

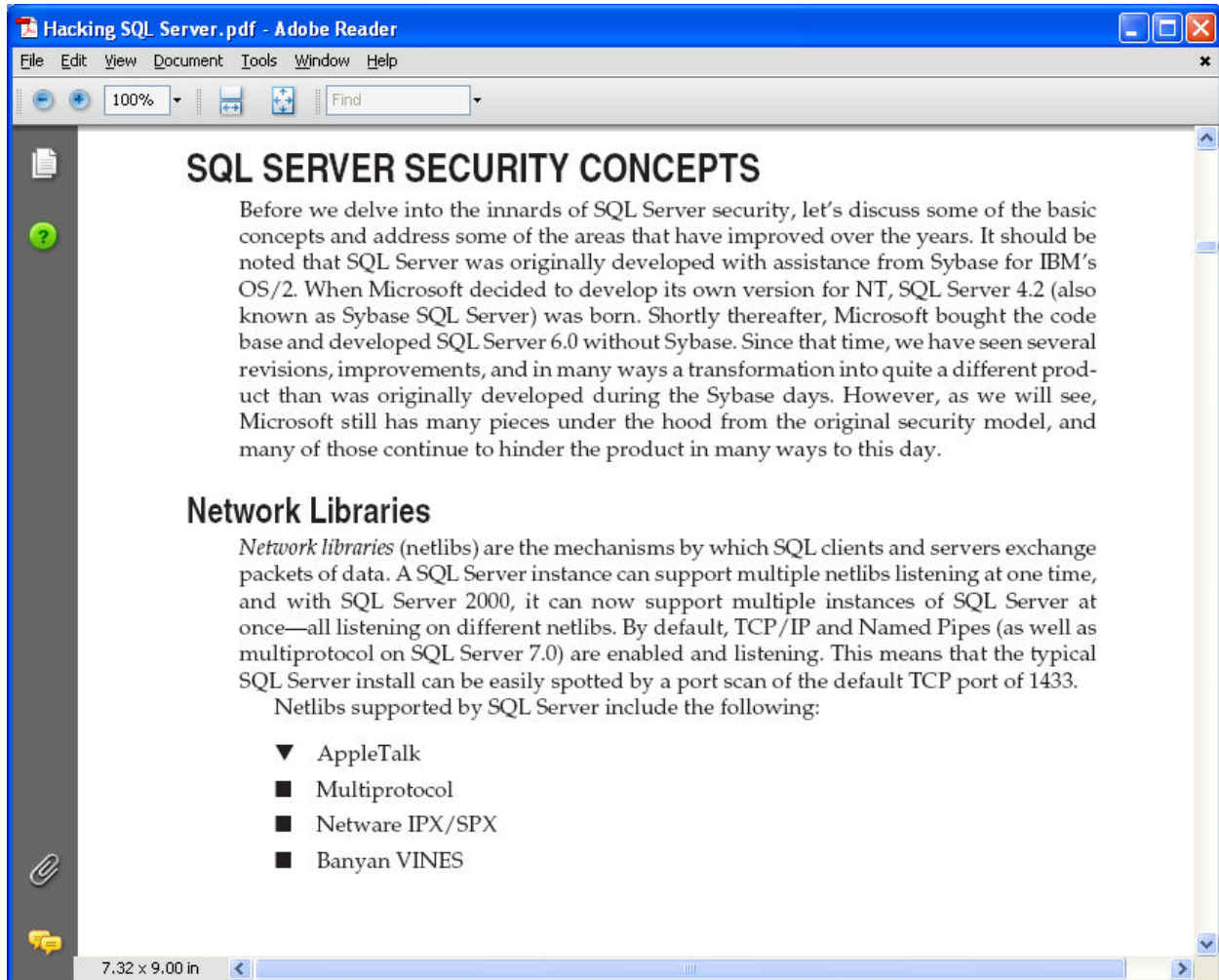


Module 42

Hacking Database Servers

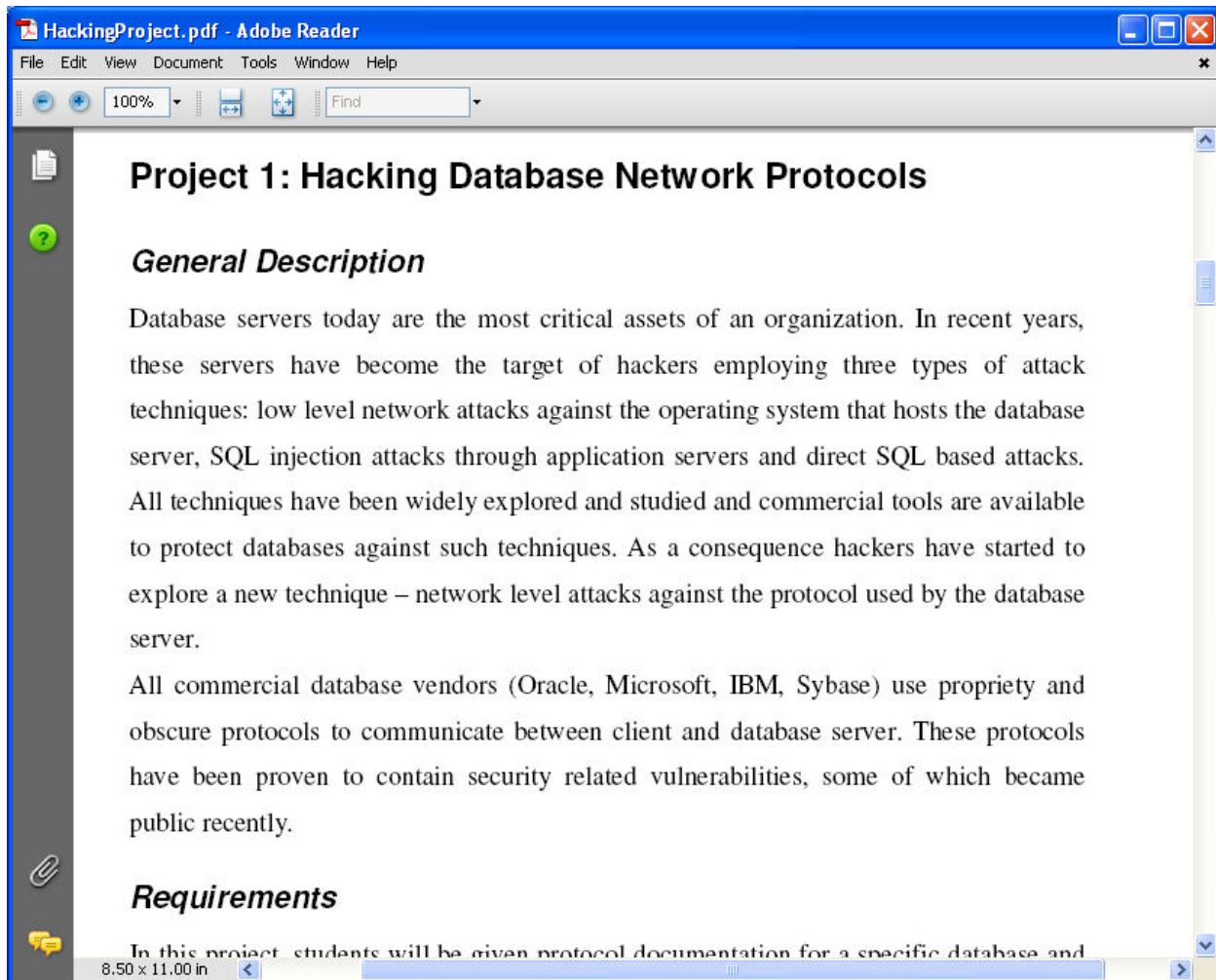
Lab 42-01

- In the **CEHv6 Labs CD-ROM**, navigate to **Module 42**
- Open the **Hacking SQL Server.pdf** file and read the content



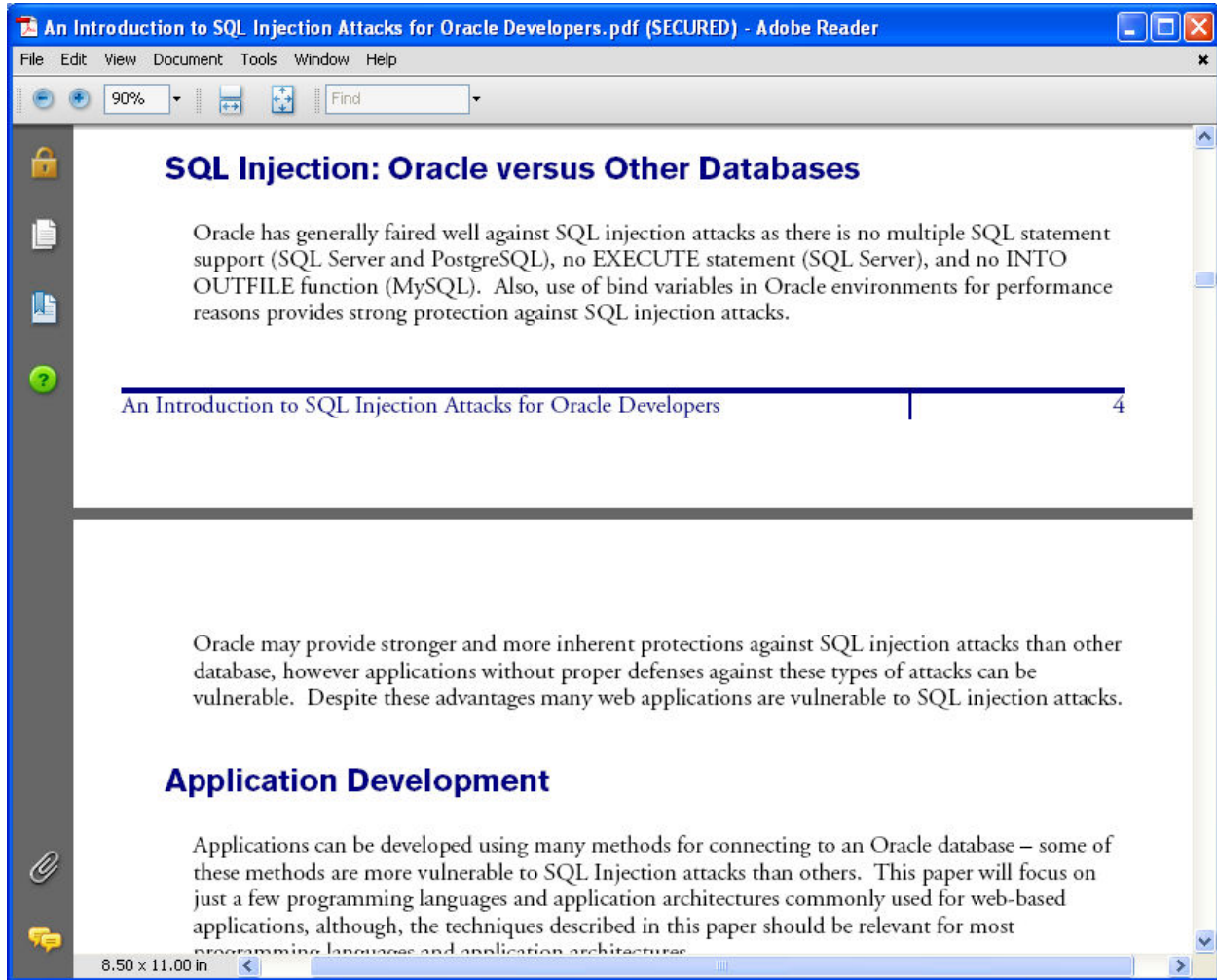
Lab 42-02

- In the **CEHv6 Labs CD-ROM**, navigate to **Module 42**
- Open the **HackingProject.pdf** file and read the content



Lab 42-03

- In the CEHv6 Labs CD-ROM, navigate to **Module 42**
- Open the **An Introduction to SQL Injection Attacks for Oracle Developers.pdf** file and read the content



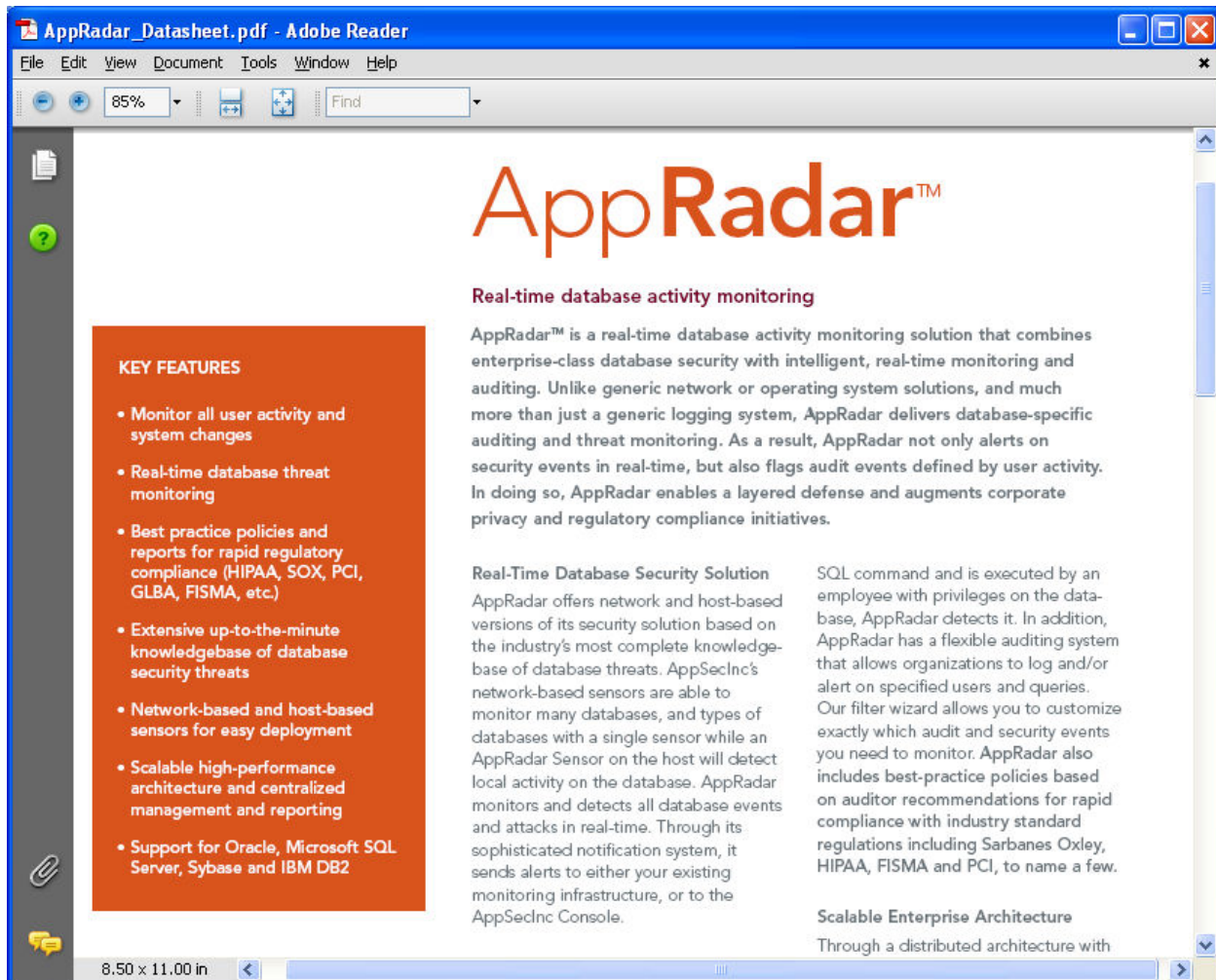
Lab 42-04

- In the CEHv6 Labs CD-ROM, navigate to **Module 42**
- Open the **sql.pdf** file and read the content



Lab 42-05

- In the CEHv6 Labs CD-ROM, navigate to **Module 42**
- Open the **AppRadar_Datasheet.pdf** and read the content



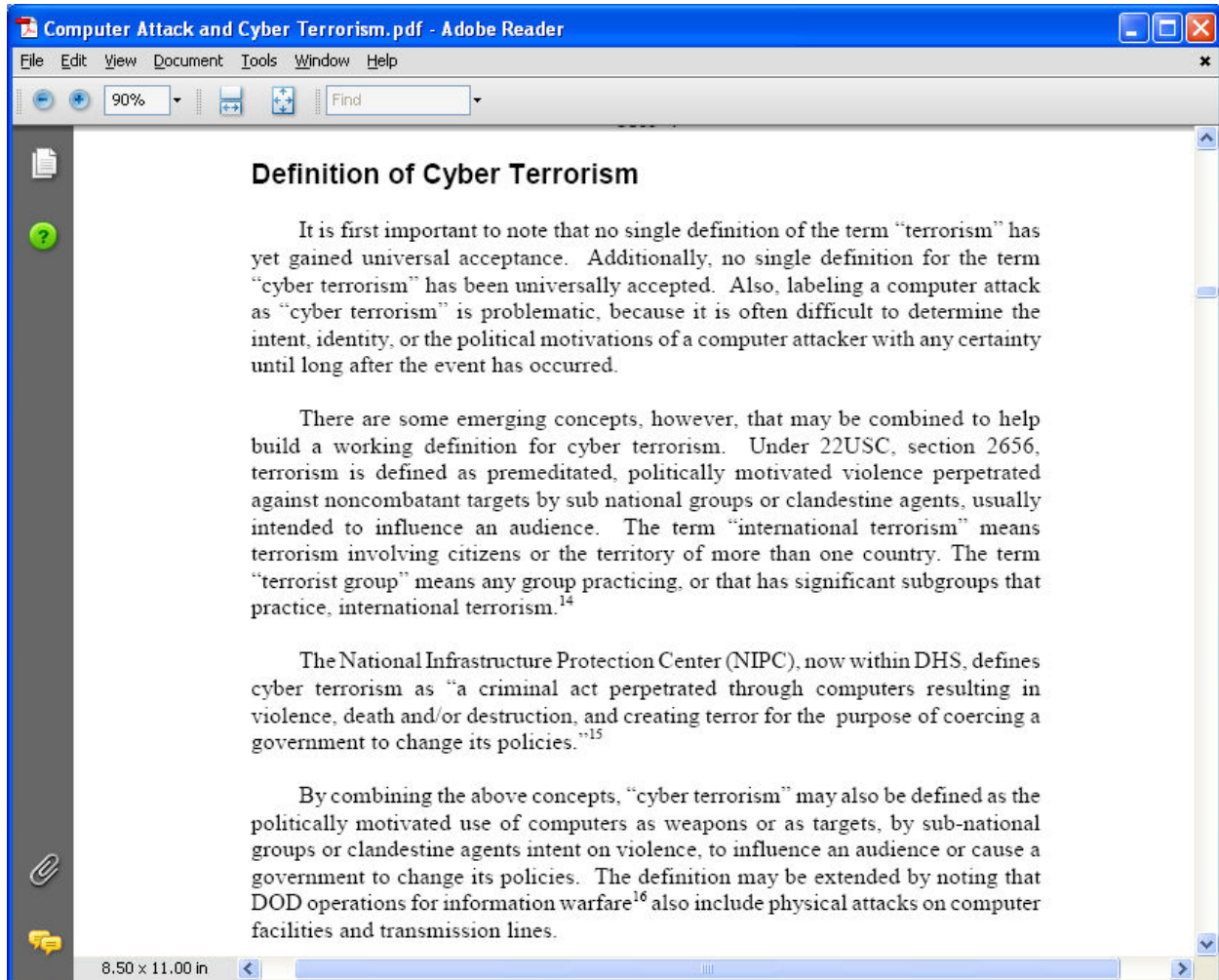


Module 43

Cyber Warfare- Hacking, Al-Qaida, and Terrorism

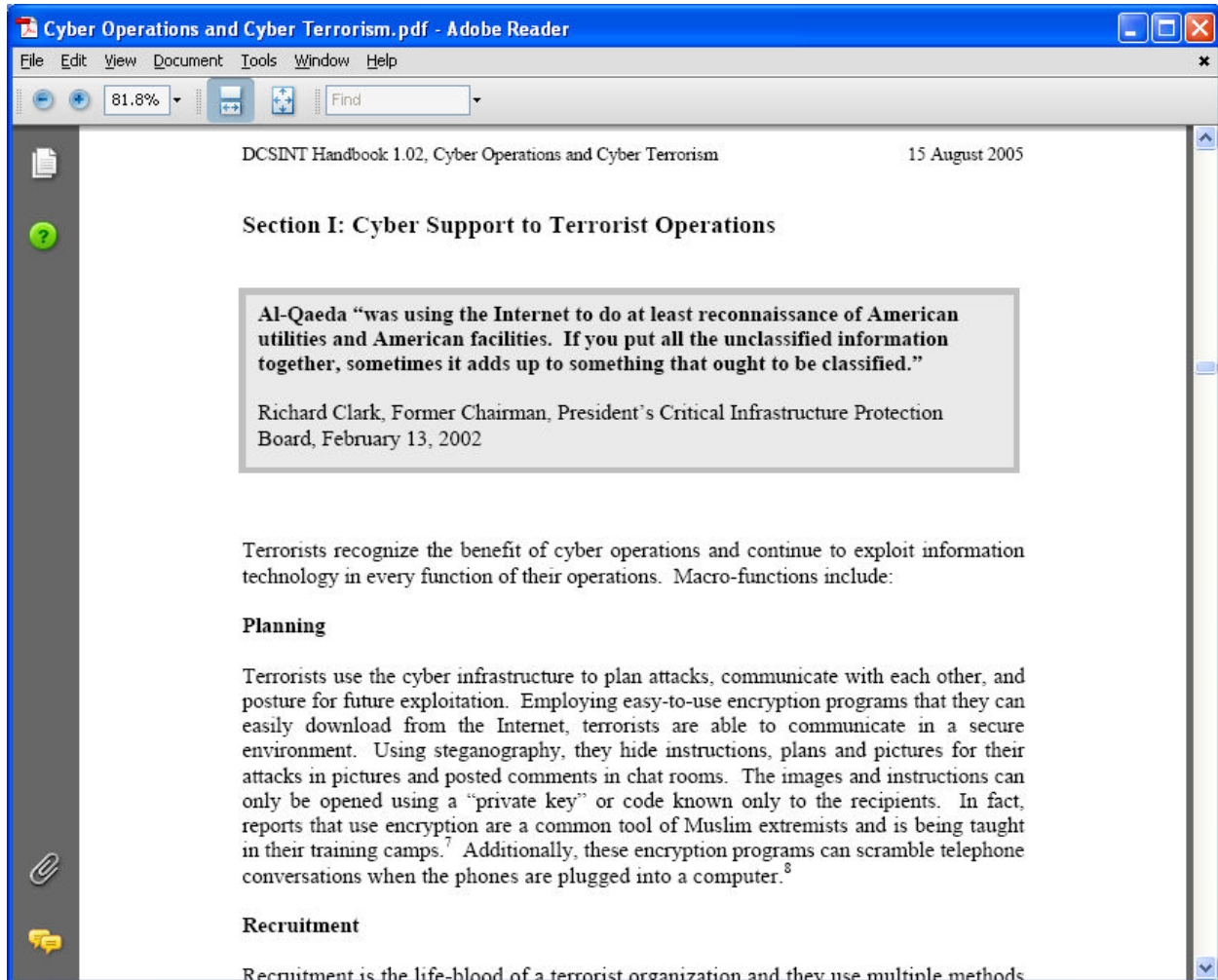
Lab 43-01

- In the CEHv6 Labs CD-ROM, navigate to **Module 43**
- Open the **Computer Attack and Cyber Terrorism.pdf** and read the content



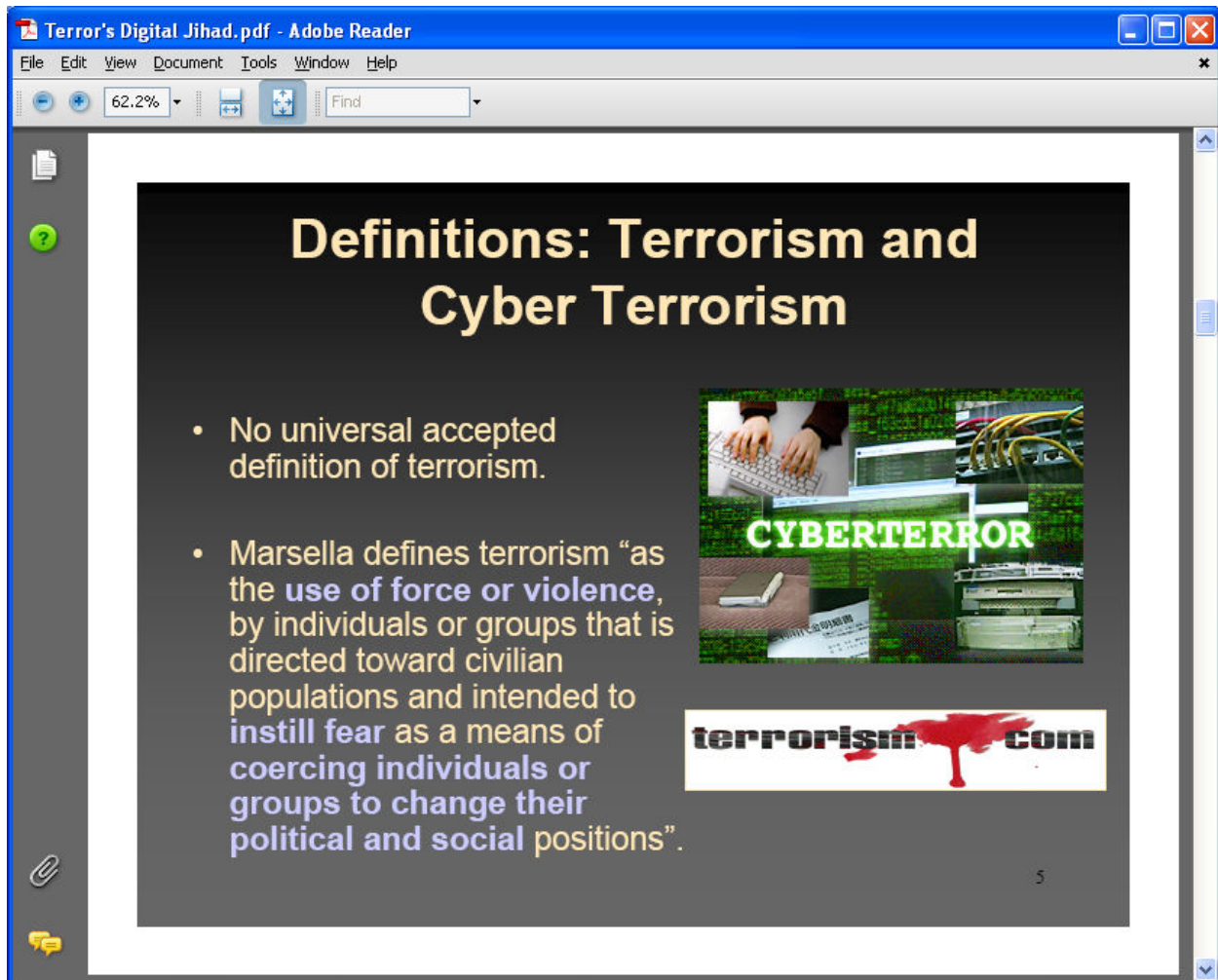
Lab 43-02

- In the **CEHv6 Labs CD-ROM**, navigate to **Module 43**
- Open the **Cyber Operations and Cyber Terrorism.pdf** and read the content



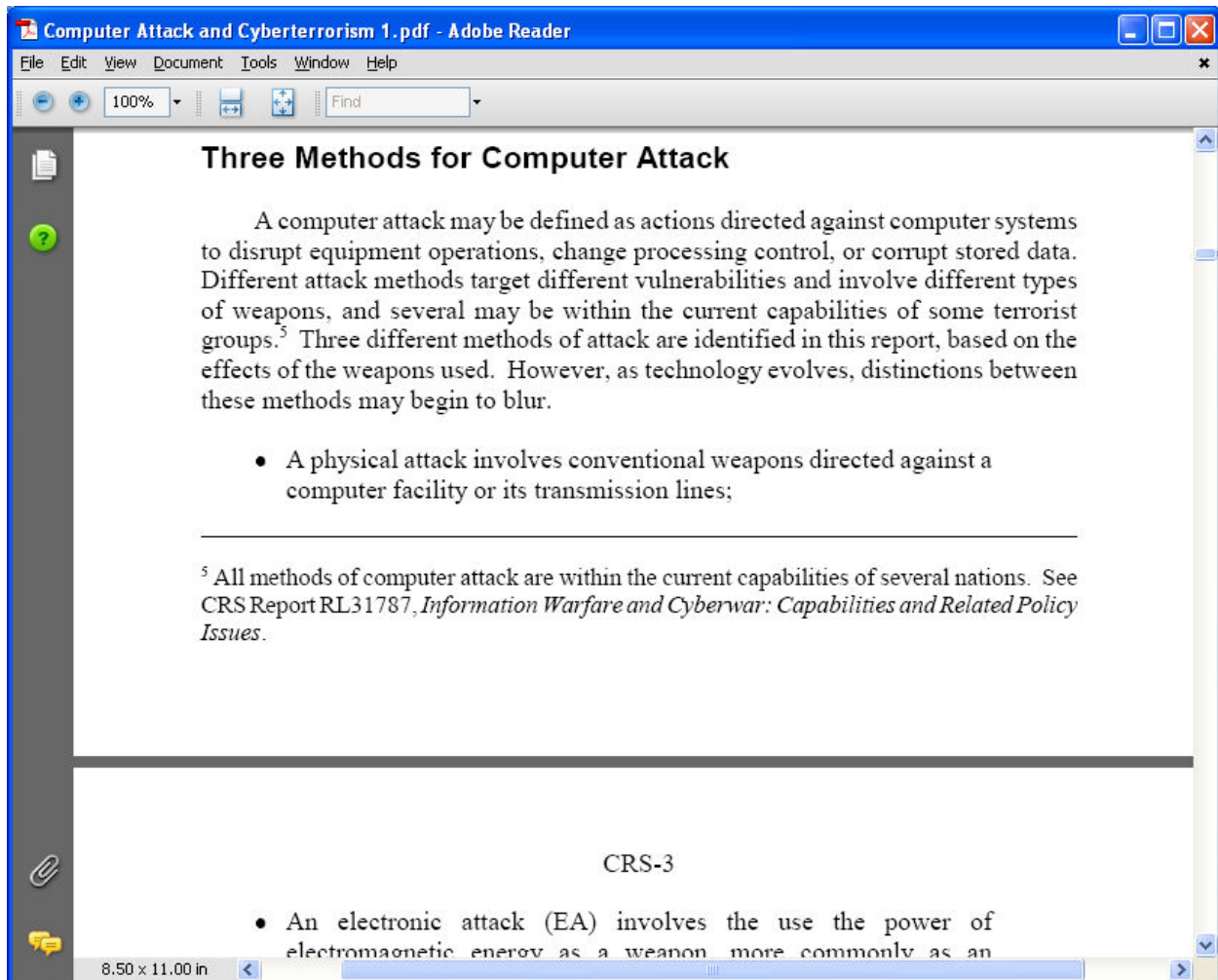
Lab 43-03

- In the **CEHv6 Labs CD-ROM**, navigate to **Module 43**
- Open the **Terror's Digital Jihad.pdf** and read the content



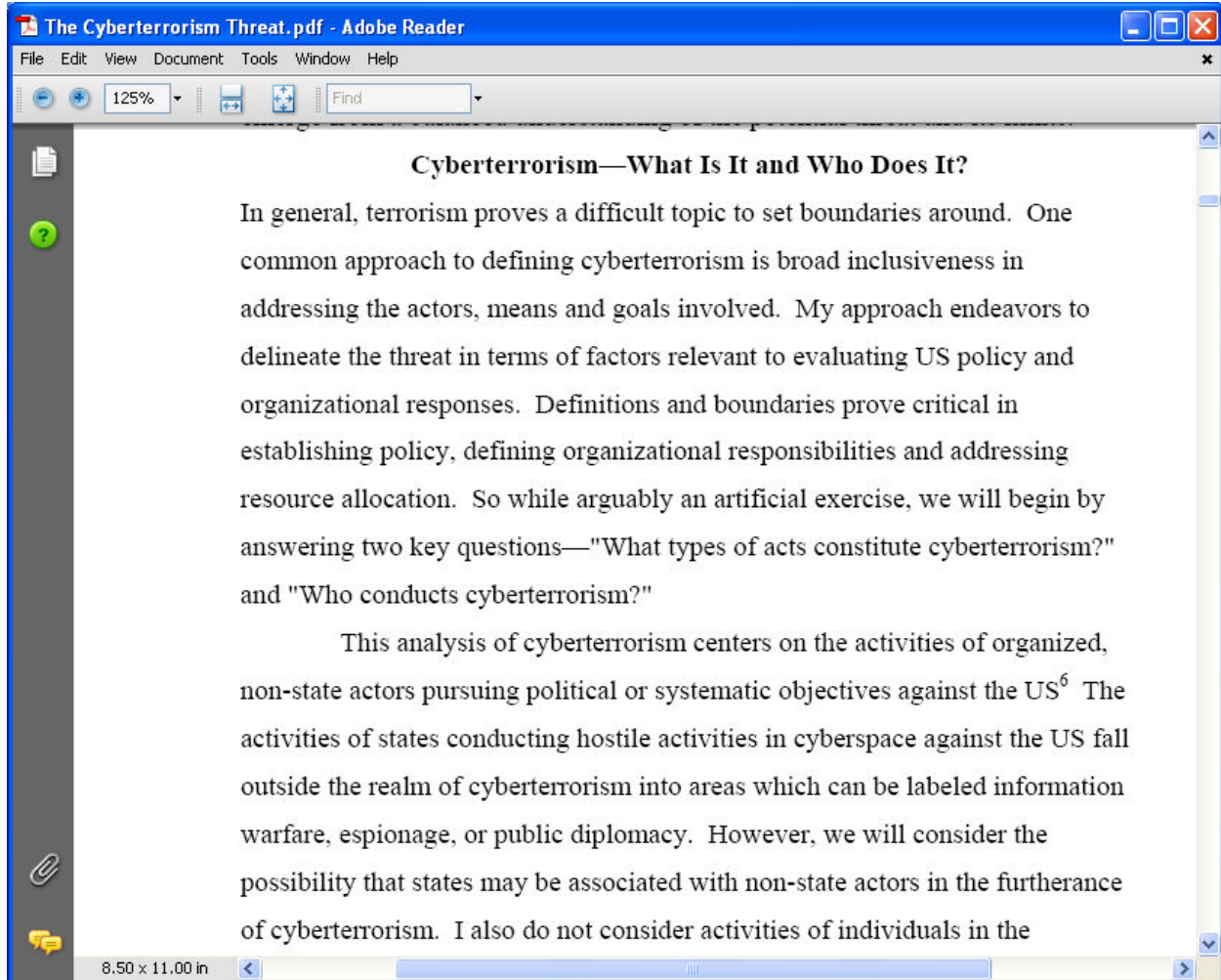
Lab 43-04

- In the **CEHv6 Labs CD-ROM**, navigate to **Module 43**
- Open the **Computer Attack and Cyberterrorism 1.pdf** and read the content



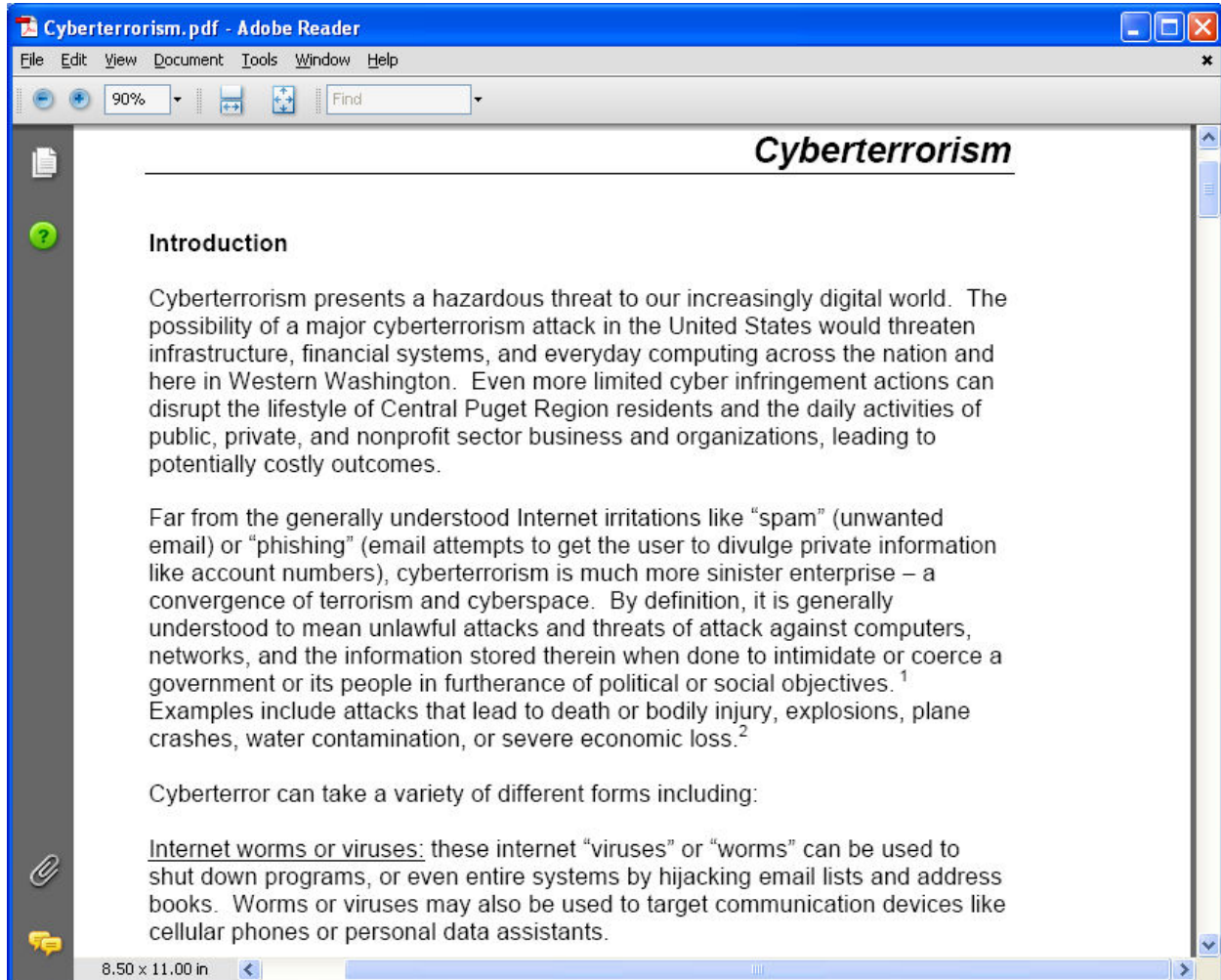
Lab 43-05

- In the **CEHv6 Labs CD-ROM**, navigate to **Module 43**
- Open **The Cyberterrorism Threat.pdf** and read the content



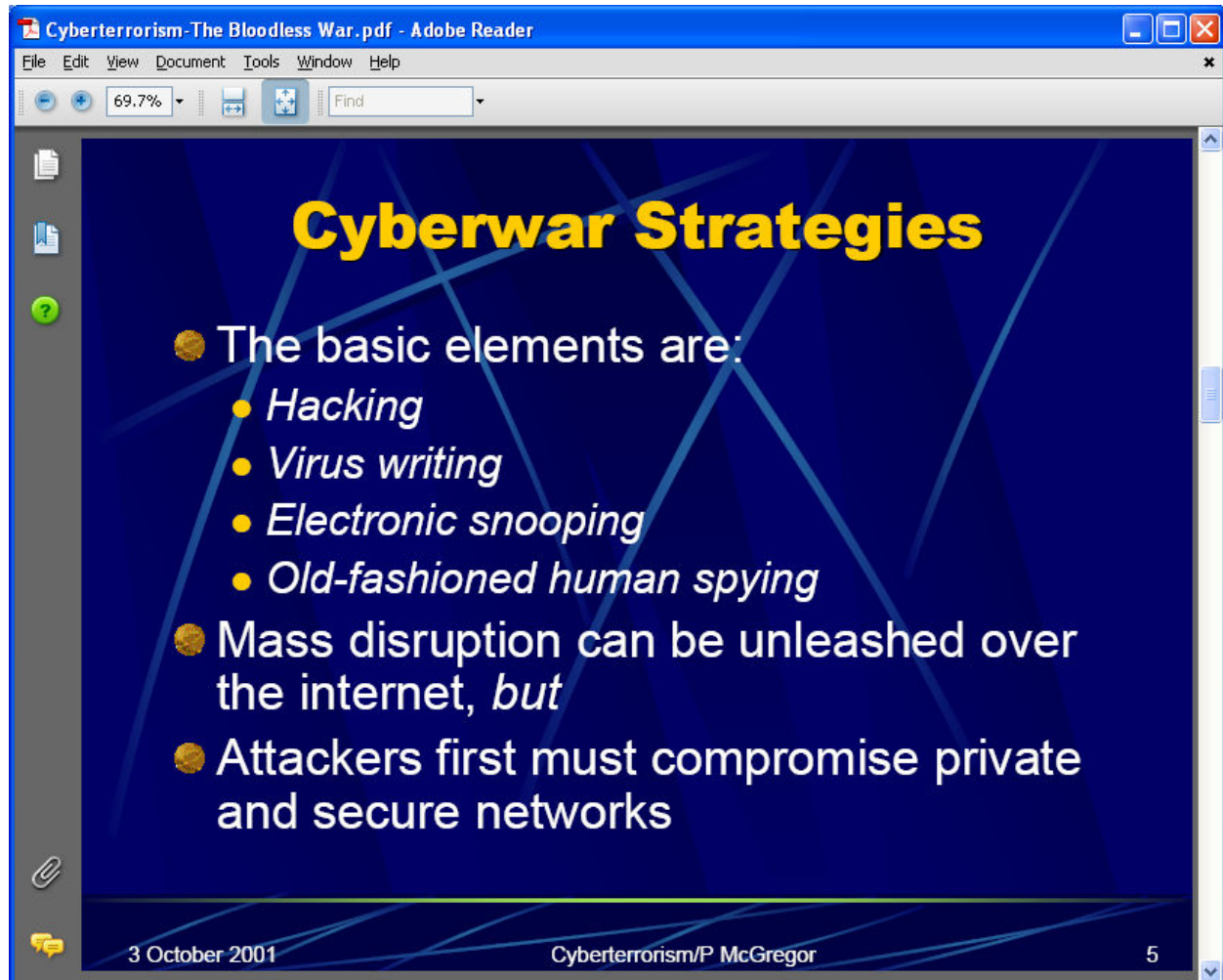
Lab 43-06

- In the **CEHv6 Labs CD-ROM**, navigate to **Module 43**
- Open the **Cyberterrorism.pdf** and read the content



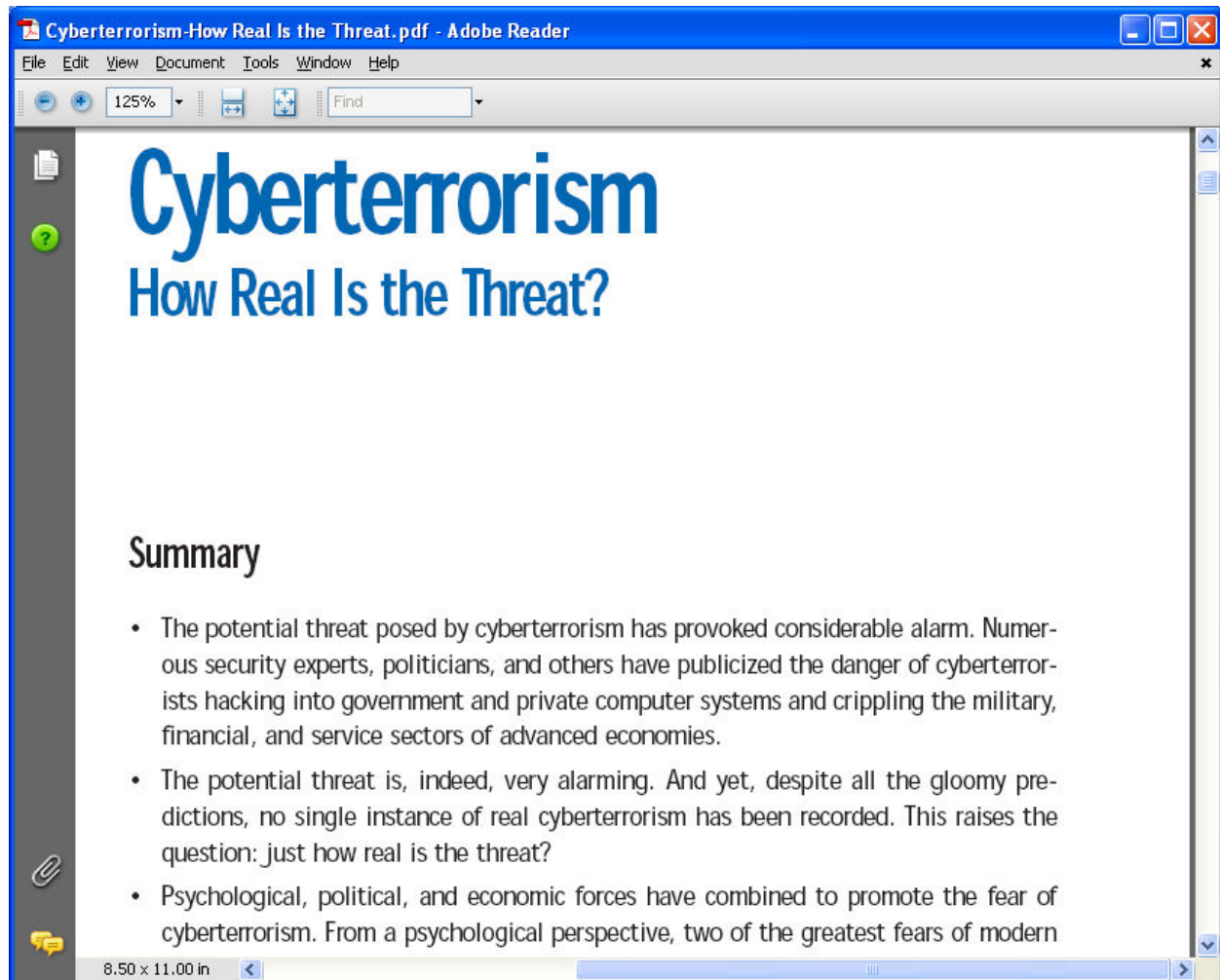
Lab 43-07

- In the CEHv6 Labs CD-ROM, navigate to **Module 43**
- Open the **Cyberterrorism-The Bloodless War.pdf** and read the content



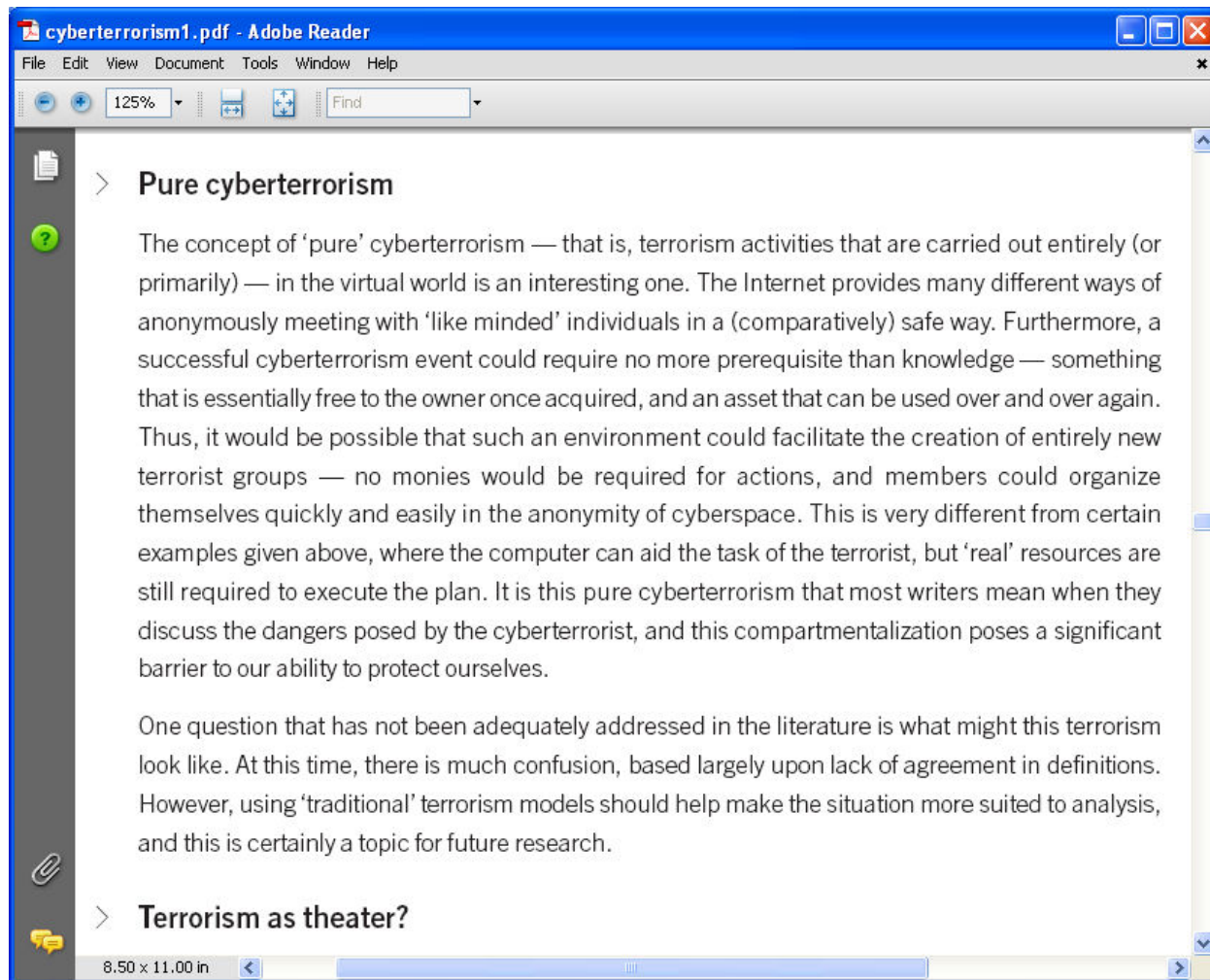
Lab 43-08

- In the **CEHv6 Labs CD-ROM**, navigate to **Module 43**
- Open the **Cyberterrorism-How Real Is the Threat.pdf** and read the content



Lab 43-09

- In the **CEHv6 Labs CD-ROM**, navigate to **Module 43**
- Open the **1yberterrorism 1.pdf** and read the content





Module 44

Internet Content Filtering Techniques

Lab 44-01

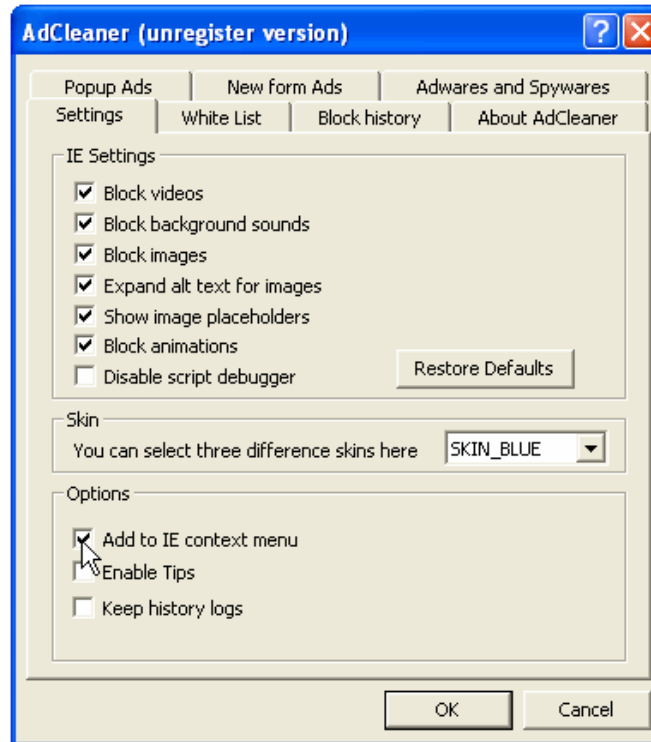
Objective:

Use **Ad Cleaner** to block adware and popups.

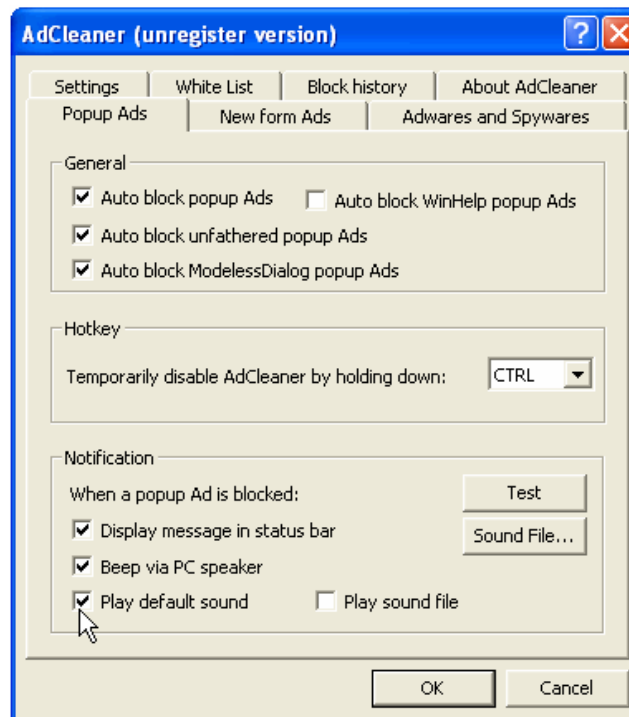
- In the **CEHv6 Labs CD-ROM**, navigate to **Module 44**
- Install and launch **AdCleaner** program



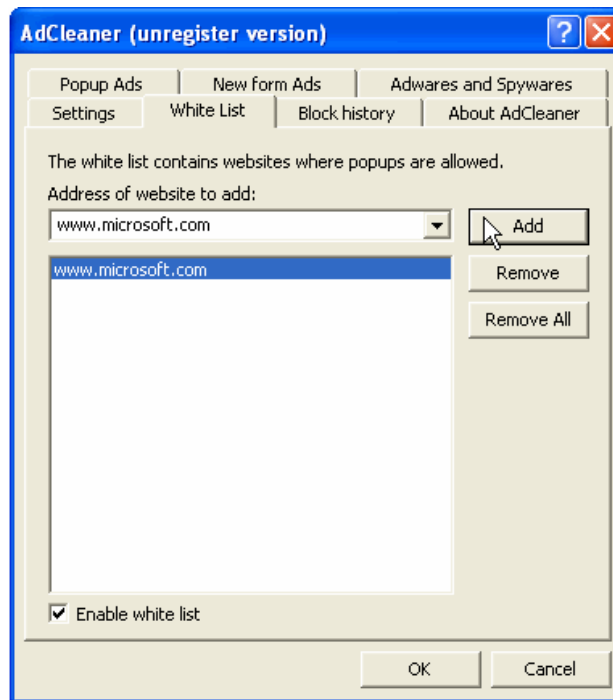
- Go to Settings tab. Set the required IE settings and Options by enabling the check boxes



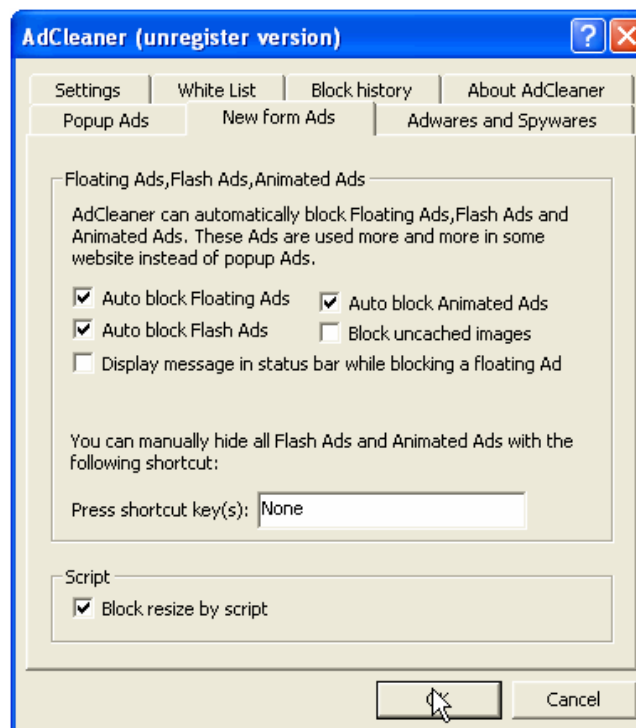
- Go to **Popup Ads** tab and check the required options to block popup ads



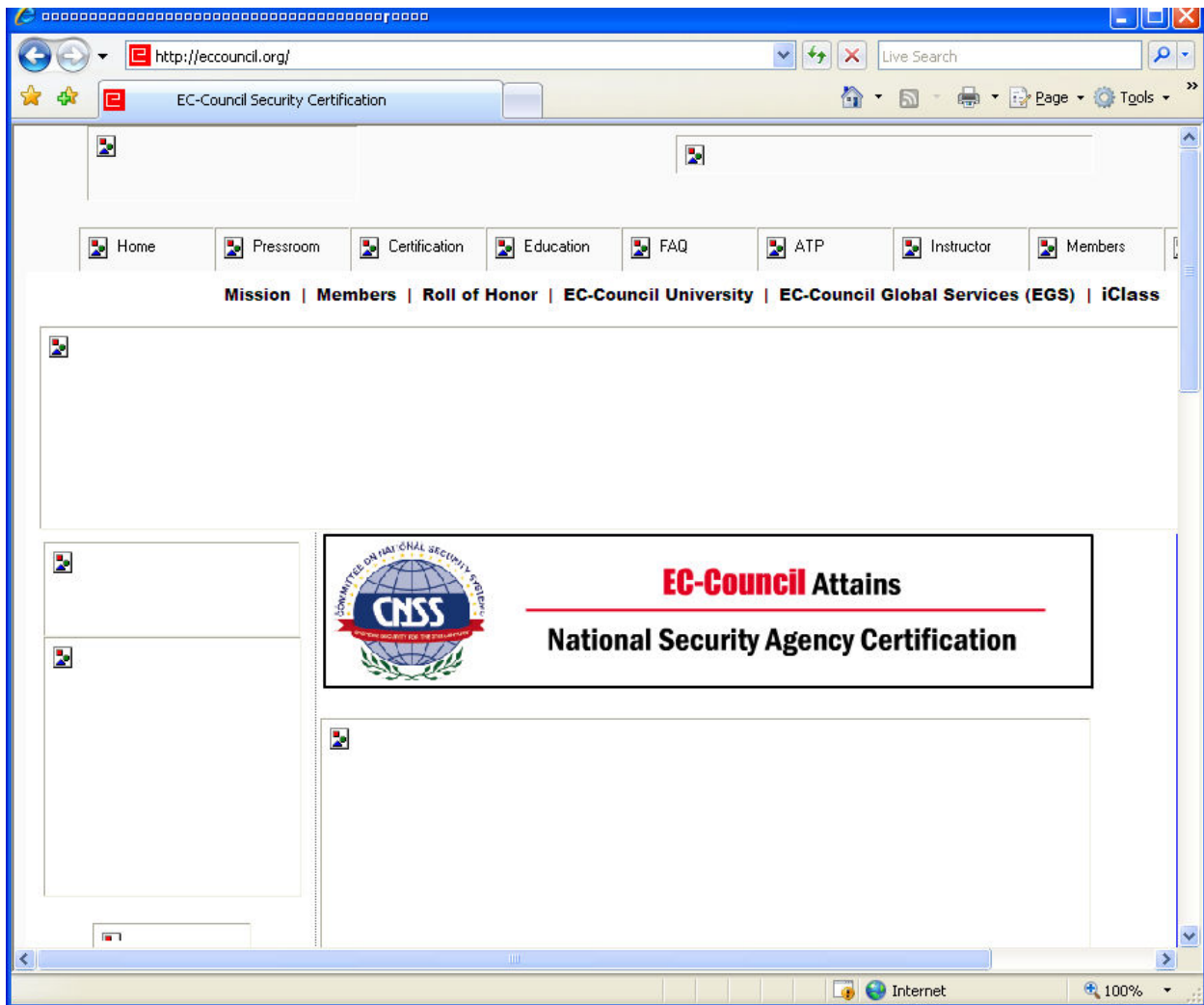
- Go to **White List** tab and click **Add** button to add websites for which you want the popups to be allowed



- Go to **New form Ads** tab to block the new form of ads. Check the required options and click **OK**.



- Open a site in IE , the adware and pop-ups will be blocked



Lab 44-02

Objective:

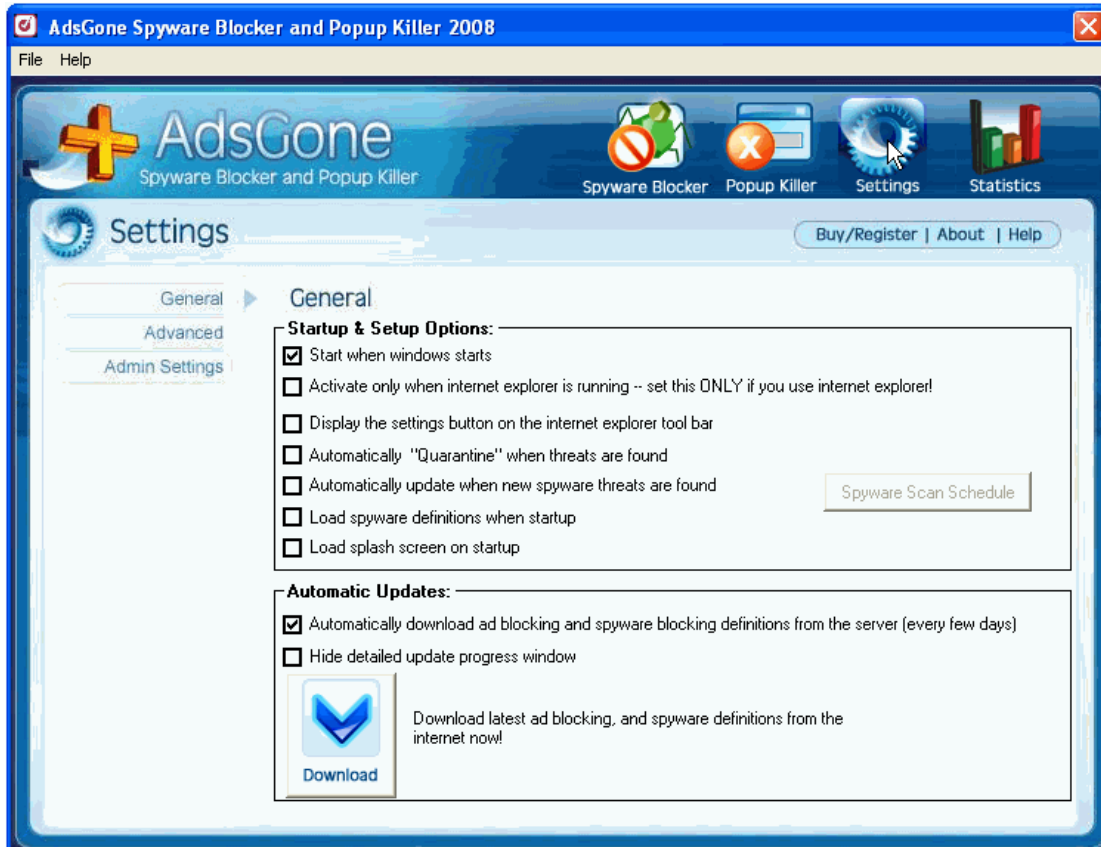
Use **AdsGone Popup Killer** to avoid hazardous popup and banner advertisements.

- In the **CEHv6 Labs CD-ROM**, navigate to **Module 44**
- Install and launch **AdsGone Popup Killer** program

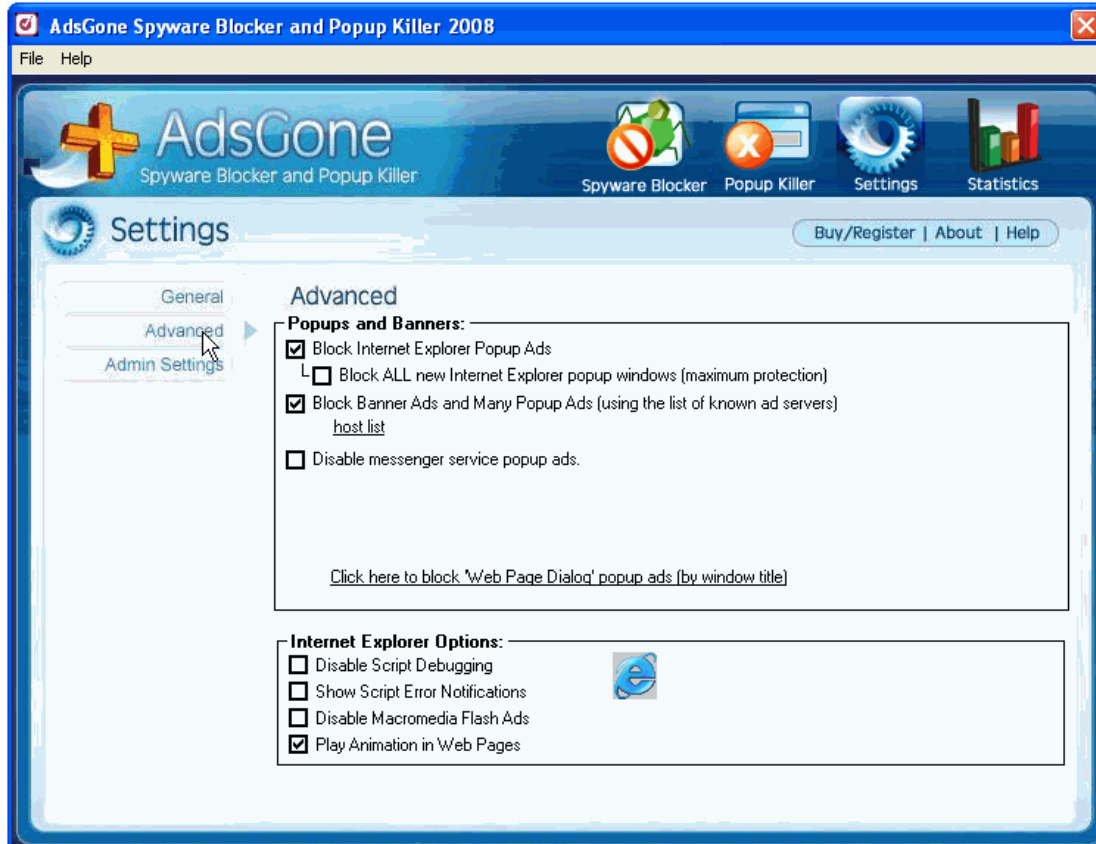




- Click on the **Settings** button. **General** settings are displayed by default.



