Installation Guide
TupInsight 3.0

(Last revised: July, 2005)

Contents

1. Welcome

Welcome to the installation guide for the TupInsight 3.0 Internet activity monitoring and web access control system. This guide will explain in detail the fundamental concepts, installation preparation, and step-by-step installation procedure. This document will walk you through a typical installation process that will give you a fully functioning system.

2. About TupInsight

TupInsight is an easy-to-install and -use system that is specifically designed for small & midsize businesses, private agencies, educational institutions, government organizations, as well as households. It uses one computer not only to monitor and record other hosts' web behaviors on a local area network (LAN) but also to restrict online activities according to customized filtering Internet policies. There are following main functions and features of TupInsight:

A. *Capturing all Emails sent/received on the whole local network*

   TupInsight records in real-time all the Emails sent/received (including POP3/SMTP and HTTP protocols), and displays information such as MAC (Media Access Control) address (or adapter address), IP address, time sent/received, title, sender/receiver, attachment(s), content, and size.

B. *Snapshoting all the webpages viewed on the whole local network and copying all the uploaded/downloaded files (FTP protocol)*

   TupInsight provides the snapshots of viewed webpages for an administrator to preview and stores copies of all the FTP files. It also shows other information such as title, site, visited time, and size.

C. *Monitoring chat sessions (such as Yahoo, AOL, MSN, and ICQ), game activities, and other use of online applications self-definable by the administrator*

   TupInsight logs online activities to show the host information, tool used, time online/offline, and data flow.

D. *Enforcing web access control according to the administrator's customization*

   TupInsight can freely set privilege rights of web access for and monitoring action on different classes of hosts in detail. It restricts all or specific online activities for an individual host, a workgroup, or the whole network, in specific time periods, with preset blocking lists. TupInsight has the filtering function to forgo monitoring a small special

group of hosts.

E. Scanning and detecting host names for networked computers

TupInsight automatically collects and analyzes the available data of computers on the whole local network to reveal their host names, IP addresses, and MAC addresses, and classifies the captured messages into categories for different hosts.

F. Based on the client/server architecture to support distributed management of data

TupInsight adopts the separation of server and client program to achieve levels of data distribution.

G. Featuring an easy-to-navigate user interface

TupInsight implements a hierarchical design in order to group related items together. Its straightforward interface makes it easy to add, view, edit, and categorize data and information.

For more information about the TupInsight 3.0 system, please visit our website: http// www.tupsoft.com.

3. System Requirements

CPU	Pentium III 500 MHz or higher
Operation System	Microsoft Windows 2000/XP/Server 2003
Memory	A minimum of 256 MB
Free Hard Disk Space	At least 20 MB (for programs only, additional for captured data)

4. Installation Instructions

A. Fundamental concepts

The data-capturing feature of TupInsight 3.0 is based on eavesdropping on a local computer network. Ethernet is the most widely used local area network (LAN) technology, a "shared medium" in which packet information is broadcast to all the hosts on the same segment, and interfaces, such as network adaptors, are designed to bypass the packets not destinated to them. A sniffer program, however, turns a host into promiscuous mode, capturing all the packets for further decoding and data-mining.
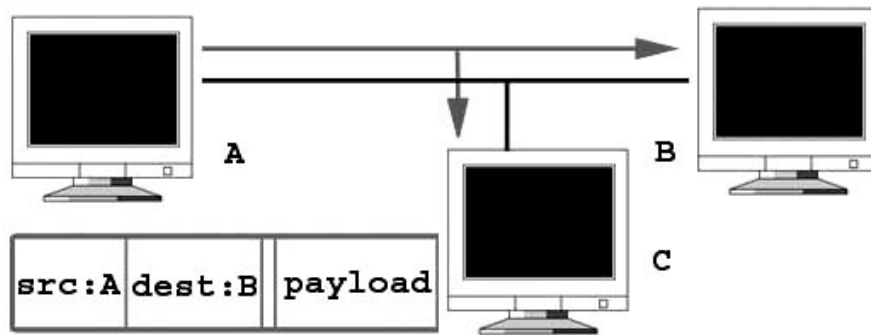
Fig. 1.   C sniffs A's packets.

B. Hardware preparation

In order to catch "everything" and effectively enforce web access control on the whole LAN, the capture engine of TupInsight should be installed at one of the following three positions on a network.

Case one: If the networking infrastructure is a traditional shared hub-based LAN, the TupInsight engine can be installed on any computer host on the network. See Fig. 2.
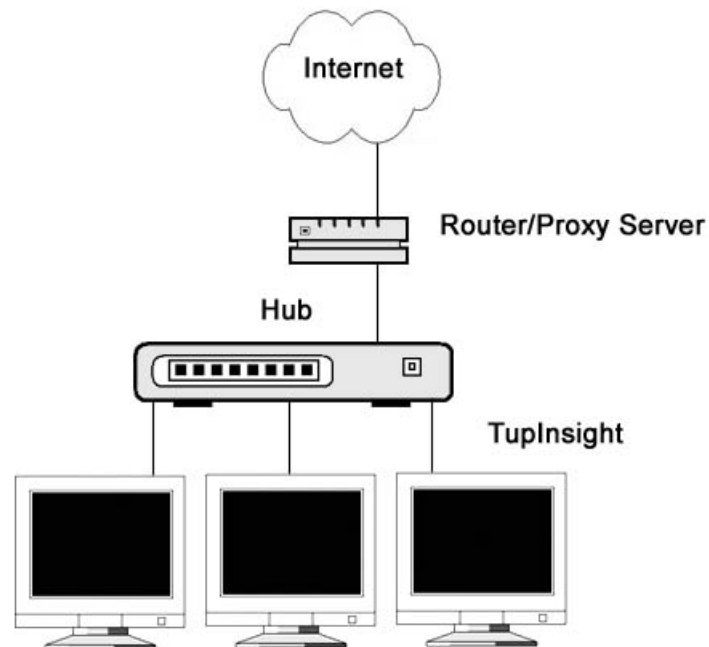

