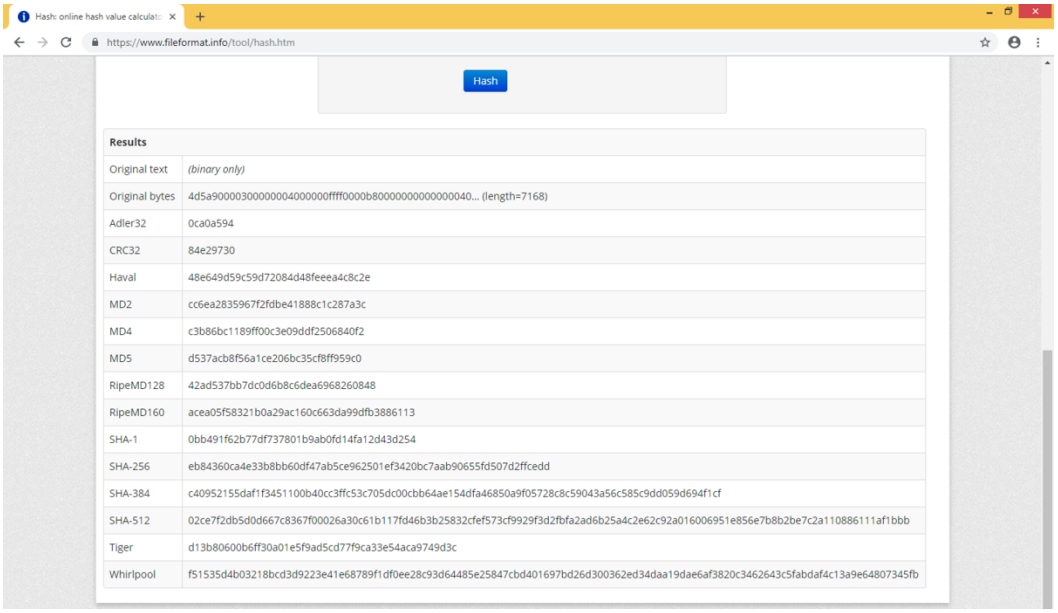
The purpose of this lab is to use all of the basic static and dynamic tools we have covered in class to construct our own examples of usage. For this lab, I am going to use the “Lab03-01” from the Chapter_3L folder provided in the malware analysis labs.

STATIC TOOLS/ANALYSIS:

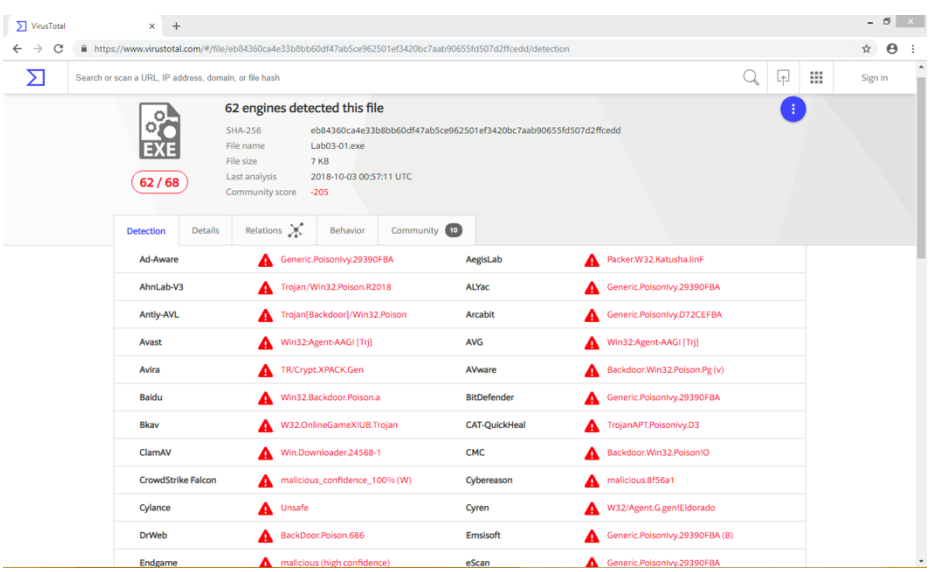
The first thing I did was find the hashes using an online tool. The image below shows all the different hashes.



Hash

Results	
Original text	*(binary only)*
Original bytes	4d5a90000300000004000000ffff0000b8000000000000040... (length=7168)
Adler32	0ca0a594
CRC32	84e29730
Haval	48e649d59c59d72084d48feeea4c8c2e
MD2	cc6ea2835967f2fdbe41888c1c287a3c
MD4	c3b86bc1189ff00c3e09ddf2506840f2
MD5	d537acb8f56a1ce206bc35cf8ff959c0
RipeMD128	42ad537bb7dc0d6b8c6dea6968260848
RipeMD160	acea05f58321b0a29ac160c663da99dfb3886113
SHA-1	0bb491f62b77df737801b9ab0fd14fa12d43d254
SHA-256	eb84360ca4e33b8bb60df47ab5ce962501ef3420bc7aab90655fd507d2ffcedd
SHA-384	c40952155daf1f3451100b40cc3ffc53c705dc00cbb64ae154dfa46850a9f05728c8c59043a56c585c9dd059d694f1cf
SHA-512	02ce7f2db5d0d667c8367f00026a30c61b117fd46b3b25832cfef573cf9929f3d2fbfa2ad6b25a4c2e62c92a016006951e856e7b8b2be7c2a110886111af1bbb
Tiger	d13b80600b6ff30a01e5f9ad5cd77f9ca33e54aca9749d3c
Whirlpool	f51535d4b03218bcd3d9223e41e68789f1df0ee28c93d64485e25847cbd401697bd26d300362ed34daa19dae6af3820c3462643c5fabdaf4c13a9e64807345fb

I then proceeded to analyze the file using VirusTotal to detect the type of malware. As can be seen in the image below, 62 different engines detected the file to contain malware and be of a malicious nature.



