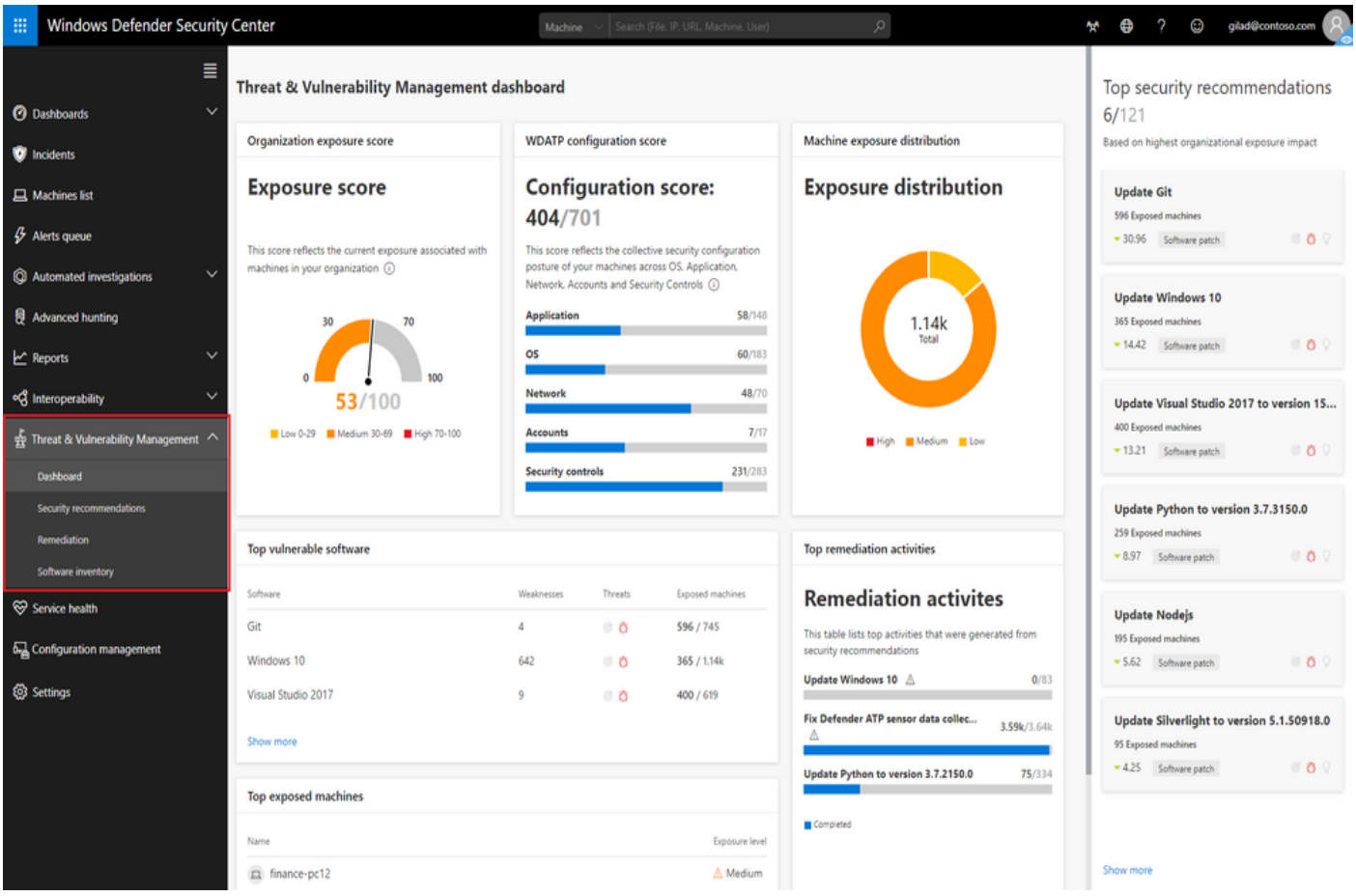
EXPERIMENT NO 1

Windows Defender

AIM: To Prevent PC against latest threats using Windows Defender.

Windows Defender Advanced Threat Protection (now rebranded as Microsoft Defender for Endpoint) is a post-breach solution that detects, investigates, and responds to security threats on your network. Microsoft Defender for Endpoint keeps your network secure by continuously evaluating and identifying existing weaknesses in your system, addressing security concerns, and investigating security attacks that take place. It is important to note that Microsoft Defender for Endpoint is not an anti-virus product (and cannot be substituted for one), but a post-breach solution that complements the capabilities of anti-virus solutions. Microsoft Defender for Endpoint is designed to help you after your network security has been breached.

Threat and vulnerability management



Windows Advanced Threat Protection consistently performs real-time analysis on endpoints. It retains visibility over all software in a device. It is constantly working on identifying and assessing any security vulnerabilities that might exist in any of the applications on your device.

With Windows Defender Advanced Threat Protection, you can see your overall exposure score, vulnerable software and machines in your network, and what you can do to remediate the issues.

When it discovers any weakness or vulnerability in any device, it promptly alerts you and provides recommendations to remediate it.

Attack surface reduction

We can reduce the risk of a potential threat by minimizing areas where cyberattacks can take place. This can be done through various controls put in place by Windows Defender for Endpoint, such as only allowing applications marked as 'trusted' to run on the device, allowing you to restrict certain behaviors in files and applications, as well as preventing untrusted websites, applications and files from accessing all areas in the device.

Next generation protection

Windows Defender for Endpoint leverages Microsoft's sophisticated technology and ongoing research in machine learning and threat resistance to provide you with behavior-based antivirus protection, cloud-delivered blocking, and constant product updates.

Endpoint detection and response

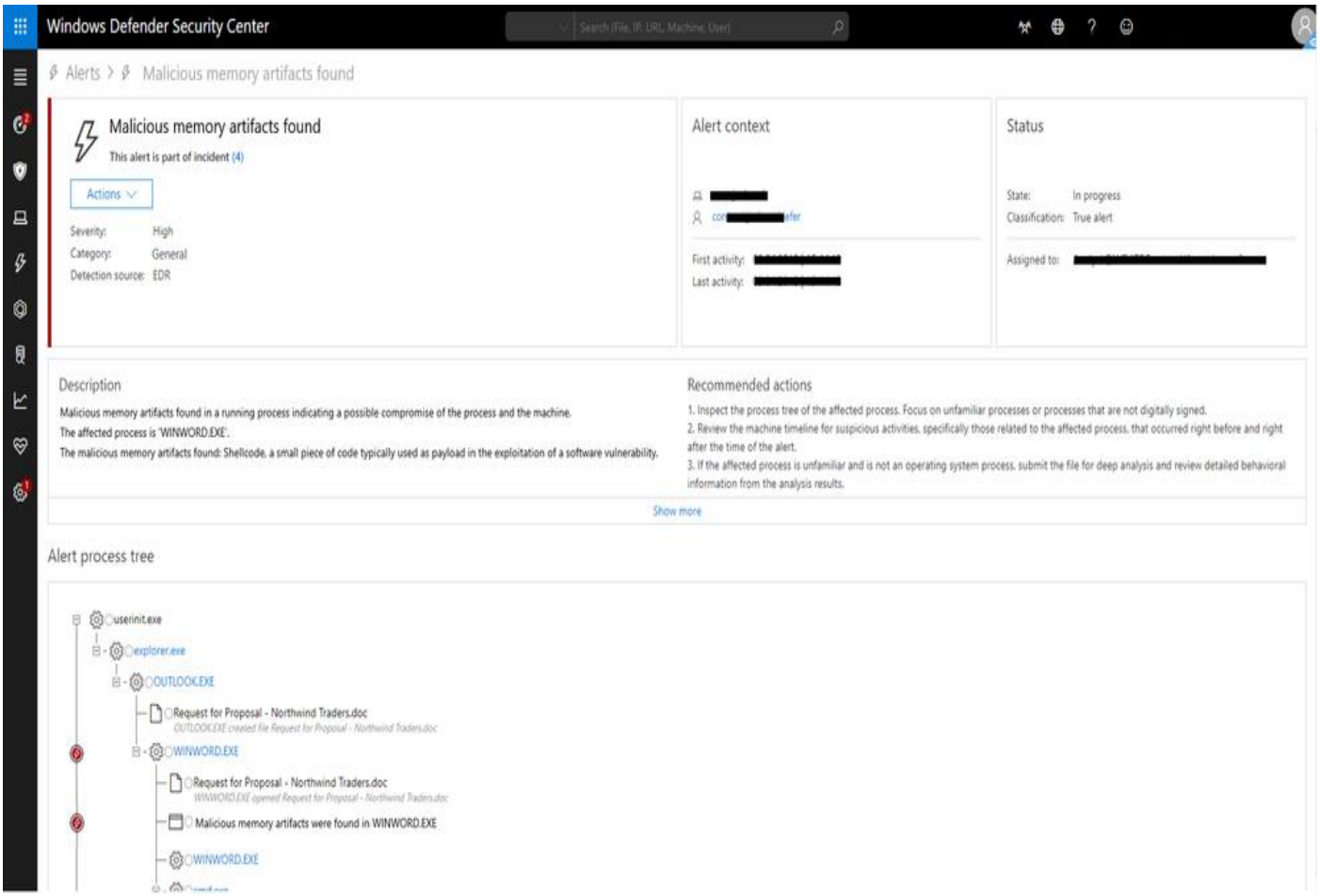
Being a post-breach solution, Windows Defender Advanced Threat Protection offers endpoint detection and response (EDR) capabilities that identify and warn you about suspicious activities.

Once suspicious activity is detected in your network, you will immediately be alerted and provided with data to investigate the threat and make an informed decision about your next steps.

The Defender for Endpoint dashboard gives you access to in-depth data and analysis of different aspects of your security system from a centralized portal.

The endpoint detection and response in Windows Defender for Endpoint primarily consist of the following features and capabilities:

- **Alerts:** When a threat is detected, you will instantly receive an alert in your dashboard, along with basic information such as what the threat is, which device it has been found in, how severe it is, etc.
- **Investigation:** Your security team can investigate the threat further through features such as a timeline of events, which gives you a complete history of the threat since it arrived in your system, along with the list of machines that it has infected.
- **Remediation:** You will also be provided with a set of recommended next steps based on the behavior of the threat, and you can choose which action you would like to take.



Observation : Thus, Windows Defender has been successfully analyzed.

EXPERIMENT NO 2

Microsoft Security Essentials

Aim: To Protect PC using Microsoft Security Essentials.