Fig. 2. On a traditional shared hub-based LAN, the engine can be installed on any host machine.

Case two: The switched infrastructure is now the de facto technique used to build local area networks. Unlike hubs, switches prevent promiscuous sniffing. However, you can still install

the TupInsight program on your Internet gateway, a proxy server or a PC shared the same Ethernet segment with the router (see Case three). Any Internet traffic will pass through the gateway and therefore TupInsight could catch/restrict them. Since most modern switches now support "port mirroring," it also allows a network administrator to monitor LAN traffic on any computer connected to one designated switch port.
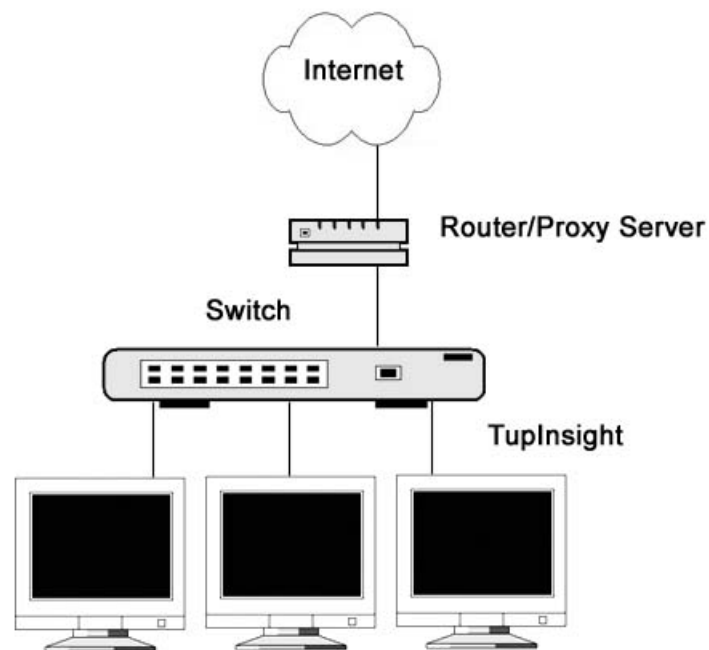

Fig. 3. On a switched LAN, the engine is installed on the gateway machine or a host connected to the "management port" of the top-level switch.

Case three: If the Internet gateway is a router rather than a computer, the simplest and most common solution to capture and block web traffic is to place a shared hub between the router and the top-level switch, as shown in Fig. 4. For any Internet bandwidth less than 5 Mbps, as in the case of most small & midsize business networking infrastructures, this will not exert any negative impact on the Internet access. The typical bandwidth for those networks is less than 1.5 Mbps.
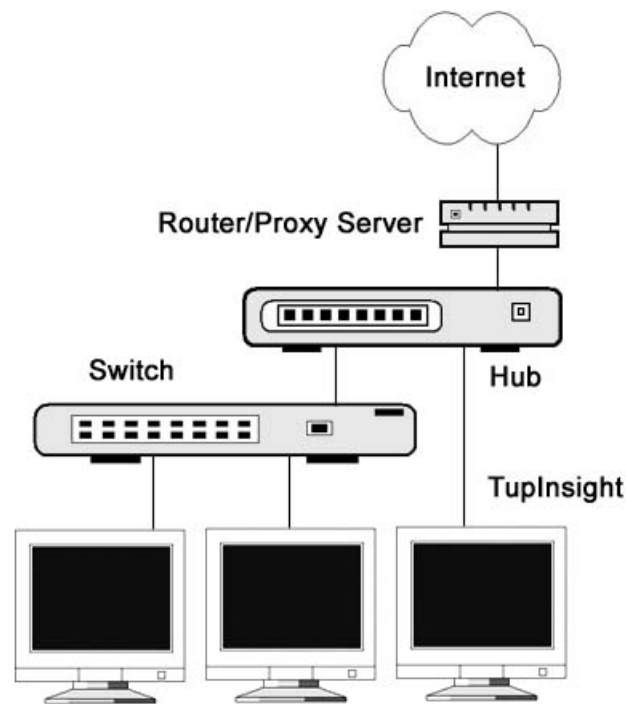
Fig. 4. If the Internet gateway is not a computer, the most common solution is to add a shared hub between the router and the top-level switch.

