# การนำเสนอข้อมูลการสื่อสารในระบบเครือข่าย คอมพิวเตอร์โดยใช้กระดาน 3 มิติ

ชนาธิป ชื่นมนัส

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตรมหาบัณฑิต (วิทยาการคอมพิวเตอร์)
คณะสถิติประยุกต์
สถาบันบัณฑิตพัฒนบริหารศาสตร์
2552

**การนำเสนอข้อมูลการสื่อสารในระบบเครือข่าย**
**คอมพิวเตอร์โดยใช้กระดาน 3 มิติ**
**ชนาธิป ชื่นมนัส**
**คณะสถิติประยุกต์**

---

คณะกรรมการสอบวิทยานิพนธ์ ได้พิจารณาแล้วเห็นสมควรอนุมัติให้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต (วิทยาการคอมพิวเตอร์)

รองศาสตราจารย์ ..... ประธานกรรมการ
(ดร.พิพัฒน์ หิรัณย์วณิชชากร)

ผู้ช่วยศาสตราจารย์ ..... กรรมการและอาจารย์ที่ปรึกษาวิทยานิพนธ์
(ดร.โอม ศรนิล)

รองศาสตราจารย์ ..... กรรมการ
(ดร.สุรพงค์ เอื้อวัฒนามงคล)

ผู้ช่วยศาสตราจารย์ ..... กรรมการ
(ดร.รวิวรรณ เทนอิสสระ)

รองศาสตราจารย์ ..... คณบดี
(ดร.สุรพงค์ เอื้อวัฒนามงคล)
วันที่ 27 เดือน พ.ค. พ.ศ. 2552

# บทคัดย่อ

**ชื่อวิทยานิพนธ์** การนำเสนอข้อมูลการสื่อสารในระบบเครือข่ายคอมพิวเตอร์ โดยใช้กระดาน 3 มิติ
**ชื่อผู้เขียน** นายชนาธิป ชื่นมนัส
**ชื่อปริญญา** วิทยาศาสตรมหาบัณฑิต (วิทยาการคอมพิวเตอร์)
**ปีการศึกษา** 2552

---

วิทยานิพนธ์ฉบับนี้เสนอวิธีการนำเสนอข้อมูลการสื่อสารในเครือข่ายคอมพิวเตอร์ เพื่อช่วยให้ผู้ดูแลระบบเครือข่ายเข้าใจสภาวะการติดต่อสื่อสาร และสามารถตรวจจับความผิดปกติที่เกิดขึ้นในเครือข่าย โดยใช้เทคนิคคอมพิวเตอร์กราฟฟิกส์ 3 มิติและการออกแบบส่วนประสานกับผู้ใช้ในการควบคุมการแสดงผลและค้นหาข้อมูล ข้อมูลการสื่อสารจะถูกแสดงบนแผ่น 3 แผ่นที่ตั้งฉากกัน ใน พื้นที่ 3 มิติ การแสดงความสัมพันธ์ระหว่างข้อมูลบนแผ่นกระดานแต่ละแผ่นใช้เส้นเชื่อมระหว่างวัตถุบนแผ่นกระดานทั้งสาม และใช้สีของเส้นในการกำหนดปริมาณของการติดต่อสื่อสารในเครือข่ายคอมพิวเตอร์ ระบบ ต้นแบบได้ถูกพัฒนาขึ้นตามหลักการออกแบบที่นำเสนอและทำการประเมินประสิทธิผลโดยผู้ประเมินจำนวน 6 คน ผลการประเมินประสิทธิผลแสดงให้เห็นว่าผู้ประเมินส่วนใหญ่มีระดับความพึงพอใจต่อส่วนประกอบต่างๆ ของระบบอยู่ในระดับมาก และวิธีการนำเสนอข้อมูลการสื่อสารที่เสนอในงานวิจัยนี้สามารถช่วยให้ผู้ใช้เข้าใจความผิดปกติที่เกิดขึ้นภายในเครือข่ายคอมพิวเตอร์ได้

# ABSTRACT


| | |
|---|---|
| **Title of Thesis** | Three Dimensional Panel Approach to Network Traffic Visualization |
| **Author** | Mr. Chanatip Chuenmanus |
| **Degree** | Master of Science (Computer Science) |
| **Year** | 2009 |


---


This thesis proposes a novel approach to visualize network traffic which helps network administrators understand status of the traffic and detect anomalies in the communications. Data are displayed on perpendicular panels divided into three parts in a three-dimensional space. Relationships between data on different panels are represented as colored links connecting objects on those panels.

A prototype application is created according to the design principle and evaluated by six experimenters. The results show that the approach is satisfactory, and it can help administrators detect and understand anomalies in the network traffic.

# กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลงได้เนื่องมาจากบุคคลหลายท่านให้ความกรุณาช่วยเหลือในการให้ข้อมูล คำแนะนำปรึกษา ข้อเสนอแนะและความคิดเห็นต่างๆ และให้กำลังใจ

ผู้เขียนขอขอบพระคุณ อาจารย์ที่ปรึกษาวิทยานิพนธ์ ผศ.ดร.โอม ศรนิล ในความกรุณาของท่านที่ได้ให้คำแนะนำปรึกษาในทุกด้าน ให้ข้อมูลและแนวทางการทำวิจัยในทุกขั้นตอน ขอขอบพระคุณ รศ.ดร.พิพัฒน์ หิรัณย์วณิชชากร ขอขอบพระคุณ รศ.ดร.สุรพงค์ เอื้อวัฒนามงคล และขอขอบพระคุณ ผศ.ดร.รวิวรรณ เทนอิสสระ ที่ได้สละเวลาในการตรวจทานแก้ไข จนวิทยานิพนธ์ฉบับนี้สำเร็จสมบูรณ์

ขอขอบพระคุณ อาจารย์ทุกท่านของผู้เขียน ที่ได้ถ่ายทอดความรู้ให้แก่ผู้เขียน ขอขอบคุณเจ้าหน้าที่ของคณะสถิติประยุกต์ทุกท่าน ที่ได้ให้ความช่วยเหลือและประสานงานเป็นอย่างดี และขอขอบคุณ เพื่อนของผู้เขียน ที่ได้ให้กำลังใจแก่ผู้เขียนตลอดมา

ในท้ายที่สุดนี้ ขอกราบขอบพระคุณ บิดา มารดา และยายของผู้เขียน ที่ได้ส่งเสริมสนับสนุน เป็นกำลังใจ อีกทั้งให้ความรักและความปรารถนาดีแก่ผู้เขียนมาโดยตลอด ขอขอบคุณ แมวของผู้เขียน ที่ทำให้ผู้เขียนอารมณ์ดีและผ่อนคลายในการทำวิทยานิพนธ์ฉบับนี้อยู่เสมอ

ชนาธิป ชื่นมนัส

เมษายน 2552

# สารบัญ

หน้า

# สารบัญตาราง

**ตารางที่** **หน้า**

# สารบัญภาพ

**ภาพที่** **หน้า**

# บทที่ 1

# บทนำ

## 1.1 ความเป็นมาของปัญหา

ปัญหาการบุกรุกทางเครือข่ายคอมพิวเตอร์ในปัจจุบัน มีแนวโน้มของความรุนแรงและปริมาณของปัญหาที่เพิ่มขึ้นอยู่ตลอดเวลา เหตุการณ์ต่างๆ ที่เกิดขึ้นในเครือข่ายคอมพิวเตอร์เป็นสิ่งที่ผู้ดูแลระบบต้องใช้ความเชี่ยวชาญ และประสบการณ์ในการวิเคราะห์ว่ามีความผิดปกติหรือมีผู้บุกรุกหรือไม่ เนื่องจากข้อมูลที่อยู่ในเครือข่ายคอมพิวเตอร์มีปริมาณมากและมีความซับซ้อน อีกทั้งการที่ผู้บุกรุกมีวิธีการที่หลากหลายในการโจมตี ทำให้มีวิธีจำนวนมากที่ใช้ เพื่อวิเคราะห์ความผิดปกติหรือผู้บุกรุก การ ออกแบบระบบที่ช่วยผู้ดูแลระบบในการตรวจสอบถึงความผิดปกติจึงมีความจำเป็น

Network Intrusion Detection System (NIDS) เป็นระบบที่ถูกออกแบบ เพื่อช่วยตรวจสอบเครือข่ายคอมพิวเตอร์จากการโจมตี โดยจะวิเคราะห์ข้อมูลในเครือข่ายหรือ Packet ที่ส่งผ่านกันในเครือข่ายว่าเป็นการบุกรุกหรือไม่ โดยเปรียบเทียบกับกฎหรือรูปแบบที่ได้กำหนดไว้หรือจากสถิติการโจมตีที่ผ่านมา ข้อมูลที่ได้จะแสดงให้ผู้ดูแลระบบ ทราบถึงเหตุการณ์และเวลาที่เกิดขึ้นในเครือข่าย เพื่อจะได้หยุดความเสียหายไว้ได้ทัน

เทคนิคการแสดงข้อมูลในปัจจุบัน ส่วนใหญ่จะเป็น แบบ Textual คือแสดงข้อมูลในรูปแบบตัวอักษร โดยจะเน้นไปที่การแสดงรายละเอียดของข้อมูล แต่ยังขาดการแสดงภาพรวมของข้อมูล การที่ข้อมูลมีปริมาณมากทำให้ยากแก่ผู้ใช้ในการวิเคราะห์ข้อมูลหรือความผิดปกติ จึงได้มีการพัฒนาเทคนิคในการแสดงข้อมูลให้ดียิ่งขึ้น

Visualization คือเทคนิคที่ใช้ในการนำข้อมูลที่เป็นนามธรรมมาแสดงให้เป็นภาพ เพื่อเพิ่มประสิทธิผลในการติดต่อสื่อสาร หรือทำให้เข้าใจข้อมูลได้ง่ายขึ้น เช่น การใช้สี รูปร่าง หรือสัญลักษณ์ เทคนิคที่ใช้จะแตกต่างกันขึ้นกับชนิดของข้อมูล และลักษณะการแสดงข้อมูล เป็นต้น

ในงานวิจัยนี้ได้นำเสนอโปรแกรมต้นแบบ ซึ่งใช้เทคนิค Visualization ในการนำเสนอข้อมูลการสื่อสารในเครือข่ายคอมพิวเตอร์บนแผ่นกระดาน 3 แผ่น ที่ตั้งฉากกัน ใน พื้นที่ 3 มิติ โดยใช้เส้นเชื่อมระหว่างวัตถุบนแผ่นกระดานทั้งสาม ในการแสดง ความสัมพันธ์ระหว่างข้อมูลบนแผ่นกระดานแต่ละแผ่น และใช้สีของเส้นในการกำหนดปริมาณของการติดต่อสื่อสารในเครือข่ายคอมพิวเตอร์ แนวคิดนี้แตกต่างจากแนวคิดที่ใช้ในงานวิจัยอื่นในการแสดงให้ผู้ใช้เห็นถึงภาพรวม

ของข้อมูล โดยการจัดวางข้อมูลที่แตกต่างกันในพื้นที่บนแผ่นกระดานทั้งสามซึ่งช่วยให้ผู้ใช้วิเคราะห์ข้อมูลได้ง่ายขึ้น และแสดงความสัมพันธ์ระหว่างข้อมูลบนแผ่นกระดานแต่ละแผ่นโดยใช้เส้นเชื่อมระหว่างวัตถุบนแผ่นกระดานทั้งสาม

## 1.2 วัตถุประสงค์งานวิจัย

งานวิจัยนี้มีวัตถุประสงค์เพื่อนำเสนอวิธีการแสดงข้อมูลโดยใช้เทคนิค Visualization 3 มิติ เพื่อให้ผู้ผู้ดูแลระบบเครือข่ายสามารถทราบถึงสภาวะการสื่อสาร และเข้าใจความผิดปกติที่เกิดขึ้นภายในเครือข่ายคอมพิวเตอร์ได้

## 1.3 ขอบเขตงานวิจัย

นำเสนอวิธีการแสดงข้อมูลโดยใช้เทคนิค Visualization 3 มิติ เพื่อแสดงข้อมูลและความผิดปกติที่เกิดขึ้นภายในเครือข่ายคอมพิวเตอร์ โดยงานวิจัยนี้มุ่งเน้นที่วิธีการแสดงข้อมูล และการออกแบบส่วนประสานกับผู้ใช้ (User Interface) ในการควบคุมการแสดงผลและการค้นหาข้อมูล

## 1.4 วิธีการดำเนินงานวิจัย

1.4.1 ศึกษาเอกสารและงานวิจัยที่เกี่ยวข้อง
1.4.2 ออกแบบโครงสร้างและหลักการทำงานของระบบ
1.4.3 พัฒนาระบบต้นแบบตามที่ได้ออกแบบไว้
1.4.4 ทำการประเมินประสิทธิผลของระบบ
1.4.5 สรุปผลการวิจัยและข้อเสนอแนะ

## 1.5 ประโยชน์ที่คาดว่าจะได้รับ

ช่วยให้ผู้ดูแลระบบเครือข่ายเข้าใจสภาวะการสื่อสาร และตรวจจับเหตุการณ์ผิดปกติที่เกิดขึ้นในเครือข่ายคอมพิวเตอร์ได้

# บทที่ 2

# งานวิจัยที่เกี่ยวข้อง

## 2.1 งานวิจัยที่เกี่ยวข้อง

Visualization คือวิธีการที่ใช้ในการนำข้อมูลที่เป็นนามธรรมมาแสดงให้เป็นภาพ เพื่อเพิ่มประสิทธิผลในการติดต่อสื่อสาร หรือทำให้เข้าใจข้อมูลได้ง่ายขึ้น การใช้เทคนิค Visualization มีหลายวิธี ซึ่ง แต่ละวิธีเหมาะสมที่จะใช้ในการแสดงข้อมูลที่แตกต่างกัน การเลือกใช้เทคนิคใดนั้นขึ้นกับองค์ประกอบหลายอย่าง เช่น ชนิดของข้อมูลที่จะนำมาแสดง วิธีที่ต้องการแสดงข้อมูล เป็นต้น

ในปัจจุบันมีงานวิจัยที่นำเอาเทคนิค Visualization มาใช้โดยมีจุดประสงค์เพื่อเพิ่มประสิทธิผลในการแสดงข้อมูลการติดต่อสื่อสารภายในเครือข่ายคอมพิวเตอร์ และช่วยในการวิเคราะห์ความผิดปกติที่เกิดขึ้นในเครือข่าย ในบทนี้เราจะแนะนำงานวิจัย ที่สำคัญที่ได้นำเทคนิคดังกล่าวมาใช้

### 2.1.1 NVisionIP

โปรแกรม NVisionIP (Lakkaraju, Yurcik and Lee, 2004: 65-72; Bearavolu, Lakkaraju, and Yurcik, 2005: 1-5) พัฒนาขึ้นโดยภาษา Java โปรแกรมถูกออกแบบมาเพื่อช่วยเหลือผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ ในการตรวจสอบสถานะของเครือข่ายที่ใช้ IP Address ใน Class B การออกแบบโครงสร้างของระบบใช้ D2K Data Mining Software Package ในการวิเคราะห์ข้อมูล และแสดงข้อมูลในลักษณะของ Drill-Down Levels ซึ่งแบ่งเป็น 3 ระดับ ได้แก่

Galaxy View แสดงภาพรวมของเครือข่ายคอมพิวเตอร์ ประกอบด้วยแกน 2 แกน ได้แก่ Subnet และ Host ข้อมูลที่แสดงจะใช้สีในการกำหนดปริมาณของข้อมูลในเครือข่าย ดังแสดงในภาพที่ 2.1 ซึ่งมีรายละเอียดดังนี้

(1) Menu Bar

(2) แสดงรายละเอียดต่างๆ ของโปรแกรม

(3) แสดงรายละเอียดต่างๆ ที่แสดงอยู่บน Grid

(4) แสดงรายละเอียดของ Filters ที่กำลังใช้งานอยู่

(5) ปุ่มควบคุมการเปลี่ยนแกนของ Grid และปุ่มกำหนด Filters

(6) แสดงสีที่กำหนดปริมาณของข้อมูลภายในเครือข่าย

(7) ปุ่มกำหนดรายละเอียดของสี

(8) กำหนดช่วงเวลาของข้อมูลที่จะแสดง

(9) ปุ่มสำหรับกำหนดมุมมองของ View

(10) ส่วนที่ให้ผู้ใช้สามารถเพิ่มบันทึกหรือข้อความ

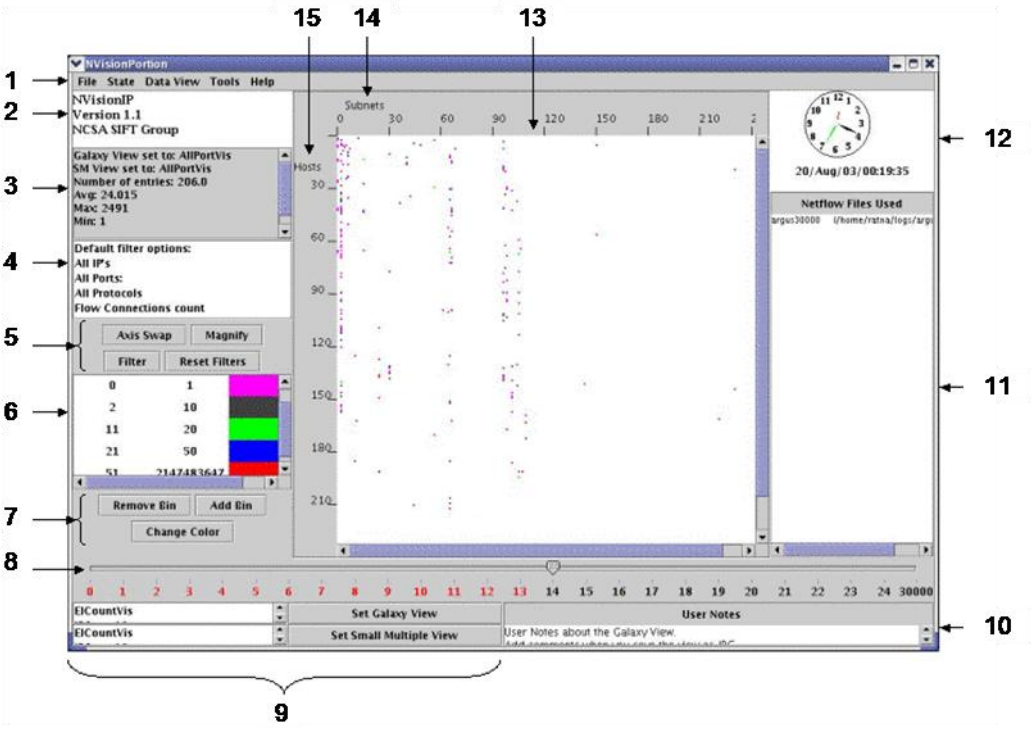
(11) แสดงรายละเอียดของข้อมูลที่ใช้ในโปรแกรม

(12) แสดงเวลาของข้อมูลที่แสดง

(13) แกน XY Grid ที่แสดงเครือข่ายใน Class B

(14) แกนของ Subnet

(15) แกนของ Hosts




**ภาพที่ 2.1** การแสดงผลในระดับ Galaxy View ของโปรแกรม NvisonIP

**แหล่งที่มา:** Bearavolu and others, 2005: 2.

Small Multiple View แสดงข้อมูลจากเครื่องคอมพิวเตอร์ทั้งหมดที่อยู่ภายในเครือข่าย โดยใช้กราฟ 2 กราฟในการแสดงปริมาณของข้อมูลของ Well-Known Port และ Port อื่นๆ และใช้สีในการกำหนดหมายเลขของ Port ดังแสดงในภาพที่ 2.2 ซึ่งมีรายละเอียดดังนี้

(1) แสดงช่วงของ IP Address ที่เลือก

(2) ปุ่มกำหนดมาตราส่วนของกราฟ

(3) ปุ่มกำหนดจำนวนของกราฟ

(4) แสดงสีที่กำหนด Port หรือ Protocol

(5) ปุ่มกำหนดรายละเอียดของสี

(6) ปุ่ม Reset ที่ใช้ในคืนการตั้งค่าต่างๆ

(7) ปุ่มแสดง Machine View

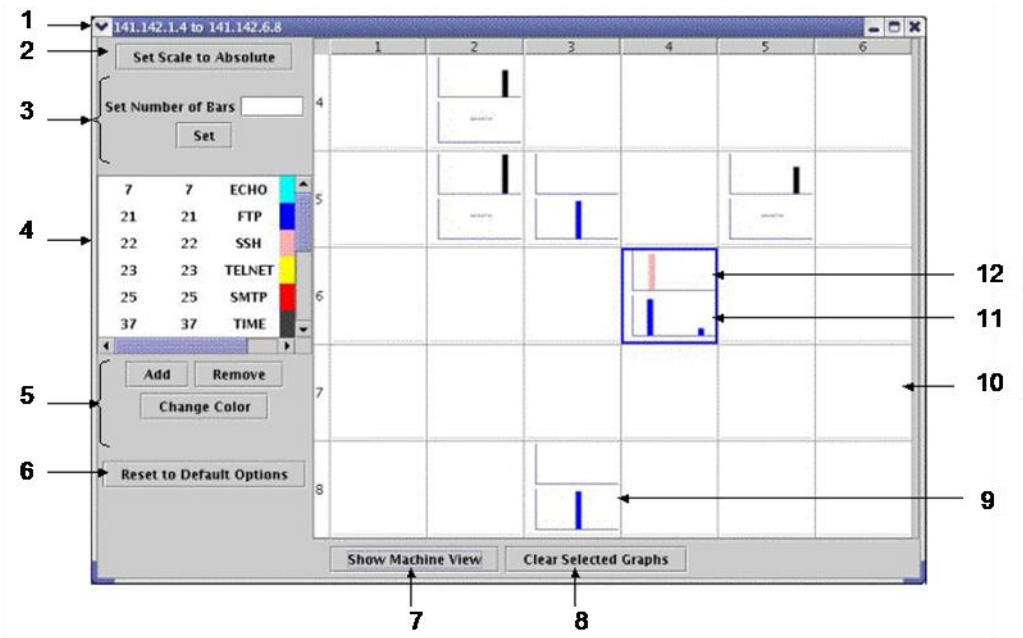
(8) ปุ่มคืนค่าการเลือกกราฟ

(9) แสดงรายละเอียดของ IP Address หมายเลขหนึ่ง

(10) แสดง IP Address ที่ไม่ได้มีการใช้งานใดๆ

(11) กราฟด้านล่างแสดง Port อื่นๆ ที่มีการใช้งาน

(12) กราฟด้านบนแสดง Port พิเศษที่มีการใช้งาน




**ภาพที่ 2.2** การแสดงผลในระดับ Small Multiple View ของโปรแกรม NvisonIP

**แหล่งที่มา:** Bearavolu and others, 2005: 3.

Machine View แสดงข้อมูลจากเครื่องคอมพิวเตอร์หนึ่งเครื่องภายในเครือข่าย โดยใช้กราฟในการแสดงปริมาณของข้อมูลใน Protocol และ Port ทั้งหมดที่ใช้โดยเครื่องคอมพิวเตอร์หนึ่งเครื่อง ดังแสดงในภาพที่ 2.3 ซึ่งมีรายละเอียดดังนี้

