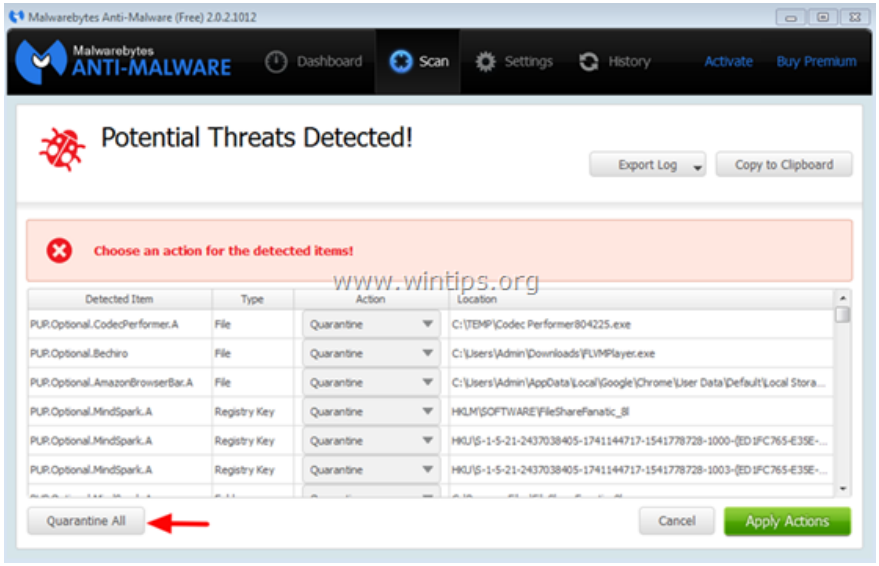
Remove original Network Packet Analyzer adware

Network Packet Analyzer is adware installed with plugins (toolbar, extensions - extensions or add-ons) on web browser to redirect users to other websites or display popup windows reports on pages that users visit.

Network Packet Analyzer is adware installed with plugins (toolbar, extensions - extensions or add-ons) on web browser to redirect users to other websites or display popup windows reports on pages that users visit.

Network Packet Analyzer can be installed on popular web browsers like Internet Explorer, Google Chrome or Mozilla Firefox without user permission. These advertising programs can handle malware in code to attack security on users' computers.



Technically, Network Packet Analyzer is not really a virus, it is just an unwanted program (PUP), which can be installed on your computer. If the software advertises the Network packet analyzer to attack the system, each time you access and browse the Internet on the Internet, the screen will display popup windows, banner ads, etc. in some cases it is The reason why the user's computer is slow, the browsing speed slows down.

Therefore when installing any software, certain programs that you download from the Internet or always pay attention to the installation terms of the program because the software installers will contain the installation part Additional soft you don't want.

Simply put, do not install any unrelated software attached to the program or software installer that you want to install. When installing any one program on your computer:

1. On the installation screen, do not click Next continuously without reading the terms.

2. Read the terms carefully before clicking Accept.
3. Always choose Custom installation.
4. Refuse to install additional software that you do not want to install.
5. Disregarding the options says that the browser homepage and search engines will be changed.

The Network Packet Analyzer adware removal steps

Step 1: Use RogueKiller Free to remove Network Packet Analyzer

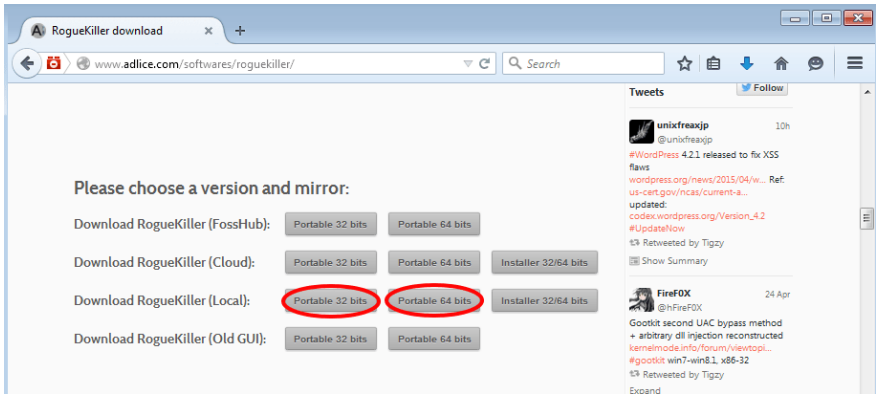
RogueKiller is an antivirus program, capable of finding, blocking and removing malware and some other software like rootkits, rogues, worms, .

1. Download RogueKiller to your device and install it.

Download RogueKiller to your device and install it here.

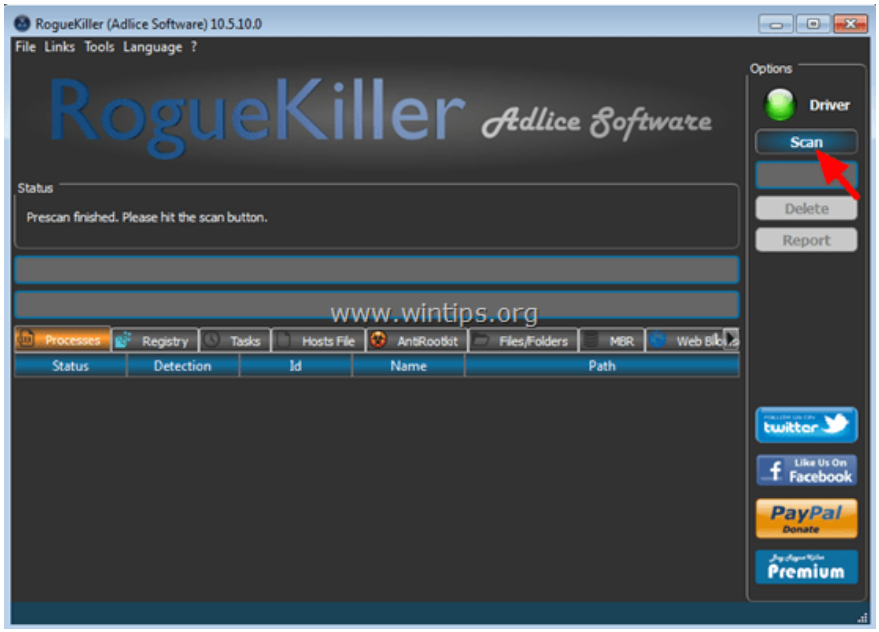
Note:

Downloading the x86 or x64 version depends on your operating system version. To find the operating system version, right-click the computer icon, and then select Properties. On the Properties window, find the System Type entry and check if it is a 32-bit or 64-bit version.



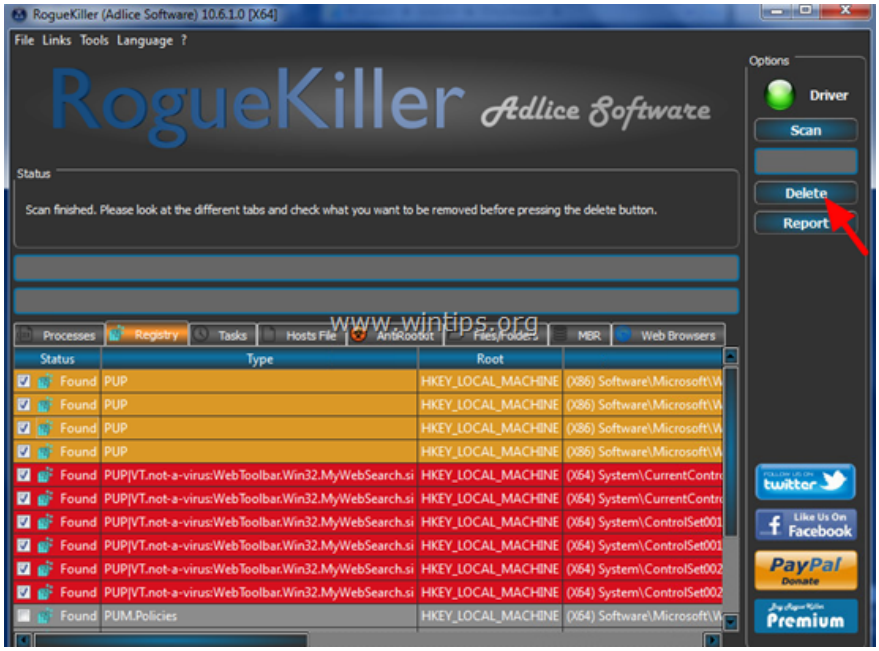
2. Double click to run RogueKiller.