C. TupInsight installation package

The installation package consists of three parts:

- Engine.exe is for the installation of the TupInsight engine in capturing Emails, Webpages, FTP files, and other data and blocking/filtering web activities.
- Console.exe is the interface for viewing captured messages and managing host information.
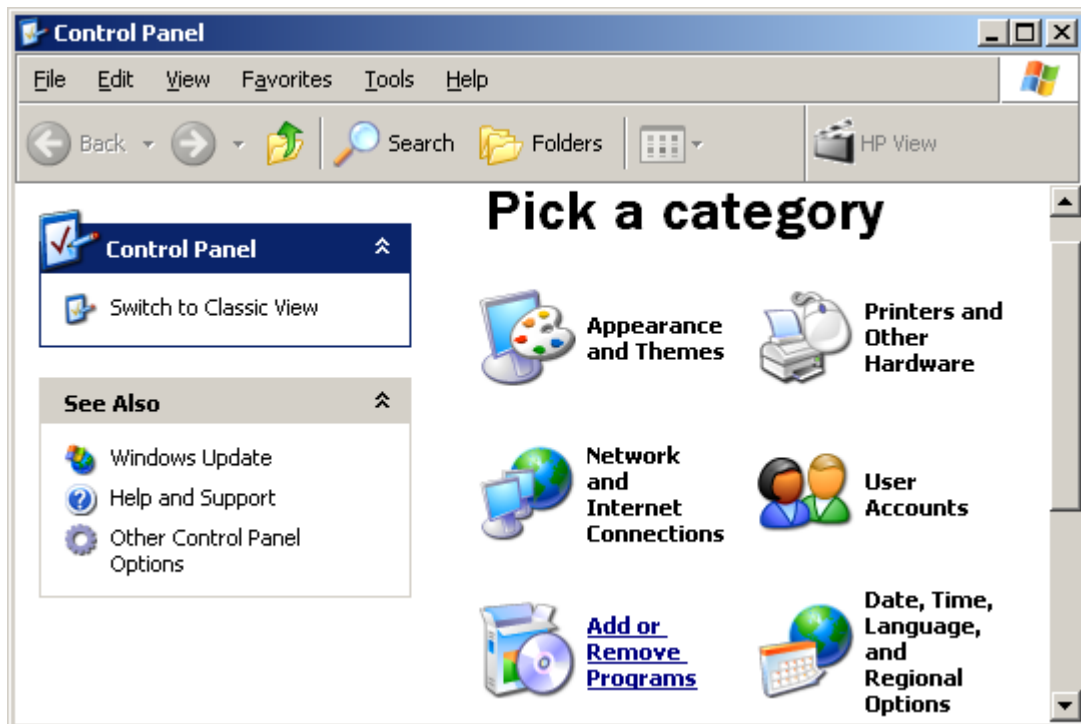- Installation guide for the TupInsight program.
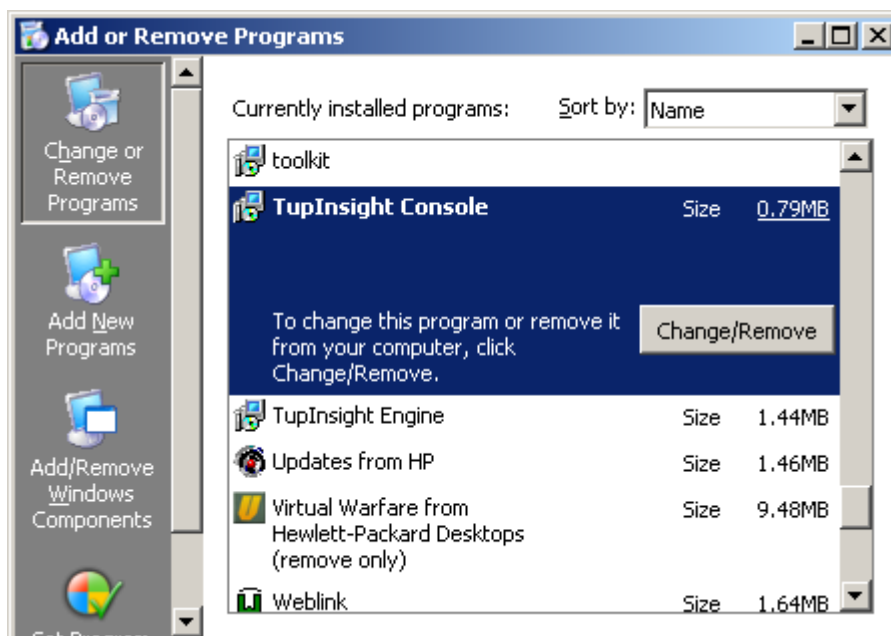
D. Installation procedure

1) Pre-install preparation

(A) Make sure the old version of TupInsight was uninstalled when installing a newer one.
(B) Make sure there are at least 20 MB of free hard disk space for the programs. (If the engine and the console program are separately installed in different host machines, 10 MB would be enough.)

