CMSC 491/691 Malware Analysis HW 2

Name: Daniel Roh
Assigned: 2/10/2020
Due: 2/19/2020 by 5:00pm

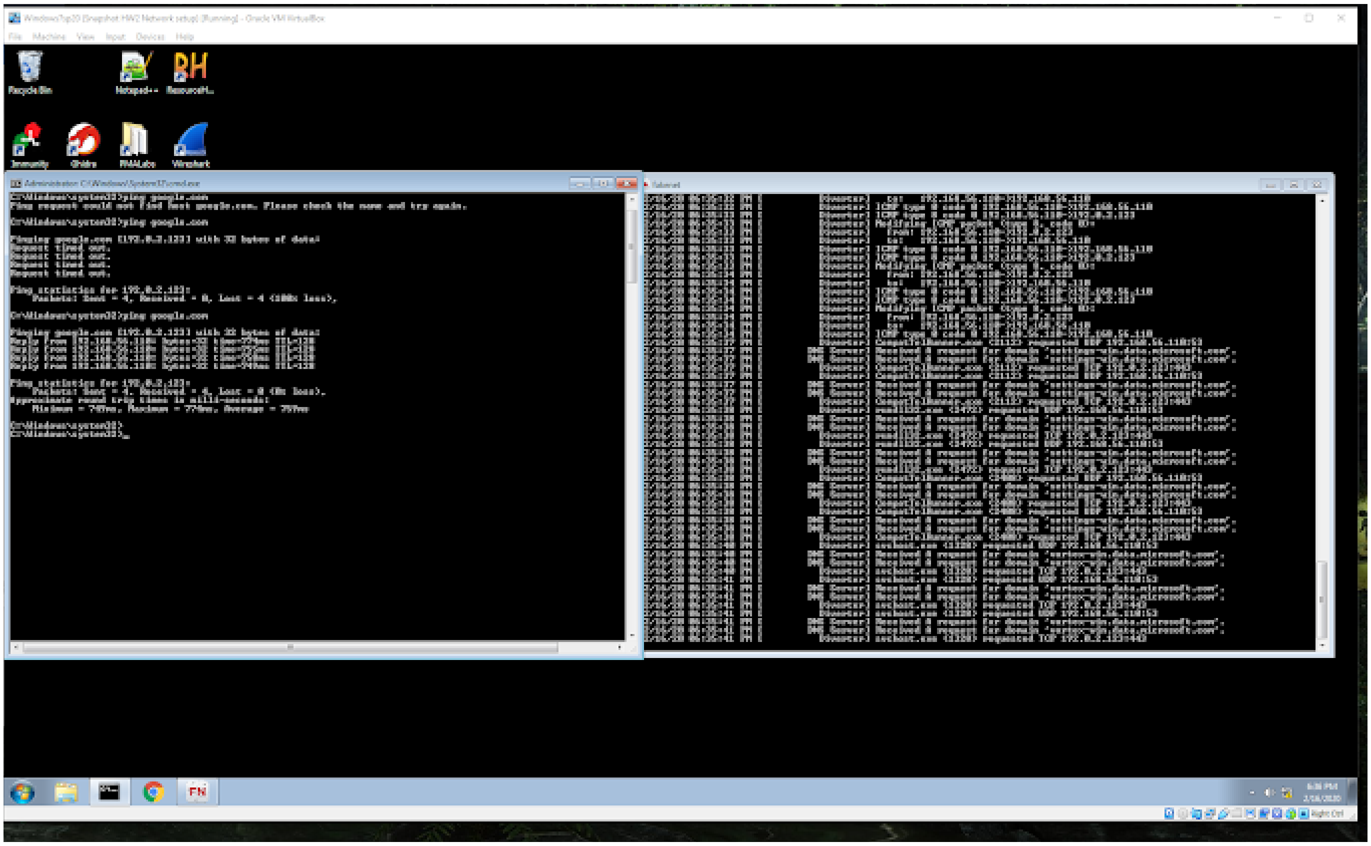
Download and extract hw2.7z on a virtual machine. The password to the zip file is "infected", without the quotes. The file contains hw2.exe and hw2_2.exe, which are live malware samples.

Once you have downloaded the malware, use the network settings in VirtualBox to set your VM to Host-only mode. **You should only run the malware while your VM is not connected to the internet!**

Hint: Chapter 3 of your Practical Malware Analysis textbook is a great resource, and other parts of your textbook may be helpful as well!