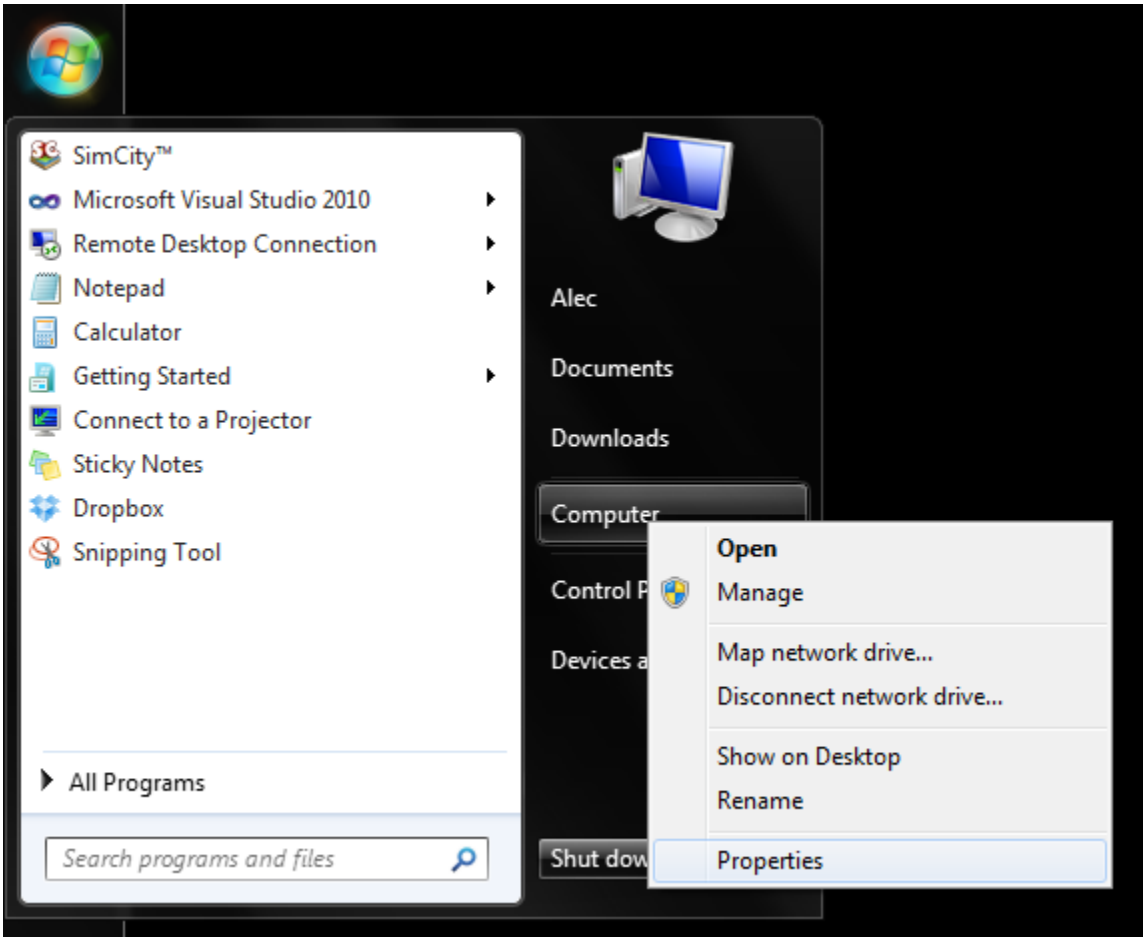
Description

To install Microsoft Security Essentials on Windows 7, follow these steps.

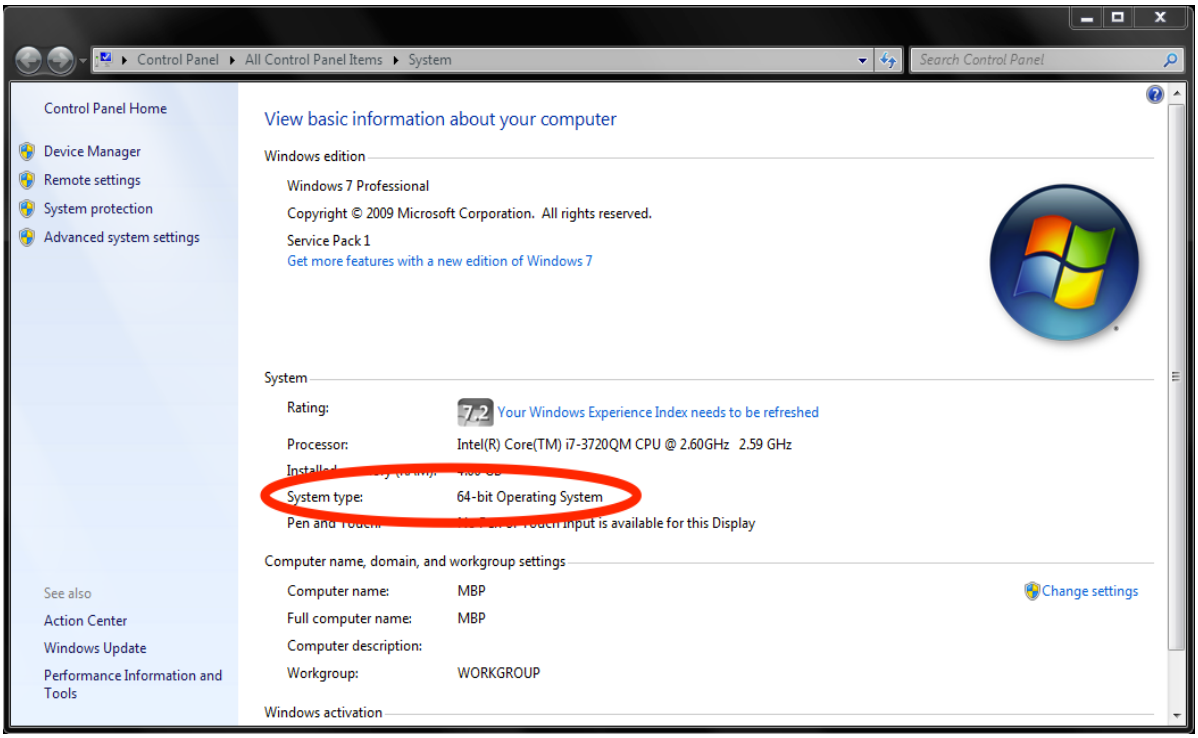
Instructions

Identify If You Have a 32-bit or 64-bit Version

1. Open the System Properties by selecting the Start button, right-clicking Computer, and then selecting Properties.



2. Under the System heading, you can view the system type.



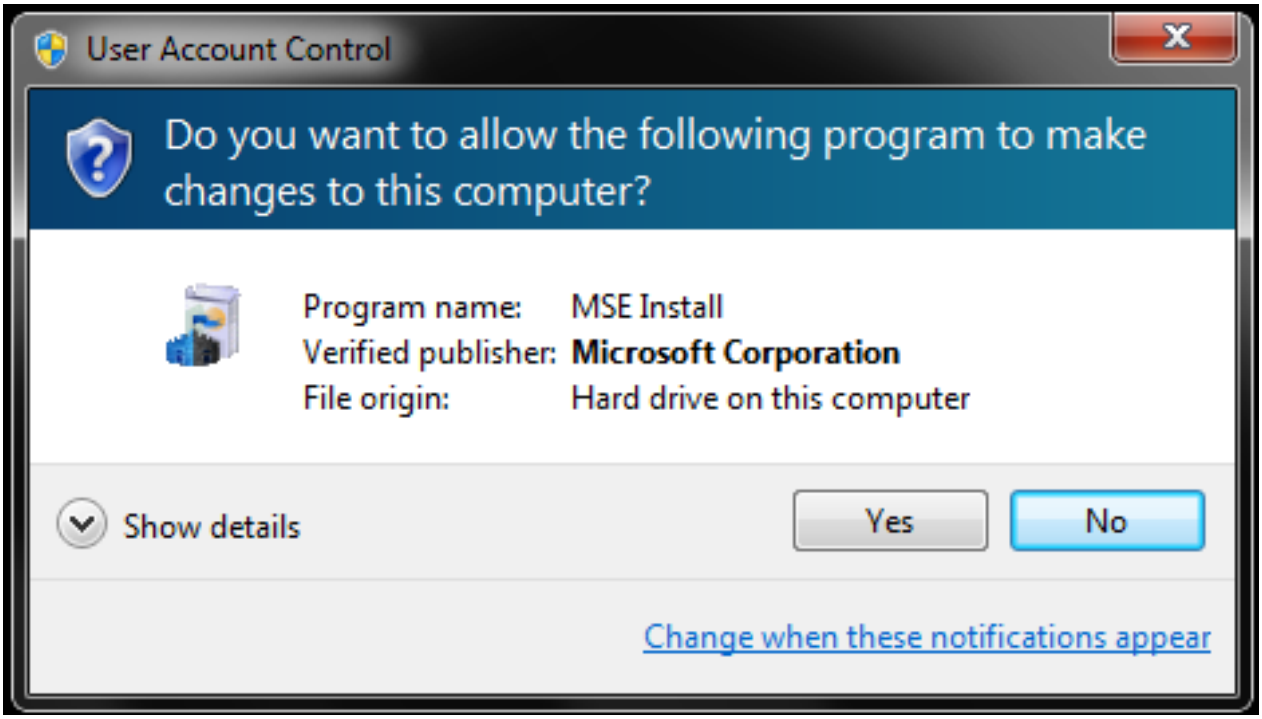
Install Security Essentials

Once you have determined which operating systems version you have installed, download and install the corresponding version of Microsoft Security Essentials.

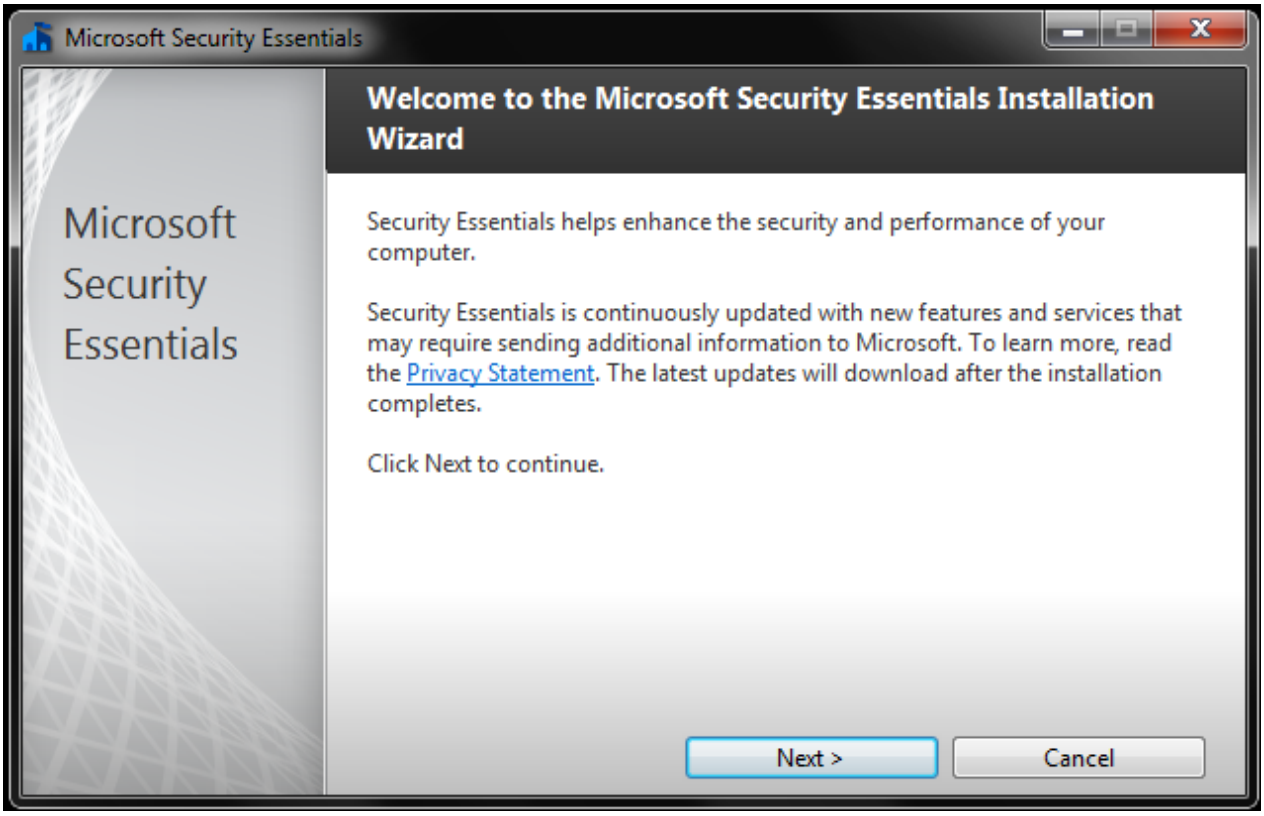
1. Download Microsoft Security Essentials from the Microsoft site.

