禪

[illegible]

[illegible]

[illegible]

1- [illegible] PowerShell

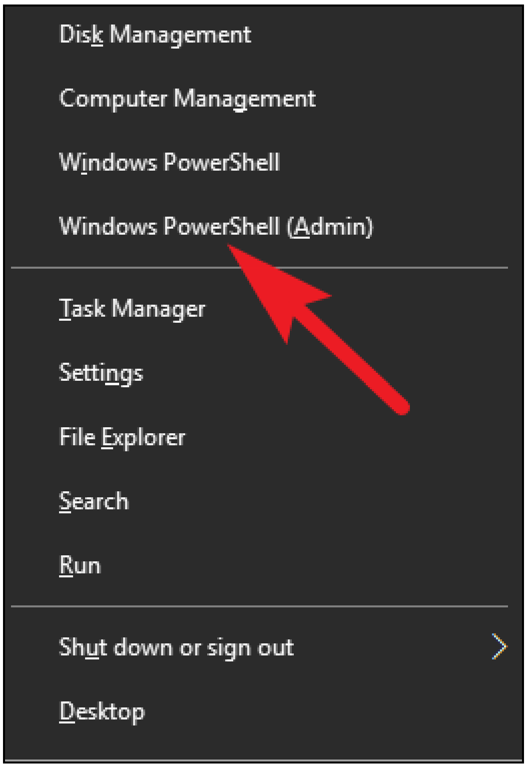
[illegible] netstat [illegible] XP [illegible] Service Pack 2 [illegible] 10 [illegible].

[illegible] administrator [illegible] Windows+X [illegible] PowerShell [illegible] Power User [illegible] "PowerShell (Admin)" [illegible] Command Prompt [illegible] administrator [illegible].

[illegible]

[illegible]

[illegible]

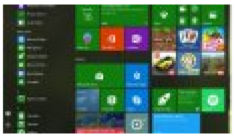


[illegible]:

```
netstat -abf 5 > activity.txt
```

[illegible] -a [illegible] -b [illegible] -f [illegible] DNS [illegible] 5 [illegible] 5 [illegible] ">" [illegible] "activity.txt" [illegible].

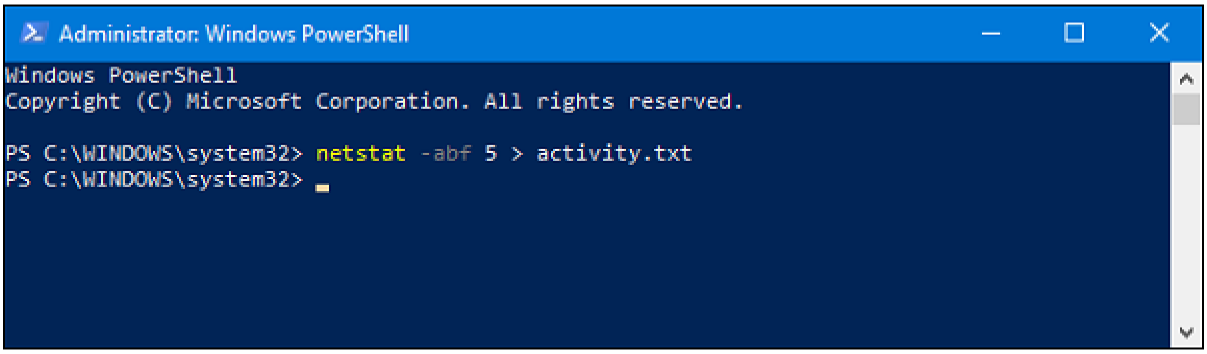
[illegible]



[illegible]

[illegible] 10 [illegible]