3. After the Pre-Scan process has finished, click **the Scan button** to perform a system-wide scan.

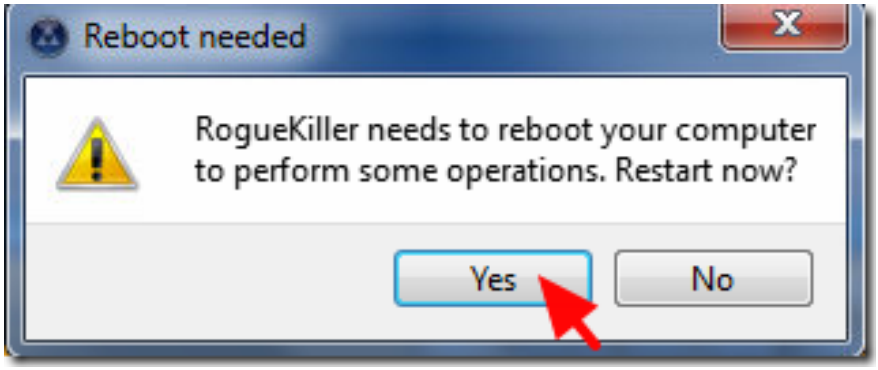


Be patient and wait until Rogue Killer wipes your system.

4. When the scan finishes, select all the items found on the Registry tab and the Web Browsers tab and then click Delete to remove all detected items.



If required, click Yes to restart your computer.



Step 2: Uninstall Network Packet Analyzer on Windows

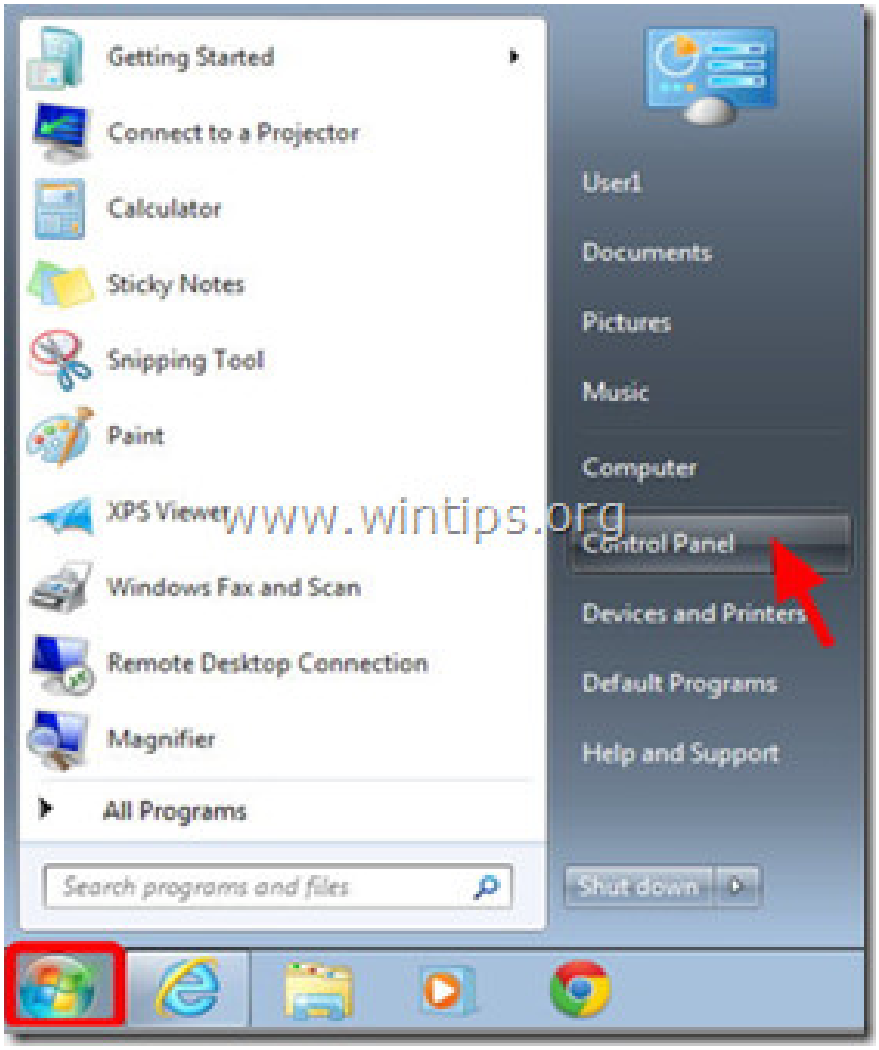
1. First open the Windows Control Panel window. To do this thing:

- On Windows 8 and 8.1:

Right-click the **Start** button in the bottom left corner of the screen, then select **Control Panel** .

Alternatively, press the Windows + R key combination to open the Run command window.

On the Run command window, enter **control panel** there and press **Enter** .



- On Windows 7, Vista XP:

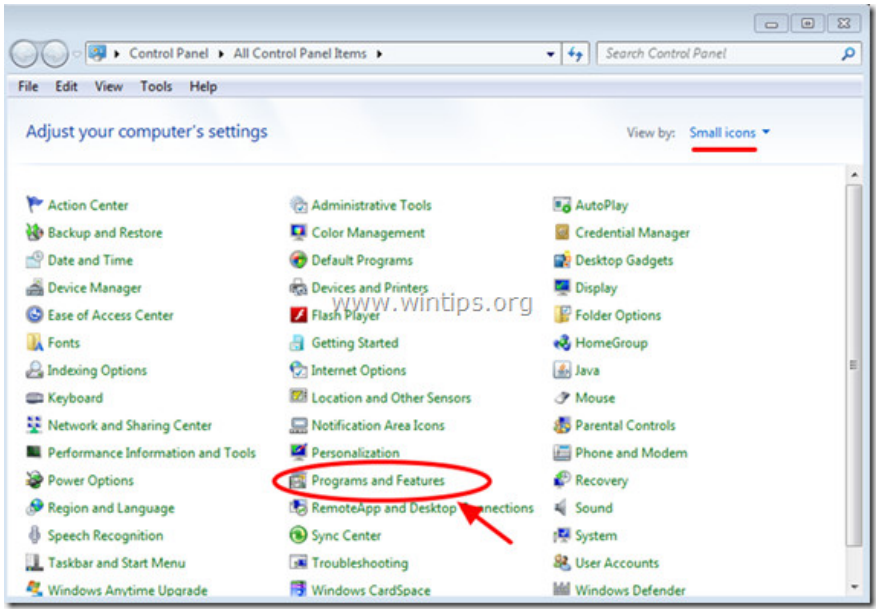
Go to Start => Control Panel .

- On Windows XP:

Go to Start => Settings => Control Panel

2. Find and click **Programs and Features** (or Uninstall a Program) if you use Windows 8, 7 and Vista.

On Windows XP, find and click **Add or Remove Programs** .