- If your computer is running a 64-bit operating system, download the ENUS\amd64\MSEInstall.exe option.
- If your computer is running a 32-bit operating system, download the ENUS\x86\MSEInstall.exe option.

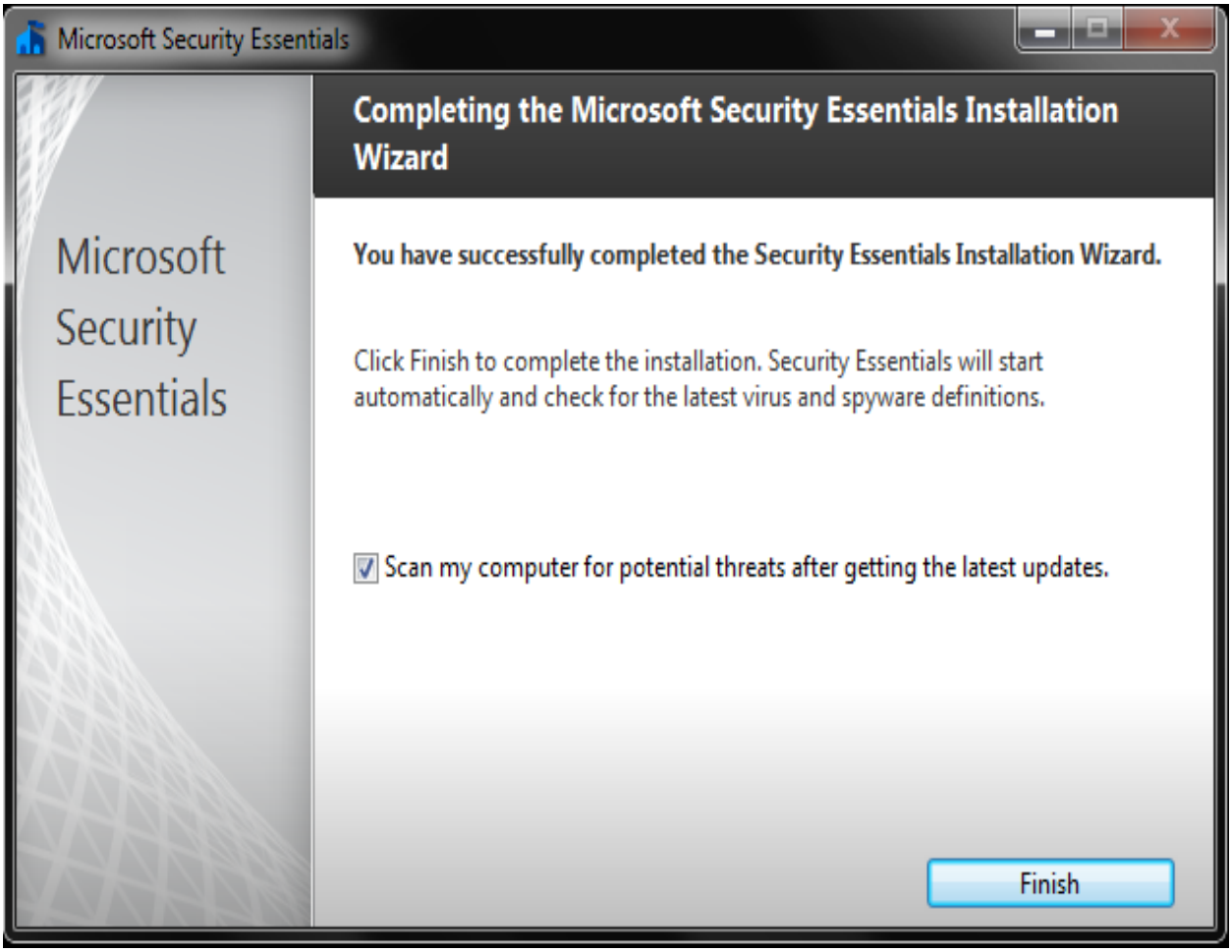
2. Once the download finishes, double-click the file to run the installer. You may get a pop-up box asking you to "allow the following program to make changes to this computer." Select Yes.



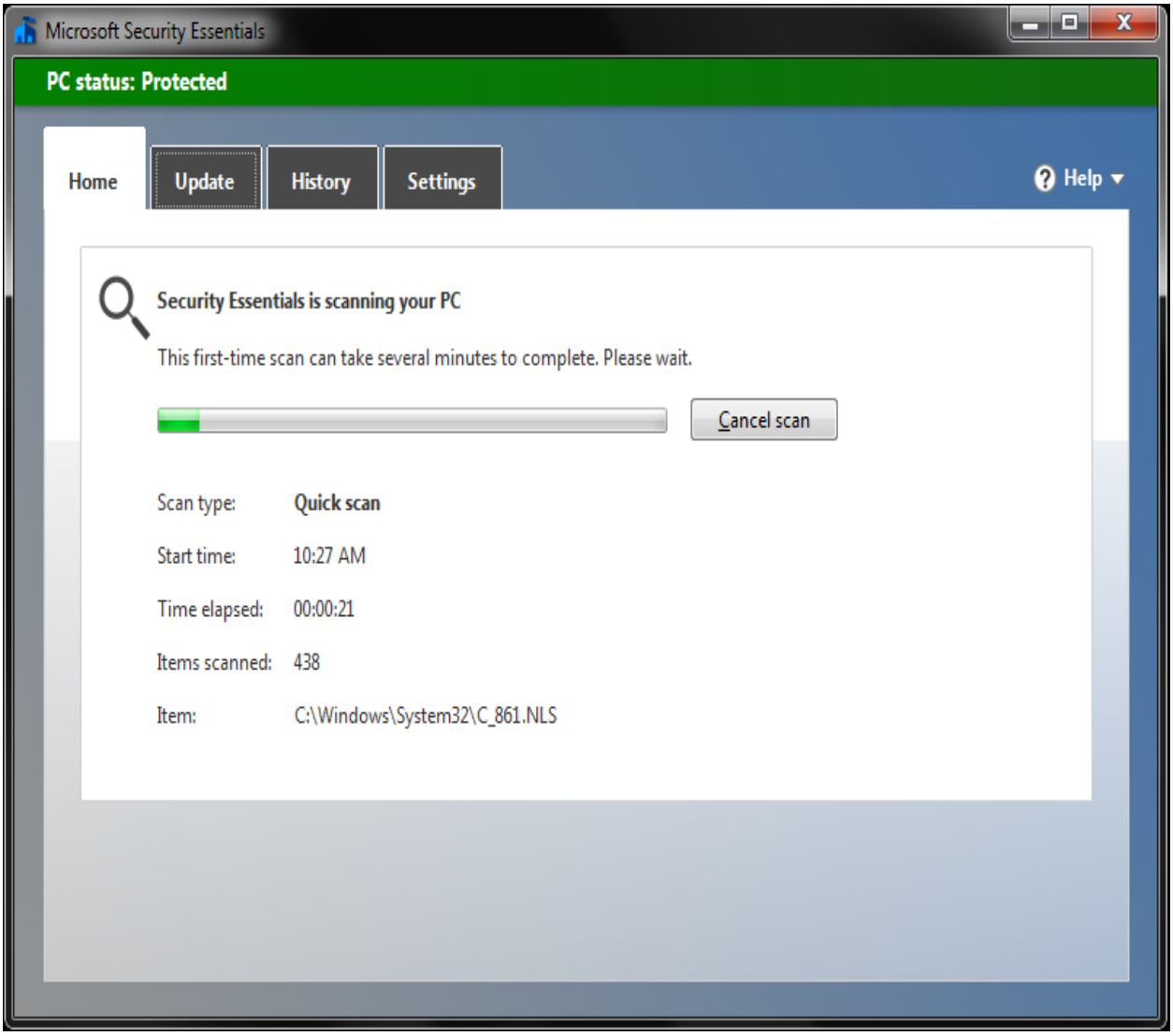
3. Once the installer extracts and runs, select Next



- Read through the Software License Terms, and select I Accept.
- Select Join the Customer Experience Improvement Program and then Next.
- Check the box for If no firewall is turned on, turn on Windows Firewall and select Next.
- Confirm that you don't have any other anti-virus programs installed, then select Install.
- When the program successfully installs, you should see the message, You have successfully completed the Security Essentials Installation Wizard.



9. Select Finish, and allow Microsoft Security Essentials to perform an initial scan of your computer.



Observation: Microsoft Security Essentials scanned for virus and protect the system from intruders

EXPERIMENT NO 3

XIAO STEGANOGRAPHY

Aim: To hide the secret data from unauthorized users in order to prevent confidentiality, integrity and availability of data.

XIAO STEGANOGRAPHY

Xiao Steganography is a tool which is used to hide the secret data from unauthorized users in order to prevent confidentiality, integrity and availability of data. .Xiao Steganography is free software that can be used to hide secret files in BMP images or in WAV files. Usage of this tool is easy, as it can be downloaded and used. Any BMP image or WAV file can be added to its interface. Then the file, which we want to hide, is added. Xiao also supports encryption. We can select from various algorithms like RC4, Triple DES, DES, Triple DES 112, RC2 and hashing SHA, MD4, MD2, MD5.

To read the hidden message from this file, we will have to use this software again. This software will read the file and will decode the hidden file from it. But we extract the hidden file from any other software other than Xiao, as it has been hidden or encrypted using Xiao only.

Following are the various steps that show encoding and decoding as achieved by Xiao:

A. Encoding/Encrypting using Xiao

1) Open Xiao tool to implement Steganography, as shown in Fig. 1. This is the first snapshot when the tool is opened after being downloaded.

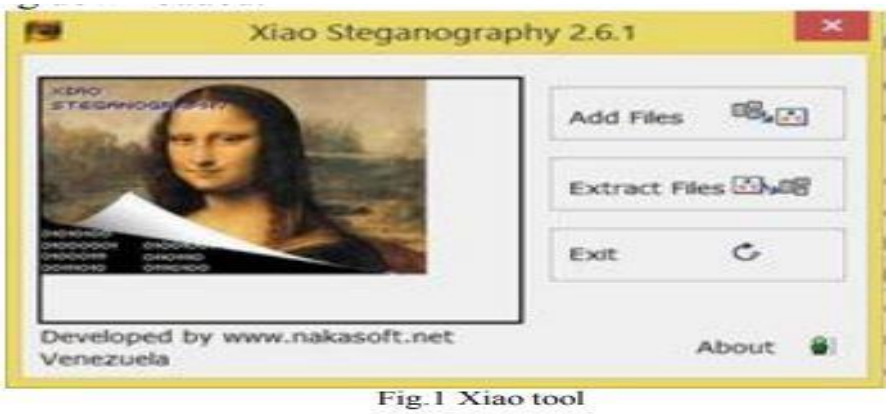


Fig.1 Xiao tool

2) As shown in Fig. 2, cover image or the target file, as popularized by Xiao is selected. For this the Load Target File option should be clicked.