- Click **Advanced** link to configure advanced settings.



- Click on **Admin Settings** link to configure administrative settings and explore various options.

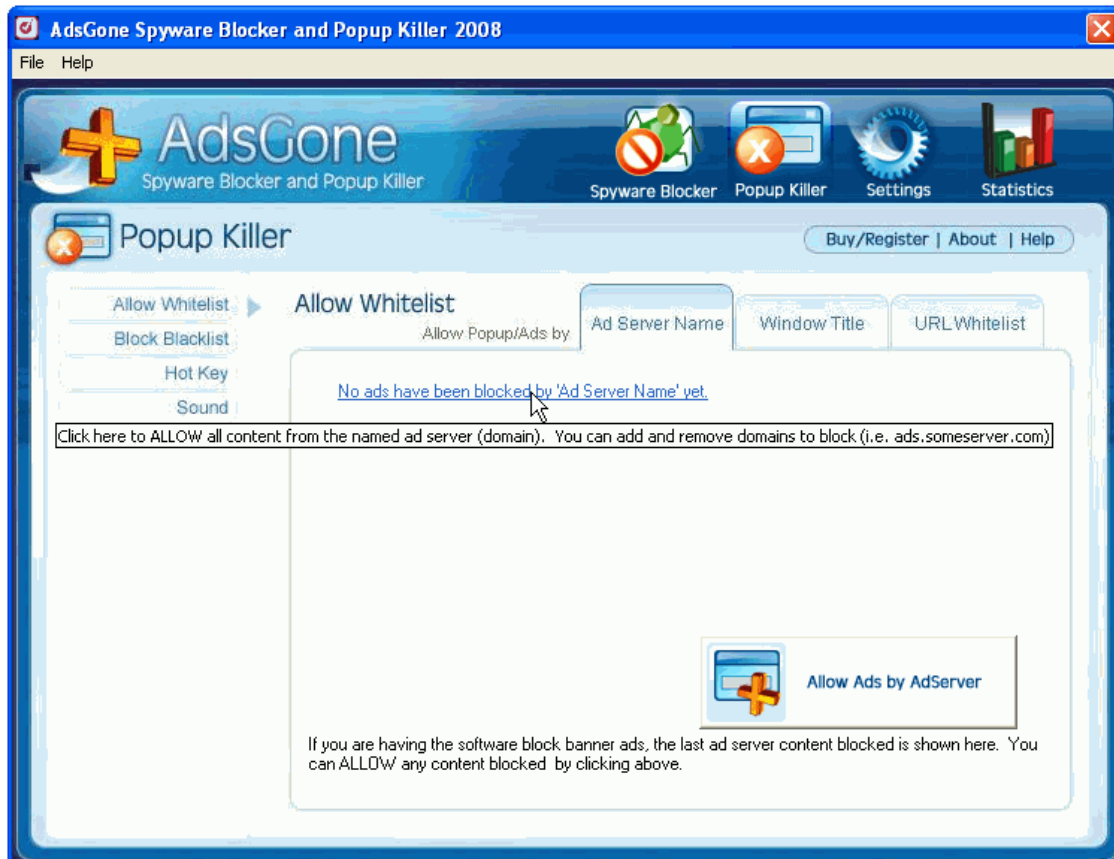




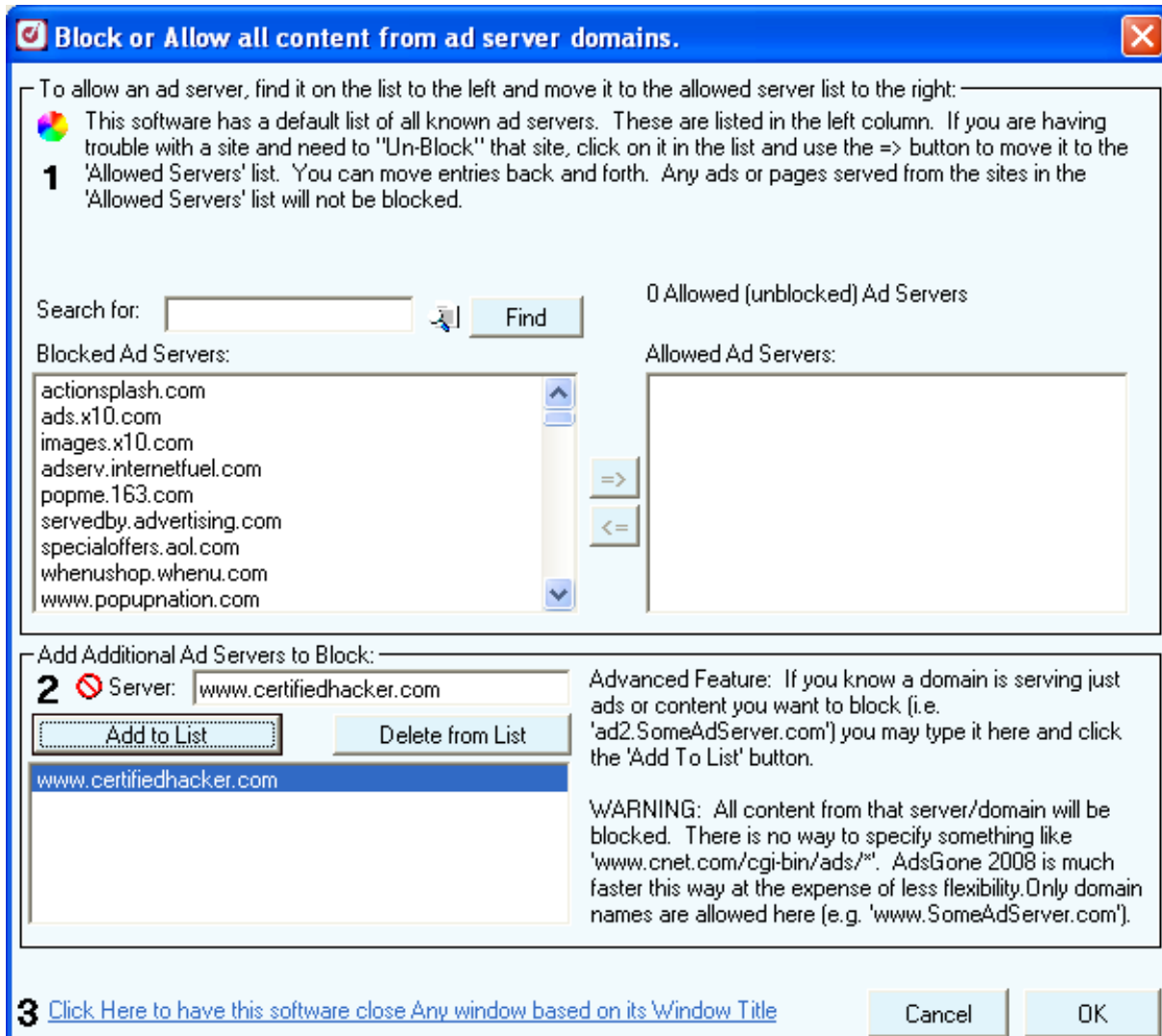
- Click **Popup Killer** button to configure the popup killer.



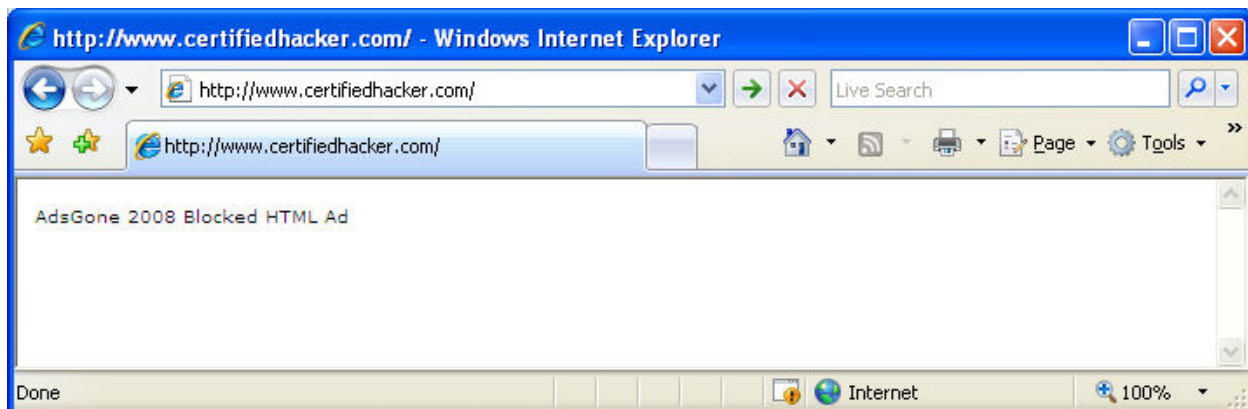
- Go to **Ad server Name** tab and click on **No ads have been blocked 'Ad Server' Name Yet** link



- Enter the ad server name and click **Add to List**.



- Try to open blocked site.

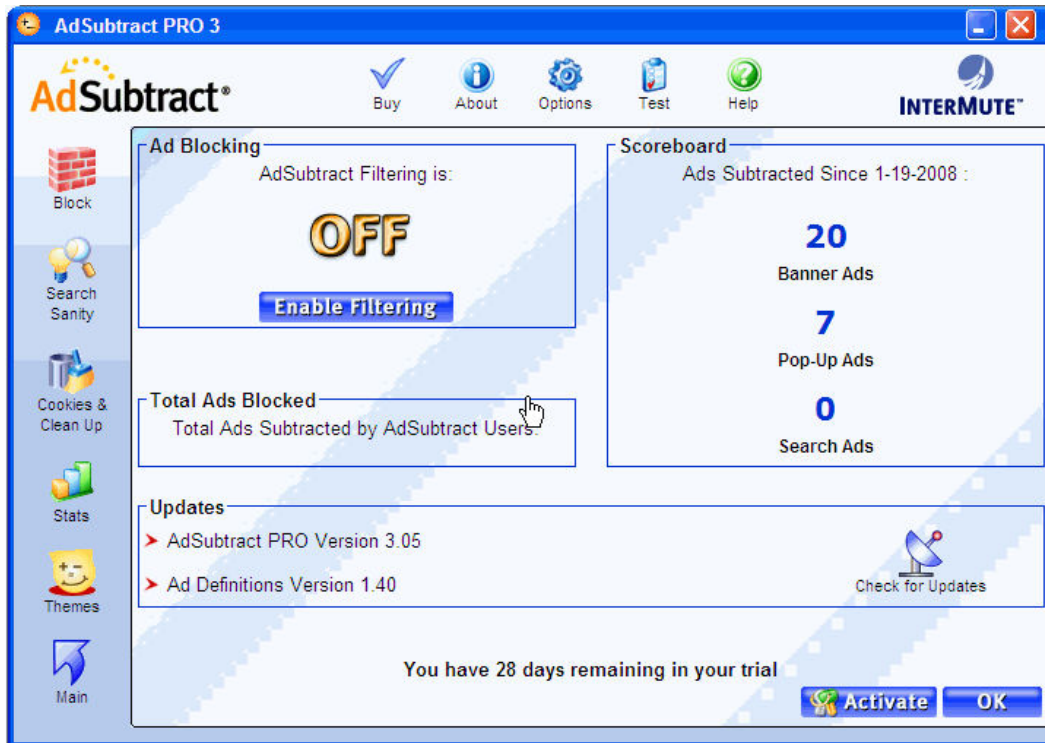


Lab 44-03

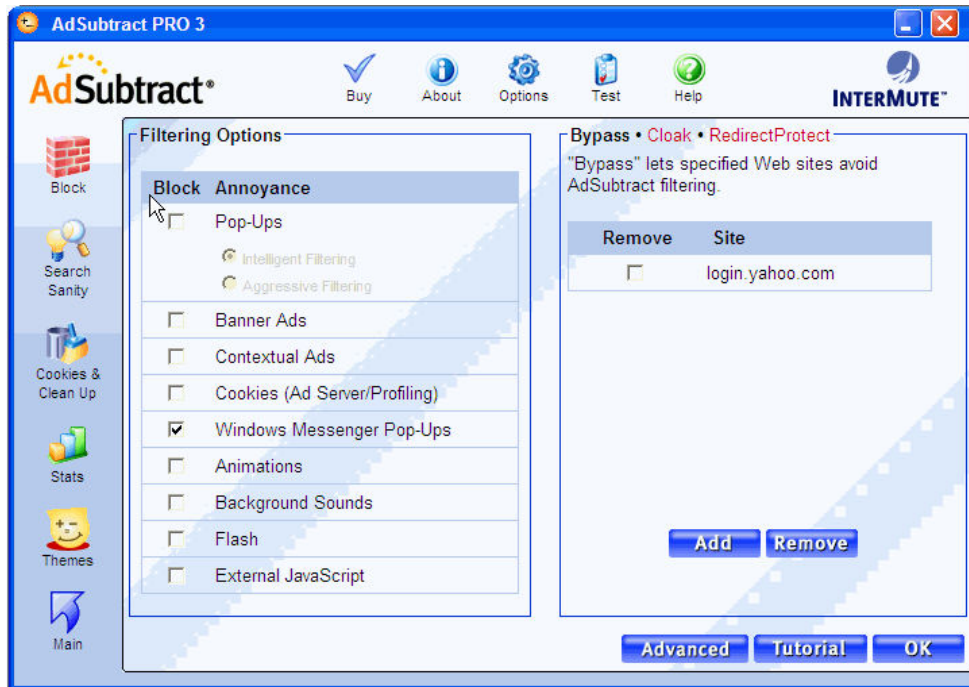
Objective:

Use **AdSubtract** to block banner ads, contextual ads, Pop-ups, animations on web pages, background sounds and ad server cookies.

- In the **CEHv6 Labs CD-ROM** navigate to **Module 44**
- Install and launch **AdSubtract** program



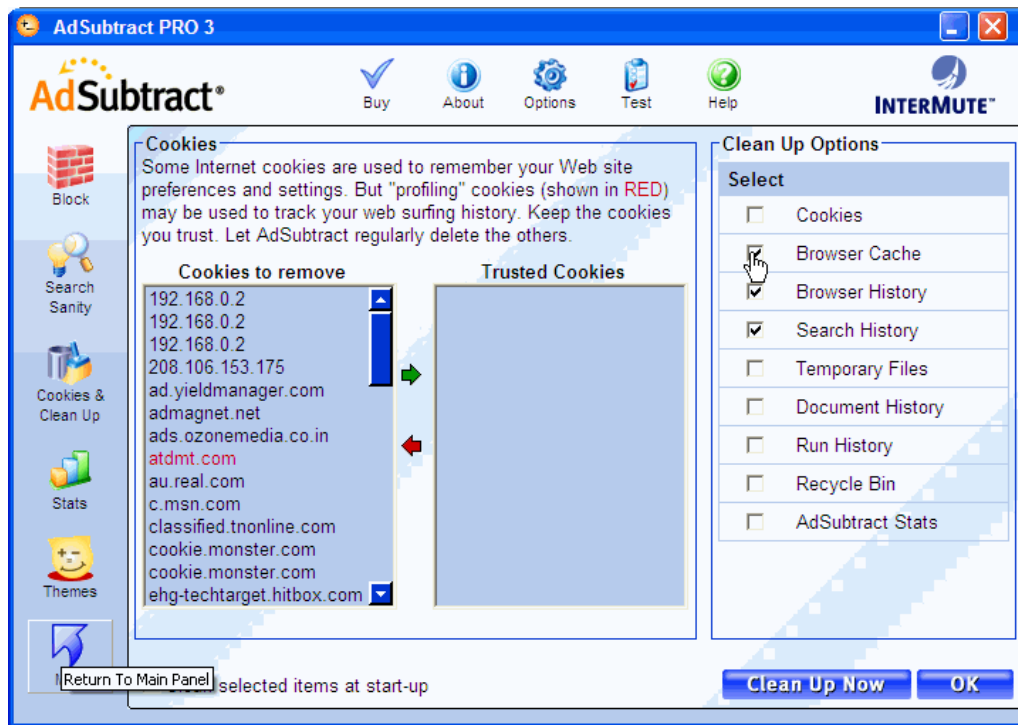
- Click **Block**  icon to set the filtering options. Check the desired options.



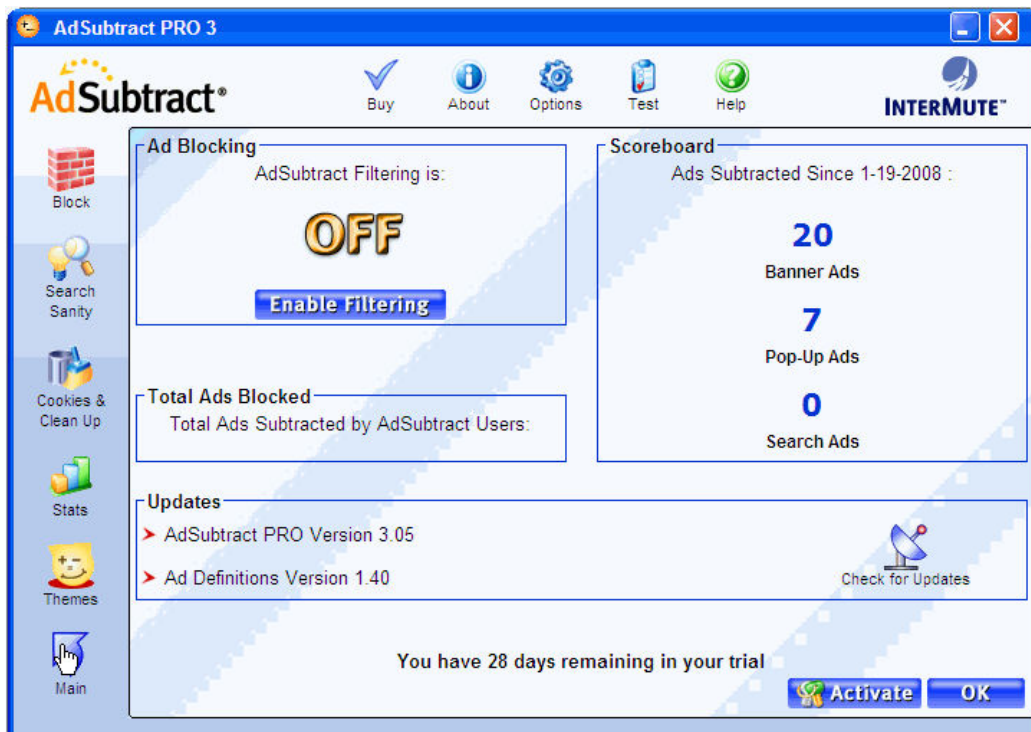
- Click **Search Sanity**  icon to block sponsored and paid ads in popular search engines.



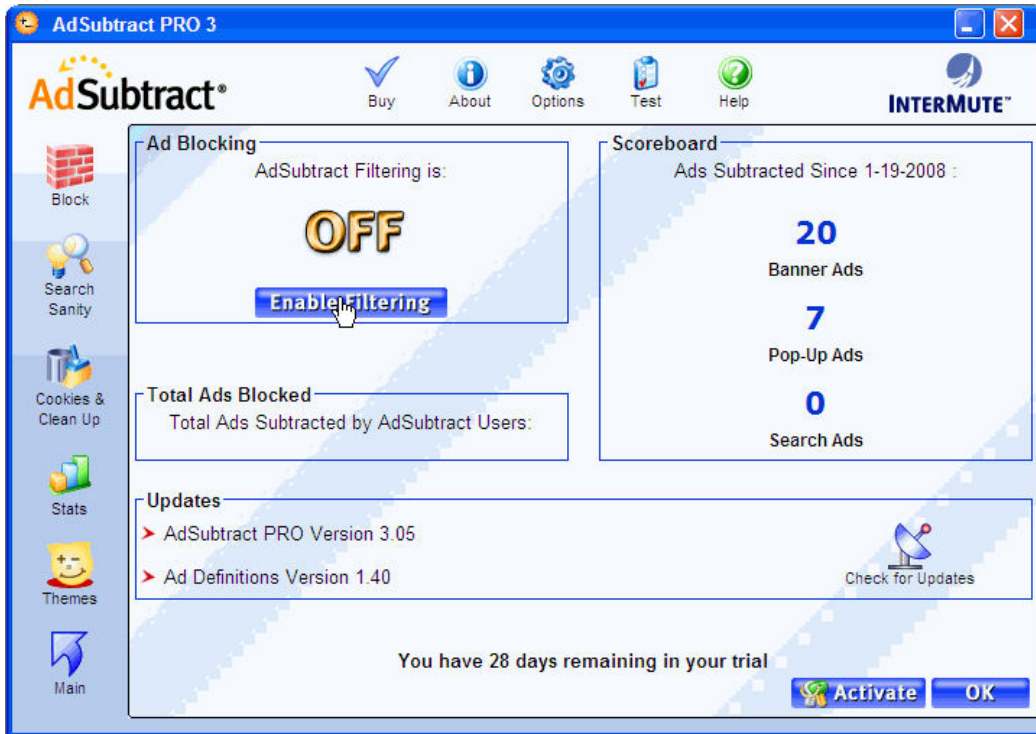
- Click **Cookies & Clean Up**  to cleanup cookies and check the required **Clean up options**.



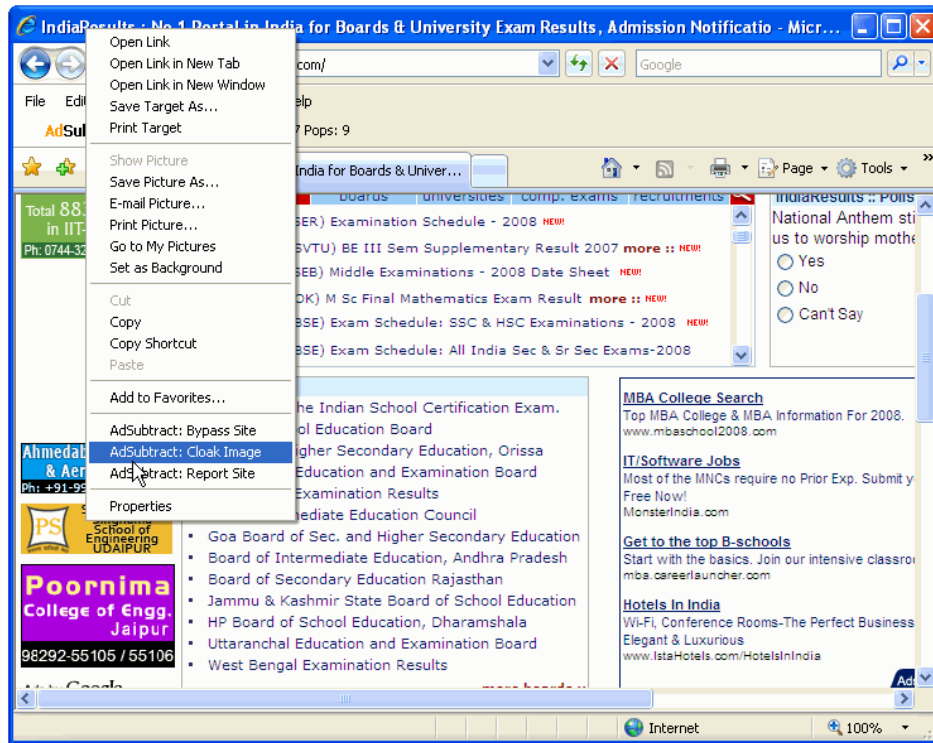
- Click **Main**  icon to return to the main screen.



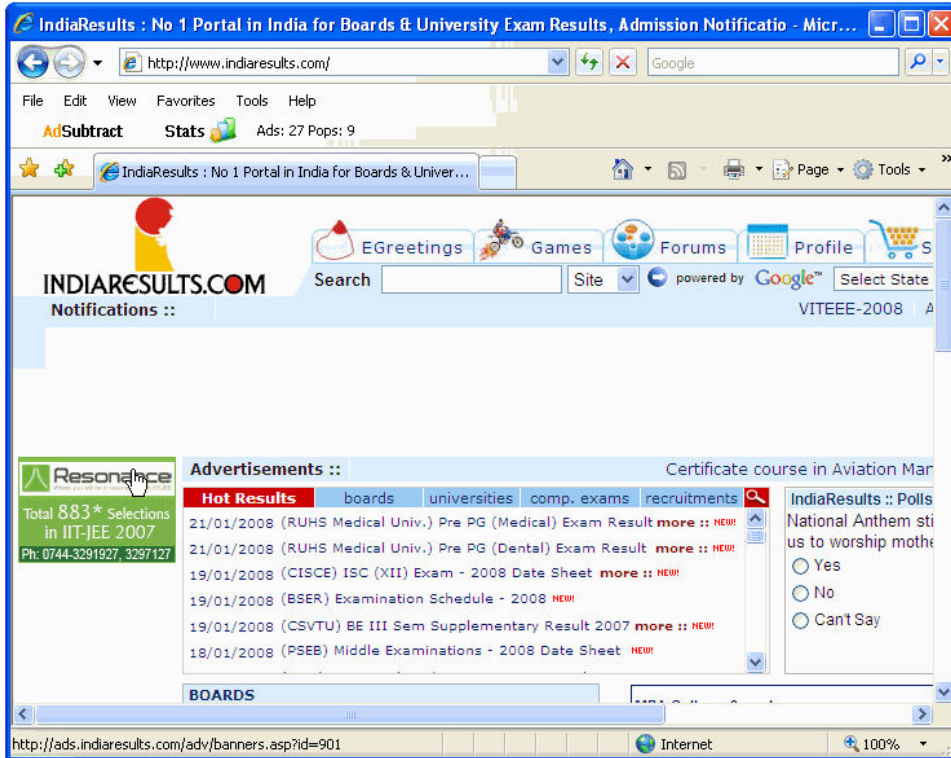
Click **Enable Filtering** to start filtering.




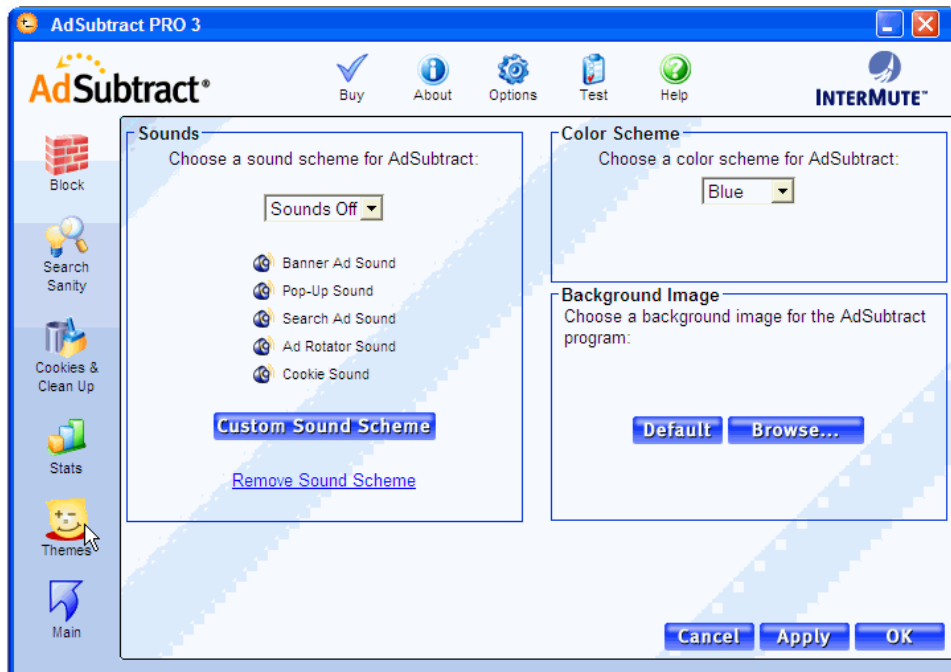
- To cloak an image in the browser select the image, right click and select **AdSubtract: Cloak image**




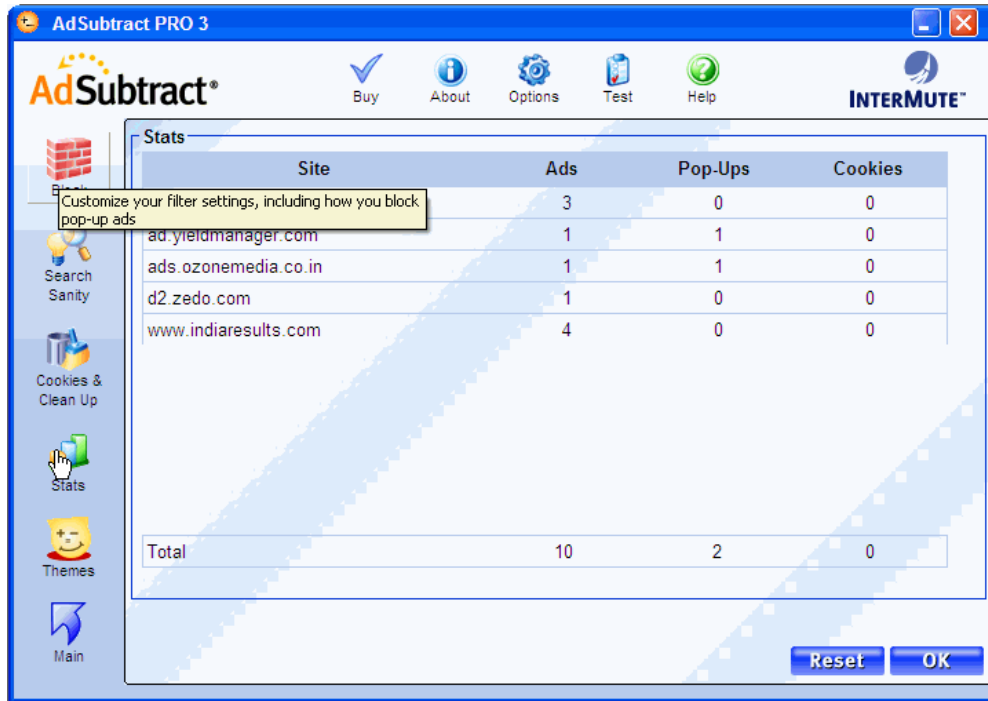
- The site after blocking the images



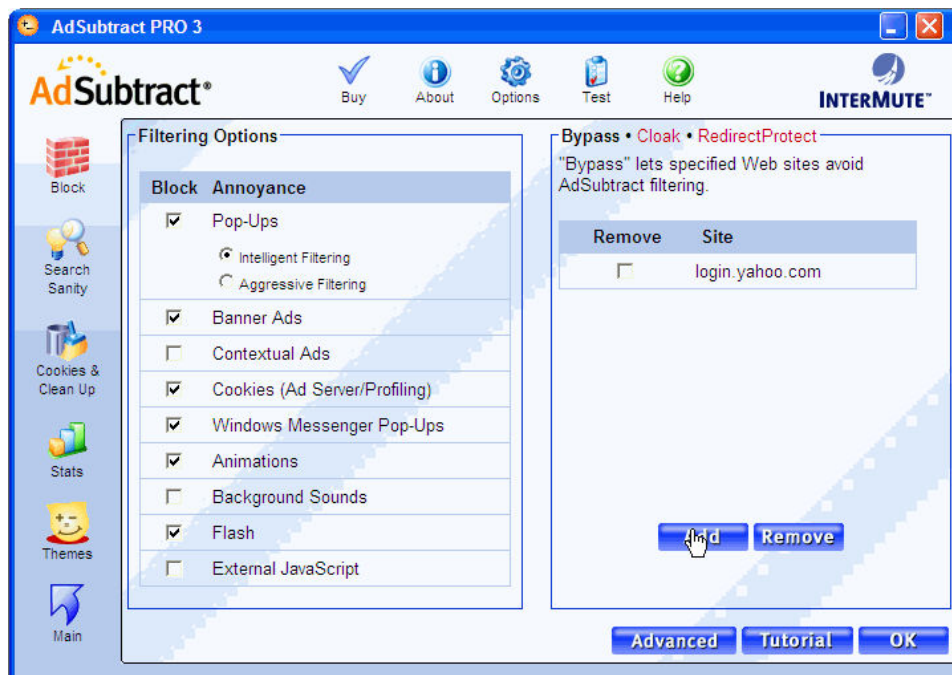
- To set themes, Click **Themes** 



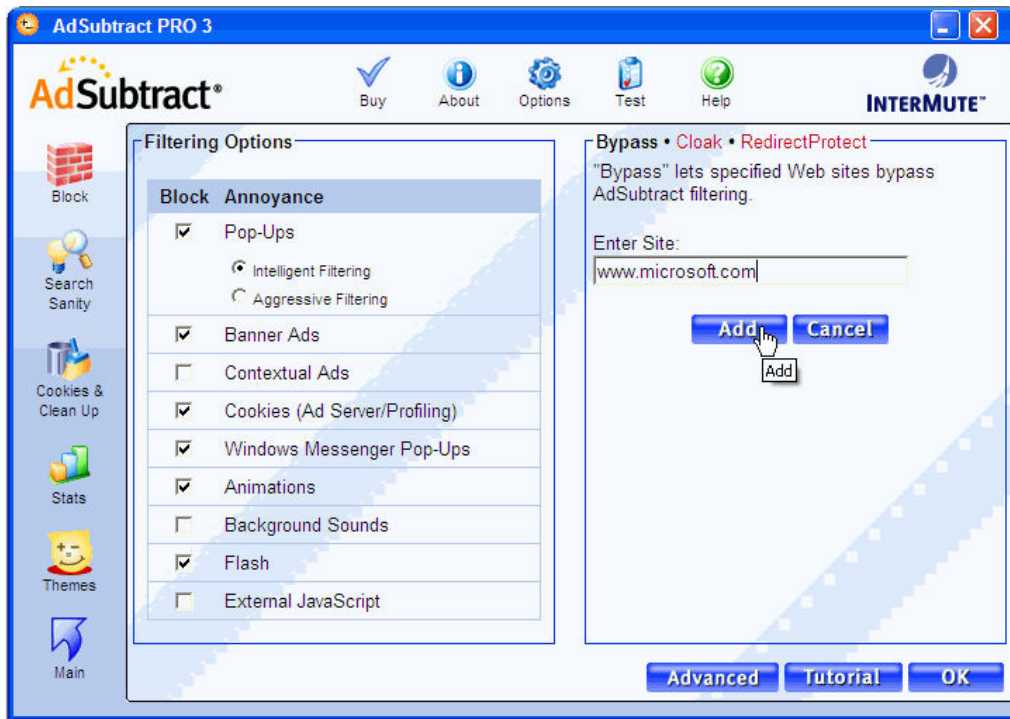
- To view statistics, Click **Stats** 



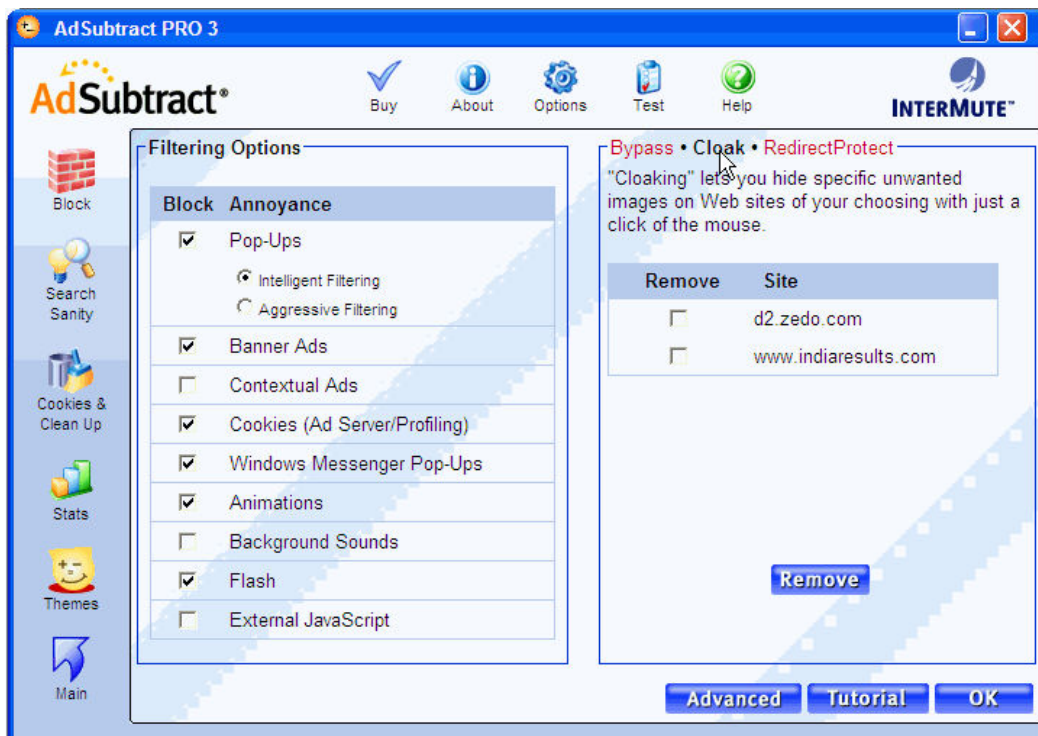
▪ To bypass a website, Click **Block**→ **Bypass**→ **Add**



▪ Enter the site address, Click **Add**



To hide specific unwanted images, Click **Cloak**

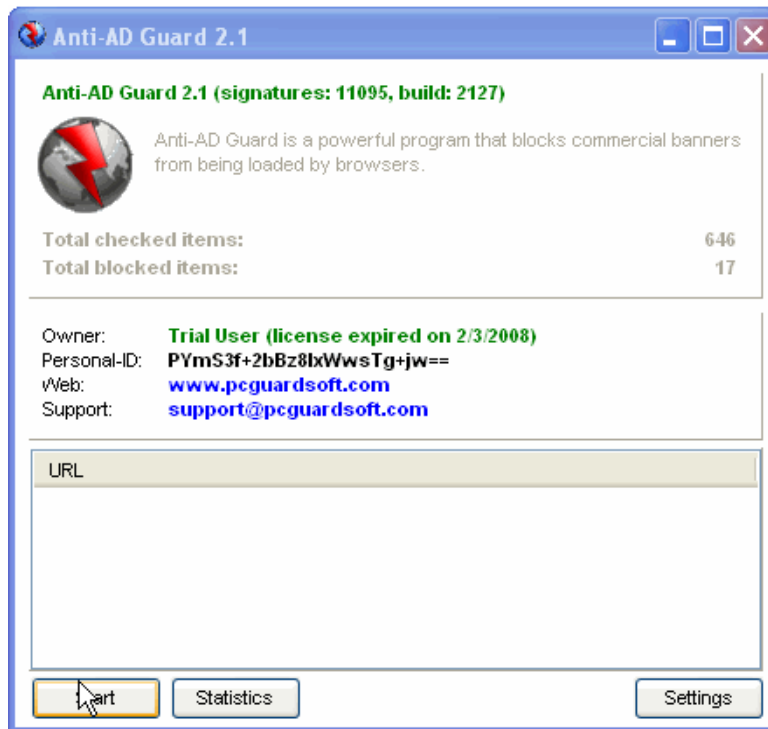


Lab 44-04

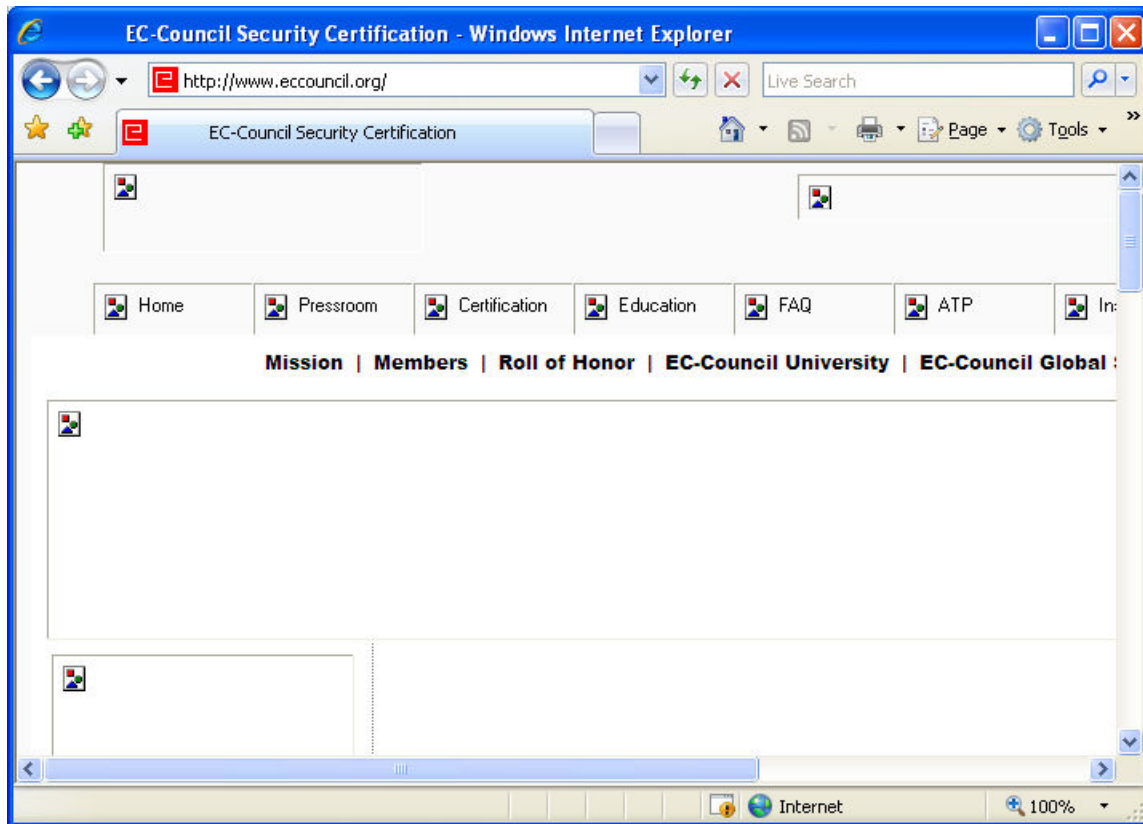
Objective:

Use **Anti AD Guard** program to block commercial banners loaded by the browsers.

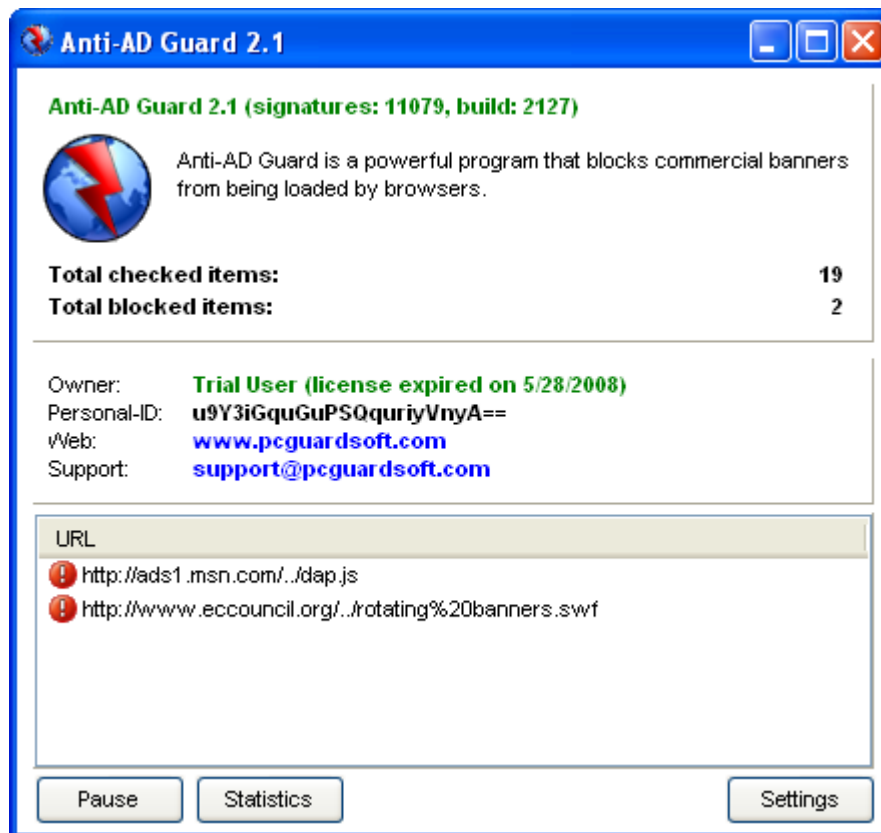
- In the **CEHv6 Labs CD-ROM** navigate to **Module 44**
- Install and launch **Anti-AD Guard** program
- Click **Start** to Start Anti Ad Guard



- Browse any site



- Check the blocked pop-ups



Lab 44-05

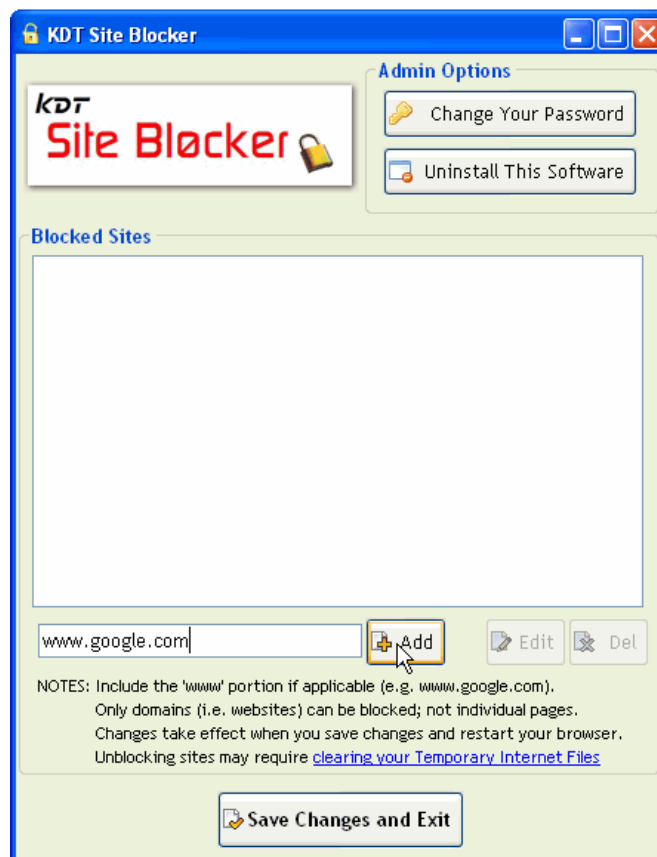
Objective:

Use **KDT site blocker** to block the desired web pages by adding the link.

- In the **CEHv6 Labs CD-ROM** navigate to **Module 44**
- Install and launch **KDT site blocker** program

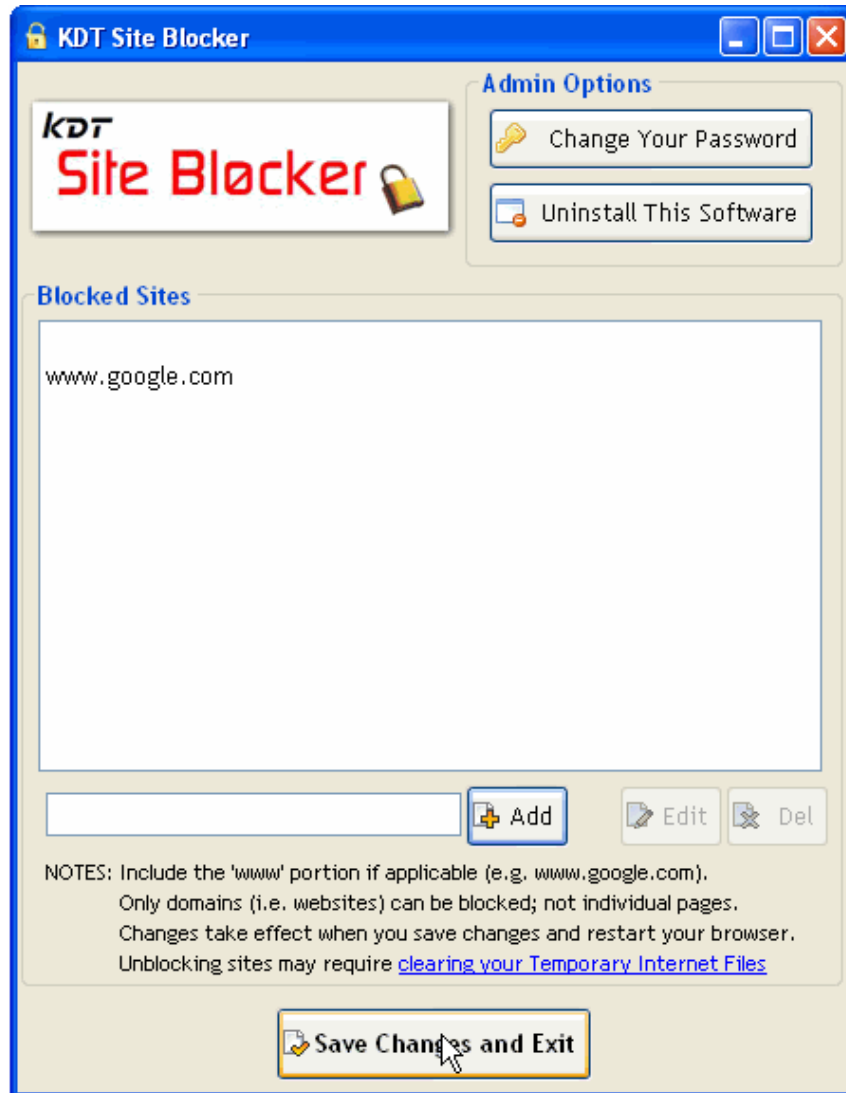


- Enter the site address to be blocked and click on **Add** button.



Click **Save**

- **Changes and Exit** button



- Open the site, 'This website has been **BLOCKED** from viewing' message appears



Lab 44-06

Objective:

Use **Stop-the-Pop-Up Lite** to block pop-up windows from appearing as you surf the web.

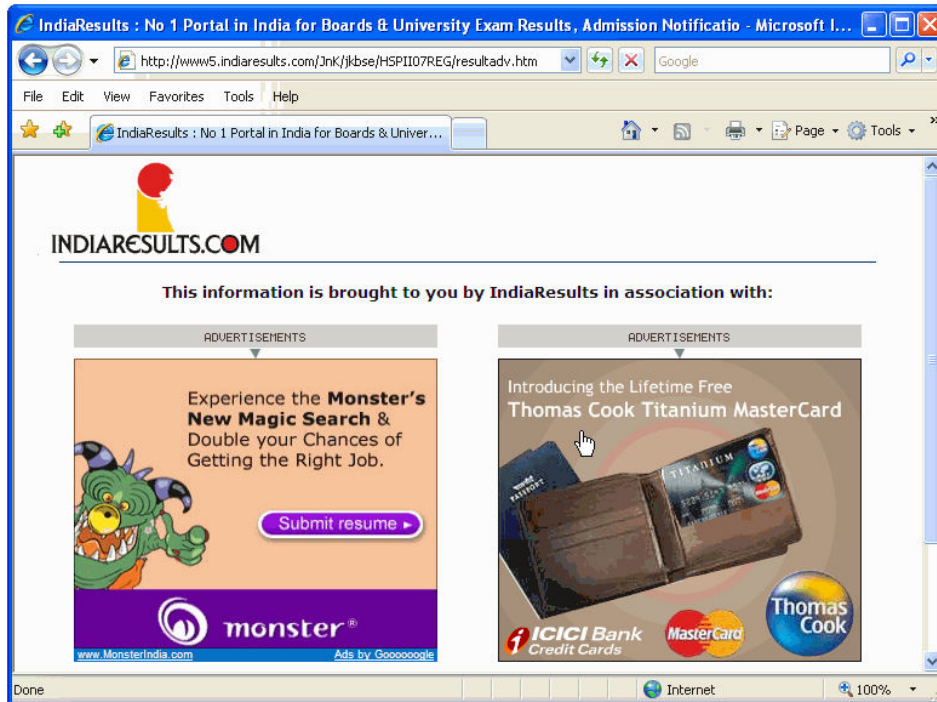
- In the **CEHv6 Labs CD-ROM** navigate to **Module 44**
- Install and launch **Stop-the-Pop-Up Lite** program



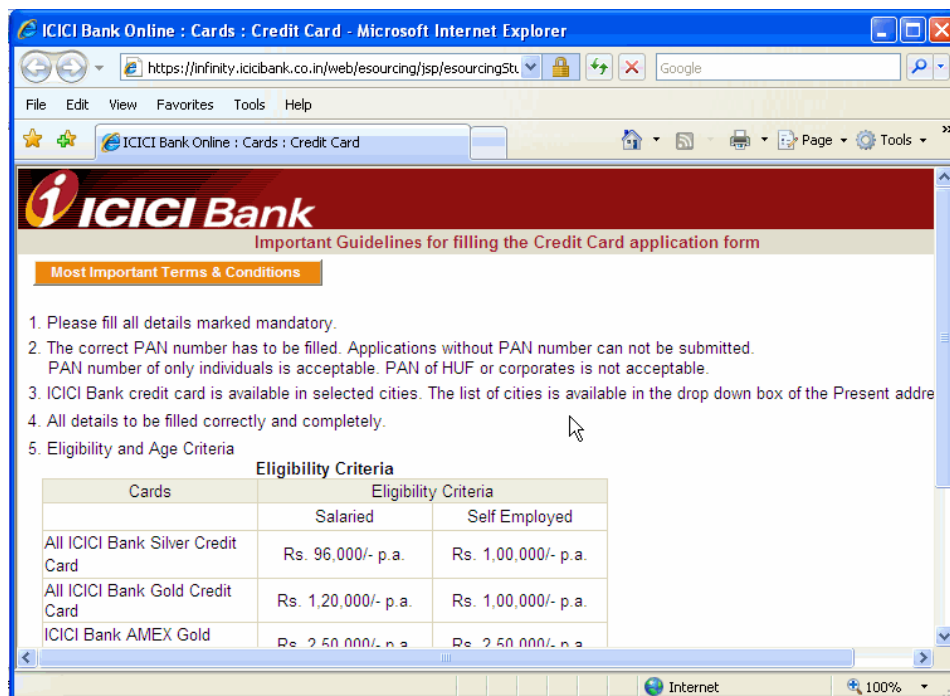
- To disable blocking popups, check the option **Disable pop-up killer** in the control panel



- Open a site in the IE browser



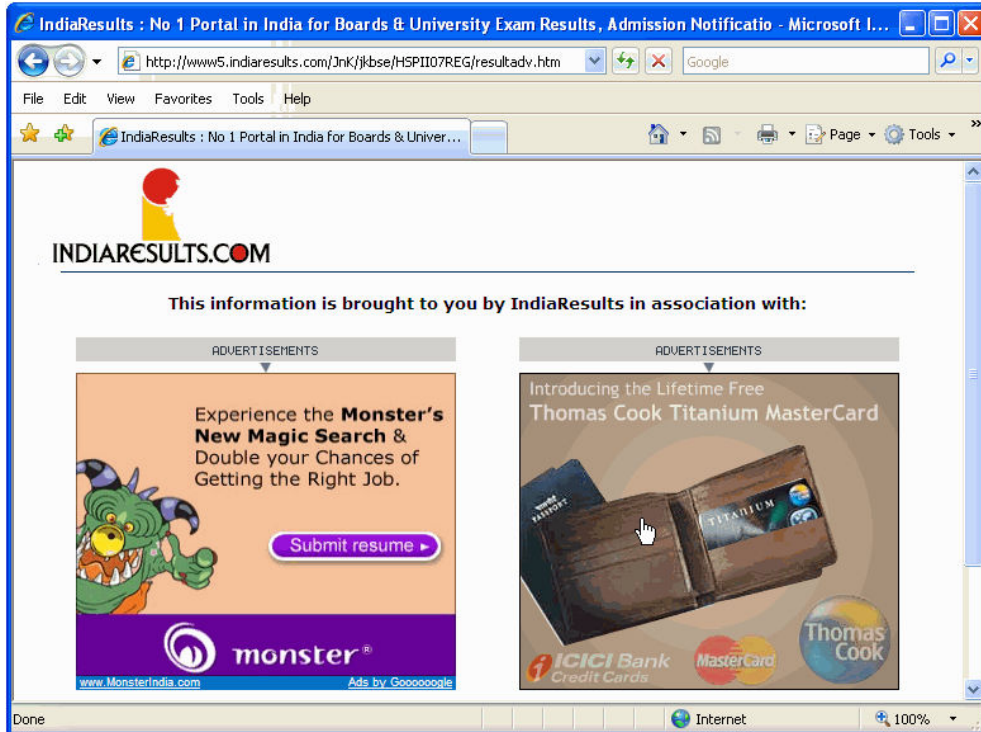
- As the popups are disabled the popup window opens



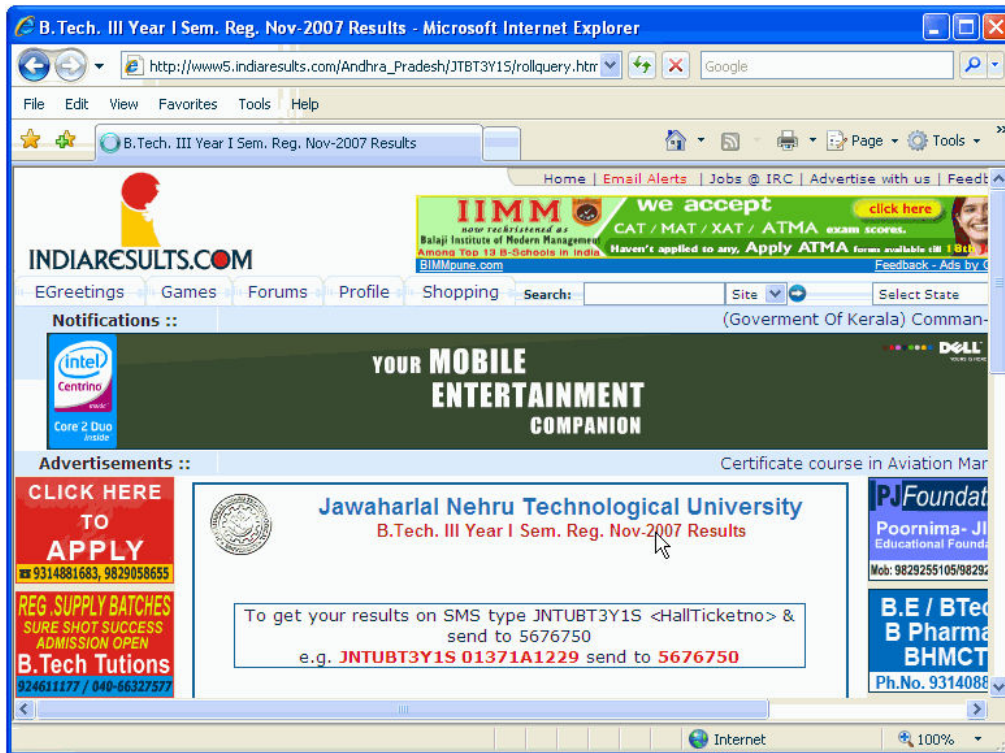
- To enable the blocking popup uncheck the option **Disable pop-up Killer** in the control panel



- Now, Browse the site in the IE browser



- skipped resulting the next window



- The number of popups blocked is shown on the control panel

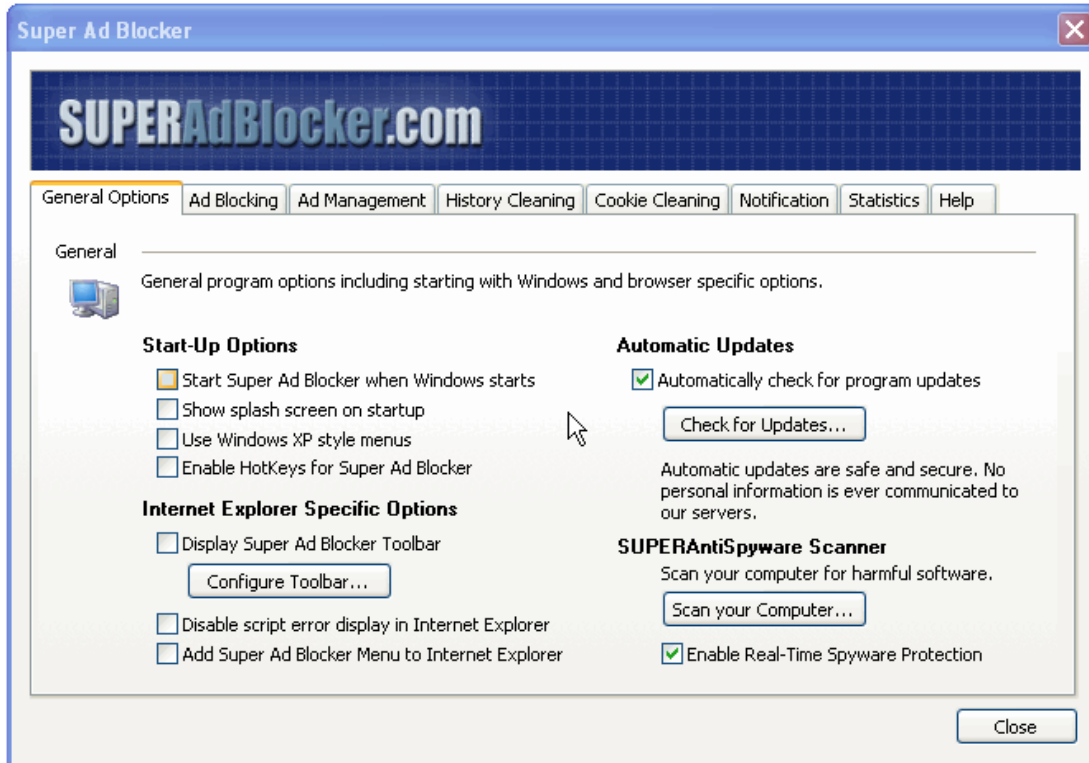


Lab 44-09

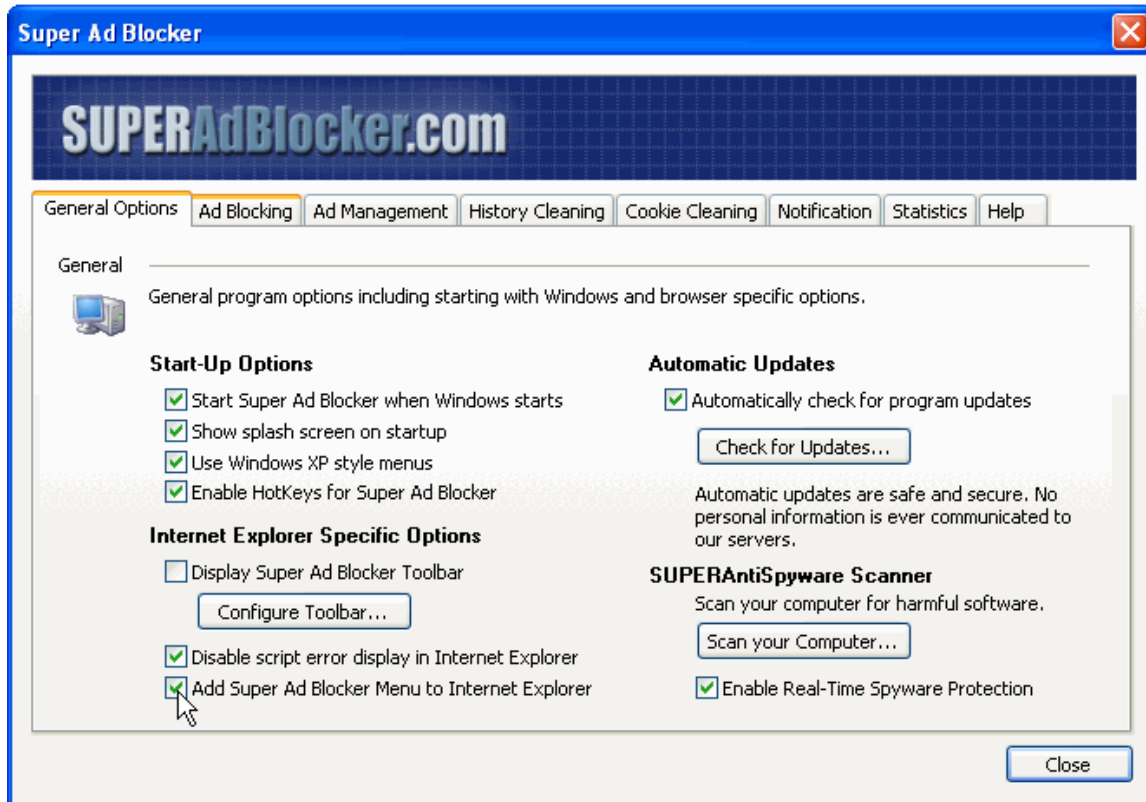
Objective:

Use **Super Ad Blocker** to prevent the ads such as Pop-Up and Pop-Under, Flash and Rich Media Ads, Fly-in and Slide-in Ads, Common Ad Banners, Web Page Dialog Ads, Desktop Messenger Ads, Spyware/Adware Ads, etc.

