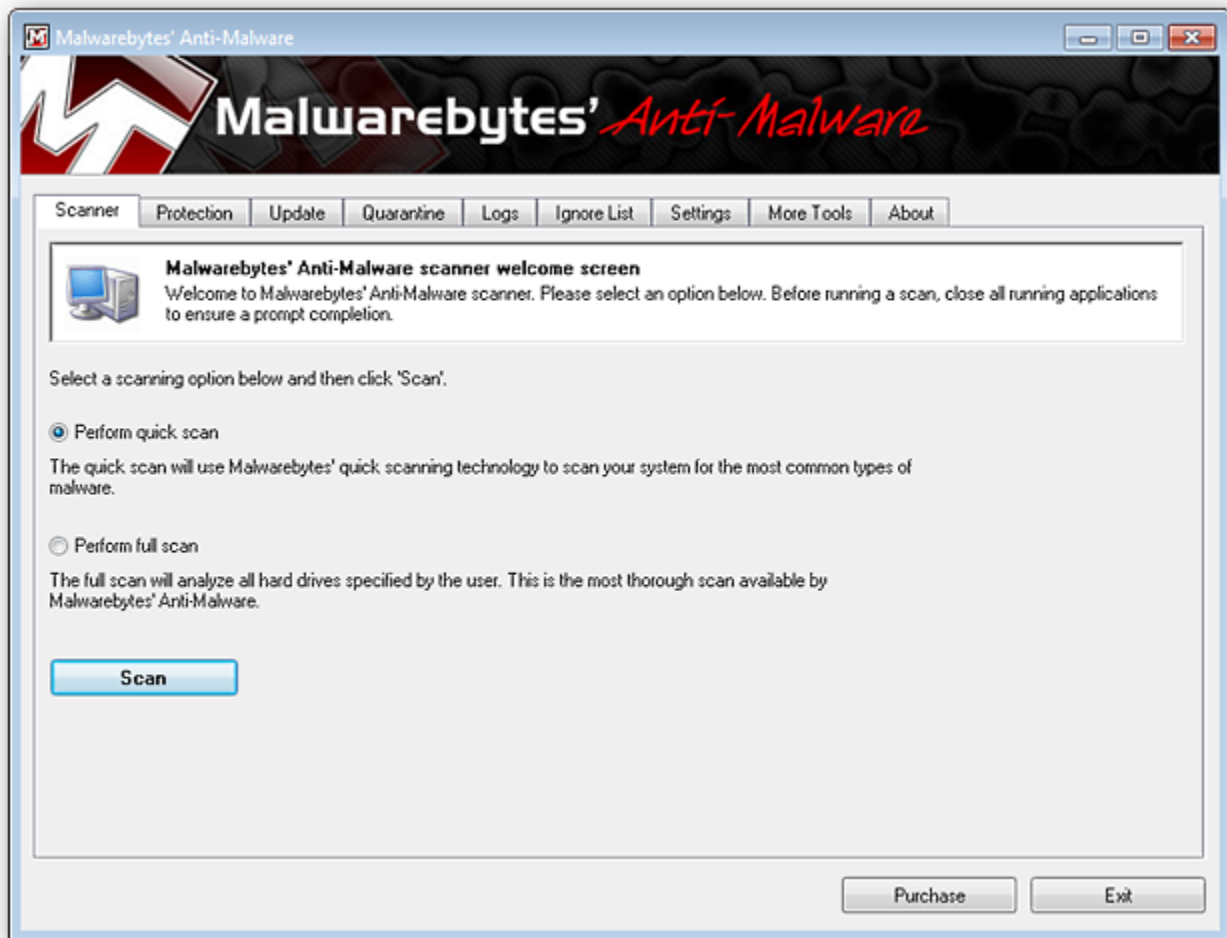
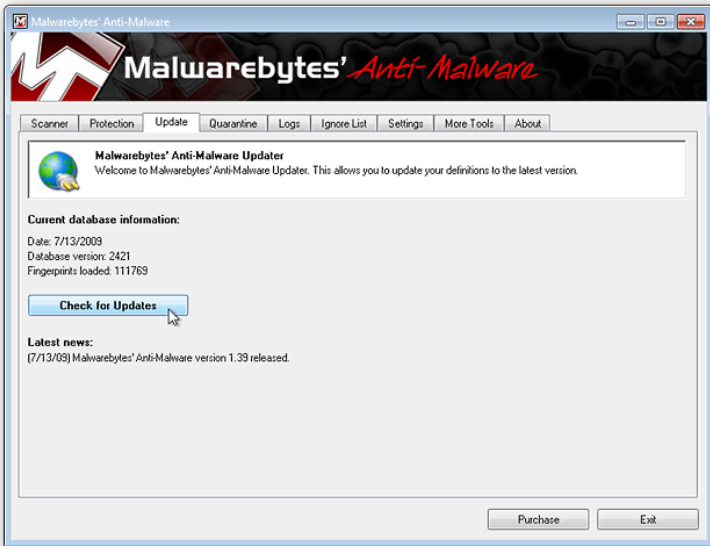


