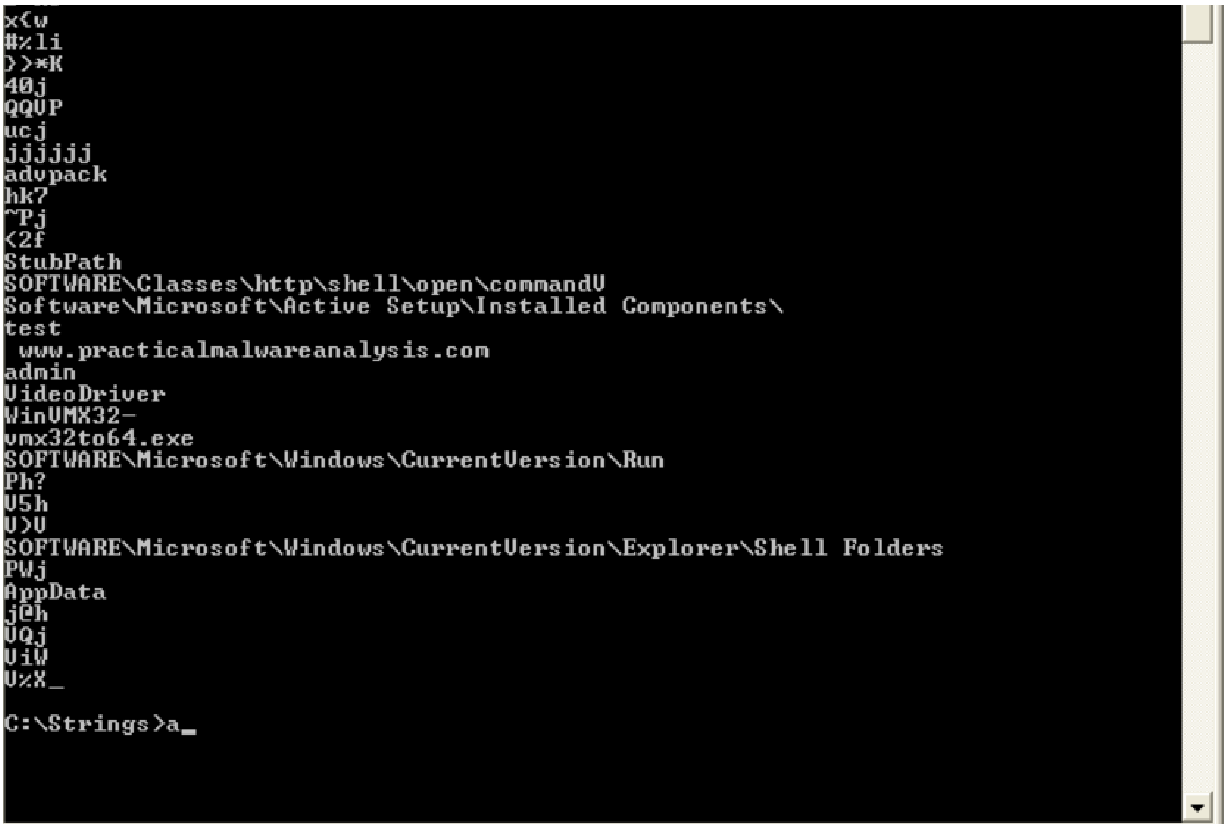
Song Yang (sea.yang@rutgers.edu)
Xin Yang (xin.yang@rutgers.edu)
Zhuohang Li (zl299@scarletmaik.rutgers.edu)

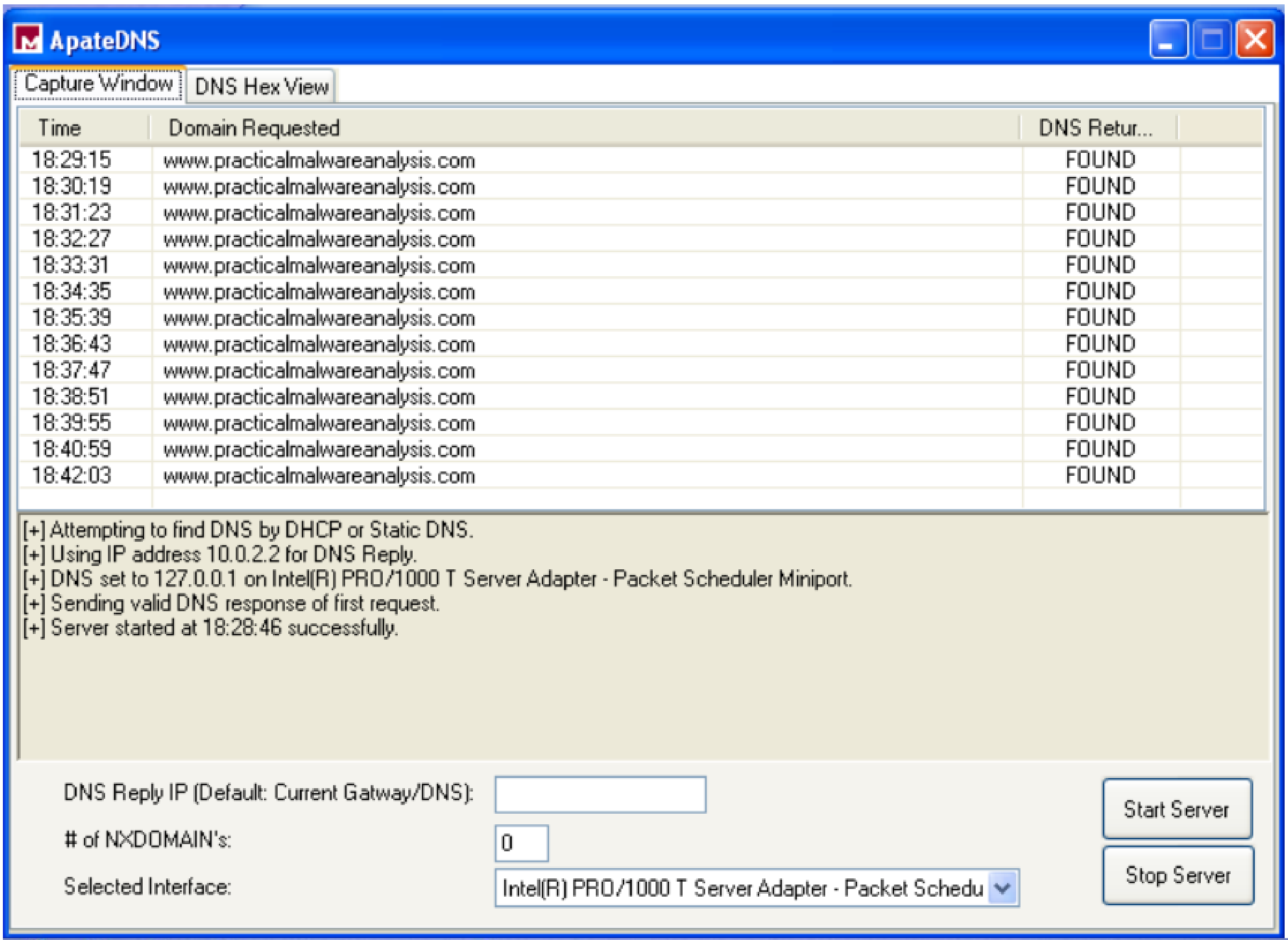
Homework 2
Lab01-01.exe:

1. I can see both in PEview and Dependency Walker, it has only one import that is ExitProcess imported from kernel32.dll. In strings, apart form exitprocess and kernel32.dll, it also have url www.practicalmawareanalysis.com , vmx32to64.exe and two more path that might be used to save or kill.



```
x<w
#%li
D>*K
40j
QQUP
ucj
jjjjjj
advpack
hk?
~Pj
<2f
StubPath
SOFTWARE\Classes\http\shell\open\commandV
Software\Microsoft\Active Setup\Installed Components\
test
 www.practicalmalwareanalysis.com
admin
VideoDriver
WinVMX32-
vmx32to64.exe
SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Ph?
V5h
V>V
SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
PWj
AppData
j@h
VQj
ViW
V%X_

C:\Strings>a_
```

2. Trying to find host-based indicators. I used ApateDNS. I found that, after running the malware, it sends a request to find DNS of www.practicalmawareanalysis.com in every 65 seconds. And furthermore, in process monitor, as mentioned in problem 1, i find a string named vmx32to64.exe, the malware open a process in which the file is copied to C:\Windows\System32 and a column is written in regedit which is VideoDriver autostart. The behavior above also explains the path string we found in question 1. Related pictures are shown below.



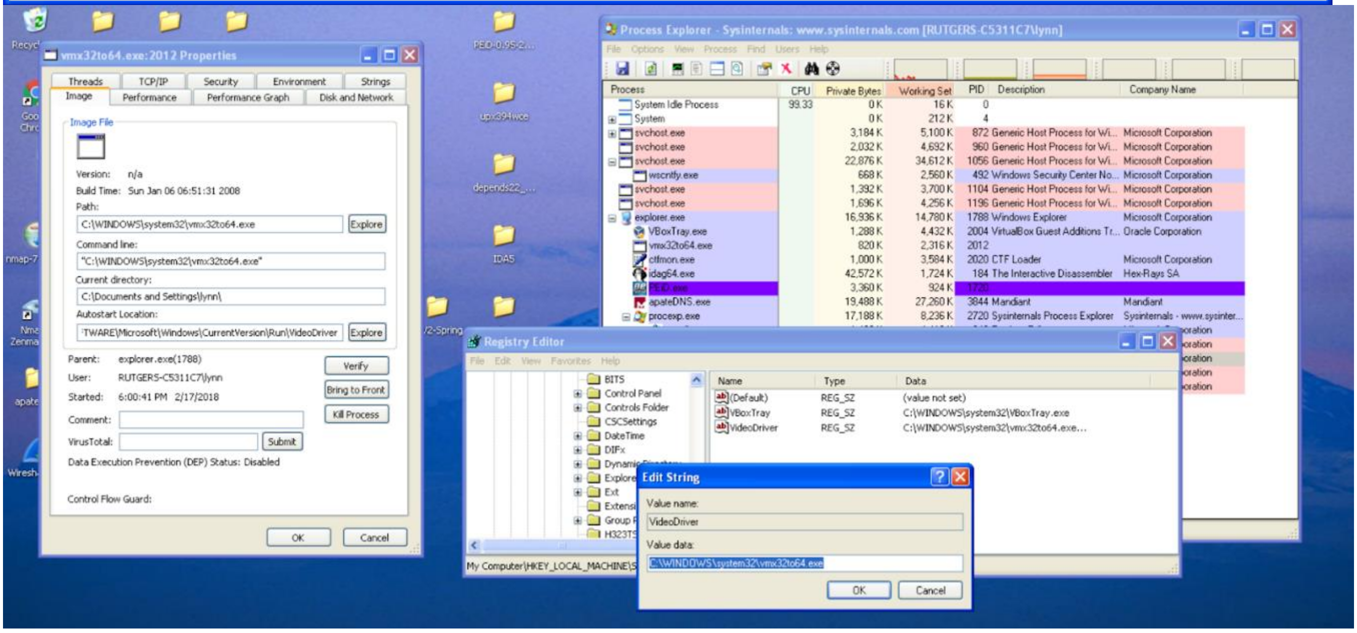
Time	Domain Requested	DNS Retur...
18:29:15	www.practicalmalwareanalysis.com	FOUND
18:30:19	www.practicalmalwareanalysis.com	FOUND
18:31:23	www.practicalmalwareanalysis.com	FOUND
18:32:27	www.practicalmalwareanalysis.com	FOUND
18:33:31	www.practicalmalwareanalysis.com	FOUND
18:34:35	www.practicalmalwareanalysis.com	FOUND
18:35:39	www.practicalmalwareanalysis.com	FOUND
18:36:43	www.practicalmalwareanalysis.com	FOUND
18:37:47	www.practicalmalwareanalysis.com	FOUND
18:38:51	www.practicalmalwareanalysis.com	FOUND
18:39:55	www.practicalmalwareanalysis.com	FOUND
18:40:59	www.practicalmalwareanalysis.com	FOUND
18:42:03	www.practicalmalwareanalysis.com	FOUND

```
[+] Attempting to find DNS by DHCP or Static DNS.
[+] Using IP address 10.0.2.2 for DNS Reply.
[+] DNS set to 127.0.0.1 on Intel(R) PRO/1000 T Server Adapter - Packet Scheduler Miniport.
[+] Sending valid DNS response of first request.
[+] Server started at 18:28:46 successfully.
```

