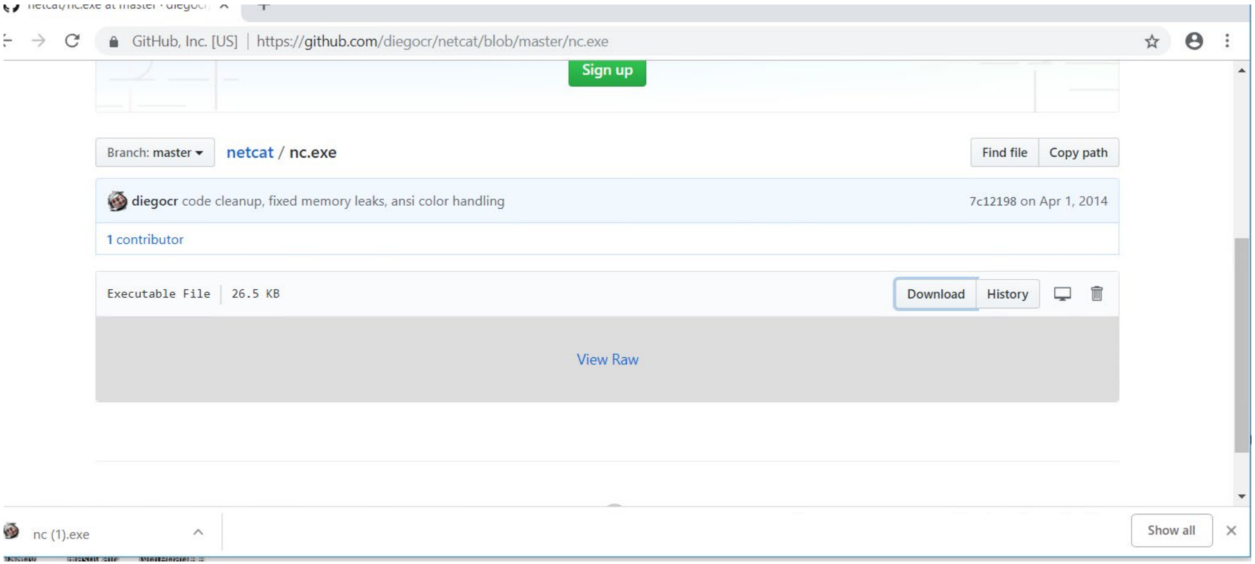
Kiauna Newman ISyS-470 September 30, 2018

Course Textbook Exercise 5.1 Finding Malicious Programs


netcat/nc.exe at master · diegocr/

GitHub, Inc. [US] | https://github.com/diegocr/netcat/blob/master/nc.exe

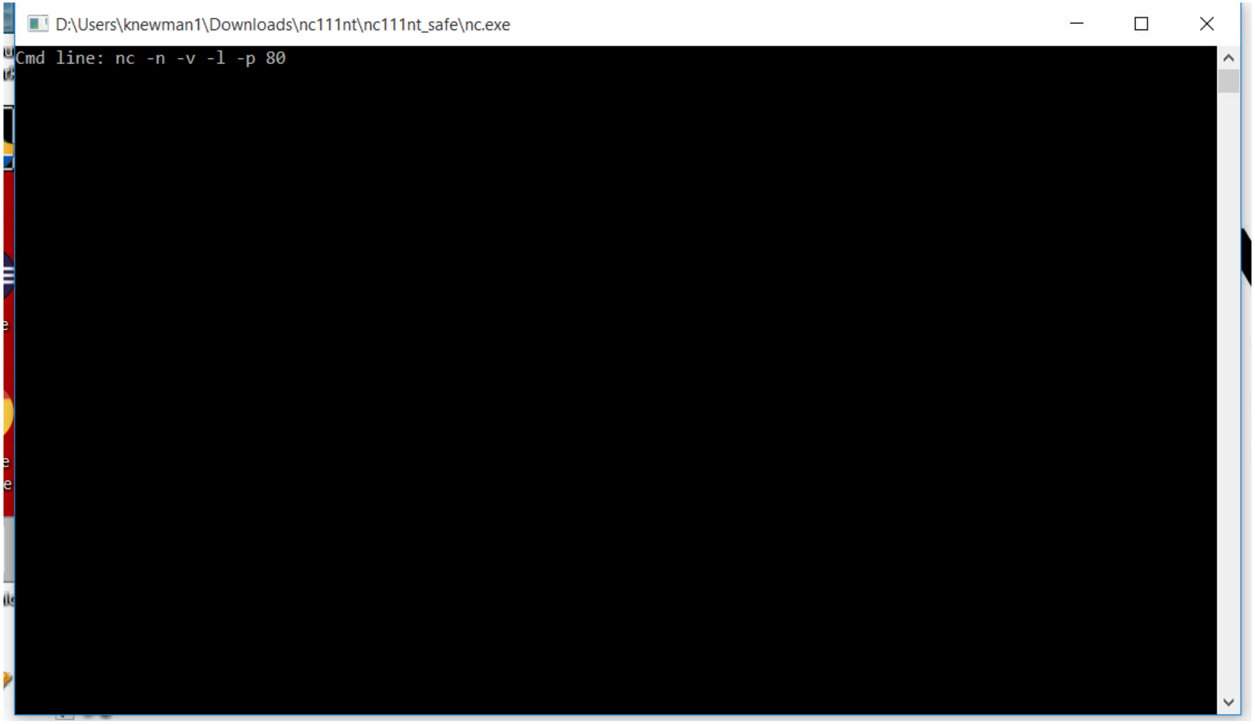
Branch: master ▾ netcat / nc.exe

diegocr code cleanup, fixed memory leaks, ansi color handling 7c12198 on Apr 1, 2014

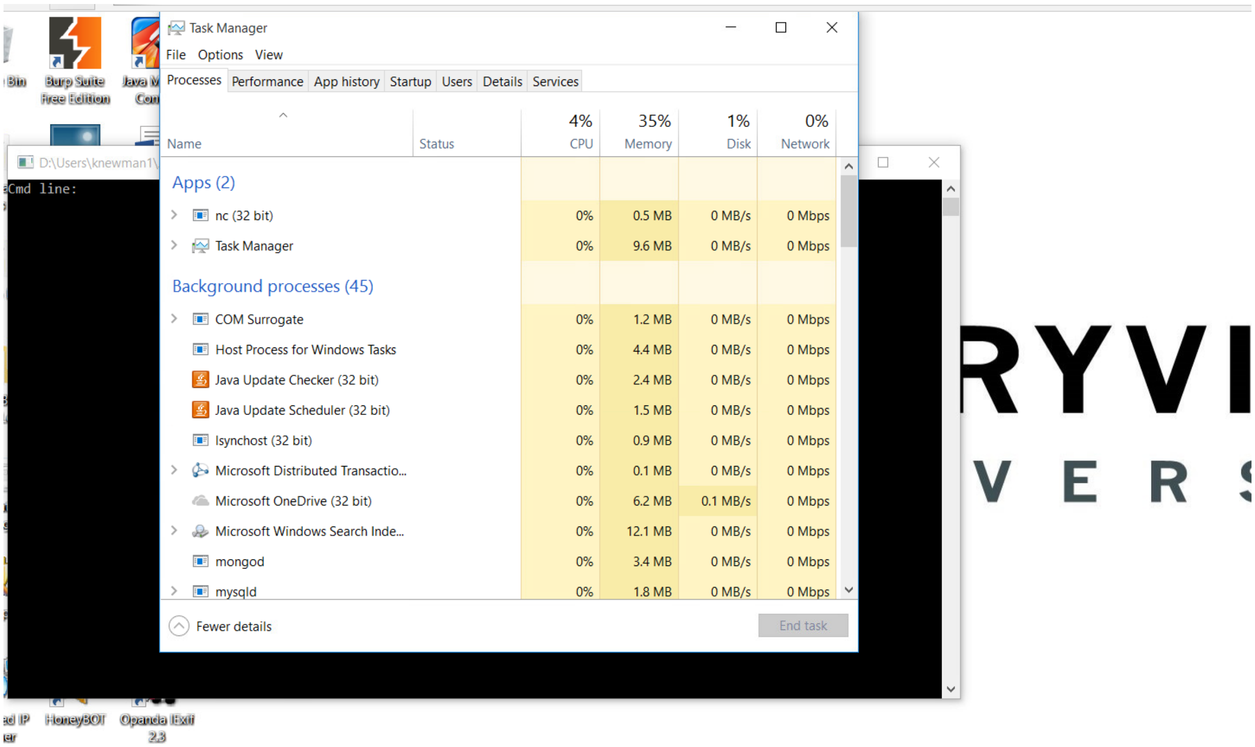
1 contributor

Executable File | 26.5 KB

nc (1).exe

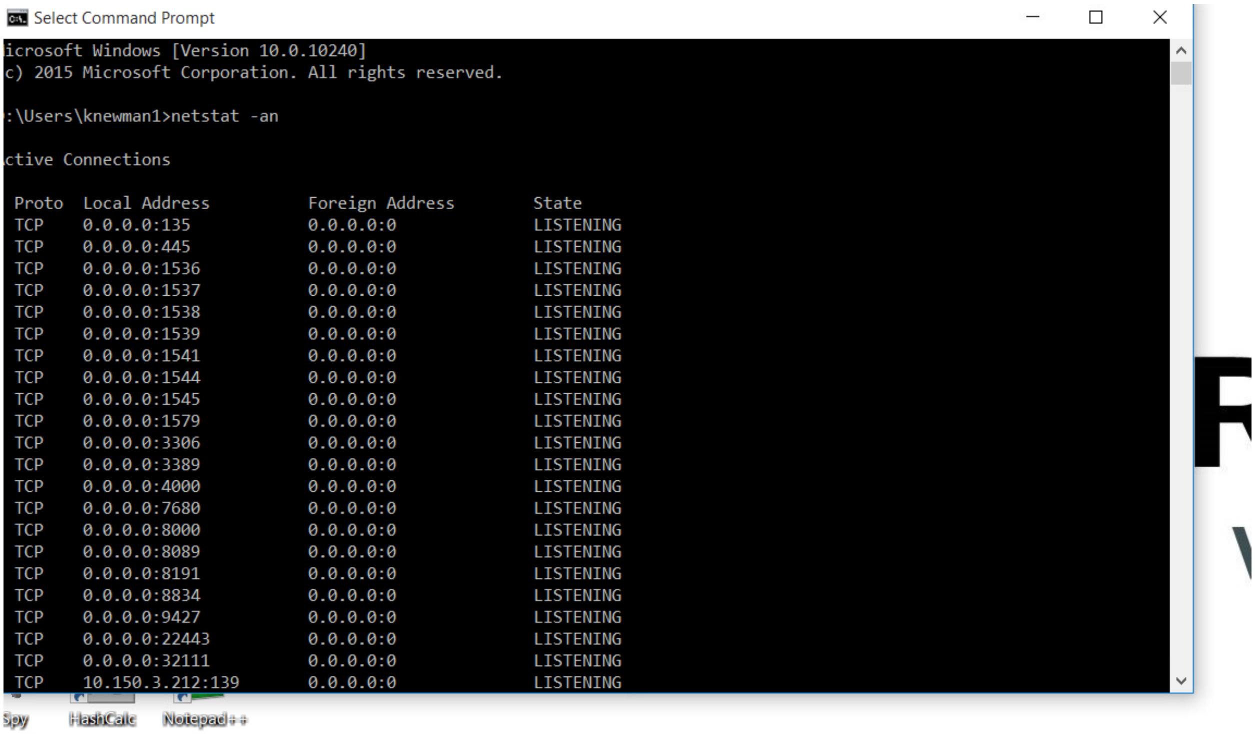

D:\Users\knewman1\Downloads\nc111nt\nc111nt_safe\nc.exe

```
Cmd line: nc -n -v -l -p 80
```

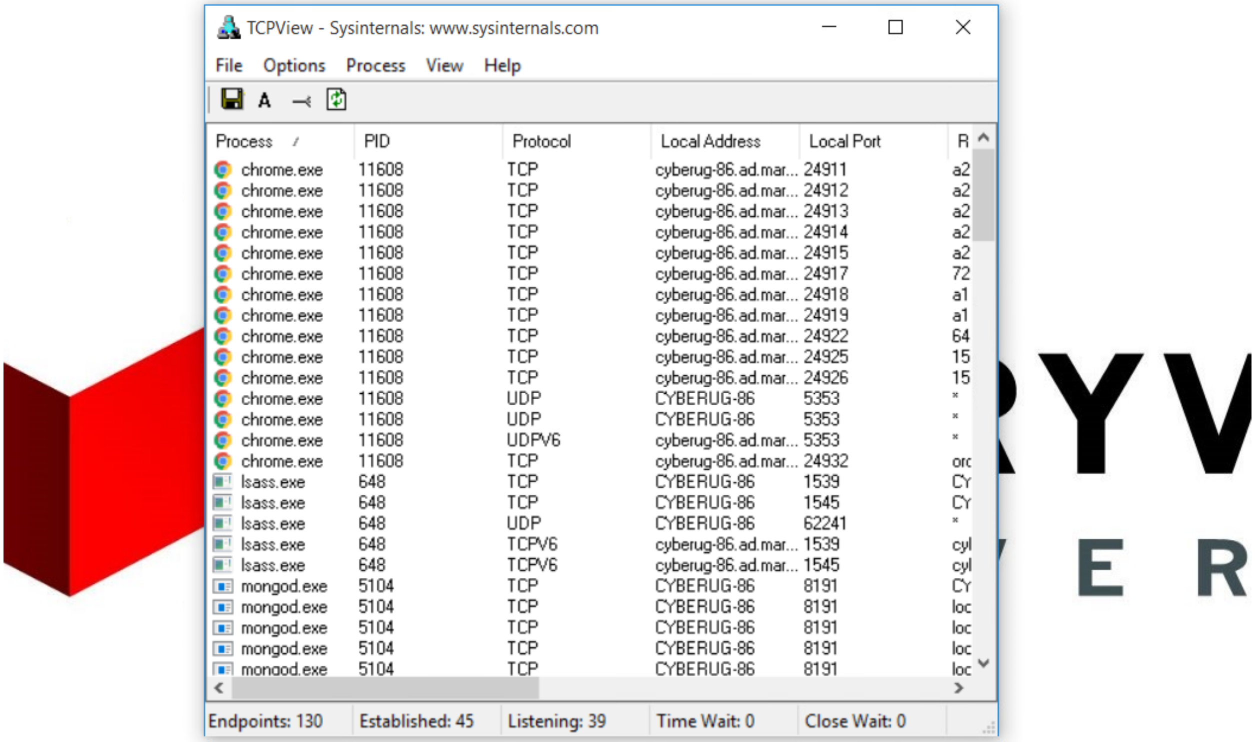


```
Cmd line:
```

Name	Status	4% CPU	35% Memory	1% Disk	0% Network
Apps (2)					
nc (32 bit)		0%	0.5 MB	0 MB/s	0 Mbps
Task Manager		0%	9.6 MB	0 MB/s	0 Mbps
Background processes (45)					
COM Surrogate		0%	1.2 MB	0 MB/s	0 Mbps
Host Process for Windows Tasks		0%	4.4 MB	0 MB/s	0 Mbps
Java Update Checker (32 bit)		0%	2.4 MB	0 MB/s	0 Mbps
Java Update Scheduler (32 bit)		0%	1.5 MB	0 MB/s	0 Mbps
Isynchost (32 bit)		0%	0.9 MB	0 MB/s	0 Mbps
Microsoft Distributed Transactio...		0%	0.1 MB	0 MB/s	0 Mbps
Microsoft OneDrive (32 bit)		0%	6.2 MB	0.1 MB/s	0 Mbps
Microsoft Windows Search Inde...		0%	12.1 MB	0 MB/s	0 Mbps
mongod		0%	3.4 MB	0 MB/s	0 Mbps
mysqld		0%	1.8 MB	0 MB/s	0 Mbps