Part 1: hw2.exe (50 pts)

1) Follow the FakeNet-NG network config instructions on the course website. Provide a screenshot of your VM once you have completed step 9, showing a successful ping command while FakeNet-NG is running. (10 pts)

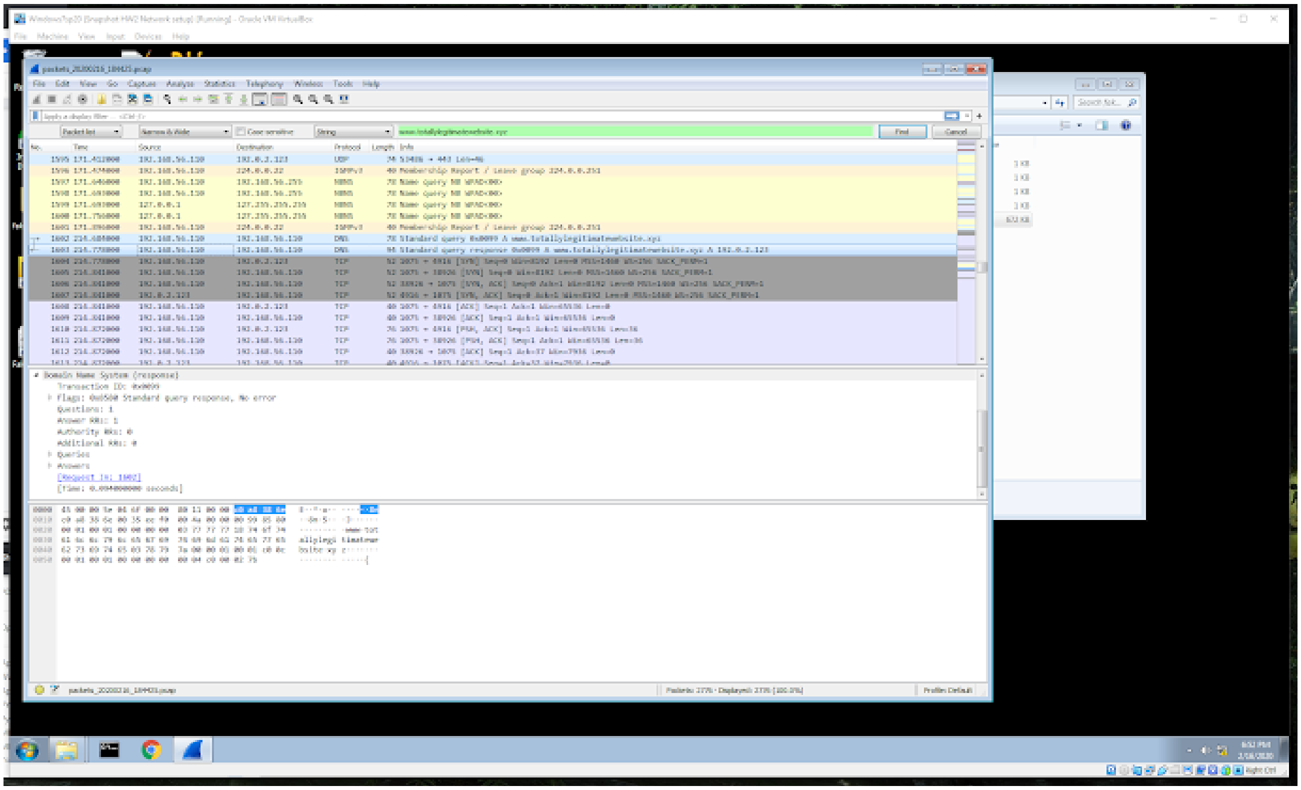


```
C:\Windows\system32>ping google.com
Ping request could not find host google.com. Please check the name and try again.

C:\Windows\system32>ping google.com

Pinging google.com [192.0.2.123] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.0.2.123:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Windows\system32>ping google.com

Pinging google.com [192.0.2.123] with 32 bytes of data:
Reply from 192.168.56.118: bytes=32 time=[illegible] TTL=128
Reply from 192.168.56.118: bytes=32 time=[illegible] TTL=128
Reply from 192.168.56.118: bytes=32 time=[illegible] TTL=128
Reply from 192.168.56.118: bytes=32 time=[illegible] TTL=128

Ping statistics for 192.0.2.123:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = [illegible], Maximum = [illegible], Average = [illegible]

C:\Windows\system32>
C:\Windows\system32>_
```