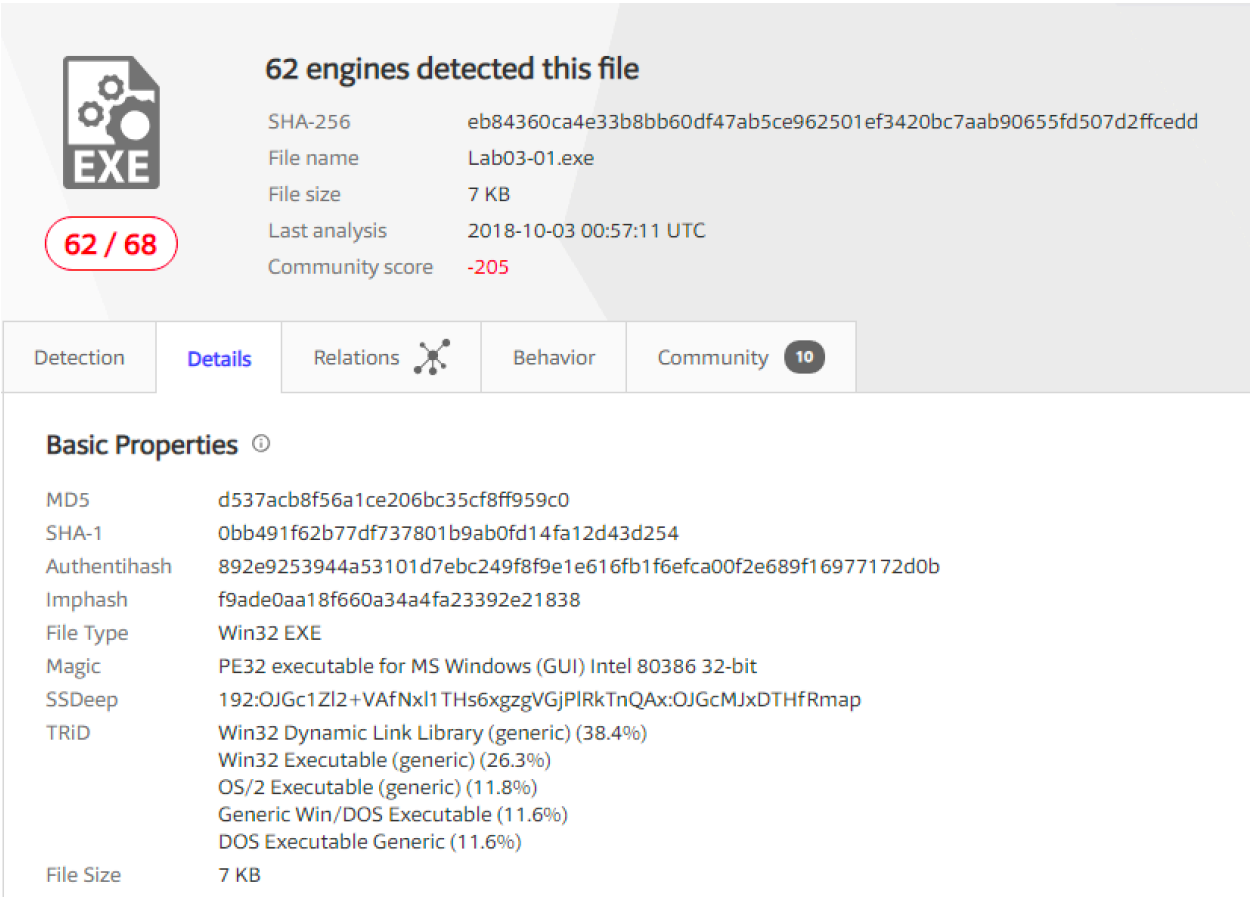
62 engines detected this file

SHA-256	eb84360ca4e33b8bb60df47ab5ce962501ef3420bc7aab90655fd507d2ffcedd
File name	Lab03-01.exe
File size	7 KB
Last analysis	2018-10-03 00:57:11 UTC
Community score	-205