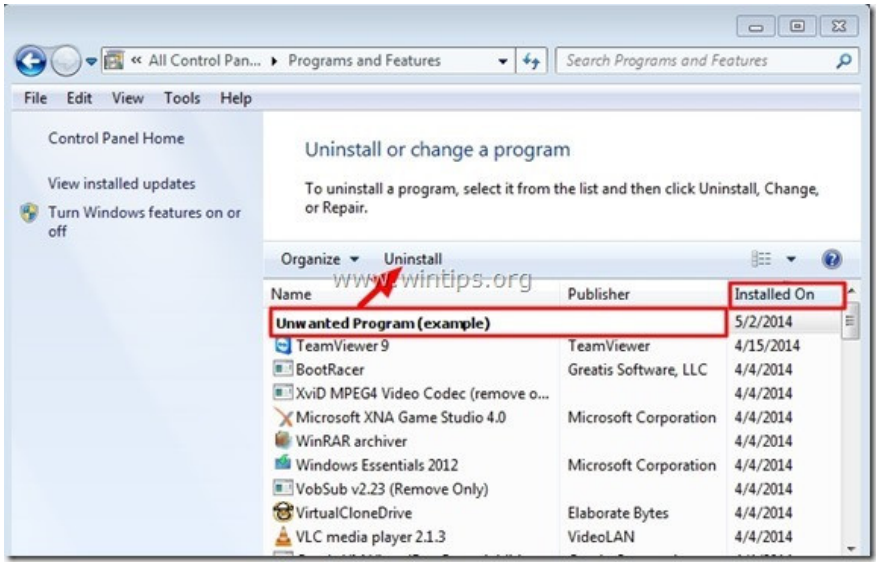


3. On the Uninstall or change a program window, click **Installed On** to arrange programs by date.

Next find and uninstall the program named:

1. Network Packet Analyzer (from Logic Net)
2. Online Ad Scanner

Next find and uninstall programs of unknown origin.



Step 3: Remove Network Packet Analyzer ads with 'AdwCleaner'

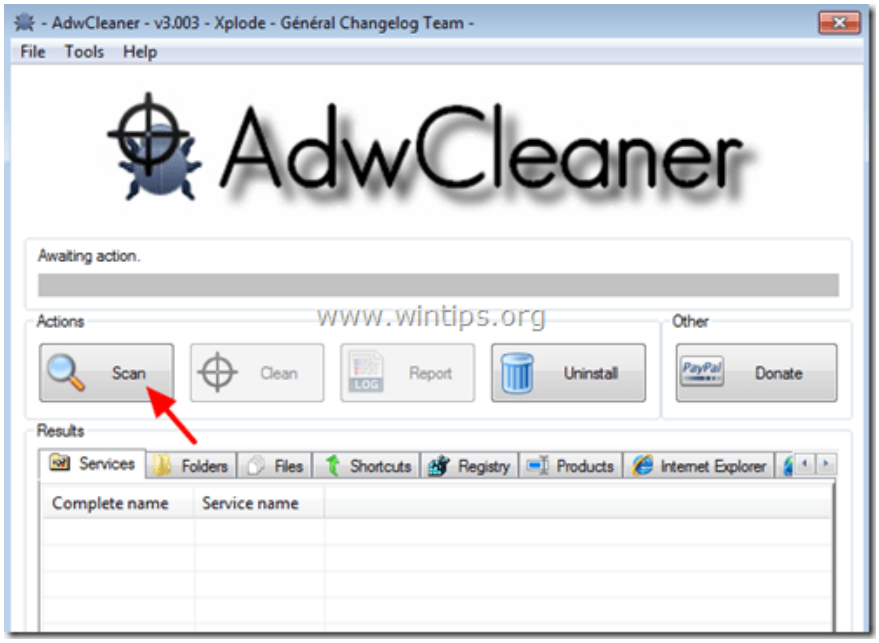
AdwCleaner is a free utility that can support the removal of advertising programs on your computer.

1. Download AdwCleaner to your device and install it.

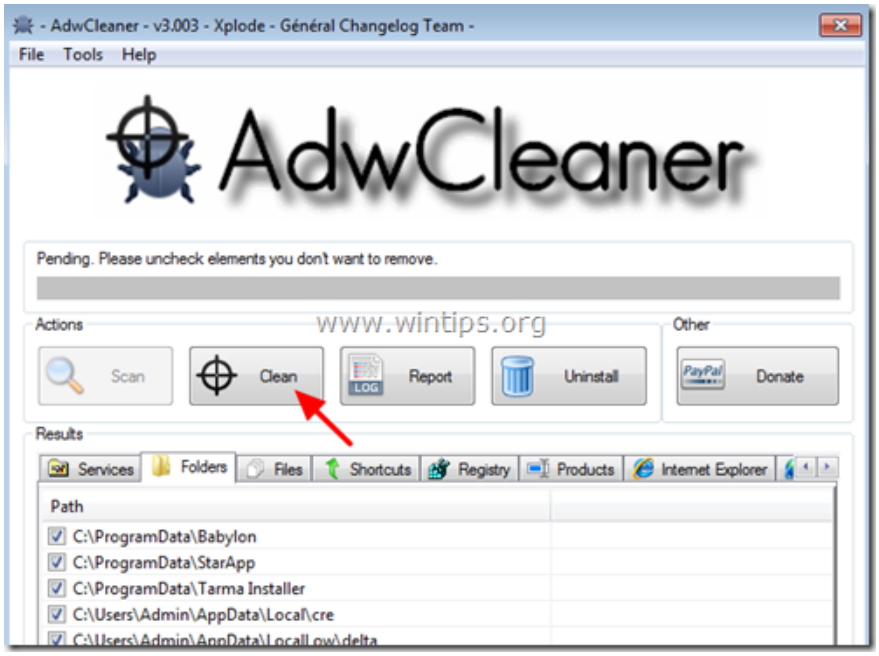
Download AdwCleaner to your device and install it here.

2. Close all the programs you are open, then double-click AdwCleaner to open the program on your computer.

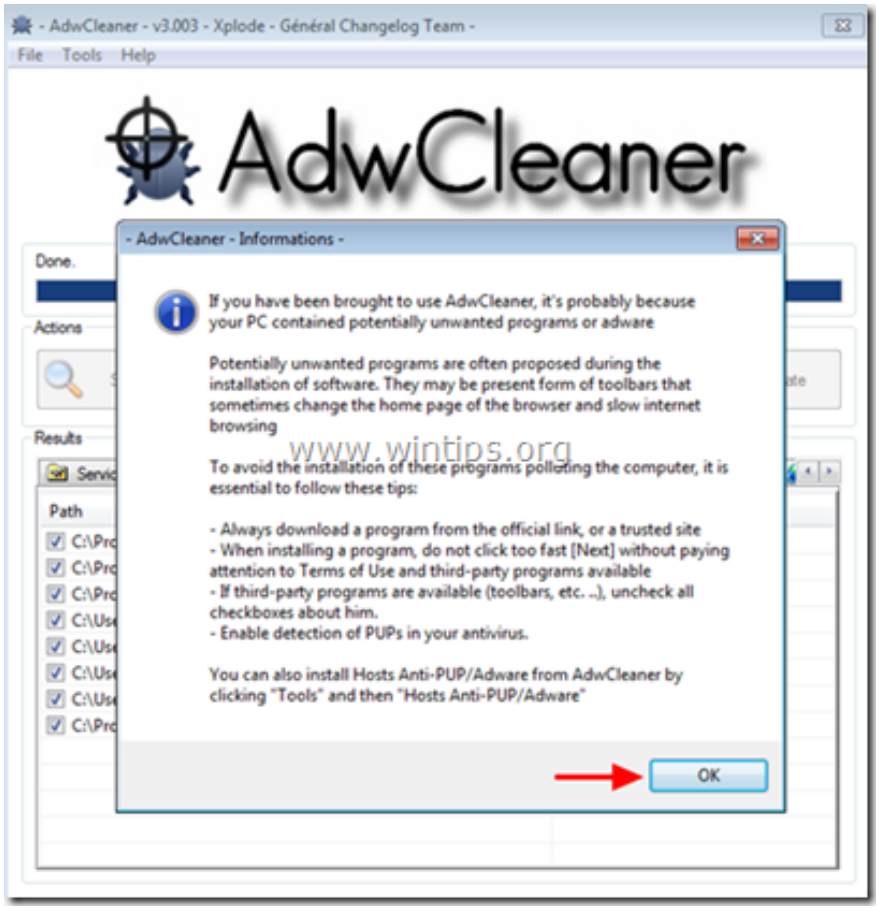
3. Accept the terms and then click the **Scan** button.