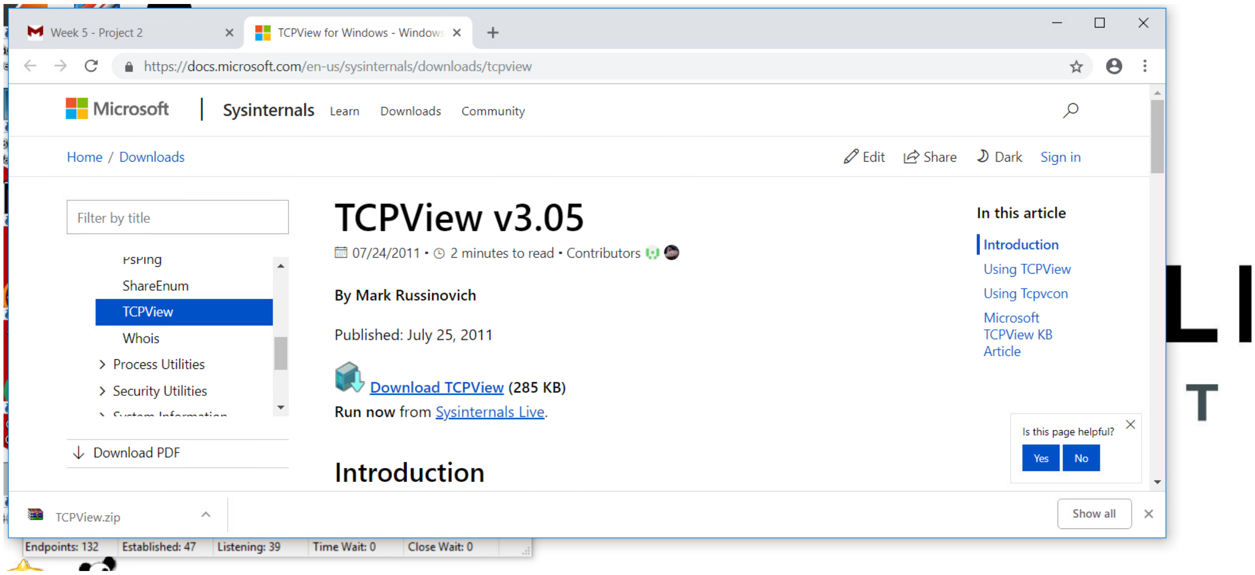


```
icrosoft Windows [Version 10.0.10240]
c) 2015 Microsoft Corporation. All rights reserved.

:\Users\knewman1>netstat -an

ctive Connections

 Proto  Local Address          Foreign Address        State
 TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
 TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
 TCP    0.0.0.0:1536           0.0.0.0:0              LISTENING
 TCP    0.0.0.0:1537           0.0.0.0:0              LISTENING
 TCP    0.0.0.0:1538           0.0.0.0:0              LISTENING
 TCP    0.0.0.0:1539           0.0.0.0:0              LISTENING
 TCP    0.0.0.0:1541           0.0.0.0:0              LISTENING
 TCP    0.0.0.0:1544           0.0.0.0:0              LISTENING
 TCP    0.0.0.0:1545           0.0.0.0:0              LISTENING
 TCP    0.0.0.0:1579           0.0.0.0:0              LISTENING
 TCP    0.0.0.0:3306           0.0.0.0:0              LISTENING
 TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING
 TCP    0.0.0.0:4000           0.0.0.0:0              LISTENING
 TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING
 TCP    0.0.0.0:8000           0.0.0.0:0              LISTENING
 TCP    0.0.0.0:8089           0.0.0.0:0              LISTENING
 TCP    0.0.0.0:8191           0.0.0.0:0              LISTENING
 TCP    0.0.0.0:8834           0.0.0.0:0              LISTENING
 TCP    0.0.0.0:9427           0.0.0.0:0              LISTENING
 TCP    0.0.0.0:22443          0.0.0.0:0              LISTENING
 TCP    0.0.0.0:32111          0.0.0.0:0              LISTENING
 TCP    10.150.3.212:139       0.0.0.0:0              LISTENING
```


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

Process	PID	Protocol	Local Address	Local Port	R
chrome.exe	11608	TCP	cyberug-86.ad.mar...	24911	a2
chrome.exe	11608	TCP	cyberug-86.ad.mar...	24912	a2
chrome.exe	11608	TCP	cyberug-86.ad.mar...	24913	a2
chrome.exe	11608	TCP	cyberug-86.ad.mar...	24914	a2
chrome.exe	11608	TCP	cyberug-86.ad.mar...	24915	a2
chrome.exe	11608	TCP	cyberug-86.ad.mar...	24917	72
chrome.exe	11608	TCP	cyberug-86.ad.mar...	24918	a1
chrome.exe	11608	TCP	cyberug-86.ad.mar...	24919	a1
chrome.exe	11608	TCP	cyberug-86.ad.mar...	24922	64
chrome.exe	11608	TCP	cyberug-86.ad.mar...	24925	15
chrome.exe	11608	TCP	cyberug-86.ad.mar...	24926	15
chrome.exe	11608	UDP	CYBERUG-86	5353	*
chrome.exe	11608	UDP	CYBERUG-86	5353	*
chrome.exe	11608	UDPV6	cyberug-86.ad.mar...	5353	*
chrome.exe	11608	TCP	cyberug-86.ad.mar...	24932	orc
lsass.exe	648	TCP	CYBERUG-86	1539	CY
lsass.exe	648	TCP	CYBERUG-86	1545	CY
lsass.exe	648	UDP	CYBERUG-86	62241	*
lsass.exe	648	TCPV6	cyberug-86.ad.mar...	1539	cyl
lsass.exe	648	TCPV6	cyberug-86.ad.mar...	1545	cyl
mongod.exe	5104	TCP	CYBERUG-86	8191	CY
mongod.exe	5104	TCP	CYBERUG-86	8191	loc
mongod.exe	5104	TCP	CYBERUG-86	8191	loc
mongod.exe	5104	TCP	CYBERUG-86	8191	loc
mongod.exe	5104	TCP	CYBERUG-86	8191	loc

Endpoints: 130 | Established: 45 | Listening: 39 | Time Wait: 0 | Close Wait: 0



TCPView v3.05

07/24/2011 • 2 minutes to read • Contributors

By Mark Russinovich

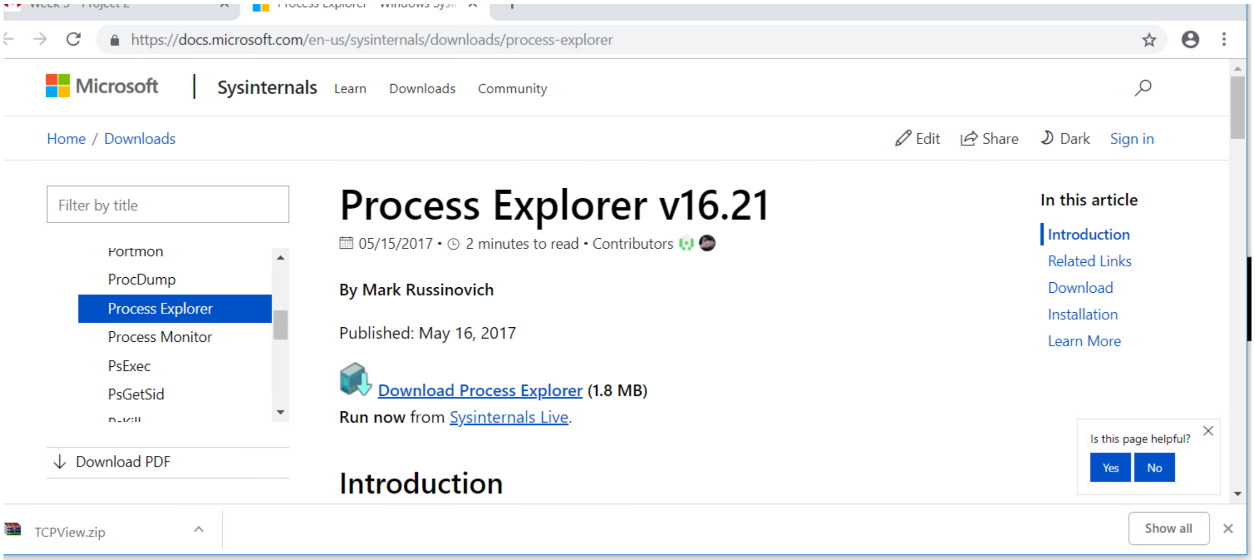
Published: July 25, 2011

Download TCPView (285 KB)

Run now from Sysinternals Live.

Introduction

Endpoints: 132 | Established: 47 | Listening: 39 | Time Wait: 0 | Close Wait: 0



Process Explorer v16.21

05/15/2017 • 2 minutes to read • Contributors

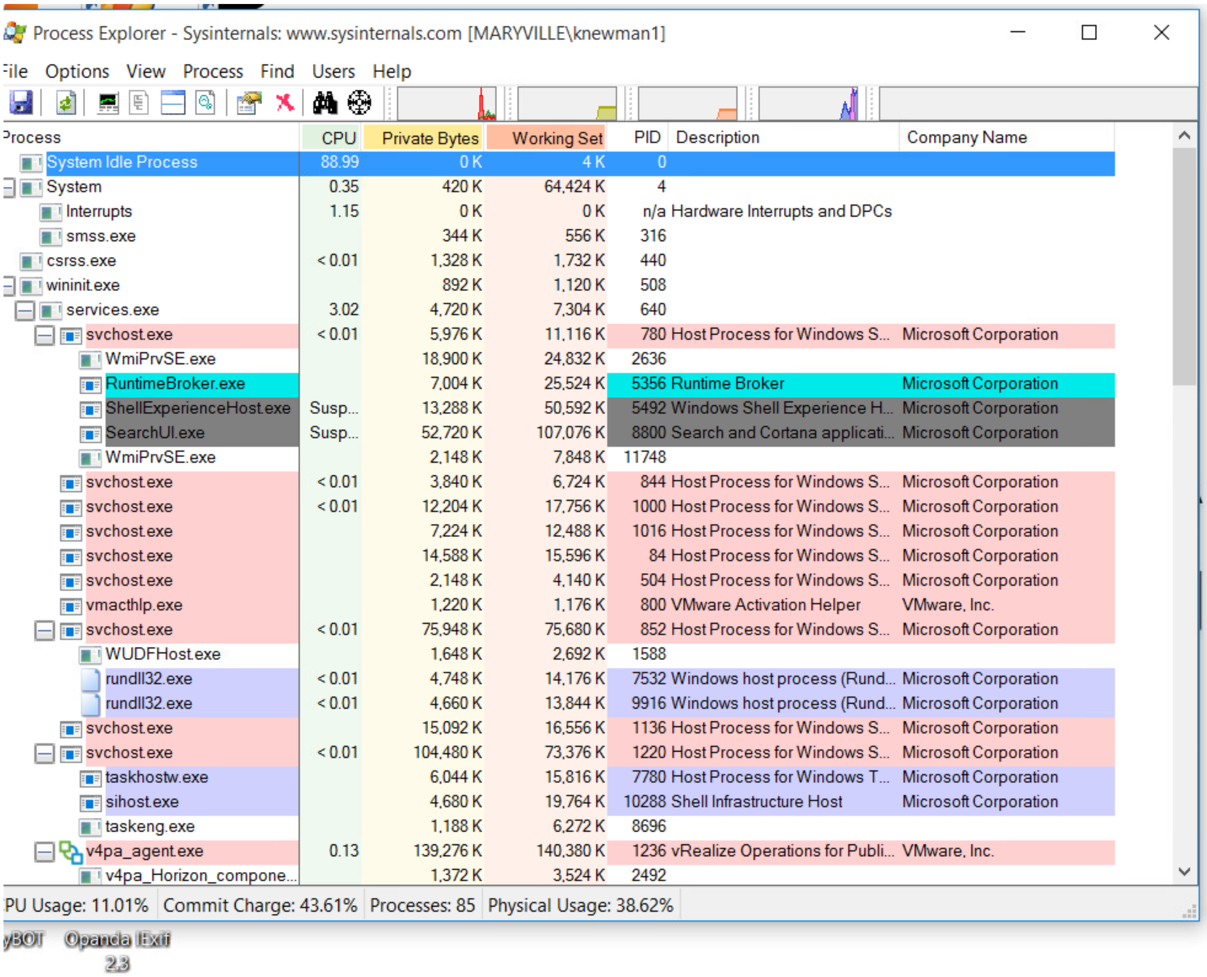
By Mark Russinovich

Published: May 16, 2017

Download Process Explorer (1.8 MB)

Run now from Sysinternals Live.

