Department of Computer Science;

Faculty of Science, Khon Kaen University

Course No : 322766

Course Name : Computer Networks

Student Name/Last Name : Chanida Tawornrach

Student ID : 585020144-2

Student Name/Last Name : Worapoj Suwanpipob

Student ID : 585020071-3

Student Name/Last Name : Weerachart Lertyingyod

Student ID : 575020247-1

Student Name/Last Name : Nontachai Danpakdee

Student ID : 575020246-3

Submission Date : 29th October 2015

Consent : I have worked with other students listed below WITHOUT copying word by word! all penalties will be concurred otherwise (providing student's signature)

คู่มือการใช้งานเครื่องมือ Colasoft Capsa 8 Enterprise

Colasoft Capsa พัฒนาโดยบริษัท Colasoft จากประเทศสหรัฐอเมริกา เป็นโปรแกรมที่ถูกพัฒนาขึ้นมาเพื่อที่จะเอาไว้มอนิเตอร์ดูการรับส่งข้อมูลในวงเน็ตเวิร์คหรือวง LAN ได้อย่างละเอียด มีฟังก์ชันการใช้งานที่ครอบคลุมหลากหลาย เช่น มีระบบตรวจสอบและป้องกันไฟล์ที่ไม่พึงประสงค์ที่จะบุกรุกเข้ามาในข้อมูลระบบเครือข่าย สังเกตปริมาณการรับส่งข้อมูลที่อาจผิดปกติ ผิดเพี้ยนไปจากเดินที่เคยเป็น นอกจากนี้ยังใช้แสดงค่าปริมาณและสถิติการรับส่งข้อมูลในระบบเครือข่ายได้ (Bandwidth Statistics) สามารถตรวจสอบข้อมูลเครือข่ายการใช้งานโปรแกรมบนเว็บเบราว์เซอร์ต่างๆได้ ซึ่งสนับสนุนโปรโตคอลแบบต่างๆ หรือพวกโปรแกรมแชทและอื่นๆอีกมากมาย แต่สำหรับในเวอร์ชั่นฟรีจะไม่สามารถรองรับการดูข้อมูลของเครือข่ายบางอย่างได้

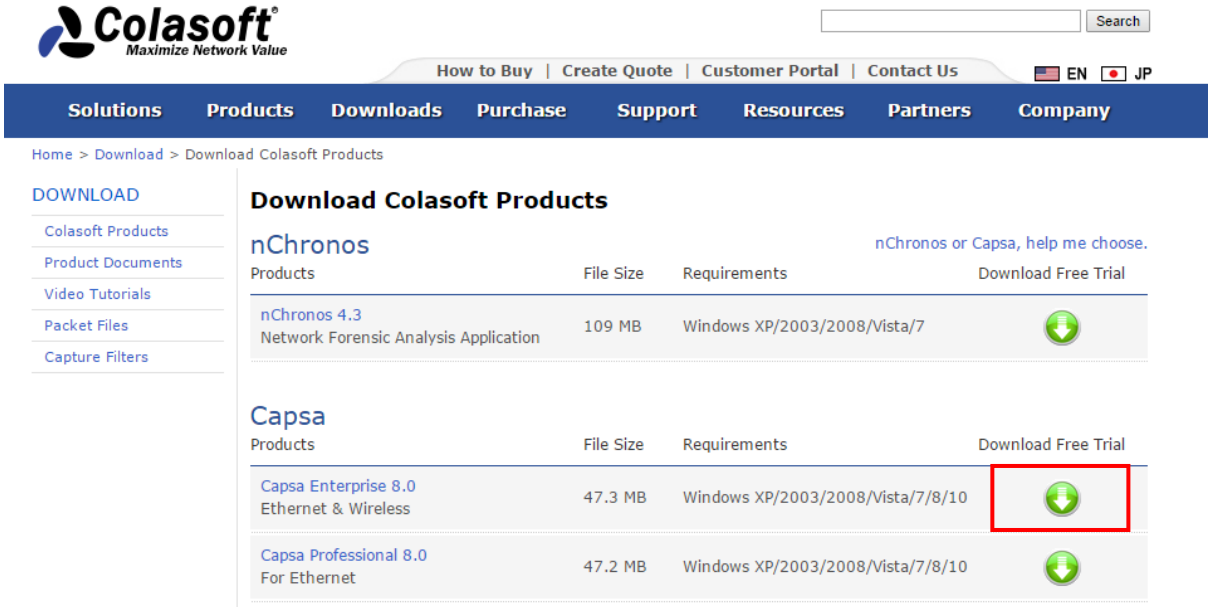
คุณสมบัติ

1. มีระบบตรวจสอบและป้องกันในการใช้งานของ TCP พอร์ทจากไฟล์ที่ไม่พึงประสงค์ (Malware) จากทาง DoS (DDoS), Worm และ ARP
2. สามารถแสดงค่าปริมาณและสถิติการรับส่งข้อมูลในระบบเครือข่ายได้ในรูปแบบกราฟและตัวเลข
3. มีฟังก์ชั่นในการดูข้อมูลเครือข่ายของการใช้งานโปรแกรมต่างๆ บนเว็บเบราว์เซอร์ได้ เช่น HTTP, E-Mail, DNS, FTP และโปรแกรมอื่นๆ อีกมากมาย
4. สามารถวิเคราห์ข้อมูลในด้านโปรโตคอลของระบบเครือข่ายได้มากกว่า 300 โปรโตคอล
5. มีการแสดงรายการชื่อพร้อมรายละเอียดของ Host ทั้งหมดในระบบเครือข่าย เช่น Traffic, IP, MAC หรือ อื่นๆ
6. มีระบบอัตโนมัติในการแนะนำการใช้และวิธีการแก้ไขปัญหาต่างๆ ช่วยให้ใช้งานและวิเคราะห์ข้อมูลได้ดีขึ้น
7. สามารถดูข้อมูลรายการย้อนหลังได้อย่างละเอียด

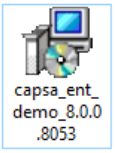
การติดตั้งและถอนการติดตั้งโปรแกรม

การติดตั้งโปรแกรม

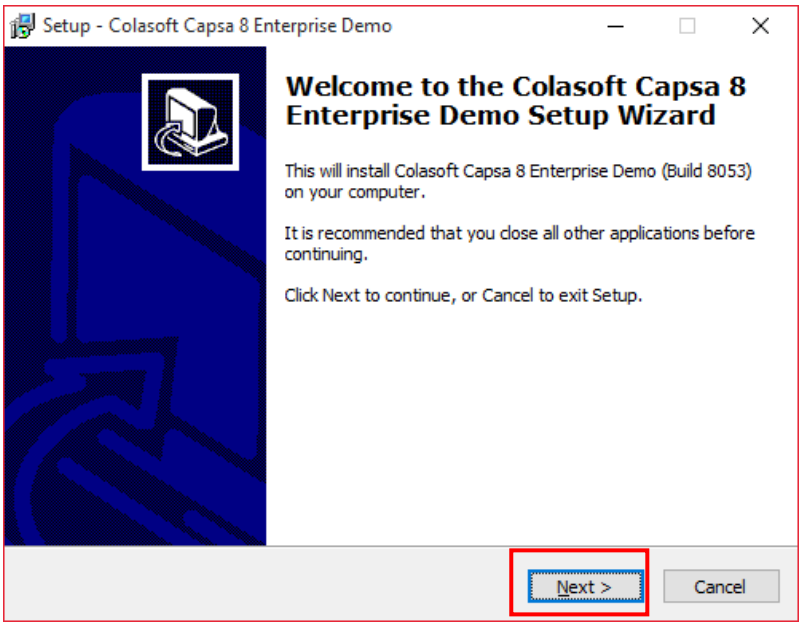
1. ดาวน์โหลดโปรแกรม Colasoft Capsa ที่เว็บไซต์ http://www.colasoft.com/download/ โดยตัวโปรแกรมจะเป็นตัวทดลองใช้งานฟรี 15 วันเท่านั้น



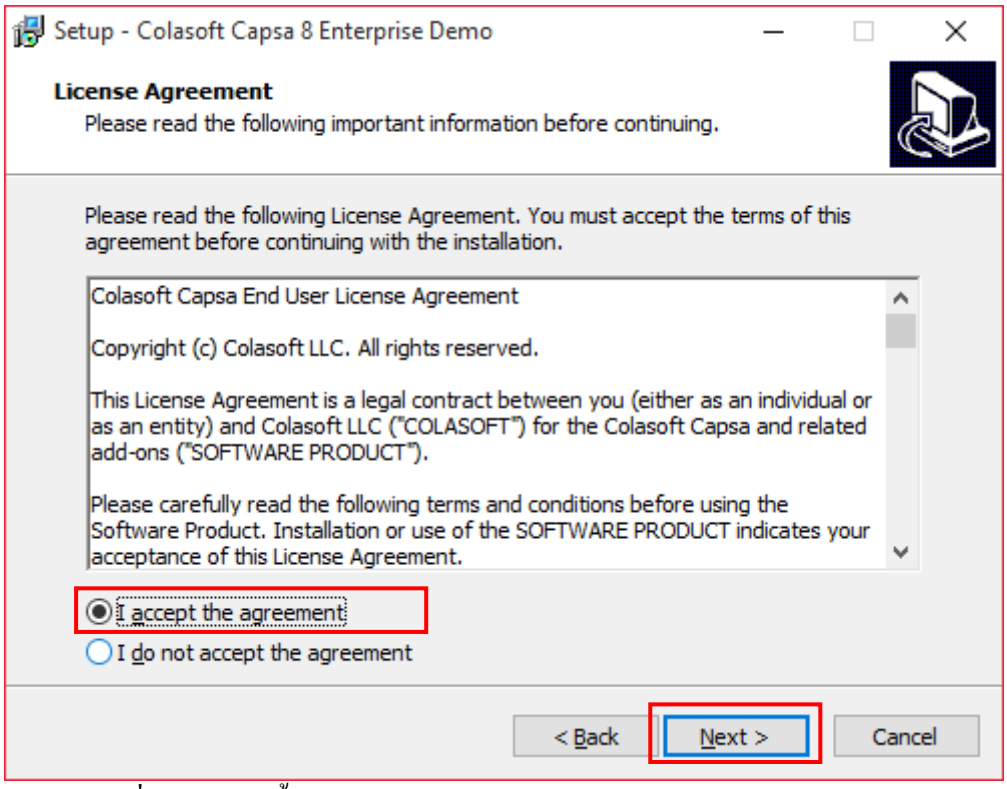
2. คลิกไฟล์ที่ชื่อว่า capsa_ent_demo_8.0.0.8053.exe เพื่อทำการติดตั้งโปรแกรม



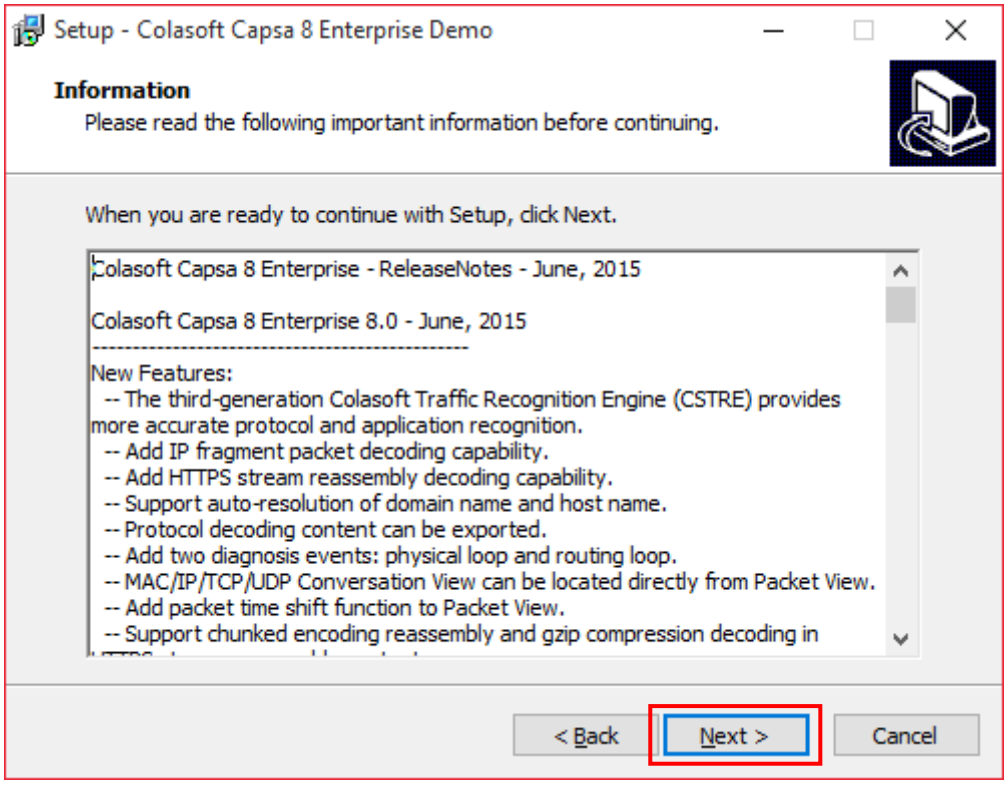
3. คลิก Next เพื่อทำการติดตั้ง



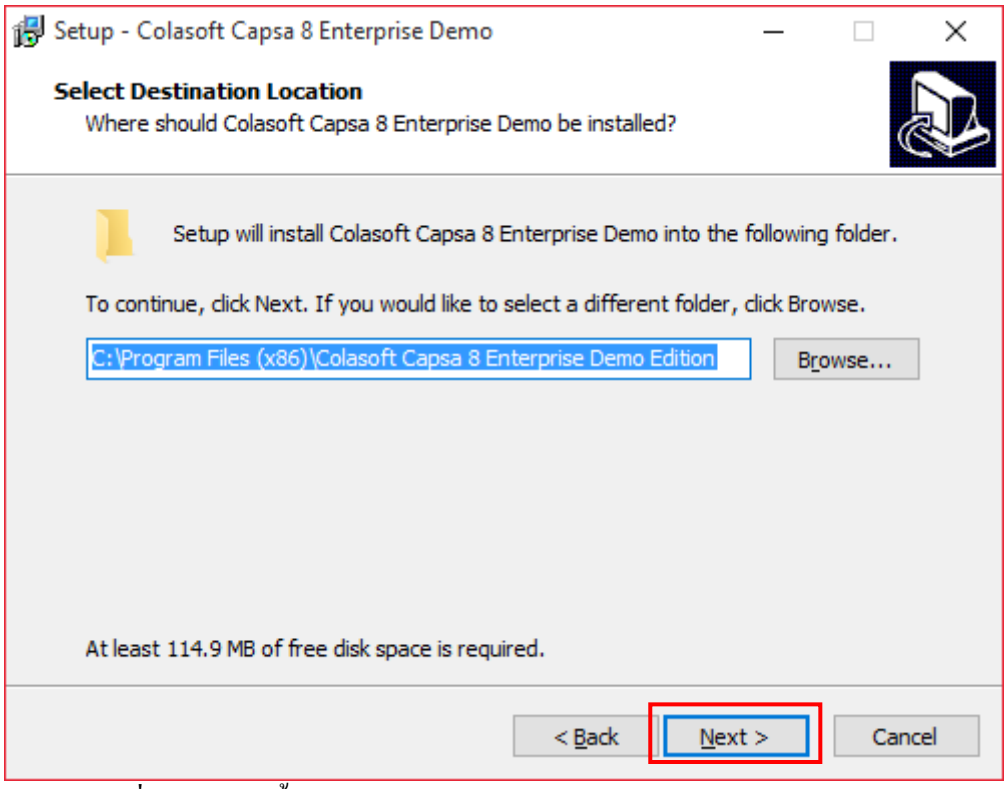
4. เลือก I accept the terms in the license agreement แล้วทำการคลิก Next เพื่อไปในขั้นตอนต่อไป



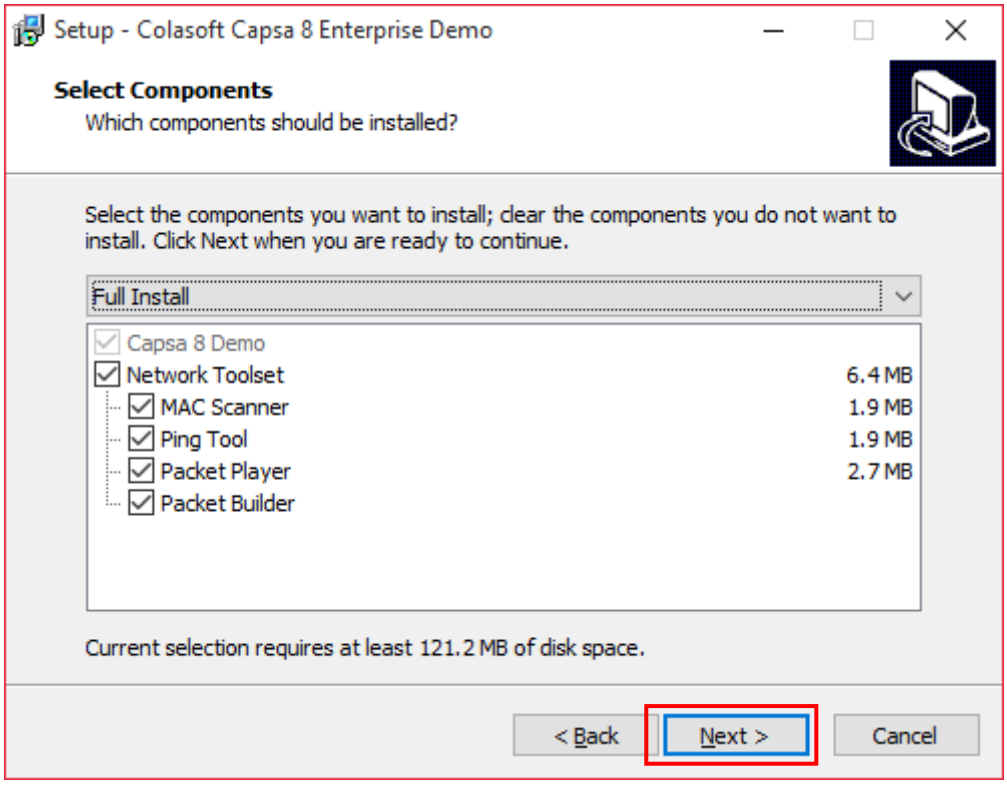
5. คลิก Next เพื่อทำการติดตั้ง



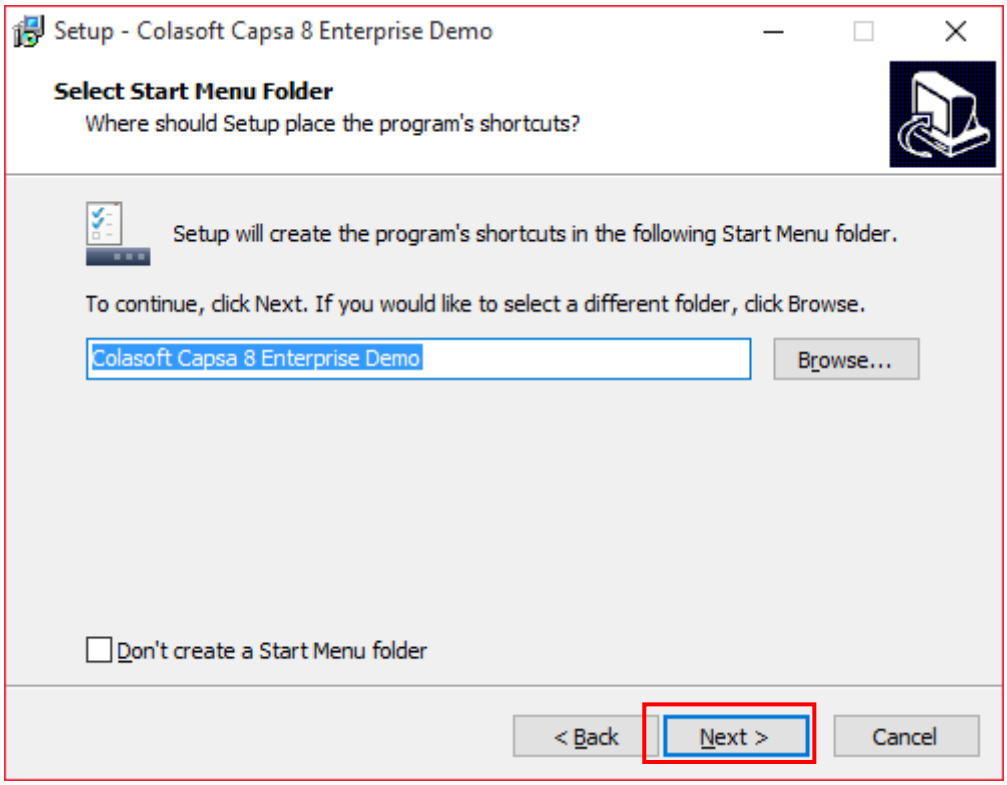
6. เลือกที่อยู่ของโปรแกรม (แนะนำให้ใช้ที่อยู่ที่โปแกรมกำหนดให้) และให้ทำการคลิก Next