(1) แสดง IP Address ที่เลือก

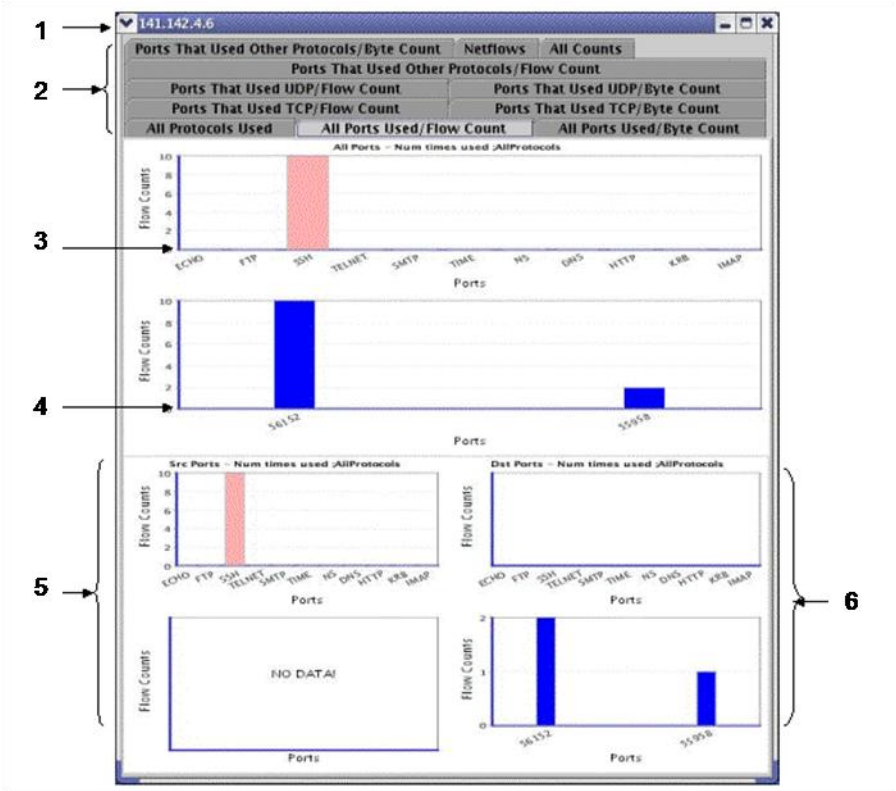
(2) Tab ที่ใช้แสดงรายละเอียดต่างๆ

(3) แสดงปริมาณข้อมูลที่ใช้ใน Port พิเศษของ IP ที่เลือก

(4) แสดงปริมาณข้อมูลที่ใช้ใน Port อื่นๆของ IP ที่เลือก

(5) กราฟแสดง Source Port ที่มีการใช้งาน

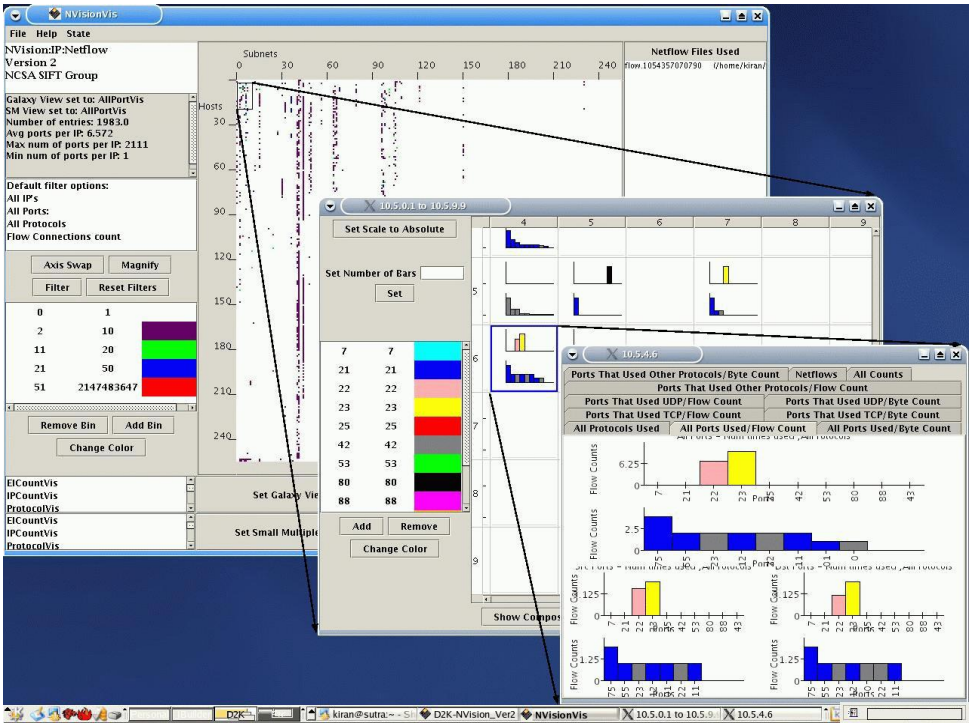
(6) กราฟแสดง Destination Port ที่มีการใช้งาน




**ภาพที่ 2.3** การแสดงผลในระดับ Machine View ของโปรแกรม NvisonIP

**แหล่งที่มา:** Bearavolu and others, 2005: 4.

ประโยชน์ของโปรแกรมนี้คือช่วยให้ผู้ใช้สามารถวิเคราะห์รูปแบบการโจมตีที่เกิดขึ้น และเข้าใจถึงการเปลี่ยนแปลงที่เกิดขึ้นในเครือข่ายคอมพิวเตอร์ โดย ใช้วิธีการแสดงข้อมูลที่มีความละเอียดแตกต่างกัน 3 ระดับคือ Galaxy View, Small Multiple View และ Machine View ดังแสดงในภาพที่ 2.4 ซึ่งผู้ใช้ สามารถเลือกระดับข้อมูลที่ต้องการและแสดงให้เห็นถึงความสัมพันธ์ของข้อมูลในระดับที่ต่างกันได้



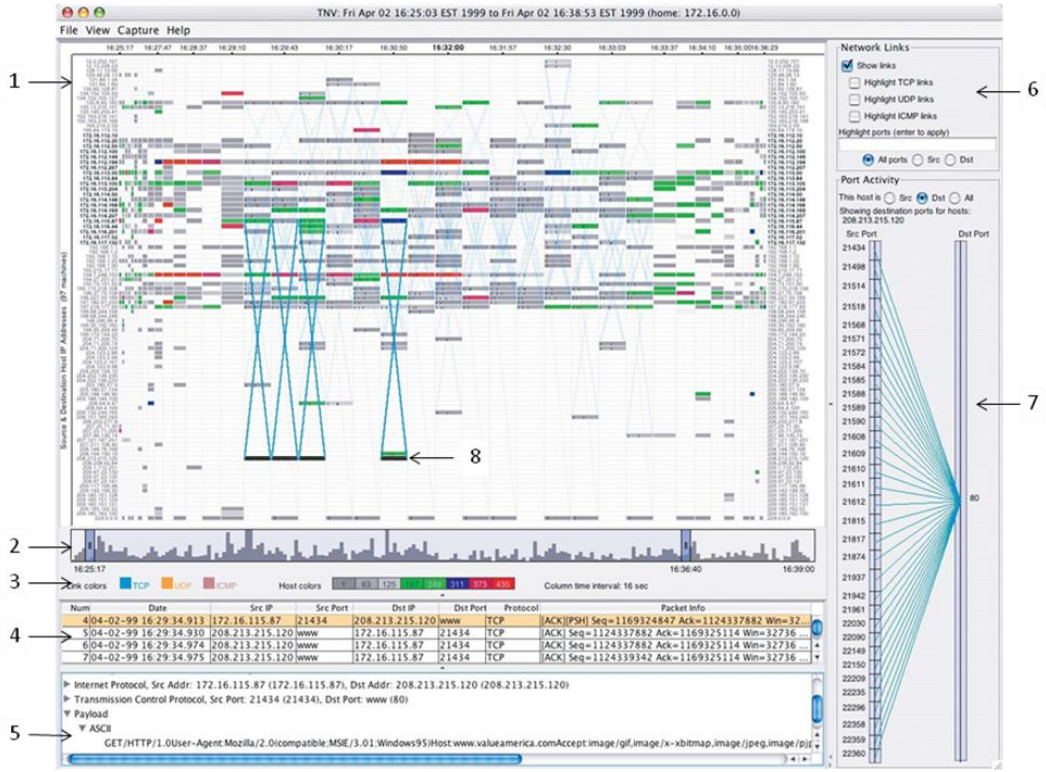

**ภาพที่ 2.4** แสดงความสัมพันธ์ในการแสดงข้อมูลที่แตกต่างกัน 3 ระดับ ของโปรแกรม NvisonIP

**แหล่งที่มา:** Lakkaraju and others, 2004: 70.

### 2.1.2 Time-Based Network Traffic Visualizer (TNV)

โปรแกรม TNV (Goodall, Lutters, Rheingans and Komlodi, 2005: 47-54, 2006: 72-80) พัฒนาขึ้นโดยใช้ภาษา Java และใช้ Jpcap Library ในการดักจับ Packet ในเครือข่าย โปรแกรมนี้ถูกออกแบบมาเพื่อวิเคราะห์การบุกรุก รูปแบบการโจมตีของผู้บุกรุก และสำรวจข้อมูลการสื่อสารในเครือข่าย ซึ่งช่วยให้ผู้ดูแลระบบสามารถเรียนรู้ระบบเครือข่ายในโครงสร้างระดับใหญ่และระดับย่อย

แนวคิดในการออกแบบโปรแกรม เพื่อสนับสนุนผู้ดูแลระบบในการดูแลระบบเครือข่าย และการวิเคราะห์ข้อมูลในเครือข่ายที่ซับซ้อน ช่วยให้เข้าใจความสัมพันธ์ของเหตุการณ์ระหว่าง Host และเข้าใจถึงการโจมตีและความผิดปกติที่เกิดขึ้นได้ โดยมีเวลาเป็นข้อมูลสำคัญในการวิเคราะห์ซึ่งจะบอกช่วงที่เกิดเหตุการณ์ และช่วงที่เกิดความผิดปกติได้ การออกแบบส่วนประสานกับผู้ใช้จะเป็นในลักษณะของ Matrix โดย Column จะแสดงเวลา และ Row จะแสดงถึง Host โดยมี Network Link แสดงความสัมพันธ์ระหว่าง Host และมี Port Activity View แสดงภาพรวมของ Port ที่ถูกใช้งานโดย Host ที่เลือก




**ภาพที่ 2.5** แสดงภาพของโปรแกรม TNV

**แหล่งที่มา:** Goodall and others, 2006: 75.

ส่วนต่างๆ ของโปรแกรม TNV ดังแสดงในภาพที่ 2.5 ประกอบไปด้วย

(1) Main Visualization Matrix เป็นส่วนแสดงหน้าจอหลักของโปรแกรม แกน X แสดงถึง Host IP Address แกน Y แสดงถึง Network Packet Timestamps และใช้เส้น (Network Link) ในการแสดงความสัมพันธ์ระหว่าง Host

(2) แสดงภาพรวมของการเปลี่ยนแปลงของข้อมูล

(3) สีแสดงจำนวนของ Packet เพื่อให้สามารถสังเกตได้ง่าย และใช้ในการกำหนดประเภทของ Protocol

(4) ตารางแสดง Packet ทั้งหมดของ Host ที่เลือก

(5) แสดงรายละเอียดของ Packet ที่เลือกในตารางหมายเลข 4

(6) Emphasis Filtering Panel ปุ่มควบคุมการกำหนด Filter ในการแสดงข้อมูล

(7) Port Activity View แสดงรายละเอียด Port ที่กำลังใช้งานของ Host ที่เลือก

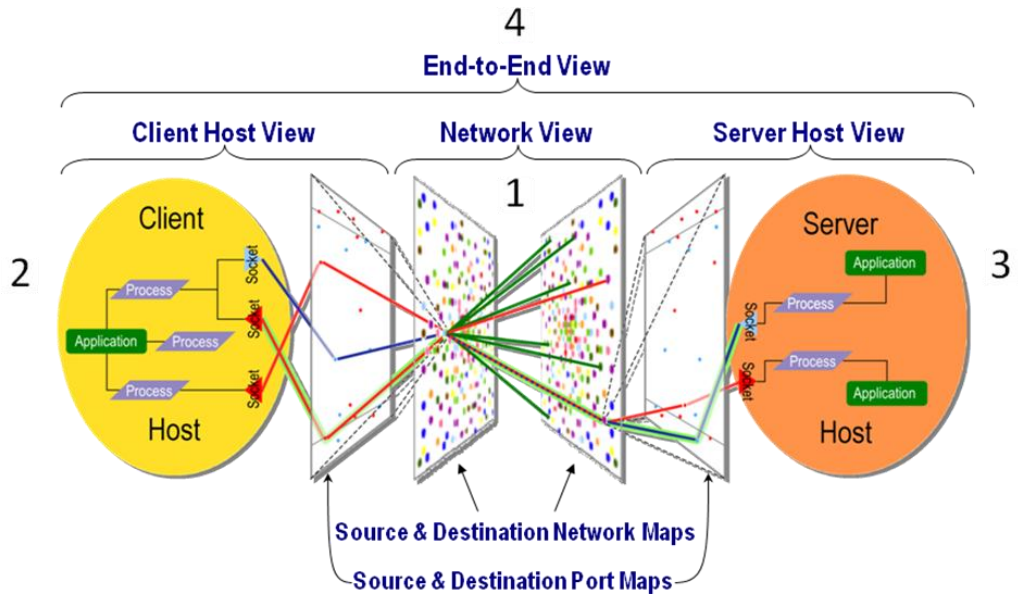
(8) ตัวอย่าง Host ที่ผู้ใช้สามารถเลือกได้

ประโยชน์ของโปรแกรม TNV คือ การแสดงภาพรวมของข้อมูลทั้งหมดในหน้าจอหลัก โดยใช้ Matrix-Based Visualization ในการวิเคราะห์ข้อมูลและกิจกรรมที่เกิดขึ้นในเครือข่าย ในส่วนของ Port Activity View จะแสดงภาพรวมของ Port ที่ถูกใช้งานโดย Host ที่เลือก และผู้ใช้สามารถเข้าถึงรายละเอียดของข้อมูลในเครือข่าย ซึ่งจะช่วยให้ผู้ใช้เห็นทั้งมุมมองขนาดใหญ่และมุมมองขนาดย่อยได้

### 2.1.3 NetworkEye

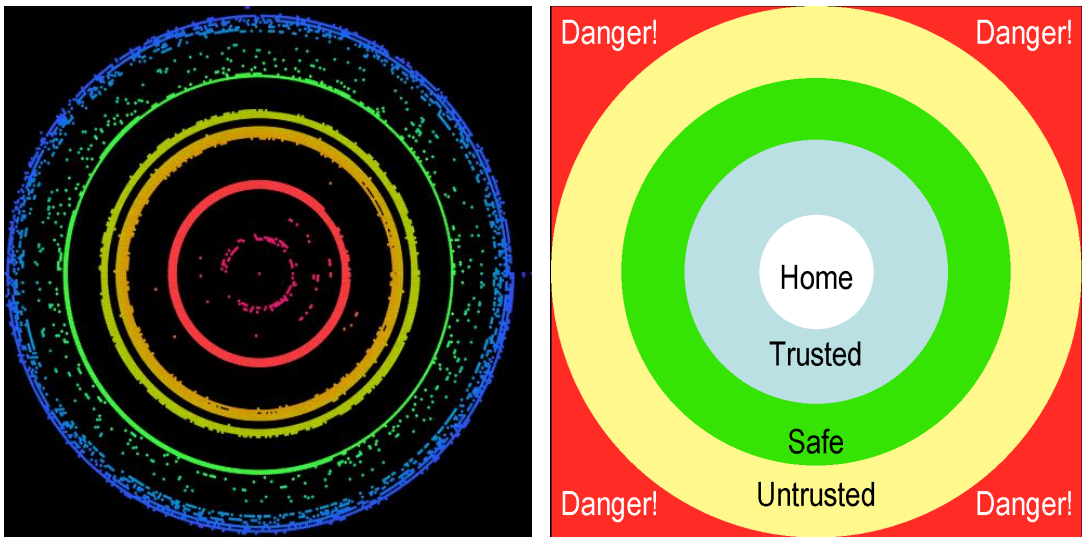
โปรแกรม NetworkEye (Fink, Ball, North, Jawalkar, and Correa, 2004: 1-15) ถูกออกแบบมาเพื่อให้ผู้ดูแลระบบมองเห็นถึงการติดต่อสื่อสารที่เกิดขึ้นภายในเครือข่าย แนวคิดที่ใช้ในการออกแบบคือ End-to-End Visualization ซึ่งเน้นไปที่การติดต่อระหว่าง End-Point รวมถึง Application, Process, Socket และ Port ที่ตอบสนองต่อการติดต่อสื่อสารทั้งหมดในเครือข่าย ซึ่งจะช่วยให้ผู้ใช้มองเห็นภาพรวม และสามารถเข้าถึงรายละเอียดย่อยของเครือข่ายได้ โปรแกรมนี้สามารถแบ่งส่วนการทำงานได้ดังในภาพที่ 2.6 ซึ่งประกอบด้วย

(1) Network View ส่วนนี้จะทำการแทนแต่ละ IP Address ด้วย Pixels ซึ่งเรียกว่า Network Pixel Map โดยโปรแกรม Network Eye จะแสดง IP Address ที่ไม่ซ้ำกันทั้งหมดในรูปของ Pixels ซึ่งสามารถแสดงได้พร้อมกันถึง 100,000 IP Address จากนั้นจึงกำหนดสีและความสว่างของ Pixels ตามประเภทและระดับของกิจกรรม ดังแสดงในภาพที่ 2.7 ซึ่งแบ่งเป็น 5 ระดับ ได้แก่ Home, Trusted, Safe, Untrusted และ Danger โดยให้ตำแหน่งที่ใกล้ศูนย์กลางที่สุดเป็นตำแหน่งของ Host ที่เชื่อถือได้มากที่สุด ระดับความน่าเชื่อถืออาจกำหนดโดยให้ IP Address ที่อยู่ภายในองค์กรมีความน่าเชื่อถือที่สุด ระดับที่อันตรายอาจเป็น IP Address ที่อยู่ใน Blacklists หรืออยู่ไกลจากองค์กร สำหรับเส้นที่แสดงการติดต่อกันระหว่าง IP Address จะเรียกว่า Communication Visualization ดังแสดงในภาพที่ 2.8 โดยสีของเส้นแสดงถึงประเภทของการติดต่อสื่อสาร ความหนาบางของเส้นแสดงปริมาณของการติดต่อสื่อสาร



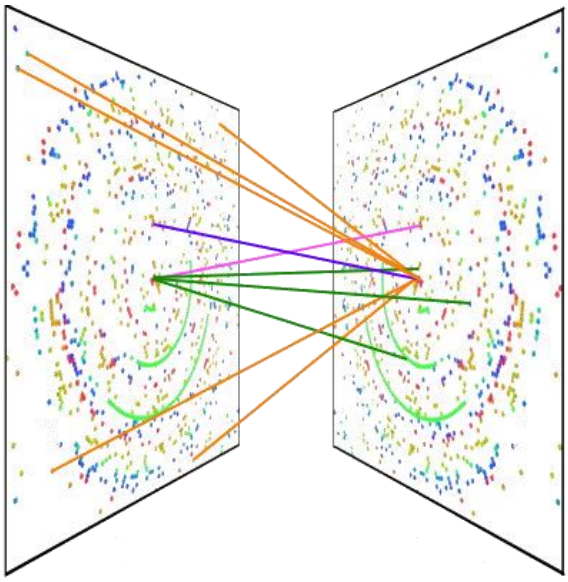

**ภาพที่ 2.6** การออกแบบส่วนประกอบต่างๆ ของโปรแกรม NetworkEye

**แหล่งที่มา:** Fink and others, 2004: 7.



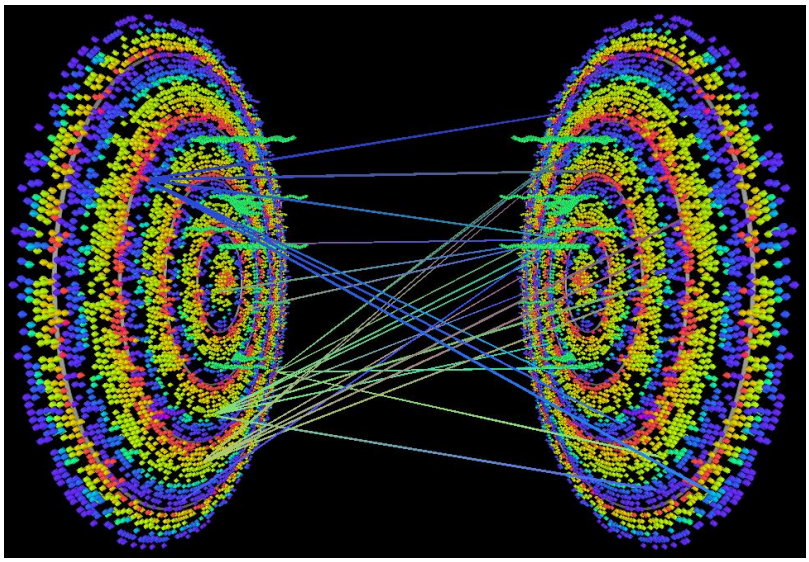

**ภาพที่ 2.7** การออกแบบในส่วน Network Pixel Map และ Trust Levels ของโปรแกรม NetworkEye

**แหล่งที่มา:** Fink and others, 2004: 8.



**ภาพที่ 2.8** การออกแบบในส่วน Communication Visualization ของโปรแกรม NetworkEye

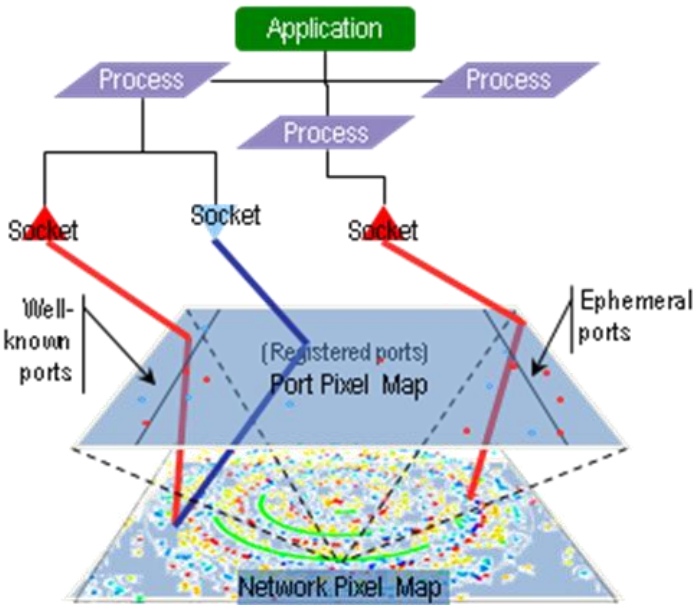
**แหล่งที่มา:** Fink and others, 2004: 8.