DNS Reply IP (Default: Current Gatway/DNS):

# of NXDOMAIN's: 0

Selected Interface: Intel(R) PRO/1000 T Server Adapter - Packet Schedu



Version: n/a

Build Time: Sun Jan 06 06:51:31 2008

Path: C:\WINDOWS\system32\vmx32to64.exe

Command line: "C:\WINDOWS\system32\vmx32to64.exe"

Current directory: C:\Documents and Settings\lynn\

Autostart Location: TWARE\Microsoft\Windows\CurrentVersion\Run\VideoDriver

Parent: explorer.exe(1788)

User: RUTGERS-C5311C7\lynn

Started: 6:00:41 PM 2/17/2018

Comment:

VirusTotal:

Data Execution Prevention (DEP) Status: Disabled

Control Flow Guard:

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	99.33	0 K	16 K	0		
System		0 K	212 K	4		
svchost.exe		3,184 K	5,100 K	872	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		2,032 K	4,692 K	960	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		22,876 K	34,612 K	1056	Generic Host Process for Wi...	Microsoft Corporation
wscntfy.exe		668 K	2,560 K	492	Windows Security Center No...	Microsoft Corporation
svchost.exe		1,392 K	3,700 K	1104	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		1,696 K	4,256 K	1196	Generic Host Process for Wi...	Microsoft Corporation
explorer.exe		16,936 K	14,780 K	1788	Windows Explorer	Microsoft Corporation
VBoxTray.exe		1,288 K	4,432 K	2004	VirtualBox Guest Additions Tr...	Oracle Corporation
vmx32to64.exe		820 K	2,316 K	2012		
ctfmon.exe		1,000 K	3,584 K	2020	CTF Loader	Microsoft Corporation
idag64.exe		42,572 K	1,724 K	184	The Interactive Disassembler	Hex-Rays SA
PEiD.exe		3,360 K	924 K	1720		
apateDNS.exe		19,488 K	27,260 K	3844	Mandiant	Mandiant
procexp.exe		17,188 K	8,236 K	2720	Sysinternals Process Explorer	Sysinternals - www.sysinter...

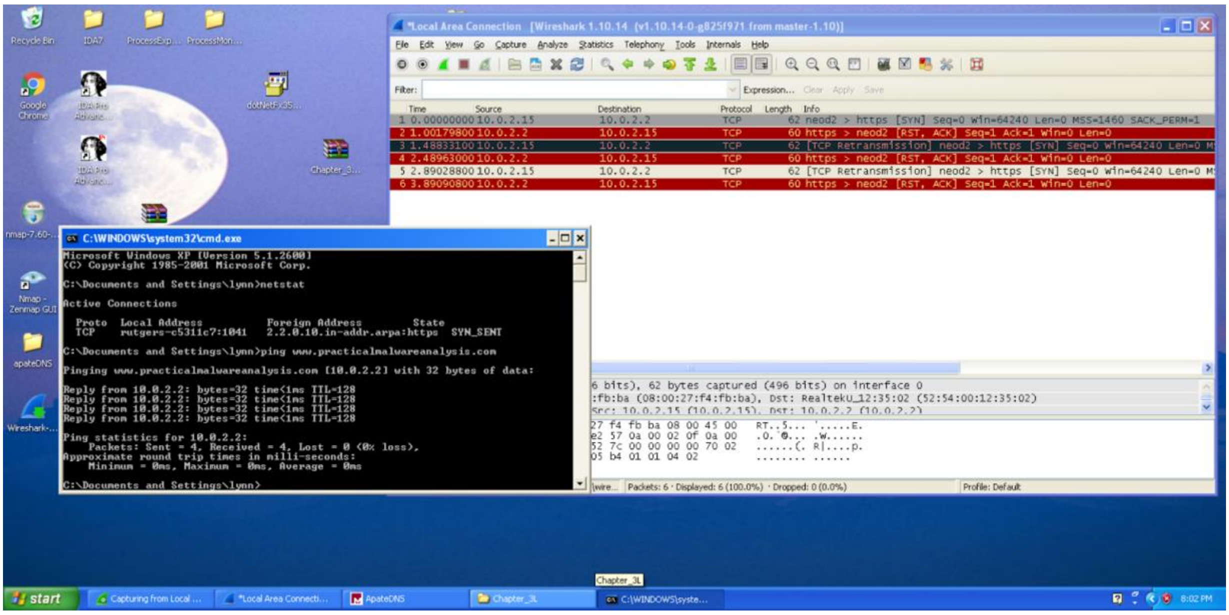
Name	Type	Data
(Default)	REG_SZ	(value not set)
VBoxTray	REG_SZ	C:\WINDOWS\system32\VBoxTray.exe
VideoDriver	REG_SZ	C:\WINDOWS\system32\vmx32to64.exe...

My Computer\HKEY_LOCAL_MACHINE\S

Value name: VideoDriver

Value data: C:\WINDOWS\system32\vmx32to64.exe

3. The ip of www.practicalmawareanalysis.com look like 10.0.2.2 as this malware will request this ip once starts, and after it sends request to DNS, i get packages from wireshark. It seems that it is trying to build a tcp link.


*Local Area Connection [Wireshark 1.10.14 (v1.10.14-0-g825f971 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
C:\WINDOWS\system32\cmd.exe
start
Capturing from Local ...
*Local Area Connecti...
ApateDNS
Chapter_3L
C:\WINDOWS\syste...
8:02 PM

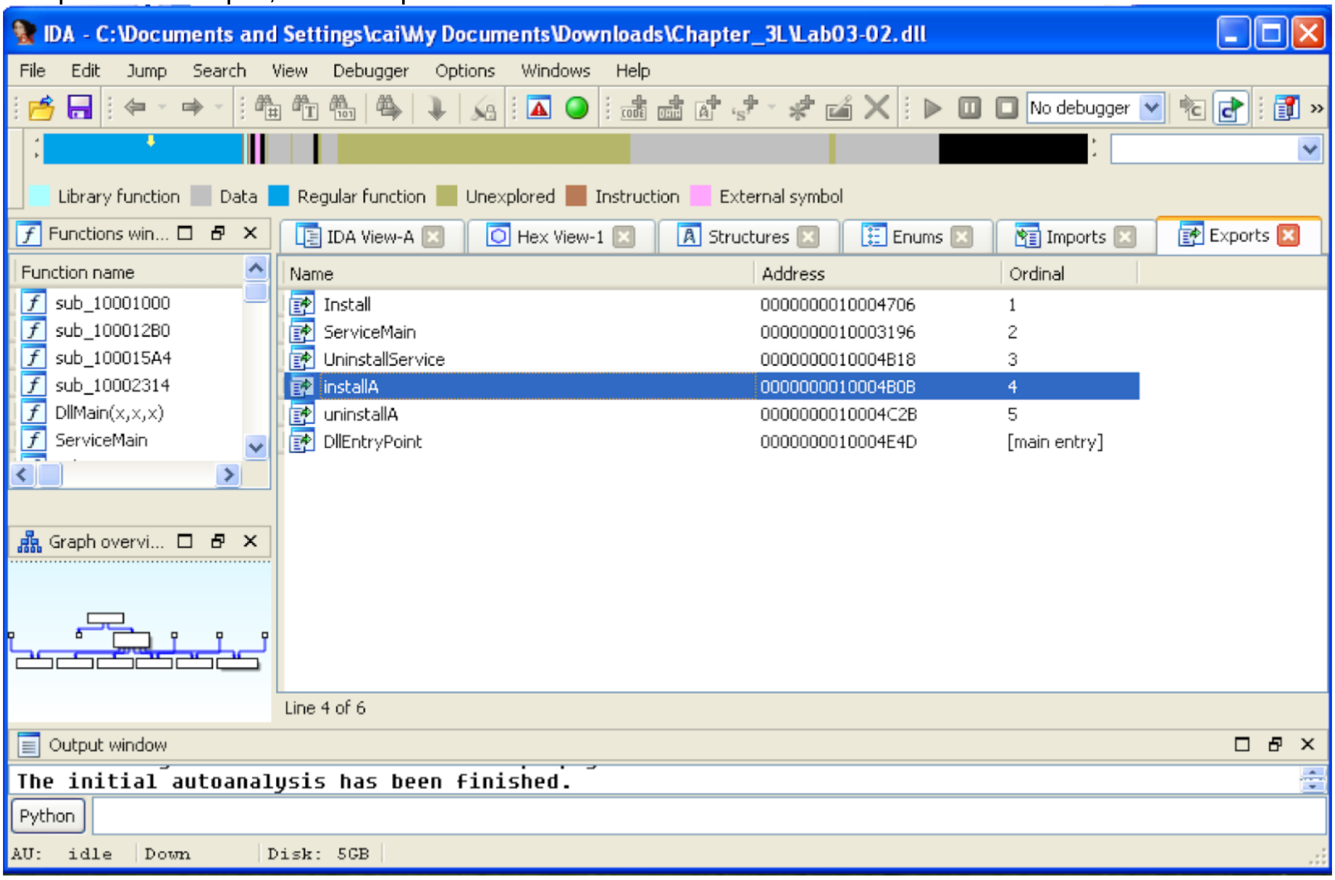
```
  Time        Source      Destination  Protocol  Length  Info
1 0.000000000 10.0.2.15   10.0.2.2     TCP       62 neod2 > https [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
2 1.00179800  10.0.2.2    10.0.2.15    TCP       60 https > neod2 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3 1.48833100  10.0.2.15   10.0.2.2     TCP       62 [TCP Retransmission] neod2 > https [SYN] Seq=0 Win=64240 Len=0 M
4 2.48963000  10.0.2.2    10.0.2.15    TCP       60 https > neod2 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
5 2.89028800  10.0.2.15   10.0.2.2     TCP       62 [TCP Retransmission] neod2 > https [SYN] Seq=0 Win=64240 Len=0 M
6 3.89090800  10.0.2.2    10.0.2.15    TCP       60 https > neod2 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

```
6 bits), 62 bytes captured (496 bits) on interface 0
:fb:ba (08:00:27:f4:fb:ba), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Src: 10.0.2.15 (10.0.2.15), Dst: 10.0.2.2 (10.0.2.2)

27 f4 fb ba 08 00 45 00   RT..5... '.....E.
e2 57 0a 00 02 0f 0a 00   .O.`@... .W......
52 7c 00 00 00 00 70 02   ......(. R|....p.
05 b4 01 01 04 02         ........ ......