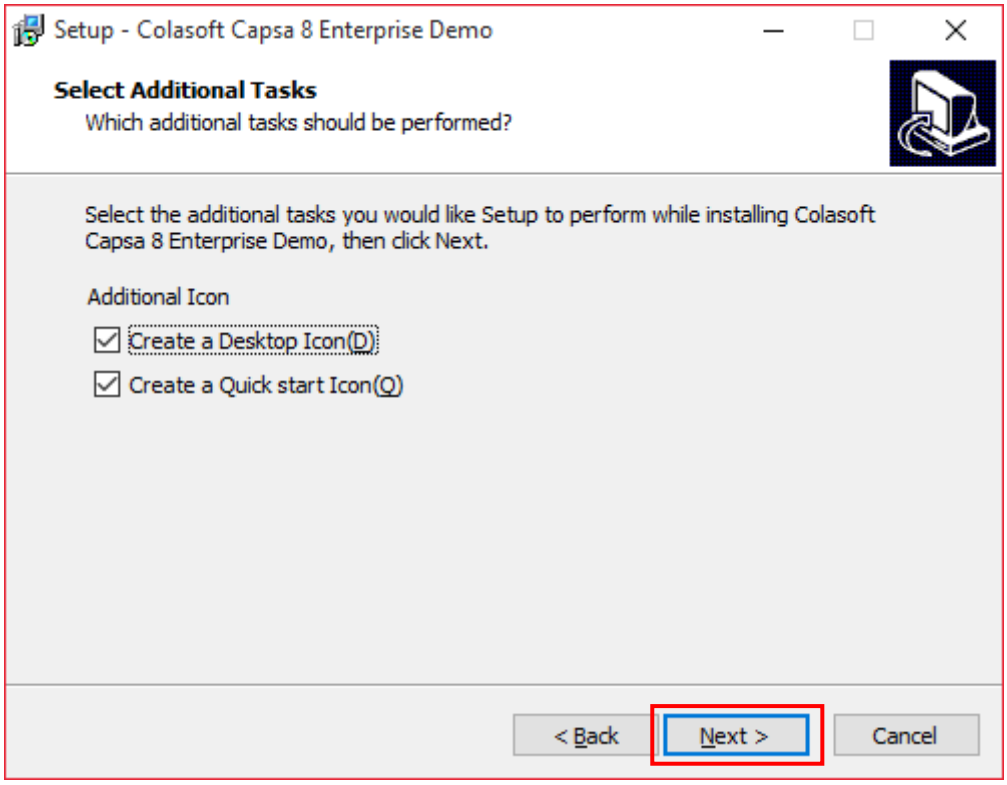


7. คลิก Next เพื่อทำการติดตั้ง

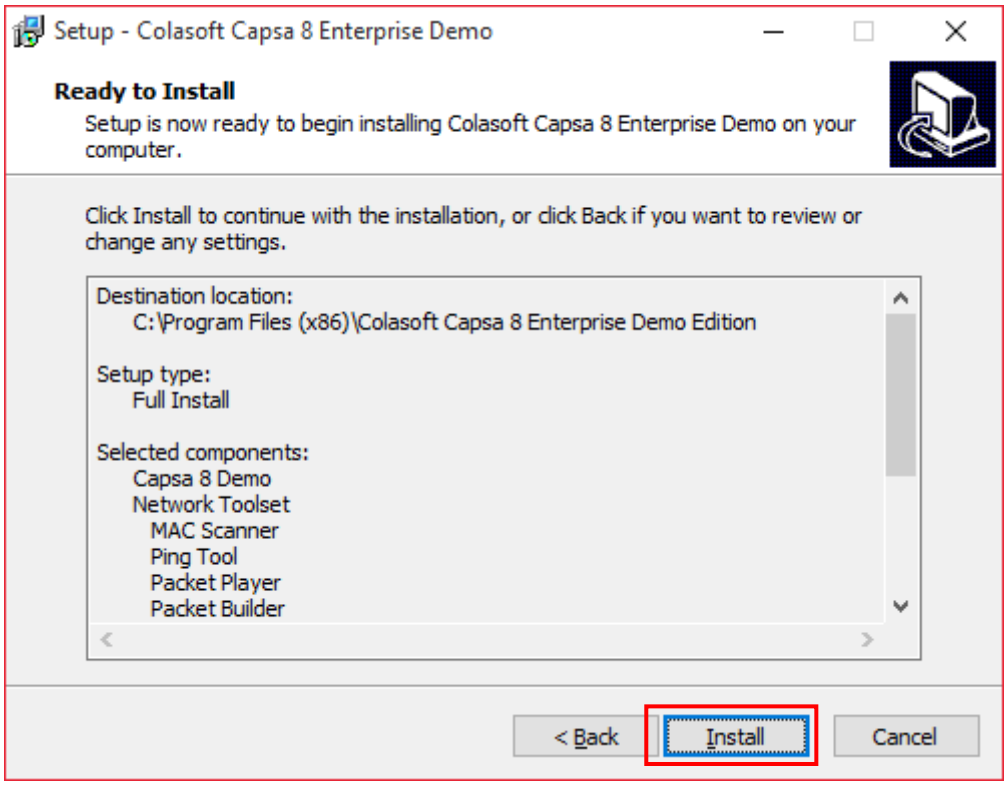


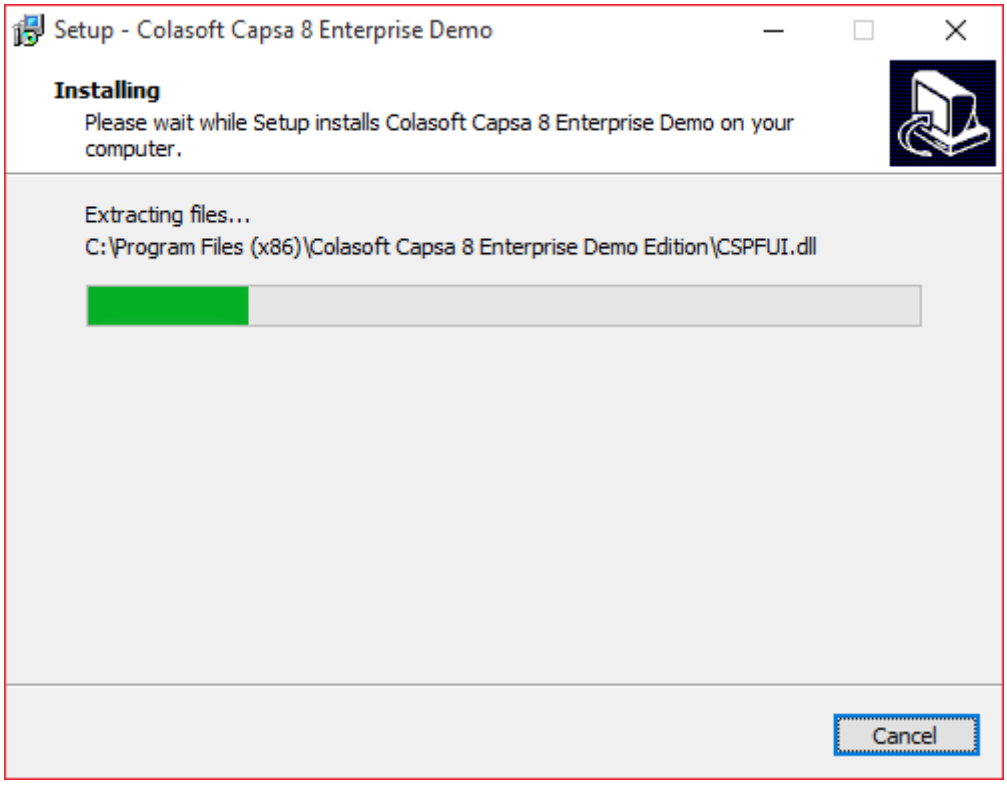
8. คลิก Next เพื่อทำการติดตั้ง



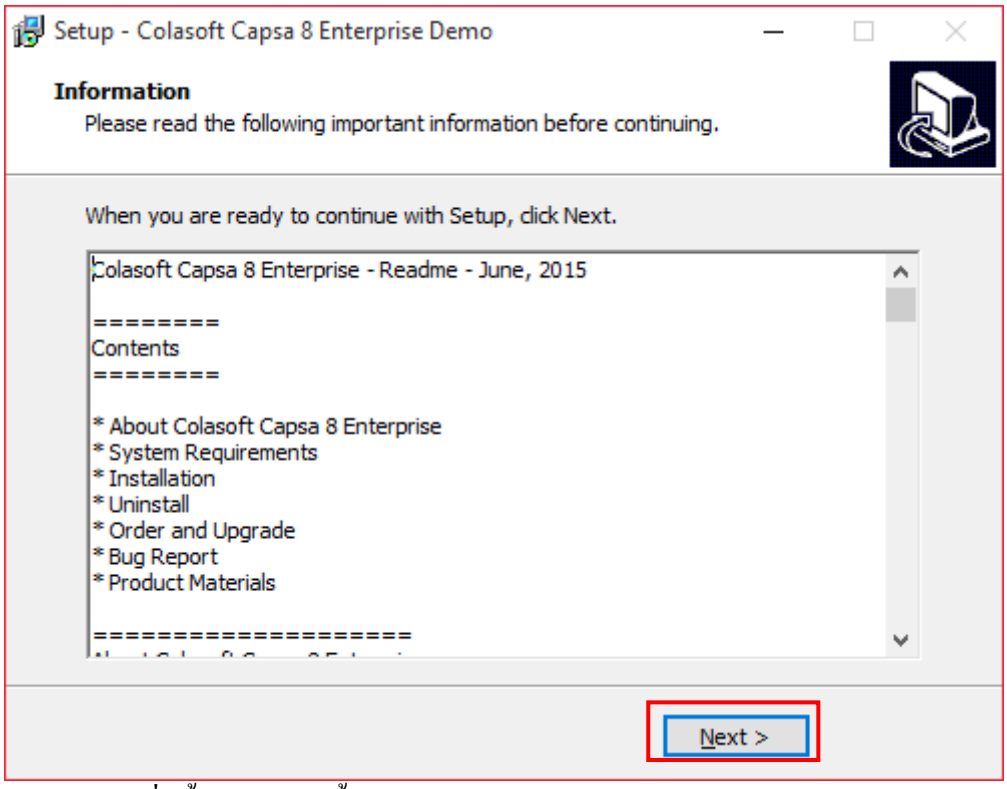


9. คลิก Install เพื่อทำการติดตั้งโปรแกรม

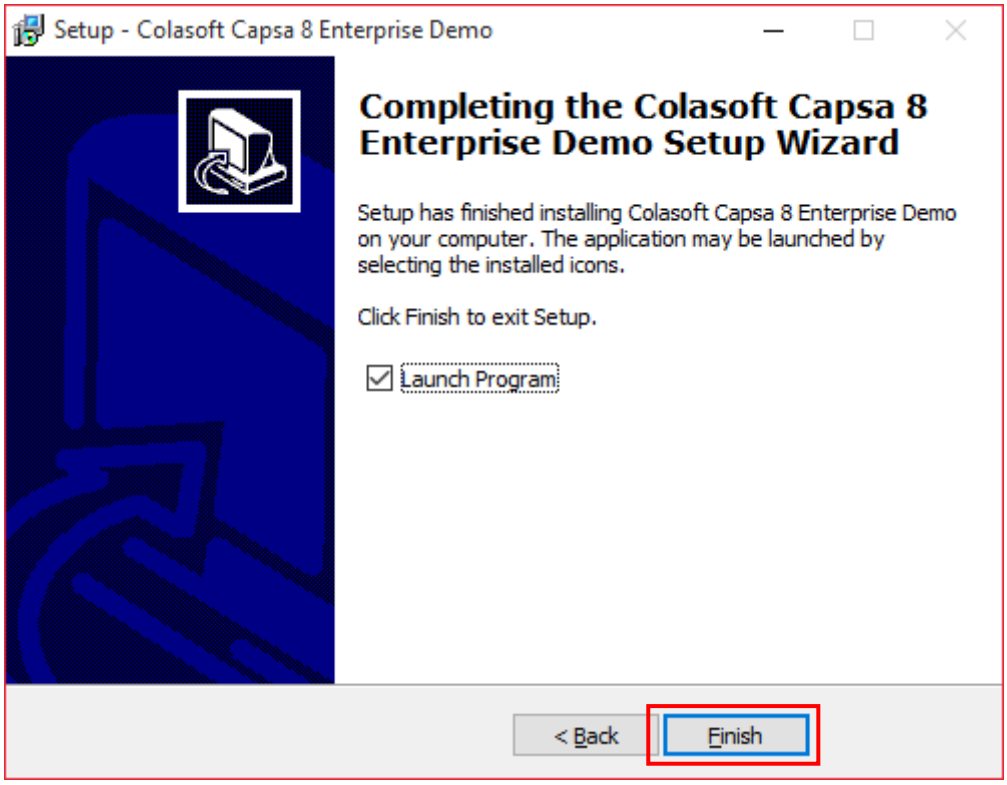




10. คลิก Next



11. คลิก Finish เพื่อสิ้นสุดการติดตั้งโปรแกรม



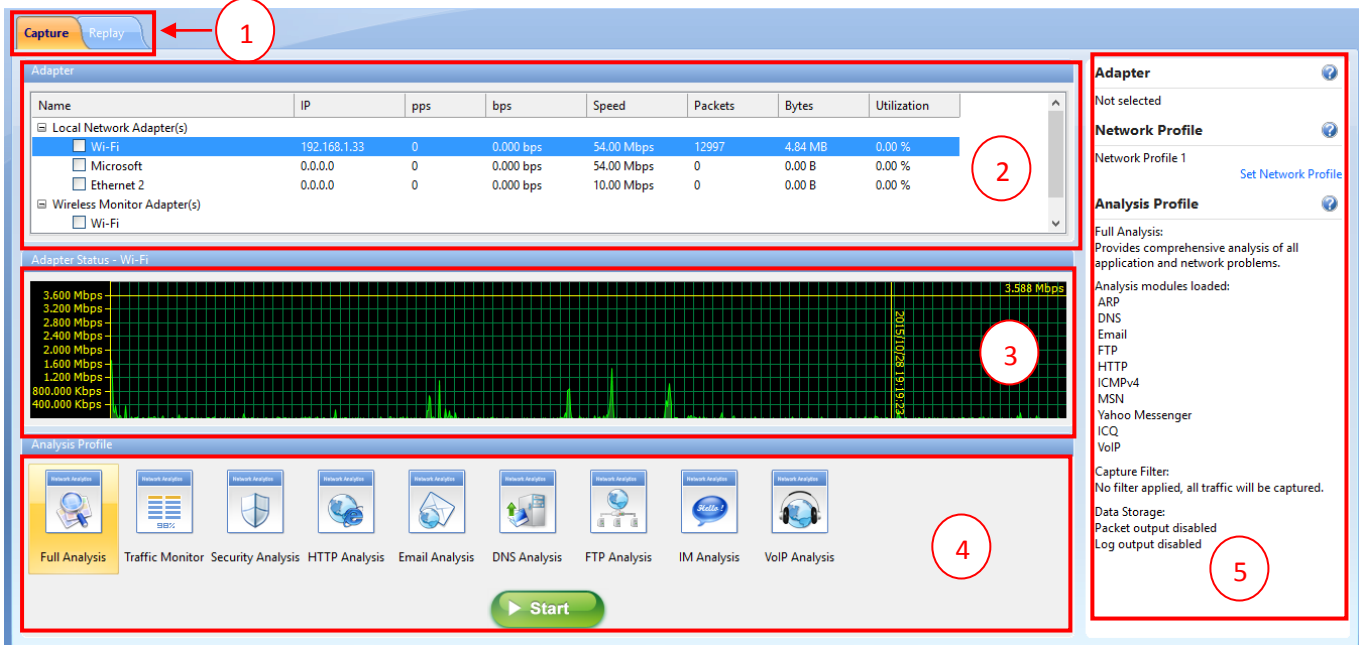
การถอนการติดตั้งโปรแกรม

การถอนการติดตั้งโปรแกรมมีอยู่ 2 วิธี ดังนี้

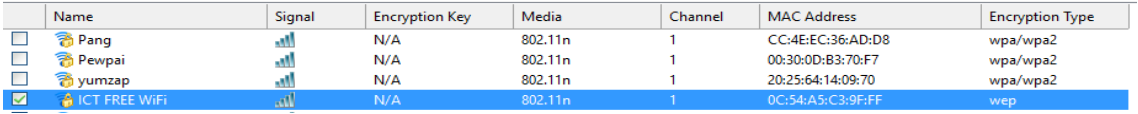
1. การถอนการติดตั้งโปรแกรม Colosoft Capsa ให้คลิกที่ปุ่ม Start > All Programs > ColasoftCapsa8 > Uninstall Colosoft Capsa 8
2. การถอนการติดตั้งโปรแกรม โดยเข้าที่ Control Panel > ดับเบิ้ลคลิก Programs and Features > เลือก Uninstall or change a program > ค้นหาโปรแกรม Capsa ที่อยู่ในรายการ > คลิกขวาที่โปรแกรมแล้วเลือก Uninstall

