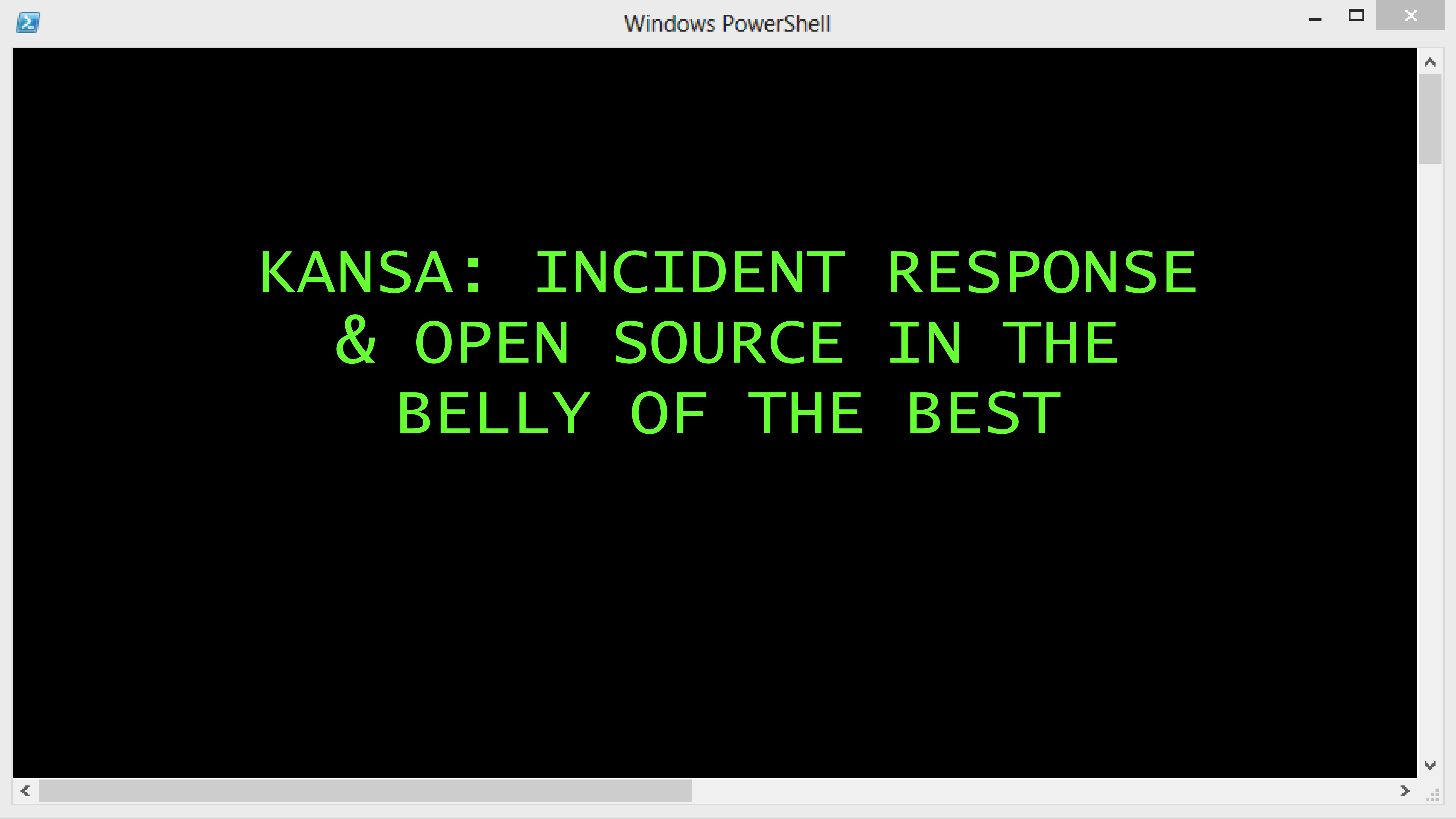
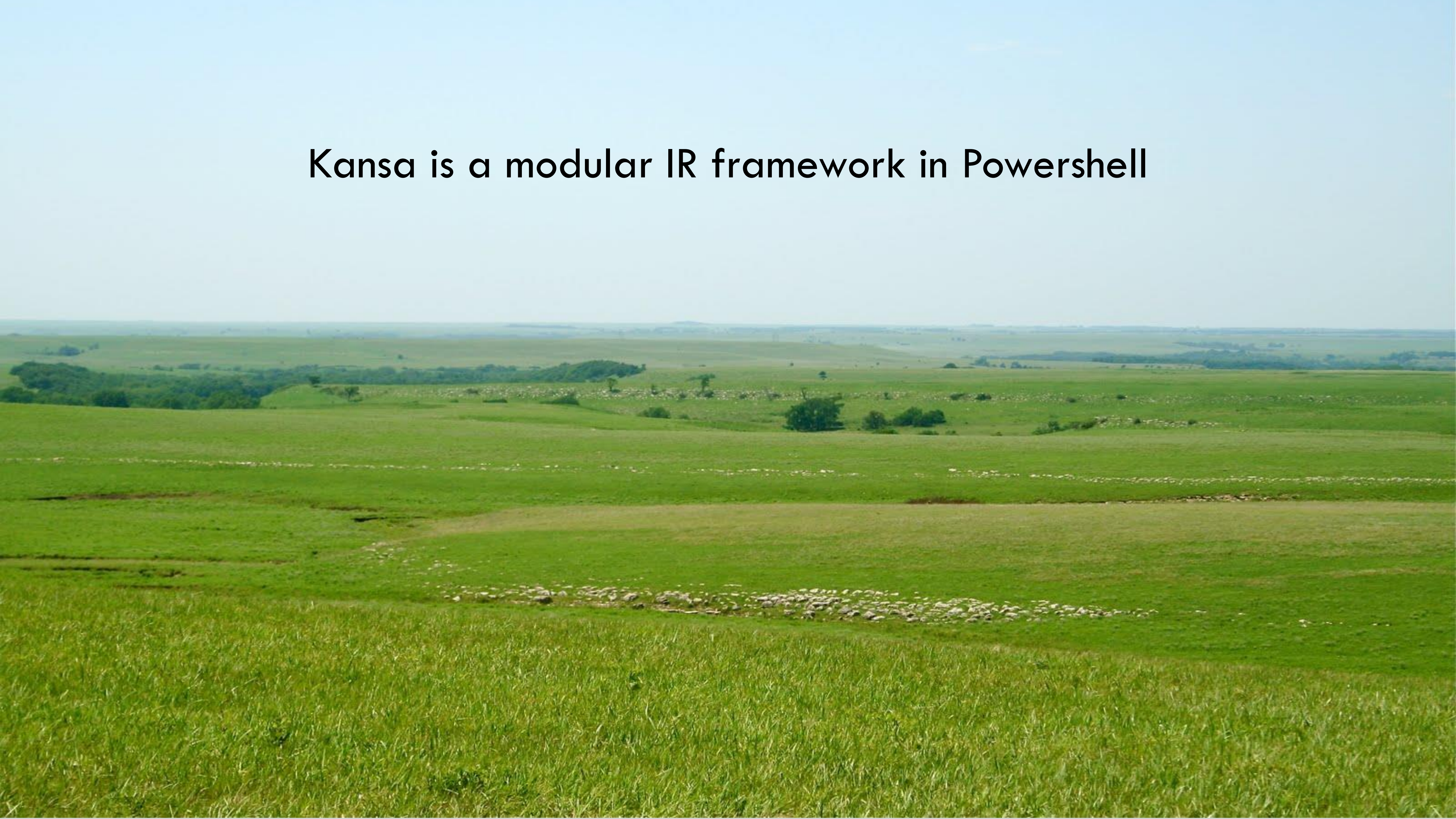
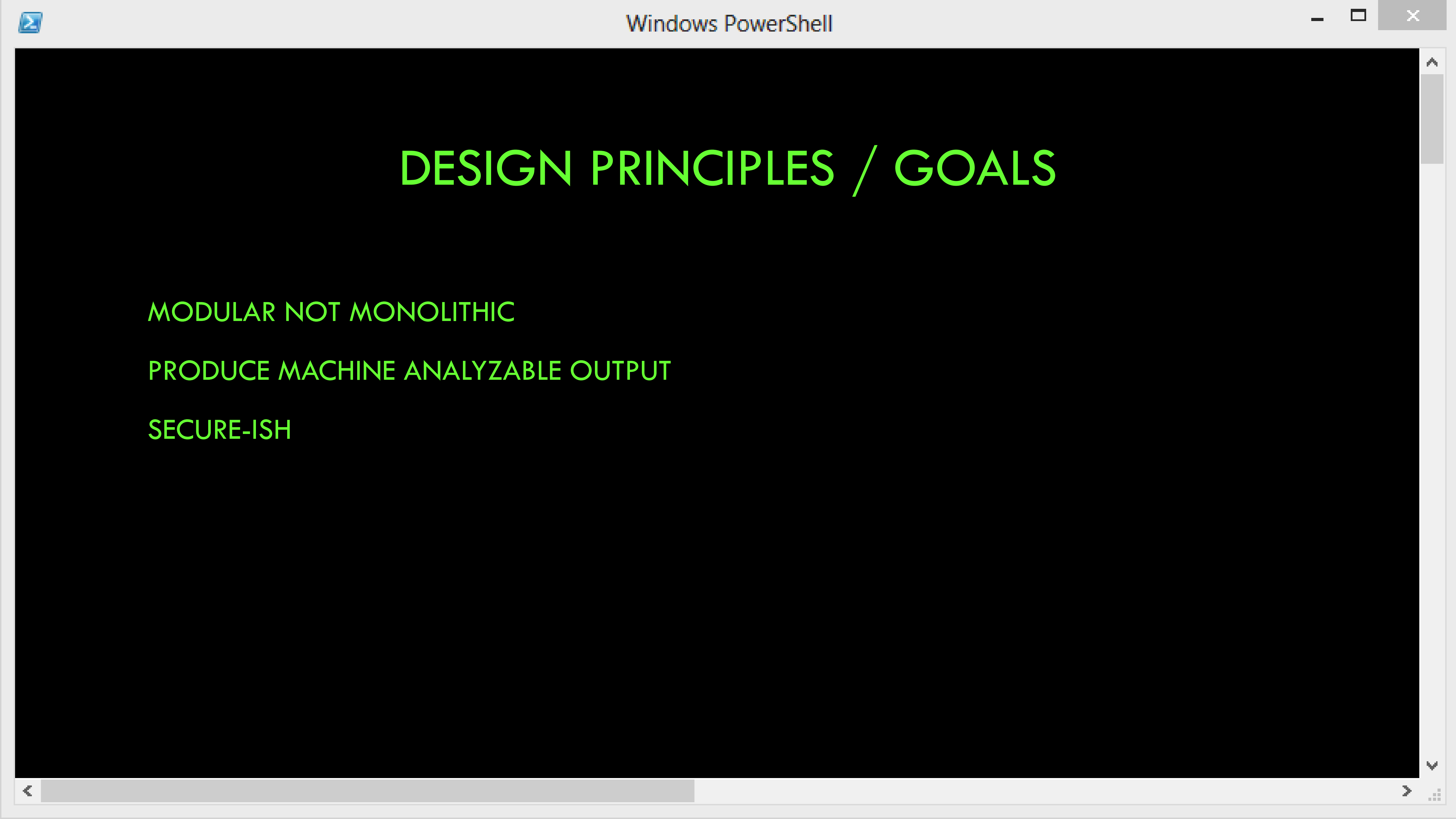


KANSA: INCIDENT RESPONSE & OPEN SOURCE IN THE BELLY OF THE BEST

Kansa is a modular IR framework in Powershell



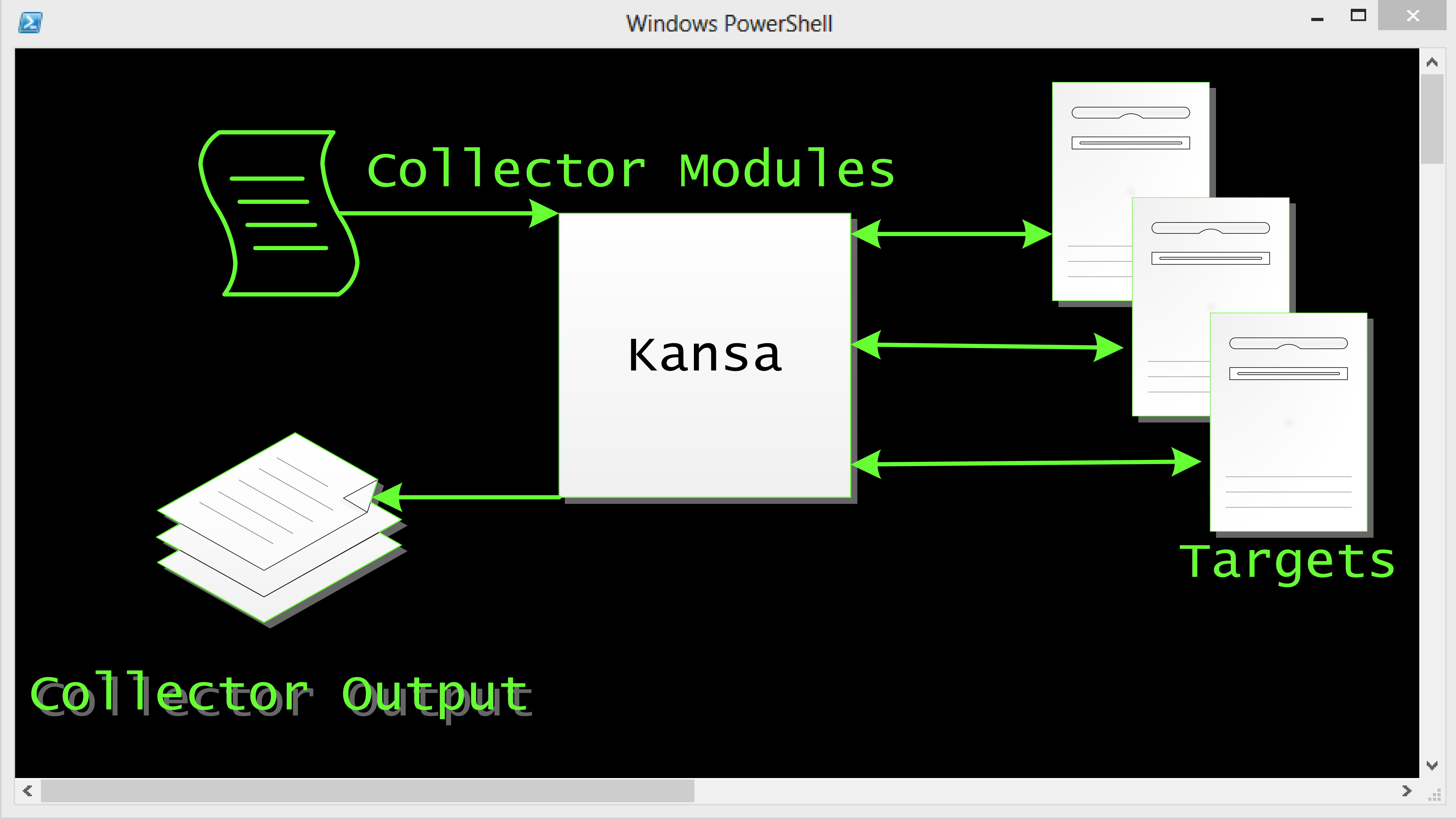


DESIGN PRINCIPLES / GOALS

MODULAR NOT MONOLITHIC

PRODUCE MACHINE ANALYZABLE OUTPUT

SECURE-ISH


Windows PowerShell
Collector Modules
Kansa
Targets
Collector Output

Windows PowerShell

Windows Remote Management and Powershell

- Native on Win7/2k8 and later
- Non-delegated Kerberos network logons
- Runs across hosts in parallel
- Read/Write enabled

