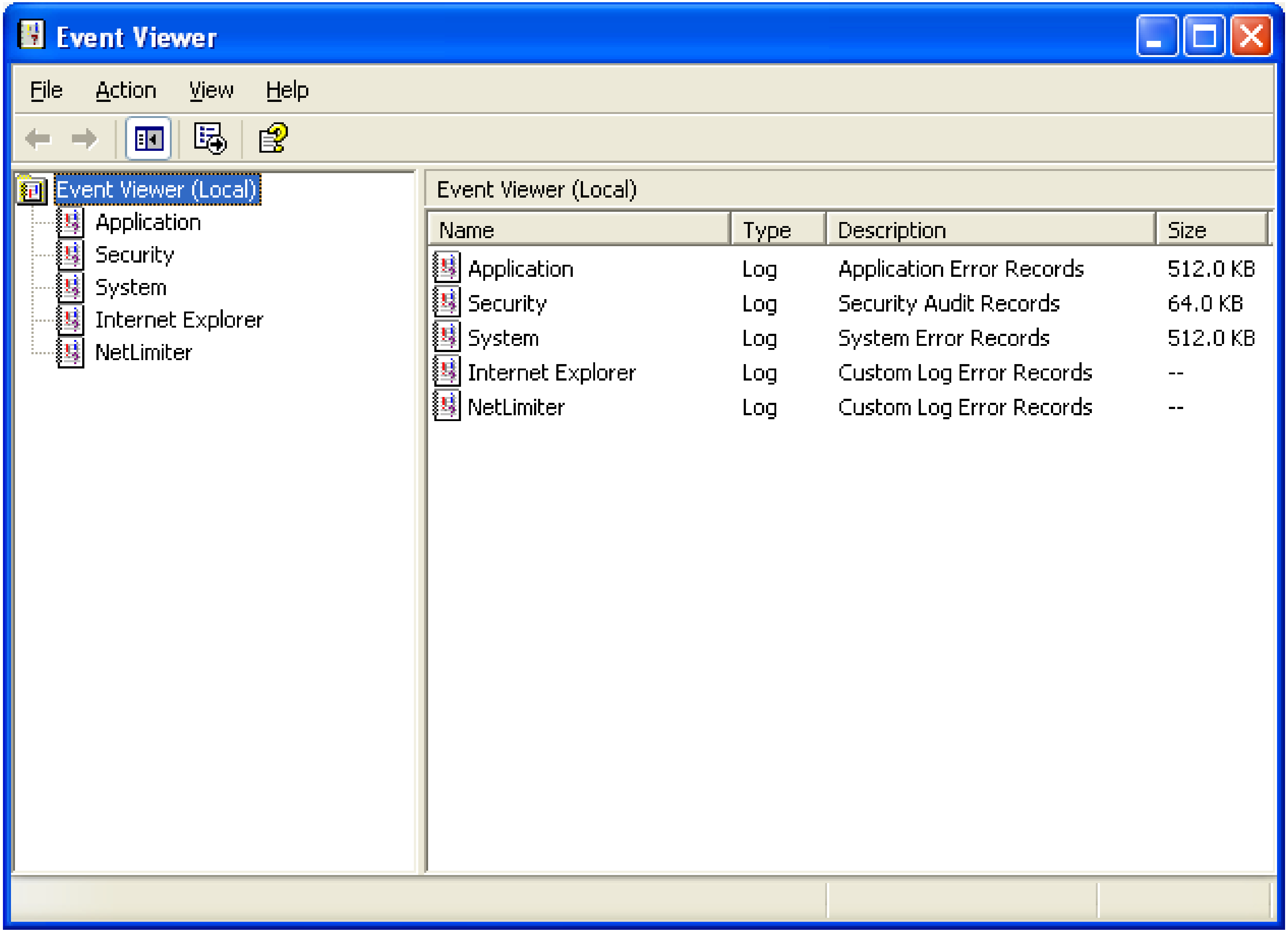
Event Viewer

Patrick.j.rice@gmail.com

Was of getting to event viewer

- Go to
  - Start
  - Control Panel,
  - Administrative Tools
  - Event Viewer

- Go to
  - Start
  - Run
  - type in "eventvwr.msc"



Name	Type	Description	Size
Application	Log	Application Error Records	512.0 KB
Security	Log	Security Audit Records	64.0 KB
System	Log	System Error Records	512.0 KB
Internet Explorer	Log	Custom Log Error Records	--
NetLimiter	Log	Custom Log Error Records	--

What does it give us

- Application log
  - The application log contains events logged by applications or programs. For example, a database program might record a file error in the application log. Program developers decide which events to monitor.
- Security log
  - The security log records events such as valid and invalid logon attempts, as well as events related to resource use such as creating, opening, or deleting files or other objects. An administrator can specify what events are recorded in the security log. For example, if you have enabled logon auditing, attempts to log on to the system are recorded in the security log.
- System log
  - The system log contains events logged by Windows XP system components. For example, the failure of a driver or other system component to load during startup is recorded in the system log. The event types logged by system components are predetermined by Windows XP.