หน้าแรกของโปรแกรม

หน้าเริ่มต้นของโปรแกรม Capsa เวอร์ชั่น 8 ซึ่งจะมีรายละเอียดแต่ละส่วนการใช้งานดังนี้



1. Analysis Mode tabs จะมีอยู่ 2 แท็บ ได้แก่ Capture tab และ Replay tab
   1.1. Capture tab ใช้สำหรับตรวจสอบข้อมูลที่อยู่ในเครือข่าย
   1.2. Replay tab ใช้สำหรับการย้อนดูข้อมูลที่ได้ทำการตรวจสอบไป
2. Adapter List section เป็นรายการที่ใช้ในการเชื่อมต่อเครือข่าย ได้แก่ Local Network Adapter(s) กับ Wireless Monitor Adapter(s)
3. Adapter Status section จะมีการแสดงข้อมูลออกเป็น 2 แบบ ดังนี้
   3.1. เมื่อเลือกแบบ Local Network Adapter จะมีการแสดงสถานะ traffic แบบ real-time
   3.2. เมื่อเลือกแบบ Wireless Monitor Adapter จะมีการแสดงสถานะ AP และรายการทั้งหมดของ APs

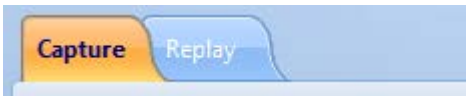


4. Analysis Profile section เป็นรายการที่ใช้ในการวิเคราะห์
5. Configuration Info section เป็นการแสดงข้อมูลที่ใช้ในการวิเคราะห์ มีอยู่ 3 ส่วนดังนี้
   5.1. Adapter เป็นการแสดงอะแดปเตอร์ที่เลือกไว้ในส่วนของ Adapter List section
   5.2. Network Profile เป็นการแสดงรายละเอียดของเครือข่าย
   5.3. Analysis Profile รายละเอียดที่ใช้ในการวิเคราะห์ซึ่งจะแสดงรายละเอียดแค่บางส่วนที่นำไปใช้ในการวิเคราะห์ รวมทั้งแสดง modules, packet และ data storage information

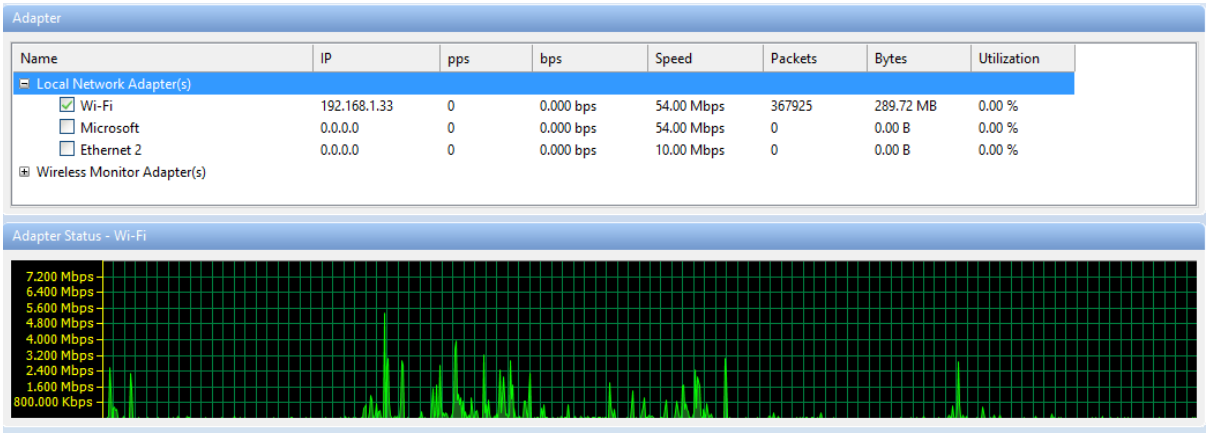
การใช้งานโปรแกรมแบบ Capture

การเริ่มต้นใช้งานโปรแกรมแบบ Local Network Adapter

1. เลือก Capture tab ที่อยู่ในส่วน Analysis Mode Tabs



2. เลือก Network Adapter ที่อยู่ในส่วน Adapter List Section ซึ่งจะแสดงสถานะ traffic แบบ real-time



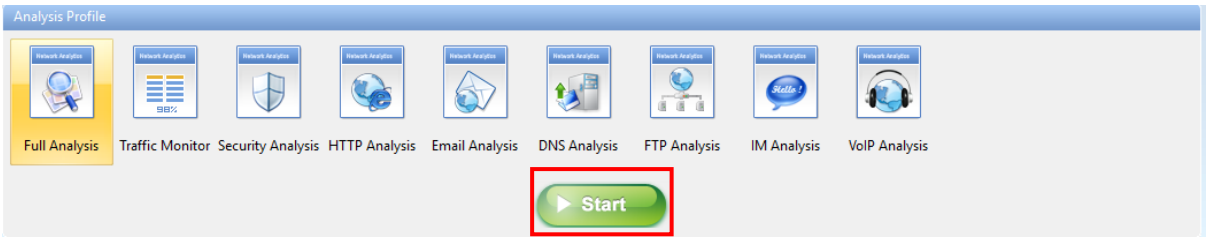
3. เลือกเครื่องมือที่จะใช้ในการวิเคราะห์ที่อยู่ในส่วน Analysis Profile ซึ่งจะมีดังนี้
   3.1 Full Analysis เป็นการวิเคราะห์แบบครอบคลุมการใช้งานทั้งหมด
   3.2 Traffic Monitor มีแสดง traffic เชิงสถิติและวิเคราะห์ประสิทธิภาพของอ็อบเจกต์หลัก รวมไปถึง MAC Address, IP Address และ Protocol
   3.3 Security Analysis เป็นการวิเคราะห์ความเสี่ยงโดยเฉพาะศักยภาพในความปลอดภัยของเครือข่าย
   3.4 HTTP Analysis วิเคราะห์การใช้งานบนเว็บแอพพลิเคชั่น (รูปแบบของ HTTP)
   3.5 Email Analysis วิเคราะห์การใช้งานอีเมล์ (รูปแบบของ POP3 และ SMTP) และตรวจสอบเนื้อหาและสิ่งที่แนบมากับอีเมล์
   3.6 DNS Analysis วิเคราะห์การใช้งาน DNS เช่น การวินิจฉัยข้อผิดพลาดการใช้งานของ DNS

3.7 FTP Analysis การวิเคราะห์การใช้งาน FTP (รูปแบบ TCP พอร์ต 21 และ 20)

3.8 IM Analysis การวิเคราะห์ข้อความ

3.9 VoIP Analysis การวิเคราะห์การสื่อสารทางเสียงผ่านอินเทอร์เน็ต

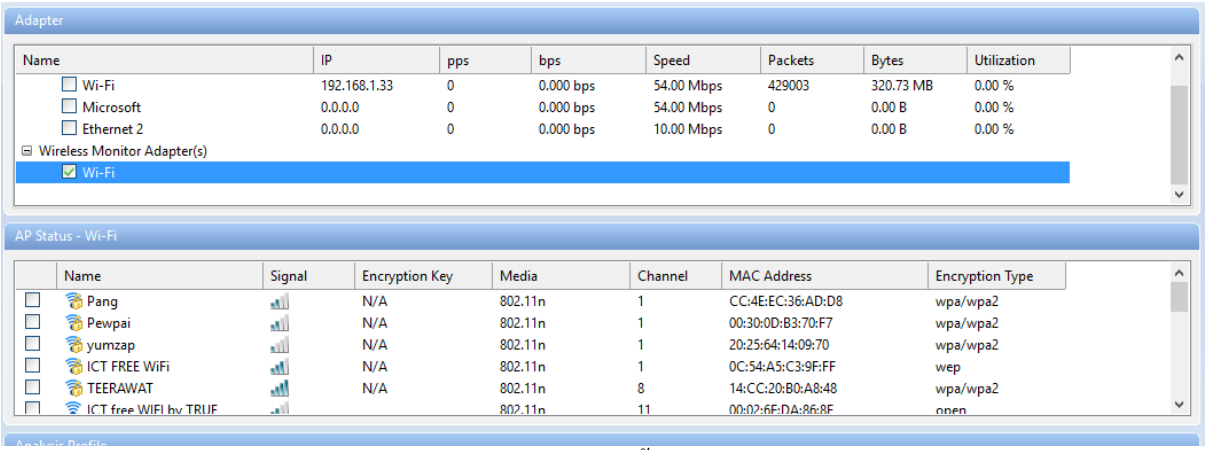
4. คลิกปุ่ม Start เพื่อเริ่มในการวิเคราะห์



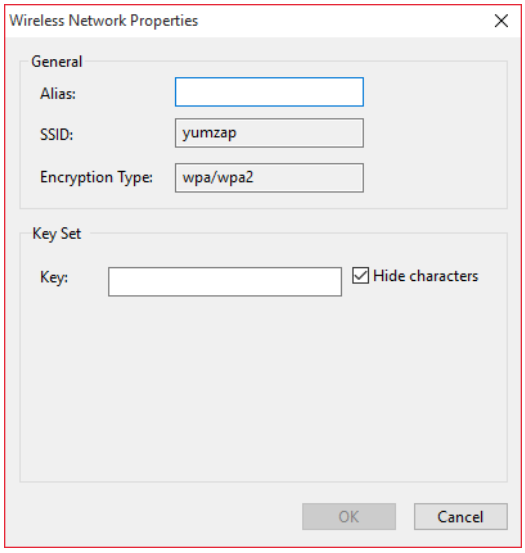
การเริ่มต้นใช้งานโปรแกรมแบบ Wireless Network Adapters

1. เลือก Capture tab ที่อยู่ในส่วน Analysis Mode Tabs

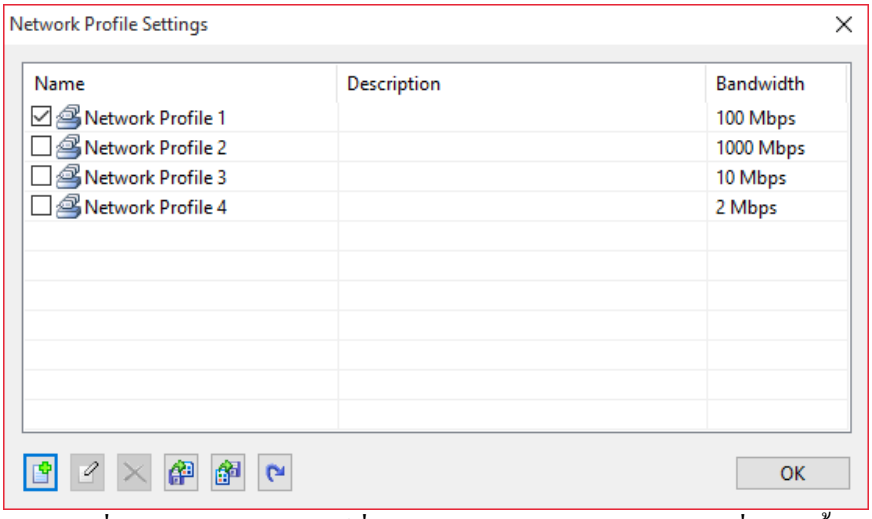
2. เลือก wireless network adapter ที่อยู่ในส่วน Adapter List ซึ่งจะแสดง Aps ที่มีอยู่ทั้งหมด



3. เลือก AP ที่ต้องการ โดยระบบจะมีการถามรหัส นอกจากนี้สามารถเลือก AP ได้มากกว่าหนึ่ง



4. คลิก Set Network Profile ที่อยู่ในส่วน Configuration Info section แล้วเลือก Network Profile โดยมี Bandwidth ที่แตกต่างกัน



5. เลือกรายละเอียดที่จะใช้ในการวิเคราะห์ที่อยู่ในส่วนของ Analysis Profile ซึ่งมีดังนี้

5.1. Full Analysis เป็นการวิเคราะห์แบบครอบคลุมการใช้งานทั้งหมด

5.2. Traffic Monitor มีแสดง traffic เชิงสถิติและวิเคราะห์ประสิทธิภาพของอ็อบเจกต์หลัก รวมไปถึง MAC Address, IP Address และ Protocol

5.3. Security Analysis เป็นการวิเคราะห์ความเสี่ยงโดยเฉพาะศักยภาพในความปลอดภัยของเครือข่าย

5.4. HTTP Analysis วิเคราะห์การใช้งานบนเว็บแอพพลิเคชั่น (รูปแบบของ HTTP)

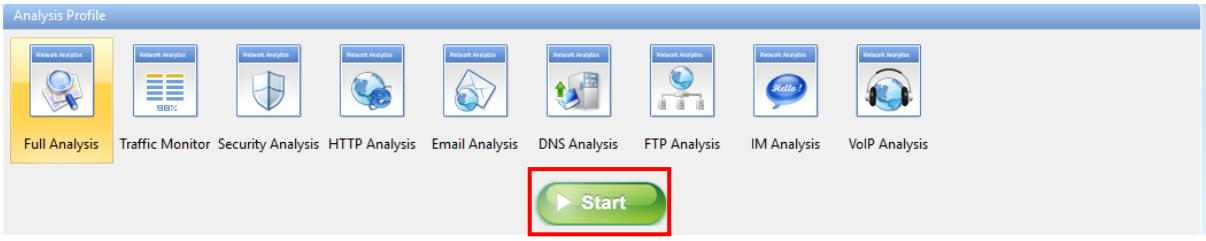
5.5. Email Analysis วิเคราะห์การใช้งานอีเมล์ (รูปแบบของ POP3 และ SMTP) และตรวจสอบเนื้อหาและสิ่งที่แนบมากับอีเมล์

5.6. DNS Analysis วิเคราะห์การใช้งาน DNS เช่น การวินิจฉัยข้อผิดพลาดการใช้งานของ DNS

5.7. FTP Analysis การวิเคราะห์การใช้งาน FTP (รูปแบบ TCP พอร์ต 21 และ 20)

5.8. IM Analysis การวิเคราะห์ข้อความ

6. คลิกปุ่ม Start เพื่อเริ่มในการวิเคราะห์

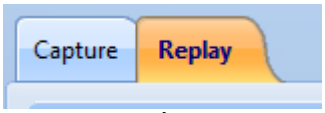


การใช้งานโปรแกรมแบบ Replay

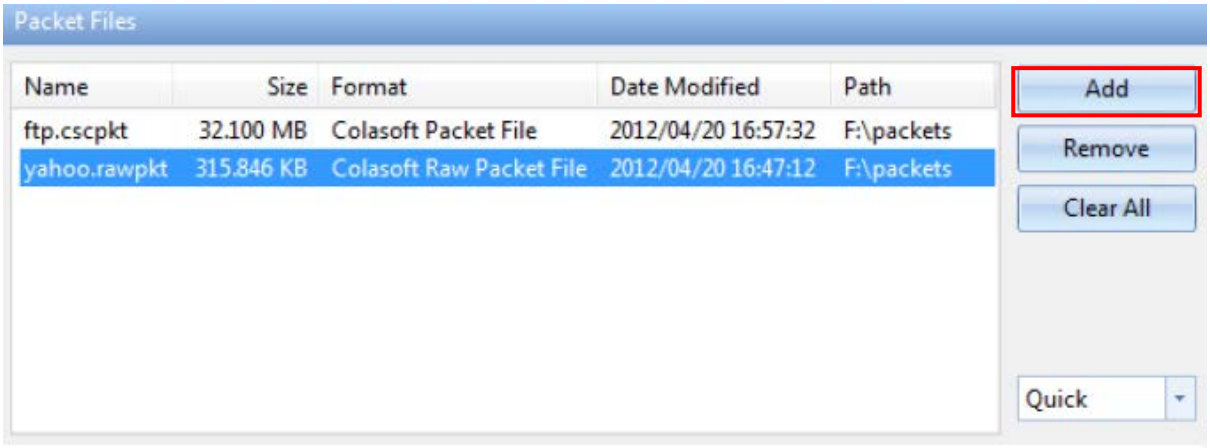
Capsa ไม่ได้ใช้ในการวิเคราะห์แบบ real-time เพียงอย่างเดียว แต่ยังสามารถนำแพ็คเก็ตที่ต้องการมาวิเคราะห์ได้

ขั้นตอนการใช้งานดังนี้

1. เลือกแท็บ Replay ที่อยู่ในส่วน Analysis Mode



2. เพิ่มไฟล์ packet จากในส่วนของ Packet Files ซึ่งมีรายละเอียดดังนี้



2.1. Add เป็นการเพิ่มไฟล์ที่มีการเก็บแพ็คเก็ตย้อนหลัง โดยจพมีเวลาประทับไว้ในไฟล์แพ็คเก็ตนั้น

2.2. Remove เป็นการลบไฟล์แพ็คเก็ตที่เลือกไว้

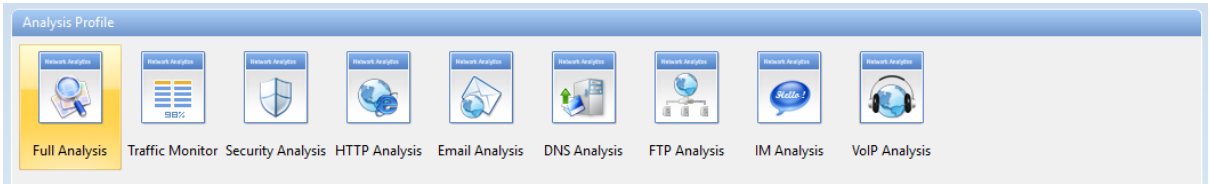
2.3. Clear All ลบไฟล์แพ็คเก็ตในลิสต์ทั้งหมด

