\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

As you edit this file, type your name here

NO COLLABORATION OF ANY KIND

CMSC 491/691 Malware Analysis

Midterm Exam Spring 2019

Extract midterm2019.7z on a Windows XP virtual machine. The password is infected. Use basic static analysis tools to answer the following questions about midterm2019.exe:

1. Is midterm2019.exe packed? Justify your answer with three reasons. (9 pts)  
     
   Packed (Y/N):
2. List five strings, imports, and/or metadata in midterm2019.exe that you believe are suspicious. Describe why each of them is suspicious. (10 pts)

Prepare any tools you need to perform basic dynamic analysis and set your VM to **Internal Network**. Take a snapshot of your VM so that you can easily revert to this point later. Run midterm2019.exe and answer the following questions:

1. Where does midterm2019.exe copy itself to? Make sure to list the full file path. (2 pts)
2. What other PE files does the malware create, if any? (4 pts)
3. How does the malware gain persistence? (4 pts)

Use IDA Pro to answer the following question about midterm2019.exe:

1. In a sentence or two, summarize what sub\_401428 in midterm2019.exe does. (8 pts)
2. In a few sentences, summarize what sub\_4011FA does. How long is the timer set? (10 pts)
3. In a few sentences, summarize what sub\_4012D9 (StartAddress) does. (8 points)
4. Why does the malware call gethostbyname at 0x4012E4? (4 pts)

Regarding the file that midterm2019.exe creates at 0x4014F0:

1. Provide a detailed analysis (at least one paragraph) of what this file does. Make sure to describe which Windows API functions are used perform any malicious activity. (16 pts)
2. This file creates a .txt file on the infected system. What is the full path of the .txt file? Provide a screenshot of its contents. (9 pts)

Regarding the file that midterm2019.exe creates at 0x4015D8:

1. Provide a detailed analysis (at least one paragraph) of what this file does. Make sure to describe which Windows API functions are used perform any malicious activity. (16 pts)