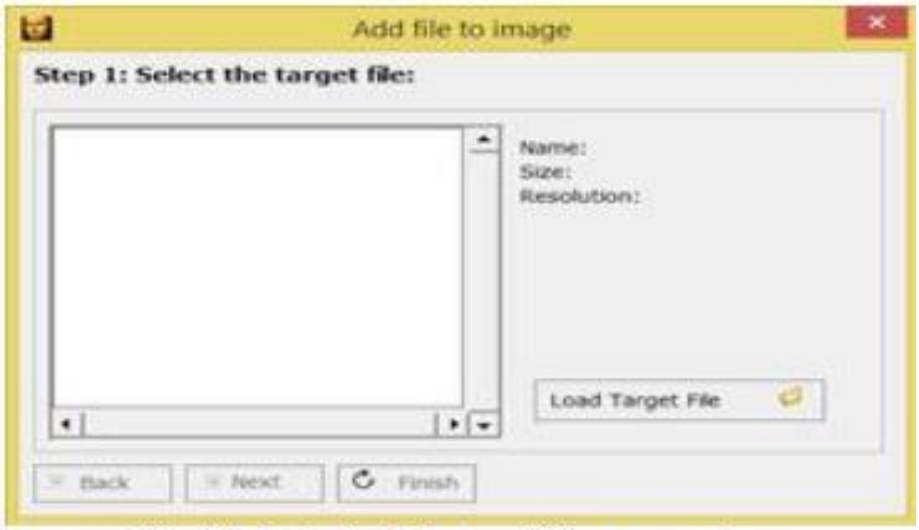


Fig. 2 Select to load the target file or cover image

3) Fig. 3 depicts out target image. The secret message will be embedded in this target file. Select this target file to conceal our secret data.

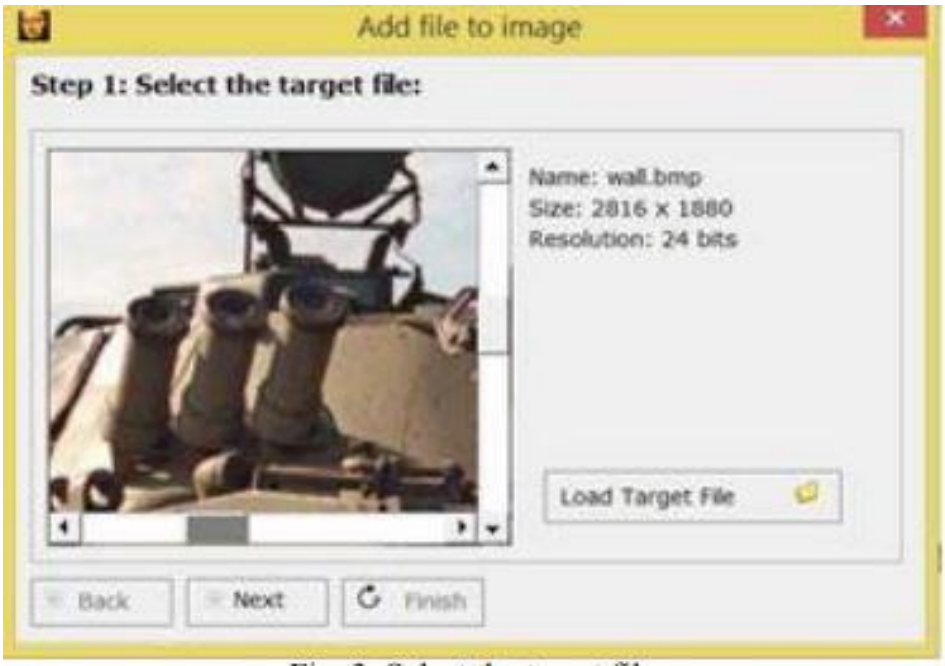


Fig. 3 Select the target file

4) By selecting on Add File button in Fig. 4, we will be able to select our Secret file or confidential data, which will be embedded in our target file. The remaining size is mentioned in KB. This suggests the size available to add the secret data in the form of files.

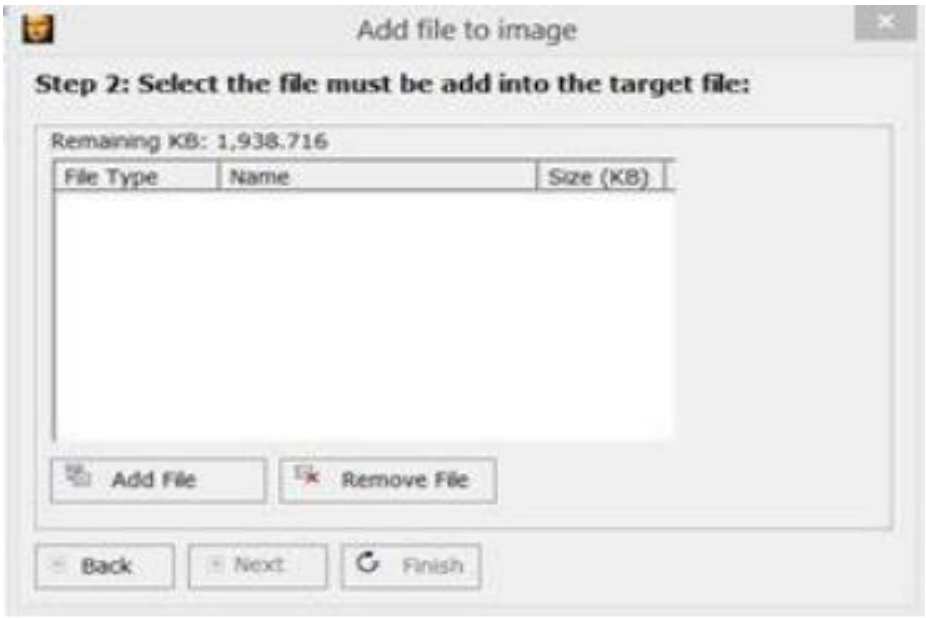


Fig. 4 Select the file to be added into the target file

5) Fig. 5 shows that we are hiding an image called Koala. Further files can be embedded using the Add File option.

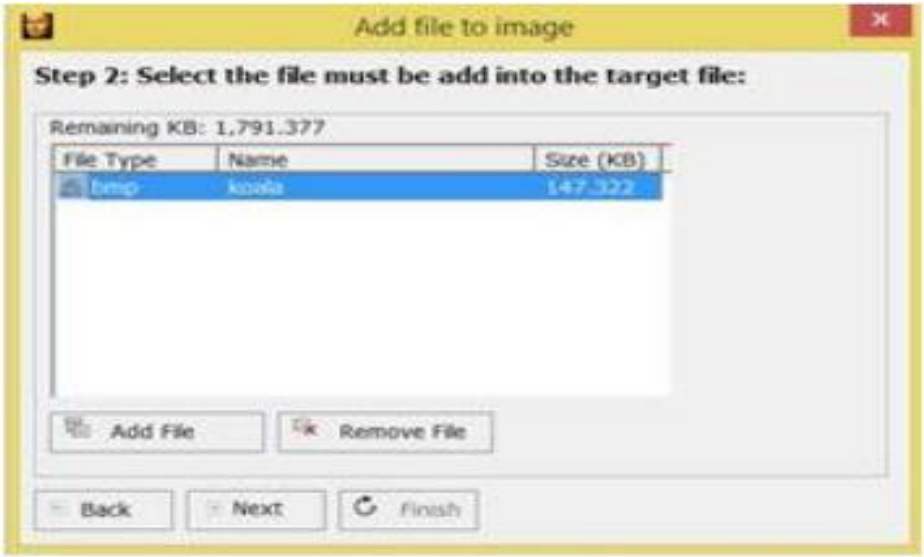


Fig. 5 Secret File added

6) In Fig. 6, we need to select the encryption option and a password to provide double security of our confidential message/image. There are four hashing algorithms and five encryption algorithms available as depicted below:

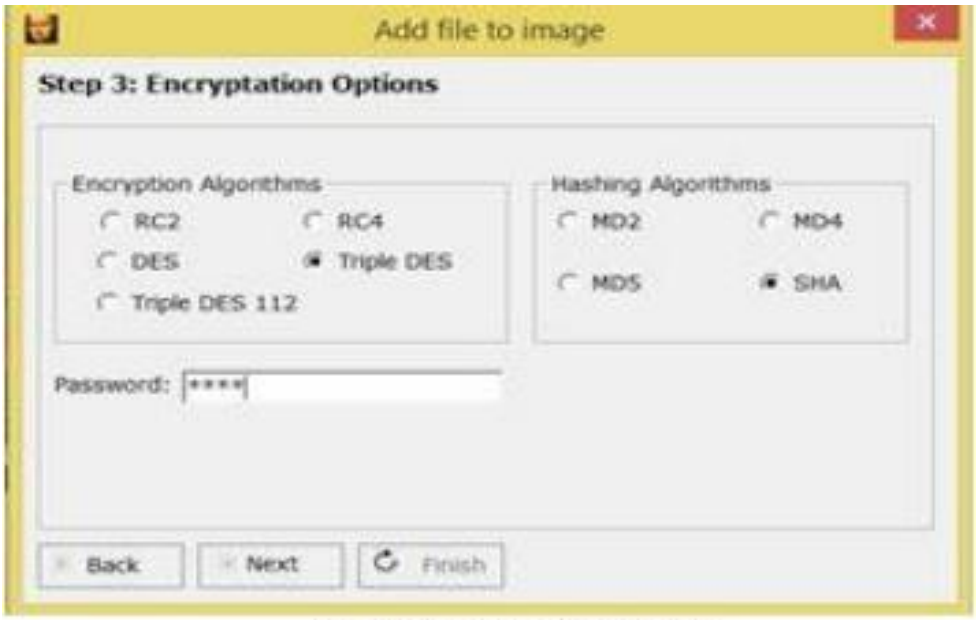


Fig. 6 Select the algorithms

7) After applying the appropriate encryption algorithm and a strong password on our secret message, we can embed it in our target files as shown in Fig. 7. This snapshot depicts a progress bar exhibiting the merging of both the files i.e. Target File or Cover Image and our Secret image.

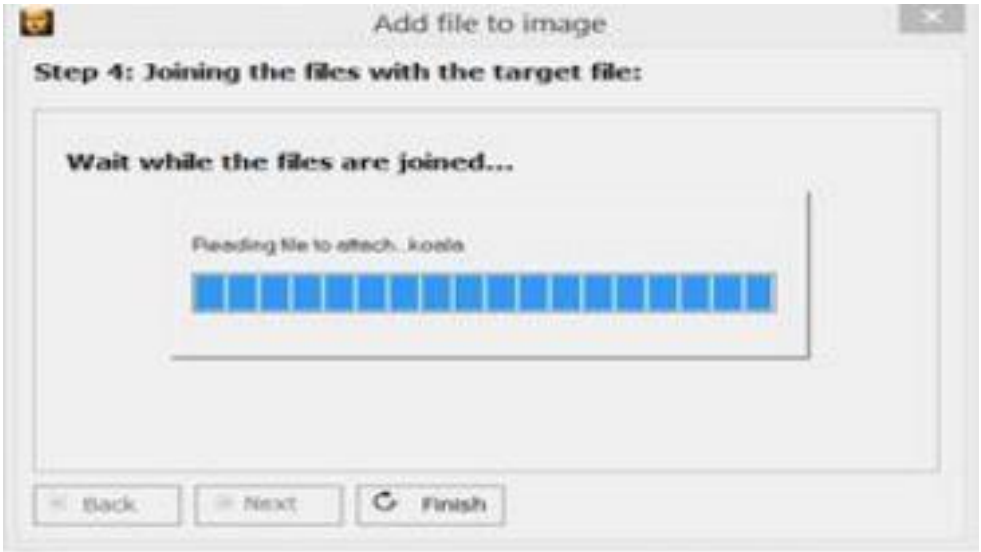


Fig. 7 Joining the files with the target file

8) All the above seven steps accord with embedding process and Fig. 8 shows that steganography was successfully accomplished.