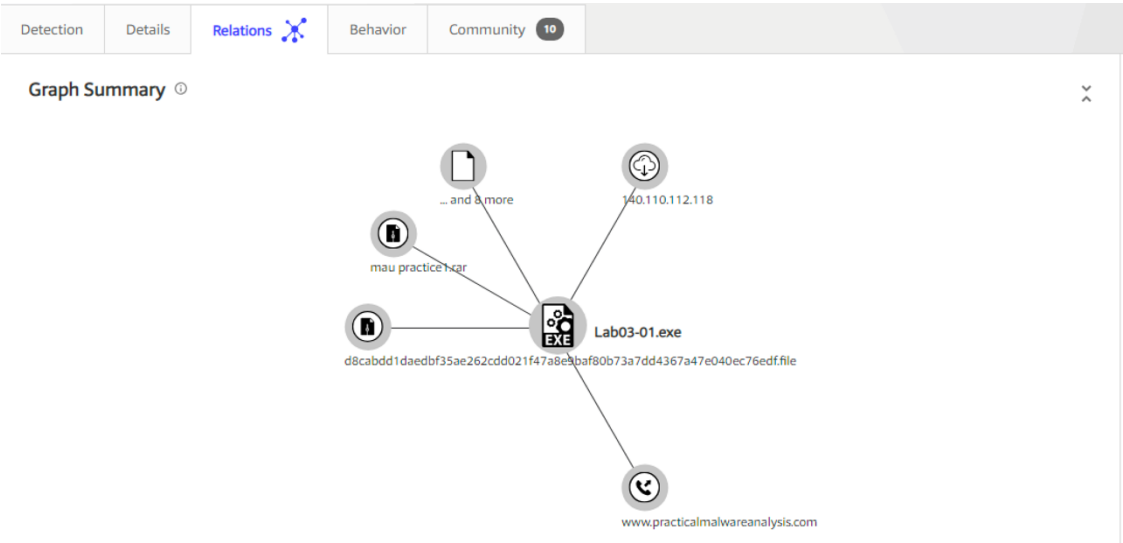
62 / 68

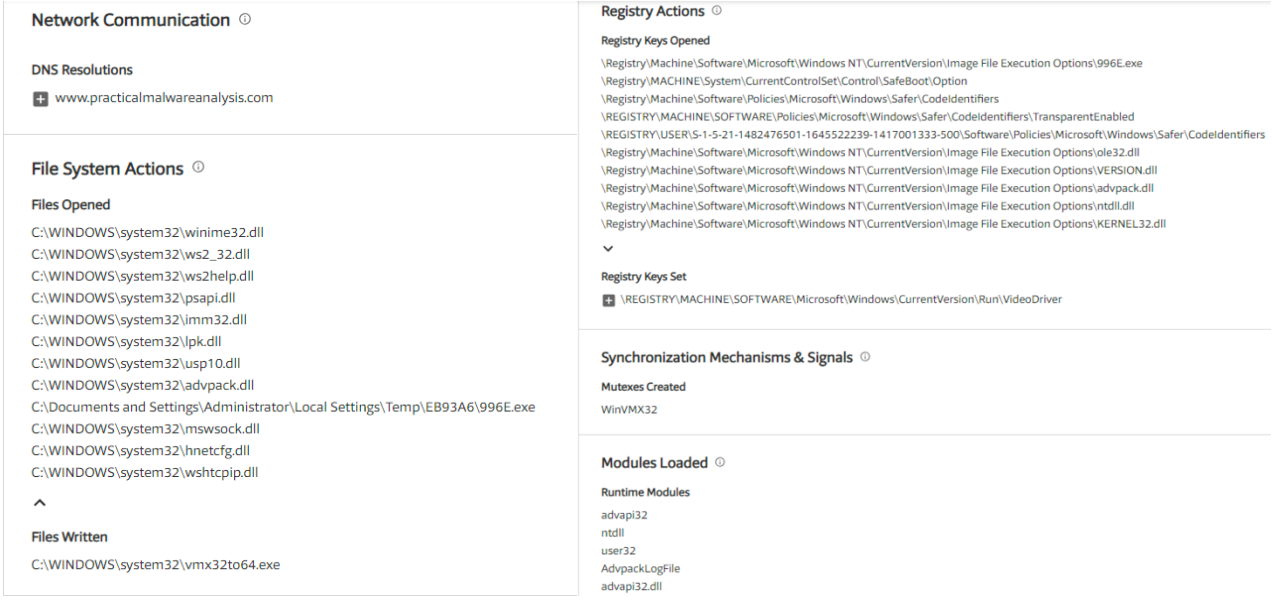
Ad-Aware	Generic.PoisonIvy.29390FBA	AegisLab	Packer.W32.Katusha.linF
AhnLab-V3	Trojan/Win32.Poison.R2018	ALYac	Generic.PoisonIvy.29390FBA
Antiy-AVL	Trojan[Backdoor]/Win32.Poison	Arcabit	Generic.PoisonIvy.D72CEFBA
Avast	Win32:Agent-AAGI [Trj]	AVG	Win32:Agent-AAGI [Trj]
Avira	TR/Crypt.XPACK.Gen	AVware	Backdoor.Win32.Poison.Pg (v)
Baidu	Win32.Backdoor.Poison.a	BitDefender	Generic.PoisonIvy.29390FBA
Bkav	W32.OnlineGameXIUB.Trojan	CAT-QuickHeal	TrojanAPT.PoisonIvy.D3
ClamAV	Win.Downloader.24568-1	CMC	Backdoor.Win32.Poison!O
CrowdStrike Falcon	malicious_confidence_100% (W)	Cybereason	malicious.8f56a1
Cylance	Unsafe	Cyren	W32/Agent.G.gen!Eldorado
DrWeb	BackDoor.Poison.686	Emsisoft	Generic.PoisonIvy.29390FBA (B)
Endgame	malicious (high confidence)	eScan	Generic.PoisonIvy.29390FBA

As can be seen in the details pane below, the hashes here match the hashes from the first image. Another thing to note is that the file type is a Win32 exe and is a PE32 executable.



The image below shows the relations chart and where the malware connects to at some point during execution.





Network Communication

DNS Resolutions

www.practicalmalwareanalysis.com

File System Actions

Files Opened

C:\WINDOWS\system32\winime32.dll
C:\WINDOWS\system32\ws2_32.dll
C:\WINDOWS\system32\ws2help.dll
C:\WINDOWS\system32\psapi.dll
C:\WINDOWS\system32\imm32.dll
C:\WINDOWS\system32\lpk.dll
C:\WINDOWS\system32\usp10.dll
C:\WINDOWS\system32\advpack.dll
C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\996E.exe
C:\WINDOWS\system32\mswsock.dll
C:\WINDOWS\system32\hnetcfg.dll
C:\WINDOWS\system32\wshtcpip.dll

Files Written

C:\WINDOWS\system32\vmx32to64.exe

Registry Actions

Registry Keys Opened

\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\996E.exe
\Registry\MACHINE\System\CurrentControlSet\Control\SafeBoot\Option
\Registry\Machine\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers
\REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers\TransparentEnabled
\REGISTRY\USER\S-1-5-21-1482476501-1645522239-1417001333-500\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ole32.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\VERSION.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\advpack.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ntdll.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\KERNEL32.dll