2) Uninstalling the existing TupInsight program

1. Double-click "Add/remove program" in the Windows Control Panel.

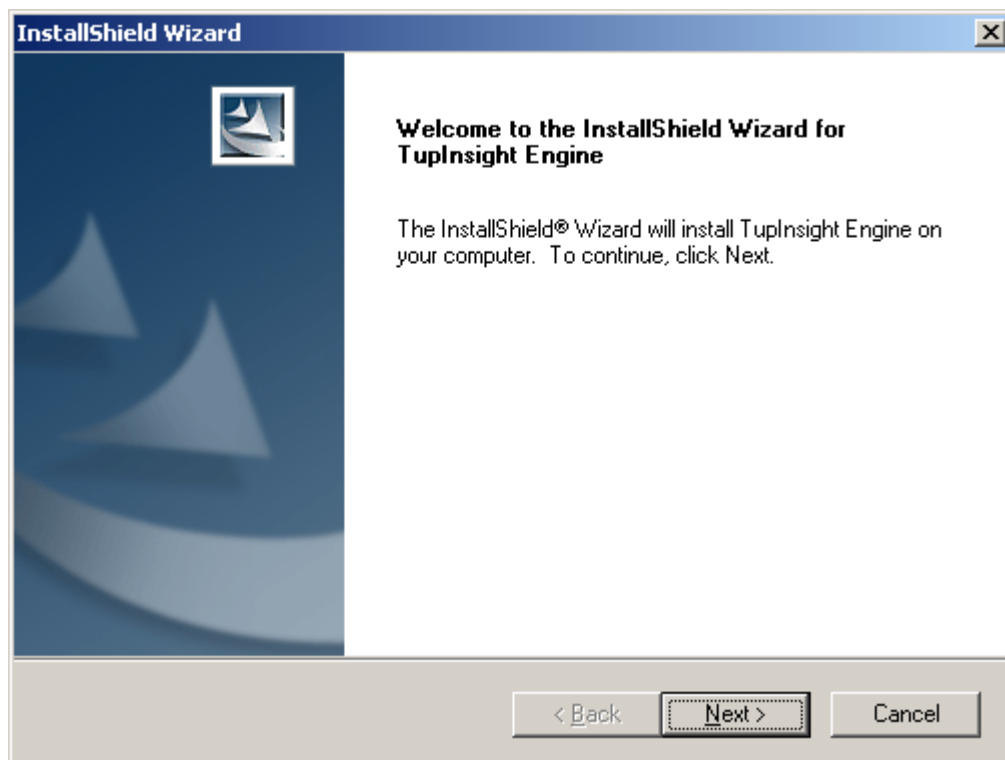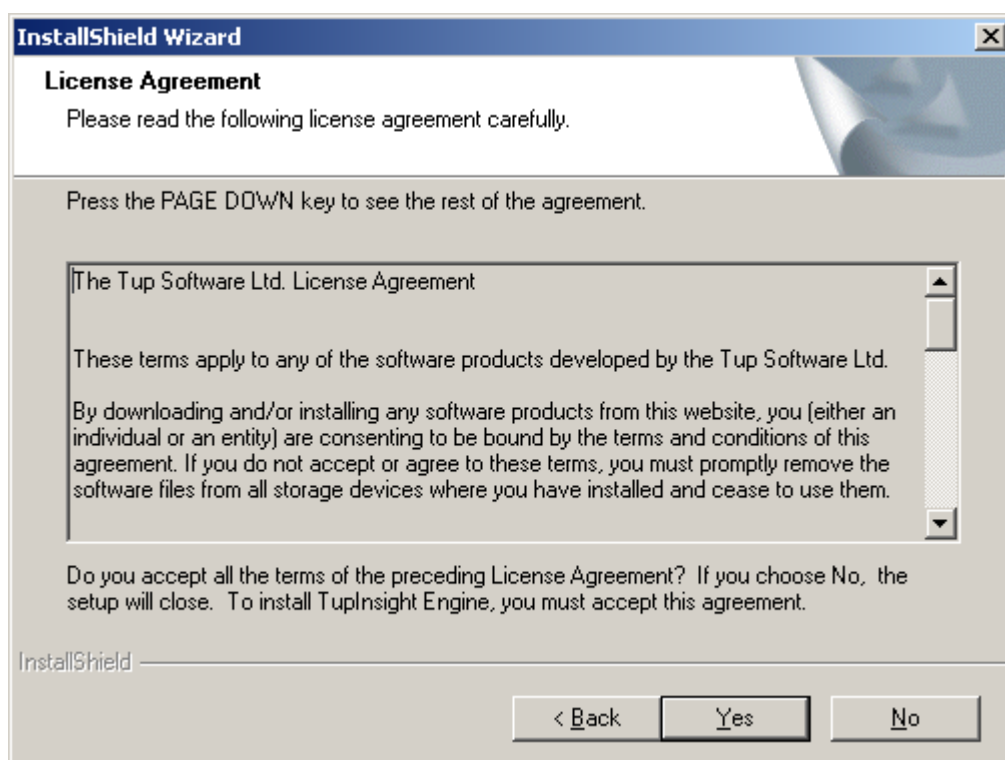2. Select the TupInsight console or engine and click "Change/Remove."