Remove Malware Quickly with Malwarebytes' Anti-Malware

When you first start Malwarebytes' Anti-Malware up, this is the window that you will see. Malwarebytes' Anti-Malware has a very nice tabbed interface to make shifting between functions smooth and quick. At this point it is set to "Perform quick scan" as the default.

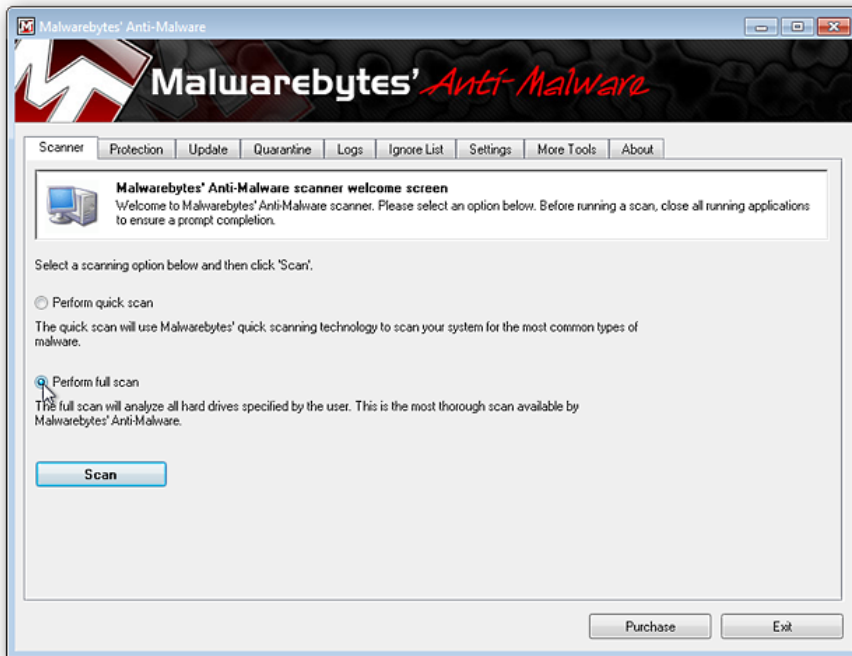


If you did not check for updates during the install process, now is a good time to do so. Here you can see the current database version (and associated date) along with the number of malware signatures that it will scan for. Updates usually run between 2.0 – 2.5 MB in size. Click "Check for Updates" to get the latest database signatures.

