LabSheet 04:

การติดตั้งโปรแกรมส่งล๊อกไฟล์บนเซิร์ฟเวอร์ที่มีระบบปฏิบัติการ Windows (IIS Log)

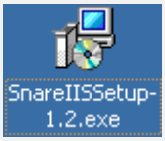
Date: 8 August 2008

Program name: SnareIIS

Description: Send IIS log files to Centralized Log Server (logger.ku.ac.th)

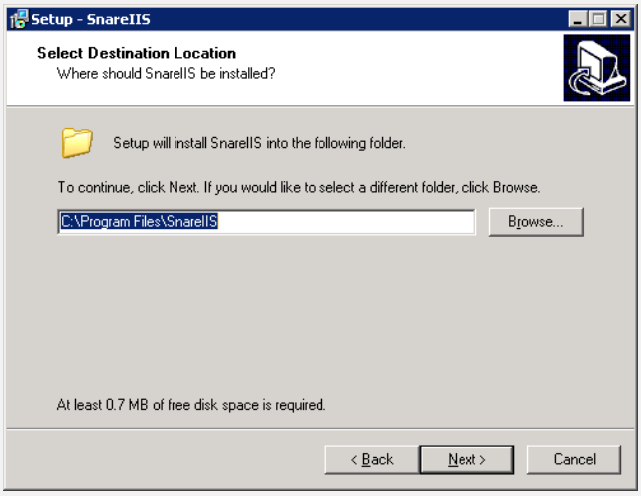
Step:

1. Download : http://ftp.ku.ac.th/pub/syslog-ng/snare/SnareIISSetup-1.2.exe
2. ติดตั้งโปรแกรม

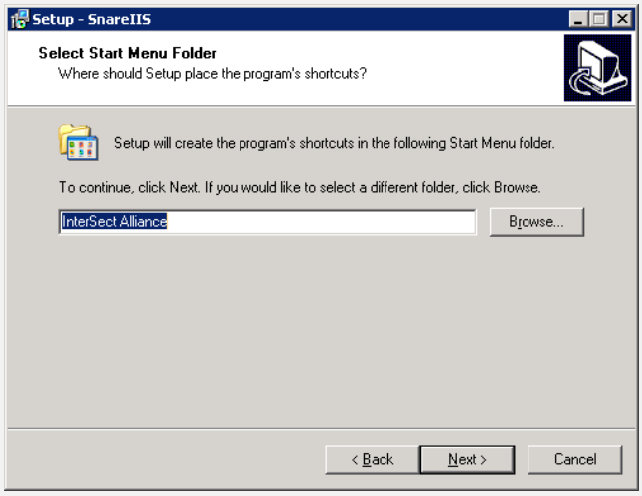


ดับเบิ้ลคลิกที่ชื่อโปรแกรม

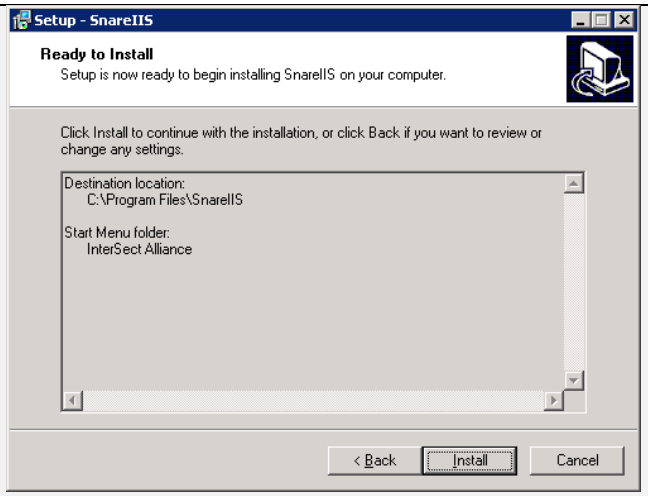
คลิกที่ปุ่ม Next >



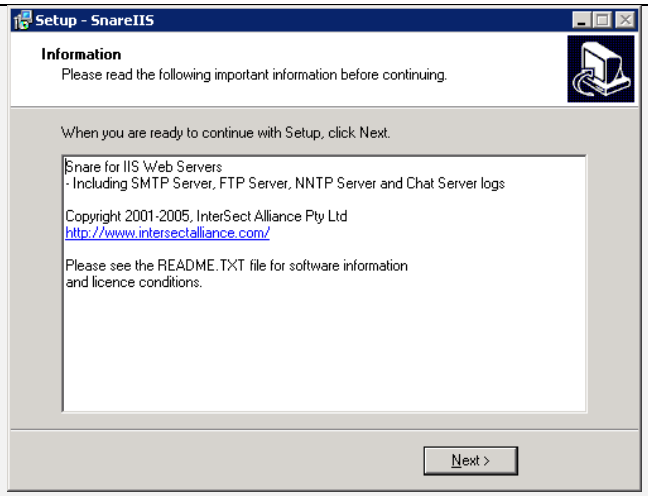
คลิกที่ปุ่ม Next >



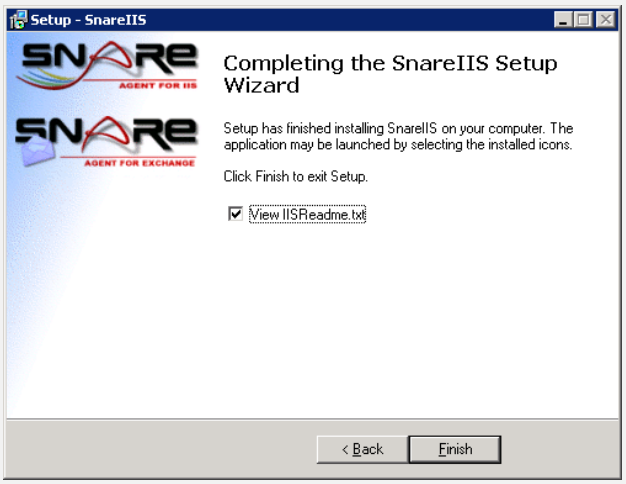
คลิกที่ปุ่ม Next >



คลิกที่ปุ่ม Install

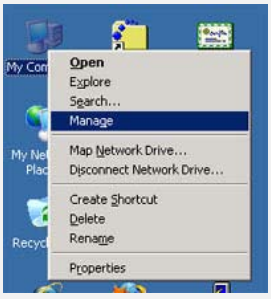


คลิกที่ปุ่ม Next >

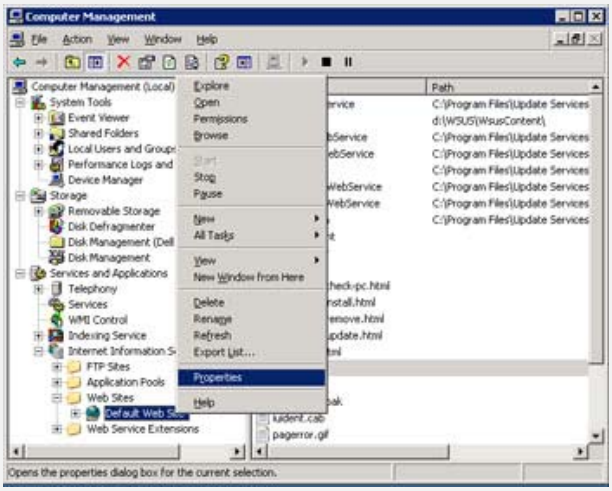


เสร็จแล้วคลิกที่ปุ่ม Finish

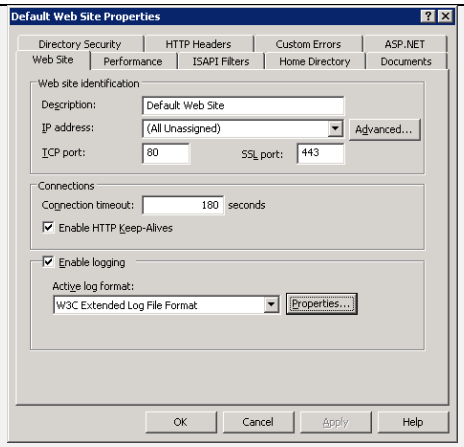
3. ปรับแต่งค่าของข้อมูลล๊อกไฟล์ที่จะจัดเก็บ ดังนี้