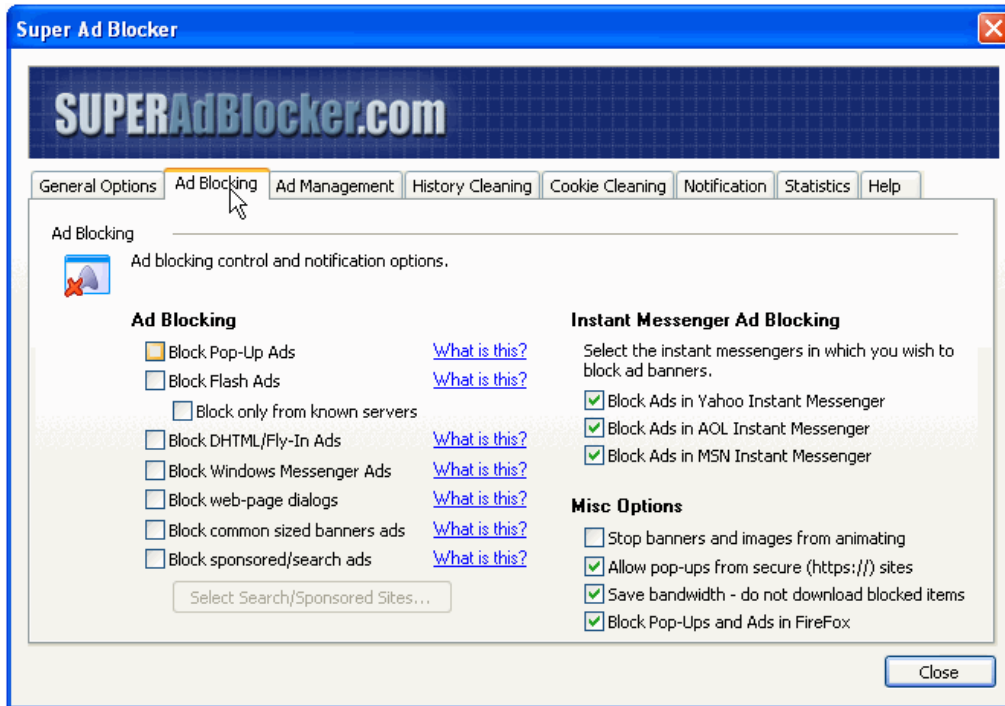
- In the **CEHv6 Labs CD-ROM** navigate to **Module 44**
- Install and launch **Super Ad Blocker** program



- Go **General Options** tab and check the desired options



- Go to **Ad Blocking** tab and explore various options



- the IE browser Open a site in

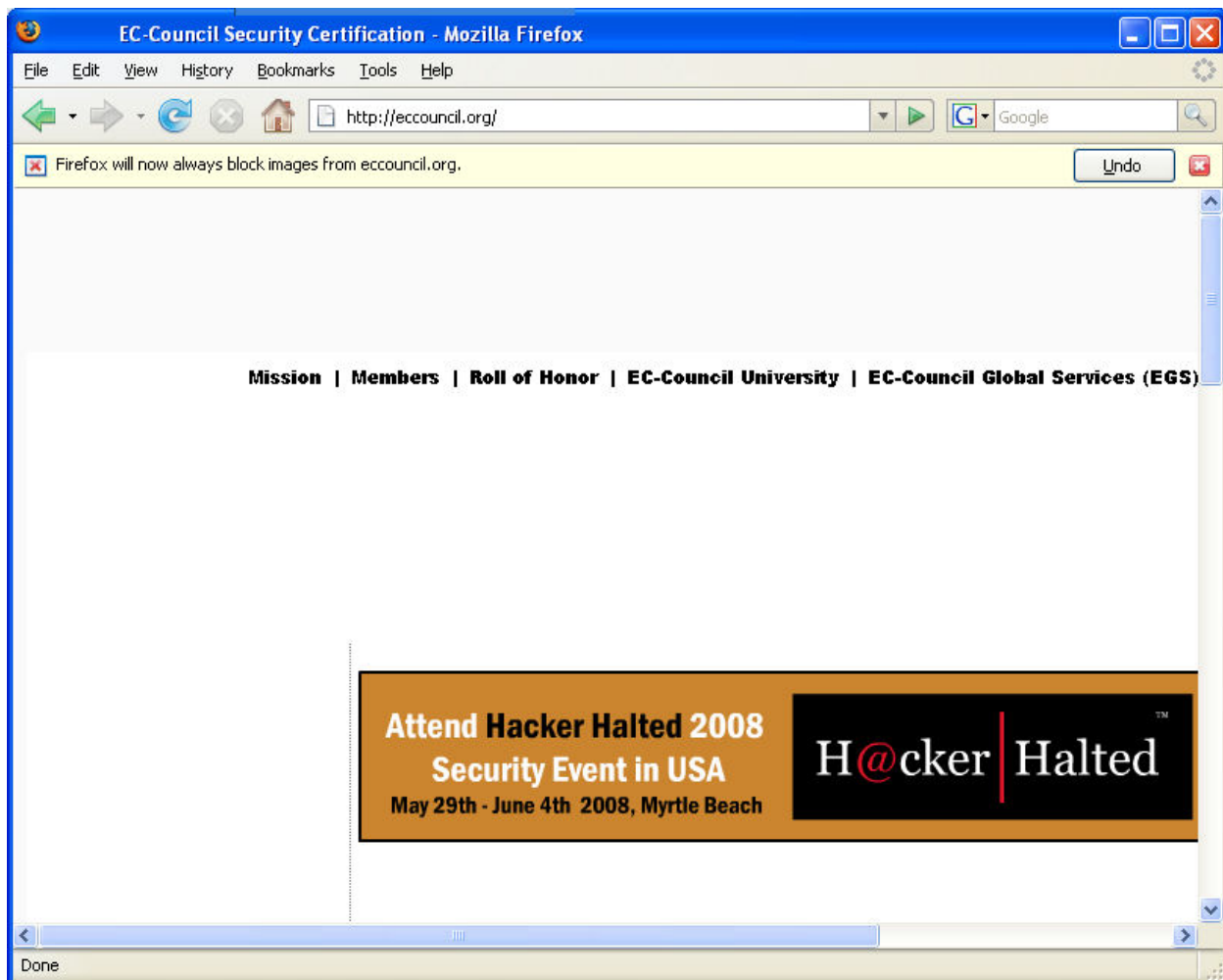


- an image and click on Block Image from eccouncil.org

Write click on



- Again open the same site and check blocked image



Lab 44-10

Objective:

Use **iProtectYou** software for internet content filtering to protect children from accessing harmful information on the Internet.

- In the **CEHv6 Labs CD-ROM** navigate to **Module 44**
- Install and launch **i Protect You** program

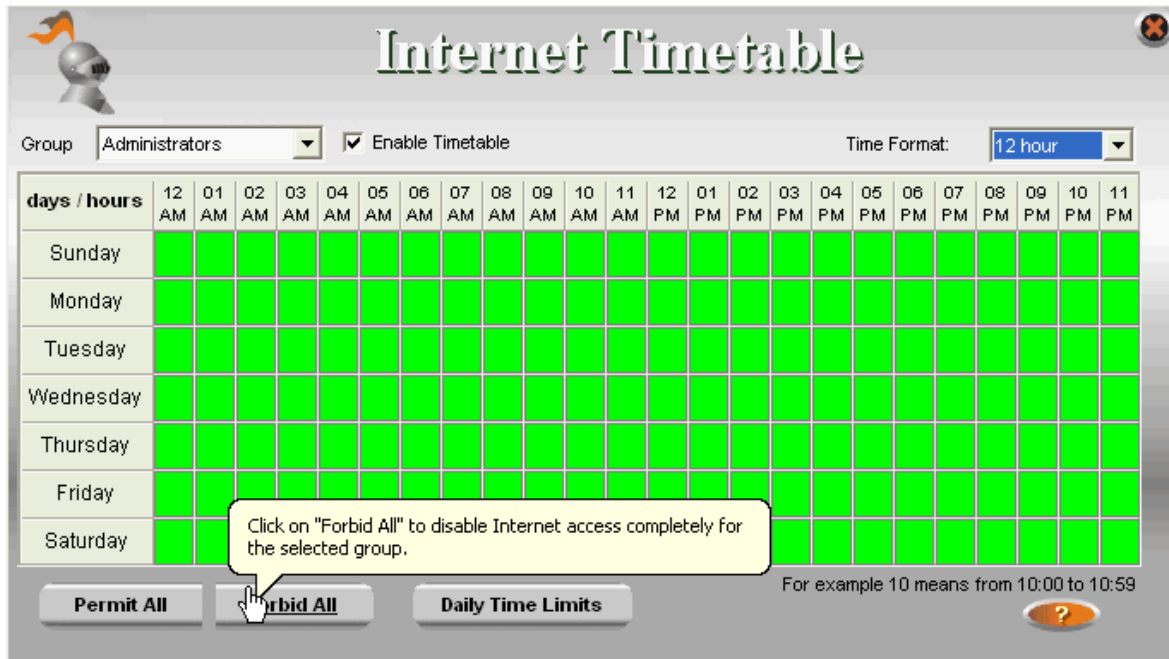


- **Timetable** to set time table

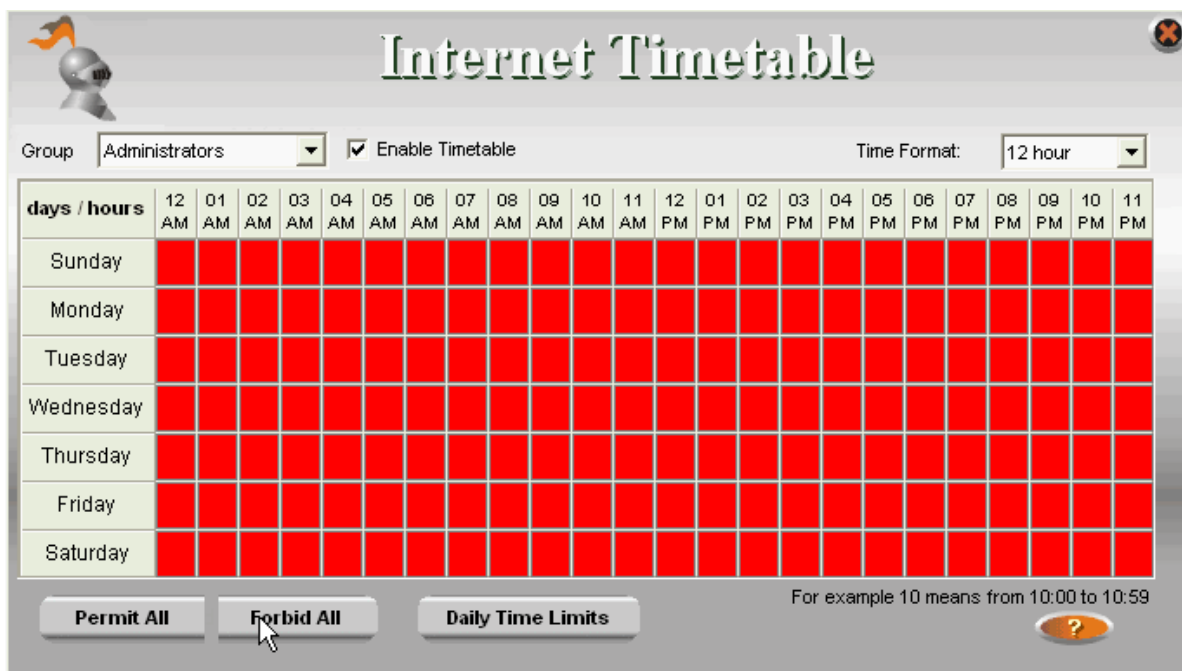
Click **Internet**



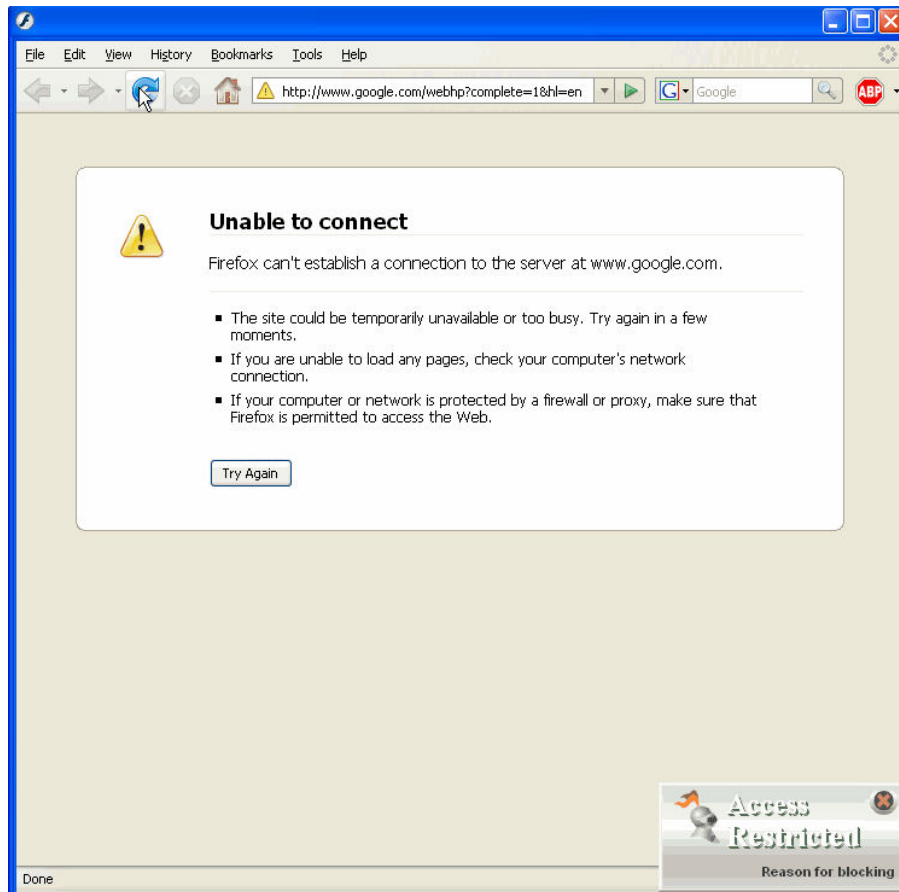
- To disable internet access continuously for a group, Click **Forbid All**



- The color changes after disabling the internet access



- Access restriction message will appear while browsing a site

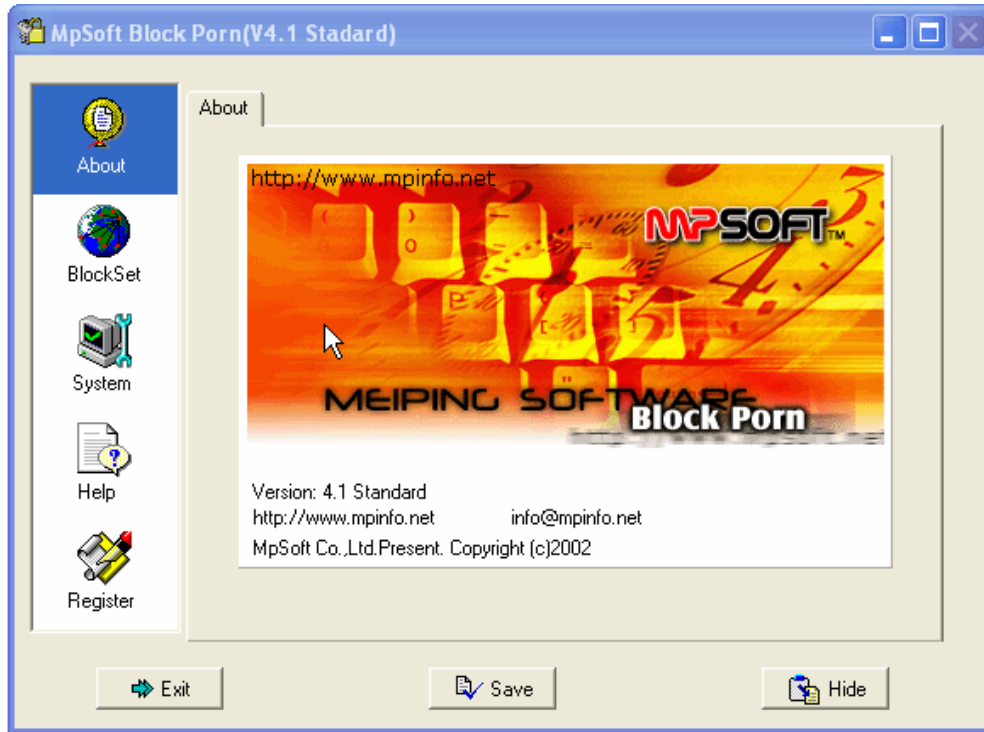


Lab 44-11

Objective:

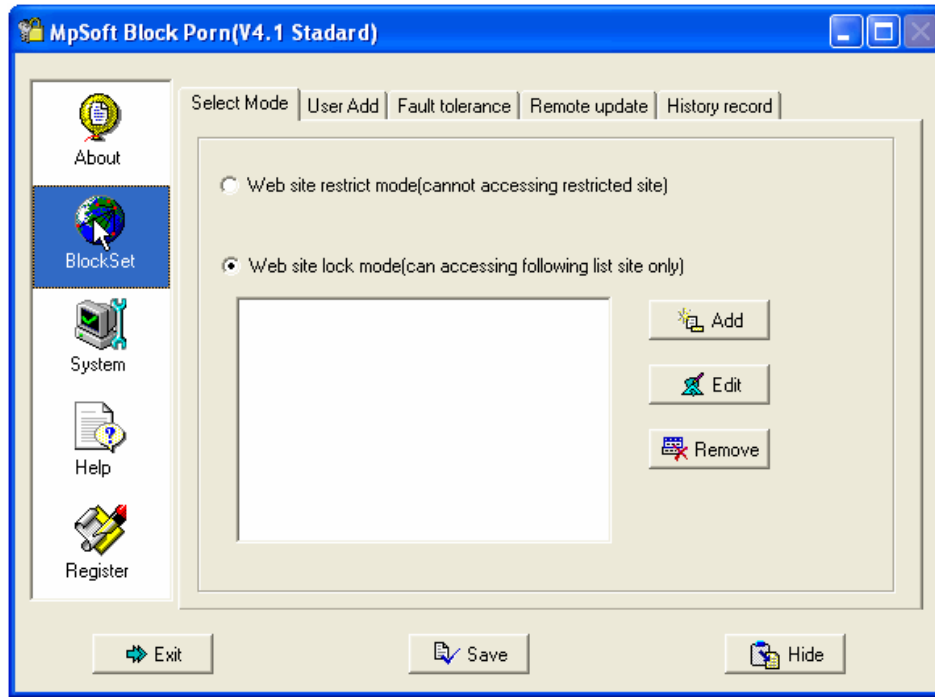
Use **Block Porn** to block anti pornography material or adult material on the Internet by adopting advanced interception technology.

- In the **CEHv6 Labs CD-ROM** navigate to **Module 44**
- Install and launch **Block Porn** program

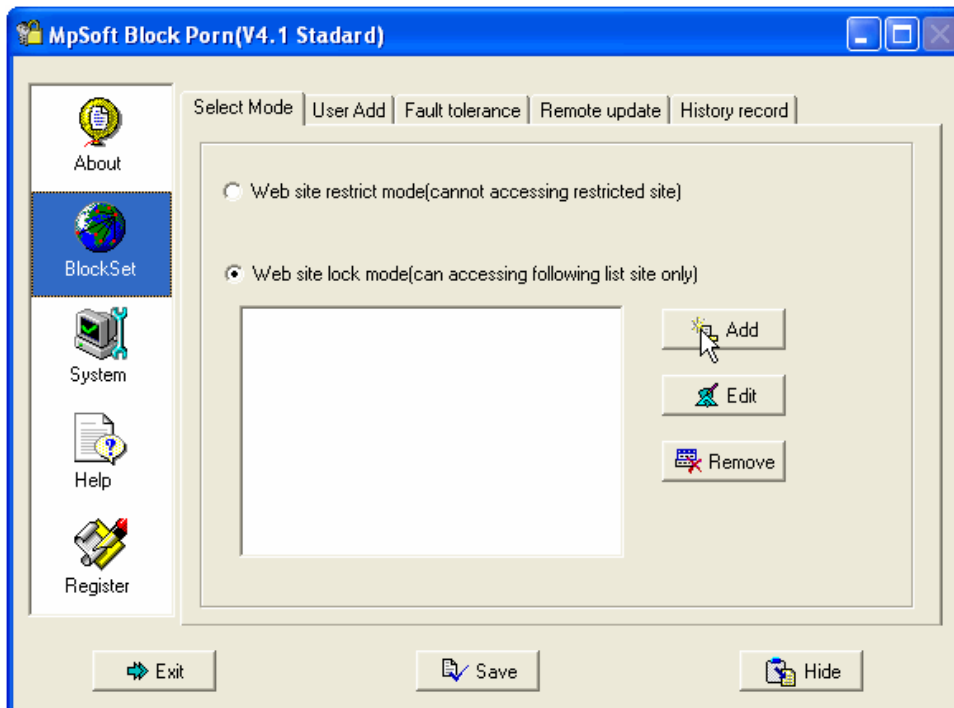




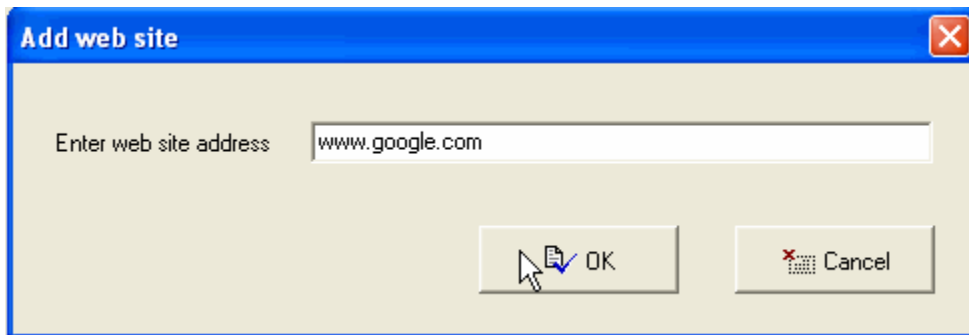
- To set the website restrictions, Click **Block Set**



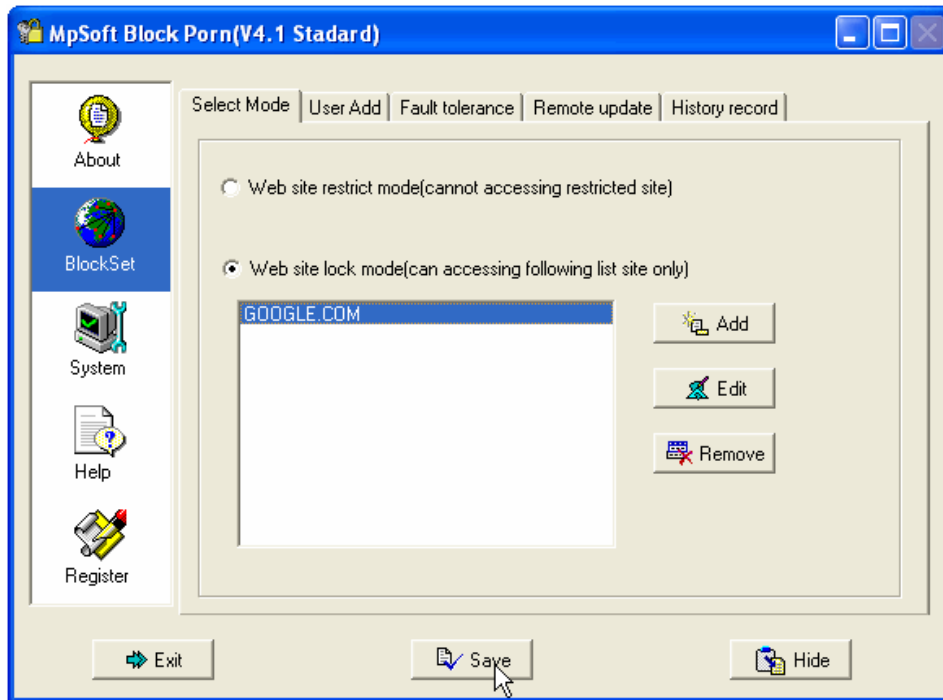
- To add website, Click **Add**



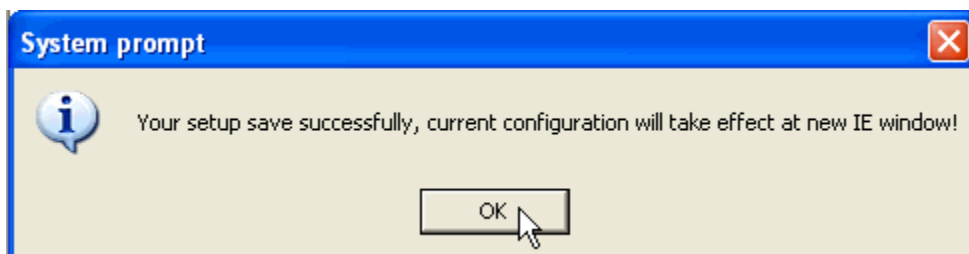
- Enter the website address and click **OK**



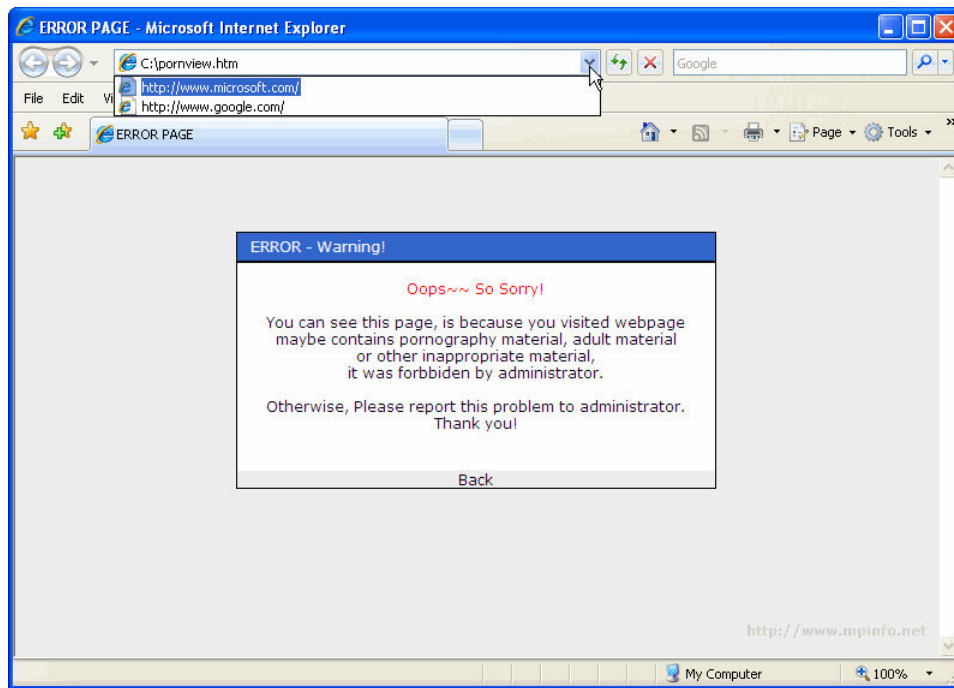
- To apply changes, Click **Save**



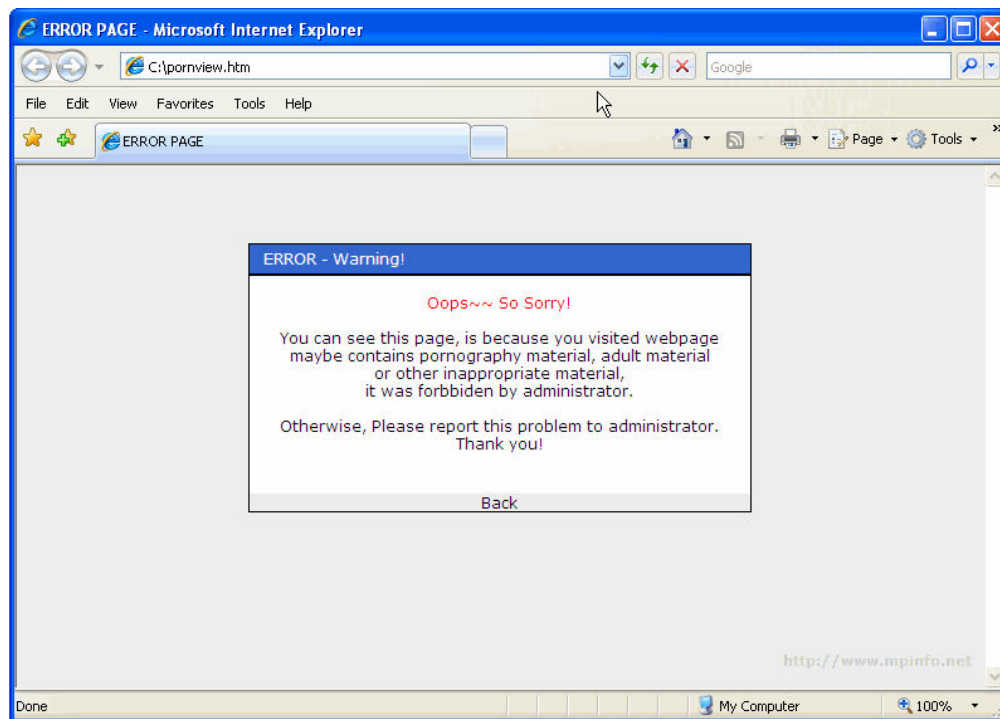
- When the prompting message appears, Click **OK**



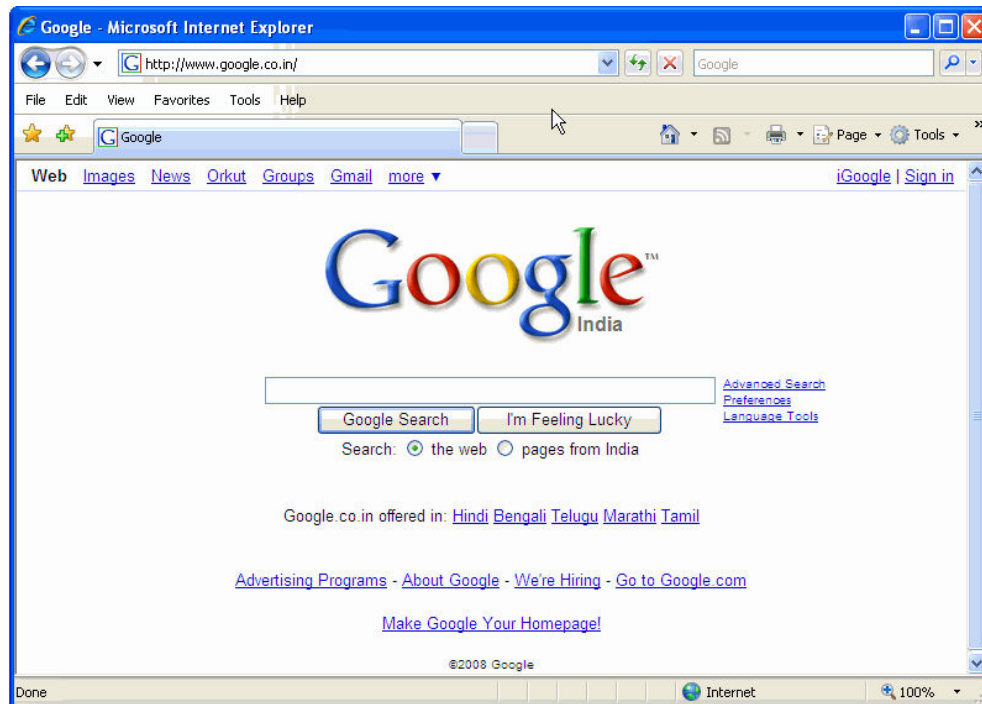
- Select the site other than one added to the list in the browser



- It displays an error message as shown

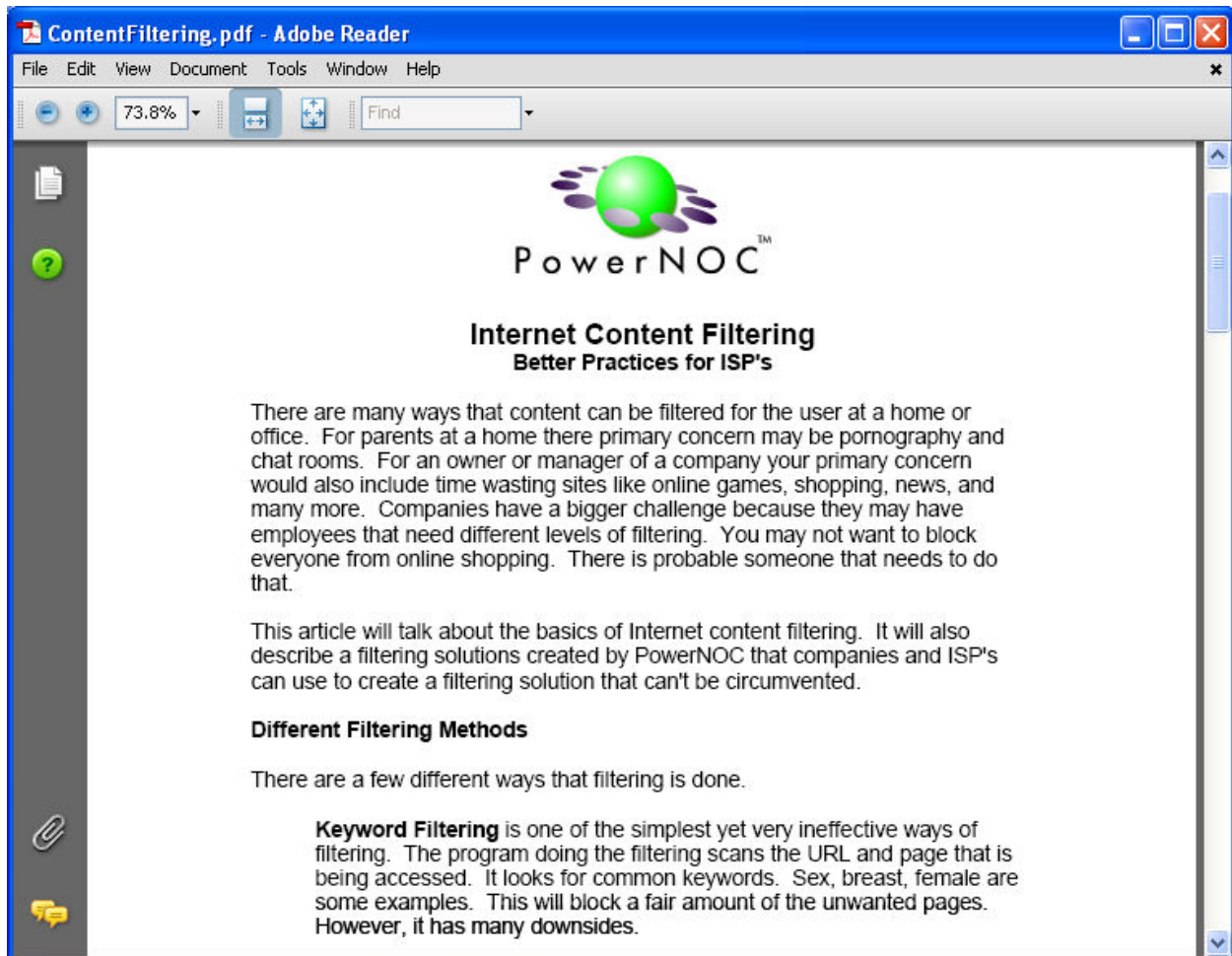


- The site added to list can be accessed without any restrictions



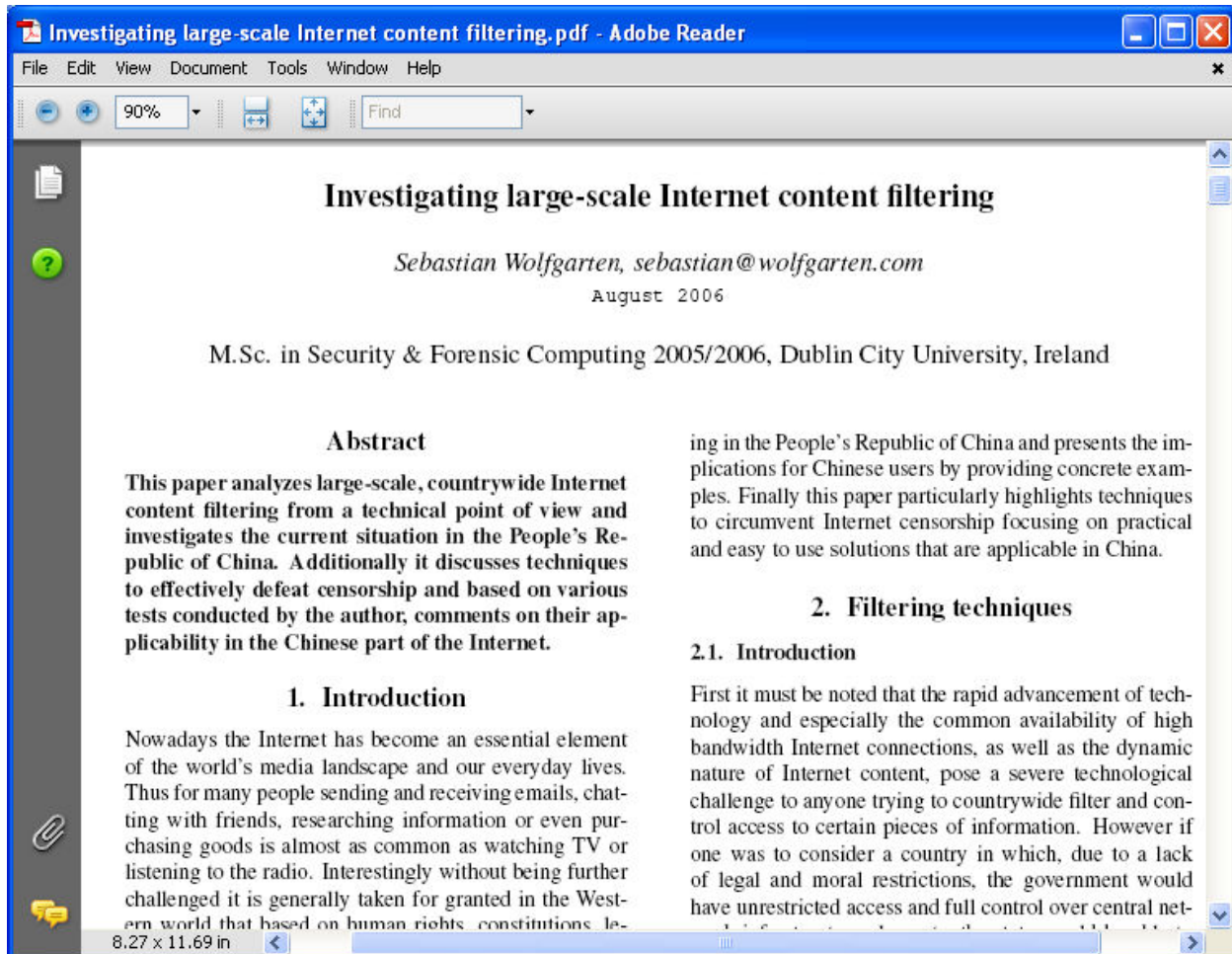
Lab 44-13

- In the **CEHv6 Labs CD-ROM** navigate to **Module 44**
- Open the **ContentFiltering.pdf** and read the content



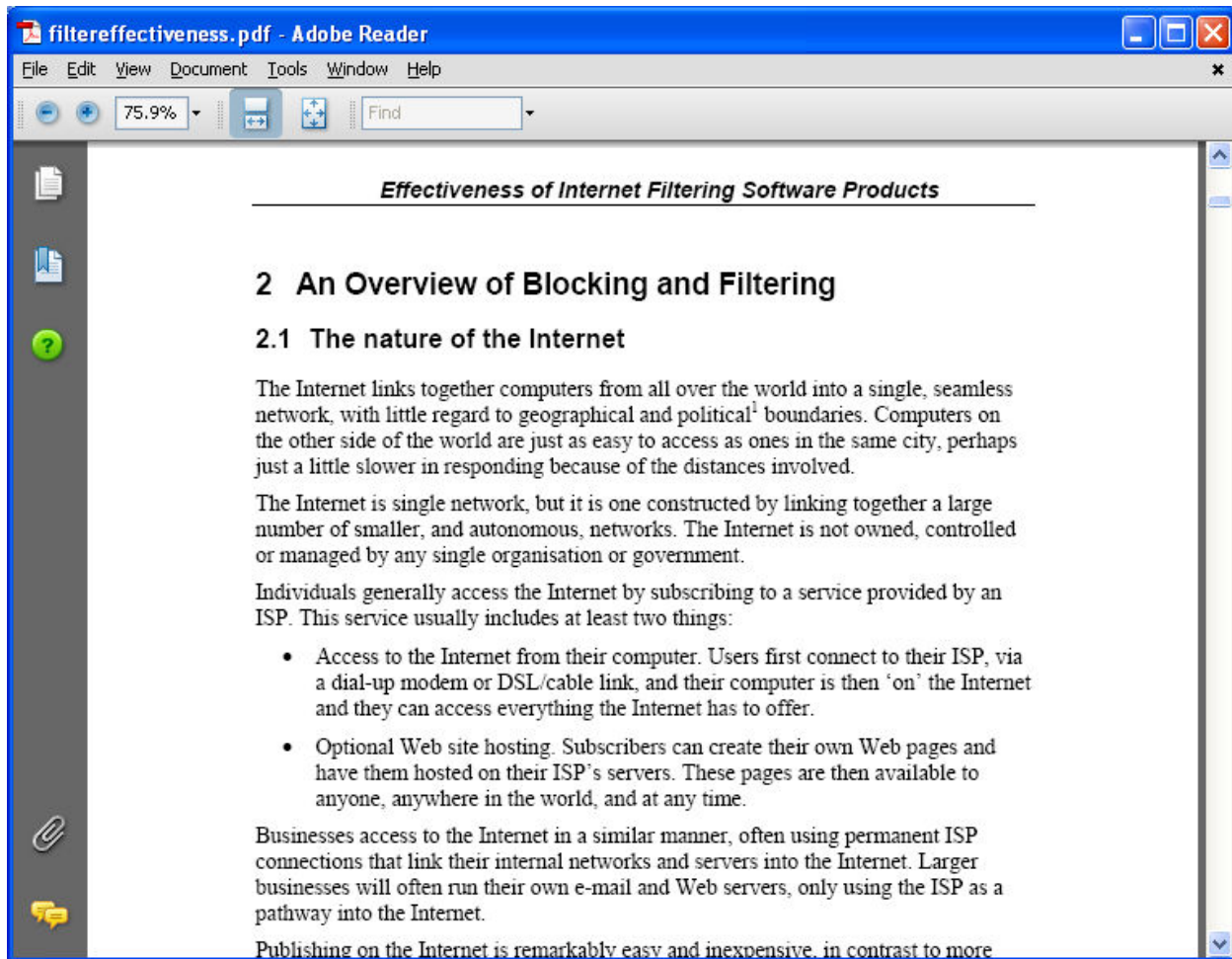
Lab 44 -15

- In the **CEHv6 Labs CD-ROM** navigate to **Module 44**
- Open the **Investigating large-scale Internet content filtering.pdf** and read the content



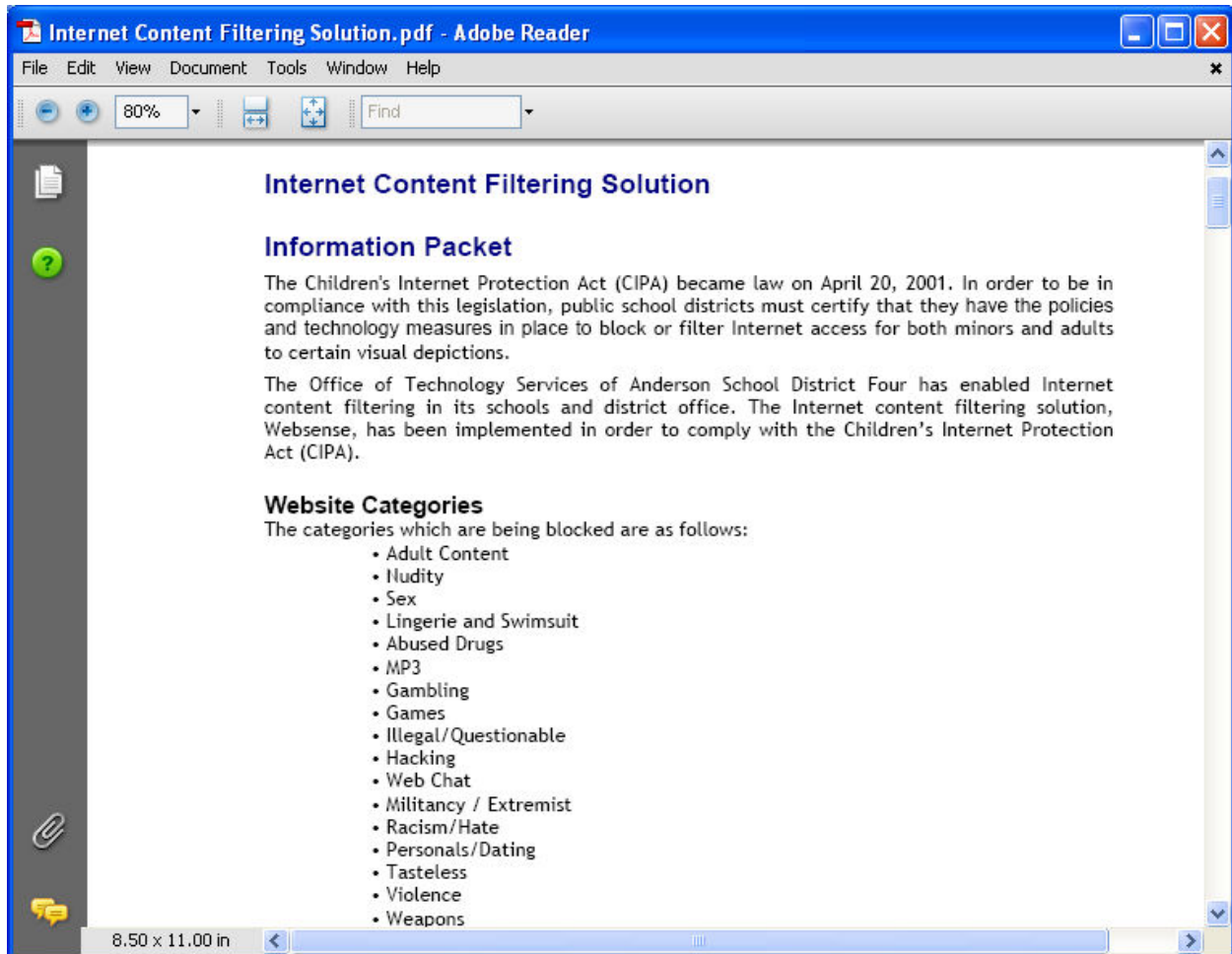
Lab 44-16

- In the CEHv6 Labs CD-ROM navigate to **Module 44**
- Open the **filtereffectiveness.pdf** and read the content



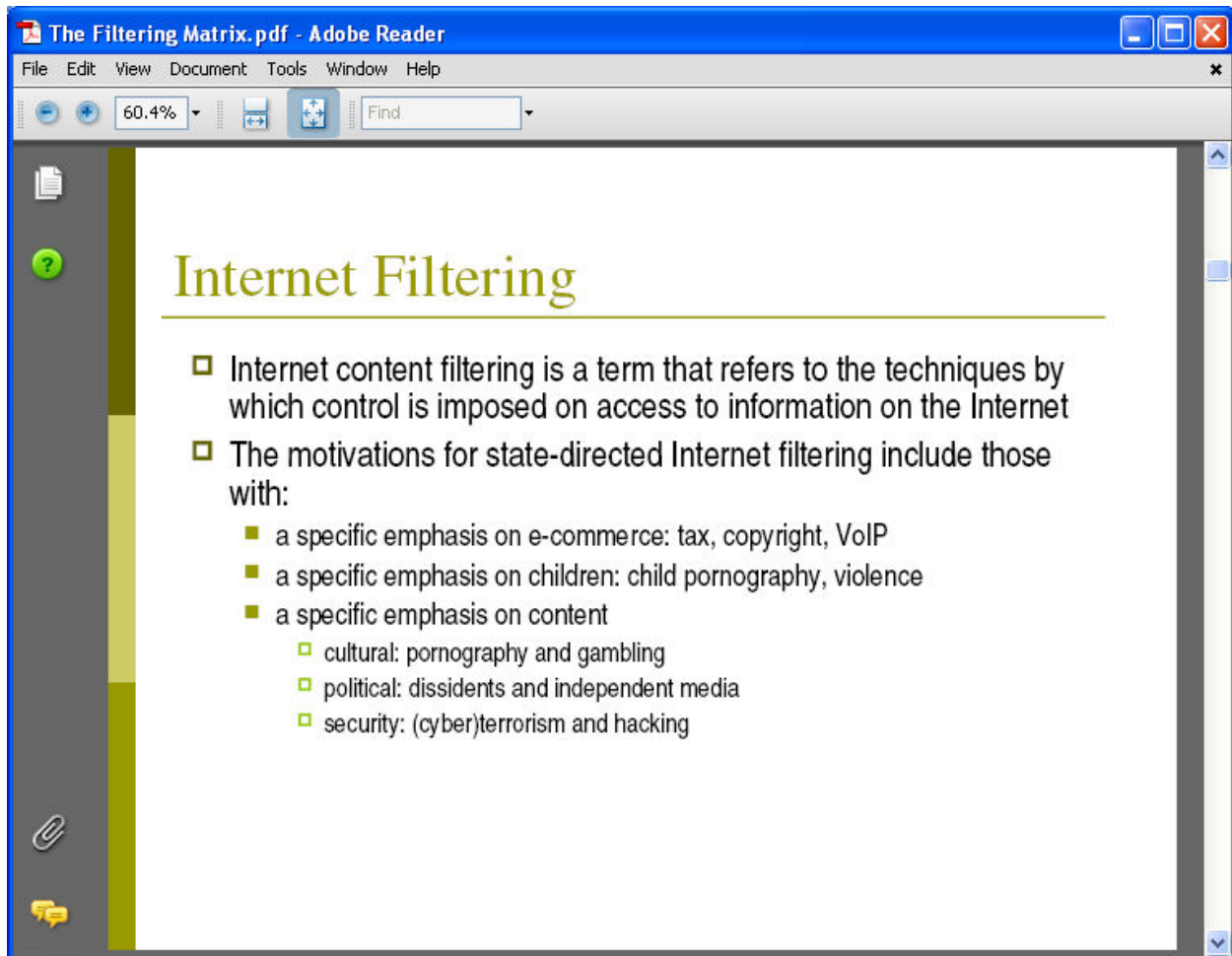
Lab 44-17

- In the **CEHv6 Labs CD-ROM** navigate to **Module 44**
- Open the **Internet Content Filtering Solution.pdf** and read the content



Lab 44-18

- In the **CEHv6 Labs CD-ROM** navigate to **Module 44**
- Open the **The Filtering Matrix.pdf** and read the content





Module 45

Privacy on the Internet

Lab 45-01

Objective:

Use **HistoryKill** to securely delete history traces on computer with the File Shredder.

- In the **CEHv6 Labs CD-ROM** navigate to **Module 45**
- Install and launch “**History Kill**” program



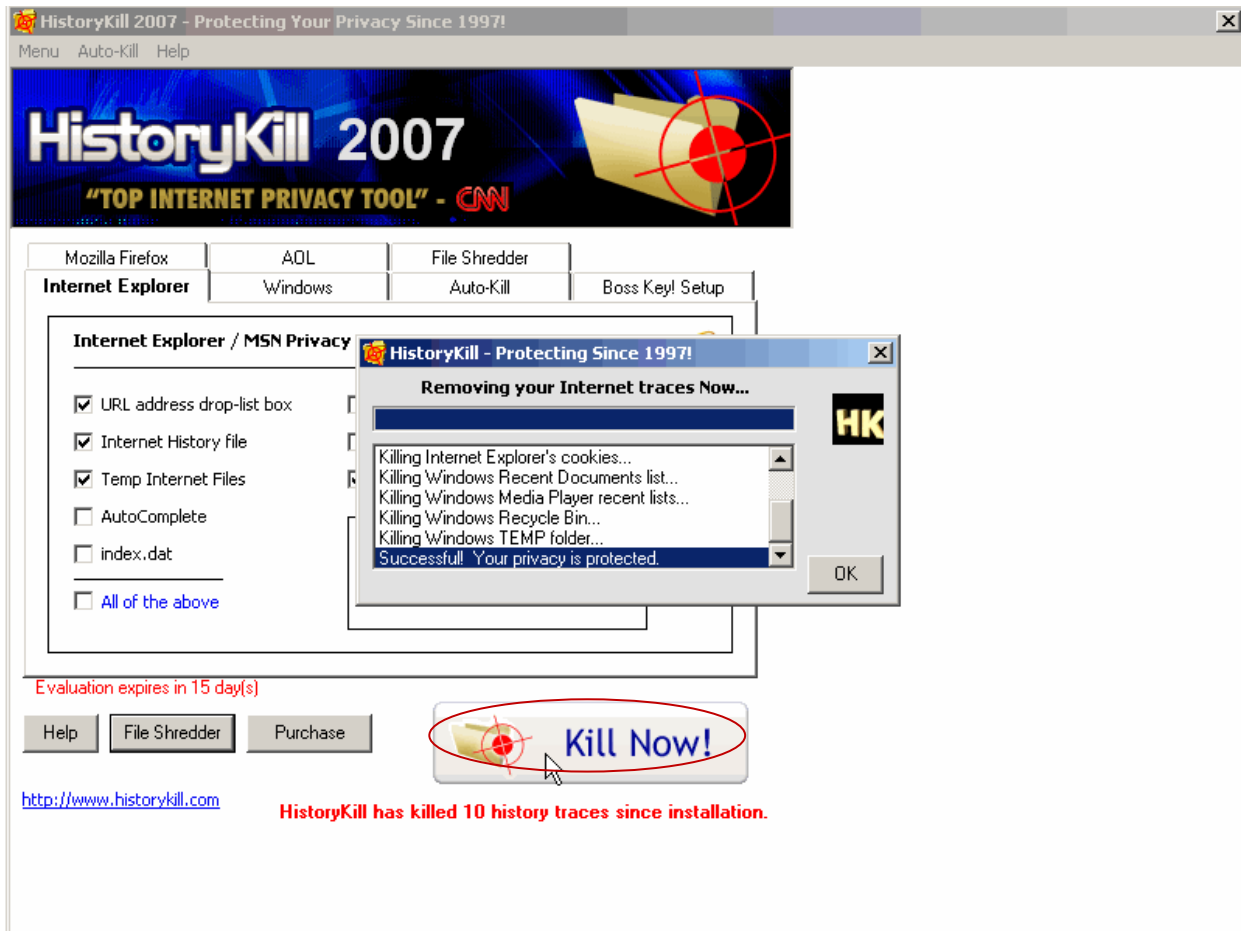
- Click on **Internet Explorer**



- Select the required Options from the list



- Click on **Kill Now** to remove the Internet traces



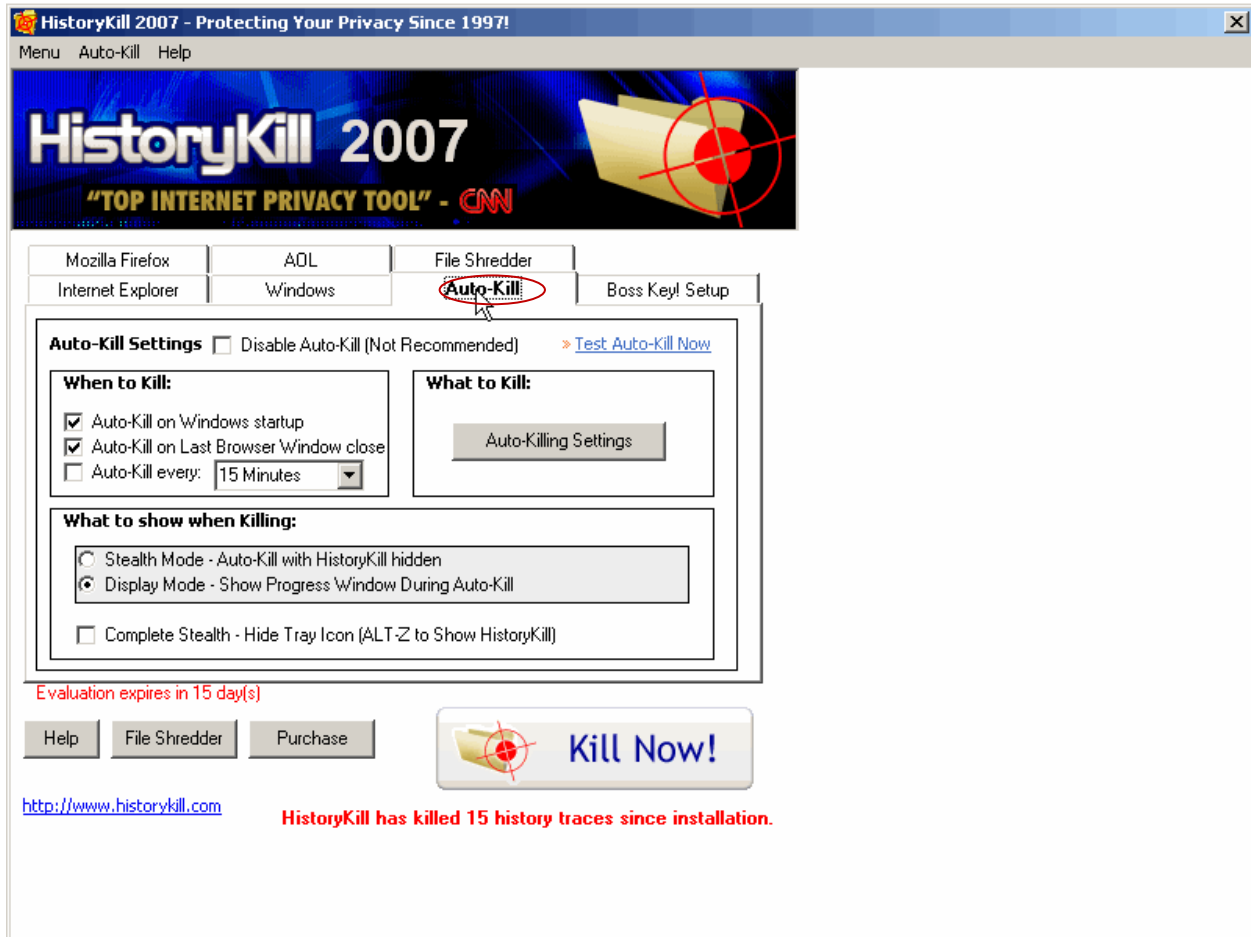
- Click on **Windows**



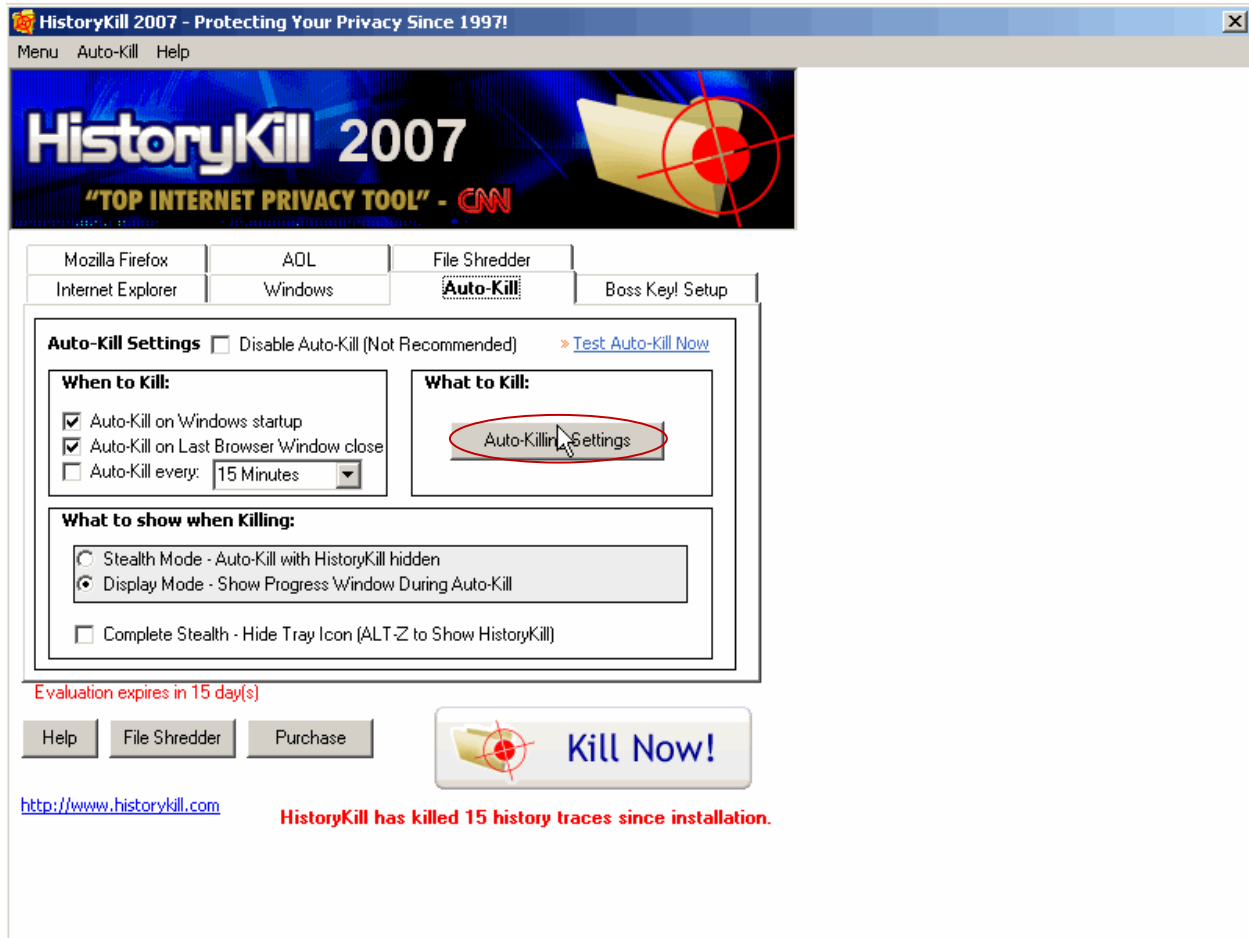
- Click on **Kill Now** to remove the Internet traces



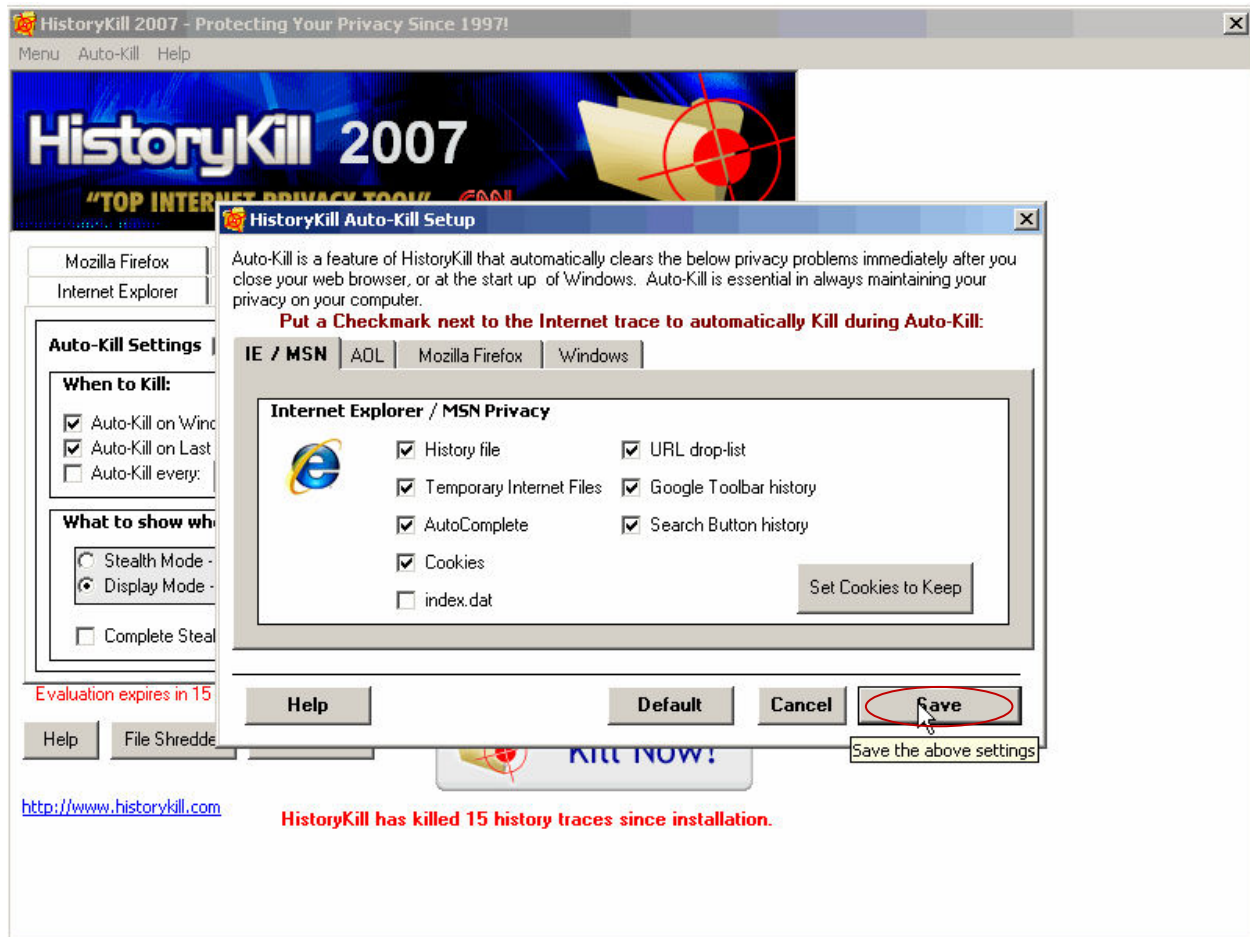
- Click on **Auto-Kill**



- Click on **Auto-Killing Settings**



- Select the options and click on **Save**



- Click on **Kill Now** to remove the Internet Traces



- Click on **File Shredder**



- **Save the Changes**

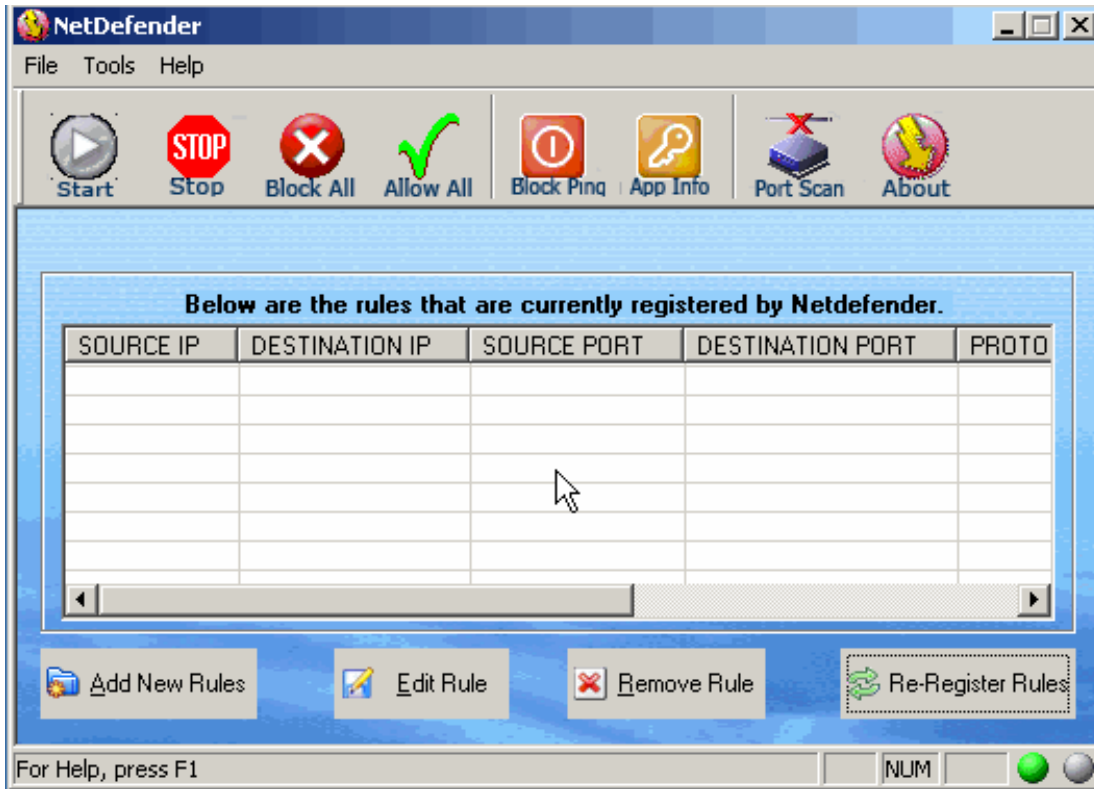


Lab 45-02

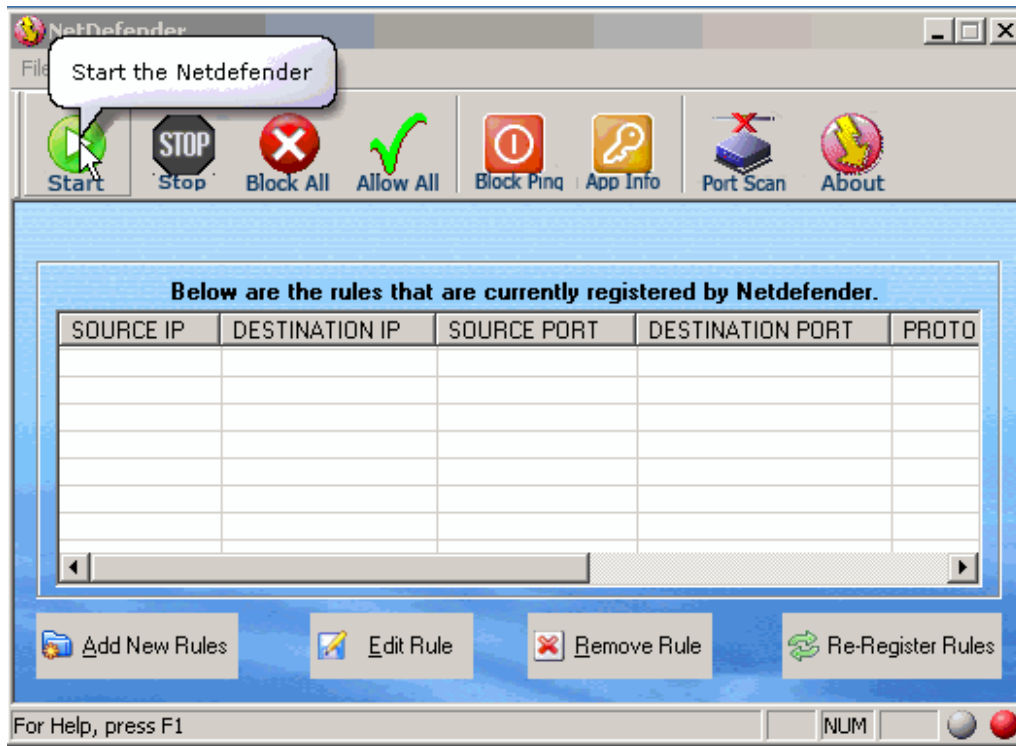
Objective:

Use **NetDefender Firewall** to block all referring traffic.