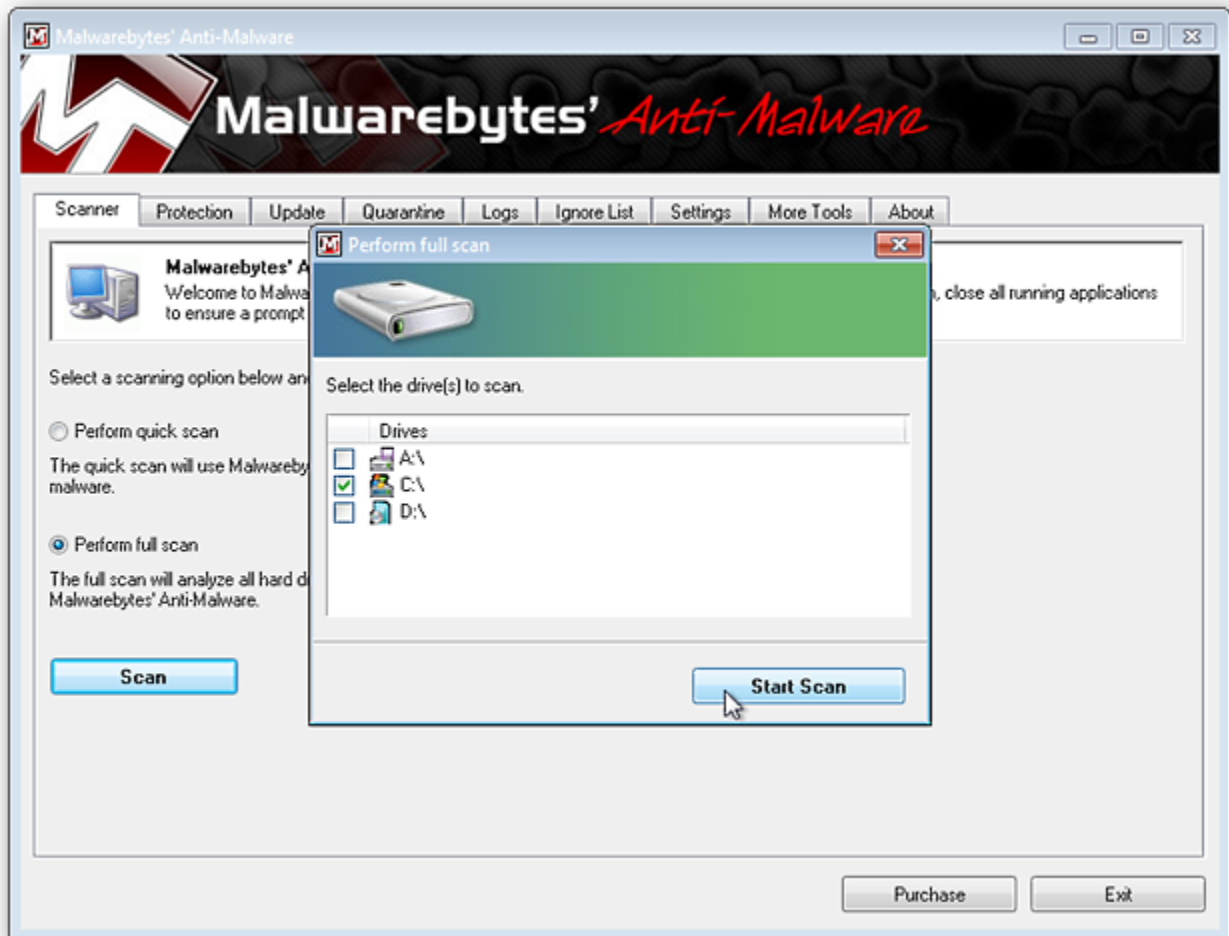


Scanning for Malware

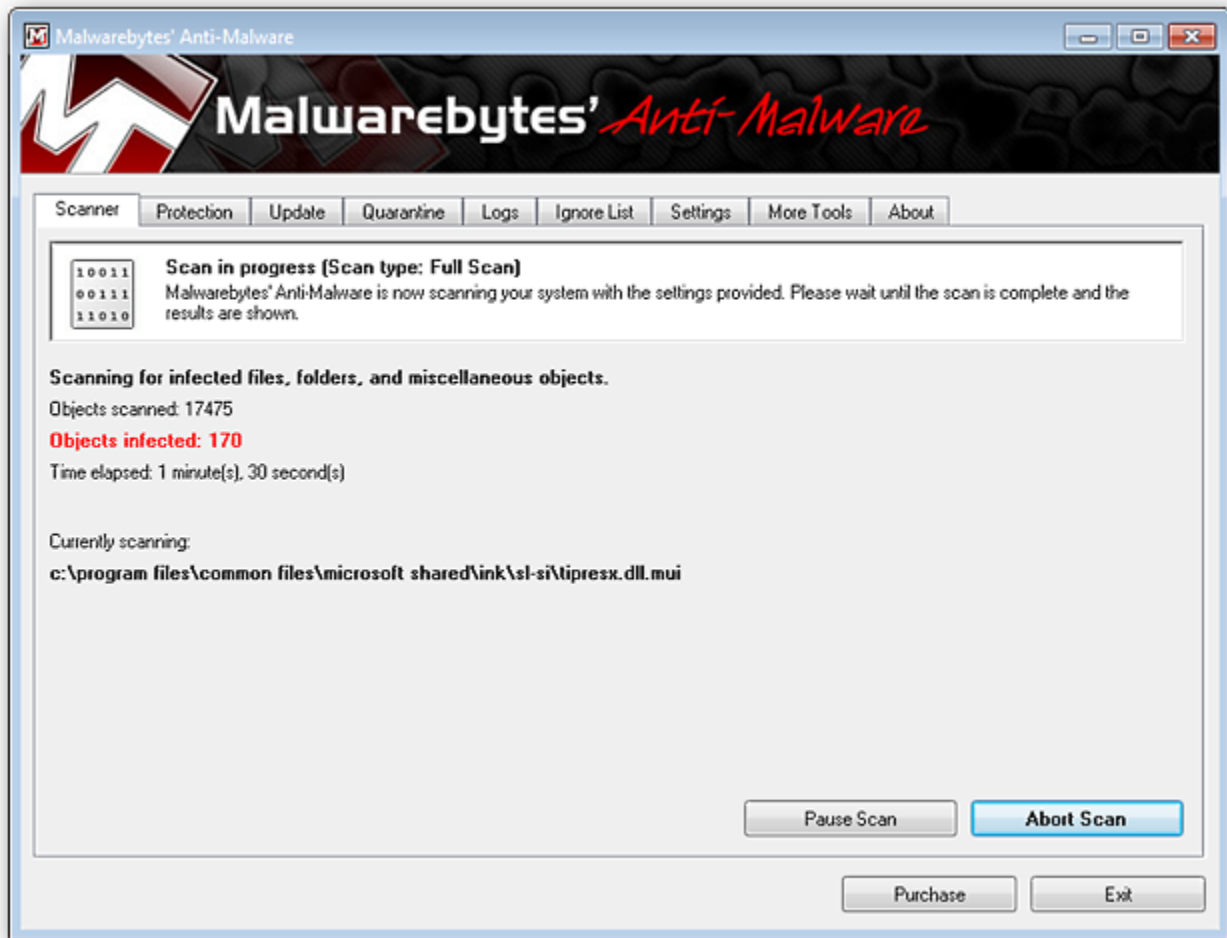
Once you have all the latest updates applied, it is time to start scanning. It is recommended to go with the "Perform full scan" setting. Click "Scan" to get started.



Once you have clicked “Scan”, you will see this pop up window asking you to choose which drives you would like to have scanned. Select the ones that you would liked to have scanned and click “Start Scan”.