4. After the scan finishes, click **Clean** to remove all malicious programs and unwanted programs.



5. On the AdwCleaner - Information window, click **OK,** then click **OK** again to restart your computer.



6. After the restart process is finished, a new **notepad** window will appear. It contains advertisements, Registry keys and files that have been emptied by AdWCleaner. Your task is to **close** this **Notepad file** .

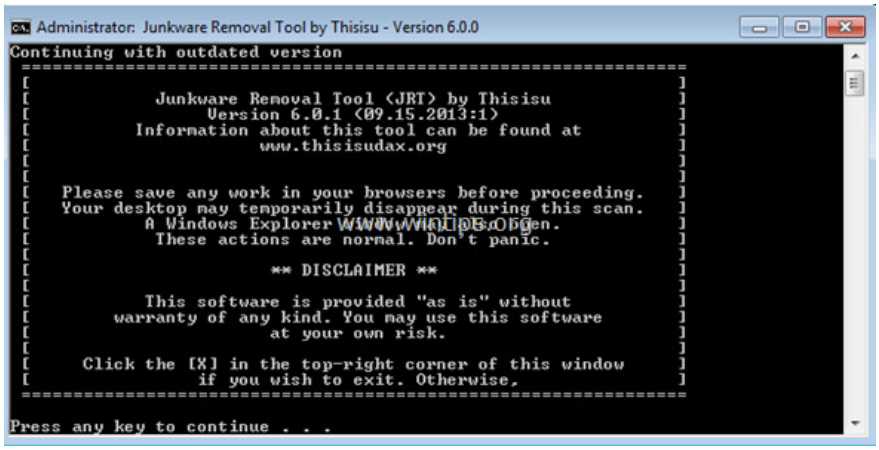
Step 4: Remove the Network Packet Analyzer Ads ad using the Junkware Removal Tool

1. Download the Junkware Removal Tool to your computer and install it.

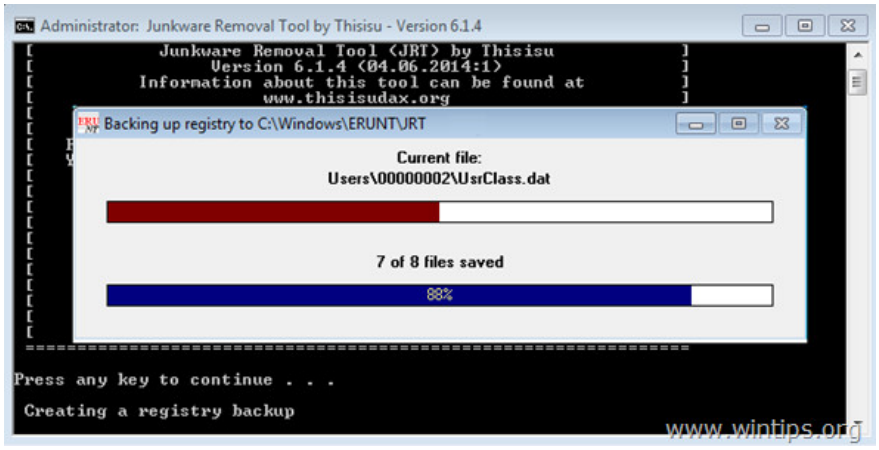
Download the Junkware Removal Tool to your computer and install it here.

2. After successfully downloading and installing the Junkware Removal Tool, proceed to open the program.

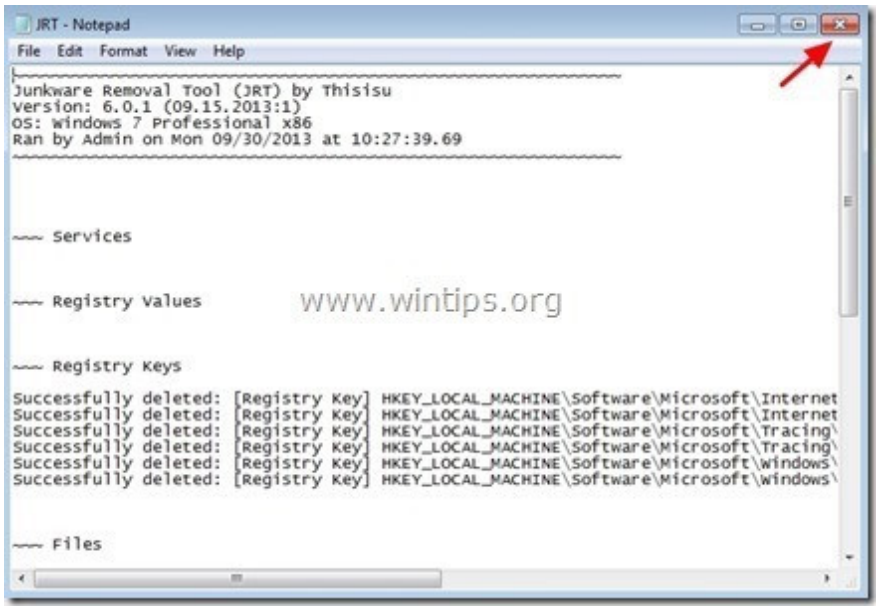
Press any key to start scanning your computer with JRT - Junkware Removal Tool.



3. Wait for JRT to scan and clean your system.



4. Close the JRT log file and restart your computer.



Step 5: Use Malwarebytes Anti-Malware Free to remove Network Packet Analyzer Adware

1. Download Malwarebytes Anti-Malware to your computer and install it

Download Malwarebytes Anti-Malware to your computer and install it here.

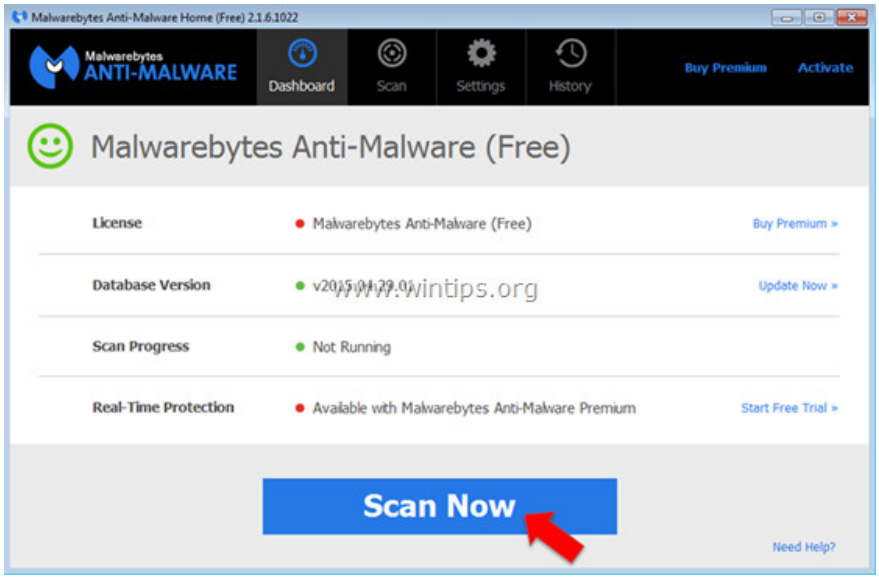
Note:

On the final installation window, uncheck the Enable free Trial of Malwarebytes Anti-Malware PRO section to use the free version of the application.

