TimeStomp Evaluation

Contents

[Introduction 3](#_Toc42947864)

[Installing TimeStomp 3](#_Toc42947865)

[Disabling Windows Defender 5](#_Toc42947866)

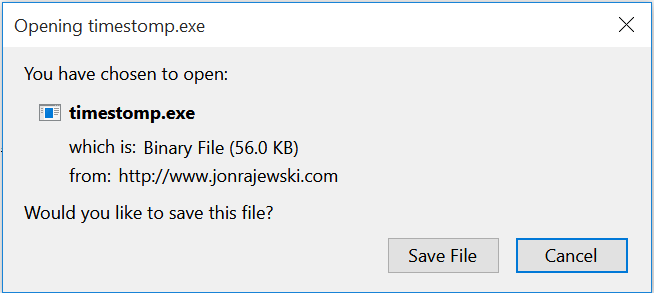
[Conclusions 6](#_Toc42947867)

# Introduction

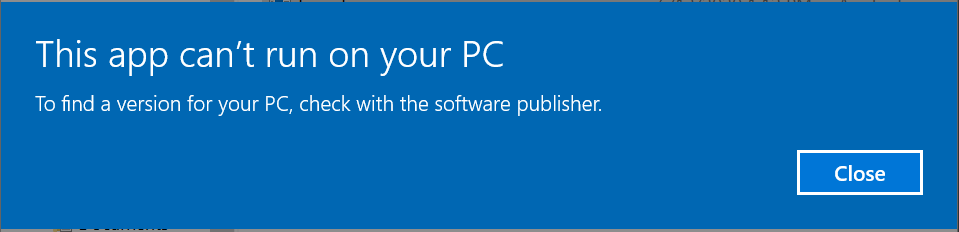
TimeStomp is a piece of anti-forensics software that is designed to edit the MACE (Modified-Accessed-Created-Entry) attributes of a file. These attributes, if left intact, can aid a forensic investigator in putting together a timeline for events on a computer. By carefully taking note of when suspicious files were created, where, and by whom, they might be able to determine how the breach occurred. If, however, we modify all these timestamps to read the same value, or to read completely random values the process of creating the timeline will be much more complex. This will slow down the rate of investigation, making it more time intensive, and therefore expensive, to complete an investigation of the case.

# Installing TimeStomp

My first step in installing TimeStomp was finding a website where it was available to be downloaded. Thankfully, former LCDI head Jon Rajewski has a copy of the tool available to download on his blog. You can find it, and other forensic resources, available at <https://www.jonrajewski.com/resources/>

To download the tool, I simply clicked on the “TimeStomp.exe” link under the “Anti-Forensic Tools” section of the page. When prompted by windows, I opted to save the file.  


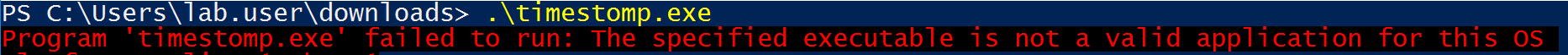
Doing this placed the “timestomp.exe” program into my windows downloads folder. Attempting to running this executable gave me the windows notice that “This app can’t run on your PC”



This error led me to seek out another sort of the program. I found a github repository of various cybersecurity tools maintained by the user codejanus. You can find the repository here <https://github.com/codejanus/ToolSuite>