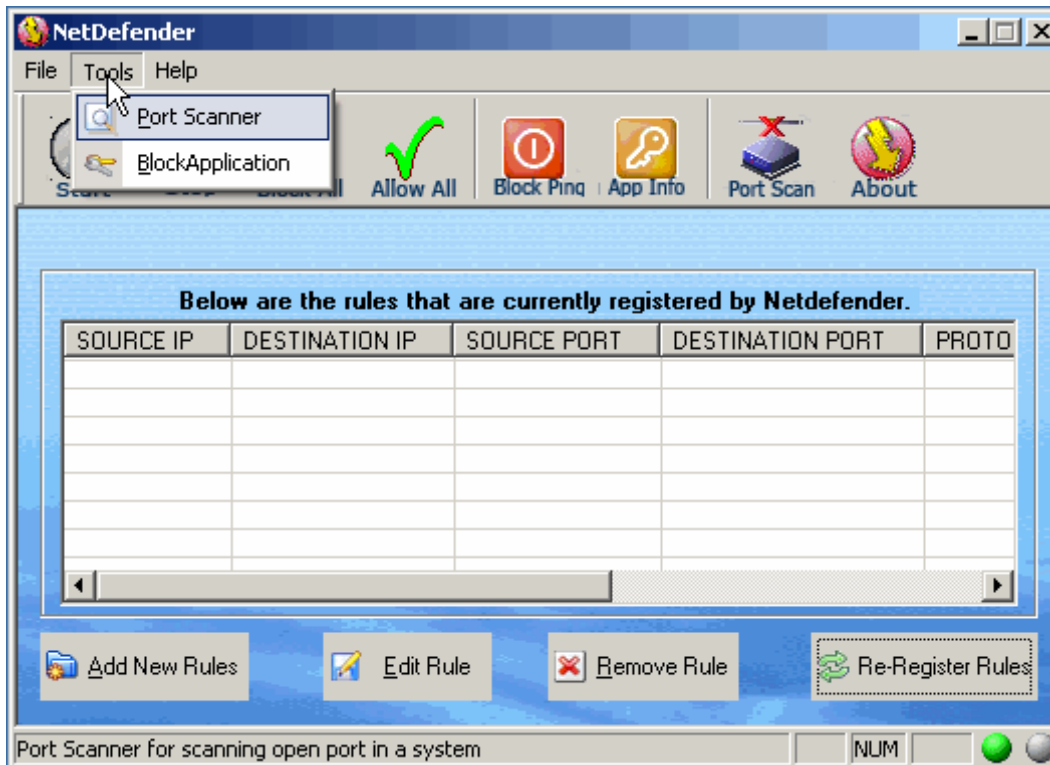
- In the **CEHv6 Labs CD-ROM** navigate to **Module 45**
- Install and launch “**NetDefender Firewall**” program



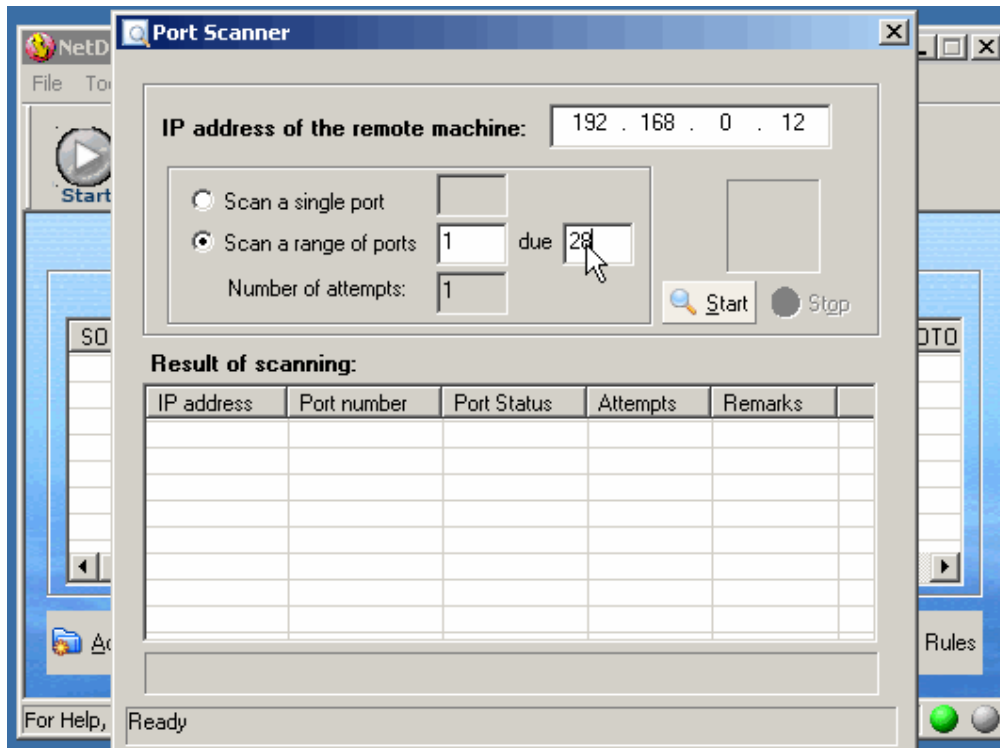
- Click on **Start**



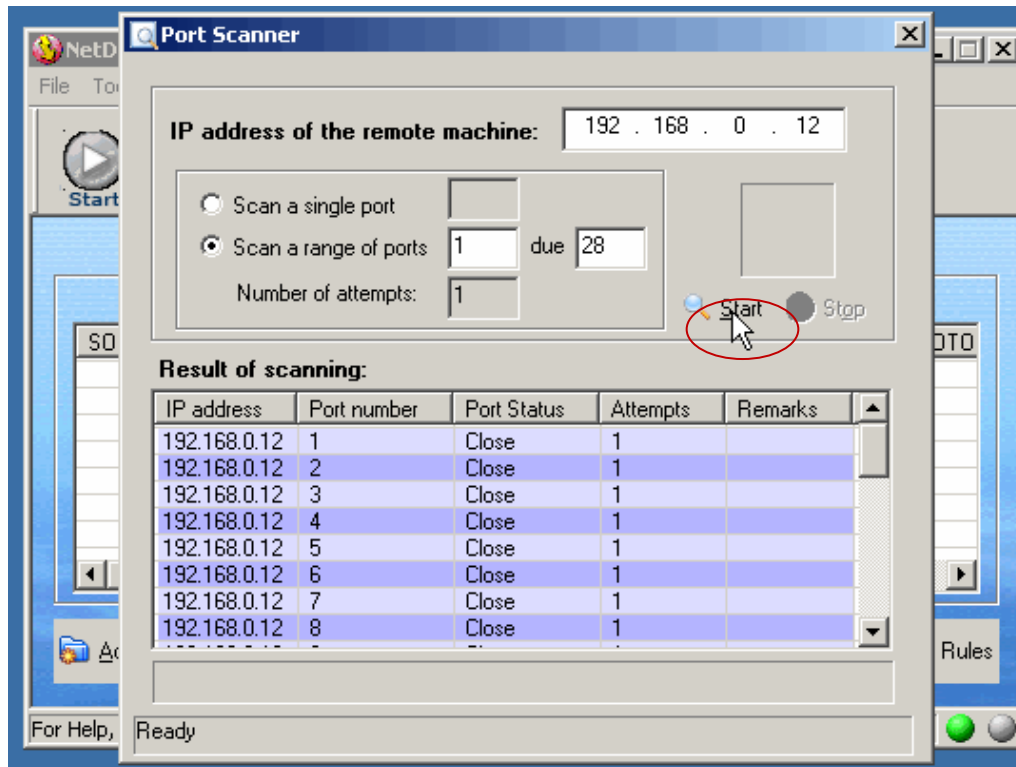
- Click on **Tools** and **Select Port Scanner**



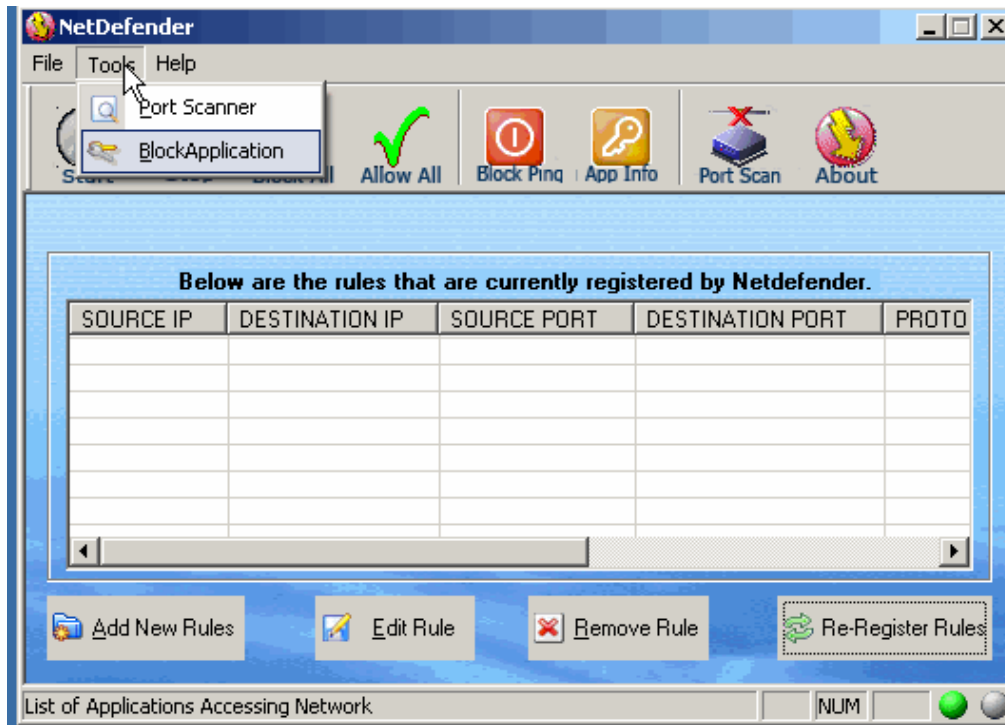
- Write the **IP Address** and **Range of Ports**



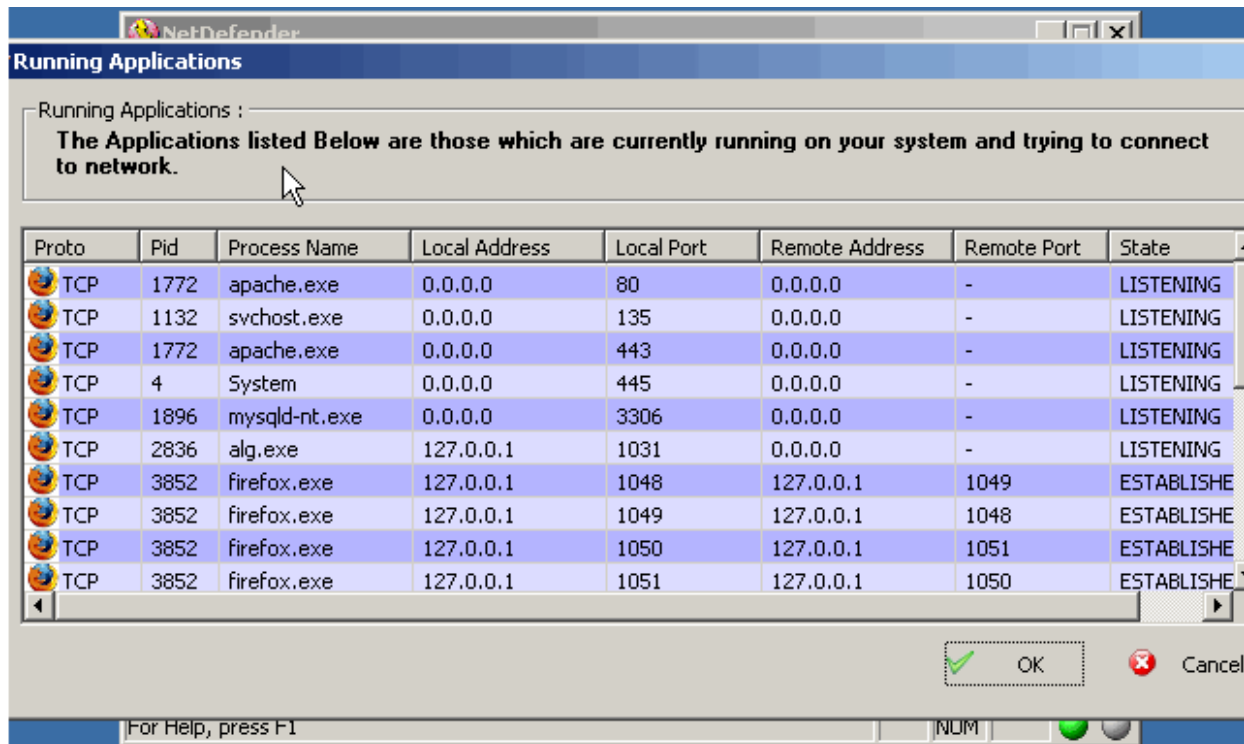
- Click on **Start** and check the **Result of Scanning**



- Click on **Tools** and **Select on BlockScanner**



- Check on **Running Application**

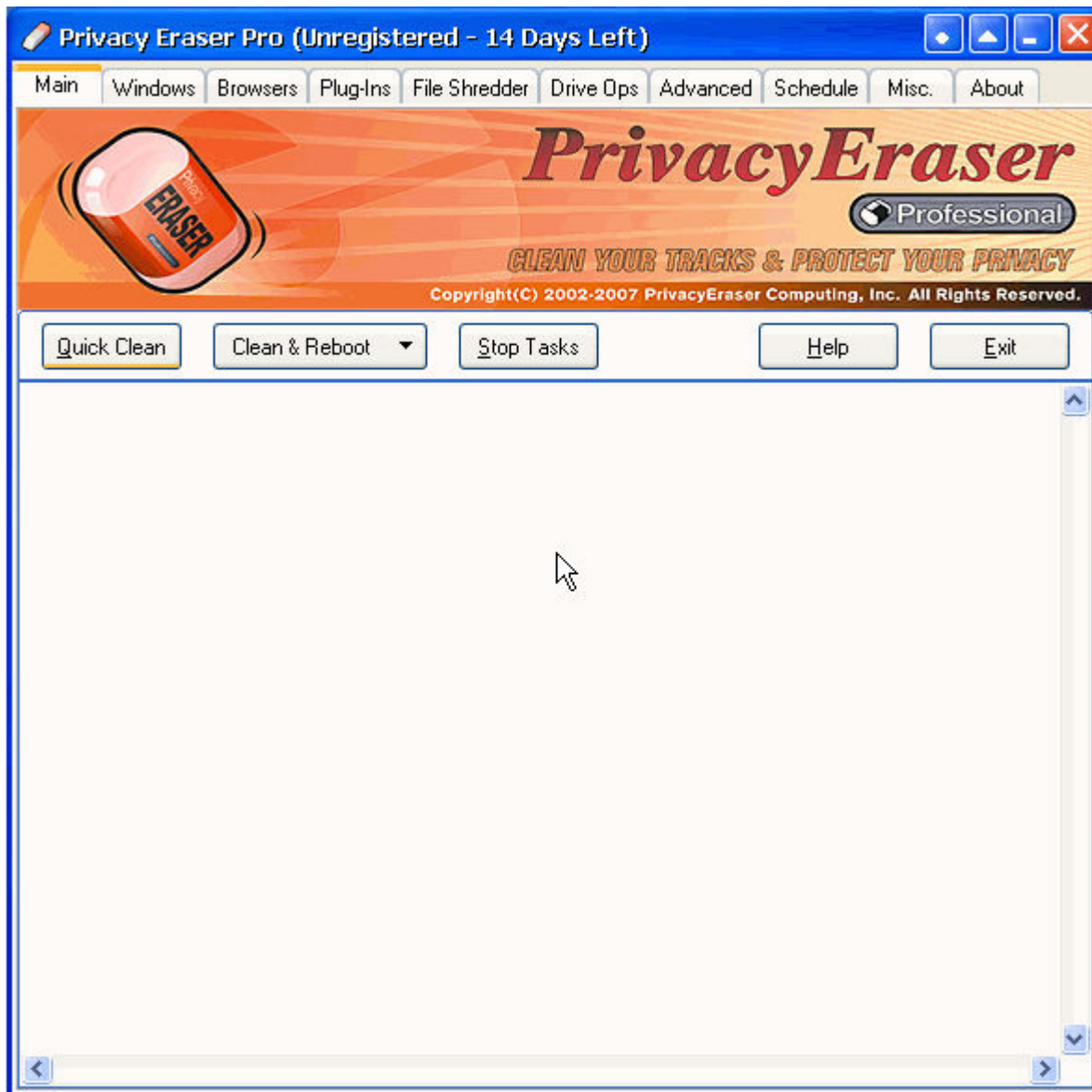


Lab 45-03

Objective:

Privacy Eraser is an Internet **Eraser** that protects Internet **privacy** by cleaning up all the tracks of Internet and computer activities.

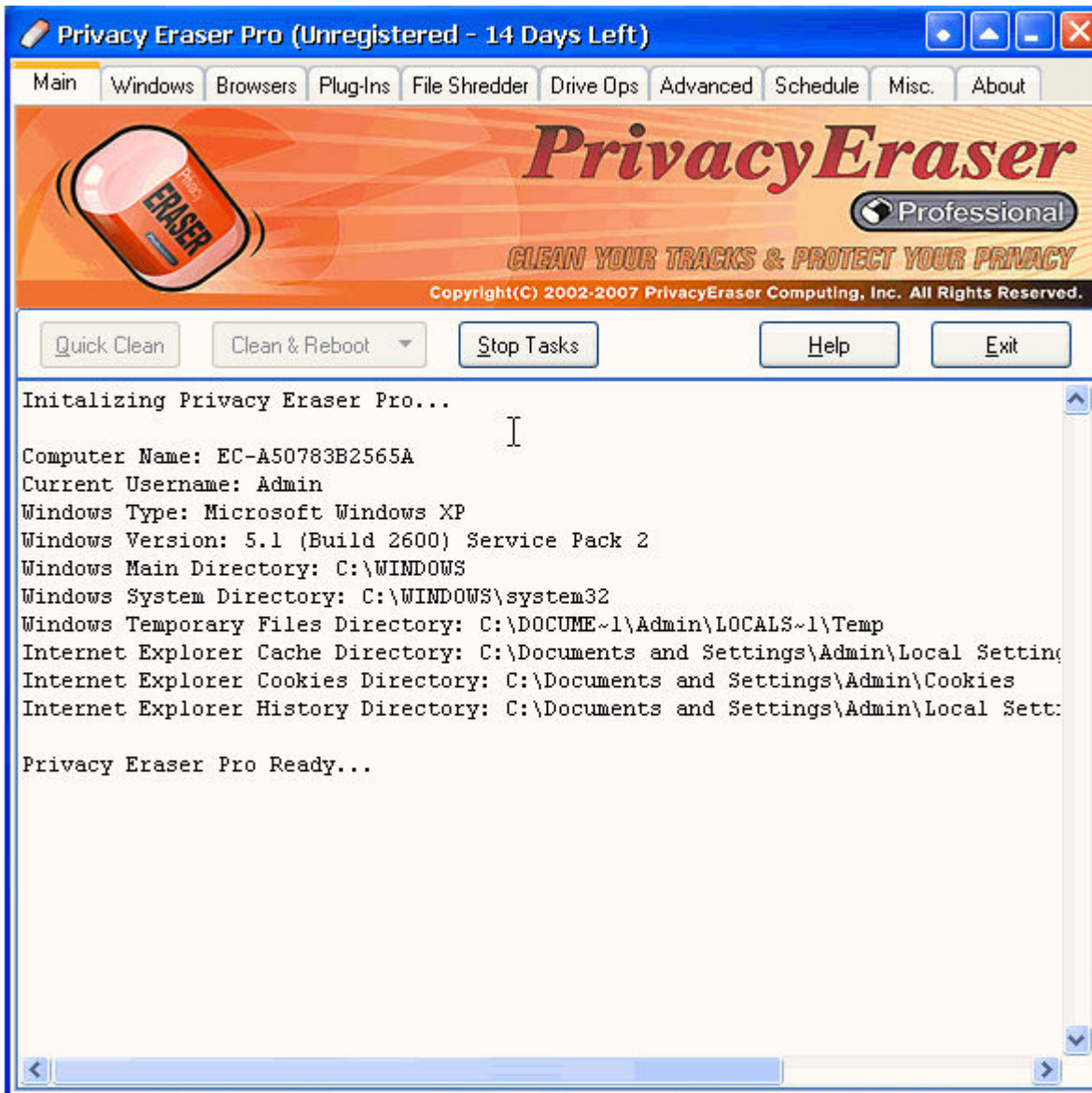
- In the **CEHv6 Labs CD-ROM** navigate to **Module 45**
- Install and launch "**Privacy Eraser**" program



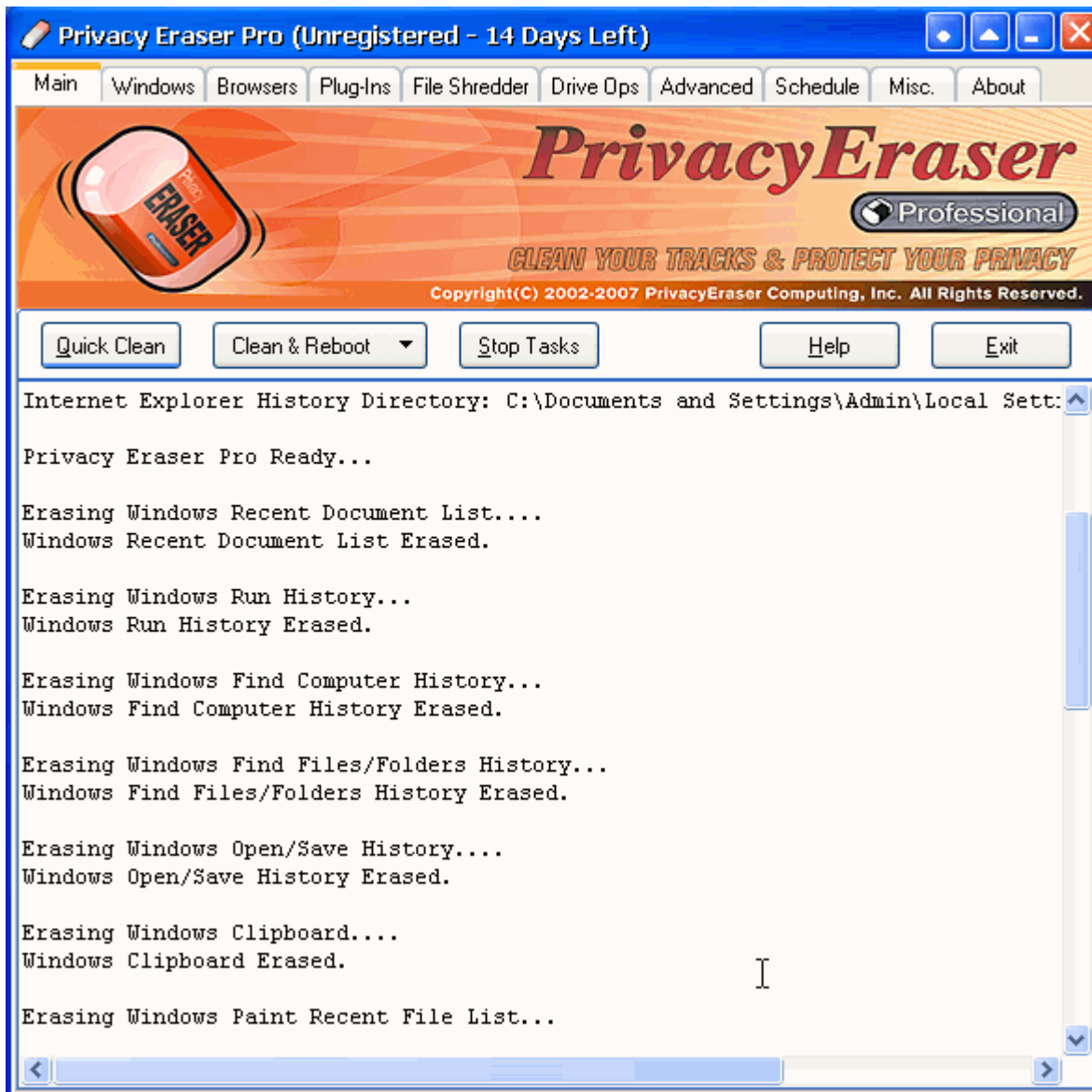
- Click on **Quick Clean**



- Privacy Eraser Pro is Initializing



- Tracks for the Internet and Computer Activity are erased

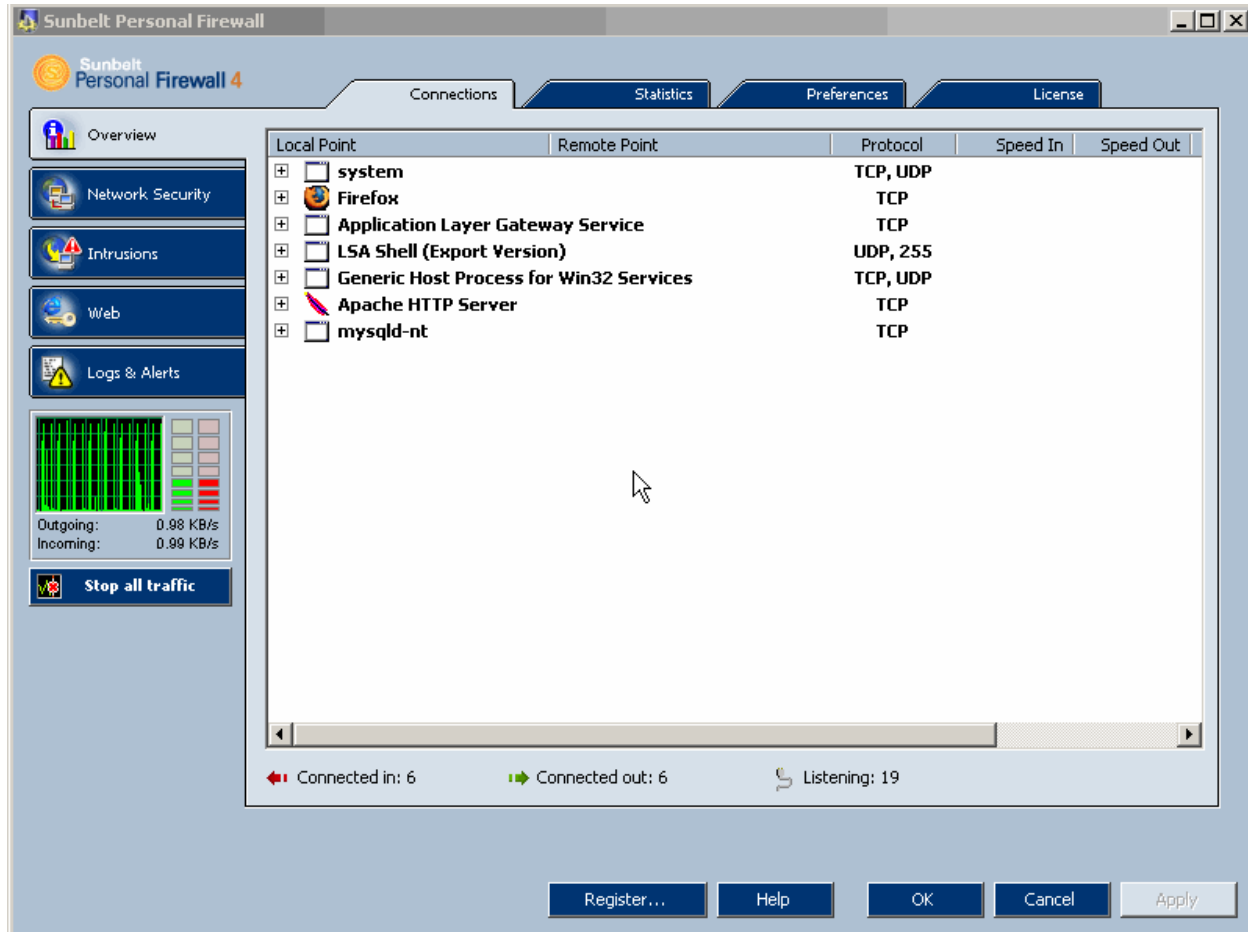


Lab 45-04

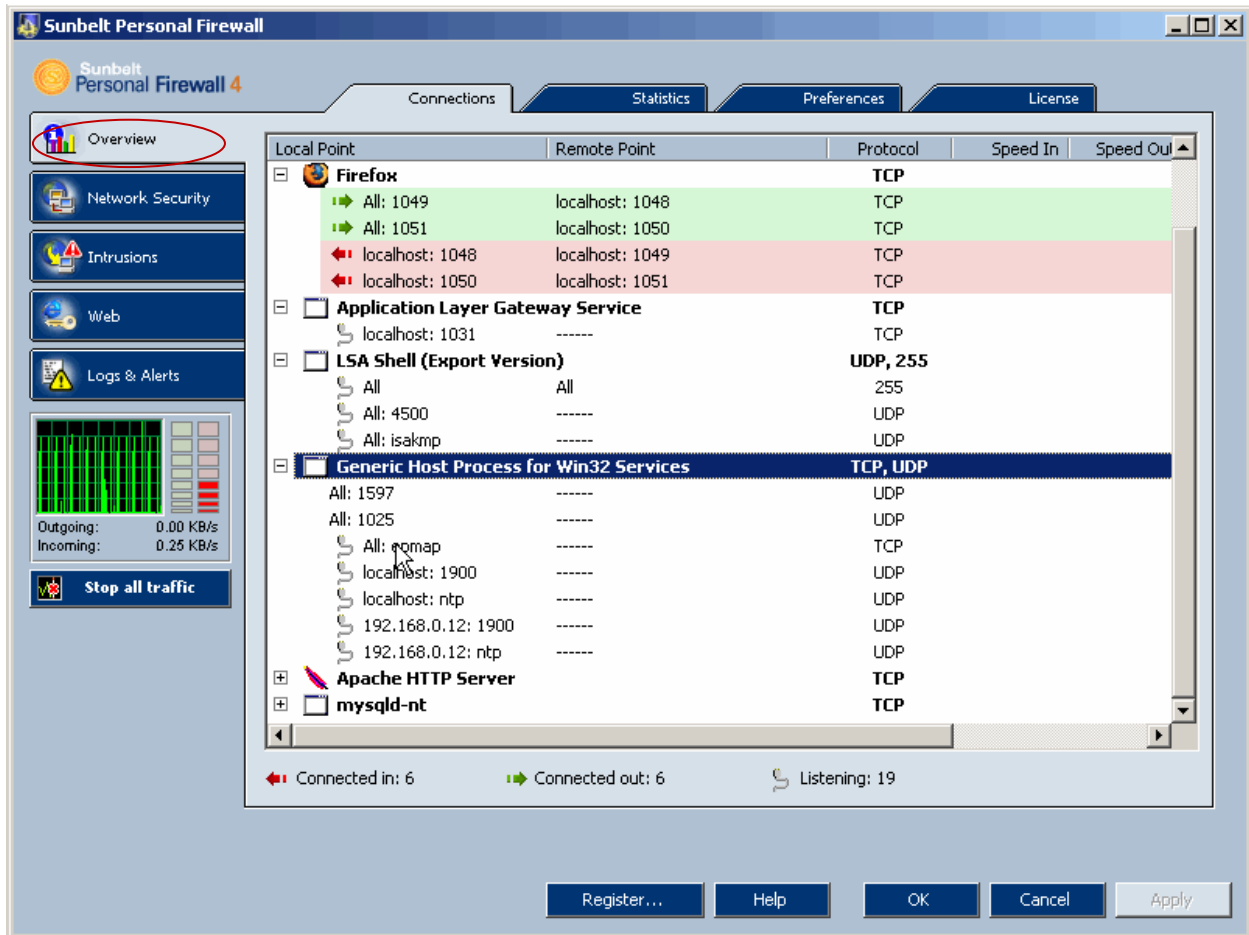
Objective:

Use **Sunbelt Personal Firewall** to protect and control your Internet connection.

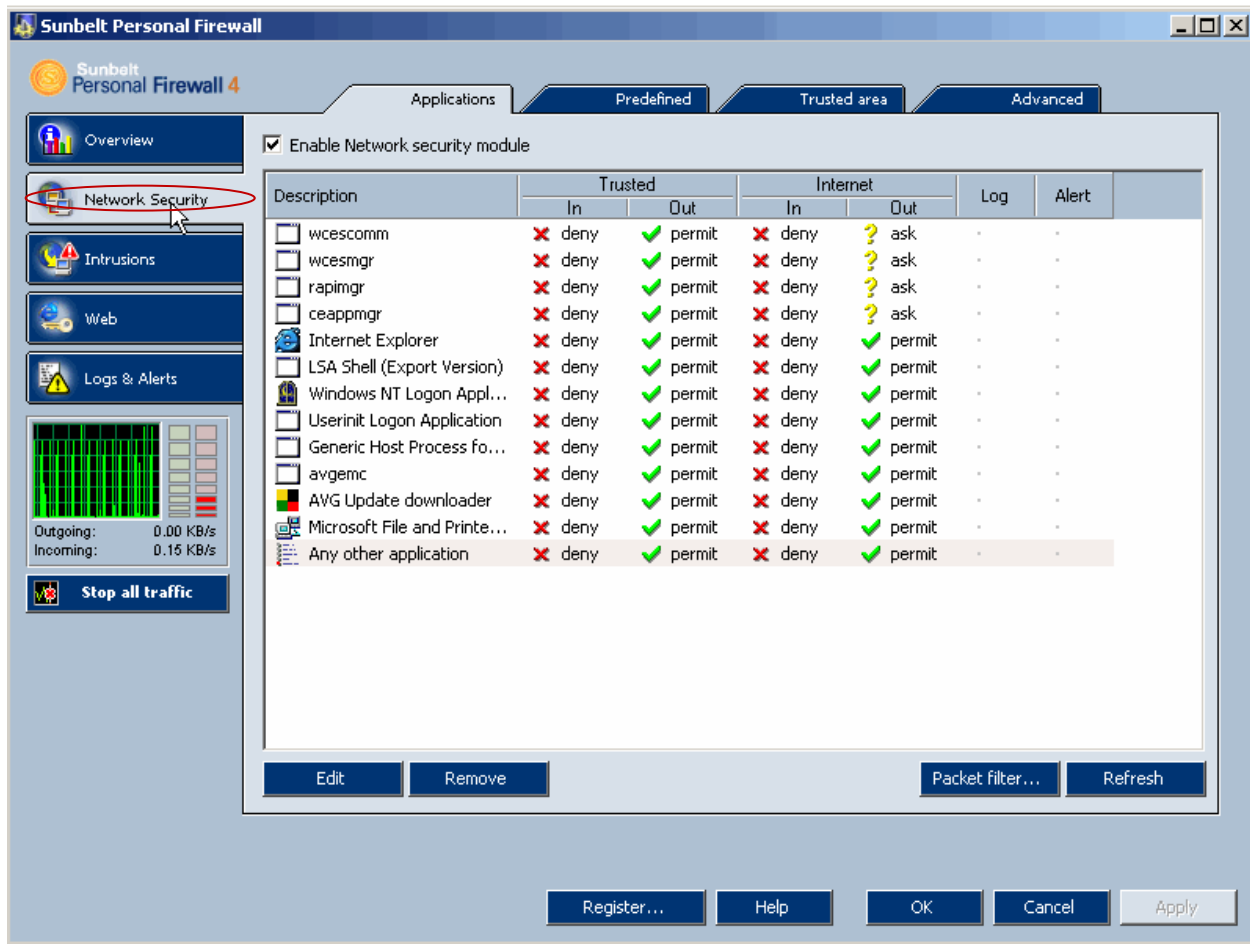
- In the **CEHv6 Labs CD-ROM** navigate to **Module 45**
- Install and launch “**Sunbelt Personal Firewall**” program



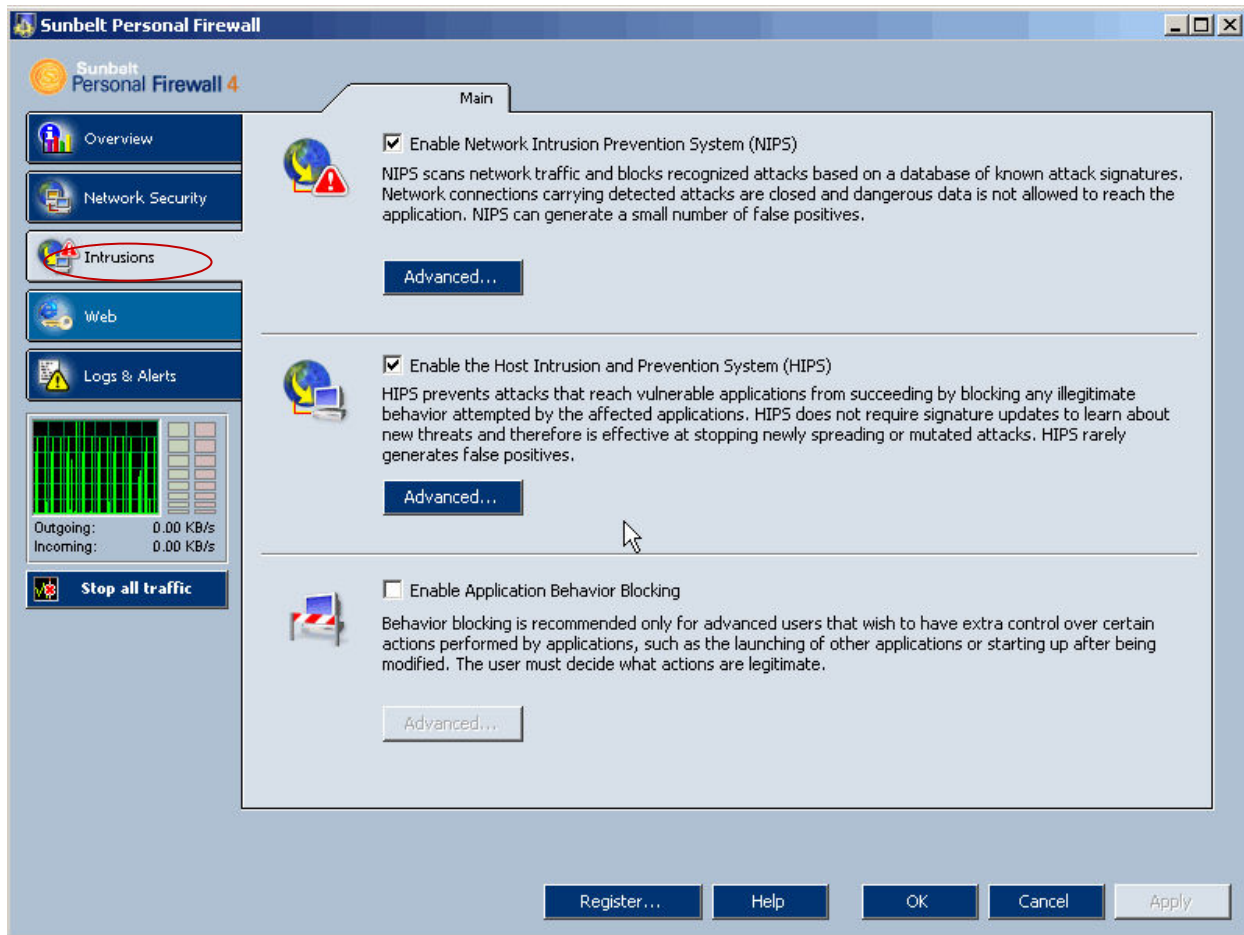
- Check the **Overview** of the System



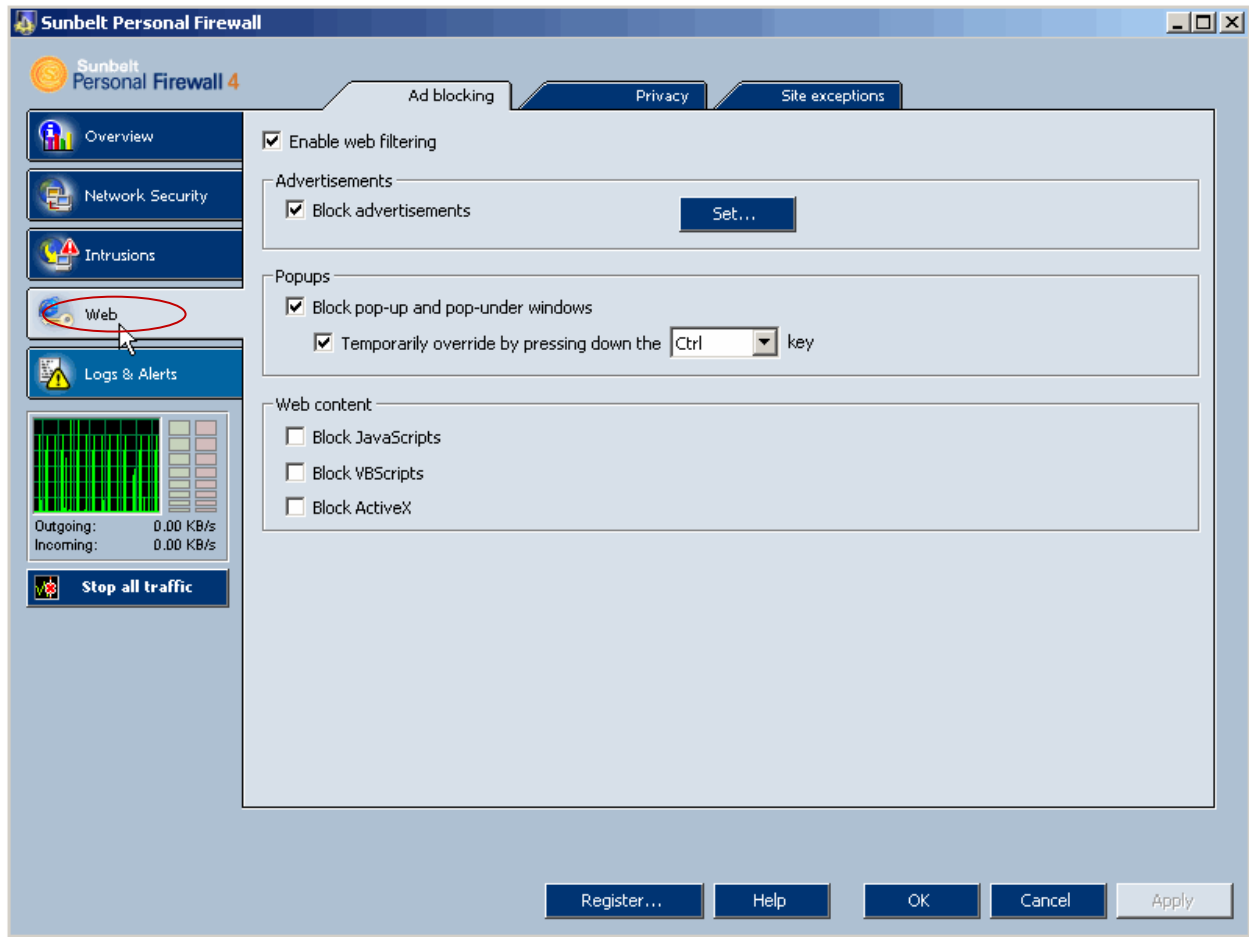
- Click on **Network Security**



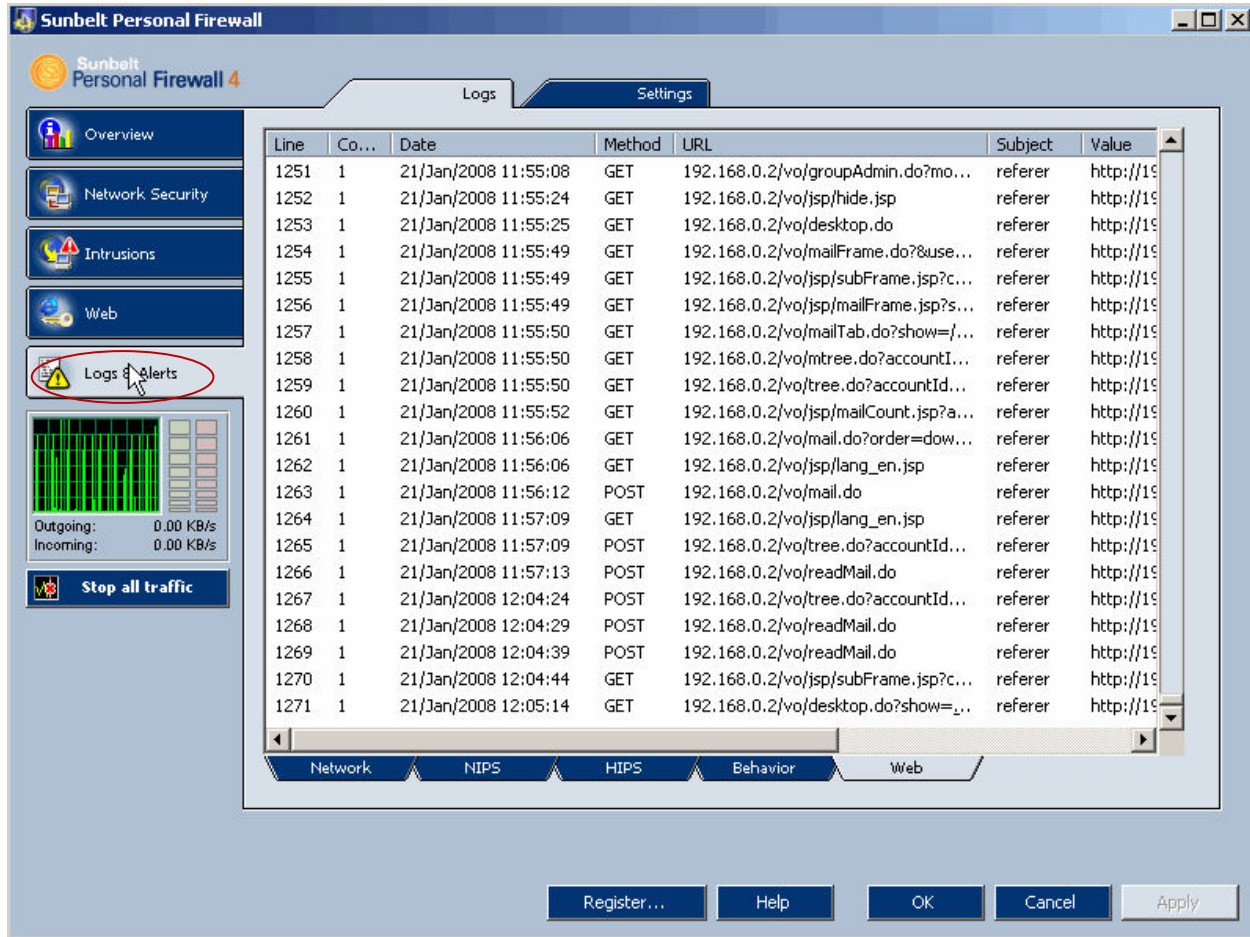
- Click on **Instructions** and Select the tabs



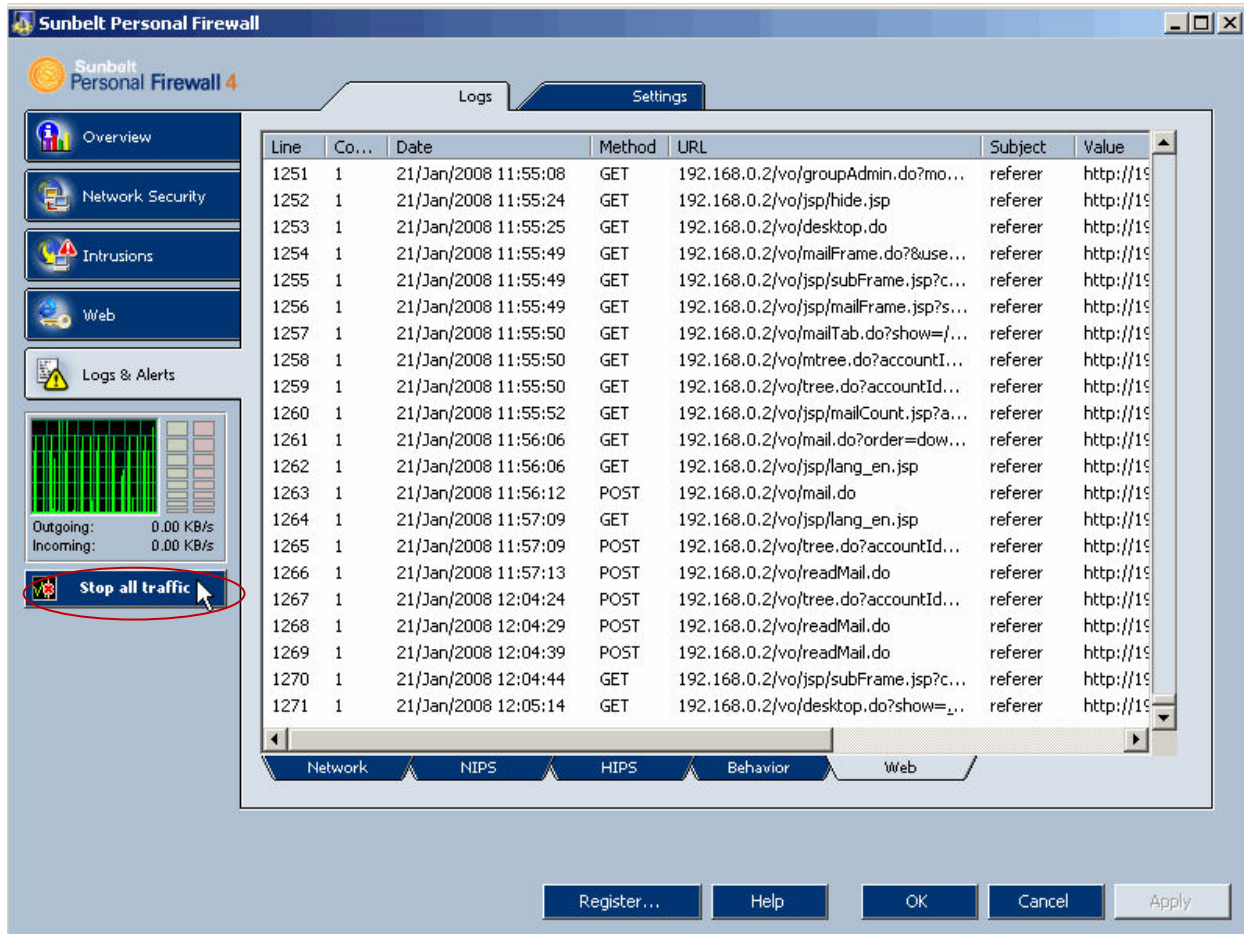
- Click on **Web** and Select the Tabs



- Click on **Logs and Alerts**



- To stop all traffic , Click on **Stop all traffic**

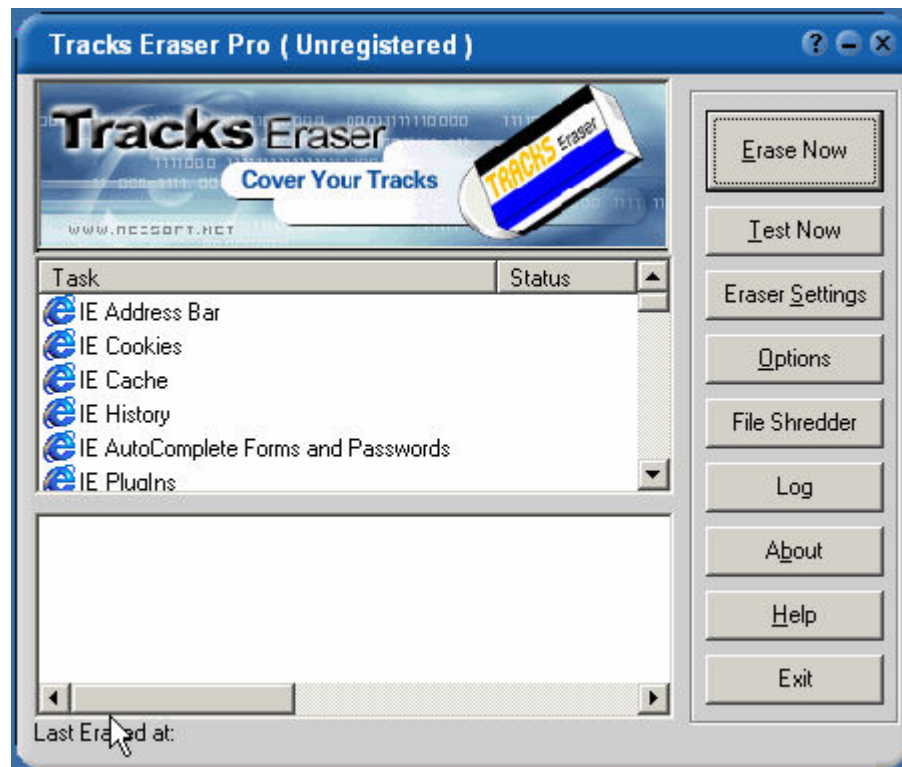


Lab 45-05

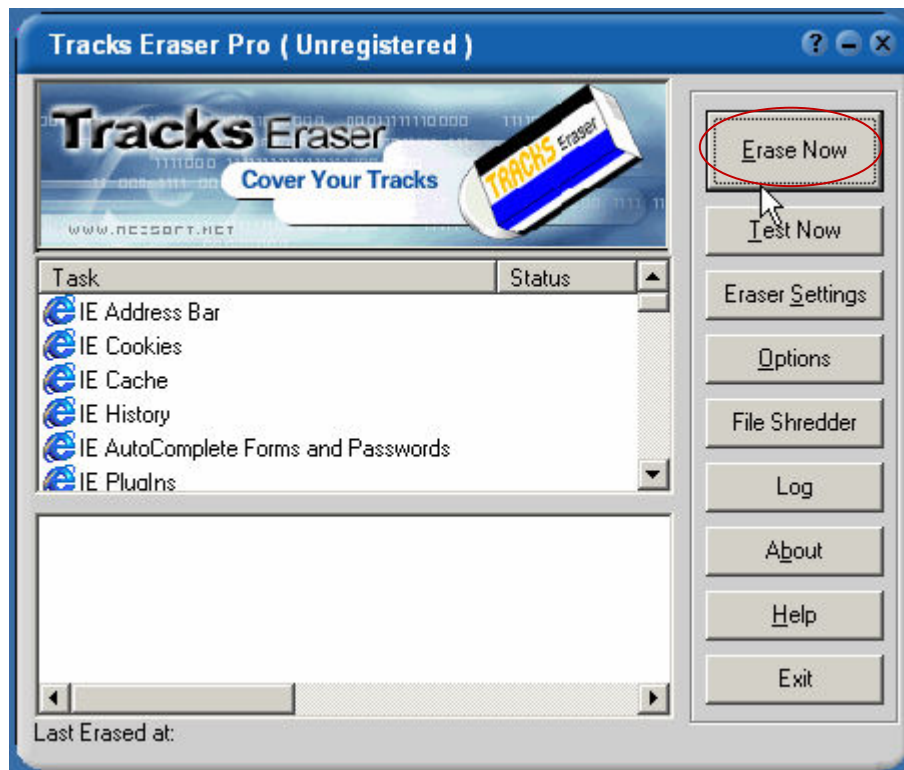
Objective:

Use **TraceEraser Pro** to delete internet history tracks and to protect privacy.

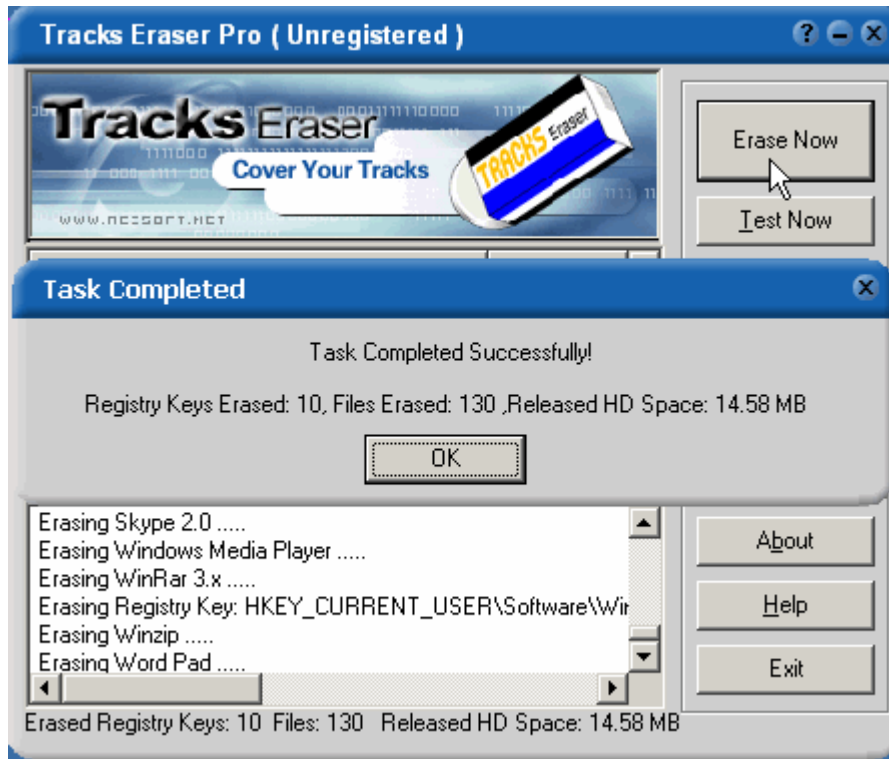
- In the **CEHv6 Labs CD-ROM** navigate to **Module 45**
- Install and launch “**TraceEraser Pro**” program



- Click on **Erase Now** to erase all tracks



- Click on **OK**

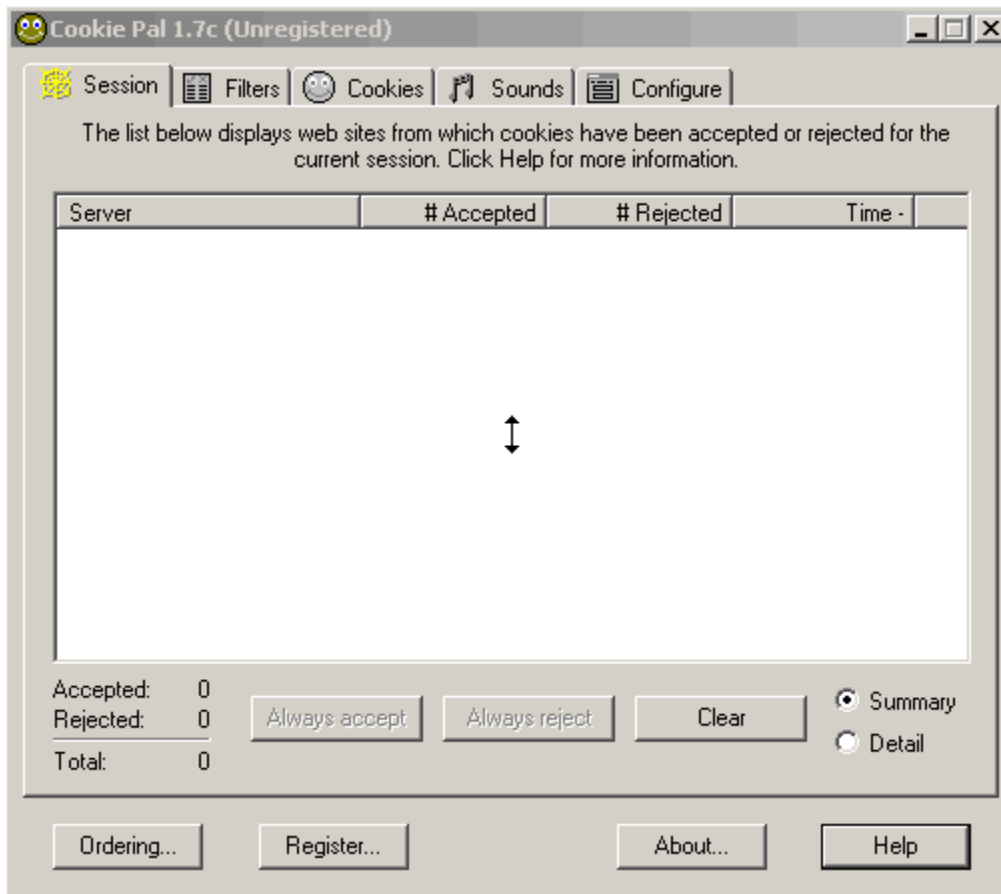


Lab 45-06

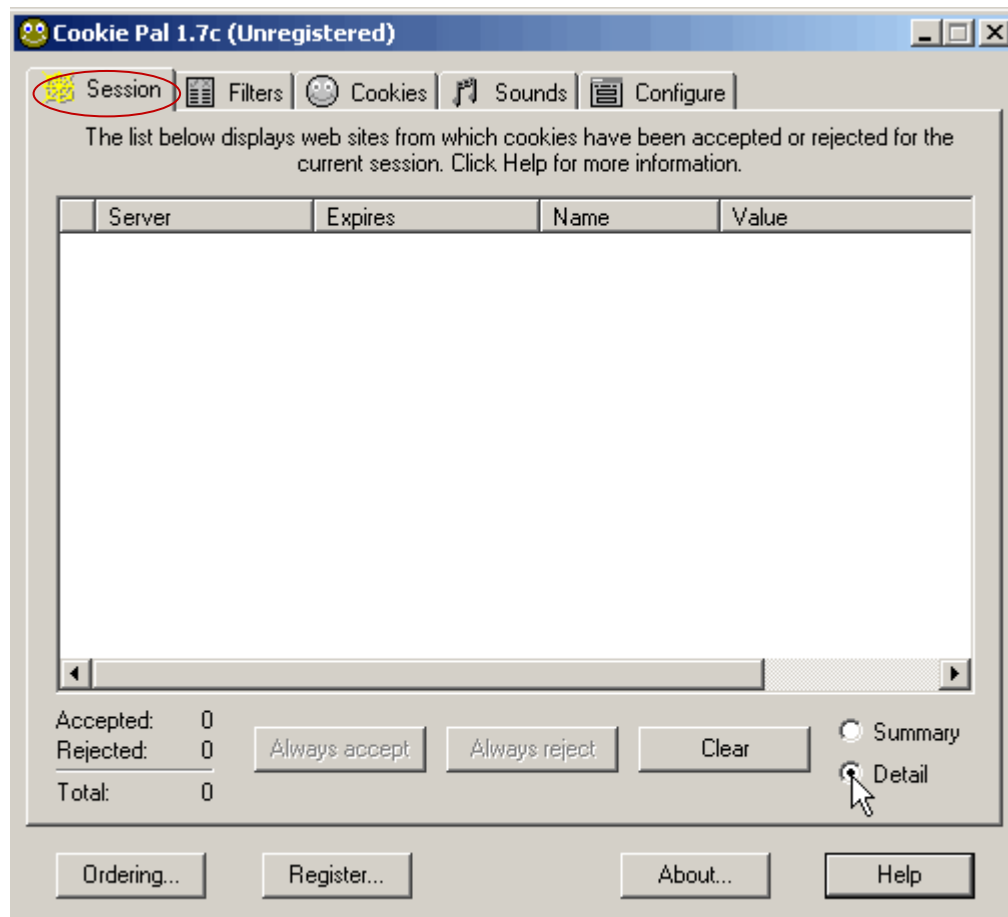
Objective:

Use **Cookie Pal** to protect privacy on Internet.