**ภาพที่ 2.9** แสดงภาพของ Network View ที่สร้างตามแนวคิดที่ได้ออกแบบไว้

**แหล่งที่มา:** Fink and others, 2004: 8.

(2), (3) Host View แสดงความสัมพันธ์ระหว่าง Applications, Processes, Sockets, Ports และ Remote Hosts โดยทำการแทน Pixel ซึ่งแสดง Port ในการติดต่อสื่อสาร เรียกว่า Port Pixel Map ดังแสดงในภาพที่ 2.10 โดยผู้ใช้สามารถเลือกการติดต่อสื่อสารที่สนใจและค้นหาเฉพาะ Hosts, Ports, Sockets, Processes และ Applications ที่ต้องการ โดยที่หมายเลข (2) จะเป็นส่วนของ Client Host View และหมายเลข (3) เป็นส่วนของ Server Host View




**ภาพที่ 2.10** การออกแบบในส่วน Host View ของโปรแกรม NetworkEye

**แหล่งที่มา:** Fink and others, 2004: 9.

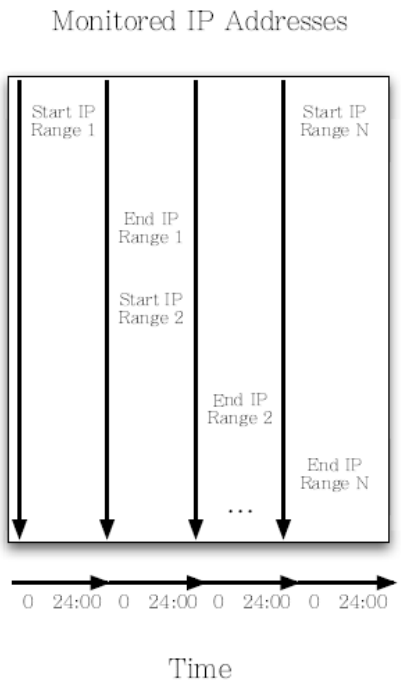
(4) End-to-End View คือการนำคุณลักษณะของ Network View และ Host View มารวมกันเพื่อให้ได้ภาพของ End-to-End ซึ่งจะช่วยให้ผู้ดูแลระบบมุ่งเน้นไปที่การติดต่อสื่อสารในจุดที่สนใจและแสดงถึง Applications, Processes, Sockets และ Ports ที่ใช้ในการติดต่อสื่อสารทั้งหมด

ประโยชน์ของโปรแกรม NetworkEye คือ แสดงข้อมูลและเหตุการณ์ผิดปกติภายในเครือข่ายคอมพิวเตอร์ เพื่อเพิ่มประสิทธิผลของระบบในการวิเคราะห์ความผิดปกติ และลดเวลาในการตรวจสอบเครือข่ายคอมพิวเตอร์

### 2.1.4 IDS RainStorm

IDS RainStorm (Abdullah, Lee, Conti, Copeland and Stasko, 2005: 1-10) ถูกออกแบบมาเพื่อแสดง IP Address ใน Class B โปรแกรมนี้จะแบ่งมุมมองออกเป็น 2 ส่วน ได้แก่ Main View สำหรับแสดงภาพรวมทั้งหมดของระบบและ Zoom View สำหรับแสดงข้อมูลที่ละเอียดขึ้นเมื่อผู้ใช้เลือกช่วงของ IP Address ที่ต้องการ รายละเอียดในแต่ละส่วนเป็นดังนี้

Main View หน้าจอหลักสำหรับแสดงภาพรวมทั้งหมดของระบบ โดยใช้เทคนิคการแสดงข้อมูลในลักษณะจากบนลงล่าง ( Top-to-Bottom) ดังแสดงในภาพที่ 2.11 แต่ละแกนในแนวตั้งแสดง IP Address ในลำดับที่ต่างกัน แกนในแนวนอนแสดงช่วงเวลาภายใน 24 ชั่วโมง ภาพที่ 2.12 จะแสดงโปรแกรมในส่วนของ Main View ที่สร้างจากแนวคิดที่ได้ออกแบบไว้ แต่ละ Pixel ในแกน X แสดงข้อมูลในช่วง 20 นาที และแต่ละช่วง IP Address ในแกน Y จะแสดงได้ประมาณ 20 IP Address เมื่อผู้ใช้เลื่อนเมาส์เลือกพื้นที่ใน Main View จะเกิดเป็นกล่องสีแดงในช่วง IP Address ที่เลือกตรงตำแหน่งนั้น IP Address ที่เลือกจะแสดงที่ด้านบนของกล่องสีแดง เมื่อผู้ใช้คลิกบนภาพจะปรากฏหน้าจอที่ 2 ขึ้นมาซึ่งจะเป็นภาพขยายของกล่องสีแดงที่ได้เลือกไว้ ซึ่งหน้าจอดังกล่าวนี้ก็คือส่วนของ Zoom View

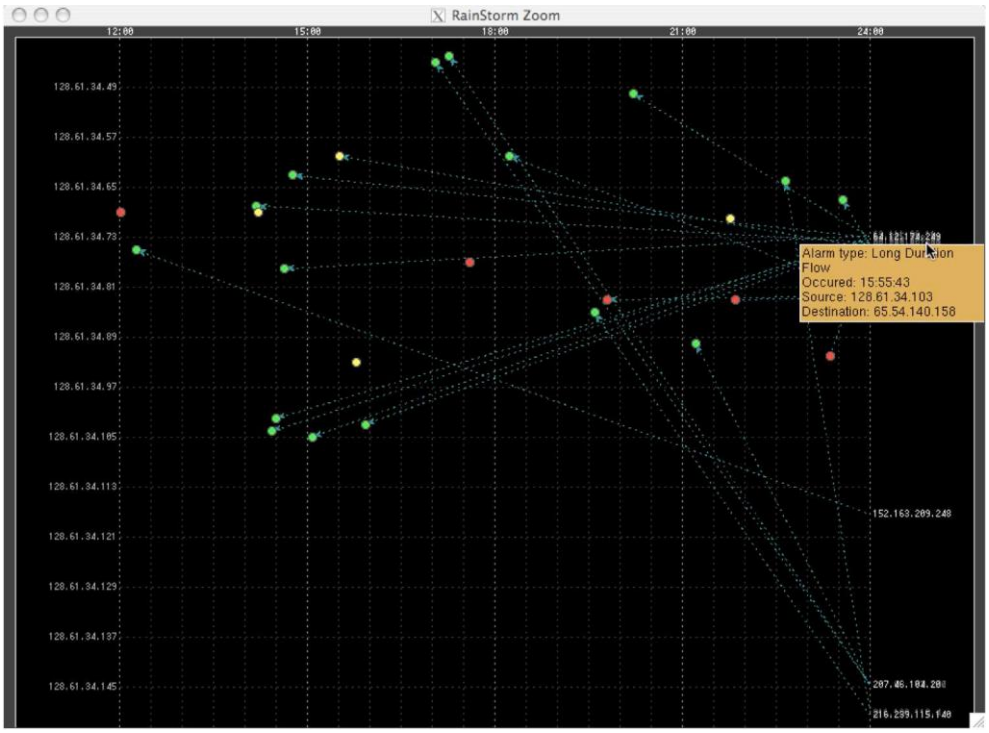



**ภาพที่ 2.11** วิธีการแสดงข้อมูล IP Address ของโปรแกรม IDS RainStorm

**แหล่งที่มา:** Abdullah and others, 2005: 2.


**ภาพที่ 2.12** โปรแกรม IDS RainStorm ในส่วนของ Main View

**แหล่งที่มา:** Abdullah and others, 2005: 4.




**ภาพที่ 2.13** โปรแกรม IDS RainStorm ในส่วนของ Zoom View

**แหล่งที่มา:** Abdullah and others, 2005: 6.

Zoom View เป็นส่วนที่แสดงรายละเอียดจากการเลือกของผู้ใช้ในส่วนของ Main View ดังแสดงในภาพที่ 2.13 ซึ่งแสดง IP Address ที่มาจากภายในที่ด้านซ้ายของแกน และแสดง IP Address ที่มาจากภายนอกที่ด้านขวาของแกน จุดสีแต่ละจุดคือ Alarm Severity (สัญญาณเตือนถึงความผิดปกติ) สีแดงหมายถึงมีความผิดปกติที่มีความรุนแรงสูง สีเหลืองหมายถึงมีความรุนแรงปานกลาง สีเขียวหมายถึงมีความรุนแรงต่ำ ซึ่งระดับสีนี้ผู้ใช้สามารถกำหนดเองได้ เส้นแสดงถึงการติดต่อระหว่าง IP Address ภายนอกและ IP Address ภายใน เมื่อผู้ใช้วางเคอร์เซอร์ของเมาส์ไว้เหนือไอคอนหรือข้อความ ข้อมูลที่เป็นคำอธิบายจะถูกขยายออกมา เรียกว่า Glossing

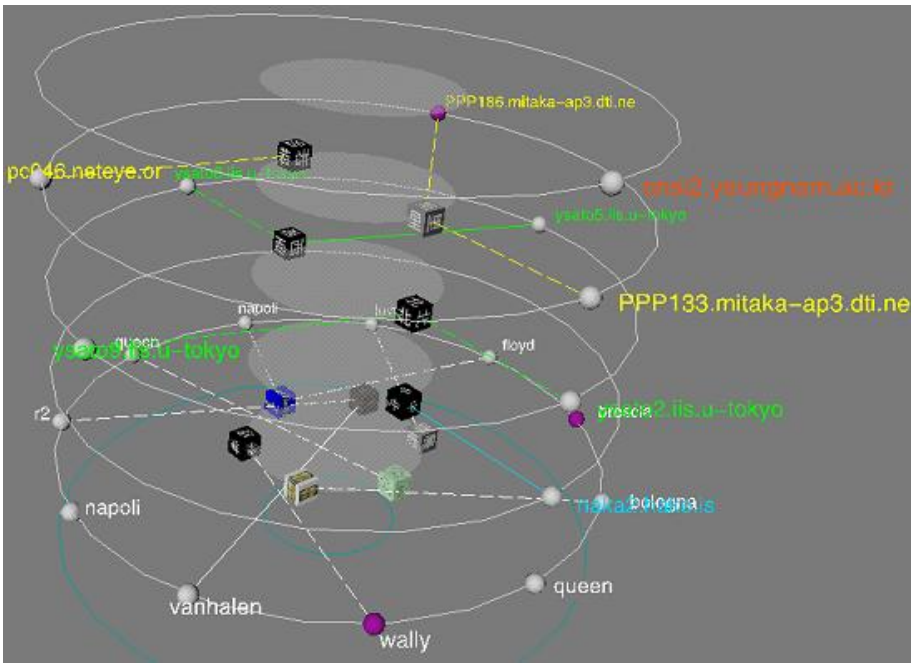
IDS RainStorm มีประโยชน์สำหรับเครือข่ายขนาดใหญ่ ช่วยในการวิเคราะห์แบบเรียลไทม์ แสดง IP Address ทั้งภายในและภายนอก และแสดงสัญญาณเตือนถึงความผิดปกติที่เกิดขึ้น มีความสามารถในการกรองข้อมูลที่เรียกว่า Filtering ทั้งใน Main View และ Zoom View ผู้ใช้สามารถเลือกแสดงเฉพาะสัญญาณเตือนที่เป็นสีแดง เหลือง หรือเขียวได้ ซึ่งช่วยให้ผู้ใช้วิเคราะห์สัญญาณเตือนที่เกิดขึ้นในเวลาเดียวกันได้

### 2.1.5 Tudumi

Tudumi (Takada and Koike, 2002: 560-566) ถูกออกแบบมาให้เป็น Log Visualization System ประกอบด้วยฟังก์ชันที่ช่วยผู้ดูแลระบบในการตรวจสอบผู้ใช้และความผิดปกติจากการบุกรุกในเครือข่ายคอมพิวเตอร์ขนาดใหญ่ การแสดงข้อมูลของโปรแกรมจะแสดงในลักษณะของดิสก์ ( Disks) ซึ่งแบ่งเป็นระดับชั้นโดยแบ่งเป็น 2 กลุ่มคือ ดิสก์ชั้นล่างสุดแสดงข้อมูลของผู้ใช้ และชั้นอื่นๆ ที่อยู่เหนือขึ้นไปแสดงการเข้าถึงข้อมูลในเครือข่ายและข้อมูลการใช้งานระบบเครือข่ายของผู้ใช้ดังแสดงในภาพที่ 2.14

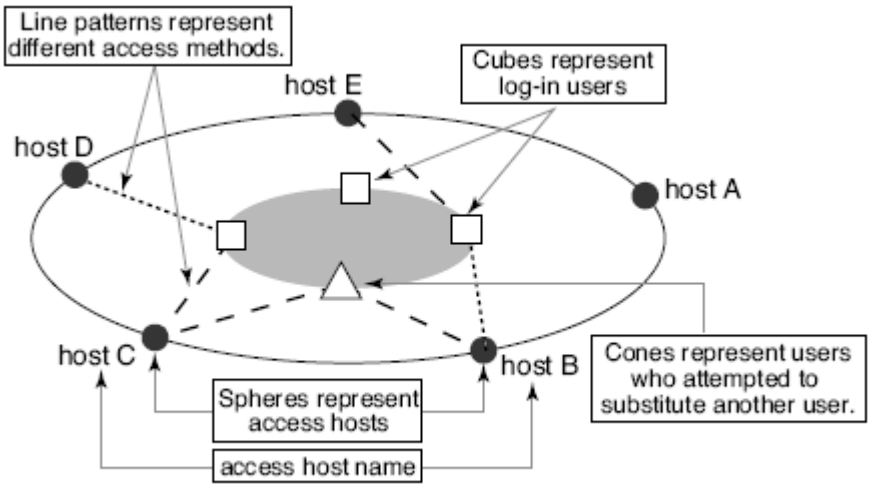
ภาพที่ 2.15 แสดงโปรแกรม Tudumi ในการเข้าถึง Hosts และการเข้าสู่ระบบของผู้ใช้ การเข้าถึง Hosts ( Access Hosts) จะแสดงเป็นทรงกลมที่วงด้านนอกของดิสก์ การเข้าสู่ระบบของผู้ใช้ ( Log-in Users) จะแสดงเป็นสี่เหลี่ยมลูกบาศก์กับภาพที่วงด้านในของดิสก์ เส้นที่โยงระหว่างทรงกลมและลูกบาศก์แสดงถึงความสัมพันธ์ระหว่างการเข้าถึง Hosts และการเข้าสู่ระบบของผู้ใช้ รูปแบบที่ต่างกันของเส้นแสดงถึงวิธีการเข้าถึงข้อมูล เส้นประที่หยาบแสดงถึง Terminal Use คือผู้ใช้ที่เข้าสู่ระบบและมีการใช้คำสั่งบางอย่าง เส้นประที่ละเอียดแสดงถึงมีการถ่ายโอนไฟล์ และเส้นประหนาแสดงถึงการใช้งานในทั้งสองกรณี

โดยทั่วไปผู้ดูแลระบบจะมีเกณฑ์ในการตัดสินว่า แต่ละเหตุการณ์เป็นพฤติกรรมปกติหรือไม่ โปรแกรม Tudumi สามารถแสดงกฎเหล่านั้นเป็นภาพแทนได้ คือกฎในการเข้าถึง Hosts และกฎในการเข้าสู่ระบบของผู้ใช้ โดยจะแทนกฎเกี่ยวกับการเข้าถึง Hosts ในลักษณะชั้นของดิสก์เรียกว่า Layers ผู้ดูแลระบบสามารถกำหนดกฎสำหรับการเข้าถึง Hosts ได้ โดเมนที่มาจากต่างประเทศจะปรากฏที่ชั้นบนสุดของดิสก์ดังแสดงในภาพที่ 2.16



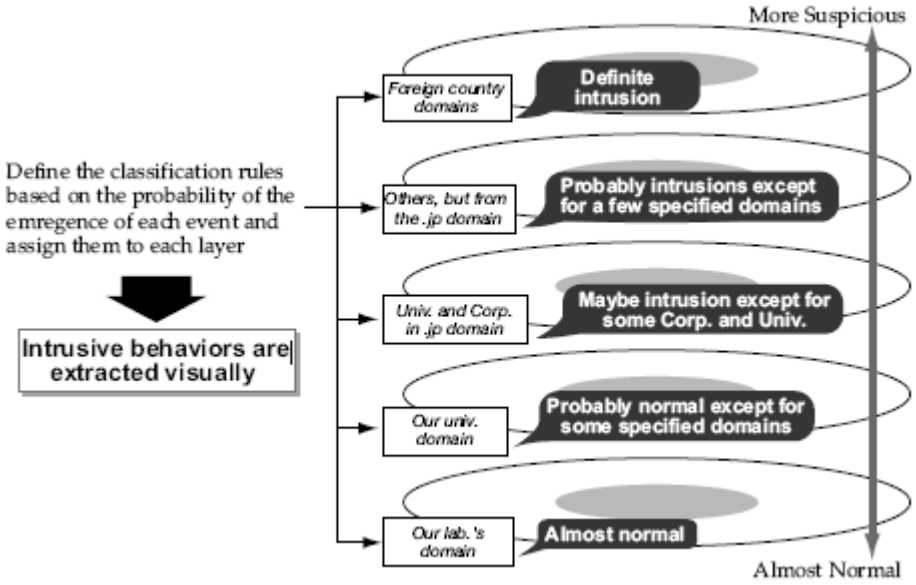

**ภาพที่ 2.14** การแสดงข้อมูลโดยใช้ลักษณะของดิสก์ของโปรแกรม Tudumi

**แหล่งที่มา:** Takada and Koike, 2002: 562.



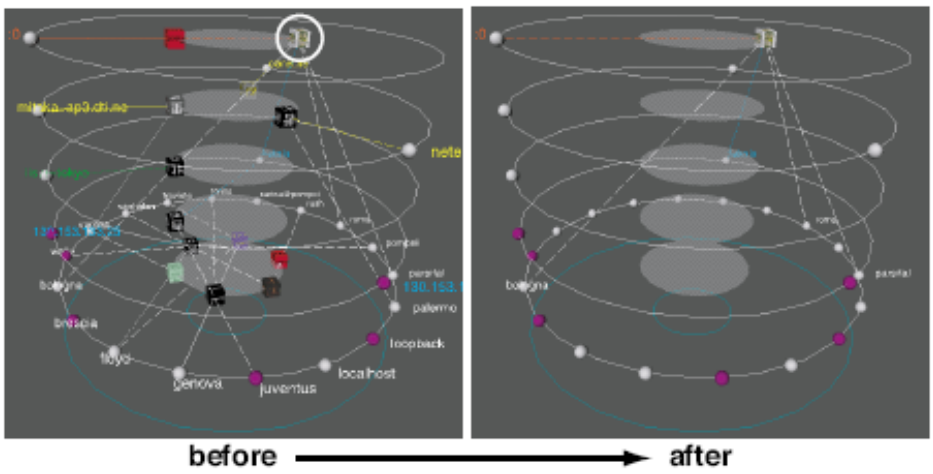

**ภาพที่ 2.15** แนวคิดการออกแบบ Network Access และ Log-in User ของโปรแกรม Tudumi

**แหล่งที่มา:** Takada and Koike, 2002: 562.




**ภาพที่ 2.16** แสดงระดับชั้นซึ่งแสดงกฎเกี่ยวกับการเข้าถึง Hosts ของโปรแกรม Tudumi

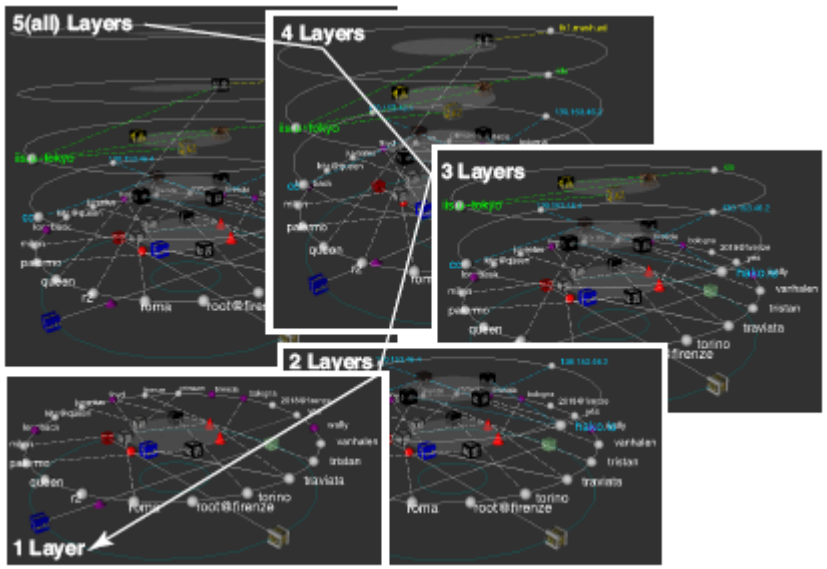
**แหล่งที่มา:** Takada and Koike, 2002: 563.




