาระมาน. "การทำ Pen-test แบบมืออาชีพ."
https://medium.com/@nontawatt/-penetration-test

[4] techtalkthai. "5 การโจมตีที่พบบ่อยบน Wi-Fi พร้อมวิธีรับมือ."
https://www.techtalkthai.com/5-common-wi-fi-attacks/.

[5] อำนาจ มีมงคล, และอรรณพ ขันธิกุล. *การออกแบบและติดตั้งระบบ WirelessLAN : เจาะลึกการทำงานของ มาตรฐานไวร์เลส 802.11 abgn.* นนทบุรี : ไอดี พรีเมียร์, 2553.

[6] Vivek Ramachandran, Cameron Buchanan. "Kali Linux Wireless Penetration Testing." https://prakashkhadka.com.np/ebooks/kali_linux/Kali%20Linux%20Wireless%20Penetration%20Testing.pdf.

[7] จตุชัย แพงจันทร์. *Master in Security 3rd Edition.* นนทบุรี : ไอดีซี พรีเมียร์, 2558.

[8] Tanapoj Chaivanichanan. "รวม syntax พื้นฐานของภาษา Python ฉบับรวบรัด."
https://www.tamemo.com/post/137/python-basic-syntax/.

[9] Suphakit Annoppornchai. "Python คืออะไร โปรแกรมภาษาไพธอน ใช้ทำอะไร."
https://saixiii.com/python-programming/.