



**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 :** 29<sup>th</sup> 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 เป็นโปรแกรมที่ถูกพัฒนาขึ้นมาเพื่อที่จะเอาไว้มอนิเตอร์การรับส่งข้อมูลในวงเน็ตเวิร์คหรือวง LAN ได้อย่างละเอียด มีฟังก์ชันการใช้งานที่ครอบคลุมหลากหลาย เช่น มีระบบตรวจสอบและป้องกันไฟล์ที่ไม่พึงประสงค์ที่จะบุกรุกเข้ามาในข้อมูลระบบเครือข่าย สังเกตปริมาณการรับส่งข้อมูลที่อาจผิดปกติ ผิดเพี้ยน ไปจากเดิมที่เคยเป็น นอกจากนี้ยังใช้แสดงค่าปริมาณและสถิติการรับส่งข้อมูลในระบบเครือข่ายได้ (Bandwidth Statistics) สามารถตรวจสอบข้อมูลเครือข่ายการใช้งานโปรแกรมบนเว็บเบราว์เซอร์ต่างๆ ได้ ซึ่งสนับสนุนโปรโตคอลแบบต่างๆ หรือพวกโปรแกรมแชทและอื่นๆอีกมากมาย แต่สำหรับในเวอร์ชันฟรีจะไม่สามารถรองรับการดูข้อมูลของเครือข่ายบางอย่างได้

### คุณสมบัติ

1. มีระบบตรวจสอบและป้องกันในการใช้งานของ TCP พอร์ตจากไฟล์ที่ไม่พึงประสงค์ (Malware) จากทาง DoS (DDoS), Worm และ ARP
2. สามารถแสดงค่าปริมาณและสถิติการรับส่งข้อมูลในระบบเครือข่ายได้ในรูปแบบกราฟและตัวเลข
3. มีฟังก์ชันในการดูข้อมูลเครือข่ายของการใช้งานโปรแกรมต่างๆ บนเว็บเบราว์เซอร์ได้ เช่น HTTP, E-Mail, DNS, FTP และ โปรแกรมอื่นๆ อีกมากมาย
4. สามารถวิเคราะห์ข้อมูลในด้านโปรโตคอลของระบบเครือข่ายได้มากกว่า 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

Home > Download > Download Colasoft Products

**DOWNLOAD**

- Colasoft Products
- Product Documents
- Video Tutorials
- Packet Files
- Capture Filters

### Download Colasoft Products

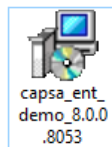
nChronos nChronos or Capsa, help me choose.

Products	File Size	Requirements	Download Free Trial
nChronos 4.3 Network Forensic Analysis Application	109 MB	Windows XP/2003/2008/Vista/7	

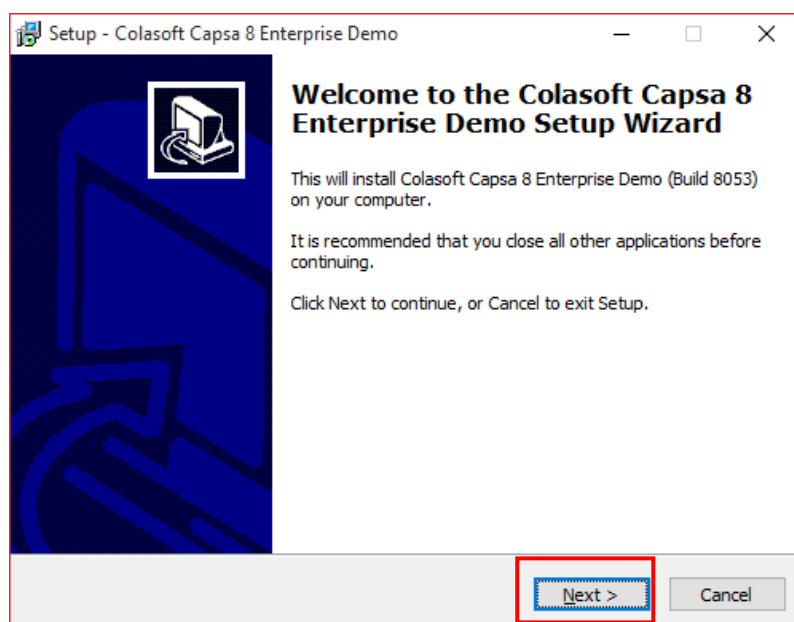
### Capsa

Products	File Size	Requirements	Download Free Trial
Capsa Enterprise 8.0 Ethernet & Wireless	47.3 MB	Windows XP/2003/2008/Vista/7/8/10	
Capsa Professional 8.0 For Ethernet	47.2 MB	Windows XP/2003/2008/Vista/7/8/10	

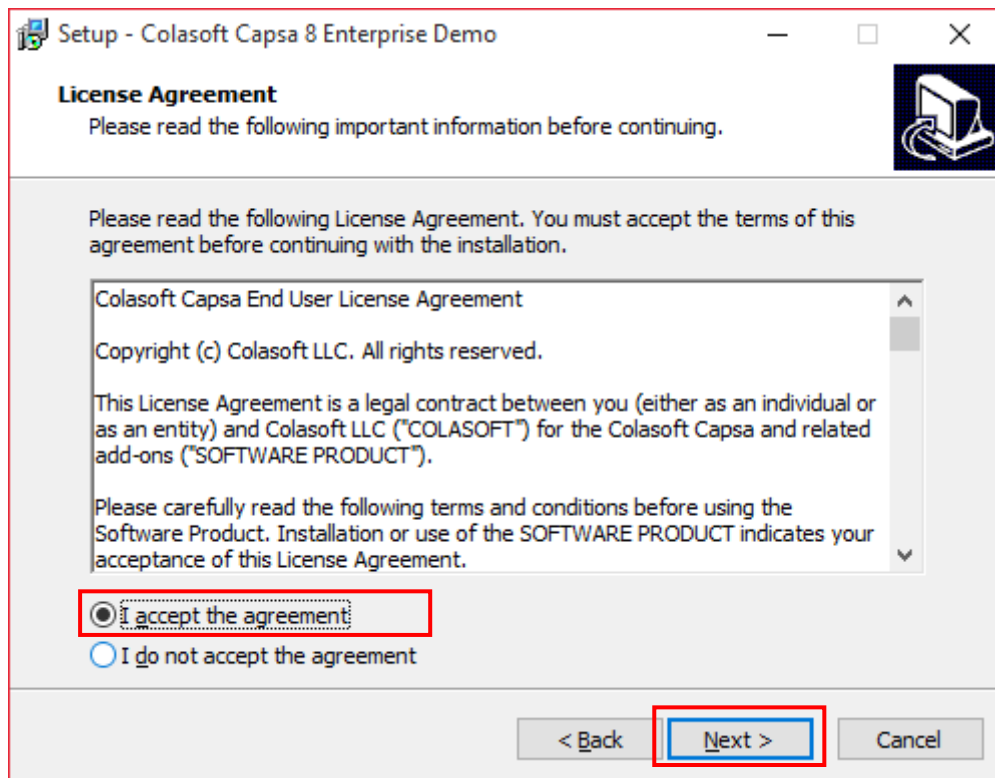
2. คลิกไฟล์ที่ชื่อว่า capsa\_ent\_demo\_8.0.0.8053.exe เพื่อทำการติดตั้งโปรแกรม



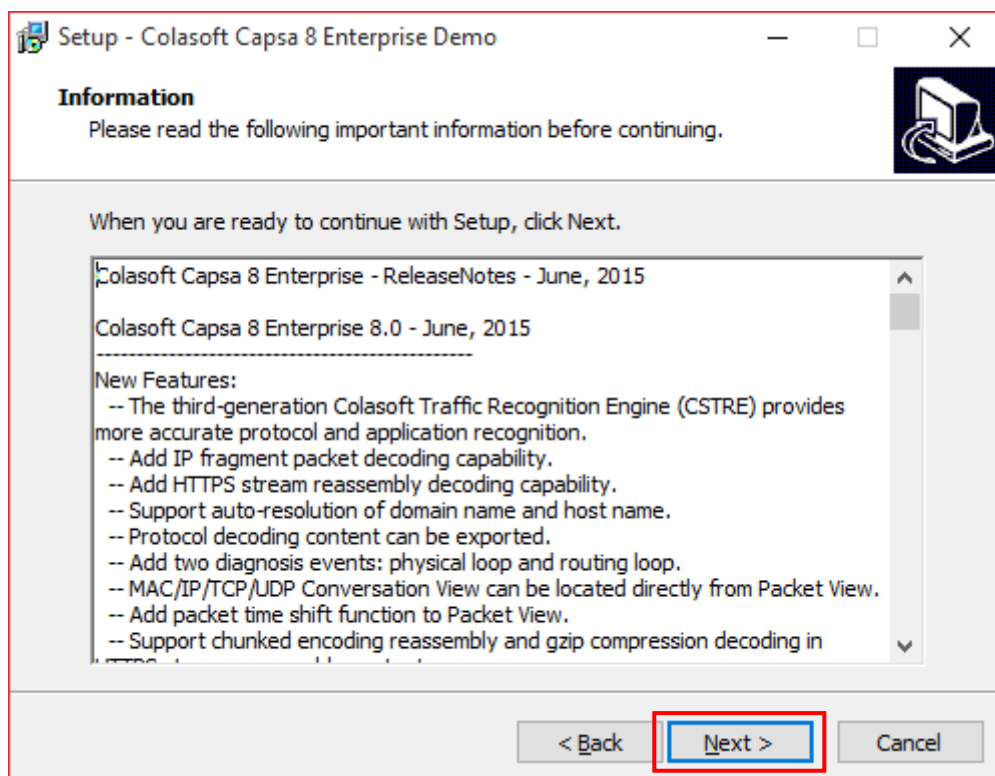
3. คลิก Next เพื่อทำการติดตั้ง



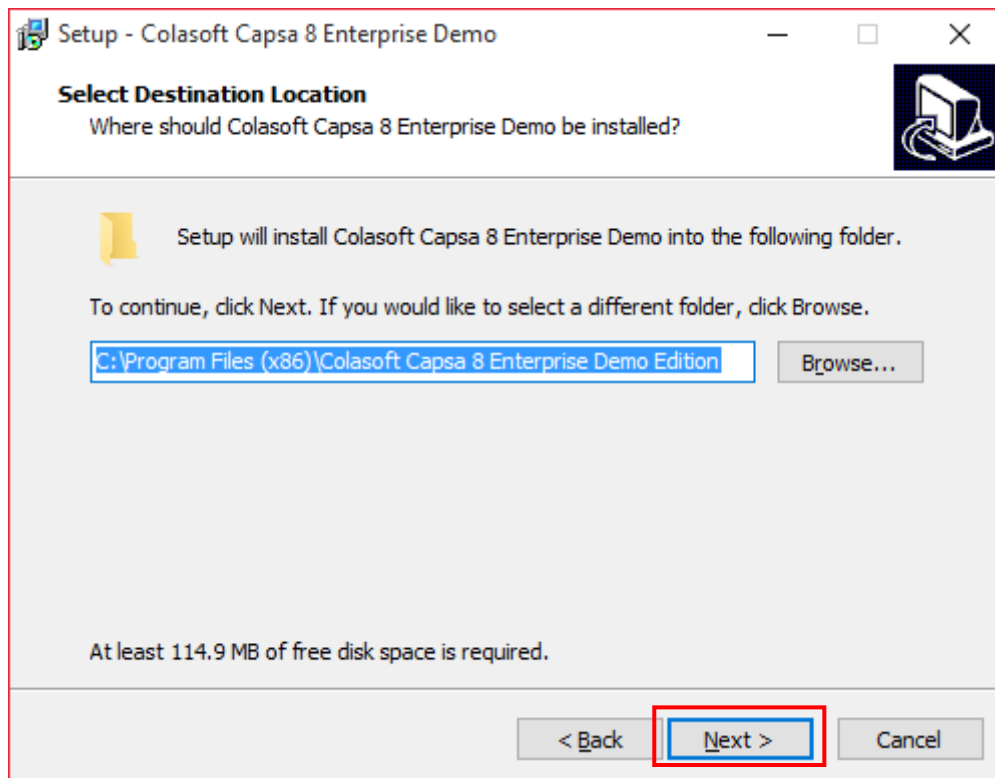
4. เลือก I accept the terms in the license agreement แล้วทำการคลิก Next เพื่อไปในขั้นตอนต่อไป