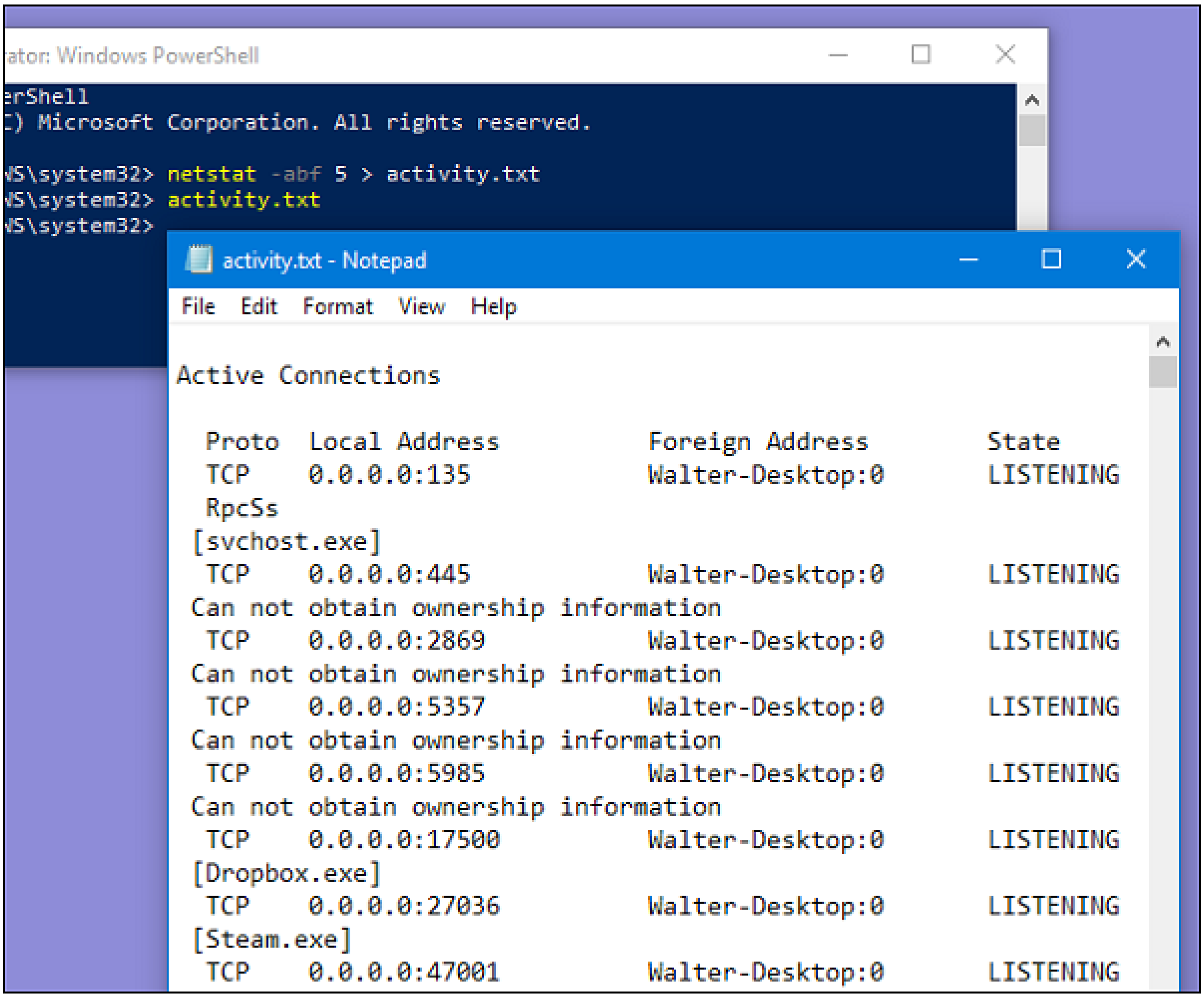
[illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] Ctrl+C [illegible] [illegible] [illegible] [illegible] [illegible] [illegible].



