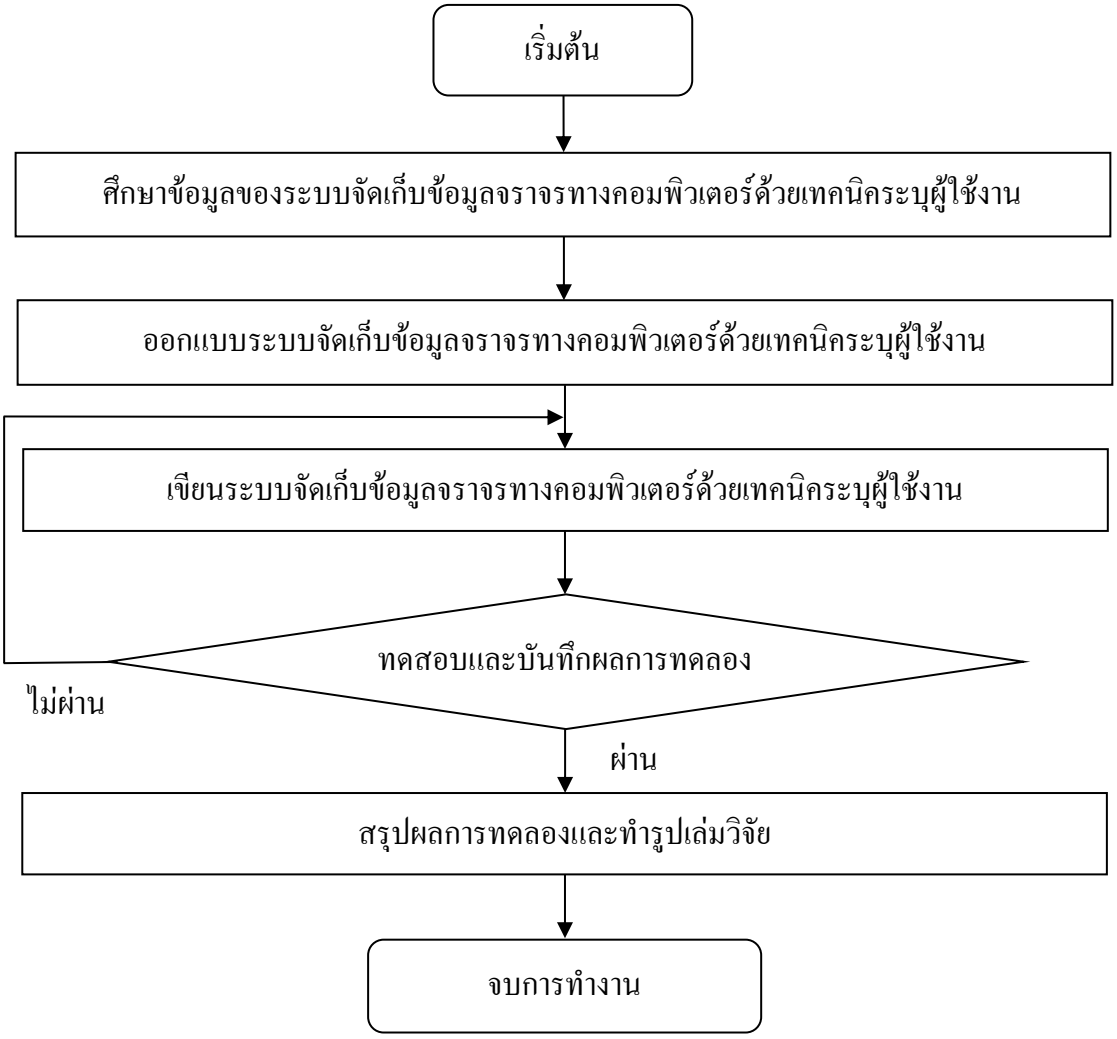
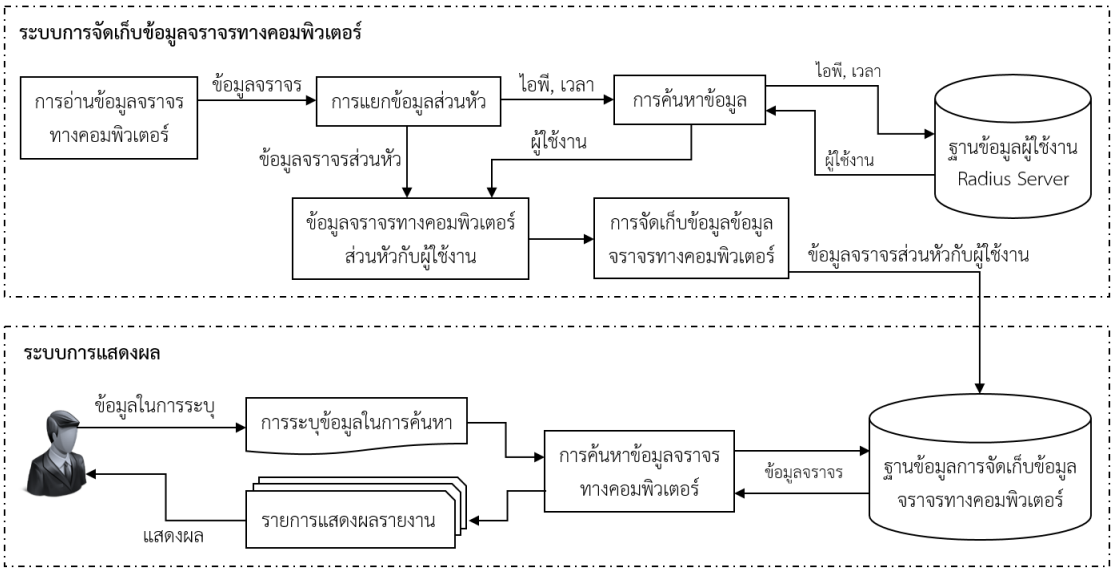
บทที่ 3
วิธีดำเนินการวิจัย