Registry Keys Set

\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\VideoDriver

Synchronization Mechanisms & Signals

Mutexes Created

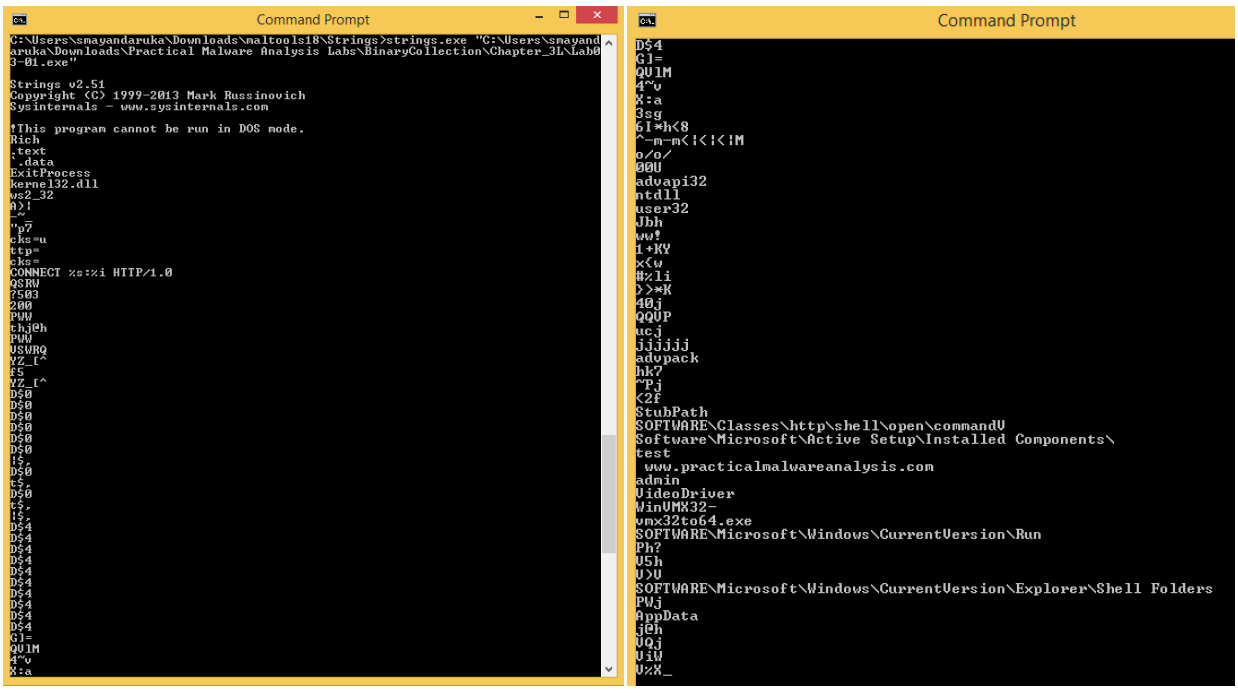
WinVMX32

Modules Loaded

Runtime Modules

advapi32
ntdll
user32
AdvpackLogFile
advapi32.dll

As can be seen in the above two images, a list of the DLLs used by the malware are listed. We can also see the registry keys that are opened by the malware and the different modules that are loaded.



Command Prompt

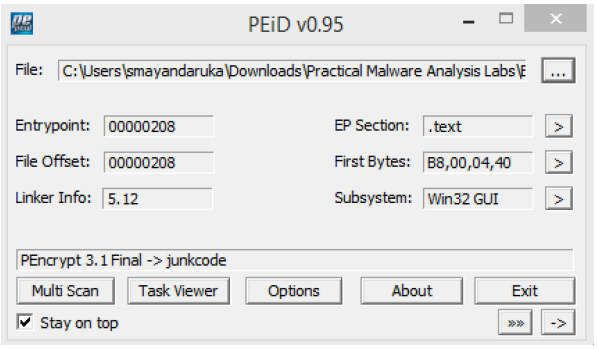
```
C:\Users\smayandaruka\Downloads\maltools18\Strings>strings.exe "C:\Users\smayand
aruka\Downloads\Practical Malware Analysis Labs\BinaryCollection\Chapter_3L\Lab0
3-01.exe"

Strings v2.51
Copyright (C) 1999-2013 Mark Russinovich
Sysinternals - www.sysinternals.com

!This program cannot be run in DOS mode.
Rich
.text
`.data
ExitProcess
kernel32.dll
ws2_32
A>i
t~
"y7
cks=u
ttp=
cks=
CONNECT %s:%i HTTP/1.0
QSRV
?503
200
PUW
thj@h
PUW
USVRQ
VZ_[^
f5
VZ_[^
D$0
D$0
D$0
D$0
D$0
D$0
t$,
D$0
t$,
D$0
t$,
t$,
D$4
D$4
D$4
D$4
D$4
D$4
D$4
D$4
D$4
D$4
G]=
QU1M
4^v
X:a
```