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\WINDOWS\system32> netstat -abf 5 > activity.txt
PS C:\WINDOWS\system32> _
```

[illegible] [illegible] [illegible] [illegible] "activity.txt" [illegible] [illegible] [illegible]. [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] PowerShell [illegible] [illegible].



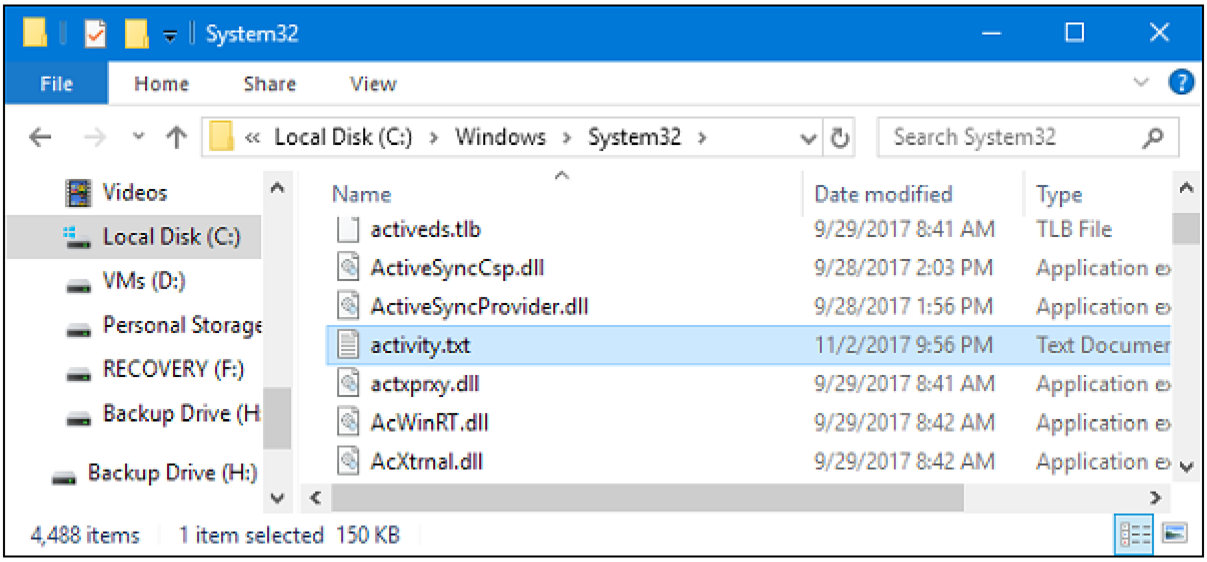
```
erShell
C) Microsoft Corporation. All rights reserved.

WS\system32> netstat -abf 5 > activity.txt
WS\system32> activity.txt
WS\system32>
```