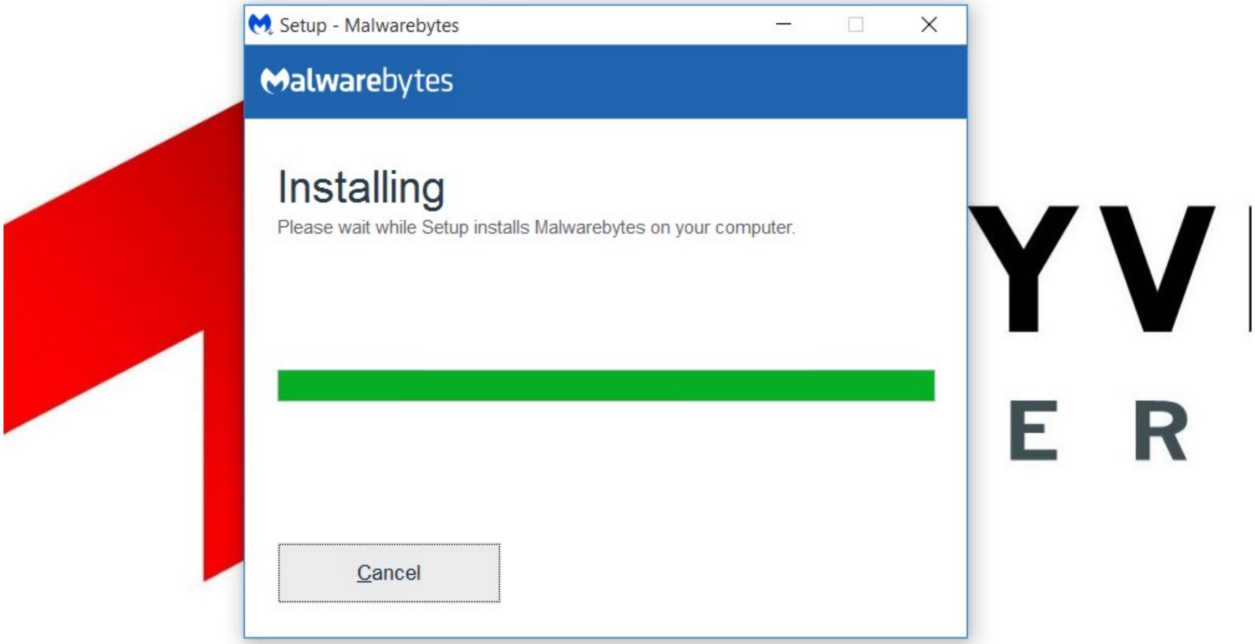
Introduction



Process Explorer - Sysinternals: www.sysinternals.com [MARYVILLE\knewman1]
File Options View Process Find Users Help
yBOT
Opanda IExif 2.3

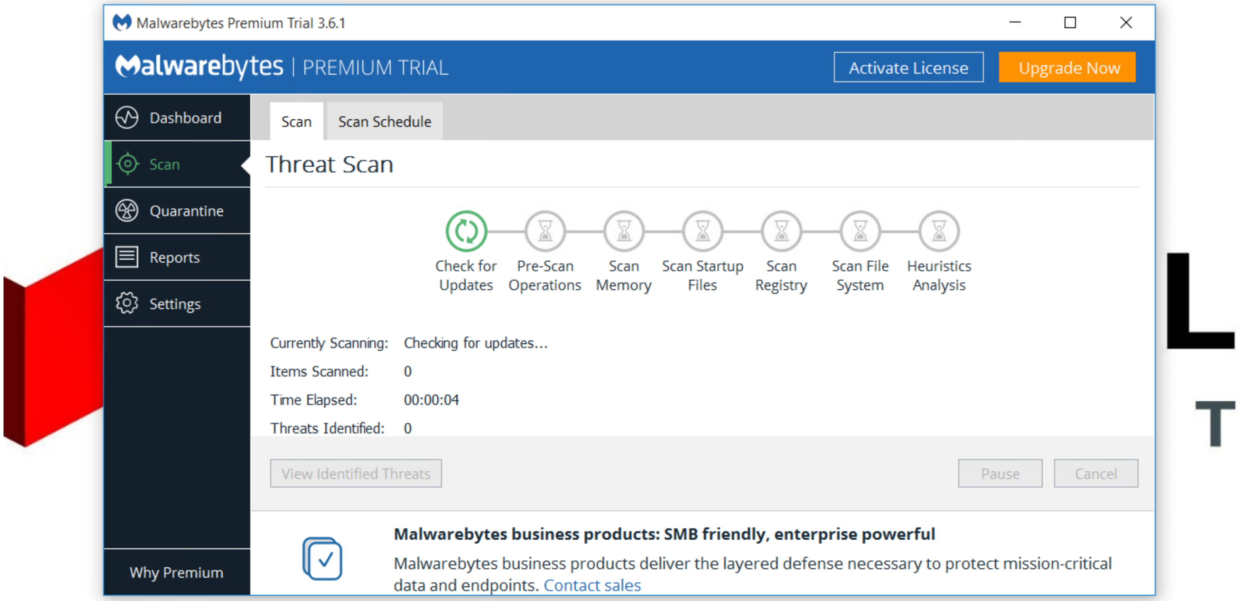
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	88.99	0 K	4 K	0		
System	0.35	420 K	64,424 K	4		
Interrupts	1.15	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		344 K	556 K	316		
csrss.exe	< 0.01	1,328 K	1,732 K	440		
wininit.exe		892 K	1,120 K	508		
services.exe	3.02	4,720 K	7,304 K	640		
svchost.exe	< 0.01	5,976 K	11,116 K	780	Host Process for Windows S...	Microsoft Corporation
WmiPrvSE.exe		18,900 K	24,832 K	2636		
RuntimeBroker.exe		7,004 K	25,524 K	5356	Runtime Broker	Microsoft Corporation
ShellExperienceHost.exe	Susp...	13,288 K	50,592 K	5492	Windows Shell Experience H...	Microsoft Corporation
SearchUI.exe	Susp...	52,720 K	107,076 K	8800	Search and Cortana applicati...	Microsoft Corporation
WmiPrvSE.exe		2,148 K	7,848 K	11748		
svchost.exe	< 0.01	3,840 K	6,724 K	844	Host Process for Windows S...	Microsoft Corporation
svchost.exe	< 0.01	12,204 K	17,756 K	1000	Host Process for Windows S...	Microsoft Corporation
svchost.exe		7,224 K	12,488 K	1016	Host Process for Windows S...	Microsoft Corporation
svchost.exe		14,588 K	15,596 K	84	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,148 K	4,140 K	504	Host Process for Windows S...	Microsoft Corporation
vmacthlp.exe		1,220 K	1,176 K	800	VMware Activation Helper	VMware, Inc.
svchost.exe	< 0.01	75,948 K	75,680 K	852	Host Process for Windows S...	Microsoft Corporation
WUDFHost.exe		1,648 K	2,692 K	1588		
rundll32.exe	< 0.01	4,748 K	14,176 K	7532	Windows host process (Rund...	Microsoft Corporation
rundll32.exe	< 0.01	4,660 K	13,844 K	9916	Windows host process (Rund...	Microsoft Corporation
svchost.exe		15,092 K	16,556 K	1136	Host Process for Windows S...	Microsoft Corporation
svchost.exe	< 0.01	104,480 K	73,376 K	1220	Host Process for Windows S...	Microsoft Corporation
taskhostw.exe		6,044 K	15,816 K	7780	Host Process for Windows T...	Microsoft Corporation
sihost.exe		4,680 K	19,764 K	10288	Shell Infrastructure Host	Microsoft Corporation
taskeng.exe		1,188 K	6,272 K	8696		
v4pa_agent.exe	0.13	139,276 K	140,380 K	1236	vRealize Operations for Publi...	VMware, Inc.
v4pa_Horizon_compone...		1,372 K	3,524 K	2492		

CPU Usage: 11.01% Commit Charge: 43.61% Processes: 85 Physical Usage: 38.62%



Installing

Please wait while Setup installs Malwarebytes on your computer.

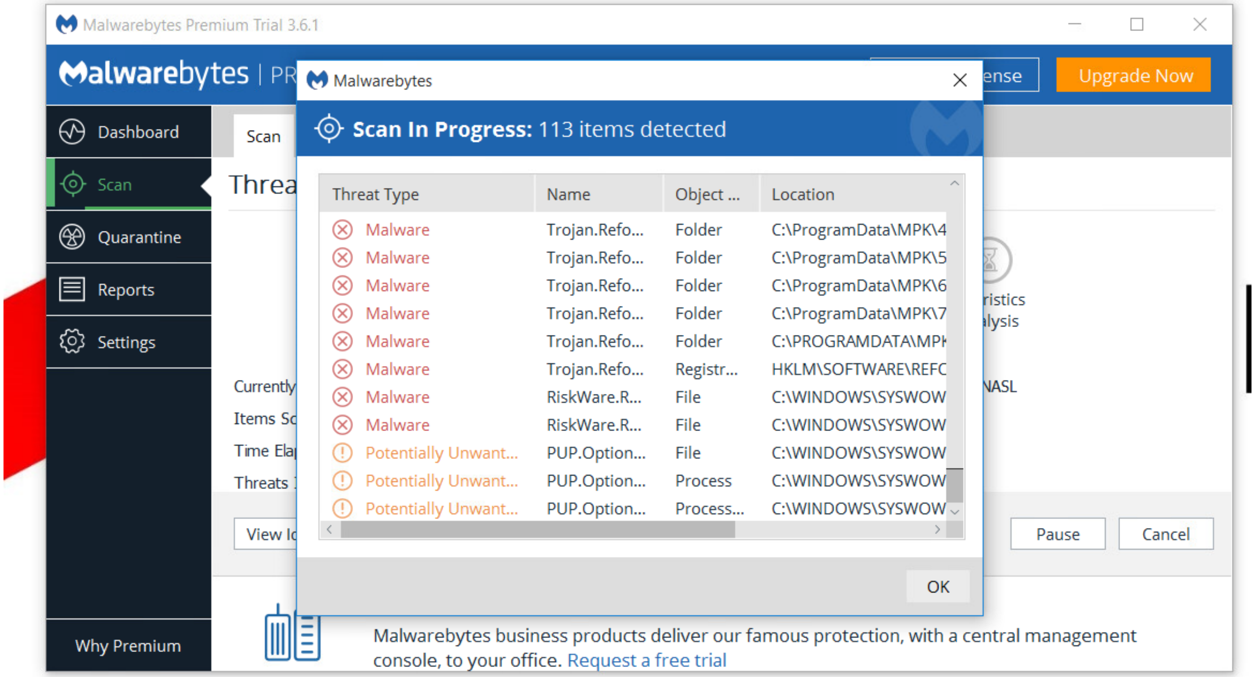


Threat Scan

Currently Scanning: Checking for updates...
Items Scanned: 0
Time Elapsed: 00:00:04
Threats Identified: 0

Malwarebytes business products: SMB friendly, enterprise powerful

Malwarebytes business products deliver the layered defense necessary to protect mission-critical data and endpoints. Contact sales



Malwarebytes Premium Trial 3.6.1

Malwarebytes | PR

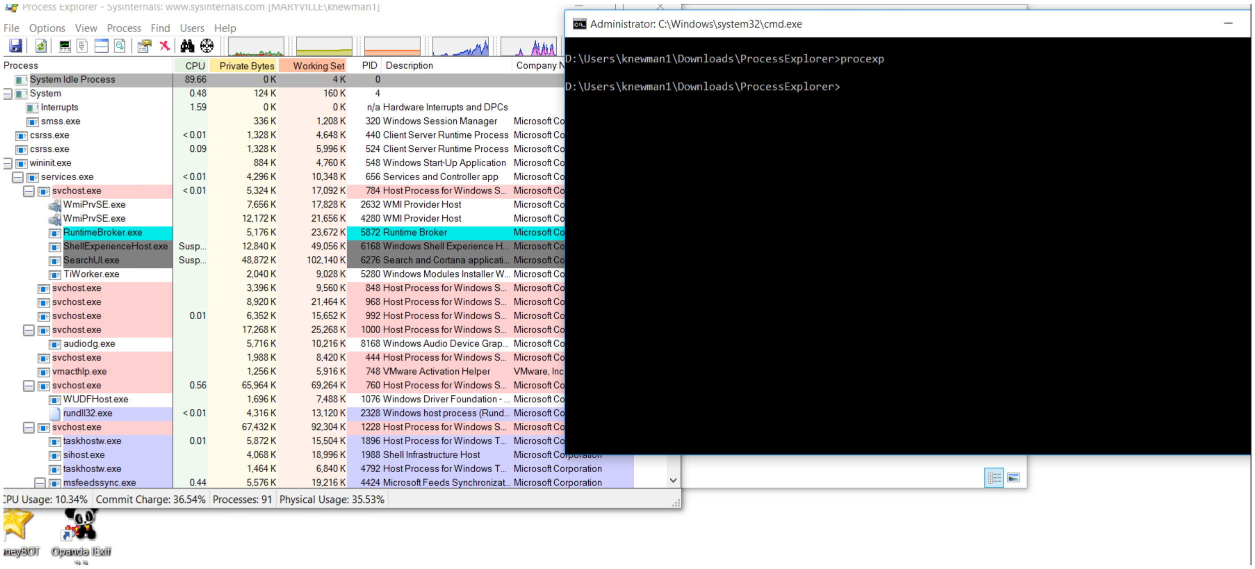
Malwarebytes

Scan In Progress: 113 items detected

Threat Type	Name	Object ...	Location
Malware	Trojan.Refo...	Folder	C:\ProgramData\MPK\4
Malware	Trojan.Refo...	Folder	C:\ProgramData\MPK\5
Malware	Trojan.Refo...	Folder	C:\ProgramData\MPK\6
Malware	Trojan.Refo...	Folder	C:\ProgramData\MPK\7
Malware	Trojan.Refo...	Folder	C:\PROGRAMDATA\MPK
Malware	Trojan.Refo...	Registr...	HKLM\SOFTWARE\REFC
Malware	RiskWare.R...	File	C:\WINDOWS\SYSWOW
Malware	RiskWare.R...	File	C:\WINDOWS\SYSWOW
Potentially Unwant...	PUP.Option...	File	C:\WINDOWS\SYSWOW
Potentially Unwant...	PUP.Option...	Process	C:\WINDOWS\SYSWOW
Potentially Unwant...	PUP.Option...	Process...	C:\WINDOWS\SYSWOW

Malwarebytes business products deliver our famous protection, with a central management console, to your office. Request a free trial

Course Textbook Exercise 5.2 Using Process Explorer



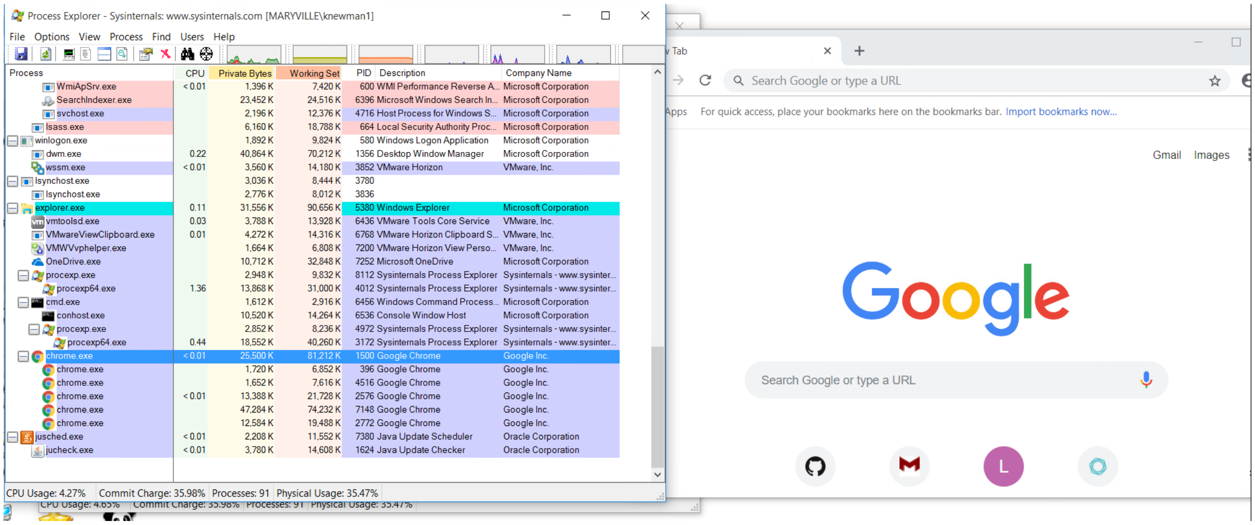
Process Explorer - Sysinternals: www.sysinternals.com [MARYVILLE\knewman1]