\wire...  Packets: 6 · Displayed: 6 (100.0%) · Dropped: 0 (0.0%)    Profile: Default
```

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\lynn>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    rutgers-c5311c7:1041   2.2.0.10.in-addr.arpa:https  SYN_SENT

C:\Documents and Settings\lynn>ping www.practicalmalwareanalysis.com

Pinging www.practicalmalwareanalysis.com [10.0.2.2] with 32 bytes of data:

Reply from 10.0.2.2: bytes=32 time<1ms TTL=128
Reply from 10.0.2.2: bytes=32 time<1ms TTL=128
Reply from 10.0.2.2: bytes=32 time<1ms TTL=128
Reply from 10.0.2.2: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\lynn>
```

Lab03-02.dll:

1. Open it in IDA pro, check exports.



Function name
sub_10001000
sub_100012B0
sub_100015A4
sub_10002314
DllMain(x,x,x)
ServiceMain

Name	Address	Ordinal
Install	0000000010004706	1
ServiceMain	0000000010003196	2
UninstallService	0000000010004B18	3
installA	0000000010004B0B	4
uninstallA	0000000010004C2B	5
DllEntryPoint	0000000010004E4D	[main entry]

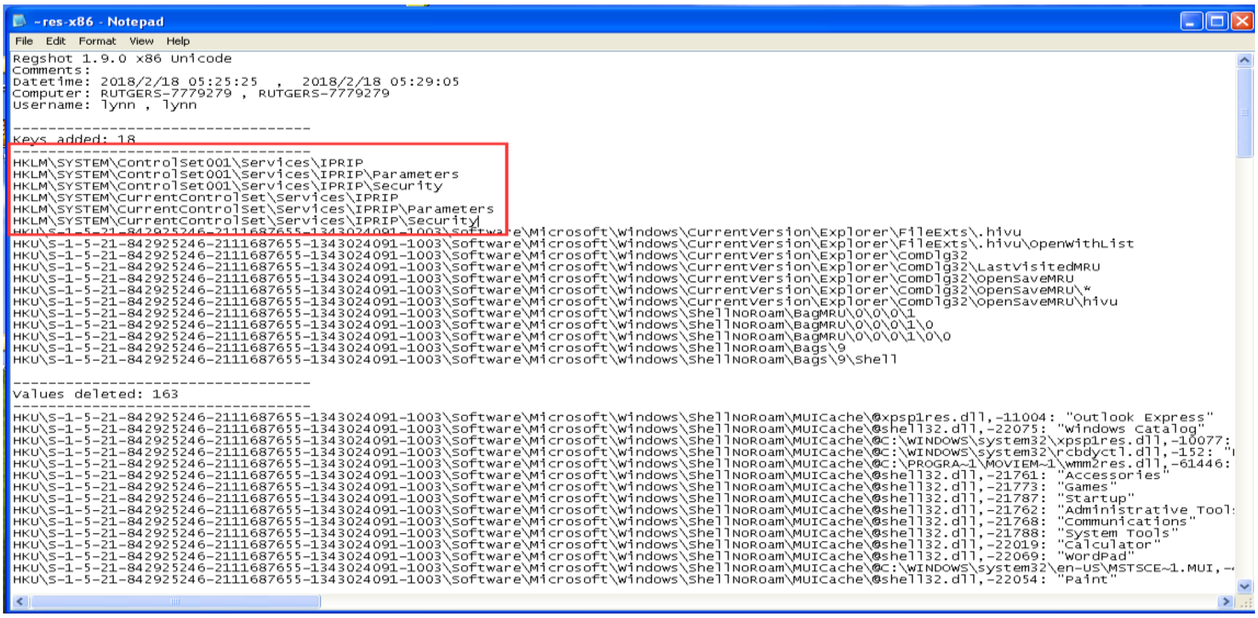
Line 4 of 6

```
The initial autoanalysis has been finished.
```

AU: idle Down Disk: 5GB

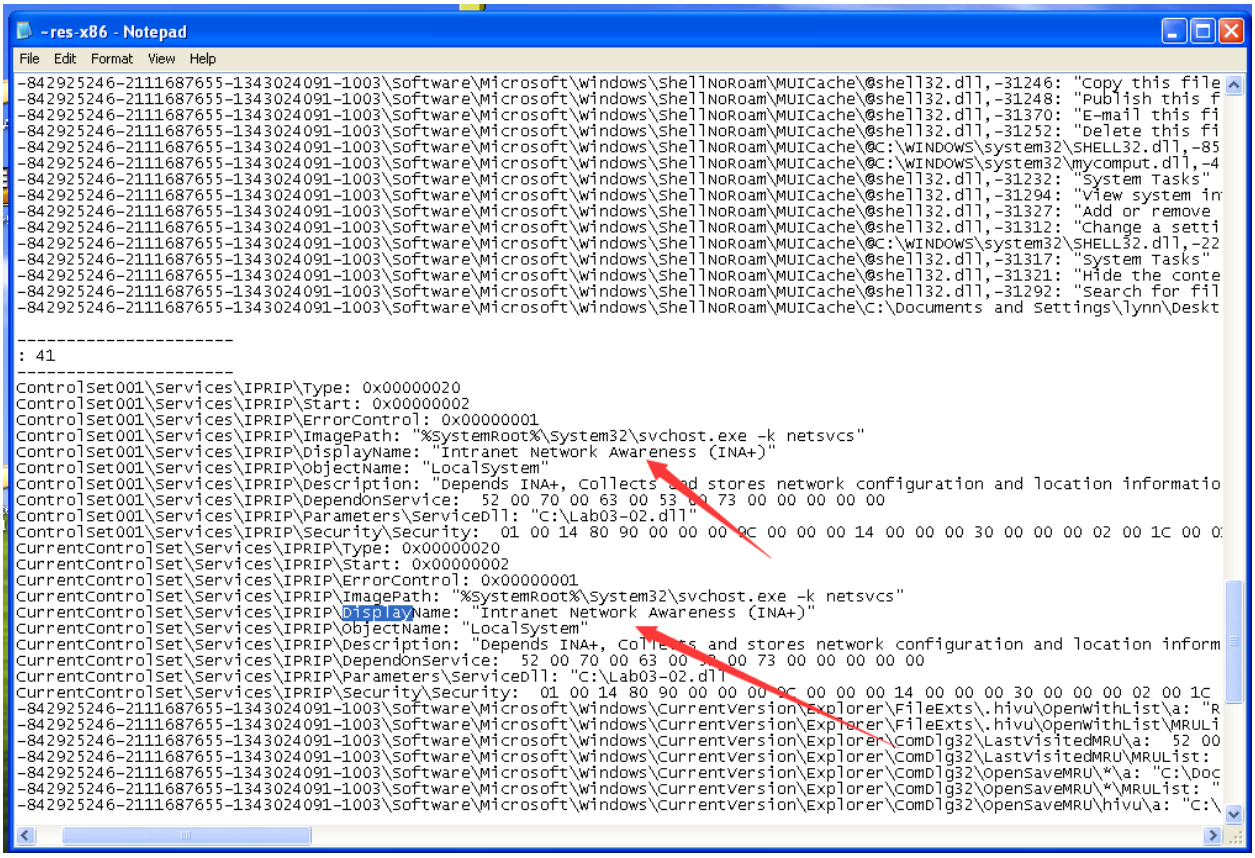
Install it using command rundll32.exe Lab03-02.dll, installA.

2. As we get from regshot, after running dll file, the changes the did to register is that it add several new keys. They all plugged down below IPRIP service.



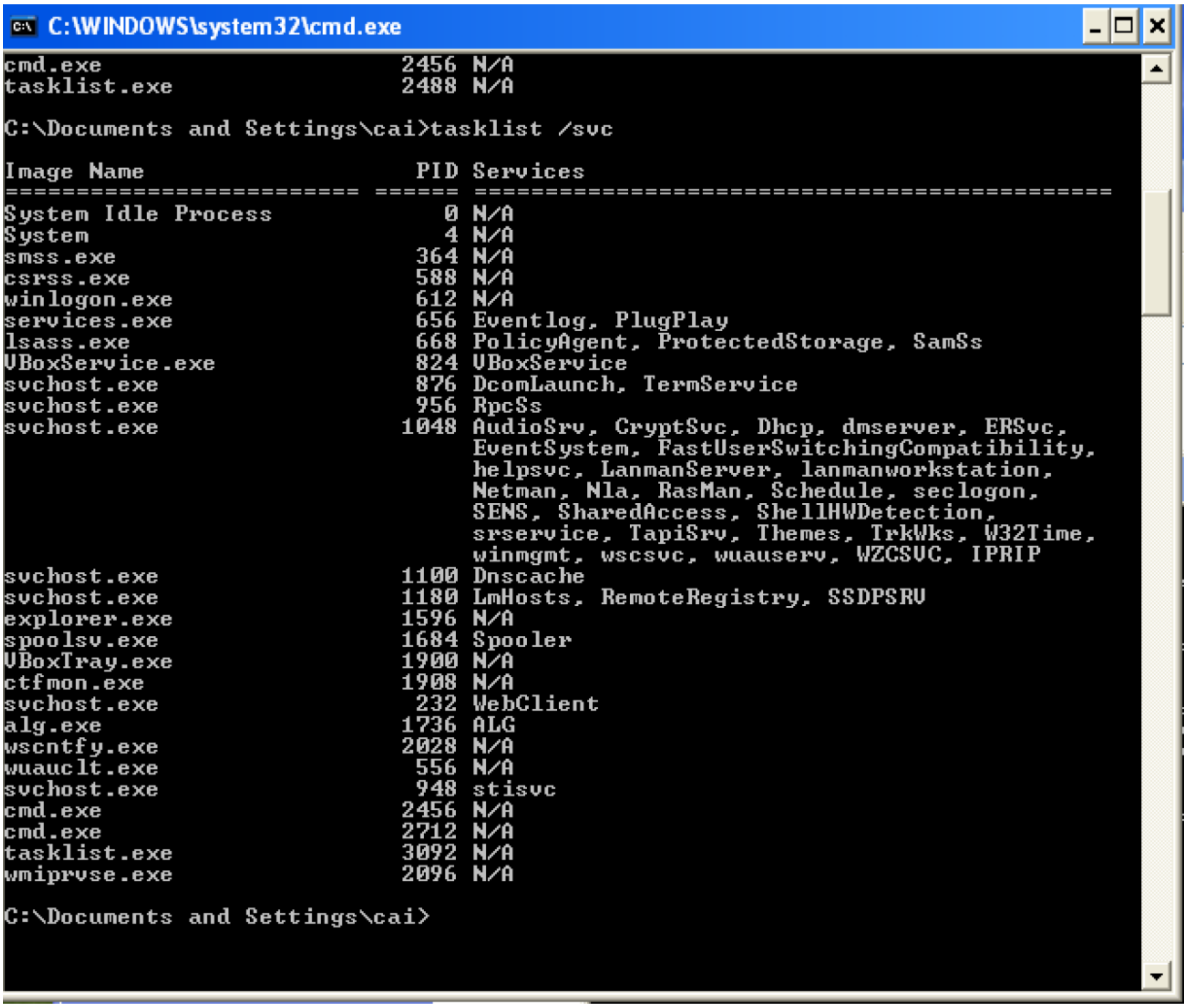
```
Regshot 1.9.0 x86 Unicode
Comments:
Datetime: 2018/2/18 05:25:25  ,  2018/2/18 05:29:05
Computer: RUTGERS-7779279 , RUTGERS-7779279
Username: lynn , lynn

----------------------------------
Keys added: 18
----------------------------------
HKLM\SYSTEM\ControlSet001\Services\IPRIP
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Parameters
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Security
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Parameters
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Security
HKU\S-1-5-21-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.hivu
HKU\S-1-5-21-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.hivu\OpenWithList
HKU\S-1-5-21-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32
HKU\S-1-5-21-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU
HKU\S-1-5-21-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU
HKU\S-1-5-21-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\*
HKU\S-1-5-21-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\hivu
HKU\S-1-5-21-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\ShellNoRoam\BagMRU\0\0\0\1
HKU\S-1-5-21-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\ShellNoRoam\BagMRU\0\0\0\1\0
HKU\S-1-5-21-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\ShellNoRoam\BagMRU\0\0\0\1\0\0
HKU\S-1-5-21-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\9
HKU\S-1-5-21-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\9\Shell

----------------------------------
Values deleted: 163
----------------------------------
HKU\S-1-5-21-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache\@xpsp1res.dll,-11004: "Outlook Express"
HKU\S-1-5-21-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache\@shell32.dll,-22075: "Windows Catalog"
HKU\S-1-5-21-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache\@C:\WINDOWS\system32\xpsp1res.dll,-10077:
HKU\S-1-5-21-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache\@C:\WINDOWS\system32\rcbdyctl.dll,-152: "
HKU\S-1-5-21-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache\@C:\PROGRA~1\MOVIEM~1\wmm2res.dll,-61446:
HKU\S-1-5-21-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache\@shell32.dll,-21761: "Accessories"
HKU\S-1-5-21-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache\@shell32.dll,-21773: "Games"
HKU\S-1-5-21-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache\@shell32.dll,-21787: "Startup"
HKU\S-1-5-21-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache\@shell32.dll,-21762: "Administrative Tool:
HKU\S-1-5-21-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache\@shell32.dll,-21768: "Communications"
HKU\S-1-5-21-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache\@shell32.dll,-21788: "System Tools"
HKU\S-1-5-21-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache\@shell32.dll,-22019: "Calculator"
HKU\S-1-5-21-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache\@shell32.dll,-22069: "WordPad"
HKU\S-1-5-21-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache\@C:\WINDOWS\system32\en-US\MSTSCE~1.MUI,-
HKU\S-1-5-21-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache\@shell32.dll,-22054: "Paint"
```