บนหน้าจอ Desktop คลิกเมาส์ขวาที่ไอคอน My Computer แล้วเลือกเมนู Manage >

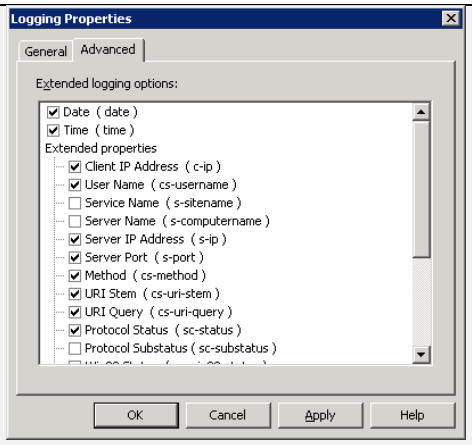


จากหน้าจอ Computer management คลิกเมนู Services and Applications > Internet Information Services (IIS) Manager > Web Sites แล้วคลิกเมาส์ขวาที่เมนู Default Web Site เลือกเมนู Properties >



จากหน้าจอ Default Web Site Properties เลือกแท็บ Web Site

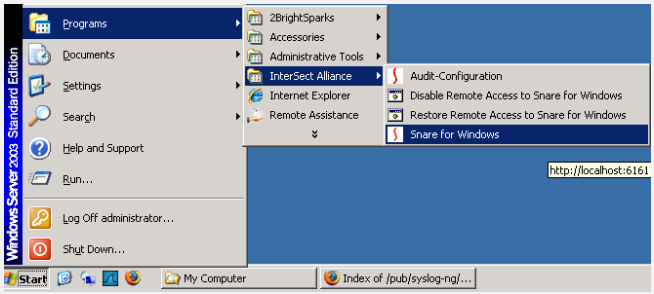
- คลิกเครื่องหมายถูกหน้า Enable logging
- Active log format เลือกเป็น W3C Extended Log File Format
- คลิกปุ่ม Properties >

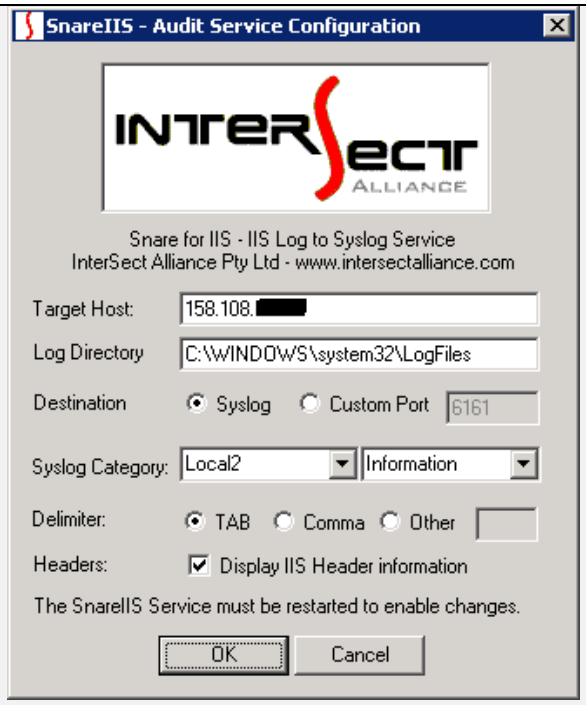


จากหน้าจอ Logging Properties ให้คลิกแท็บ Advanced แล้วคลิกเครื่องหมายถูกหน้าข้อมูลที่จะจัดเก็บ ดังนี้

