

# PC Tools HIT Scan

This document outlines the step-by-step process for running the PC Tools “HIT Scan” program.

This software has been tested on the following operating systems.

Windows XP

Windows Vista

Windows 7

## **Step 1: Running "HIT Scan"**

This step explains how to run the “HIT Scan” program.

## **Step 2: The “Alternate Operating System” data gathering phase of the “HIT Scan” tool**

This step shows the “Alternate Operating System” data gathering phase of the “HIT Scan” tool.

## **Step 3: Locate and send the “HIT Scan” report logs to PC Tools**

This step explains how to locate the “HIT Scan” logs.

## **Step 4: Removal of infections (if detected by “HIT Scan”)**

This step explains how to use the “HIT Scan” to remove any infections that it detects on your computer.

### **Step 1: Running "HIT Scan"**

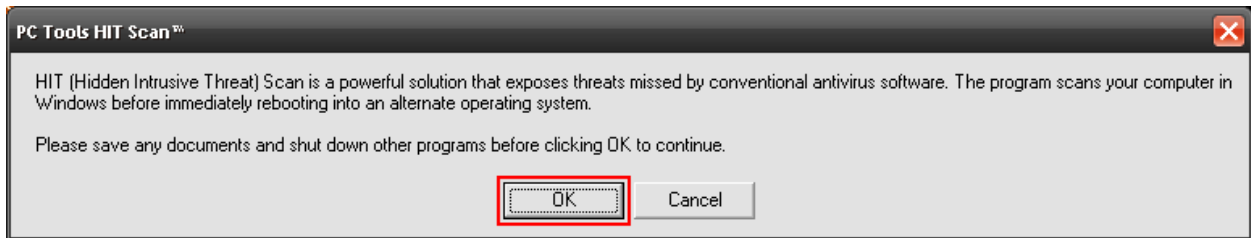
1. Download "HIT Scan" from the following link and save it to your Desktop (to make it easy to find):

<http://downloads.support.pctools.com/HITScan.exe>

2. We suggest you disconnect your computer from the Internet (i.e. un-plug the Ethernet cable / disconnect from Wireless) to limit any outside interference while "HIT Scan" is running, but this is optional and not mandatory.

3. Double-click on the "HITScan.exe" file to start the "HIT Scan" program

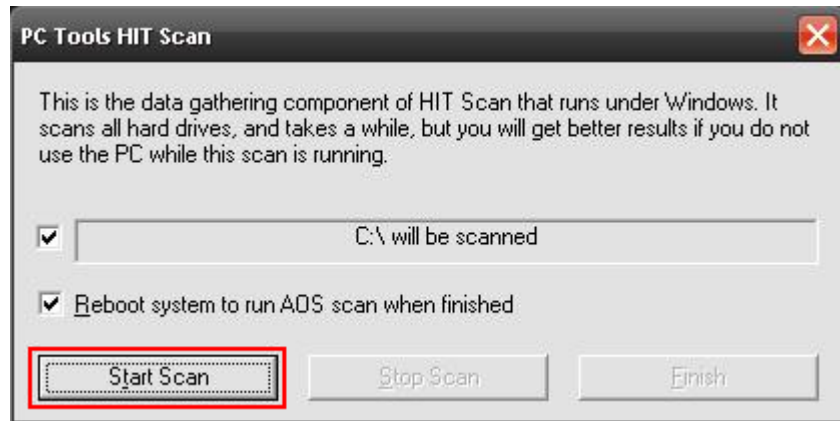
4. Select "OK" to allow the installation to proceed