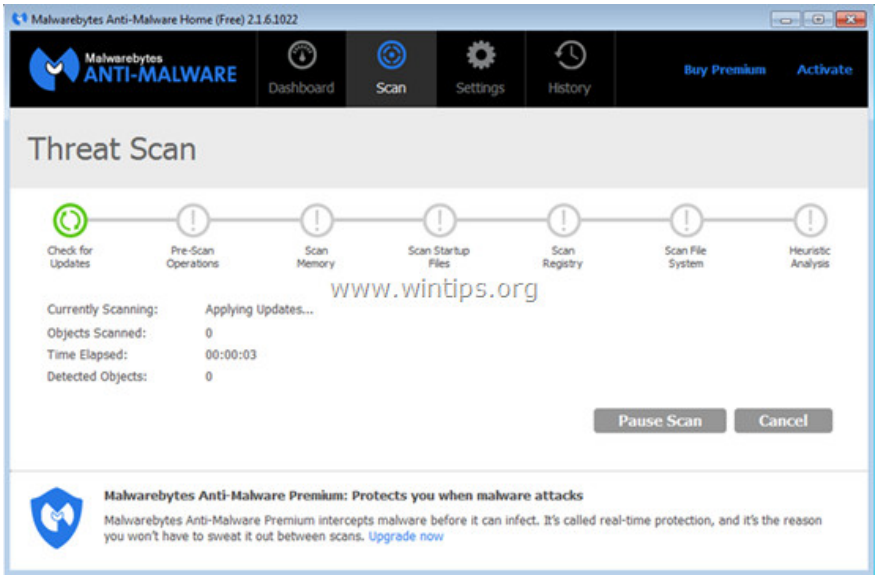
2. Run Malwarebytes Anti-Malware and allow the program to update to the latest version as needed.

3. After the update process finishes, click **Scan Now** to start the scan of your system and remove unwanted programs.

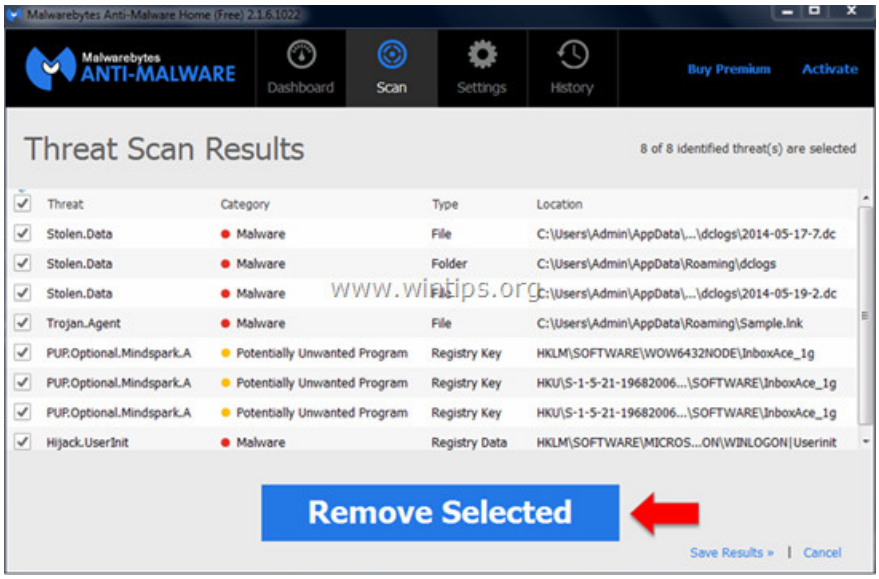
4. Wait for Malwarebytes Anti-Malware to complete the scanning process on your system.



5. After the scanning process is finished, click **Quarantine All** (Remove Selected) to remove all detected malicious files.



6. Wait until Malwarebytes Anti-Malware removes all malicious files on the system, then proceed to restart your computer to complete the process of removing malware.

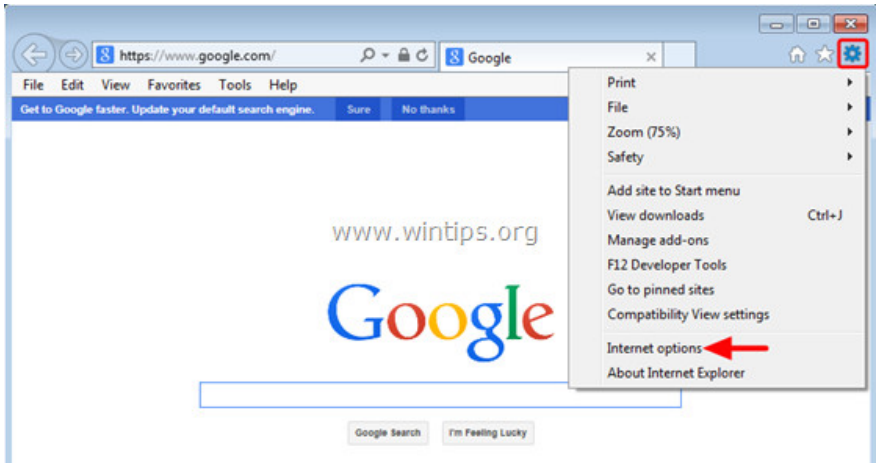


Step 6: Remove Network Packet Analyzer from Internet Explorer, Chrome and Firefox browsers