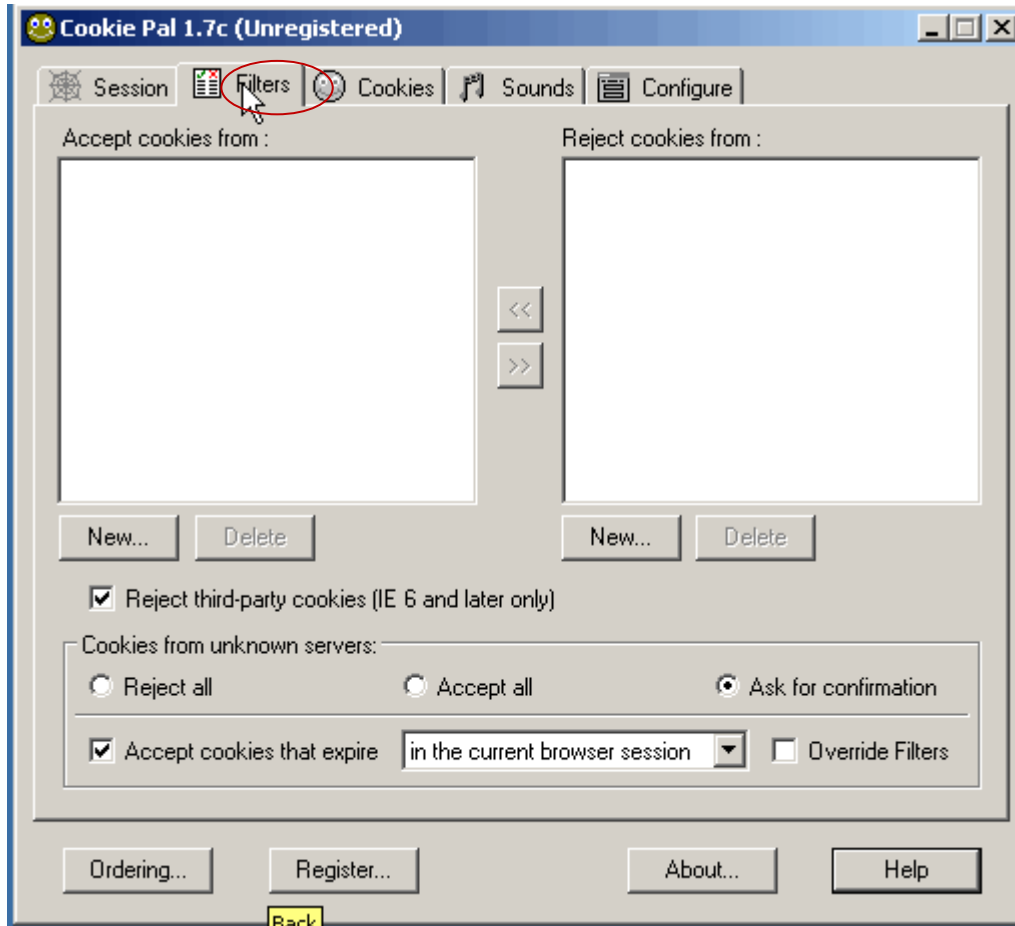
- In the **CEHv6 Labs CD-ROM** navigate to **Module 45**
- Install and launch “**Cookie Pal**” program



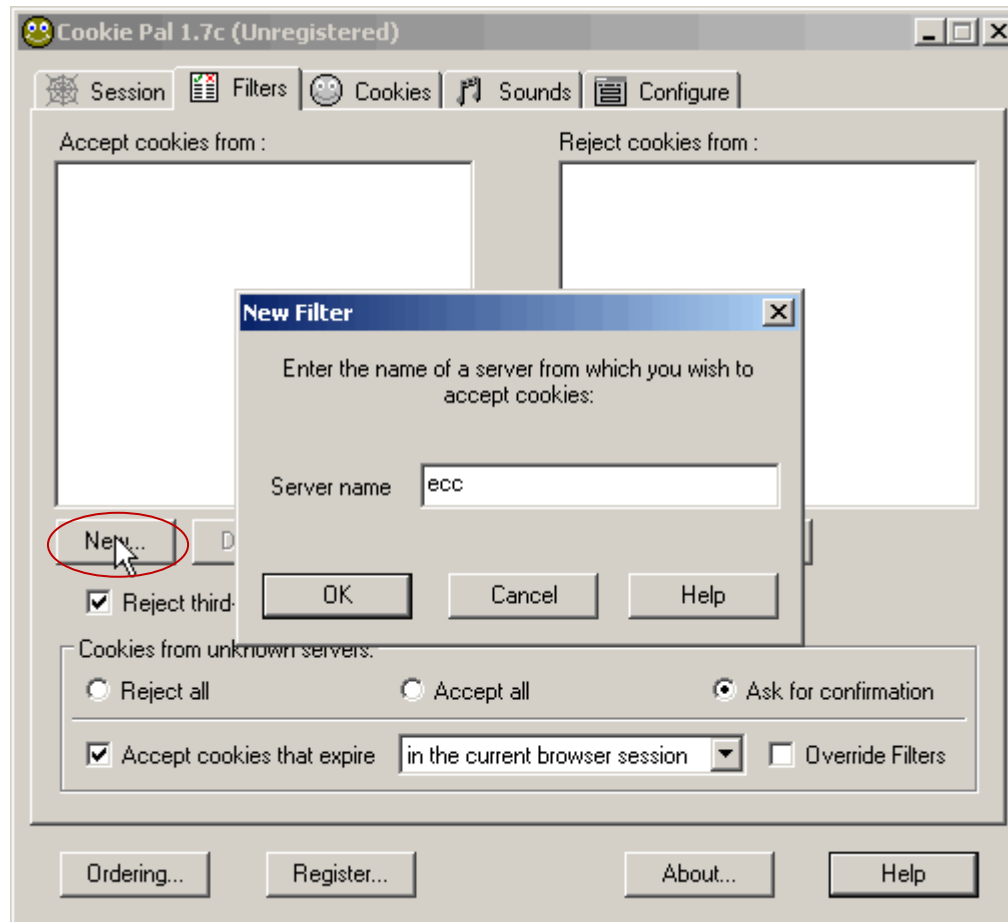
- Click on **Session** to accept or reject cookies for current session



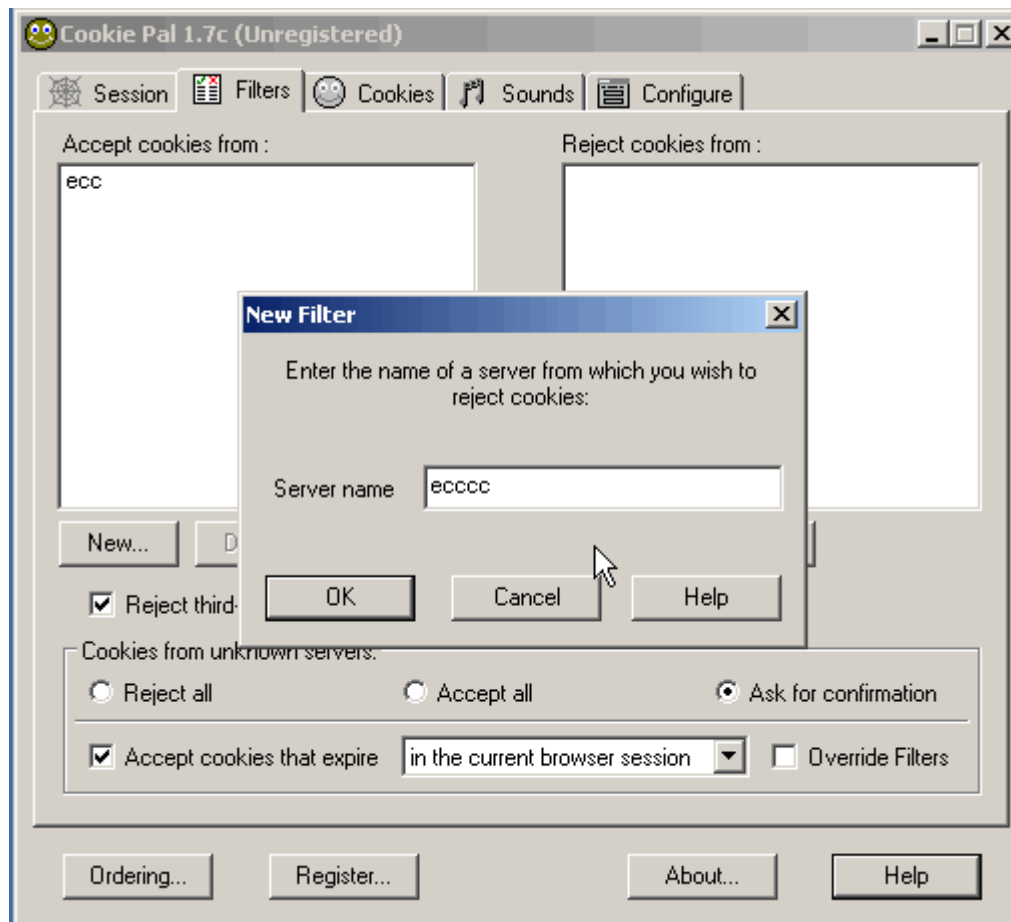
- Click on **Filter** to provide information to accept and reject cookies



- Click on **New** and write the name of server from which to accept cookies

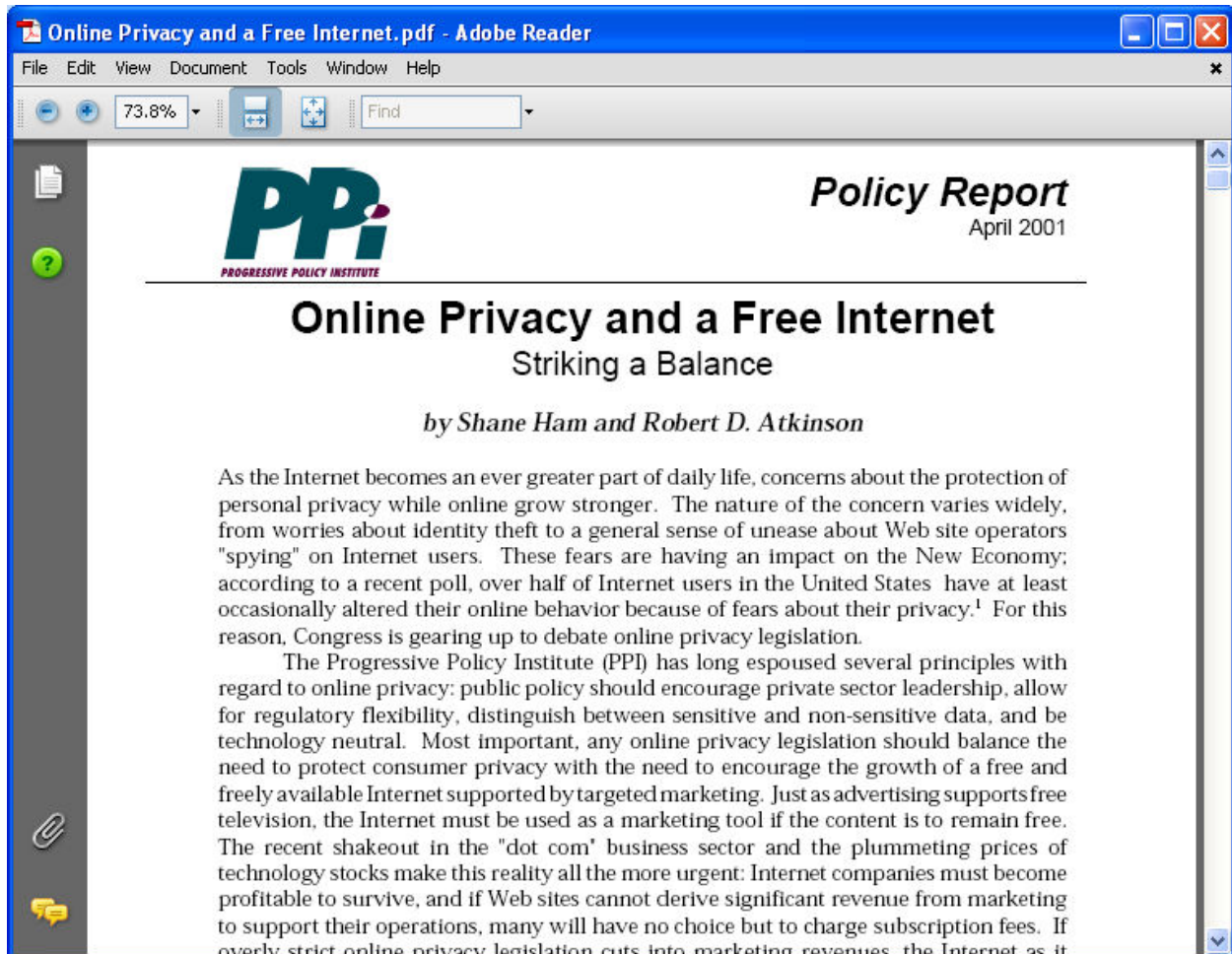


- Click **New** and write the name of server from which to reject cookies



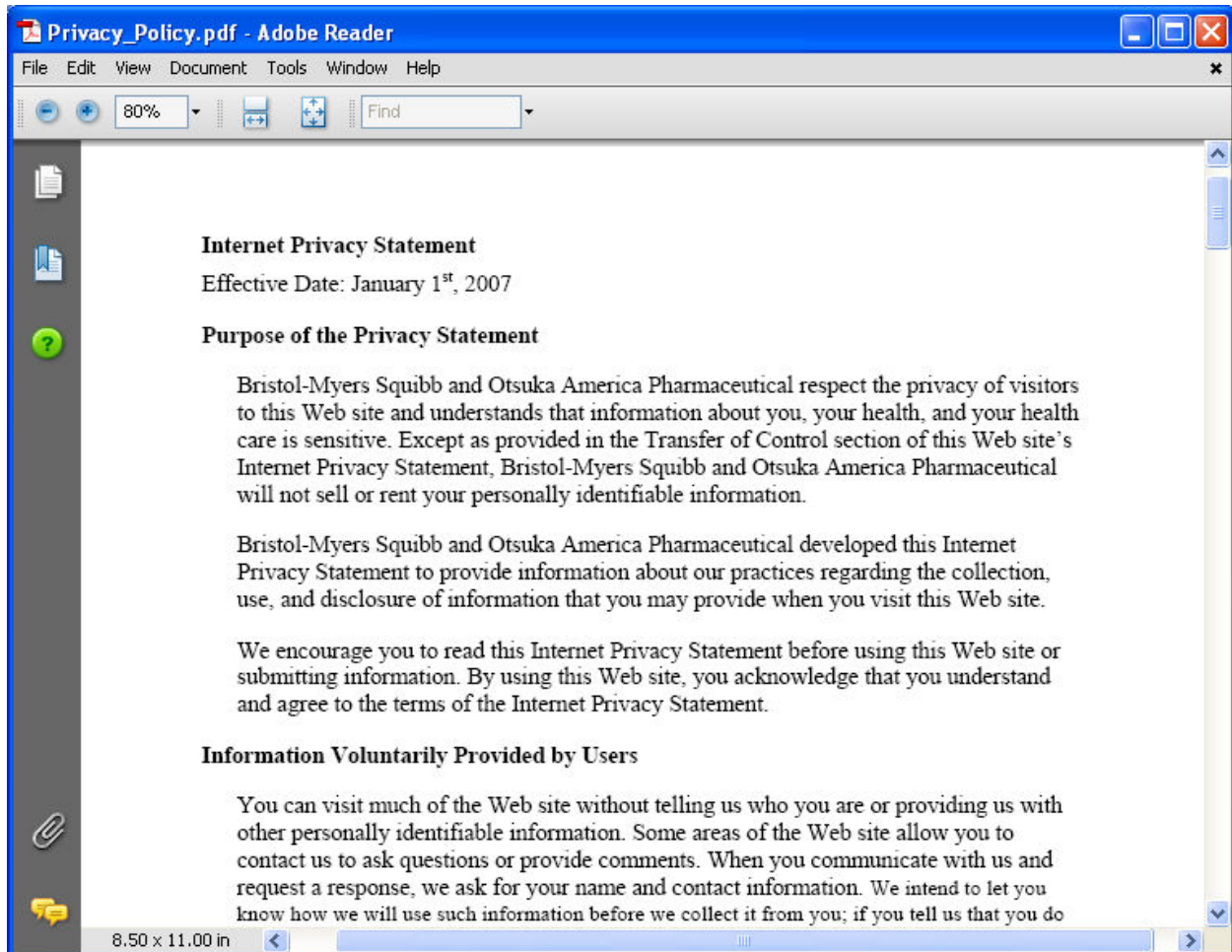
Lab 45-07

- In the **CEHv6 Labs CD-ROM** navigate to **Module 45**
- Open the **Online Privacy and a Free Internet.pdf** and read the content



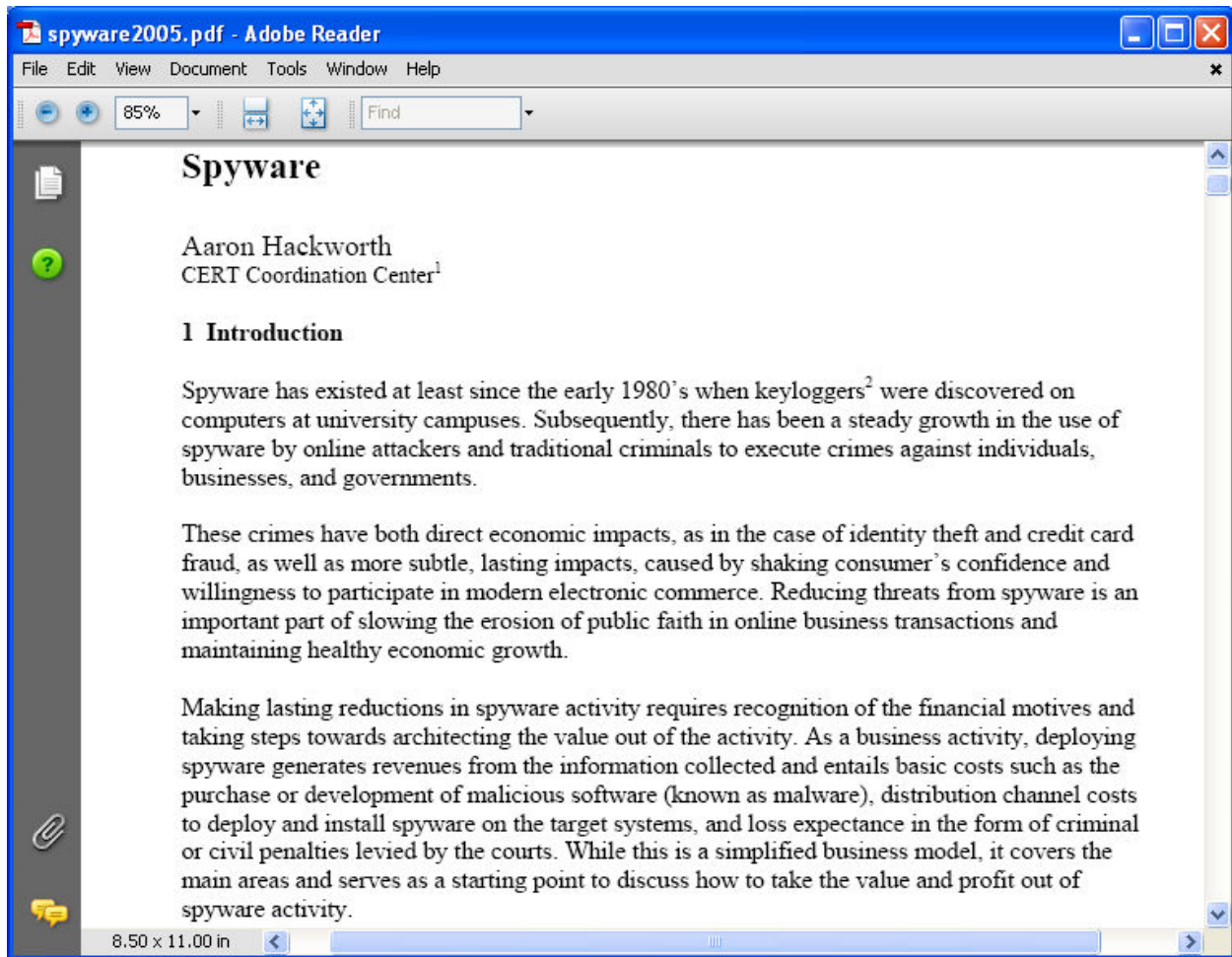
Lab 45-08

- In the **CEHv6 Labs CD-ROM** navigate to **Module 45**
- Open the **Privacy_Policy.pdf** and read the content



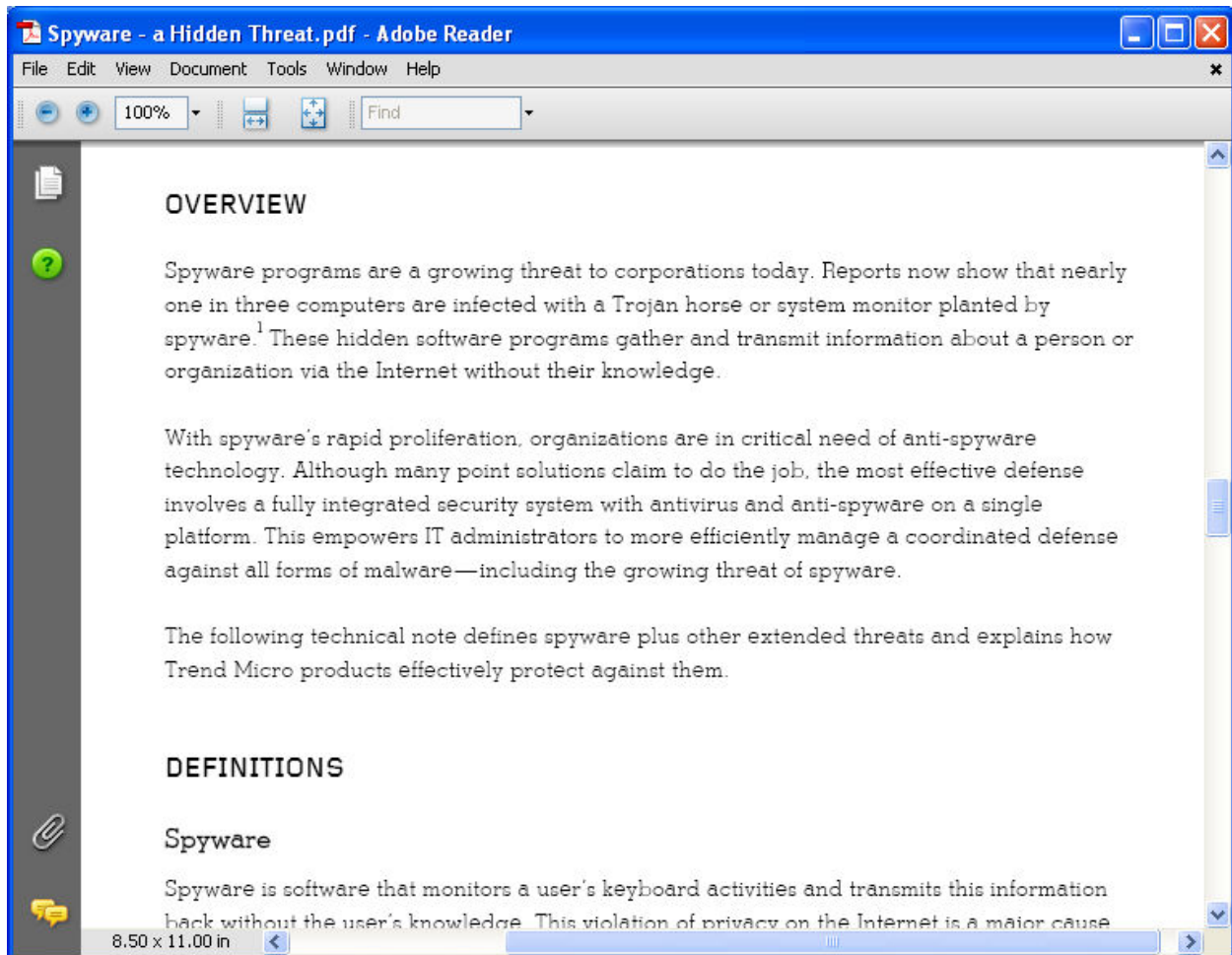
Lab 45-09

- In the CEHv6 Labs CD-ROM navigate to **Module 45**
- Open the **spyware2005.pdf** and read the content



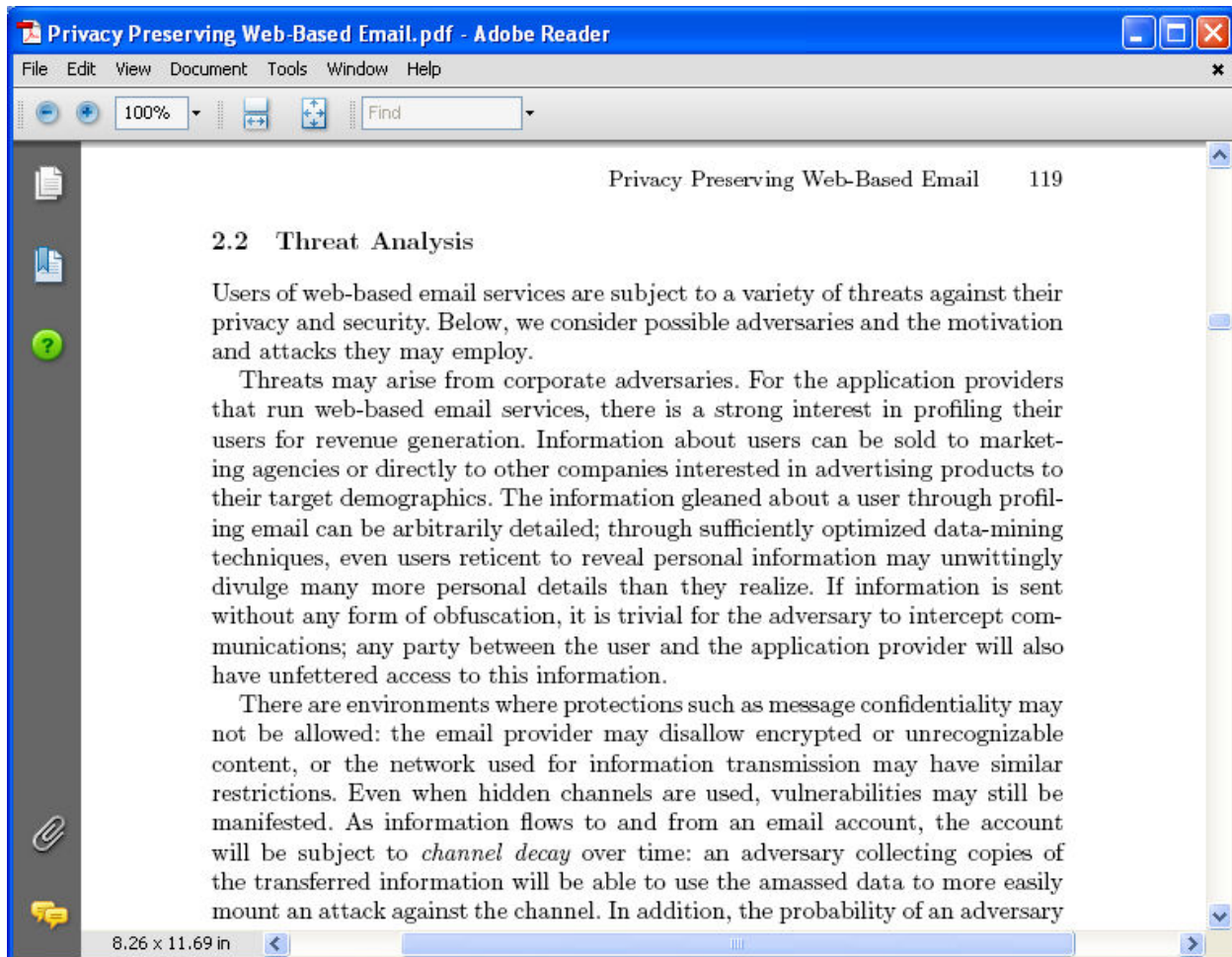
Lab 45-10

- In the **CEHv6 Labs CD-ROM** navigate to **Module 45**
- Open the **Spyware – a Hidden Threat.pdf** and read the content



Lab 45-11

- In the **CEHv6 Labs CD-ROM** navigate to **Module 45**
- Open the **Privacy Preserving Web-Based Email.pdf** and read the content





Module 46

Securing Laptop Computers

Lab 46-01

Objective:

Use **Connection Manager Pro** to manage available network connections.

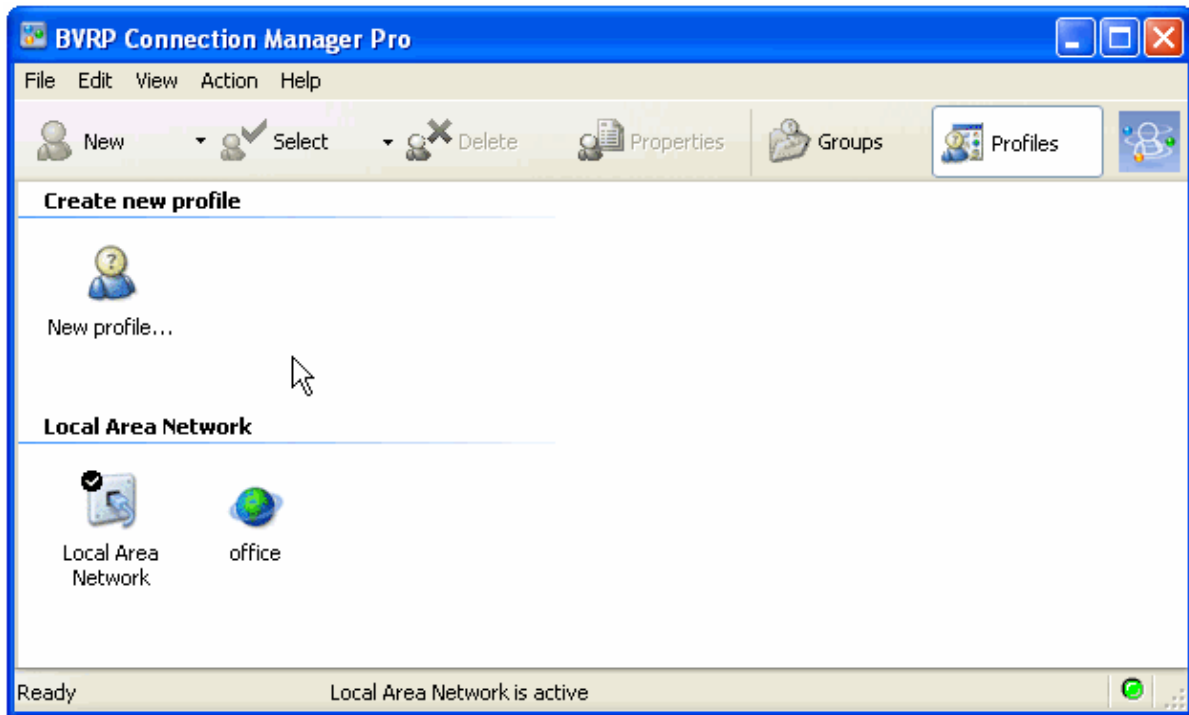
- In the **CEHv6 Labs CD-ROM** navigate to **Module 46**
- Install and launch **BVRP Connection Manager Pro** program



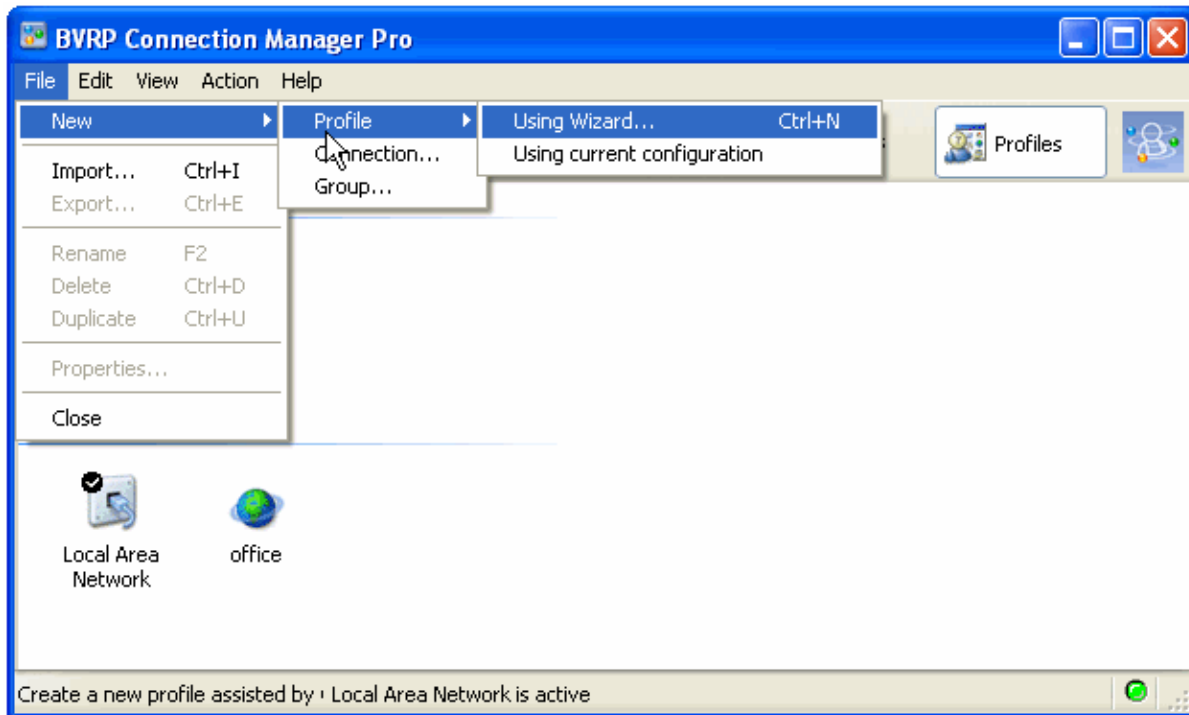
- To setup a profile click on  and click profile name (e.g. **office**)



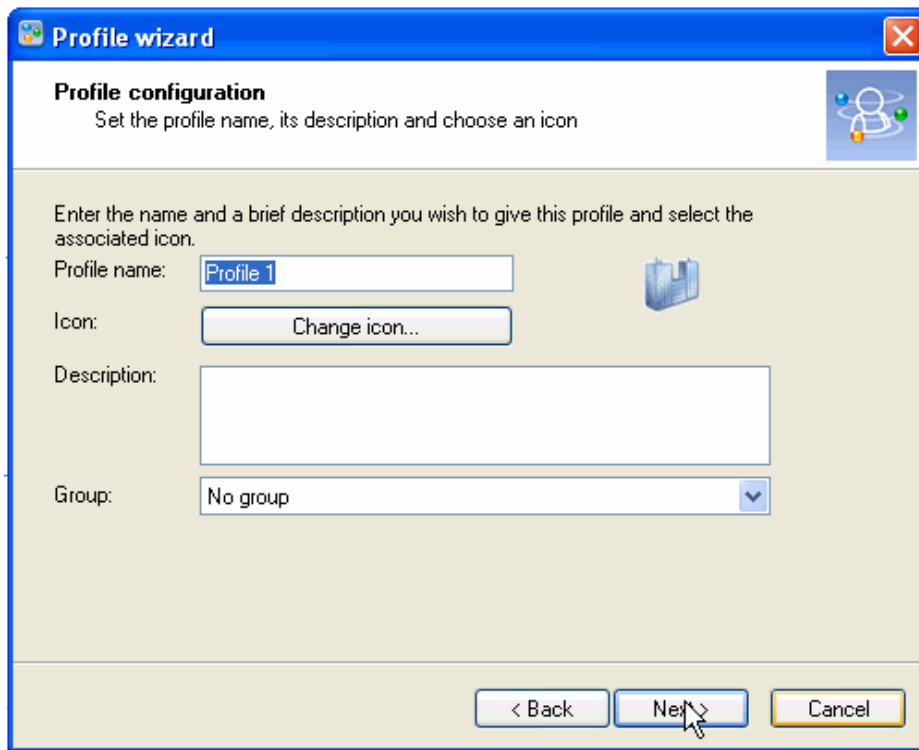
- The List of Profiles is as shown



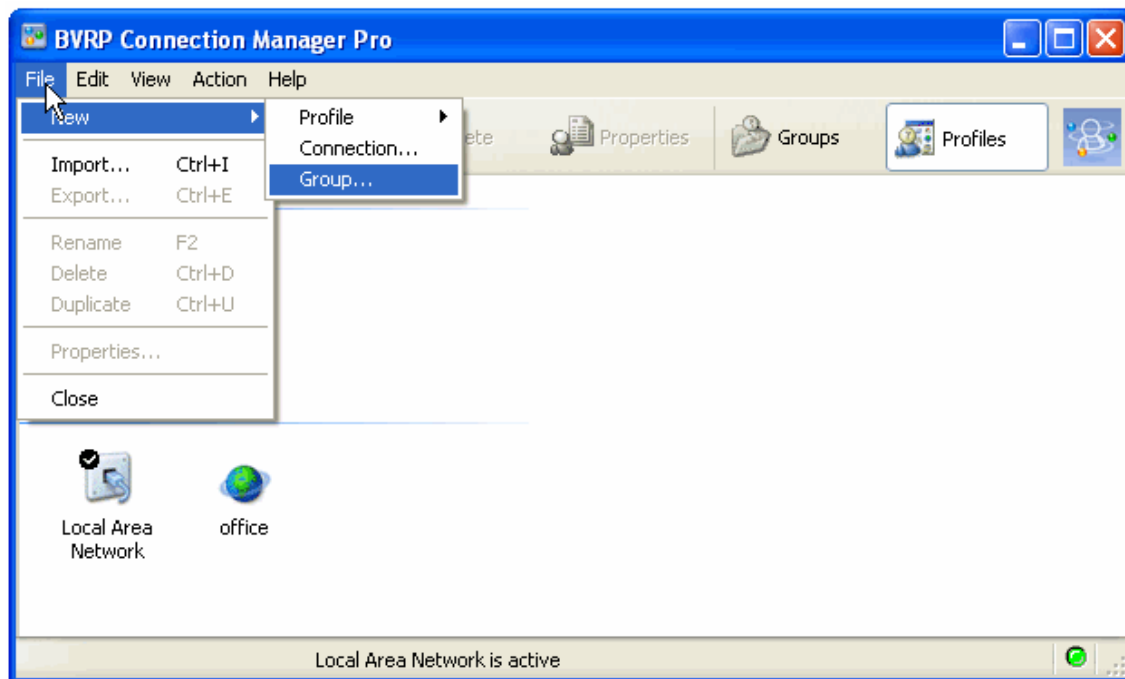
- To create a profile Using Wizard, click on **File→New→Profile→Using Wizard**



- Enter the profile information and click **Next**




- To create a New Group click on **File→New→Group**



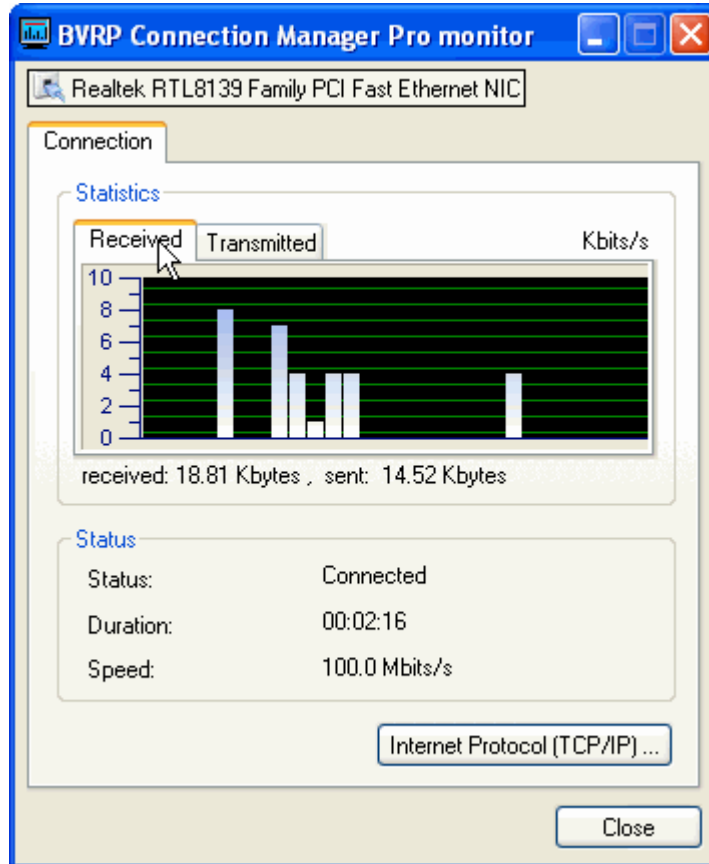
- To connect to the wireless network click on 



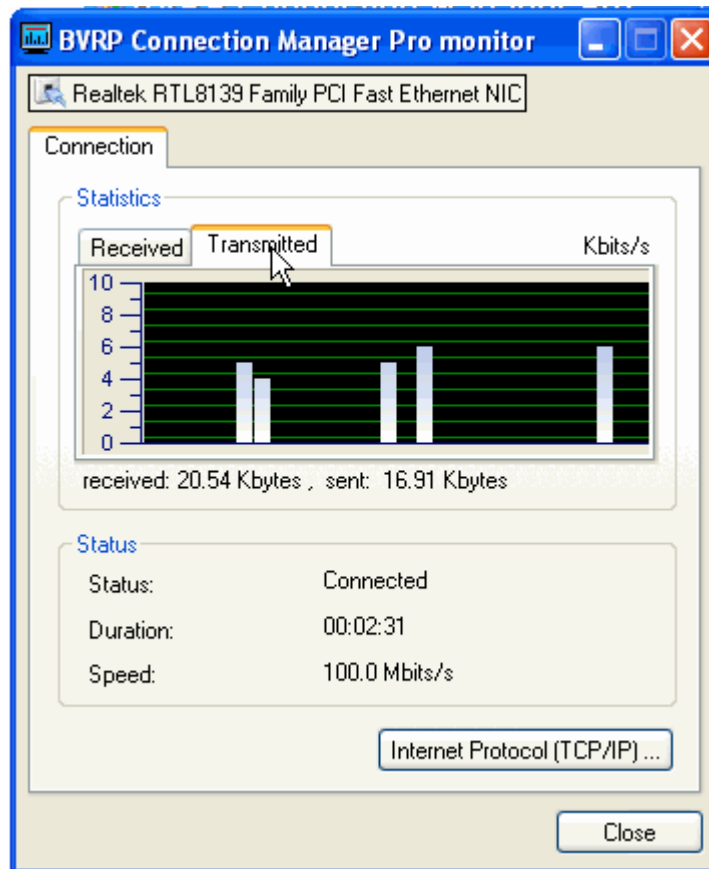
- To Monitor Data Transmission and Receiving click on 



- To check statistics of the received data click on **Received**



- To check the statistics of transmitted data click on **Transmitted**





- To set the settings click on , click on **Main Screen Settings**

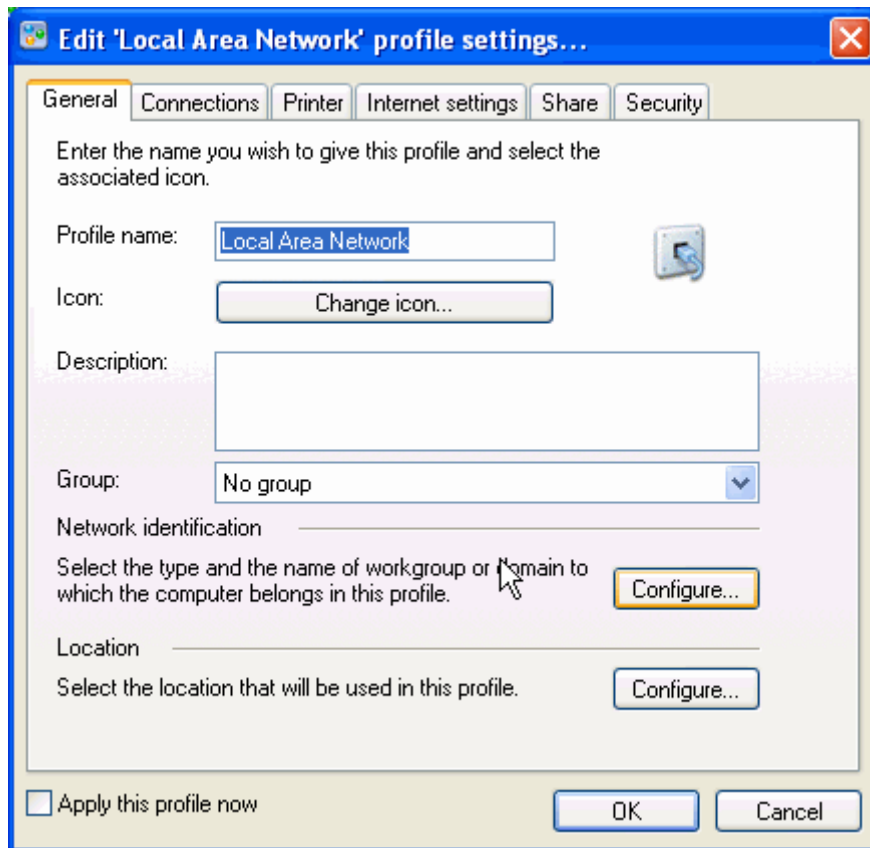




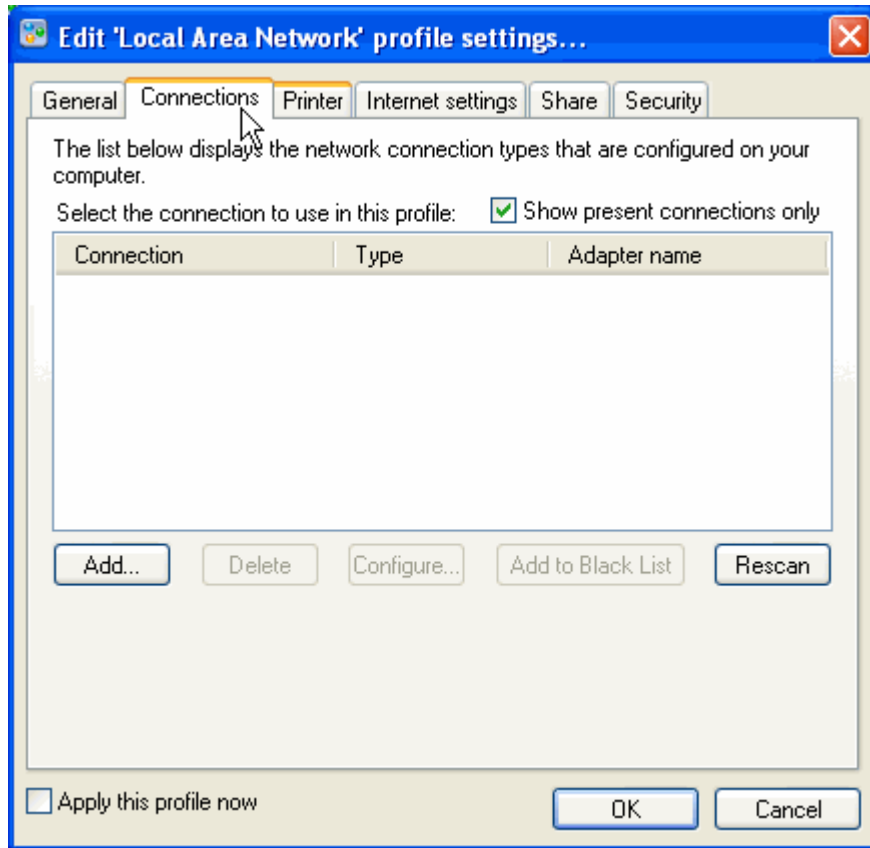
- To set properties for a profile click on , Click on **Current profile properties**



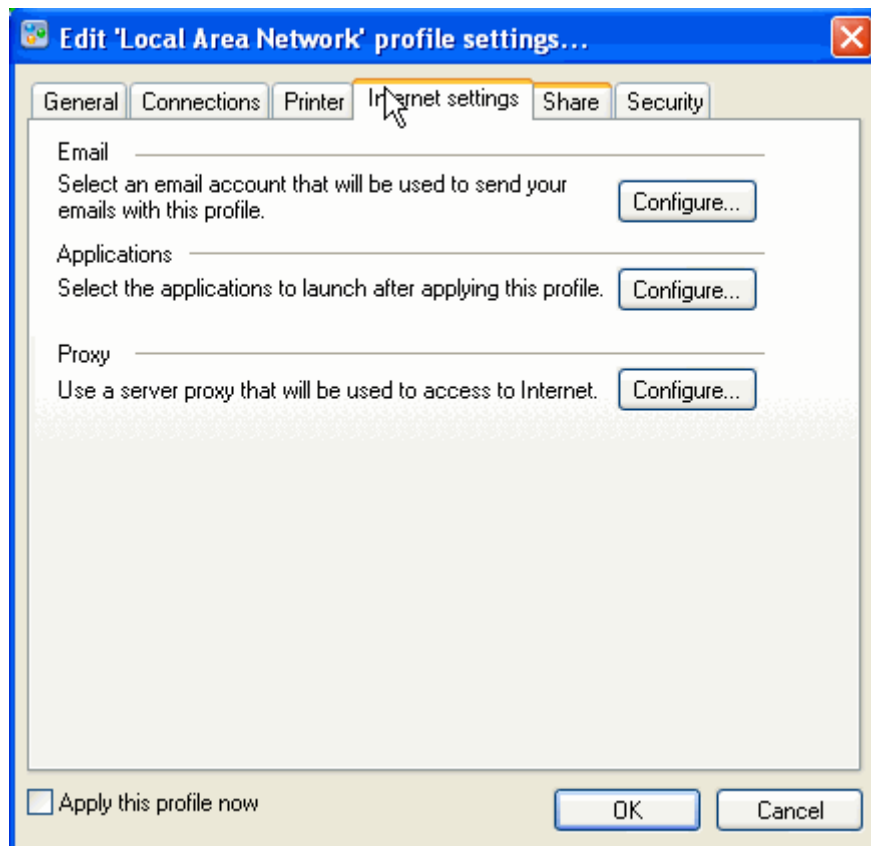
- To set General settings click on **General**→**Configure**



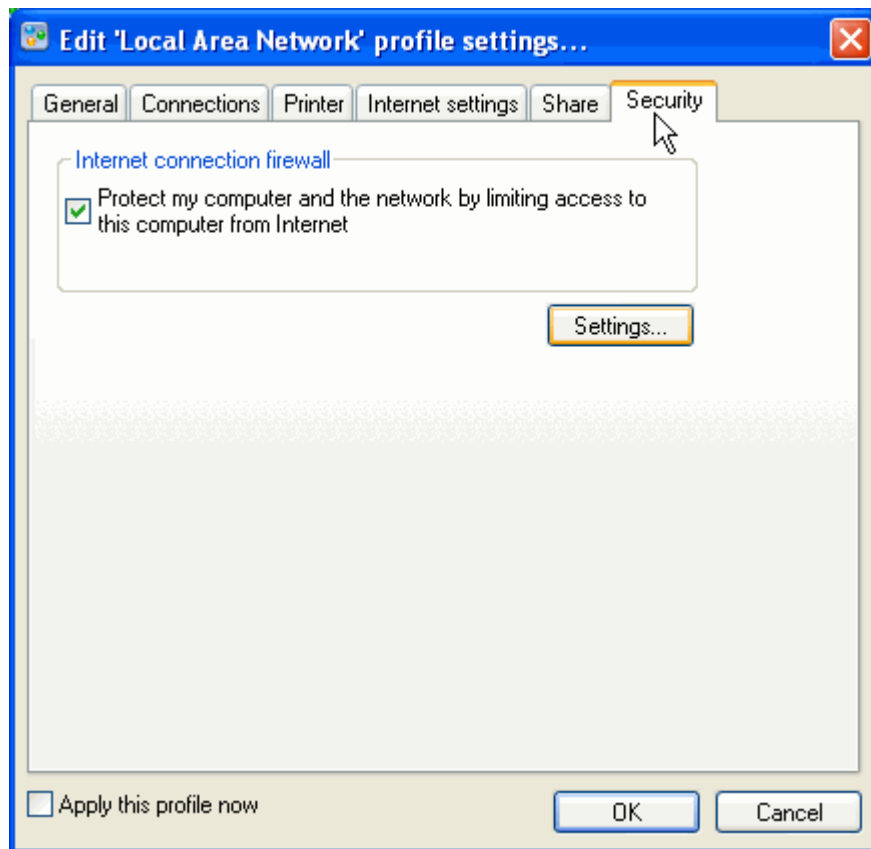
- To View the network connections and adding click **connections**→ **Add**



- To Set the internet settings click on **Internet settings**



- Go to Security tab. Click on **Settings** to set the Security Settings.



- To set the profile preferences click on  → click on **Profile Preferences**

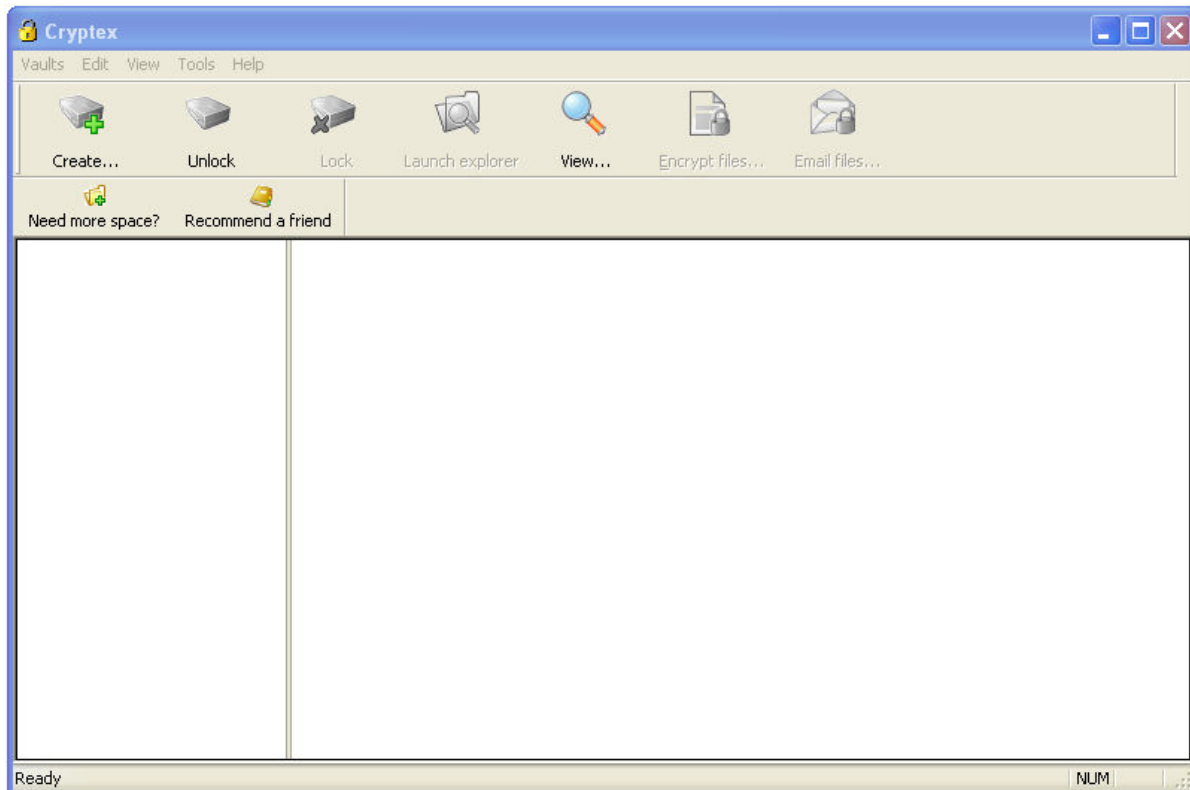


Lab 46- 02

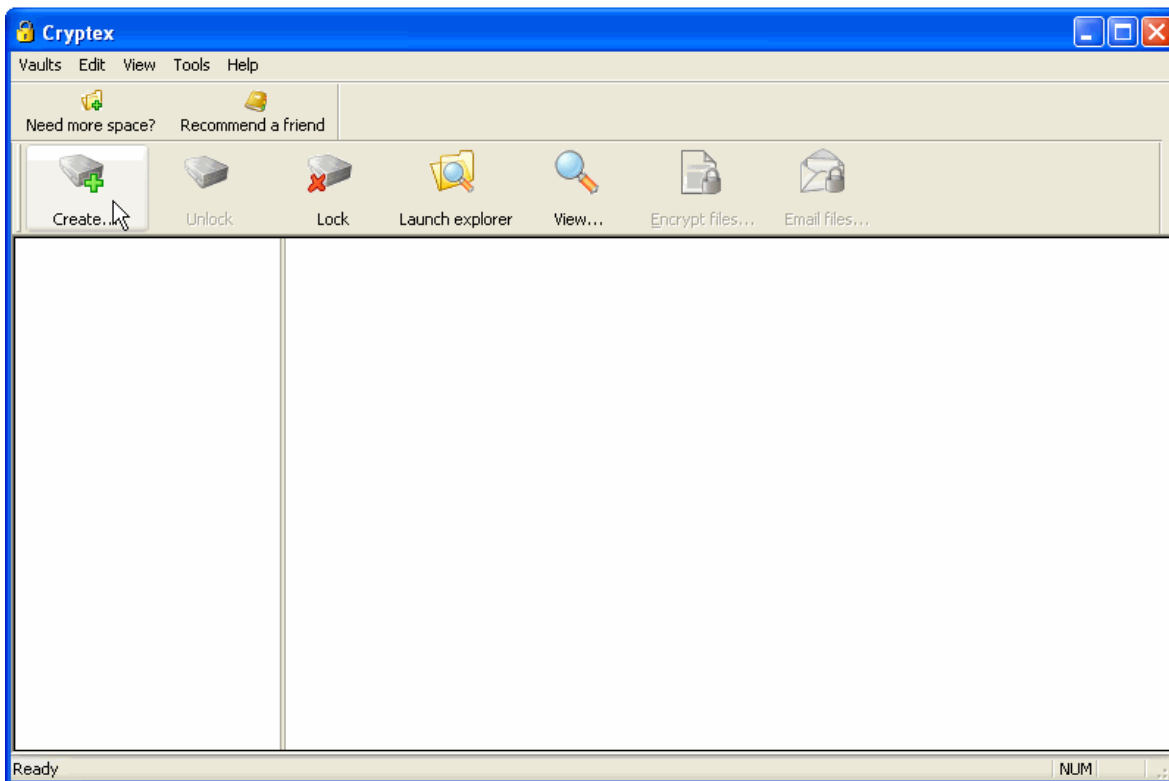
Objective:

Use **Cryptex** tool is to secure information on a PC, by creating a vault

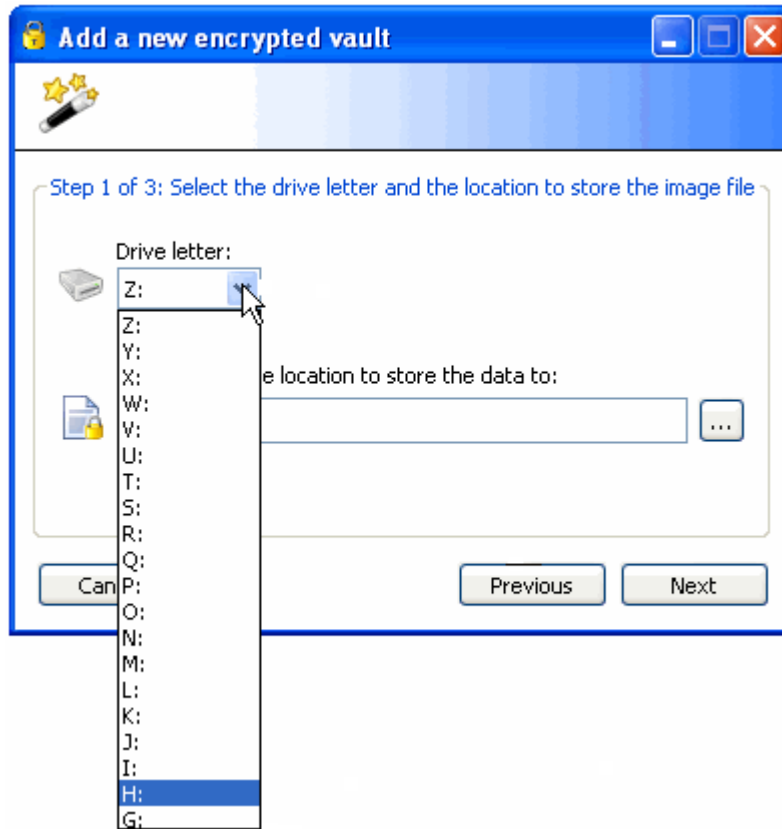
- In the **CEHv6 Labs CD-ROM** navigate to **Module 46**
- Install and launch **Cryptex** program



- Click on **Create**  icon to create a vault



- Select a drive for creating a vault



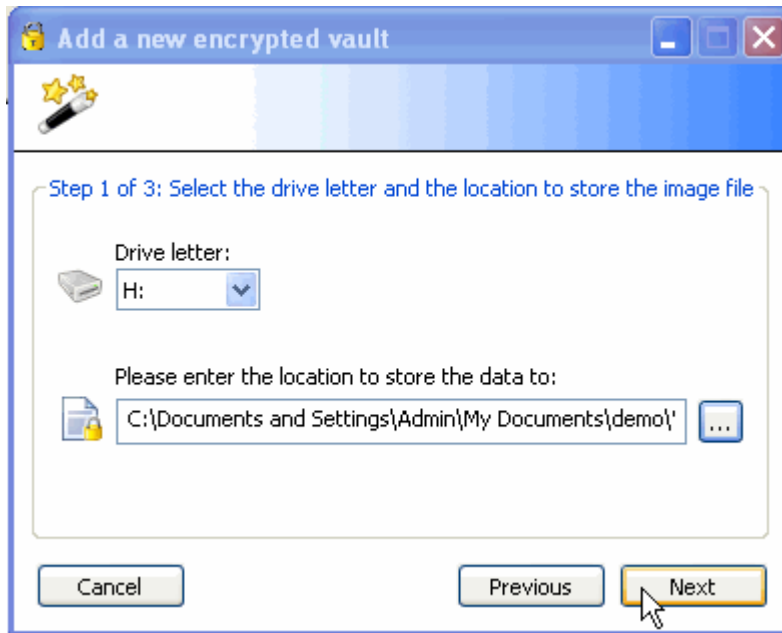
- Browse a file from a particular location