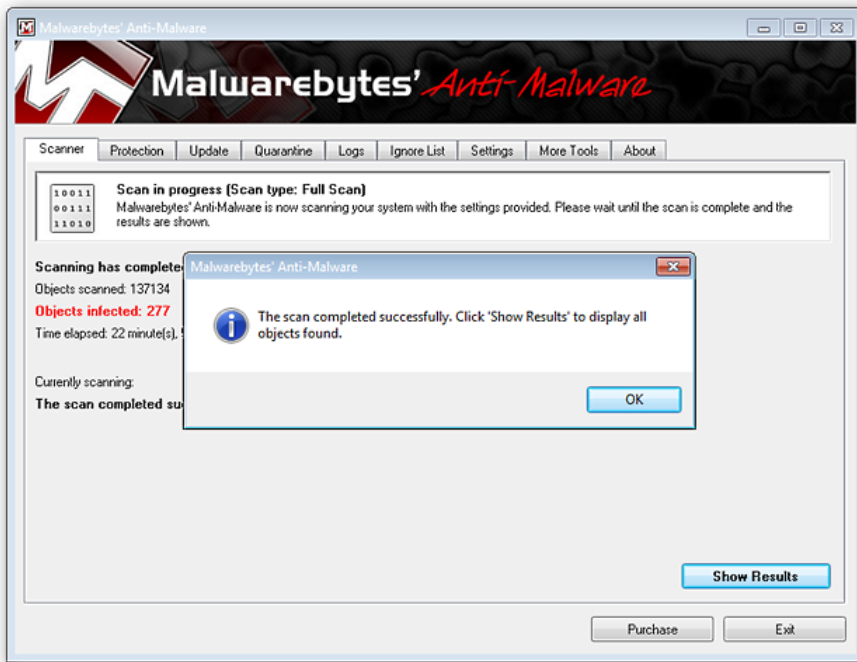


You can see what the scanning process looks like here. Malwarebytes' Anti-Malware found 170 infected files on our example system within the first 1.5 minutes...now that is quick! You can also see exactly where and what Malwarebytes' Anti-Malware is currently scanning.

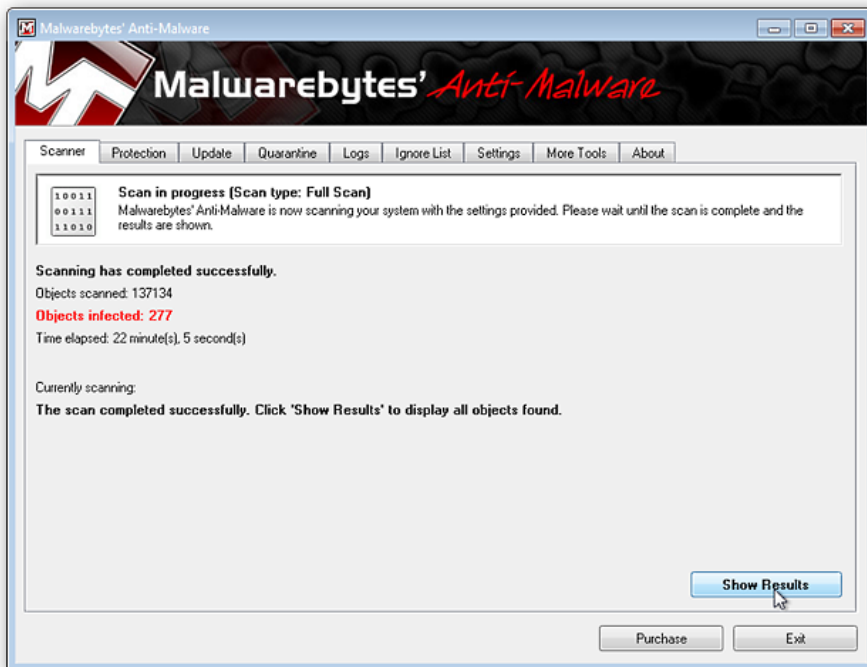


Once Scanning is Complete

Once Malwarebytes' Anti-Malware has finished scanning your computer, it will display the number of items scanned, the number of infected objects found, and time elapsed. Notice that it took less than 23 minutes to scan our example system! Click "OK" to close the Scan Complete Message Window.

