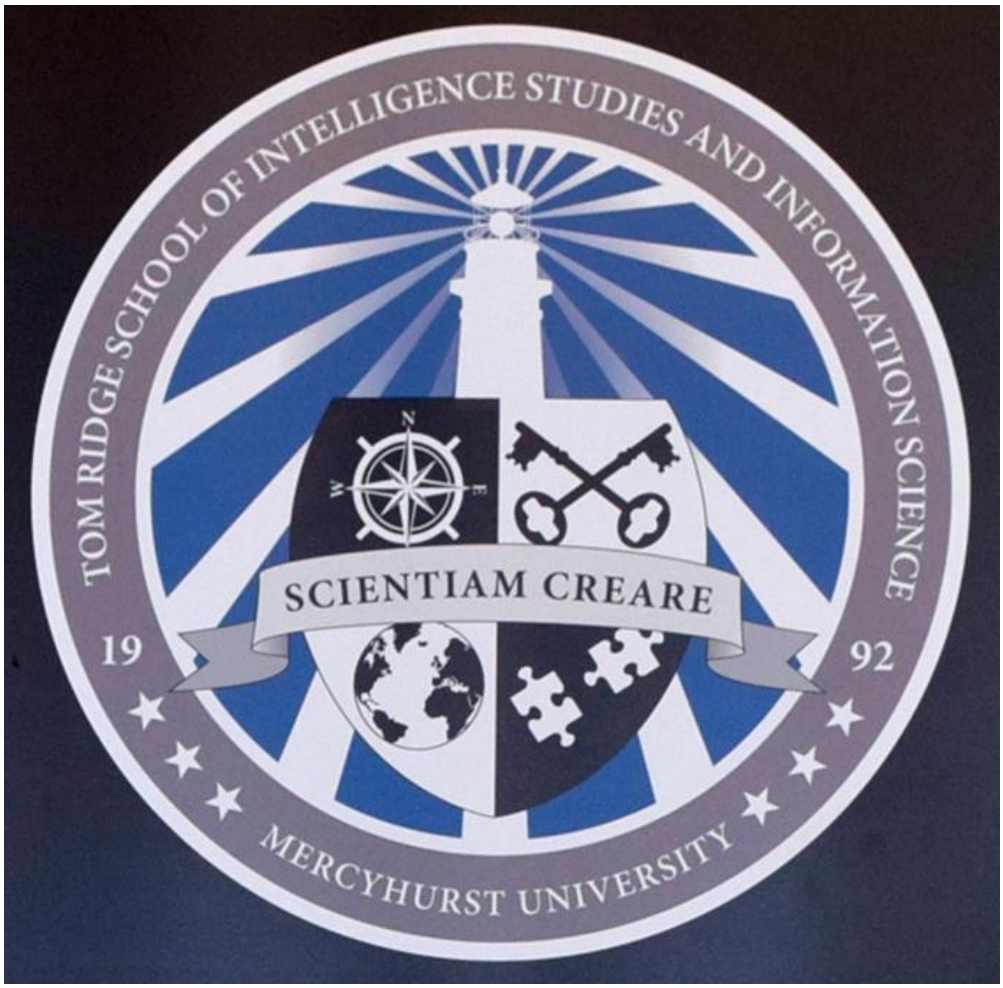
Jadyn Moore

Software Validation Report
CIS 262 - Digital Forensics



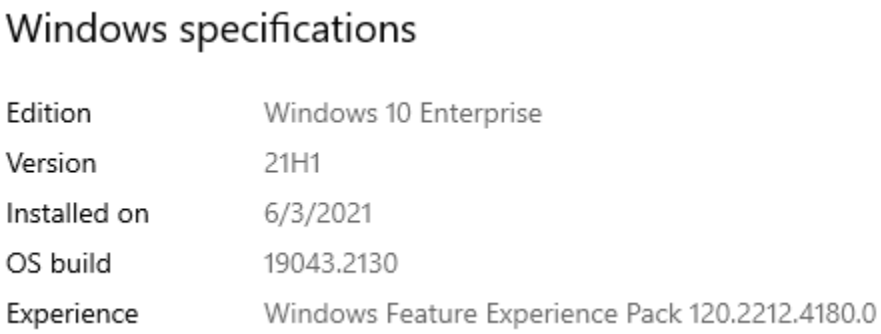
Tasking:

Jadyn Moore

Create a Forensic Validation Report regarding the usability / effectiveness of the software tool "Orion" Software USB Write Blocker. The URL/SITE for the tool is: [Orion USB Write Blocker - Orion Forensics LAB Thailand]

Important to know:

- Versions of software being used in test:
    - Version of Orion: v1.0.0
    - Windows specifications:



- Test media:
    - 30 GB USB Drive named TACO
    - File system: FAT32
    - Used Space: 30.2 MB
    - Free Space: 29.1

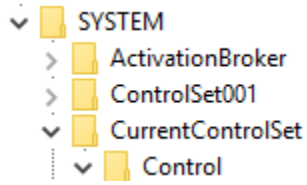
Summary:

The first step of our process is to give ourselves a basis of what proper write blocking is like. We will then be going through the process of how the Orion write blocker works, along with coming to a final conclusion of what we found throughout our testing. The general consensus of this study will be a reflection of our learnings, and testing.

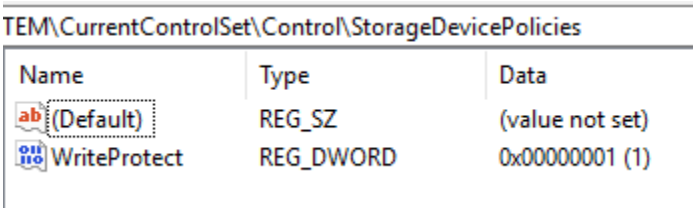
Part 1: Windows Registry

Jadyn Moore

1. Edit our windows registry by going into the following folder



2. We then right click on control to add ourselves a new key named StorageDevicePolicies
3. We make a new DWORD titled 32-bit value
4. The next move is to switch the value to one as shown below:



5. We test to see if this still works by removing the USB, reinserting it, and making sure we cannot write on any of our devices

Part 2: Walkthrough of Orion

Jadyn Moore

The following is a guide on how to use the “Orion” Software USB Write Blocker. This is an analysis of our tool based on its functionality and accessibility.

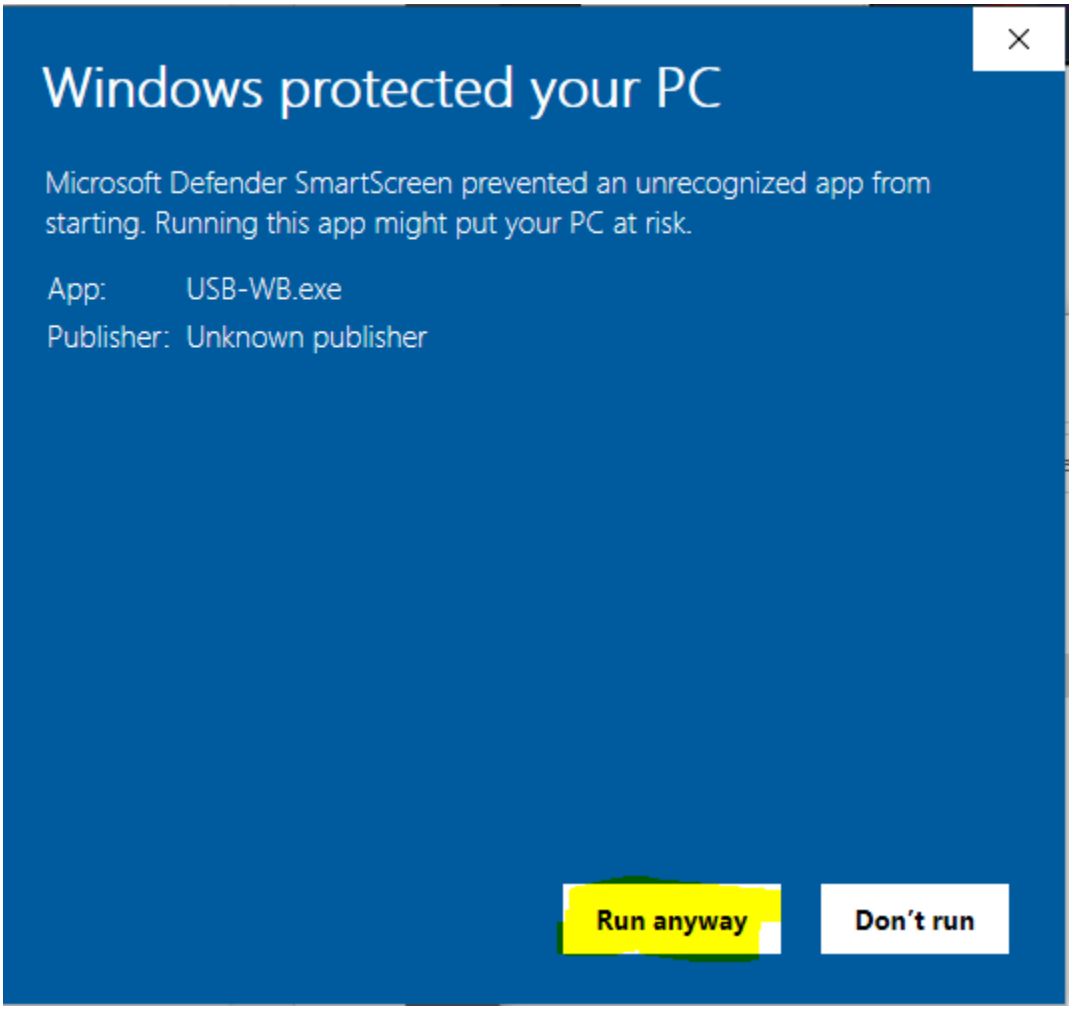
1. Download “Orion” at [Orion USB Write Blocker -Orion Forensics LAB Thailand]
2. After download has been completed, we are met with the following:

Name	Type	Compressed size	Password ...	Size	Ratio	Date modified
client.wyc	WYC File	54 KB	No	54 KB	1%	2/1/2016 8:49 PM
README	Microsoft Edge PDF Docu...	239 KB	No	256 KB	7%	2/9/2016 2:44 PM
USB-WB	Application	500 KB	No	632 KB	21%	2/4/2016 8:54 AM
USB-WB.exe.config	XML Configuration File	1 KB	No	1 KB	38%	2/1/2016 2:55 PM
wyUpdate	Application	180 KB	No	435 KB	59%	9/6/2012 6:04 AM

3. Out of this selection, choose our third one down:

USB-WB	Application	500 KB	No	632 KB	21%	2/4/2016 8:54 AM

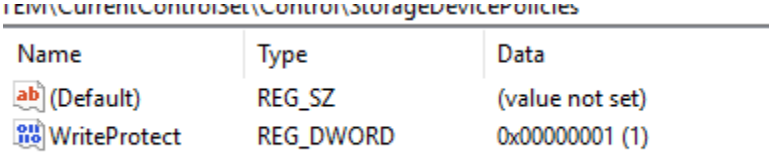
4. We will be met with the following screen:



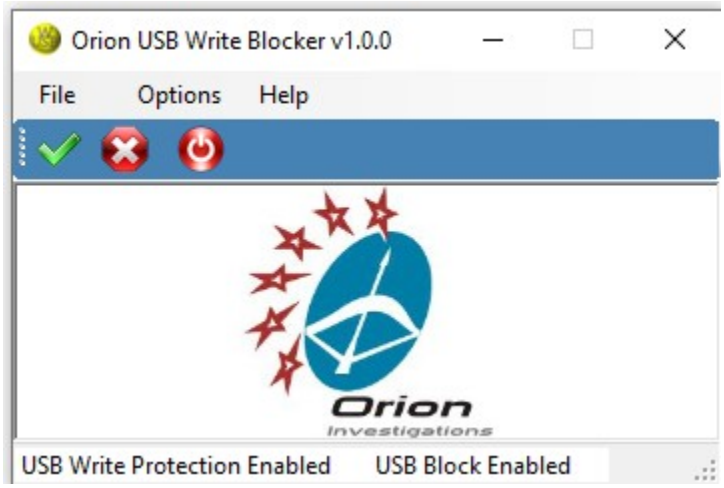
5. After clicking run anyway, the next popup we get is the Orion screen:

Jadyn Moore

6. We opened up regedit, and changed the value in DWORD from 0 to 1 to allow Orion to make our files only readable when activated. This is shown below:



7. It is as simple as clicking our checkmark for our write protection to be enabled:



Conclusion:

Jadyn Moore

The first part of our testing showed us how we could manually navigate ourselves through the thing that would be automated in our next test. This testing was important, that way we could understand the logistics of what is going on in the background during automation.
In section 2, we see that Orion is rather capable. The use of a switch on/off to determine whether or not we could write on our USB was much more convenient, and worked smoother than I expected. With all this being put on the table I believe it is safe to say that Orion is most definitely capable as a USB write blocker software tool.