**ภาพที่ 2.17** แสดงตัวอย่างของการเลือกวัตถุของโปรแกรม Tudumi

**แหล่งที่มา:** Takada and Koike, 2002: 565.

รูปภาพที่แสดงอยู่บนลูกบาศก์แต่ละลูกจะแสดงภาพที่เป็นตัวแทนของผู้ใช้แต่ละคนซึ่งใช้ในการแบ่งกลุ่มของผู้ใช้ ถ้าผู้ใช้คลิกที่ลูกบาศก์จะสามารถแสดงข้อมูลเฉพาะที่ผู้ใช้เลือกและข้อมูลที่เกี่ยวข้องดังแสดงในภาพที่ 2.17




**ภาพที่ 2.18** แสดงตัวอย่างการควบคุมระดับชั้นของโปรแกรม Tudumi

**แหล่งที่มา:** Takada and Koike, 2002: 565.

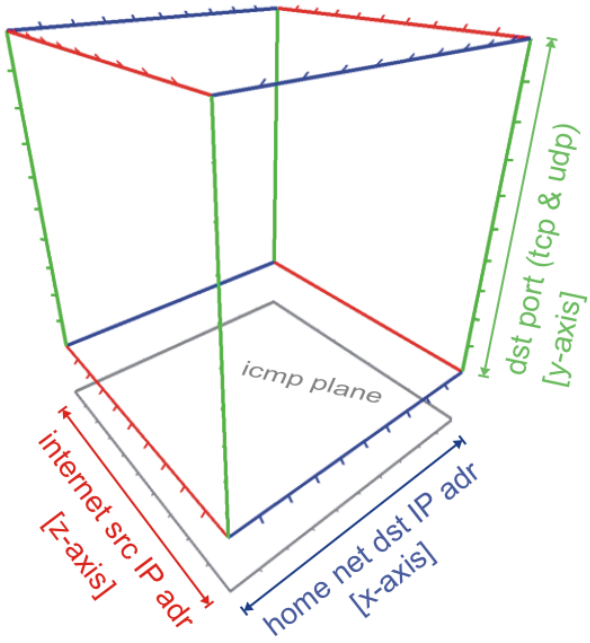
โปรแกรมสามารถแสดงเฉพาะส่วนหนึ่งของชั้นที่ผู้ใช้เลือกดังแสดงในภาพที่ 2.18 เพื่อการควบคุมจำนวนข้อมูลที่แสดง และเพื่อลดขอบเขตการมองของผู้ใช้ที่เกิดจากการแสดงจำนวนของข้อมูลมากเกินไป

ประโยชน์ของโปรแกรม Tudumi ช่วยให้ผู้ดูแลระบบติดตามและตรวจสอบ Log และทำให้การตรวจหาเหตุการณ์ที่มีความผิดปกติจากการบุกรุกในเครือข่ายคอมพิวเตอร์ได้ง่ายขึ้น

### 2.1.6 InetVis

InetVis (Riel, 2006: 1) เป็นโปรแกรมซึ่งใช้เทคนิค 3-D Scatter-Plot Visualization สำหรับแสดงภาพในเครือข่ายคอมพิวเตอร์ เพื่อช่วยในการสังเกตกิจกรรมต่างๆ และรูปแบบของการติดต่อสื่อสารที่ผิดปกติในเครือข่ายขนาดใหญ่ แนวคิดในการออกแบบโปรแกรมนี้มาจาก Spinning Cube of Potential Doom โดย Stephen Lau โดยกำหนดให้ Destination Address (Home Network) แสดงในแกน X ของกราฟซึ่งเป็นสีน้ำเงิน Source Address (External

Internet Range) แสดงในแกน Z ของกราฟซึ่งเป็นสีแดง Ports (TCP และ UDP) แสดงในแกน Y ของกราฟซึ่งเป็นสีเขียว และ ICMP จะแสดงอยู่ด้านล่างของ TCP/UDP โดยเป็นแผ่นสีเทาหรือขาว ดังแสดงในภาพที่ 2.19

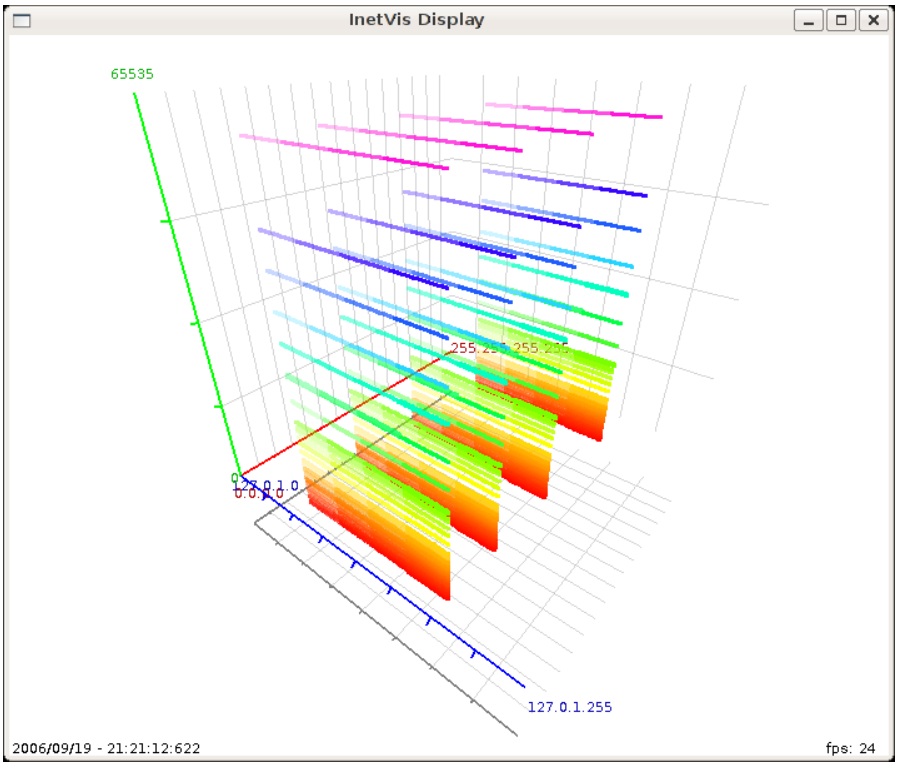



**ภาพที่ 2.19** การออกแบบวิธีการแสดงข้อมูลของโปรแกรม InetVis

**แหล่งที่มา:** Riel, 2006: 1.

ส่วนประสานกับผู้ใช้ (User Interface) จะแบ่งออกเป็นสี่หน้าจอการทำงานได้แก่ หน้าจอแสดงข้อมูล (Dedicated Display Panel) หน้าจอควบคุมหลัก (Main Control Panel), หน้าจอตั้งค่าการวาดกราฟ (Plotter Settings) และ หน้าจอตั้งค่าการอ้างอิงของเฟรม (Reference Frame Settings)

หน้าจอแสดงข้อมูล (Display Pane) แสดงในภาพที่ 2.20 สามารถควบคุมมุมมองของข้อมูลด้วยเมาส์ เมื่อกดเมาส์ปุ่มซ้ายจะสามารถหมุนมุมมองรอบวัตถุ กดเมาส์ปุ่มขวาจะสามารถเลื่อนแกนไปตามแนว X-Y ล้อเลื่อนที่ปุ่มกลางจะเลื่อนแกนไปตามแนว Z และเมื่อกดเมาส์ปุ่มกลางจะสามารถย่อ ขยาย มุมมองได้




**ภาพที่ 2.20** หน้าจอแสดงข้อมูลของโปรแกรม InetVis

**แหล่งที่มา:** Riel, 2006: 1.

หน้าจอควบคุม (Control Panel) แสดงในภาพที่ 2.21 ทำหน้าที่ควบคุมการแสดงข้อมูล ประกอบด้วย

(1) เมนูหลัก (Main Menu) สำหรับคำสั่งต่างๆ เช่น เปิดไฟล์ กำหนดโหมดที่จะแสดง

(2) ปุ่มควบคุมตำแหน่งที่จะแสดงเหตุการณ์ซ้ำ (Replay Position Controls)

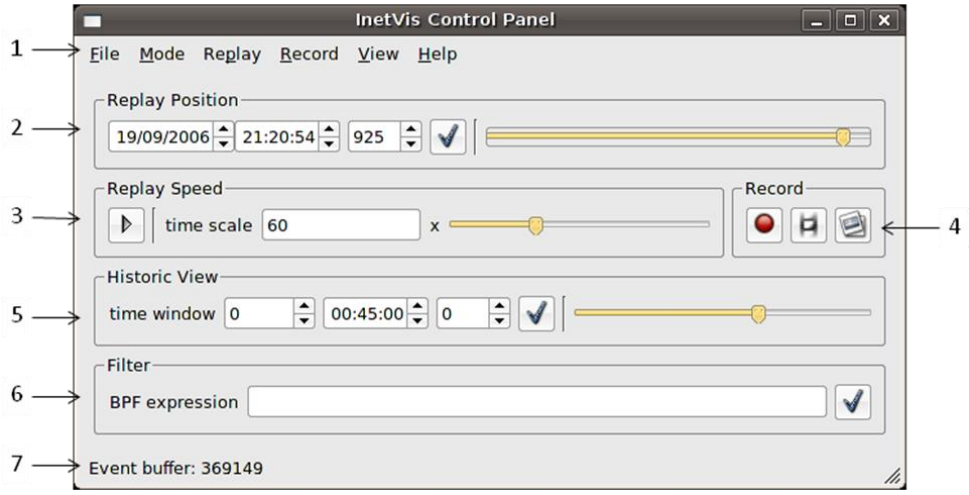
(3) ปุ่มควบคุมความเร็วของเหตุการณ์ที่จะแสดงซ้ำ (Replay Speed Controls)

(4) ปุ่มควบคุมการบันทึกเหตุการณ์ (Recording Controls)

(5) ปุ่มแสดงเหตุการณ์ที่เคยเกิดขึ้น (Historic View)

(6) ตัวกรองการแสดงผล (Filter)

(7) รายงานจำนวนของ Packets ปัจจุบันที่อยู่ใน Buffer




**ภาพที่ 2.21** หน้าจอควบคุมของโปรแกรม InetVis

**แหล่งที่มา:** Riel, 2006: 1.

หน้าจอตั้งค่าการวาดกราฟ ( Plotter Settings) แสดงในภาพที่ 2.22 กำหนดค่าและควบคุมการวาดกราฟที่แสดงข้อมูลประกอบด้วย

(1) ส่วนกำหนดค่า Destination Home Network Range

(2) ส่วนกำหนดค่า Source Internet Network Range

(3) ส่วนกำหนดค่า Port Range

(4) ส่วนกำหนดค่าสีที่ใช้ กำหนดสีของพื้นหลัง กำหนดความโปร่งแสง

(5) ส่วนกำหนดค่าขนาด ความเรียบ ความนูน ของจุดที่ใช้วาดกราฟ

หน้าจอตั้งค่าการอ้างอิงของเฟรม ( Reference Frame Settings) แสดงในภาพที่ 2.23 ประกอบด้วย

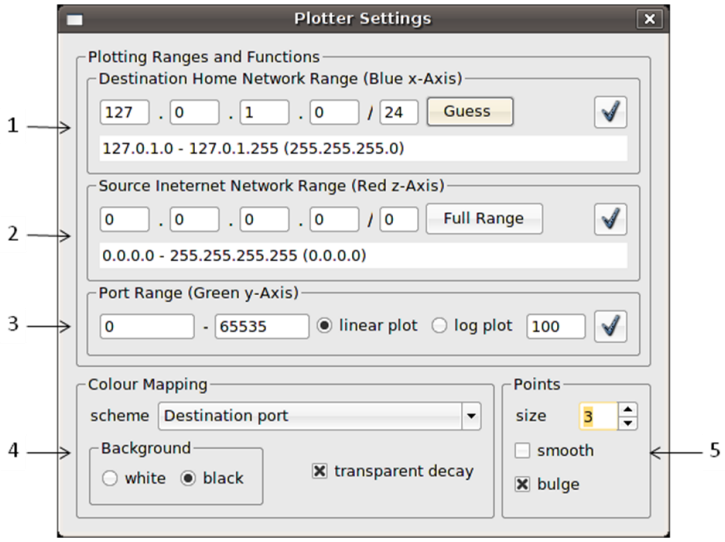
(1) ส่วนกำหนดโหมดการแสดงภาพ (Projection Mode)

(2) ส่วนกำหนดเฟรมที่อ้างอิง (Reference Frame)

(3) ส่วนกำหนดความโปร่งแสงของเส้นตาราง (Transparent Grid)

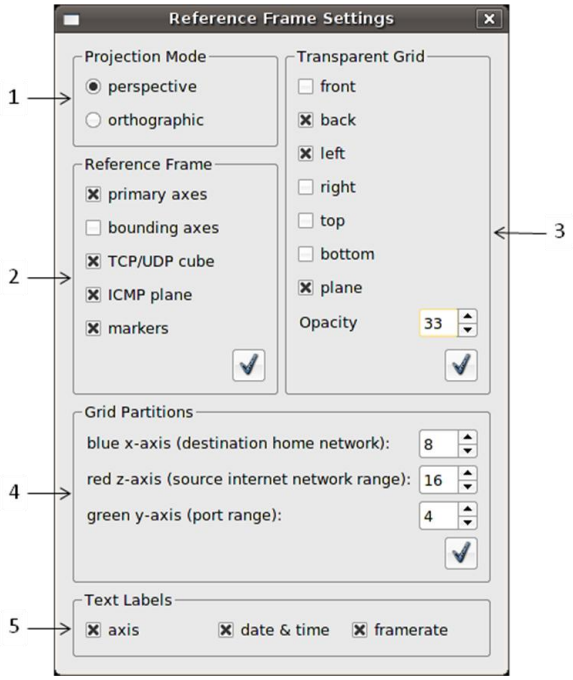
(4) ส่วนกำหนดการแบ่งความถี่ของเส้นตาราง (Grid Partitions)

(5) ส่วนกำหนดการแสดงแถบตัวอักษร (Text Labels)




**ภาพที่ 2.22** หน้าจอตั้งค่าการวาดกราฟของโปรแกรม InetVis

**แหล่งที่มา:** Riel, 2006: 1.




**ภาพที่ 2.23** หน้าจอตั้งค่าการอ้างอิงของเฟรมของโปรแกรม InetVis

**แหล่งที่มา:** Riel, 2006: 1.

ประโยชน์ของโปรแกรม InetVis คือช่วยในการสังเกตกิจกรรมต่างๆ และรูปแบบของการติดต่อสื่อสารที่ผิดปกติในเครือข่ายขนาดใหญ่ ช่วยในการสำรวจเครือข่ายคอมพิวเตอร์และช่วยแสดงข้อมูลให้เข้าใจได้ดียิ่งขึ้น

## 2.2 ผลสรุปที่ได้จากการศึกษางานวิจัยที่เกี่ยวข้อง

จากงานวิจัยต่างๆ ที่ได้กล่าวมาจะเห็นได้ว่า แต่ละงานวิจัย ใช้เทคนิคในการแสดงข้อมูลภายในเครือข่ายคอมพิวเตอร์ แหล่งข้อมูลที่ใช้ ข้อมูลที่นำมาแสดง และฟังก์ชั่นแตกต่างกันไป สามารถสรุปได้ดังตารางที่ 2.1 ซึ่ง ในวิทยานิพนธ์ฉบับนี้ได้นำเทคนิคต่างๆ ที่ได้ศึกษาจากงานวิจัยข้างต้นมาเป็นแนวทางและประยุกต์ใช้ โดยเลือกคุณลักษณะที่เหมาะสมมาใช้ในงานวิจัย ซึ่งพิจารณาจากวัตถุประสงค์ของงานวิจัยเป็นหลัก โดยมีรายละเอียดคือ เทคนิคที่ใช้แสดงข้อมูลจะแสดงข้อมูลบนแผ่นกระดาน (Plate) 3 แผ่น ที่ตั้งฉากกัน ในพื้นที่ 3 มิติ และ แสดงความสัมพันธ์ระหว่างข้อมูลบนแผ่นกระดานแต่ละแผ่น โดยใช้เส้นเชื่อมระหว่างวัตถุบนแผ่นกระดานทั้งสาม และใช้สีของเส้นในการกำหนดปริมาณของการติดต่อสื่อสารในเครือข่ายคอมพิวเตอร์ แหล่งข้อมูลที่ใช้จะนำมาจากผลของการวิเคราะห์ที่ Snort ตรวจจับได้ (Snort Log) ข้อมูลที่จะแสดงประกอบด้วย IP Address, Port, Timestamp, Signature และ Header ซึ่งแนวคิดในการออกแบบและหลักการทำงานของระบบจะกล่าวถึงในบทถัดไป

**ตารางที่ 2.1** รายละเอียดโดยรวมของงานวิจัยที่เกี่ยวข้อง

| งานวิจัย | เทคนิคที่ใช้แสดงข้อมูล | แหล่งข้อมูลที่ใช้ | ข้อมูลที่แสดง | ฟังก์ชั่นที่มี |
|---|---|---|---|---|
| NvisonIP | XY Grid, Drill-Down Levels | NetFlow | IP Address, Port, Protocol | Color Mapping, Zooming, Frame Animation, Graph |
| TNV | Matrix-Based | NetFlow | IP Address, Port, Protocol, Timestamp | Filtering, Zooming, Color Mapping, Network Links |
| NetworkEye | End-to-End | NetFlow | IP Address, Port, Protocol, Files in Use | Pixel Map, Trust Levels, Network Links, Color Mapping |
| IDS RainStorm | Parallel Coordinate Plot | Snort Log | IP Address, Alarm, Time stamp | Zooming, Filtering, Color Mapping |

**ตารางที่ 2.1** (ต่อ)

| งานวิจัย | เทคนิคที่ใช้แสดงข้อมูล | แหล่งข้อมูลที่ใช้ | ข้อมูลที่แสดง | ฟังก์ชั่นที่มี |
|---|---|---|---|---|
| Tudumi | Disks | Log-Files | IP Address, Network Access, Log-in User | Filtering, Network Links, Color Mapping |
| InetVis | 3D-Scatter Plot | NetFlow | IP Address, Port | Filtering, Color Mapping |

# บทที่ 3

# การออกแบบและหลักการทำงานของระบบ

## 3.1 โครงสร้างการทำงานของระบบ

โครงสร้างการทำงานของระบบสามารถแบ่งการทำงานออกเป็น 3 ส่วนได้ดังนี้

### 3.1.1 ระบบตรวจจับการบุกรุกในระดับเครือข่ายคอมพิวเตอร์

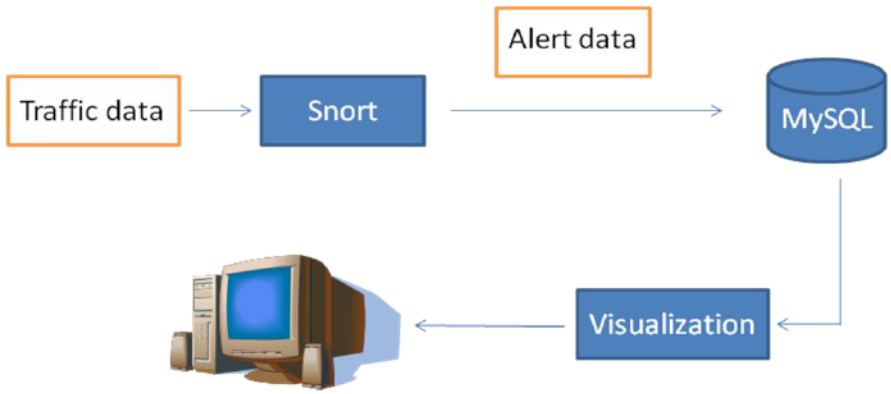
Network Intrusion Detection System (NIDS) คือระบบตรวจจับการบุกรุกในระดับเครือข่ายคอมพิวเตอร์ มีหน้าที่วิเคราะห์ข้อมูลต่างๆ ที่เกิดขึ้นในเครือข่ายคอมพิวเตอร์ว่าเป็นการบุกรุกหรือไม่ โดยการพิจารณาจากข้อกำหนดและกฎที่ได้ระบุไว้ หรือจากการเก็บสถิติของการบุกรุกที่เกิดขึ้นในระบบ ในงานวิจัยนี้ได้นำเอา Snort ซึ่งเป็นโปรแกรมสำหรับตรวจจับการบุกรุกทางเครือข่ายมาใช้ในการวิเคราะห์ข้อมูลในเครือข่ายคอมพิวเตอร์ เพื่อหาถึงความพยายามในการบุกรุกหรือความผิดปกติที่เกิดขึ้นจากการโจมตีในระบบเครือข่าย โปรแกรม Snort มีการทำงานหลักอยู่ 3 การทำงานคือ 1 ) Packet Sniffer ทำหน้าที่ในการตรวจจับ Packet ในเครือข่ายคอมพิวเตอร์ 2 ) Packet Logger ทำหน้าที่บันทึกข้อมูลต่างๆ ซึ่งตรวจจับได้จากเครือข่ายคอมพิวเตอร์ 3 ) NIDS ทำหน้าที่วิเคราะห์การบุกรุกหรือความผิดปกติที่เกิดขึ้นในเครือข่ายคอมพิวเตอร์ ในงานวิจัยนี้ได้ใช้การทำงานในส่วนของ NIDS ของ Snort มาช่วยในการวิเคราะห์การบุกรุก ข้อมูลที่วิเคราะห์หรือตรวจจับได้จาก Snort (Snort Log) จะทำการเก็บไว้ในระบบฐานข้อมูล และแสดงเป็นภาพในระบบที่พัฒนาขึ้นต่อไป

### 3.1.2 ระบบฐานข้อมูล

ระบบฐานข้อมูลทำหน้าที่ในการเก็บ Alert Data (ข้อมูลต่างๆ ที่วิเคราะห์หรือตรวจจับได้จาก Snort) ในงานวิจัยนี้ได้ใช้ MySQL เป็นฐานข้อมูล ข้อมูลที่เก็บไว้จะใช้ในการวิเคราะห์และนำข้อมูลมาแสดงในระบบ ข้อมูลที่มีการจัดเก็บประกอบด้วย IP Address, Port, IP Header, TCP Header, UDP Header, ICMP Header, Data Payload, Signature (หมายเลขที่ Snort ใช้ในการระบุลักษณะของความผิดปกติในเครือข่ายที่ตรวจจับได้) และ Timestamp