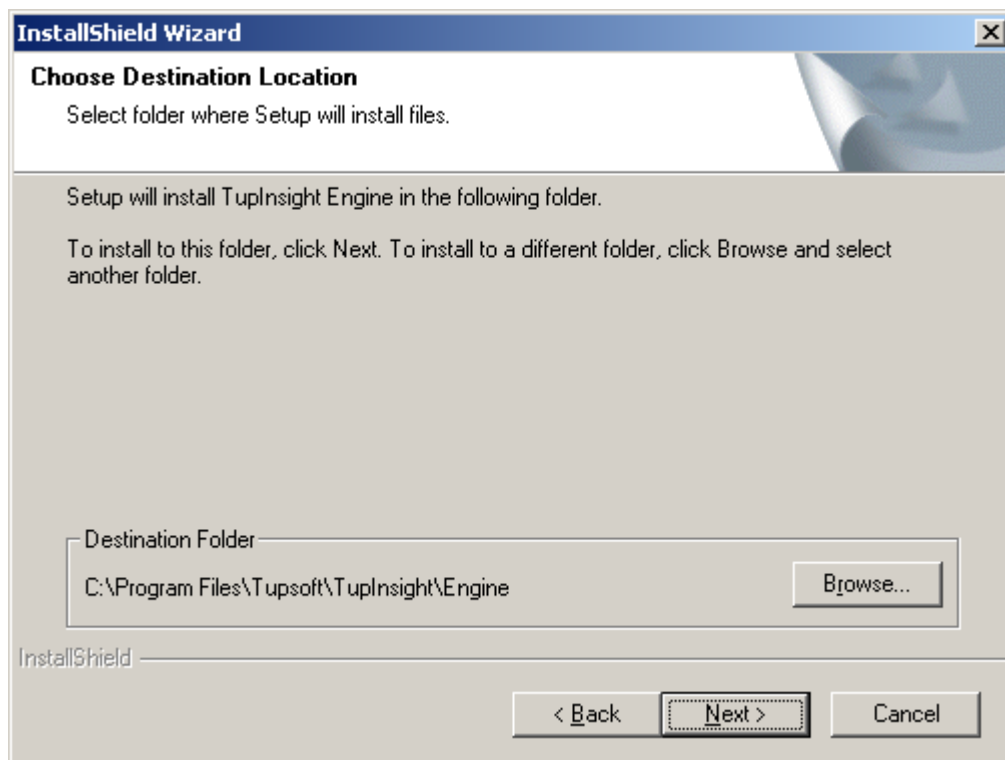**3) Installing the TupInsight engine**

1. Double-click the installation program "Engine.exe," so that the following dialog window appears.
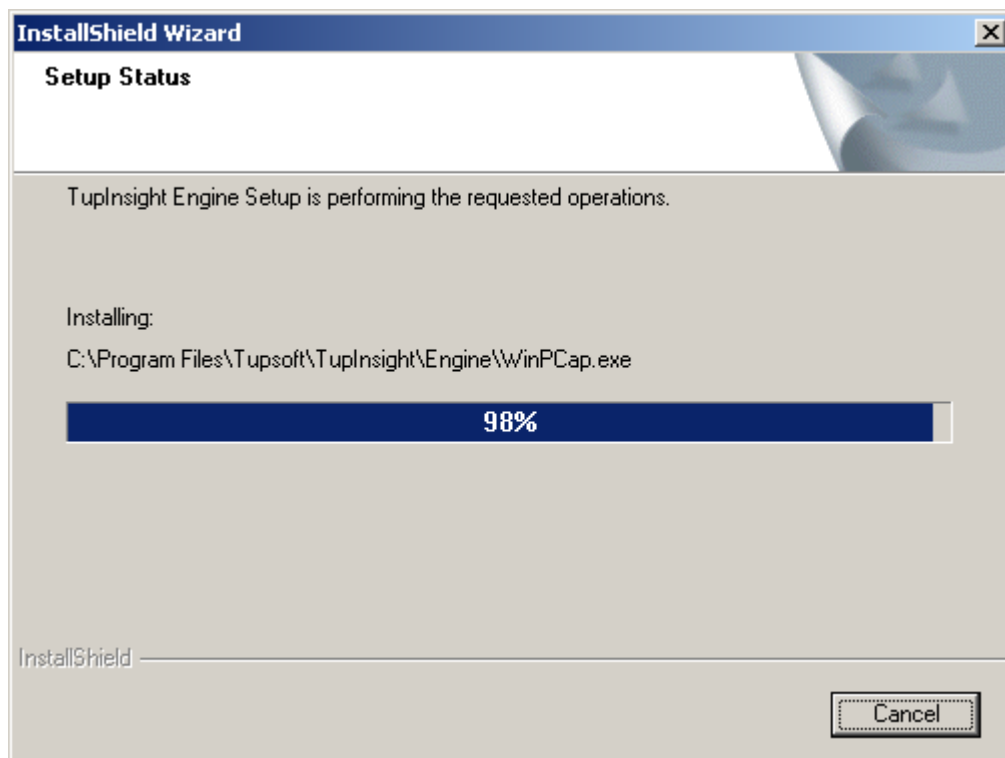