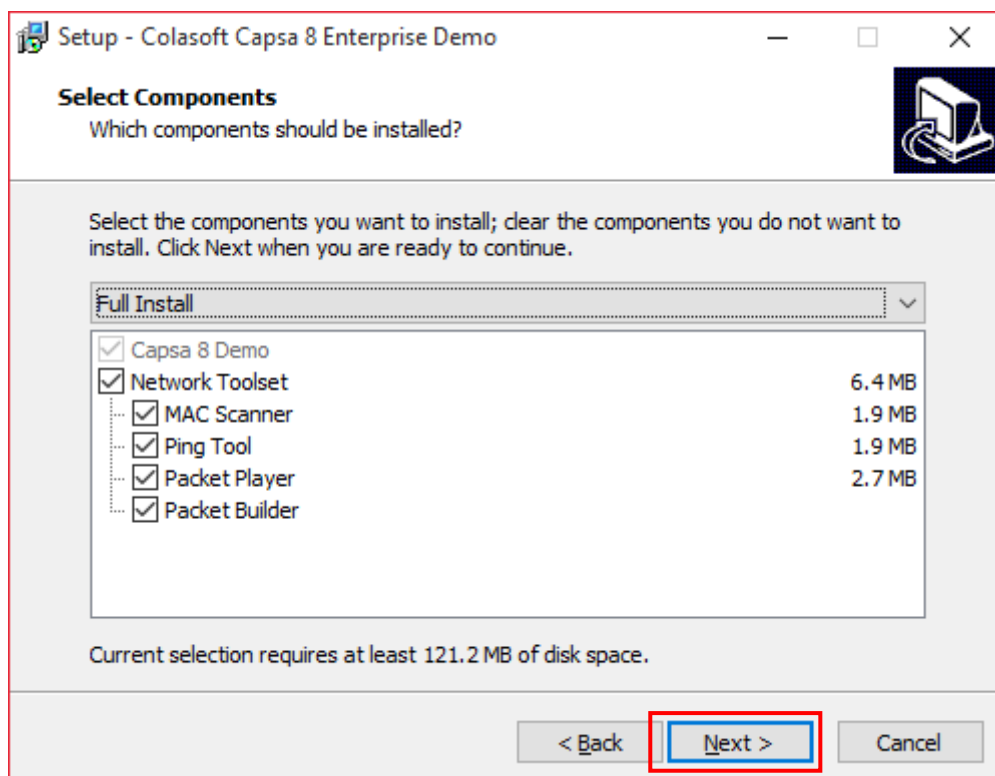
5. คลิก Next เพื่อทำการติดตั้ง



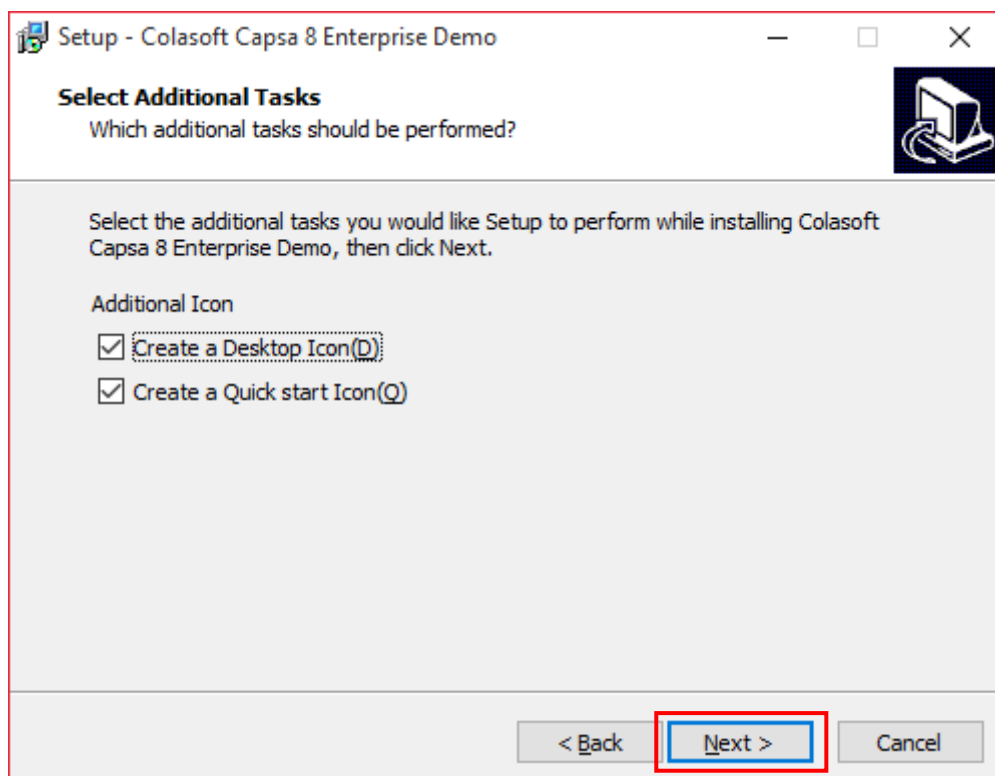
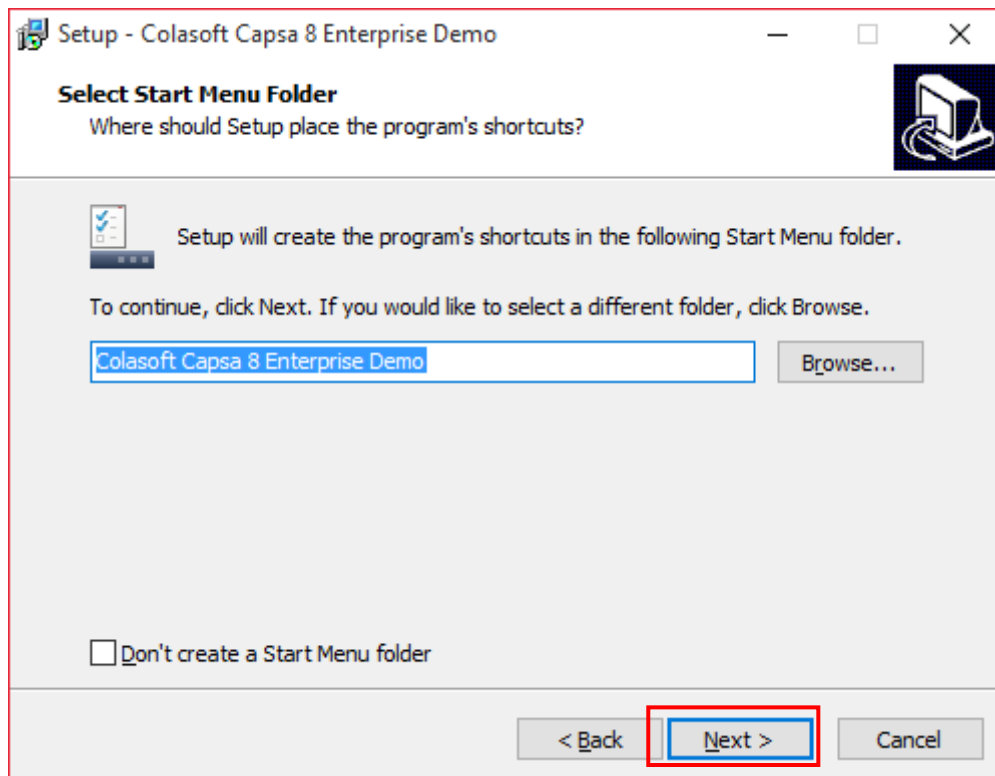
6. เลือกที่อยู่ของโปรแกรม (แนะนำให้ใช้ที่อยู่ที่โปรแกรมกำหนดให้) และให้ทำการคลิก Next



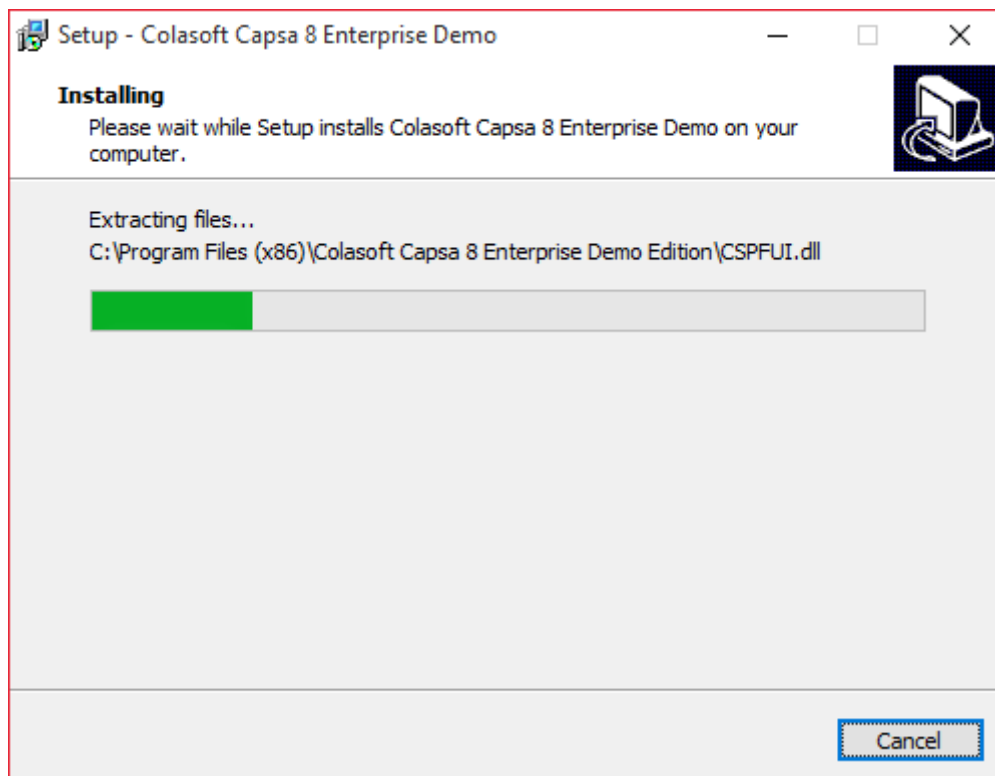
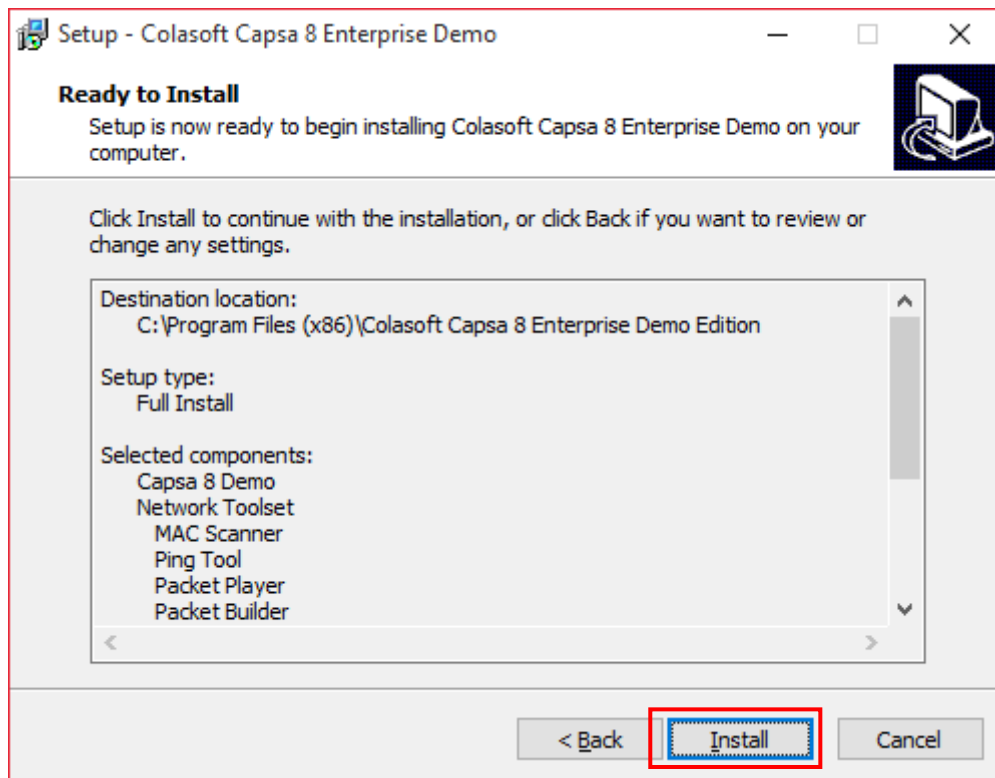
7. คลิก Next เพื่อทำการติดตั้ง



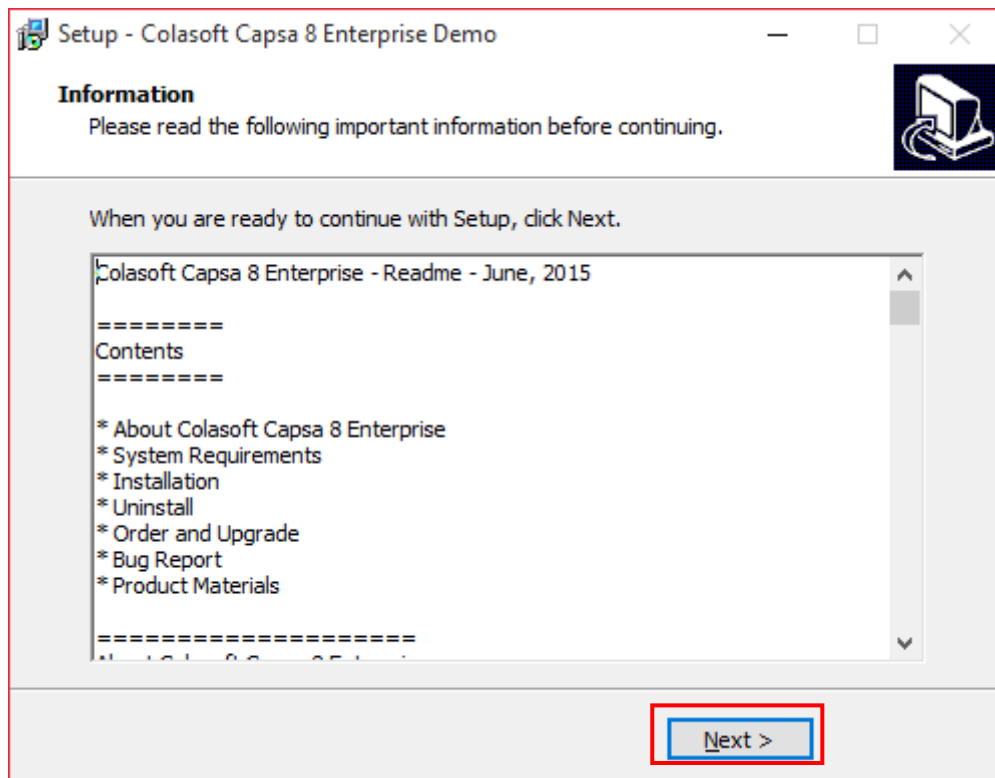
8. คลิก Next เพื่อทำการติดตั้ง



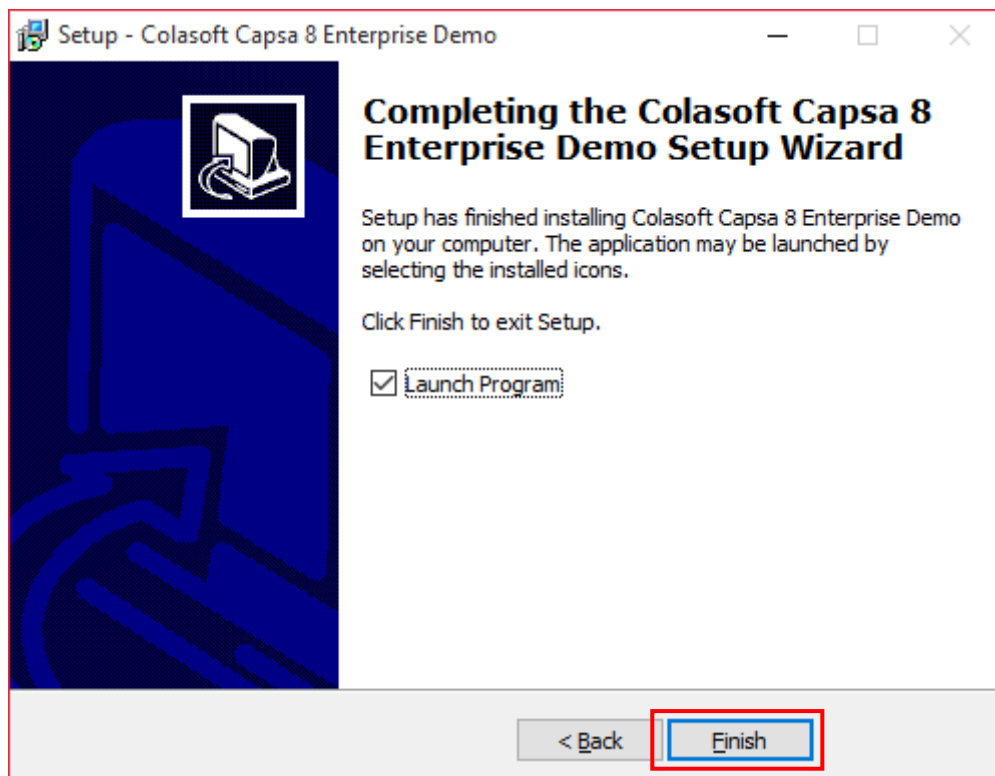
9. คลิก Install เพื่อทำการติดตั้งโปรแกรม



10. คลิก Next



11. คลิก Finish เพื่อสิ้นสุดการติดตั้งโปรแกรม





## การถอนการติดตั้งโปรแกรม

การถอนการติดตั้งโปรแกรมมีอยู่ 2 วิธี ดังนี้

1. การถอนการติดตั้งโปรแกรม Colosoft Capsa ให้คลิกที่ปุ่ม Start > All Programs > ColosoftCapsa8 > 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 เวอร์ชัน 8 ซึ่งจะมีรายละเอียดแต่ละส่วนการใช้งานดังนี้

The screenshot shows the Capsa 8 interface with the following numbered callouts:

- 1: Capture and Replay buttons at the top left.
- 2: Adapter List table showing network adapters like Wi-Fi, Microsoft, Ethernet 2, and Wireless Monitor Adapter(s).
- 3: Adapter Status graph showing real-time traffic for the selected Wi-Fi adapter.
- 4: Analysis Profile section with various analysis modules like Full Analysis, Traffic Monitor, Security Analysis, etc.
- 5: Network Profile and Analysis Profile details on the right sidebar.