ในการจัดทำโครงการได้แบ่งขั้นตอนการดำเนินงานเป็น 2 ขั้นตอน คือ การศึกษาข้อมูลเพื่อสร้างระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ด้วยเทคนิคระบุผู้ใช้งานและการทดสอบประสิทธิภาพของระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ด้วยเทคนิคระบุผู้ใช้งาน ดังแสดงในภาพที่ 3.1



ภาพที่ 3.1 แผนภาพแสดงขั้นตอนการดำเนินงานวิจัย

ระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ด้วยเทคนิคระบุผู้ใช้งานแบ่งออกเป็น 2 ส่วน คือ ระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์และระบบการแสดงผล 1) ระบบการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ทำการอ่านข้อมูลจราจรทางคอมพิวเตอร์ทั้งหมด ส่งต่อไปยังระบบแยกข้อมูลส่วนหัวและทำการค้นหาผู้ใช้งานในฐานข้อมูล Radius Server โดยใช้ไอพีและเวลา เมื่อได้ผู้ใช้งานแล้ว ข้อมูลผู้ใช้งานจะถูกนำไปรวมกับข้อมูลจราจรทางคอมพิวเตอร์ จากนั้นระบบจะทำการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์และผู้ใช้งานลงในฐานข้อมูล 2) ระบบการแสดงผล ระบุข้อมูลที่ต้องการค้นหา จากนั้นข้อมูลที่ต้องการค้นหาจะถูกส่งไปค้นหาในฐานข้อมูล ข้อมูลจะถูกกรองตามที่ผู้ดูแลเป็นคนกำหนด เช่น ระบุไอพี วัน เวลา ผู้ใช้งาน และข้อมูลที่ค้นหาได้จะถูกส่งกลับมายังรายการแสดงผลรายงานและแสดงผลให้ผู้ดูแล ดังภาพที่ 3.2