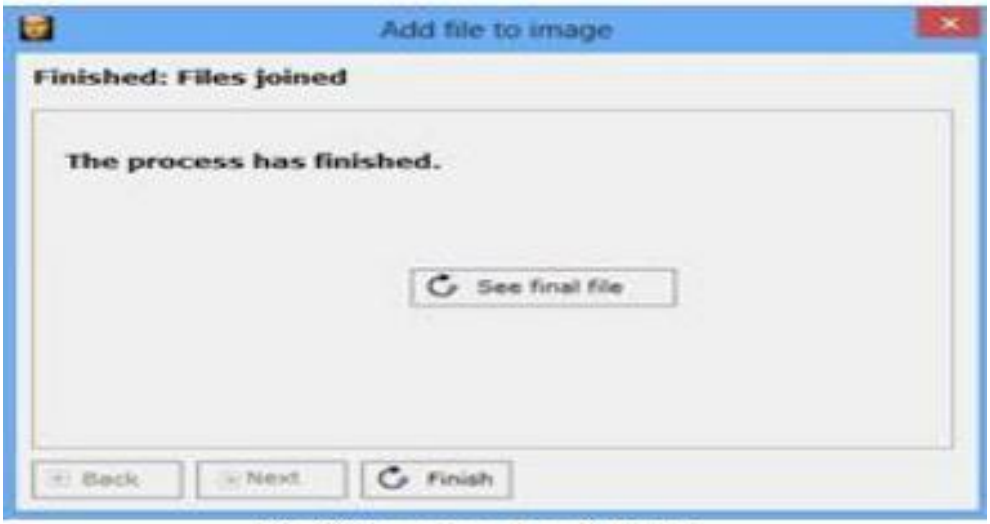


Fig. 8 The process has finished

B. Encoding/Decrypting using Xiao 1) Now at the decoding end, if an authenticated user wants to extract the secret message from the target file or the cover image, then receiver needs to click on the Extract file option as shown in Fig. 9

Fig. 9 Xiao tool – Extracting Files

2) In Fig. 10, we need to select Source file. This is the same target file or cover image which was used for encoding the confidential data.

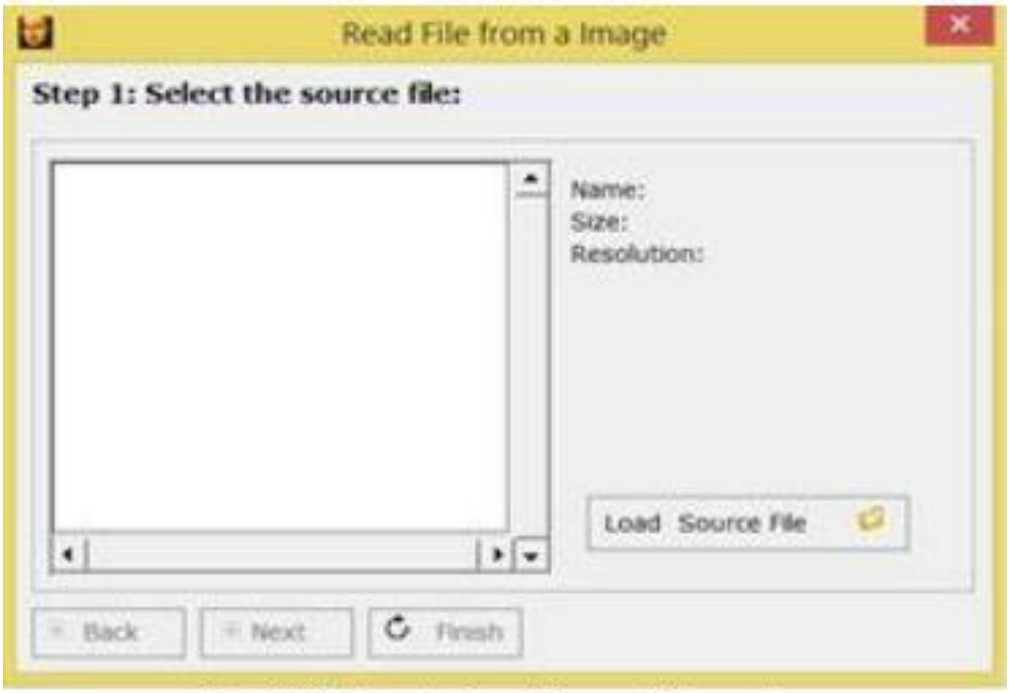


Fig. 10 Select the Load Source File option

3) Fig. 11 shows the Cover Image or the target file. By clicking on Extracting Load file, we can extract our secret koala file.

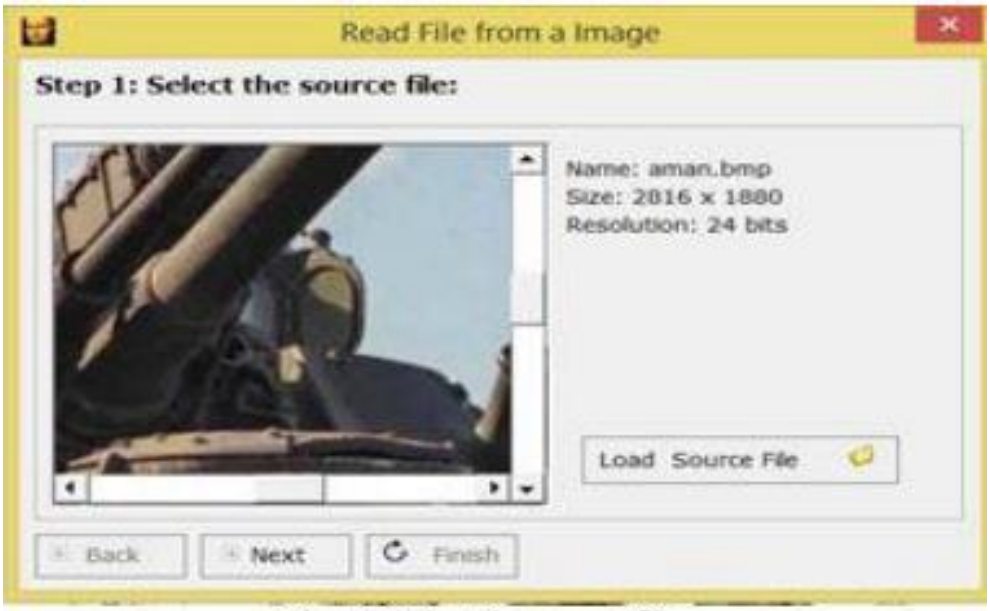


Fig. 11 Select the source file

4) Fig. 12 depicts our embedded target file ready for decryption

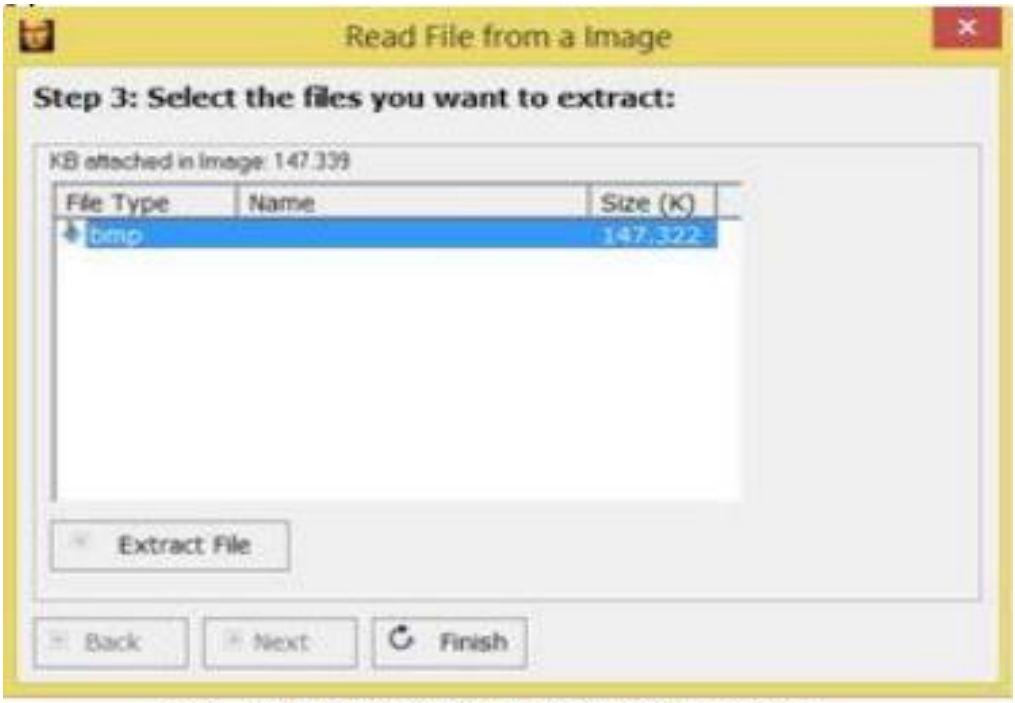


Fig. 12 Targert File to be decoded/decrypted

5) Here we can easily see our secret image koala which we embedded. This secret image is the actual message intended for the recipient which could be saved at any path using the Save As option as depicted in Fig. 13

Fig. 13 Save as file

6) Fig. 14 shows the secret file had been extracted by the receiver successfully.

Fig. 14 File extract was successful

Observation: This tool hide and retrieve data successfully.

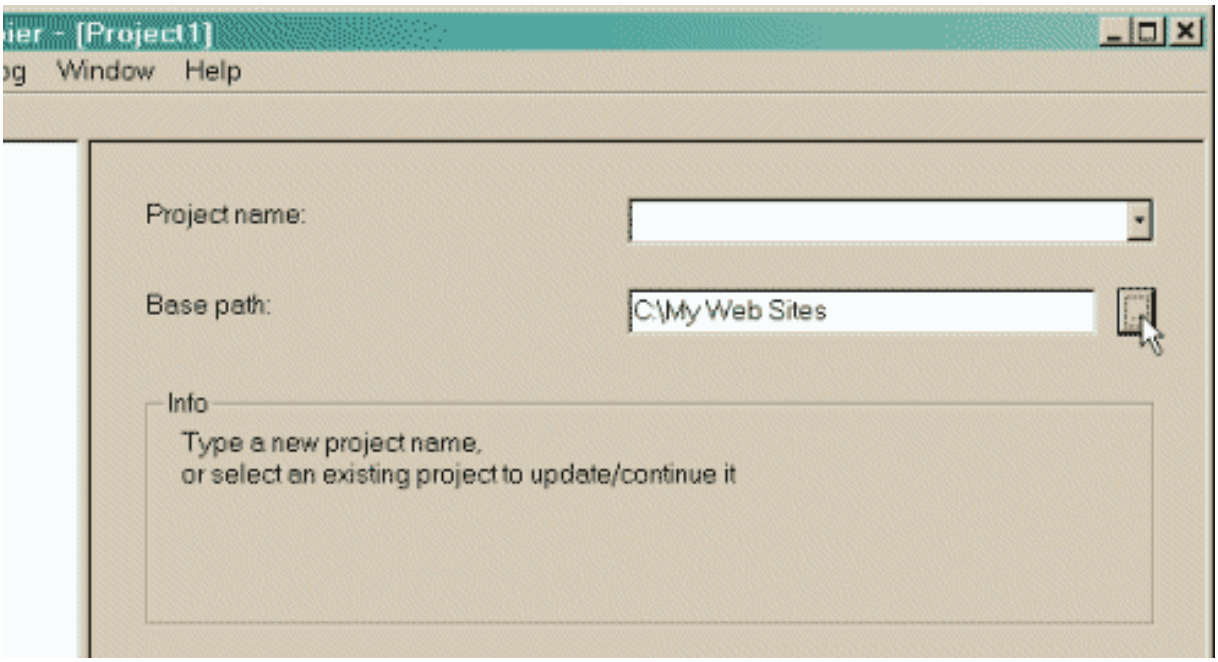
EXPERIMENT NO 4

HTTrack

Aim: To Mirror a Website using HTTrack.