It add a new service named IPRIP. So use command: net start IPRIP to start service. And it also said the name of the service should displayed as Intranet Network Awareness (INA+).



```
-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache\@shell32.dll,-31246: "Copy this file
-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache\@shell32.dll,-31248: "Publish this f
-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache\@shell32.dll,-31370: "E-mail this fi
-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache\@shell32.dll,-31252: "Delete this fi
-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache\@C:\WINDOWS\system32\SHELL32.dll,-85
-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache\@C:\WINDOWS\system32\mycomput.dll,-4
-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache\@shell32.dll,-31232: "System Tasks"
-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache\@shell32.dll,-31294: "View system in
-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache\@shell32.dll,-31327: "Add or remove
-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache\@shell32.dll,-31312: "Change a setti
-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache\@C:\WINDOWS\system32\SHELL32.dll,-22
-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache\@shell32.dll,-31317: "System Tasks"
-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache\@shell32.dll,-31321: "Hide the conte
-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache\@shell32.dll,-31292: "Search for fil
-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache\C:\Documents and Settings\lynn\Deskt

----------------------
: 41
----------------------
ControlSet001\Services\IPRIP\Type: 0x00000020
ControlSet001\Services\IPRIP\Start: 0x00000002
ControlSet001\Services\IPRIP\ErrorControl: 0x00000001
ControlSet001\Services\IPRIP\ImagePath: "%SystemRoot%\System32\svchost.exe -k netsvcs"
ControlSet001\Services\IPRIP\DisplayName: "Intranet Network Awareness (INA+)"
ControlSet001\Services\IPRIP\ObjectName: "LocalSystem"
ControlSet001\Services\IPRIP\Description: "Depends INA+, Collects and stores network configuration and location informatio
ControlSet001\Services\IPRIP\DependOnService:  52 00 70 00 63 00 53 00 73 00 00 00 00 00
ControlSet001\Services\IPRIP\Parameters\ServiceDll: "C:\Lab03-02.dll"
ControlSet001\Services\IPRIP\Security\Security:  01 00 14 80 90 00 00 00 9C 00 00 00 14 00 00 00 30 00 00 00 02 00 1C 00 0
CurrentControlSet\Services\IPRIP\Type: 0x00000020
CurrentControlSet\Services\IPRIP\Start: 0x00000002
CurrentControlSet\Services\IPRIP\ErrorControl: 0x00000001
CurrentControlSet\Services\IPRIP\ImagePath: "%SystemRoot%\System32\svchost.exe -k netsvcs"
CurrentControlSet\Services\IPRIP\DisplayName: "Intranet Network Awareness (INA+)"
CurrentControlSet\Services\IPRIP\ObjectName: "LocalSystem"
CurrentControlSet\Services\IPRIP\Description: "Depends INA+, Collects and stores network configuration and location inform
CurrentControlSet\Services\IPRIP\DependOnService:  52 00 70 00 63 00 53 00 73 00 00 00 00 00
CurrentControlSet\Services\IPRIP\Parameters\ServiceDll: "C:\Lab03-02.dll
CurrentControlSet\Services\IPRIP\Security\Security:  01 00 14 80 90 00 00 00 9C 00 00 00 14 00 00 00 30 00 00 00 02 00 1C
-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.hivu\OpenWithList\a: "R
-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.hivu\OpenWithList\MRULi
-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU\a:  52 00
-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU\MRUList:
-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\*\a: "C:\Doc
-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\*\MRUList: "
-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\hivu\a: "C:\
```

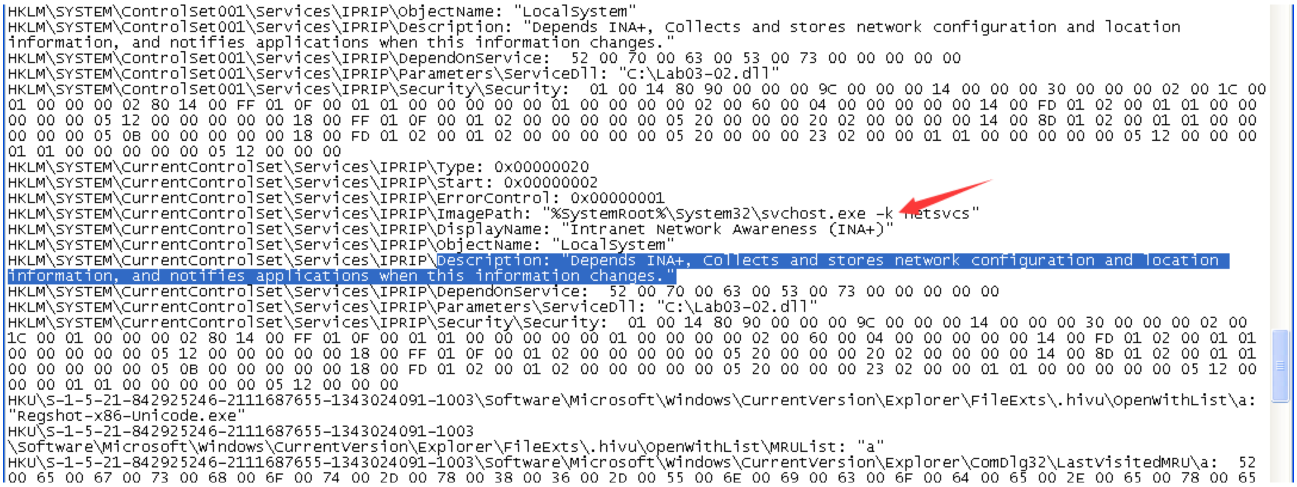
3.Use command tasklist /svc to show all services. From here we can find IPRIP with PID of 1048.



```
cmd.exe                       2456 N/A
tasklist.exe                  2488 N/A

C:\Documents and Settings\cai>tasklist /svc

Image Name                   PID Services
========================= ====== =============================================
System Idle Process            0 N/A
System                         4 N/A
smss.exe                     364 N/A
csrss.exe                    588 N/A
winlogon.exe                 612 N/A
services.exe                 656 Eventlog, PlugPlay
lsass.exe                    668 PolicyAgent, ProtectedStorage, SamSs
VBoxService.exe              824 VBoxService
svchost.exe                  876 DcomLaunch, TermService
svchost.exe                  956 RpcSs
svchost.exe                 1048 AudioSrv, CryptSvc, Dhcp, dmserver, ERSvc,
                                 EventSystem, FastUserSwitchingCompatibility,
                                 helpsvc, LanmanServer, lanmanworkstation,
                                 Netman, Nla, RasMan, Schedule, seclogon,
                                 SENS, SharedAccess, ShellHWDetection,
                                 srservice, TapiSrv, Themes, TrkWks, W32Time,
                                 winmgmt, wscsvc, wuauserv, WZCSVC, IPRIP
svchost.exe                 1100 Dnscache
svchost.exe                 1180 LmHosts, RemoteRegistry, SSDPSRV
explorer.exe                1596 N/A
spoolsv.exe                 1684 Spooler
VBoxTray.exe                1900 N/A
ctfmon.exe                  1908 N/A
svchost.exe                  232 WebClient
alg.exe                     1736 ALG
wscntfy.exe                 2028 N/A
wuauclt.exe                  556 N/A
svchost.exe                  948 stisvc
cmd.exe                     2456 N/A
cmd.exe                     2712 N/A
tasklist.exe                3092 N/A
wmiprvse.exe                2096 N/A

C:\Documents and Settings\cai>
```

4. As the IPRIP service is started by svchost, we can set a filter to see the PID 1048, this filter contains lots of other processes so it can be hard to distinguish the malware.