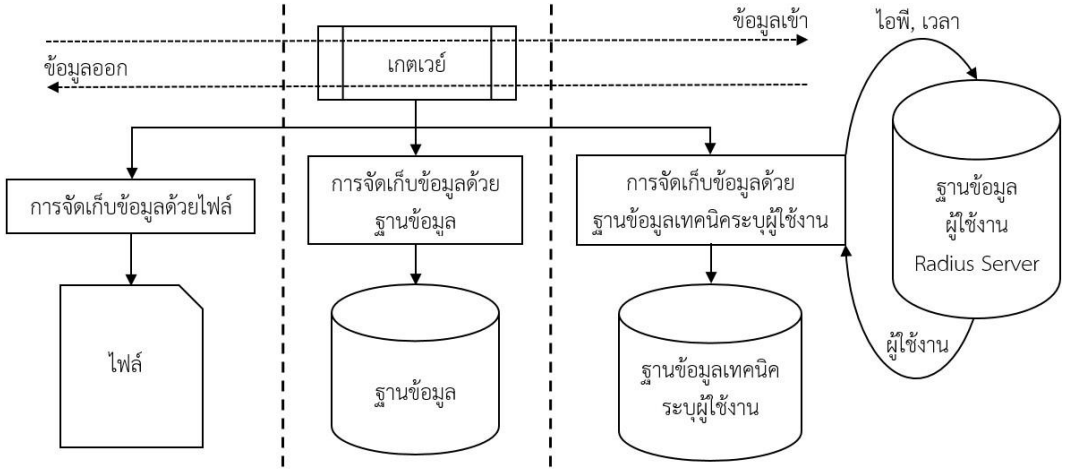
ภาพที่ 3.2 ขั้นตอนการทำงานของระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ด้วยเทคนิคระบุผู้ใช้งาน

ข้อมูลจราจรทางคอมพิวเตอร์ถูกจัดเก็บในระบบฐานข้อมูลโดยการจัดเก็บข้อมูลจะมีวิธีการดังนี้ ข้อมูลจราจรทางคอมพิวเตอร์จะมีการสื่อสารข้อมูลผ่านเกตเวย์และตัวเกตเวย์จะทำการส่งข้อมูลจราจรทางคอมพิวเตอร์ไปจัดเก็บข้อมูลไว้ในไฟล์และฐานข้อมูล ซึ่งในการออกแบบการทดลองจะใช้การทดลองทั้งหมด 3 แบบคือ การจัดเก็บข้อมูลด้วยไฟล์ การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ด้วยฐานข้อมูลและการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ด้วยฐานข้อมูลด้วยเทคนิคระบุผู้ใช้งาน มีรายละเอียดดังนี้

1) การจัดเก็บข้อมูลด้วยไฟล์ข้อมูลการสื่อสารผ่านเกตเวย์และทำการจัดเก็บข้อมูลไว้ในไฟล์ซึ่งเป็นวิธีการทั่วไปของระบบการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ วิธีการนี้ไม่ซับซ้อนและรวดเร็วในการเขียนข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลไม่มีการปรับแต่งหรือแก้ไขแต่การเข้าถึงข้อมูลใช้เวลานานขึ้นอยู่กับขนาดของไฟล์

2) การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ด้วยฐานข้อมูลข้อมูลการสื่อสารผ่านเกตเวย์และทำการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ด้วยฐานข้อมูล แต่ยังไม่มีส่วนของการระบุผู้ใช้งานซึ่งเป็นวิธีการที่อำนวยความสะดวกในการบันทึกข้อมูลได้เป็นอย่างดีเป็นการจัดเก็บข้อมูลที่ทันสมัย ลดการซ้ำซ้อนในการจัดเก็บข้อมูล รวมทั้งกำหนดผู้ที่ได้รับอนุญาตให้ใช้งานระบบฐานข้อมูลทำให้มีความปลอดภัยมากขึ้น ในการเข้าถึงข้อมูลมีความสะดวกรวดเร็วขึ้น

3) การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ด้วยฐานข้อมูลด้วยเทคนิคระบุผู้ใช้งานเป็นส่วนของการจัดเก็บข้อมูลที่มีการแยกข้อมูลส่วนหัวและทำการค้นหาผู้ใช้งานโดยใช้ไอพี, เวลา จากนั้นข้อมูลผู้ใช้งานจะถูกนำไปรวมกับข้อมูลจราจรทางคอมพิวเตอร์และทำการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ด้วยฐานข้อมูล ดังภาพที่ 3.3