2) Run FLOSS on hw2.exe. A domain name is encoded within the file. What is the domain name? (8 pts)

- www.totallylegitimatewebsite.xyz

3) With FakeNet-NG running, run hw2.exe. After the malware runs for about a minute, open the .pcap file of your FakeNet-NG session using Wireshark. Provide a screenshot of the DNS query that the malware made to the domain from question 2. (12 pts)


packets_20200216_184425.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Packet list
Narrow & Wide
Case sensitive
String
www.totallylegitimatewebsite.xyz
Find
Cancel

```
No.   Time        Source           Destination      Protocol Length Info
1595 171.412000  192.168.56.130   192.0.2.123      UDP      74 53486 → 443 Len=46
1596 171.474000  192.168.56.130   224.0.0.22       IGMPv3   40 Membership Report / Leave group 224.0.0.251
1597 171.646000  192.168.56.130   192.168.56.255   NBNS     78 Name query NB WPAD<00>
1598 171.693000  192.168.56.130   192.168.56.255   NBNS     78 Name query NB WPAD<00>
1599 171.693000  127.0.0.1        127.255.255.255  NBNS     78 Name query NB WPAD<00>
1600 171.756000  127.0.0.1        127.255.255.255  NBNS     78 Name query NB WPAD<00>
1601 171.896000  192.168.56.130   224.0.0.22       IGMPv3   40 Membership Report / Leave group 224.0.0.251
1602 214.684000  192.168.56.130   192.168.56.130   DNS      78 Standard query 0x0099 A www.totallylegitimatewebsite.xyz
1603 214.778000  192.168.56.130   192.168.56.130   DNS      94 Standard query response 0x0099 A www.totallylegitimatewebsite.xyz A 192.0.2.123
1604 214.778000  192.168.56.130   192.0.2.123      TCP      52 1071 → 4916 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1605 214.841000  192.168.56.130   192.168.56.130   TCP      52 1071 → 10926 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1606 214.841000  192.168.56.130   192.168.56.130   TCP      52 10926 → 1071 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1607 214.841000  192.0.2.123      192.168.56.130   TCP      52 4916 → 1071 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1608 214.841000  192.168.56.130   192.0.2.123      TCP      40 1071 → 4916 [ACK] Seq=1 Ack=1 Win=65536 Len=0
1609 214.841000  192.168.56.130   192.168.56.130   TCP      40 1071 → 10926 [ACK] Seq=1 Ack=1 Win=65536 Len=0
1610 214.872000  192.168.56.130   192.0.2.123      TCP      76 1071 → 4916 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=36
1611 214.872000  192.168.56.130   192.168.56.130   TCP      76 1071 → 10926 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=36
1612 214.872000  192.168.56.130   192.168.56.130   TCP      40 10926 → 1071 [ACK] Seq=1 Ack=37 Win=7936 Len=0
1613 214.872000  192.0.2.123      192.168.56.130   TCP      40 4916 → 1071 [ACK] Seq=1 Ack=37 Win=7936 Len=0
```

```
Domain Name System (response)
    Transaction ID: 0x0099
  > Flags: 0x8500 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  > Answers
    [Request In: 1602]
    [Time: 0.094000000 seconds]
```

packets_20200216_184425.pcap | Packets: 2776 · Displayed: 2776 (100.0%) | Profile: Default

4) The malware opens multiple network connections to the same destination IP address and port. What port does the malware connect to? What is one of the ports that the malware listens on? How did you find this information? (8 pts)

- The malware connects to port 4916
- One of the ports that the malware listens on is port 1032
- This information was found by taking a look at the source and destination ip addresses. Since the source was 192.168.56.110 and the destination which I assume was the malware on wireshark was 192.0.3.123. After looking at 192.9.3.123 calls to the computer, I found that port 1032 was the one port that was constantly being used.

5) Connect to an IP address and port that the malware is listening on. What command did you use to do this? What malicious behavior is the network connection being used for? (12 pts)

- “Question 1.5 is FOBAR’ed” - Dr. Nickolas

Part 2: hw2_2.exe (50 pts)

Note: When you run the malware, it seems to crash explorer.exe if you press any keys while in the VM.