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

	Name	Signal	Encryption Key	Media	Channel	MAC Address	Encryption Type
<input type="checkbox"/>	Pang	📶	N/A	802.11n	1	CC:4E:EC:36:AD:D8	wpa/wpa2
<input type="checkbox"/>	Pewpai	📶	N/A	802.11n	1	00:30:0D:B3:70:F7	wpa/wpa2
<input type="checkbox"/>	yumzap	📶	N/A	802.11n	1	20:25:64:14:09:70	wpa/wpa2
<input checked="" type="checkbox"/>	ICT FREE WIFI	📶	N/A	802.11n	1	0C:54:A5:C3:9F:FF	wep

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

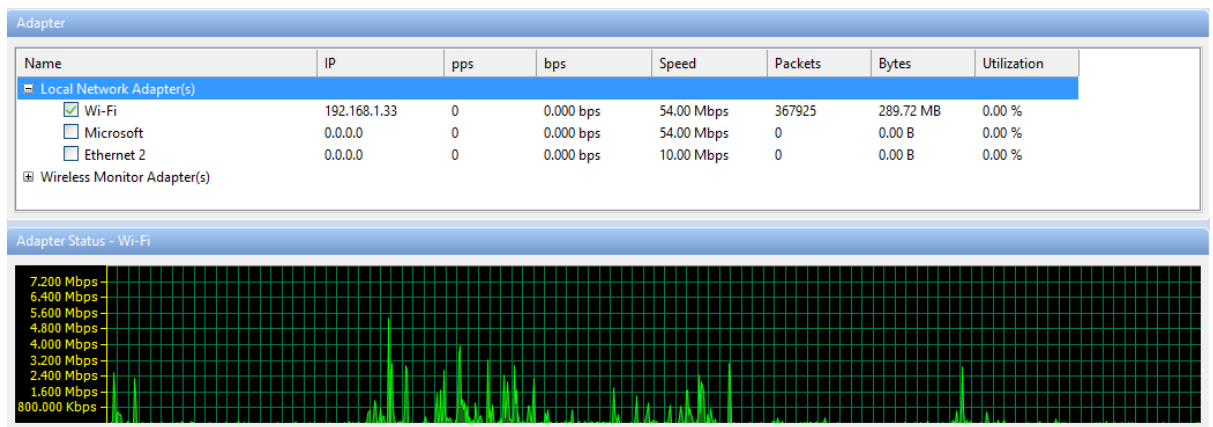
## การใช้งานโปรแกรมแบบ Capture

การเริ่มต้นใช้งาน โปรแกรมแบบ Local Network Adapter

1. เลือก Capture tab ที่อยู่ในส่วน Analysis Mode Tabs



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



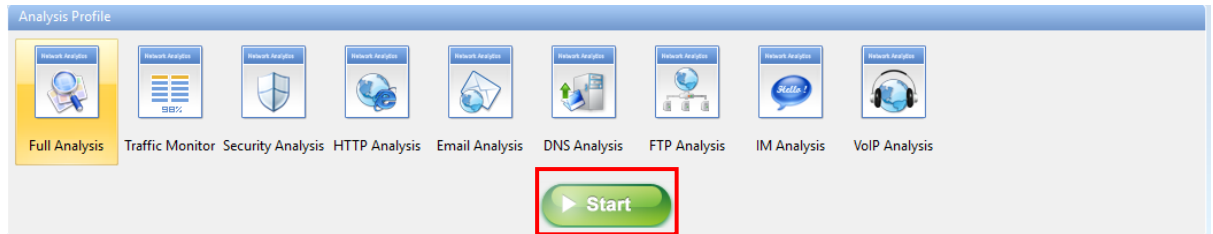
3. เลือกเครื่องมือที่จะใช้ในการวิเคราะห์ที่อยู่ในส่วน Analysis Profile ซึ่งจะมีดังนี้
  - 3.1 Full Analysis เป็นการวิเคราะห์แบบครอบคลุมการใช้งานทั้งหมด
  - 3.2 Traffic Monitor มีแสดง traffic เชิงสถิติและวิเคราะห์ประสิทธิภาพของอ็อบเจกต์หลัก รวมไปถึง MAC Address, IP Address และ Protocol
  - 3.3 Security Analysis เป็นการวิเคราะห์ความเสี่ยงโดยเฉพาะศักยภาพในความปลอดภัยของเครือข่าย
  - 3.4 HTTP Analysis วิเคราะห์การใช้งานบนเว็บแอปพลิเคชัน (รูปแบบของ HTTP)
  - 3.5 Email Analysis วิเคราะห์การใช้งานอีเมล (รูปแบบของ POP3 และ SMTP) และตรวจสอบเนื้อหาและสิ่งที่แนบมากับอีเมล
  - 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

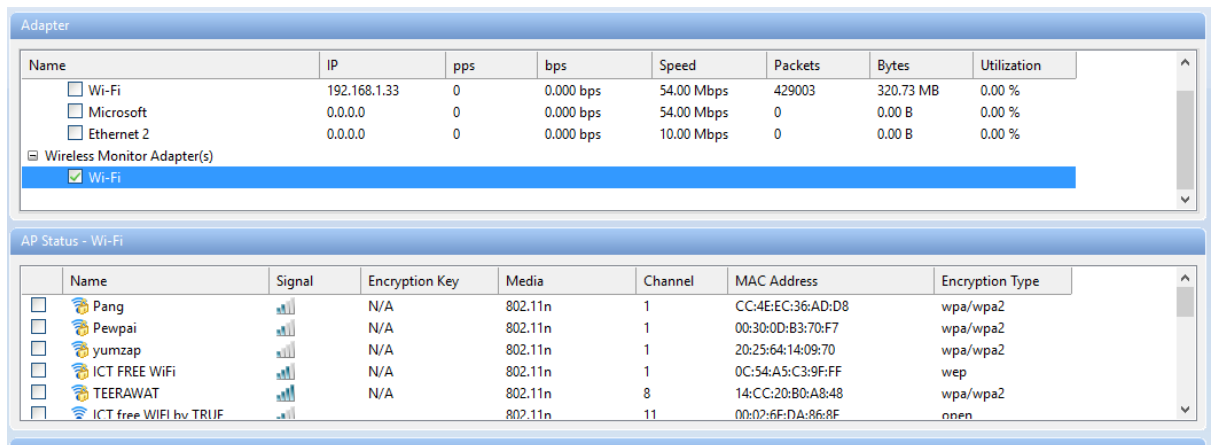


การเริ่มต้นใช้งาน โปรแกรมแบบ Wireless Network Adapters

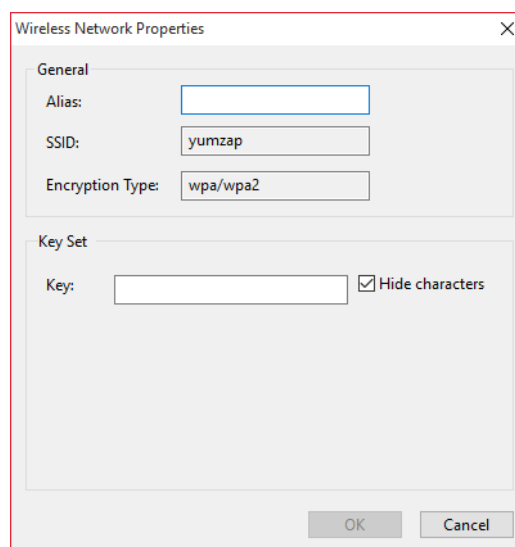
1. เลือก Capture tab ที่อยู่ในส่วน Analysis Mode Tabs



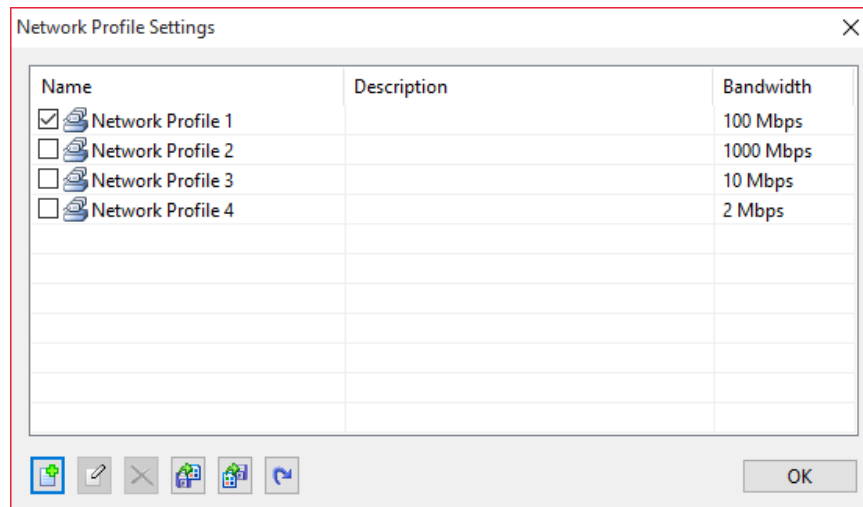
2. เลือก wireless network adapter ที่อยู่ในส่วน Adapter List ซึ่งจะแสดง Aps ที่มีอยู่ทั้งหมด



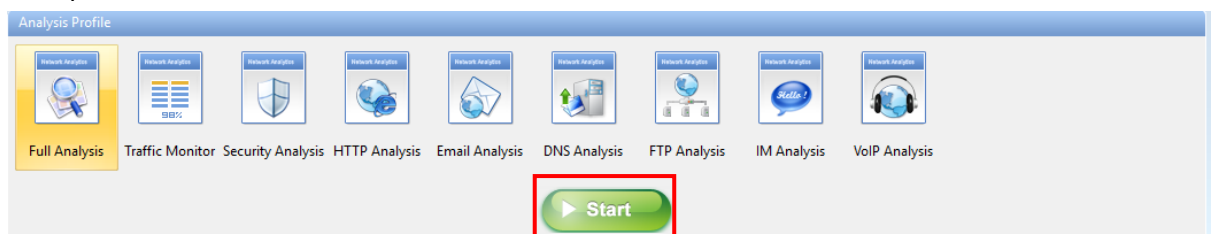
3. เลือก AP ที่ต้องการ โดยระบบจะมีการถามรหัส นอกจากนี้สามารถเลือก AP ได้มากกว่าหนึ่ง



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 เิงสถิติและวิเคราะห์ประสิทธิภาพของอ็อบเจกต์หลัก รวมไปถึง MAC Address, IP Address และ Protocol
  - 5.3. Security Analysis เป็นการวิเคราะห์ความเสี่ยง โดยเฉพาะศักยภาพในความปลอดภัยของเครือข่าย
  - 5.4. HTTP Analysis วิเคราะห์การใช้งานบนเว็บแอปพลิเคชัน (รูปแบบของ HTTP)
  - 5.5. Email Analysis วิเคราะห์การใช้งานอีเมล (รูปแบบของ POP3 และ SMTP) และตรวจสอบเนื้อหาและสิ่งที่แนบมากับอีเมล
  - 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

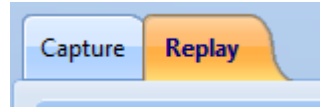


## การใช้งานโปรแกรมแบบ Replay

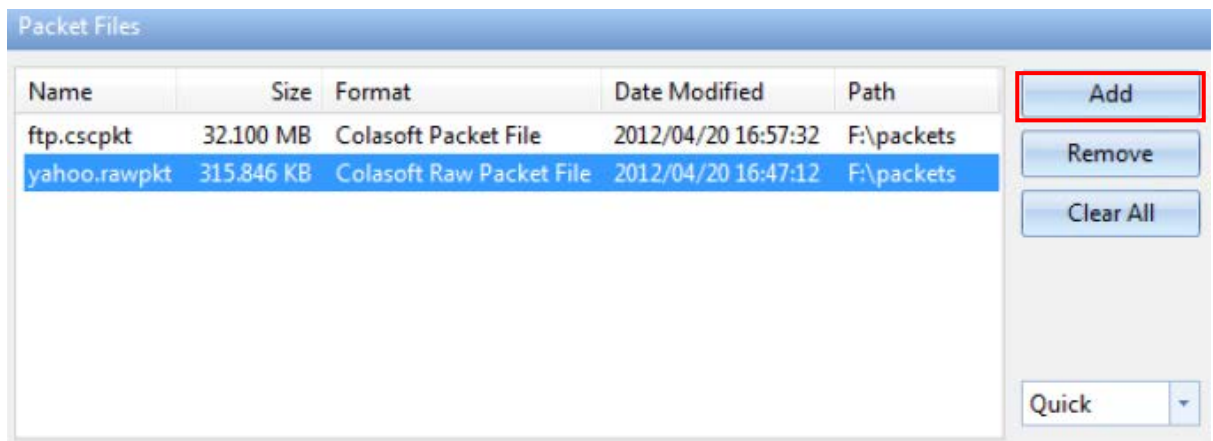
Capsa ไม่ได้ใช้ในการวิเคราะห์แบบ real-time เพียงอย่างเดียว แต่ยังสามารถนำแพ็คเก็ตที่ต้องการมาวิเคราะห์ได้

ขั้นตอนการใช้งานดังนี้

1. เลือกแท็บ Replay ที่อยู่ในส่วน Analysis Mode



2. เพิ่มไฟล์ packet จากในส่วนของ Packet Files ซึ่งมีรายละเอียดดังนี้



- 2.1. Add เป็นการเพิ่มไฟล์ที่มีการเก็บแพ็คเก็ตย้อนหลัง โดยจะมีเวลาประทับไว้ในไฟล์แพ็คเก็ตนั้น

- 2.2. Remove เป็นการลบไฟล์แพ็คเก็ตที่เลือกไว้

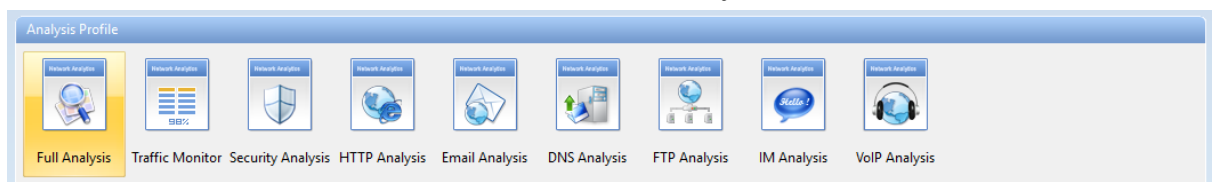
- 2.3. Clear All ลบไฟล์แพ็คเก็ตในลิสต์ทั้งหมด

- 2.4. Replay Speed เป็นการกำหนดความเร็ว

2.4.1. Quick จะทำการเล่นแพ็คเก็ตย้อนหลังอย่างรวดเร็ว

2.4.2. Normal แพ็คเก็ตจะย้อนหลังอย่างช้า แต่ได้รายละเอียดที่ถูกต้อง

3. เลือกเครื่องมือที่ต้องการที่จะใช้ในการวิเคราะห์ให้เหมาะสมที่อยู่ในส่วนของ Analysis Profile