Step 1 : Choose a project name and destination folder

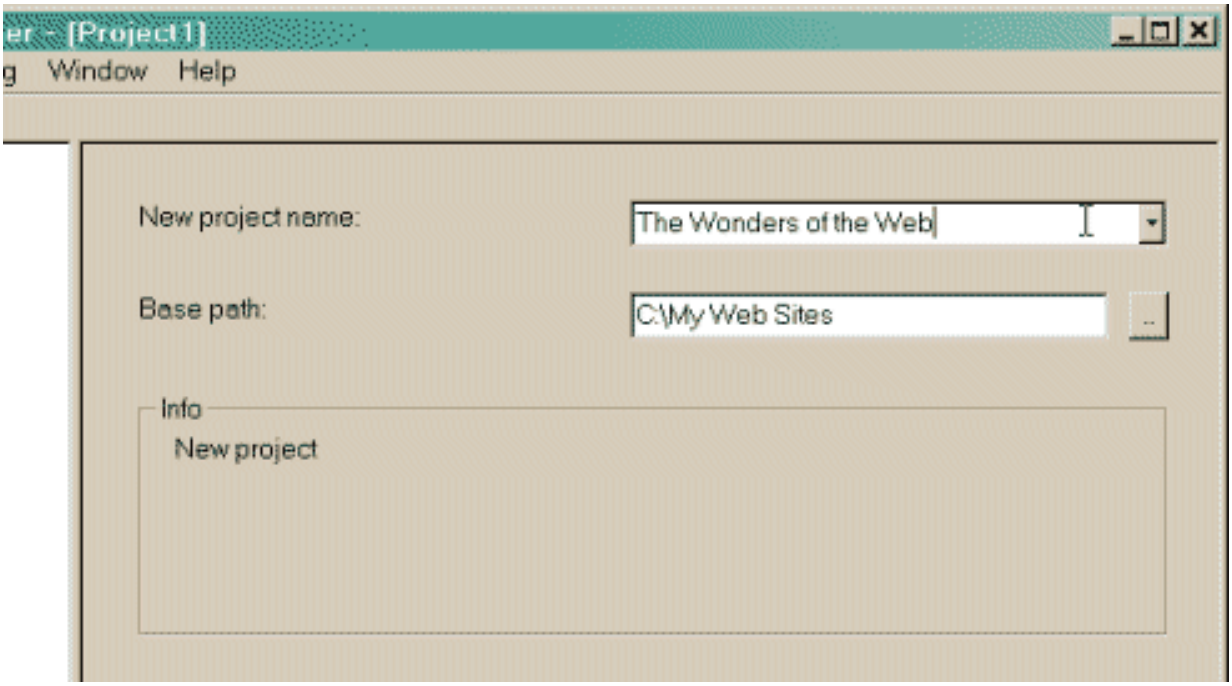
1. Change the destination folder if necessary .It is more convenient to organize all mirrors in one directory, for example My Web Sites. If you already have made mirrors using HTTrack, be sure that you have selected the correct folder.



2. Select the project name:

   Select a new project name

   This name is, for example, the theme of the mirrored sites, for example My Friend's Site.



OR

Select an existing project for update/retry

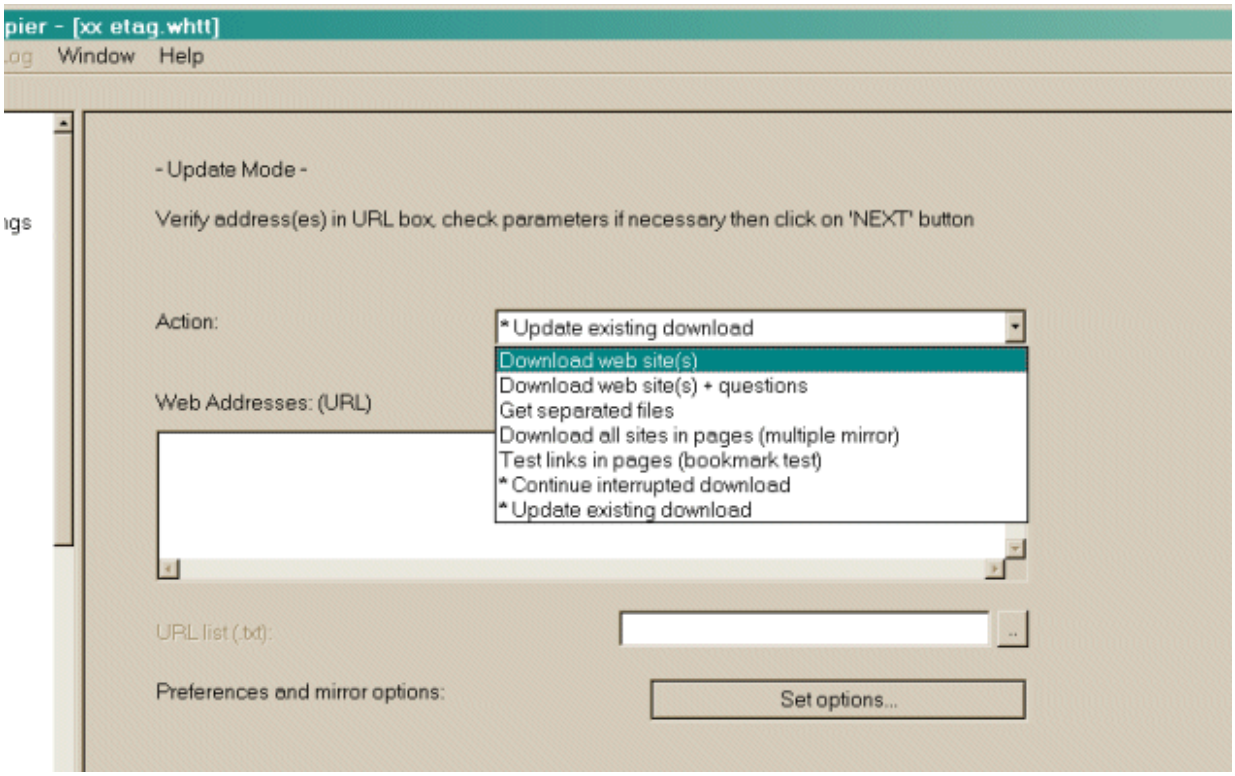
Directly select the existing project name in the popup list.

3. Click on the NEXT button
4. Go to the next step...

Step 2 : Fill the addresses

1. **Select an action**.

   The default action is Download web sites.



- Download web site(s)

  Will transfert the desired sites with default options

- Download web site(s) + questions

  Will transfert the desired sites with default options, and ask questions if any links are considered as potentially downloadable

- Get individual files

  Will only get the desired files you specify (for example, ZIP files), but will not spider through HTML files

- Download all sites in pages (multiple mirror)

  Will download all sites that appears in the site(s) selected. If you drag & drop your bookmark file, this option lets you mirror all your favorite sites

- Test links in pages (bookmark test)

  Will test all links indicated. Useful to check a bookmark file

- Continue interrupted download

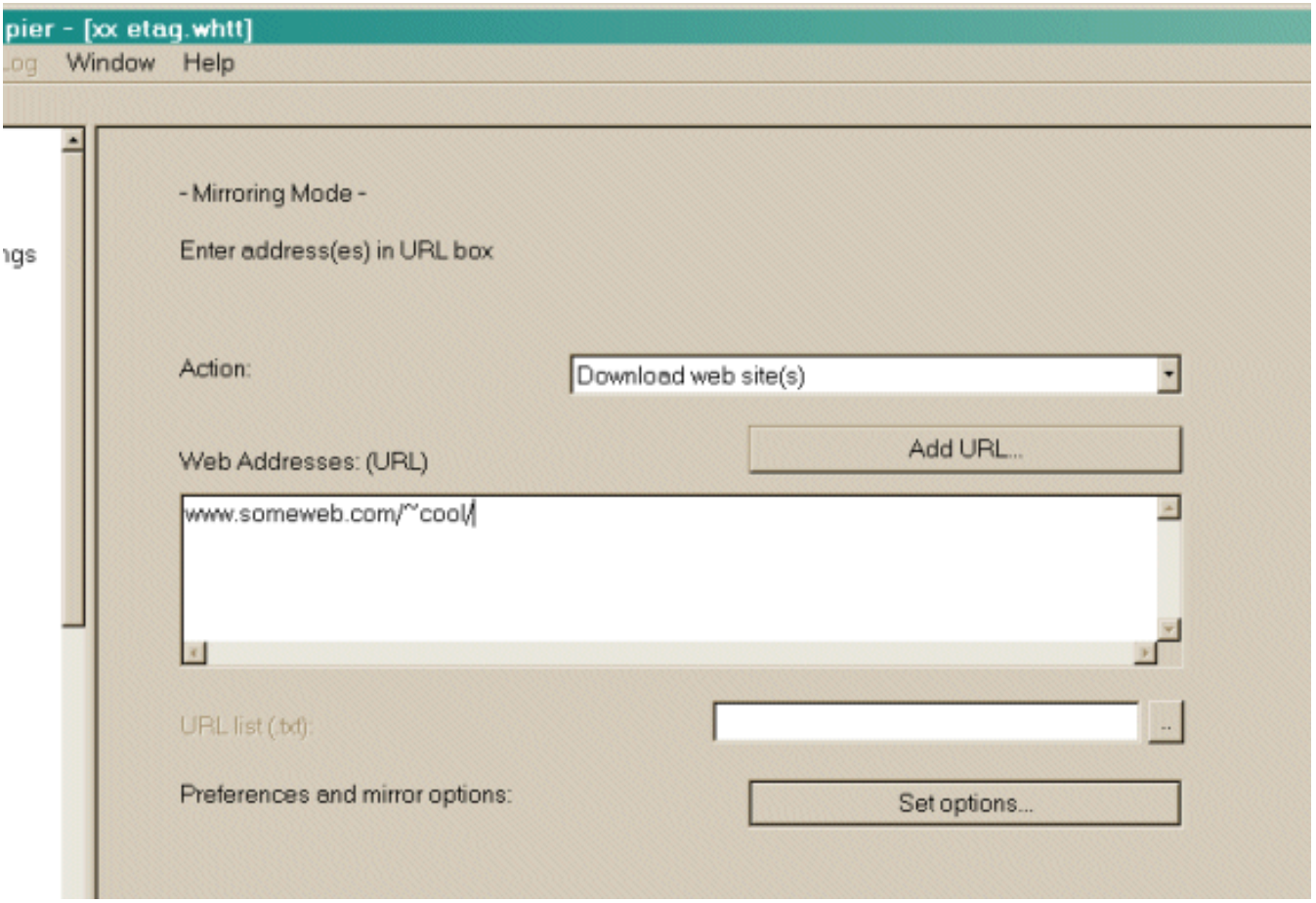
Use this option if a download has been interrupted (user interruption, crash..)