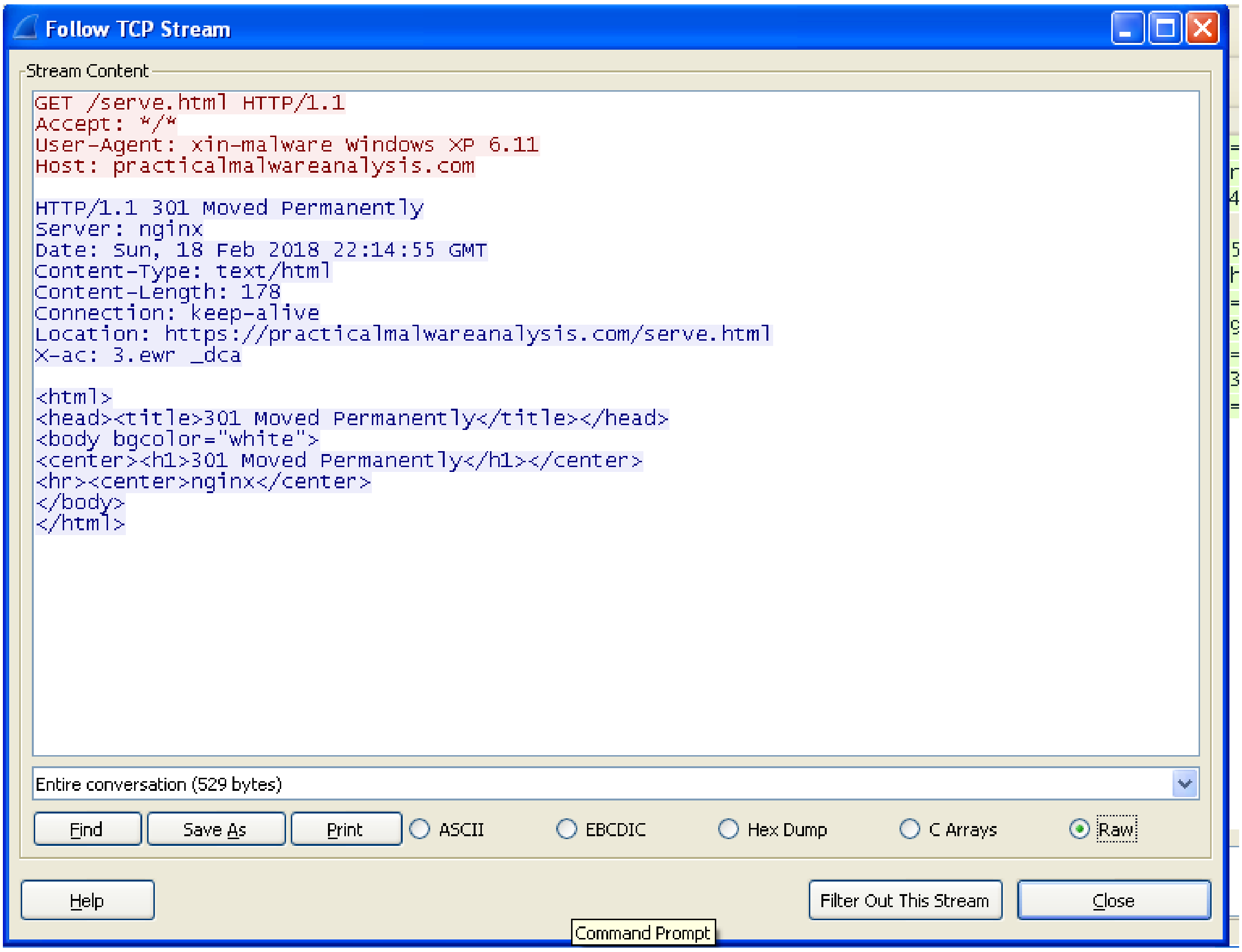
5.This malware installs a service named ‘Intranet Network Awareness (INA+)’ to ‘HKLM\SYSTEM\CurrentControlSet\Services\IPRIP’, and it claims it will collect and store network configuration and location information.



```
HKLM\SYSTEM\ControlSet001\Services\IPRIP\ObjectName: "LocalSystem"
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Description: "Depends INA+, Collects and stores network configuration and location
information, and notifies applications when this information changes."
HKLM\SYSTEM\ControlSet001\Services\IPRIP\DependOnService:  52 00 70 00 63 00 53 00 73 00 00 00 00 00
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Parameters\ServiceDll: "C:\Lab03-02.dll"
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Security\Security:  01 00 14 80 90 00 00 00 9C 00 00 00 14 00 00 00 30 00 00 00 02 00 1C 00
01 00 00 00 02 80 14 00 FF 01 0F 00 01 01 00 00 00 00 00 01 00 00 00 00 02 00 60 00 04 00 00 00 00 00 14 00 FD 01 02 00 01 01 00 00
00 00 00 05 12 00 00 00 00 00 18 00 FF 01 0F 00 01 02 00 00 00 00 00 05 20 00 00 00 20 02 00 00 00 00 14 00 8D 01 02 00 01 01 00 00
00 00 00 05 0B 00 00 00 00 00 18 00 FD 01 02 00 01 02 00 00 00 00 00 05 20 00 00 00 23 02 00 00 01 01 00 00 00 00 00 05 12 00 00 00
01 01 00 00 00 00 00 05 12 00 00 00
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Type: 0x00000020
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Start: 0x00000002
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\ErrorControl: 0x00000001
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\ImagePath: "%SystemRoot%\System32\svchost.exe -k netsvcs"
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\DisplayName: "Intranet Network Awareness (INA+)"
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\ObjectName: "LocalSystem"
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Description: "Depends INA+, Collects and stores network configuration and location
information, and notifies applications when this information changes."
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\DependOnService:  52 00 70 00 63 00 53 00 73 00 00 00 00 00
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Parameters\ServiceDll: "C:\Lab03-02.dll"
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Security\Security:  01 00 14 80 90 00 00 00 9C 00 00 00 14 00 00 00 30 00 00 00 02 00
1C 00 01 00 00 00 02 80 14 00 FF 01 0F 00 01 01 00 00 00 00 00 01 00 00 00 00 02 00 60 00 04 00 00 00 00 00 14 00 FD 01 02 00 01 01
00 00 00 00 00 05 12 00 00 00 00 00 18 00 FF 01 0F 00 01 02 00 00 00 00 00 05 20 00 00 00 20 02 00 00 00 00 14 00 8D 01 02 00 01 01
00 00 00 00 00 05 0B 00 00 00 00 00 18 00 FD 01 02 00 01 02 00 00 00 00 00 05 20 00 00 00 23 02 00 00 01 01 00 00 00 00 00 05 12 00
00 00 01 01 00 00 00 00 00 05 12 00 00 00
HKU\S-1-5-21-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.hivu\OpenWithList\a:
"Regshot-x86-Unicode.exe"
HKU\S-1-5-21-842925246-2111687655-1343024091-1003
\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.hivu\OpenWithList\MRUList: "a"
HKU\S-1-5-21-842925246-2111687655-1343024091-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU\a:  52
00 65 00 67 00 73 00 68 00 6F 00 74 00 2D 00 78 00 38 00 36 00 2D 00 55 00 6E 00 69 00 63 00 6F 00 64 00 65 00 2E 00 65 00 78 00 65
```

6. By checking the wireshark and apateDNS, nothing shows on apateDNS. But we can find a HTTP GET request and the host is practicalmalwareanalysis.com, also we can find some

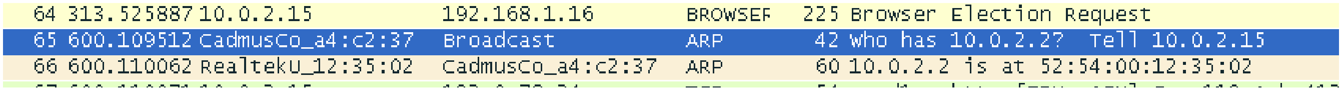
information about the website which uses a nginx server and the html page is 301 moved permanently. And we can still find this malware trying to find 10.0.2.2 and keeps sending broadcast.



```
GET /serve.html HTTP/1.1
Accept: */*
User-Agent: xin-malware Windows XP 6.11
Host: practicalmalwareanalysis.com

HTTP/1.1 301 Moved Permanently
Server: nginx
Date: Sun, 18 Feb 2018 22:14:55 GMT
Content-Type: text/html
Content-Length: 178
Connection: keep-alive
Location: https://practicalmalwareanalysis.com/serve.html
X-ac: 3.ewr _dca

<html>
<head><title>301 Moved Permanently</title></head>
<body bgcolor="white">
<center><h1>301 Moved Permanently</h1></center>
<hr><center>nginx</center>
</body>
</html>
```

Entire conversation (529 bytes)

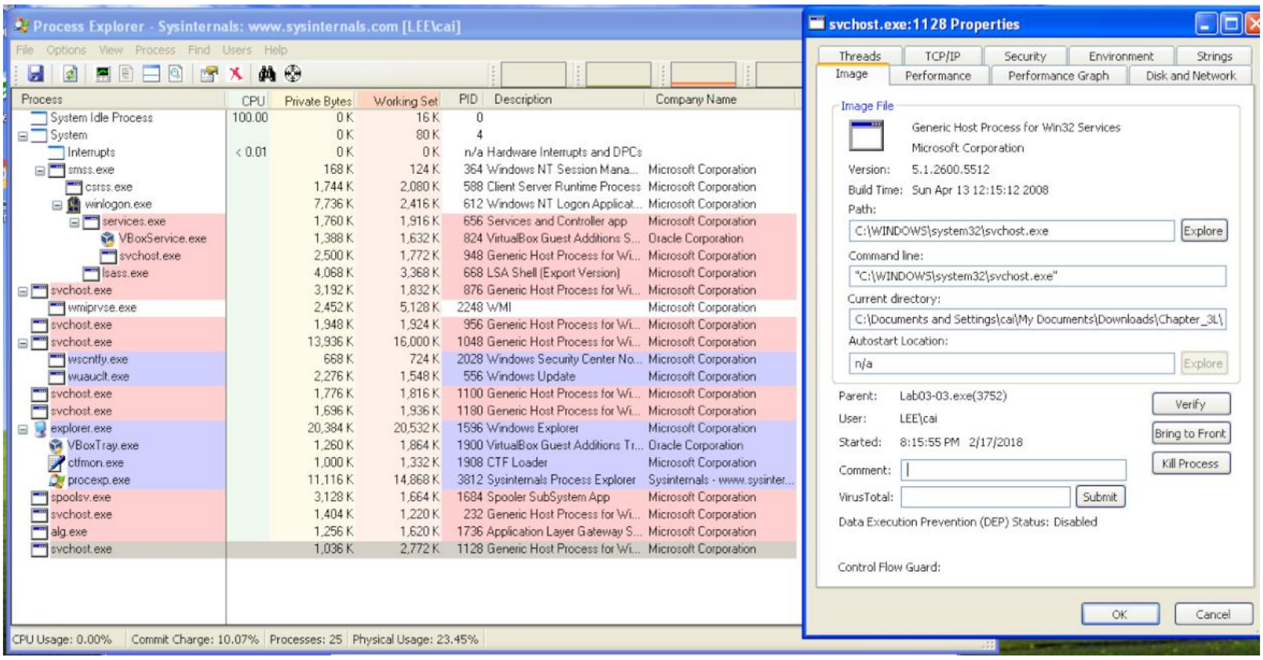
○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw



```
64 313.525887 10.0.2.15           192.168.1.16        BROWSER  225 Browser Election Request
65 600.109512 CadmusCo_a4:c2:37   Broadcast           ARP       42 Who has 10.0.2.2?  Tell 10.0.2.15
66 600.110062 RealtekU_12:35:02   CadmusCo_a4:c2:37   ARP       60 10.0.2.2 is at 52:54:00:12:35:02
```

Lab03-03.exe:

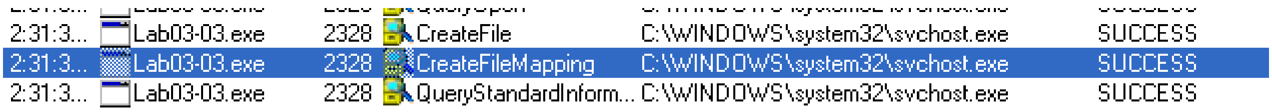
1. It created a new svchost.exe process.