2.4. Replay Speed เป็นการกำหนดความเร็ว

2.4.1. Quick จะทำการเล่นแพ็คเก็ตย้อนหลังอย่างรวดเร็ว

2.4.2. Normal แพ็คเก็ตจะย้อนหลังอย่างช้า แต่ได้รายละเอียดที่ถูกต้อง

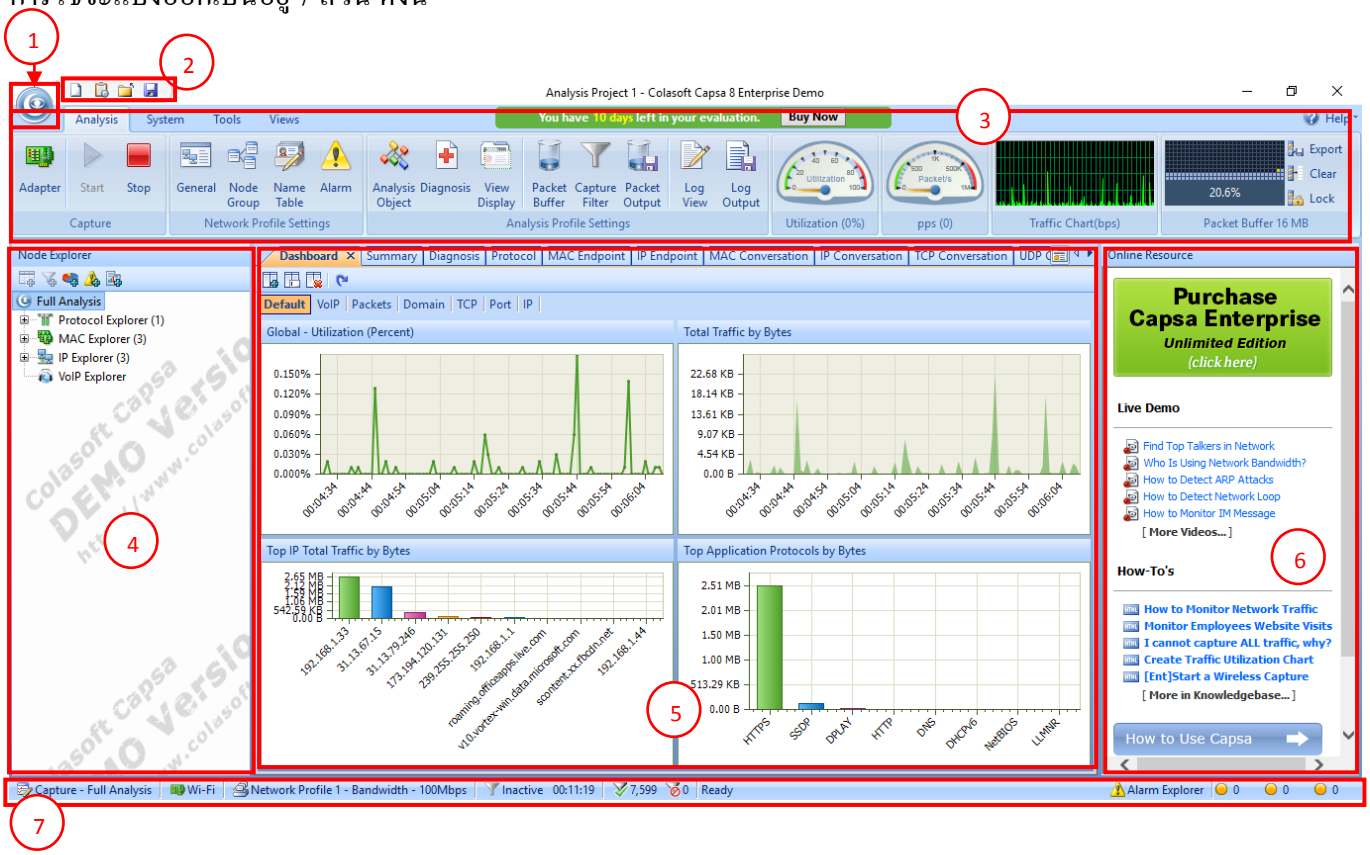
3. เลือกเครื่องมือที่ต้องการที่จะใช้ในการวิเคราะห์ให้เหมาะสมที่อยู่ในส่วนของ Analysis Profile



4. คลิกปุ่ม Start เพื่อทำการเริ่มวิเคราะห์

Main User Interface

หลังจากที่เริ่มต้นในการวิเคราะห์โปรเจค ไม่ว่าจะเลือกแบบ real-time capturing หรือ replaying packets ก็จะเข้าสู่หน้าการใช้งานที่เหมือนกัน ซึ่งจะแสดงให้เห็นสถิติและเครือข่ายเน็ตเวิร์ค ในส่วนหน้าต่างการใช้จะแบ่งออกเป็นอยู่ 7 ส่วน ดังนี้



1. Menu button เป็นปุ่มเมนูที่อยู่มุมบนซ้ายของหน้าต่างการใช้งาน โดยมีลิสต์รายการดังนี้
   1.1. New เป็นการสร้างโปรเจคการวิเคราะห์ใหม่
   1.2. Task Scheduler เป็นแท็บในการกำหนดเวลาการทำงาน
   1.3. Configurations Backup เป็นการนำเข้าและการส่งออกของข้อมูล โดยจะบันทึกเป็นนามสกุลไฟล์ที่ชื่อว่า .csgcf (Colasoft Global Configuration File)
   1.4. Print เป็นคำสั่งในการสั่งพิมพ์หน้าปัจจุบันหรือกำหนดค่าในการพิมพ์
   1.5. Resource เป็นการวิเคราะห์เครือข่ายโดยการนำข้อมูลมาจากอินเทอร์เน็ต โดยมี 2 ทางดังนี้
      1.5.1. Colasoft Home Page เปิดจากหน้าเพจของ Colasoft
      1.5.2. Forum เปิดจากบอร์ด โดยสามารถขอความช่วยเหลือและเรียนรู้ทักษะการใช้เครื่องมือในการวิเคราะห์ได้
   1.6. Product เป็นข้อมูลที่ของผลิตภัณฑ์
      1.6.1. Product License เป็นการต่ออายุใบอนุญาต
      1.6.2. Check Update ตรวจสอบเวอร์ชั่นของโปรแกรม

1.6.3. About เป็นการอธิบายลิขสิทธิ์และข้อมูลของใบอนุญาตของผลิตภัณฑ์

1.7. Close เป็นคำสั่งในการปิดโปรเจคและกลับไปยังหน้าเริ่มต้น

1.8. Recent Files แสดงรายการที่เคยทำการเปิดไฟล์แพ็คเก็ต

1.9. Options เป็นการกำหนดการตั้งค่าของโปรเจคที่ใช้ในการวิเคราะห์

1.10. Exit ออกจากโปรแกรม

2. Quick Access Icons มีไอคอนดังนี้

2.1. ไอคอนสำหรับการสร้างโปรเจคการวิเคราะห์ใหม่

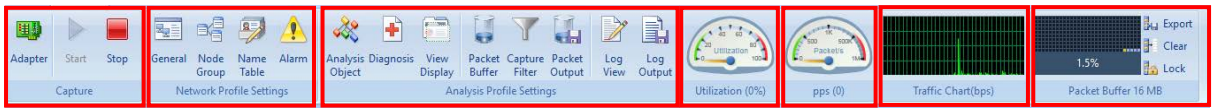
2.2. ไอคอนในการกำหนดเวลาการทำงาน

2.3. ไอคอนเพื่อกลับไปยังหน้าเริ่มต้น

2.4. ไอคอนสำหรับการบันทึกแพ็คเก็ต ซึ่งนามสกุลดังนี้ Colasoft Packet File (*.cscpkt), Colasoft Raw Packet File (*.rawpkt), Colasoft Raw Packet File (v2) (*.rawpkt), Accellent 5Views Packet File (*.5vw), EtherPeek Packet File (V9) (*.pkt), HP Unix Nettl Packet File (*.TRC0; TRC1), libpcap (Wireshark, Ethereal, Tcpdump, etc.) (*.cap; pcap), Microsoft Network Monitor 1.x, 2.x (*.cap), Novell LANalyzer (*.tr1), NetXRay2.0, and Windows Sniffer (*.cap), Sun_Snoop (*.Snoop) และ Visual Network Traffic Capture (*.cap).

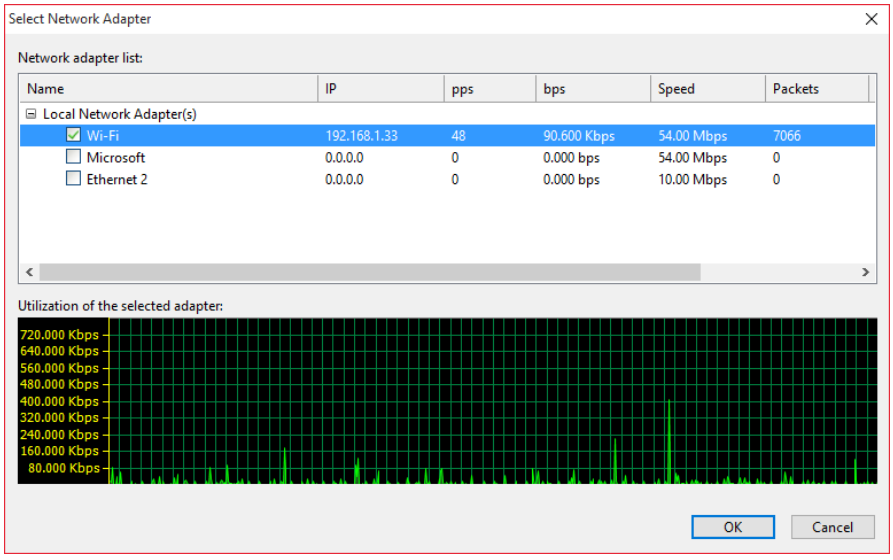
3. Ribbon ซึ่งแบ่งออกเป็น 4 ส่วนดังนี้

3.1. Analysis เป็นการตั้งค่าสำหรับการวิเคราะห์ ประกอบไปด้วย



3.1.1. ในกรณีส่วนของฟังก์ชั่น Capture

- Adapter สามารถเลือกหรือเปลี่ยนแปลง Network Adapter เพื่อใช้ในการวิเคราะห์



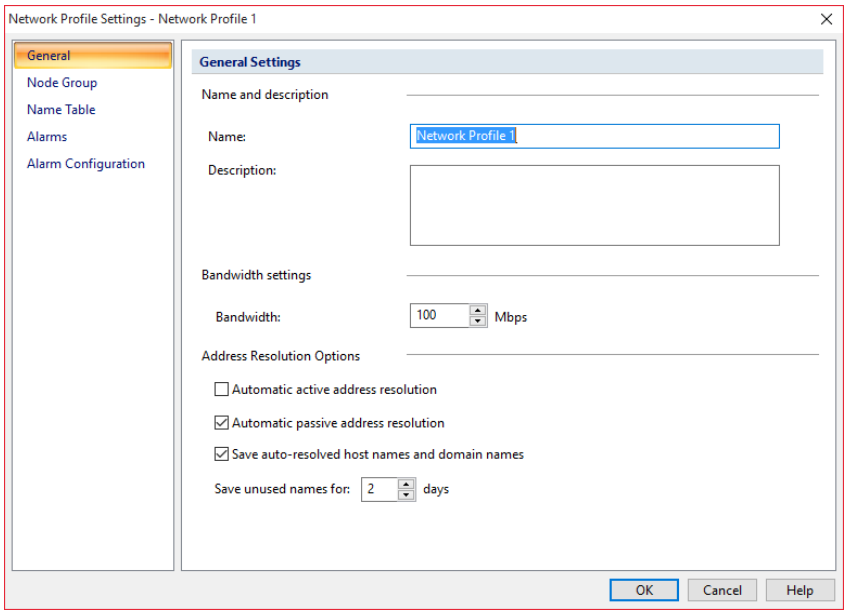
- Start เริ่มการวินิจฉัยแพ็คเก็ต
- Stop สิ้นการวินัจฉัยแพ็คเก็ต

3.1.2. ในกรณีส่วนของฟังก์ชัน Replay

- File เป็นการเปิดการจัดการหรือเปลี่ยนแปลงไฟล์แพ็คเก็ตใหม่
- Start เริ่มการวินิจฉัยแพ็คเก็ต
- Pause หยุดการวินัจฉัยแพ็คเก็ตชั่วคราว
- Stop สิ้นการวินัจฉัยแพ็คเก็ต

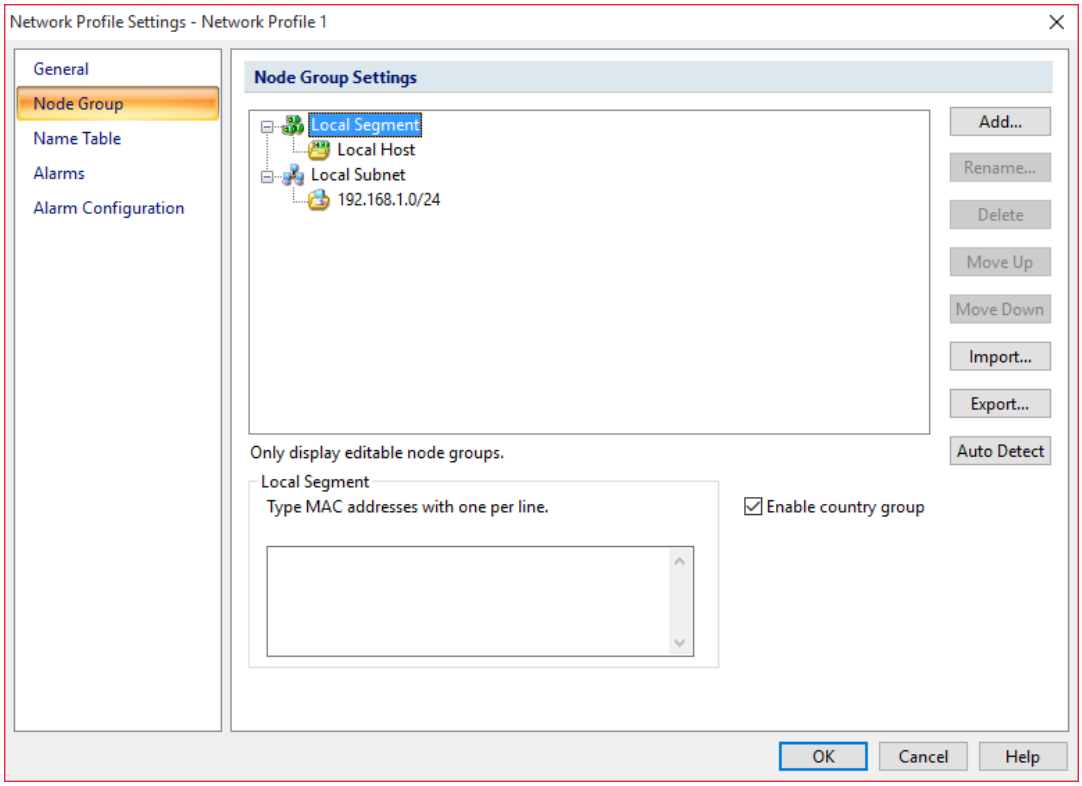
3.1.3. Network Profile Settings เป็นการตั้งค่าพารามิเตอร์สำหรับ Network Profile โดยมีอยู่ 4 ส่วนดังนี้

3.1.3.1. General ซึ่งมีรายละเอียดดังนี้



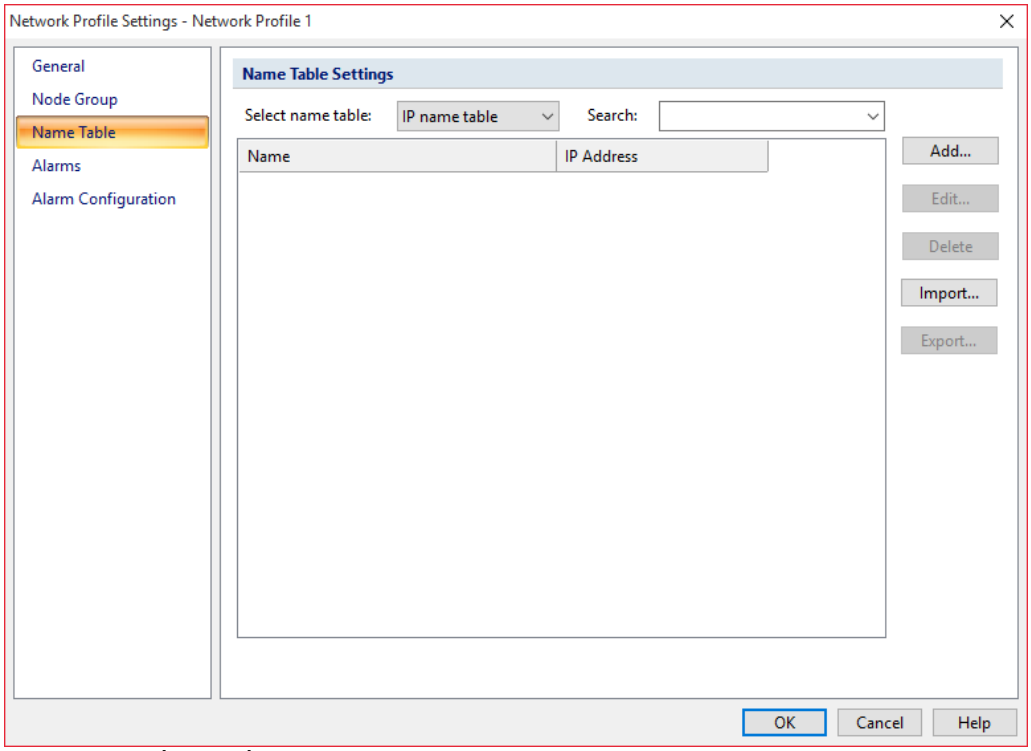
- Name ชื่อของ Network Profile
- Description คำอธิบายเกี่ยวกับรายละเอียดของ Network
- Bandwidth กำหนด bandwidth ที่จะใช้ในเครือข่าย
- Automatic active address resolution เป็นการใช้งาน DNS แบบอัตโนมัติ
- Save auto-resolved host names and domain names
- Save unused names ระบุวันที่ใช้ โดยมีค่าเริ่มต้นที่ 2 วัน

3.1.3.2. Node Group เป็นกลุ่มที่ถูกนำมาใช้ในการจัดการ MAC และ IP Address ของเครือข่าย

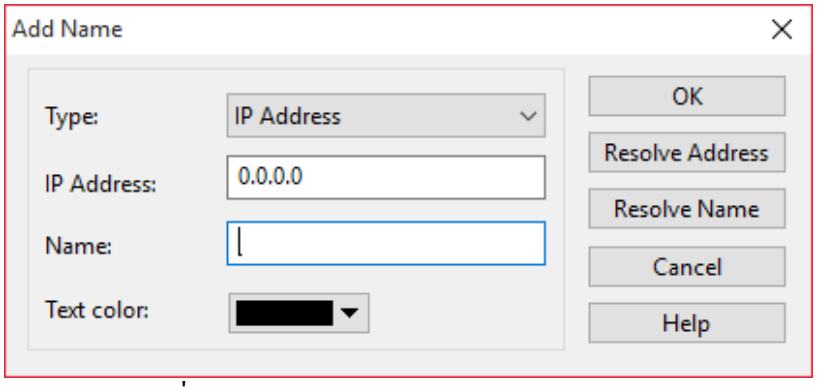


- Add เป็นการเพิ่มโหนดใหม่ในกลุ่มโหนดที่ได้เลือกไว้
- Rename แก้ไขชื่อของกลุ่มโหนดที่เลือกไว้
- Delete ลบกลุ่มโหนดที่เลือกไว้
- Move Up การย้ายกลุ่มโหนดขึ้นมา
- Move Down การย้ายกลุ่มโหนดลงมา
- Import การนำไฟล์ .cscng เข้าในรายการ
- Export การบันทึกไฟล์เป็น .cscng
- Auto Detect ตรวจสอบกลุ่มของ MAC Address และ IP Address ของเครือข่ายปัจจุบัน