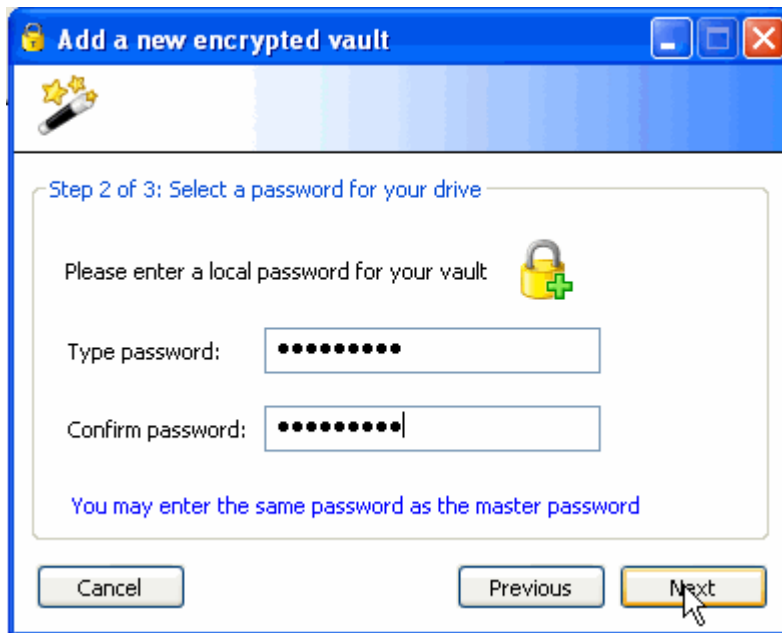
- Click **OK**



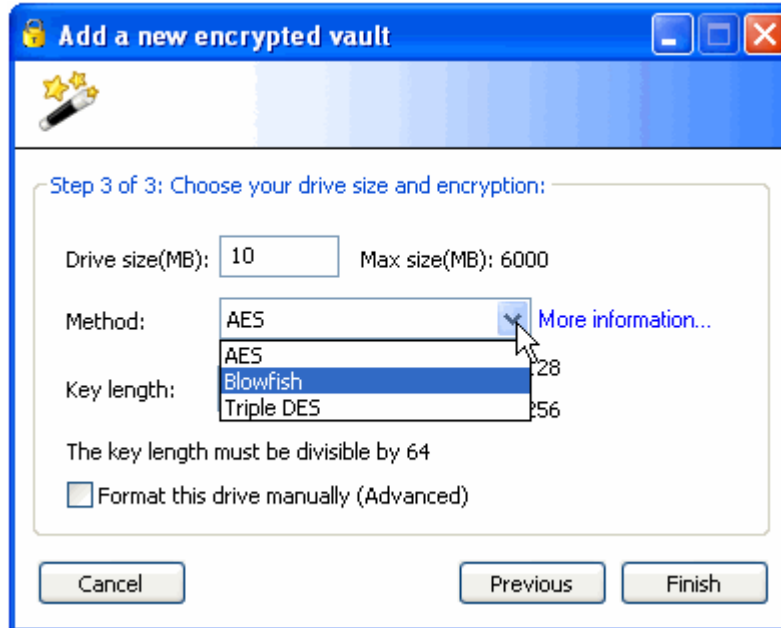
- Click **Next**



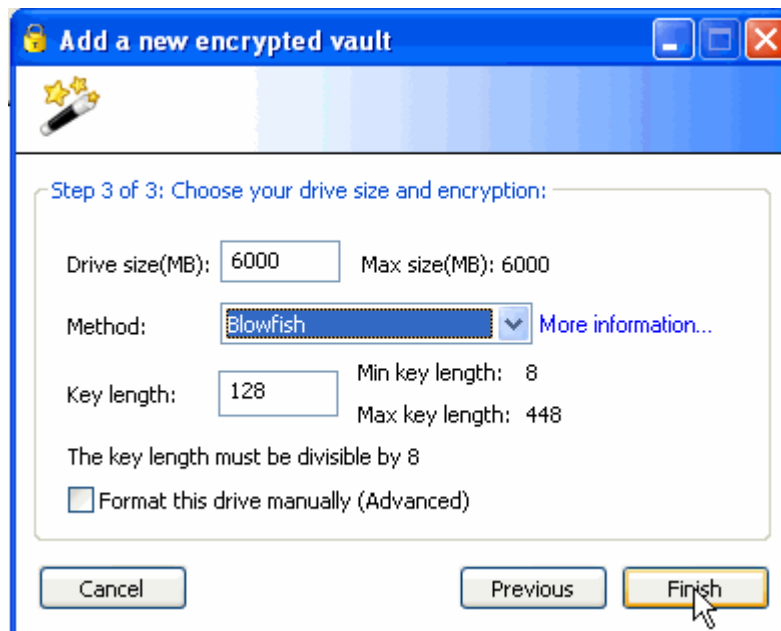
- Enter a password and click **Next**



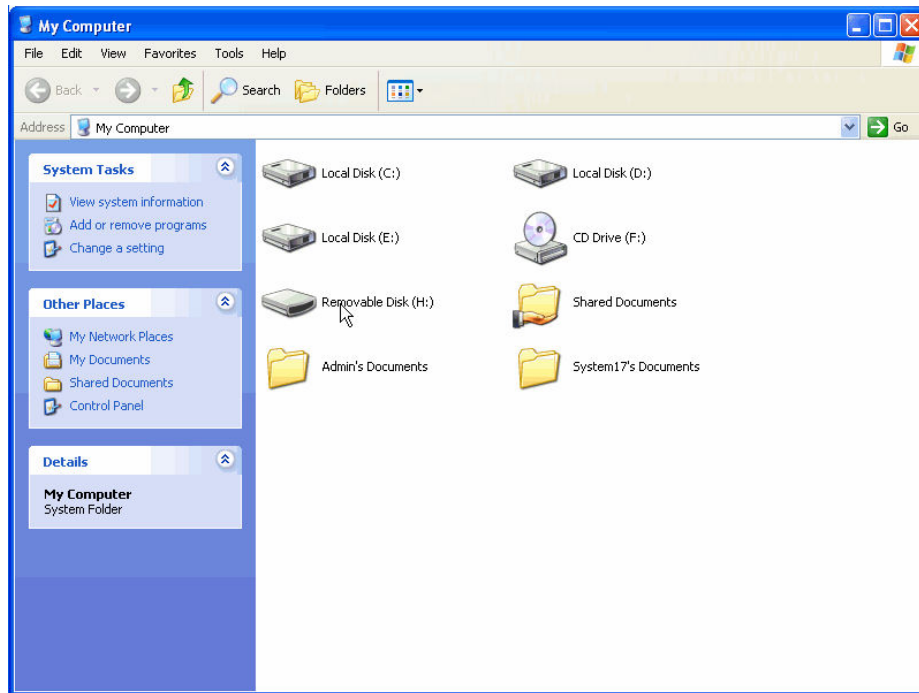
- Select desired encryption algorithm



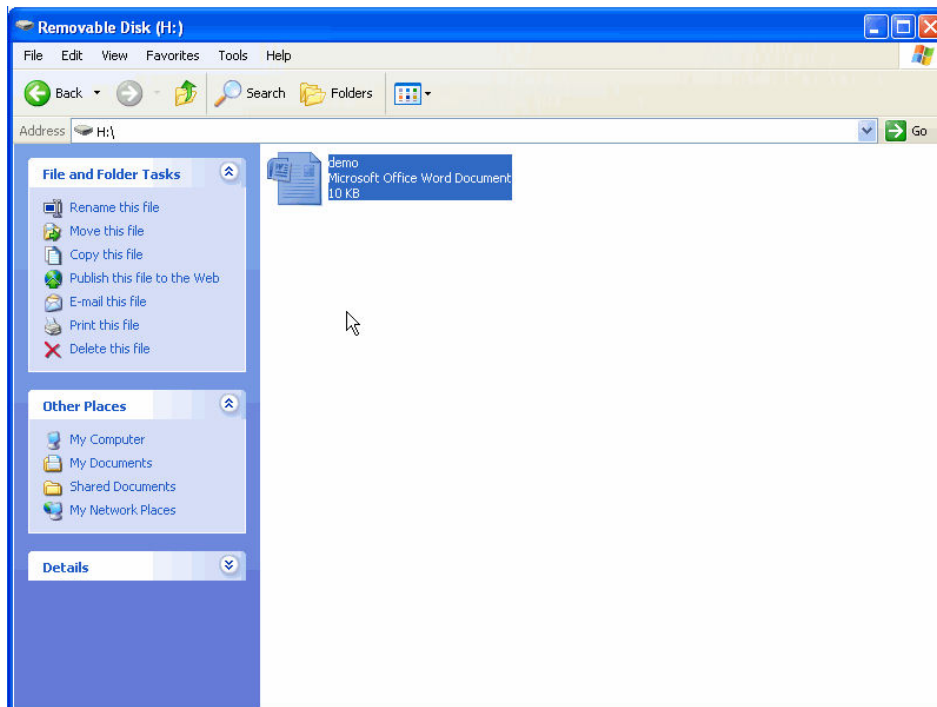
- Click **Finish**



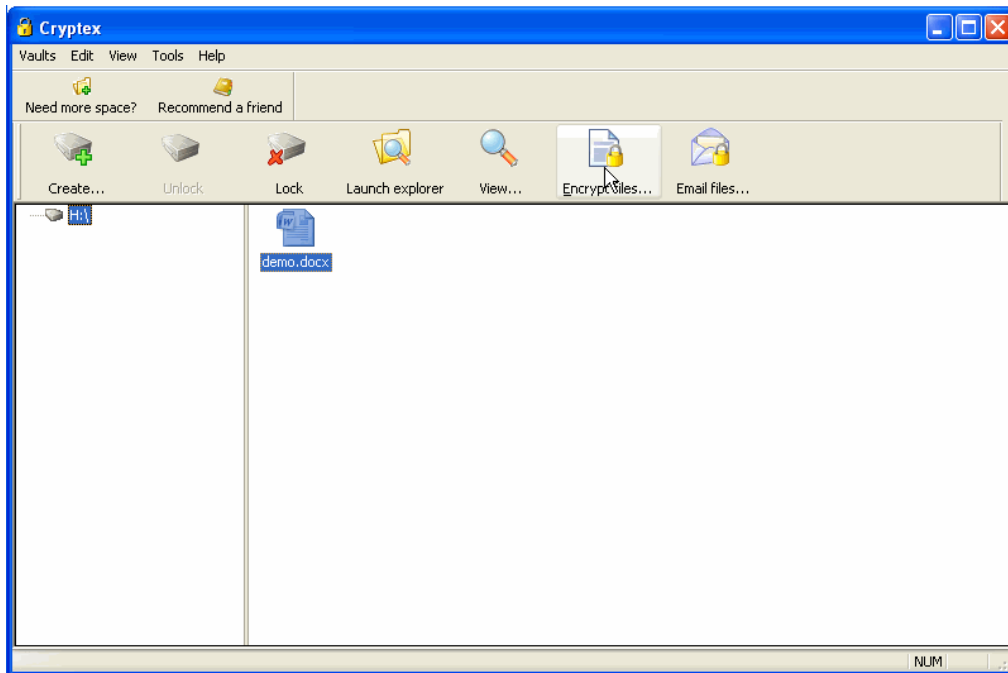
- The Removable drive is created



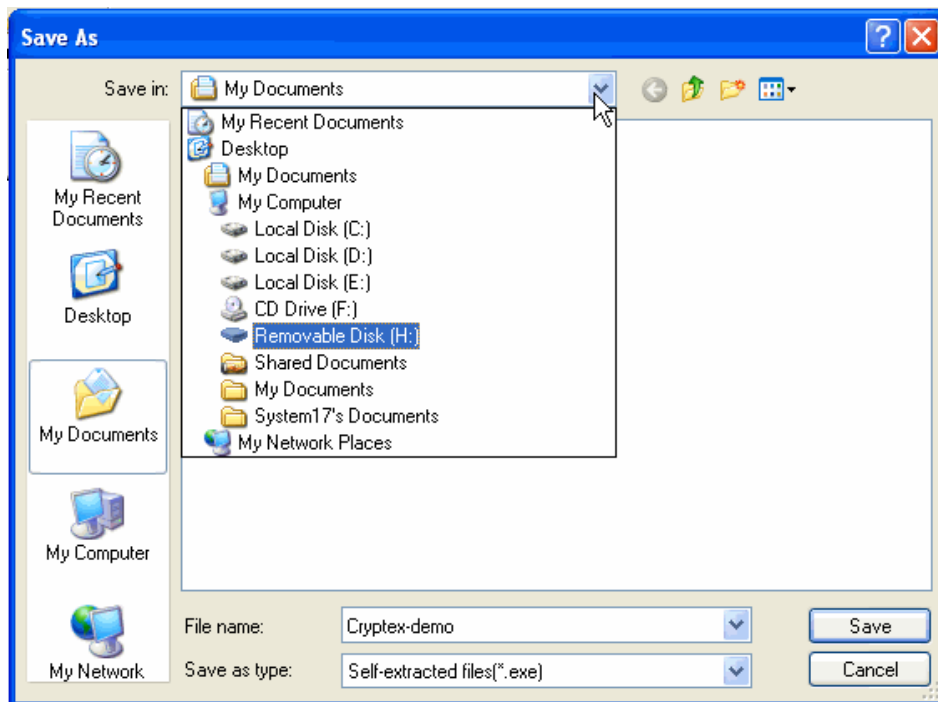
- Select a document to be encrypted



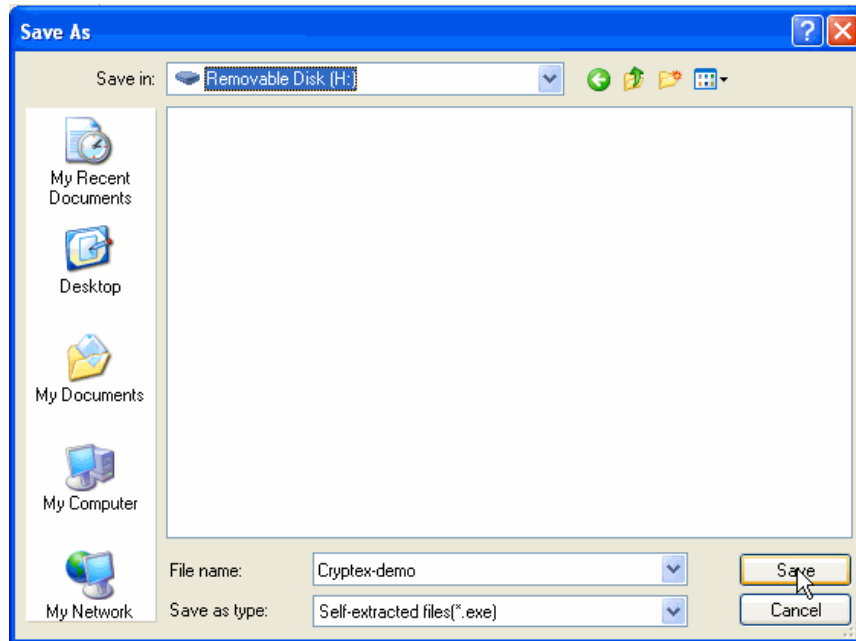
- Select a document and click on **Encrypt files**



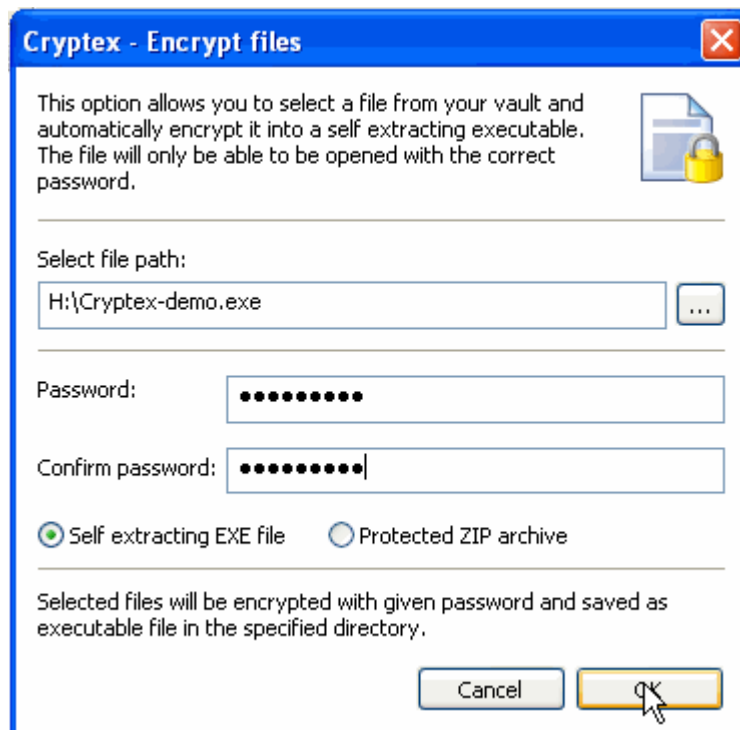
- Select a location to save the encrypted file



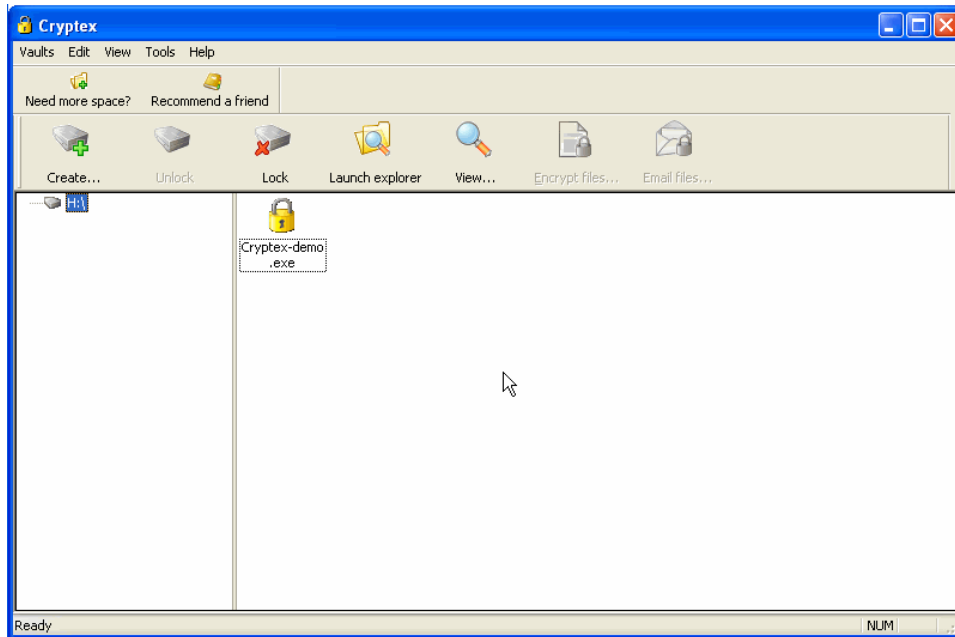
- Click **Save**



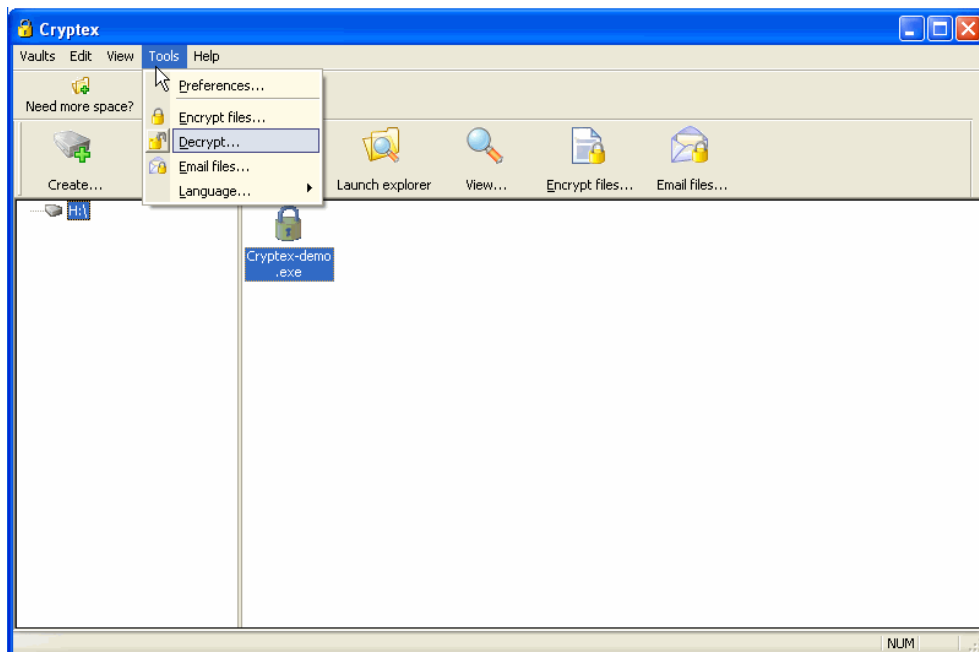
- Enter the Password for Encryption and click **Ok**



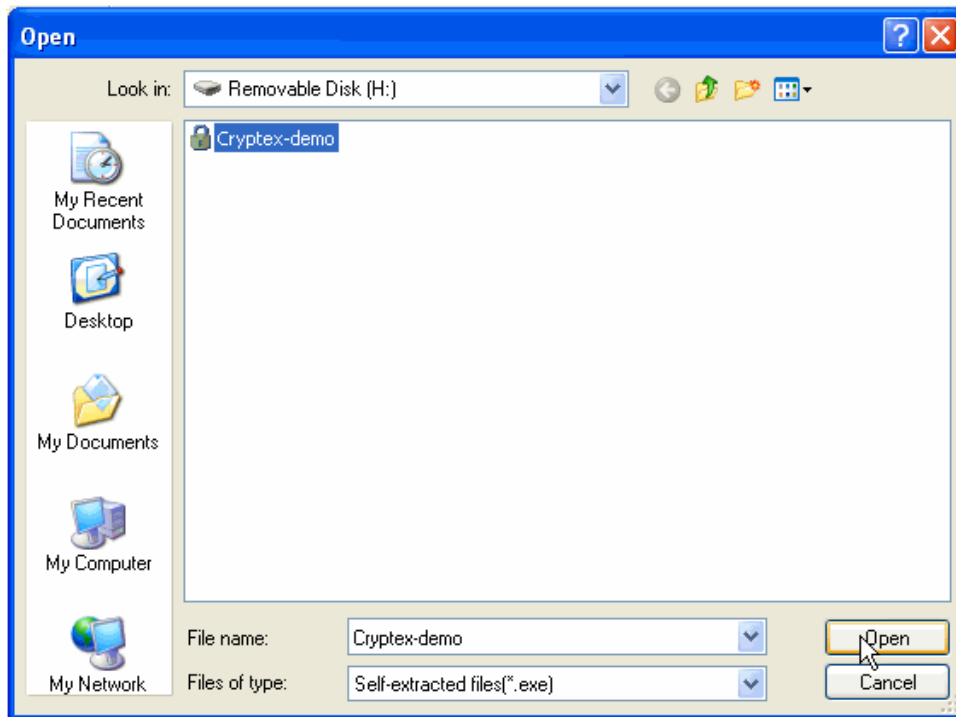
- The file encrypted is as shown



- To decrypt the file Click on **Tools**→ **Decrypt**



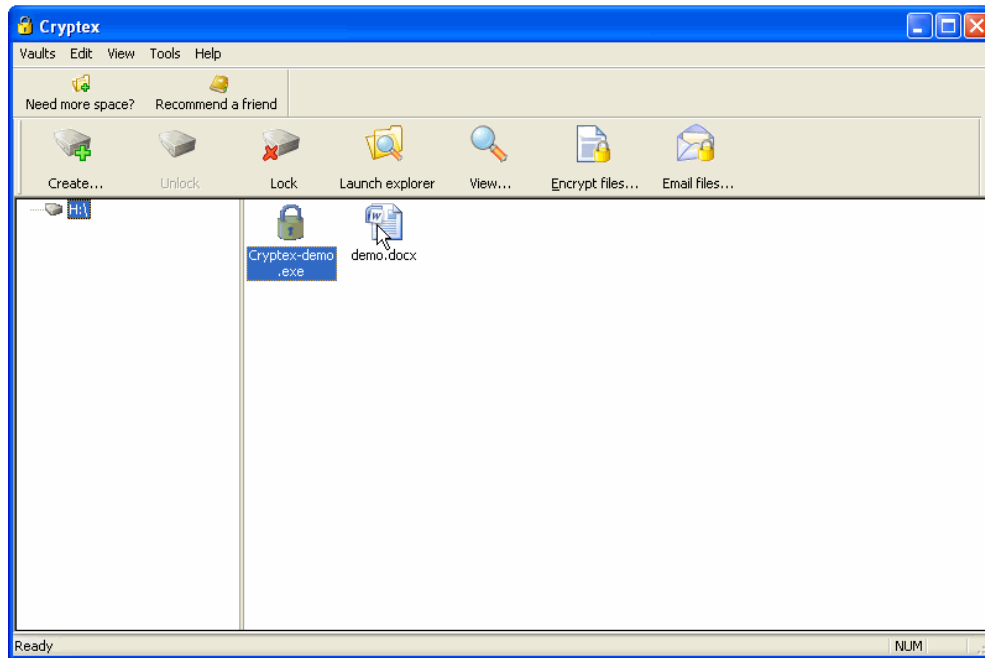
- Browse the file from the location and click **Open**



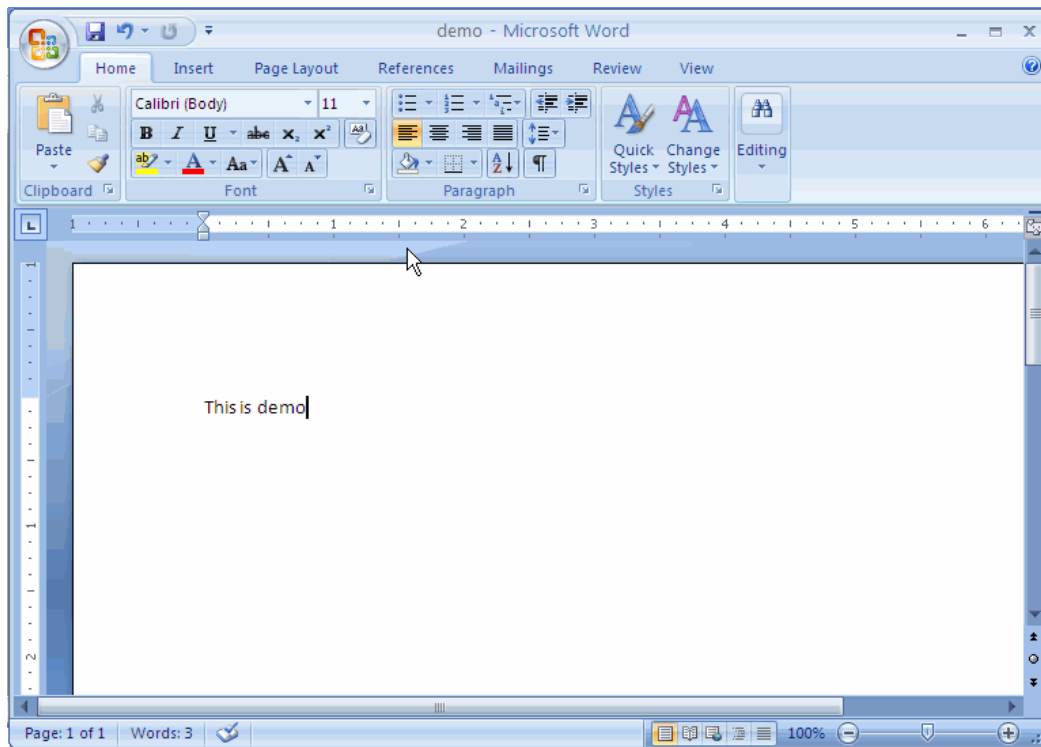
- Enter the password and click **Extract**



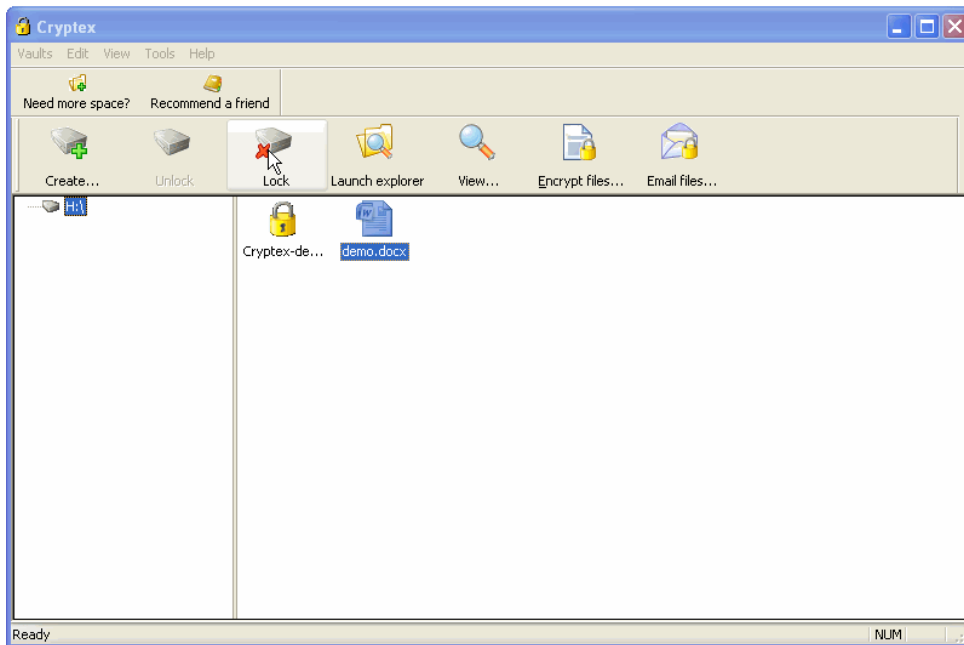
- The file after decryption is as shown



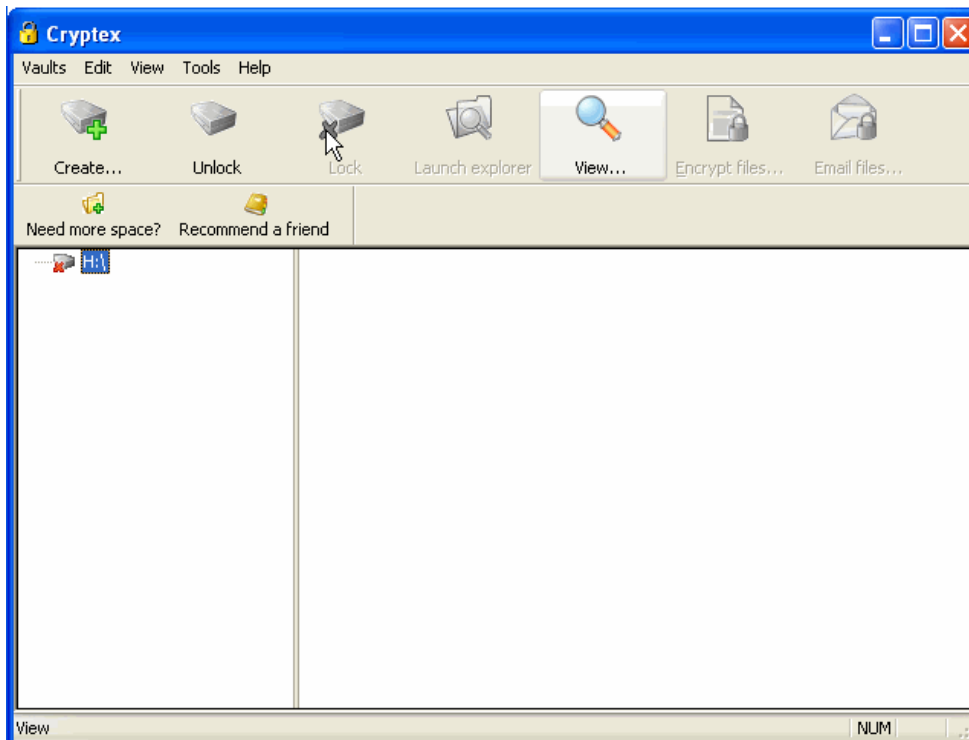
- The Content in the decrypted file



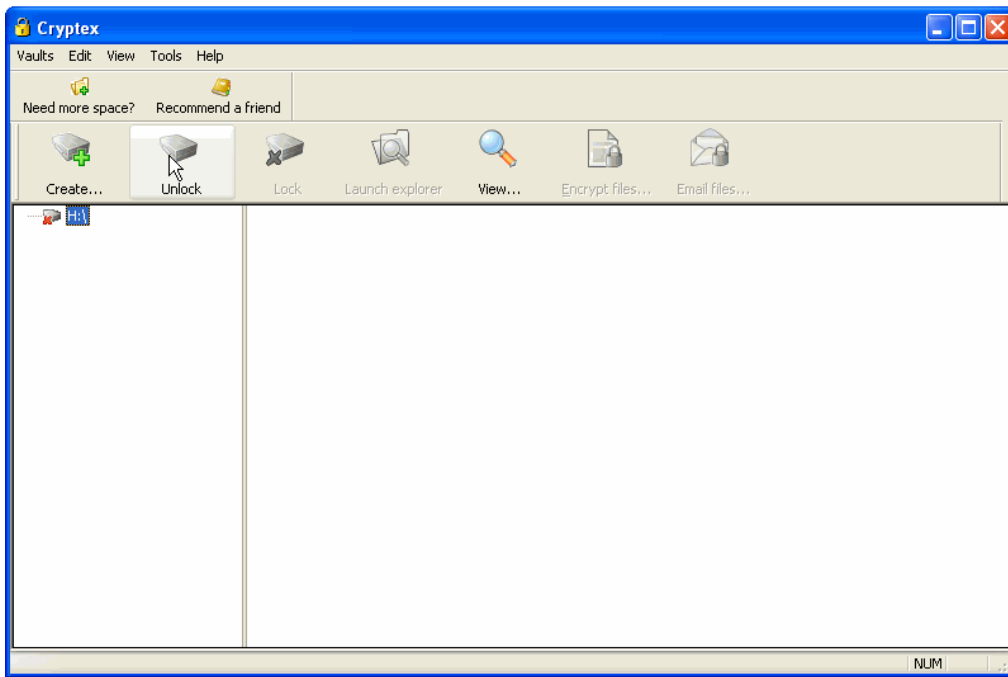
- To lock a particular drive, select a particular drive and click on **Lock** button 



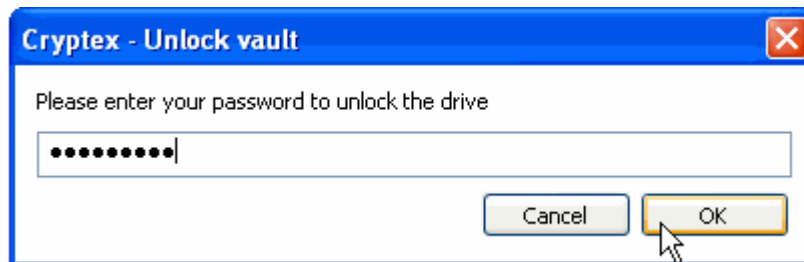
- The drive locked is as shown



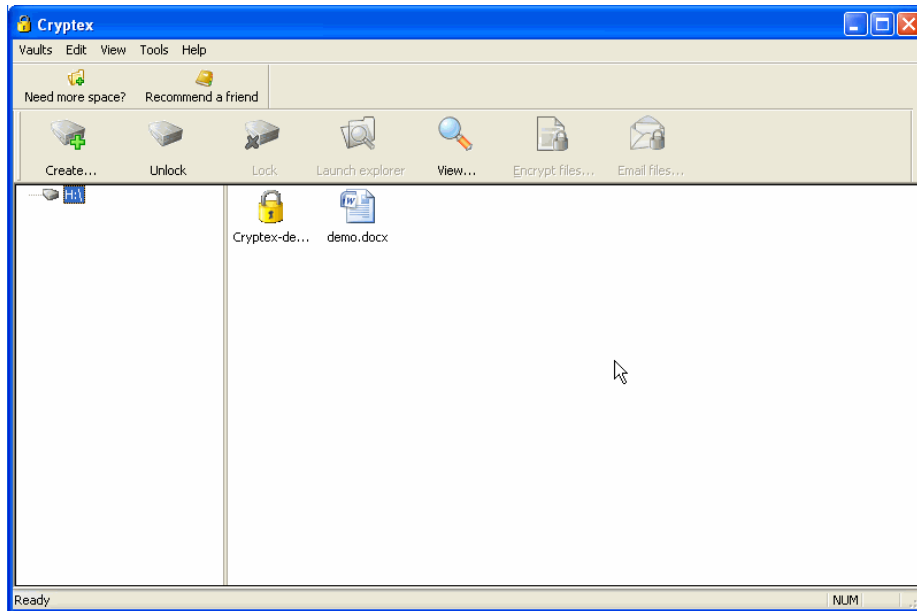
- To unlock a drive click on **Unlock** button



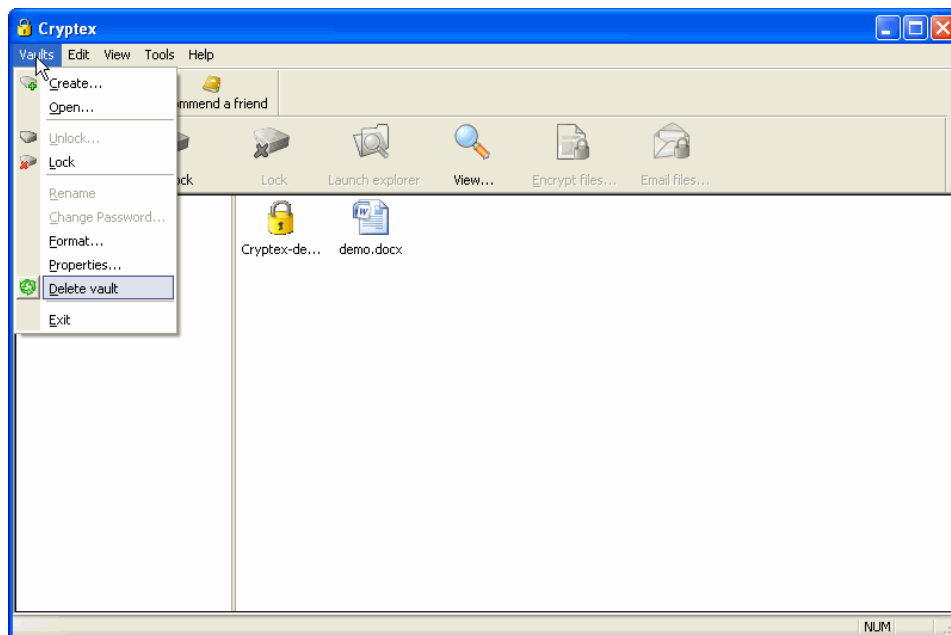
- Enter Password and click **Ok**



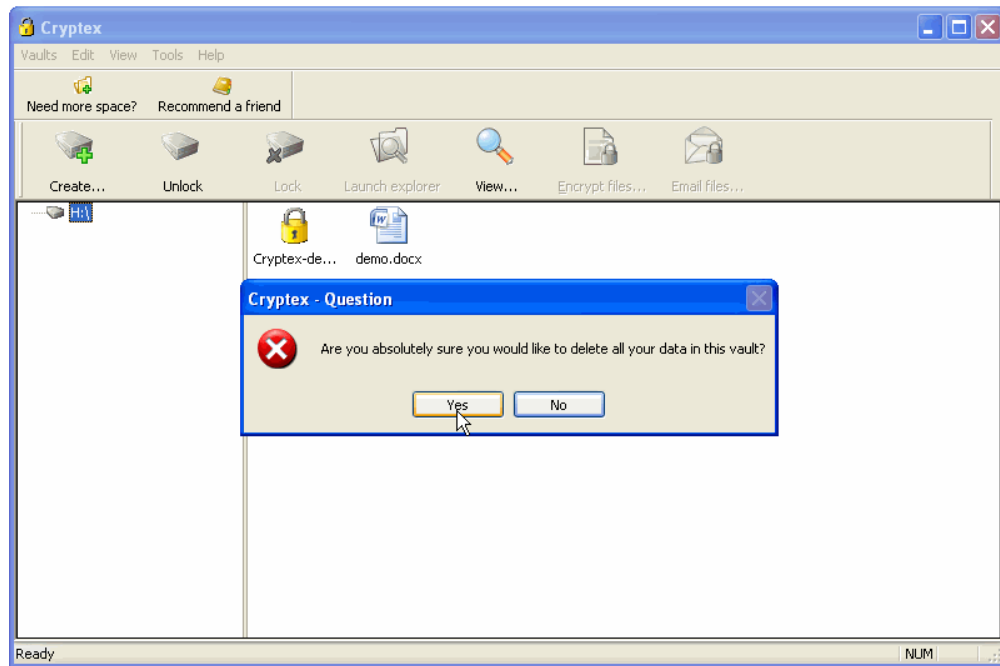
- The drive unlocked is as shown



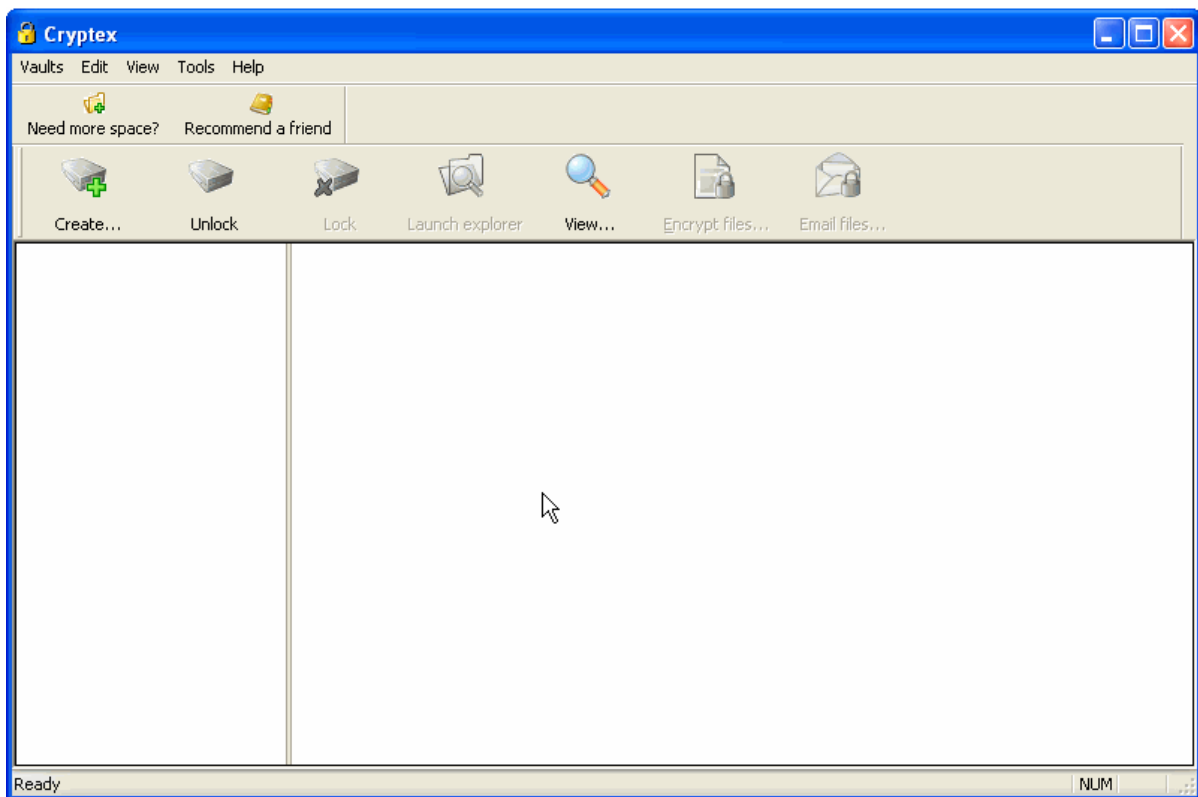
- To delete a Vault click on **Vaults→Delete Vault**



- Click **Yes** to delete the vault



- After deleting the Vaults

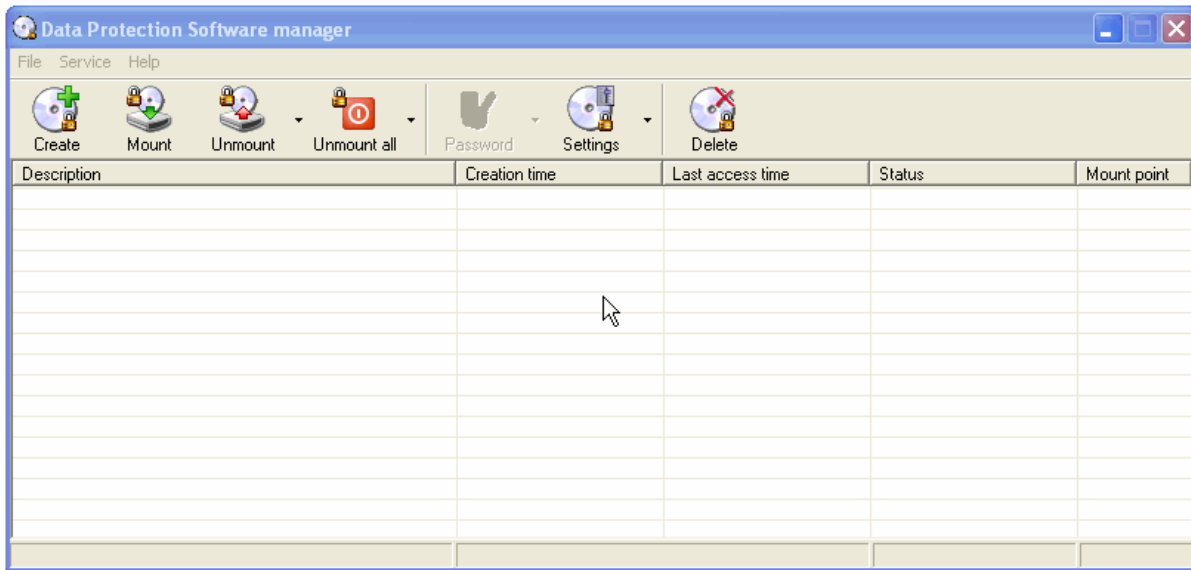



Lab 46-03

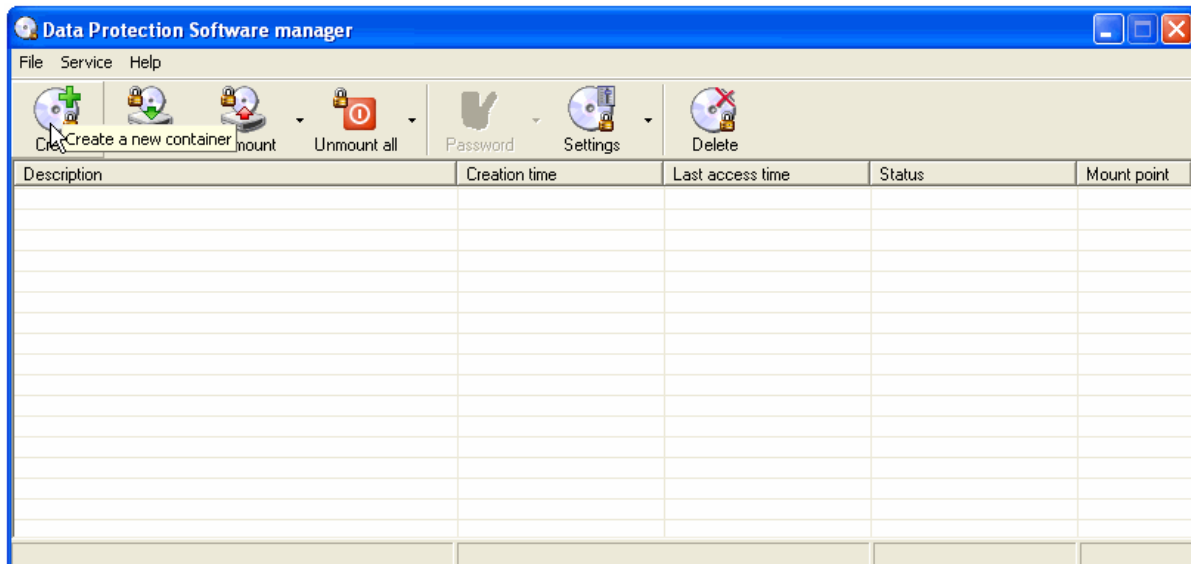
Objective:

Use **Data Protection Software** is to provide security and confidentiality for data on a removable medium.

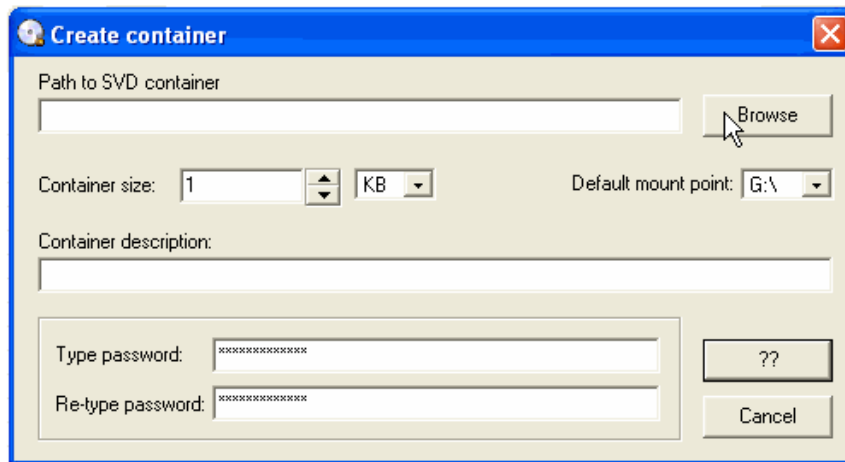
- In the **CEHv6 Labs CD-ROM** navigate to **Module 46**
- Install and launch **Data Protection Software** program



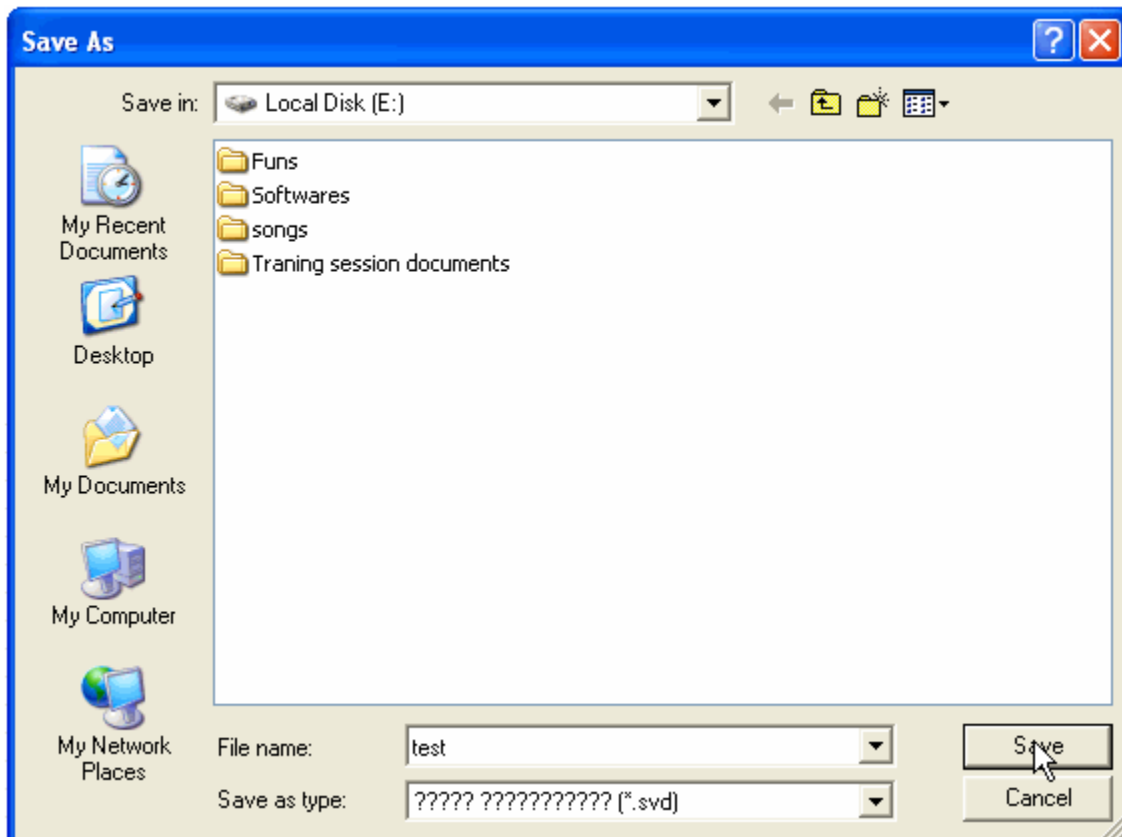
- Click on **Create**  to create a new container




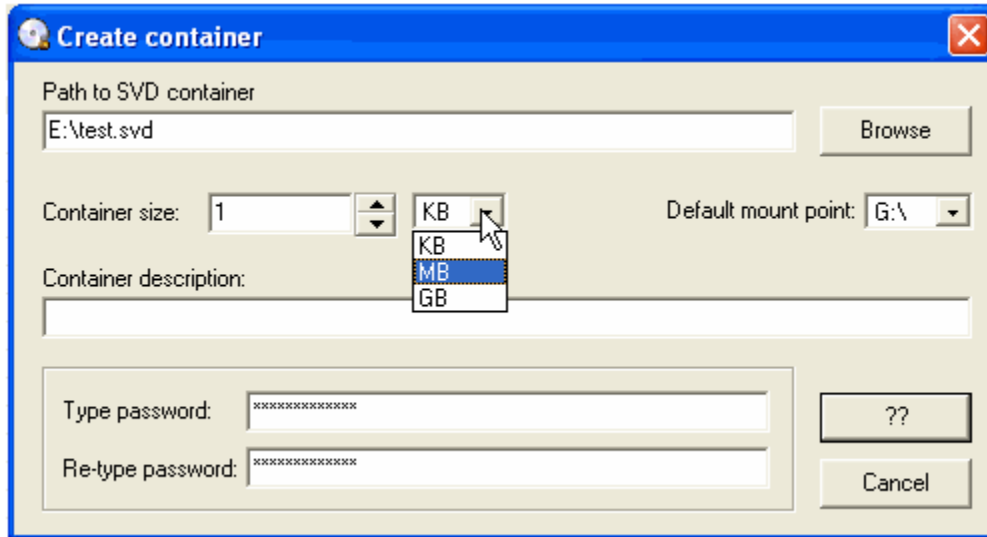
- Select a desired location to save the container, click **Browse**




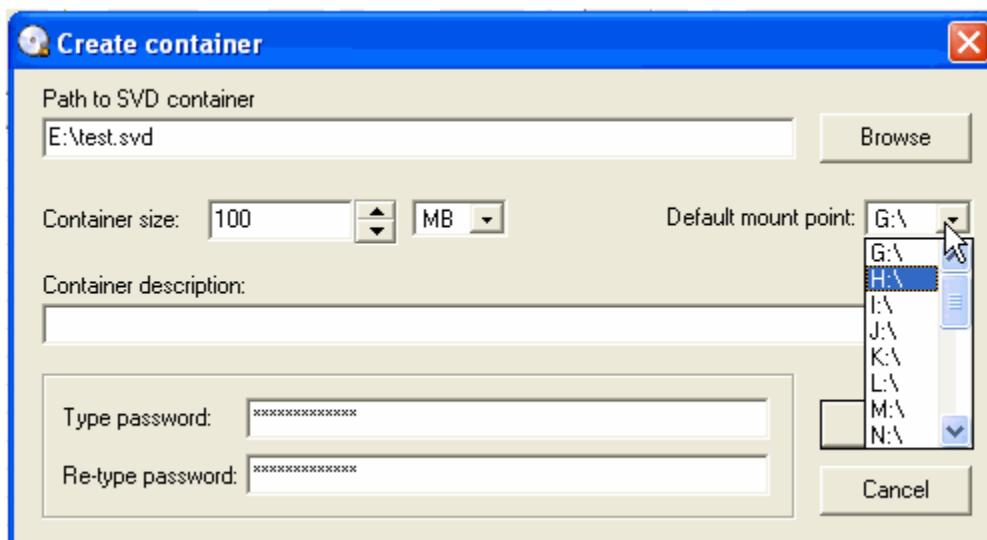
- Enter the file name and click **Save**



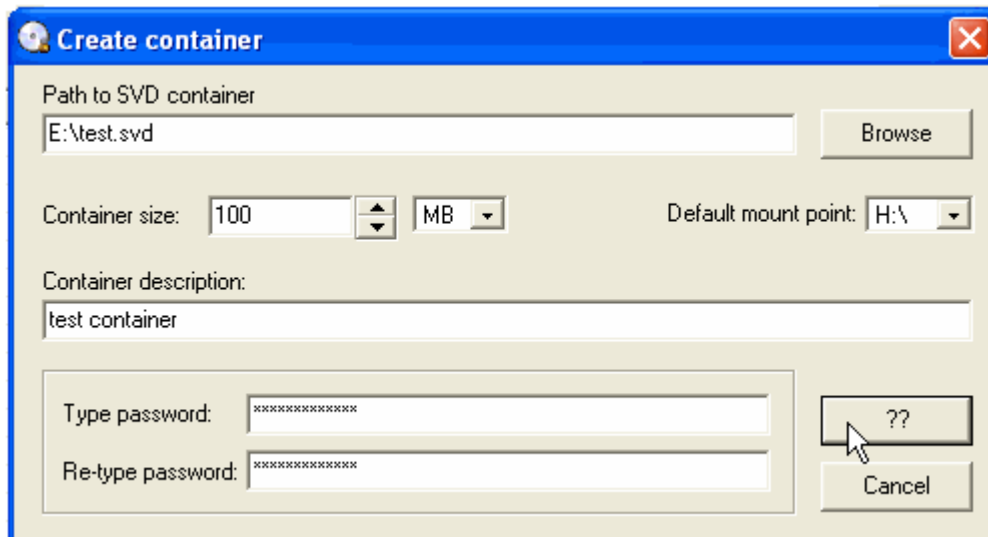
- Click on , select the desired size of the container



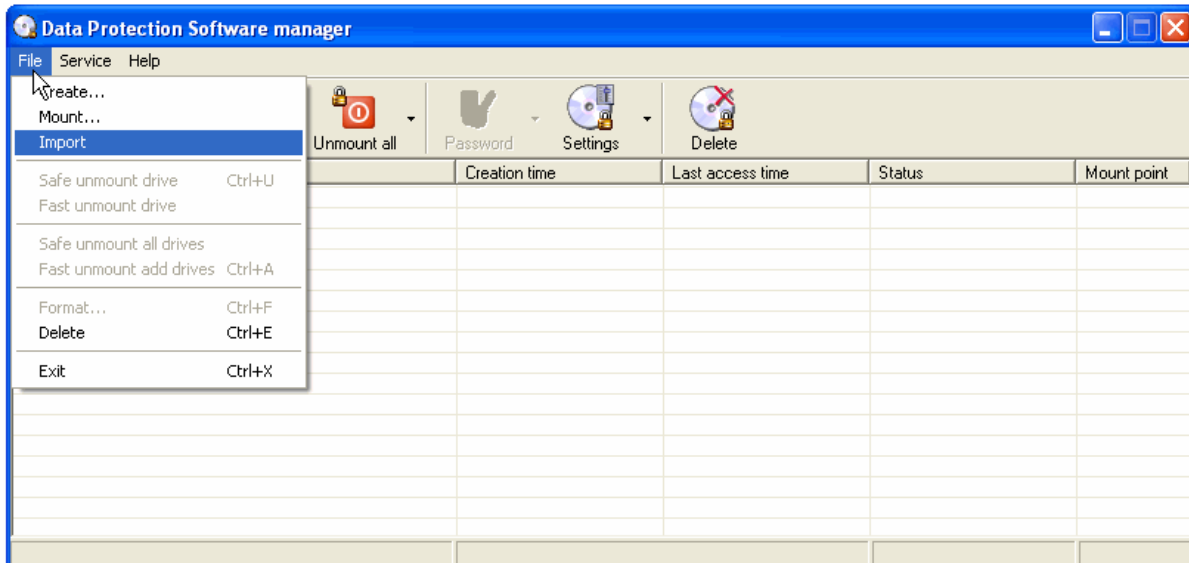
- Click on , select the desired drive to set the Default mount point



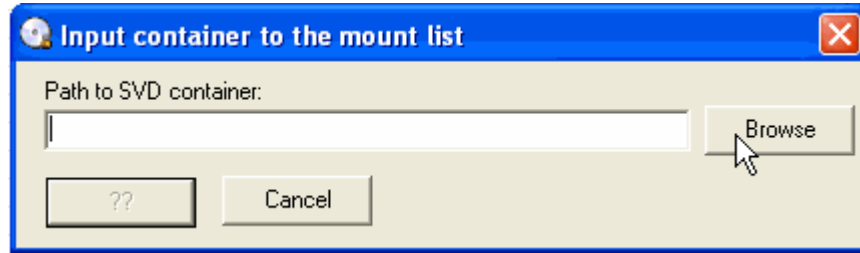
- Click on  button to create a container



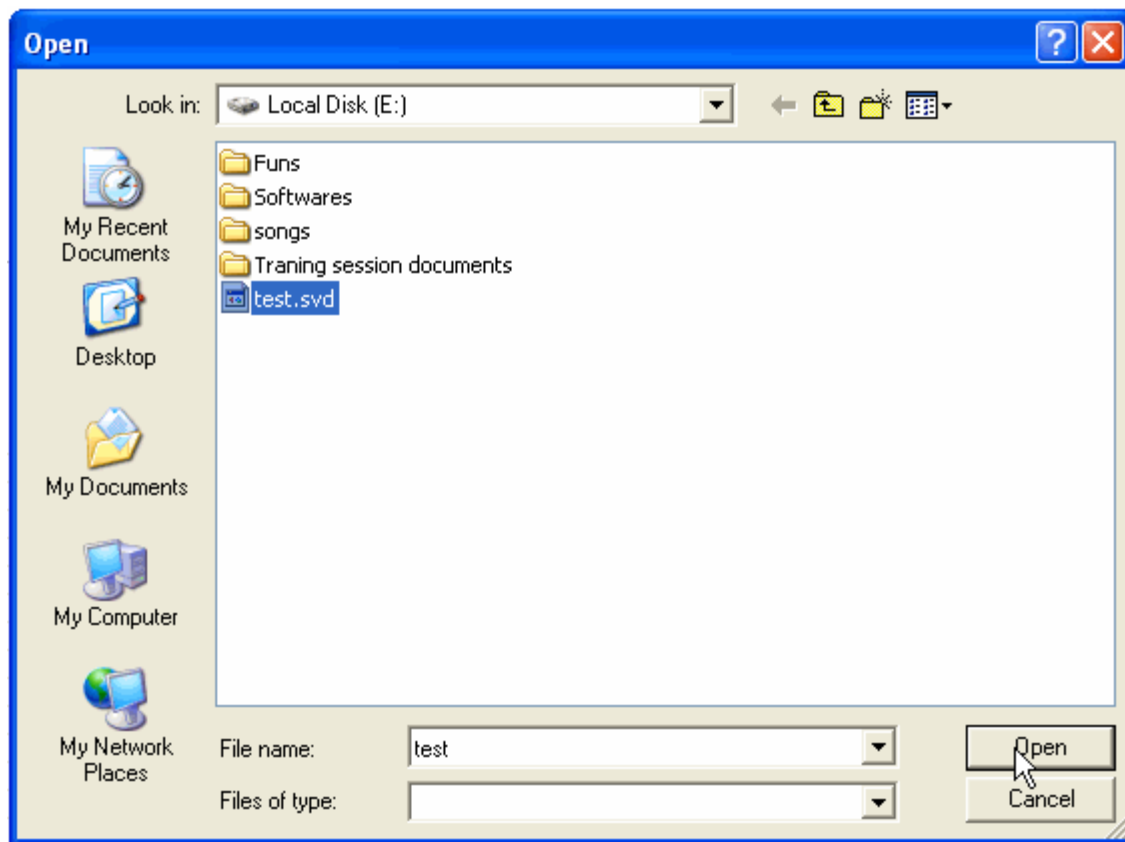
- To import a created container click on **File→Import**



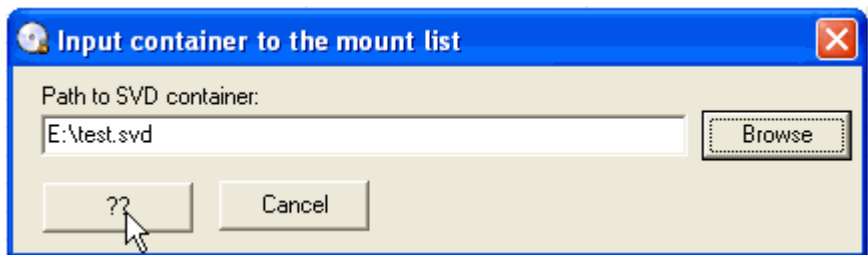
- Click **Browse**



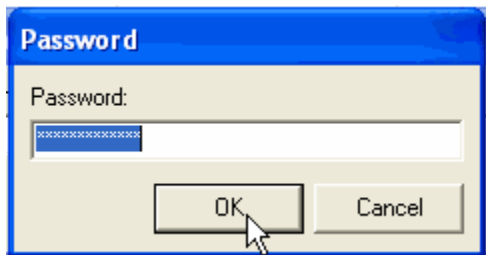
- Browse the file and click **Open**



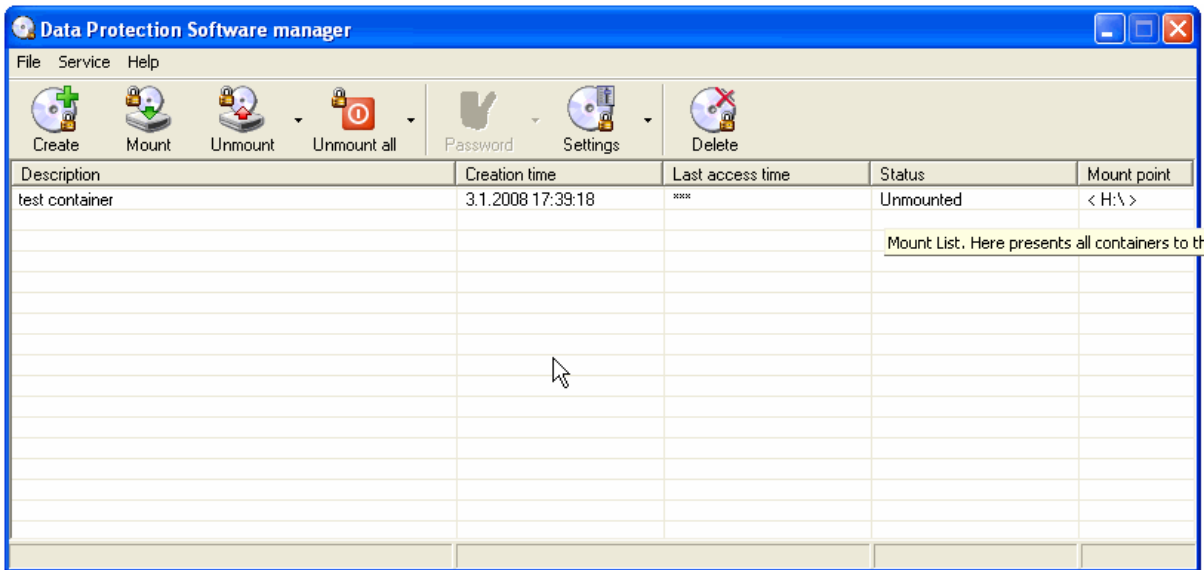
- Click on



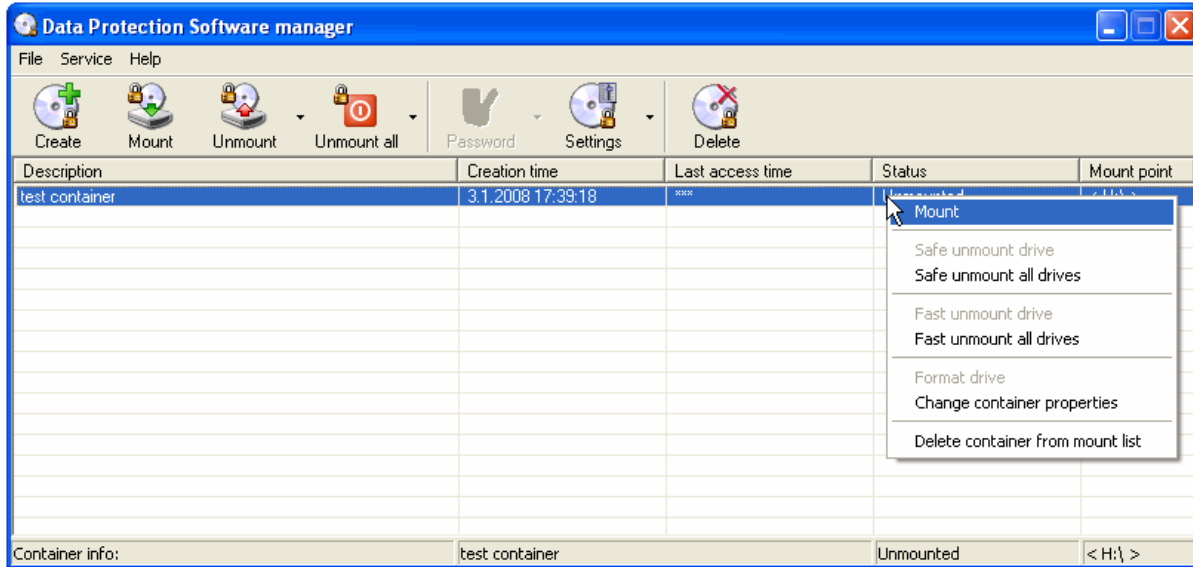
- Enter Password Click **Ok**



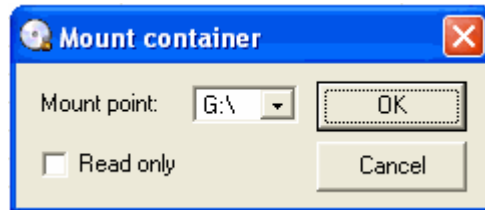
- File imported



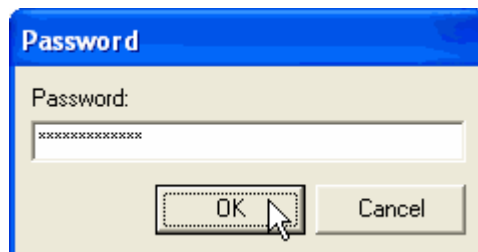
- To mount the imported container, Right click and select **Mount**