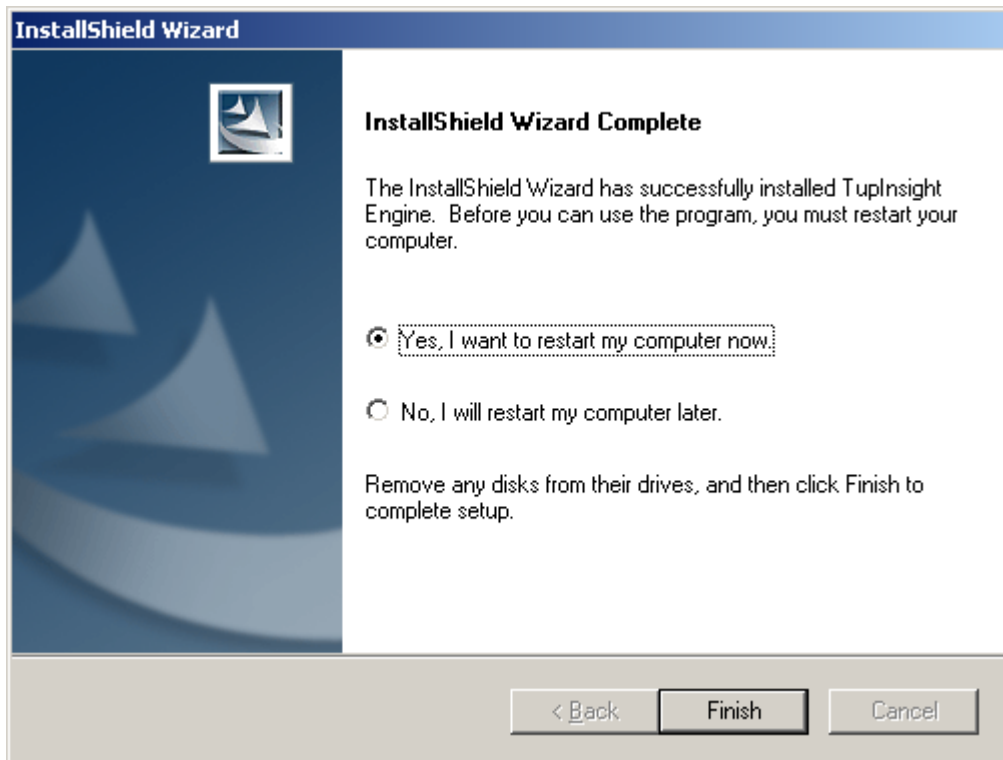2. Single-click "Next" to show the License Agreement as follows.

3. Single-click "Yes" to bring up the following dialog window.

4. Select the destination folder and single-click "Next."

5.   After the above installation steps, you will be asked whether to restart the computer.

6.   Select and single-click "Yes, I want to restart my computer now" to finish the installation procedure.

4)   Installing the TupInsight console

The TupInsight console will be installed on the computer where the administrator can lookup and manage the captured messages.

The installation steps of the TupInsight console are similar to that of the engine, but you will not be asked to restart the computer at the end of installation.

5.   Getting started

The TupInsight engine will auto start after restarting the computer. The console is connected to the engine via TCP protocol and the default port number range is 12881—12885. (If it conflicts with others, you can alter it).

The captured messages are transferred from the engine to the console through TCP protocol. A logon window will pop up automatically when the console is started. To logon, enter the IP address/hostname on which the Engine is installed.

TupInsight is based on the client/server architecture and allows multiple clients logging on the server at the same time. Different operators logon the system with different user names and can be authorized with different levels of rights. Admin is the default administrator for the system and is
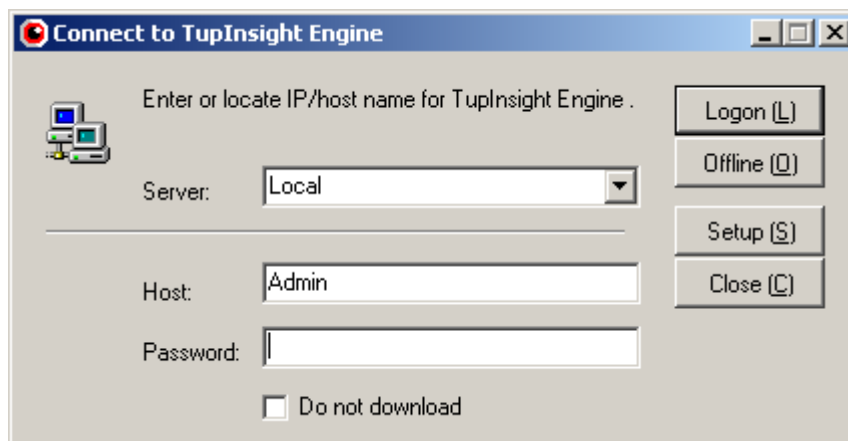
allowed to access all the captured data.