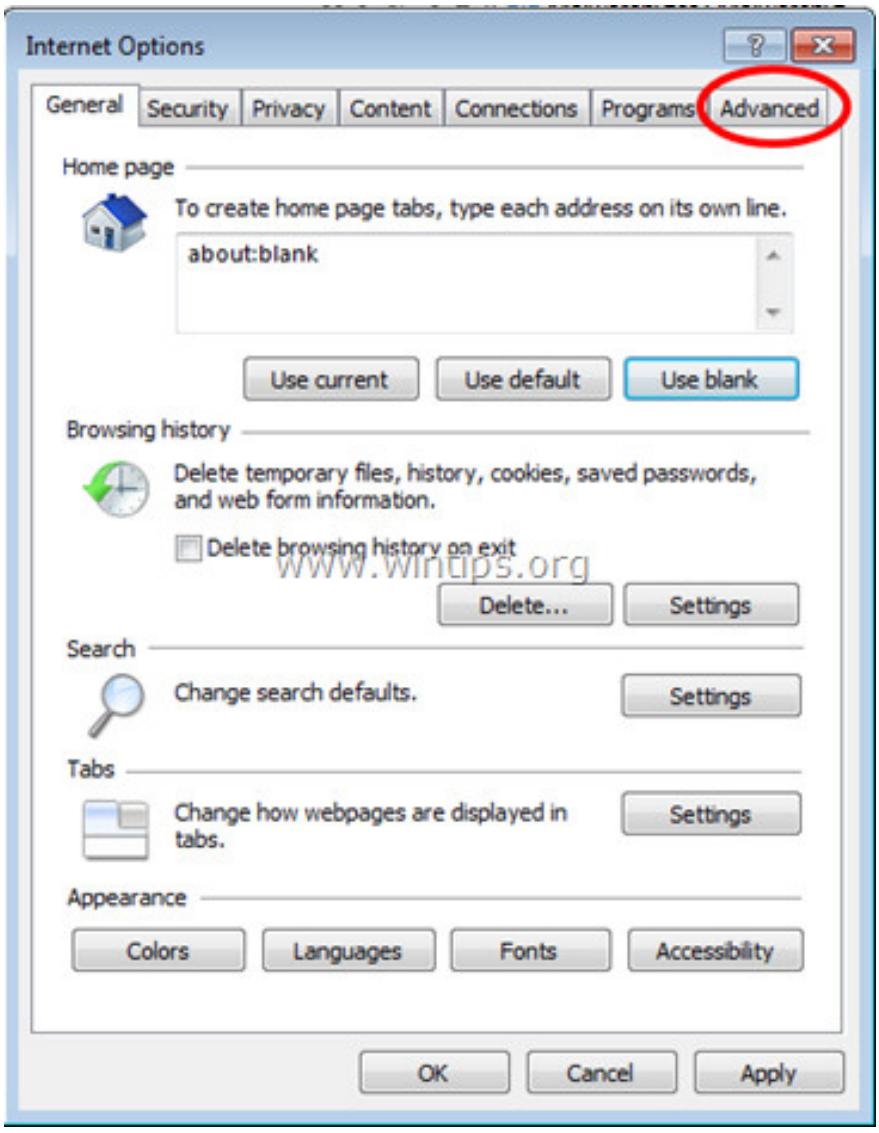
To ensure that Network Packet Analyzer has been completely removed from Internet Explorer, proceed to reset Internet Explorer settings to the initial default state.

- Internet Explorer browser:

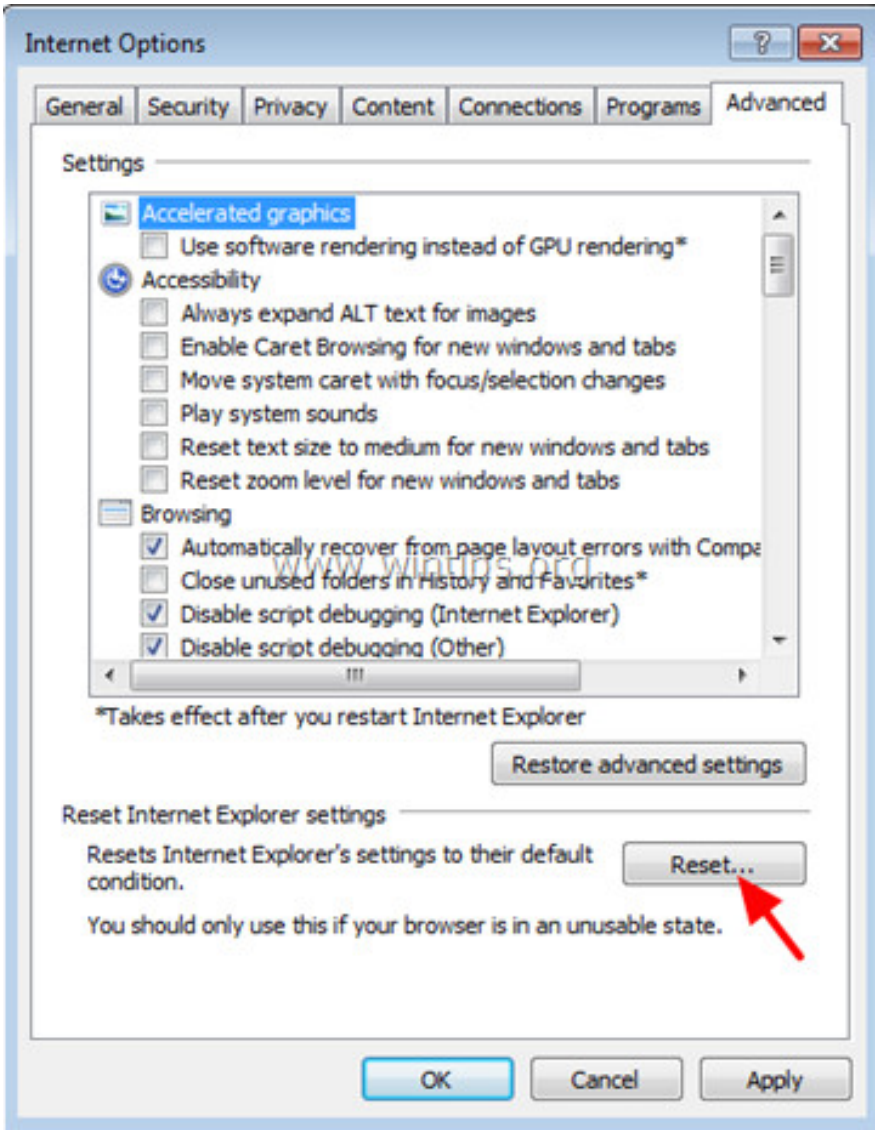
1. On the Internet Explorer browser window, find and click the jag icon in the top right corner of the screen, select **Internet Options** .



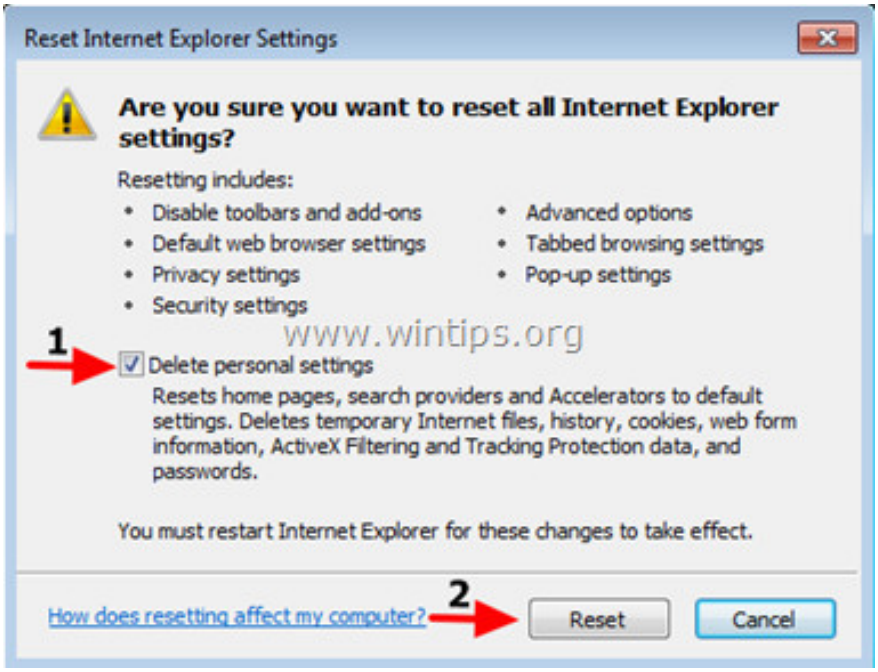
2. Next on the Internet Option window, find and click the **Advanced** tab **.**