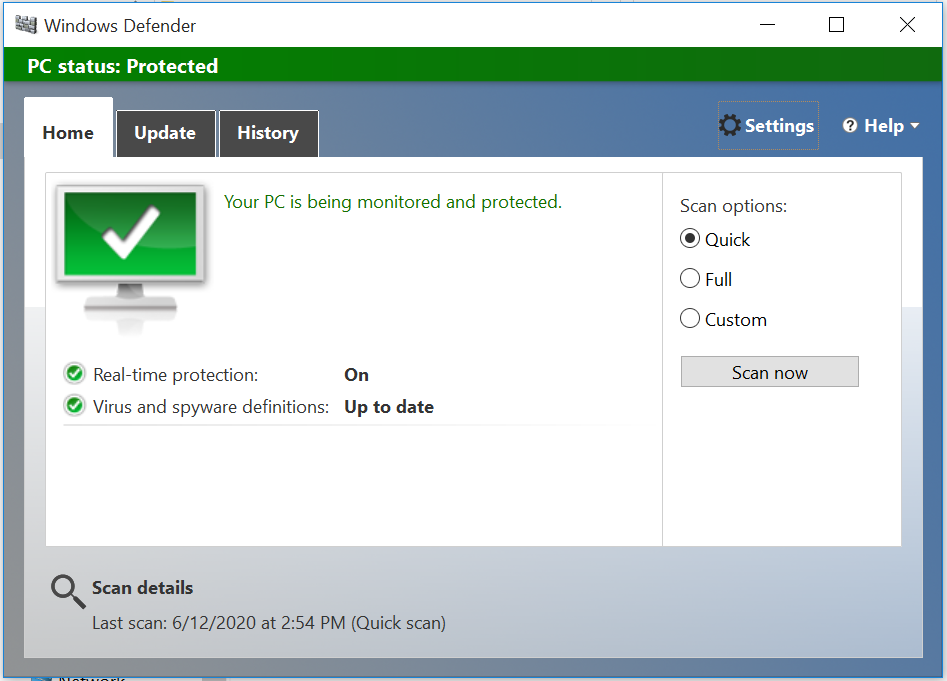
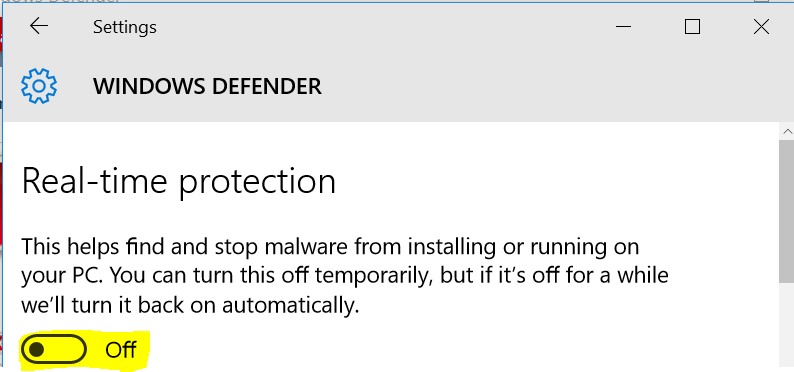
This repository contained a copy of timestomp that I attempted to download. While this version of the program did seem to run, it was also immediately detected by Windows Defender which detected it as a virus. I disabled Windows Defender following the steps underlined in the “Disabling Windows Defender” section.

After disabling Windows Defender, I redownloaded TimeStomp and attempted to run it both by trying to launch it as an application, as well as trying to call it at the powershell command line. Unfortunately, neither method worked, both displaying the same “This executable is not a valid application for this OS” error. For this reason, I was forced to seek out an alternative application that did work for Windows 10.



# Disabling Windows Defender

In order to complete the installation process for TimeStomp.exe, I was required to disable Windows Defender, which analyzed and detected the program as a virus. To do this, I took the following steps.

1. I launched Windows Defender and received the following view.  
   
2. I clicked the settings button visible in the upper right-hand corner in the above screenshot
3. In the windows setting menu that was created, I disabled Real-time protection. This would keep Windows Defender from actively trying to scan my PC while it was in use.  
   

With these steps completed, Windows Defender is disabled for long enough for the evaluation to be completed.

# Conclusions

While timestomp is one of the most referenced pieces of anti-forensics softwar, it does not appear to run on a basic Windows 10 installation. Windows 10 is an incredibly common operating system to find in modern enterprise environments as well as in home user use. If it is unable to affect these machines, the tool is unfortunately not worth considering.

However, timestomp is just one tool that can perform this type of technique. I will instead be analyzing other tools that should be able to edit the MACE values of files on Windows 10 systems.