```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            Walter-Desktop:0       LISTENING
  RpcSs
 [svchost.exe]
  TCP    0.0.0.0:445            Walter-Desktop:0       LISTENING
 Can not obtain ownership information
  TCP    0.0.0.0:2869           Walter-Desktop:0       LISTENING
 Can not obtain ownership information
  TCP    0.0.0.0:5357           Walter-Desktop:0       LISTENING
 Can not obtain ownership information
  TCP    0.0.0.0:5985           Walter-Desktop:0       LISTENING
 Can not obtain ownership information
  TCP    0.0.0.0:17500          Walter-Desktop:0       LISTENING
 [Dropbox.exe]
  TCP    0.0.0.0:27036          Walter-Desktop:0       LISTENING
 [Steam.exe]
  TCP    0.0.0.0:47001          Walter-Desktop:0       LISTENING
```

[illegible] [illegible] [illegible] [illegible] \Windows\System32 [illegible] [illegible].



System32

File Home Share View

« Local Disk (C:) › Windows › System32 ›

Search System32

Name	Date modified	Type
activeds.tlb	9/29/2017 8:41 AM	TLB File
ActiveSyncCsp.dll	9/28/2017 2:03 PM	Application e
ActiveSyncProvider.dll	9/28/2017 1:56 PM	Application e
activity.txt	11/2/2017 9:56 PM	Text Documer
actxprxy.dll	9/29/2017 8:41 AM	Application e
AcWinRT.dll	9/29/2017 8:42 AM	Application e
AcXtmal.dll	9/29/2017 8:42 AM	Application e

4,488 items 1 item selected 150 KB

[illegible]

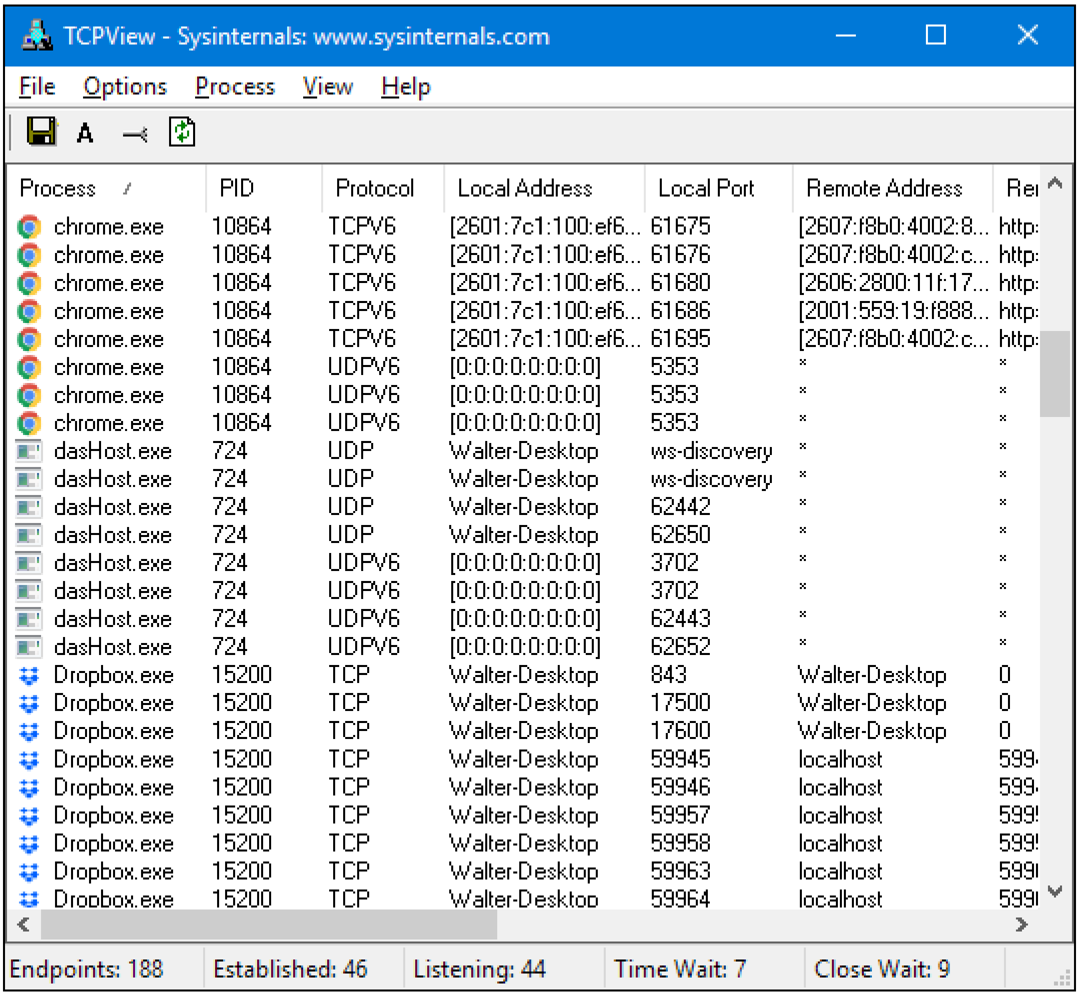
[illegible] "what is" [illegible]

[illegible]

[illegible]

[illegible] 10 [illegible]

[illegible] TCPView


TCPView - Sysinternals: www.sysinternals.com
File Options Process View Help

Process	PID	Protocol	Local Address	Local Port	Remote Address	Rei
chrome.exe	10864	TCPV6	[2601:7c1:100:ef6...	61675	[2607:f8b0:4002:8...	http:
chrome.exe	10864	TCPV6	[2601:7c1:100:ef6...	61676	[2607:f8b0:4002:c...	http:
chrome.exe	10864	TCPV6	[2601:7c1:100:ef6...	61680	[2606:2800:11f:17...	http:
chrome.exe	10864	TCPV6	[2601:7c1:100:ef6...	61686	[2001:559:19:f888...	http:
chrome.exe	10864	TCPV6	[2601:7c1:100:ef6...	61695	[2607:f8b0:4002:c...	http:
chrome.exe	10864	UDPV6	[0:0:0:0:0:0:0:0]	5353	*	*
chrome.exe	10864	UDPV6	[0:0:0:0:0:0:0:0]	5353	*	*
chrome.exe	10864	UDPV6	[0:0:0:0:0:0:0:0]	5353	*	*
dasHost.exe	724	UDP	Walter-Desktop	ws-discovery	*	*
dasHost.exe	724	UDP	Walter-Desktop	ws-discovery	*	*
dasHost.exe	724	UDP	Walter-Desktop	62442	*	*
dasHost.exe	724	UDP	Walter-Desktop	62650	*	*
dasHost.exe	724	UDPV6	[0:0:0:0:0:0:0:0]	3702	*	*
dasHost.exe	724	UDPV6	[0:0:0:0:0:0:0:0]	3702	*	*
dasHost.exe	724	UDPV6	[0:0:0:0:0:0:0:0]	62443	*	*
dasHost.exe	724	UDPV6	[0:0:0:0:0:0:0:0]	62652	*	*
Dropbox.exe	15200	TCP	Walter-Desktop	843	Walter-Desktop	0
Dropbox.exe	15200	TCP	Walter-Desktop	17500	Walter-Desktop	0
Dropbox.exe	15200	TCP	Walter-Desktop	17600	Walter-Desktop	0
Dropbox.exe	15200	TCP	Walter-Desktop	59945	localhost	599
Dropbox.exe	15200	TCP	Walter-Desktop	59946	localhost	599
Dropbox.exe	15200	TCP	Walter-Desktop	59957	localhost	599
Dropbox.exe	15200	TCP	Walter-Desktop	59958	localhost	599
Dropbox.exe	15200	TCP	Walter-Desktop	59963	localhost	599
Dropbox.exe	15200	TCP	Walter-Desktop	59964	localhost	599

Endpoints: 188 | Established: 46 | Listening: 44 | Time Wait: 7 | Close Wait: 9

[illegible] TCPView [illegible]. [illegible] Whois [illegible].

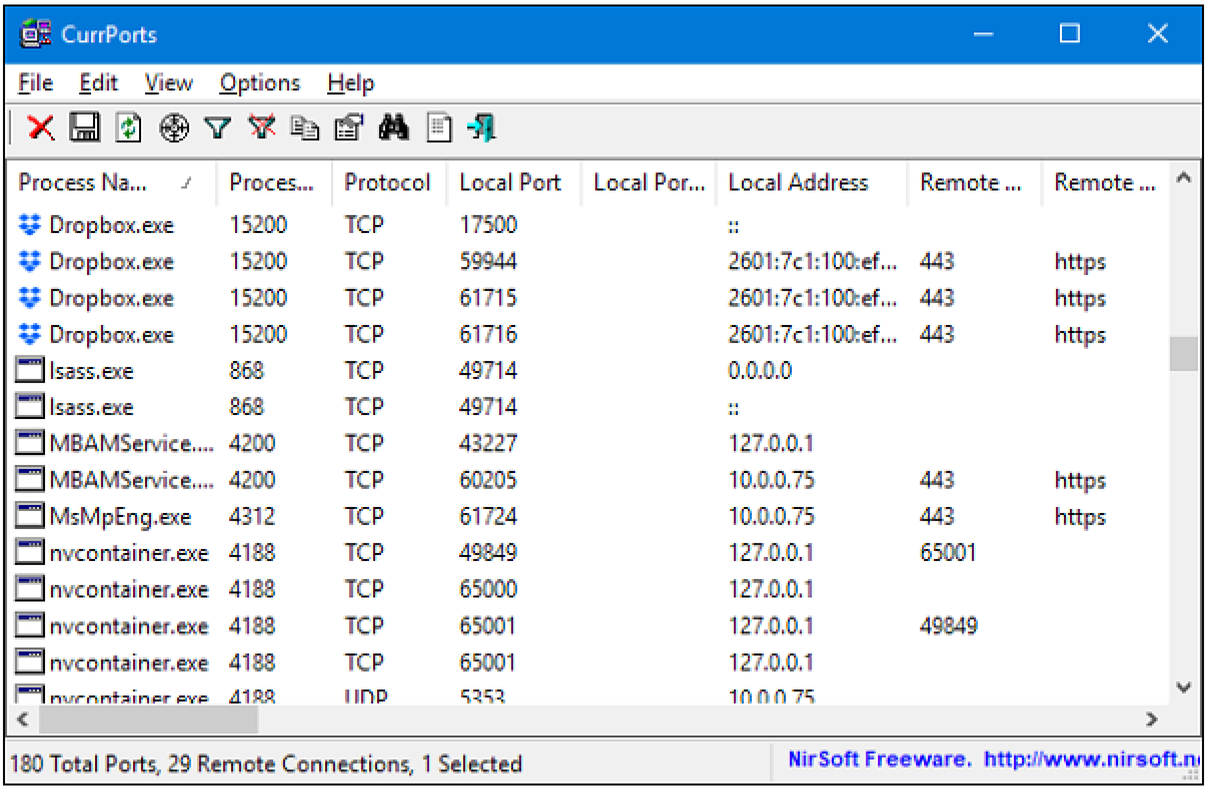
[illegible]. [illegible]. [illegible] TIME_WAIT [illegible].

[illegible]

[illegible] 10 [illegible]

[illegible] 10 [illegible]

[illegible]: [illegible] CurrPorts



Process Na...	Proces...	Protocol	Local Port	Local Por...	Local Address	Remote ...	Remote ...
Dropbox.exe	15200	TCP	17500		::		
Dropbox.exe	15200	TCP	59944		2601:7c1:100:ef...	443	https