1) Investigate the strings of hw2_2.exe. Answer the following questions: (8 pts)

a) What IP address is listed in the strings?

- 192.168.123.194

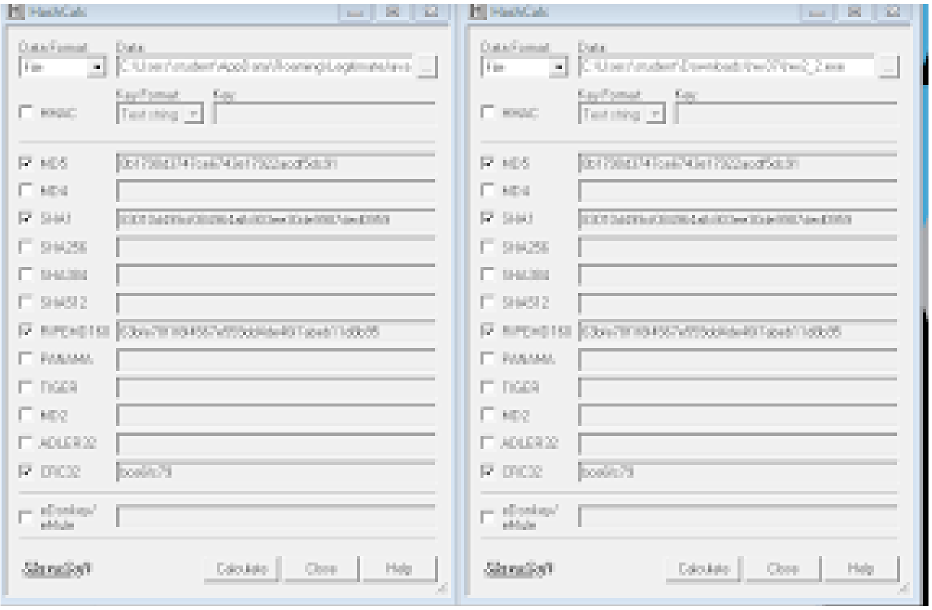
b) What suspicious mutex is listed in the strings?

- CheckOutThisSuperUniqueMutex

2) Run hw2_2.exe. Where does the malware copy itself to? How did you find this information? Show that hw2_2.exe and the copied file are identical. (10 pts)

- C:\Users\student\AppData\Roaming\LegitimateJavaPlugin\javaplugin.exe
- This information was found by using regshot to take a snapshot of the registry before and after the malware was run. After the malware was run a comparison of the two were used to produce a txt file of all of the changes made to the registry. After looking at the changed made, one line for the malware's persistence was found which pointed to the location that the malware was now moved too and "disguised"

- MD5 Hash of HW2.2.exe: 0b1790d3747ce6743e17922acdf5dc91
- MD5 Hash of JavaPlugin.exe: 0b1790d3747ce6743e17922acdf5dc91