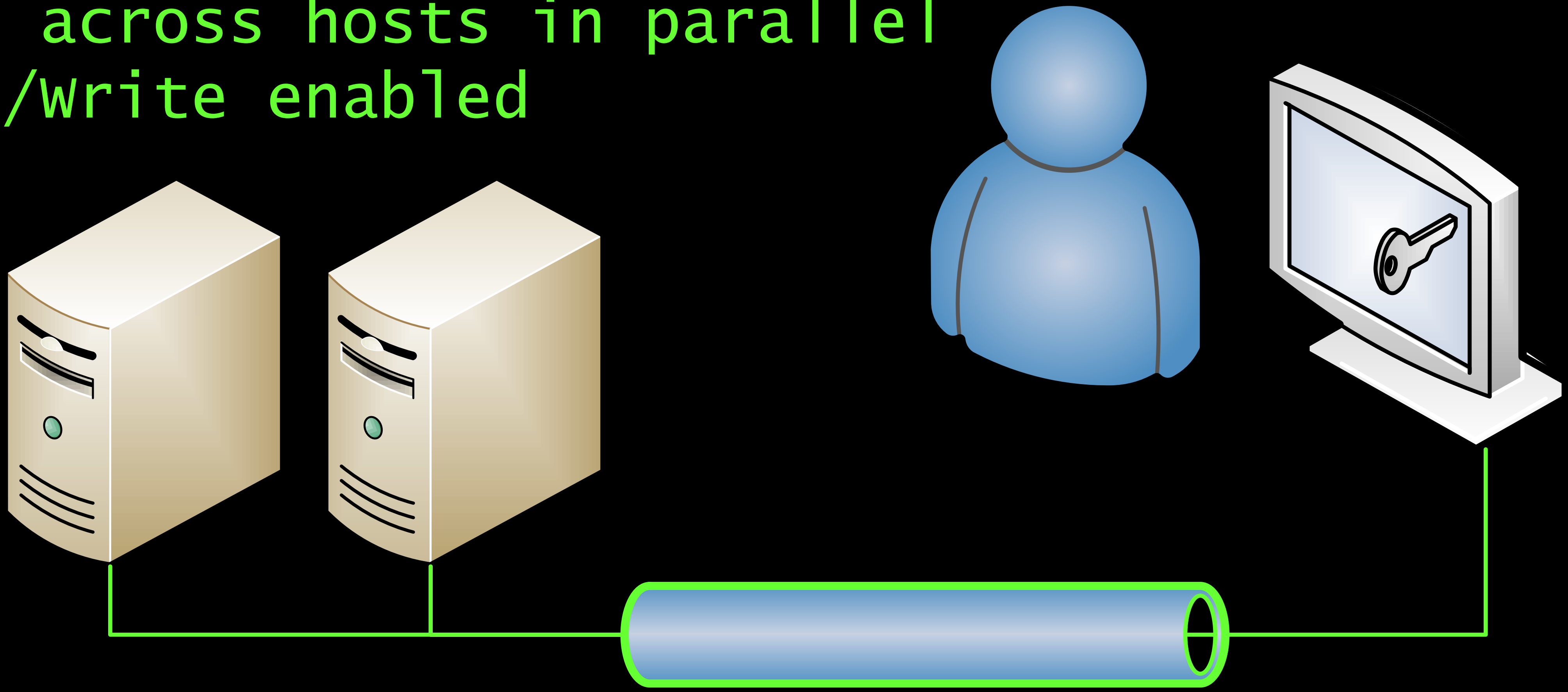
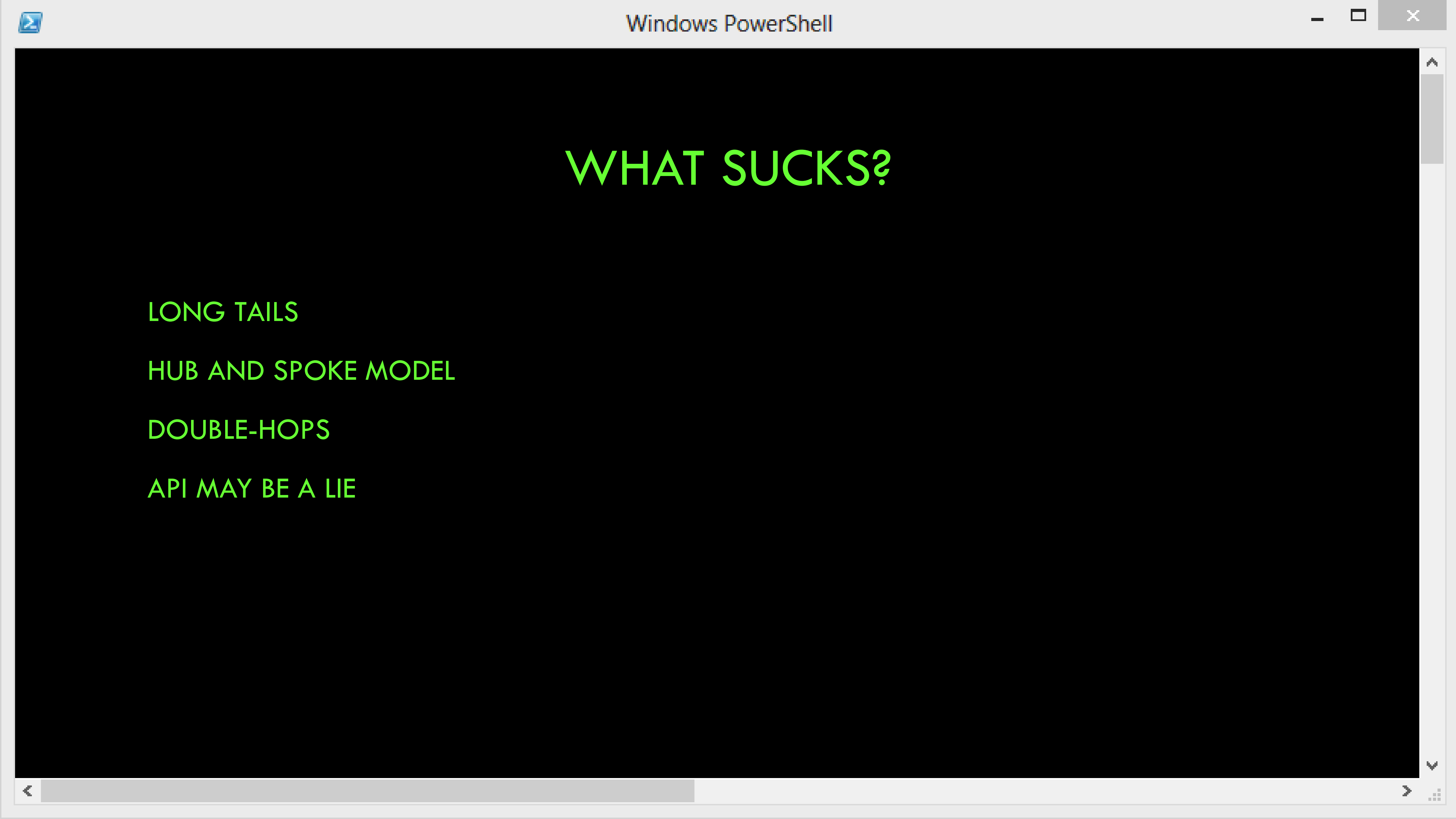


Photo Credit: https://www.flickr.com/photos/mobilestreetlife/



WHAT SUCKS?

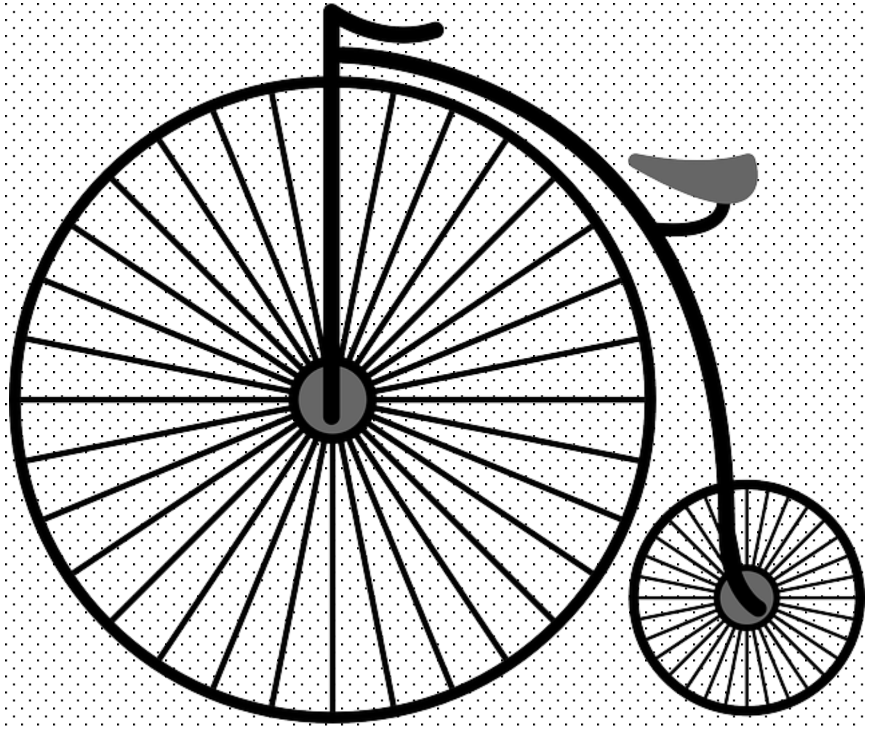
LONG TAILS

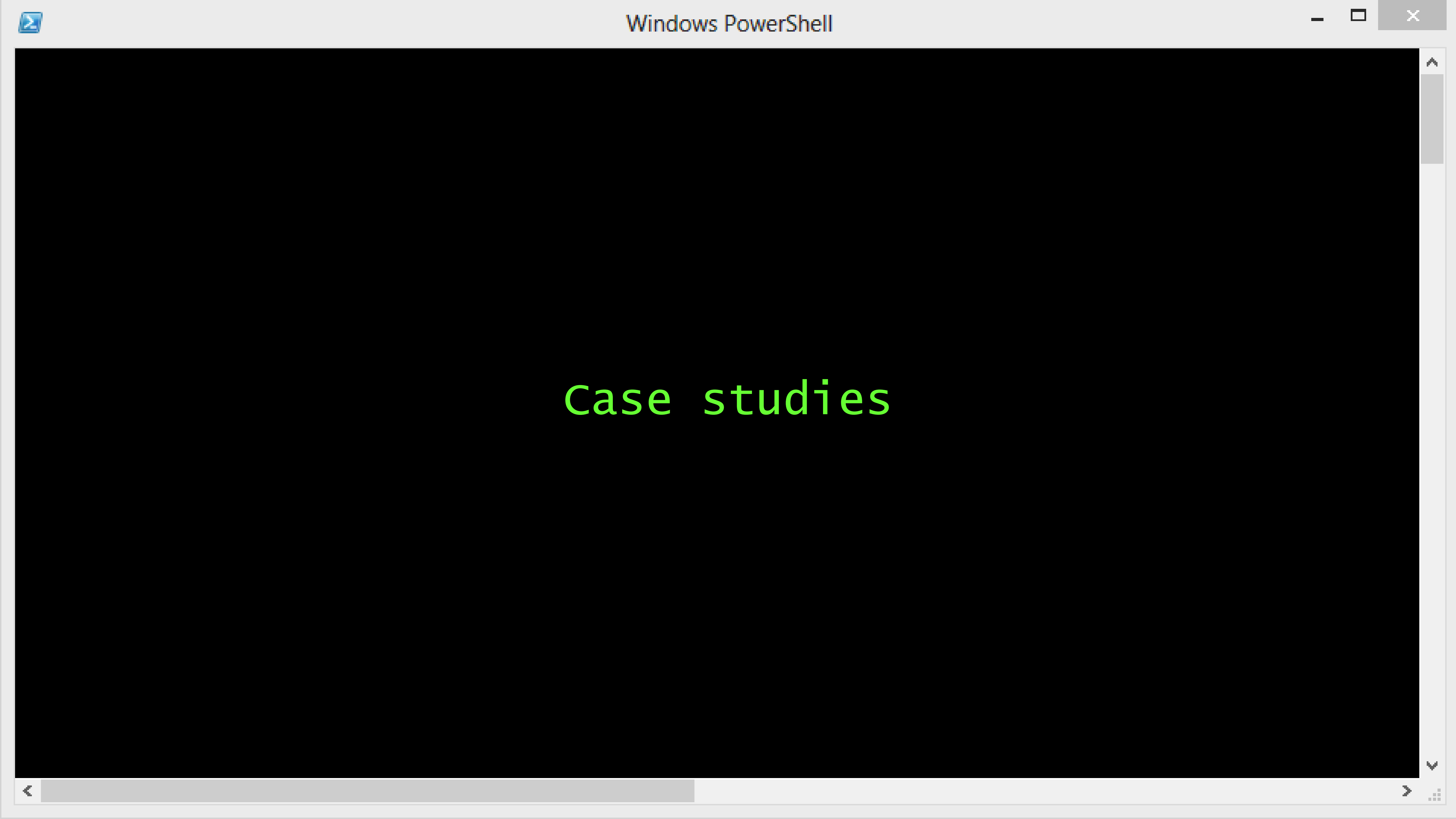
HUB AND SPOKE MODEL

DOUBLE-HOPS

API MAY BE A LIE

HUB AND SPOKE MODEL (SUBOPTIMAL)





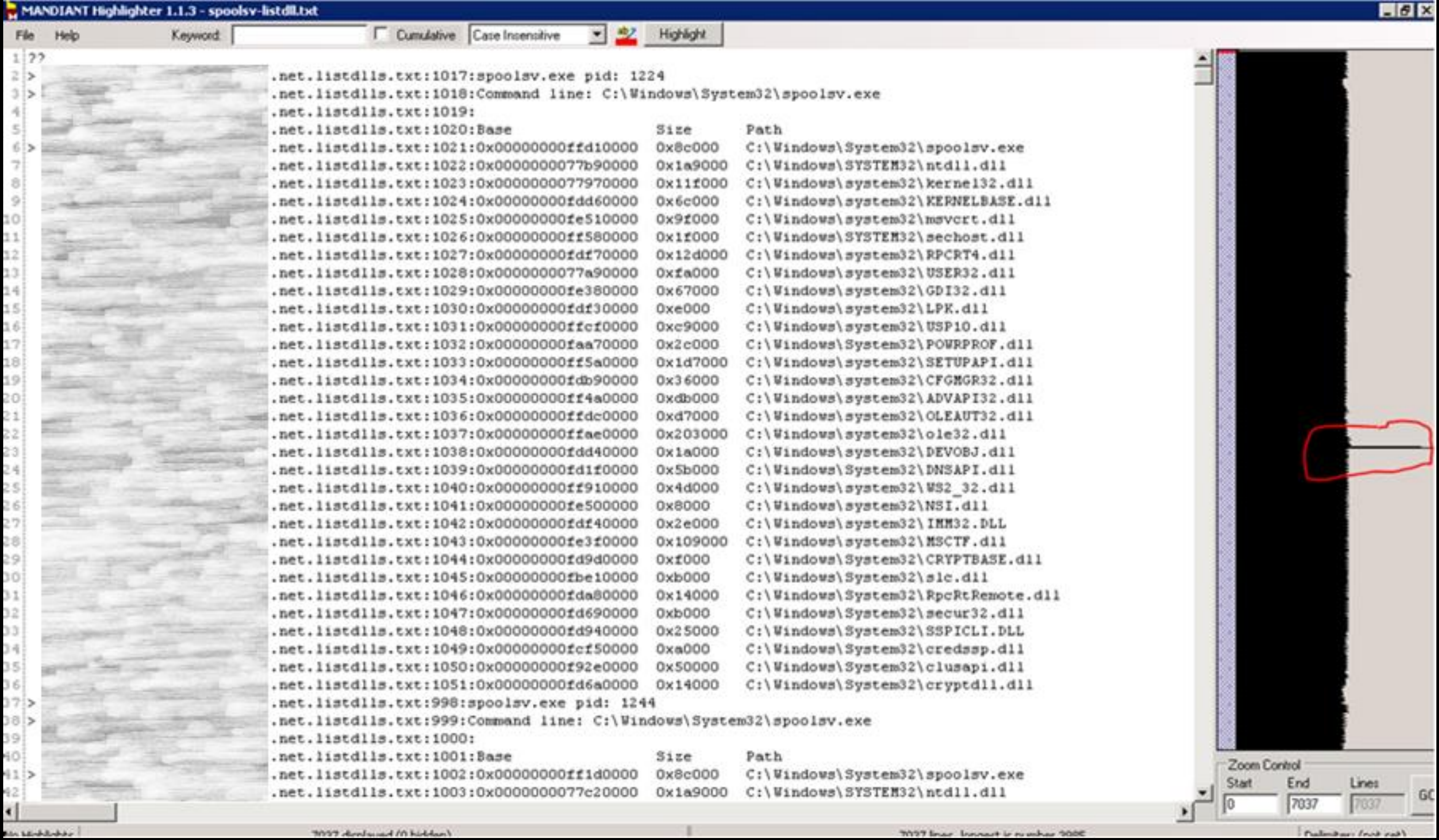
Case studies

WHY HUNT
WHEN YOU CAN SEINE?

LARGE SCALE HUNTING AND ANALYSIS

WHY HUNT WHEN YOU CAN SEINE?

SCALE – IT’S COMPLICATED: HUNTING AND ANALYSIS



```
??
> [redacted] .net.listdlls.txt:1017:spoolsv.exe pid: 1224
>   .net.listdlls.txt:1018:Command line: C:\Windows\System32\spoolsv.exe
    .net.listdlls.txt:1019:
    .net.listdlls.txt:1020:Base                 Size      Path
>   .net.listdlls.txt:1021:0x00000000ffd10000  0x8c000   C:\Windows\System32\spoolsv.exe
    .net.listdlls.txt:1022:0x0000000077b90000  0x1a9000  C:\Windows\SYSTEM32\ntdll.dll
    .net.listdlls.txt:1023:0x0000000077970000  0x11f000  C:\Windows\system32\kernel32.dll
    .net.listdlls.txt:1024:0x00000000fdd60000  0x6c000   C:\Windows\system32\KERNELBASE.dll
    .net.listdlls.txt:1025:0x00000000fe510000  0x9f000   C:\Windows\system32\msvcrt.dll
    .net.listdlls.txt:1026:0x00000000ff580000  0x1f000   C:\Windows\SYSTEM32\sechost.dll
    .net.listdlls.txt:1027:0x00000000fdf70000  0x12d000  C:\Windows\system32\RPCRT4.dll
    .net.listdlls.txt:1028:0x0000000077a90000  0xfa000   C:\Windows\system32\USER32.dll
    .net.listdlls.txt:1029:0x00000000fe380000  0x67000   C:\Windows\system32\GDI32.dll
    .net.listdlls.txt:1030:0x00000000fdf30000  0xe000    C:\Windows\system32\LPK.dll
    .net.listdlls.txt:1031:0x00000000ffcf0000  0xc9000   C:\Windows\system32\USP10.dll
    .net.listdlls.txt:1032:0x00000000faa70000  0x2c000   C:\Windows\System32\POWRPROF.dll
    .net.listdlls.txt:1033:0x00000000ff5a0000  0x1d7000  C:\Windows\system32\SETUPAPI.dll
    .net.listdlls.txt:1034:0x00000000fdb90000  0x36000   C:\Windows\system32\CFGMGR32.dll
    .net.listdlls.txt:1035:0x00000000ff4a0000  0xdb000   C:\Windows\system32\ADVAPI32.dll
    .net.listdlls.txt:1036:0x00000000ffdc0000  0xd7000   C:\Windows\system32\OLEAUT32.dll
    .net.listdlls.txt:1037:0x00000000ffae0000  0x203000  C:\Windows\system32\ole32.dll
    .net.listdlls.txt:1038:0x00000000fdd40000  0x1a000   C:\Windows\system32\DEVOBJ.dll
    .net.listdlls.txt:1039:0x00000000fd1f0000  0x5b000   C:\Windows\System32\DNSAPI.dll
    .net.listdlls.txt:1040:0x00000000ff910000  0x4d000   C:\Windows\system32\WS2_32.dll
    .net.listdlls.txt:1041:0x00000000fe500000  0x8000    C:\Windows\system32\NSI.dll
    .net.listdlls.txt:1042:0x00000000fdf40000  0x2e000   C:\Windows\system32\IMM32.DLL
    .net.listdlls.txt:1043:0x00000000fe3f0000  0x109000  C:\Windows\system32\MSCTF.dll
    .net.listdlls.txt:1044:0x00000000fd9d0000  0xf000    C:\Windows\System32\CRYPTBASE.dll
    .net.listdlls.txt:1045:0x00000000fbe10000  0xb000    C:\Windows\System32\slc.dll
    .net.listdlls.txt:1046:0x00000000fda80000  0x14000   C:\Windows\System32\RpcRtRemote.dll
    .net.listdlls.txt:1047:0x00000000fd690000  0xb000    C:\Windows\System32\secur32.dll
    .net.listdlls.txt:1048:0x00000000fd940000  0x25000   C:\Windows\System32\SSPICLI.DLL
    .net.listdlls.txt:1049:0x00000000fcf50000  0xa000    C:\Windows\System32\credssp.dll
    .net.listdlls.txt:1050:0x00000000f92e0000  0x50000   C:\Windows\System32\clusapi.dll
    .net.listdlls.txt:1051:0x00000000fd6a0000  0x14000   C:\Windows\System32\cryptdll.dll
>   .net.listdlls.txt:998:spoolsv.exe pid: 1244
>   .net.listdlls.txt:999:Command line: C:\Windows\System32\spoolsv.exe
    .net.listdlls.txt:1000:
    .net.listdlls.txt:1001:Base                 Size      Path
>   .net.listdlls.txt:1002:0x00000000ff1d0000  0x8c000   C:\Windows\System32\spoolsv.exe
    .net.listdlls.txt:1003:0x0000000077c20000  0x1a9000  C:\Windows\SYSTEM32\ntdll.dll
```