Process	CPU	Private Bytes	Working Set	PID	Description	Company N
System Idle Process	89.66	0 K	4 K	0		
System	0.48	124 K	160 K	4		
Interrupts	1.59	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		336 K	1,208 K	320	Windows Session Manager	Microsoft Co
csrss.exe	< 0.01	1,328 K	4,648 K	440	Client Server Runtime Process	Microsoft Co
csrss.exe	0.09	1,328 K	5,996 K	524	Client Server Runtime Process	Microsoft Co
wininit.exe		884 K	4,760 K	548	Windows Start-Up Application	Microsoft Co
services.exe	< 0.01	4,296 K	10,348 K	656	Services and Controller app	Microsoft Co
svchost.exe	< 0.01	5,324 K	17,092 K	784	Host Process for Windows S...	Microsoft Co
WmiPrvSE.exe		7,656 K	17,828 K	2632	WMI Provider Host	Microsoft Co
WmiPrvSE.exe		12,172 K	21,656 K	4280	WMI Provider Host	Microsoft Co
RuntimeBroker.exe		5,176 K	23,672 K	5872	Runtime Broker	Microsoft Co
ShellExperienceHost.exe	Susp...	12,840 K	49,056 K	6168	Windows Shell Experience H...	Microsoft Co
SearchUI.exe	Susp...	48,872 K	102,140 K	6276	Search and Cortana applicati...	Microsoft Co
TiWorker.exe		2,040 K	9,028 K	5280	Windows Modules Installer W...	Microsoft Co
svchost.exe		3,396 K	9,560 K	848	Host Process for Windows S...	Microsoft Co
svchost.exe		8,920 K	21,464 K	968	Host Process for Windows S...	Microsoft Co
svchost.exe	0.01	6,352 K	15,652 K	992	Host Process for Windows S...	Microsoft Co
svchost.exe		17,268 K	25,268 K	1000	Host Process for Windows S...	Microsoft Co
audiodg.exe		5,716 K	10,216 K	8168	Windows Audio Device Grap...	Microsoft Co
svchost.exe		1,988 K	8,420 K	444	Host Process for Windows S...	Microsoft Co
vmacthlp.exe		1,256 K	5,916 K	748	VMware Activation Helper	VMware, Inc
svchost.exe	0.56	65,964 K	69,264 K	760	Host Process for Windows S...	Microsoft Co
WUDFHost.exe		1,696 K	7,488 K	1076	Windows Driver Foundation - ...	Microsoft Co
rundll32.exe	< 0.01	4,316 K	13,120 K	2328	Windows host process (Rund...	Microsoft Co
svchost.exe		67,432 K	92,304 K	1228	Host Process for Windows S...	Microsoft Co
taskhostw.exe	0.01	5,872 K	15,504 K	1896	Host Process for Windows T...	Microsoft Co
sihost.exe		4,068 K	18,996 K	1988	Shell Infrastructure Host	Microsoft Corporation
taskhostw.exe		1,464 K	6,840 K	4792	Host Process for Windows T...	Microsoft Corporation
msfeedssync.exe	0.44	5,576 K	19,216 K	4424	Microsoft Feeds Synchronizat...	Microsoft Corporation

PU Usage: 10.34% Commit Charge: 36.54% Processes: 91 Physical Usage: 35.53%

Administrator: C:\Windows\system32\cmd.exe

```
D:\Users\knewman1\Downloads\ProcessExplorer>procexp

D:\Users\knewman1\Downloads\ProcessExplorer>
```

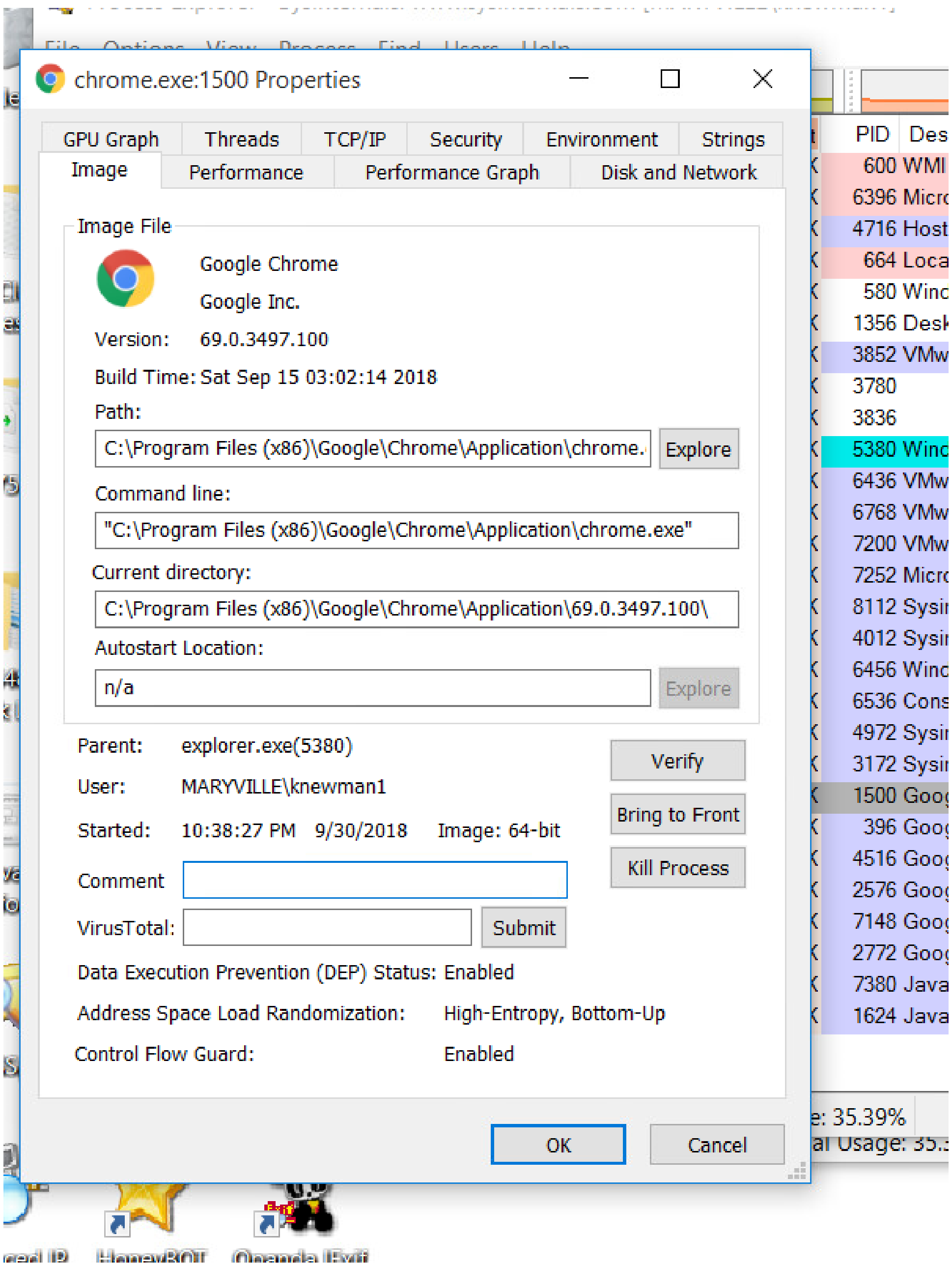

Process Explorer - Sysinternals: www.sysinternals.com [MARYVILLE\knewman1]
File
Options
View
Process
Find
Users
Help
Tab
Search Google or type a URL
Apps
Gmail
Images
Google
Search Google or type a URL
L

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
WmiApSrv.exe	< 0.01	1,396 K	7,420 K	600	WMI Performance Reverse A...	Microsoft Corporation
SearchIndexer.exe		23,452 K	24,516 K	6396	Microsoft Windows Search In...	Microsoft Corporation
svchost.exe		2,196 K	12,376 K	4716	Host Process for Windows S...	Microsoft Corporation
lsass.exe		6,160 K	18,788 K	664	Local Security Authority Proc...	Microsoft Corporation
winlogon.exe		1,892 K	9,824 K	580	Windows Logon Application	Microsoft Corporation
dwm.exe	0.22	40,864 K	70,212 K	1356	Desktop Window Manager	Microsoft Corporation
wssm.exe	< 0.01	3,560 K	14,180 K	3852	VMware Horizon	VMware, Inc.
lsynchost.exe		3,036 K	8,444 K	3780		
lsynchost.exe		2,776 K	8,012 K	3836		
explorer.exe	0.11	31,556 K	90,656 K	5380	Windows Explorer	Microsoft Corporation
vmtoolsd.exe	0.03	3,788 K	13,928 K	6436	VMware Tools Core Service	VMware, Inc.
VMwareViewClipboard.exe	0.01	4,272 K	14,316 K	6768	VMware Horizon Clipboard S...	VMware, Inc.
VMWVvphelper.exe		1,664 K	6,808 K	7200	VMware Horizon View Perso...	VMware, Inc.
OneDrive.exe		10,712 K	32,848 K	7252	Microsoft OneDrive	Microsoft Corporation
procexp.exe		2,948 K	9,832 K	8112	Sysinternals Process Explorer	Sysinternals - www.sysinter...
procexp64.exe	1.36	13,868 K	31,000 K	4012	Sysinternals Process Explorer	Sysinternals - www.sysinter...
cmd.exe		1,612 K	2,916 K	6456	Windows Command Process...	Microsoft Corporation
conhost.exe		10,520 K	14,264 K	6536	Console Window Host	Microsoft Corporation
procexp.exe		2,852 K	8,236 K	4972	Sysinternals Process Explorer	Sysinternals - www.sysinter...
procexp64.exe	0.44	18,552 K	40,260 K	3172	Sysinternals Process Explorer	Sysinternals - www.sysinter...
chrome.exe	< 0.01	25,500 K	81,212 K	1500	Google Chrome	Google Inc.
chrome.exe		1,720 K	6,852 K	396	Google Chrome	Google Inc.
chrome.exe		1,652 K	7,616 K	4516	Google Chrome	Google Inc.
chrome.exe	< 0.01	13,388 K	21,728 K	2576	Google Chrome	Google Inc.
chrome.exe		47,284 K	74,232 K	7148	Google Chrome	Google Inc.
chrome.exe		12,584 K	19,488 K	2772	Google Chrome	Google Inc.
jusched.exe	< 0.01	2,208 K	11,552 K	7380	Java Update Scheduler	Oracle Corporation
jucheck.exe	< 0.01	3,780 K	14,608 K	1624	Java Update Checker	Oracle Corporation

CPU Usage: 4.27% Commit Charge: 35.98% Processes: 91 Physical Usage: 35.47%

CPU Usage: 4.65% Commit Charge: 35.98% Processes: 91 Physical Usage: 35.47%

For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...



chrome.exe:1500 Properties

Image File

Google Chrome

Google Inc.

Version: 69.0.3497.100

Build Time: Sat Sep 15 03:02:14 2018

Path:

C:\Program Files (x86)\Google\Chrome\Application\chrome.

Command line:

"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"

Current directory:

C:\Program Files (x86)\Google\Chrome\Application\69.0.3497.100\

Autostart Location:

n/a

Parent: explorer.exe(5380)

User: MARYVILLE\knewman1

Started: 10:38:27 PM 9/30/2018 Image: 64-bit

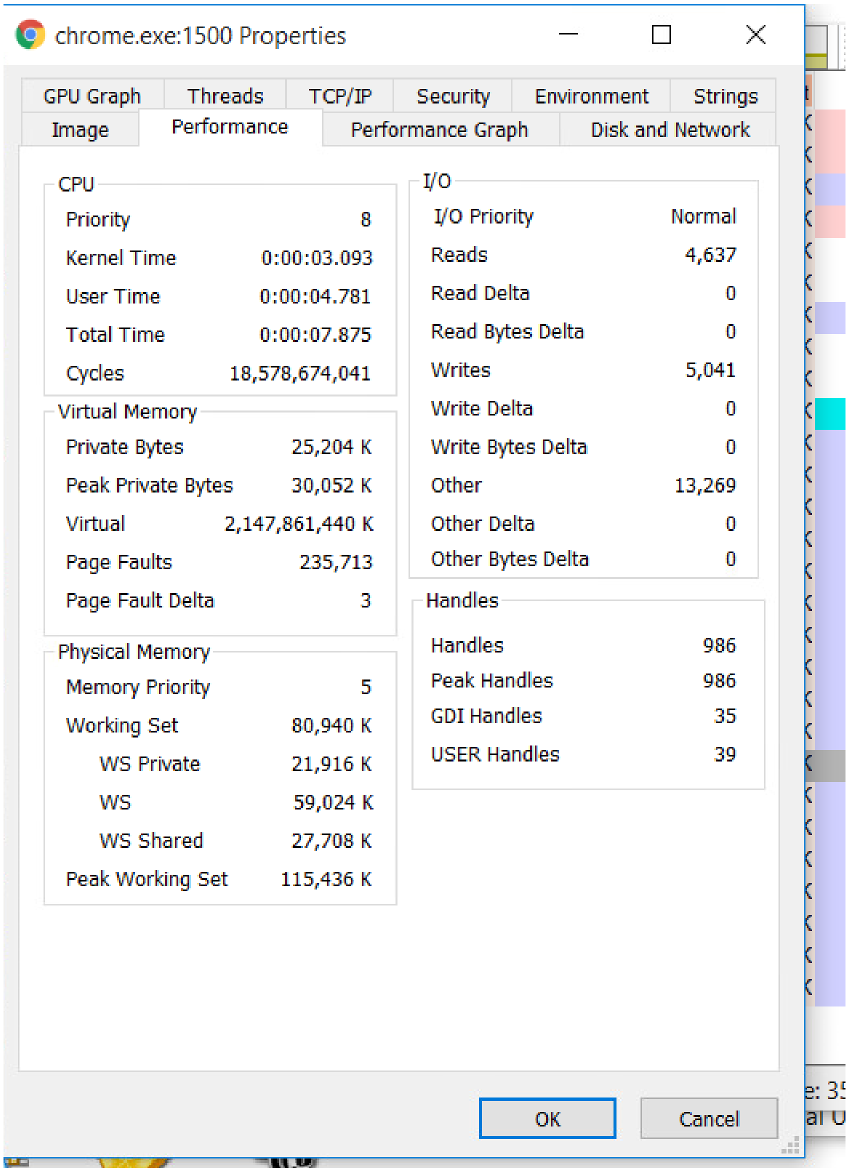
Comment

VirusTotal:

Data Execution Prevention (DEP) Status: Enabled

Address Space Load Randomization: High-Entropy, Bottom-Up

Control Flow Guard: Enabled



CPU

Priority	8
Kernel Time	0:00:03.093
User Time	0:00:04.781
Total Time	0:00:07.875
Cycles	18,578,674,041

Virtual Memory

Private Bytes	25,204 K
Peak Private Bytes	30,052 K
Virtual	2,147,861,440 K
Page Faults	235,713
Page Fault Delta	3