3.1.3.3. Name Table เป็นการจัดการ MAC และ IP Address ที่สามารถใช้ในการวิเคราะห์

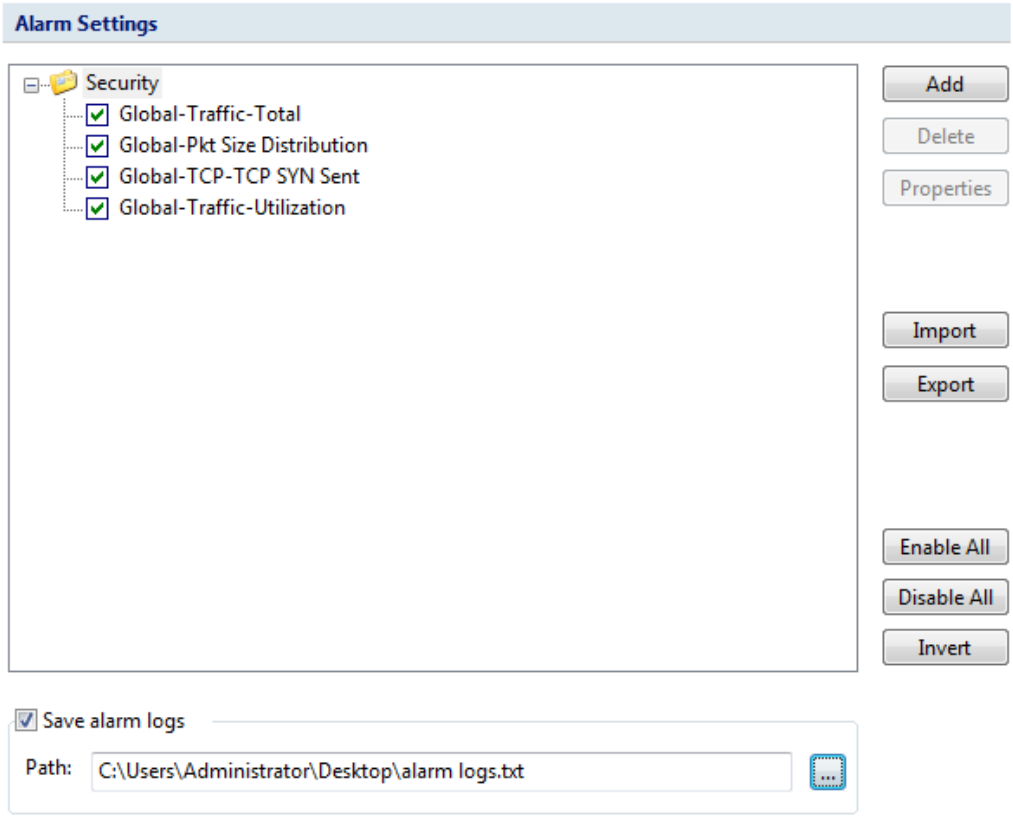


- Add เพิ่มชื่อและที่อยู่



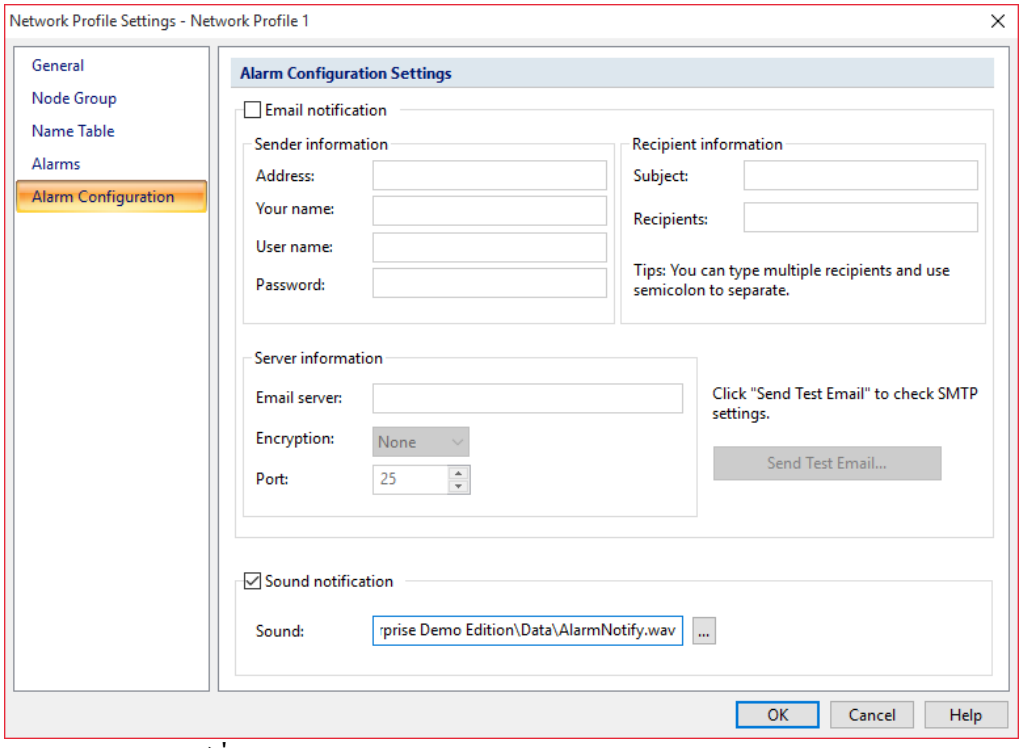
- Edit แก้ไขรายการที่เลือกไว้
- Delete ลบรายการที่เลือกไว้
- Import นำไฟล์จากข้างนอกเข้ามาใช้ โดยจะต้องเป็นไฟล์นามสกุล .cscont
- Export การบันทึกไฟล์ ซึ่งจะเป็นนามสกุลไฟล์ .cscont

3.1.3.4. Alarm Settings เป็นการตั้งค่าในการเตือนภัยภายในเครือข่าย



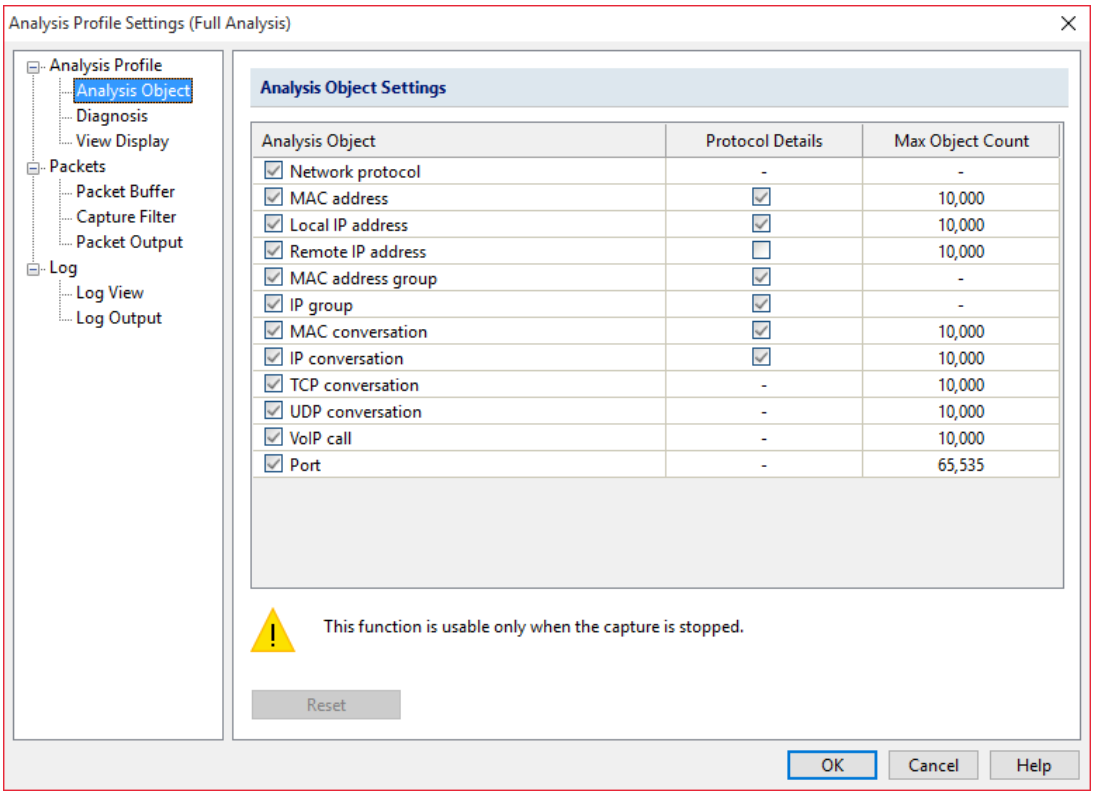
- Add สร้างการแจ้งเตือนภัย
- Delete ลบการแจ้งเตือนภัยที่เลือกไว้ในรายการ
- Properties ปรับเปลี่ยนคุณสมบัติของการเตือนภัยที่เลือก
- Import โหลดการแจ้งเตือนภัย โดยจะต้องเป็นนามสกุลไฟล์ .csalarm
- Export บันทึกการแจ้งเตือนภัย โดยจะต้องเป็นนามสกุลไฟล์ .csalarm
- Enable All เลือกการเตือนภัยทั้งหมด
- Disable All ยกเลิกการเตือนภัยทั้งหมด
- Invert การสลับรายการแจ้งเตือนภัย
- Save alarm logs เป็นการบันทึกไฟล์การเตือนภัยเป็นนามสกุลไฟล์ .txt โดยจะมีการระบุเส้นทางที่จะจัดเก็บไฟล์

3.1.3.5. Alarm Configuration เป็นการตั้งค่าการแจ้งเตือนผ่านอีเมล์และการตั้งค่าเสียงการแจ้งเตือน



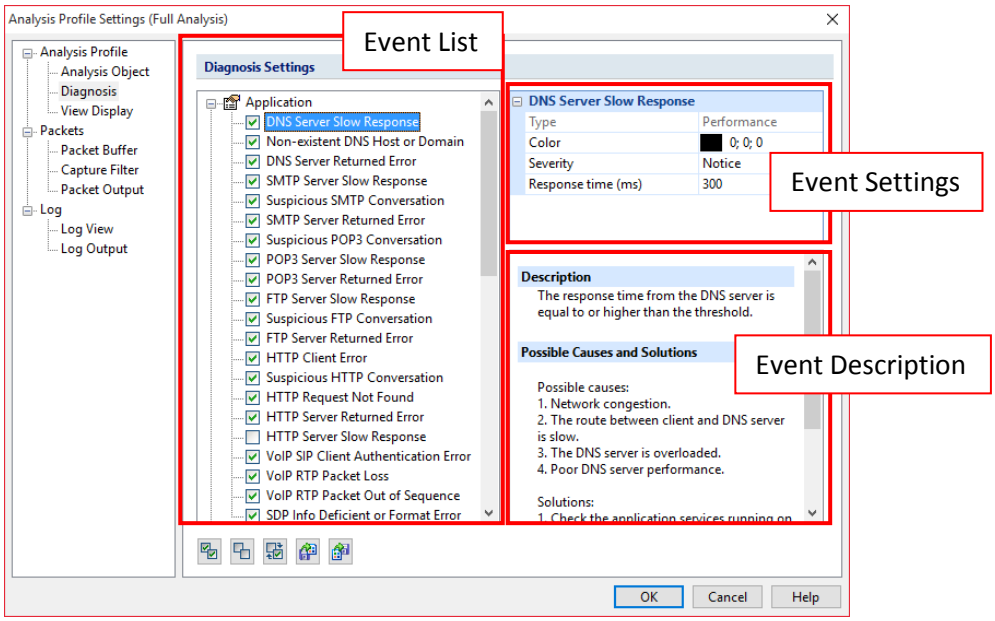
- Address อีเมล์ที่จะทำการส่ง
- Your name ชื่อผู้ส่ง
- User name อีเมล์ที่ใช้งานโดยจะมีการเชื่อมต่อเมล์เซิฟเวอร์
- Password รหัสผ่านอีเมล์ที่ใช้งาน
- Subject ชื่อเรื่องที่ต้องการแจ้งเตือน
- Recipients ผู้รับอีเมล์สำหรับการแจ้งเตือน โดยสามารถแจ้งเตือนภัยได้หลายอีเมล์ โดยใช้สัญลักษณ์ “,” คั่น
- Email server ที่อยู่ของเมล์เซิฟเวอร์
- Encryption ประเภทการเชื่อมต่อของเมล์เซิฟเวอร์
- Port หมายเลขพอร์ตที่ใช้ในการเชื่อมต่อกับเมล์เซิฟเวอร์
- Sound notification เป็นการตั้งค่าเสียงที่ใช้ในการเตือนภัย

3.1.4. Analysis Profile เป็นการตั้งค่าการวิเคราะห์ซึ่งสามารถปรับเปลี่ยนการวิเคราะห์ได้



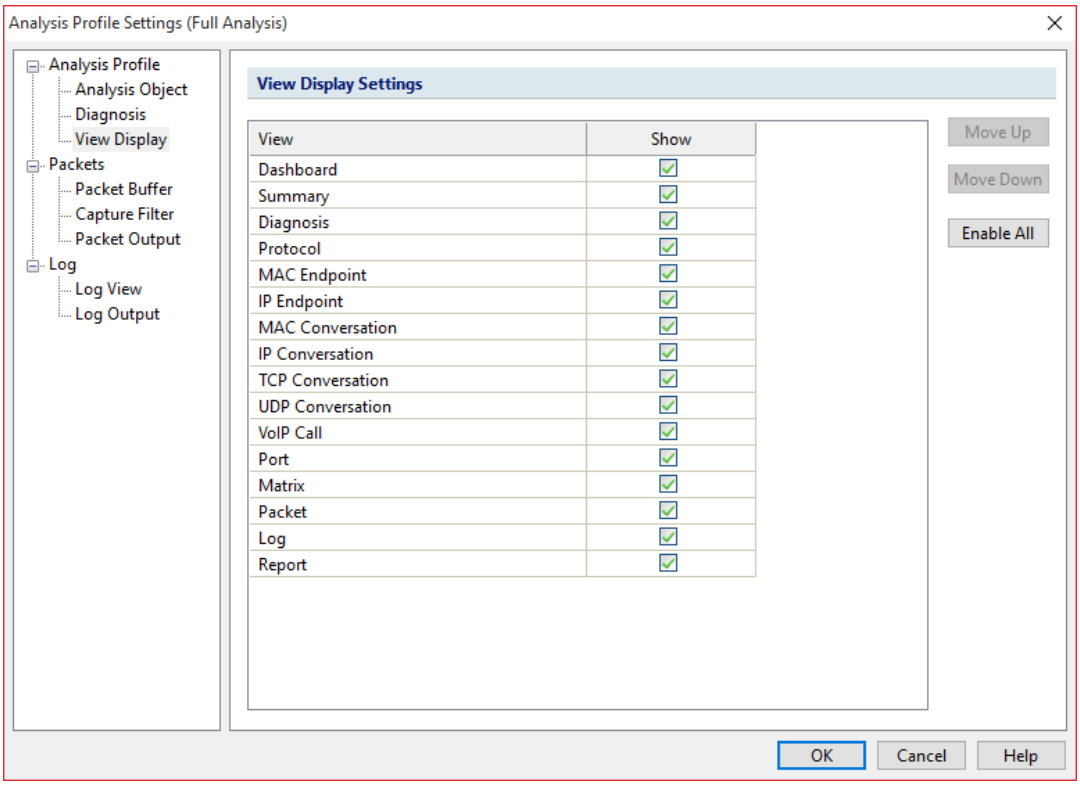
- Analysis Object เป็นส่วนของเน็ตเวิร์คโปรโตคอล
- Protocol Details การตั้งค่าการแสดงผลของข้อมูล traffic
- Max Object Count จำนวนในการวิเคราะห์ในแต่ละครั้ง โดยจะเริ่มต้นตั้งแต่ 1 ถึง 10,000 เท่านั้น

3.1.5. Diagnosis เป็นแท็บในการแสดงเหตุการณ์ของการวินิจฉัยที่มีอยู่ทั้งหมดในโมดูลของการวิเคราะห์เหตุการณ์ในปัจจุบัน ซึ่งเหตุการณ์การวินิจฉัยทั้งหมดจะถูกแบ่งออกเป็นลำดับชั้นโปรโตคอล

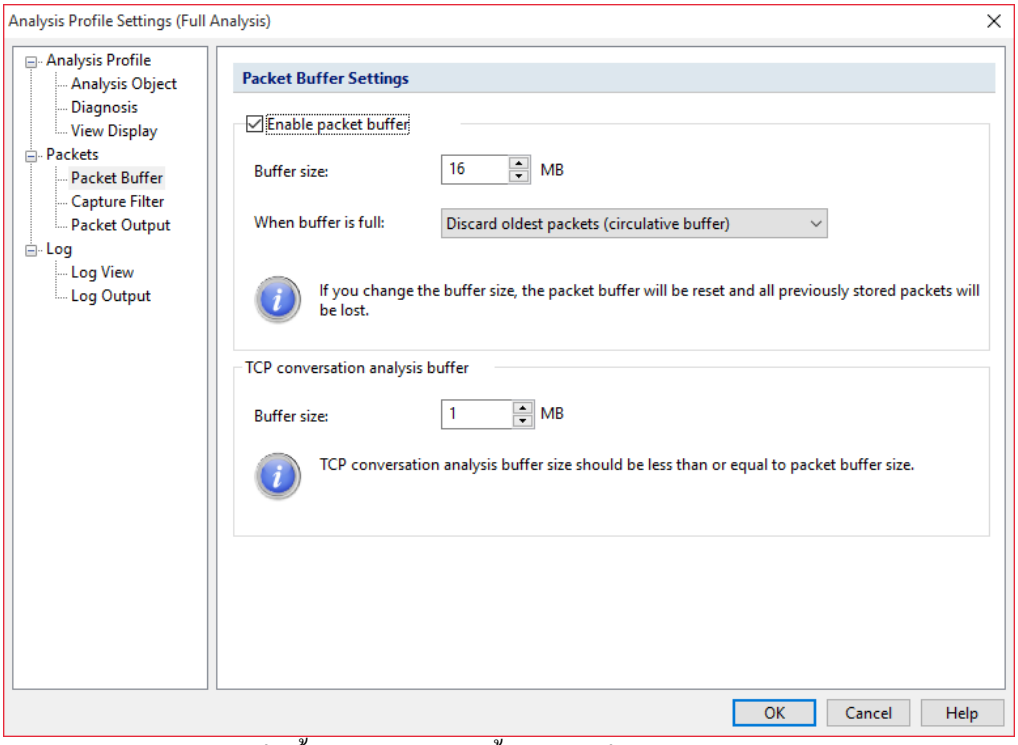


- Event List รายการทั้งหมดของการวินิจฉัยที่มีอยู่ในปัจจุบัน
- Event Setting สามารถเลือกในการแก้ไขเหตุการณ์ในส่วนของรายชื่อที่แสดงอยู่ใน Event List
- Event Description เป็นส่วนในการอธิบายของแต่ละเหตุการณ์และรายละเอียดของเครือข่าย
- เลือกเหตุการณ์ที่เกิดขึ้นทั้งหมด
- ไม่เลือกเหตุการณ์ที่เกิดขึ้นทั้งหมด
- สลับการเลือกของเหตุการณ์
- เรียกใช้เหตุการณ์
- บันทึกเหตุการณ์ทั้งหมด