- Date
- Time
- Client IP Address
- User Name
- Server IP Address
- Server Port
- Method
- URI Stem
- URI Query
- Protocol Status
- User Agent
- Referer

4. ปรับแต่งค่าคอนฟิกของโปรแกรม SnareIIS ไปที่เมนู Start > Programs > InterSect Alliance > Audit-Configuration





- กำหนดค่าต่างๆ ดังนี้

  ช่อง Target Host: --> IPAddress Log Server (158.108.5.154)

  Log Directory: --> C:\WINDOWS\system32\LogFiles

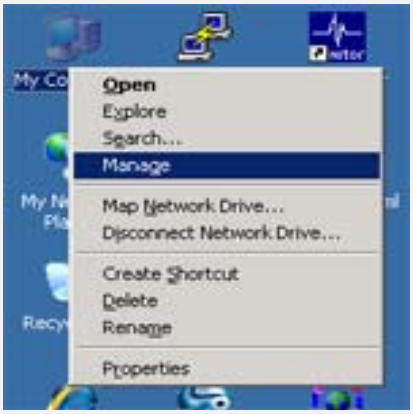
  Destination --> คลิกเลือก Syslog

  Syslog Category: --> เลือก Local2 และ Information

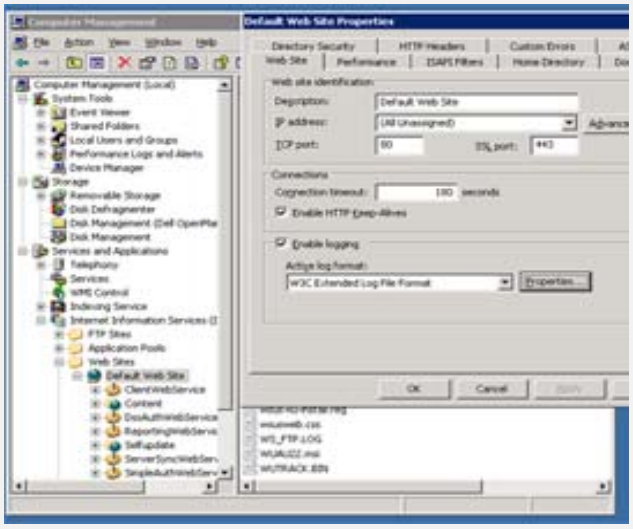
  ช่อง Headers: --> คลิกเครื่องหมายถูก

- เสร็จแล้ว คลิกที่ปุ่ม OK

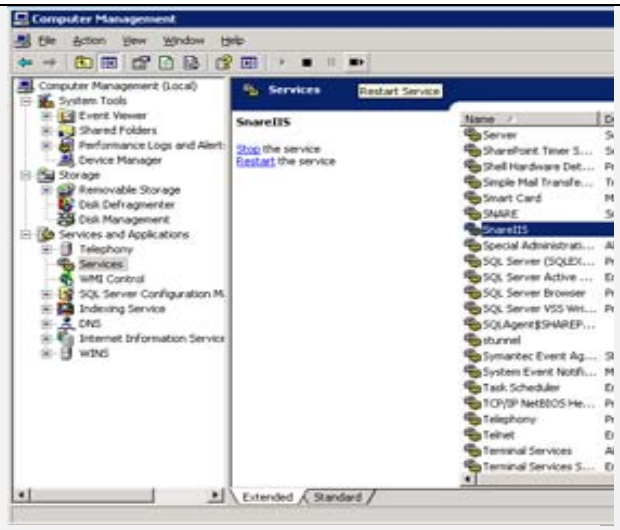
5. เริ่มการทำงานใหม่ของโปรแกรม SnareIIS



บนหน้าจอ Desktop คลิกเมาส์ขวาบนไอคอน My Computer > Manage >



คลิกเมนู Services and Application > Services >



คลิกเลือกโปรแกรม SnareIIS แล้วคลิกปุ่ม Restart Services