### 3.1.3 ระบบการสร้างภาพนามธรรม

ทำหน้าที่ในการแสดงข้อมูลที่นำมาจากฐานข้อมูลตามเงื่อนไขที่ผู้ใช้กำหนดในรูปแบบสามมิติ โดยใช้หลักการของ Visualization ซึ่งเป็นการใช้เส้น รูปร่าง และสี เพื่อแทนความหมายของข้อมูล



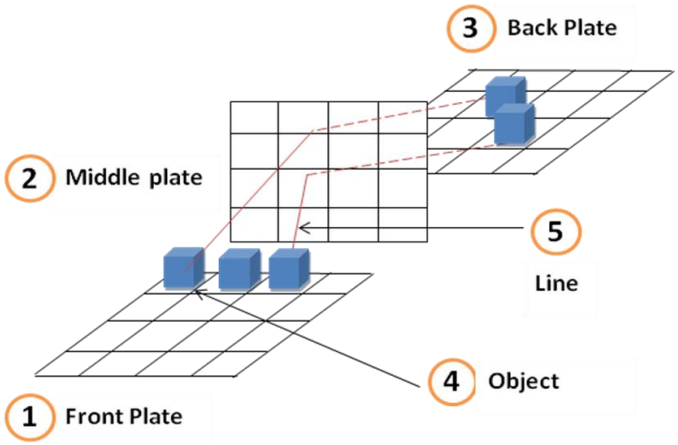

**ภาพที่ 3.1** โครงสร้างการทำงานของระบบที่นำเสนอในงานวิจัย

## 3.2 การออกแบบระบบ

การออกแบบหน้าจอการใช้งานของระบบ จะยึดหลักของความง่ายในการใช้งานของผู้ใช้ ความสัมพันธ์ของข้อมูลที่นำมาแสดง การให้อิสระแก่ผู้ใช้ในการกำหนดข้อมูลที่จะนำมาแสดง และการแสดงข้อมูลที่ได้ในรูปแบบ 3 มิติ การอธิบายส่วนประกอบต่างๆ ของระบบจะเริ่มจากการอธิบายภาพโดยรวมของระบบ และรายละเอียดของระบบในแต่ละส่วน

### 3.2.1 แนวคิดในการออกแบบระบบ

ข้อมูลการสื่อสารในเครือข่ายจะถูกแสดงบนแผ่นกระดาน 3 แผ่นที่ตั้งฉากกันในพื้นที่ 3 มิติ โดยใช้เส้นเชื่อมระหว่างวัตถุบนแผ่นกระดานทั้งสามในการแสดงความสัมพันธ์ระหว่างข้อมูล และใช้สีของเส้นในการแสดงปริมาณของการติดต่อสื่อสารในเครือข่าย แนวคิดในการออกแบบการแสดงข้อมูลในเครือข่ายของระบบที่นำเสนอในงานวิจัยแสดงดังรูป 3. 2 ซึ่งประกอบด้วยส่วนต่างๆ ดังนี้




**ภาพที่ 3.2** แนวคิดในการออกแบบการแสดงข้อมูลในเครือข่ายของระบบที่นำเสนอในงานวิจัย

(1) Front Plate เป็นพื้นที่สำหรับวางวัตถุที่แสดงถึง Source IP Address

(2) Middle Plate เป็นพื้นที่สำหรับวางวัตถุที่แสดงถึง Port

(3) Back Plate เป็นพื้นที่สำหรับวางวัตถุที่แสดงถึง Destination IP Address

(4) Object แสดงถึงวัตถุที่วางอยู่บน Plate ซึ่งผู้ใช้สามารถคลิกเลือกวัตถุได้

(5) Line แสดงถึงเส้นซึ่งใช้แสดงความสัมพันธ์ระหว่างวัตถุที่อยู่บน Plate ทั้งสาม

แนวคิดในการออกแบบการแสดงข้อมูลบนแผ่นกระดานทั้งสาม แบ่งพื้นที่ในการแสดงข้อมูลออกเป็นสามส่วน แต่ละส่วนใช้แสดงข้อมูลที่แตกต่างกัน การใช้เส้นสีในการแสดงความสัมพันธ์ของข้อมูล สามารถช่วยให้ผู้ใช้มองเห็นภาพรวมของการติดต่อสื่อสารในเครือข่ายและทำการค้นหาข้อมูลที่ต้องการได้ง่ายขึ้น

### 3.2.2 ภาพรวมของระบบ

ภาพรวมของระบบจะประกอบด้วยหน้าจอหลายส่วนที่มีวัตถุประสงค์ในการใช้งานที่แตกต่างกัน แต่มีความสัมพันธ์กันในด้านข้อมูล ซึ่งแสดงดังภาพที่ 3. 3 โดยสามารถแบ่งส่วนประกอบหลักของระบบได้ดังนี้

3.2.2.1 หน้าจอแสดงข้อมูลในรูปแบบ 3 มิติ (หมายเลข 1)

3.2.2.2 ส่วนกำหนดวันและเวลาของข้อมูลที่แสดง (หมายเลข 2)

3.2.2.3 ส่วนควบคุมการแสดงข้อมูลของ IP Address (หมายเลข 3)

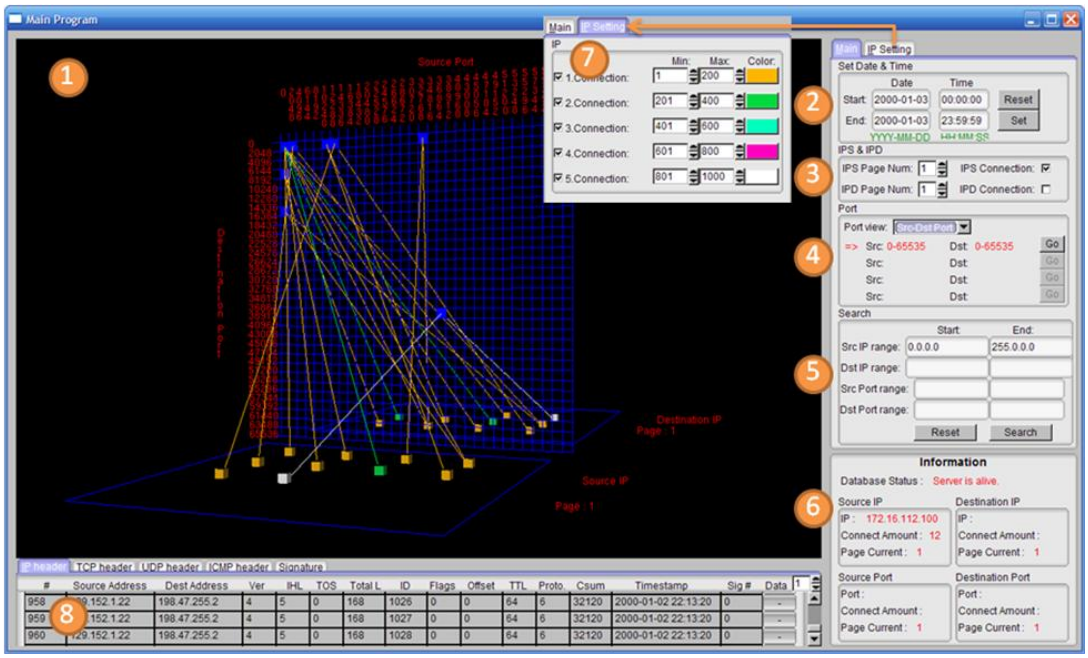
3.2.2.4 ส่วนควบคุมการแสดงข้อมูลของ Port (หมายเลข 4)

3.2.2.5 ส่วนกำหนดค่าในการค้นหาข้อมูล (หมายเลข 5)

3.2.2.6 ส่วนแสดงรายละเอียดของวัตถุในหน้าจอแสดงข้อมูล (หมายเลข 6)

3.2.2.7 ส่วนกำหนดรายละเอียดของความสัมพันธ์ระหว่างข้อมูล (หมายเลข 7)

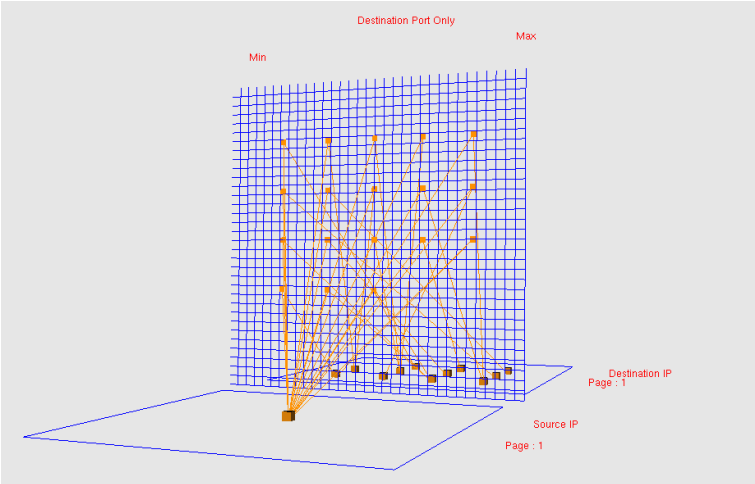
3.2.2.8 ส่วนแสดงรายละเอียดของข้อมูล Header และ Signature (หมายเลข 8)




**ภาพที่ 3.3** ภาพรวมและส่วนประกอบต่าง ๆ ของระบบที่นำเสนอในงานวิจัย

### 3.2.3 หน้าจอแสดงข้อมูลในรูปแบบ 3 มิติ

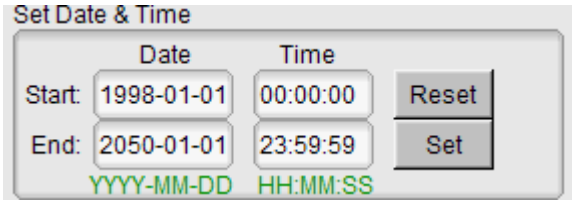
หน้าจอแสดงข้อมูลในรูปแบบ 3 มิติ มีแนวคิดในการออกแบบโดยข้อมูลการสื่อสารในเครือข่ายจะถูกแสดงบนแผ่นกระดาน 3 แผ่นที่ตั้งฉากกันในพื้นที่ 3 มิติ และแสดงความสัมพันธ์ระหว่างข้อมูลบนแผ่นกระดานโดยใช้เส้นเชื่อมระหว่างวัตถุบนแผ่นกระดานทั้งสาม ใช้สีของเส้นในการกำหนดปริมาณของการติดต่อสื่อสารในเครือข่าย ผู้ใช้งานสามารถหมุนมุมมองในการแสดงข้อมูลโดยการคลิกและเลื่อนเมาส์ปุ่มซ้าย เมื่อผู้ใช้คลิกและเลื่อนเมาส์ปุ่มขวาจะสามารถเลื่อนมุมมองในการแสดงข้อมูล และเมื่อผู้ใช้เลื่อนลูกเลื่อนที่กลางเมาส์จะสามารถย่อขยายมุมมองของวัตถุได้ หน้าจอแสดงข้อมูลในเครือข่ายในรูปแบบ 3 มิติได้พัฒนาขึ้นตามแนวคิดที่ได้ออกแบบไว้แสดงได้ดังภาพที่ 3.4




**ภาพที่ 3.4** หน้าจอแสดงข้อมูลของเครือข่ายในรูปแบบ 3 มิติ

### 3.2.4 ส่วนกำหนดวันและเวลาของข้อมูลที่แสดง

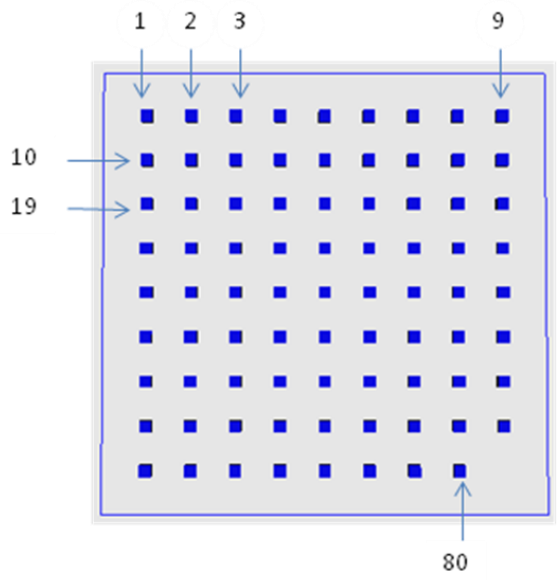
ผู้ใช้สามารถกำหนดวันและเวลาของเหตุการณ์การสื่อสารในเครือข่ายที่ต้องการแสดงข้อมูล หรือสามารถกำหนดช่วงเวลาที่ต้องการแสดงข้อมูลได้ ดังภาพที่ 3.5



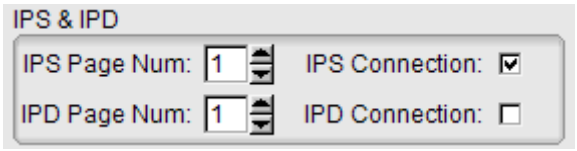

**ภาพที่ 3.5** ส่วนกำหนดวันและเวลาของข้อมูลที่แสดง

### 3.2.5 ส่วนควบคุมการแสดงข้อมูลของ IP Address

ส่วนควบคุมการแสดงข้อมูลของ IP Address ประกอบด้วย Source IP Address และ Destination IP Address ซึ่งแสดงอยู่บน Front Plate และ Back Plate ตามลำดับ โดยใช้วัตถุรูปลูกบาศก์ 1 ลูกแทน IP Address 1 IP การจัดเรียงวัตถุจะเรียงตามหมายเลข IP Address จากน้อยไปมาก โดยเริ่มจากมุมบนด้านซ้ายของ Plate ไปจนหมดแถวหนึ่งแล้วเริ่มตัวต่อไปใหม่จากด้านซ้ายของแถวที่ 2 เรียงกันไปจนถึงตัวสุดท้ายคือมุมล่างขวาของ Plate ตามภาพที่ 3.6




**ภาพที่ 3.6** แสดงตัวอย่างการเรียงลำดับ IP Address จำนวน 80 IP ที่แสดงบน Plate




**ภาพที่ 3.7** ส่วนที่ใช้ในการกำหนด Page ในการแสดงข้อมูลของ IP Address

ใน Plate 1 Plate จะกำหนดให้มีขนาด 30 x30 ทำให้สามารถรองรับข้อมูลได้สูงสุด 900 IP Address ในแต่ละ Plate ถ้ามี IP Address มากกว่า 900 IP จะกำหนดให้แสดงในหน้าที่ 2 ซึ่งถูกกำหนดโดยหมายเลขที่เรียกว่า Page เช่น ข้อมูลของ IP Address 2000 IP จะใช้ Page ในการแสดงข้อมูลทั้งหมด 3 Page โดยส่วนที่ใช้ในการกำหนด Page ในการแสดงข้อมูลแสดงดังภาพที่ 3.7 เหตุผลที่ต้องกำหนดจำนวนของ IP Address ที่จะแสดงต่อ Plate หนึ่งๆ นั้นเพราะการแสดง IP Address ทั้งหมดในคราวเดียวจะทำให้มุมมองมีขนาดใหญ่เกินไป และการแสดงความสัมพันธ์ของข้อมูลจะซับซ้อนยากที่ผู้ใช้จะเข้าใจเนื่องจากข้อมูลมีปริมาณมาก

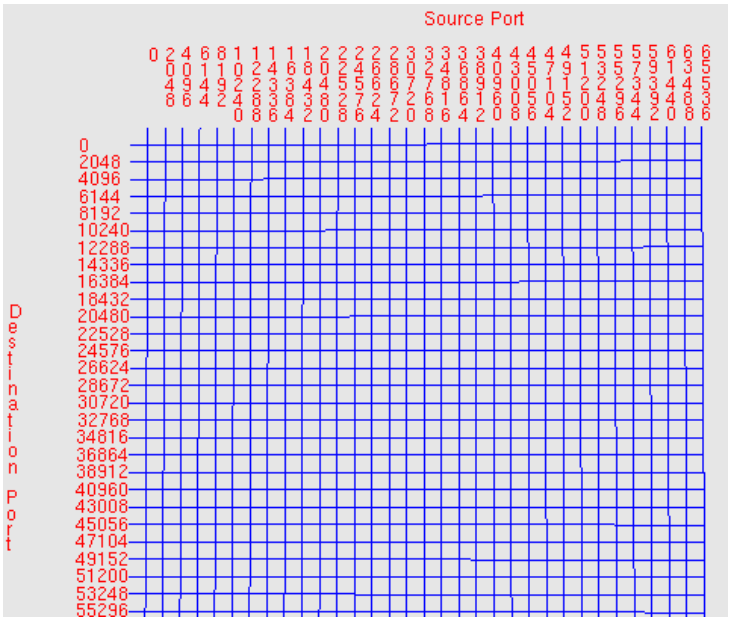
### 3.2.6 ส่วนควบคุมการแสดงข้อมูลของ Port

ส่วนควบคุมการแสดงข้อมูลของ Port ใน Middle Plate ซึ่งผู้ใช้สามารถกำหนดมุมมองของ Port ได้สามมุมมอง คือ

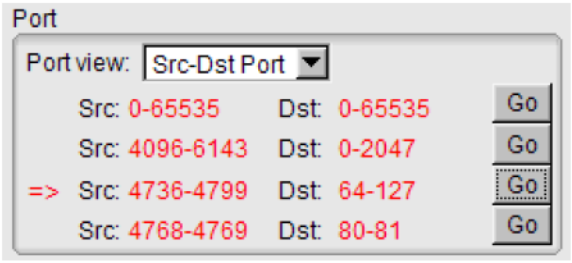
3.2.6.1 มุมมองของ Source-Destination Port

มุมมองนี้จะแสดงทั้ง Source Port และ Destination Port ร่วมกันเพื่อให้เห็นภาพรวมของ Port ทั้งหมด และง่ายต่อการวิเคราะห์ข้อมูลของ Port ที่มีการใช้งาน โดยกำหนดให้ Plate มีขนาด 32x32 ช่อง แกน X แทน Source Port และแกน Y แทน Destination Port ค่าของ Source Port 0 และ Destination Port 0 อยู่ที่ตำแหน่งมุมบนด้านซ้ายของ Plate ดังแสดงในภาพที่ 3. 8 Port ที่มีการใช้งานจะแสดงด้วยวัตถุรูปทรงสี่เหลี่ยม เช่นเดียวกับ IP Address

Port จะมีค่าสูงสุดได้ 65536 ค่า เมื่อนำมาแสดงบน Plate ที่มี 32 ช่องจะทำให้แต่ละช่องจะมีข้อมูลได้ 2048 Port ถ้า Port ที่มีการใช้งานแสดงอยู่ในช่องหนึ่ง จะยังไม่สามารถรู้ได้ว่า Port ที่ใช้งานมีค่าอะไรเพราะมีค่าที่เป็นไปได้ 2048 ค่า การที่จะรู้ได้ว่าข้อมูลนั้นคือ Port อะไรก็ต่อเมื่อกำหนด Scale ให้ 1 ช่องแทน 1 Port แสดงว่าจะต้องมี Plate ขนาด 65536x65536 ช่อง ซึ่งเป็นไปไม่ได้ที่จะทำเช่นนั้น การแก้ปัญหานี้ทำได้โดยกำหนด Plate ให้แบ่งเป็นระดับชั้นเรียกว่า Layer ดังแสดงในภาพที่ 3. 9 ซึ่งผู้ใช้สามารถเลือก Layer ที่ต้องการแสดงได้ โดยสามารถแบ่ง Layer ได้เป็น 4 Layer ดังนี้




**ภาพที่ 3.8** แสดง Middle Plate ในมุมมองของ Source-Destination Port




**ภาพที่ 3.9** ส่วนควบคุมที่ใช้กำหนดระดับชั้น (Layer) ในมุมมองของ Source-Destination Port

1) Layer 1

Plate ในระดับนี้จะมีขนาด 32x32 ช่อง แต่ละช่องจะมีข้อมูลของ Port ได้ 2048 Port

2) Layer 2

Plate ในระดับนี้จะมีขนาด 32x32 ช่อง แต่ละช่องจะมีข้อมูลของ Port ได้ 64 Port

3) Layer 3

Plate ในระดับนี้จะมีขนาด 32x32 ช่อง แต่ละช่องจะมีข้อมูลของ Port ได้ 2 Port

4) Layer 4

Plate ในระดับนี้จะมีขนาด 2x2 ช่อง แต่ละช่องจะมีข้อมูลของ Port ได้ 1 Port

การหาว่า Port ที่มีการใช้งานแสดงอยู่ในช่องๆ หนึ่งคือ Port อะไร ตัวอย่างเช่น ข้อมูลของ Port ที่มีการใช้งานมี Source Port เป็น 80 และ Destination Port เป็น 2049

1) Layer 1

ข้อมูลที่มีการใช้งานอยู่ในช่วง Source Port เท่ากับ 0 ถึง 2047 และ Destination Port เท่ากับ 2048 ถึง 4095 ดังแสดงในภาพที่ 3.10

2) Layer 2

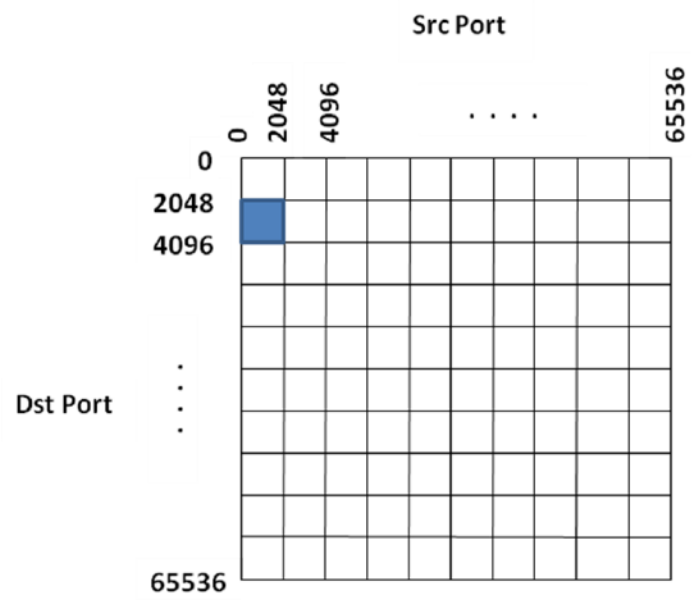
ข้อมูลที่มีการใช้งานอยู่ในช่วง Source Port เท่ากับ 64 ถึง 127 และ Destination Port เท่ากับ 2048 ถึง 2111 ดังแสดงในภาพที่ 3.11