Dropbox.exe	15200	TCP	61715		2601:7c1:100:ef...	443	https
Dropbox.exe	15200	TCP	61716		2601:7c1:100:ef...	443	https
lsass.exe	868	TCP	49714		0.0.0.0		
lsass.exe	868	TCP	49714		::		
MBAMService....	4200	TCP	43227		127.0.0.1		
MBAMService....	4200	TCP	60205		10.0.0.75	443	https
MsMpEng.exe	4312	TCP	61724		10.0.0.75	443	https
nvcontainer.exe	4188	TCP	49849		127.0.0.1	65001	
nvcontainer.exe	4188	TCP	65000		127.0.0.1		
nvcontainer.exe	4188	TCP	65001		127.0.0.1	49849	
nvcontainer.exe	4188	TCP	65001		127.0.0.1		
nvcontainer.exe	4188	UDP	5353		10.0.0.75		

180 Total Ports, 29 Remote Connections, 1 Selected

[illegible] [illegible] CurrPorts [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] UDP [illegible] TCP/IP [illegible] [illegible] [illegible]
[illegible] [illegible].

[illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible]. [illegible].

[illegible] CurrPorts [illegible] [illegible] [illegible] [illegible] [illegible] NT [illegible] [illegible] 10 [illegible]. [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] [illegible] 64 [illegible] [illegible] [illegible].

[illegible]:
[illegible] [illegible]
[illegible]:
howtogeek
[illegible] [illegible]:
[illegible]
[illegible] [illegible]:
10:40 - 22/08/1396
[illegible]:
[illegible] [illegible] - [illegible] [illegible] - [illegible] [illegible] - [illegible] - [illegible] [illegible] - [illegible] [illegible]

[illegible]
[illegible]: https://www.shabakeh-mag.com/workshop/10621/%DA%86%DA%AF%D9%88%D9%86%D9%87-%D8%A7%D8%AA%D8%B5%D8%A7%D9%84-%D9%85%D8%AE%D9%81%DB%8C%D8%A7%D9%86%D9%87-%DA%A9%D8%A7%D9%85%D9%BE%DB%8C%D9%88%D8%AA%D8%B1-%D8%A8%D9%87-%D9%88%D8%A8%D8%B3%D8%A7%DB%8C%D8%AA%E2%80%8C%D9%87%D8%A7%DB%8C-%D9%85%D8%AE%D8%AA%D9%84%D9%81-%D8%B1%D8%A7-%D9%BE%DB%8C%D8%AF%D8%A7-%DA%A9%D9%86%DB%8C%D9%85%D8%9F