Physical Memory

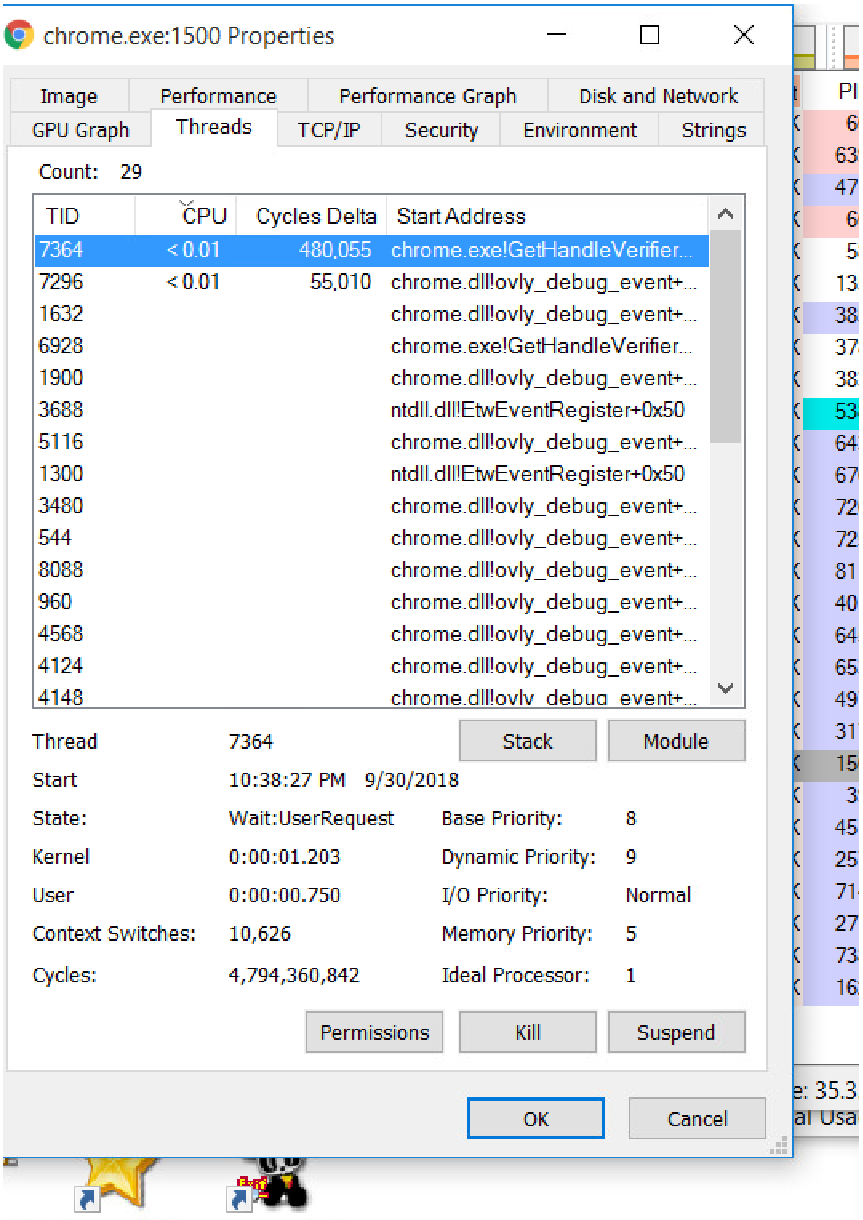
Memory Priority	5
Working Set	80,940 K
WS Private	21,916 K
WS	59,024 K
WS Shared	27,708 K
Peak Working Set	115,436 K

I/O

I/O Priority	Normal
Reads	4,637
Read Delta	0
Read Bytes Delta	0
Writes	5,041
Write Delta	0
Write Bytes Delta	0
Other	13,269
Other Delta	0
Other Bytes Delta	0

Handles

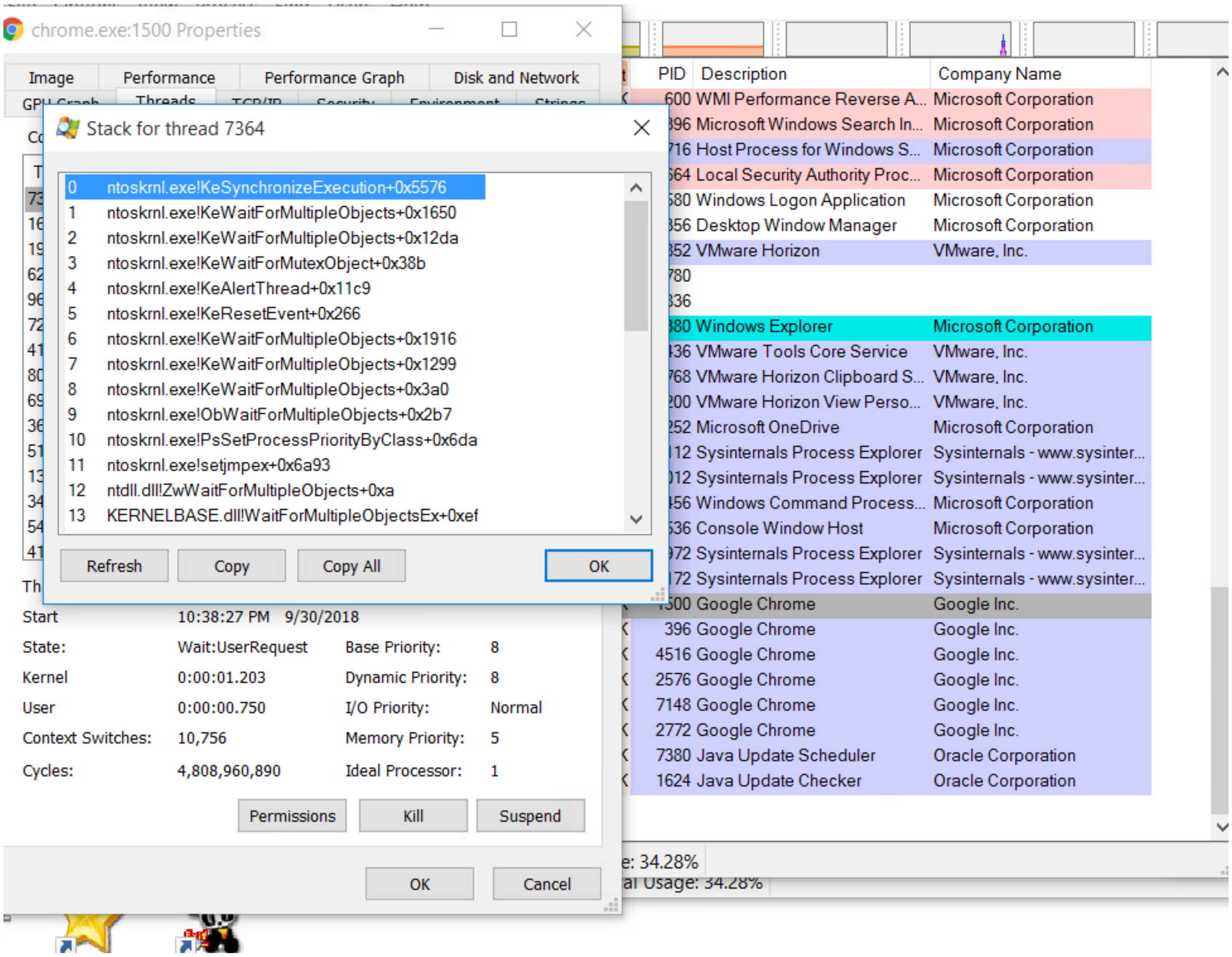
Handles	986
Peak Handles	986
GDI Handles	35
USER Handles	39



Count: 29

TID	CPU	Cycles Delta	Start Address
7364	< 0.01	480,055	chrome.exe!GetHandleVerifier...
7296	< 0.01	55,010	chrome.dll!ovly_debug_event+...
1632			chrome.dll!ovly_debug_event+...
6928			chrome.exe!GetHandleVerifier...
1900			chrome.dll!ovly_debug_event+...
3688			ntdll.dll!EtwEventRegister+0x50
5116			chrome.dll!ovly_debug_event+...
1300			ntdll.dll!EtwEventRegister+0x50
3480			chrome.dll!ovly_debug_event+...
544			chrome.dll!ovly_debug_event+...
8088			chrome.dll!ovly_debug_event+...
960			chrome.dll!ovly_debug_event+...
4568			chrome.dll!ovly_debug_event+...
4124			chrome.dll!ovly_debug_event+...
4148			chrome.dll!ovly_debug_event+...

Thread	7364		
Start	10:38:27 PM 9/30/2018		
State:	Wait:UserRequest	Base Priority:	8
Kernel	0:00:01.203	Dynamic Priority:	9
User	0:00:00.750	I/O Priority:	Normal
Context Switches:	10,626	Memory Priority:	5
Cycles:	4,794,360,842	Ideal Processor:	1

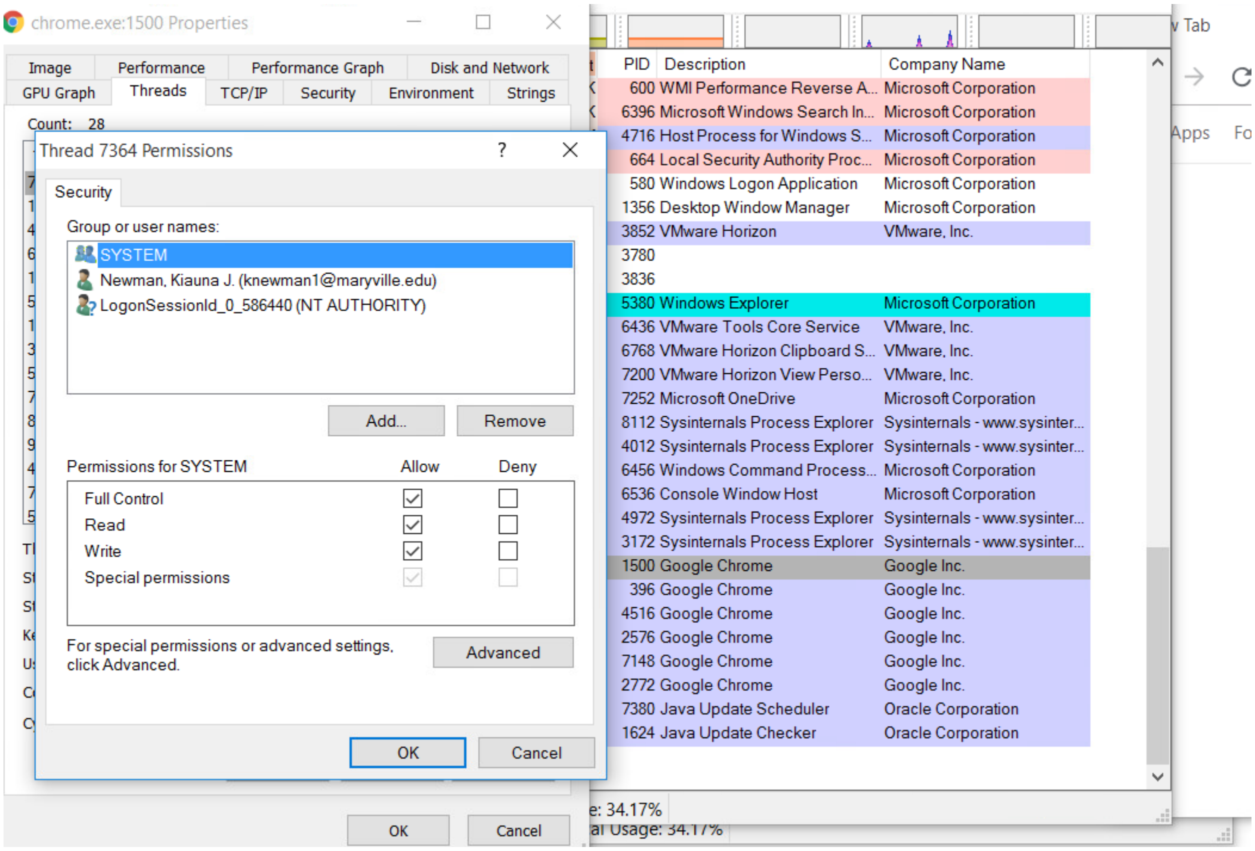


```
0   ntoskrnl.exe!KeSynchronizeExecution+0x5576
1   ntoskrnl.exe!KeWaitForMultipleObjects+0x1650
2   ntoskrnl.exe!KeWaitForMultipleObjects+0x12da
3   ntoskrnl.exe!KeWaitForMutexObject+0x38b
4   ntoskrnl.exe!KeAlertThread+0x11c9
5   ntoskrnl.exe!KeResetEvent+0x266
6   ntoskrnl.exe!KeWaitForMultipleObjects+0x1916
7   ntoskrnl.exe!KeWaitForMultipleObjects+0x1299
8   ntoskrnl.exe!KeWaitForMultipleObjects+0x3a0
9   ntoskrnl.exe!ObWaitForMultipleObjects+0x2b7
10  ntoskrnl.exe!PsSetProcessPriorityByClass+0x6da
11  ntoskrnl.exe!setjmpex+0x6a93
12  ntdll.dll!ZwWaitForMultipleObjects+0xa
13  KERNELBASE.dll!WaitForMultipleObjectsEx+0xef
```

```
Start              10:38:27 PM  9/30/2018
State:             Wait:UserRequest    Base Priority:      8
Kernel             0:00:01.203         Dynamic Priority:   8
User               0:00:00.750         I/O Priority:       Normal
Context Switches:  10,756              Memory Priority:    5
Cycles:            4,808,960,890       Ideal Processor:    1
```

PID	Description	Company Name
600	WMI Performance Reverse A...	Microsoft Corporation
396	Microsoft Windows Search In...	Microsoft Corporation
716	Host Process for Windows S...	Microsoft Corporation
364	Local Security Authority Proc...	Microsoft Corporation
580	Windows Logon Application	Microsoft Corporation
356	Desktop Window Manager	Microsoft Corporation
352	VMware Horizon	VMware, Inc.
780		
336		
380	Windows Explorer	Microsoft Corporation
436	VMware Tools Core Service	VMware, Inc.
768	VMware Horizon Clipboard S...	VMware, Inc.
200	VMware Horizon View Perso...	VMware, Inc.
252	Microsoft OneDrive	Microsoft Corporation
112	Sysinternals Process Explorer	Sysinternals - www.sysinter...
012	Sysinternals Process Explorer	Sysinternals - www.sysinter...
456	Windows Command Process...	Microsoft Corporation
536	Console Window Host	Microsoft Corporation
972	Sysinternals Process Explorer	Sysinternals - www.sysinter...
172	Sysinternals Process Explorer	Sysinternals - www.sysinter...
1500	Google Chrome	Google Inc.
396	Google Chrome	Google Inc.
4516	Google Chrome	Google Inc.
2576	Google Chrome	Google Inc.
7148	Google Chrome	Google Inc.
2772	Google Chrome	Google Inc.
7380	Java Update Scheduler	Oracle Corporation
1624	Java Update Checker	Oracle Corporation

e: 34.28%
al Usage: 34.28%



chrome.exe:1500 Properties

Count: 28

Thread 7364 Permissions

Group or user names:

- SYSTEM
- Newman, Kiauna J. (knewman1@maryville.edu)
- LogonSessionId_0_586440 (NT AUTHORITY)

Permissions for SYSTEM	Allow	Deny
Full Control	☑	□
Read	☑	□
Write	☑	□
Special permissions	☑	□

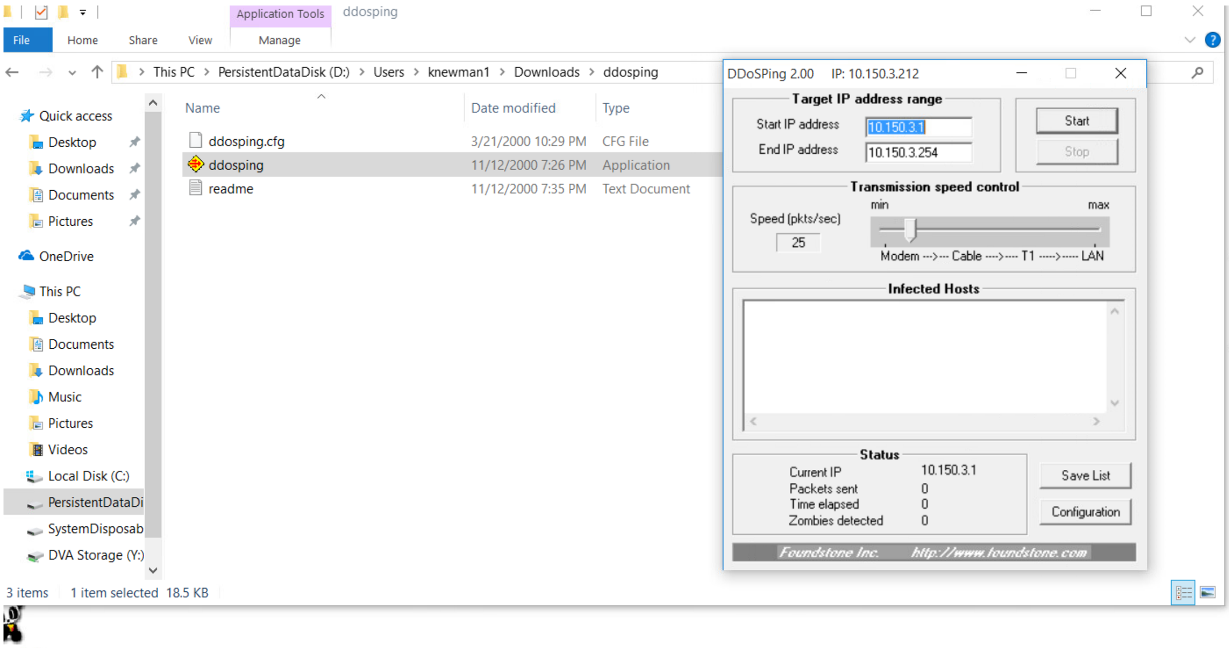
For special permissions or advanced settings, click Advanced.

PID	Description	Company Name
600	WMI Performance Reverse A...	Microsoft Corporation
6396	Microsoft Windows Search In...	Microsoft Corporation
4716	Host Process for Windows S...	Microsoft Corporation
664	Local Security Authority Proc...	Microsoft Corporation
580	Windows Logon Application	Microsoft Corporation
1356	Desktop Window Manager	Microsoft Corporation
3852	VMware Horizon	VMware, Inc.
3780		
3836		
5380	Windows Explorer	Microsoft Corporation
6436	VMware Tools Core Service	VMware, Inc.
6768	VMware Horizon Clipboard S...	VMware, Inc.
7200	VMware Horizon View Perso...	VMware, Inc.
7252	Microsoft OneDrive	Microsoft Corporation
8112	Sysinternals Process Explorer	Sysinternals - www.sysinter...
4012	Sysinternals Process Explorer	Sysinternals - www.sysinter...
6456	Windows Command Process...	Microsoft Corporation
6536	Console Window Host	Microsoft Corporation
4972	Sysinternals Process Explorer	Sysinternals - www.sysinter...
3172	Sysinternals Process Explorer	Sysinternals - www.sysinter...
1500	Google Chrome	Google Inc.
396	Google Chrome	Google Inc.
4516	Google Chrome	Google Inc.
2576	Google Chrome	Google Inc.
7148	Google Chrome	Google Inc.
2772	Google Chrome	Google Inc.
7380	Java Update Scheduler	Oracle Corporation
1624	Java Update Checker	Oracle Corporation

e: 34.17%

al Usage: 34.17%

Course Textbook Exercise 6.1 Scanning for DDoS Programs



This PC > PersistentDataDisk (D:) > Users > knewman1 > Downloads > ddosping

Name	Date modified	Type
ddosping.cfg	3/21/2000 10:29 PM	CFG File
ddosping	11/12/2000 7:26 PM	Application
readme	11/12/2000 7:35 PM	Text Document

3 items 1 item selected 18.5 KB

DDoSPing 2.00 IP: 10.150.3.212

Target IP address range

Start IP address 10.150.3.1

End IP address 10.150.3.254

Transmission speed control

Speed (pkts/sec) 25

Infected Hosts

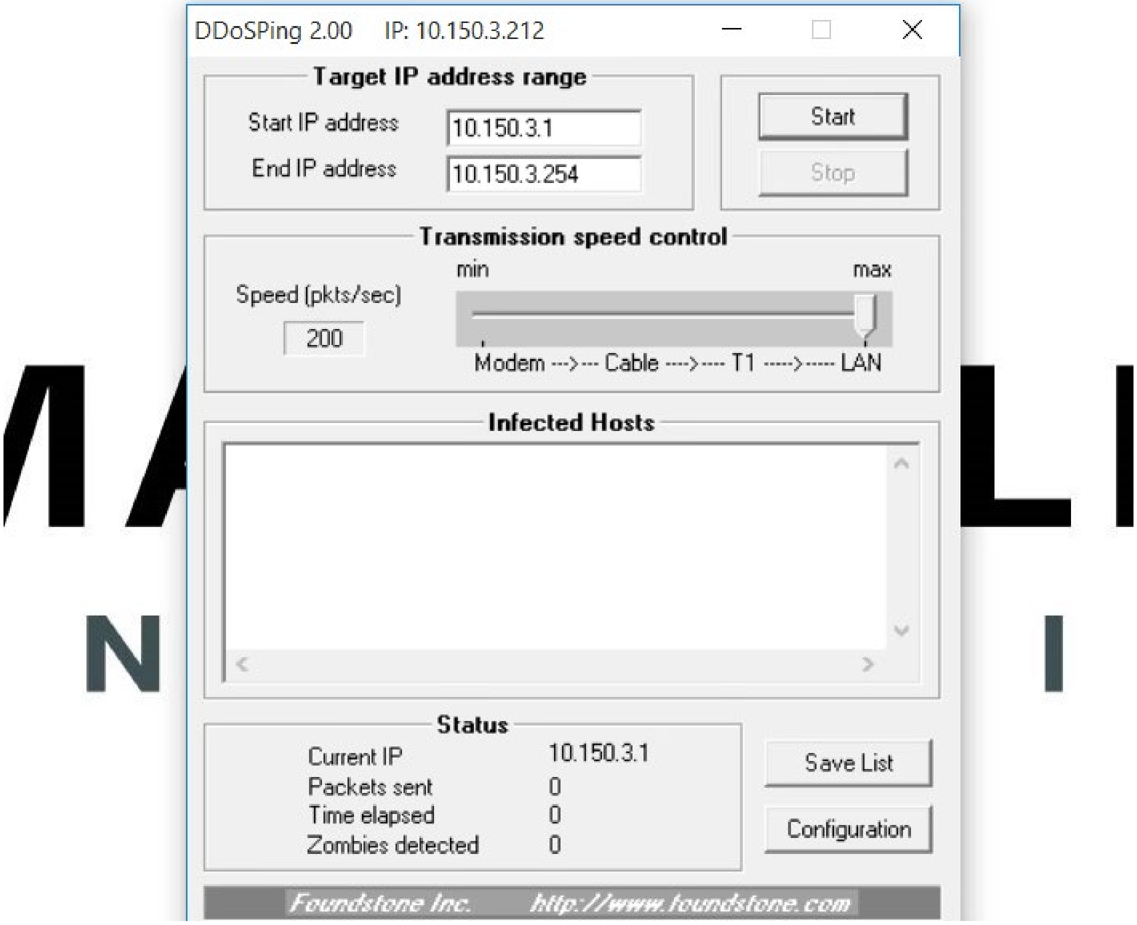
Status

Current IP 10.150.3.1

Packets sent 0

Time elapsed 0

Zombies detected 0



DDoSPing 2.00 IP: 10.150.3.212

Target IP address range

Start IP address: 10.150.3.1

End IP address: 10.150.3.254

Transmission speed control

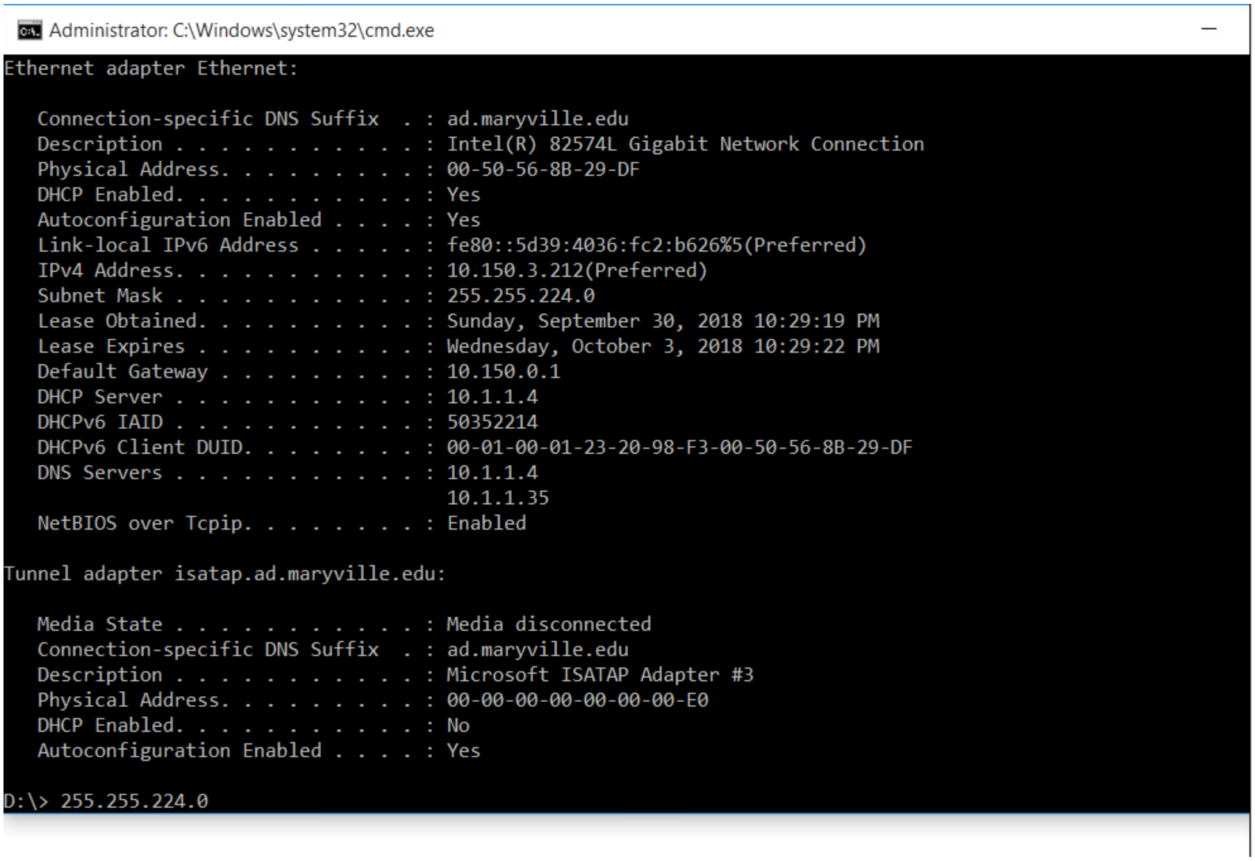
Speed (pkts/sec): 200

Infected Hosts

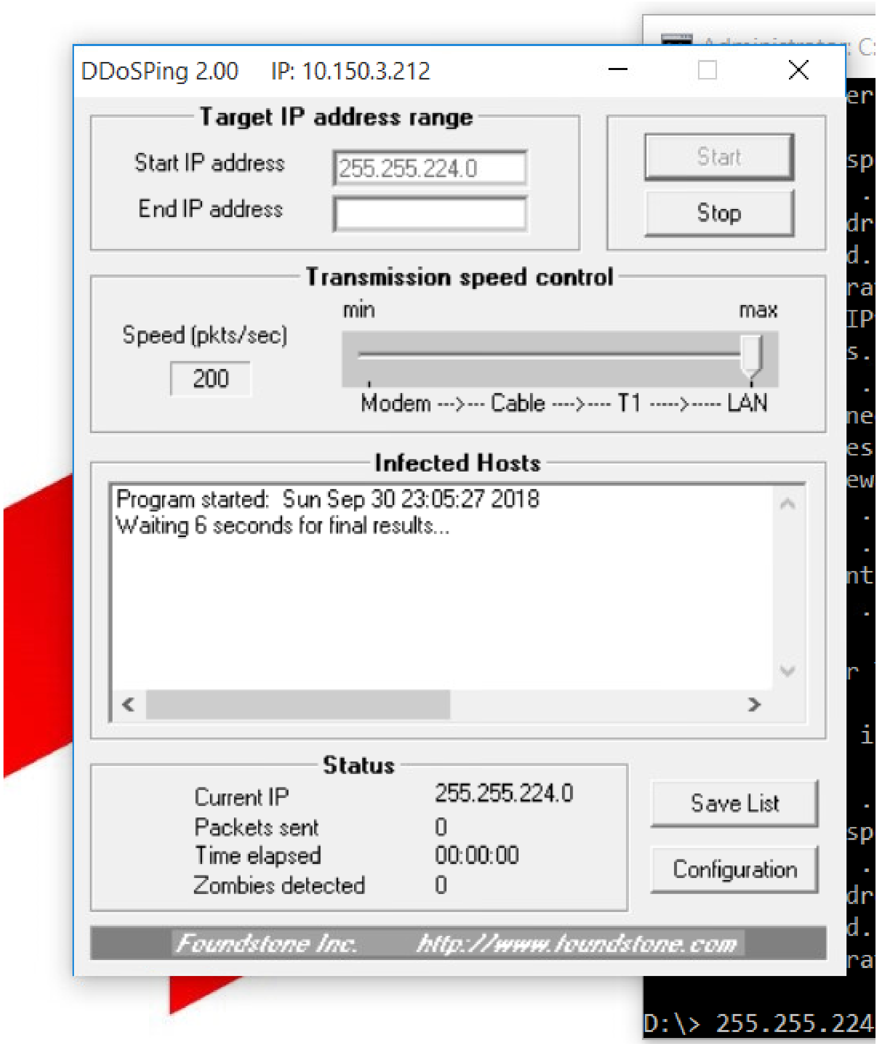
Status

```
Current IP          10.150.3.1
Packets sent        0
Time elapsed        0
Zombies detected    0
```