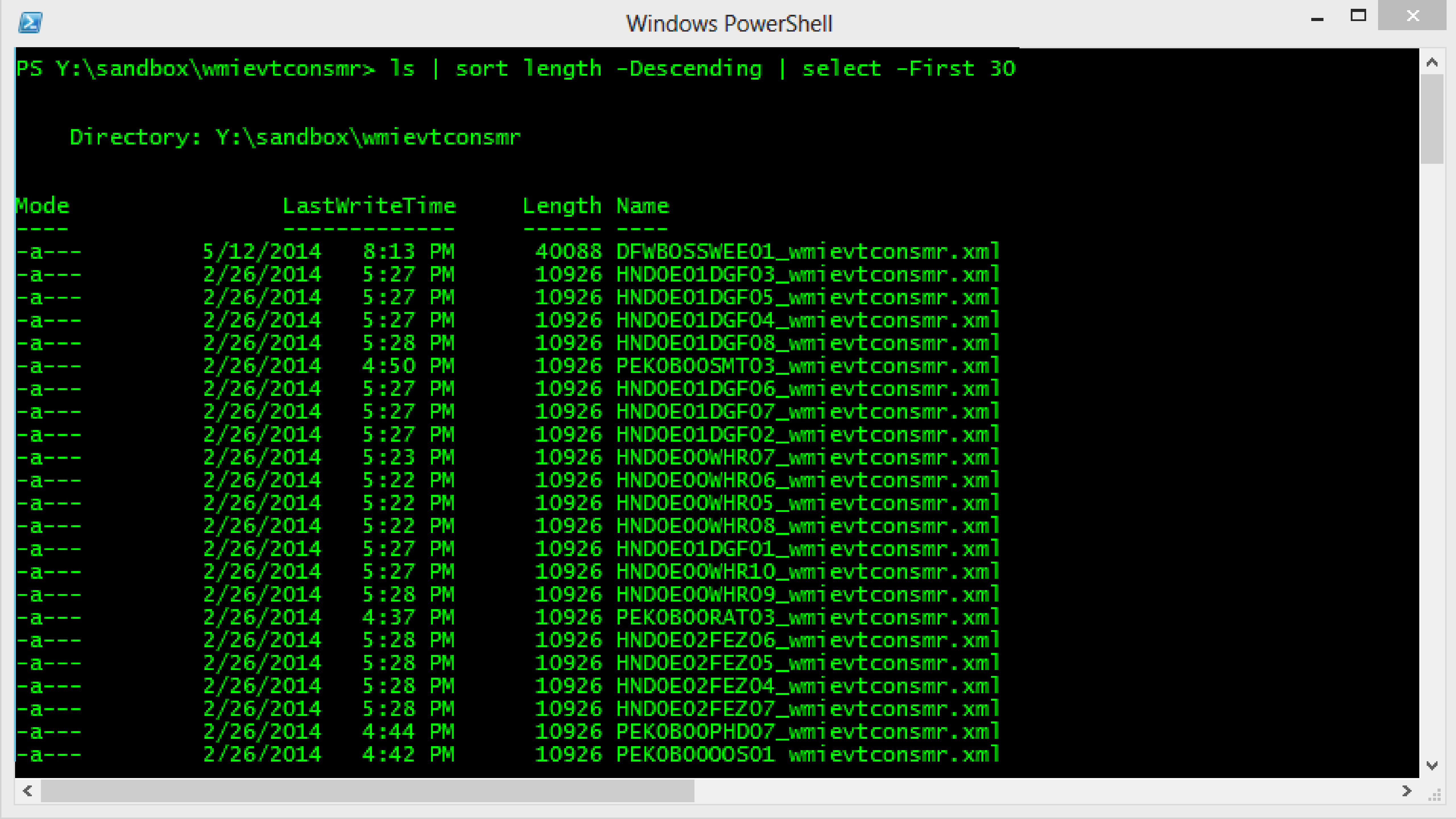
Zoom Control
Start: 0 End: 7037 Lines: 7037 GO

No Highlights

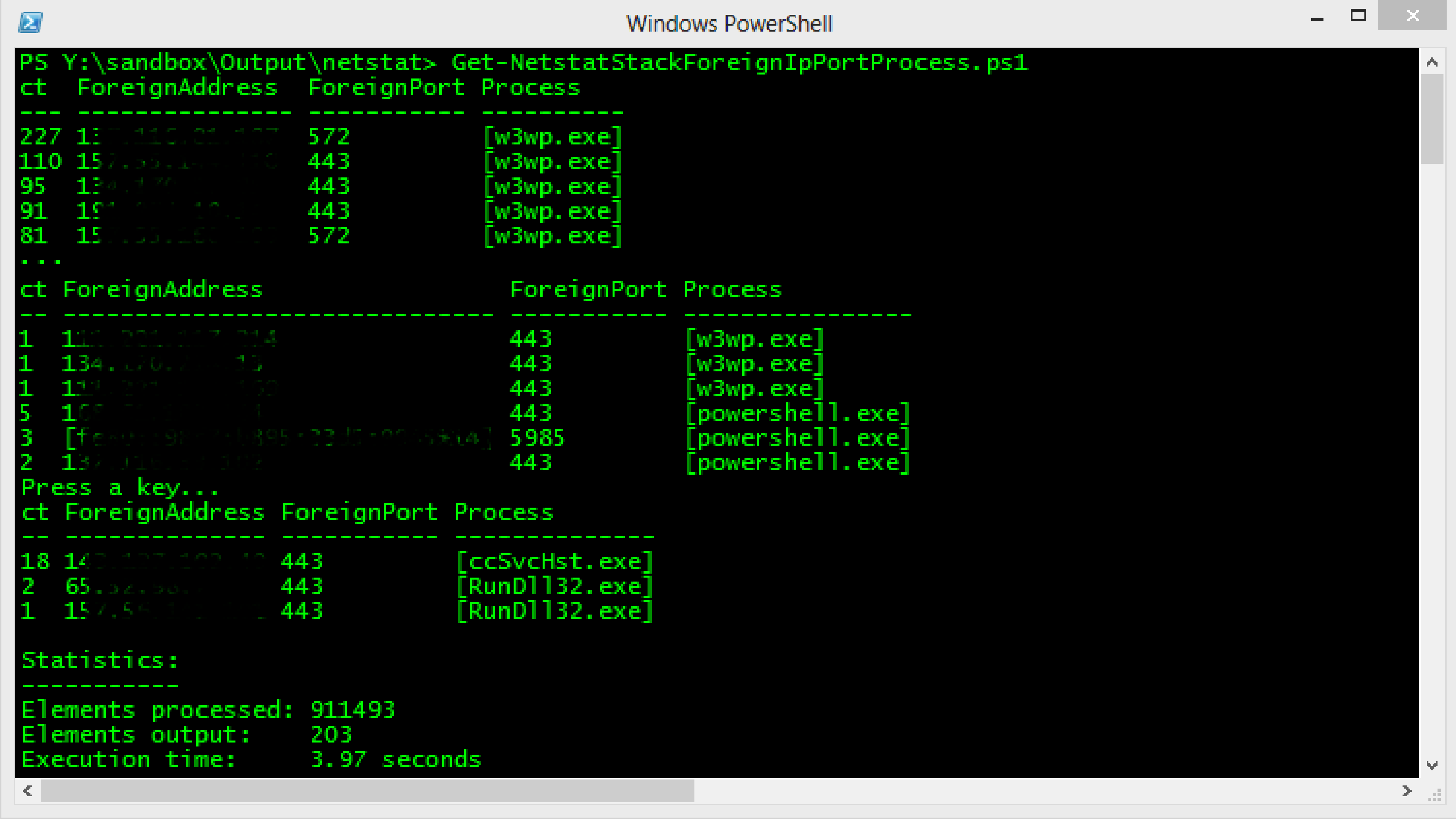
7037 displayed (0 hidden)

7037 lines, longest is number 2985

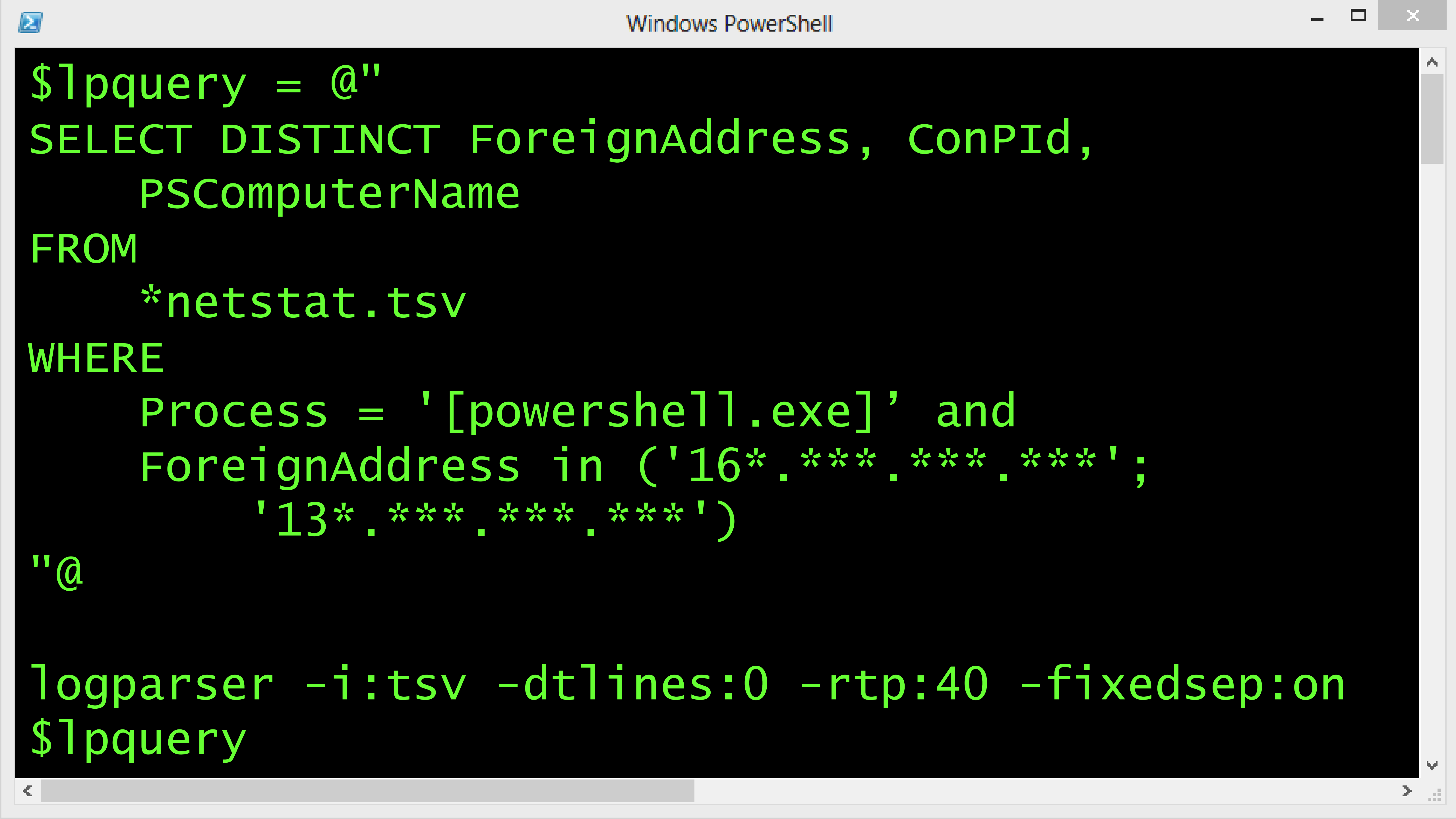
Delimiter: (not set)



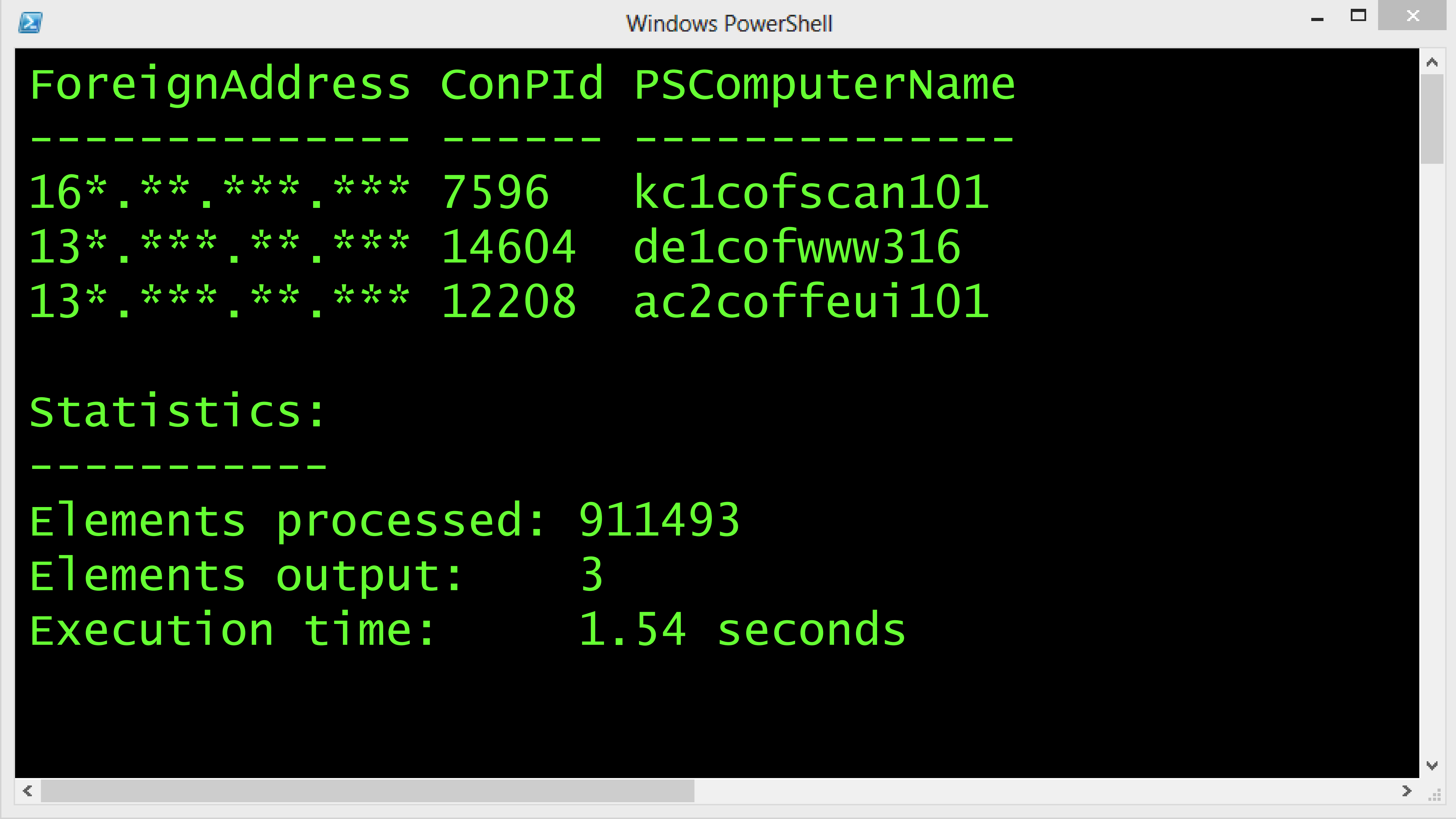
```
PS Y:\sandbox\wmievtconsmr> ls | sort length -Descending | select -First 30


    Directory: Y:\sandbox\wmievtconsmr


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
-a---         5/12/2014   8:13 PM      40088 DFWBOSSWEE01_wmievtconsmr.xml
-a---         2/26/2014   5:27 PM      10926 HND0E01DGF03_wmievtconsmr.xml
-a---         2/26/2014   5:27 PM      10926 HND0E01DGF05_wmievtconsmr.xml
-a---         2/26/2014   5:27 PM      10926 HND0E01DGF04_wmievtconsmr.xml
-a---         2/26/2014   5:28 PM      10926 HND0E01DGF08_wmievtconsmr.xml
-a---         2/26/2014   4:50 PM      10926 PEK0B00SMT03_wmievtconsmr.xml
-a---         2/26/2014   5:27 PM      10926 HND0E01DGF06_wmievtconsmr.xml
-a---         2/26/2014   5:27 PM      10926 HND0E01DGF07_wmievtconsmr.xml
-a---         2/26/2014   5:27 PM      10926 HND0E01DGF02_wmievtconsmr.xml
-a---         2/26/2014   5:23 PM      10926 HND0E00WHR07_wmievtconsmr.xml
-a---         2/26/2014   5:22 PM      10926 HND0E00WHR06_wmievtconsmr.xml
-a---         2/26/2014   5:22 PM      10926 HND0E00WHR05_wmievtconsmr.xml
-a---         2/26/2014   5:22 PM      10926 HND0E00WHR08_wmievtconsmr.xml
-a---         2/26/2014   5:27 PM      10926 HND0E01DGF01_wmievtconsmr.xml
-a---         2/26/2014   5:27 PM      10926 HND0E00WHR10_wmievtconsmr.xml
-a---         2/26/2014   5:28 PM      10926 HND0E00WHR09_wmievtconsmr.xml
-a---         2/26/2014   4:37 PM      10926 PEK0B00RAT03_wmievtconsmr.xml
-a---         2/26/2014   5:28 PM      10926 HND0E02FEZ06_wmievtconsmr.xml
-a---         2/26/2014   5:28 PM      10926 HND0E02FEZ05_wmievtconsmr.xml
-a---         2/26/2014   5:28 PM      10926 HND0E02FEZ04_wmievtconsmr.xml
-a---         2/26/2014   5:28 PM      10926 HND0E02FEZ07_wmievtconsmr.xml
-a---         2/26/2014   4:44 PM      10926 PEK0B00PHD07_wmievtconsmr.xml
-a---         2/26/2014   4:42 PM      10926 PEK0B000OS01 wmievtconsmr.xml
```