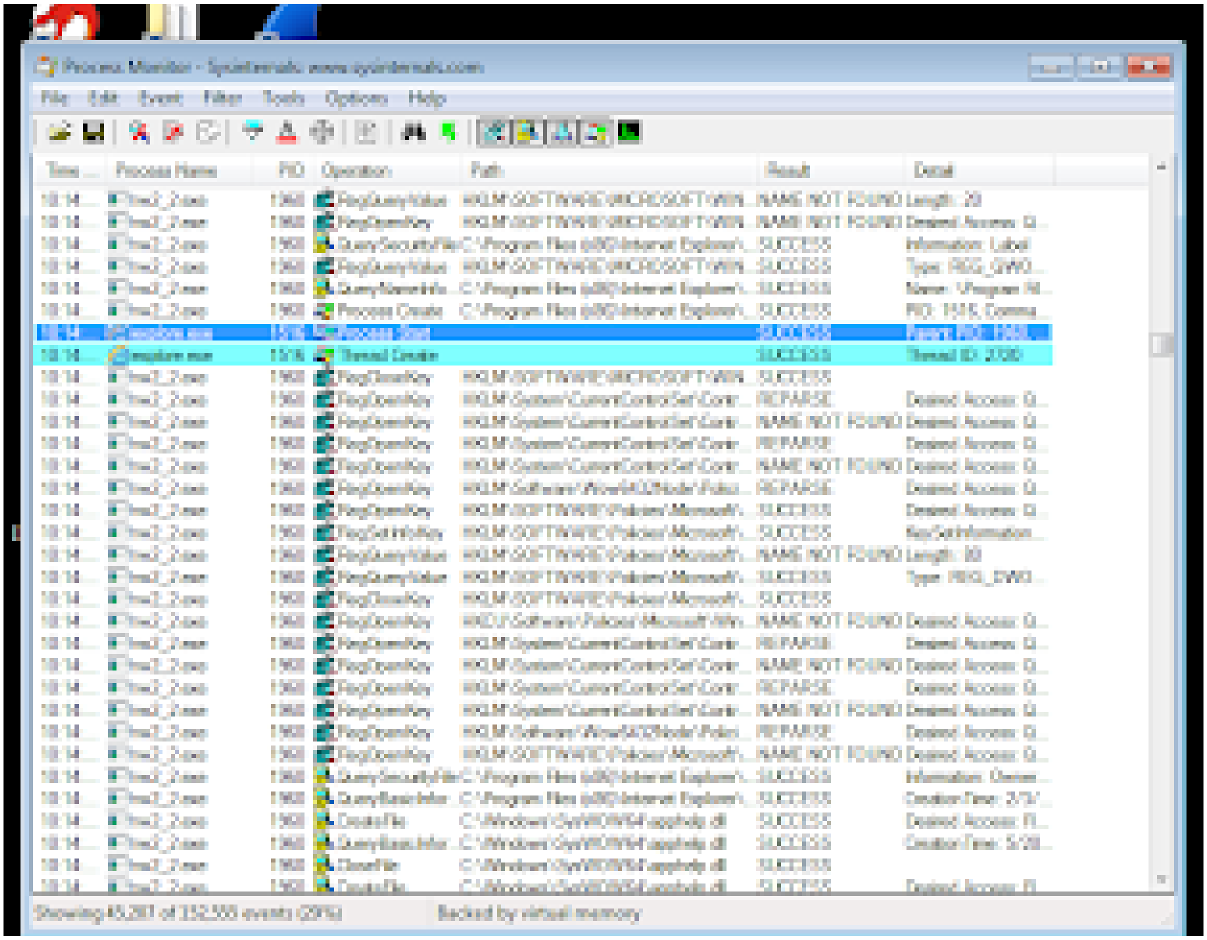
3) What is the registry key that the malware uses for persistence? What is the full file path of the file that is made persistent? How did you find this information? (12 pts)

- HKU\S-1-5-21-419295087-873244694-3473264175-1001\Software\Microsoft\Windows\CurrentVersion\Run\NotASuspiciousJavaPlugin:"C:\Users\student\AppData\Roaming\LegitimateJavaPlugin\javaplugin.exe"
- "C:\Users\student\AppData\Roaming\LegitimateJavaPlugin\javaplugin.exe"

- This information was found by using regshot to take a shot of the registry and then taking another shot of the registry after the malware was run. From there by using the regshot compare tool, a list of all of the changed registries where listed in which the malwares persistences change was caught

4) What is the name of the process that hw2_2.exe creates? What is its PID? Provide a screenshot of this process creation in Procmon. (10 pts)