Start
Stop
min
max
Modem --->--- Cable ---->---- T1 ----->----- LAN
Save List
Configuration
Foundstone Inc. http://www.foundstone.com



```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : ad.maryville.edu
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-50-56-8B-29-DF
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::5d39:4036:fc2:b626%5(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.150.3.212(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.224.0
   Lease Obtained. . . . . . . . . . : Sunday, September 30, 2018 10:29:19 PM
   Lease Expires . . . . . . . . . . : Wednesday, October 3, 2018 10:29:22 PM
   Default Gateway . . . . . . . . . : 10.150.0.1
   DHCP Server . . . . . . . . . . . : 10.1.1.4
   DHCPv6 IAID . . . . . . . . . . . : 50352214
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-23-20-98-F3-00-50-56-8B-29-DF
   DNS Servers . . . . . . . . . . . : 10.1.1.4
                                       10.1.1.35
   NetBIOS over Tcpip. . . . . . . . : Enabled

Tunnel adapter isatap.ad.maryville.edu:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : ad.maryville.edu
   Description . . . . . . . . . . . : Microsoft ISATAP Adapter #3
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes

D:\> 255.255.224.0
```


DDoSPing 2.00 IP: 10.150.3.212
Target IP address range
Start
Stop
Transmission speed control
min
max
Modem --->--- Cable ---->---- T1 ----->----- LAN
Infected Hosts
Status
Save List
Configuration
Foundstone Inc. http://www.foundstone.com

Start IP address: 255.255.224.0

End IP address:

Speed (pkts/sec): 200

```
Program started:  Sun Sep 30 23:05:27 2018
Waiting 6 seconds for final results...
```

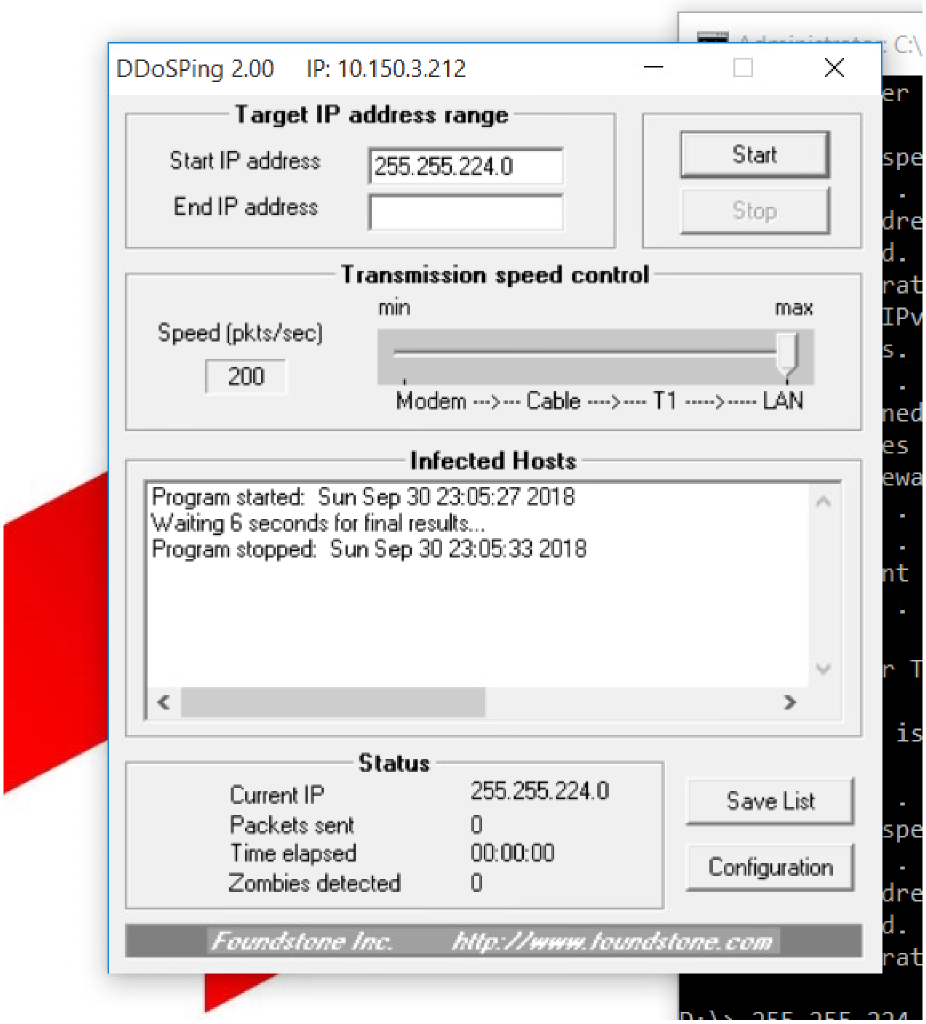
Current IP: 255.255.224.0

Packets sent: 0

Time elapsed: 00:00:00

Zombies detected: 0

```
D:\> 255.255.224
```



DDoSPing 2.00 IP: 10.150.3.212

Target IP address range

Start IP address 255.255.224.0

End IP address

Transmission speed control

Speed (pkts/sec) 200

Infected Hosts

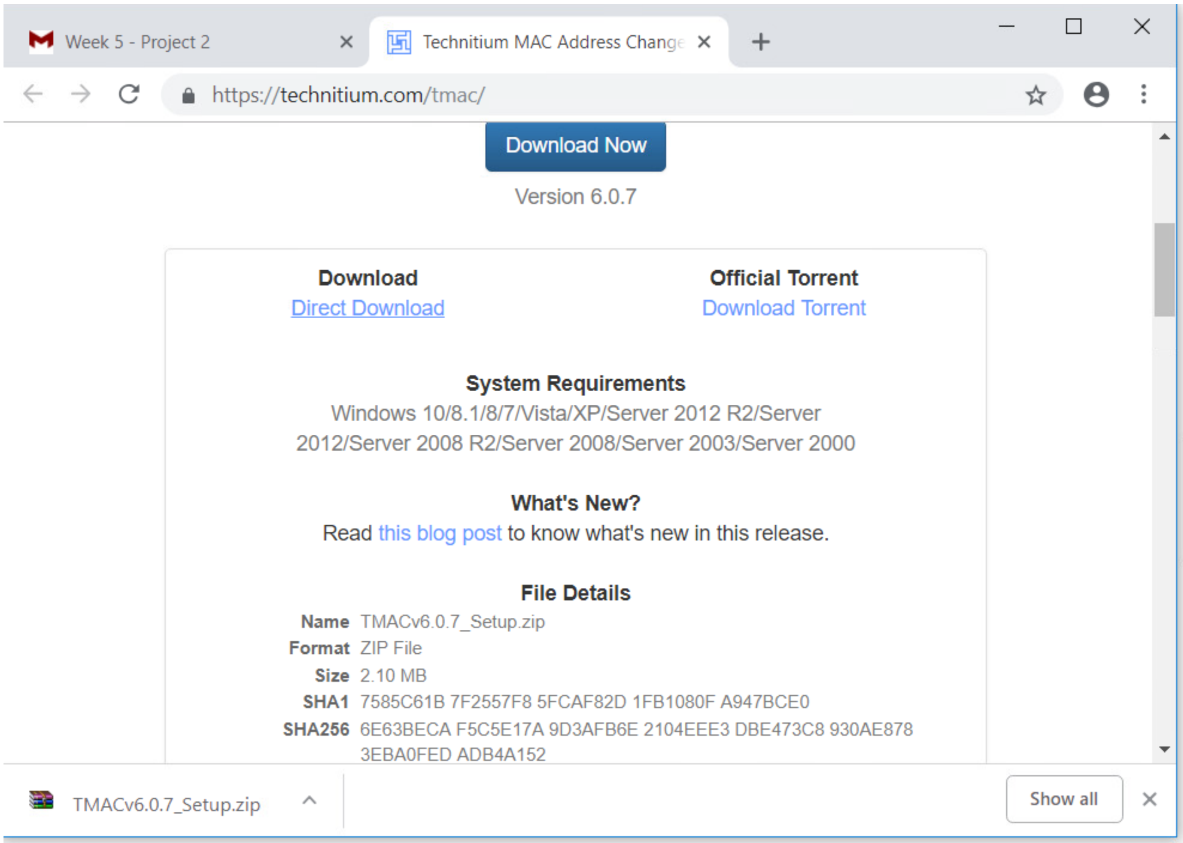
```
Program started:  Sun Sep 30 23:05:27 2018
Waiting 6 seconds for final results...
Program stopped:  Sun Sep 30 23:05:33 2018
```

Status

Current IP	255.255.224.0
Packets sent	0
Time elapsed	00:00:00
Zombies detected	0

Start
Stop
min
max
Modem ---›--- Cable ----›---- T1 -----›----- LAN
Save List
Configuration
Foundstone Inc. http://www.foundstone.com

Course Textbook Exercise 6.2 Using SMAC to Spoof Your MAC Address



Version 6.0.7

Download
Direct Download

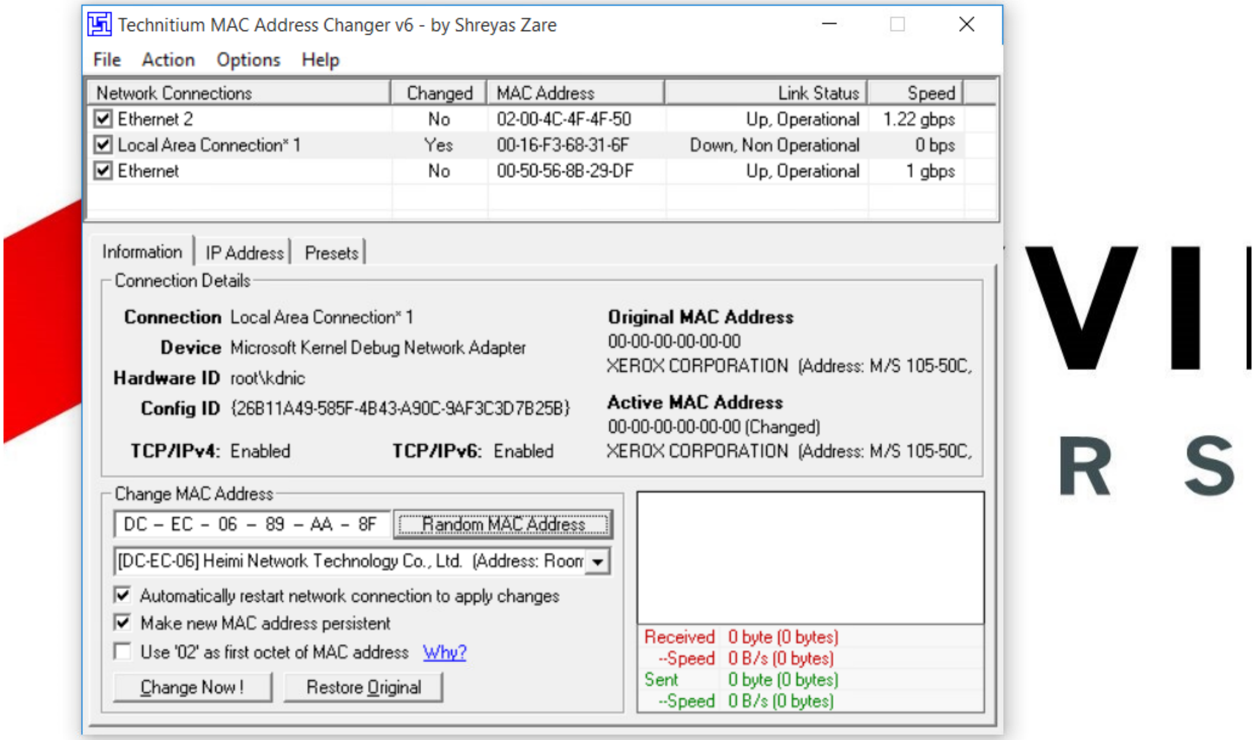
Official Torrent
Download Torrent

System Requirements
Windows 10/8.1/8/7/Vista/XP/Server 2012 R2/Server 2012/Server 2008 R2/Server 2008/Server 2003/Server 2000

What's New?
Read this blog post to know what's new in this release.

File Details

Name	TMACv6.0.7_Setup.zip
Format	ZIP File
Size	2.10 MB
SHA1	7585C61B 7F2557F8 5FCAF82D 1FB1080F A947BCE0
SHA256	6E63BECA F5C5E17A 9D3AFB6E 2104EEE3 DBE473C8 930AE878 3EBA0FED ADB4A152



Network Connections	Changed	MAC Address	Link Status	Speed
☑ Ethernet 2	No	02-00-4C-4F-4F-50	Up, Operational	1.22 gbps
☑ Local Area Connection* 1	Yes	00-16-F3-68-31-6F	Down, Non Operational	0 bps
☑ Ethernet	No	00-50-56-8B-29-DF	Up, Operational	1 gbps

Information | IP Address | Presets

Connection Details

Connection Local Area Connection* 1

Device Microsoft Kernel Debug Network Adapter

Hardware ID root\kdnic

Config ID {26B11A49-585F-4B43-A90C-9AF3C3D7B25B}

TCP/IPv4: Enabled **TCP/IPv6:** Enabled

Original MAC Address
00-00-00-00-00-00
XEROX CORPORATION (Address: M/S 105-50C,

Active MAC Address
00-00-00-00-00-00 (Changed)
XEROX CORPORATION (Address: M/S 105-50C,

Change MAC Address

DC – EC – 06 – 89 – AA – 8F [Random MAC Address]

[DC-EC-06] Heimi Network Technology Co., Ltd. (Address: Roon

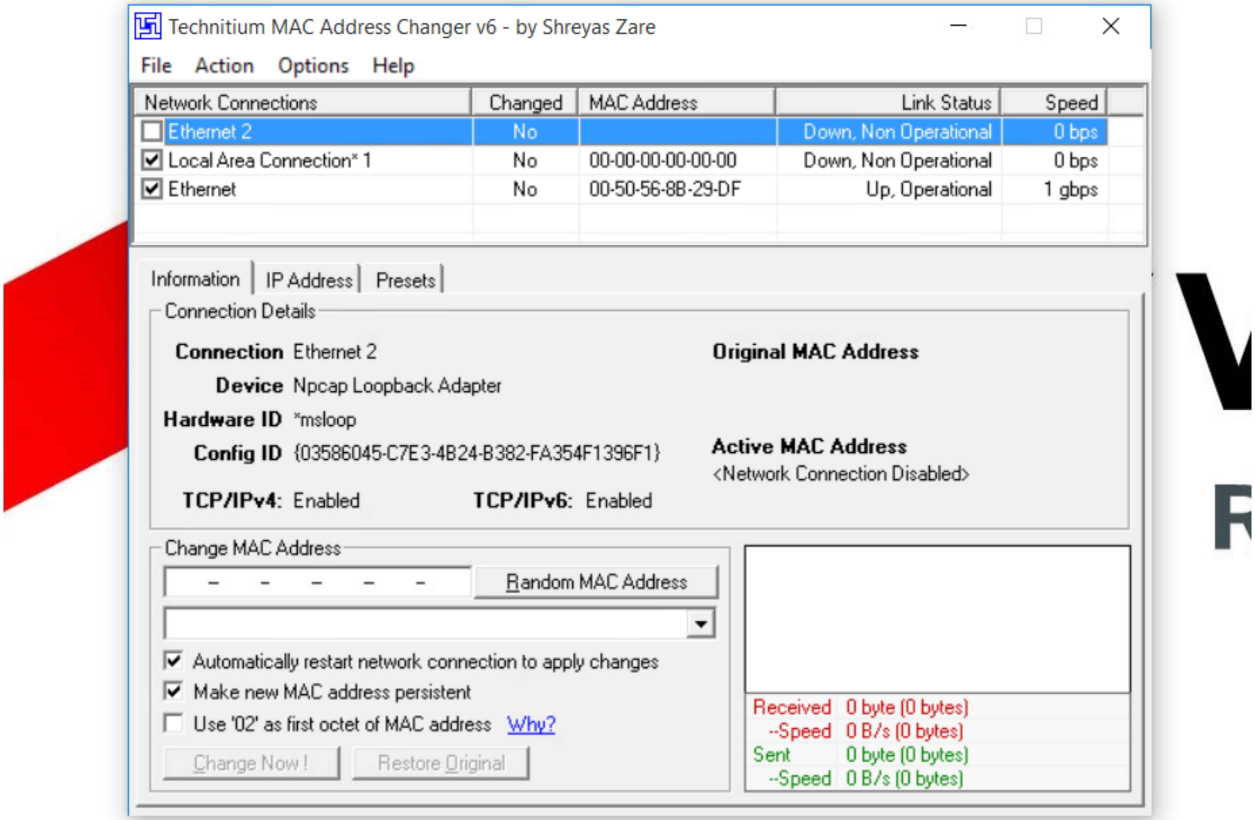
☑ Automatically restart network connection to apply changes

☑ Make new MAC address persistent

☐ Use '02' as first octet of MAC address Why?