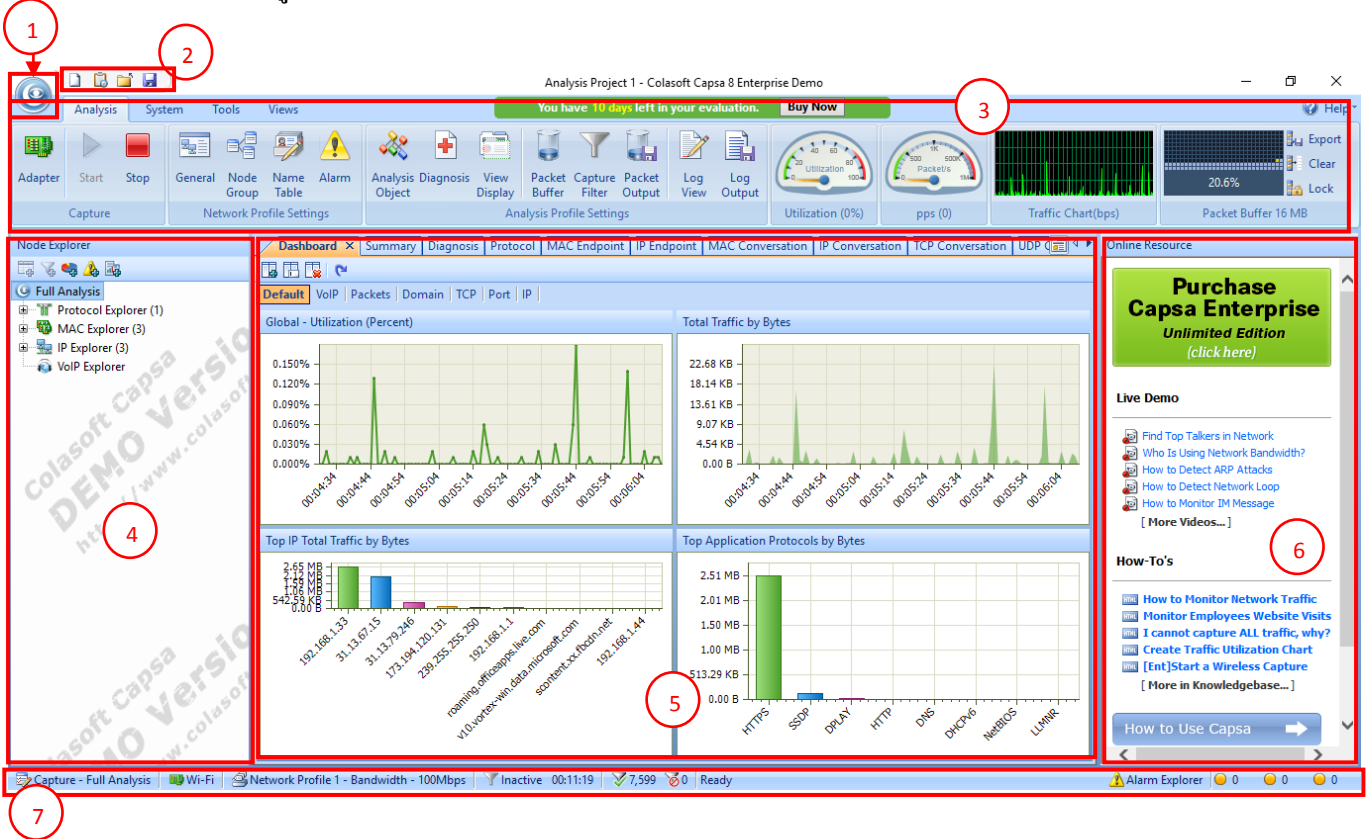


4. คลิกปุ่ม Start เพื่อทำการเริ่มวิเคราะห์



## Main User Interface

หลังจากที่เริ่มต้นในการวิเคราะห์โปรเจกต์ ไม่ว่าจะเลือกแบบ real-time capturing หรือ replaying packets ก็จะเข้าสู่หน้าการใช้งานที่เหมือนกัน ซึ่งจะแสดงให้เห็นสถิติและเครือข่ายเน็ตเวิร์ค ในส่วนหน้าต่าง การใช้งานแบ่งออกเป็นอยู่ 7 ส่วน ดังนี้



1. Menu button เป็นปุ่มเมนูที่อยู่มุมบนซ้ายของหน้าต่างการใช้งาน โดยมีลิสต์รายการดังนี้
  - 1.1. New เป็นการสร้างโปรเจกต์การวิเคราะห์ใหม่
  - 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 เป็นข้อมูลของผลิตภัณฑ์
    - 1.6.1. Product License เป็นการต่ออายุใบอนุญาต
    - 1.6.2. Check Update ตรวจสอบเวอร์ชันของโปรแกรม

1.6.3. About เป็นการอธิบายลิขสิทธิ์และข้อมูลของใบอนุญาตของผลิตภัณฑ์


1.7. Close เป็นคำสั่งในการปิดโปรเจกต์และกลับไปยังหน้าเริ่มต้น

1.8. Recent Files แสดงรายการที่เคยทำการเปิดไฟล์แฟ้มที่

1.9. Options เป็นการกำหนดการตั้งค่าของโปรเจกต์ที่ใช้ในการวิเคราะห์


1.10. Exit ออกจากโปรแกรม

2. Quick Access Icons มีไอคอนดังนี้

2.1.  ไอคอนสำหรับการสร้างโปรเจกต์การวิเคราะห์ใหม่

2.2.  ไอคอนในการกำหนดเวลาการทำงาน

2.3.  ไอคอนเพื่อกลับไปยังหน้าเริ่มต้น

2.4.  ไอคอนสำหรับการบันทึกแฟ้มที่แฟ้มที่ 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).

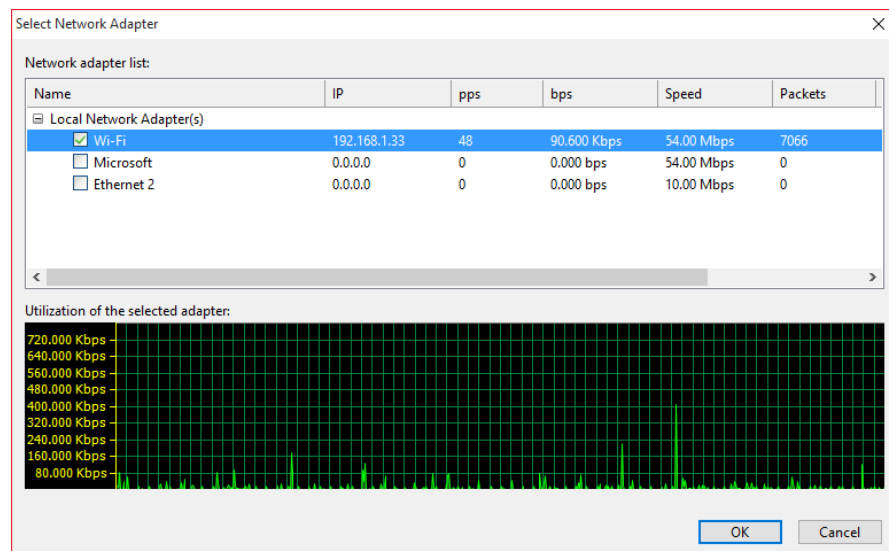
3. Ribbon ซึ่งแบ่งออกเป็น 4 ส่วนดังนี้

3.1. Analysis เป็นการตั้งค่าสำหรับการวิเคราะห์ ประกอบไปด้วย



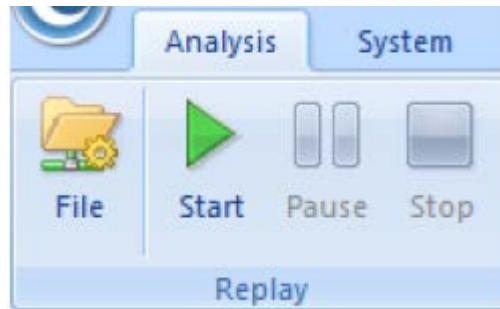
3.1.1. ในกรณีส่วนของฟังก์ชัน Capture

- Adapter สามารถเลือกหรือเปลี่ยนแปลง Network Adapter เพื่อใช้ในการวิเคราะห์



- Start เริ่มการวินิจฉัยแพ็คเก็ต
- Stop สิ้นการวินิจฉัยแพ็คเก็ต

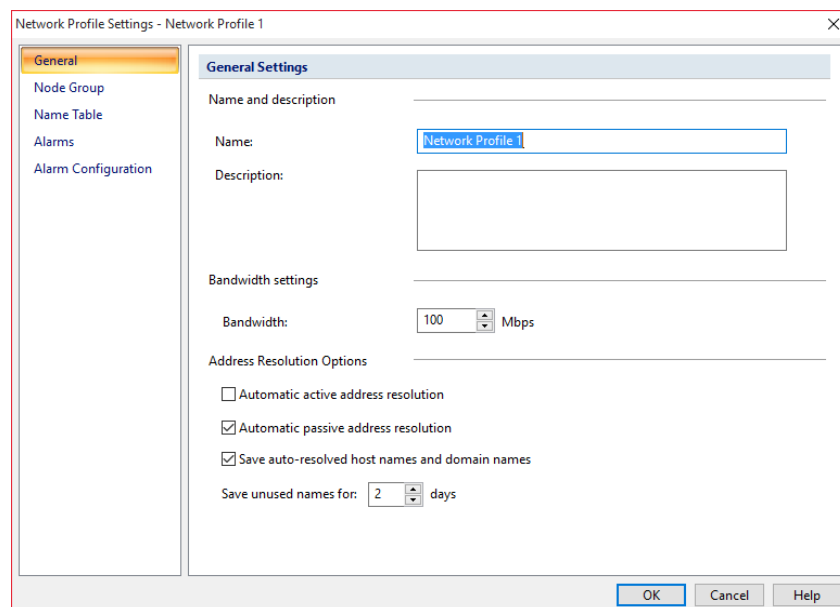
### 3.1.2. ในกรณีส่วนของฟังก์ชัน Replay



- File เป็นการเปิดการจัดการหรือเปลี่ยนแปลงไฟล์แพ็คเก็ตใหม่
- Start เริ่มการวินิจฉัยแพ็คเก็ต
- Pause หยุดการวินิจฉัยแพ็คเก็ตชั่วคราว
- Stop สิ้นการวินิจฉัยแพ็คเก็ต

### 3.1.3. Network Profile Settings เป็นการตั้งค่าพารามิเตอร์สำหรับ Network Profile โดยมีอยู่ 4 ส่วนดังนี้

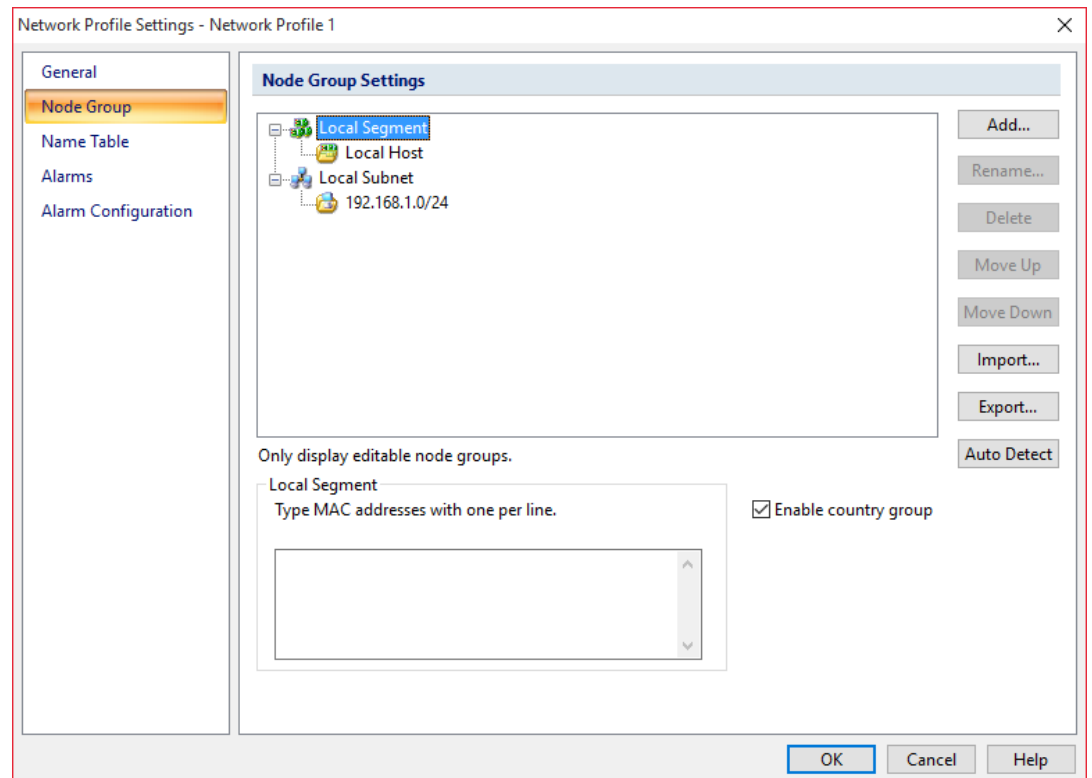
#### 3.1.3.1. General ซึ่งมีรายละเอียดดังนี้



- 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

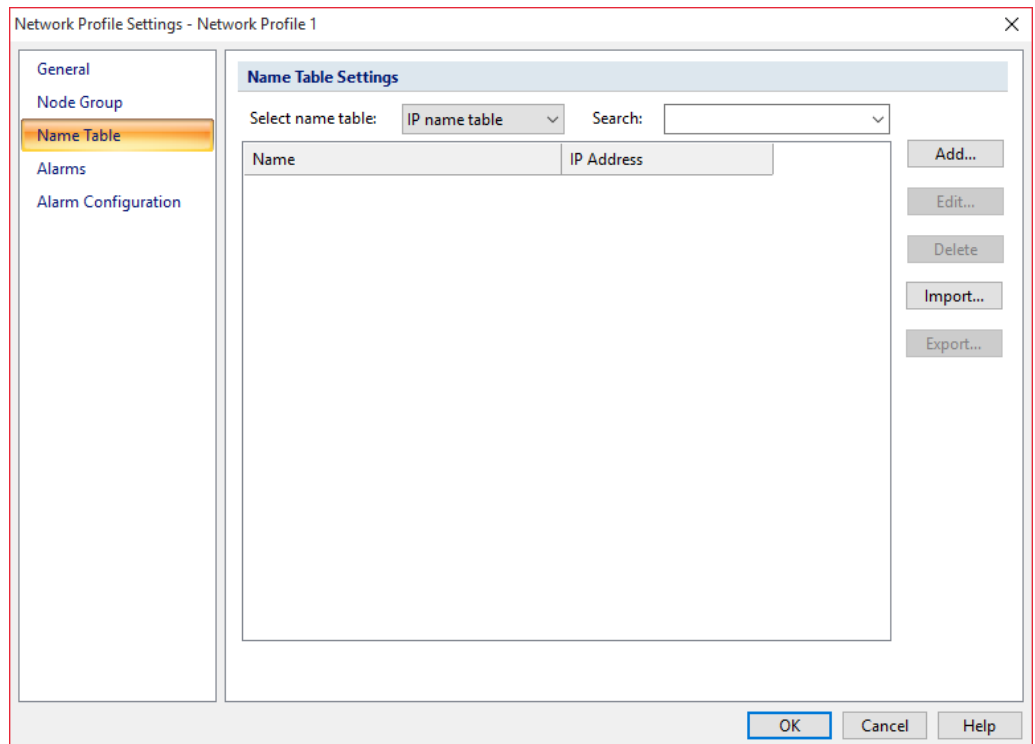


### 3.1.3.2. Node Group เป็นกลุ่มที่ถูกนำมาใช้ในการจัดการ MAC และ IP Address ของ เครือข่าย

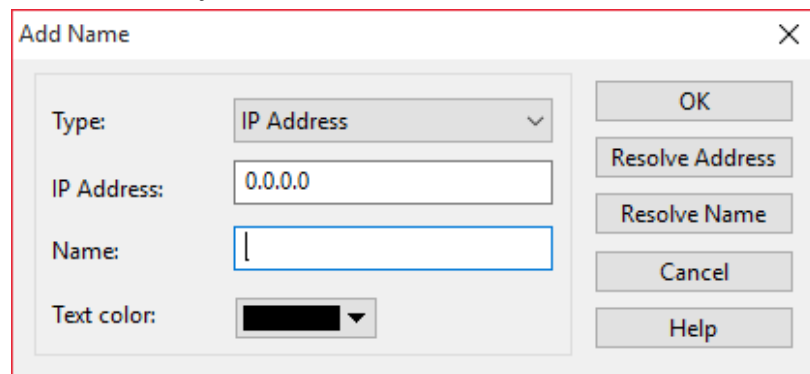


- Add เป็นการเพิ่มโหนดใหม่ในกลุ่มโหนดที่เลือกไว้
- Rename แก้ไขชื่อของกลุ่มโหนดที่เลือกไว้
- Delete ลบกลุ่มโหนดที่เลือกไว้
- Move Up การย้ายกลุ่มโหนดขึ้นมา
- Move Down การย้ายกลุ่มโหนดลงมา
- Import การนำไฟล์ .cscng เข้าในรายการ
- Export การบันทึกไฟล์เป็น .cscng
- Auto Detect ตรวจสอบกลุ่มของ MAC Address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