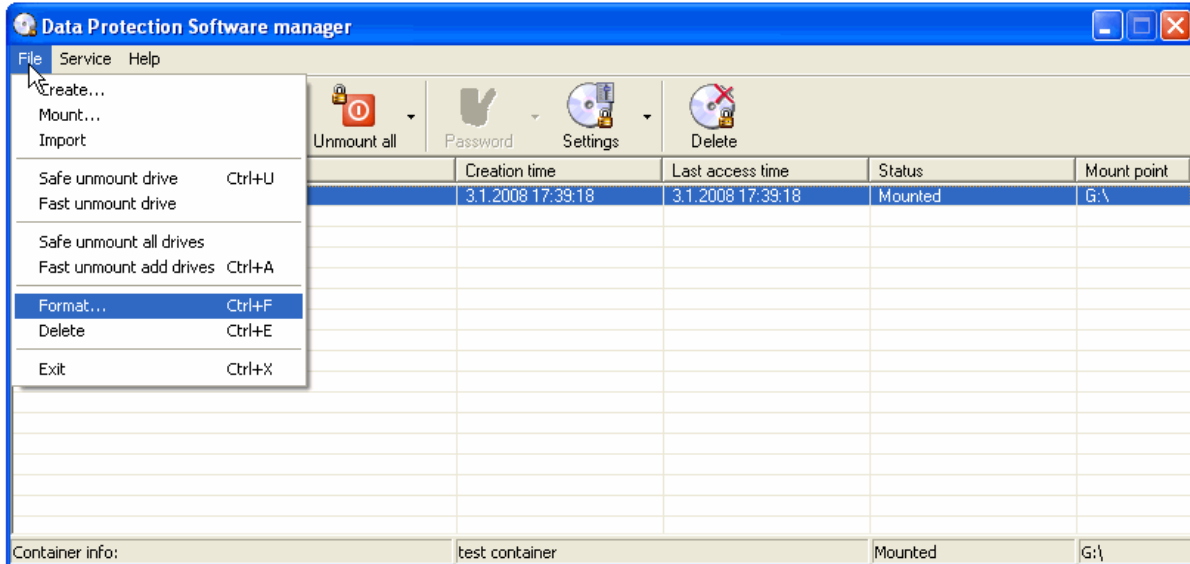
- Select the Mount point click **Ok**




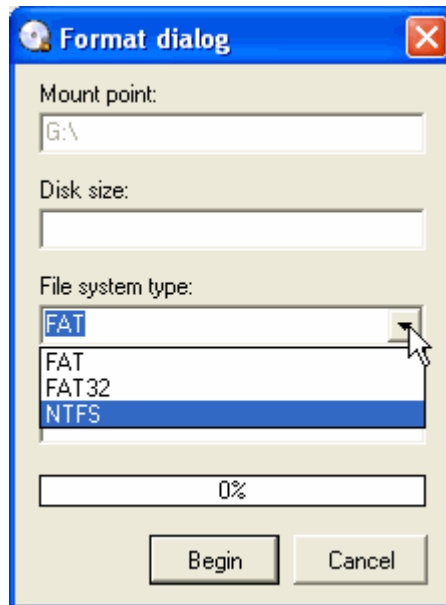
- Enter password click **Ok**



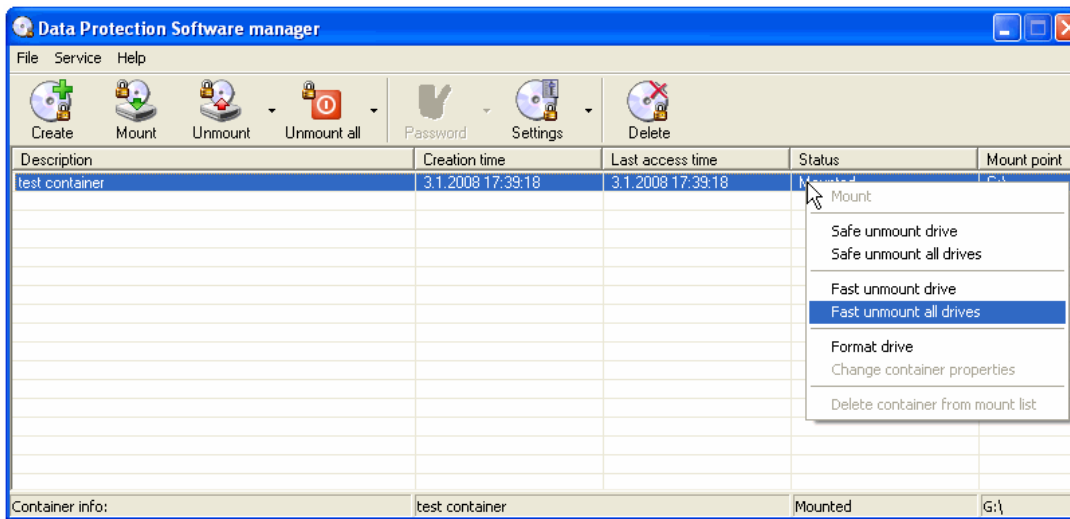
- To format the mounted container, click on **File→Format**




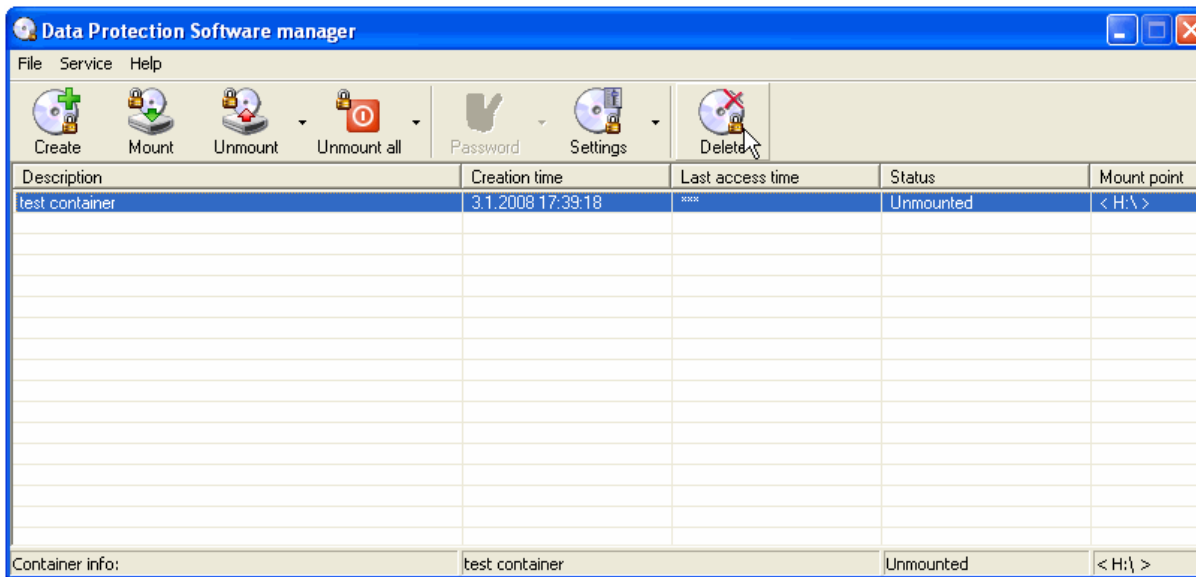
- Click on , select the desired file system to format the drive, Click **Begin**



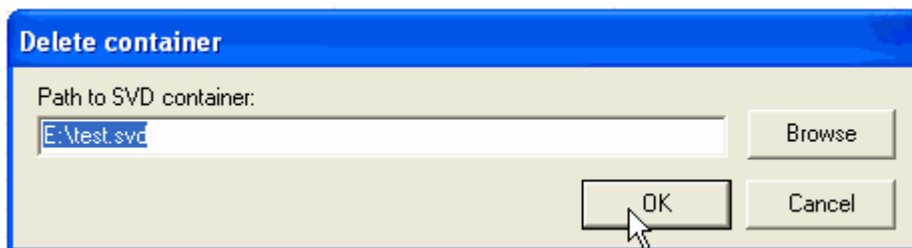
- To unmount the drives, select the items in the list, right click and select **Fast unmount all drives**



- To delete a container click **Delete** 



- Browse the file and Click **Ok**

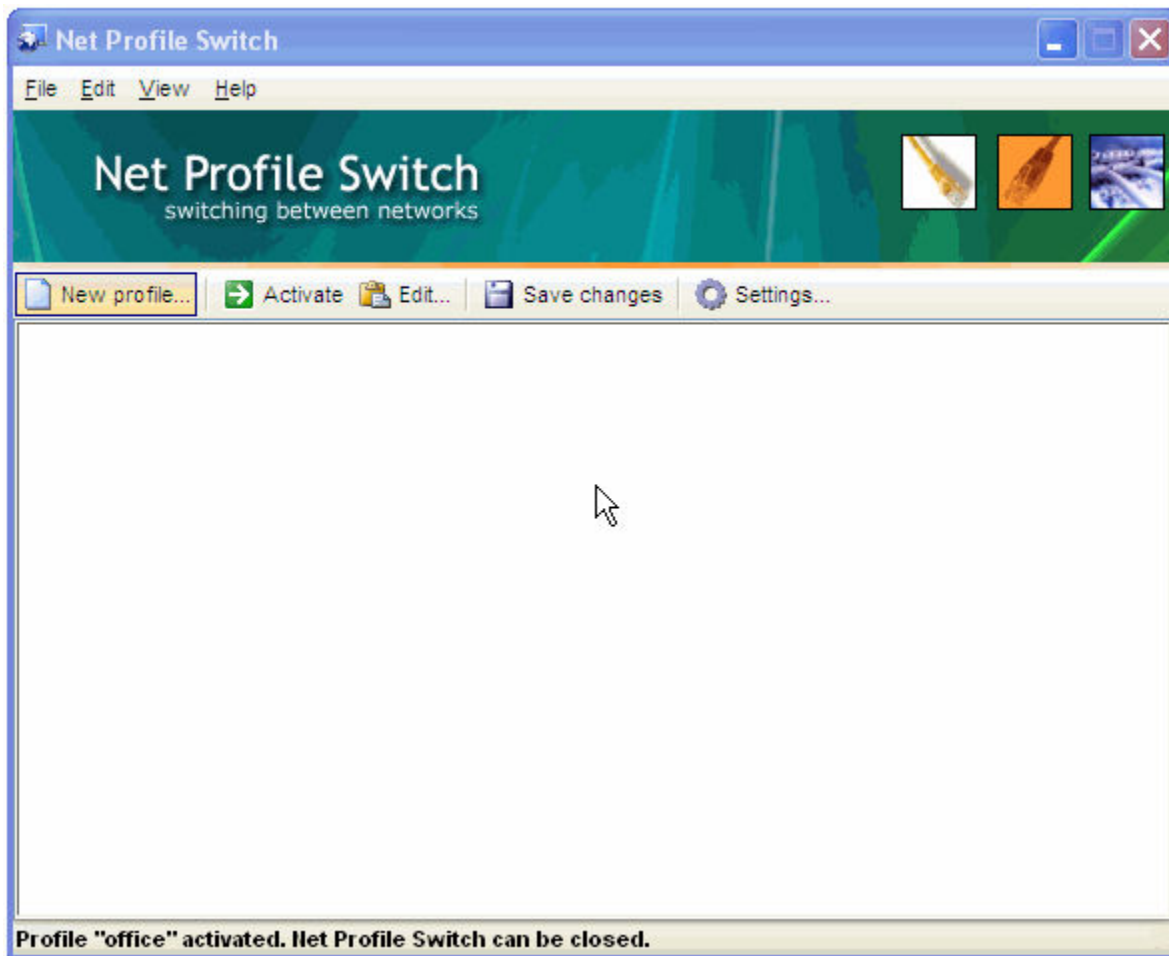


Lab 46 -04

Objective:

Use **Net Profile switch** Tool to store and switch between two or more network configuration sets.

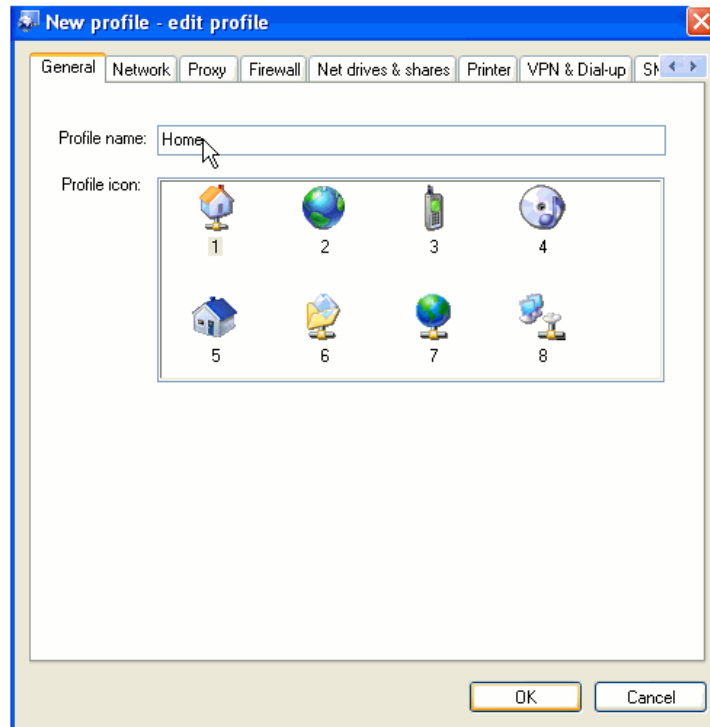
- In the **CEHv6 Labs CD-ROM** navigate to **Module 46**
- Install and launch **Net Profile Switch** program



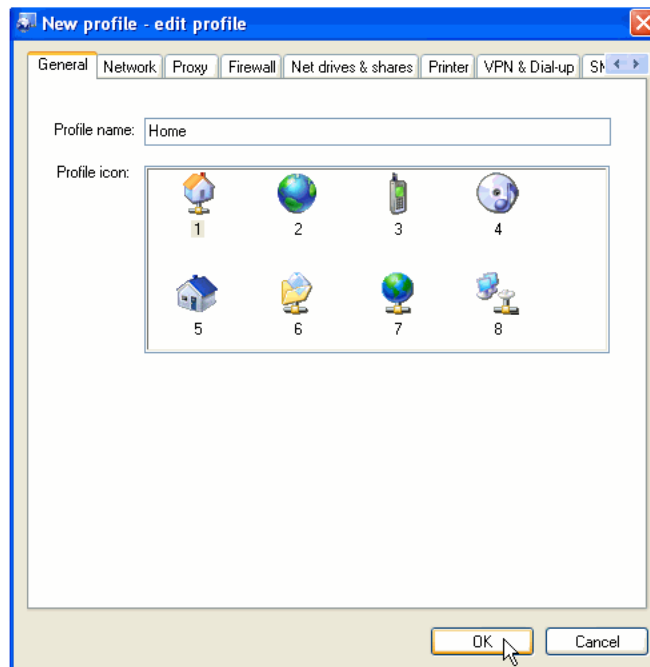
- To create a new profile click on **New Profile**



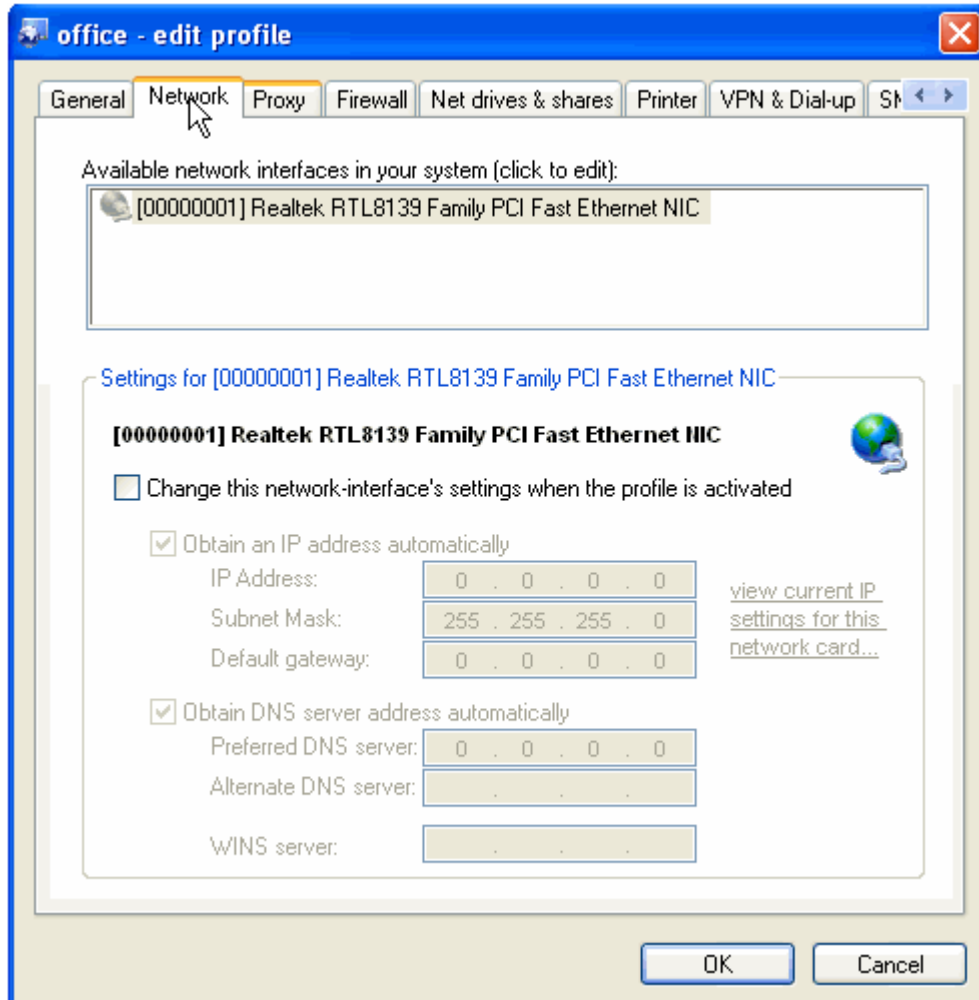
- To set an icon for a profile, Enter the profile name select a profile icon



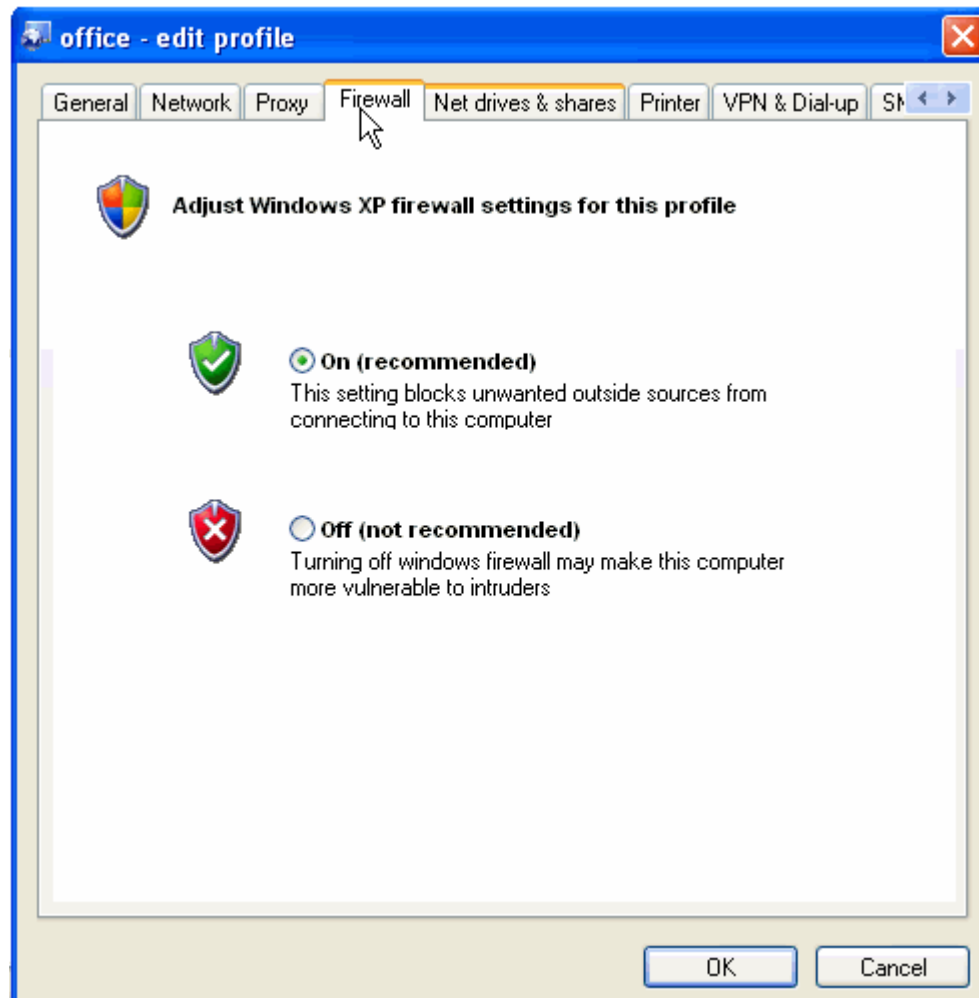
- click **OK**



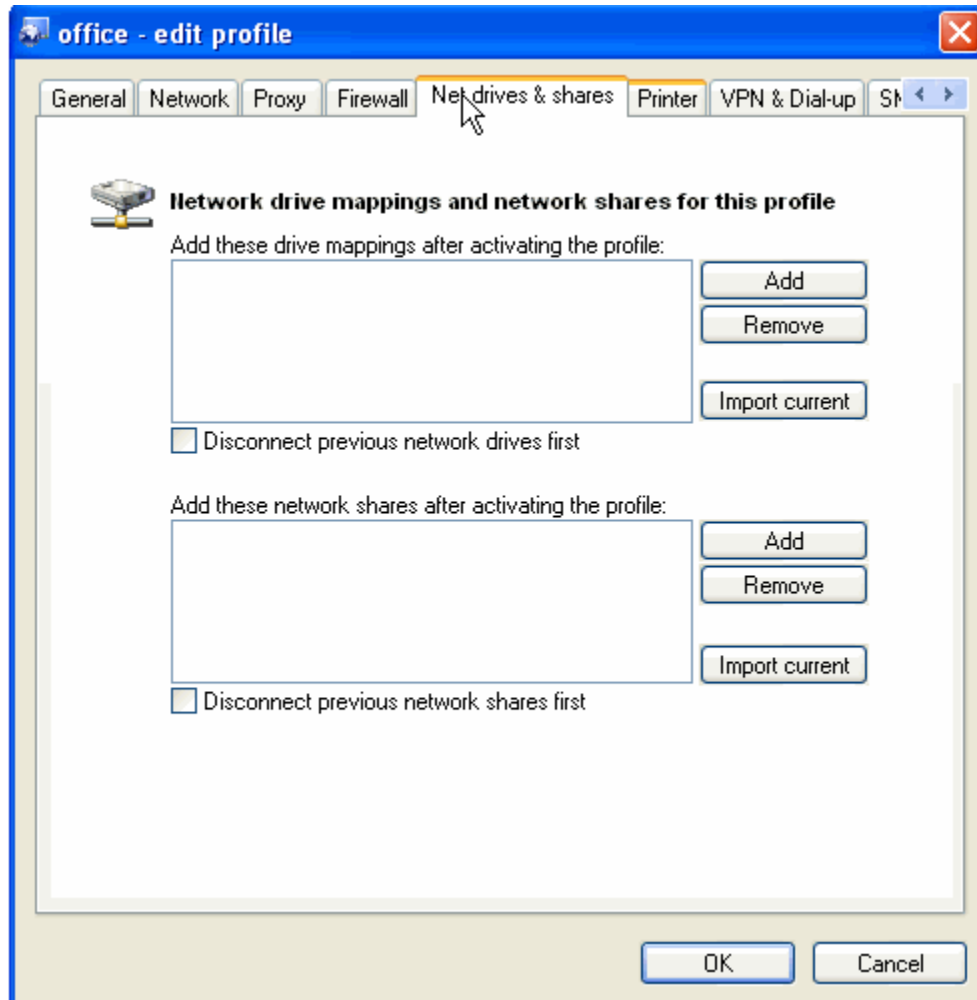
- To set the network settings go to **Network** tab



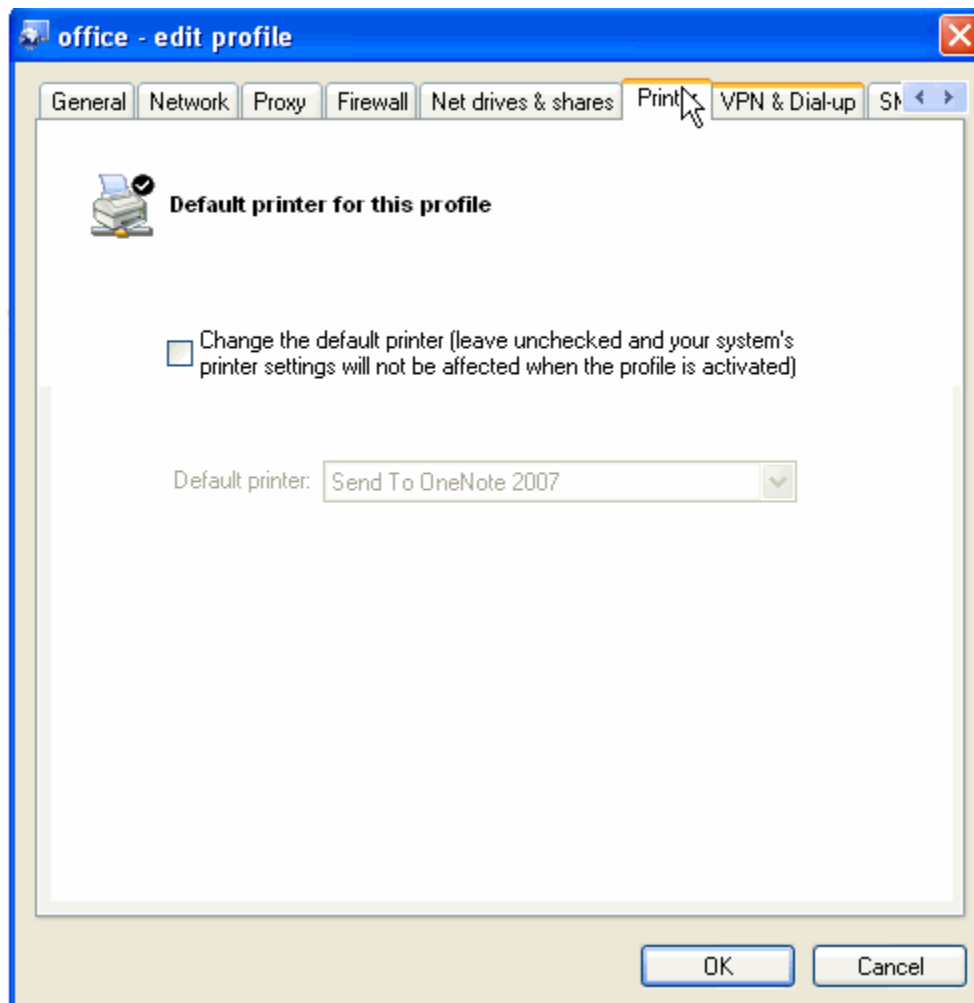
- To set the firewall settings click on **Firewall**



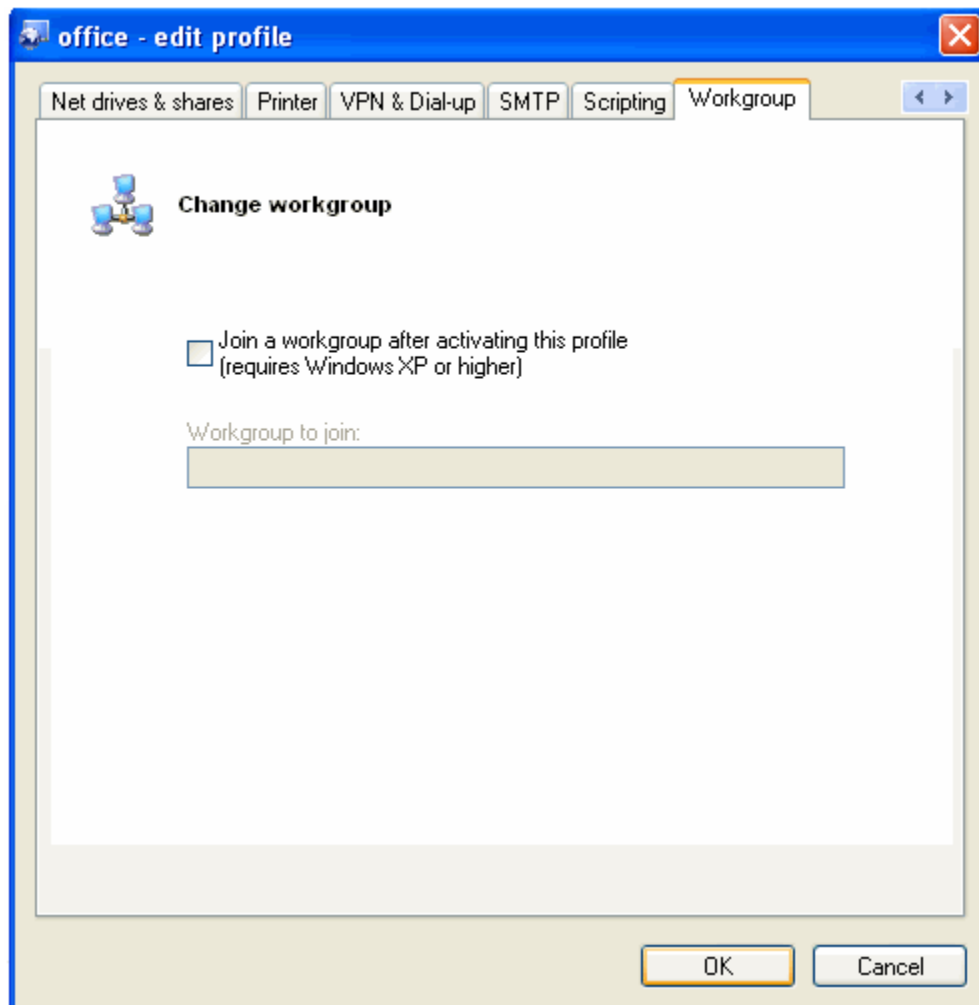
- To set Net drives & shares settings click on **Net drives & shares**



- To set the printer settings click on **Printer**



- To set the workgroup settings click on **work group**→**Ok**

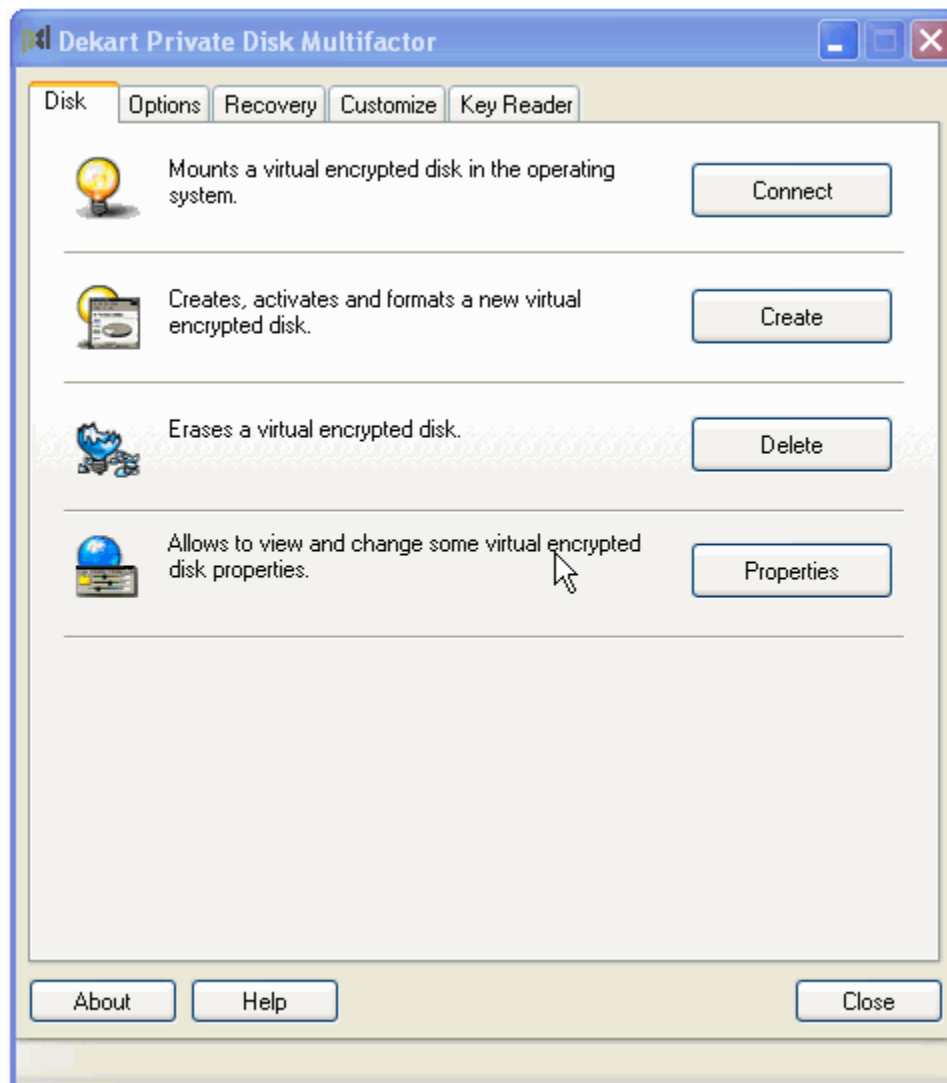


Lab 46-06

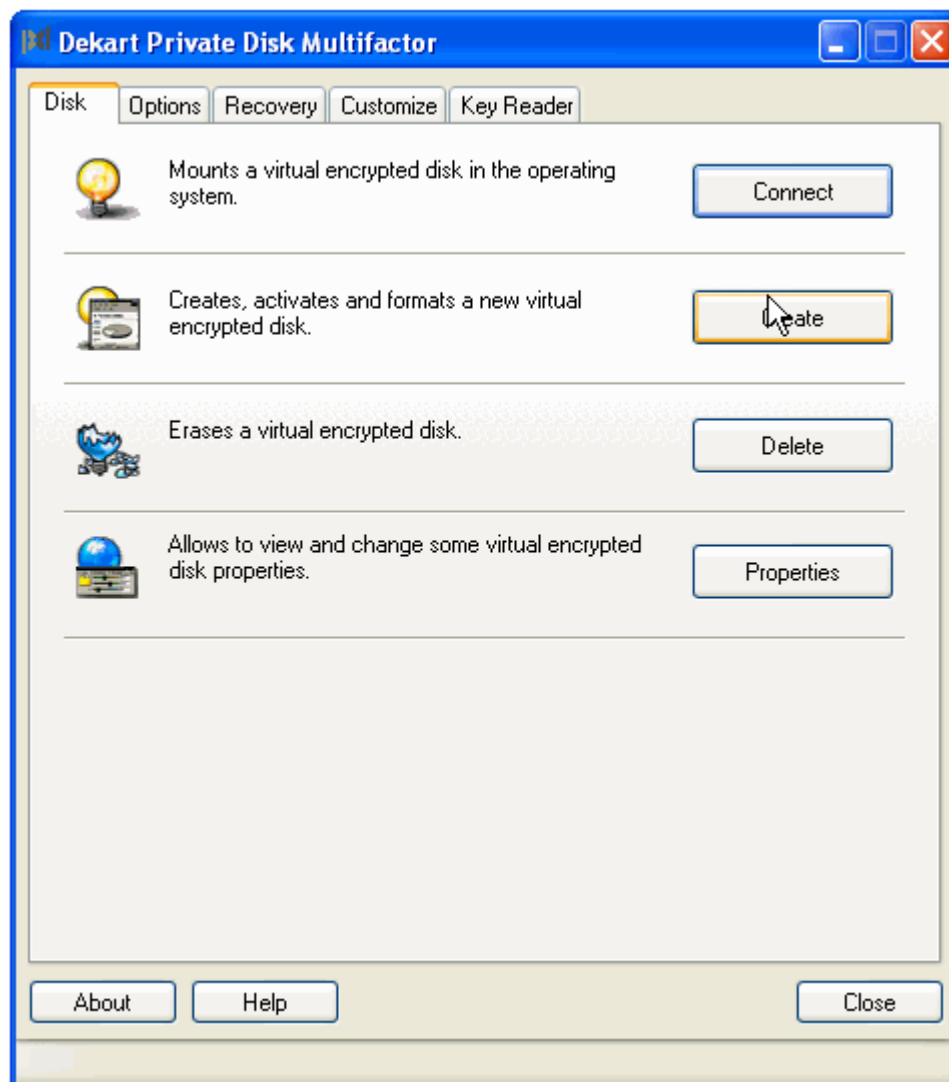
Objective:

Use **Private Disk Multifactor** to provide data confidentiality on Laptops.

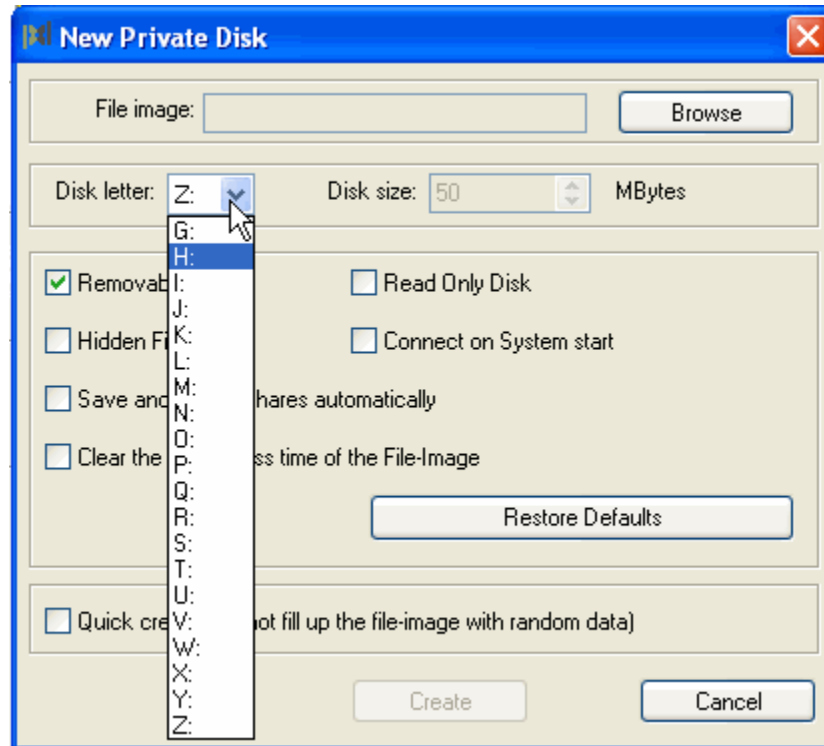
- In the **CEHv6 Labs CD-ROM** navigate to **Module 46**
- Install and launch **Dekart Private Disk Multifactor** program



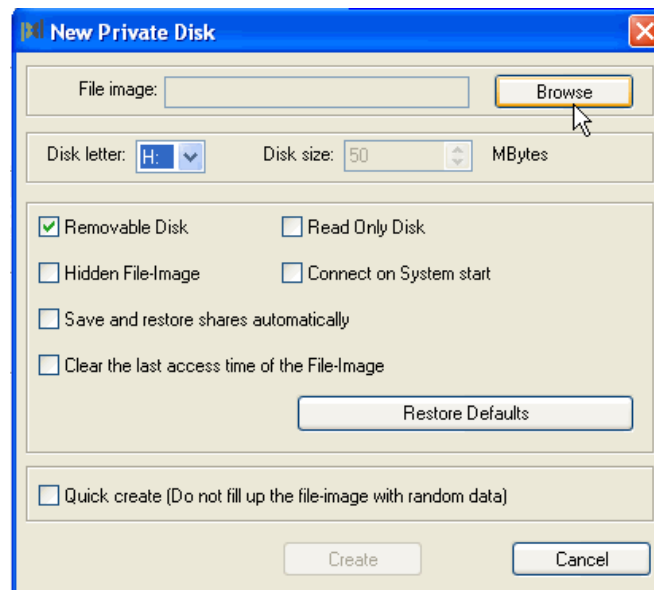
- To create a virtual encrypted disk , Click on **Disk→ Create**



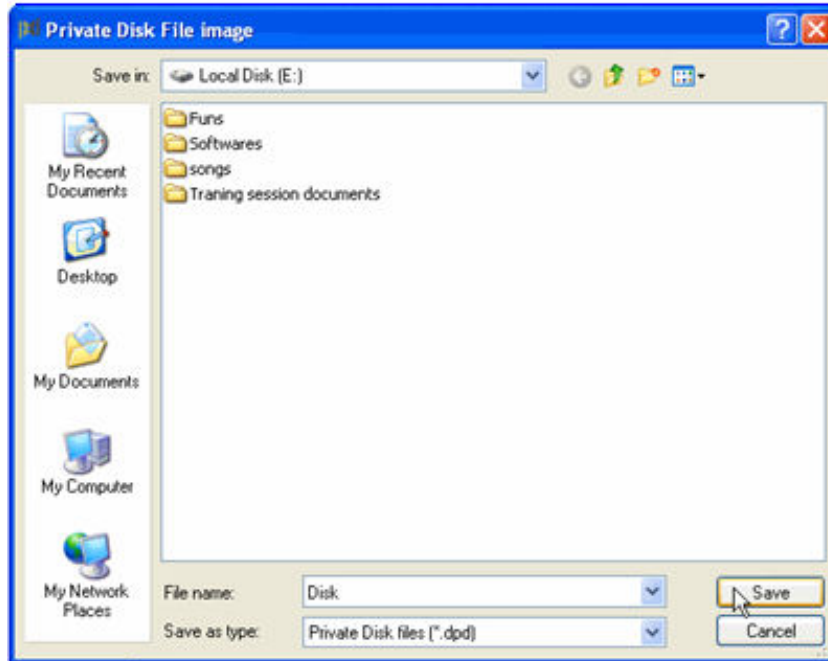
- Select the desired drive to be created



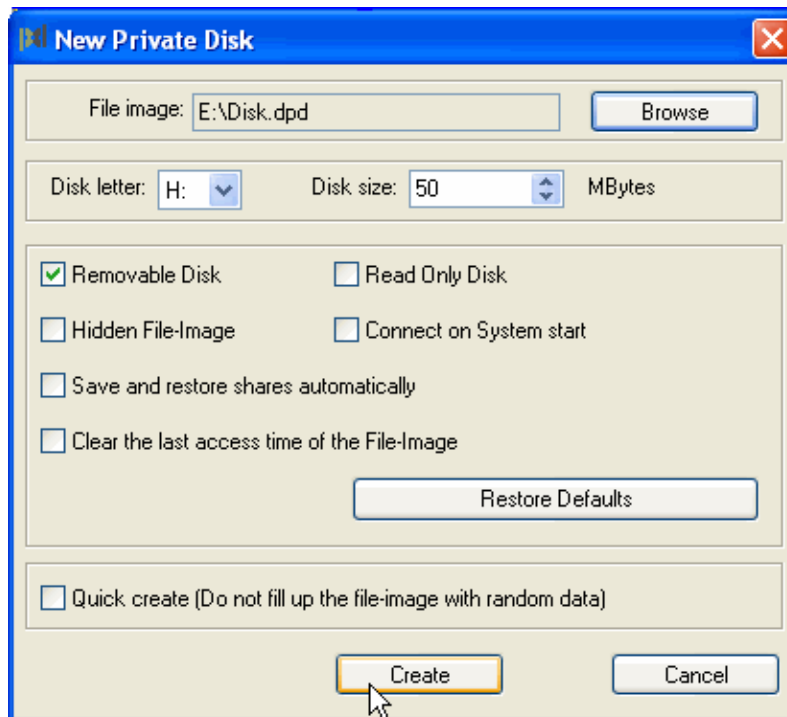
- Select the location to save a particular drive, click on **Browse**



- Enter disk name, click **Save**



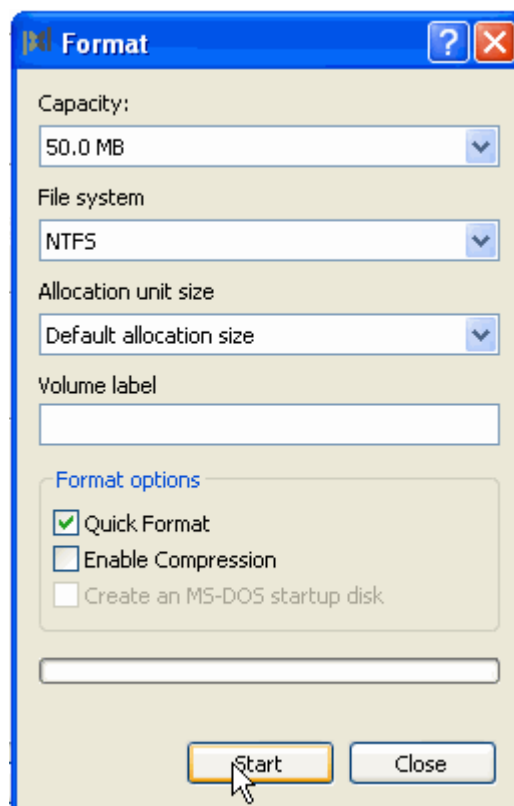
- Click **Create**



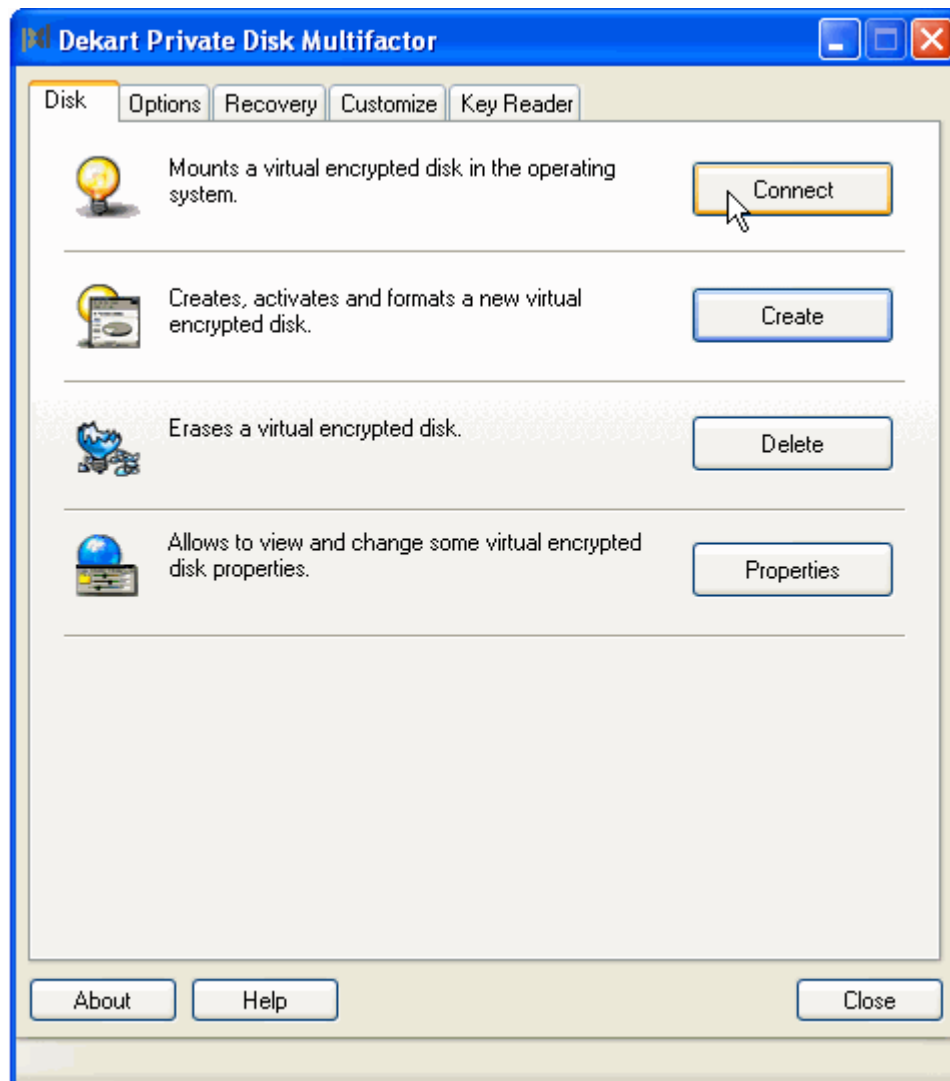
- To set the password Enter the password and click **OK**



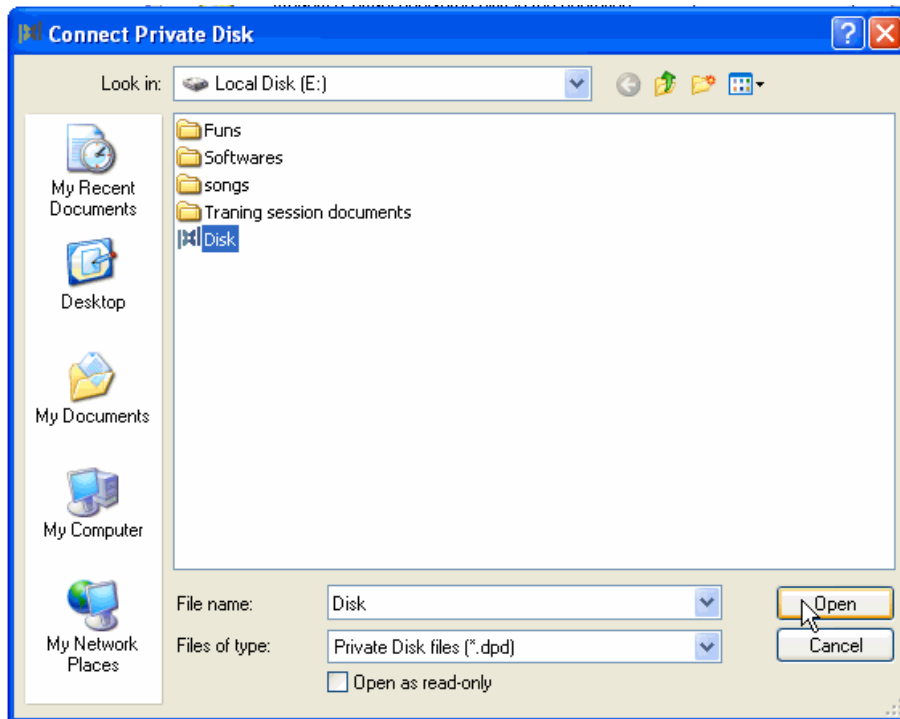
- When the formatted message appears, click on **start**



- To mount a disk into the virtual operating system click on **Connect**



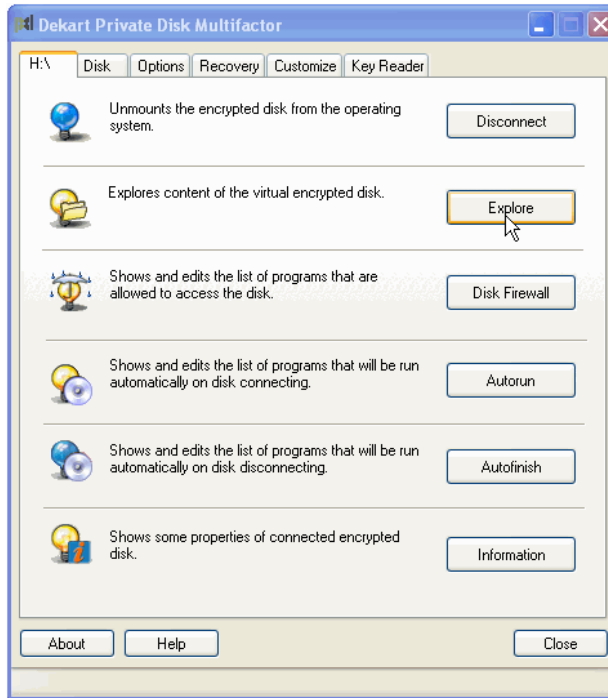
- Browse the disk, Click **Open**



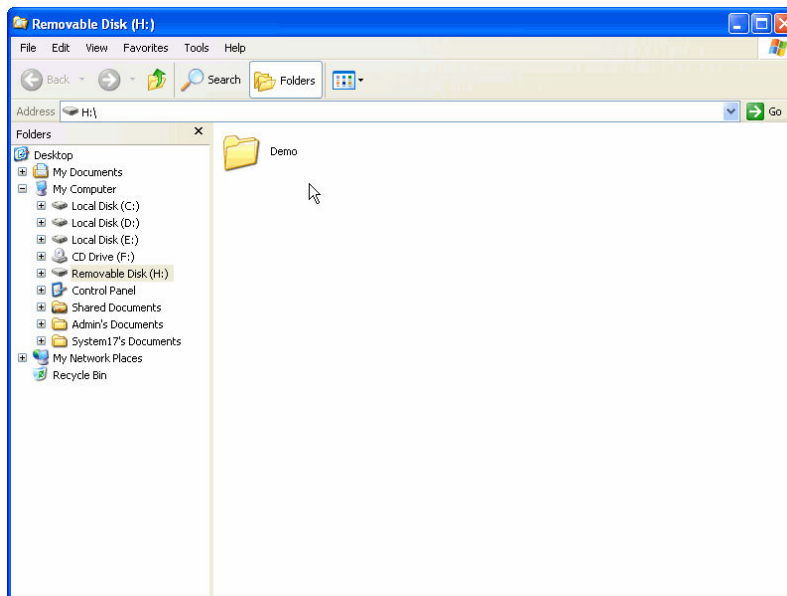
- Enter Password, click **Ok**



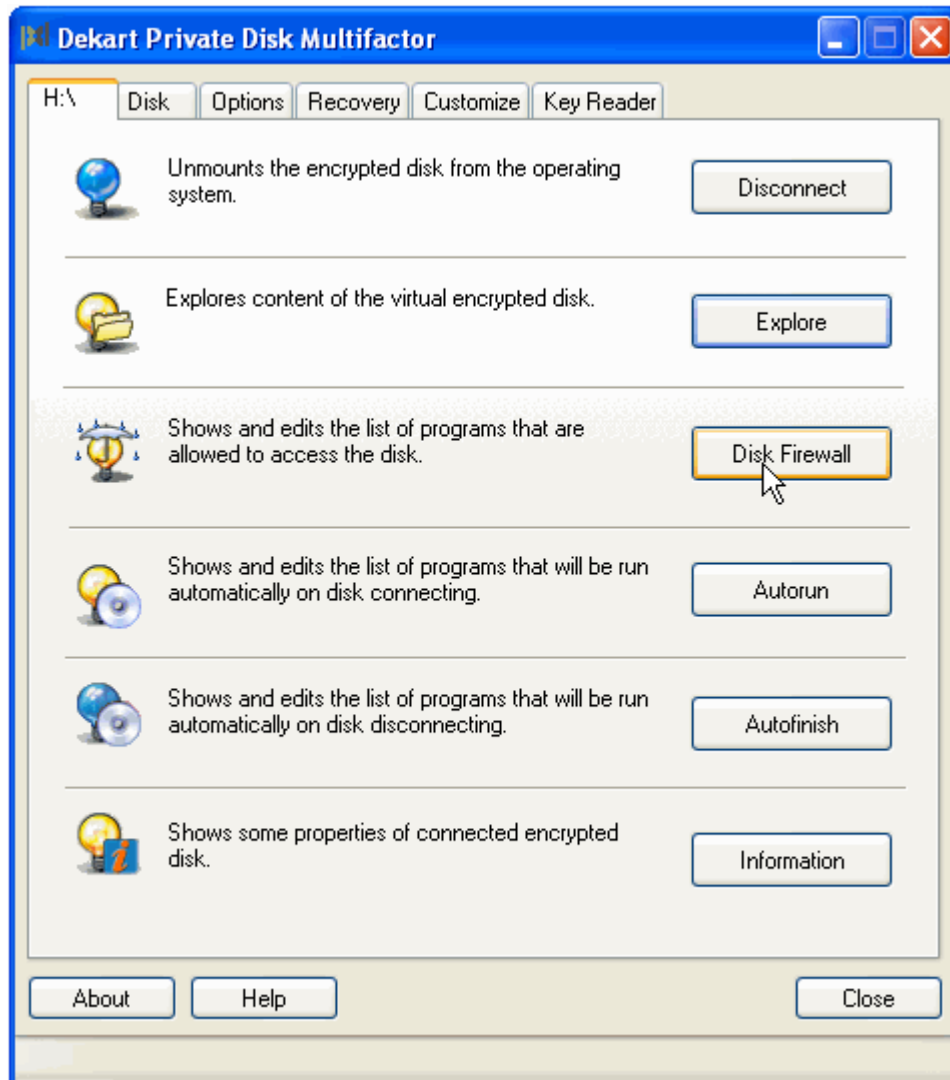
- To explore content of virtual disk click **Explore**



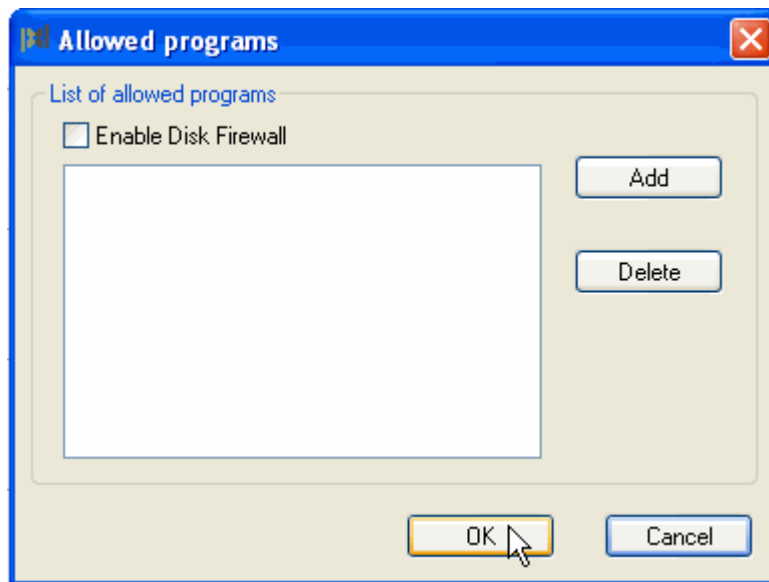
- The Explored Virtual disk



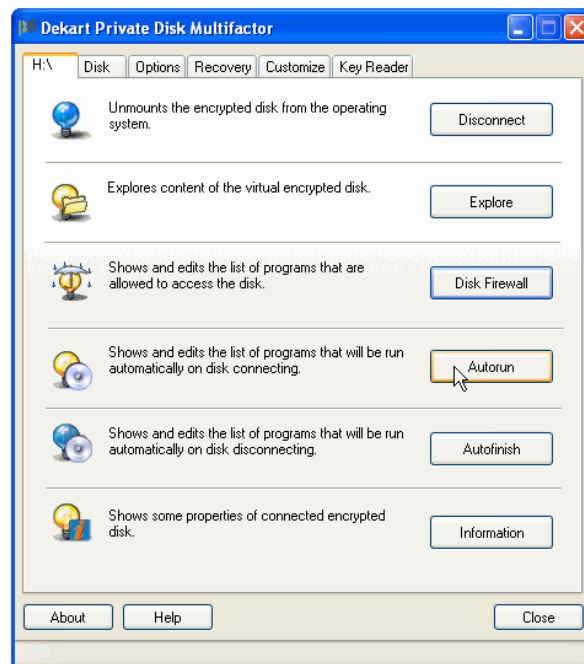
- To view the list of programs those are allowed to access the disk, click on **H:\-->Disk Firewall**



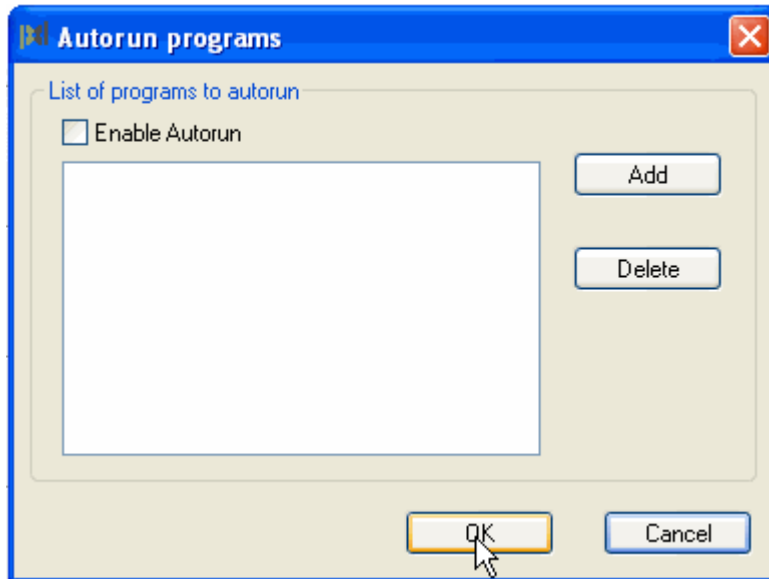
- To add the program that are able to access the disk, click on **Add** → **Ok** , check the **Enable Disk Firewall** box



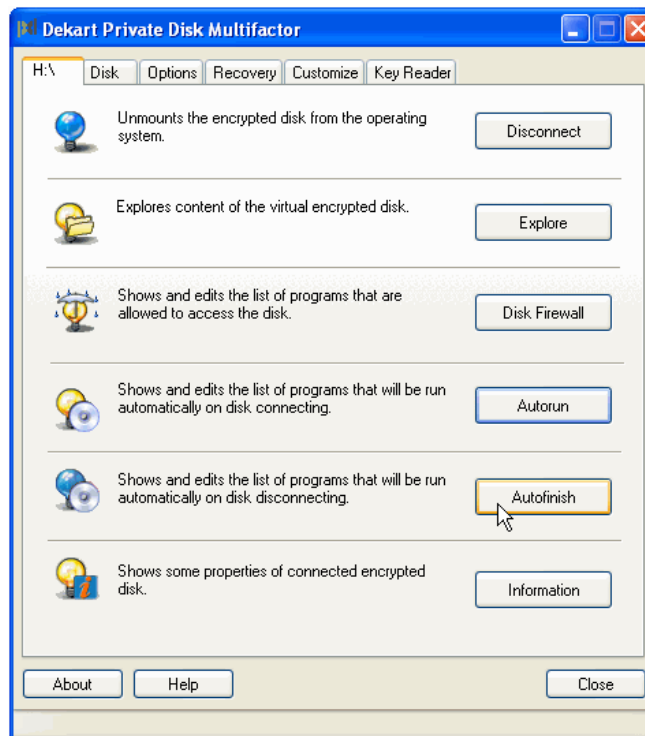
- To view and edit the list of programs running automatically after disk connecting, click on **Autorun**



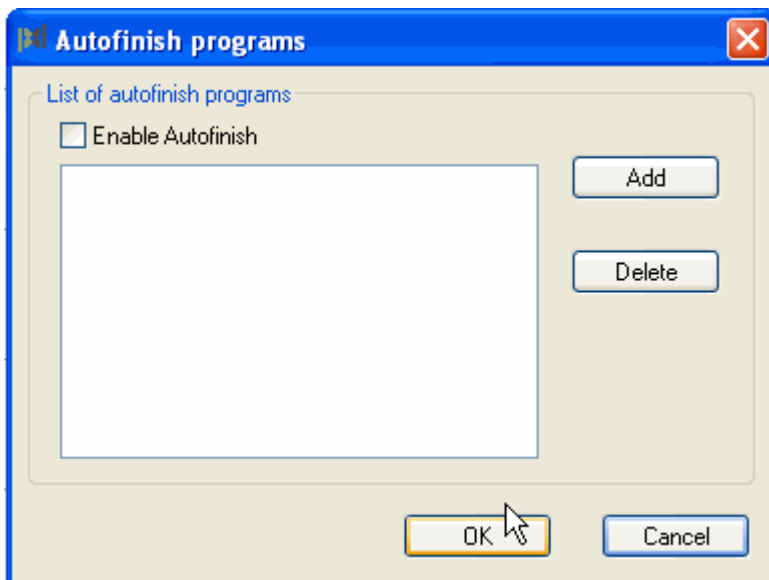
- To add list of programs Click **Add→Ok**



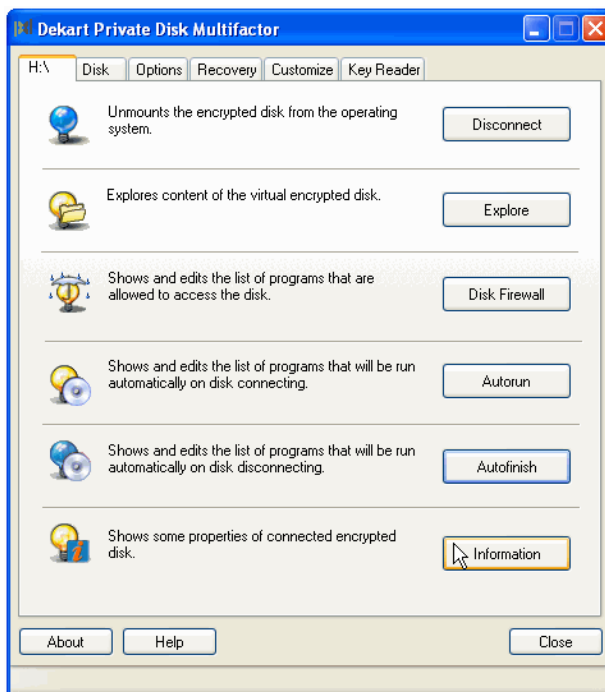
- To view and list of programs that run automatically on disk disconnecting, click **Autofinish**