- Update existing download

  Use this option to update an existing project. The engine will recheck the complete structure, checking each downloaded file for any updates on the web site.

2. **Enter the site's addresses**

   You can click on the Add a URL button to add each address, or just type them in the box



3. You may define options by clicking on the Set options button

   You can define filters or download parameters in the option panel

4. You may also add a URL by clicking on the Add a URL button

This option lets you define additional parameters (login/password) for the URL, or capture a complex URL from your browser.

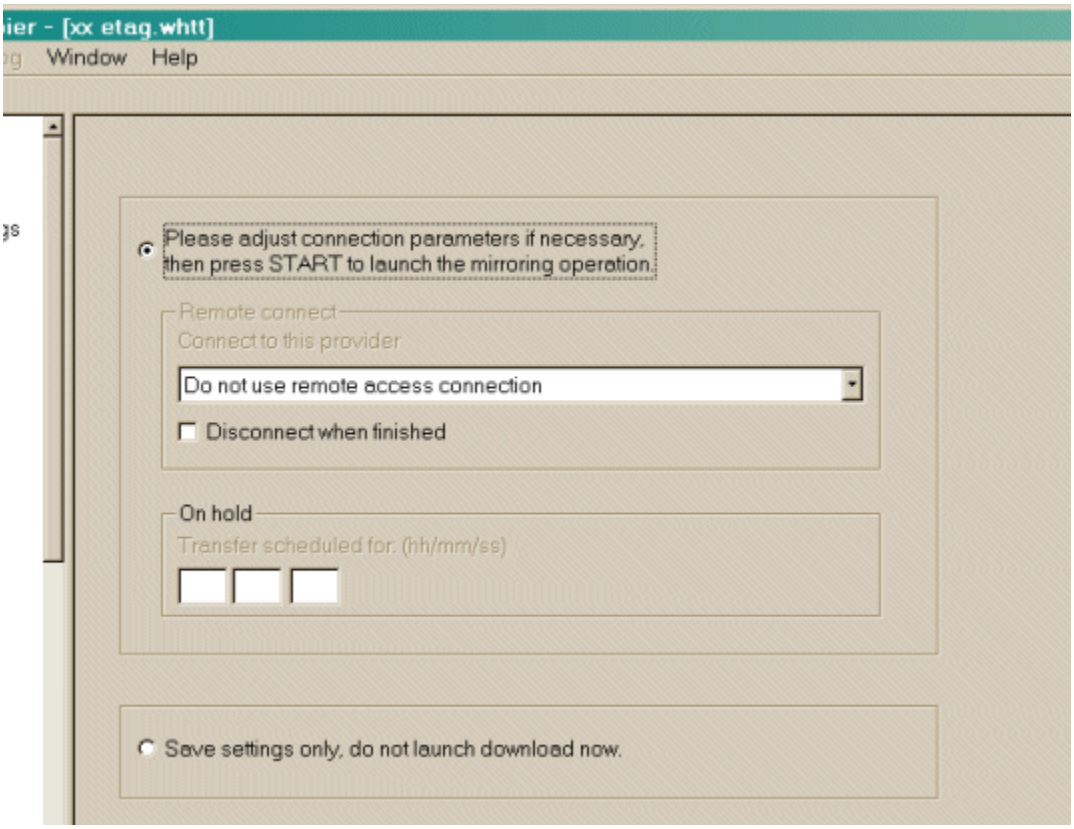
5. Click on the NEXT button.
6. Go to the next step...

Step 3 : Ready to start

1. If you want, you may connect immediately or delay the mirror
   If you don't select anything, HTTrack will assume that you are already connected to the Internet and that you want to start the mirror action now

- Connect to this provider
  You can select here a specific provider to connect to when begining the mirror if you are not already connected to the Internet.
- Disconnect when finished
  Click on this checkbox to ask httrack to disconnect the network when mirror is finished.
- Shutdown PC when finished
  Click on this checkbox to ask httrack to shutdown your computer when mirror is finished.
- On Hold
  You can enter here the time of the mirror start. You can delay up to 24 hours a mirror using this feature.

2. **Click on the FINISH button**



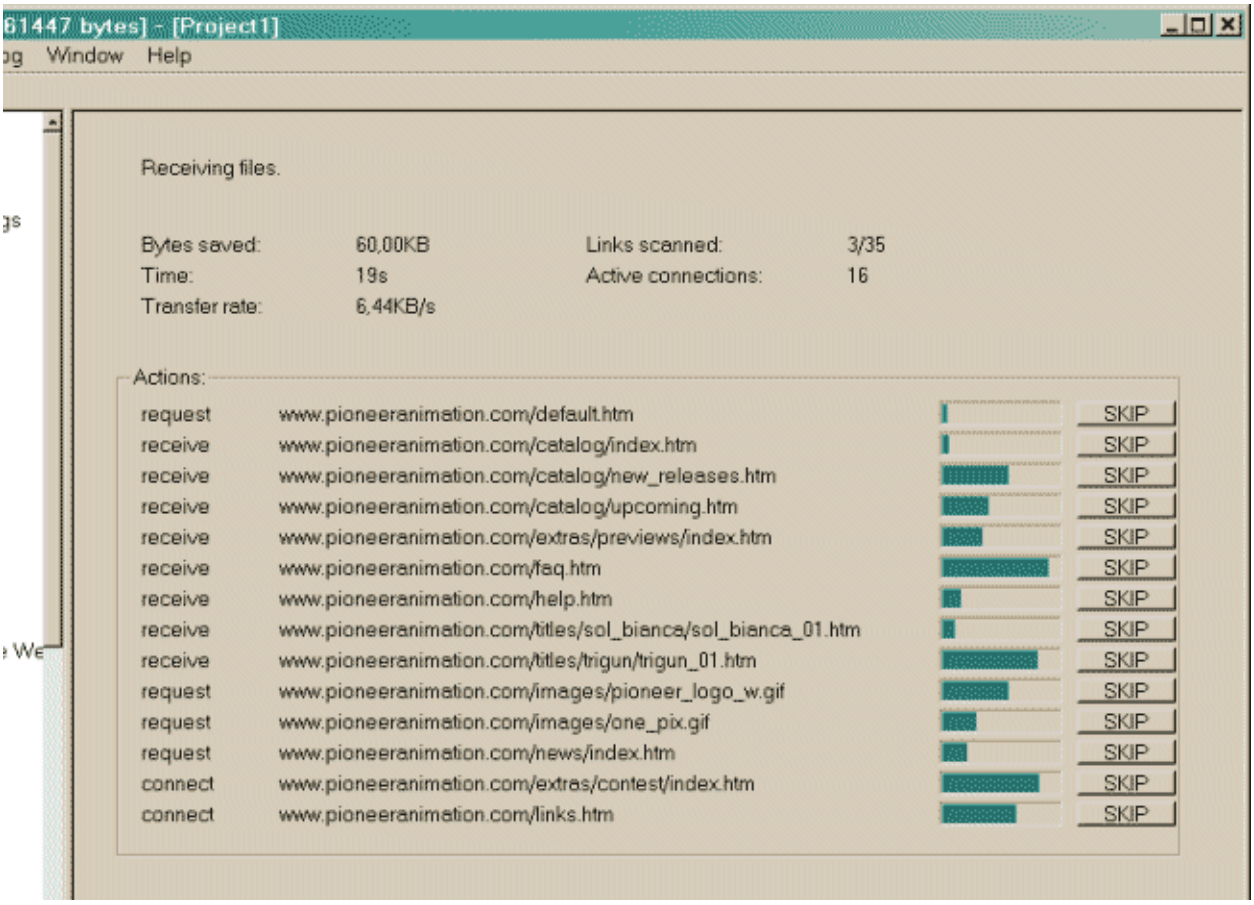
3. **Go to the next step...**

Step 4 : Wait!

1. Wait until the mirror is finishing

   You can cancel at any time the mirror, or cancel files currently downloaded for any reasons (file too big, for example)

   Options can be changed during the mirror: maximum number of connections, limits...

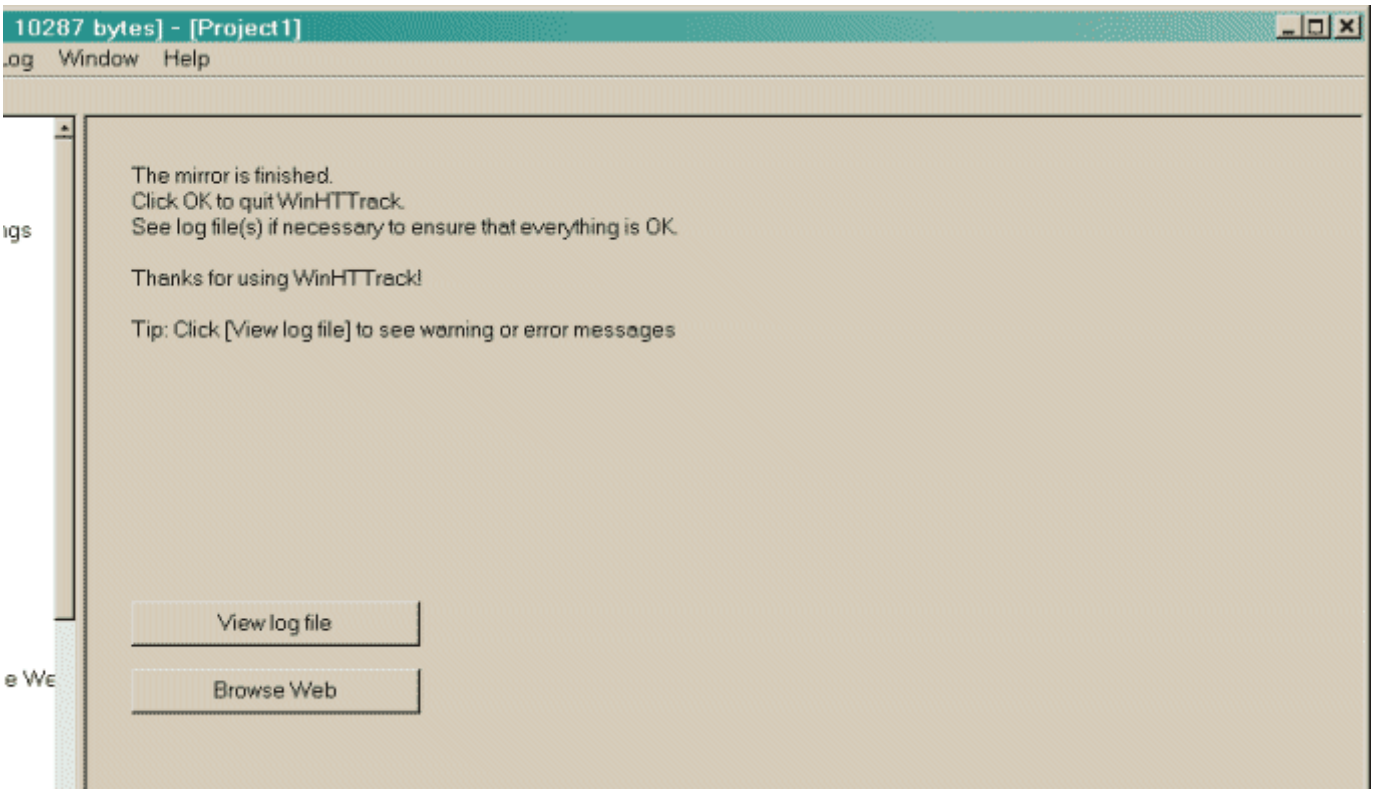


2.Go to the next step...