### 3.1.3.3. Name Table เป็นการจัดการ MAC และ IP Address ที่สามารถใช้ในการวิเคราะห์

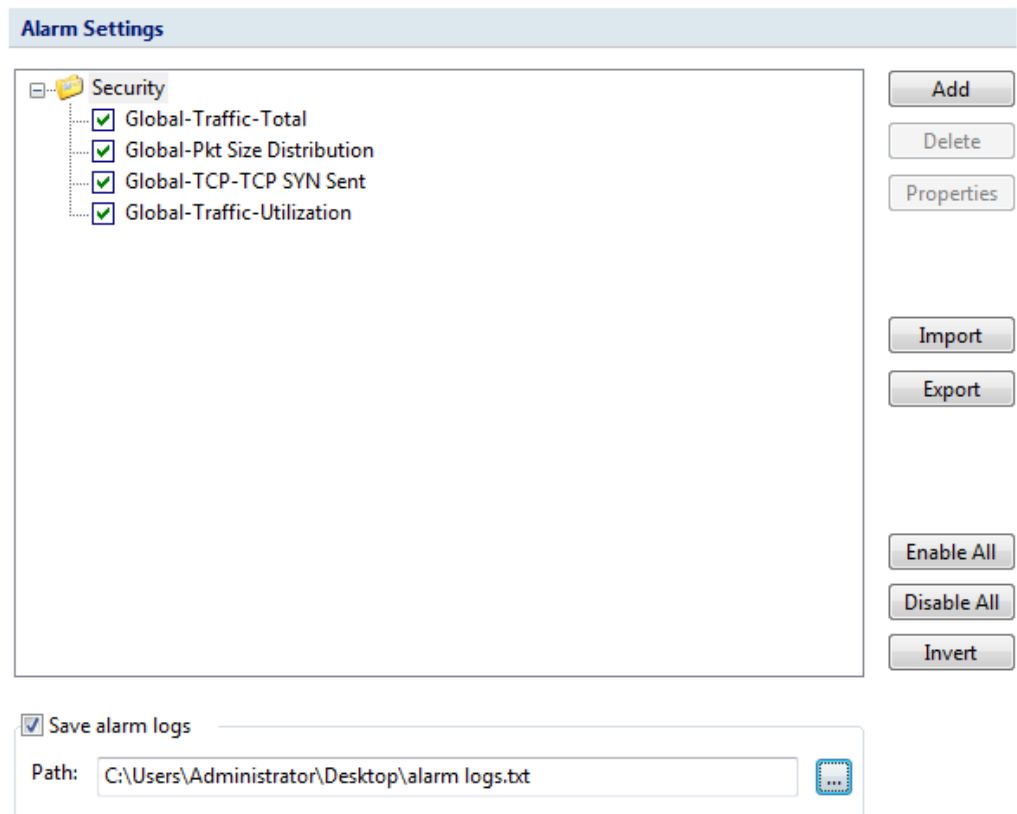


- Add เพิ่มชื่อและที่อยู่



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

### 3.1.3.4. Alarm Settings เป็นการตั้งค่าในการเตือนภัยภายในเครือข่าย

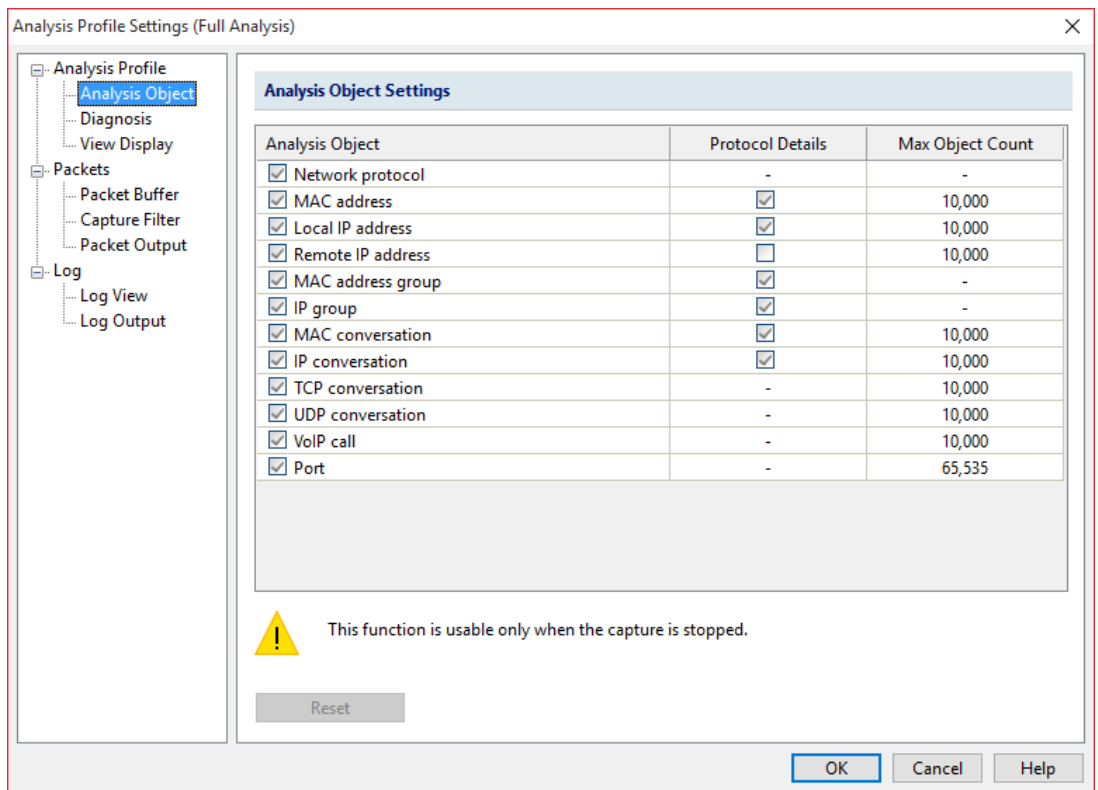


- Add สร้างการแจ้งเตือนภัย
- Delete ลบการแจ้งเตือนภัยที่เลือกไว้ในรายการ
- Properties ปรับเปลี่ยนคุณสมบัติของการเตือนภัยที่เลือก
- Import โหลดการแจ้งเตือนภัย โดยจะต้องเป็นนามสกุลไฟล์ .csalarm
- Export บันทึกการแจ้งเตือนภัย โดยจะต้องเป็นนามสกุลไฟล์ .csalarm
- Enable All เลือกการเตือนภัยทั้งหมด
- Disable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

### 3.1.3.5. Alarm Configuration เป็นการตั้งค่าการแจ้งเตือนผ่านอีเมลและการตั้งค่าเสียงการแจ้งเตือน

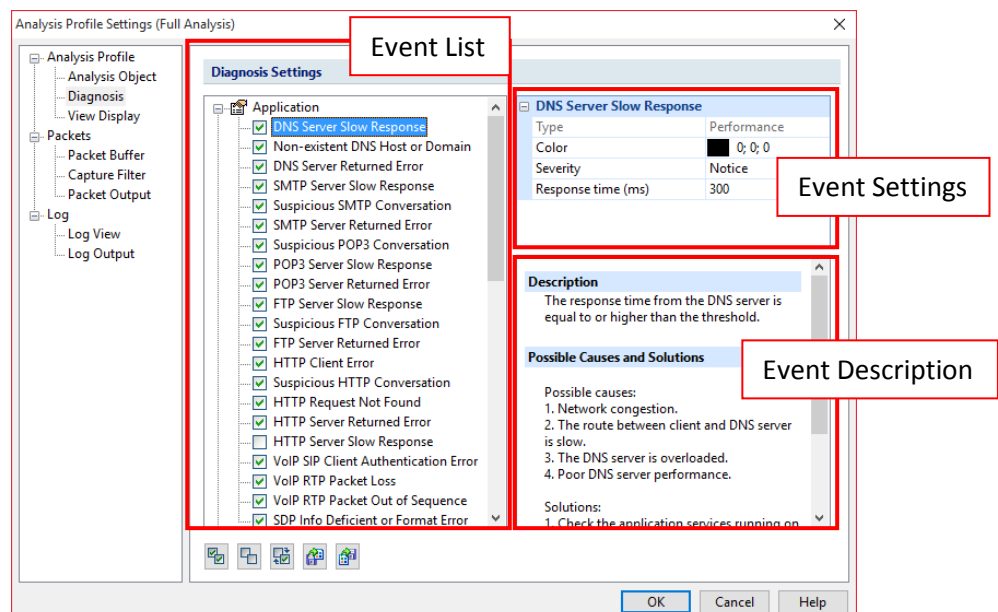
- Address อีเมลที่จะทำการส่ง
- Your name ชื่อผู้ส่ง
- User name อีเมลที่ใช้งาน โดยจะมีการเชื่อมต่อเมลเซิร์ฟเวอร์
- Password รหัสผ่านอีเมลที่ใช้งาน
- Subject ชื่อเรื่องที่ต้องการแจ้งเตือน
- Recipients ผู้รับอีเมลสำหรับการแจ้งเตือน โดยสามารถแจ้งเตือนกันได้หลายอีเมล โดยใช้สัญลักษณ์ “;” คั่น
- Email server ที่อยู่ของเมลเซิร์ฟเวอร์
- Encryption ประเภทการเชื่อมต่อของเมลเซิร์ฟเวอร์
- Port หมายเลขพอร์ตที่ใช้ในการเชื่อมต่อกับเมลเซิร์ฟเวอร์
- Sound notification เป็นการตั้งค่าเสียงที่ใช้ในการเตือนภัย






### 3.1.4. Analysis Profile เป็นการตั้งค่าการวิเคราะห์ซึ่งสามารถปรับเปลี่ยนการวิเคราะห์ได้



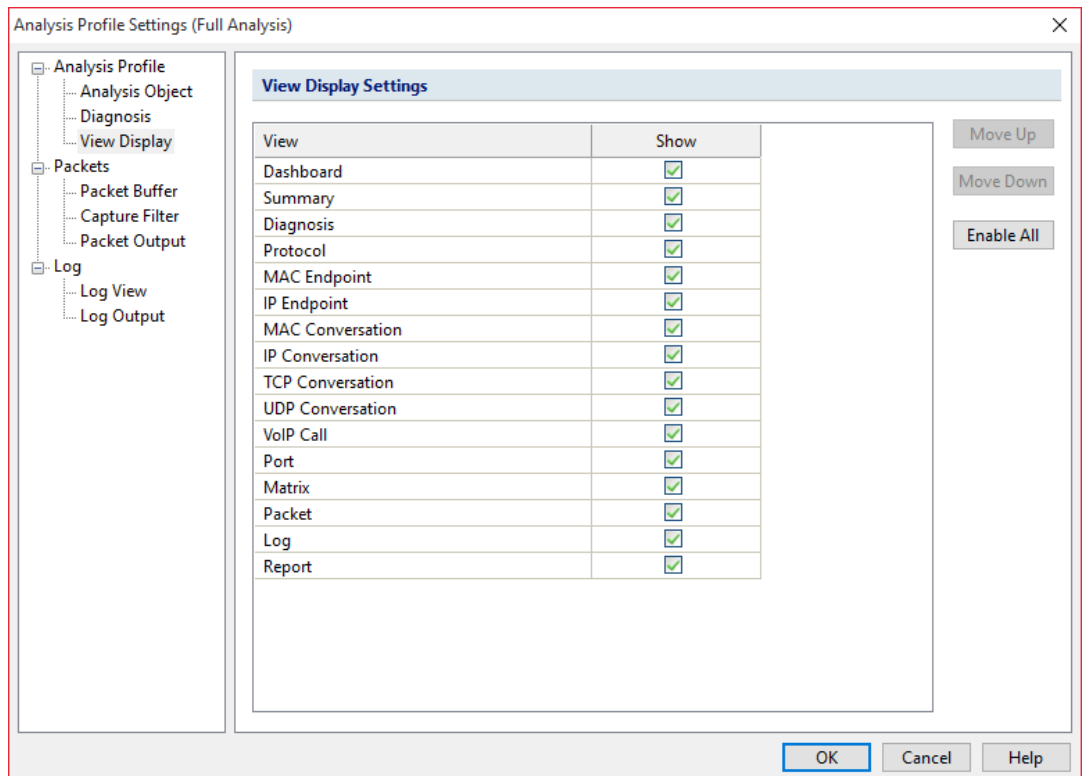
- Analysis Object เป็นส่วนของเน็ตเวิร์ก โปรโตคอล
- Protocol Details การตั้งค่าการแสดงผลของข้อมูล traffic
- Max Object Count จำนวนในการวิเคราะห์ในแต่ละครั้ง โดยจะเริ่มต้นตั้งแต่ 1 ถึง 10,000 เท่านั้น

### 3.1.5. Diagnosis เป็นแท็บในการแสดงเหตุการณ์ของการวินิจฉัยที่มีอยู่ทั้งหมดในโมดูลของการวิเคราะห์เหตุการณ์ในปัจจุบัน ซึ่งเหตุการณ์การวินิจฉัยทั้งหมดจะถูกแบ่งออกเป็นลำดับชั้นโปรโตคอล

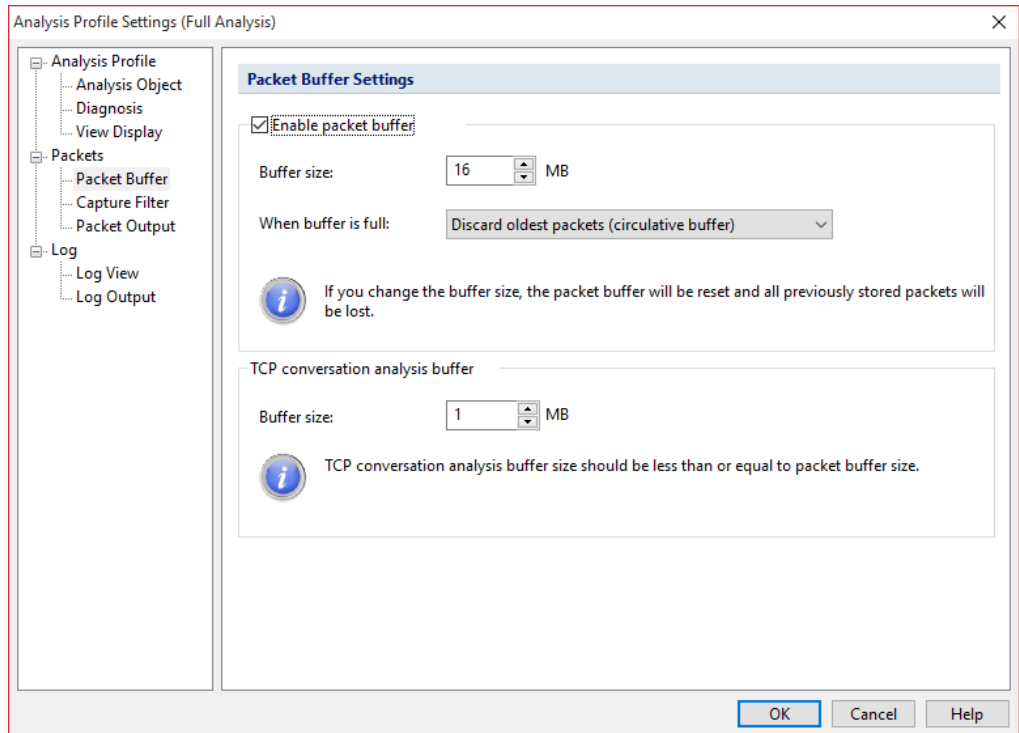


- Event List รายการทั้งหมดของการวินิจฉัยที่มีอยู่ในปัจจุบัน
- Event Setting สามารถเลือกในการแก้ไขเหตุการณ์ในส่วนของรายชื่อที่แสดงอยู่ใน Event List
- Event Description เป็นส่วนในการอธิบายของแต่ละเหตุการณ์และรายละเอียดของเครือข่าย
  -  เลือกเหตุการณ์ที่เกิดขึ้นทั้งหมด
  -  ไม่เลือกเหตุการณ์ที่เกิดขึ้นทั้งหมด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