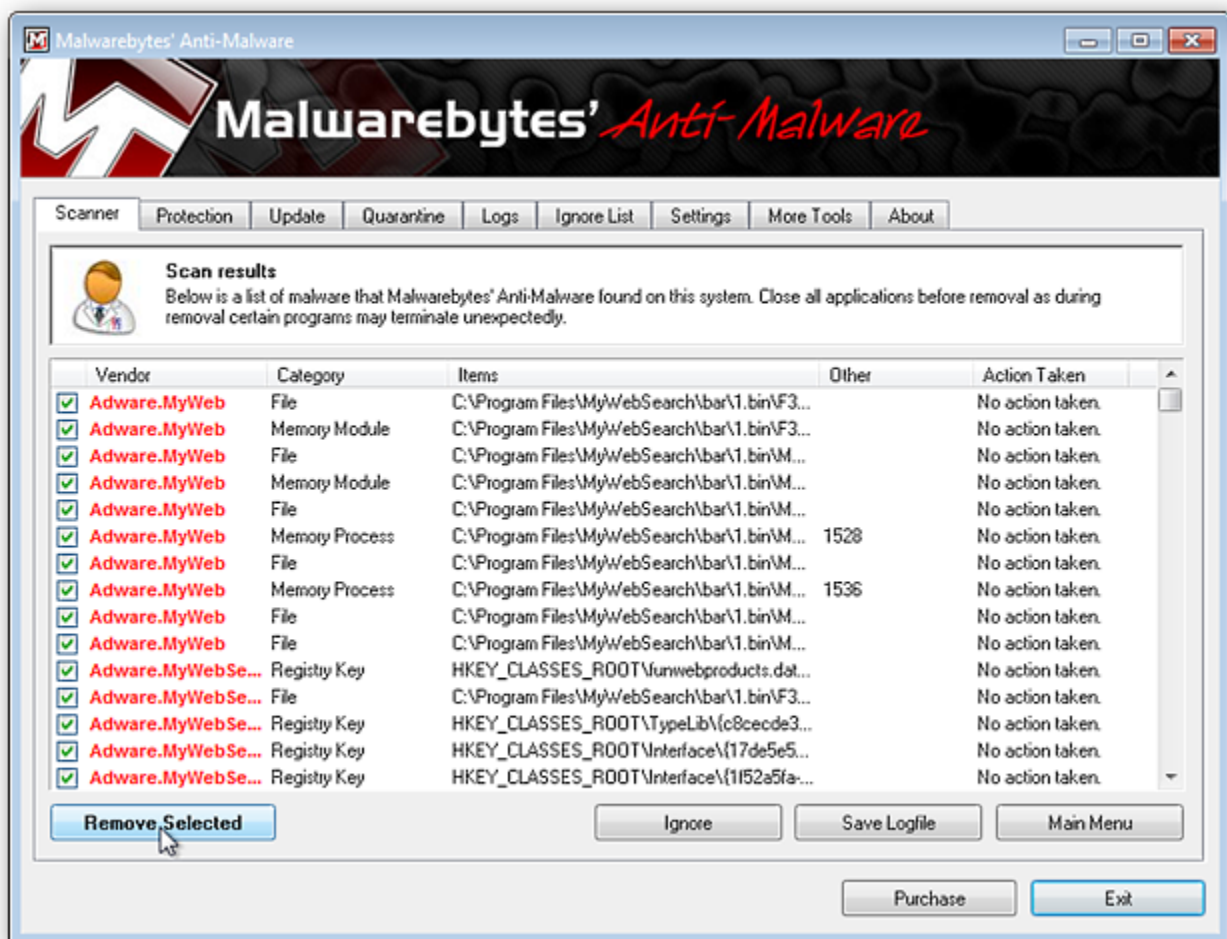


To see what Malwarebytes' Anti-Malware found, click "Show Results".