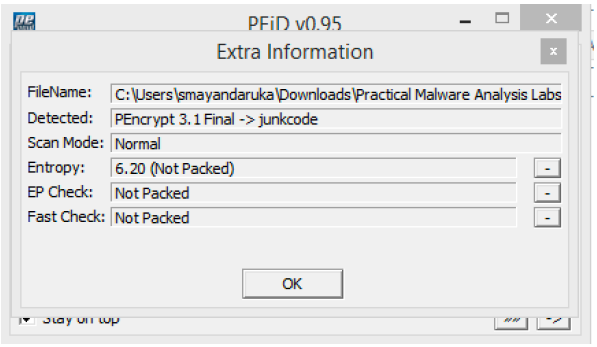
Command Prompt

```
D$4
G]=
QU1M
4^v
X:a
3sg
6I*h<8
^-m-m<!<!<!M
o/o/
00U
advapi32
ntdll
user32
Jbh
vv!
1+KY
x{w
#%1i
>>*K
40j
QQUP
ucj
jjjjjj
advpack
hk?
^Pj
<2f
StubPath
SOFTWARE\Classes\http\shell\open\commandU
Software\Microsoft\Active Setup\Installed Components\
test
www.practicalmalwareanalysis.com
admin
VideoDriver
WinVMX32-
vmx32to64.exe
SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Ph?
U5h
U>U
SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
PUj
AppData
j@h
UQj
UiW
U%X_
```

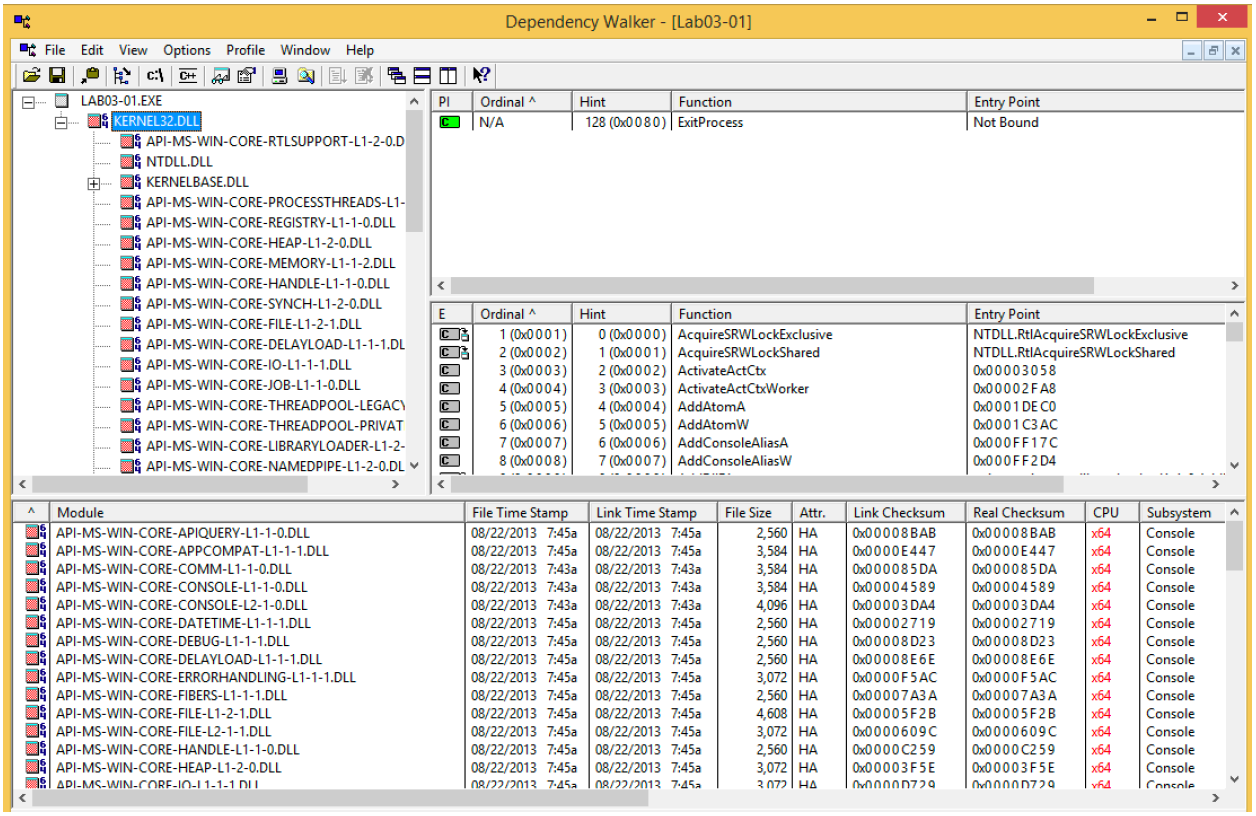
I ran the strings command to extract every ASCII and Unicode string. This can help us determine any hardcoded IPs or domains as well as error messages. In the above images, the one on the right is a lot more interesting because we can see the registry keys hardcoded as well as a few user accounts like user32 and admin. We also see a hardcoded domain name.

The next step was to determine whether the executable is packed or not. As can be seen in the images below, the entry point and the file offset match which indicates that this file is not packed.