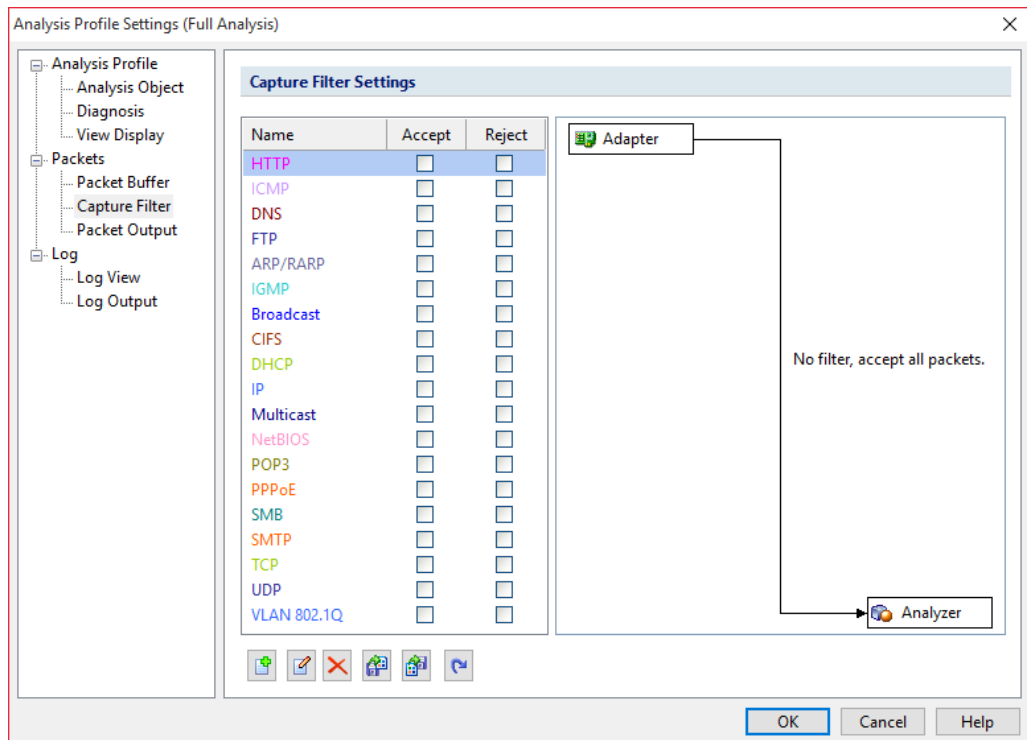
### 3.1.6. View Display เป็นการปรับเปลี่ยนมุมมองที่แสดงทางสถิติของการวิเคราะห์



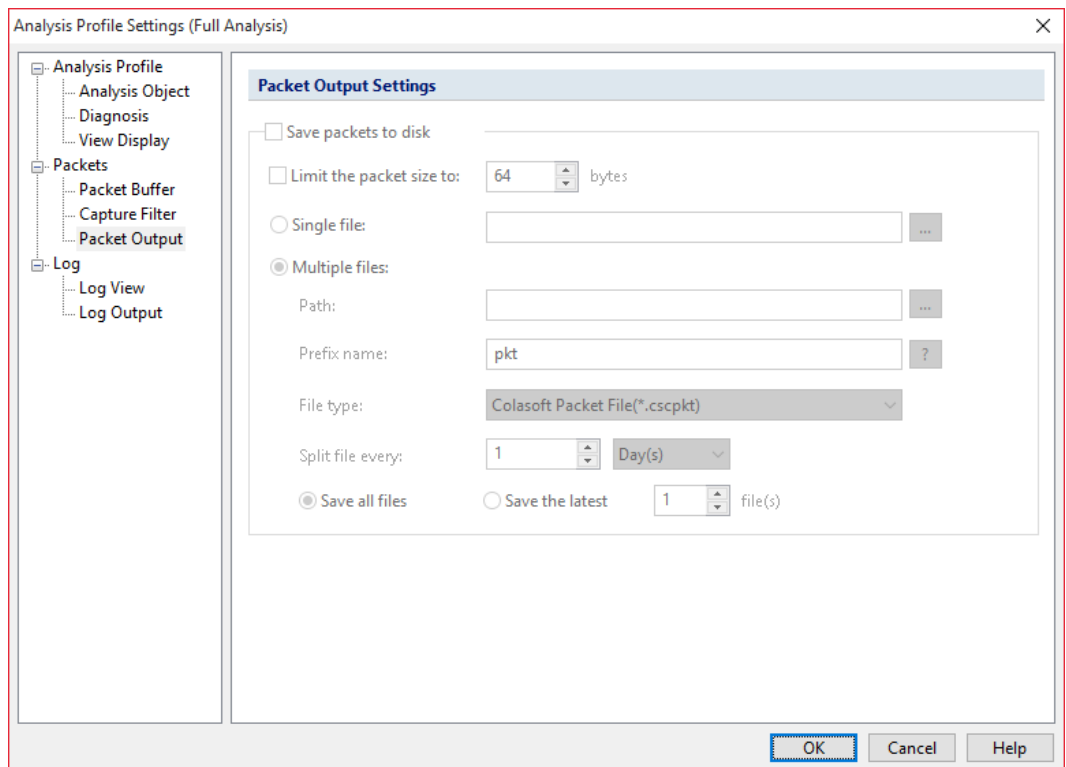
3.1.7. Packet Buffer เป็นการแสดงแพ็คเก็ตทั้งหมดที่ถูกเก็บไว้ในแพ็คเก็ตบัฟเฟอร์ ดังนั้นขนาดของบัฟเฟอร์จะช่วยให้การวิเคราะห์ได้



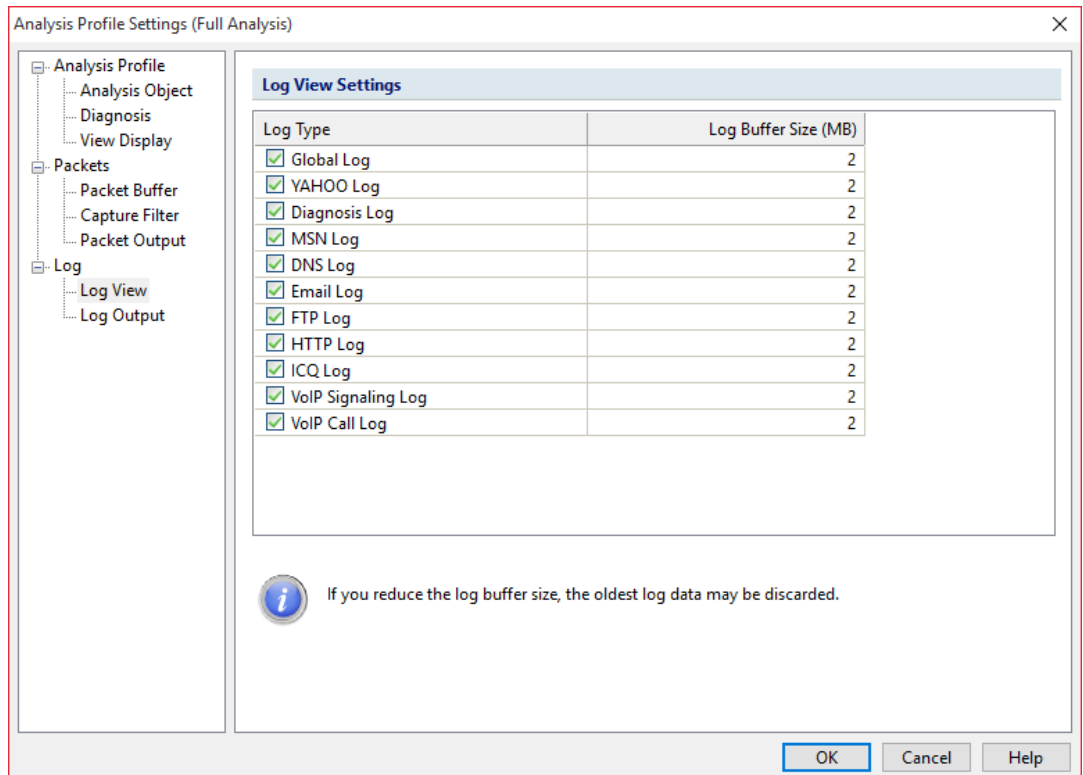
3.1.8. Capture Filter แท็บนี้มีไว้สำหรับการตั้งค่าและเป็นตัวตรวจสอบข้อมูล โดยจะวิเคราะห์แพ็คเก็ตทั้งหมดที่ส่งผ่านอะแดปเตอร์



### 3.1.9. Packet Output เป็นส่วนในการบันทึกแพ็คเกจที่ใช้ในการวิเคราะห์อัตโนมัติ

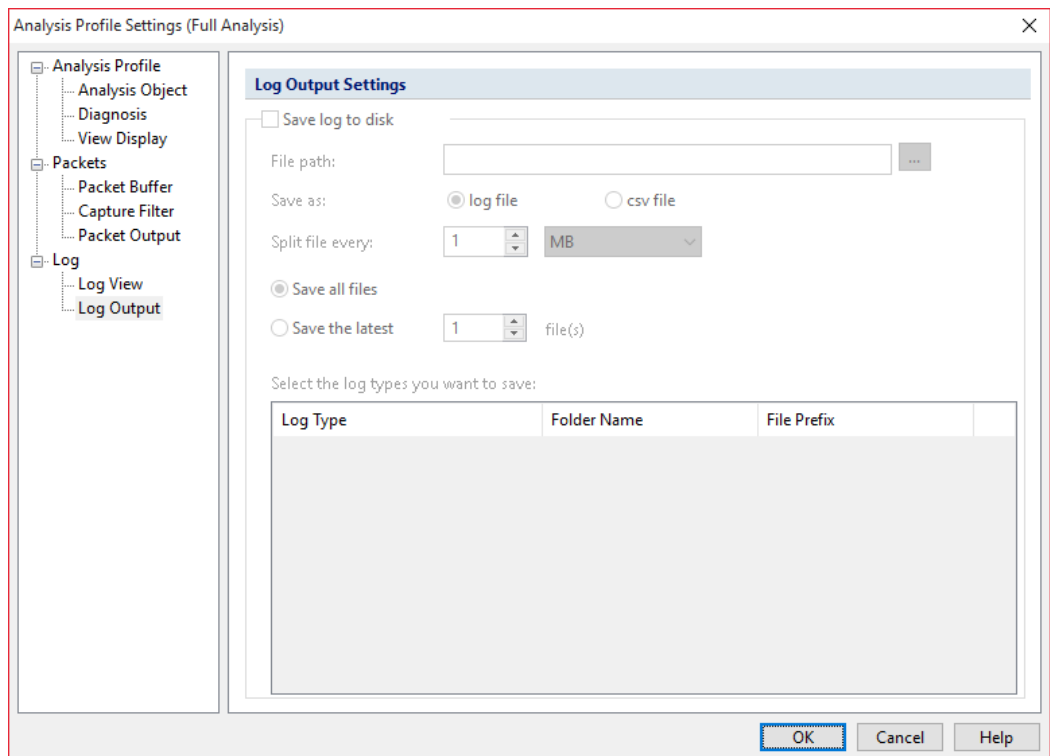


### 3.1.10. Log View การวิเคราะห์และใช้งาน traffic เช่น DNS, HTTP, Email, FTP และการสนทนาของ MSN กับ Yahoo

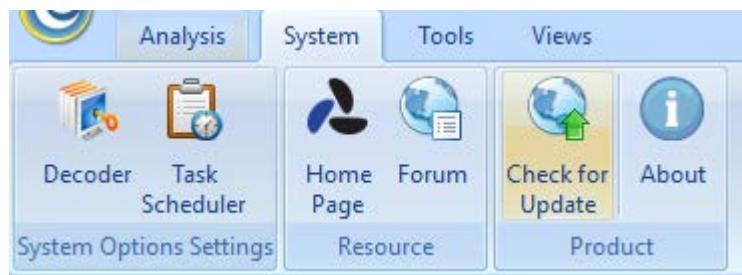




### 3.1.11. Log Output เป็นการบันทึกข้อมูลของแพ็คเก็ตในส่วนของ Log View อัตโนมัติ

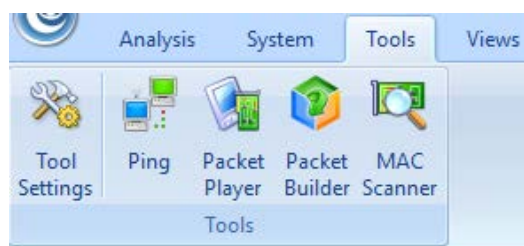


### 3.2. System ประกอบไปด้วยส่วนของสินค้าและการจัดการทรัพยากร

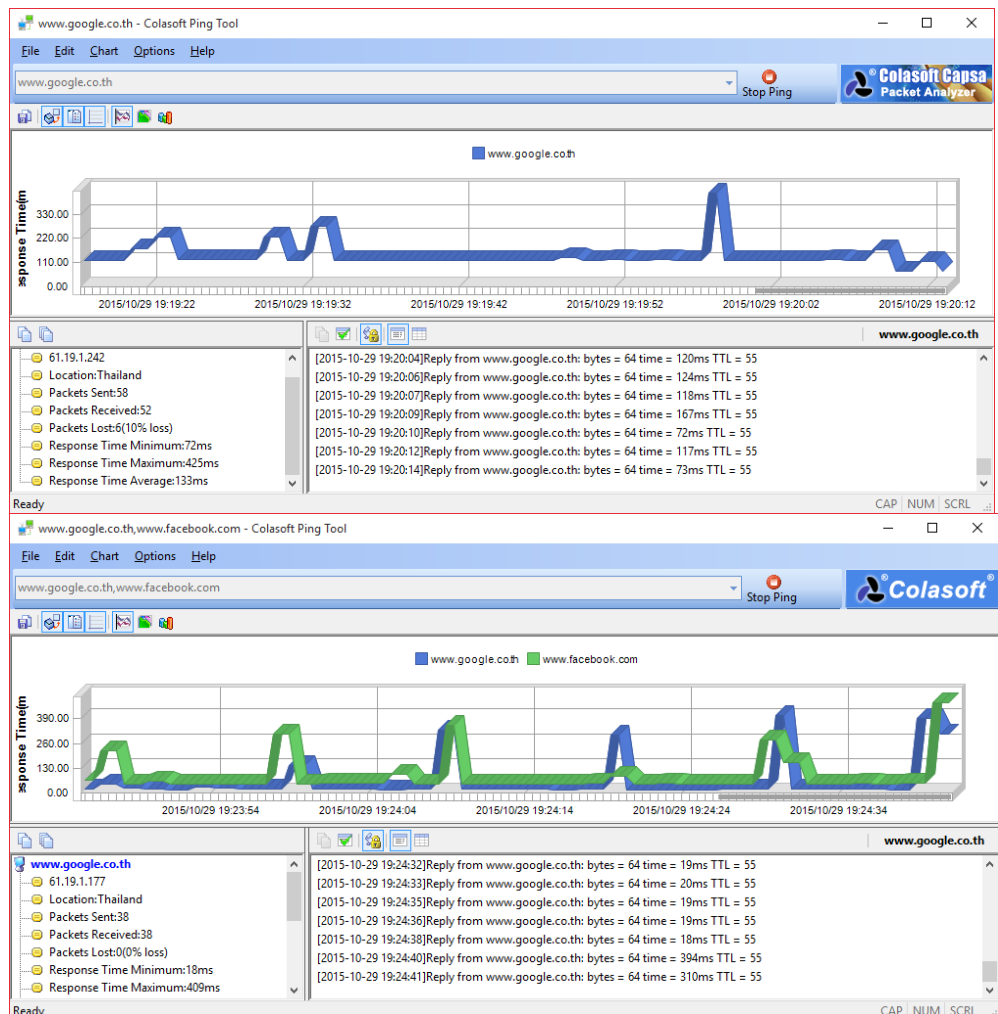


- Decoder เป็นส่วนในการตั้งค่าของโปรโตคอล
- Task Scheduler การกำหนดช่วงเวลาในการทำงาน ซึ่งสามารถทำการเพิ่มงานเข้าไปได้ ใช้ได้เฉพาะ Capsa แบบ Enterprise เท่านั้น
- Home Page ไปยังหน้าเพจของเว็บไซต์ Colasoft
- Forum ไปฟอรัมของ Colasoft
- Check for Update ตรวจสอบเวอร์ชันของผลิตภัณฑ์
- About เป็นการอธิบายลิขสิทธิ์และข้อมูลของใบอนุญาตของผลิตภัณฑ์