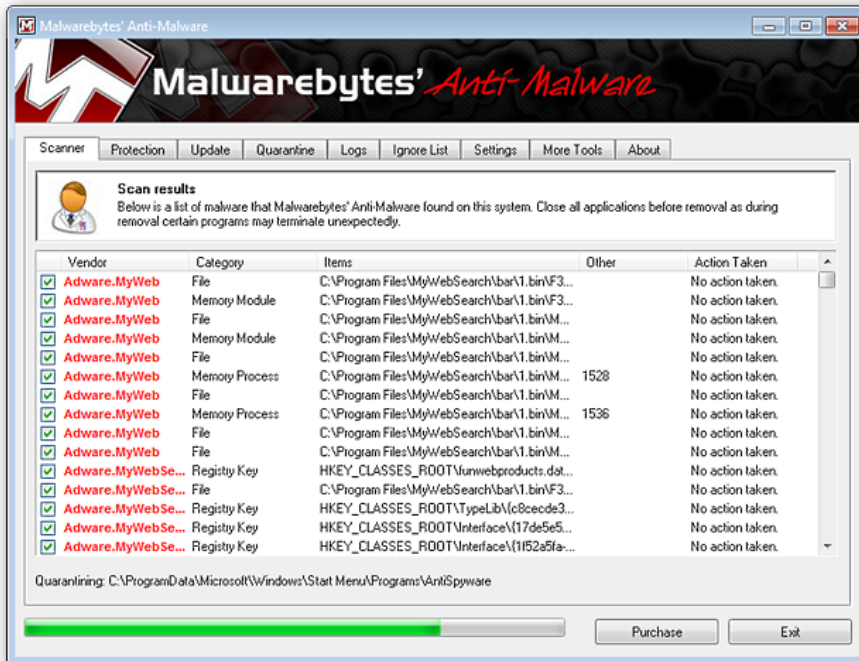


Removing the Malware

After clicking “Show Results”, you will see the following window with a compiled list of all malware objects found. You can see the names of the malware, category (i.e. file, memory process, registry key, etc.), and the location on your system. Notice that for the moment that “No action taken” is listed for everything. This allows you the opportunity to check for any false positives that might have occurred. Once you have looked over the list and verified the items that you want taken care of, click “Remove Selected” to remove the malware from your system.

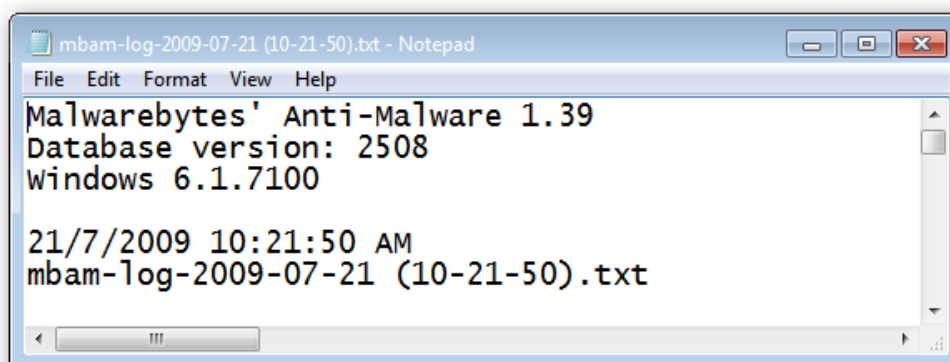


This is what the removal process looks like. As with other functions in Malwarebytes' Anti-Malware, this part of the process also goes very quickly (*wonderful!*).