3) Layer 3

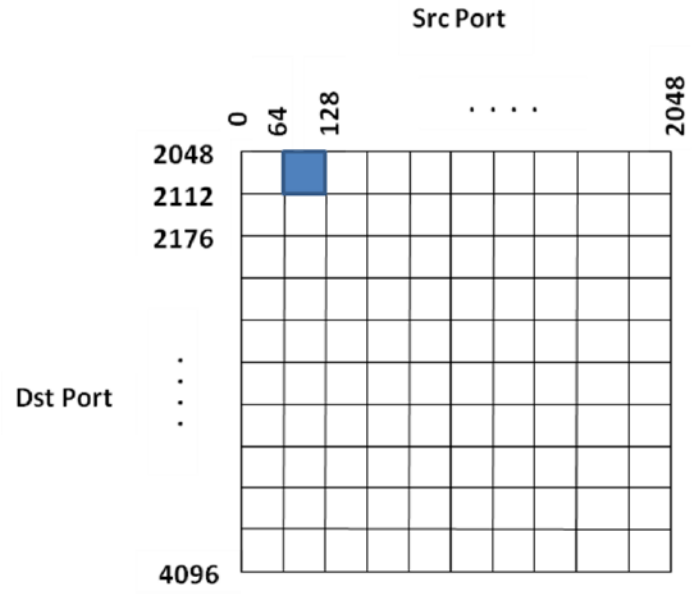
ข้อมูลที่มีการใช้งานอยู่ในช่วง Source Port เท่ากับ 80 ถึง 81 และ Destination Port เท่ากับ 2048 ถึง 2049 ดังแสดงในภาพที่ 3.12

4) Layer 4

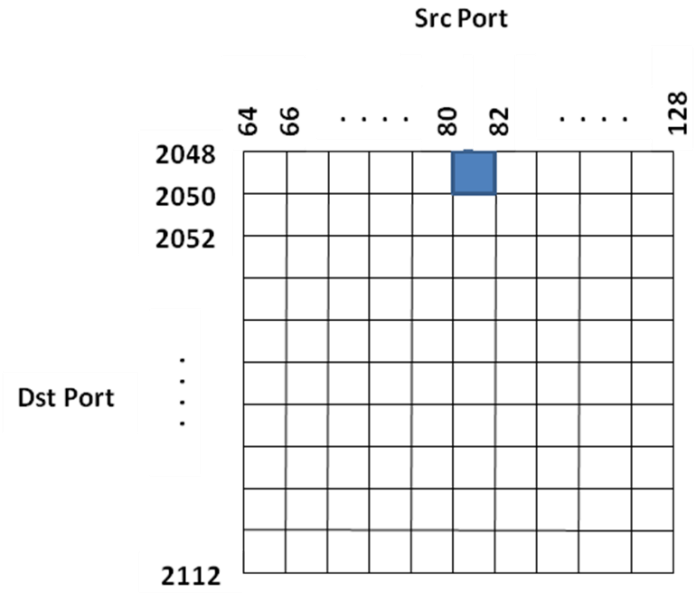
ข้อมูลที่มีการใช้งานอยู่ในช่วง Source Port เท่ากับ 80 และ Destination Port เท่ากับ 2049 ดังแสดงในภาพที่ 3.13 ซึ่งจะได้ข้อมูลที่ต้องการ



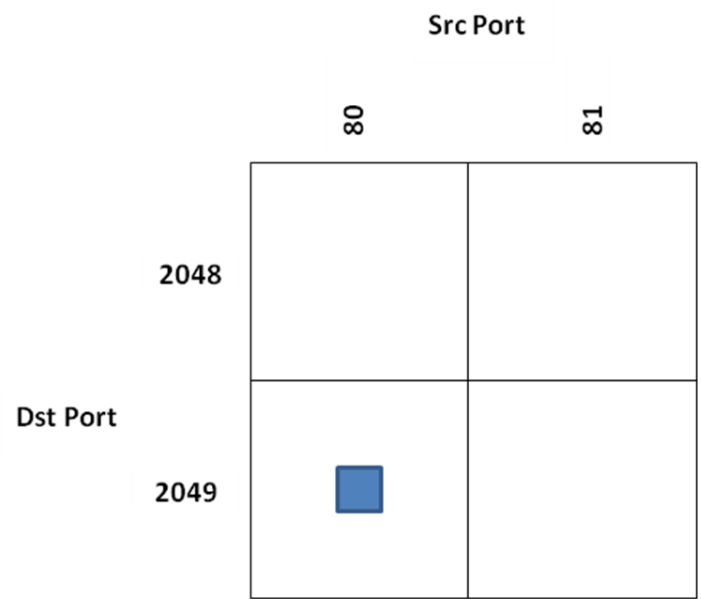

**ภาพที่ 3.10** แสดงข้อมูลที่มีการใช้งานใน Layer 1 ของ Plate




**ภาพที่ 3.11** แสดงข้อมูลที่มีการใช้งานใน Layer 2 ของ Plate



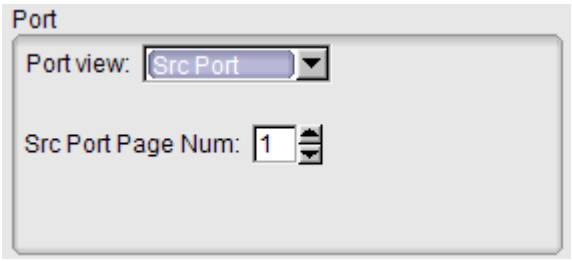

**ภาพที่ 3.12** แสดงข้อมูลที่มีการใช้งานใน Layer 3 ของ Plate




**ภาพที่ 3.13** แสดงข้อมูลที่มีการใช้งานใน Layer 4 ของ Plate

3.2.6.2 มุมมองของ Source Port

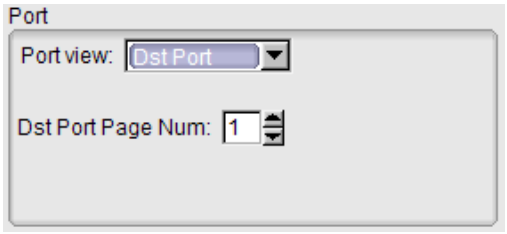
แสดง Source Port ที่มีการติดต่อสื่อสารในเครือข่ายใน Middle Plate โดยใช้วัตถุรูปทรงสี่เหลี่ยม 1 รูปแทน Source Port แต่ละ Port การจัดเรียง Port จะเรียงตามหมายเลข Port เหมือนกับการเรียงหมายเลข IP Address แต่ละ Plate มีขนาด 32x32 ช่อง สามารถรองรับข้อมูลได้ 1024 Port ถ้ามี Port มากกว่า 1024 Port จะกำหนดให้แสดงในหน้าถัดไป ซึ่งถูกกำหนดโดยหมายเลขที่เรียกว่า Page เช่นเดียวกับ IP Address เช่น ข้อมูลของ Port 2000 Port จะต้องใช้ Page ในการแสดงข้อมูลทั้งหมด 2 Page โดยที่ผู้ใช้สามารถเปลี่ยน Page ไปยัง Page ที่ต้องการแสดงข้อมูลได้ดังแสดงในภาพที่ 3.14




**ภาพที่ 3.14** ส่วนควบคุมที่ใช้กำหนด Page ในมุมมองของ Source Port

3.2.6.3 มุมมองของ Destination Port

แสดง Destination Port ที่มีการติดต่อสื่อสารในเครือข่ายใน Middle Plate โดยมีการแสดงข้อมูลเช่นเดียวกับ Source Port ดังแสดงในภาพที่ 3.15



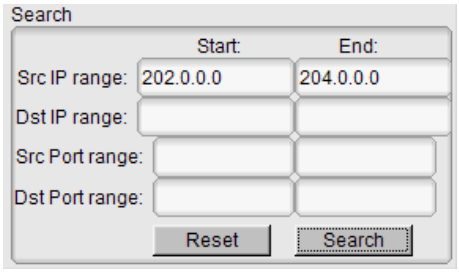

**ภาพที่ 3.15** ส่วนควบคุมที่ใช้กำหนด Page ในมุมมองของ Destination Port

### 3.2.7 ส่วนกำหนดค่าในการค้นหาข้อมูล

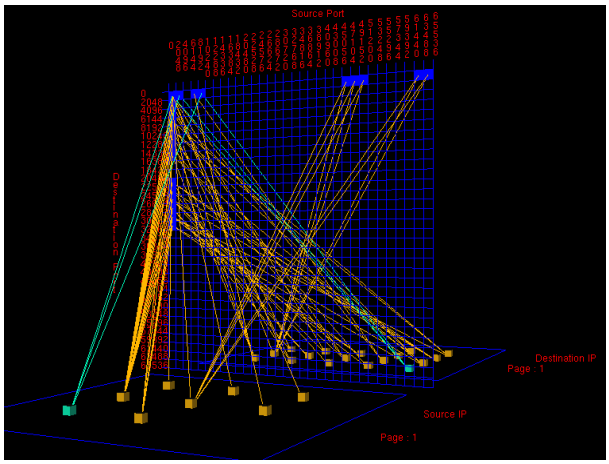
ส่วนนี้ใช้สำหรับกำหนดค่าในการค้นหาสำหรับแสดงข้อมูล Source IP, Destination IP, Source Port และ Destination Port ในหน้าจอแสดงข้อมูลในรูปแบบ 3 มิติ โดยข้อมูลที่แสดงเป็นข้อมูลที่ผู้ใช้กำหนดในเงื่อนไขของการค้นหาเท่านั้น ซึ่งสามารถแบ่งได้ 2 รูปแบบดังนี้

3.2.7.1 การค้นหาโดยระบุข้อมูลในการค้นหา

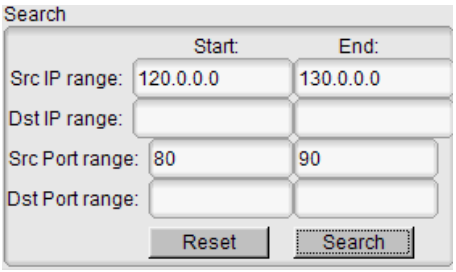
ผู้ใช้สามารถระบุข้อมูลของ Source IP, Destination IP, Source Port และ Destination Port ที่จะทำการค้นหา หรือระบุช่วงของข้อมูลที่จะทำการค้นหาได้ เช่น ผู้ใช้ระบุ Source IP Address ที่จะทำการค้นหาระหว่าง 202.0.0.0 ถึง 204.0.0.0 ดังแสดงในภาพที่ 3.16 ผลที่ได้จะแสดงข้อมูลของ Source IP Address ในช่วงที่ระบุเท่านั้นดังแสดงในภาพที่ 3.17 ผู้ใช้สามารถเลือกข้อมูลที่จะทำการค้นหามากกว่า 1 ข้อมูลได้ เช่น ผู้ใช้ระบุข้อมูลที่จะค้นหาคือ Source IP Address 120.0.0.0 ถึง 130.0.0.0 และ Source Port 80 ถึง 90 ดังแสดงในภาพที่ 3.18 ผลที่ได้แสดงดังภาพที่ 3.19



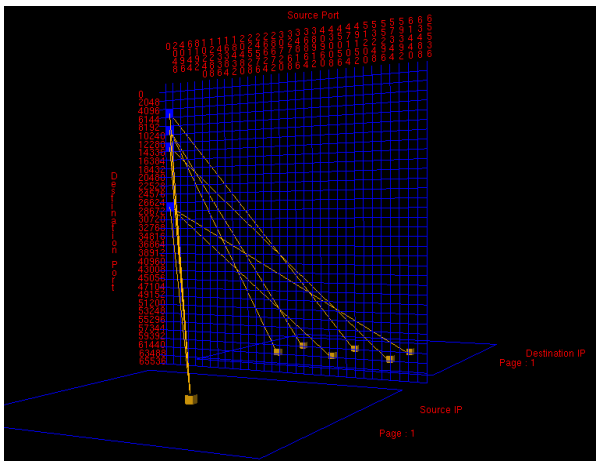

**ภาพที่ 3.16** แสดงตัวอย่างของการระบุข้อมูลในการค้นหา




**ภาพที่ 3.17** แสดงผลที่ได้จากการการค้นหา Source IP Address 202.0.0.0 ถึง 204.0.0.0



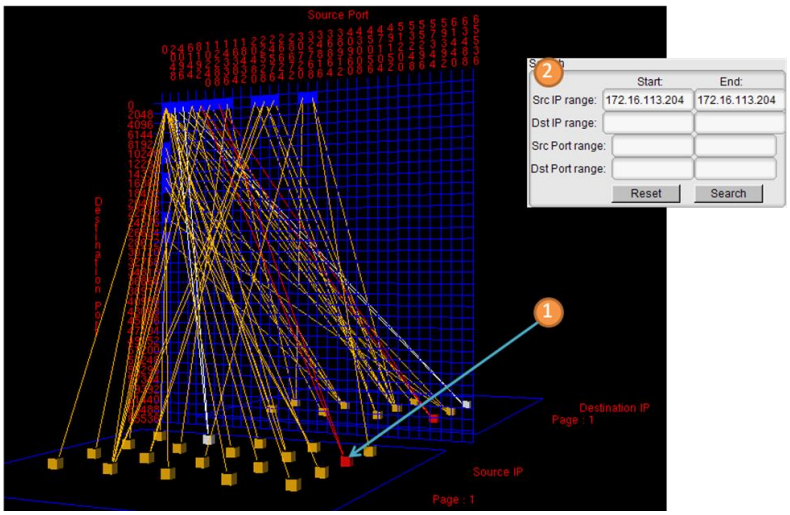

**ภาพที่ 3.18** แสดงตัวอย่างของการระบุข้อมูลมากกว่า 1 ข้อมูลในการค้นหา



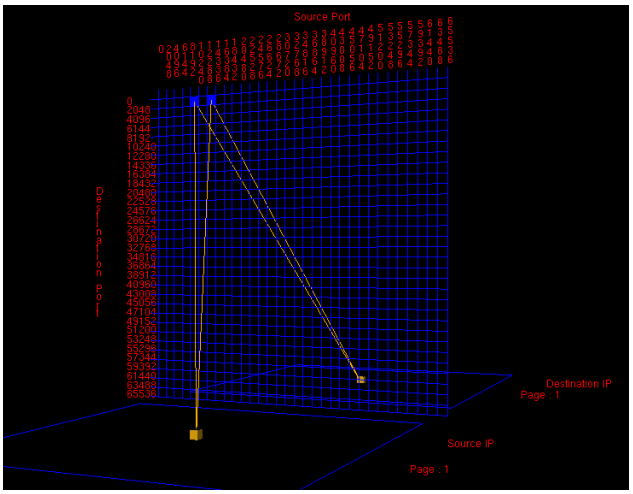

**ภาพที่ 3.19** แสดงผลที่ได้จากการการค้นหา Source IP Address 120.0.0.0 ถึง 130.0.0.0 และ Source Port 80 ถึง 90

3.2.7.2 การค้นหาโดยเลือกวัตถุในหน้าจอแสดงข้อมูล

เมื่อผู้ใช้เลือกวัตถุในหน้าจอแสดงข้อมูล วัตถุนั้นจะเปลี่ยนสีเป็นสีแดง และข้อมูลที่ผู้ใช้เลือกจะแสดงในส่วนกำหนดค่าในการค้นหา เมื่อกดปุ่มค้นหาข้อมูลหน้าจอแสดงข้อมูลจะแสดงเฉพาะวัตถุที่ผู้ใช้เลือก เช่น ผู้ใช้เลือก Source IP Address 172.16.113.204 ดังแสดงในหมายเลข 1 ของภาพที่ 3.20 จะปรากฏข้อมูลของ IP นั้นในส่วนกำหนดค่าในการค้นหาดังแสดงในหมายเลข 2 ของภาพที่ 3.20 เมื่อกดปุ่มค้นหาจะแสดงข้อมูลของ Source IP Address นั้นดังแสดงในภาพที่ 3.21




**ภาพที่ 3.20** แสดงตัวอย่างของการเลือกวัตถุเพื่อทำการค้นหา




**ภาพที่ 3.21** แสดงผลที่ได้จากการการค้นหา Source IP Address 172.16.113.204

### 3.2.8 ส่วนแสดงรายละเอียดของวัตถุในหน้าจอแสดงข้อมูล

แสดงรายละเอียดของวัตถุที่เลือกในหน้าจอแสดงข้อมูล ดังแสดงในภาพที่ 3.22 ซึ่งประกอบด้วย

3.2.8.1 Database Status

แสดงสถานะของฐานข้อมูลในขณะนั้น

3.2.8.2 Source IP

แสดงหมายเลข Source IP Address ที่ผู้ใช้เลือก, จำนวนความสัมพันธ์ของ Source IP Address ที่ผู้ใช้เลือก และหมายเลข Page ของแผ่นกระดานที่แสดง Source IP Address ในขณะนั้น

3.2.8.3 Destination IP

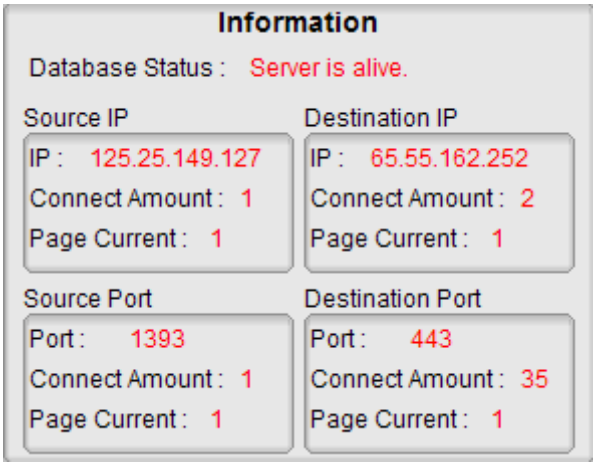
แสดงหมายเลข Destination IP Address ที่ผู้ใช้เลือก, จำนวนความสัมพันธ์ของ Destination IP Address ที่ผู้ใช้เลือก และหมายเลข Page ของแผ่นกระดานที่แสดง Destination IP ในขณะนั้น

3.2.8.4 Source Port

แสดงหมายเลข Source Port ที่ผู้ใช้เลือก, จำนวนความสัมพันธ์ของ Source Port ที่ผู้ใช้เลือก และหมายเลข Page ของแผ่นกระดานที่แสดง Source Port ในขณะนั้น

3.2.8.5 Destination Port

แสดงหมายเลข Destination Port ที่ผู้ใช้เลือก, จำนวนความสัมพันธ์ของ Destination Port ที่ผู้ใช้เลือก และหมายเลข Page ของแผ่นกระดานที่แสดง Destination Port ในขณะนั้น

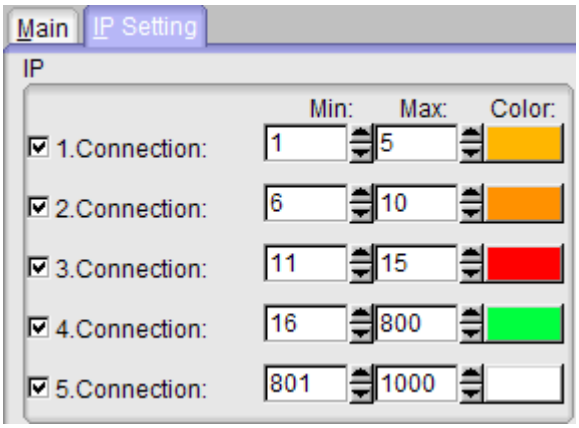



**ภาพที่ 3.22** ส่วนแสดงรายละเอียดของวัตถุในหน้าจอแสดงข้อมูล

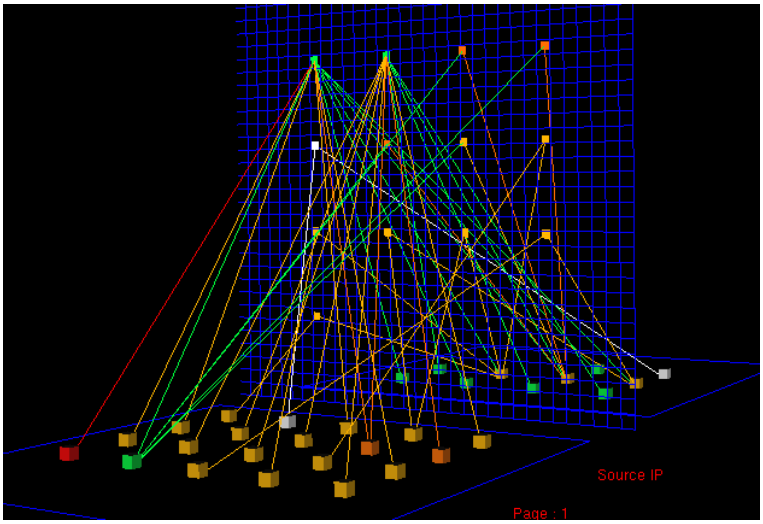
### 3.2.9 ส่วนกำหนดรายละเอียดของความสัมพันธ์ระหว่างข้อมูล

ส่วนที่ให้ผู้ใช้สามารถกำหนดรายละเอียดของเส้นที่แสดงความสัมพันธ์ระหว่างข้อมูลบนแผ่นกระดานทั้งสาม ซึ่งสามารถกำหนดช่วงของความสัมพันธ์ได้ 5 ช่วง ในแต่ละช่วงจะสามารถกำหนดสีของเส้นที่แสดงความสัมพันธ์ระหว่างวัตถุ ตามจำนวนของความสัมพันธ์ที่มีต่อวัตถุนั้น

ดังแสดงในภาพที่ 3.23 เช่น ความสัมพันธ์ที่มีค่า 1-5 แสดงด้วยสีเหลือง ความสัมพันธ์ที่มีค่า 6-10 แสดงด้วยสีส้ม ความสัมพันธ์ที่มีค่า 11-15 แสดงด้วยสีแดง เป็นต้น ผลที่ได้จะแสดงดังภาพที่ 3.24 การกำหนดให้เส้นมีสีที่ต่างกันจะทำให้เห็นถึงจำนวนความสัมพันธ์ของข้อมูลได้ง่ายขึ้น