Step 5 : Check the result

1. Check log files

   You may check the error log file, which could contain useful information if errors have occurred

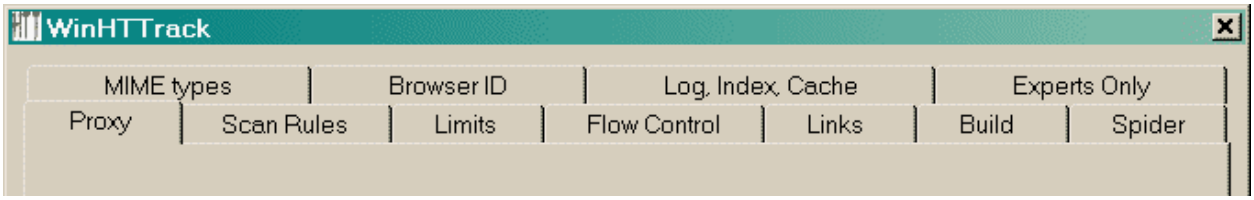


2. See the troubleshooting page

Option panel

Click on one of the option tab below to have more information's

Each option tab is described, including remarks and examples



Observation: Thus, HTTrack has been successfully analyzed and Website is Mirrored

EXPERIMENT NO 5

WIRESHARK

Aim: To analyze the packets of a network.Wireshark is a network packet analyzer.

A network packet analyzer will try to capture network packets and tries to display that packet data as detailed as possible. You could think of a network packet analyzer as a measuring device used to examine what's going on inside a network cable, just like a voltmeter is used by an electrician to examine what's going on inside an electric cable(but at a higher level, of course).

In the past, such tools were either very expensive, proprietary, or both. However, with the advent of Wireshark, all that has changed. Wireshark is perhaps one of the best open source packet analyzers available today.

Some intended purposes

Here are some examples people uses Wireshark for:

•Network administrators use it to troubles hoot network problems

•Network security engineers use it to examine security problems

•QA engineers use it to verify network applications

•Developers use it to debug protocol implementations

•People use it to learn network protocol internals beside these examples Wireshark can be helpful in many other situations too.

Features

The following are some of the many features Wireshark provides:

Available for UNIX and Windows.

•Capture live packet data from a network interface.

•Openfilescontainingpacketdatacapturedwithtcpdump/WinDump,Wireshark, and a number of other packet capture programs.

Import packets from text files containing hex dumps of packet data.

•Display packets with very detailed protocol information.

•Save packet data captured.

•Export some or all packets in a number of capture file formats.

•Filter packets on many criteria.

•Search for packets on many criteria.

•Colorize packet display based on filters.

•Create various Statistics.

Wireshark captures packets and lets you examine their contents.

ShowsWiresharkhavingcapturedsomepacketsandwaitingforyoutoexaminethem.

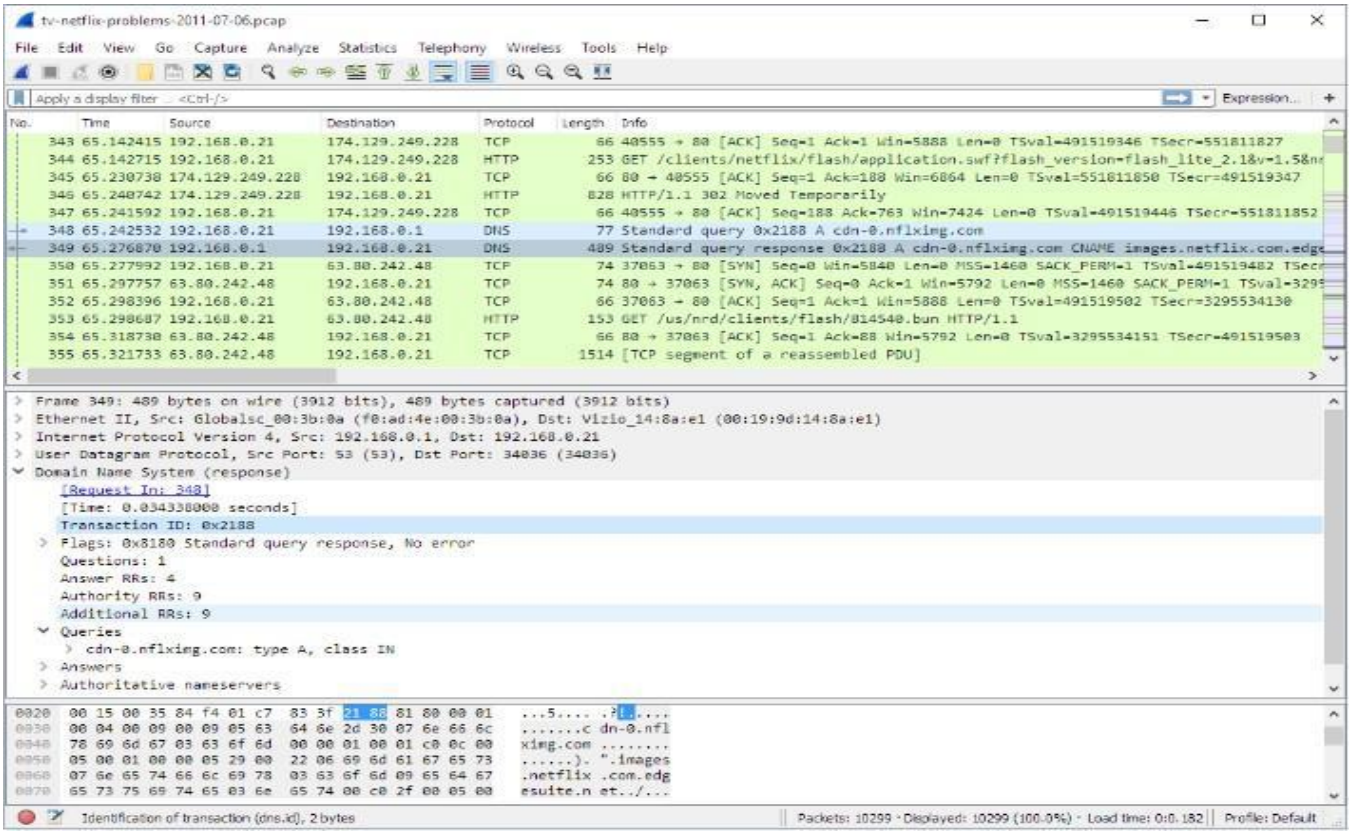


Figure: Wireshark captures packets and lets you examine their contents.

Live capture from many different network media

Wireshark can capture traffic from many different network media types - and despite its name - including wireless LAN as well. Which media types are supported, depends on many things like the operating system you are using. An overview of the supported media types can be found athttps://wiki.wireshark.org/CaptureSetup/NetworkMedia

Import files from many other capture programs

Wiresharkcanopenpacketscapturedfromalargenumberofothercaptureprograms.Foralistofinput formats see Input File Formats.

Export files for many other capture programs

Wireshark can save packets captured in a large number of formats of other capture programs. For a list of output formats see Output File Formats.

Many protocol dissectors

There are protocol dissectors (or decoders, as they are known in other products) for are at many protocols: see Protocols and Protocol Fields.

Open Source Software

Wireshark is an open source software project, and is released under the GNU General Public License (GPL).You can freely use Wireshark on any number of computers you like, without

Worrying about license keys or fees or such. In addition, all source code is freely available under the GPL. Because of that, it is very easy for people to add new protocols to Wireshark, either as plugins, or built into the source, and they often do!

What Wireshark is not

Here are somethings Wireshark does not provide:

•Wireshark isn’t an intrusion detection system. It will not warn you when someone does strange things on your network that he/she isn’t allowed to do. However, if strange things happen, Wireshark might help you figure out what is really going on.

Wireshark will not manipulate things on the network, it will only “measure” things from it. Wireshark doesn’t send packets on the network or do other active things (except for name resolutions, but even that can be disabled).

System Requirements

The amount of resources Wireshark needs depends on your environment and on the size of the capture file you are analyzing. The values below should be fine for small to medium-sized capture files no more than a few hundred MB .Larger capture files will require more memory and disk space.

NOTE

BusynetworksmeanlargecapturesWorkingwithabusynetworkcaneasilyproducehugecapturefiles.Capturingonagigabitoreven100megabitnetworkcanproducehundredsofmegabytesofcapturedatainashorttime.Afastprocessor,lotsofmemoryanddiskspaceisalways a good idea. If Wireshark runs out of memory it will crash. Seehttps://wiki.wireshark.org/KnownBugs/OutOfMemoryfor details and workarounds.AlthoughWiresharkcapturespacketsusingaseparateprocessthemaininterfaceissingle-threadedand won’t benefit much from multi-core systems.

Microsoft Windows

•The current version of Wireshark should support any version of Windows that is still within its extended support lifetime. At the time of writing this includes Windows 10, 8, 7, Vista, Server2016, Server 2012 R2, Server 2012, Server 2008R2, and Server2008.

•Anymodern64-bit AMD64/x86-64or32-bitx86 processor.

•400MBavailableRAM.Larger capture files require more RAM.

•300MBavailablediskspace.Capturefilesrequireadditionaldiskspace.

•1024 × 768 (1280 × 1024 or higher recommended) resolution with at least 16-bit color. 8-bitcolor should work but user experience will be degraded. Power users will find multiple monitors useful.

•A supported network card for capturing Ethernet. Any card supported by Windows should work. See the wiki pages on Ethernet Capture and offloading for issues that may affect your environment. 802.11. See the Wireshark wiki page. Capturing raw 802.11 information may be difficult without special equipment. Other media.

Seehttps://wiki.wireshark.org/CaptureSetup/NetworkMedia. Older versions of Windows which are outside Microsoft's extended lifecycle support window are no longer supported .It is often difficult or impossible to support these systems due to circumstances beyond our control, such as third party libraries on which we depend or due to necessary features that are only present in newer versions of Windows (such as hardened security or memory management).

Wireshark1.12wasthelastreleasebranchtosupportWindowsServer2003.Wireshark1.10was the last branch to officially support Windows XP. See the Wireshark release lifecycle page for more details.

UNIX/ Linux

Wireshark runs on most UNIX and UNIX-like platforms including mac OS and Linux. The system requirements should be comparable to the Windows values listed above.

Binary packages are available for most Unix and Linux distributions including the following platforms:

•Apple mac OS

•Debian GNU/Linux

•FreeBSD8

•Gentoo Linux

•HP-UX

•Mandriva Linux

•Net BSD

•Open PKG

•Red Hat Enterprise/ Fedora Linux

•Sun Solaris/i386

•Sun Solaris/SPARC

•Canonical Ubuntu If a binary package is not available for your platform you can download the source and try to build it. Please report your experiences to wire shark-dev[AT]wireshark.org.3

Wireshark's main window consists of parts that are commonly known from many other GUI programs.

The menu (see The Menu) is used to start actions.

The main toolbar (seeThe"Main"Toolbar) provides quick access to frequently used items from the menu.

The filter tool bar (see The "Filter" Toolbar) provides a way to directly manipulate the currently used display filter(see Filtering packets while viewing).

The packet list pane(see The"Packet List" Pane)displays a summary of each packet captured .By clicking on packets in this pane you control what is displayed in the other two panes.

The packet details pane(seeThe"PacketDetails"Pane)displaysthepacketselectedinthepacketlist pane in more detail.

The packet bytes pane(see The"Packet Bytes" Pane) displays the data from the packet selected in the packet list pane,and highlights the field selected in the packet details pane.

The statusbar(seeTheStatusbar)showssomedetailedinformationaboutthecurrentprogramstateand the captured data.

Observation: Thus,Wireshark has been successfully analyzed.