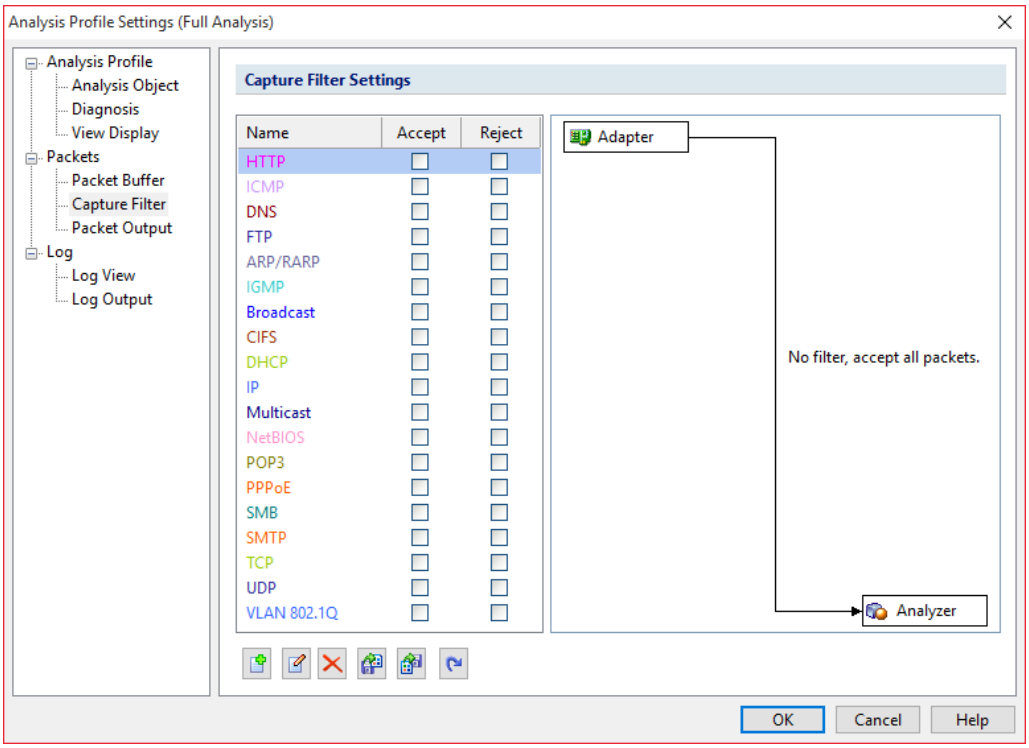
3.1.6. View Display เป็นการปรับเปลี่ยนมุมมองที่แสดงทางสถิติของการวิเคราะห์



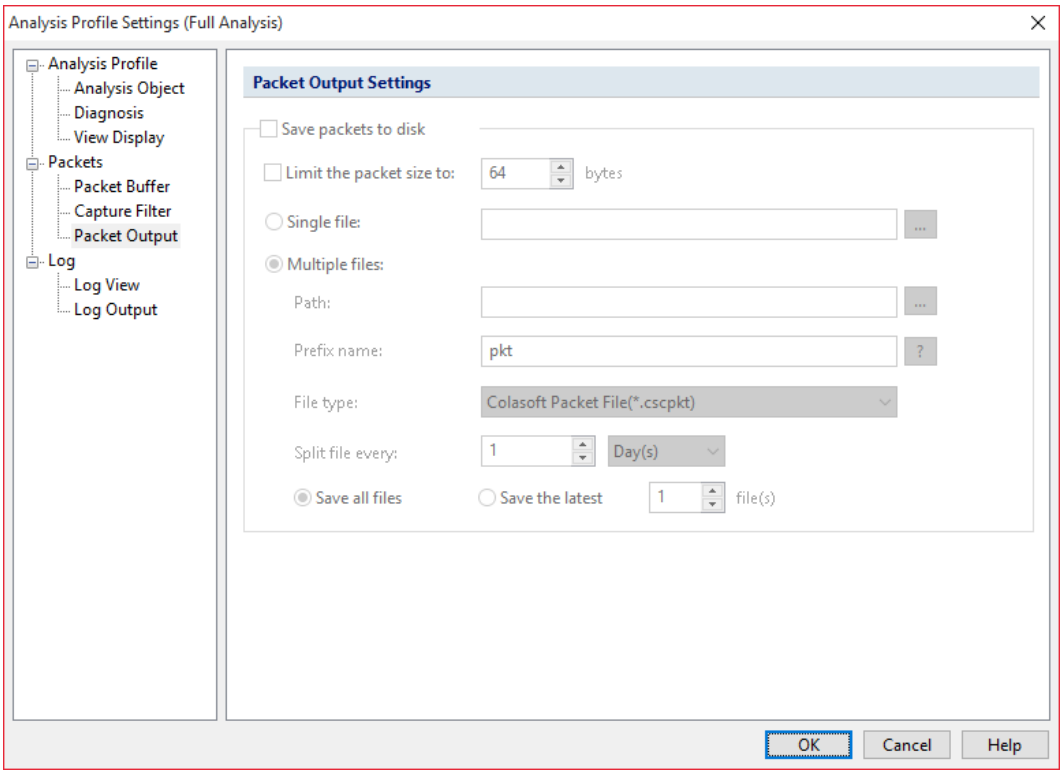
3.1.7. Packet Buffer เป็นการแสดงแพ็คเก็ตทั้งหมดที่ถูกเก็บไว้ในแพ็คเก็ตบัฟเฟอร์ ดังนั้น ขนาดของบัฟเฟอร์จะช่วยในการวิเคราะห์ได้



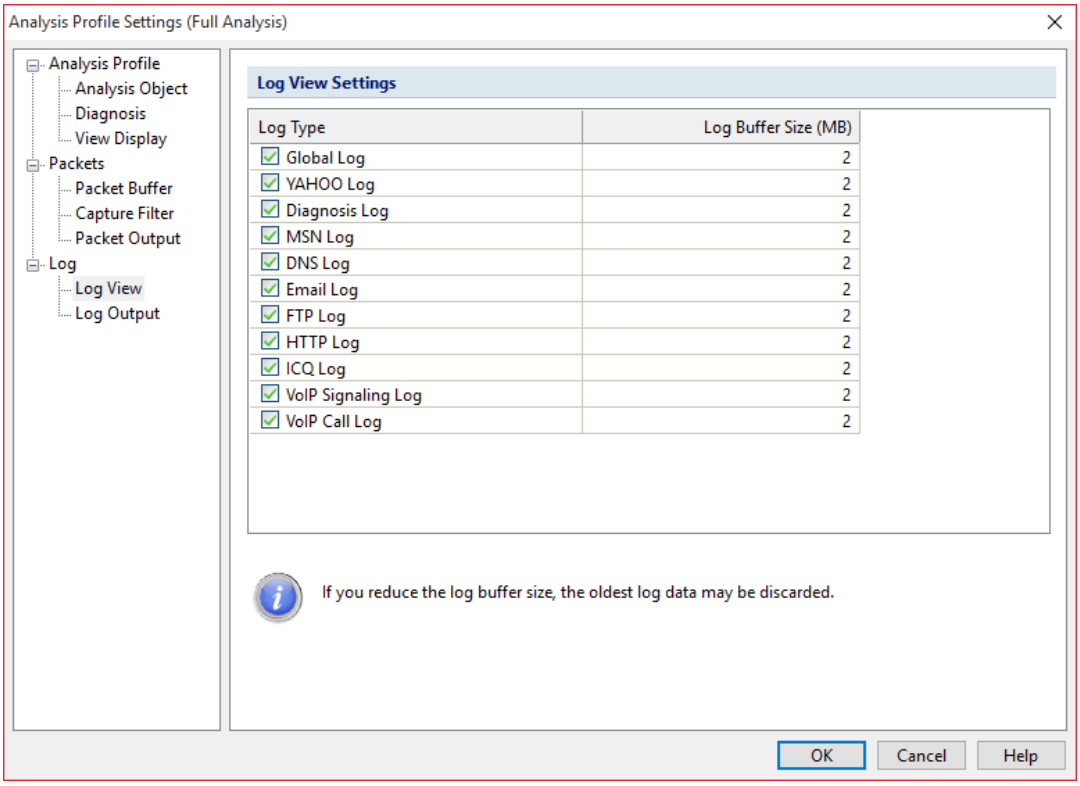
3.1.8. Capture Filter แท็บนี้มีไว้สำหรับการตั้งค่าและเป็นตัวตรวจสอบข้อมูล โดยจะวิเคราะห์แพ็คเก็ตทั้งหมดที่ส่งผ่านอะแดปเตอร์



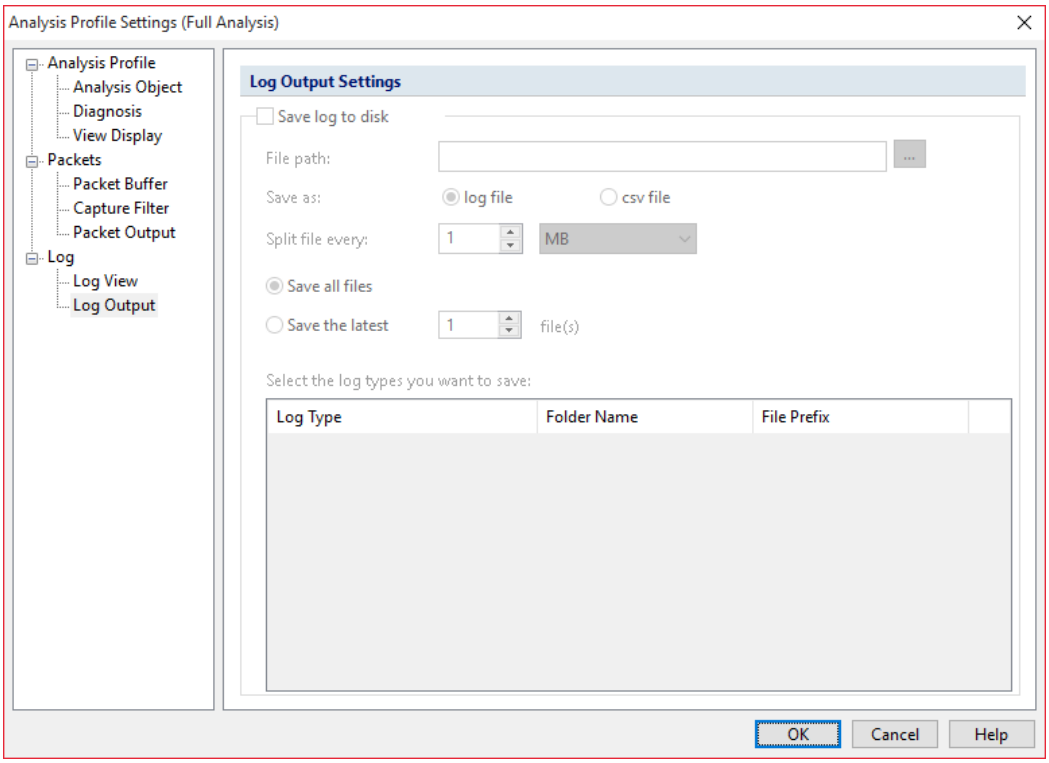
3.1.9. Packet Output เป็นส่วนในการบันทึกแพ็คเก็ตที่ใช้ในการวิเคราะห์อัตโนมัติ



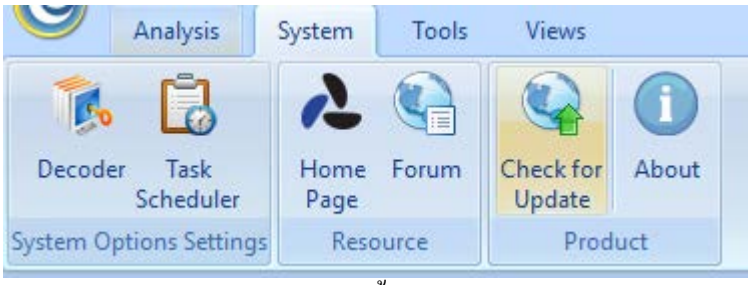
3.1.10. Log View การวิเคราะห์และการใช้งาน traffic เช่น DNS, HTTP, Email, FTP และการสนทนาของ MSN กับ Yahoo



3.1.11. Log Output เป็นการบันทึกข้อมูลของแพ็คเก็ตในส่วนของ Log View อัตโนมัติ

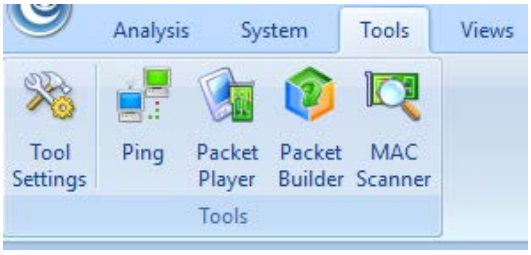


3.2. System ประกอบไปด้วยส่วนของสินค้าและการจัดการทรัพยากร

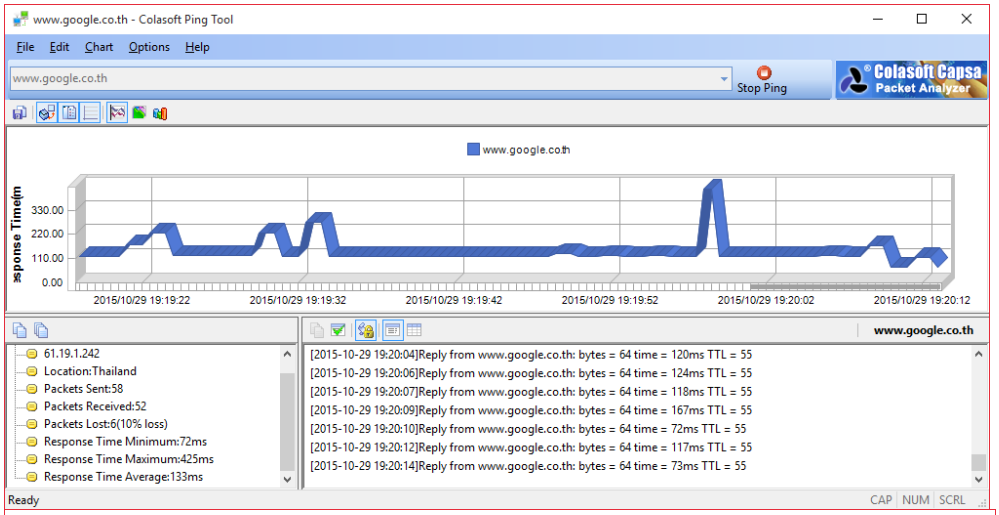


- Decoder เป็นส่วนในการตั้งค่าของโปรโตคอล
- Task Scheduler การกำหนดช่วงเวลาในการทำงาน ซึ่งสามารถทำการเพิ่มงานเข้าไปได้ ใช้ได้เฉพาะ Capsa แบบ Enterprise เท่านั้น
- Home Page ไปยังหน้าเพจของเว็บไซต์ Colasoft
- Forum ไปฟอร์มของ Colasoft
- Check for Update ตรวจสอบเวอร์ชั่นของผลิตภัณฑ์
- About เป็นการอธิบายลิขสิทธิ์และข้อมูลของใบอนุญาตของผลิตภัณฑ์

3.3. Tools เป็นเครือข่ายสำหรับเครือข่าย

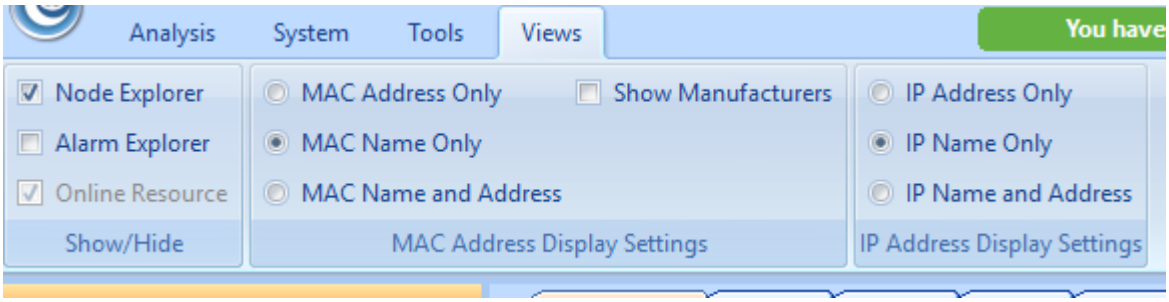


- Tool Settings เป็นเครื่องมือที่ใช้ในการตั้งค่าการจัดการ ซึ่งในระบบจะมีอยู่ 4 อย่างเดียวกัน คือ Ping, Packet Player, Packet Builder และ MAC Scanner
- Ping Tool เป็นเครื่องมือที่ใช้ในการ ping ที่มีประสิทธิภาพโดยมีการแสดงรูปแบบกราฟเพื่อให้มีการเปรียบเทียบเวลาในการตอบสนองและยังสามารถเปรียบเทียบการ ping ได้มากกว่า 1 โดยวิธีใช้งานให้ใส่เว็บไซต์ที่ต้องการ แล้วกด Start Ping



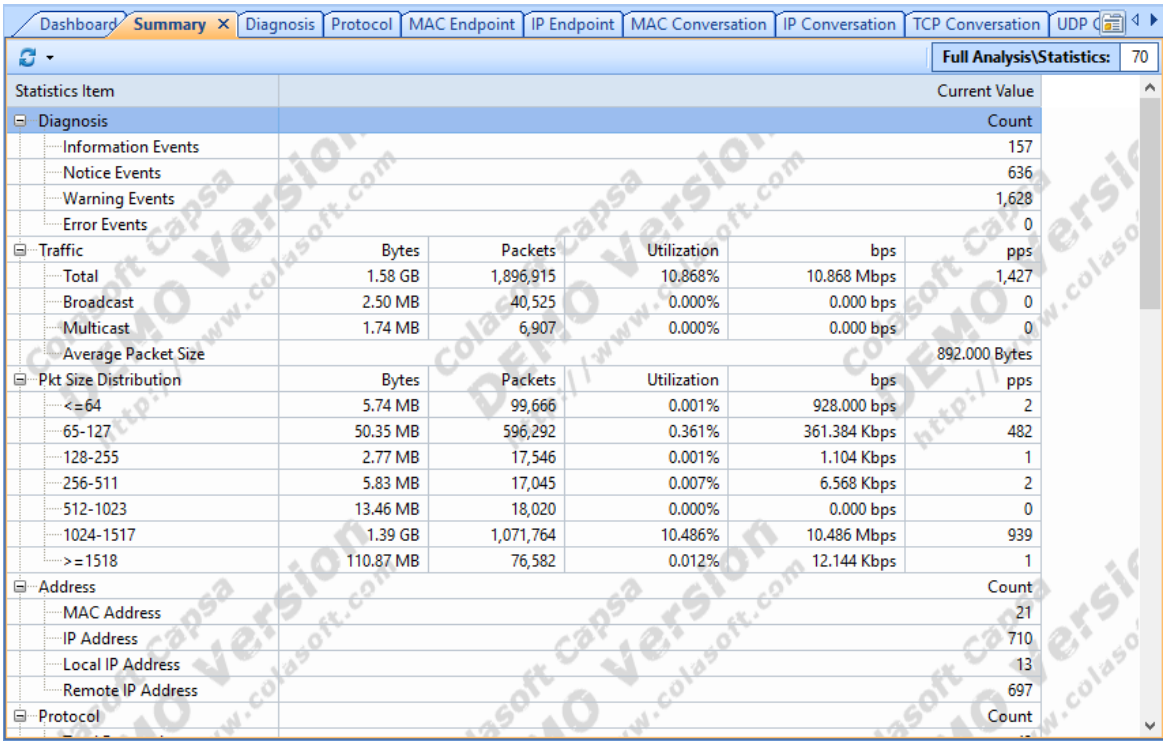
- Packet Player การนำแพ็คเก็ตมาทำการเล่นซ้ำ โดยสามารถเปิดไฟล์แพ็คเก็ตจากการเซฟเป็นนามสกุลไฟล์ .cscpke
- Packet Builder เป็นเครื่องมือที่มีประโยชน์ที่ใช้สำหรับการสร้างแพ็คเก็ตเครือข่าย ซึ่งสามารถกำหนดคุณสมบัติได้ด้วยตนเองและยังป้องกันการโจมตีจากเครือข่าย
- MAC Scanner เป็นเครื่องมือที่ใช้ในการสแกน MAC Address และ IP Address ในเครือข่าย