A. Connecting to the TupInsight engine

1. Once the console is running, a screen shows "Tips of the Day."
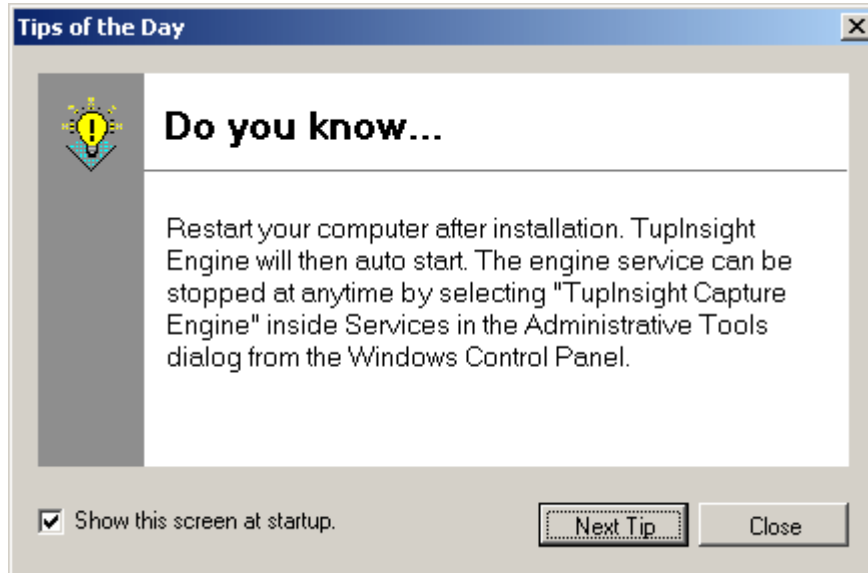
2. Single-click "Close," a dialog window for connecting to the TupInsight engine appears.

3. The default server is the local host, and the user name is Admin with blank (NULL) as the password.
4. After the installation, the administrator password can be changed.
5. If the console and the engine are installed on different computers, the console will automatically search the IP address where the engine is installed and add it into the server list.
6. Enter the password and single-click "Logon."
7. Once successfully, the main user interface will appear.
8. If single-clicking "Offline," another logon window appears to prevent an invalid user from
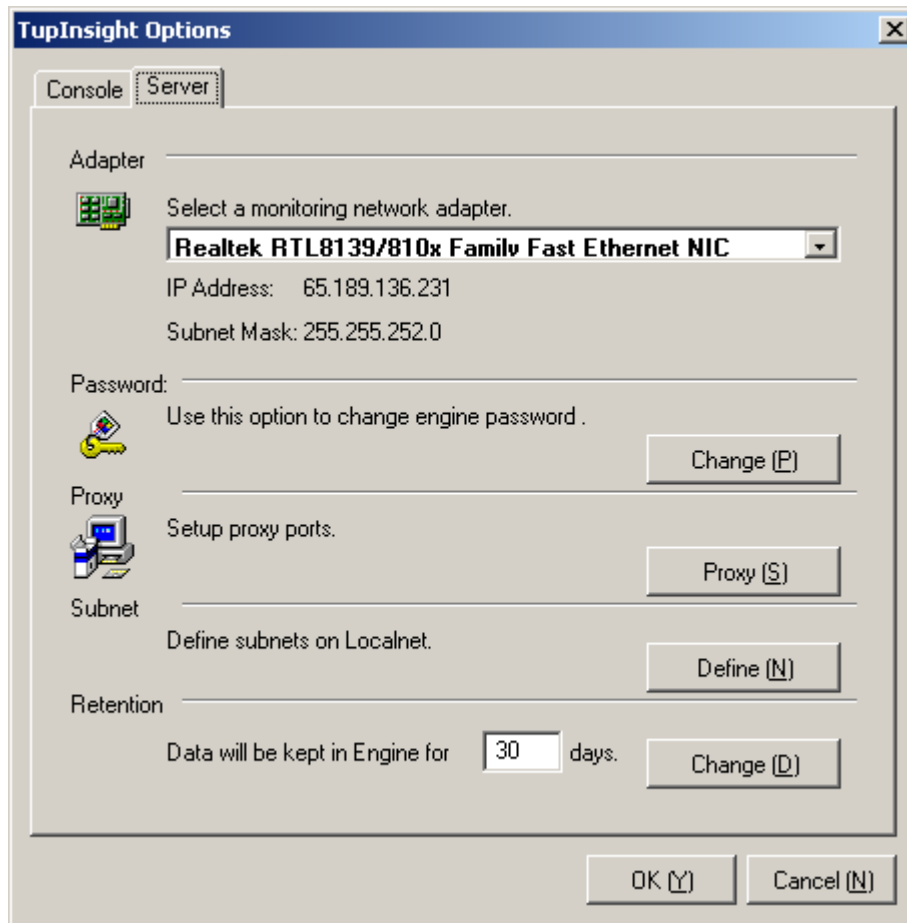
viewing the captured messages.
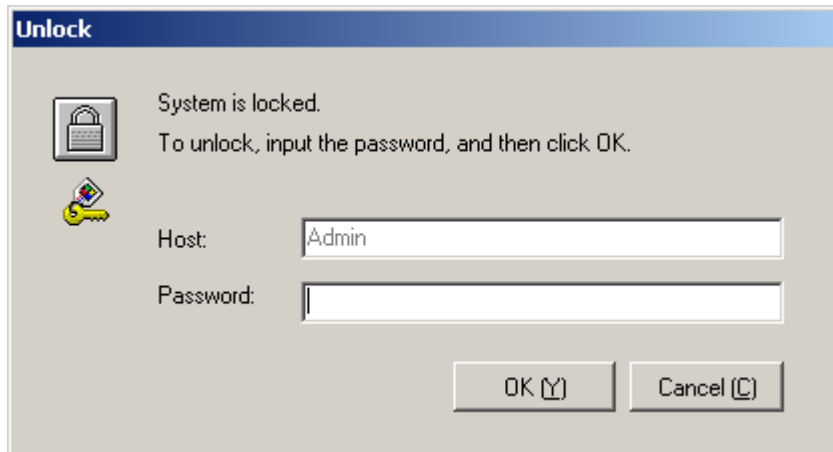
9. The default password is also blank (NULL).