5. Select the hard drives you want to scan from within the "PC Tools HIT Scan" window (e.g. "C:\")

6. Ensure the "Reboot system to run AOS scan when finished" option is selected

7. Select "Start Scan"

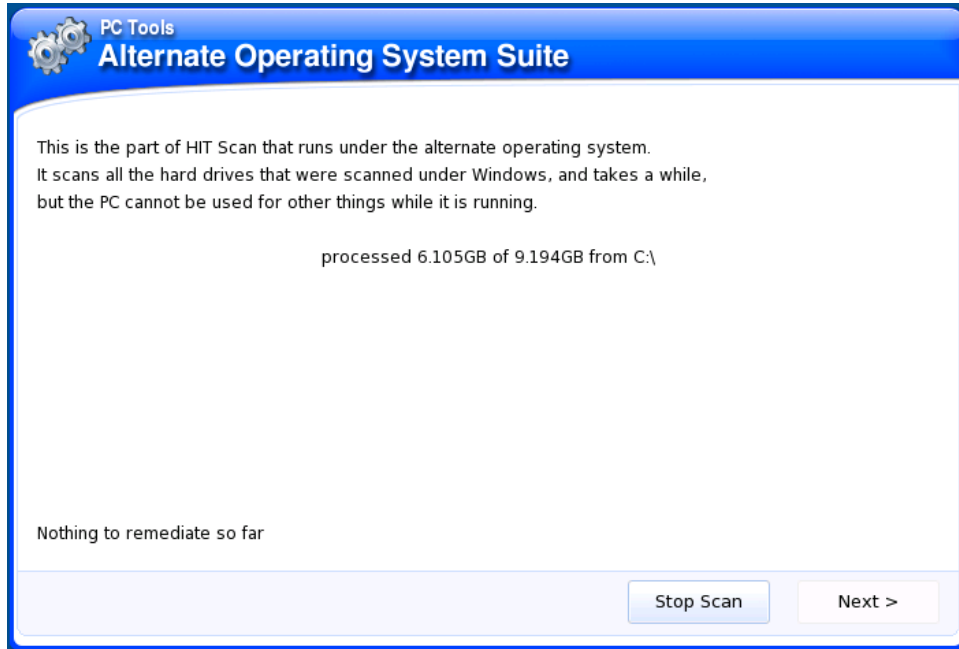


8. At this stage, the "HIT Scan" program will scan the hard drives you selected and collect information from each file. At the completion of the scan, the "HIT Scan" program will automatically reboot your computer to load the second stage of the "HIT Scan" data gather process (which occurs within the "Alternate Operating System" environment).

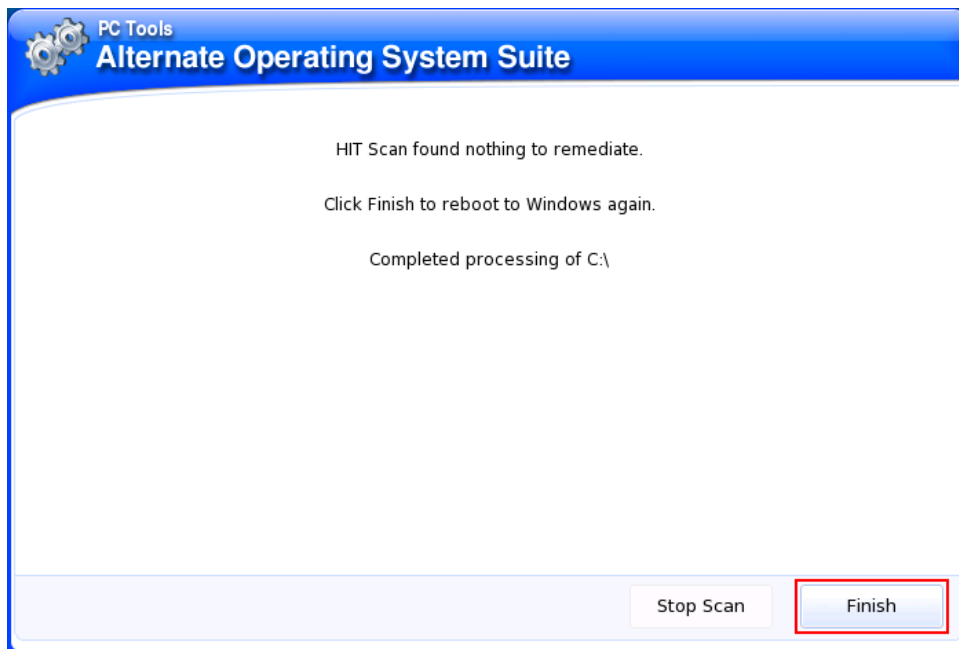
Please do not attempt to manually initiate "PC Tools HIT Scan" during the computer's boot process. Please simply allow the "HIT Scan" program to run un-interrupted and it should boot to the "Alternate Operating System" automatically.