3.4. View เป็นการกำหนดค่าของการแสดงผลของโปรแกรม

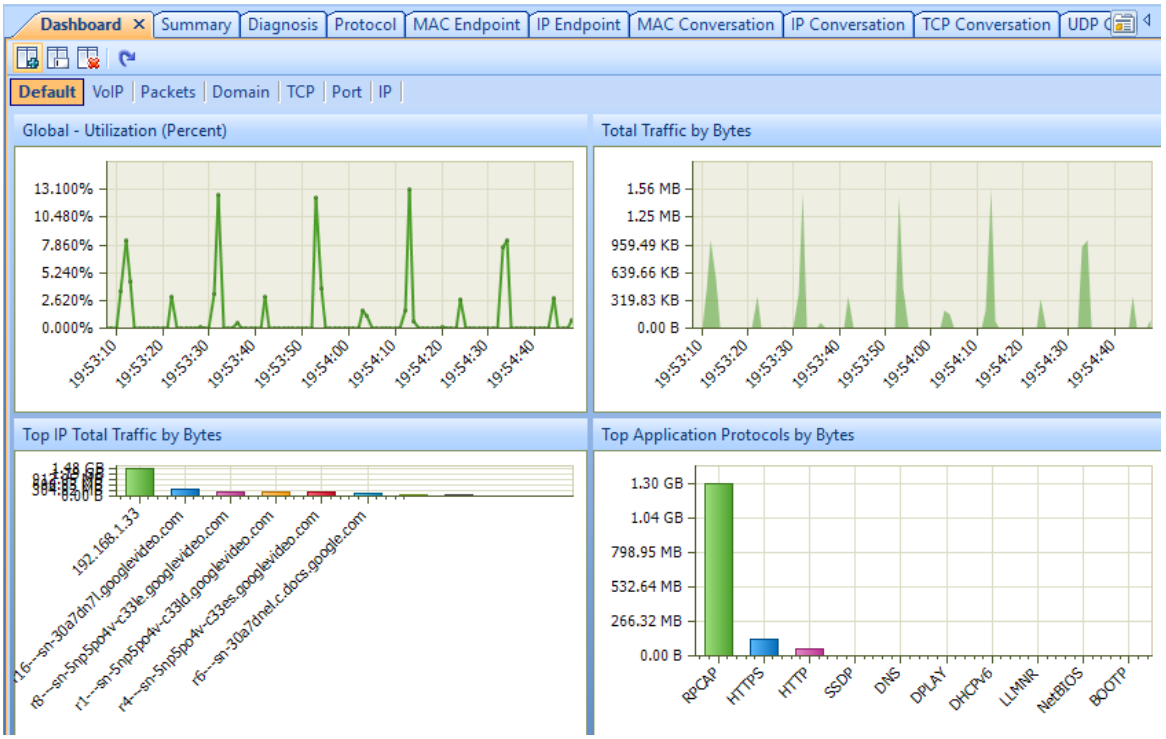


- Show/Hide เป็นการกำหนดการแสดงหน้าต่างของ Node Explorer, Alarm Explorer และ Online Resource
- MAC Address Display Settings เป็นการตั้งค่ารูปแบบของ MAC Address
  - MAC Address Only แสดงค่า MAC Address ในรูปแบบฐานสิบหก เช่น AA:BB:CC:33:44:55
  - MAC Name Only แสดง MAC Address ในรูปแบบชื่อ เช่น localhost
  - MAC Name and Address แสดงในรูปแบบฐานสิบหกพร้อมชื่อ เช่น [localhost]-AA:BB:CC:33:44:55
  - Show Manufacturers ซ่อนหรือแสดงส่วนของอะแดปเตอร์

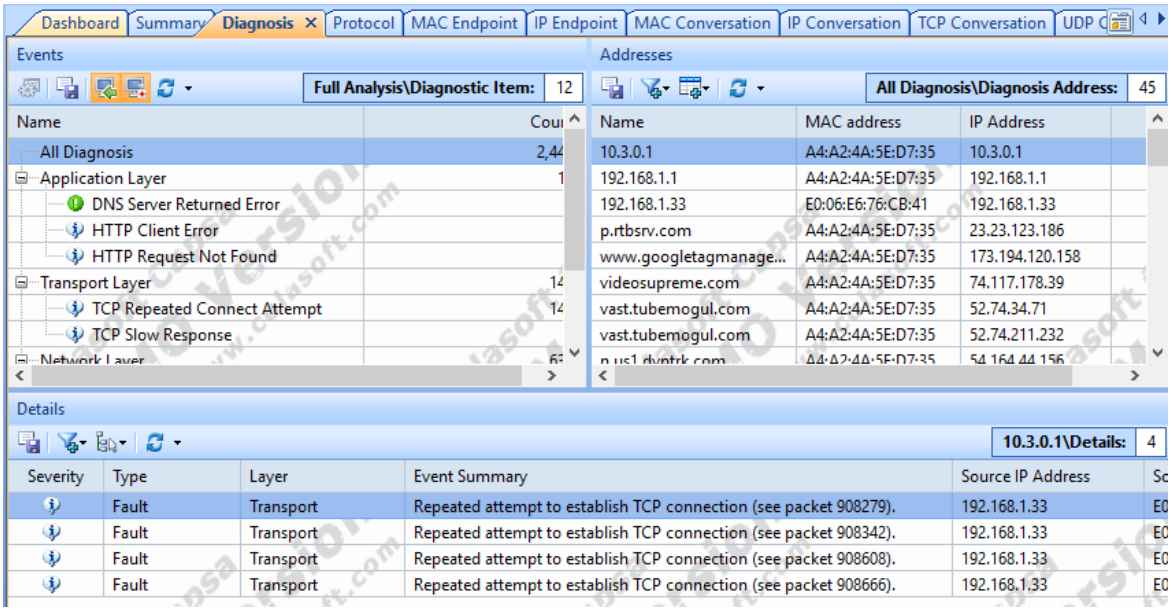
4. Node Explorer window เป็นหน้าสำหรับการแสดงผลรวมโดยสามารถดูข้อมูลต่างๆของแต่ละโหนดได้อย่างรวดเร็วและมีความแม่นยำ และสามารถเลือกประเภทที่สามารถที่ต้องการดู โดยจะแสดงข้อมูลในรูปแบบของสถิติ โดยมีไอคอนดังนี้
   - เป็นการเพิ่มโหนด Name Table
   - สร้างการ filters จากโหนดที่เลือกไว้ในรายการ
   - สร้างกราฟจากโหนดที่เลือกไว้ในรายการ
   - สร้างการแจ้งเตือนภัยจากโหนดที่เลือกไว้ในรายการ
   - สรุปรายงานจากโหนดที่เลือกไว้ในรายการ
5. Statistical views เป็นหน้าต่างการแสดงทรัพยากรแบบออนไลน์ ซึ่งจะมีการแสดงผลเชิงสถิติและกราฟ ส่วนแรกจะเป็นในส่วนของ summary ซึ่งจะสรุปภาพรวมในเครือข่ายปัจจุบัน ซึ่งจะบอกข้อมูลคร่าวๆในเครือข่าย เช่น จำนวน traffic, ขนาดของ packet, จำนวน protocol, รูปแบบการสื่อสาร



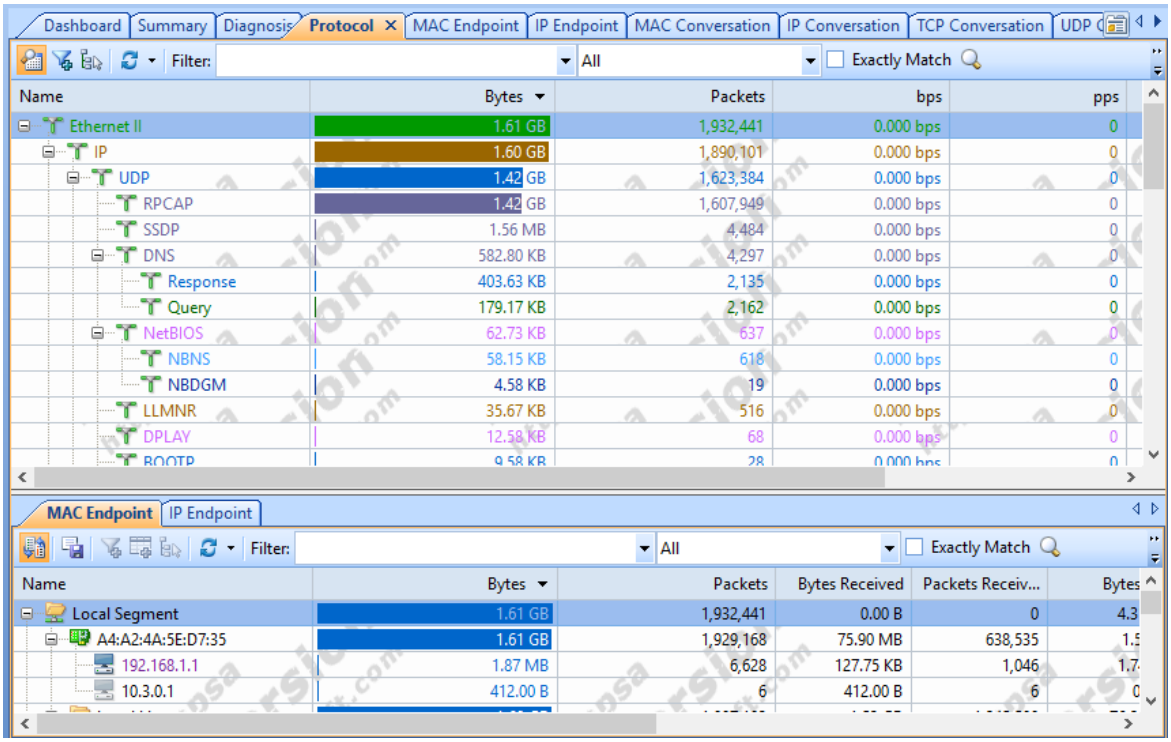
ส่วนของ Dashboard จะเป็นการสรุปการใช้งานต่างๆในระบบเครือข่ายออกมาในรูปแบบกราฟ หรือแผนภูมิ เพื่อให้ผู้ใช้งานสามารถนำไปวิเคราะห์ระบบได้ง่าย โดยจะแบ่งออกเป็น Default, VoIP, Packets, Domain, TCP, Port และ IP



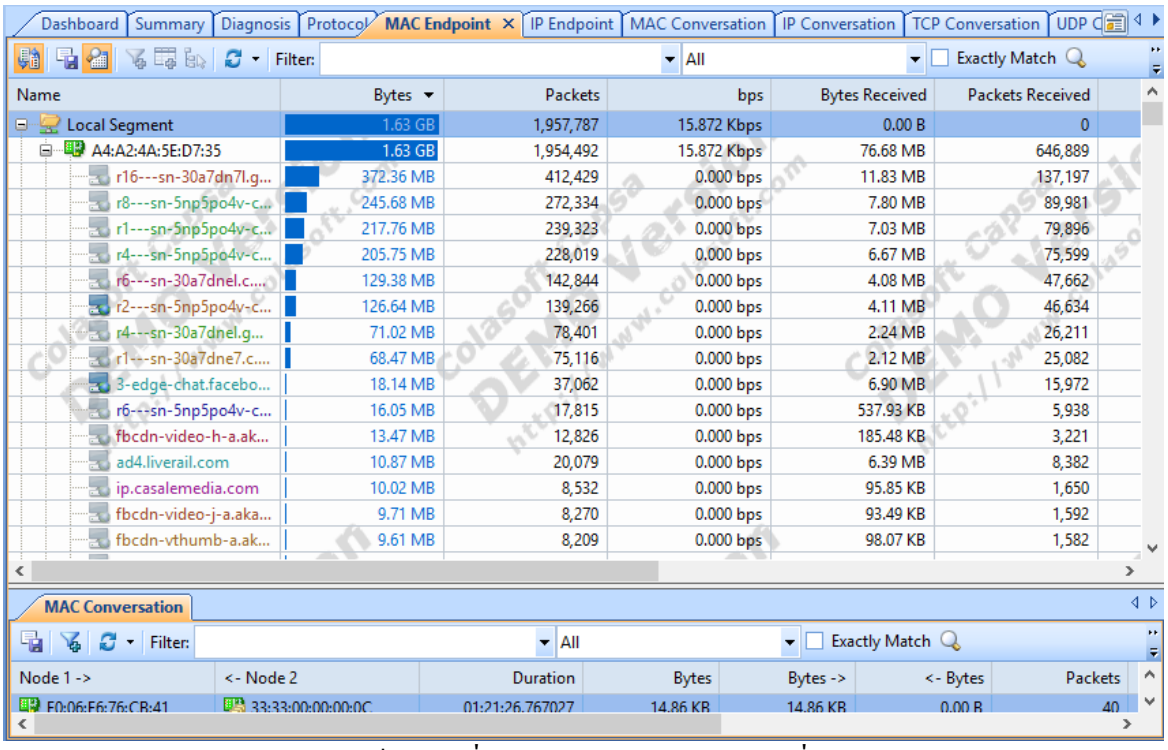
หน้าแสดง Diagnosis จะเป็นการแสดงข้อมูลของเหตุการณ์ต่าง ๆ ที่เกิดขึ้นในเน็ตเวิร์คทั้งหมด โดยแบ่งตามลำดับชั้นของเน็ตเวิร์ค ทำให้ง่ายต่อการค้นหาปัญหาเหตุการณ์ต่าง ๆ ในเน็ตเวิร์ค



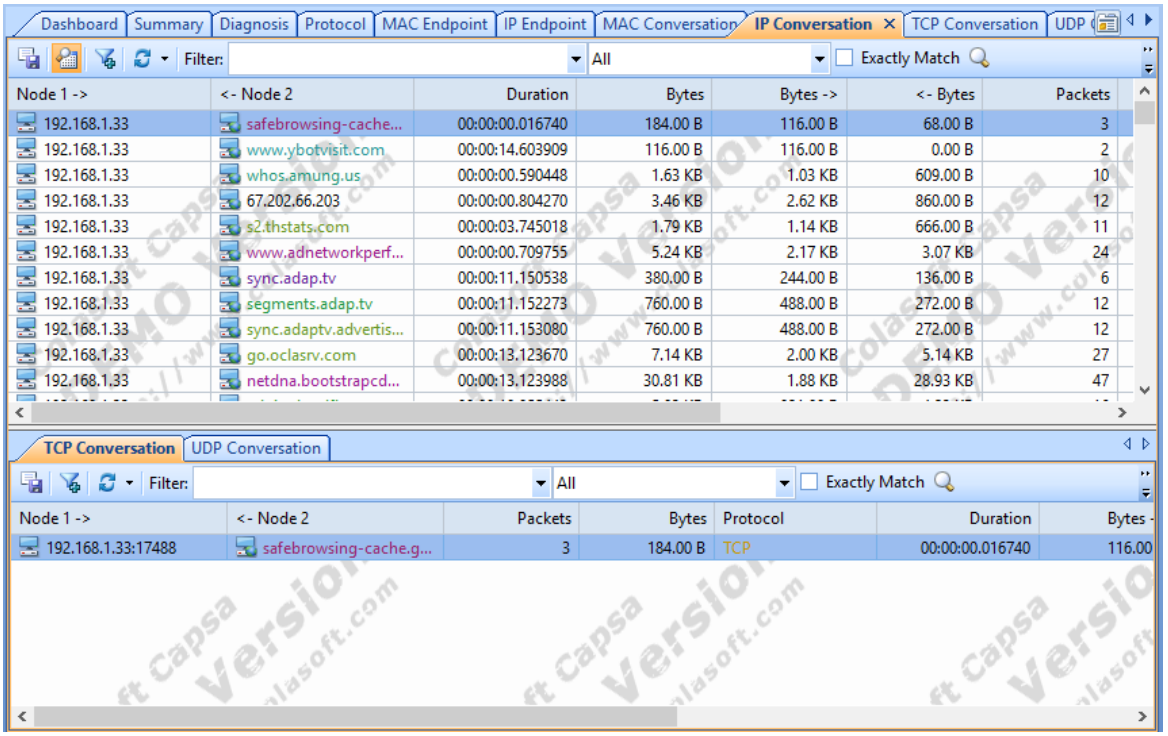
หน้าแสดง protocol จะแสดง protocol ที่มีการใช้งานอยู่ในระบบเครือข่าย โดยจะแสดงรายละเอียดของแต่ละ protocol ประกอบด้วย ขนาด, จำนวน packet, อัตราการรับ-ส่งข้อมูล