Even more if your are runnig as a domain controler

- A computer running Windows configured as a domain controller records events in two additional logs:
  - Directory service log
    - The directory service log contains events logged by the Windows directory service. For example, connection problems between the server and the global catalog are recorded in the directory service log.
  - File Replication service log
    - The File Replication service log contains events logged by the Windows File Replication service. For example, file replication failures and events that occur while domain controllers are being updated with information about sysvol changes are recorded in the file replication log.
- A computer running Windows configured as a Domain Name System (DNS) server records events in an additional log:
  - DNS server log
    - The DNS server log contains events logged by the Windows DNS service. Events associated with resolving DNS names to Internet Protocol (IP) addresses are recorded in this log.

Events that can occur

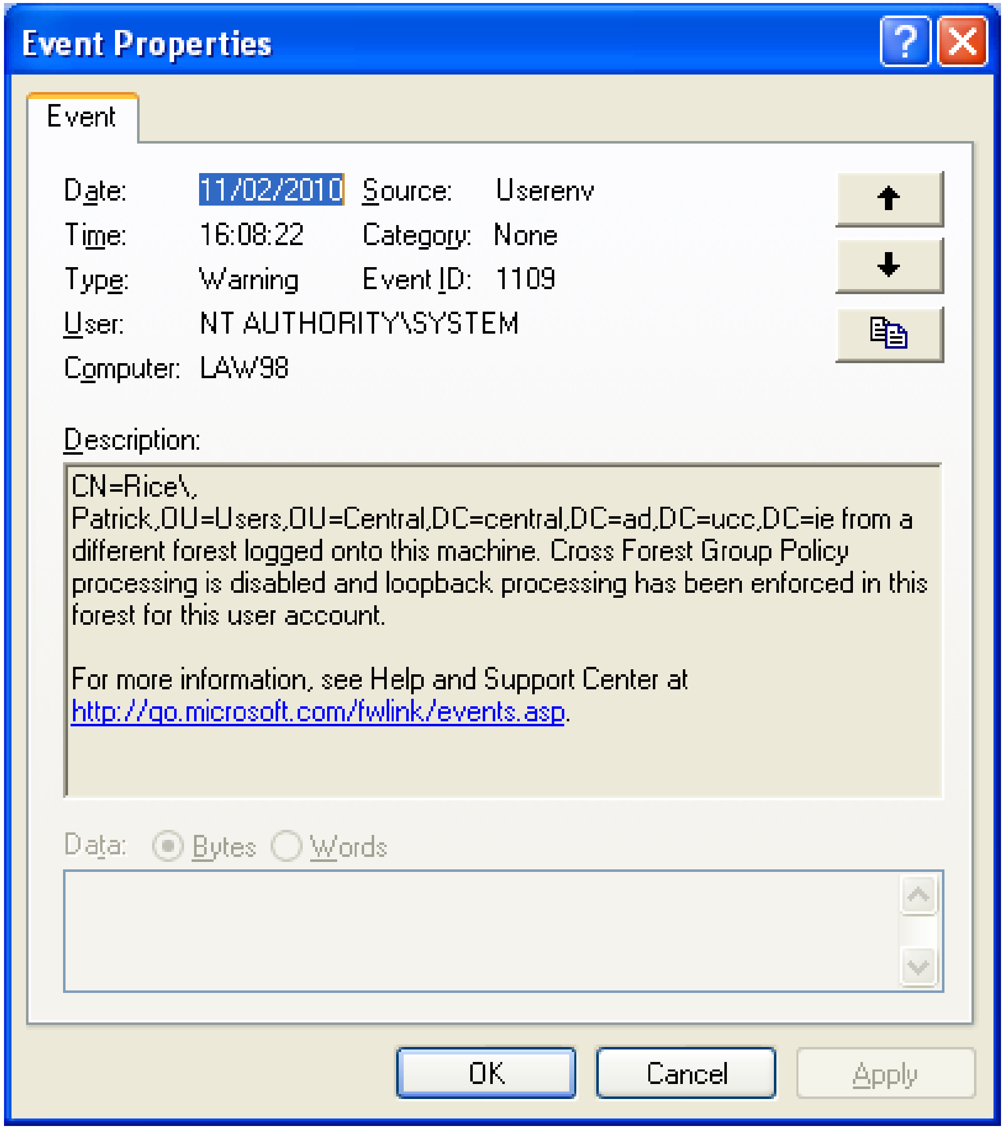
- Error
  - A significant problem, such as loss of data or loss of functionality. For example, if a service fails to load during startup, an Error event will be logged.
- Warning
  - An event that is not necessarily significant, but may indicate a possible future problem. For example, when disk space is low, a Warning event will be logged.
- Information
  - An event that describes the successful operation of an application, driver, or service. For example, when a network driver loads successfully, an Information event will be logged.