- The process that hw2_2.exe creates is iexplore.exe
- The PID is 1516



Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

```
Time ...  Process Name   PID   Operation          Path                                          Result          Detail
10:14...  hw2_2.exe      1968  RegQueryValue      HKLM\SOFTWARE\MICROSOFT\WIN...                NAME NOT FOUND  Length: 20
10:14...  hw2_2.exe      1968  RegOpenKey         HKLM\SOFTWARE\MICROSOFT\WIN...                NAME NOT FOUND  Desired Access: Q...
10:14...  hw2_2.exe      1968  QuerySecurityFile  C:\Program Files (x86)\Internet Explorer\...  SUCCESS         Information: Label
10:14...  hw2_2.exe      1968  RegQueryValue      HKLM\SOFTWARE\MICROSOFT\WIN...                SUCCESS         Type: REG_DWO...
10:14...  hw2_2.exe      1968  QueryNameInfo...   C:\Program Files (x86)\Internet Explorer\...  SUCCESS         Name: \Program Fi...
10:14...  hw2_2.exe      1968  Process Create     C:\Program Files (x86)\Internet Explorer\...  SUCCESS         PID: 1516, Comma...
10:14...  iexplore.exe   1516  Process Start                                                    SUCCESS         Parent PID: 1968,...
10:14...  iexplore.exe   1516  Thread Create                                                    SUCCESS         Thread ID: 2700
10:14...  hw2_2.exe      1968  RegCloseKey        HKLM\SOFTWARE\MICROSOFT\WIN...                SUCCESS
10:14...  hw2_2.exe      1968  RegOpenKey         HKLM\System\CurrentControlSet\Contr...        REPARSE         Desired Access: Q...
10:14...  hw2_2.exe      1968  RegOpenKey         HKLM\System\CurrentControlSet\Contr...        NAME NOT FOUND  Desired Access: Q...
10:14...  hw2_2.exe      1968  RegOpenKey         HKLM\System\CurrentControlSet\Contr...        REPARSE         Desired Access: Q...
10:14...  hw2_2.exe      1968  RegOpenKey         HKLM\System\CurrentControlSet\Contr...        NAME NOT FOUND  Desired Access: Q...
10:14...  hw2_2.exe      1968  RegOpenKey         HKLM\Software\Wow6432Node\Polici...           REPARSE         Desired Access: Q...
10:14...  hw2_2.exe      1968  RegOpenKey         HKLM\SOFTWARE\Policies\Microsoft\...          SUCCESS         Desired Access: Q...
10:14...  hw2_2.exe      1968  RegSetInfoKey      HKLM\SOFTWARE\Policies\Microsoft\...          SUCCESS         KeySetInformation...
10:14...  hw2_2.exe      1968  RegQueryValue      HKLM\SOFTWARE\Policies\Microsoft\...          NAME NOT FOUND  Length: 20
10:14...  hw2_2.exe      1968  RegQueryValue      HKLM\SOFTWARE\Policies\Microsoft\...          SUCCESS         Type: REG_DWO...
10:14...  hw2_2.exe      1968  RegCloseKey        HKLM\SOFTWARE\Policies\Microsoft\...          SUCCESS
10:14...  hw2_2.exe      1968  RegOpenKey         HKCU\Software\Policies\Microsoft\Win...       NAME NOT FOUND  Desired Access: Q...
10:14...  hw2_2.exe      1968  RegOpenKey         HKLM\System\CurrentControlSet\Contr...        REPARSE         Desired Access: Q...
10:14...  hw2_2.exe      1968  RegOpenKey         HKLM\System\CurrentControlSet\Contr...        NAME NOT FOUND  Desired Access: Q...
10:14...  hw2_2.exe      1968  RegOpenKey         HKLM\System\CurrentControlSet\Contr...        REPARSE         Desired Access: Q...
10:14...  hw2_2.exe      1968  RegOpenKey         HKLM\System\CurrentControlSet\Contr...        NAME NOT FOUND  Desired Access: Q...
10:14...  hw2_2.exe      1968  RegOpenKey         HKLM\Software\Wow6432Node\Polici...           REPARSE         Desired Access: Q...
10:14...  hw2_2.exe      1968  RegOpenKey         HKLM\SOFTWARE\Policies\Microsoft\...          NAME NOT FOUND  Desired Access: Q...
10:14...  hw2_2.exe      1968  QuerySecurityFile  C:\Program Files (x86)\Internet Explorer\...  SUCCESS         Information: Owner...
10:14...  hw2_2.exe      1968  QueryBasicInfor... C:\Program Files (x86)\Internet Explorer\...  SUCCESS         CreationTime: 2/3/...
10:14...  hw2_2.exe      1968  CreateFile         C:\Windows\SysWOW64\apphelp.dll               SUCCESS         Desired Access: R...
10:14...  hw2_2.exe      1968  QueryBasicInfor... C:\Windows\SysWOW64\apphelp.dll               SUCCESS         CreationTime: 5/20...
10:14...  hw2_2.exe      1968  CloseFile          C:\Windows\SysWOW64\apphelp.dll               SUCCESS
10:14...  hw2_2.exe      1968  CreateFile         C:\Windows\SysWOW64\apphelp.dll               SUCCESS         Desired Access: R...
Showing 45,207 of 152,555 events (29%)    Backed by virtual memory
```

5) Investigate the process from question 4 in Process Explorer. What DLL is loaded by this process that does not have the company name “Microsoft Corporation”? What is the full file path of this DLL? (10 pts)

- SecureDLL.dll
- C:\Users\student\Downloads\hw2\SecureDLL.dll