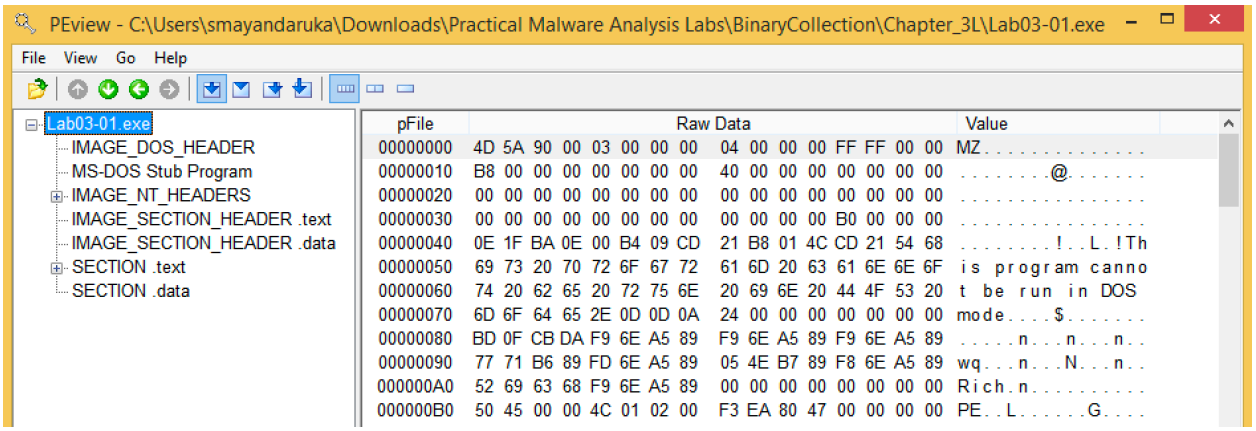


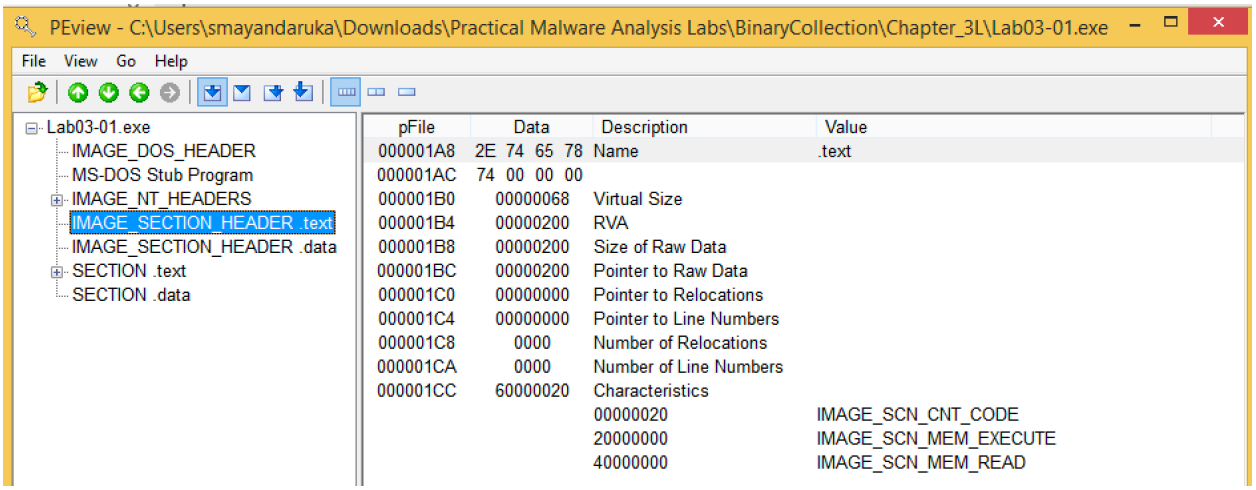


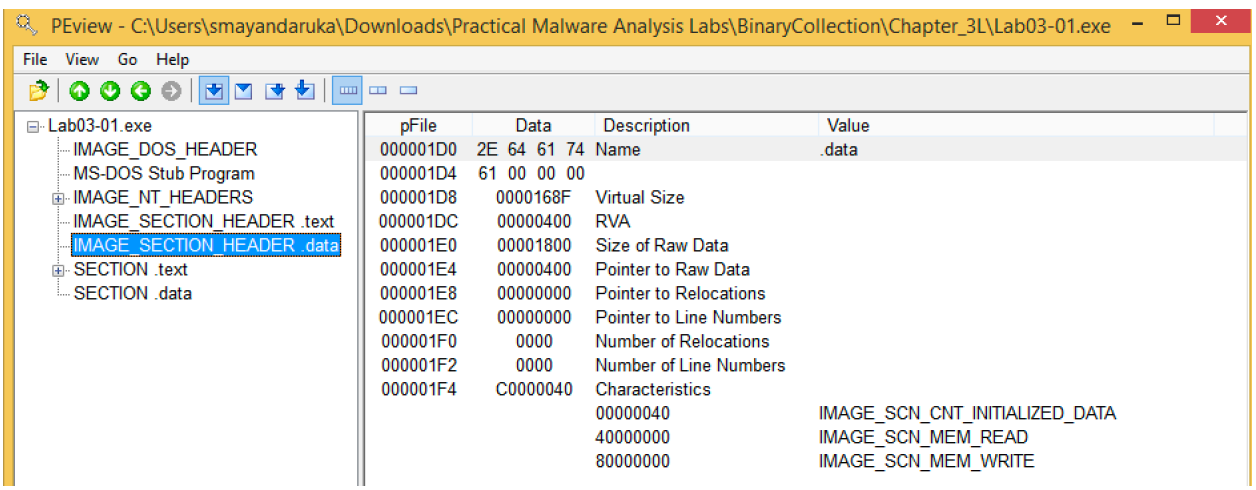
I proceeded to use dependency walker to determine the dynamically linked libraries used by the executable. The image below shows the findings:



As can be seen in the above image, this executable uses the Kernel32 DLL, and we also see the rest of the dependencies. This DLL is a pretty common one since it contains core functionality, and access as well as manipulation of memory and files.







The above images show the output from PEview where we can see the various sizes of the headers as well as other interesting information.

This concludes the static analysis stage. Moving forward is the dynamic analysis.