**ภาพที่ 3.23** ส่วนกำหนดรายละเอียดของเส้นที่แสดงความสัมพันธ์ระหว่างข้อมูล



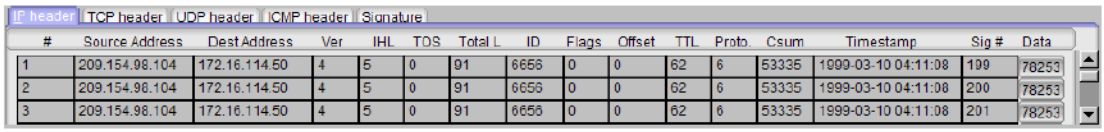

**ภาพที่ 3.24** แสดงผลจากการกำหนดรายละเอียดของเส้นที่แสดงความสัมพันธ์ระหว่างข้อมูล

### 3.2.10 ส่วนแสดงรายละเอียดของข้อมูล Header และ Signature

แสดงรายละเอียดของ IP Header, TCP Header, UDP Header, ICMP Header และ Signature โดยมีรายละเอียดดังนี้

3.2.10.1 IP Header แสดงรายละเอียดของ IP Header ดังภาพที่ 3.25 ซึ่งประกอบด้วย

1) Version (4 bits) หมายเลขเวอร์ชันของ Protocol
2) Internet Header Length (4 bits) ความยาวของ Header ในหน่วย 32 bit words ค่าทั่วไปจะมีค่าเป็น 5 (5*32-bit)
3) Type of Service (8 bits) ใช้เป็นข้อมูลสำหรับ Router ในการเลือกการส่งข้อมูล
4) Total Length (16 bits) ความยาวทั้งหมดของ IP Datagram (byte)
5) Identification (16 bits) หมายเลขของ Datagram
6) Flags (3 bits)
7) Fragment Offset (13 bits) ใช้ในการกำหนดตำแหน่งข้อมูลใน Datagram
8) Time to Live (8 bits) กำหนดจำนวนครั้งที่มากที่สุดที่ Datagram จะส่งระหว่าง Hop เพื่อป้องกันการส่งข้อมูลที่ไม่สิ้นสุด
9) Protocol (8 bits) ระบุ Protocol ที่ใช้ใน Datagram
10) Header Checksum (16 bits) ใช้ในการตรวจสอบความถูกต้องของข้อมูลใน Header


IP header | TCP header | UDP header | ICMP header | Signature

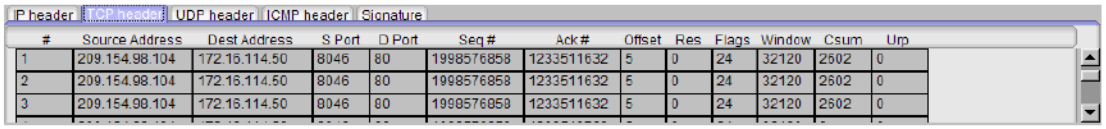
| # | Source Address | Dest Address | Ver | IHL | TOS | Total L | ID | Flags | Offset | TTL | Proto | Csum | Timestamp | Sig # | Data |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 209.154.98.104 | 172.16.114.50 | 4 | 5 | 0 | 91 | 6656 | 0 | 0 | 62 | 6 | 53335 | 1999-03-10 04:11:08 | 199 | 78253 |
| 2 | 209.154.98.104 | 172.16.114.50 | 4 | 5 | 0 | 91 | 6656 | 0 | 0 | 62 | 6 | 53335 | 1999-03-10 04:11:08 | 200 | 78253 |
| 3 | 209.154.98.104 | 172.16.114.50 | 4 | 5 | 0 | 91 | 6656 | 0 | 0 | 62 | 6 | 53335 | 1999-03-10 04:11:08 | 201 | 78253 |

**ภาพที่ 3.25** ส่วนแสดงรายละเอียดของ IP Header

3.2.10.2 TCP Header แสดงรายละเอียดของ TCP Header ดังภาพที่ 3.26 ซึ่งประกอบด้วย

1) Source Port (16 bits)
2) Destination Port (16 bits)
3) Sequence Number (32 bits) หมายเลขบอกลำดับในการสื่อสารในแต่ละครั้ง
4) Acknowledgment Number (32 bits) เหมือนกับ Sequence Number แต่จะใช้ในการตอบรับ

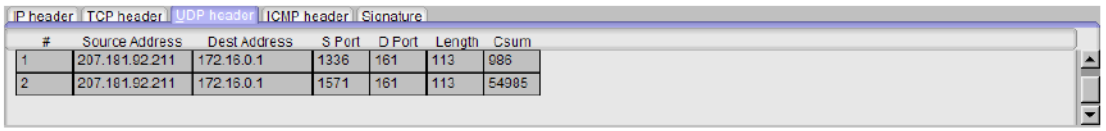
5) Data Offset (4 bits) บอกตำแหน่งที่ Data เริ่มต้น
6) Reserved (3 bits)
7) Flags (6 bits) ควบคุมจังหวะการรับส่งข้อมูล
8) Window (16 bits)
9) Header Checksum (16 bits) ใช้ในการตรวจสอบความถูกต้องของข้อมูลใน Header
10) Urgent Pointer (16 bits)




**ภาพที่ 3.26** ส่วนแสดงรายละเอียดของ TCP Header

3.2.10.3 UDP Header แสดงรายละเอียดของ UDP Header ดังภาพที่ 3.27 ซึ่งประกอบด้วย

1) Source Port (16 bits)
2) Destination Port (16 bits)
3) Length (16 bits) ความยาวของ Datagram
4) Header Checksum (16 bits) ใช้ในการตรวจสอบความถูกต้องของข้อมูลใน Header

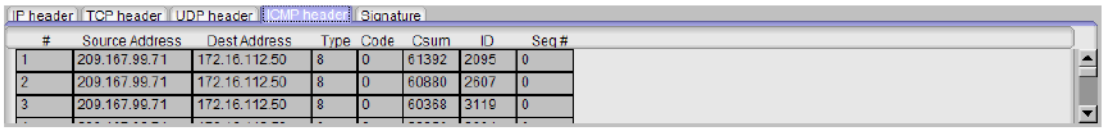



**ภาพที่ 3.27** ส่วนแสดงรายละเอียดของ UDP Header

3.2.10.4 ICMP Header แสดงรายละเอียดของ ICMP Header ดังภาพที่ 3.28 ซึ่งประกอบด้วย

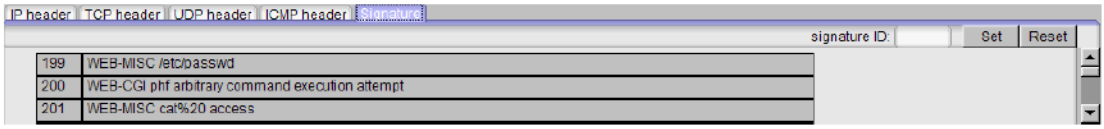
1) Type (8 bits)
2) Code (8 bits)

3) Header Checksum (16 bits) ใช้ในการตรวจสอบความถูกต้องของข้อมูลใน Header




**ภาพที่ 3.28** ส่วนแสดงรายละเอียดของ ICMP Header

3.2.10.5 Signature แสดงรายละเอียดของ Signature ดังภาพที่ 3.29 โดย Signature คือหมายเลขที่ Snort ใช้ในการระบุลักษณะของความผิดปกติในเครือข่ายที่ตรวจจับได้ โดยผู้ใช้สามารถระบุหมายเลข Signature ที่ต้องการค้นหาได้




**ภาพที่ 3.29** ส่วนแสดงรายละเอียดของ Signature

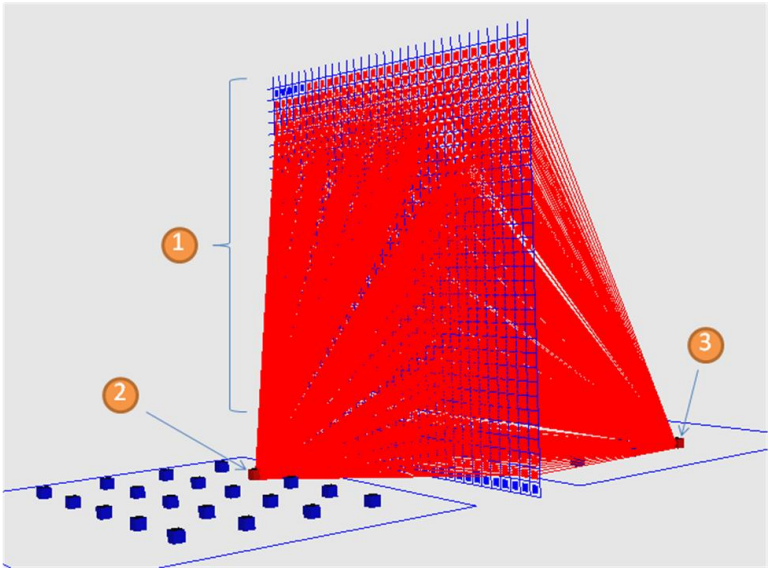
## 3.3 ตัวอย่างการวิเคราะห์ลักษณะการโจมตีและเหตุการณ์ผิดปกติที่เกิดขึ้นในเครือข่ายคอมพิวเตอร์

ในส่วนนี้จะแสดงถึงการใช้เทคนิค Visualization ในการแสดงลักษณะการโจมตีแบบต่างๆ และสถานการณ์ที่ผิดปกติที่เกิดขึ้นในเครือข่ายคอมพิวเตอร์

### 3.3.1 Port Scans

Port Scans เป็นรูปแบบการโจมตีแบบหนึ่งที่สามารถตรวจพบได้ง่าย โดยจะมีการใช้งาน Port เป็นจำนวนมากใน Host หนึ่ง Host การโจมตีเกิดขึ้นโดยผู้โจมตีสแกนหาว่า Port ไหนมีการเปิดใช้งานบ้างบน Host ที่ต้องการโจมตี จุดประสงค์เพื่อตรวจสอบว่ามีบริการใดบ้างบนระบบที่รอรับการเชื่อมต่อ หรืออยู่ในสถานะที่ให้บริการได้บน Host ที่ต้องการโจมตี จากภาพ ที่ 3.30 หมายเลข 1 แสดงถึงจำนวน Port ที่มีการใช้งานซึ่งมีจำนวนมาก โดยผู้โจมตีคือ Host

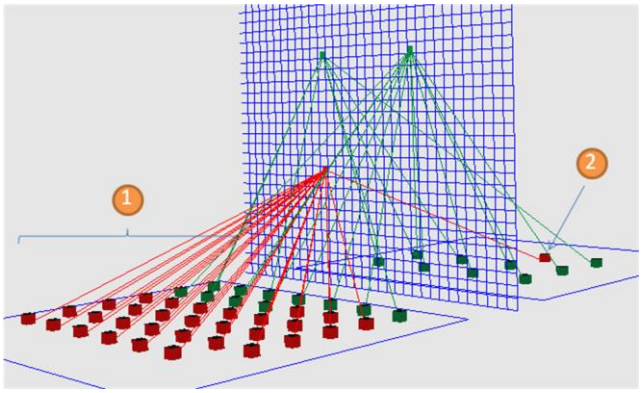
หมายเลข 2 ในภาพที่ 3.30 และผู้ถูกโจมตีคือ Host หมายเลข 3 ในภาพที่ 3.30 เส้นสีแดงแสดงความสัมพันธ์ระหว่าง Source IP, Destination IP และ Port ที่มีการใช้งานอยู่




**ภาพที่ 3.30** แสดงลักษณะของความผิดปกติที่เกิดจาก Port Scans

### 3.3.2 Denial of Service Attacks

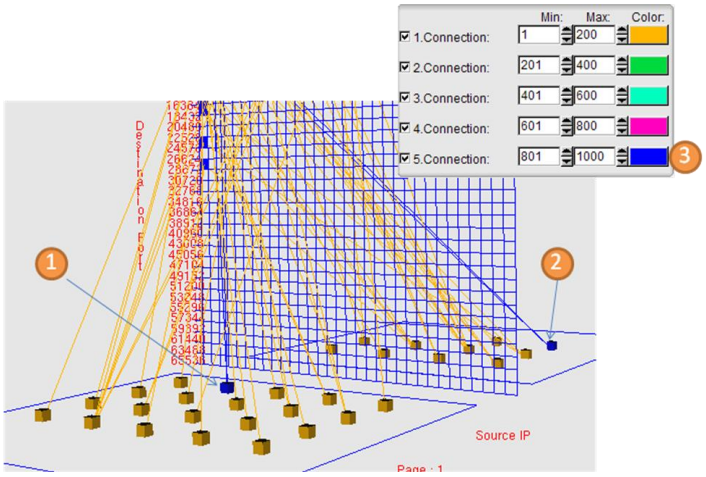
Denial of Service Attacks เป็นการโจมตีที่มีจุดประสงค์เพื่อทำให้เครือข่ายปฏิเสธการให้บริการหรือไม่สามารถดำเนินการต่อไป เนื่องจากไม่สามารถเข้าใช้บริการหรือทรัพยากรในระบบได้ ซึ่งการโจมตีแบบนี้มีด้วยกันหลายวิธี ในภาพที่ 3.31 เป็นการโจมตีแบบ Denial of Service Attacks วิธีหนึ่งเรียกว่า Smurf Attack โดยจากภาพ 3.31 หมายเลข 1 เป็น Host ที่อยู่ในเครือข่ายเดียวกันซึ่งทั้งหมดได้รับ Broadcast Message มาจาก Host หนึ่งที่เป็นผู้โจมตีแต่ได้ทำการปลอม IP Address เป็นของผู้ที่ต้องการโจมตีคือหมายเลข 2 ในภาพที่ 3.31 เมื่อ Host ทุก Host ในหมายเลข 1 ทำการส่ง Echo Message กลับไปที่หมายเลข 2 พร้อมกันในปริมาณมากจะทำให้ Host หมายเลข 2 หยุดการทำงานไปได้




**ภาพที่ 3.31** แสดงลักษณะของความผิดปกติที่เกิดจาก Denial of Service Attacks

### 3.3.3 ปริมาณของการติดต่อสื่อสารในเครือข่ายที่มากผิดปกติ

ปริมาณของการติดต่อสื่อสารในเครือข่าย เป็นปัจจัยหนึ่งในการวิเคราะห์ความผิดปกติที่เกิดขึ้น Host ที่มีปริมาณการติดต่อสื่อสารมากในช่วงเวลาสั้นๆ เป็นเหตุการณ์หนึ่งที่ผู้ดูแลระบบควรให้ความสนใจ เพราะอาจเป็นเป้าหมายของการโจมตีหรือมีความผิดปกติเกิดขึ้น โดยสามารถตรวจสอบ Host ที่มีปริมาณการติดต่อสื่อสารได้โดยใช้สีในการจำแนก จากภาพที่ 3.32 พบว่า Host หมายเลข 1 และ Host หมายเลข 2 มีการติดต่อสื่อสารในปริมาณที่มากซึ่งแสดงด้วยเส้นสีฟ้า โดยสังเกตได้จาก ส่วนกำหนดรายละเอียดของเส้นที่แสดงความสัมพันธ์ระหว่างข้อมูล ดังแสดงในหมายเลข 3 ของภาพที่ 3.32




**ภาพที่ 3.32** แสดงลักษณะของความผิดปกติที่เกิดจากปริมาณของการติดต่อสื่อสารที่มากผิดปกติ

# บทที่ 4

# การประเมินประสิทธิผลของวิธีการที่นำเสนอ

## 4.1 วิธีการประเมินประสิทธิผล

ข้อมูลการติดต่อสื่อสารในเครือข่ายคอมพิวเตอร์ที่ใช้ในการประเมินประสิทธิผลนี้มาจาก DARPA Intrusion Detection Evaluation Data Sets ในปี ค .ศ.1999 ซึ่ง สร้างขึ้นโดย The Information Systems Technology Group (IST) of MIT Lincoln Laboratory

การประเมินประสิทธิผลมีจุดประสงค์ เพื่อวัดระดับ ความพึงพอใจของผู้ใช้ที่มีต่อการออกแบบส่วนประสานกับผู้ใช้และส่วนประกอบต่าง ๆ ของระบบ และ วัดประสิทธิผลของวิธีการแสดงข้อมูลที่ได้นำเสนอในงานวิจัยนี้ เพื่อ ช่วยให้ผู้ใช้สามารถสังเกตและเข้าใจความผิดปกติที่เกิดขึ้นภายในเครือข่ายคอมพิวเตอร์ได้

การประเมินประสิทธิผลจะทำโดยกลุ่มผู้ประเมินจำนวน 6 คน รายละเอียดและข้อมูลของกลุ่มผู้ประเมินแสดงไว้ดังตารางที่ 4.1 การ ประเมินประสิทธิผลเริ่มด้วยการอธิบายให้ผู้ประเมินเข้าใจถึงวัตถุประสงค์ของงานวิจัย แนวคิดในการออกแบบระบบ และจุดประสงค์ของการ ประเมินประสิทธิผล จากนั้นจะให้ผู้ ประเมินได้ใช้งานระบบและทำการตอบแบบสอบถามซึ่งแบ่งเป็น 2 ส่วน ดังนี้

ส่วนที่ 1 เป็นส่วนที่เก็บข้อมูลเกี่ยวกับความพึงพอใจของผู้ประเมินที่มีต่อระบบ โดยจะให้ผู้ประเมินได้ทดลองใช้งานระบบในส่วนต่าง ๆ จุดประสงค์ในการ ประเมินประสิทธิผลส่วนนี้เพื่อวัดระดับความพึงพอใจของผู้ใช้ที่มีต่อการออกแบบส่วนประสานกับผู้ใช้ และส่วนประกอบต่าง ๆ ของระบบ แบบสอบถามส่วนนี้มีต้นแบบมาจาก Questionnaire for User Interface Satisfaction (QUIS) โดยนำมาประยุกต์ใช้เพื่อให้เหมาะสมกับการใช้เป็นแบบสอบถามสำหรับงานวิจัยนี้

ส่วนที่ 2 ใช้เหตุการณ์จำลองที่มีความผิดปกติเกิดขึ้นในเครือข่าย โดยจะให้ผู้ ประเมินอธิบายถึงลักษณะของความผิดปกติ หรือการโจมตีที่เกิดขึ้นในแต่ละข้อโดยสังเขป จุดประสงค์ในการประเมินประสิทธิผลส่วนนี้เพื่อวัดประสิทธิผลของงานวิจัยให้ตรงตามวัตถุประสงค์ว่า วิธีการแสดงข้อมูลโดยใช้เทคนิค Visualization ที่ได้นำเสนอในงานวิจัยนี้จะช่วยให้ผู้ใช้สามารถสังเกตและเข้าใจความผิดปกติที่เกิดขึ้นภายในเครือข่ายคอมพิวเตอร์ได้หรือไม่

**ตารางที่ 4.1** ข้อมูลของกลุ่มผู้ประเมินประสิทธิผล

| | ตำแหน่ง (ปัจจุบัน) | สถานที่ทำงาน | ประสบการณ์การทำงาน |
|---|---|---|---|
| ผู้ประเมิน คนที่ 1 | Analyst Programmer | DST International Co., Ltd. | ● RIA Web Application for Mutual Fund's Transfer Agency, 2007 - Present<br>● A JavaScript API Providing a Streaming Real-Time Quote Data, 2007<br>● SDS - Web Services for Snapshot Financial Data, 2006 - 2007<br>● IRIS - A Web Application for Software Process Management System, 2004 - 2006 |
| ผู้ประเมิน คนที่ 2 | ครูสอนวิชา คอมพิวเตอร์ | โรงเรียนวัดอ้อมน้อย (สังกัด สพฐ.) | ● ครูอัตราจ้าง โรงเรียนวัดอ้อมน้อย (สังกัด สพฐ.)<br>● กำลังศึกษา การบริหารสารสนเทศ มหาวิทยาลัยวลัยลักษณ์<br>● สำเร็จหลักสูตร ใบประกอบวิชาชีพครู มหาวิทยาลัยราชภัฏบ้านสมเด็จ |
| ผู้ประเมิน คนที่ 3 | Senior Application Engineer | The Stock Exchange of Thailand | ● SET Community Portal - Web Application for Information Disclosure, 2006 - Present<br>● Price Reporting System - Real Time Application & Web Services for Information Dissemination, 2005 - 2006<br>● Market for Alternative Investment - Web Application for Information Representation, 2005<br>● SET Information Management System Data Warehouse - Web Application for Information Management System, 2004 - 2005 and 2008 - 2009<br>● SET Market Analysis and Reporting Tool - Web Application for Information Representation, 2004 |

**ตารางที่ 4.1** (ต่อ)

| | ตำแหน่ง (ปัจจุบัน) | สถานที่ทำงาน | ประสบการณ์การทำงาน |
|---|---|---|---|
| ผู้ประเมินคนที่ 4 | System Administrator | National Science and Technology Development Agency, National Electronics and Computer Technology Center | ● System Administrator, 2004 - Present<br>● Web Server Setting, 2004 - Present<br>● Web Application Programmer, 2004 - Present<br>● Computer Testing Engineer, 2004 - Present |
| ผู้ประเมินคนที่ 5 | Senior Project Developer | Freewill Solutions Co., Ltd. | ● iFIS - Stock Trading Application, 2007 - Present<br>● IIA - Insurance Management Application, 2004 - 2006 |
| ผู้ประเมินคนที่ 6 | Senior Developer (SA) | CSI Group (Thailand) | ● Sales Management System, Office Sale Department, 2009<br>● Excite Tax Management, Denso, 2008<br>● PMCS (Permission Control System), Denso, 2008<br>● E-Budgeting System, Denso, 2007 - 2009<br>● ATM (Automated Teller Machine), Fujitsu, 2006<br>● POS (Point of Sale), Family Mart, 2005<br>● Asset Management System, Office Admin Department, 2005<br>● Coil Management System, Sumikin coil Center, 2004<br>● Production Control System , Siam Toyota, 2004 |

## 4.2 ผลที่ได้จากการประเมินประสิทธิผล

ผลการประเมินประสิทธิผลที่ได้จากแบบสอบถามในส่วนที่ 1 การวัดระดับความพึงพอใจของผู้ประเมินที่มีต่อระบบ แสดงไว้ในตารางที่ 4.2 ซึ่งมีผลการประเมินประสิทธิผลดังนี้

ความพึงพอใจของผู้ประเมินที่มีต่อระบบในภาพรวม พบว่าผู้ ประเมินส่วนใหญ่มีระดับความพึงพอใจอยู่ในระดับมาก (ระดับที่ 4) โดยมีผู้เลือก 23 จาก 36 ข้อ คิดเป็น 63.89 %