**Step 2: The “Alternate Operating System” data gathering phase of the “HIT Scan” tool**

9. Once the "Alternate Operating System" interface has fully loaded you will see the “Alternate Operating System” data gathering phase start running automatically.

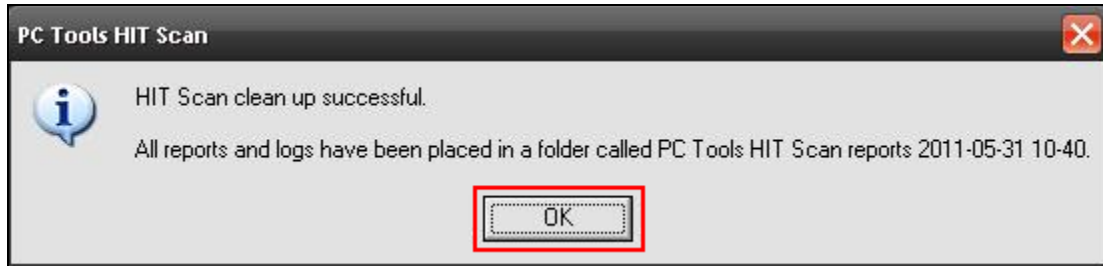


10. At the completion of the “Alternate Operating System” data gathering phase, click “Finish”



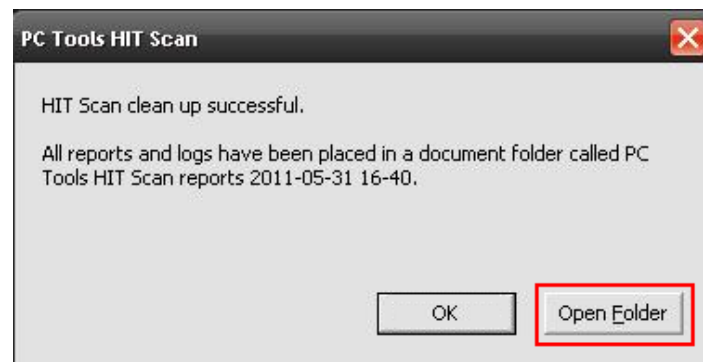
### **Step 3: Locate and send the “HIT Scan” report logs to PC Tools**

- 11.** Once the computer has booted back in to Windows, the “HIT Scan” program should automatically uninstall itself. Select “OK” from the “PC Tools HIT Scan” window that appears.



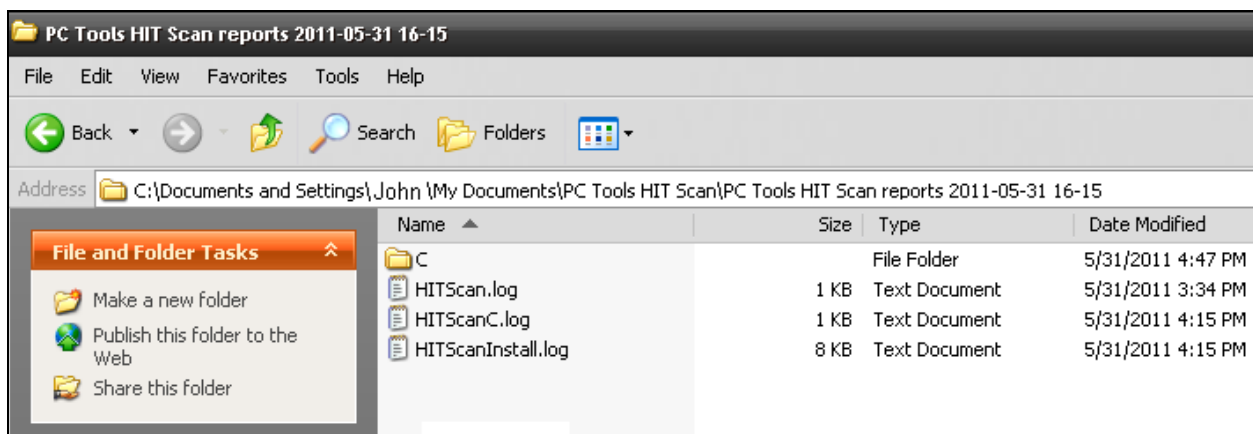
- 12.** Reconnect your computer to the Internet (i.e. plug in the Ethernet cable / reconnect to Wireless) if you previously disconnected it.