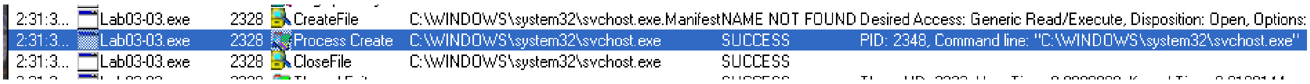
```
Process Explorer - Sysinternals: www.sysinternals.com [LEE\cai]
Process                CPU     Private Bytes  Working Set   PID  Description                           Company Name
System Idle Process    100.00            0 K         16 K     0
System                                   0 K         80 K     4
  Interrupts           < 0.01            0 K          0 K   n/a  Hardware Interrupts and DPCs
  smss.exe                             168 K        124 K   364  Windows NT Session Mana...            Microsoft Corporation
    csrss.exe                        1,744 K      2,080 K   588  Client Server Runtime Process         Microsoft Corporation
    winlogon.exe                     7,736 K      2,416 K   612  Windows NT Logon Applicat...          Microsoft Corporation
      services.exe                   1,760 K      1,916 K   656  Services and Controller app           Microsoft Corporation
        VBoxService.exe              1,388 K      1,632 K   824  VirtualBox Guest Additions S...       Oracle Corporation
        svchost.exe                  2,500 K      1,772 K   948  Generic Host Process for Wi...        Microsoft Corporation
      lsass.exe                      4,068 K      3,368 K   668  LSA Shell (Export Version)            Microsoft Corporation
svchost.exe                          3,192 K      1,832 K   876  Generic Host Process for Wi...        Microsoft Corporation
  wmiprvse.exe                       2,452 K      5,128 K  2248  WMI                                   Microsoft Corporation
svchost.exe                          1,948 K      1,924 K   956  Generic Host Process for Wi...        Microsoft Corporation
svchost.exe                         13,936 K     16,000 K  1048  Generic Host Process for Wi...        Microsoft Corporation
  wscntfy.exe                          668 K        724 K  2028  Windows Security Center No...         Microsoft Corporation
  wuauclt.exe                        2,276 K      1,548 K   556  Windows Update                        Microsoft Corporation
svchost.exe                          1,776 K      1,816 K  1100  Generic Host Process for Wi...        Microsoft Corporation
svchost.exe                          1,696 K      1,936 K  1180  Generic Host Process for Wi...        Microsoft Corporation
explorer.exe                        20,384 K     20,532 K  1596  Windows Explorer                      Microsoft Corporation
  VBoxTray.exe                       1,260 K      1,864 K  1900  VirtualBox Guest Additions Tr...      Oracle Corporation
  ctfmon.exe                         1,000 K      1,332 K  1908  CTF Loader                            Microsoft Corporation
  procexp.exe                       11,116 K     14,868 K  3812  Sysinternals Process Explorer         Sysinternals - www.sysinter...
spoolsv.exe                          3,128 K      1,664 K  1684  Spooler SubSystem App                 Microsoft Corporation
svchost.exe                          1,404 K      1,220 K   232  Generic Host Process for Wi...        Microsoft Corporation
alg.exe                              1,256 K      1,620 K  1736  Application Layer Gateway S...        Microsoft Corporation
svchost.exe                          1,036 K      2,772 K  1128  Generic Host Process for Wi...        Microsoft Corporation

CPU Usage: 0.00% | Commit Charge: 10.07% | Processes: 25 | Physical Usage: 23.45%
```

```
svchost.exe:1128 Properties
Image File
  Generic Host Process for Win32 Services
  Microsoft Corporation
Version:     5.1.2600.5512
Build Time:  Sun Apr 13 12:15:12 2008
Path:
  C:\WINDOWS\system32\svchost.exe
Command line:
  "C:\WINDOWS\system32\svchost.exe"
Current directory:
  C:\Documents and Settings\cai\My Documents\Downloads\Chapter_3L\
Autostart Location:
  n/a
Parent:      Lab03-03.exe(3752)
User:        LEE\cai
Started:     8:15:55 PM   2/17/2018
Comment:
VirusTotal:
Data Execution Prevention (DEP) Status: Disabled

Control Flow Guard:
```

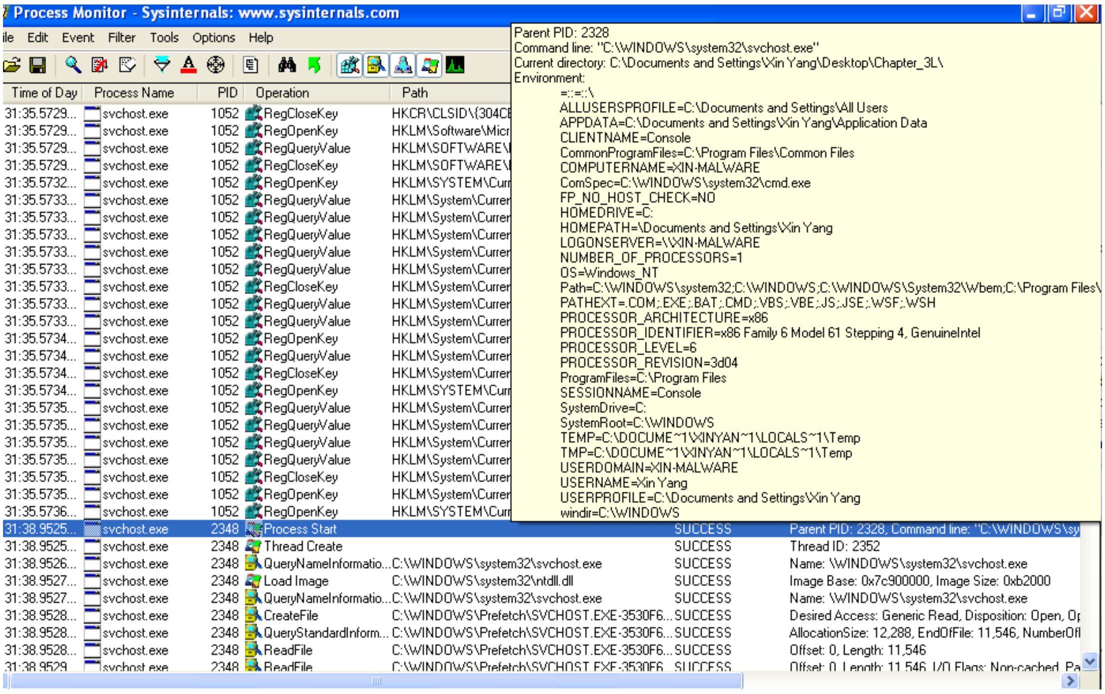
2.From process monitor, we can see it is trying to map and create another svchost.exe process. And the strings in memory refers to a file named ‘practicalmalwareanalysis.log’ , which can’t be a normal system process. Then we filter svchost.exe and we find there’s a new svchost.exe created at the directory of malware, and the parent process is exactly the Lab03-03.exe.



```
2:31:3...  Lab03-03.exe  2328  CreateFile               C:\WINDOWS\system32\svchost.exe  SUCCESS
2:31:3...  Lab03-03.exe  2328  CreateFileMapping        C:\WINDOWS\system32\svchost.exe  SUCCESS
2:31:3...  Lab03-03.exe  2328  QueryStandardInform...   C:\WINDOWS\system32\svchost.exe  SUCCESS
```