ความพึงพอใจของผู้ประเมินที่มีต่อส่วนการจัดการเกี่ยวกับหน้าจอ พบว่าผู้ ประเมินส่วนใหญ่มีระดับความพึงพอใจอยู่ในระดับมาก (ระดับที่ 4 ) โดยมีผู้เลือก 10 จาก 24 ข้อ คิดเป็น 41.67 %

ความพึงพอใจของผู้ประเมินที่มีต่อส่วนการจัดการข้อมูลต่างๆ ของระบบ พบว่าผู้ประเมินส่วนใหญ่มีระดับความพึงพอใจอยู่ในระดับมาก (ระดับที่ 4) โดยมีผู้เลือก 11 จาก 24 ข้อ คิดเป็น 45.83 %

ความพึงพอใจของผู้ประเมินที่มีต่อการเรียนรู้การใช้งานระบบ พบว่าผู้ ประเมินส่วนใหญ่มีระดับความพึงพอใจอยู่ในระดับมาก (ระดับที่ 4) โดยมีผู้เลือก 9 จาก 18 ข้อ คิดเป็น 50%

ความพึงพอใจของผู้ประเมินที่มีต่อความสามารถของระบบ พบว่าผู้ ประเมินส่วนใหญ่มีระดับความพึงพอใจอยู่ในระดับมากและมากที่สุด (ระดับที่ 4 และระดับที่ 5) โดยมีผู้เลือกเท่ากัน คือ 9 จาก 24 ข้อ คิดเป็น 37.5 %

สรุปผลการประเมินที่ได้จากแบบสอบถามในส่วนที่ 1 ผู้ประเมินส่วนใหญ่มีระดับความพึงพอใจอยู่ในระดับมาก โดยมีผู้เลือก 62 จาก 126 ข้อ คิดเป็น 49.21% ของจำนวนข้อทั้งหมด

**ตารางที่ 4.2** ผลที่ได้จากแบบสอบถามเพื่อประเมินประสิทธิผลในส่วนที่ 1

| ข้อคำถาม | ระดับความพึงพอใจ *(NA = ไม่สามารถระบุได้) | | | | | | |
|---|---|---|---|---|---|---|---|
| **OVERALL REACTION TO THE SOFTWARE** | | **1** | **2** | **3** | **4** | **5** | **NA** |
| 1.ภาพรวมของระบบ | แย่ | | | | 5 | 1 | ดีเยี่ยม |
| 2.การใช้งาน | ยาก | | | 1 | 5 | | ง่าย |
| 3.ความพึงพอใจที่มีต่อระบบ | ไม่พอใจ | | | | 4 | 2 | พอใจ |
| 4.ฟังก์ชันของระบบ | ไม่พอเพียง | | | | 5 | 1 | พอเพียง |
| 5.ความน่าสนใจ | น่าเบื่อ | | | | 2 | 4 | น่าสนใจ |
| 6.ความยืดหยุ่น | ไม่ยืดหยุ่น | | | 3 | 2 | 1 | ยืดหยุ่น |

**ตารางที่ 4.2** (ต่อ)

| ข้อคำถาม | ระดับความพึงพอใจ *(NA = ไม่สามารถระบุได้) | | | | | | |
|---|---|---|---|---|---|---|---|
| **SCREEN** | | **1** | **2** | **3** | **4** | **5** | | **NA** |
| 7.การอ่านตัวอักษรบนหน้าจอ | ยาก | | | 2 | 3 | 1 | ง่าย | |
| 8.การควบคุม Cursor และการเคลื่อนไหวบนหน้าจอ | ยาก | | 1 | | 2 | 3 | ง่าย | |
| 9.การแสดงข้อมูลต่าง ๆบนหน้าจอ | สับสน | | | 2 | 3 | 1 | เข้าใจง่าย | |
| 10.การจัดวางตำแหน่งของหน้าจอและปุ่มต่าง ๆ | สับสน | | | 1 | 2 | 3 | เข้าใจง่าย | |
| **SYSTEM INFORMATION** | | **1** | **2** | **3** | **4** | **5** | | **NA** |
| 11.ข้อความที่แสดงช่วยในการทำความเข้าใจข้อมูล | ไม่ช่วย | | | 3 | 3 | | ช่วย | |
| 12.ข้อความที่แสดงสอดคล้องกับสิ่งที่กำลังทำ | ไม่สอดคล้อง | | | 2 | 4 | | สอดคล้อง | |
| 13.ตำแหน่งของข้อความบนหน้าจอ | ไม่สอดคล้อง | | | 2 | 2 | 2 | สอดคล้อง | |
| 14.การป้อนข้อมูล (Input) ของผู้ใช้ | สับสน | | | | 2 | 3 | เข้าใจง่าย | 1 |
| **LEARNING** | | **1** | **2** | **3** | **4** | **5** | | **NA** |
| 15.การเรียนรู้วิธีใช้งานระบบ | ยาก | | 1 | | 4 | 1 | ง่าย | |
| 16.การจดจำชื่อและทำความเข้าใจปุ่มคำสั่งต่าง ๆ | ยาก | | | 1 | 3 | 2 | ง่าย | |
| 17.ขั้นตอนที่ใช้เพื่อให้ได้ข้อมูลที่ต้องการ | มาก | | | 1 | 2 | 3 | น้อย | |
| **SYSTEM CAPABILITIES** | | **1** | **2** | **3** | **4** | **5** | | **NA** |
| 18.ความเร็วของระบบ | ช้า | | 1 | 1 | 1 | 3 | เร็ว | |
| 19.ความน่าเชื่อถือของระบบ | ไม่น่าเชื่อถือ | | 1 | | 2 | 3 | น่าเชื่อถือ | |
| 20.การเกิด Error | บ่อย | | 1 | | 4 | 1 | ไม่เคย | |
| 21.การทำสิ่งที่ผิดพลาดให้กลับมาถูก | ยาก | | 1 | | 2 | 2 | ง่าย | 1 |

ผลการประเมินประสิทธิผลที่ได้จากแบบสอบถามในส่วนที่ 2 การวัดประสิทธิผลของงานวิจัยว่าวิธีการแสดงข้อมูลแบบใหม่โดยใช้เทคนิค Visualization ที่ได้นำเสนอในงานวิจัยนี้จะช่วยให้ผู้ใช้สามารถสังเกตและเข้าใจความผิดปกติที่เกิดขึ้นภายในเครือข่ายคอมพิวเตอร์ได้หรือไม่ แสดงไว้ในตารางที่ 4.3 ซึ่งมีผลการประเมินประสิทธิผลดังนี้

คำถามข้อที่ 1 เหตุการณ์ที่กำหนดไว้มีลักษณะของความผิดปกติคือ มีจำนวนของ Source IP หลาย IP ทำการติดต่อไปยัง Destination IP 202.168.23.6 ในจำนวนที่มากผิดปกติ และ Source IP เหล่านั้นอยู่ในเครือข่ายเดียวกัน ผลที่ได้จากแบบสอบถามพบว่าผู้ ประเมินทุกคนสามารถระบุ Destination IP ที่เกิดความผิดปกติและลักษณะของความผิดปกติได้ถูกต้อง

คำถามข้อที่ 2 เหตุการณ์ที่กำหนดไว้มีลักษณะของความผิดปกติคือ มีการติดต่อจาก Source IP 129.152.1.22 ไปที่ Destination IP 198.47.255.2 โดยการติดต่อแต่ละครั้งจะใช้ Source Port ที่แตกต่างกันซึ่งมีจำนวนมากผิดปกติ ผลที่ได้จากแบบสอบถามพบว่าผู้ประเมินทุกคนสามารถระบุ Destination IP ที่เกิดความผิดปกติและลักษณะของความผิดปกติได้ถูกต้อง

คำถามข้อที่ 3 เหตุการณ์ที่กำหนดไว้มีลักษณะของความผิดปกติคือ มีการติดต่อจาก Source IP 212.160.184.82 ไปที่ Destination IP 212.160.184.82 ซึ่งเป็นค่าเดียวกันในปริมาณที่มากผิดปกติ ผลที่ได้จากแบบสอบถามพบว่ามีผู้ ประเมิน 4 คนที่สามารถระบุ Destination IP ที่เกิดความผิดปกติและลักษณะของความผิดปกติได้ถูกต้อง มีผู้ประเมิน 1 คนที่ระบุ Destination IP ที่เกิดความผิดปกติและลักษณะของความผิดปกติไม่ถูกต้อง และมีผู้ประเมิน 1 คนที่ไม่สามารถระบุ Destination IP ที่เกิดความผิดปกติและลักษณะของความผิดปกติได้

คำถามข้อที่ 4 เหตุการณ์ที่กำหนดไว้มีลักษณะของความผิดปกติคือ มีการติดต่อจาก Source IP 200.34.150.37 ไปที่ Destination IP 160.168.47.47 โดยการติดต่อแต่ละครั้งจะใช้ Destination Port ที่แตกต่างกันซึ่งมีจำนวนมากผิดปกติ ผลที่ได้จากแบบสอบถามพบว่ามีผู้ประเมิน 3 คนที่สามารถระบุ Destination IP ที่เกิดความผิดปกติและลักษณะของความผิดปกติได้ถูกต้อง และมีผู้ประเมิน 3 คนที่ระบุ Destination IP ที่เกิดความผิดปกติและลักษณะของความผิดปกติไม่ถูกต้อง

สรุปผลการประเมินประสิทธิผลที่ได้จากแบบสอบถามในส่วนที่ 2 วิธีการแสดงข้อมูลแบบใหม่โดยใช้เทคนิค Visualization ที่ได้นำเสนอในงานวิจัยนี้ช่วยให้ผู้ใช้สามารถเข้าใจความผิดปกติที่เกิดขึ้นภายในเครือข่ายคอมพิวเตอร์ได้ โดยวัดจากจำนวนข้อที่ผู้ ประเมินสามารถระบุลักษณะของความผิดปกติได้ถูกต้อง 19 จาก 24 ข้อ คิดเป็น 79.17 % ของจำนวนข้อทั้งหมด

**ตารางที่ 4.3** ผลที่ได้จากแบบสอบถามเพื่อประเมินประสิทธิผลในส่วนที่ 2

| ลักษณะของความผิดปกติ | จำนวนผู้ประเมินที่ระบุลักษณะความผิดปกติได้ถูกต้อง | จำนวนผู้ประเมินที่ระบุลักษณะความผิดปกติไม่ถูกต้อง | จำนวนผู้ประเมินที่ไม่สามารถระบุลักษณะความผิดปกติได้ |
|---|---|---|---|
| 1. มีจำนวนการติดต่อจากหลาย Source IP ไปที่ Destination IP 202.168.23.6 ในจำนวนที่มากผิดปกติ | 6 | | |
| 2. มีการติดต่อจาก Source IP 129.152.1.22 ไปที่ Destination IP 198.47.255.2 โดยการติดต่อแต่ละครั้งจะใช้ Source Port ที่แตกต่างกันซึ่งมีจำนวนมากผิดปกติ | 6 | | |
| 3. มีการติดต่อจาก Source IP 212.160.184.82 ไปที่ Destination IP 212.160.184.82 ซึ่งเป็นค่าเดียวกันในปริมาณที่มากผิดปกติ | 4 | 1 | 1 |
| 4. มีการติดต่อจาก Source IP 200.34.150.37 ไปที่ Destination IP 160.168.47.47 โดยการติดต่อแต่ละครั้งจะใช้ Destination Port ที่แตกต่างกันซึ่งมีจำนวนมากผิดปกติ | 3 | 3 | |

จากแบบสอบถามทั้ง 2 ส่วน สรุป ผลการประเมินประสิทธิผลได้ว่า ผู้ประเมินส่วนใหญ่มีระดับความพึงพอใจต่อการออกแบบส่วนประสานกับผู้ใช้และส่วนประกอบต่างๆ ของระบบอยู่ในระดับมาก โดยวัดจากระดับความพึงพอใจ ในลักษณะการใช้งานของผู้ประเมิน และ วิธีการแสดงข้อมูลโดยใช้เทคนิค Visualization ที่นำเสนอในงานวิจัยนี้ช่วยให้ผู้ใช้สามารถตรวจจับและเข้าใจความผิดปกติที่เกิดขึ้นภายในเครือข่ายคอมพิวเตอร์ได้

# บทที่ 5

# สรุปผลการวิจัยและข้อเสนอแนะ

## 5.1 สรุปผลการวิจัย

วิทยานิพนธ์ฉบับนี้เสนอวิธีการนำเสนอข้อมูลการสื่อสารในเครือข่ายคอมพิวเตอร์ เพื่อช่วยให้ผู้ดูแลระบบเครือข่ายเข้าใจสภาวะการติดต่อสื่อสาร และสามารถตรวจจับความผิดปกติที่เกิดขึ้นในเครือข่าย โดยใช้เทคนิคคอมพิวเตอร์กราฟฟิกส์ 3 มิติและการออกแบบส่วนประสานกับผู้ใช้ในการควบคุมการแสดงผลและค้นหาข้อมูล ข้อมูลการสื่อสารจะถูกแสดงบนแผ่นกระดา น (Plate) 3 แผ่น ที่ตั้งฉากกันในพื้นที่ 3 มิติ การแสดงความสัมพันธ์ระหว่างข้อมูลบนแผ่นกระดานแต่ละแผ่นใช้เส้นเชื่อมระหว่างวัตถุบนแผ่นกระดานทั้งสาม และใช้สีของเส้นในการกำหนดปริมาณของการติดต่อสื่อสารในเครือข่ายคอมพิวเตอร์

วิธีการที่นำเสนอประกอบด้วยส่วนประกอบที่สำคัญ 3 ส่วน คือ ส่วนที่หนึ่งระบบการตรวจจับการบุกรุกในระดับเครือข่ายคอมพิวเตอร์ ทำหน้าที่วิเคราะห์การสื่อสารในเครือข่ายคอมพิวเตอร์ว่าเป็นการบุกรุกหรือไม่ ส่วนที่สองระบบฐานข้อมูล ทำหน้าที่ในการ จัดเก็บผลของการวิเคราะห์ที่ได้จากระบบตรวจจับการบุกรุก และส่วนที่สามระบบการ สร้างภาพนามธรรม ทำหน้าที่แสดงข้อมูลในเครือข่ายคอมพิวเตอร์ในลักษณะ 3 มิติ ซึ่งใช้เทคนิค Visualization ในการแสดงข้อมูล โดยจะแสดงข้อมูลบนแผ่นกระดาน 3 แผ่นที่ตั้งฉากกัน ในพื้นที่ 3 มิติ โดยใช้ตำแหน่งของแผ่นกระดานในการกำหนดพื้นที่ในการแสดงข้อมูล ประกอบด้วย 1 ) แผ่นกระดานด้านหน้า (Front Plate) เป็นพื้นที่สำหรับแสดงข้อมูลของ Source IP Address 2) แผ่นกระดานตรงกลาง (Middle Plate) เป็นพื้นที่สำหรับแสดงข้อมูลของ Port 3) แผ่นกระดานด้านหลัง (Back Plate) เป็นพื้นที่สำหรับแสดงข้อมูลของ Destination IP Address โดยใช้เส้นในการแสดงความสัมพันธ์ระหว่างข้อมูลบนแผ่นกระดานทั้งสาม และใช้สีของเส้นในการกำหนดปริมาณของการติดต่อสื่อสารในเครือข่ายคอมพิวเตอร์ ผู้ใช้งานสามารถหมุนและย่อขยายมุมมองในการแสดงข้อมูลได้

ระบบต้นแบบได้ถูกพัฒนาขึ้นตามหลักการออกแบบที่นำเสนอ และทำการประเมินประสิทธิผลโดยใช้แบบสอบถามกับผู้ประเมินจำนวน 6 คน ผลการ ประเมินประสิทธิผลสรุปได้ว่าผู้ประเมินส่วนใหญ่มีระดับความพึงพอใจต่อการออกแบบส่วนประสานกับผู้ใช้ และส่วนประกอบต่างๆ ของระบบอยู่ในระดับมาก โดยวัดจากระดับความพึงพอใจ ในการใช้งานของผู้ประเมิน และ

วิธีการแสดงข้อมูลแบบใหม่โดยใช้เทคนิค Visualization ที่ได้เสนอในงานวิจัยนี้ช่วยให้ผู้ใช้สามารถตรวจจับและเข้าใจความผิดปกติที่เกิดขึ้นภายในเครือข่ายคอมพิวเตอร์ได้

## 5.2 ข้อเสนอแนะ

ในส่วนของการแสดงข้อมูล การพัฒนาต่อไปในอนาคตควรปรับปรุงรูปแบบการแสดงรายละเอียดของข้อมูล โดยเมื่อนำเมาส์ไปชี้ที่วัตถุควรจะแสดงรายละเอียดของข้อมูลเป็นกล่องข้อความ (Tooltip) เหนือวัตถุนั้นได้

ในส่วนของการออกแบบส่วนประสานกับผู้ใช้ ควรปรับปรุงให้ง่ายต่อการใช้งานของผู้ใช้และเป็นประโยชน์ในการใช้งานยิ่งขึ้น เช่น การพัฒนาในส่วนของการค้นหาข้อมูล ให้สามารถทำการค้นหา IP Address หลาย IP Address พร้อมกัน หรือทำการค้นหาในลักษณะเงื่อนไข เช่น ไม่เท่ากับ มากกว่า หรือน้อยกว่าได้ และพัฒนาในส่วนของการแสดงรายละเอียดของ Header ให้สามารถจับเก็บผลของการแสดงข้อมูลเป็น Text Files หรือพิมพ์ออกเป็นรายงานได้ เป็นต้น

# บรรณานุกรม


Abdullah, Kulsoom; Lee, Chris; Conti, Gregory; Copeland, John A. and Stasko, John. 2005. IDS RainStorm: Visualizing IDS Alarms. In **VizSEC: Proceedings of the IEEE Workshops on Visualization for Computer Security.** Washington, DC: IEEE Computer Society. Pp. 1-10.

Archibald, Neil; Ramirez, Gilbert; Rathaus, Noam. 2005. **Nessus, Snort, & Ethereal Power Tools: Customizing Open Source Security Applications.** Rockland: Syngress.

Beale, Jay. 2004. **Snort 2.1 Intrusion Detection.** 2nd ed. Rockland: Syngress.

Beale, Jay; Temmingh, Roelof; Meer, Haroon; Walt, Charl van der and Moore, HD. 2005. **Penetration Tester's Open Source Toolkit.** Rockland: Syngress.

Bearavolu, Ratna; Lakkaraju, Kiran and Yurcik, William. 2005. **NVisionIP: An Animated State Analysis Tool for Visualizing NetFlows.** Retrieved May 8, 2008 from http://www.cert.org/flocon/2005/presentations/Bearavolu-NVisionIP-FloCon2005.pdf

Bejtlich, Richard. 2004. **The Tao of Network Security Monitoring: Beyond Intrusion Detection.** Boston: Addison Wesley.

Fink, Glenn A.; Ball, Robert; North, Chris; Jawalkar, Nipun and Correa, Ricardo. 2004. **Network Eye: End-to-End Computer Security Visualization.** Retrieved May 21, 2008 from http://people.cs.vt.edu/~finkga/downloads/Fink-etal-VizSec2004.pdf

Goodall, John R.; Lutters, Wayne G.; Rheingans, Penny and Komlodi, Anita. 2005. Preserving the Big Picture: Visual Network Traffic Analysis with TNV. In **VizSEC: Proceedings of the IEEE Workshop on Visualization for Computer Security.** Washington, DC: IEEE Computer Society. Pp. 47-54.

Goodall, John R.; Lutters, Wayne G.; Rheingans, Penny and Komlodi, Anita. 2006. Focusing on Context in Network Traffic Analysis. In **IEEE Computer Graphics and Applications.** Los Alamitos: IEEE Computer Society. Pp. 72-80.

Kasemsri, Rawiroj Robert. 2005. **A Survey, Taxonomy, and Analysis of Network Security Visualization Techniques.** Master's thesis, Georgia State University.

Kilgard, Mark J. 1996. **The OpenGL Utility Toolkit (GLUT) Programming Interface.** Retrieved June 9, 2008 from http://www.opengl.org/resources/libraries/glut/glut-3.spec.pdf

Lakkaraju, Kiran; Yurcik, William and Lee, Adam J.. 2004. NVisionIP: NetFlow Visualizations of System State for Security Situational Awareness. In **VizSEC/DMSEC: Proceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security.** New York: ACM. Pp. 65-72.

Lincoln Laboratory, Massachusetts Institute of Technology. 1999. **1999 DARPA Intrusion Detection Evaluation Data Set.** Retrieved October 15, 2008 from http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/data/1999data.html

Northcutt, Stephen; Cooper, Mark; Fearnow, Matt and Frederick, Karen. 2001. **Intrusion Signatures and Analysis.** Indianapolis: New Riders.

OpenGL. 2008. **OpenGL 2.1 Reference Pages.** Retrieved June 9, 2008 from http://www.opengl.org/sdk/docs/man

Riel, Jean-Pierre van. 2006. **InetVis: Internet Visualization for Network Traffic Analysis.** Retrieved January 22, 2009 from http://www.cs.ru.ac.za/research/g02v2468/inetvis/0.9.3/doc/inetvisdoc.html

Snort Team. 2006. **Snort Users Manual.** Retrieved July 20, 2008 from http://www.snort.org/docs/snort_htmanuals/htmanual_284

Steele, Michael E.. 2008. **Windows Intrusion Detection System (WinIDS).** Retrieved October 25, 2008 from http://www.winids.com/index.php?module=Pages&func=display&pageid=11

Sweet, Michael; Earls, Craig P.; Melcher, Matthias and Spitzak, Bill. 2006. **FLTK 1.1.8 Programming Manual.** Retrieved October 23, 2008 from http://www.fltk.org/doc-1.1/fltk.pdf

Takada, Tetsuji and Koike, Hideki. 2002. Tudumi: Information Visualization System for Monitoring and Auditing Computer Logs. In **Proceedings of 6th International Conference on Information Visualization (IV' 02).** IEEE CS Press. Pp. 560-576.

The University of Maryland. 2004. **Questionnaire for User Interaction Satisfaction (QUIS).** Retrieved January 28, 2009 from http://lap.umd.edu/quis

# ประวัติผู้เขียน

| | |
|---|---|
| **ชื่อ ชื่อสกุล** | นายชนาธิป ชื่นมนัส |
| **ประวัติการศึกษา** | ปริญญาตรี หลักสูตรวิทยาศาสตรบัณฑิต<br>สาขาศาสตร์คอมพิวเตอร์ คณะวิทยาศาสตร์<br>มหาวิทยาลัยธรรมศาสตร์ ปีการศึกษา 2546 |