B. Configuring TupInsight program during the first running

When first running TupInsight, the monitoring network adapter for the engine should be configured.

The TupInsight engine will automatically scans the network and select one as the monitoring adapter. When there are more than one network card inside the host, the automatically selected one may not be correct. You can always choose manually via the console. The procedure will be like this:

1. Run the TupInsight console and connect to the engine.

2. Single-click "Tools" from the main menu and then "Options" and select "Server," a window will appear as shown below.

TupInsight Options

Console | Server

Adapter

Select a monitoring network adapter.

Realtek RTL8139/810x Family Fast Ethernet NIC

IP Address: 65.189.136.231

Subnet Mask: 255.255.252.0

Password:

Use this option to change engine password .

Change (P)

Proxy

Setup proxy ports.

Proxy (S)

Subnet

Define subnets on Localnet.

Define (N)

Retention

Data will be kept in Engine for   30   days.

Change (D)

OK (Y)   Cancel (N)

3.   Select one from the available adapters appearing inside the box.

4.   Single-click "OK."

C.   The main user interface

When running the console, the main interface that looks like the following will appear.
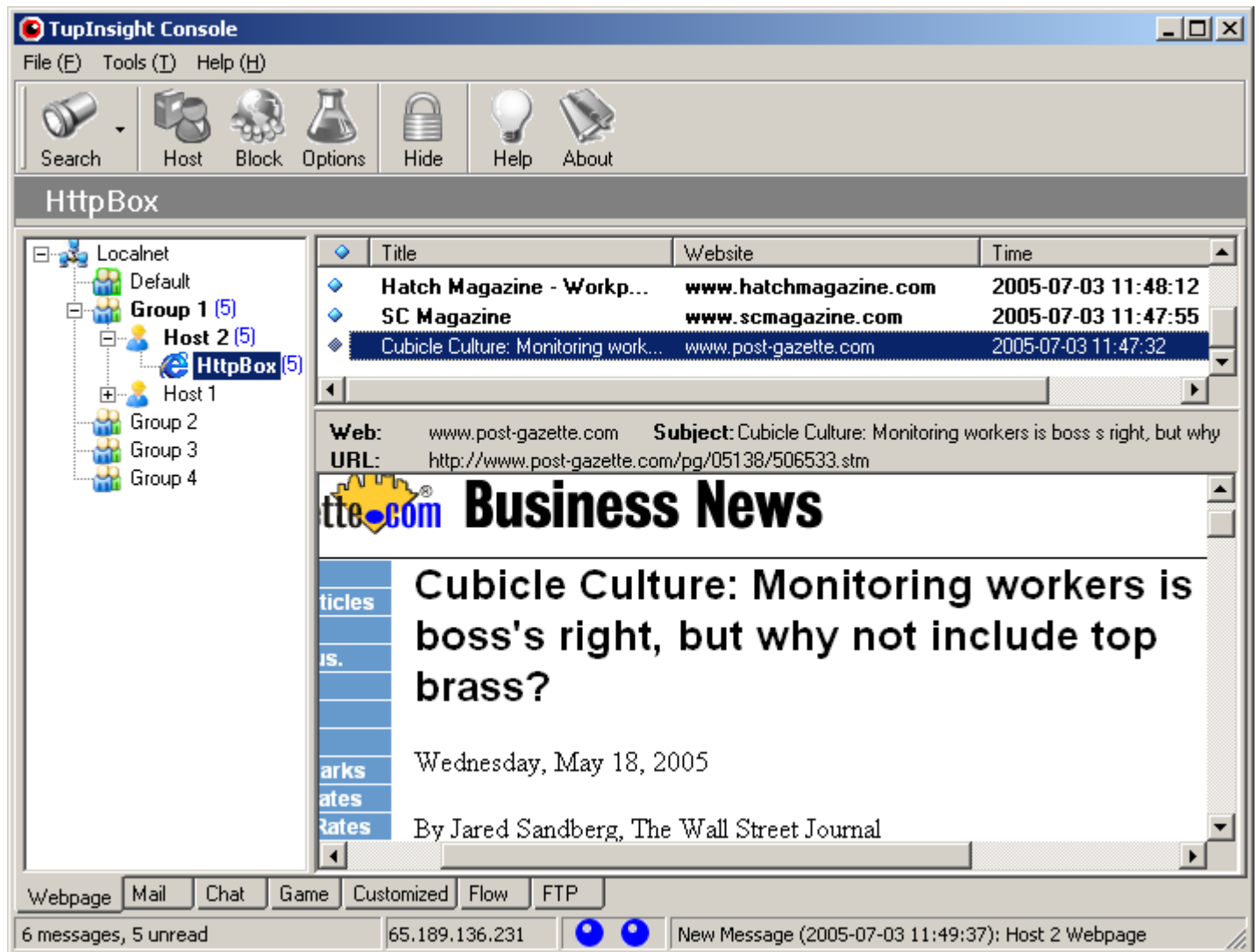
D. Other operations and features

For more functions of the TupInsight program, you can always lookup the Help document by selecting "Help" from the main menu.