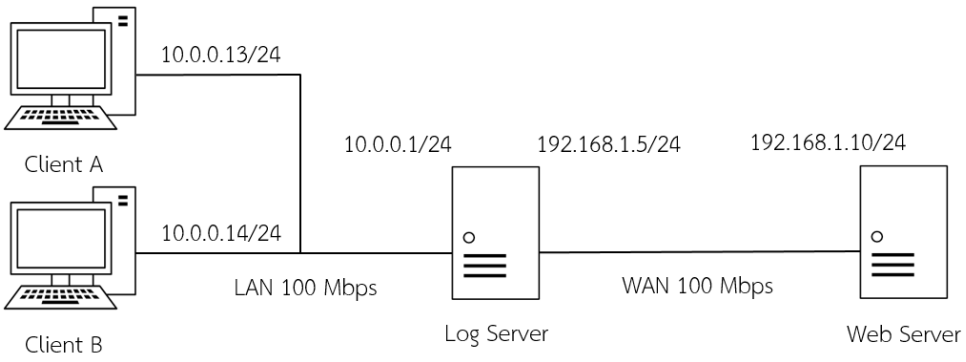


ภาพที่ 3.3 การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ทั้ง 3 รูปแบบ

การออกแบบการทดลอง

การทดลองการเข้าถึงข้อมูลของระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ด้วยเทคนิคระบุผู้ใช้งาน ประกอบด้วยการทดลอง 2 ส่วน คือ การทดลองการทำงานของระบบเก็บข้อมูลจราจรทางคอมพิวเตอร์และการทดลองหาค่าประสิทธิภาพในการเข้าถึงข้อมูลของระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ด้วยเทคนิคระบุผู้ใช้งาน การทดลองกำหนดรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์แบ่งออกเป็น 3 ส่วน คือ 1) ส่วนของเครื่องคอมพิวเตอร์ลูกข่ายจำนวน 2 เครื่อง และทำ

การเชื่อมต่อไปยังคอมพิวเตอร์แม่ข่ายที่มีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์โดยใช้ระบบปฏิบัติการลินุกซ์ซึ่งมีความเร็วในการเชื่อมต่อเครือข่ายสูงสุดที่ 100 เมกะบิตต่อวินาที โดยกำหนดเป็นไอพีภายใน 2) ส่วนของเครื่องคอมพิวเตอร์แม่ข่ายที่มีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์โดยใช้ระบบปฏิบัติการลินุกซ์ (CentOS) และใช้เซอร์วิสในการอ่านข้อมูลจราจรทางคอมพิวเตอร์ที่เป็น Tcpdump มีระบบระบุตัวตนผู้ใช้งาน RADIUS โดยควบคุมผ่านโปรแกรม Freeradius และมี Mysql เป็นฐานข้อมูลโดยมี Hotspot ที่ใช้ในการพิสูจน์ทราบตัวตน (Authentication) ซึ่งมีการเชื่อมต่ออยู่ 2 ส่วน คือ ส่วนการเชื่อมต่อของระบบเครือข่ายภายใน (LAN) และส่วนการเชื่อมต่อของระบบเครือข่ายภายนอก (WAN) โดยเชื่อมต่อไปยังเครื่องคอมพิวเตอร์แม่ข่ายที่ทำหน้าที่ในการให้บริการเว็บ 3) ส่วนของเครื่องคอมพิวเตอร์แม่ข่ายที่ทำหน้าที่ในการให้บริการเว็บโดยใช้ LAMP ซึ่งอยู่ในระบบปฏิบัติการลินุกซ์และมีความเร็วในการเชื่อมต่อเครือข่ายสูงสุดที่ 100 เมกะบิตต่อวินาที โดยกำหนดเป็นไอพีภายนอก ดังภาพที่ 3.4



ภาพที่ 3.4 การเชื่อมต่อการทดลองการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ด้วยเทคนิคระบุผู้ใช้งาน