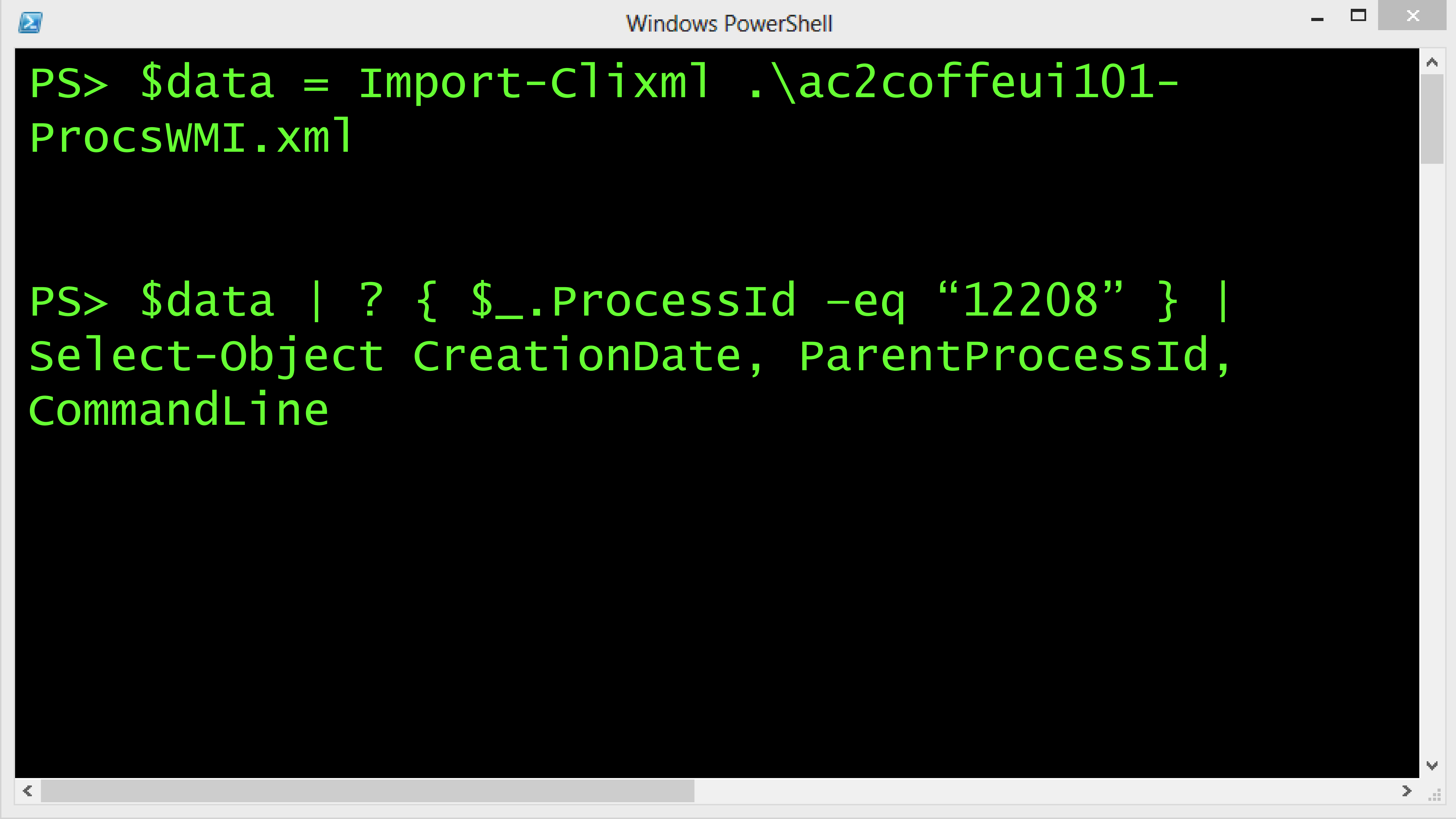
```
PS Y:\sandbox\Output\netstat> Get-NetstatStackForeignIpPortProcess.ps1
ct  ForeignAddress  ForeignPort Process
--- --------------- ----------- ---------
227 1[redacted]     572         [w3wp.exe]
110 15[redacted]    443         [w3wp.exe]
95  13[redacted]    443         [w3wp.exe]
91  1[redacted]     443         [w3wp.exe]
81  15[redacted]    572         [w3wp.exe]
...
ct ForeignAddress                 ForeignPort Process
-- ------------------------------ ----------- ----------------
1  1[redacted]                    443         [w3wp.exe]
1  134.[redacted]                 443         [w3wp.exe]
1  1[redacted]                    443         [w3wp.exe]
5  1[redacted]                    443         [powershell.exe]
3  [f[redacted]                   5985        [powershell.exe]
2  13[redacted]                   443         [powershell.exe]
Press a key...
ct ForeignAddress ForeignPort Process
-- -------------- ----------- --------------
18 14[redacted]   443         [ccSvcHst.exe]
2  65.[redacted]  443         [RunDll32.exe]
1  15[redacted]   443         [RunDll32.exe]

Statistics:
-----------
Elements processed: 911493
Elements output:    203
Execution time:     3.97 seconds
```



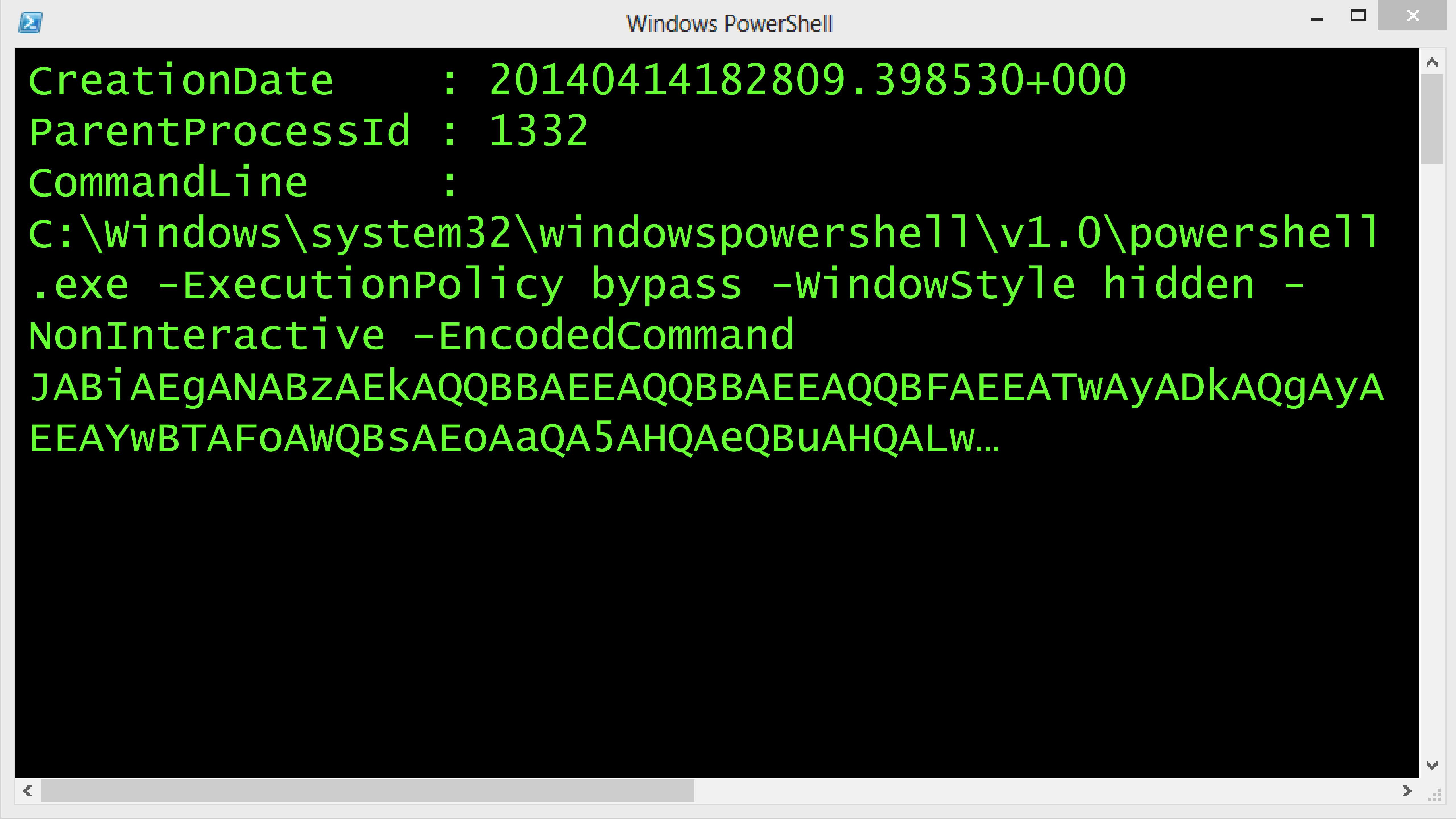
```
$lpquery = @"
SELECT DISTINCT ForeignAddress, ConPId,
    PSComputerName
FROM
    *netstat.tsv
WHERE
    Process = '[powershell.exe]’ and
    ForeignAddress in ('16*.***.***.***';
        '13*.***.***.***')
"@

logparser -i:tsv -dtlines:0 -rtp:40 -fixedsep:on
$lpquery
```



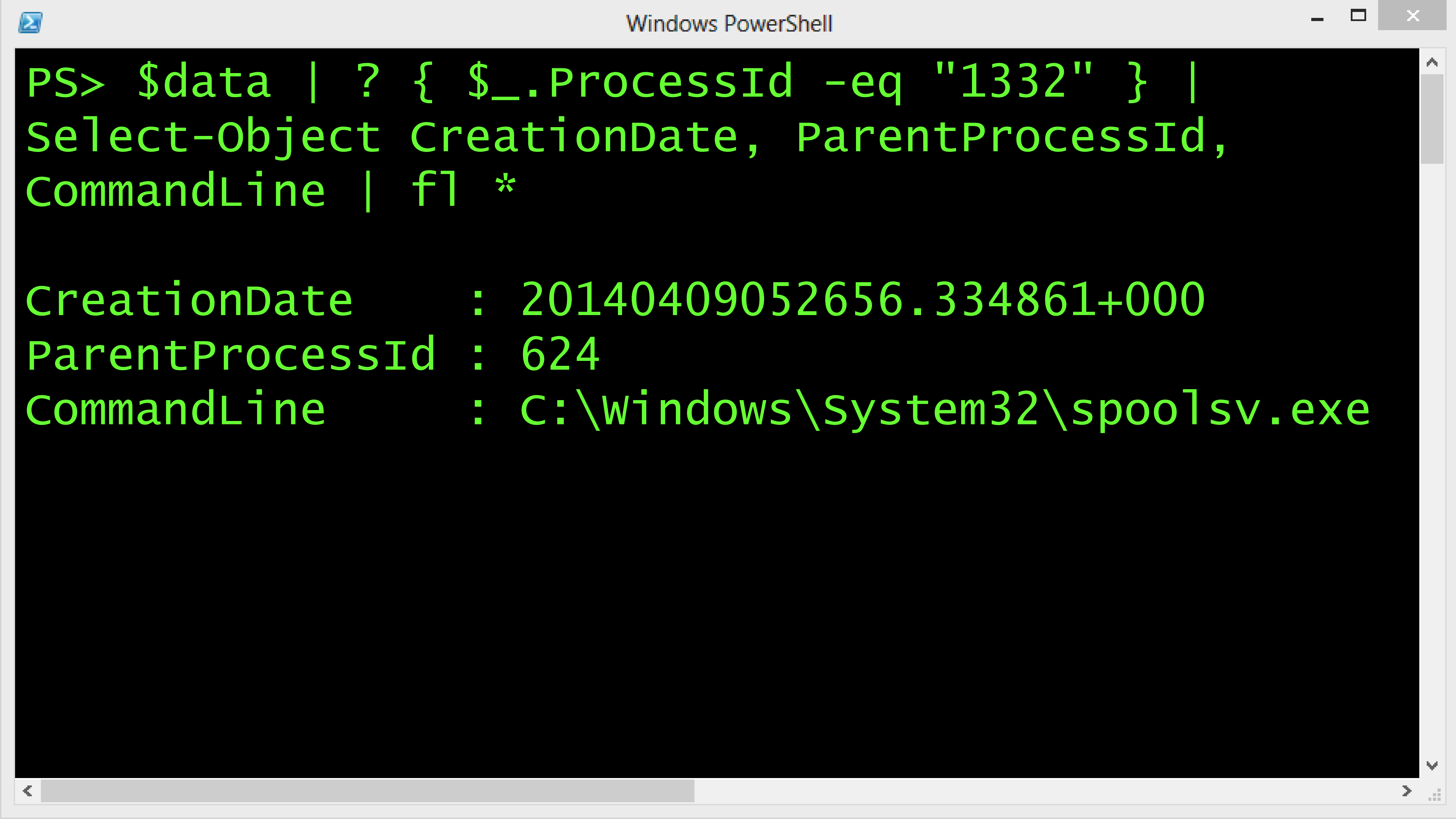
```
ForeignAddress ConPId PSComputerName
-------------- ------ --------------
16*.**.***.*** 7596   kc1cofscan101
13*.***.**.*** 14604  de1cofwww316
13*.***.**.*** 12208  ac2coffeui101


Statistics:
-----------
Elements processed: 911493
Elements output:    3
Execution time:     1.54 seconds
```



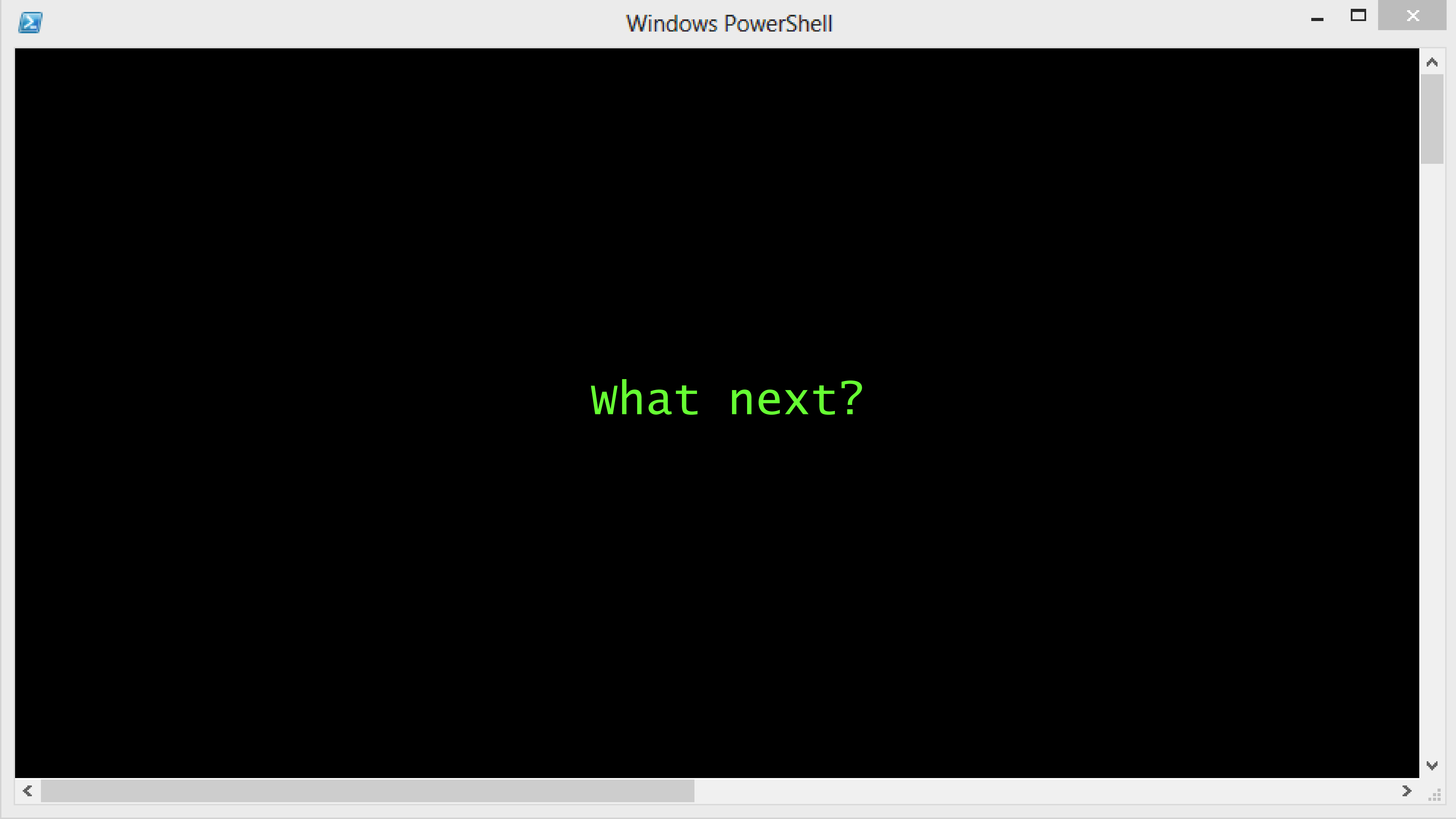
```
PS> $data = Import-Clixml .\ac2coffeui101-
ProcsWMI.xml


PS> $data | ? { $_.ProcessId –eq “12208” } |
Select-Object CreationDate, ParentProcessId,
CommandLine
```