- 13.** Select “Open Folder” from the following window that appears.



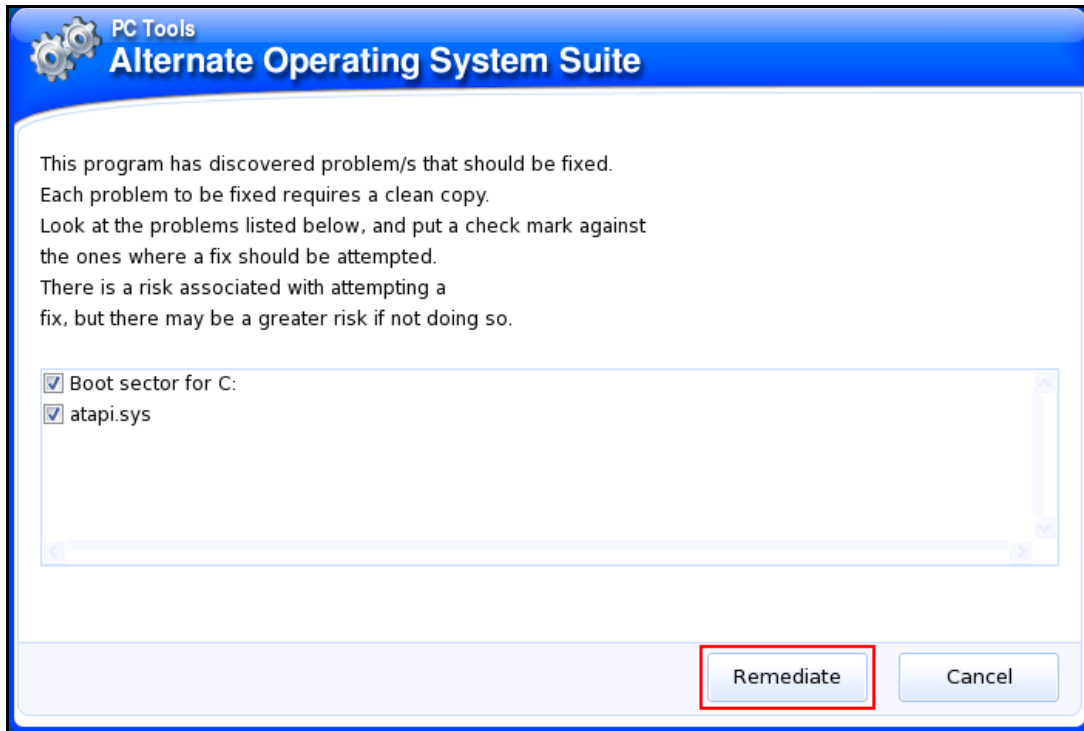
Attach all of the files and folders in the window that appears to your reply to the e-mail from PC Tools. You may need to zip / compress the folders (e.g. the “C” folder) to allow it to be attached to the e-mail.

\*\* This example (Screenshot) is from Windows XP.