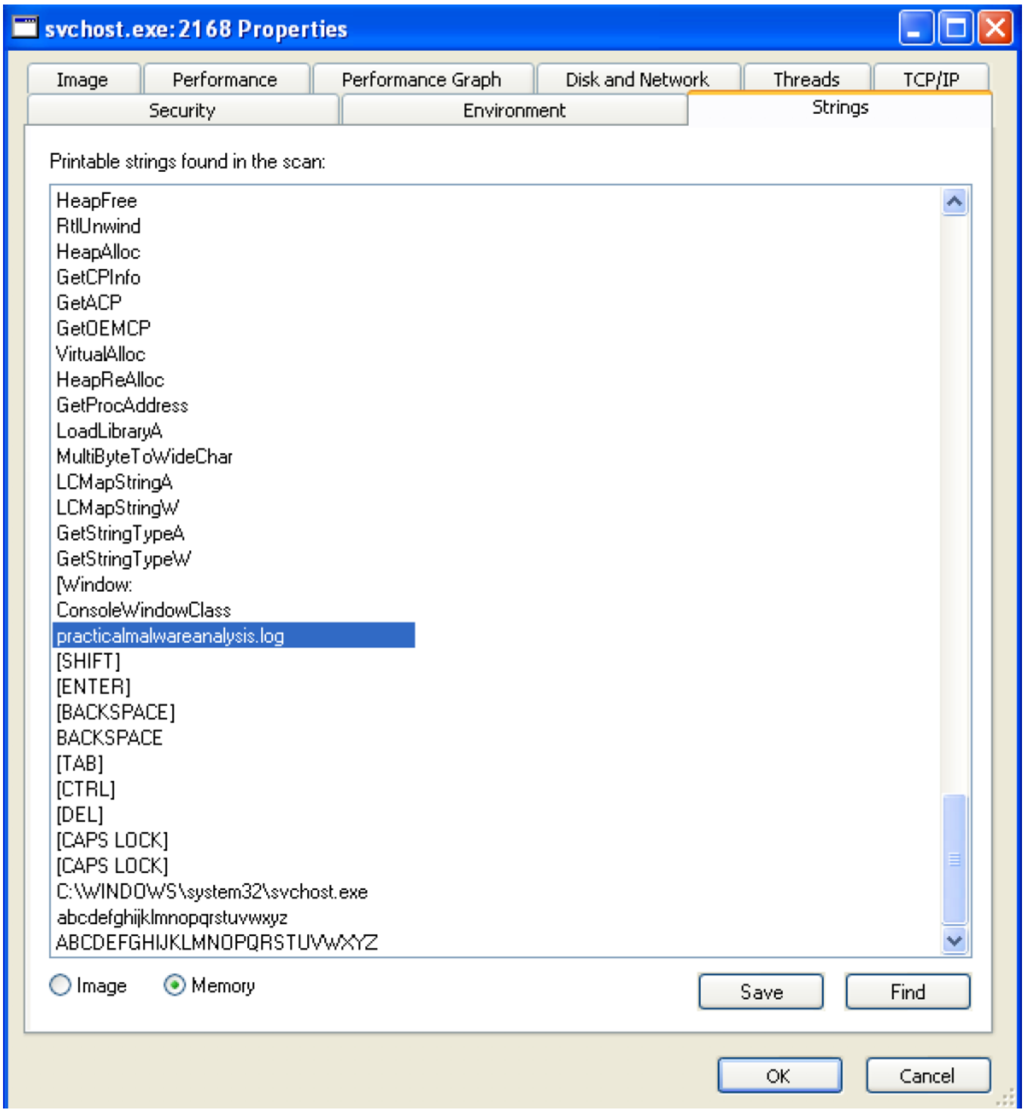


```
2:31:3...  Lab03-03.exe  2328  CreateFile      C:\WINDOWS\system32\svchost.exe.Manifest NAME NOT FOUND  Desired Access: Generic Read/Execute, Disposition: Open, Options:
2:31:3...  Lab03-03.exe  2328  Process Create  C:\WINDOWS\system32\svchost.exe          SUCCESS         PID: 2348, Command line: "C:\WINDOWS\system32\svchost.exe"
2:31:3...  Lab03-03.exe  2328  CloseFile       C:\WINDOWS\system32\svchost.exe          SUCCESS
```



```
Process Monitor - Sysinternals: www.sysinternals.com
Time of Day    Process Name  PID   Operation                Path
31:35.5729...  svchost.exe   1052  RegCloseKey              HKCR\CLSID\{304CE
31:35.5729...  svchost.exe   1052  RegOpenKey               HKLM\Software\Micr
31:35.5729...  svchost.exe   1052  RegQueryValue            HKLM\SOFTWARE\
31:35.5729...  svchost.exe   1052  RegCloseKey              HKLM\SOFTWARE\
31:35.5732...  svchost.exe   1052  RegOpenKey               HKLM\SYSTEM\Curr
31:35.5733...  svchost.exe   1052  RegQueryValue            HKLM\System\Curren
31:35.5733...  svchost.exe   1052  RegQueryValue            HKLM\System\Curren
31:35.5733...  svchost.exe   1052  RegQueryValue            HKLM\System\Curren
31:35.5733...  svchost.exe   1052  RegQueryValue            HKLM\System\Curren
31:35.5733...  svchost.exe   1052  RegQueryValue            HKLM\System\Curren
31:35.5733...  svchost.exe   1052  RegCloseKey              HKLM\System\Curren
31:35.5733...  svchost.exe   1052  RegQueryValue            HKLM\System\Curren
31:35.5733...  svchost.exe   1052  RegQueryValue            HKLM\System\Curren
31:35.5734...  svchost.exe   1052  RegOpenKey               HKLM\System\Curren
31:35.5734...  svchost.exe   1052  RegQueryValue            HKLM\System\Curren
31:35.5734...  svchost.exe   1052  RegCloseKey              HKLM\System\Curren
31:35.5734...  svchost.exe   1052  RegOpenKey               HKLM\SYSTEM\Curr
31:35.5735...  svchost.exe   1052  RegQueryValue            HKLM\System\Curren
31:35.5735...  svchost.exe   1052  RegQueryValue            HKLM\System\Curren
31:35.5735...  svchost.exe   1052  RegQueryValue            HKLM\System\Curren
31:35.5735...  svchost.exe   1052  RegQueryValue            HKLM\System\Curren
31:35.5735...  svchost.exe   1052  RegCloseKey              HKLM\System\Curren
31:35.5735...  svchost.exe   1052  RegOpenKey               HKLM\System\Curren
31:35.5736...  svchost.exe   1052  RegOpenKey               HKLM\SYSTEM\Curr
31:38.9525...  svchost.exe   2348  Process Start                                                       SUCCESS  Parent PID: 2328, Command line: "C:\WINDOWS\sy
31:38.9525...  svchost.exe   2348  Thread Create                                                       SUCCESS  Thread ID: 2352
31:38.9526...  svchost.exe   2348  QueryNameInformatio...C:\WINDOWS\system32\svchost.exe               SUCCESS  Name: \WINDOWS\system32\svchost.exe
31:38.9527...  svchost.exe   2348  Load Image               C:\WINDOWS\system32\ntdll.dll              SUCCESS  Image Base: 0x7c900000, Image Size: 0xb2000
31:38.9527...  svchost.exe   2348  QueryNameInformatio...C:\WINDOWS\system32\svchost.exe               SUCCESS  Name: \WINDOWS\system32\svchost.exe
31:38.9528...  svchost.exe   2348  CreateFile               C:\WINDOWS\Prefetch\SVCHOST.EXE-3530F6...  SUCCESS  Desired Access: Generic Read, Disposition: Open, Op
31:38.9528...  svchost.exe   2348  QueryStandardInform...   C:\WINDOWS\Prefetch\SVCHOST.EXE-3530F6...  SUCCESS  AllocationSize: 12,288, EndOfFile: 11,546, NumberOf
31:38.9528...  svchost.exe   2348  ReadFile                 C:\WINDOWS\Prefetch\SVCHOST.EXE-3530F6...  SUCCESS  Offset: 0, Length: 11,546
31:38.9529     svchost.exe   2348  ReadFile                 C:\WINDOWS\Prefetch\SVCHOST.EXE-3530F6     SUCCESS  Offset: 0, Length: 11,546, I/O Flags: Non-cached, Pa
```

```
Parent PID: 2328
Command line: "C:\WINDOWS\system32\svchost.exe"
Current directory: C:\Documents and Settings\Xin Yang\Desktop\Chapter_3L\
Environment:
        =::=::\
        ALLUSERSPROFILE=C:\Documents and Settings\All Users
        APPDATA=C:\Documents and Settings\Xin Yang\Application Data
        CLIENTNAME=Console
        CommonProgramFiles=C:\Program Files\Common Files
        COMPUTERNAME=XIN-MALWARE
        ComSpec=C:\WINDOWS\system32\cmd.exe
        FP_NO_HOST_CHECK=NO
        HOMEDRIVE=C:
        HOMEPATH=\Documents and Settings\Xin Yang
        LOGONSERVER=\\XIN-MALWARE
        NUMBER_OF_PROCESSORS=1
        OS=Windows_NT
        Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem;C:\Program Files\
        PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
        PROCESSOR_ARCHITECTURE=x86
        PROCESSOR_IDENTIFIER=x86 Family 6 Model 61 Stepping 4, GenuineIntel
        PROCESSOR_LEVEL=6
        PROCESSOR_REVISION=3d04
        ProgramFiles=C:\Program Files
        SESSIONNAME=Console
        SystemDrive=C:
        SystemRoot=C:\WINDOWS
        TEMP=C:\DOCUME~1\XINYAN~1\LOCALS~1\Temp
        TMP=C:\DOCUME~1\XINYAN~1\LOCALS~1\Temp
        USERDOMAIN=XIN-MALWARE
        USERNAME=Xin Yang
        USERPROFILE=C:\Documents and Settings\Xin Yang
        windir=C:\WINDOWS
```

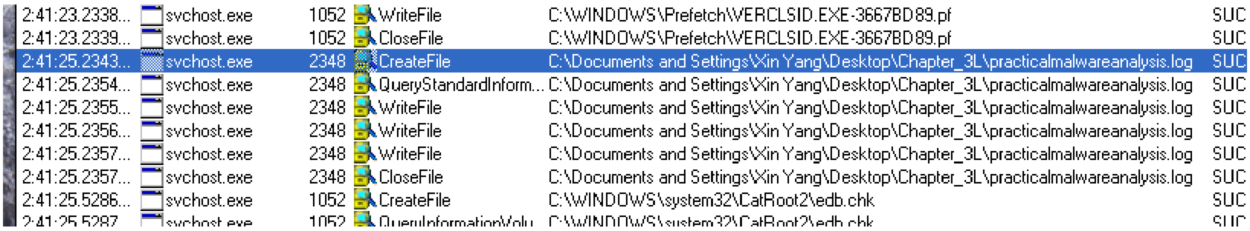


Printable strings found in the scan:

```
HeapFree
RtlUnwind
HeapAlloc
GetCPInfo
GetACP
GetOEMCP
VirtualAlloc
HeapReAlloc
GetProcAddress
LoadLibraryA
MultiByteToWideChar
LCMapStringA
LCMapStringW
GetStringTypeA
GetStringTypeW
[Window:
ConsoleWindowClass
practicalmalwareanalysis.log
[SHIFT]
[ENTER]
[BACKSPACE]
BACKSPACE
[TAB]
[CTRL]
[DEL]
[CAPS LOCK]
[CAPS LOCK]
C:\WINDOWS\system32\svchost.exe
abcdefghijklmnopqrstuvwxyz
ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

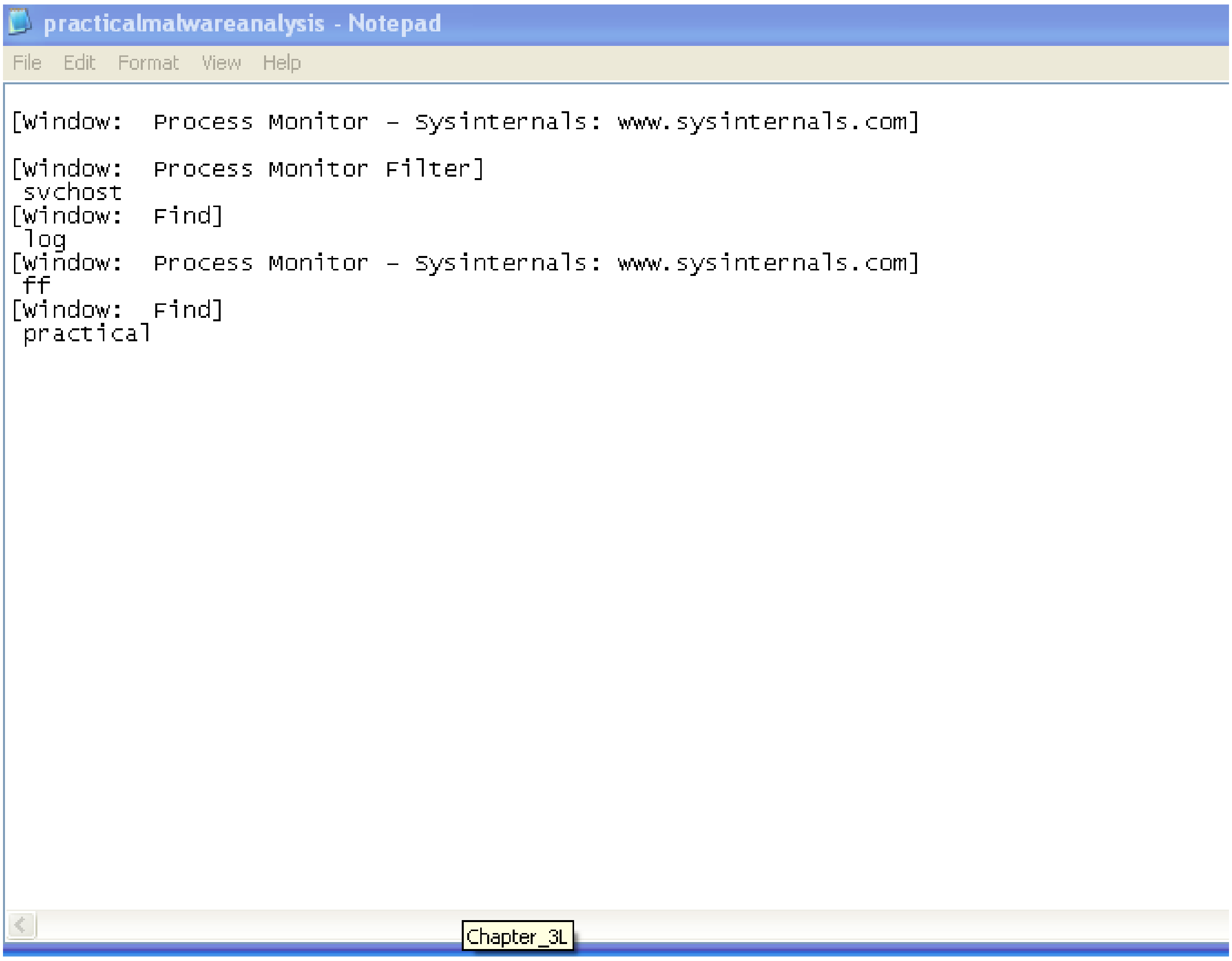
○ Image ● Memory

3.From strings we can see there’s a file named ’practicalmalwareanalysis.log’, so we search this filename in process monitor, we can see the fake svchost.exe created this practicalmalwareanalysis.log file in the directory where the malware sits.