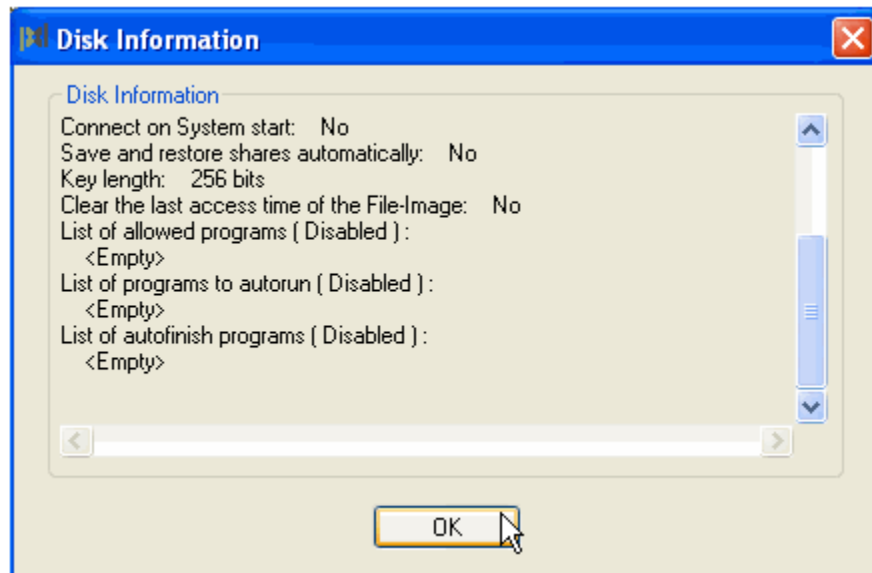
- Add the programs and click **Ok**



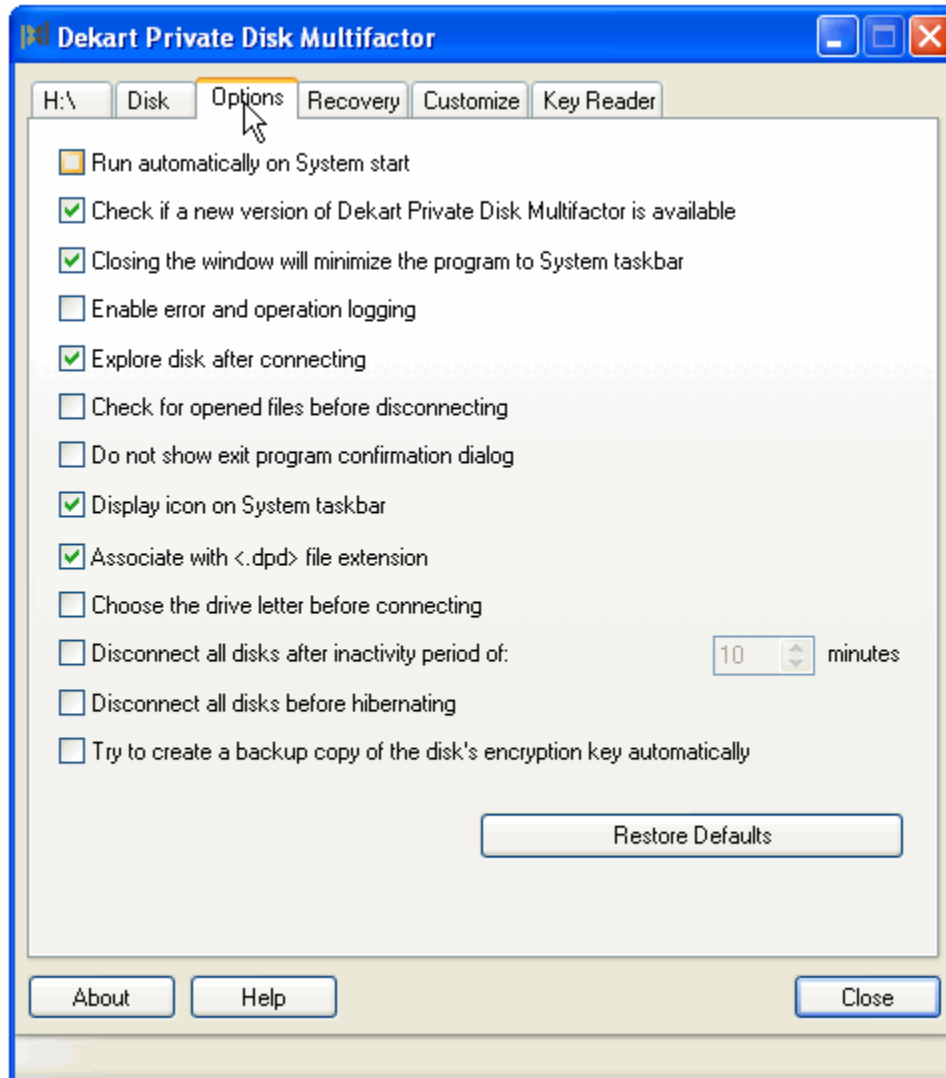
- To view the disk information, click on **Information**



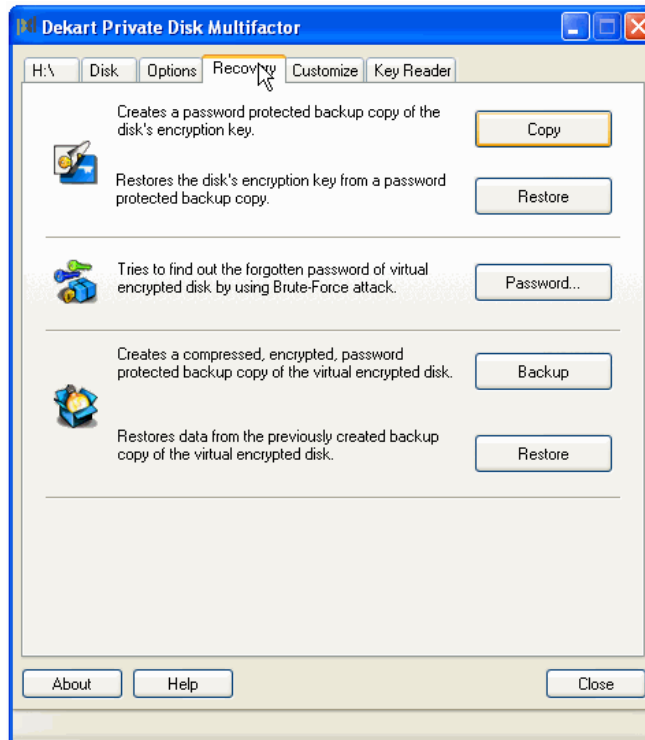
- The Disk information is as shown



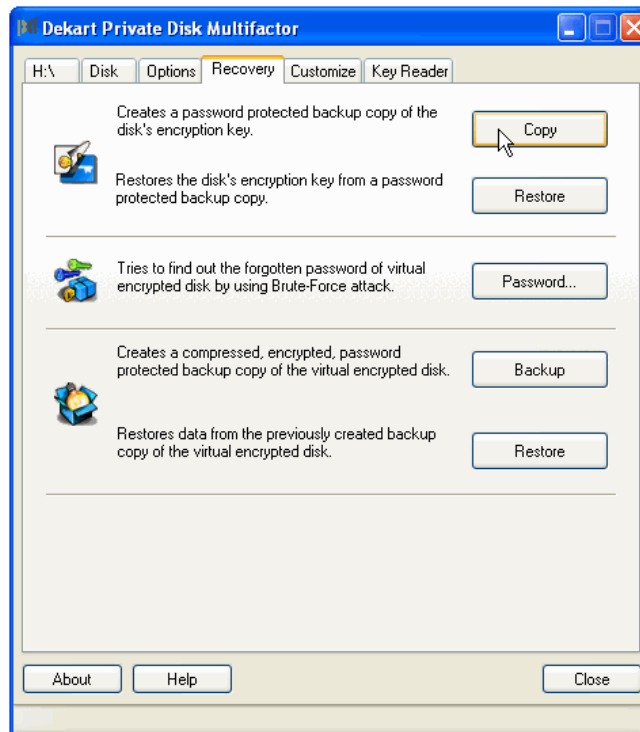
- To set the options click on **options**, check the desired dialog boxes



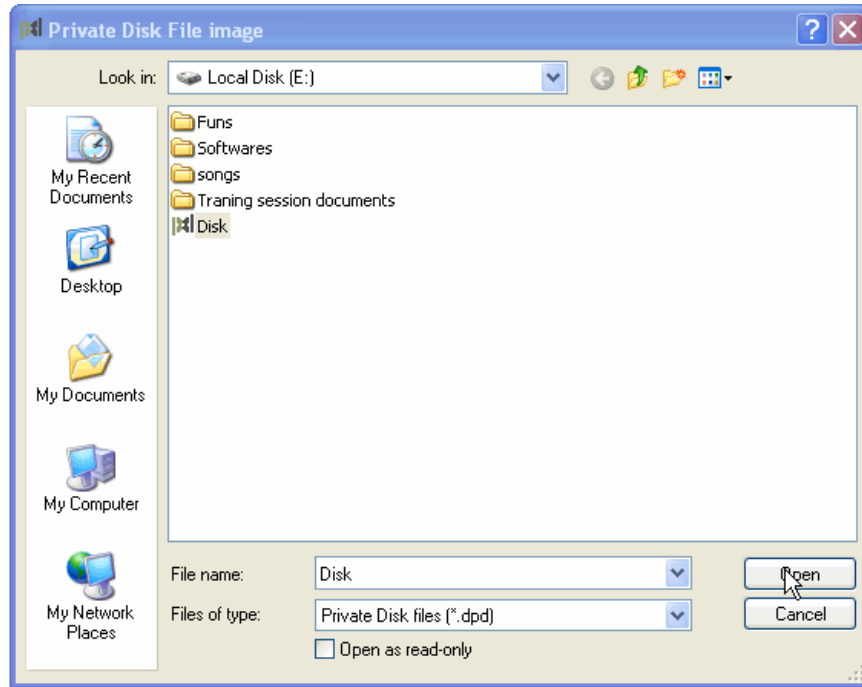
- To create a password protected copy of a disk's encryption protected key, click on **Recovery**



- Click **Copy**



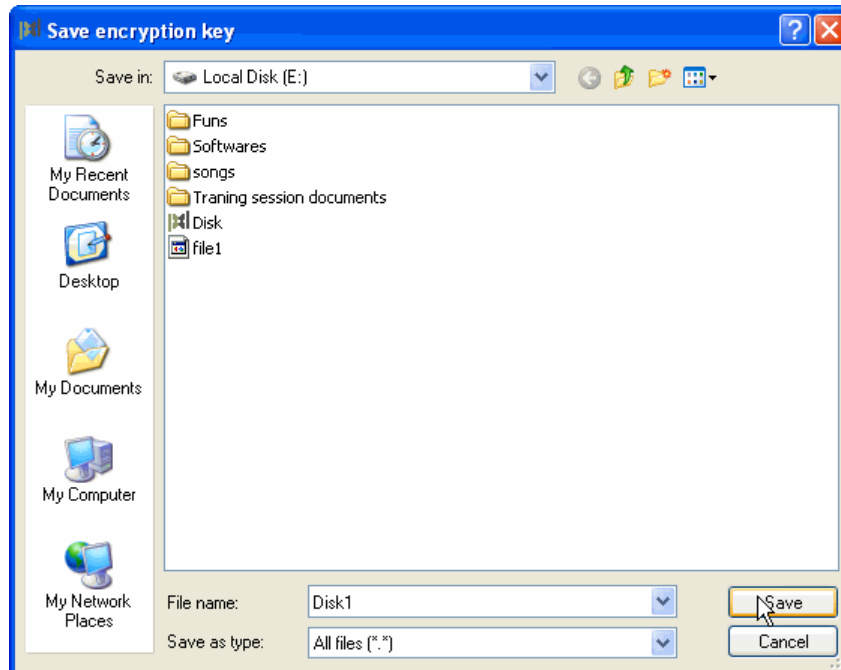
- Browse the disk from the location click **Open**



- Enter Password Click **Ok**



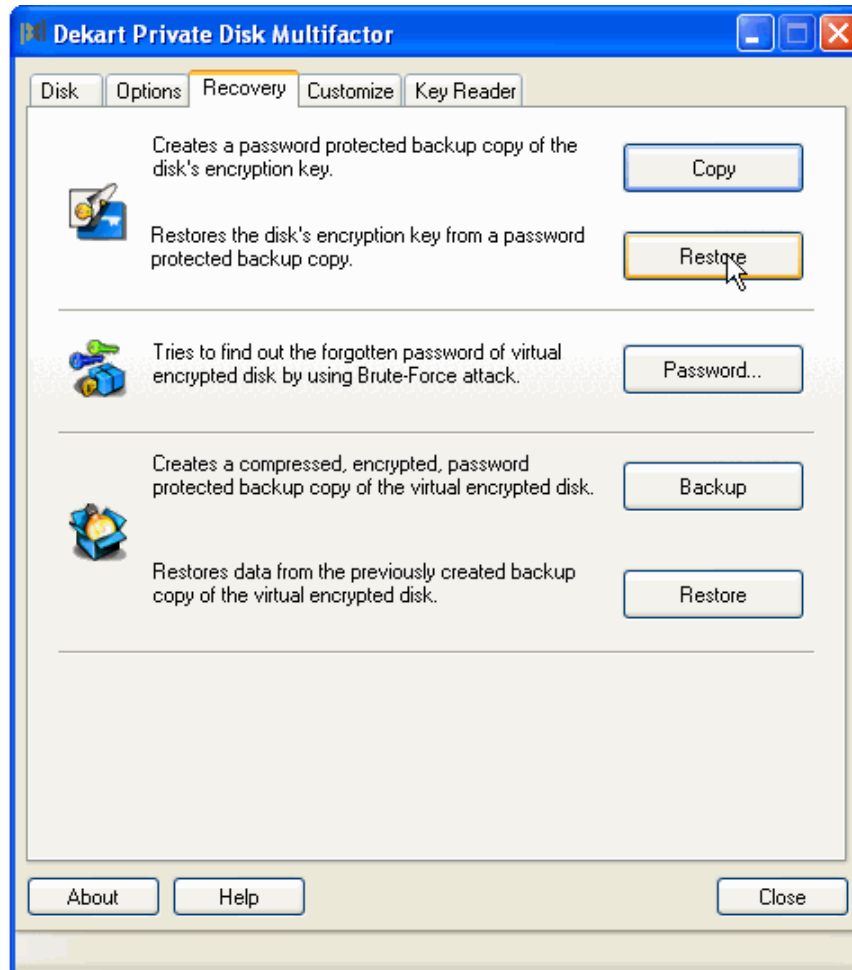
- To Save, Enter the file name and click **Save**



- Enter encryption password, click **Ok**



- To restore the disk encryption key from a password protected backup copy, click on **Restore**



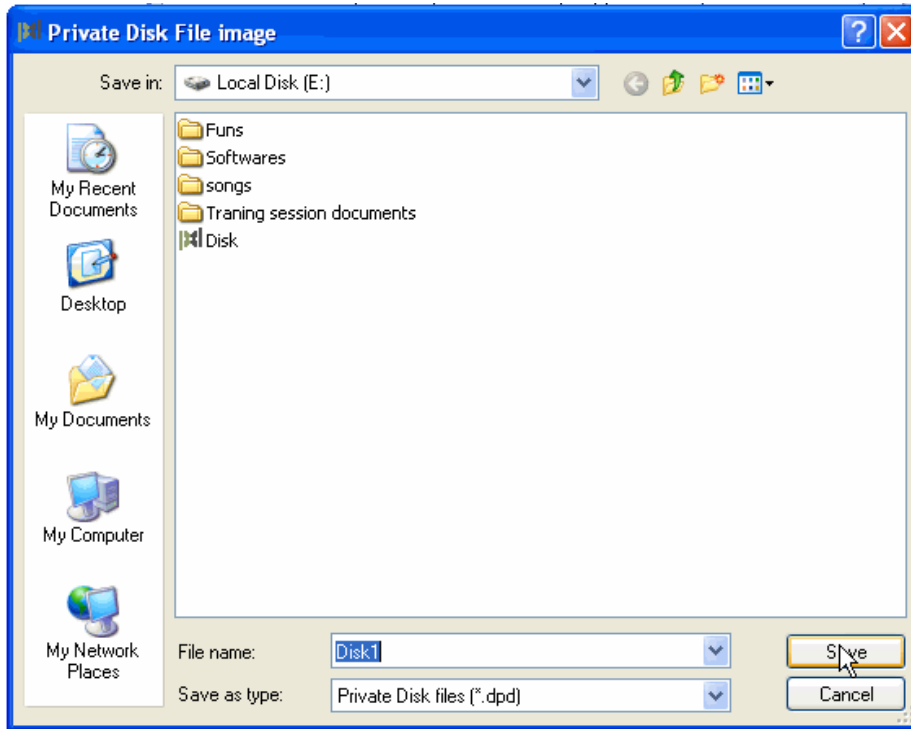
- Browse the disk, Click **Open**



- Enter Password, Click **Ok**



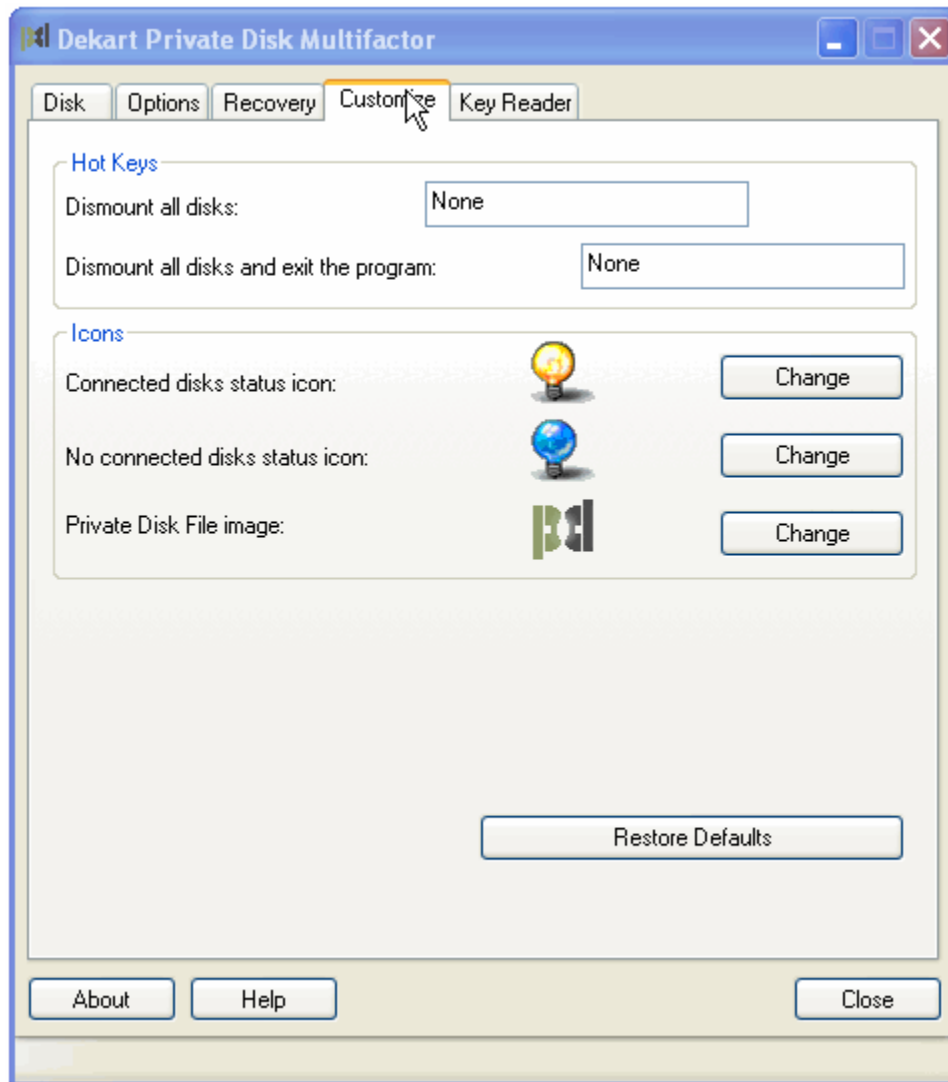
- Enter file name, Click **Save**



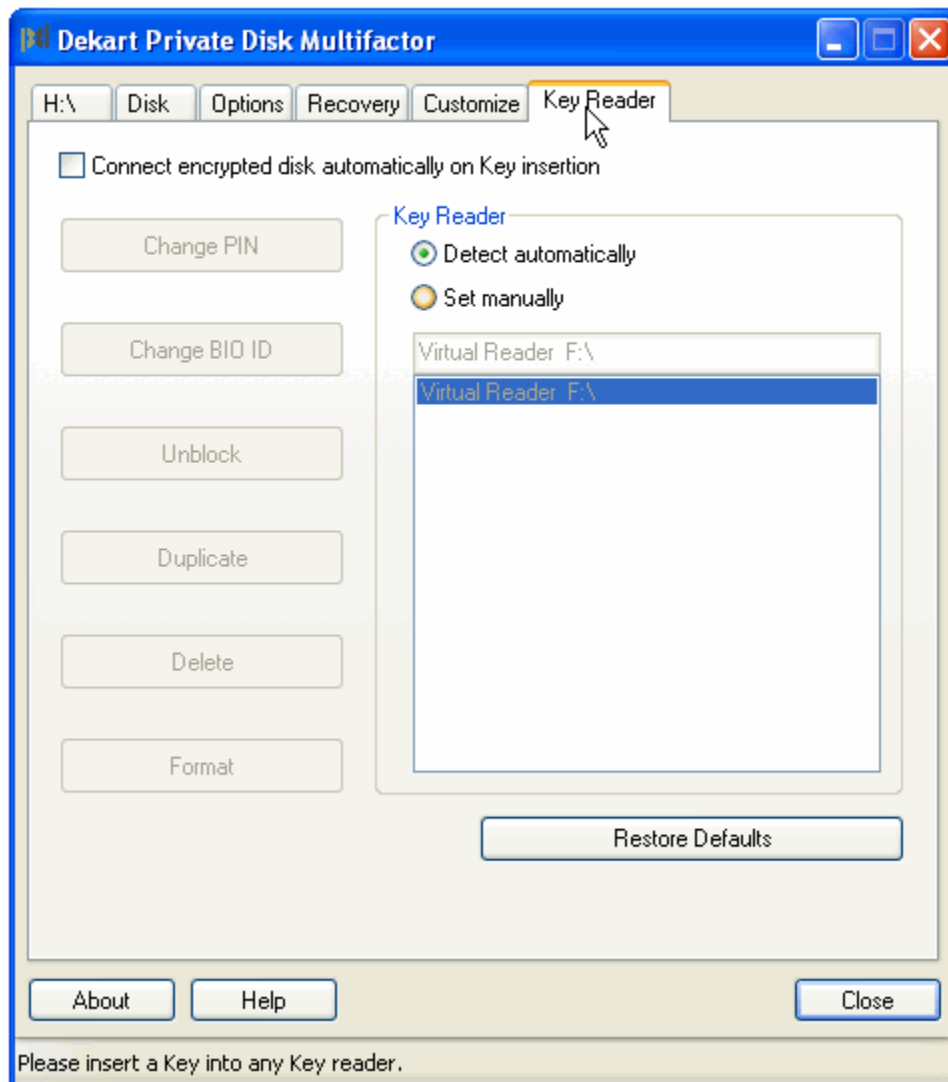
- Enter password, Click **Ok**



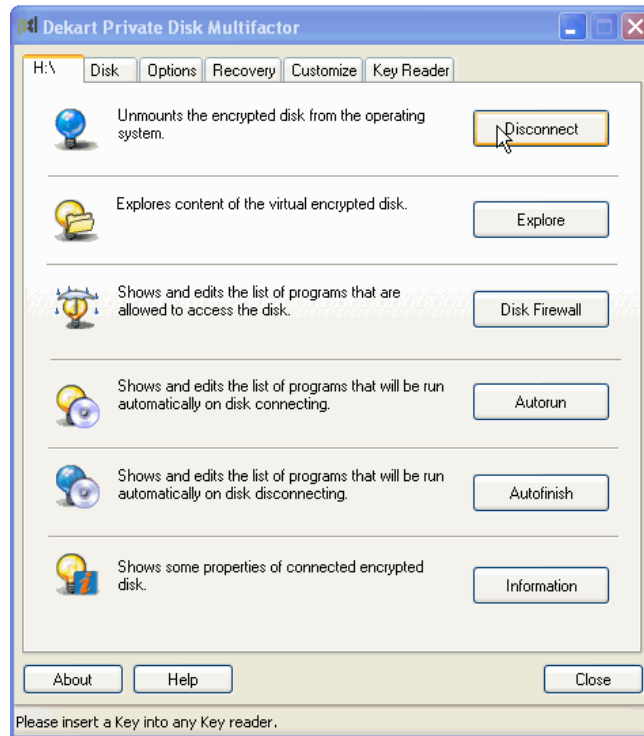
- To customize icons and set hot keys click on **customize**



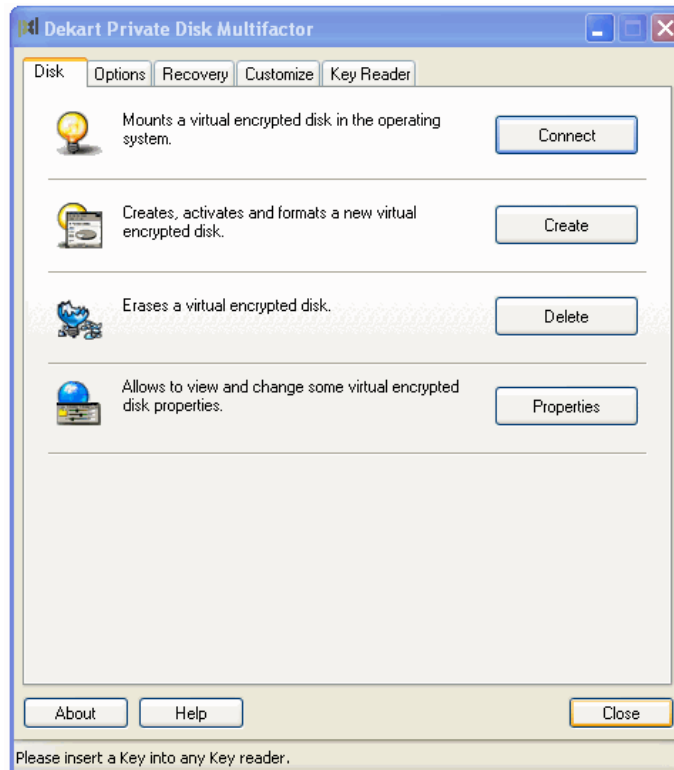
- To automatically connect disk after key insertion, click on **Key Reader**



- To unmount the encrypted disk from operating system, click on **H :\--> Disconnect**

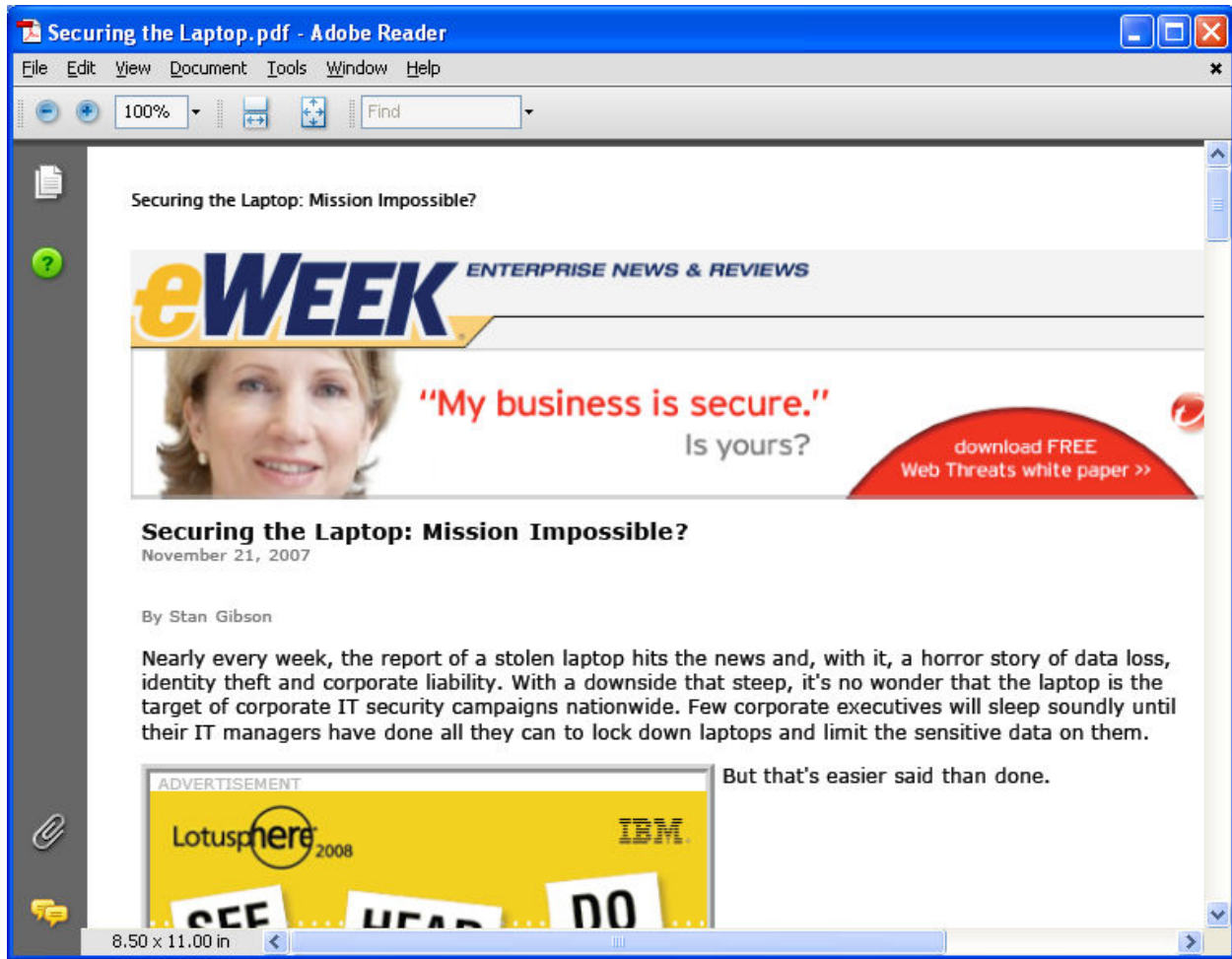


- Disk after **unmounting**



Lab 46-07

- In the **CEHv6 Labs CD-ROM** navigate to **Module 46**
- Open the **Securing the Laptop.pdf** and read the content



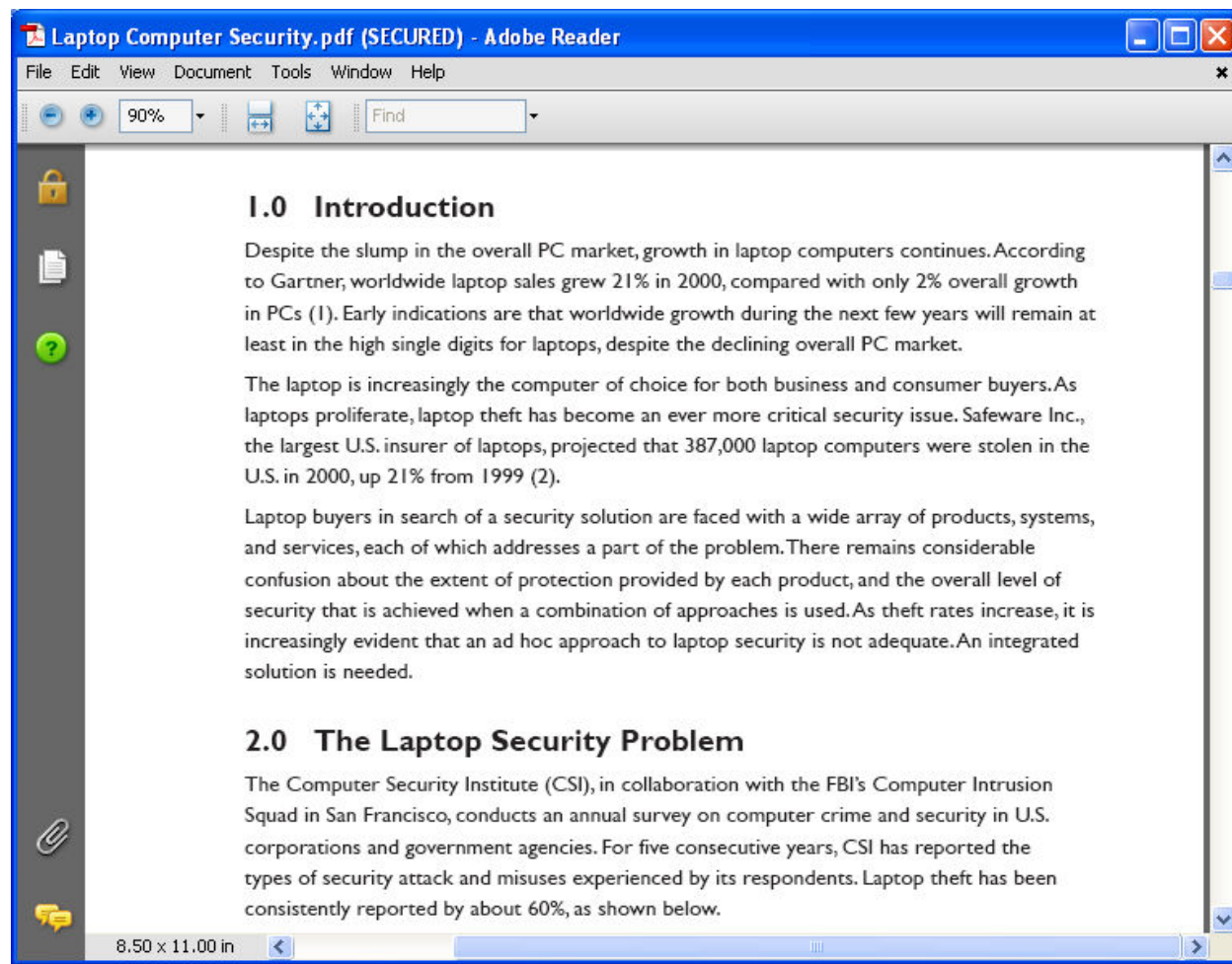
Lab 46-08

- In the **CEHv6 Labs CD-ROM** navigate to **Module 46**
- Open the **Cyber Security Tips.pdf** and read the content



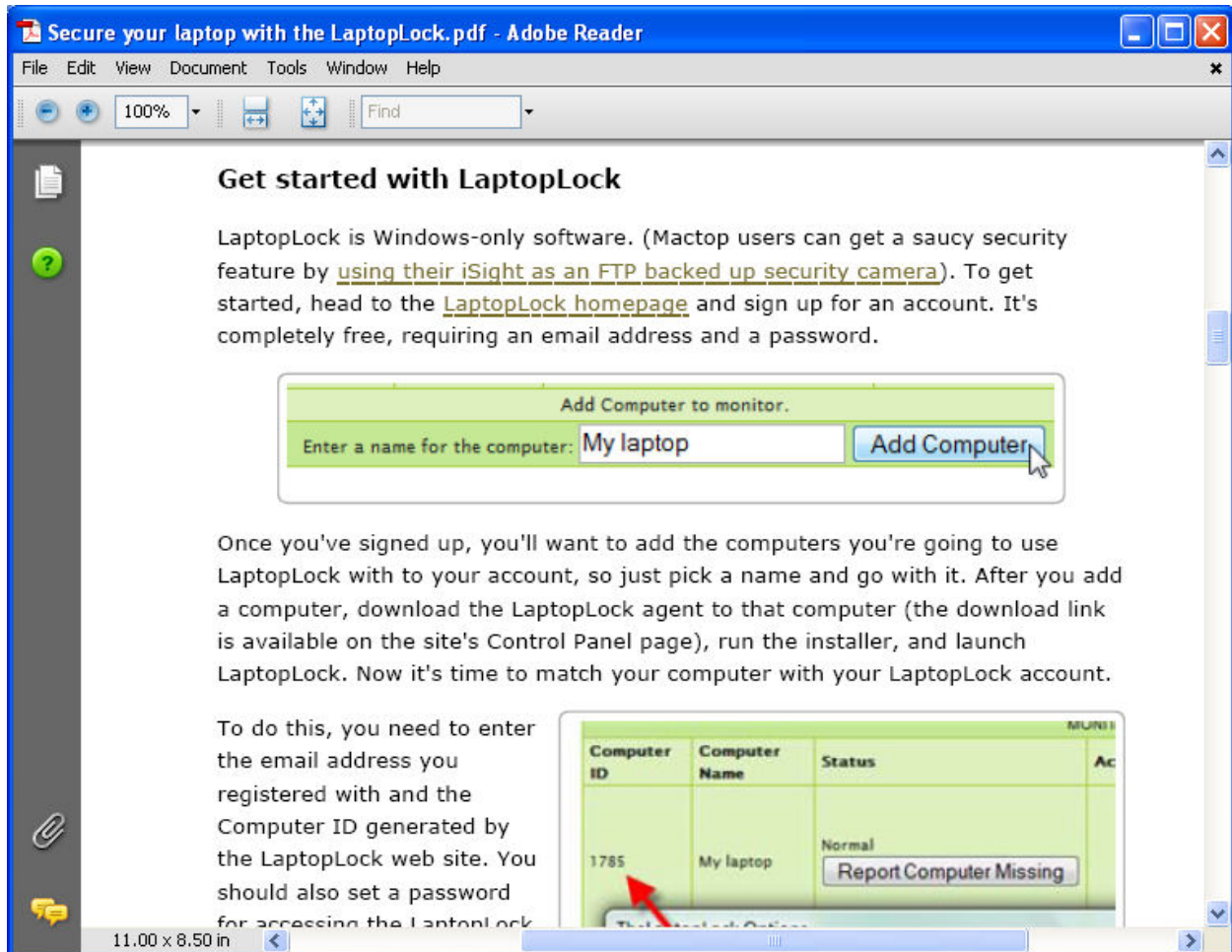
Lab 46-09

- In the **CEHv6 Labs CD-ROM** navigate to **Module 46**
- Open the **Laptop Computer Security.pdf** and read the content



Lab 46-10

- In the **CEHv6 Labs CD-ROM** navigate to **Module 46**
- Open the **Secure your laptop with the LaptopLock.pdf** and read the content



Secure your laptop with the LaptopLock.pdf - Adobe Reader

File Edit View Document Tools Window Help

100% Find

Get started with LaptopLock

LaptopLock is Windows-only software. (Mactop users can get a saucy security feature by [using their iSight as an FTP backed up security camera](#)). To get started, head to the [LaptopLock homepage](#) and sign up for an account. It's completely free, requiring an email address and a password.

Add Computer to monitor.

Enter a name for the computer:

Once you've signed up, you'll want to add the computers you're going to use LaptopLock with to your account, so just pick a name and go with it. After you add a computer, download the LaptopLock agent to that computer (the download link is available on the site's Control Panel page), run the installer, and launch LaptopLock. Now it's time to match your computer with your LaptopLock account.

To do this, you need to enter the email address you registered with and the Computer ID generated by the LaptopLock web site. You should also set a password for accessing the Laptop lock

Computer ID	Computer Name	Status	Ac
1785	My laptop	Normal	

Report Computer Missing

Lab 46-11

- In the **CEHv6 Labs CD-ROM** navigate to **Module 46**
- Open the **laptop security.pdf** and read the content



Lab 46-12

- In the **CEHv6 Labs CD-ROM** navigate to **Module 46**
- Open the **laptop_computer_security.pdf** and read the content

laptop_computer_security.pdf - Adobe Reader

File Edit View Document Tools Window Help


90% Find

Why Emphasize Laptop Security?

Laptop computers offer the convenience of mobility, but the risk of lost or stolen machines and of wrongful access to HHS data is high and climbing. The use of government-owned laptops and personally owned laptops to store HHS-related data and to access HHS networks demands attention to security precautions.

More than 1,000 laptops are stolen every day. The value of the laptops themselves is in the millions of dollars. The value of the lost data is incalculable. The FBI reports that 97 percent of stolen laptops are never recovered.

HHS policies and guidelines hold you responsible for your government-owned laptop and its data, and for government-owned data on personally owned computers. However you should never put your personal safety at risk to protect a laptop. The suggestions in this brochure will help you protect your laptop, its information, and HHS networks.



4. Most laptops come with a socket that can be attached to a security cable. If yours doesn't, your cable may come with an adhesive-backed attachment that will fasten the cable to the laptop. On the cable itself, a cylinder lock is stronger than a combination lock. While cable cutters could easily slice through the wire cables, from a thief's perspective, they are conspicuous.
5. Instead of using a laptop carrying case—especially one with the manufacturer's name on the outside—consider putting the laptop in a **padded** case, then in a backpack, briefcase, or other ordinary-looking holder.
6. Batteries, power cords, and other

11.00 x 8.50 in

Lab 46-13

- In the **CEHv6 Labs CD-ROM** navigate to **Module 46**
- Open the **securing_your_laptop.pdf** and read the content





Module 47

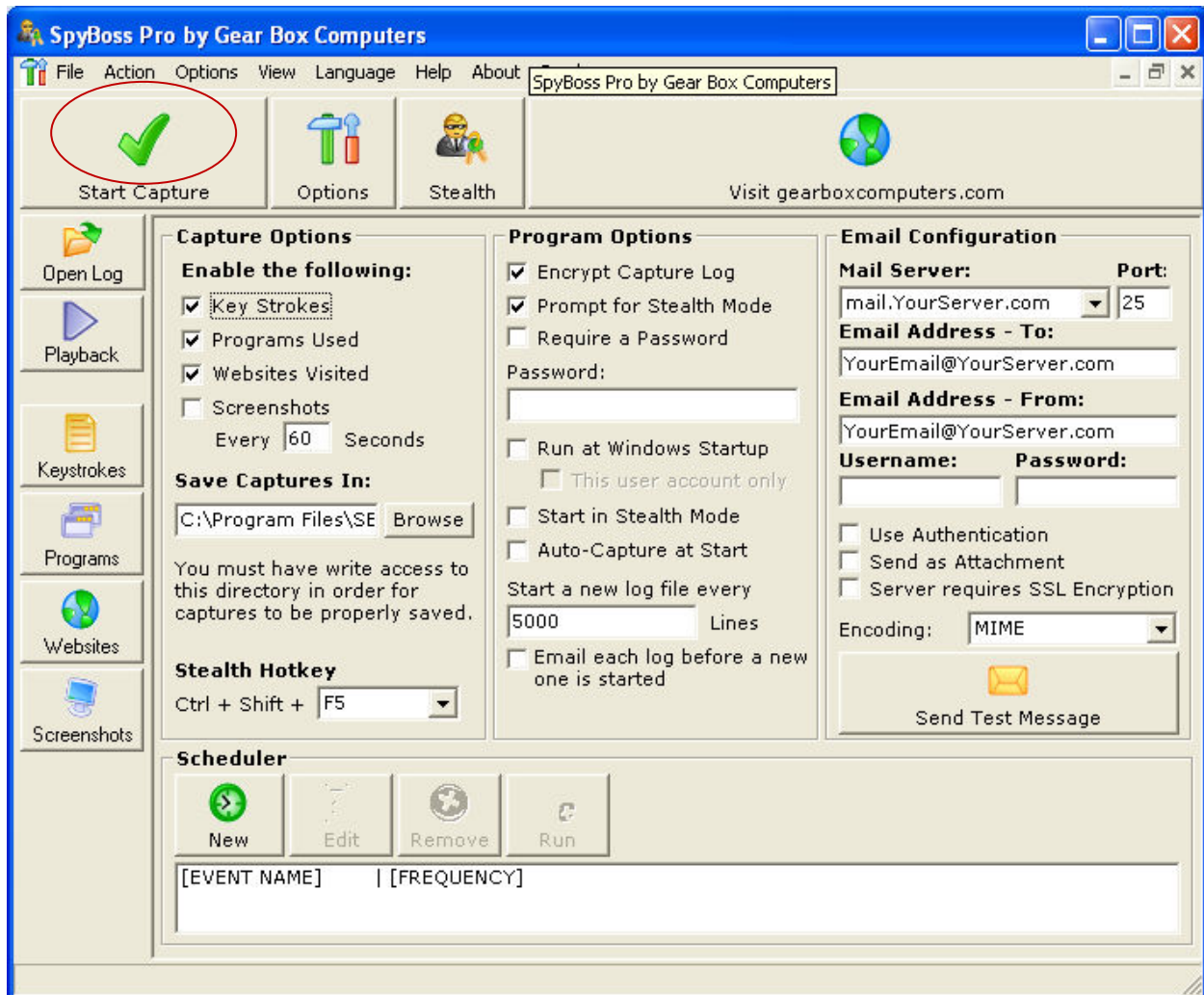
Spying Technologies

Lab 47-01

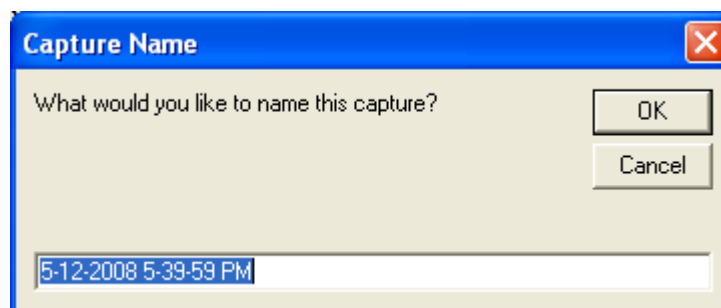
Objective:

Use **SpyBoss** to monitor everything which is doing on a Computer.

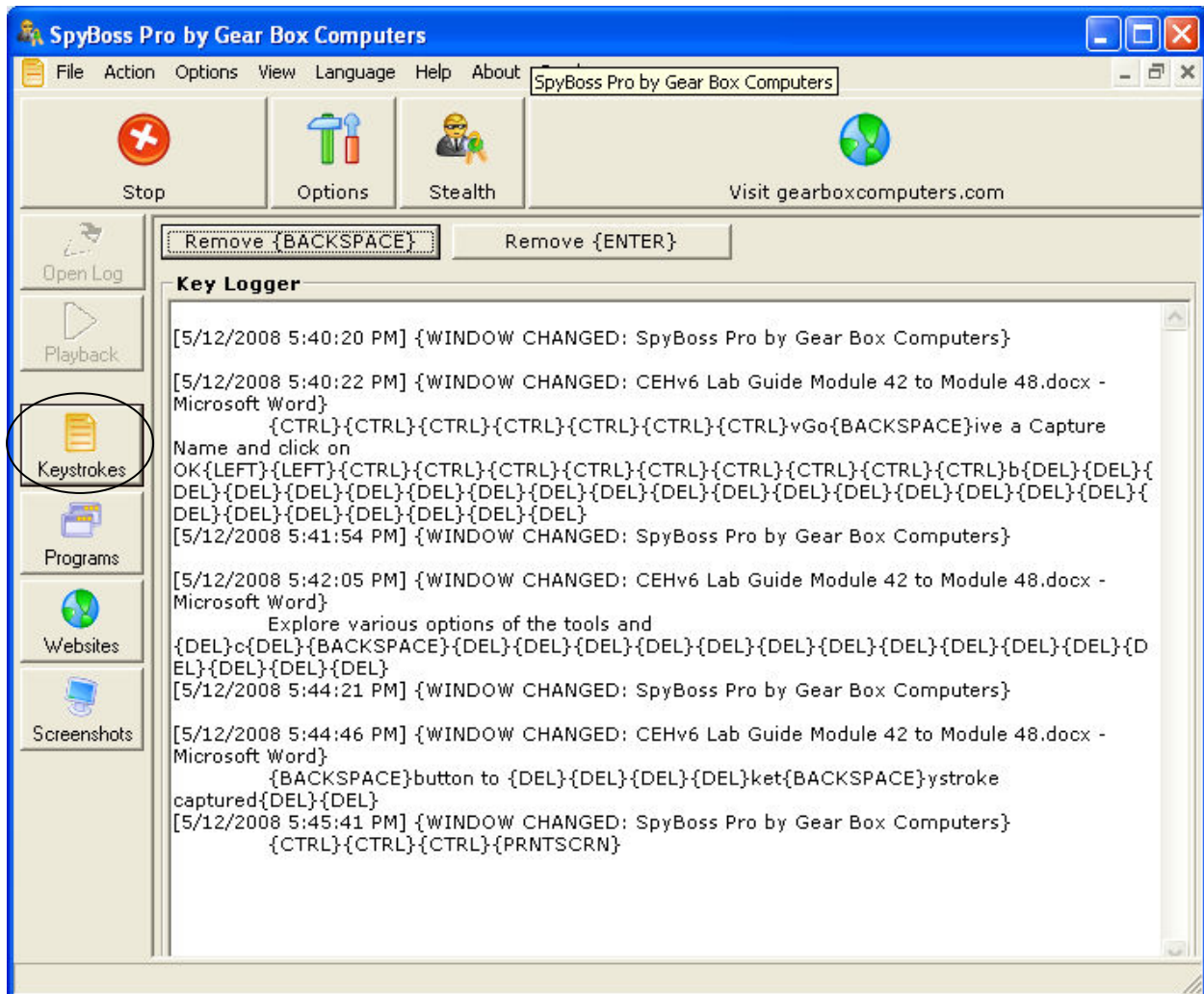
- In the **CEHv6 Labs CD-ROM** navigate to **Module 47**
- Install and launch “**SpyBoss Pro**” program
- Explore various options of the tools and click on **Start Capture** button to start capturing



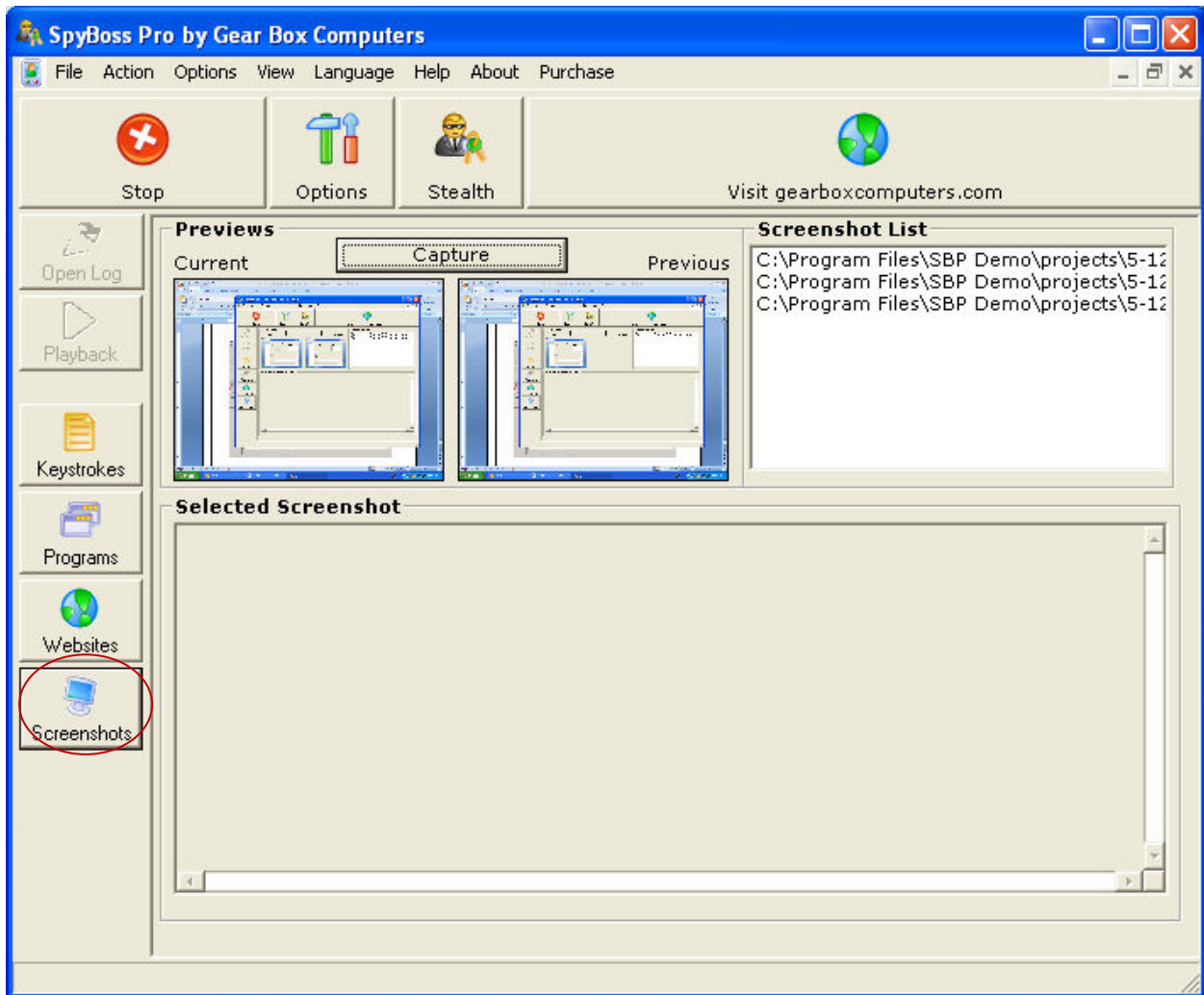
- Give a Capture Name and click on **OK**



- Click on **Keystrokes** button to check the keystroke captured

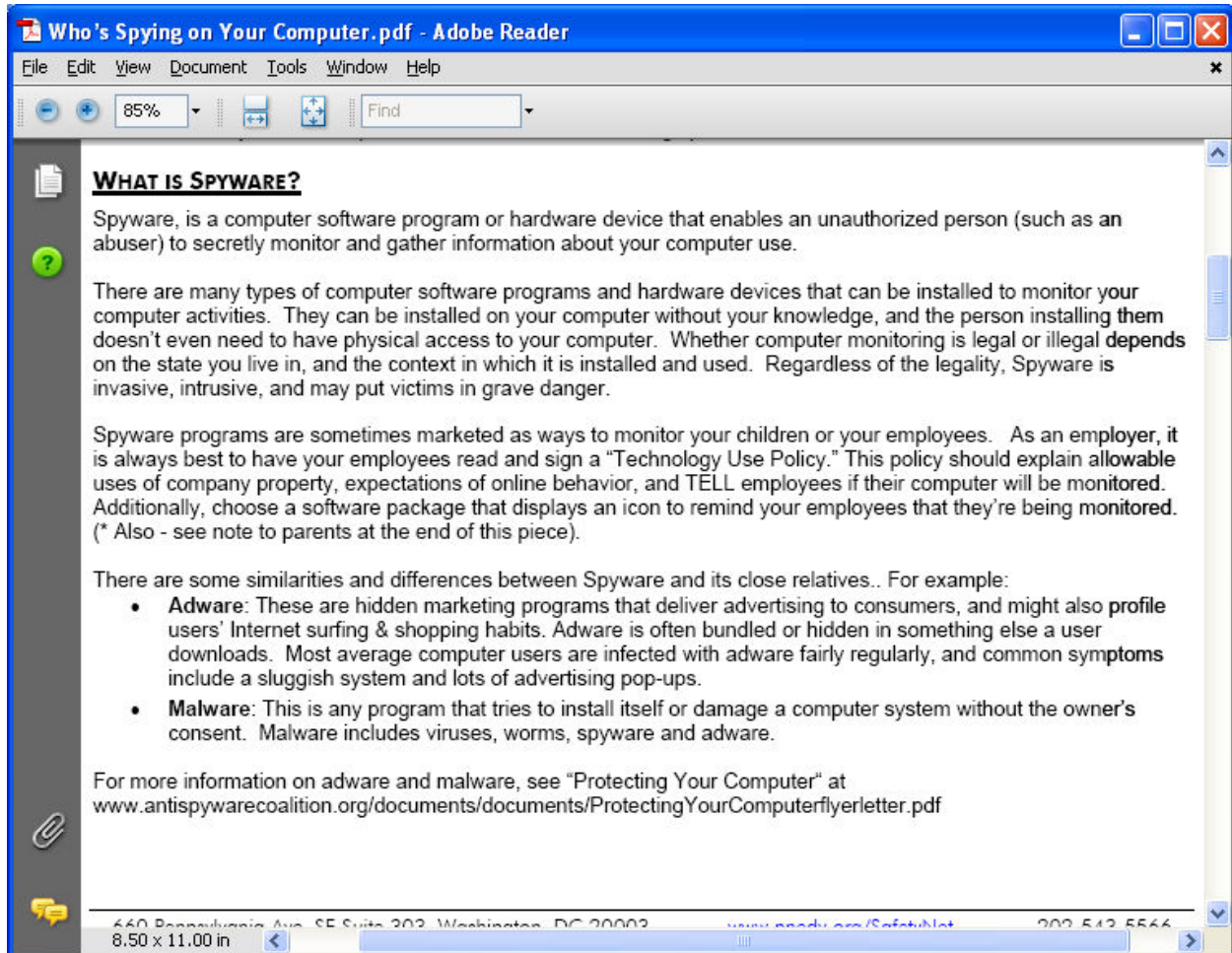


- Click on **Screenshots** button to check the captured screenshots



Lab 47-02

- In the **CEHv6 Labs CD-ROM** navigate to **Module 47**
- Open the **Who's Spying on Your Computer.pdf** and read the content



Lab 47-03

- In the **CEHv6 Labs CD-ROM** navigate to **Module 47**
- Open the **The Science of Spying.pdf** and read the content



The screenshot shows the Adobe Reader interface with the document 'The Science of Spying.pdf' open. The document content includes:

The Science of Spying

Resources for students and teachers

Purpose
To introduce teachers to 'The Science of Spying' exhibition and its accompanying educational resources, which can be downloaded from:
www.scienceofspying.com



Who will find these resources useful?

The subject of spying is a powerful theme that can excite students about a range of curriculum subjects within an engaging 'real world' context. These resources should be useful for:

- Teachers of students aged between 7-11 looking for cross-curricular stimulus in the areas of science, design, technology, literacy or drama.
- Teachers of science, design technology or computing, wishing to find new ways to engage students.
- Teachers of citizenship (or politics and sociology), at secondary level, looking for an engaging context through which to introduce complex ideas.

Each activity has been designed for

Lab 47-04

- In the **CEHv6 Labs CD-ROM** navigate to **Module 47**
- Open the **Stop the Corporate Spying.pdf** and read the content



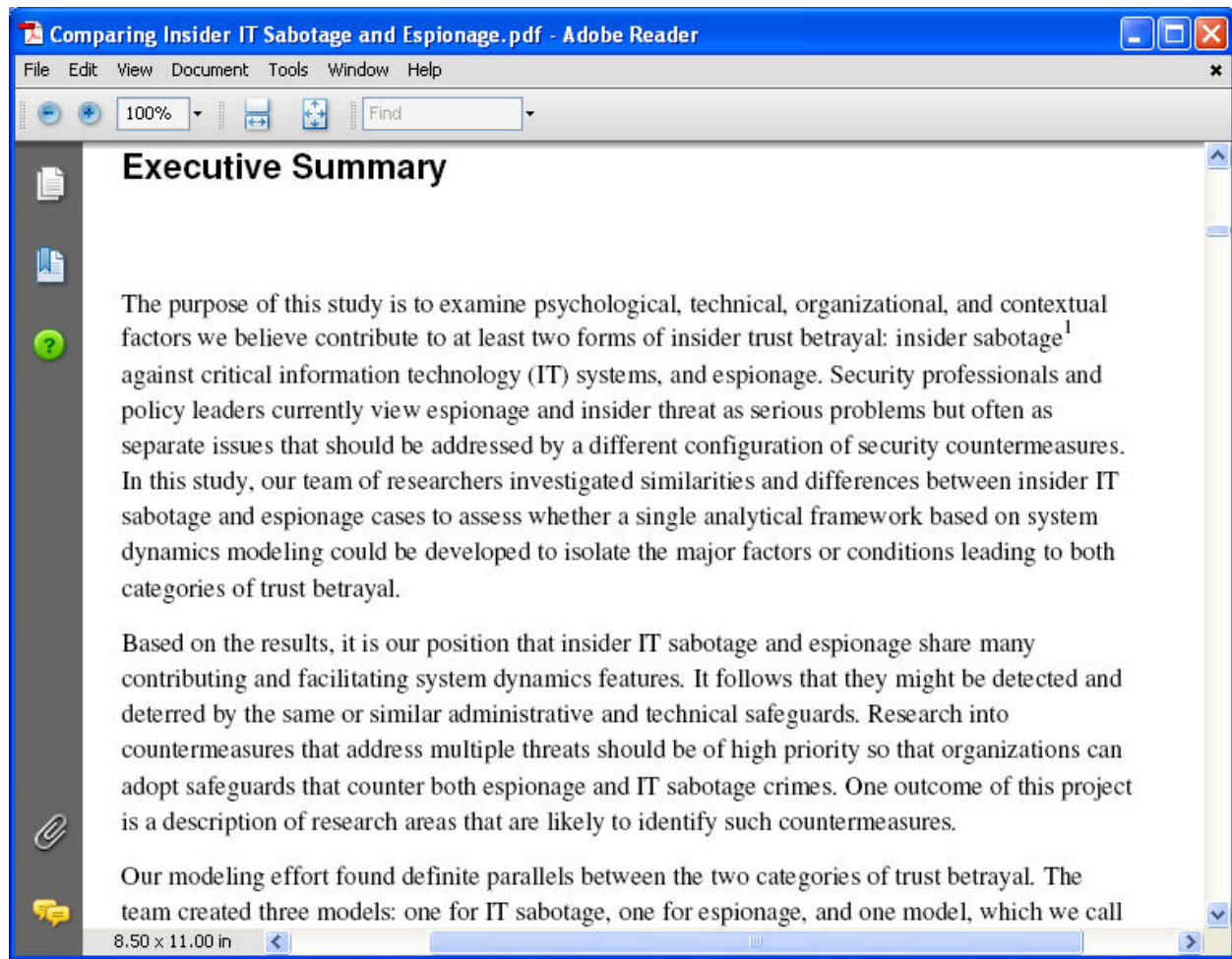


Module 48

Corporate Espionage- Hacking Using Insiders

Lab 48-01

- In the **CEHv6 Labs CD-ROM** navigate to **Module 48**
- Open the **Comparing Insider IT Sabotage and Espionage.pdf** and read the content



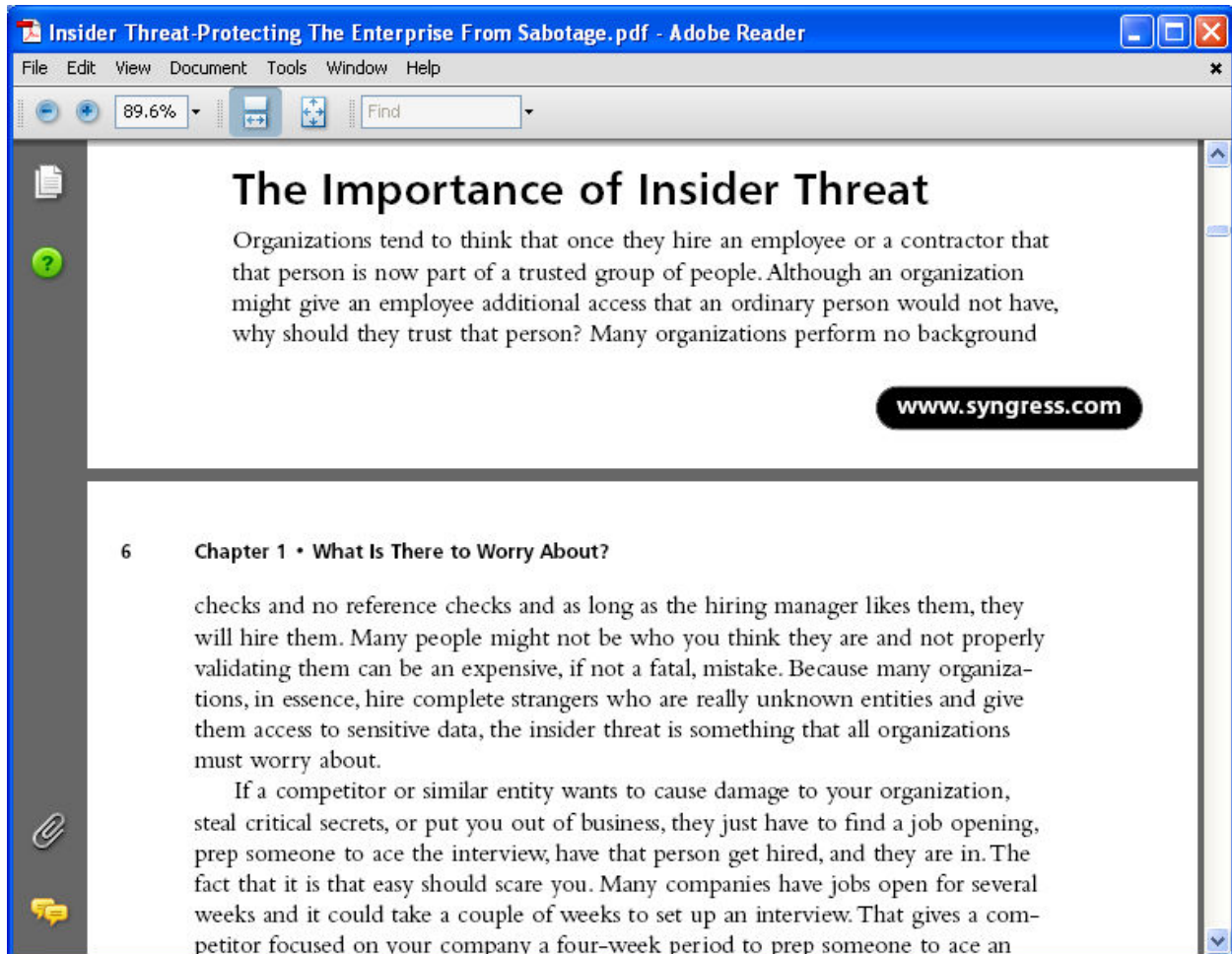
Lab 48-02

- In the **CEHv6 Labs CD-ROM** navigate to **Module 48**
- Open the **The Insider Threat.pdf** and read the content



Lab 48-03

- In the **CEHv6 Labs CD-ROM** navigate to **Module 48**
- Open the **Insider Threat-Protecting The Enterprise From Sabotage.pdf** and read the content



Lab 48-04

- In the **CEHv6 Labs CD-ROM** navigate to **Module 48**
- Open the **Corporate Espionage.pdf** and read the content

Corporate Espionage.pdf - Adobe Reader

File Edit View Document Tools Window Help

73.8% Find

Spy-Ops Training Brief

Volume 0, Brief 0
March 2005

Corporate Espionage

CONTENTS:	
Abstract	1
Objectives	1
Brief	1-8
Key Words	2
Glossary	3-4
Summary	8
References	8
Exam	9
On-line Exercise	10

Objectives:

Abstract

Corporate espionage is the dirty little secret of global business. Espionage activities are often masked under the title of competitive intelligence. But in the end, thieves or spies still acquire sensitive, restricted information assets of another entity, which may include product designs, business models, marketing plans, research and development files, customer lists, employee lists, pricing strategies and other intellectual property.

This module will provide a basic understanding of the current state of corporate espionage, as well as illustrate many techniques used in committing this new type of crime.



Brief