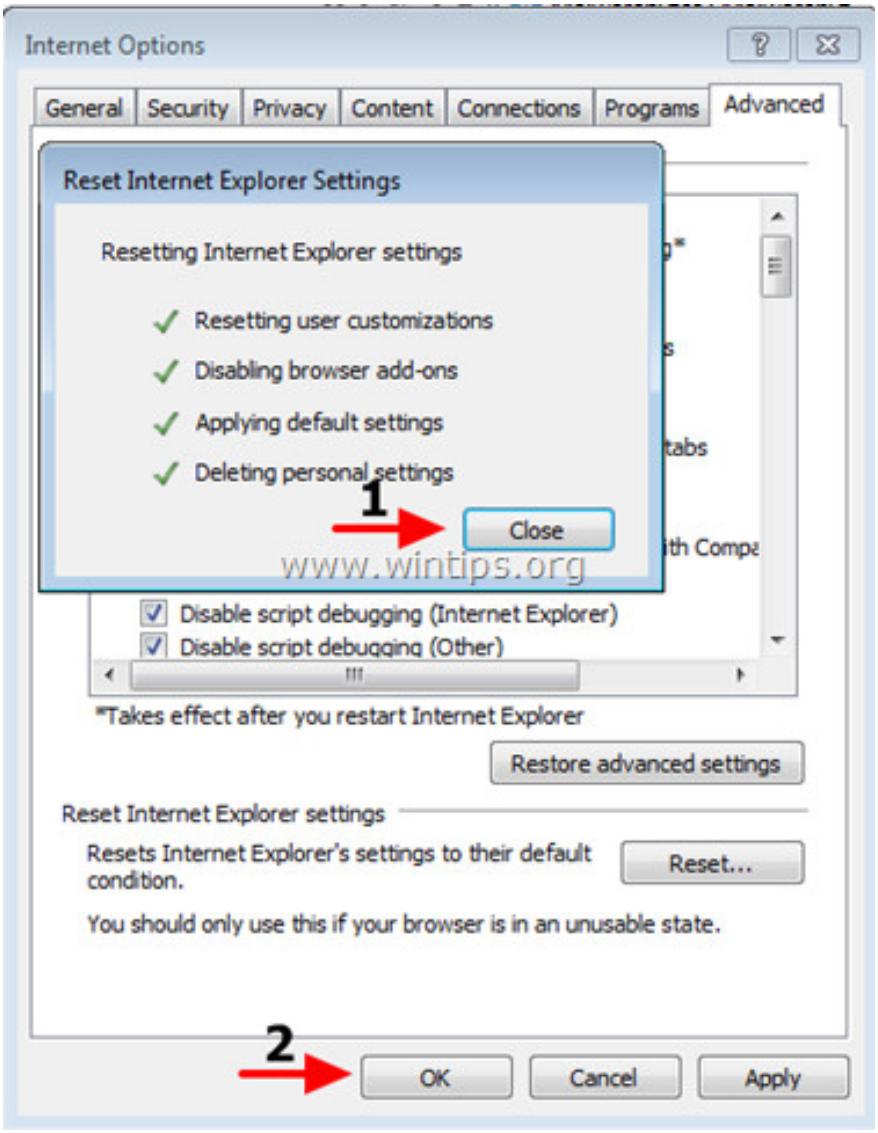
3. Select **Reset** .



4. Select '**Delete personal settings**' and select **Reset** .



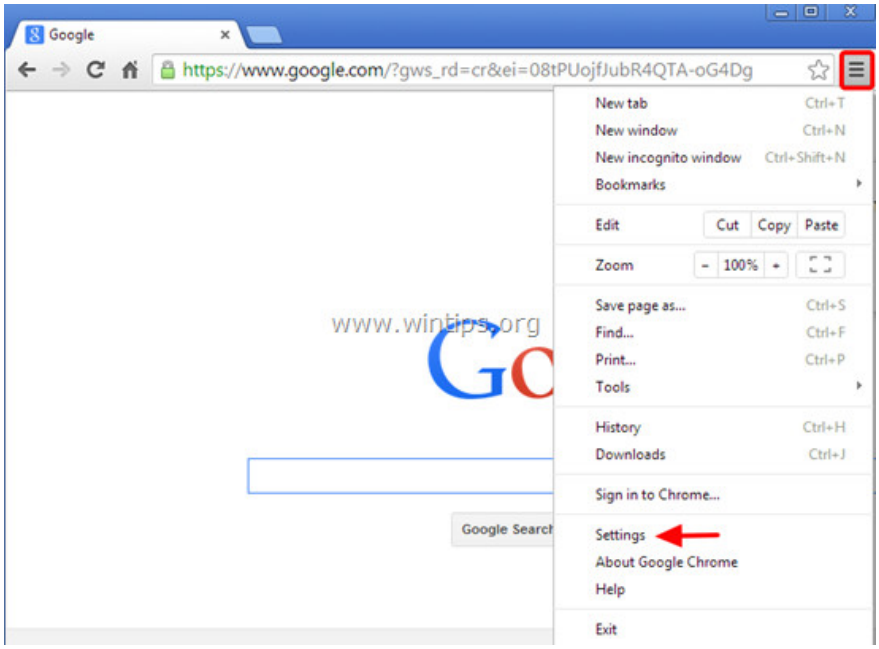
5. After the reset process finishes, click **Close** and then click **OK** to close the Internet Options window.



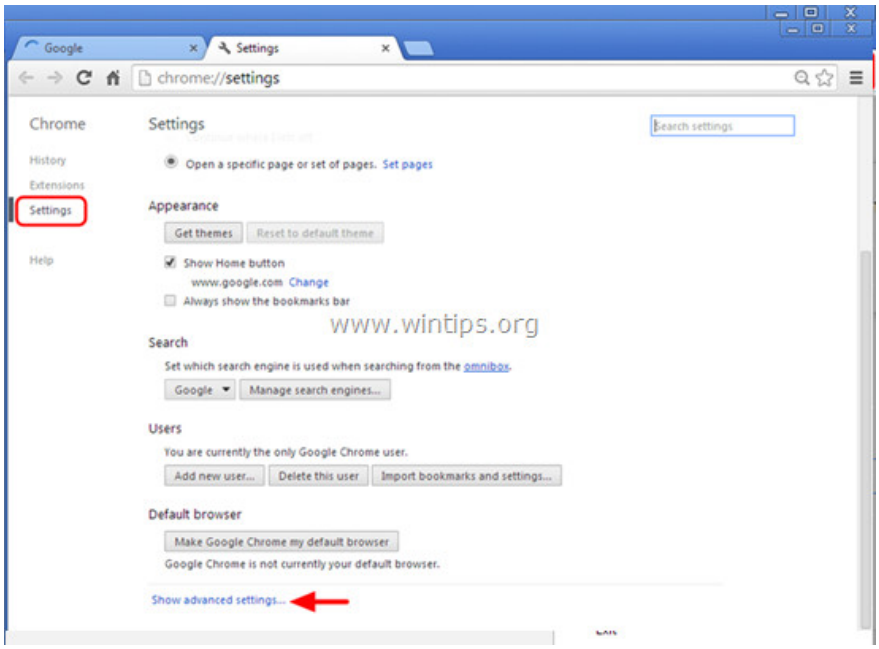
6. Close all windows, then restart your Internet Explorer browser.