Security logging

- Success Audit
  - An audited security access attempt that succeeds. For example, a user's successful attempt to log on to the system will be logged as a Success Audit event.
- Failure Audit
  - An audited security access attempt that fails. For example, if a user tries to access a network drive and fails, the attempt will be logged as a Failure Audit event.
- By default, security logging is turned off. You can use Group Policy to enable security logging. The administrator can also set auditing policies in the registry that cause the system to halt when the security log is full.

Application Errors

Example Events (Warning)



Date: 11/02/2010 Source: Userenv
Time: 16:08:22 Category: None
Type: Warning Event ID: 1109
User: NT AUTHORITY\SYSTEM
Computer: LAW98

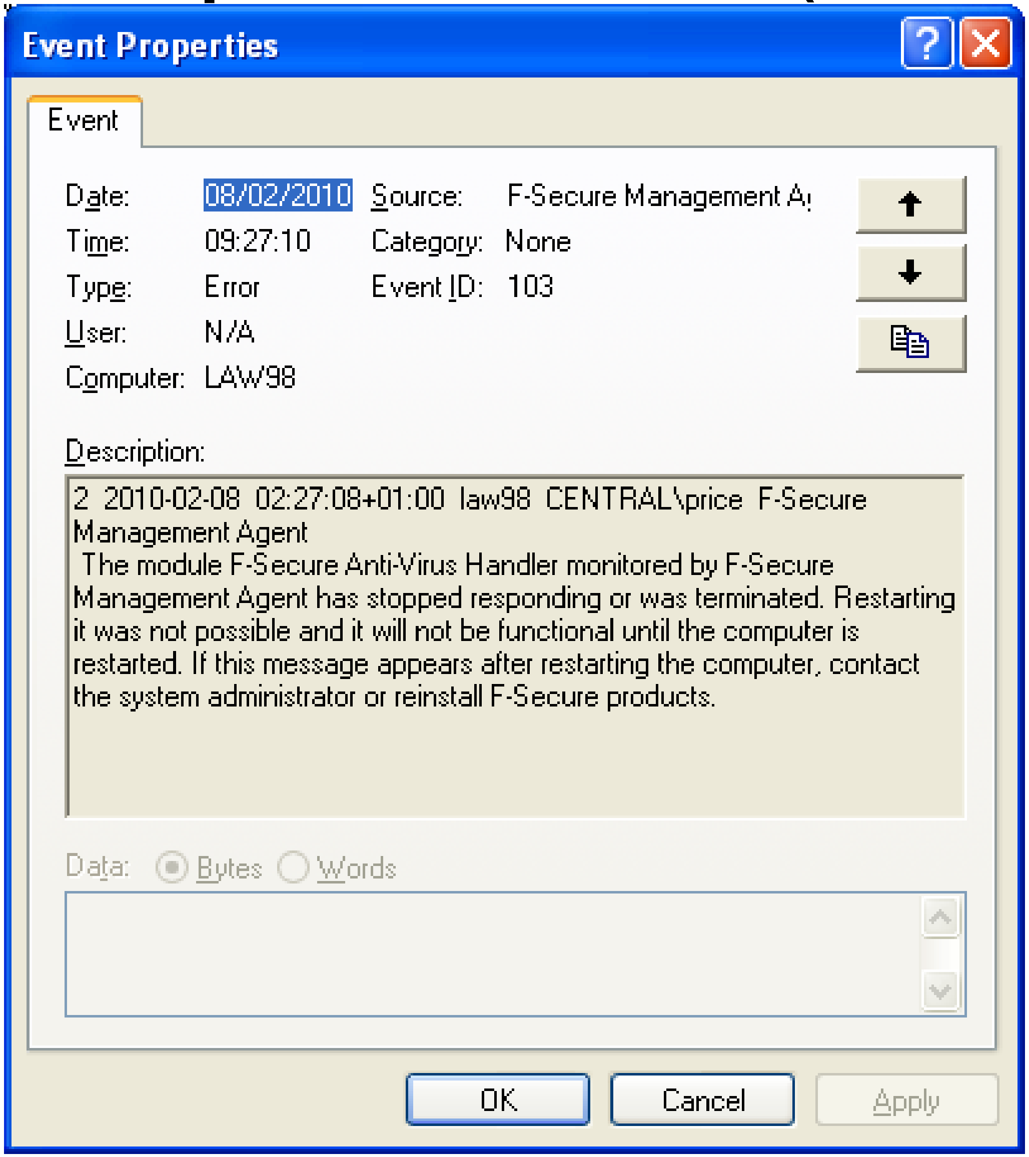
Description:

CN=Rice\, Patrick,OU=Users,OU=Central,DC=central,DC=ad,DC=ucc,DC=ie from a different forest logged onto this machine. Cross Forest Group Policy processing is disabled and loopback processing has been enforced in this forest for this user account.

For more information, see Help and Support Center at http://go.microsoft.com/fwlink/events.asp.

Data: ● Bytes ○ Words

Example Events (Error)



Date: 08/02/2010 Source: F-Secure Management A
Time: 09:27:10 Category: None
Type: Error Event ID: 103
User: N/A
Computer: LAW98

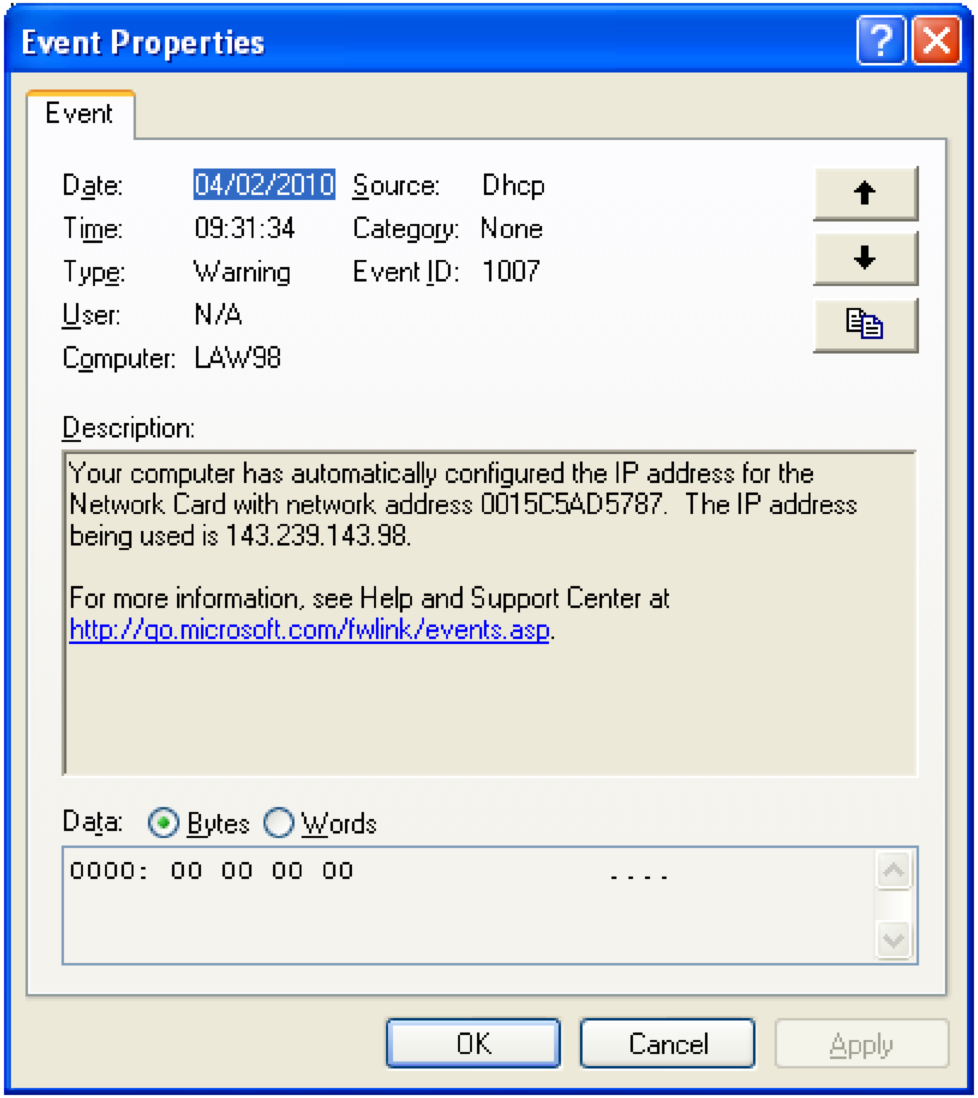
Description:

2 2010-02-08 02:27:08+01:00 law98 CENTRAL\price F-Secure Management Agent
The module F-Secure Anti-Virus Handler monitored by F-Secure Management Agent has stopped responding or was terminated. Restarting it was not possible and it will not be functional until the computer is restarted. If this message appears after restarting the computer, contact the system administrator or reinstall F-Secure products.