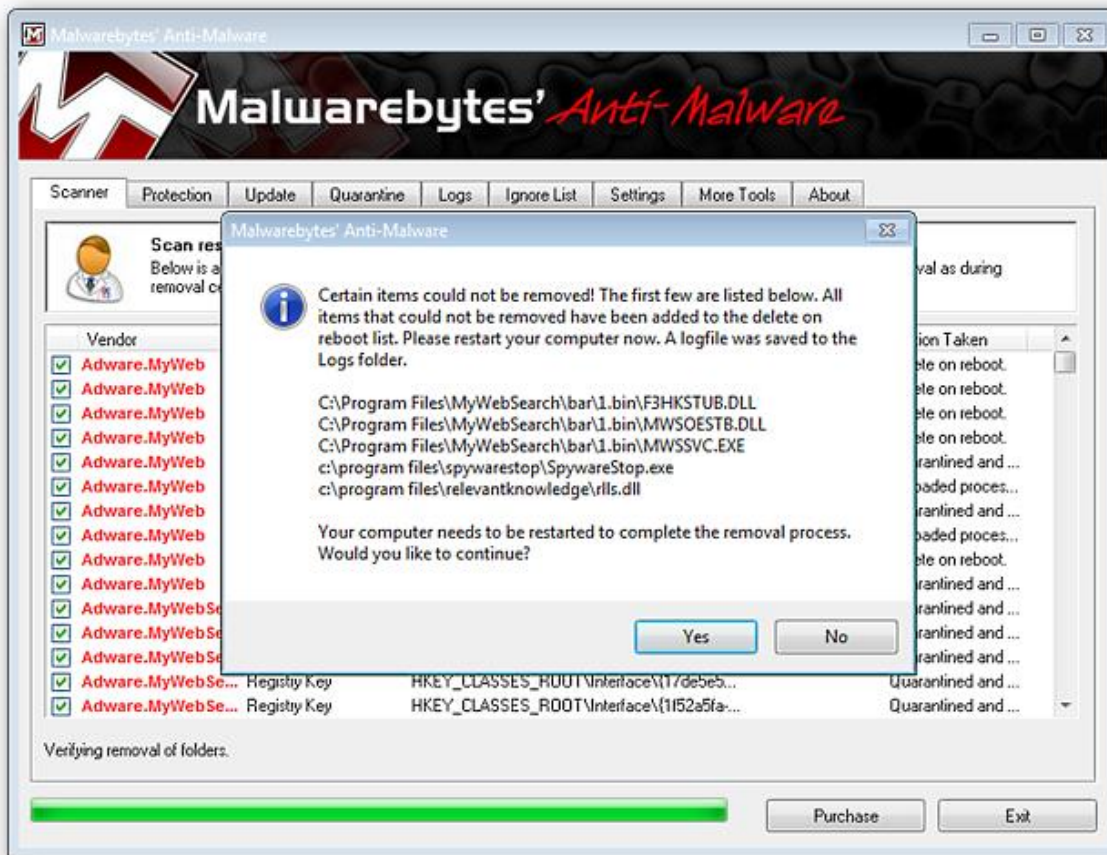


Once the Malware Removal is Completed and a Quick Look at the Reboot Request

Once Malwarebytes' Anti-Malware has finished removing the malware, it will automatically display a scan log like this.



If there are any malware problems that need to be removed during a reboot, you will see the following message detailing exactly what will be taken care of as soon as you restart your computer. Item removal during a reboot is extremely smooth and quick...on our example system the “cleanup reboot process” looked exactly like a normal reboot (*terrific!*). Click “Yes” to start the reboot process.



Conclusion

If you are looking for an anti-malware app that works quickly and well, then Malwarebytes' Anti-Malware is just the app for you. Malwarebytes' Anti-Malware works with a minimum of fuss and gets the job done, plain and simple.

[Download Malwarebytes' Anti-Malware \(version 1.39\)](#)