**Lab Assignment 10:**

**Malware Traffic Applied**

Micah Flack

Department of Computer Science, Dakota State University

CSC-840-DT1, Cyber Operations I

Dr. Michael Ham

November 3, 2022

1. For sample01.exe take a screenshot of any evidence you found that would indicate this

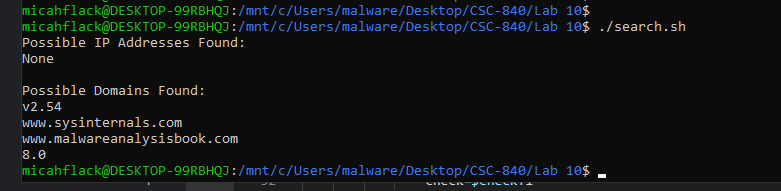
file makes some sort of network connection.





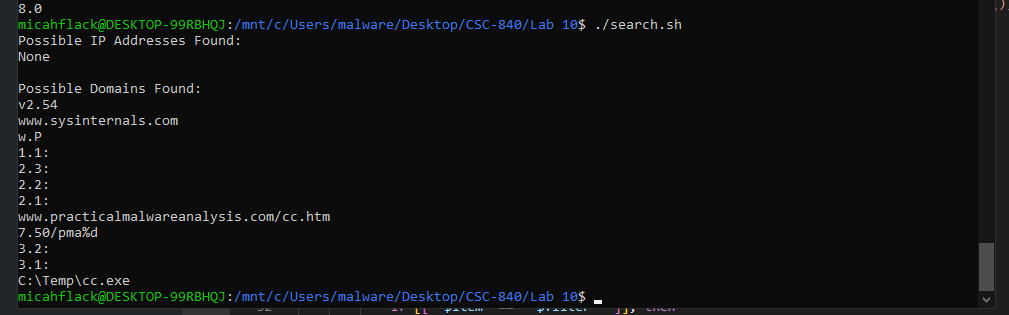
2. Take a screenshot of the output that your script produces when ran against strings.txt.

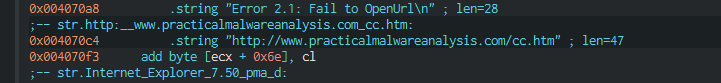
Upload your script to the dropbox as well.



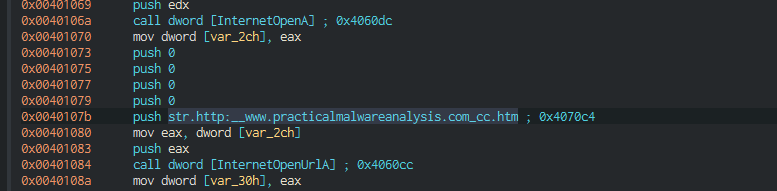
3. Take a screenshot showing how sample02.exe is trying to communicate. Either in the

screenshot or text below, show what URL it is trying to communicate with.





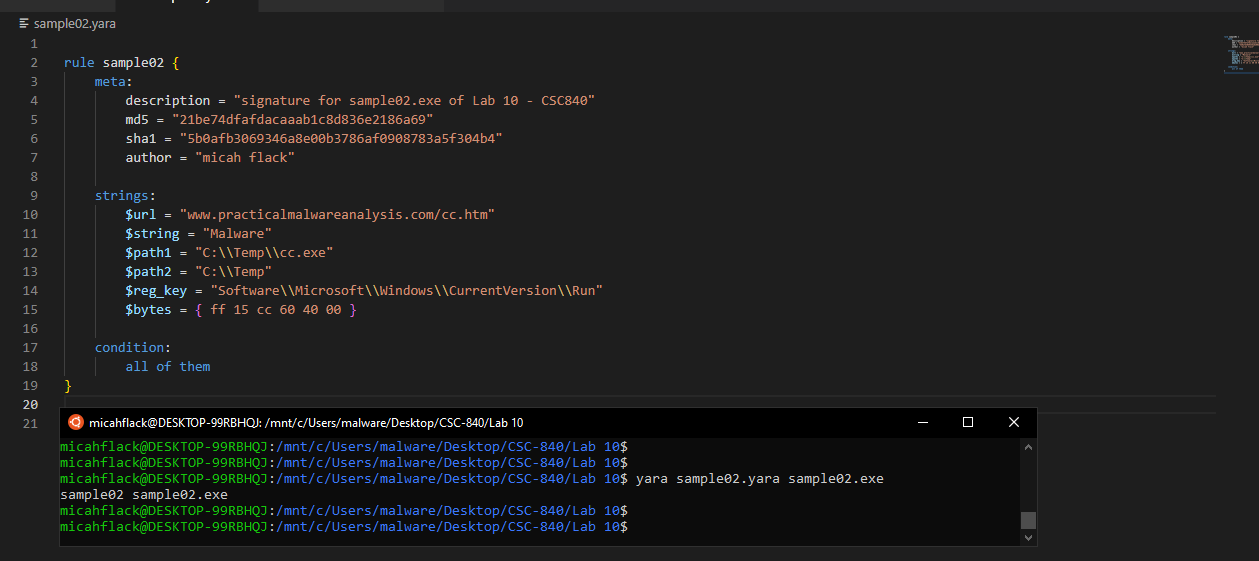
^ Which is XREF’d by the function call to InternetOpenUrlA()



[**http://www.practicalmalwareanalysis.com/cc.htm**](http://www.practicalmalwareanalysis.com/cc.htm)

4. Take a screenshot of your YARA rule alongside of the output from running YARA against

the sample02.exe file with your rule.



5. Take a screenshot of the file you pulled out of the packet capture. It is not the text file,

but something else. Open the file in front of Wireshark and take a screenshot.