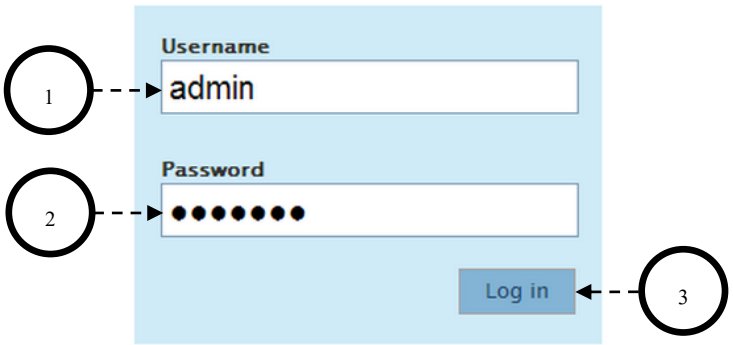
การเชื่อมต่อในการทดลองกำหนดให้เครื่องคอมพิวเตอร์แม่ข่ายที่ทำหน้าที่ในการให้บริการเว็บซึ่งมีไฟล์ขนาด 2 กิกะไบต์ กำหนดความเร็วแบนด์วิธที่ 10, 100, 1000, 10000 และ 100000 กิโลบิตต่อวินาที โดยเครื่องคอมพิวเตอร์ลูกข่ายมีการร้องขอดาวน์โหลดไฟล์จากเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการเว็บผ่านเครื่องคอมพิวเตอร์แม่ข่ายที่มีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ซึ่งเครื่องคอมพิวเตอร์ลูกข่ายดาวน์โหลดไฟล์แต่ละครั้งโดยใช้แบนด์วิธที่ต่างกัน การทดลองแบ่งเป็น 2 ส่วน คือ 1) การทดลองการทำงานของระบบเก็บข้อมูลจราจรทางคอมพิวเตอร์กำหนดค่าแบนด์วิธในเครือข่ายคอมพิวเตอร์ โดยกำหนดค่าแบนด์วิธที่ 10-100000 กิโลบิตต่อวินาที ประกอบด้วยการทดลอง 4 ส่วน คือ ส่วนค่าเฉลี่ยการทำงานของหน่วยประมวลผล, ส่วนค่าเฉลี่ยผลรวมพื้นที่หน่วยความจำที่ใช้งาน, ส่วนค่าเฉลี่ยจำนวนข้อมูลและค่าเฉลี่ยขนาดของฐานข้อมูลและไฟล์โดย

กำหนดช่วงเวลาบันทึกผลทั้งหมดที่ 100 วินาที ซึ่งจะเก็บค่าข้อมูลทุก 1 วินาที 2) การทดลองค่าประสิทธิภาพในการเข้าถึงข้อมูลของระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ด้วยเทคนิคระบุผู้ใช้งานประกอบด้วยการทดลองการเข้าถึงข้อมูล 3 ส่วน คือ ส่วนค่าเฉลี่ยประสิทธิภาพในการเข้าถึงข้อมูลของระบบจัดเก็บข้อมูล 10, 20, 30, 40, 50, 60, 70, 80, 90 และ 100 เปอร์เซ็นต์ กำหนดค่าขนาดจำนวนข้อมูลที่ 10000, 100000, 1000000 และ 10000000 ข้อมูล โดยการหาค่าเฉลี่ยเริ่มต้นด้วยการค้นหาข้อมูลในระบบจัดเก็บข้อมูล 10, 20, 30, 40, 50, 60, 70, 80, 90 และ 100 เปอร์เซ็นต์ ทำการทดลองซ้ำจำนวน 10 ครั้ง

ค่าประสิทธิภาพในการเข้าถึงข้อมูลคำนวณโดยสมการเปอร์เซ็นต์เทจอินครีส การคำนวณหาค่าเปอร์เซ็นต์อัตราการเพิ่มขึ้น (Percentage Increase) ดังสมการที่ 1 กำหนดให้ E คือ ค่าประสิทธิภาพที่เพิ่มขึ้น, N คือ ค่าความเร็วในการเข้าถึงข้อมูลที่เพิ่มขึ้น, O คือ ค่าความเร็วในการเข้าถึงข้อมูลเดิม

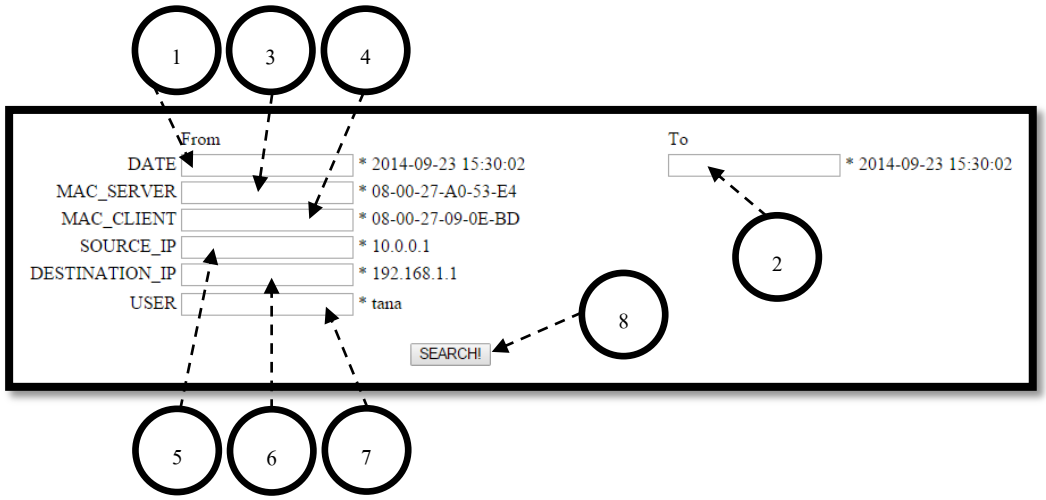
$$E = \frac{N-O}{|O|} \times 100\% \quad (1)$$