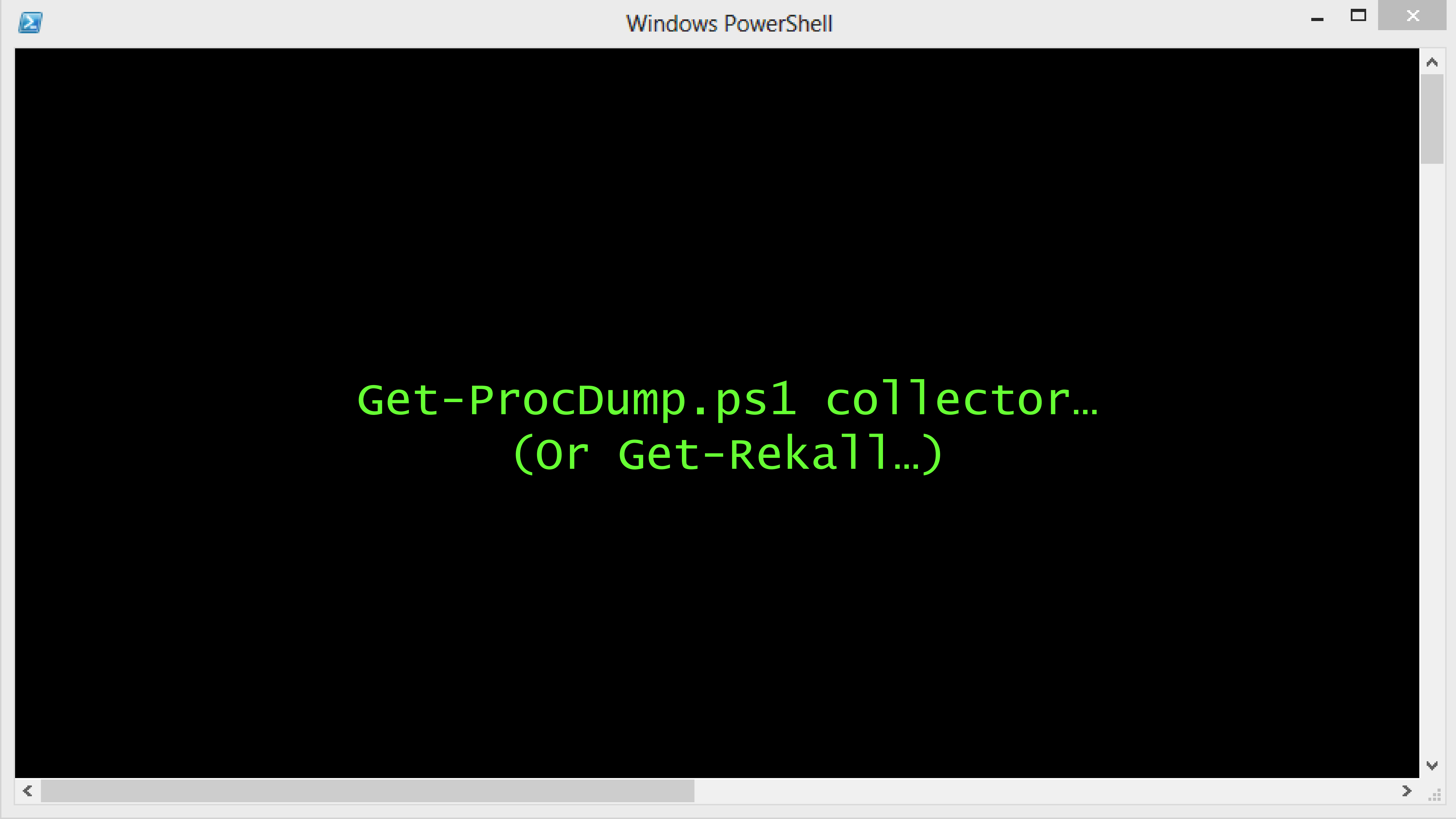
```
CreationDate    : 20140414182809.398530+000
ParentProcessId : 1332
CommandLine     :
C:\Windows\system32\windowspowershell\v1.0\powershell
.exe -ExecutionPolicy bypass -WindowStyle hidden -
NonInteractive -EncodedCommand
JABiAEgANABzAEkAQQBBAEEAQQBBAEEAQQBFAEEATwAyADkAQQgAyA
EEAYwBTAFoAWQBsAEoAaQA5AHQAeQBuAHQALw…
```



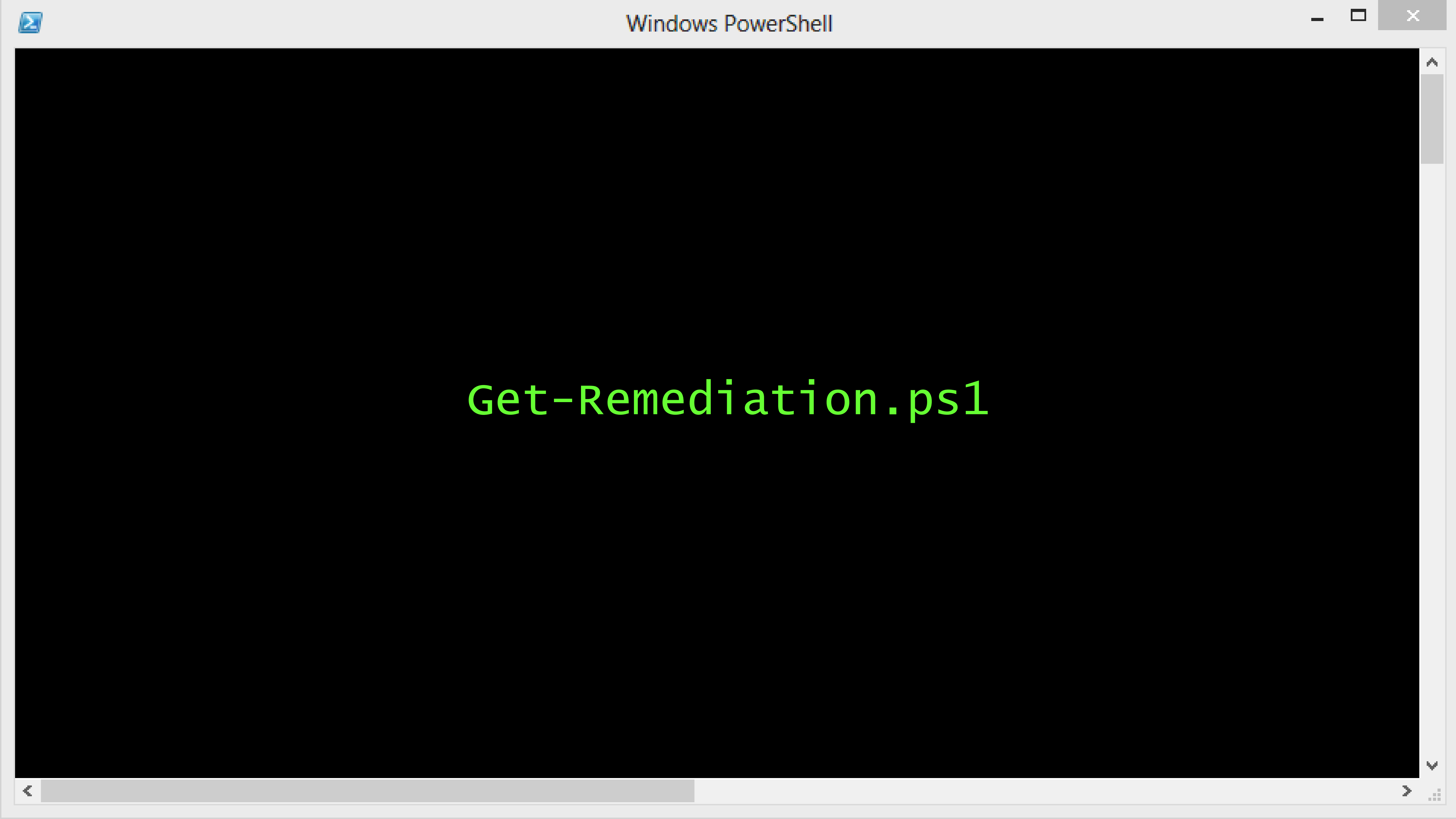
```
PS> $data | ? { $_.ProcessId -eq "1332" } |
Select-Object CreationDate, ParentProcessId,
CommandLine | fl *

CreationDate    : 20140409052656.334861+000
ParentProcessId : 624
CommandLine     : C:\Windows\System32\spoolsv.exe
```



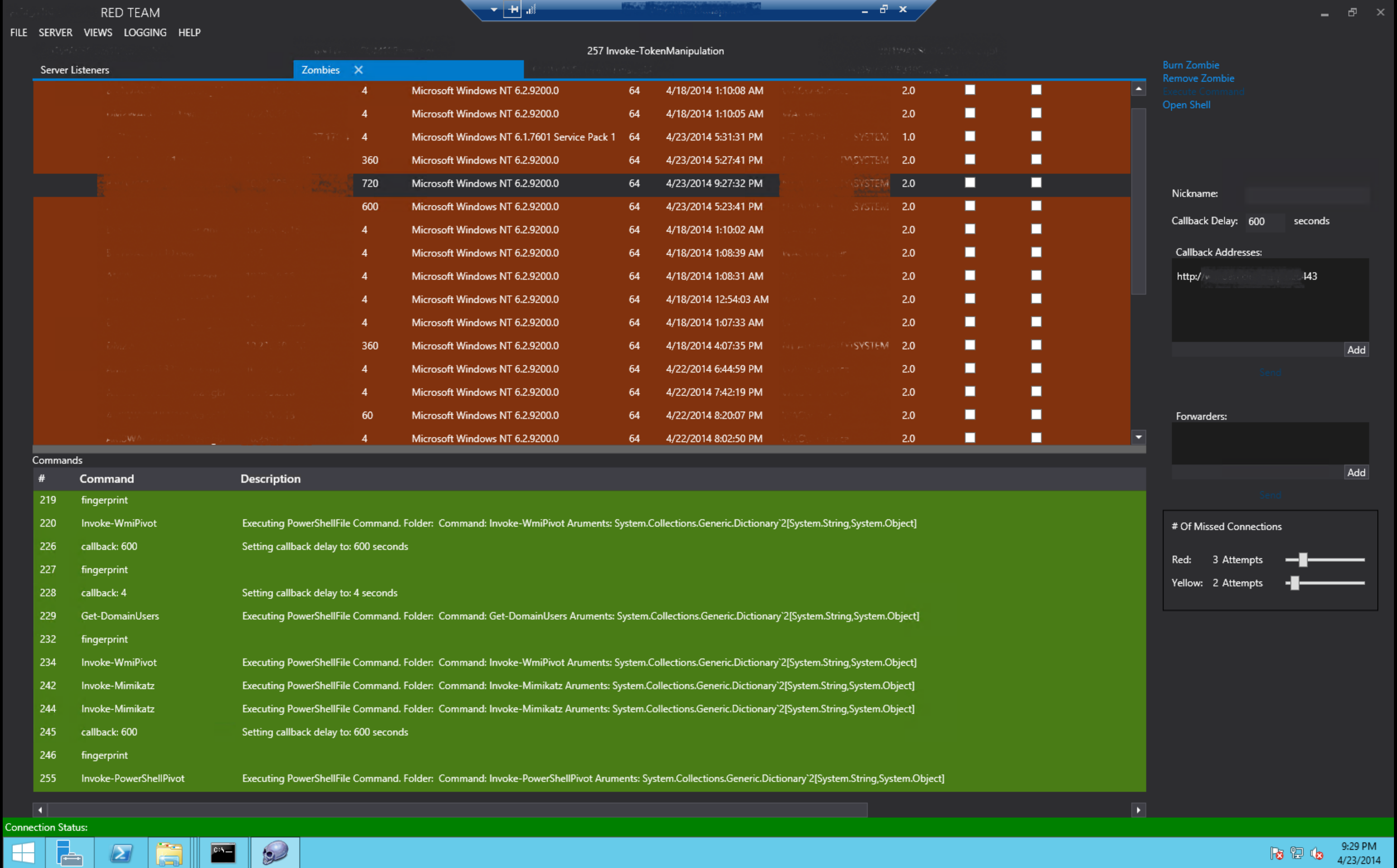
```
what next?
```



```
Get-ProcDump.ps1 collector…
(Or Get-Rekall…)
```



```
Get-Remediation.ps1
```



257 Invoke-TokenManipulation

[redacted]	4	Microsoft Windows NT 6.2.9200.0	64	4/18/2014 1:10:08 AM	[redacted]	2.0	☐	☐
[redacted]	4	Microsoft Windows NT 6.2.9200.0	64	4/18/2014 1:10:05 AM	[redacted]	2.0	☐	☐
[redacted]	4	Microsoft Windows NT 6.1.7601 Service Pack 1	64	4/23/2014 5:31:31 PM	[redacted]	1.0	☐	☐
[redacted]	360	Microsoft Windows NT 6.2.9200.0	64	4/23/2014 5:27:41 PM	[redacted]	2.0	☐	☐
[redacted]	720	Microsoft Windows NT 6.2.9200.0	64	4/23/2014 9:27:32 PM	[redacted]	2.0	☐	☐
[redacted]	600	Microsoft Windows NT 6.2.9200.0	64	4/23/2014 5:23:41 PM	[redacted]	2.0	☐	☐
[redacted]	4	Microsoft Windows NT 6.2.9200.0	64	4/18/2014 1:10:02 AM	[redacted]	2.0	☐	☐
[redacted]	4	Microsoft Windows NT 6.2.9200.0	64	4/18/2014 1:08:39 AM	[redacted]	2.0	☐	☐
[redacted]	4	Microsoft Windows NT 6.2.9200.0	64	4/18/2014 1:08:31 AM	[redacted]	2.0	☐	☐
[redacted]	4	Microsoft Windows NT 6.2.9200.0	64	4/18/2014 12:54:03 AM	[redacted]	2.0	☐	☐
[redacted]	4	Microsoft Windows NT 6.2.9200.0	64	4/18/2014 1:07:33 AM	[redacted]	2.0	☐	☐
[redacted]	360	Microsoft Windows NT 6.2.9200.0	64	4/18/2014 4:07:35 PM	[redacted]	2.0	☐	☐
[redacted]	4	Microsoft Windows NT 6.2.9200.0	64	4/22/2014 6:44:59 PM	[redacted]	2.0	☐	☐
[redacted]	4	Microsoft Windows NT 6.2.9200.0	64	4/22/2014 7:42:19 PM	[redacted]	2.0	☐	☐
[redacted]	60	Microsoft Windows NT 6.2.9200.0	64	4/22/2014 8:20:07 PM	[redacted]	2.0	☐	☐
[redacted]	4	Microsoft Windows NT 6.2.9200.0	64	4/22/2014 8:02:50 PM	[redacted]	2.0	☐	☐

Nickname:

Callback Delay: 600 seconds

Callback Addresses:

http:/[redacted]43

Forwarders:

# Of Missed Connections

Red: 3 Attempts

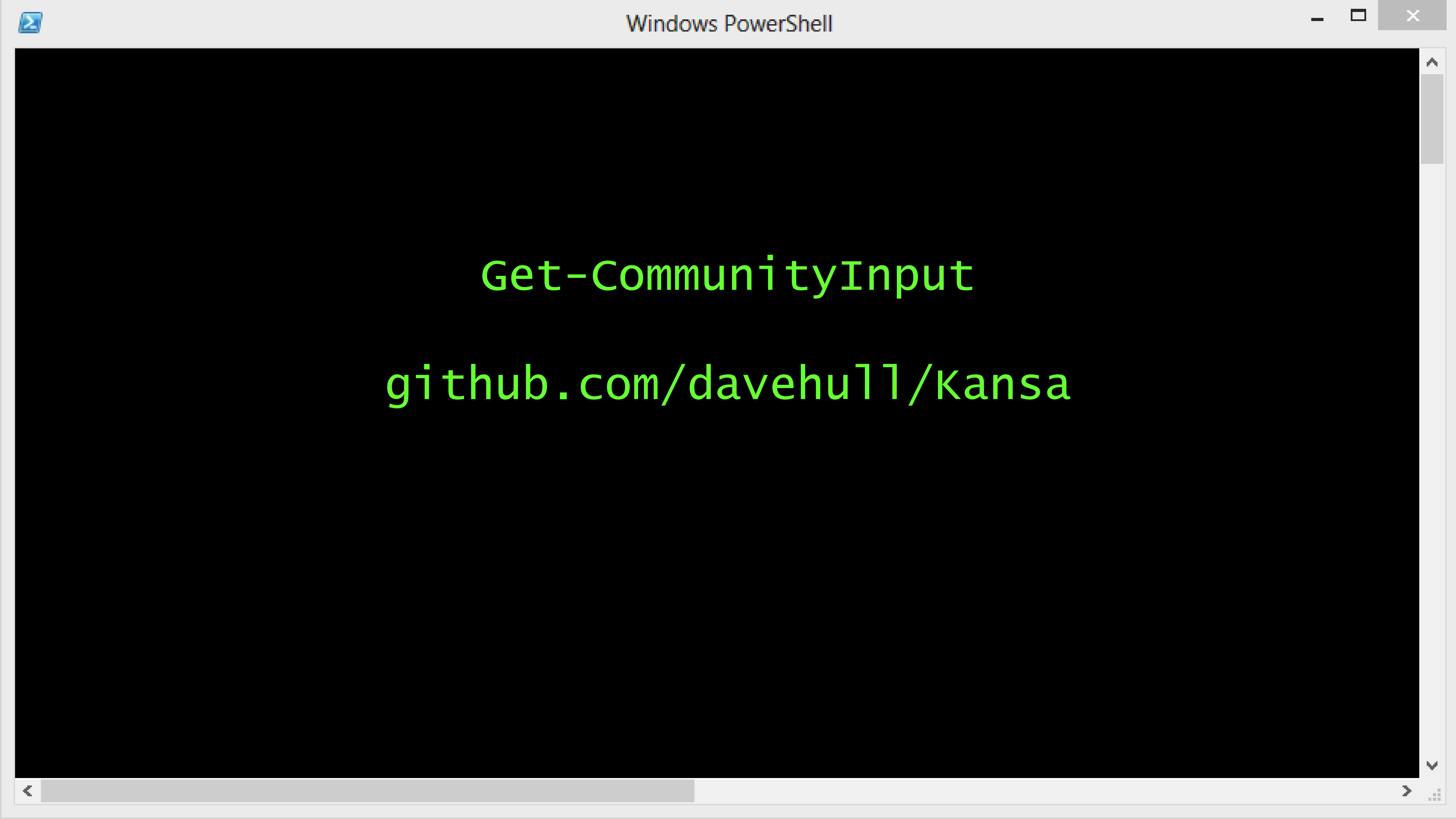
Yellow: 2 Attempts

Commands

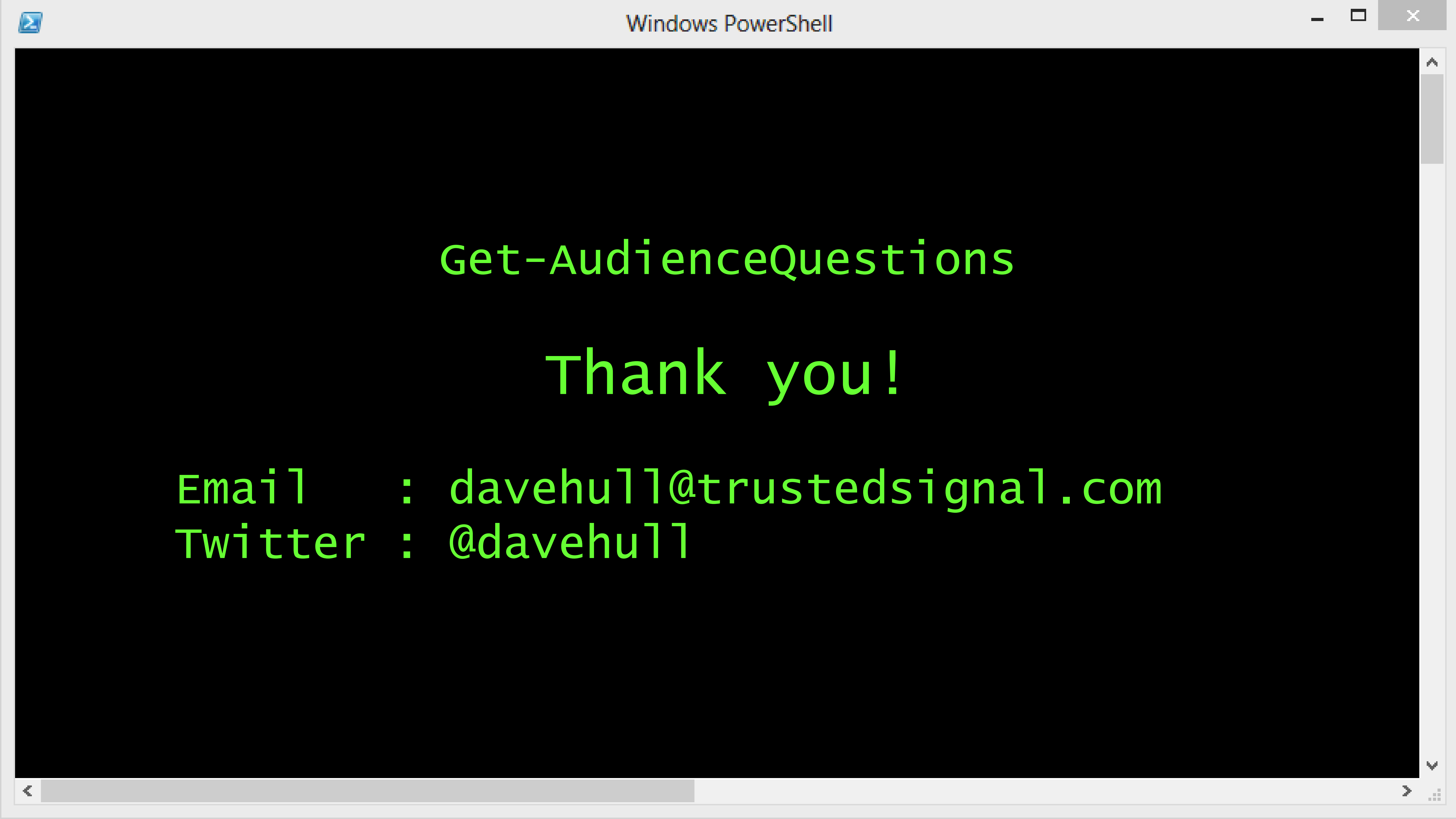
#	Command	Description
219	fingerprint	
220	Invoke-WmiPivot	Executing PowerShellFile Command. Folder: Command: Invoke-WmiPivot Aruments: System.Collections.Generic.Dictionary`2[System.String,System.Object]
226	callback: 600	Setting callback delay to: 600 seconds
227	fingerprint	
228	callback: 4	Setting callback delay to: 4 seconds
229	Get-DomainUsers	Executing PowerShellFile Command. Folder: Command: Get-DomainUsers Aruments: System.Collections.Generic.Dictionary`2[System.String,System.Object]
232	fingerprint	
234	Invoke-WmiPivot	Executing PowerShellFile Command. Folder: Command: Invoke-WmiPivot Aruments: System.Collections.Generic.Dictionary`2[System.String,System.Object]
242	Invoke-Mimikatz	Executing PowerShellFile Command. Folder: Command: Invoke-Mimikatz Aruments: System.Collections.Generic.Dictionary`2[System.String,System.Object]
244	Invoke-Mimikatz	Executing PowerShellFile Command. Folder: Command: Invoke-Mimikatz Aruments: System.Collections.Generic.Dictionary`2[System.String,System.Object]
245	callback: 600	Setting callback delay to: 600 seconds
246	fingerprint	
255	Invoke-PowerShellPivot	Executing PowerShellFile Command. Folder: Command: Invoke-PowerShellPivot Aruments: System.Collections.Generic.Dictionary`2[System.String,System.Object]

Connection Status:

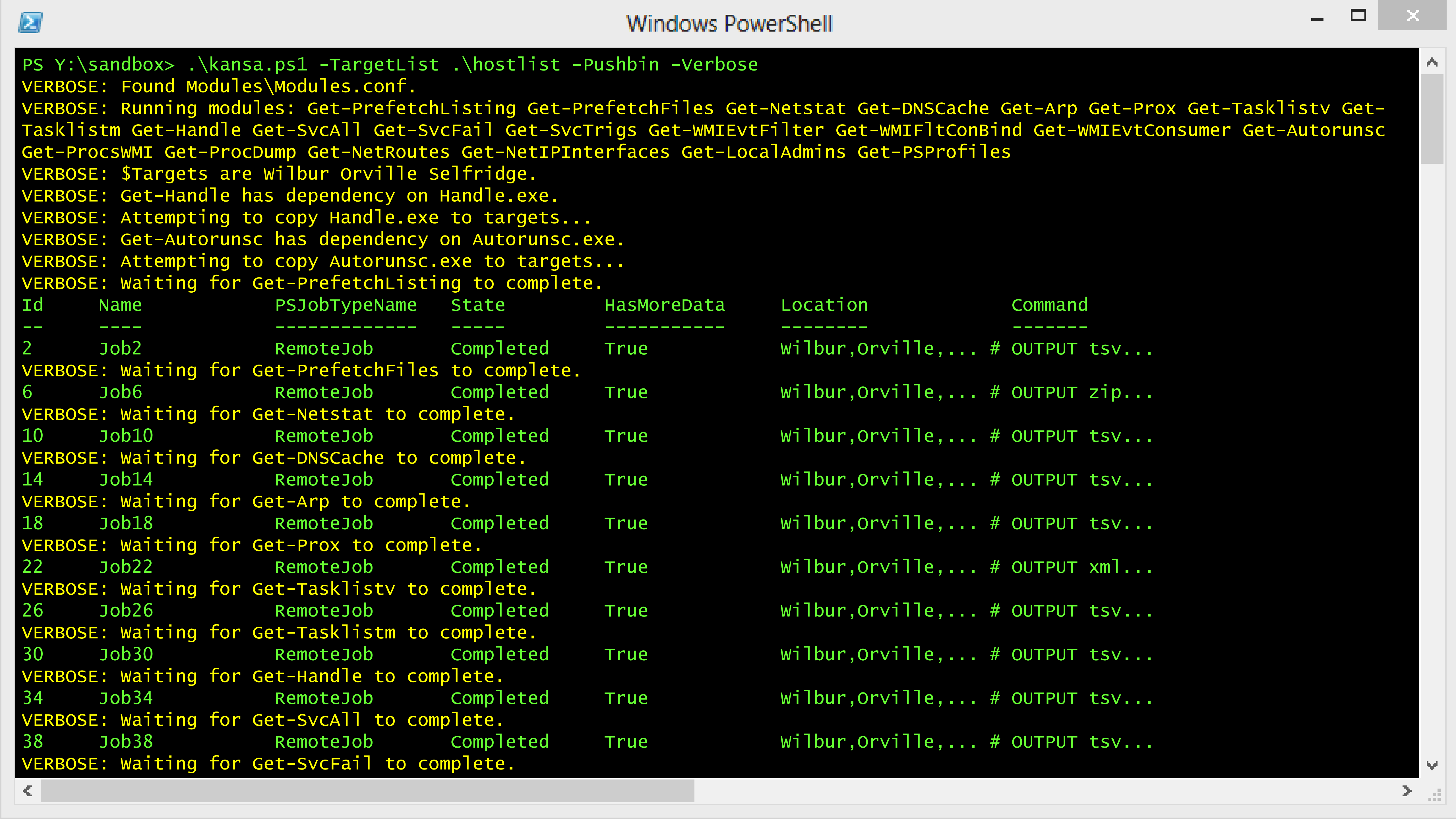
9:29 PM
4/23/2014



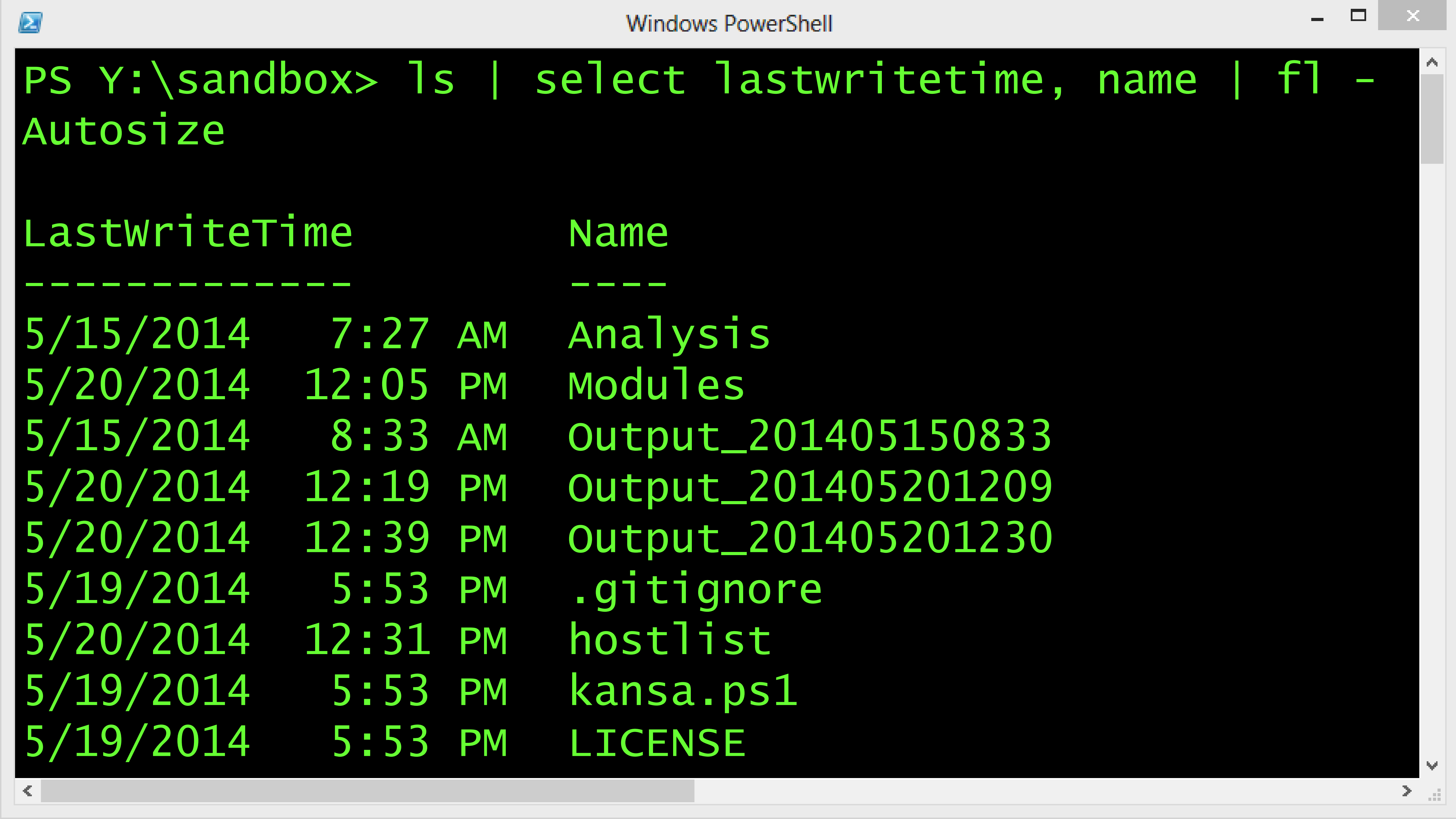
```
Get-CommunityInput

github.com/davehull/Kansa
```



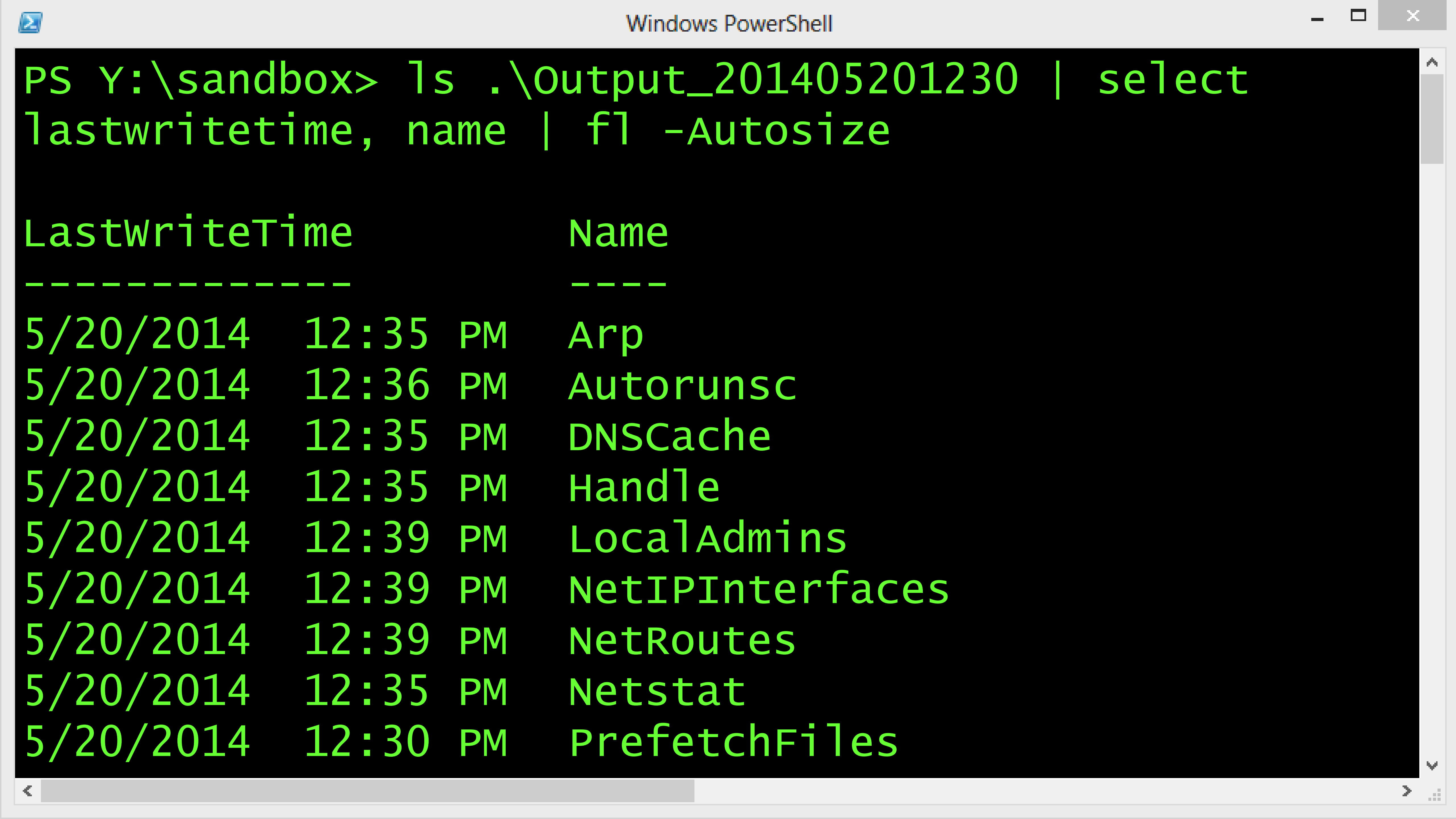
```
            Get-AudienceQuestions

                Thank you!

    Email   : davehull@trustedsignal.com
    Twitter : @davehull
```