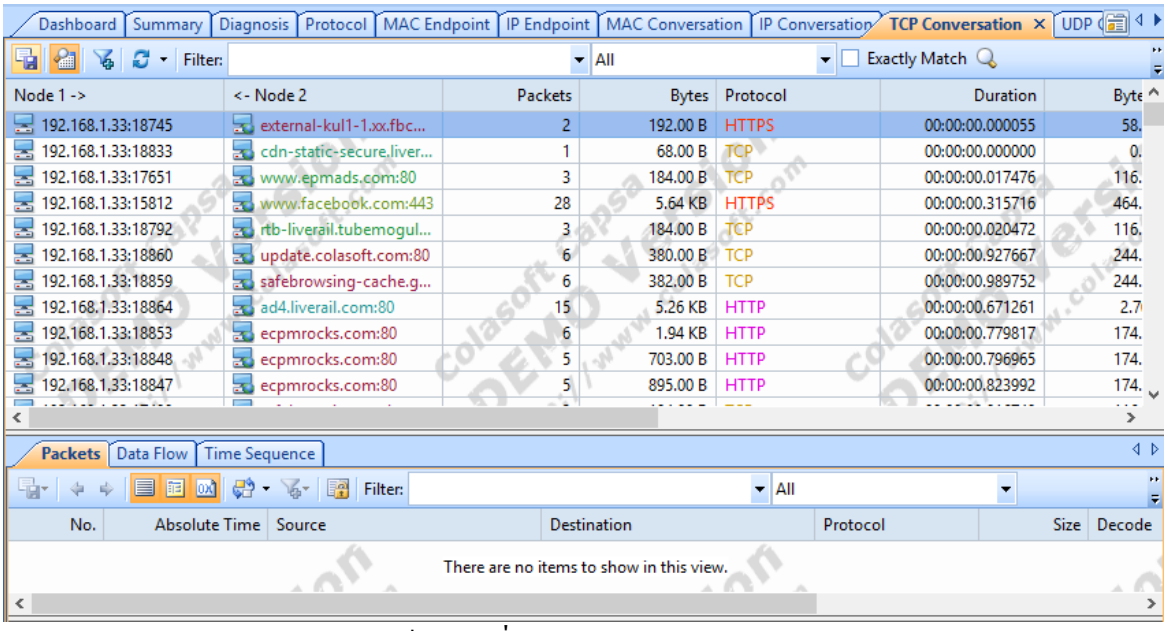
หน้าแสดง MAC Endpoint เป็นการแสดงในลักษณะของ MAC Address



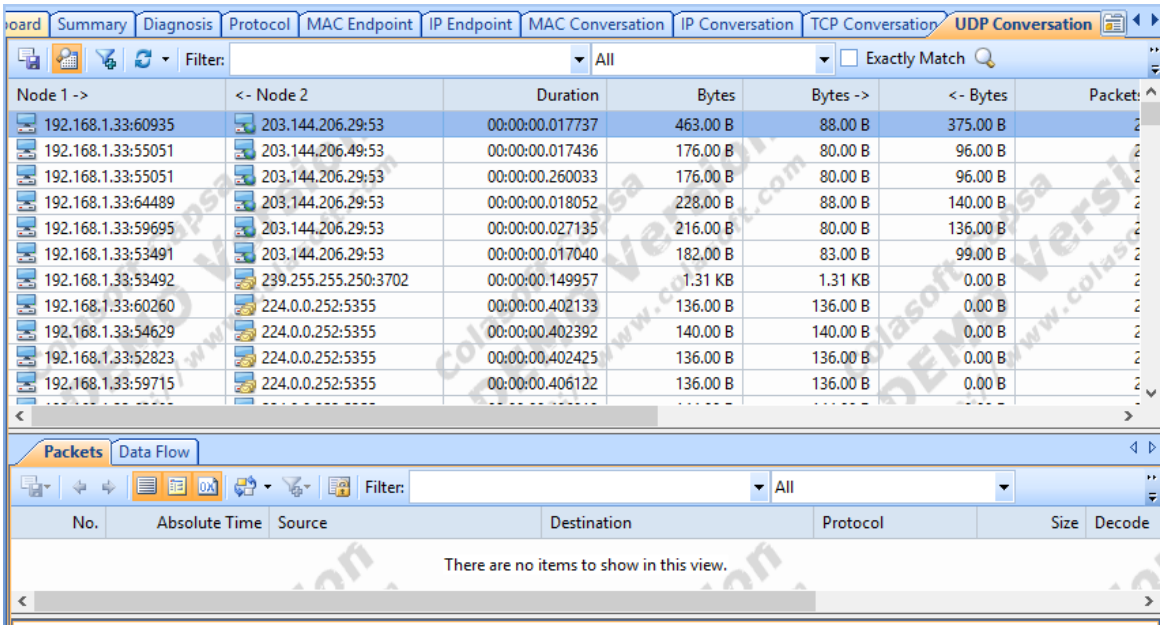
หน้าแสดง IP Conversation เป็นหน้าที่แสดงในส่วนของการติดต่อสื่อสารโดยใช้ protocol IP ว่าเครื่องมีการเชื่อมต่อไปที่โหนดใดบ้าง แต่ละโหนดที่มีการติดต่อสื่อสารไปนั้นมีขนาดข้อมูลที่สื่อสารเท่าไหร่, จำนวน packet ที่ใช้, เวลาเริ่มต้นในการส่งข้อมูลและเวลาสิ้นสุดในการส่งข้อมูล



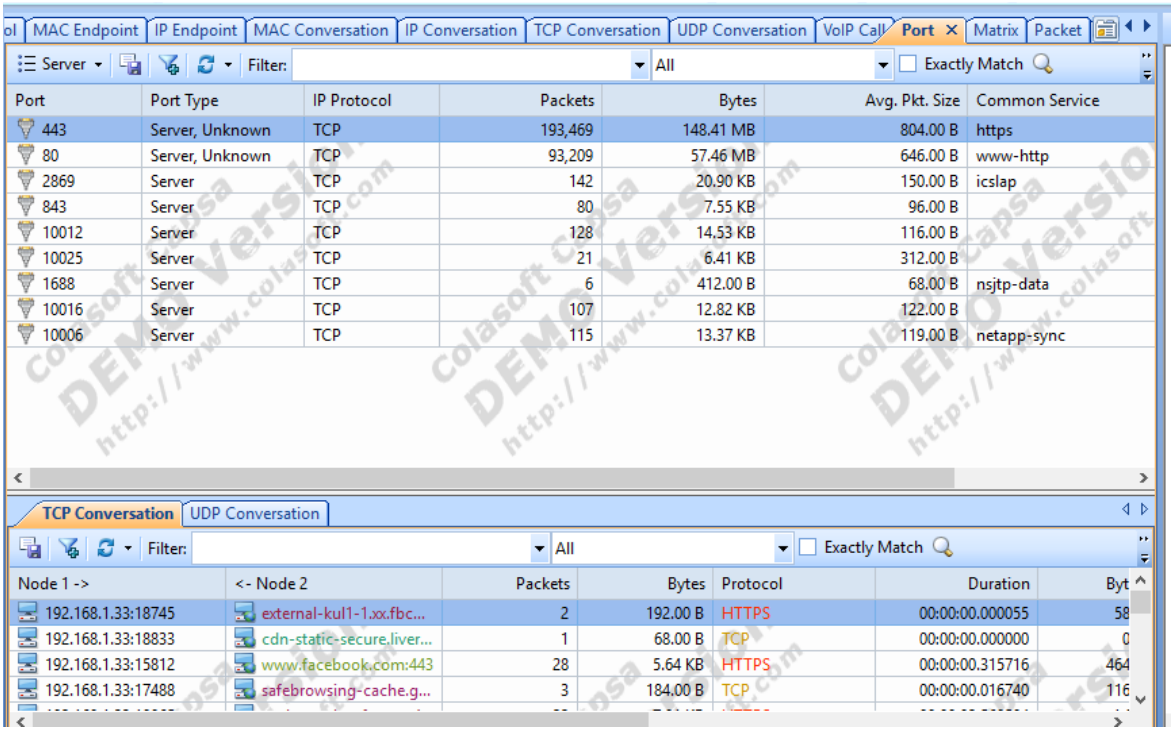
หน้าแสดง TCP Conversation เป็นหน้าที่แสดงข้อมูลเช่นเดียวกับ IP Conversation แต่จะแสดงเฉพาะการติดต่อสื่อสารระหว่างโหนดโดยใช้ protocol TCP



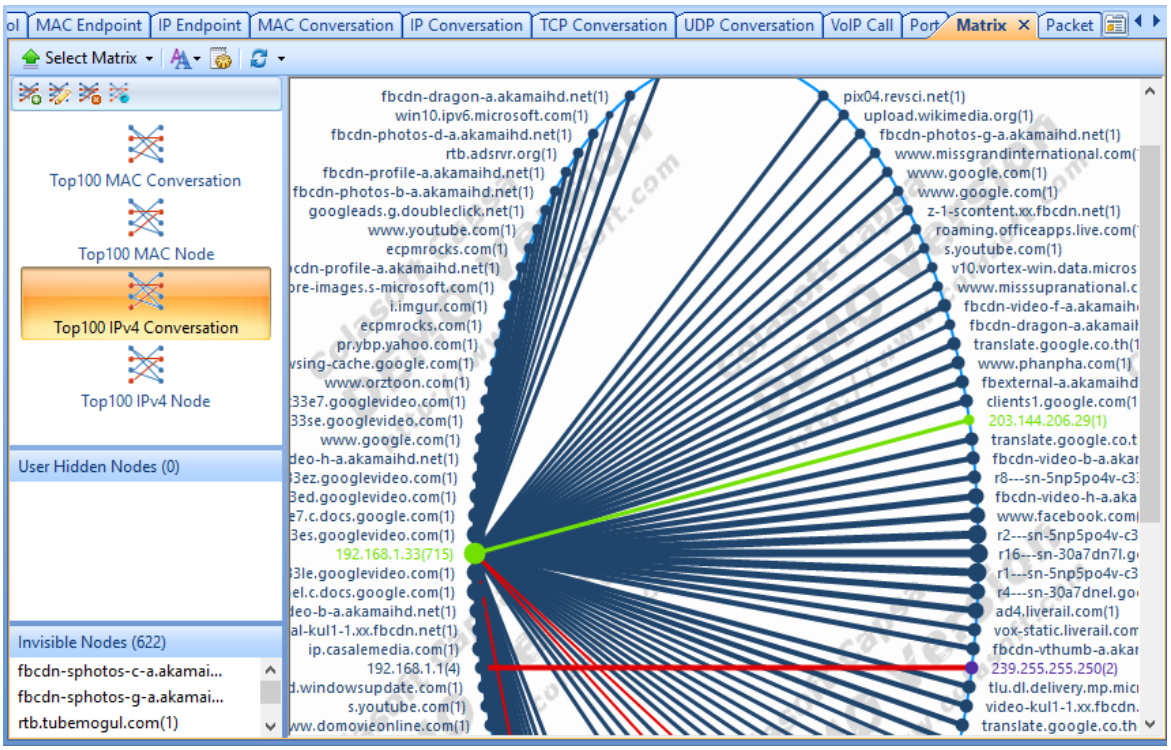
หน้าแสดง UCP Conversation เป็นหน้าที่แสดงข้อมูลเช่นเดียวกับ IP Conversation แต่จะแสดงเฉพาะการติดต่อสื่อสารระหว่างโหนดโดยใช้ protocol UCP



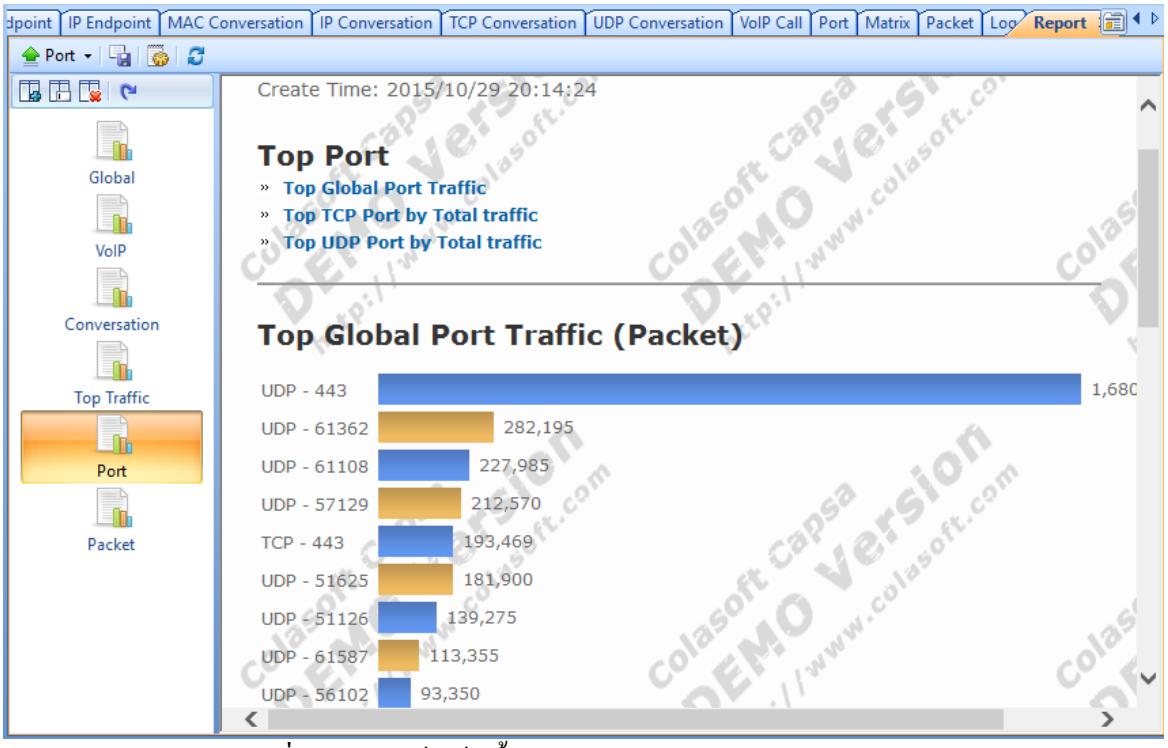
หน้าแสดง port คือ แสดง port ที่มีการใช้งานอยู่



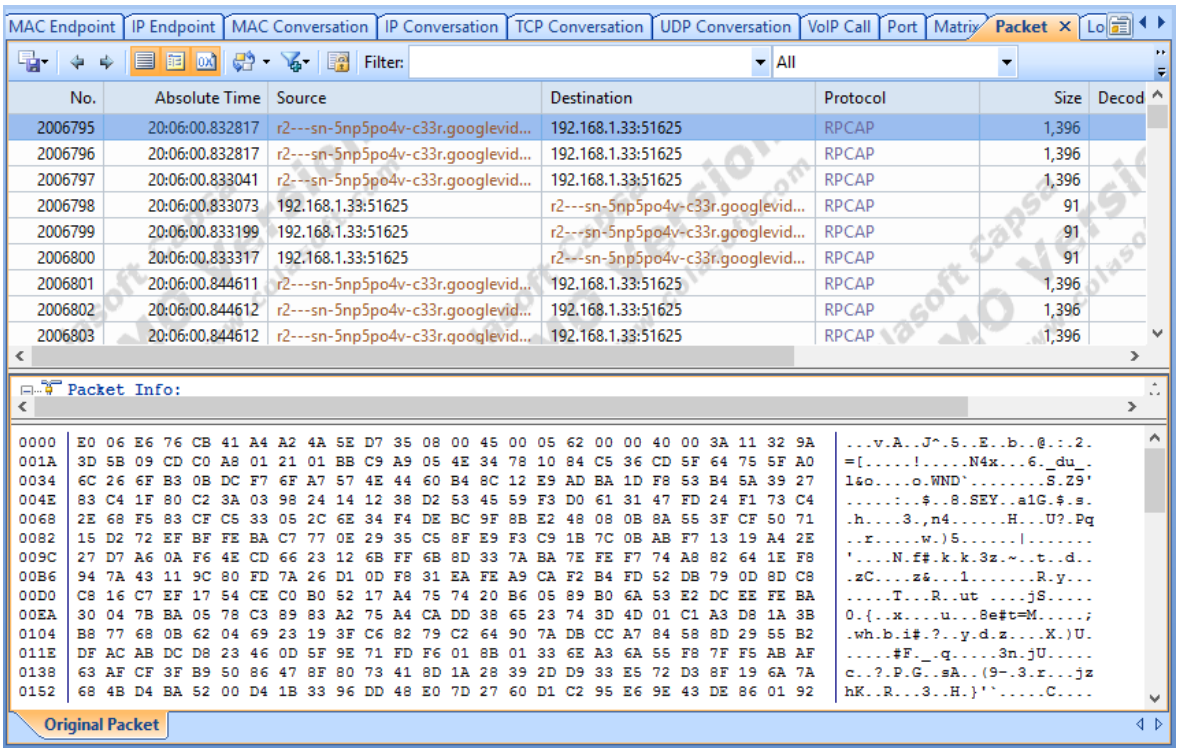
หน้าแสดง Matrix เป็นการแสดงรูปแบบการเชื่อมต่อระหว่างโหนดและทราฟฟิคในรูปแบบของกราฟ



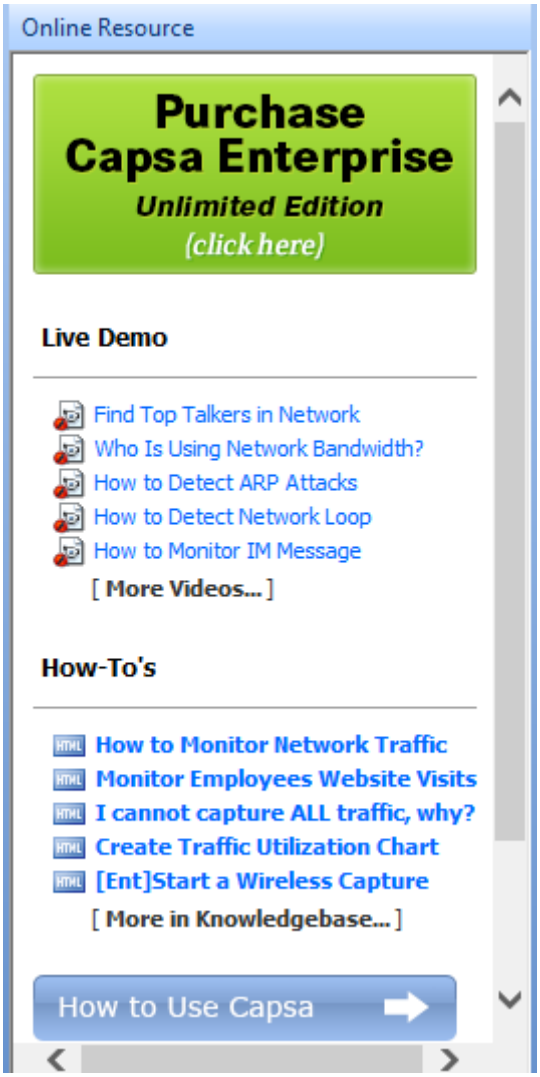
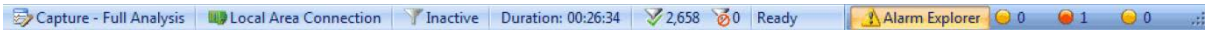
หน้า Report จะเป็นหน้าที่ให้ผู้ใช้สามารถดูผลสรุปโดยรวมของการทำงานในระบบเครือข่ายได้ ซึ่งสามารถเลือกดูได้ในหลายรูปแบบ



หน้า Packet ทำหน้าที่แสดงผลแพ็คเก็ตทั้งหมดภายเครือข่ายของผู้ใช้งาน



6. Online Resource window เป็นหน้าต่างการค้นหาทรัพยากรในรูปแบบออนไลน์โดยสามารถศึกษาขั้นตอนการใช้งานต่างๆได้



7. Status Bar เป็นแถบสถานะที่จะนำเสนอข้อมูลของโปรเจคที่ใช้ในการวิเคราะห์