### 3.3. Tools เป็นเครือข่ายสำหรับเครือข่าย

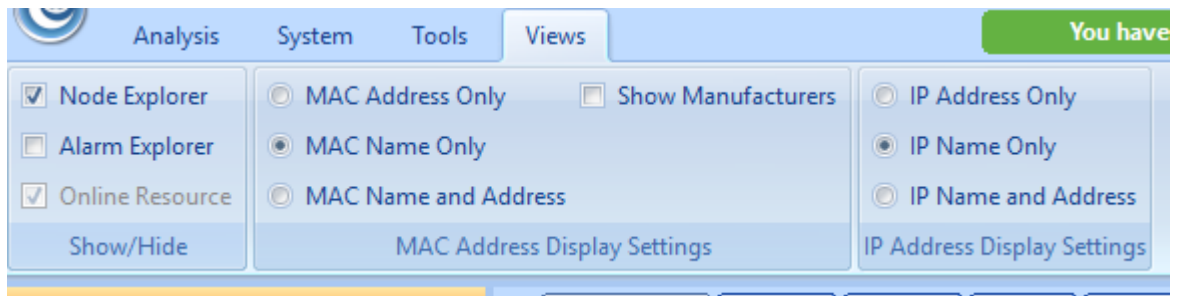







- Tool Settings เป็นเครื่องมือที่ใช้ในการตั้งค่าการจัดการ ซึ่งในระบบจะมีอยู่ 4 อย่างด้วยกัน คือ Ping, Packet Player, Packet Builder และ MAC Scanner
- Ping Tool เป็นเครื่องมือที่ใช้ในการ ping ที่มีประสิทธิภาพโดยมีการแสดงรูปแบบกราฟเพื่อให้เห็นการเปรียบเทียบเวลาในการตอบสนองและยังสามารถเปรียบเทียบการ ping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



- Packet Player การนำแพ็คเก็ตมาทำการเล่นซ้ำ โดยสามารถเปิดไฟล์แพ็คเก็ตจากการเซฟเป็นนามสกุลไฟล์ .cscpkc
- Packet Builder เป็นเครื่องมือที่มีประโยชน์ที่ใช้สำหรับการสร้างแพ็คเก็ตเครือข่ายซึ่งสามารถกำหนดคุณสมบัติได้ด้วยตนเองและยังป้องกันการโจมตีจากเครือข่าย
- MAC Scanner เป็นเครื่องมือที่ใช้ในการสแกน MAC Address และ IP Address ในเครือข่าย

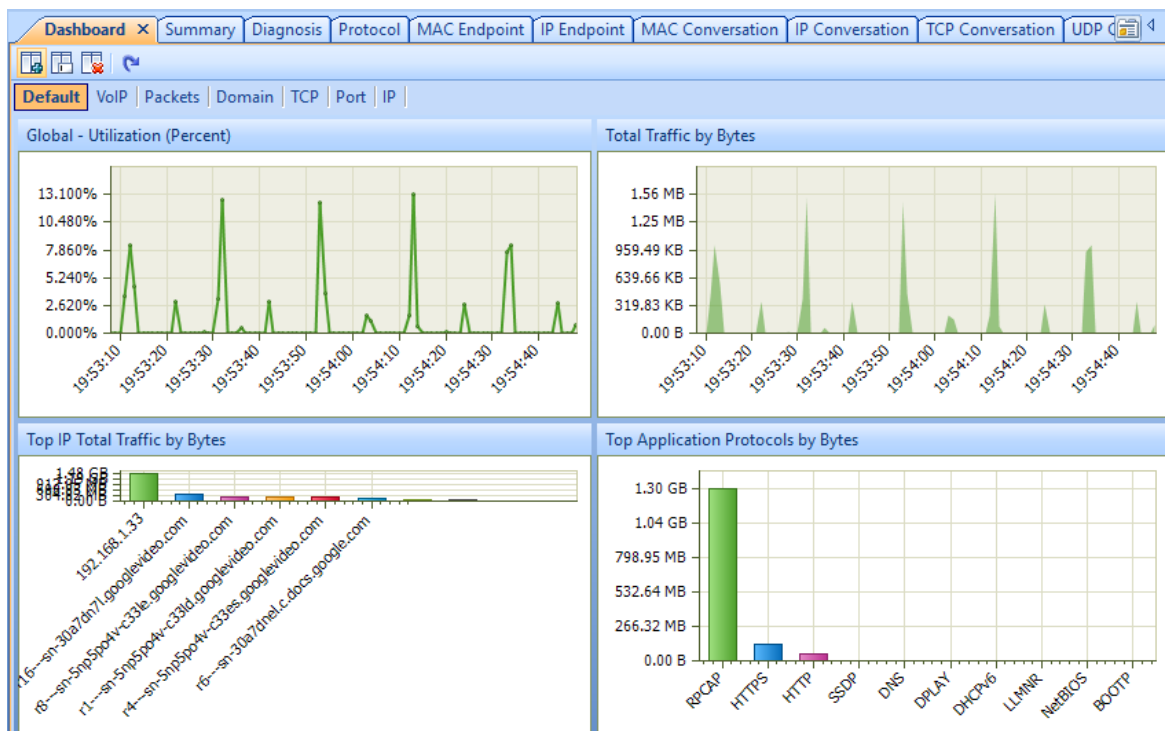
### 3.4. View เป็นการกำหนดค่าของการแสดงผลของโปรแกรม



- Show/Hide เป็นการกำหนดการแสดงผลหน้าต่างของ 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
-  เป็นการเพิ่ม โหนด Name Table
  -  สร้างการ filters จากโหนดที่เลือกไว้ในรายการ
  -  สร้างกราฟจากโหนดที่เลือกไว้ในรายการ
  -  สร้างการแจ้งเตือนภัยจากโหนดที่เลือกไว้ในรายการ
  -  สรุปรายงานจากโหนดที่เลือกไว้ในรายการ
5. Statistical views เป็นหน้าต่างการแสดงผลทรัพยากรแบบออนไลน์ ซึ่งจะมีการแสดงผลเชิงสถิติและกราฟ ส่วนแรกจะเป็นในส่วนของ summary ซึ่งจะสรุปภาพรวมในเครือข่ายปัจจุบัน ซึ่งจะบอกข้อมูลคร่าวๆในเครือข่าย เช่น จำนวน traffic, ขนาดของ packet, จำนวน protocol, รูปแบบการสื่อสาร

Full Analysis/Statistics: 70					
Statistics Item	Current Value				
<b>Diagnosis</b>					
Information Events	Count: 157				
Notice Events	Count: 636				
Warning Events	Count: 1,628				
Error Events	Count: 0				
<b>Traffic</b>					
Total	Bytes: 1.58 GB	Packets: 1,896,915	Utilization: 10.868%	bps: 10.868 Mbps	pps: 1,427
Broadcast	2.50 MB	40,525	0.000%	0.000 bps	0
Multicast	1.74 MB	6,907	0.000%	0.000 bps	0
Average Packet Size	892.000 Bytes				
<b>Pkt Size Distribution</b>					
<=64	Bytes: 5.74 MB	Packets: 99,666	Utilization: 0.001%	bps: 928.000 bps	pps: 2
65-127	50.35 MB	596,292	0.361%	361.384 Kbps	482
128-255	2.77 MB	17,546	0.001%	1.104 Kbps	1
256-511	5.83 MB	17,045	0.007%	6.568 Kbps	2
512-1023	13.46 MB	18,020	0.000%	0.000 bps	0
1024-1517	1.39 GB	1,071,764	10.486%	10.486 Mbps	939
>=1518	110.87 MB	76,582	0.012%	12.144 Kbps	1
<b>Address</b>					
MAC Address	Count: 21				
IP Address	Count: 710				
Local IP Address	Count: 13				
Remote IP Address	Count: 697				
<b>Protocol</b>					
	Count				

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



หน้าแสดง Diagnosis จะเป็นการแสดงข้อมูลของเหตุการณ์ต่าง ๆ ที่เกิดขึ้นในเน็ตเวิร์ค ทั้งหมด โดยแบ่งตามลำดับชั้นของเน็ตเวิร์ค ทำให้ง่ายต่อการค้นหาปัญหาเหตุการณ์ต่าง ๆ ในเน็ตเวิร์ค

The screenshot shows the 'Diagnosis' tab in NetworkMiner. It displays a list of events categorized by layer (Application, Transport, Network). The 'Details' section for IP 10.3.0.1 shows four fault events related to TCP connection attempts.

Severity	Type	Layer	Event Summary	Source IP Address	Sc
🚩	Fault	Transport	Repeated attempt to establish TCP connection (see packet 908279).	192.168.1.33	E0
🚩	Fault	Transport	Repeated attempt to establish TCP connection (see packet 908342).	192.168.1.33	E0
🚩	Fault	Transport	Repeated attempt to establish TCP connection (see packet 908608).	192.168.1.33	E0
🚩	Fault	Transport	Repeated attempt to establish TCP connection (see packet 908666).	192.168.1.33	E0

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

The screenshot shows the 'Protocol' and 'MAC Endpoint' tabs. The 'Protocol' tab lists various protocols like Ethernet II, IP, UDP, DNS, etc., with their respective byte and packet counts. The 'MAC Endpoint' tab shows details for the local segment and specific MAC addresses like A4:A2:4A:5E:D7:35 and IP 10.3.0.1.

Name	Bytes	Packets	Bytes Received	Packets Received	Bytes
Ethernet II	1.61 GB	1,932,441	0.00 B	0	4.3
IP	1.60 GB	1,890,101	75.90 MB	638,535	1.5
UDP	1.42 GB	1,623,384	127.75 KB	1,046	1.7
DNS	582.80 KB	4,297	412.00 B	6	0
NetBIOS	62.73 KB	637			
LLMNR	35.67 KB	516			
DPLAY	12.58 KB	68			
ROOTP	9.58 KB	28			

## หน้าแสดง MAC Endpoint เป็นการแสดงในลักษณะของ MAC Address

Name	Bytes	Packets	bps	Bytes Received	Packets Received
Local Segment	1.63 GB	1,957,787	15.872 Kbps	0.00 B	0
A4:A2:4A:5E:D7:35	1.63 GB	1,954,492	15.872 Kbps	76.68 MB	646,889
r16---sn-30a7dn7l.g...	372.36 MB	412,429	0.000 bps	11.83 MB	137,197
r8---sn-5np5po4v-c...	245.68 MB	272,334	0.000 bps	7.80 MB	89,981
r1---sn-5np5po4v-c...	217.76 MB	239,323	0.000 bps	7.03 MB	79,896
r4---sn-5np5po4v-c...	205.75 MB	228,019	0.000 bps	6.67 MB	75,599
r6---sn-30a7dnel.c...	129.38 MB	142,844	0.000 bps	4.08 MB	47,662
r2---sn-5np5po4v-c...	126.64 MB	139,266	0.000 bps	4.11 MB	46,634
r4---sn-30a7dnel.g...	71.02 MB	78,401	0.000 bps	2.24 MB	26,211
r1---sn-30a7dne7.c...	68.47 MB	75,116	0.000 bps	2.12 MB	25,082
3-edge-chat.facebo...	18.14 MB	37,062	0.000 bps	6.90 MB	15,972
r6---sn-5np5po4v-c...	16.05 MB	17,815	0.000 bps	537.93 KB	5,938
fbcdn-video-h-a.ak...	13.47 MB	12,826	0.000 bps	185.48 KB	3,221
ad4.liverail.com	10.87 MB	20,079	0.000 bps	6.39 MB	8,382
ip.casalemedia.com	10.02 MB	8,532	0.000 bps	95.85 KB	1,650
fbcdn-video-j-a.aka...	9.71 MB	8,270	0.000 bps	93.49 KB	1,592
fbcdn-vthumb-a.ak...	9.61 MB	8,209	0.000 bps	98.07 KB	1,582

Node 1 ->	<- Node 2	Duration	Bytes	Bytes ->	<- Bytes	Packets
F0:06:F6:76:CB:41	33:33:00:00:00:0C	01:21:26.767027	14.86 KB	14.86 KB	0.00 B	40

หน้าแสดง IP Conversation เป็นหน้าที่แสดงในส่วนของการติดต่อสื่อสารโดยใช้ protocol IP ว่าเครื่องมีการเชื่อมต่อไปที่ไหนคใดบ้าง แต่ละโหนดที่มีการติดต่อสื่อสารไปนั้นมึขนาดข้อมูลที่สื่อสารเท่าไร, จำนวน packet ที่ใช้, เวลาเริ่มต้นในการส่งข้อมูลและเวลาสิ้นสุดในการส่งข้อมูล

Node 1 ->	<- Node 2	Duration	Bytes	Bytes ->	<- Bytes	Packets
192.168.1.33	safebrowsing-cache...	00:00:00.016740	184.00 B	116.00 B	68.00 B	3
192.168.1.33	www.ybotvisit.com	00:00:14.603909	116.00 B	116.00 B	0.00 B	2
192.168.1.33	whos.amung.us	00:00:00.590448	1.63 KB	1.03 KB	609.00 B	10
192.168.1.33	67.202.66.203	00:00:00.804270	3.46 KB	2.62 KB	860.00 B	12
192.168.1.33	s2.thstats.com	00:00:03.745018	1.79 KB	1.14 KB	666.00 B	11
192.168.1.33	www.adnetworkperf...	00:00:00.709755	5.24 KB	2.17 KB	3.07 KB	24
192.168.1.33	sync.adap.tv	00:00:11.150538	380.00 B	244.00 B	136.00 B	6
192.168.1.33	segments.adap.tv	00:00:11.152273	760.00 B	488.00 B	272.00 B	12
192.168.1.33	sync.adaptv.advertis...	00:00:11.153080	760.00 B	488.00 B	272.00 B	12
192.168.1.33	go.oclasrv.com	00:00:13.123670	7.14 KB	2.00 KB	5.14 KB	27
192.168.1.33	netdna.bootstrapcdn...	00:00:13.123988	30.81 KB	1.88 KB	28.93 KB	47

Node 1 ->	<- Node 2	Packets	Bytes	Protocol	Duration	Bytes
192.168.1.33:17488	safebrowsing-cache.g...	3	184.00 B	TCP	00:00:00.016740	116.00

หน้าแสดง TCP Conversation เป็นหน้าที่แสดงข้อมูลเช่นเดียวกับ IP Conversation แต่จะแสดงเฉพาะการติดต่อสื่อสารระหว่างโหนดโดยใช้ protocol TCP

Node 1 ->	<- Node 2	Packets	Bytes	Protocol	Duration	Byte
192.168.1.33:18745	external-kul1-1.xx.fbc...	2	192.00 B	HTTPS	00:00:00.000055	58.
192.168.1.33:18833	cdn-static-secure.liver...	1	68.00 B	TCP	00:00:00.000000	0.
192.168.1.33:17651	www.epmads.com:80	3	184.00 B	TCP	00:00:00.017476	116.
192.168.1.33:15812	www.facebook.com:443	28	5.64 KB	HTTPS	00:00:00.315716	464.
192.168.1.33:18792	rtb-liverail.tubemogul...	3	184.00 B	TCP	00:00:00.020472	116.
192.168.1.33:18860	update.colasoft.com:80	6	380.00 B	TCP	00:00:00.927667	244.
192.168.1.33:18859	safebrowsing-cache.g...	6	382.00 B	TCP	00:00:00.989752	244.
192.168.1.33:18864	ad4.liverail.com:80	15	5.26 KB	HTTP	00:00:00.671261	2.7
192.168.1.33:18853	ecpmrocks.com:80	6	1.94 KB	HTTP	00:00:00.779817	174.
192.168.1.33:18848	ecpmrocks.com:80	5	703.00 B	HTTP	00:00:00.796965	174.
192.168.1.33:18847	ecpmrocks.com:80	5	895.00 B	HTTP	00:00:00.823992	174.