DYNAMIC TOOLS/ANALYSIS:

The first step is to use ProcMon (Process Monitor) to determine all processes activity on the system. I filtered out to look for any registry edits the executable (malware) makes on the system. The image below shows my findings:

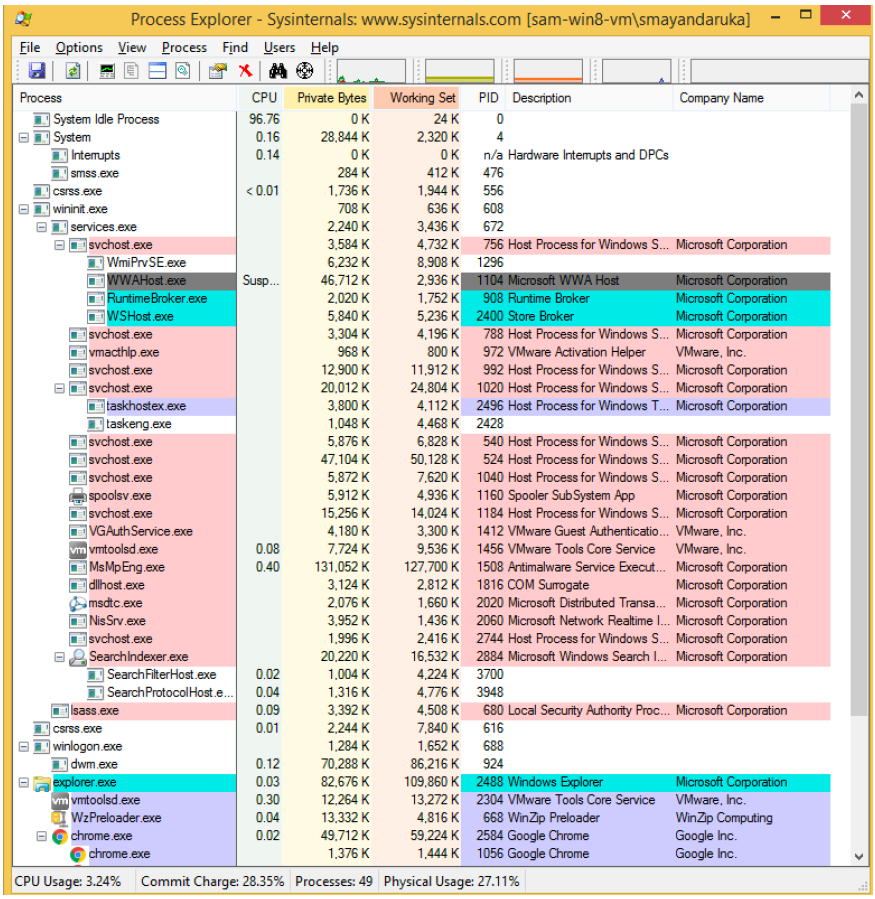
Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Sequence	Time of Day	Process Name	PID	Operation	Path	Result	Detail
0	8:59:53.3208571 PM	Explorer.EXE	2488	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\...	SUCCESS	Type: REG_BINARY, Length: 72, ...
1	8:59:53.3208992 PM	Explorer.EXE	2488	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\...	SUCCESS	Type: REG_BINARY, Length: 1,6...
2	8:59:55.0692023 PM	Explorer.EXE	2488	RegSetValue	HKCU\Software\Classes\Local Settings\Software\Microsoft\...	SUCCESS	Type: REG_BINARY, Length: 39, ...
3	8:59:55.0694305 PM	Explorer.EXE	2488	RegSetValue	HKCU\Software\Classes\Local Settings\Software\Microsoft\...	SUCCESS	Type: REG_BINARY, Length: 20, ...
4	8:59:55.0697880 PM	Explorer.EXE	2488	RegSetValue	HKCU\Software\Classes\Local Settings\Software\Microsoft\...	SUCCESS	Type: REG_BINARY, Length: 20, ...
5	8:59:55.0762336 PM	Explorer.EXE	2488	RegSetValue	HKCU\Software\Classes\Local Settings\Software\Microsoft\...	SUCCESS	Type: REG_BINARY, Length: 39, ...
6	8:59:55.0763703 PM	Explorer.EXE	2488	RegSetValue	HKCU\Software\Classes\Local Settings\Software\Microsoft\...	SUCCESS	Type: REG_BINARY, Length: 20, ...
7	8:59:55.1397392 PM	Explorer.EXE	2488	RegSetValue	HKCU\Software\Classes\Local Settings\MuiCache\8\52C64B...	SUCCESS	Type: REG_MULTI_SZ, Length: 2...
8	8:59:55.2127823 PM	svchost.exe	1020	RegSetValue	\REGISTRY\A\{F8E6ED60-8BA6-DCDC-6180-B016A5C92C9...	SUCCESS	Type: REG_QWORD, Length: 8
9	8:59:55.2128460 PM	svchost.exe	1020	RegSetValue	\REGISTRY\A\{F8E6ED60-8BA6-DCDC-6180-B016A5C92C9...	SUCCESS	Type: REG_DWORD, Length: 4, ...
10	8:59:55.2128556 PM	svchost.exe	1020	RegSetValue	\REGISTRY\A\{F8E6ED60-8BA6-DCDC-6180-B016A5C92C9...	SUCCESS	Type: REG_SZ, Length: 520, Dat...
11	8:59:55.2173610 PM	svchost.exe	1020	RegSetValue	\REGISTRY\A\{F8E6ED60-8BA6-DCDC-6180-B016A5C92C9...	SUCCESS	Type: REG_QWORD, Length: 8
12	8:59:55.2173786 PM	svchost.exe	1020	RegSetValue	\REGISTRY\A\{F8E6ED60-8BA6-DCDC-6180-B016A5C92C9...	SUCCESS	Type: REG_SZ, Length: 210, Dat...
13	8:59:55.2173857 PM	svchost.exe	1020	RegSetValue	\REGISTRY\A\{F8E6ED60-8BA6-DCDC-6180-B016A5C92C9...	SUCCESS	Type: REG_DWORD, Length: 4, ...
14	8:59:55.2173928 PM	svchost.exe	1020	RegSetValue	\REGISTRY\A\{F8E6ED60-8BA6-DCDC-6180-B016A5C92C9...	SUCCESS	Type: REG_DWORD, Length: 4, ...
15	8:59:55.2174006 PM	svchost.exe	1020	RegSetValue	\REGISTRY\A\{F8E6ED60-8BA6-DCDC-6180-B016A5C92C9...	SUCCESS	Type: REG_SZ, Length: 90, Data:...
16	8:59:55.2174068 PM	svchost.exe	1020	RegSetValue	\REGISTRY\A\{F8E6ED60-8BA6-DCDC-6180-B016A5C92C9...	SUCCESS	Type: REG_QWORD, Length: 8
17	8:59:55.2174129 PM	svchost.exe	1020	RegSetValue	\REGISTRY\A\{F8E6ED60-8BA6-DCDC-6180-B016A5C92C9...	SUCCESS	Type: REG_QWORD, Length: 8
18	8:59:55.2174188 PM	svchost.exe	1020	RegSetValue	\REGISTRY\A\{F8E6ED60-8BA6-DCDC-6180-B016A5C92C9...	SUCCESS	Type: REG_DWORD, Length: 4, ...
19	8:59:55.2174244 PM	svchost.exe	1020	RegSetValue	\REGISTRY\A\{F8E6ED60-8BA6-DCDC-6180-B016A5C92C9...	SUCCESS	Type: REG_DWORD, Length: 4, ...