#### **Step 4: Removal of infections (if detected by "HIT Scan")**

If "HIT Scan" detects any suspicious items on your computer, it will show them in the "Alternate Operating Suite" scan results screen. When this occurs, simply follow the steps shown below to remove the suspicious items



#### **1. Select "Remediate"**

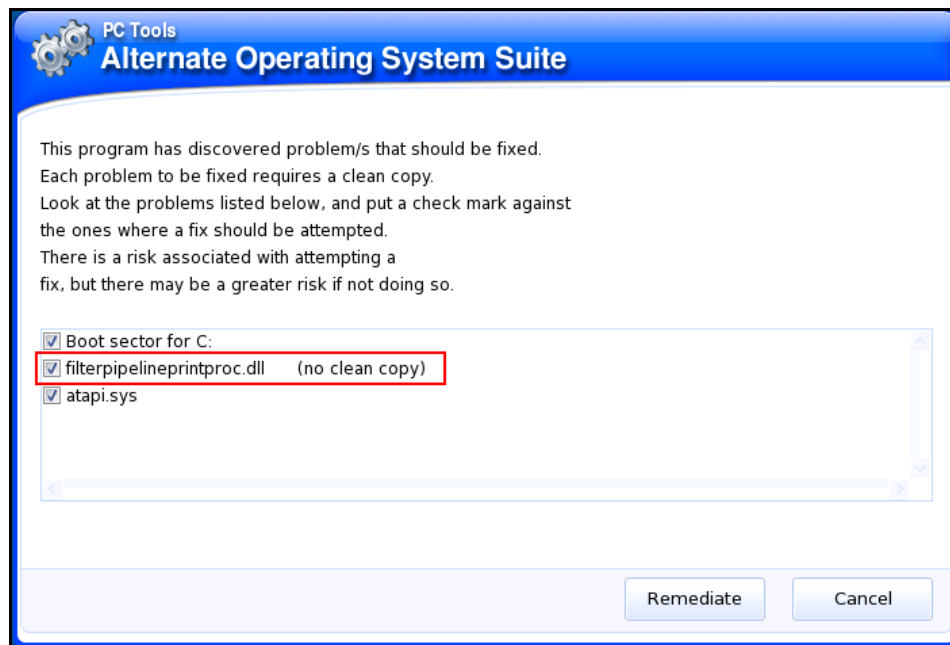
The "HIT Scan" tool will then attempt to remediate (neutralise) the suspicious files in the system and provide you with a results screen showing the outcome of this process.

#### **2. Select "Finish"**

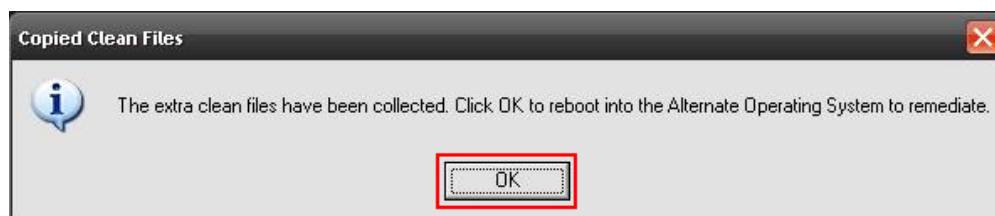
If the "HIT Scan" did detect any suspicious items and you did chose to remediate them, please let us know via reply e-mail if this resolved the issues you were having. Please also include the "PC Tools HIT Scan reports" files and folders requested in "Step 13" regardless of the outcome.

**\*NOTE:** If the “HIT Scan” tool detects a suspicious file or files, but does not have a clean (non-infected) copy of the file to use to remediate it, it will show this information in the scan results screen (see screenshot below).

This just means that the “HIT Scan” tool has identified suspicious files in the system and in order to fully neutralize them, it needs to collect clean (non-infected) copies of those files from within the Windows Operating System. To complete the remediation process, simply follow the steps shown below...



1. Select the “**Remediate**” tab
2. Select “**OK**”. This will automatically reboot the computer back to Windows to allow “HIT Scan” to collect clean copies of the files it detected. The “clean” files will be collected automatically when the computer boots back to Windows.
3. Select “**OK**” from the following window when it appears to reboot the computer back to the "Alternate Operating System" and allow “HIT Scan” to complete the remediation process.



4. Once the "Alternate Operating System" re-scan has completed, select the “**Remediate**” tab
5. Select “**Finish**” to reboot back to Windows