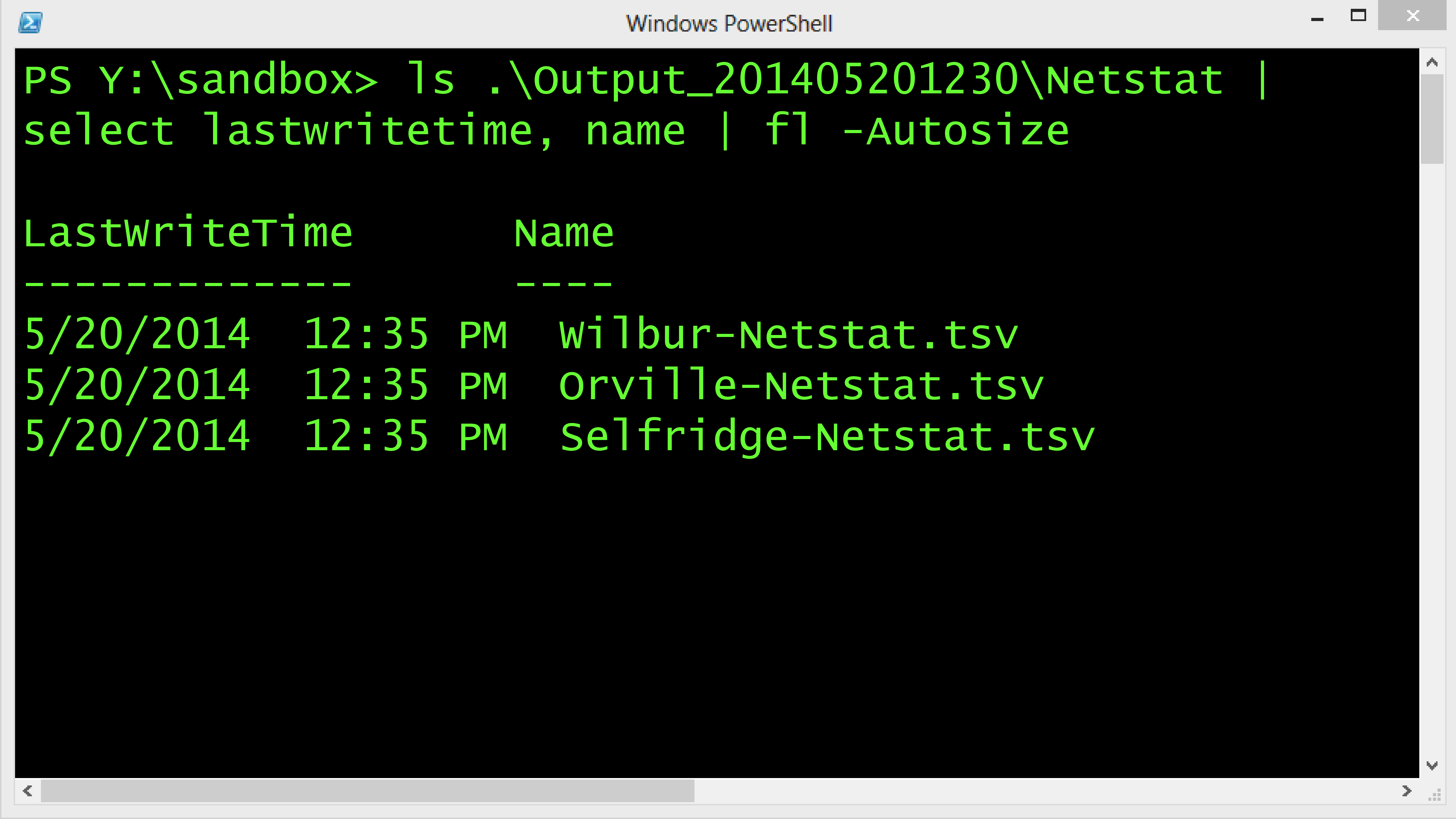
```
PS Y:\sandbox> .\kansa.ps1 -TargetList .\hostlist -Pushbin -Verbose
VERBOSE: Found Modules\Modules.conf.
VERBOSE: Running modules: Get-PrefetchListing Get-PrefetchFiles Get-Netstat Get-DNSCache Get-Arp Get-Prox Get-Tasklistv Get-
Tasklistm Get-Handle Get-SvcAll Get-SvcFail Get-SvcTrigs Get-WMIEvtFilter Get-WMIFltConBind Get-WMIEvtConsumer Get-Autorunsc
Get-ProcsWMI Get-ProcDump Get-NetRoutes Get-NetIPInterfaces Get-LocalAdmins Get-PSProfiles
VERBOSE: $Targets are Wilbur Orville Selfridge.
VERBOSE: Get-Handle has dependency on Handle.exe.
VERBOSE: Attempting to copy Handle.exe to targets...
VERBOSE: Get-Autorunsc has dependency on Autorunsc.exe.
VERBOSE: Attempting to copy Autorunsc.exe to targets...
VERBOSE: Waiting for Get-PrefetchListing to complete.
Id     Name            PSJobTypeName   State         HasMoreData     Location             Command
--     ----            -------------   -----         -----------     --------             -------
2      Job2            RemoteJob       Completed     True            Wilbur,Orville,... # OUTPUT tsv...
VERBOSE: Waiting for Get-PrefetchFiles to complete.
6      Job6            RemoteJob       Completed     True            Wilbur,Orville,... # OUTPUT zip...
VERBOSE: Waiting for Get-Netstat to complete.
10     Job10           RemoteJob       Completed     True            Wilbur,Orville,... # OUTPUT tsv...
VERBOSE: Waiting for Get-DNSCache to complete.
14     Job14           RemoteJob       Completed     True            Wilbur,Orville,... # OUTPUT tsv...
VERBOSE: Waiting for Get-Arp to complete.
18     Job18           RemoteJob       Completed     True            Wilbur,Orville,... # OUTPUT tsv...
VERBOSE: Waiting for Get-Prox to complete.
22     Job22           RemoteJob       Completed     True            Wilbur,Orville,... # OUTPUT xml...
VERBOSE: Waiting for Get-Tasklistv to complete.
26     Job26           RemoteJob       Completed     True            Wilbur,Orville,... # OUTPUT tsv...
VERBOSE: Waiting for Get-Tasklistm to complete.
30     Job30           RemoteJob       Completed     True            Wilbur,Orville,... # OUTPUT tsv...
VERBOSE: Waiting for Get-Handle to complete.
34     Job34           RemoteJob       Completed     True            Wilbur,Orville,... # OUTPUT tsv...
VERBOSE: Waiting for Get-SvcAll to complete.
38     Job38           RemoteJob       Completed     True            Wilbur,Orville,... # OUTPUT tsv...
VERBOSE: Waiting for Get-SvcFail to complete.
```



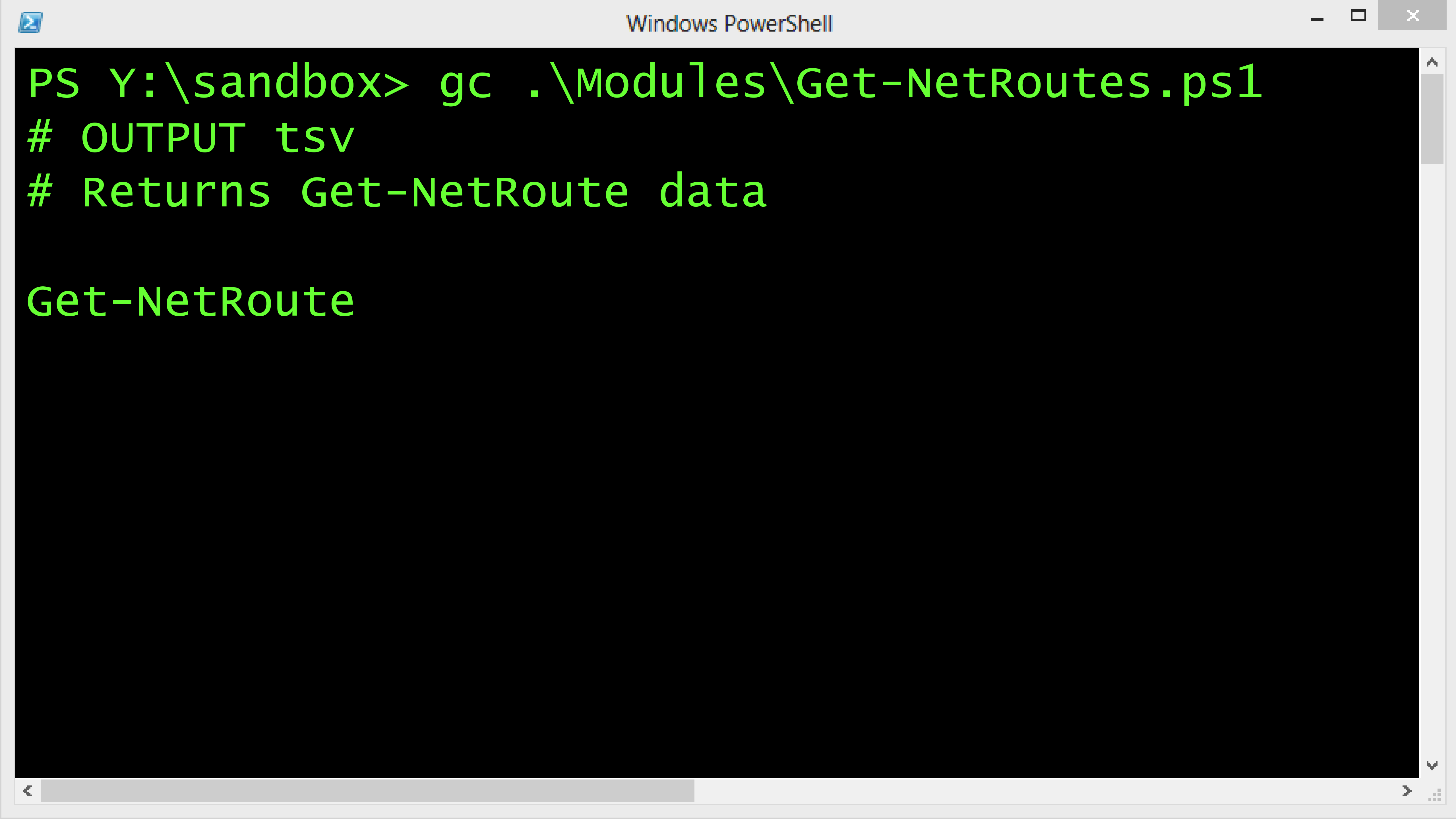
```
PS Y:\sandbox> ls | select lastwritetime, name | fl -
Autosize


LastWriteTime           Name
-------------           ----
5/15/2014   7:27 AM    Analysis
5/20/2014  12:05 PM    Modules
5/15/2014   8:33 AM    Output_201405150833
5/20/2014  12:19 PM    Output_201405201209
5/20/2014  12:39 PM    Output_201405201230
5/19/2014   5:53 PM    .gitignore
5/20/2014  12:31 PM    hostlist
5/19/2014   5:53 PM    kansa.ps1
5/19/2014   5:53 PM    LICENSE
```



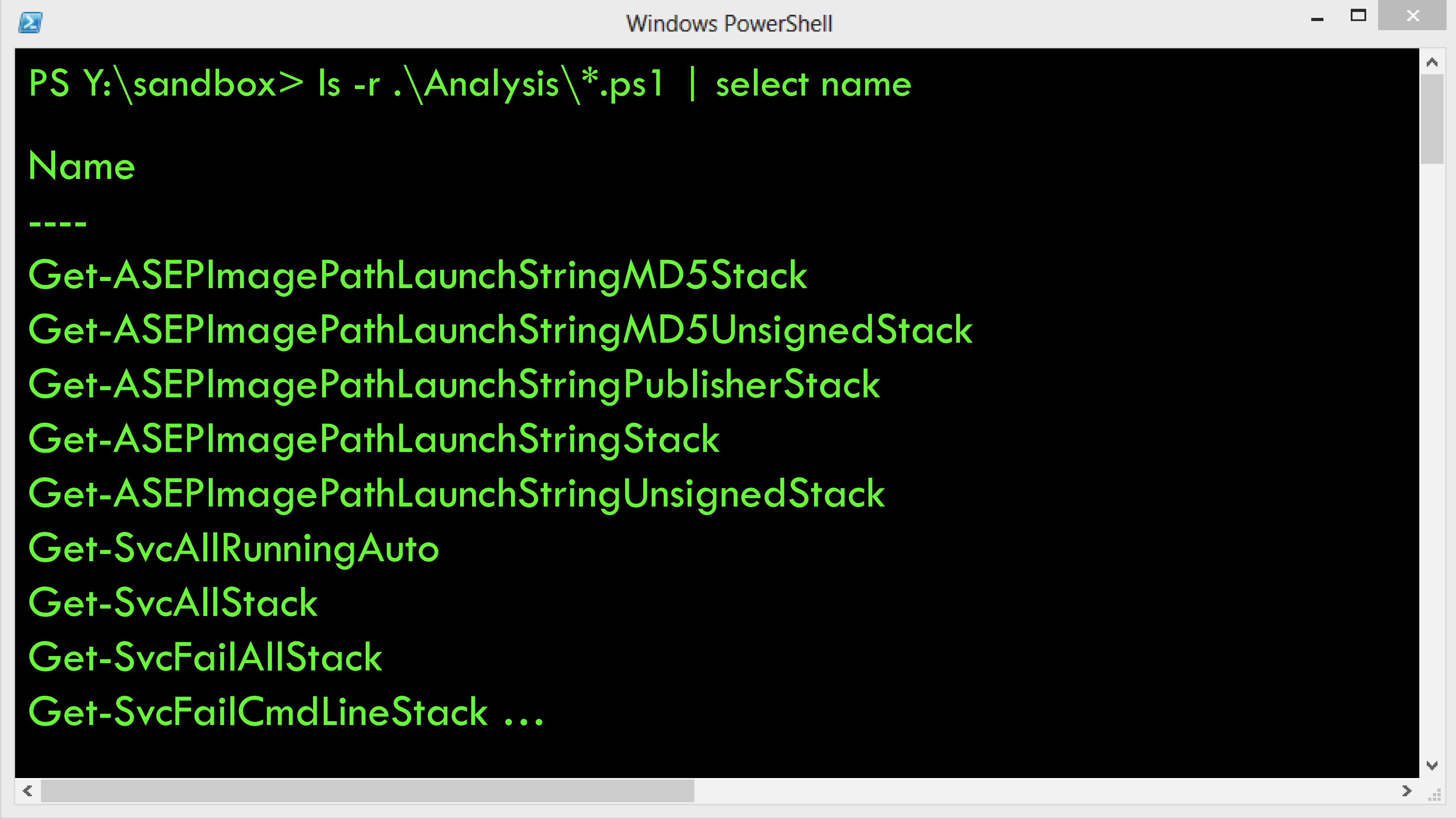
```
PS Y:\sandbox> ls .\Output_201405201230 | select
lastwritetime, name | fl -Autosize

LastWriteTime          Name
-------------          ----
5/20/2014  12:35 PM    Arp
5/20/2014  12:36 PM    Autorunsc
5/20/2014  12:35 PM    DNSCache
5/20/2014  12:35 PM    Handle
5/20/2014  12:39 PM    LocalAdmins
5/20/2014  12:39 PM    NetIPInterfaces
5/20/2014  12:39 PM    NetRoutes
5/20/2014  12:35 PM    Netstat
5/20/2014  12:30 PM    PrefetchFiles
```