การออกแบบอินเตอร์เฟส



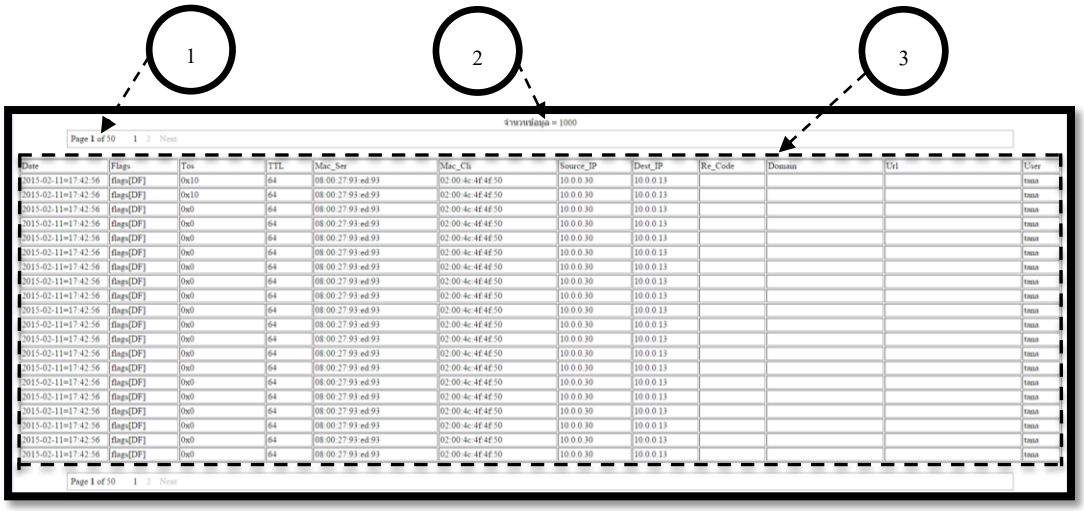
ภาพที่ 3.5 หน้าต่างเข้าสู่ระบบ TCPDUMP

จากภาพที่ 3.5 แสดงการออกแบบหน้าต่างเข้าสู่ระบบ TCPDUMP โดยหมายเลข 1 แสดงช่องใส่ Username, หมายเลข 2 แสดงช่องใส่ Password, หมายเลข 3 แสดงปุ่มกด Log in (Submit)



ภาพที่ 3.6 แสดงช่องกรอกข้อมูลค้นหา

จากภาพที่ 3.6 แสดงช่องกรอกข้อมูลค้นหา โดยหมายเลข 1 แสดงช่องใส่ วัน เดือน ปี เวลาเริ่มต้น, หมายเลข 2 แสดงช่องใส่ วัน เดือน ปี เวลาสิ้นสุด, หมายเลข 3 แสดงช่องใส่ Mac Address Server, หมายเลข 4 แสดงช่องใส่ Mac Address Client, หมายเลข 5 แสดงช่องใส่ ไอพีต้นทาง, หมายเลข 6 แสดงช่องใส่ ไอพีปลายทาง, หมายเลข 7 แสดงช่องใส่ ชื่อผู้ใช้งาน, หมายเลข 8 แสดงปุ่ม Search! (Submit)



ภาพที่ 3.7 แสดงรายการค้นหา

จากภาพที่ 3.7 แสดงรายการค้นหา โดยหมายเลข 1 แสดงจำนวนหมายเลขหน้า, หมายเลข 2 แสดงจำนวนข้อมูลที่ค้นหาได้, หมายเลข 3 แสดงรายการทั้งหมด เช่น Date, Flags, Tos, TTL, Mac_Ser, Mac_Cli, Source_IP, Destination_IP, Re_Code, Domain, Url, User เป็นต้น