- Google Chrome browser:

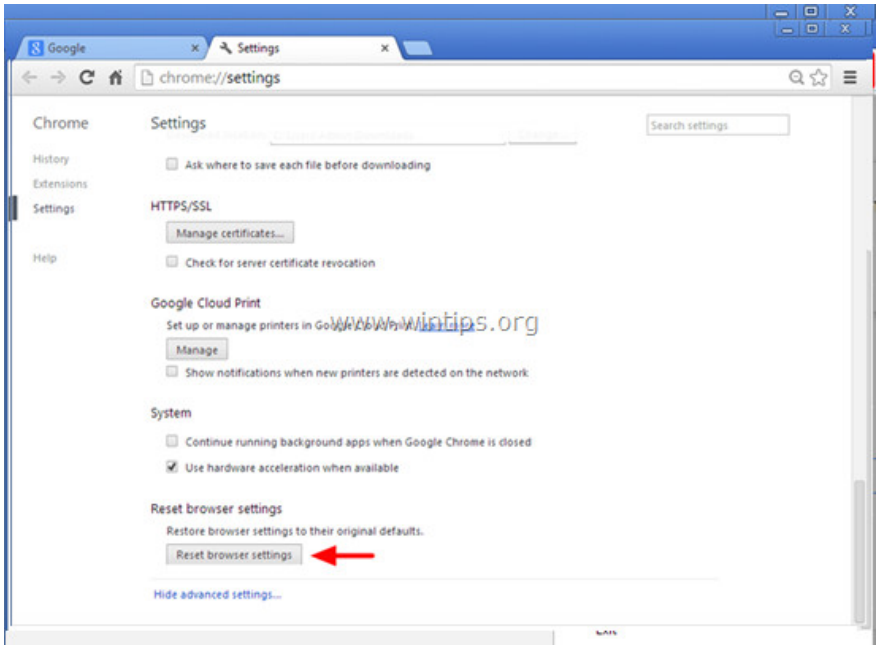
1. Open your Chrome browser, then click the 3 dash line icon in the top right corner of the screen, select **Settings.**



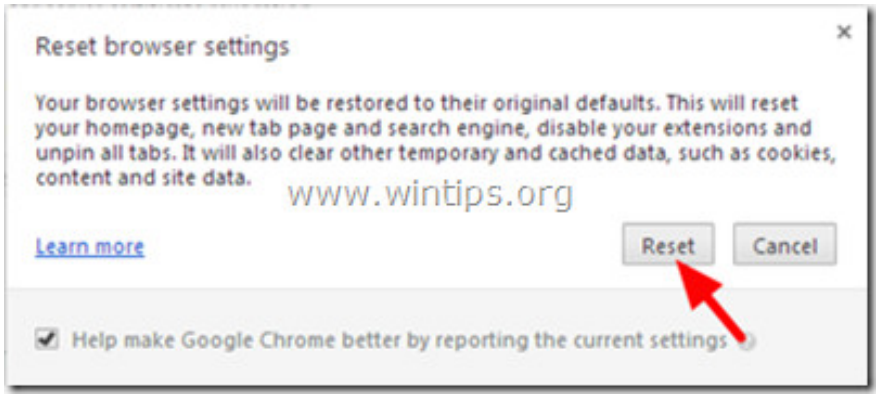
2. On the Settings window, scroll down to find and select **Show advanced settings** (show **advanced settings**).



3. Scroll down to find and select ' **Reset Browser Settings** '.



4. Click the **Reset** button again.



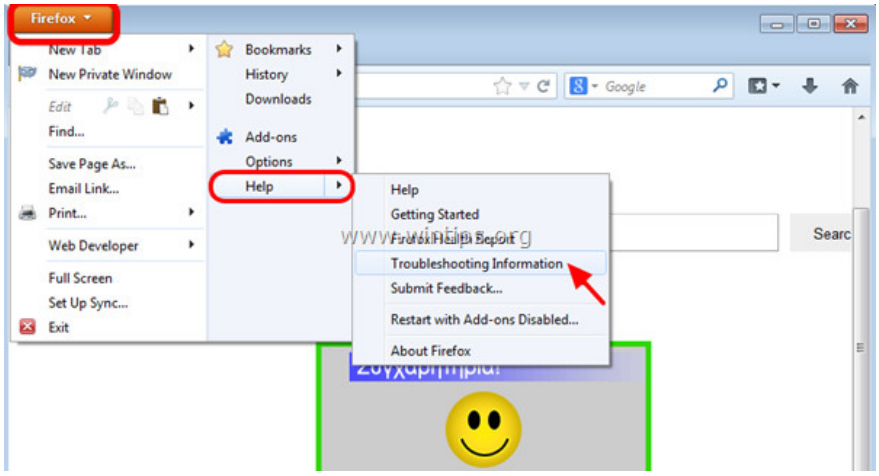
5. Restart your Chrome browser.

Note:

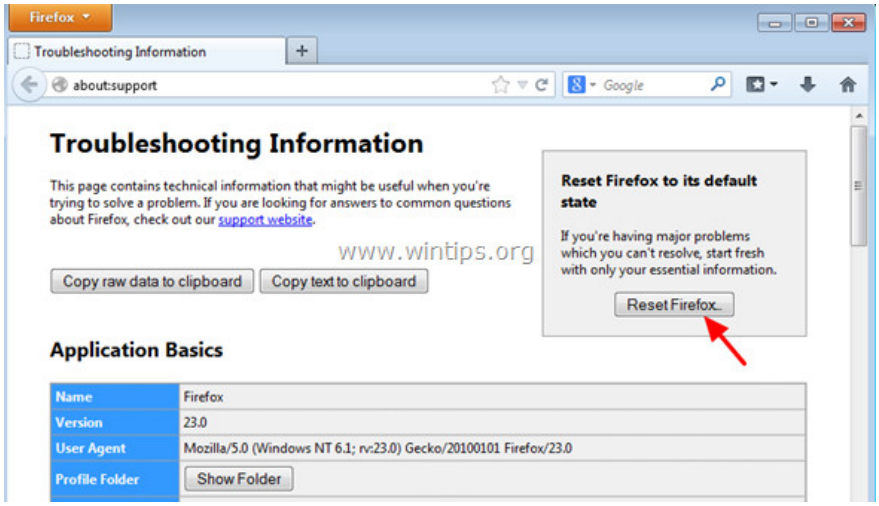
If an error occurs, then you will have to uninstall Chrome completely, then proceed to reinstall.

- Firefox browser:

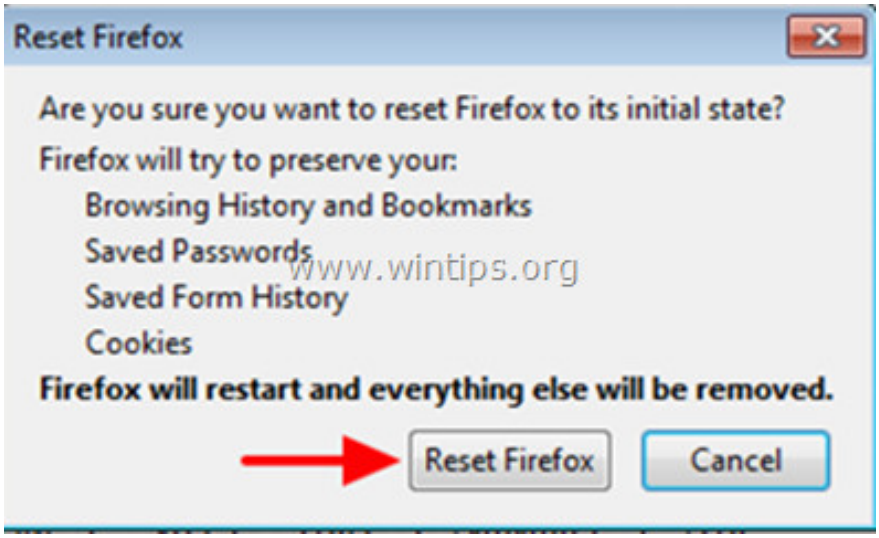
1. From the Firefox Menu, click **Help** => **Troubleshooting Information** .



2. On the Troubleshooting Information window, click **Reset Firefox** to reset your Firefox browser to its default state.



3. Next, click **Reset Firefox** again.



4. After the reset process finishes, restart your Firefox browser.

Refer to some of the following articles:

1. How to remove Trustedsurf.com on Chrome, Firefox and Internet Explorer

1. Rooted Delta Search on Chrome, Firefox and Explorer browsers

1. Want to load page speed on Edge browser faster, enable this feature

Good luck!