No.	Absolute Time	Source	Destination	Protocol	Size	Decode
There are no items to show in this view.						

หน้าแสดง UDP Conversation เป็นหน้าที่แสดงข้อมูลเช่นเดียวกับ IP Conversation แต่จะแสดงเฉพาะการติดต่อสื่อสารระหว่างโหนดโดยใช้ protocol UDP

Node 1 ->	<- Node 2	Duration	Bytes	Bytes ->	<- Bytes	Packet
192.168.1.33:60935	203.144.206.29:53	00:00:00.017737	463.00 B	88.00 B	375.00 B	2
192.168.1.33:55051	203.144.206.49:53	00:00:00.017436	176.00 B	80.00 B	96.00 B	2
192.168.1.33:55051	203.144.206.29:53	00:00:00.260033	176.00 B	80.00 B	96.00 B	2
192.168.1.33:64489	203.144.206.29:53	00:00:00.018052	228.00 B	88.00 B	140.00 B	2
192.168.1.33:59695	203.144.206.29:53	00:00:00.027135	216.00 B	80.00 B	136.00 B	2
192.168.1.33:53491	203.144.206.29:53	00:00:00.017040	182.00 B	83.00 B	99.00 B	2
192.168.1.33:53492	239.255.255.250:3702	00:00:00.149957	1.31 KB	1.31 KB	0.00 B	2
192.168.1.33:60260	224.0.0.252:5355	00:00:00.402133	136.00 B	136.00 B	0.00 B	2
192.168.1.33:54629	224.0.0.252:5355	00:00:00.402392	140.00 B	140.00 B	0.00 B	2
192.168.1.33:52823	224.0.0.252:5355	00:00:00.402425	136.00 B	136.00 B	0.00 B	2
192.168.1.33:59715	224.0.0.252:5355	00:00:00.406122	136.00 B	136.00 B	0.00 B	2

No.	Absolute Time	Source	Destination	Protocol	Size	Decode
There are no items to show in this view.						

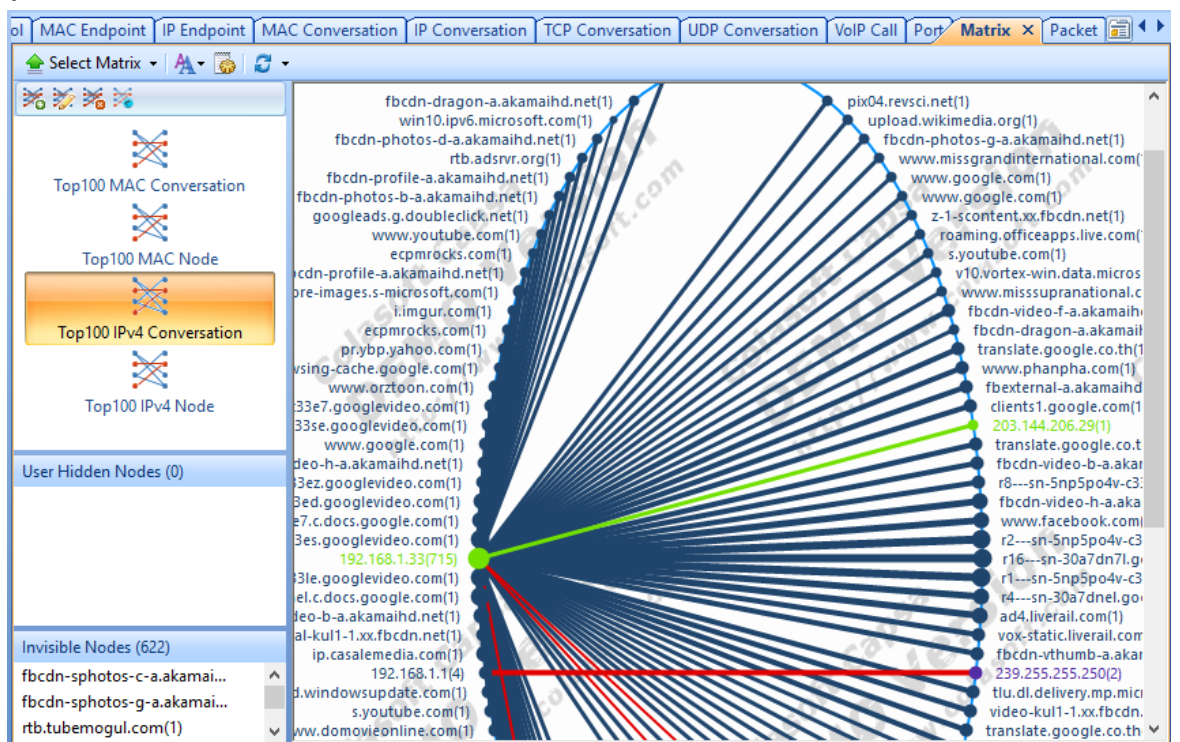
หน้าแสดง port คือ แสดง port ที่มีการใช้งานอยู่

Port	Port Type	IP Protocol	Packets	Bytes	Avg. Pkt. Size	Common Service
443	Server, Unknown	TCP	193,469	148.41 MB	804.00 B	https
80	Server, Unknown	TCP	93,209	57.46 MB	646.00 B	www-http
2869	Server	TCP	142	20.90 KB	150.00 B	icslap
843	Server	TCP	80	7.55 KB	96.00 B	
10012	Server	TCP	128	14.53 KB	116.00 B	
10025	Server	TCP	21	6.41 KB	312.00 B	
1688	Server	TCP	6	412.00 B	68.00 B	nsjtp-data
10016	Server	TCP	107	12.82 KB	122.00 B	
10006	Server	TCP	115	13.37 KB	119.00 B	netapp-sync

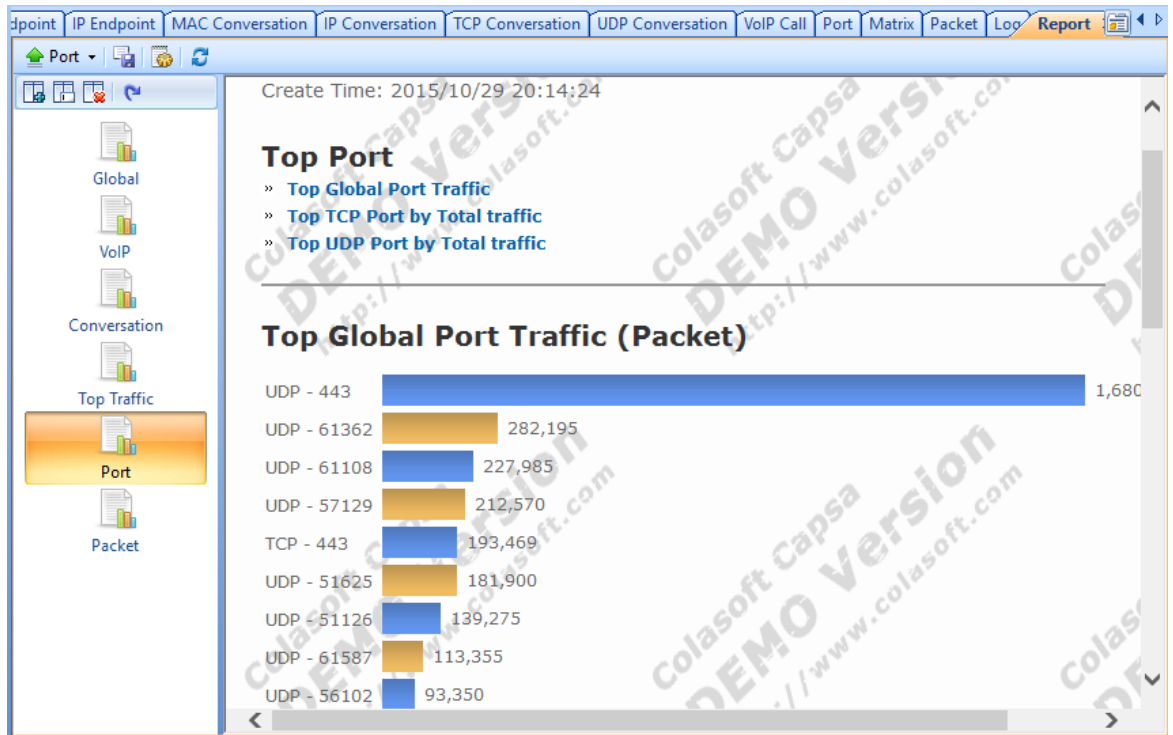
Node 1 ->	<- Node 2	Packets	Bytes	Protocol	Duration	Byt
192.168.1.33:18745	external-kul1-1.xx.fbc...	2	192.00 B	HTTPS	00:00:00.000055	58
192.168.1.33:18833	cdn-static-secure.liver...	1	68.00 B	TCP	00:00:00.000000	0
192.168.1.33:15812	www.facebook.com:443	28	5.64 KB	HTTPS	00:00:00.315716	464
192.168.1.33:17488	safebrowsing-cache.g...	3	184.00 B	TCP	00:00:00.016740	116

หน้าแสดง Matrix เป็นการแสดงรูปแบบการเชื่อมต่อระหว่างโหนดและกราฟฟิคในรูปแบบของกราฟ





หน้า Report จะเป็นหน้าที่ให้ผู้ใช้สามารถดูผลสรุปโดยรวมของการทำงานในระบบเครือข่ายได้ ซึ่งสามารถเลือกดูได้ในหลายรูปแบบ



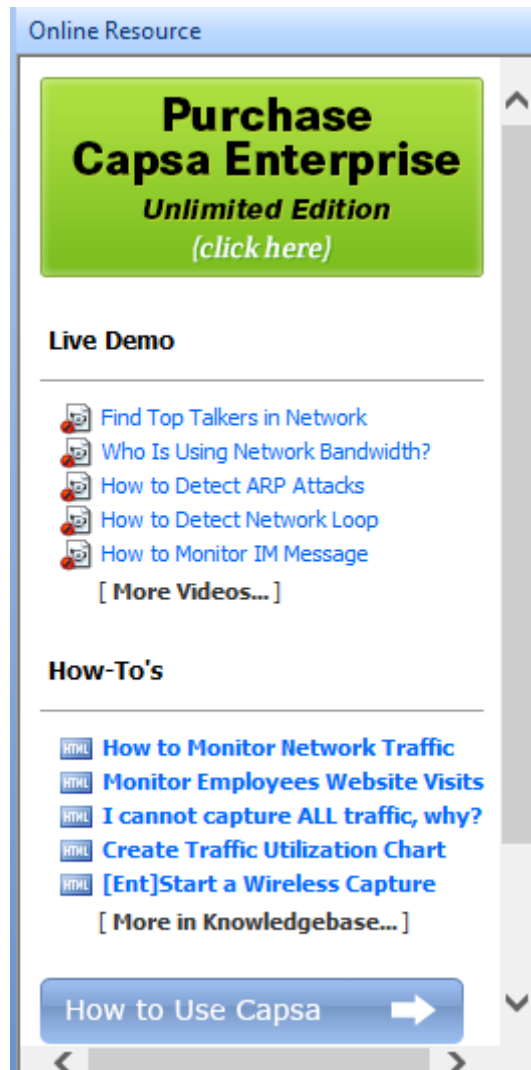
หน้า Packet ทำหน้าที่แสดงผลแพ็คเกจที่เกิดขึ้นทั้งหมดภายในเครือข่ายของผู้ใช้งาน

No.	Absolute Time	Source	Destination	Protocol	Size	Decod
2006795	20:06:00.832817	r2---sn-5np5po4v-c33r.googlevid...	192.168.1.33:51625	RPCAP	1,396	
2006796	20:06:00.832817	r2---sn-5np5po4v-c33r.googlevid...	192.168.1.33:51625	RPCAP	1,396	
2006797	20:06:00.833041	r2---sn-5np5po4v-c33r.googlevid...	192.168.1.33:51625	RPCAP	1,396	
2006798	20:06:00.833073	192.168.1.33:51625	r2---sn-5np5po4v-c33r.googlevid...	RPCAP	91	
2006799	20:06:00.833199	192.168.1.33:51625	r2---sn-5np5po4v-c33r.googlevid...	RPCAP	91	
2006800	20:06:00.833317	192.168.1.33:51625	r2---sn-5np5po4v-c33r.googlevid...	RPCAP	91	
2006801	20:06:00.844611	r2---sn-5np5po4v-c33r.googlevid...	192.168.1.33:51625	RPCAP	1,396	
2006802	20:06:00.844612	r2---sn-5np5po4v-c33r.googlevid...	192.168.1.33:51625	RPCAP	1,396	
2006803	20:06:00.844612	r2---sn-5np5po4v-c33r.googlevid...	192.168.1.33:51625	RPCAP	1,396	

Hex	ASCII
0000 E0 06 E6 76 CB 41 A4 A2 4A 5E D7 35 08 00 45 00 05 62 00 00 40 00 3A 11 32 9A	...v.A..J^..S..E..b..@...:2.
001A 3D 5B 09 CD C0 A8 01 21 01 BB C9 A9 05 4E 34 78 10 84 C5 36 CD 5F 64 75 5F A0	=[.....!.....N4x...6..du..
0034 6C 26 6F B3 0B DC F7 6F A7 57 4E 44 60 B4 8C 12 E9 AD BA 1D F8 53 B4 5A 39 27	1&o.....o.WND'.....S.Z9'
004E 83 C4 1F 80 C2 3A 03 98 24 14 12 38 D2 53 45 59 F3 D0 61 31 47 FD 24 F1 73 C4	.....\$.8.SEY..a1G\$.s.
0068 2E 68 F5 83 CF C5 33 05 2C 6E 34 F4 DE BC 9F 8B E2 48 08 0B 8A 55 3F CF 50 71	.h...3...n4...H...U?.Pg
0082 15 D2 72 EF BF FE BA C7 77 0E 29 35 C5 8F E9 F3 C9 1B 7C 0B AB F7 13 19 A4 2E	..r.....(w.)5..... .....
009C 27 D7 A6 0A F6 4E CD 66 23 12 6B FF 6B 8D 33 7A BA 7E FE F7 74 A8 82 64 1E F8	'...N.f#.k.k.3z~..t..d..
00B6 94 7A 43 11 9C 80 FD 7A 26 D1 0D F8 31 EA FE A9 CA F2 B4 FD 52 DB 79 0D 8D C8	.zC...z#...1.....R.y...
00D0 C8 16 C7 EF 17 54 CE C0 B0 52 17 A4 75 74 20 B6 05 89 B0 6A 53 E2 DC EE FE BA	.....T...R...ut.....jS....
00EA 30 04 7B BA 05 78 C3 89 83 A2 75 A4 CA DD 38 65 23 74 3D 4D 01 C1 A3 D8 1A 3B	0.{...x.....u...8e#t=M.....
0104 B8 77 68 0B 62 04 69 23 19 3F C6 82 79 C2 64 90 7A DB CC A7 84 58 8D 29 55 B2	.wh.b.i#.?.?..y.d.z...X.)U.
011E DF AC AB DC D8 23 46 0D 5F 9E 71 FD F6 01 8B 01 33 6E A3 6A 55 F8 7F F5 AB AF	.....#F...q...3n.jU....
0138 63 AF CF 3F B9 50 86 47 8F 80 73 41 8D 1A 28 39 2D D9 33 E5 72 D3 8F 19 6A 7A	c...?.P.G...sA... (9-3.r...jz
0152 68 4B D4 BA 52 00 D4 1B 33 96 DD 48 E0 7D 27 60 D1 C2 95 E6 9E 43 DE 86 01 92	hK...R...3...H.}''.....C....

6. Online Resource window เป็นหน้าต่างการค้นหาค้นหาทรัพยากรในรูปแบบออนไลน์โดยสามารถศึกษาขั้นตอนการใช้งานต่างๆได้



7. Status Bar เป็นแถบสถานะที่จะนำเสนอข้อมูลของโปรเจกต์ที่ใช้ในการวิเคราะห์