Data: ● Bytes ○ Words

System Errors

Example event (warning)



Date: 04/02/2010 Source: Dhcp
Time: 09:31:34 Category: None
Type: Warning Event ID: 1007
User: N/A
Computer: LAW98

Description:

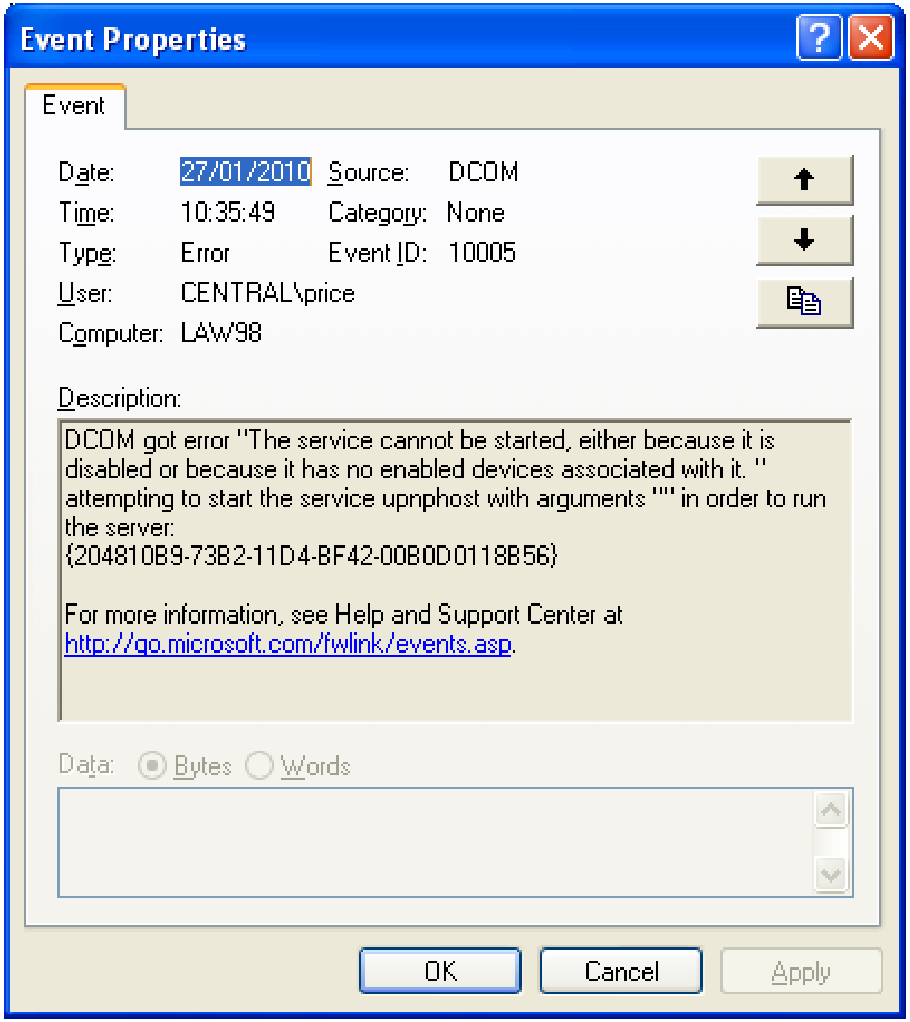
Your computer has automatically configured the IP address for the Network Card with network address 0015C5AD5787. The IP address being used is 143.239.143.98.

For more information, see Help and Support Center at http://go.microsoft.com/fwlink/events.asp.

Data: ● Bytes ○ Words

```
0000: 00 00 00 00                    ....
```

Example event (Error)



Date: 27/01/2010 Source: DCOM
Time: 10:35:49 Category: None
Type: Error Event ID: 10005
User: CENTRAL\price
Computer: LAW98

Description:

DCOM got error "The service cannot be started, either because it is disabled or because it has no enabled devices associated with it. " attempting to start the service upnphost with arguments "" in order to run the server:
{204810B9-73B2-11D4-BF42-00B0D0118B56}

For more information, see Help and Support Center at http://go.microsoft.com/fwlink/events.asp.

Data: ● Bytes ○ Words