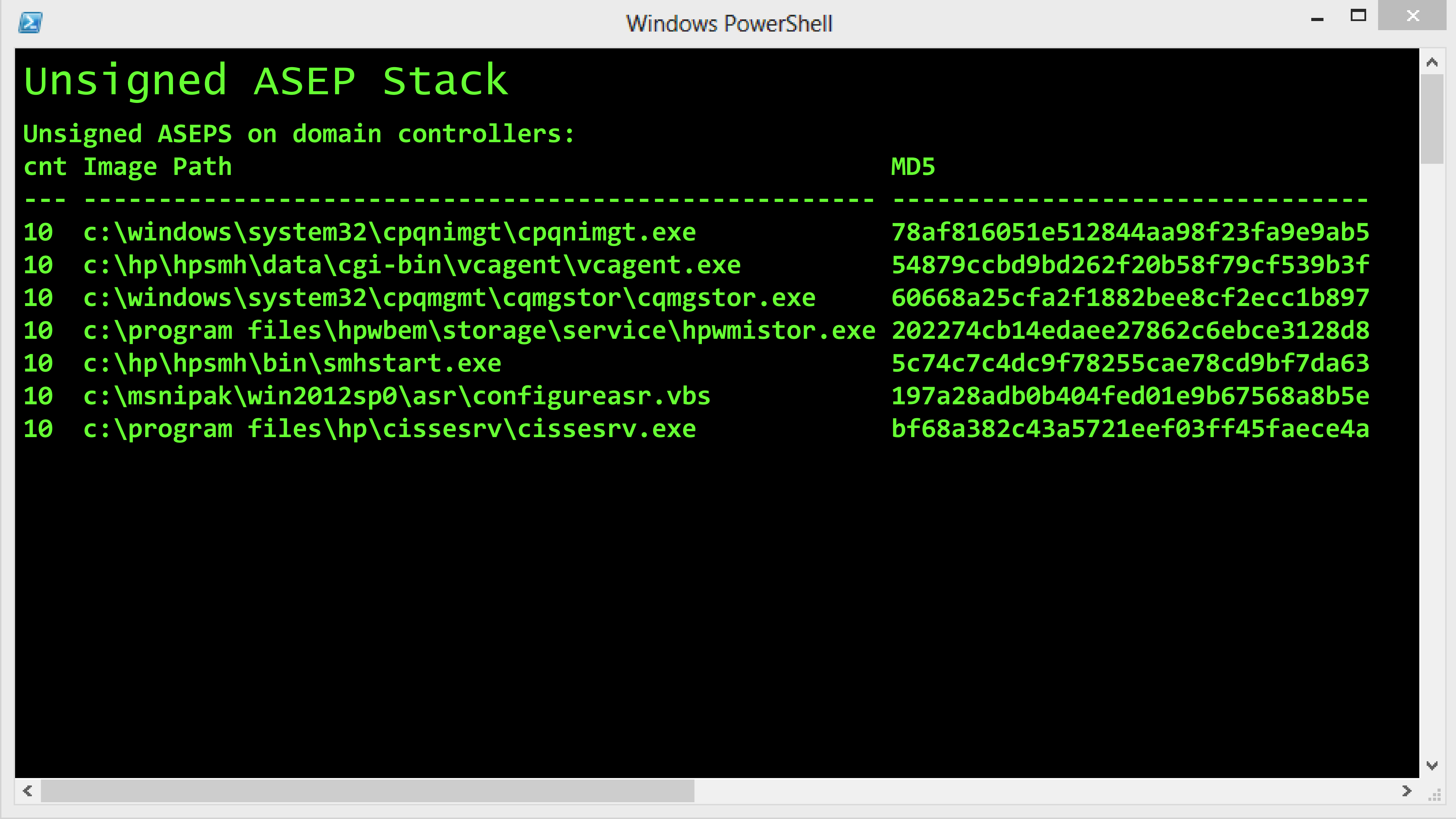
```
PS Y:\sandbox> ls .\Output_201405201230\Netstat |
select lastwritetime, name | fl -Autosize

LastWriteTime         Name
-------------         ----
5/20/2014  12:35 PM  Wilbur-Netstat.tsv
5/20/2014  12:35 PM  Orville-Netstat.tsv
5/20/2014  12:35 PM  Selfridge-Netstat.tsv
```



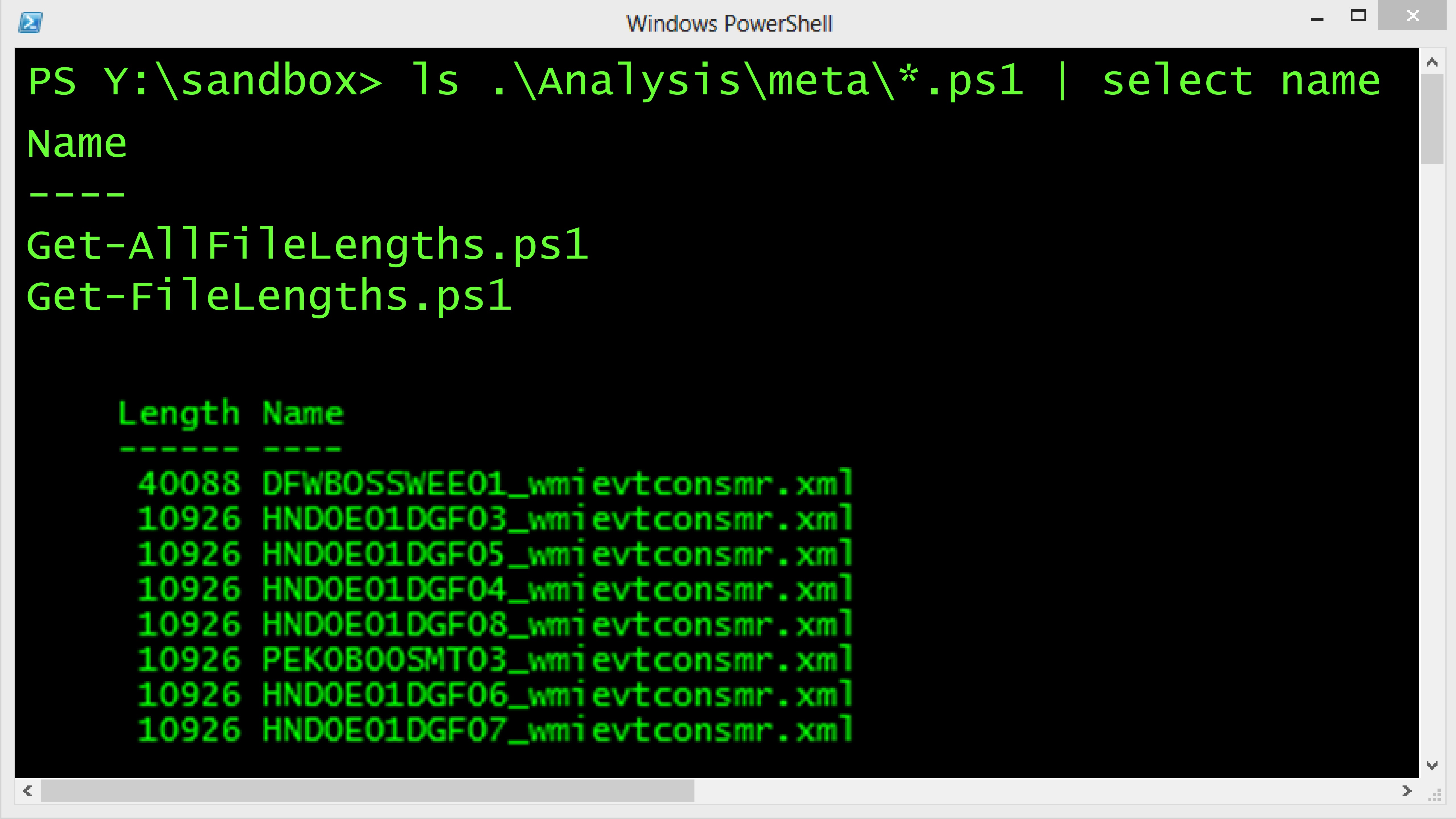
```
PS Y:\sandbox> gc .\Modules\Get-NetRoutes.ps1
# OUTPUT tsv
# Returns Get-NetRoute data

Get-NetRoute
```



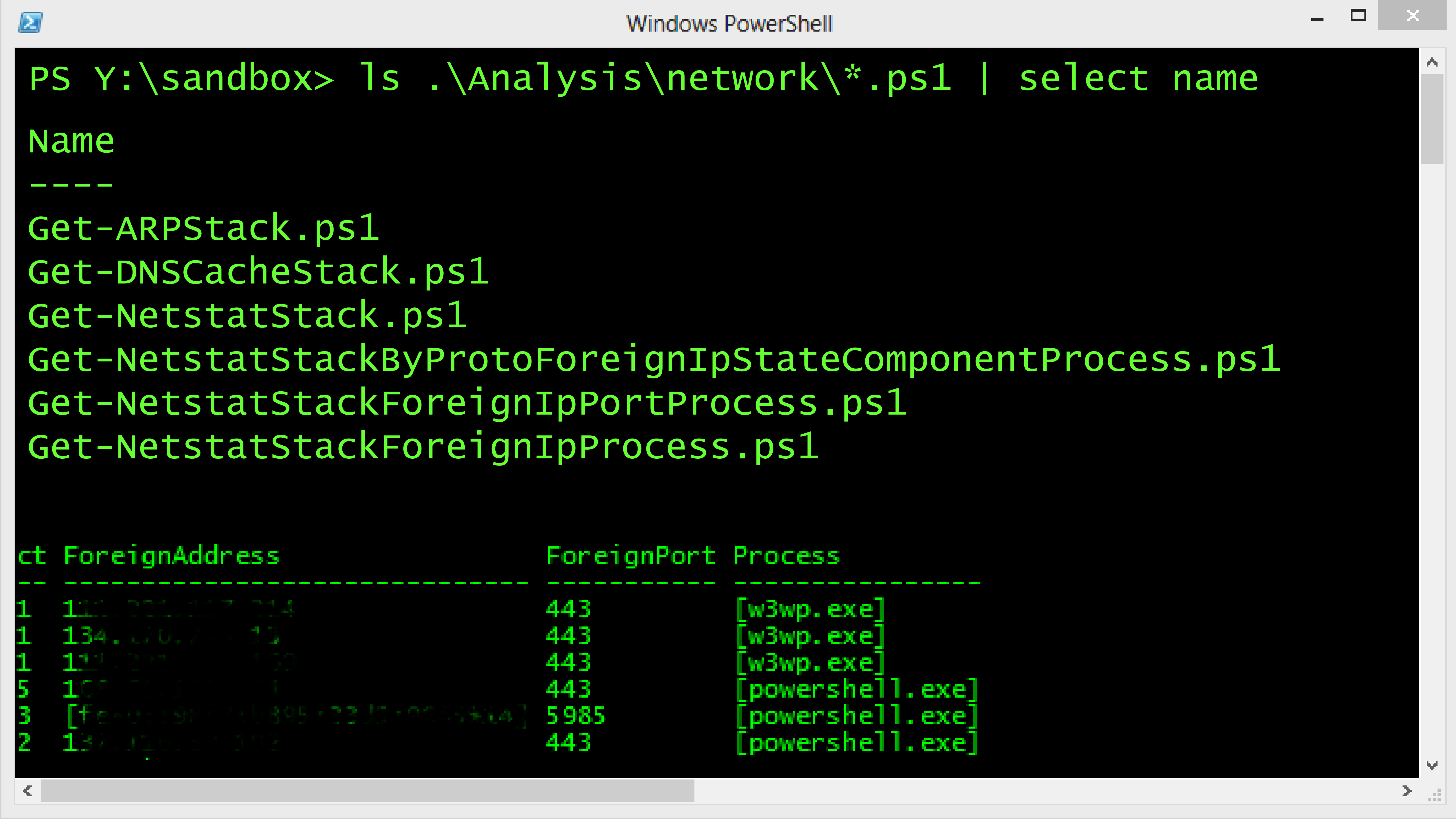
```
PS Y:\sandbox> ls -r .\Analysis\*.ps1 | select name

Name
----
Get-ASEPImagePathLaunchStringMD5Stack
Get-ASEPImagePathLaunchStringMD5UnsignedStack
Get-ASEPImagePathLaunchStringPublisherStack
Get-ASEPImagePathLaunchStringStack
Get-ASEPImagePathLaunchStringUnsignedStack
Get-SvcAllRunningAuto
Get-SvcAllStack
Get-SvcFailAllStack
Get-SvcFailCmdLineStack ...
```



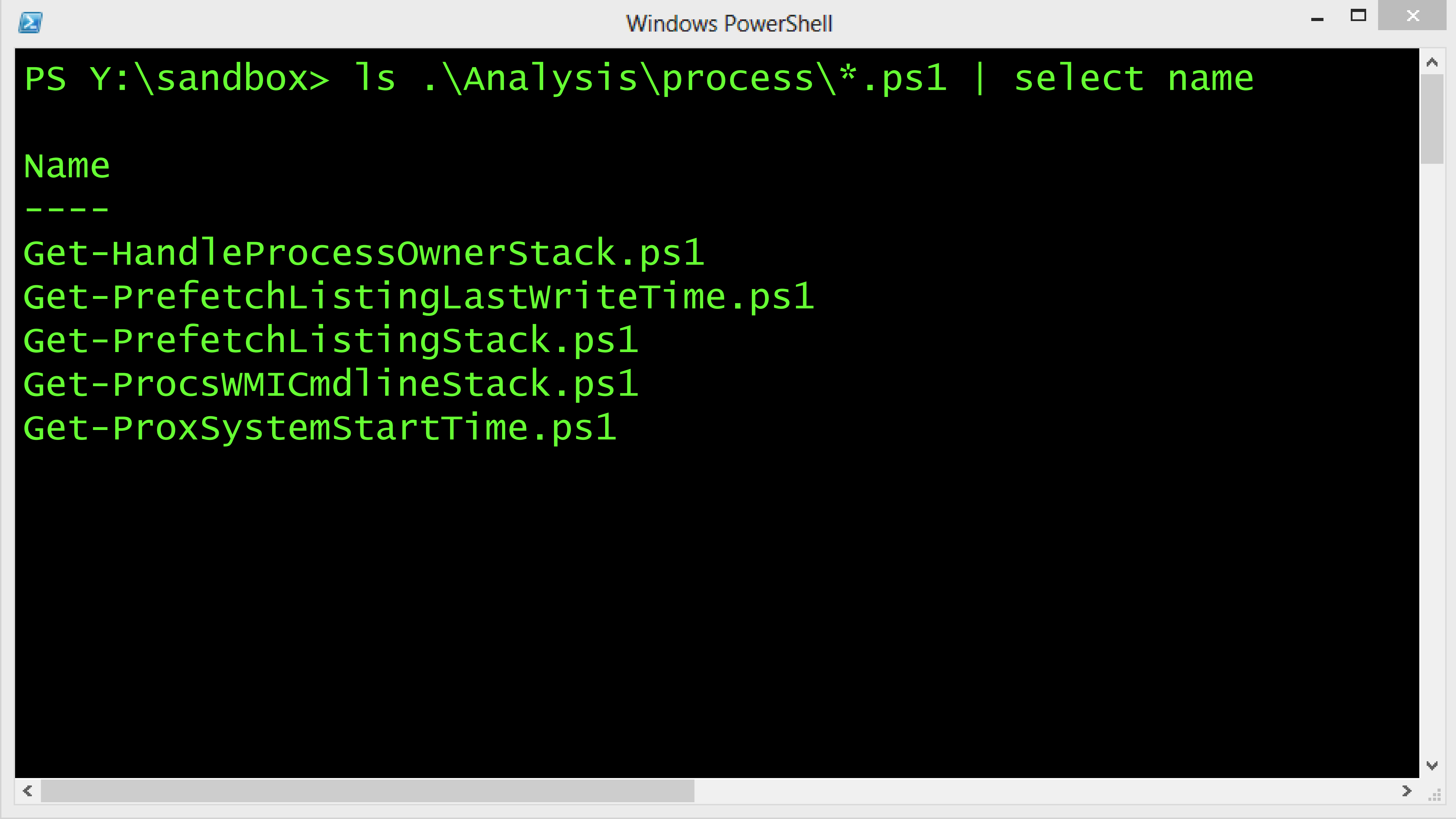
```
Unsigned ASEP Stack

Unsigned ASEPS on domain controllers:
cnt Image Path                                            MD5
--- ----------------------------------------------------- --------------------------------
10  c:\windows\system32\cpqnimgt\cpqnimgt.exe             78af816051e512844aa98f23fa9e9ab5
10  c:\hp\hpsmh\data\cgi-bin\vcagent\vcagent.exe          54879ccbd9bd262f20b58f79cf539b3f
10  c:\windows\system32\cpqmgmt\cqmgstor\cqmgstor.exe     60668a25cfa2f1882bee8cf2ecc1b897
10  c:\program files\hpwbem\storage\service\hpwmistor.exe 202274cb14edaee27862c6ebce3128d8
10  c:\hp\hpsmh\bin\smhstart.exe                          5c74c7c4dc9f78255cae78cd9bf7da63
10  c:\msnipak\win2012sp0\asr\configureasr.vbs            197a28adb0b404fed01e9b67568a8b5e
10  c:\program files\hp\cissesrv\cissesrv.exe             bf68a382c43a5721eef03ff45faece4a
```



```
PS Y:\sandbox> ls .\Analysis\meta\*.ps1 | select name

Name
----
Get-AllFileLengths.ps1
Get-FileLengths.ps1


   Length Name
   ------ ----
    40088 DFWBOSSWEE01_wmievtconsmr.xml
    10926 HNDOE01DGF03_wmievtconsmr.xml
    10926 HNDOE01DGF05_wmievtconsmr.xml
    10926 HNDOE01DGF04_wmievtconsmr.xml
    10926 HNDOE01DGF08_wmievtconsmr.xml
    10926 PEKOBOOSMT03_wmievtconsmr.xml
    10926 HNDOE01DGF06_wmievtconsmr.xml
    10926 HNDOE01DGF07_wmievtconsmr.xml
```



```
PS Y:\sandbox> ls .\Analysis\network\*.ps1 | select name

Name
----
Get-ARPStack.ps1
Get-DNSCacheStack.ps1
Get-NetstatStack.ps1
Get-NetstatStackByProtoForeignIpStateComponentProcess.ps1
Get-NetstatStackForeignIpPortProcess.ps1
Get-NetstatStackForeignIpProcess.ps1


ct ForeignAddress                    ForeignPort Process
-- --------------------------------- ----------- ----------------
1  [redacted]                        443         [w3wp.exe]
1  [redacted]                        443         [w3wp.exe]
1  [redacted]                        443         [w3wp.exe]
5  [redacted]                        443         [powershell.exe]
3  [redacted]                        5985        [powershell.exe]
2  [redacted]                        443         [powershell.exe]
```



```
PS Y:\sandbox> ls .\Analysis\process\*.ps1 | select name

Name
----
Get-HandleProcessOwnerStack.ps1
Get-PrefetchListingLastWriteTime.ps1
Get-PrefetchListingStack.ps1
Get-ProcsWMICmdlineStack.ps1
Get-ProxSystemStartTime.ps1
```