```
2:41:23.2338...  svchost.exe  1052  WriteFile               C:\WINDOWS\Prefetch\VERCLSID.EXE-3667BD89.pf                                             SUC
2:41:23.2339...  svchost.exe  1052  CloseFile               C:\WINDOWS\Prefetch\VERCLSID.EXE-3667BD89.pf                                             SUC
2:41:25.2343...  svchost.exe  2348  CreateFile              C:\Documents and Settings\Xin Yang\Desktop\Chapter_3L\practicalmalwareanalysis.log  SUC
2:41:25.2354...  svchost.exe  2348  QueryStandardInform...  C:\Documents and Settings\Xin Yang\Desktop\Chapter_3L\practicalmalwareanalysis.log  SUC
2:41:25.2355...  svchost.exe  2348  WriteFile               C:\Documents and Settings\Xin Yang\Desktop\Chapter_3L\practicalmalwareanalysis.log  SUC
2:41:25.2356...  svchost.exe  2348  WriteFile               C:\Documents and Settings\Xin Yang\Desktop\Chapter_3L\practicalmalwareanalysis.log  SUC
2:41:25.2357...  svchost.exe  2348  WriteFile               C:\Documents and Settings\Xin Yang\Desktop\Chapter_3L\practicalmalwareanalysis.log  SUC
2:41:25.2357...  svchost.exe  2348  CloseFile               C:\Documents and Settings\Xin Yang\Desktop\Chapter_3L\practicalmalwareanalysis.log  SUC
2:41:25.5286...  svchost.exe  1052  CreateFile              C:\WINDOWS\system32\CatRoot2\edb.chk                                                     SUC
2:41:25.5287     svchost.exe  1052  QueryInformationVolu    C:\WINDOWS\system32\CatRoot2\edb.chk                                                     SUC
```

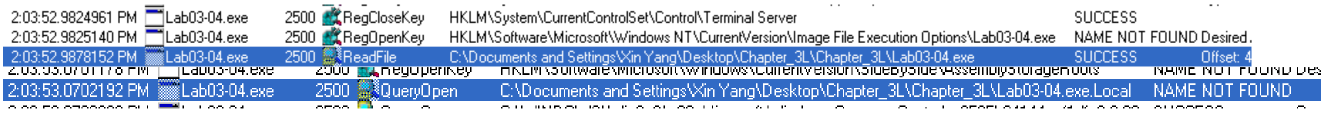
4.After open the .log file we found, we conclude this malware is a keylogger. It creates a fake svchost.exe and records the current window and what the user types. In this case this program records my operations in process monitor to find this file.


practicalmalwareanalysis - Notepad
File Edit Format View Help
Chapter_3L

```
[Window:  Process Monitor - Sysinternals: www.sysinternals.com]

[Window:  Process Monitor Filter]
 svchost
[Window:  Find]
 log
[Window:  Process Monitor - Sysinternals: www.sysinternals.com]
 ff
[Window:  Find]
 practical
```

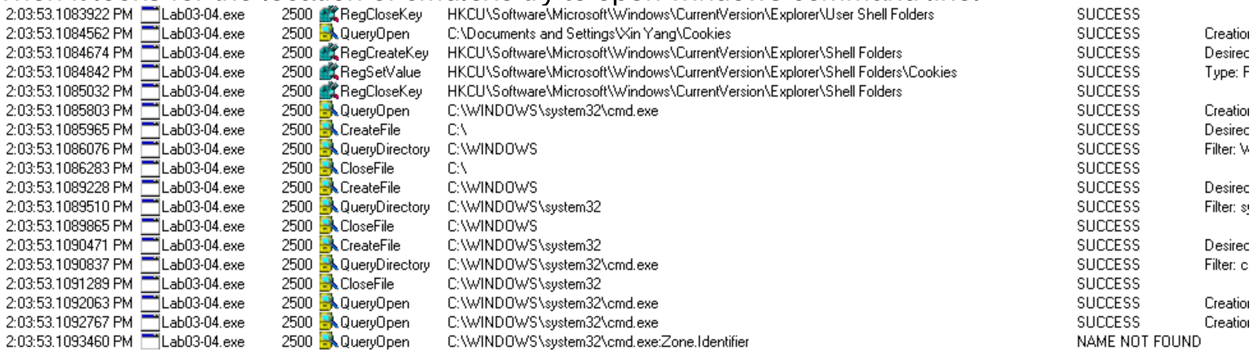
Lab03-04.exe:

1. When you run this file, a command line interface shows up and then disappear, then the Lab03-04.exe file is gone. We can no longer see this process in task manager and it's not hidden, so we guess it's likely to be deleted. From Process Monitor, we can see when we run this malware, there're a bunch of operations to the Registry, and by using regshot, we can see after running this malware, 104 values are added and 14 values are changed. Also we can see from Process Monitor that it's registering itself to registry and looking for files whose names are related to itself.



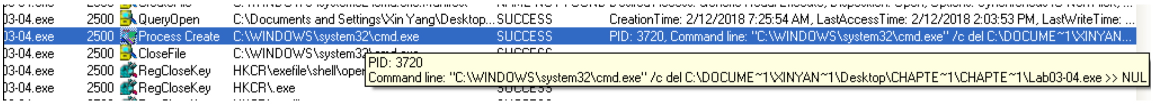
```
2:03:52.9824961 PM  Lab03-04.exe  2500  RegCloseKey  HKLM\System\CurrentControlSet\Control\Terminal Server                                          SUCCESS
2:03:52.9825140 PM  Lab03-04.exe  2500  RegOpenKey   HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Lab03-04.exe   NAME NOT FOUND Desired.
2:03:52.9878152 PM  Lab03-04.exe  2500  ReadFile     C:\Documents and Settings\Xin Yang\Desktop\Chapter_3L\Chapter_3L\Lab03-04.exe                 SUCCESS       Offset: 4
2:03:53.0701178 PM  Lab03-04.exe  2500  RegOpenKey   HKLM\Software\Microsoft\Windows\CurrentVersion\SideBySide\AssemblyStorageRoots               NAME NOT FOUND Des
2:03:53.0702192 PM  Lab03-04.exe  2500  QueryOpen    C:\Documents and Settings\Xin Yang\Desktop\Chapter_3L\Chapter_3L\Lab03-04.exe.Local          NAME NOT FOUND
```

Then it looks for the location of cmd.exe try to open windows command line.



```
2:03:53.1083922 PM  Lab03-04.exe  2500  RegCloseKey     HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders           SUCCESS
2:03:53.1084562 PM  Lab03-04.exe  2500  QueryOpen       C:\Documents and Settings\Xin Yang\Cookies                                          SUCCESS         Creatioı
2:03:53.1084674 PM  Lab03-04.exe  2500  RegCreateKey    HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders                SUCCESS         Desirec
2:03:53.1084842 PM  Lab03-04.exe  2500  RegSetValue     HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cookies        SUCCESS         Type: F
2:03:53.1085032 PM  Lab03-04.exe  2500  RegCloseKey     HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders                SUCCESS
2:03:53.1085803 PM  Lab03-04.exe  2500  QueryOpen       C:\WINDOWS\system32\cmd.exe                                                          SUCCESS         Creatioı
2:03:53.1085965 PM  Lab03-04.exe  2500  CreateFile      C:\                                                                                  SUCCESS         Desirec
2:03:53.1086076 PM  Lab03-04.exe  2500  QueryDirectory  C:\WINDOWS                                                                           SUCCESS         Filter: W
2:03:53.1086283 PM  Lab03-04.exe  2500  CloseFile       C:\                                                                                  SUCCESS
2:03:53.1089228 PM  Lab03-04.exe  2500  CreateFile      C:\WINDOWS                                                                           SUCCESS         Desirec
2:03:53.1089510 PM  Lab03-04.exe  2500  QueryDirectory  C:\WINDOWS\system32                                                                  SUCCESS         Filter: sy
2:03:53.1089865 PM  Lab03-04.exe  2500  CloseFile       C:\WINDOWS                                                                           SUCCESS
2:03:53.1090471 PM  Lab03-04.exe  2500  CreateFile      C:\WINDOWS\system32                                                                  SUCCESS         Desirec
2:03:53.1090837 PM  Lab03-04.exe  2500  QueryDirectory  C:\WINDOWS\system32\cmd.exe                                                          SUCCESS         Filter: c
2:03:53.1091289 PM  Lab03-04.exe  2500  CloseFile       C:\WINDOWS\system32                                                                  SUCCESS
2:03:53.1092063 PM  Lab03-04.exe  2500  QueryOpen       C:\WINDOWS\system32\cmd.exe                                                          SUCCESS         Creatioı
2:03:53.1092767 PM  Lab03-04.exe  2500  QueryOpen       C:\WINDOWS\system32\cmd.exe                                                          SUCCESS         Creatioı
2:03:53.1093460 PM  Lab03-04.exe  2500  QueryOpen       C:\WINDOWS\system32\cmd.exe:Zone.Identifier                                          NAME NOT FOUND
```

At last this malware will delete itself and clean up the mess, but sometimes it won’t work mostly when Process Monitor is turned on and you have to run it several times to see it deletes itself, but when you quit Process Monitor, this would delete itself immediately.



```
)3-04.exe   2500  QueryOpen       C:\Documents and Settings\Xin Yang\Desktop... SUCCESS   CreationTime: 2/12/2018 7:25:54 AM, LastAccessTime: 2/12/2018 2:03:53 PM, LastWriteTime: ...
)3-04.exe   2500  Process Create  C:\WINDOWS\system32\cmd.exe                   SUCCESS   PID: 3720, Command line: "C:\WINDOWS\system32\cmd.exe" /c del C:\DOCUME~1\XINYAN...
)3-04.exe   2500  CloseFile       C:\WINDOWS\system32
)3-04.exe   2500  RegCloseKey     HKCR\exefile\shell\oper
)3-04.exe   2500  RegCloseKey     HKCR\.exe
```

```
PID: 3720
Command line: "C:\WINDOWS\system32\cmd.exe" /c del C:\DOCUME~1\XINYAN~1\Desktop\CHAPTE~1\CHAPTE~1\Lab03-04.exe >> NUL
```

We can’t see this malware call any functions or import any libraries related to network or sockets, but when run strings command, we can however see something related to HTTP and “http://www.practicalmalwareanalysis.com”. We extract this program to different directories and we find that it only deletes the file which are clicked and runned, the other copies are still safe on the disk and not detected by the malware.

2. This malware can delete itself after opened, which can cause a problem for the analysis. We need to pause this malware before it delete itself so we can better analyze and figure out what it really did.

3. Tools like Ollydbg, which can pause the malware and analyze step by step can run this program, also the best way is to use IDA Pro and find out what reasons lead to the branch and prevent it.