20	8:59:55.2174296 PM	svchost.exe	1020	RegSetValue	\REGISTRY\A\{F8E6ED60-8BA6-DCDC-6180-B016A5C92C9...	SUCCESS	Type: REG_QWORD, Length: 8
21	8:59:55.2174361 PM	svchost.exe	1020	RegSetValue	\REGISTRY\A\{F8E6ED60-8BA6-DCDC-6180-B016A5C92C9...	SUCCESS	Type: REG_DWORD, Length: 4, ...
22	8:59:55.2174417 PM	svchost.exe	1020	RegSetValue	\REGISTRY\A\{F8E6ED60-8BA6-DCDC-6180-B016A5C92C9...	SUCCESS	Type: REG_DWORD, Length: 4, ...
23	8:59:55.2174479 PM	svchost.exe	1020	RegSetValue	\REGISTRY\A\{F8E6ED60-8BA6-DCDC-6180-B016A5C92C9...	SUCCESS	Type: REG_DWORD, Length: 4, ...
24	8:59:55.2174535 PM	svchost.exe	1020	RegSetValue	\REGISTRY\A\{F8E6ED60-8BA6-DCDC-6180-B016A5C92C9...	SUCCESS	Type: REG_DWORD, Length: 4, ...
25	8:59:55.2174596 PM	svchost.exe	1020	RegSetValue	\REGISTRY\A\{F8E6ED60-8BA6-DCDC-6180-B016A5C92C9...	SUCCESS	Type: REG_QWORD, Length: 8
26	8:59:55.2174655 PM	svchost.exe	1020	RegSetValue	\REGISTRY\A\{F8E6ED60-8BA6-DCDC-6180-B016A5C92C9...	SUCCESS	Type: REG_QWORD, Length: 8
27	8:59:55.2196219 PM	svchost.exe	1020	RegSetValue	\REGISTRY\A\{F8E6ED60-8BA6-DCDC-6180-B016A5C92C9...	SUCCESS	Type: REG_QWORD, Length: 8
28	8:59:55.2196364 PM	svchost.exe	1020	RegSetValue	\REGISTRY\A\{F8E6ED60-8BA6-DCDC-6180-B016A5C92C9...	SUCCESS	Type: REG_SZ, Length: 90, Data:...
29	8:59:55.2274619 PM	svchost.exe	524	RegSetValue	HKCU\Software\Microsoft\Windows NT\CurrentVersion\AppC...	SUCCESS	Type: REG_BINARY, Length: 60, ...
30	8:59:55.2282746 PM	Explorer.EXE	2488	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\...	SUCCESS	Type: REG_BINARY, Length: 72, ...
31	8:59:55.2283089 PM	Explorer.EXE	2488	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\...	SUCCESS	Type: REG_BINARY, Length: 1,6...
32	8:59:55.2533777 PM	Explorer.EXE	2488	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\...	SUCCESS	Type: REG_BINARY, Length: 72, ...
33	8:59:55.2534185 PM	Explorer.EXE	2488	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\...	SUCCESS	Type: REG_BINARY, Length: 1,6...
34	8:59:58.6205871 PM	Explorer.EXE	2488	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\...	SUCCESS	Type: REG_BINARY, Length: 72, ...
35	8:59:58.6209121 PM	Explorer.EXE	2488	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\...	SUCCESS	Type: REG_BINARY, Length: 1,6...
36	8:59:59.7415152 PM	svchost.exe	524	RegSetValue	HKCU\Software\Microsoft\Windows NT\CurrentVersion\AppC...	SUCCESS	Type: REG_BINARY, Length: 108...
37	9:00:01.6138827 PM	Explorer.EXE	2488	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\...	SUCCESS	Type: REG_BINARY, Length: 72, ...
38	9:00:01.6139689 PM	Explorer.EXE	2488	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\...	SUCCESS	Type: REG_BINARY, Length: 1,6...

Showing 39 of 88,911 events (0.043%) Backed by virtual memory

As we can see, this executable made a lot of registry changes such as those to Microsoft registries as well as explorer and a few others.



As can be seen in the image on the left, Process Explorer is more or less the same as Task Manager except that it gives a lot more detail. This is really useful when performing basic dynamic analysis since it allows us to determine what new processes are run when the malware is executed.

I also ran ApateDNS but there were no entries. This is likely because there was no domain name that was resolved by the malware when it executed. I did see some local traffic which is attached below.