[Change Now !] [Restore Original]

Received 0 byte (0 bytes)
--Speed 0 B/s (0 bytes)
Sent 0 byte (0 bytes)
--Speed 0 B/s (0 bytes)



Network Connections	Changed	MAC Address	Link Status	Speed
□ Ethernet 2	No		Down, Non Operational	0 bps
☑ Local Area Connection* 1	No	00-00-00-00-00-00	Down, Non Operational	0 bps
☑ Ethernet	No	00-50-56-8B-29-DF	Up, Operational	1 gbps

Connection Details

Connection Ethernet 2

Device Npcap Loopback Adapter

Hardware ID *msloop

Config ID {03586045-C7E3-4B24-B382-FA354F1396F1}

TCP/IPv4: Enabled **TCP/IPv6:** Enabled

Original MAC Address

Active MAC Address
<Network Connection Disabled>

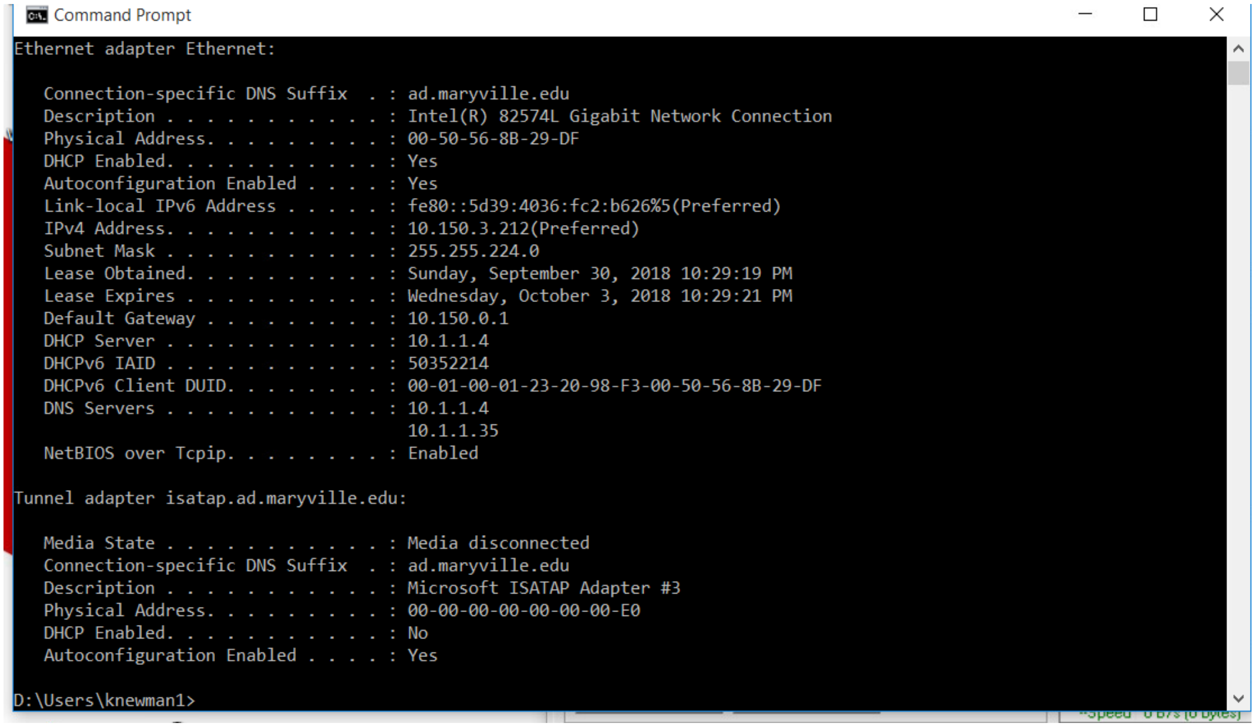
Change MAC Address

☑ Automatically restart network connection to apply changes

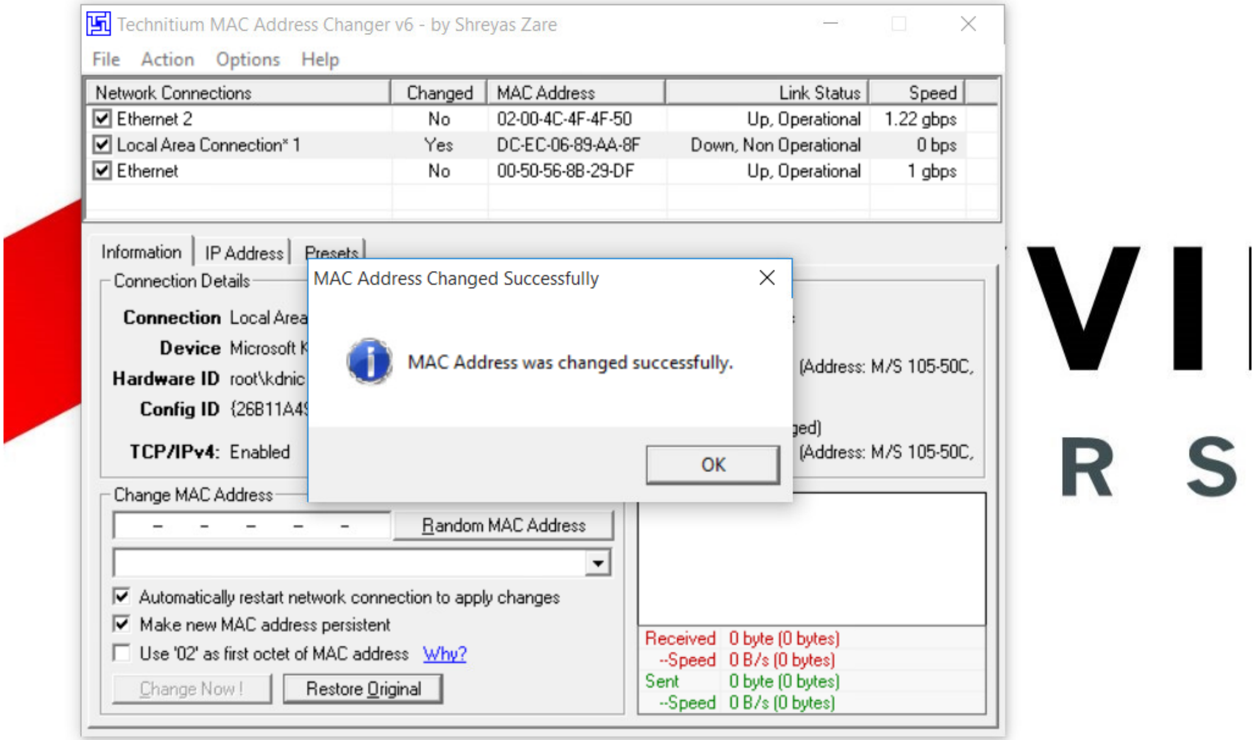
☑ Make new MAC address persistent

□ Use '02' as first octet of MAC address

Received	0 byte (0 bytes)
--Speed	0 B/s (0 bytes)
Sent	0 byte (0 bytes)
--Speed	0 B/s (0 bytes)



```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : ad.maryville.edu
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-50-56-8B-29-DF
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::5d39:4036:fc2:b626%5(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.150.3.212(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.224.0
   Lease Obtained. . . . . . . . . . : Sunday, September 30, 2018 10:29:19 PM
   Lease Expires . . . . . . . . . . : Wednesday, October 3, 2018 10:29:21 PM
   Default Gateway . . . . . . . . . : 10.150.0.1
   DHCP Server . . . . . . . . . . . : 10.1.1.4
   DHCPv6 IAID . . . . . . . . . . . : 50352214
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-23-20-98-F3-00-50-56-8B-29-DF
   DNS Servers . . . . . . . . . . . : 10.1.1.4
                                       10.1.1.35
   NetBIOS over Tcpip. . . . . . . . : Enabled

Tunnel adapter isatap.ad.maryville.edu:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : ad.maryville.edu
   Description . . . . . . . . . . . : Microsoft ISATAP Adapter #3
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes

D:\Users\knewman1>
```



Network Connections	Changed	MAC Address	Link Status	Speed
☑ Ethernet 2	No	02-00-4C-4F-4F-50	Up, Operational	1.22 gbps
☑ Local Area Connection* 1	Yes	DC-EC-06-89-AA-8F	Down, Non Operational	0 bps
☑ Ethernet	No	00-50-56-8B-29-DF	Up, Operational	1 gbps

Connection Local Area
Device Microsoft K
Hardware ID root\kdnic
Config ID {26B11A4
TCP/IPv4: Enabled

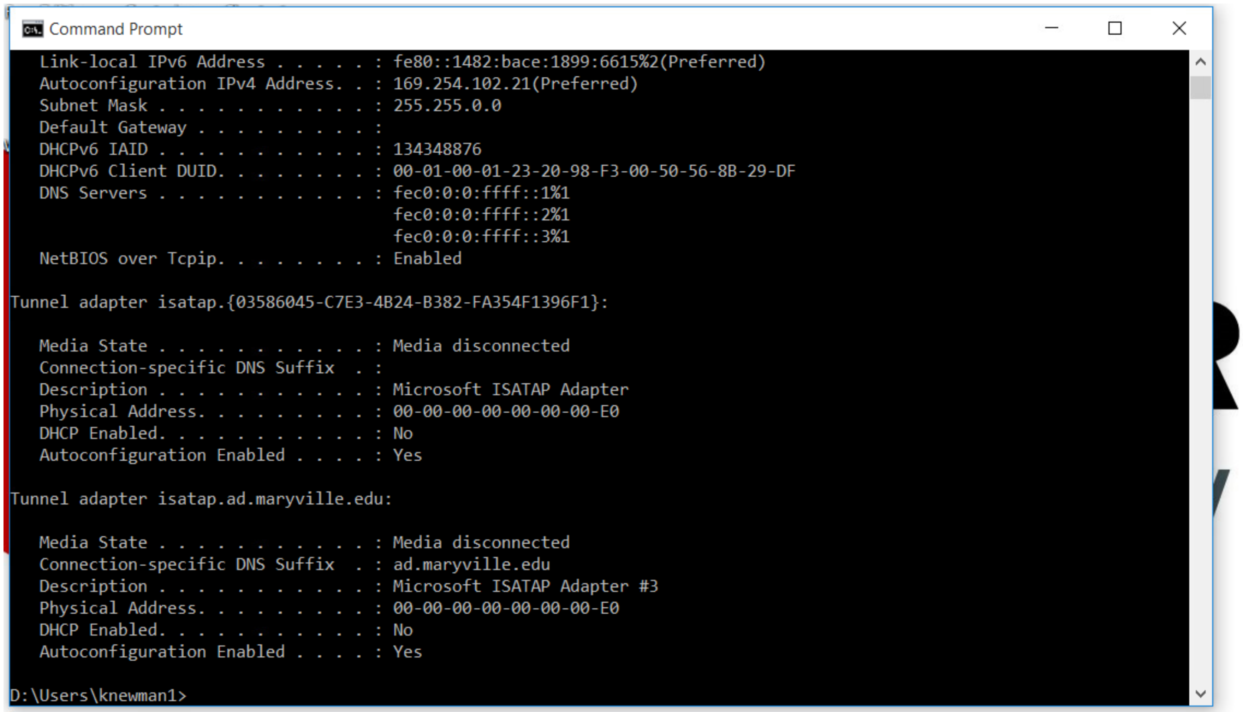
(Address: M/S 105-50C,
ged)
(Address: M/S 105-50C,

MAC Address Changed Successfully

MAC Address was changed successfully.

☑ Automatically restart network connection to apply changes
☑ Make new MAC address persistent
□ Use '02' as first octet of MAC address Why?

Received 0 byte (0 bytes)
--Speed 0 B/s (0 bytes)
Sent 0 byte (0 bytes)
--Speed 0 B/s (0 bytes)



```
   Link-local IPv6 Address . . . . . : fe80::1482:bace:1899:6615%2(Preferred)
   Autoconfiguration IPv4 Address. . : 169.254.102.21(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 134348876
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-23-20-98-F3-00-50-56-8B-29-DF
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Tunnel adapter isatap.{03586045-C7E3-4B24-B382-FA354F1396F1}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft ISATAP Adapter
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes

Tunnel adapter isatap.ad.maryville.edu:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : ad.maryville.edu
   Description . . . . . . . . . . . : Microsoft ISATAP Adapter #3
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes

D:\Users\knewman1>
```

Deliverable (not in Course Textbook)

IMPORTANT NOTE

EICAR cannot be held responsible when these files or your AV scanner in combination with these files cause any damage to your computer. **YOU DOWNLOAD THESE FILES AT YOUR OWN RISK.** Download these files only if you are sufficiently secure in the usage of your AV scanner. EICAR cannot and will not provide any help to remove these files from your computer. Please contact the manufacturer/vendor of your AV scanner to seek such help.

Download area using the standard protocol http

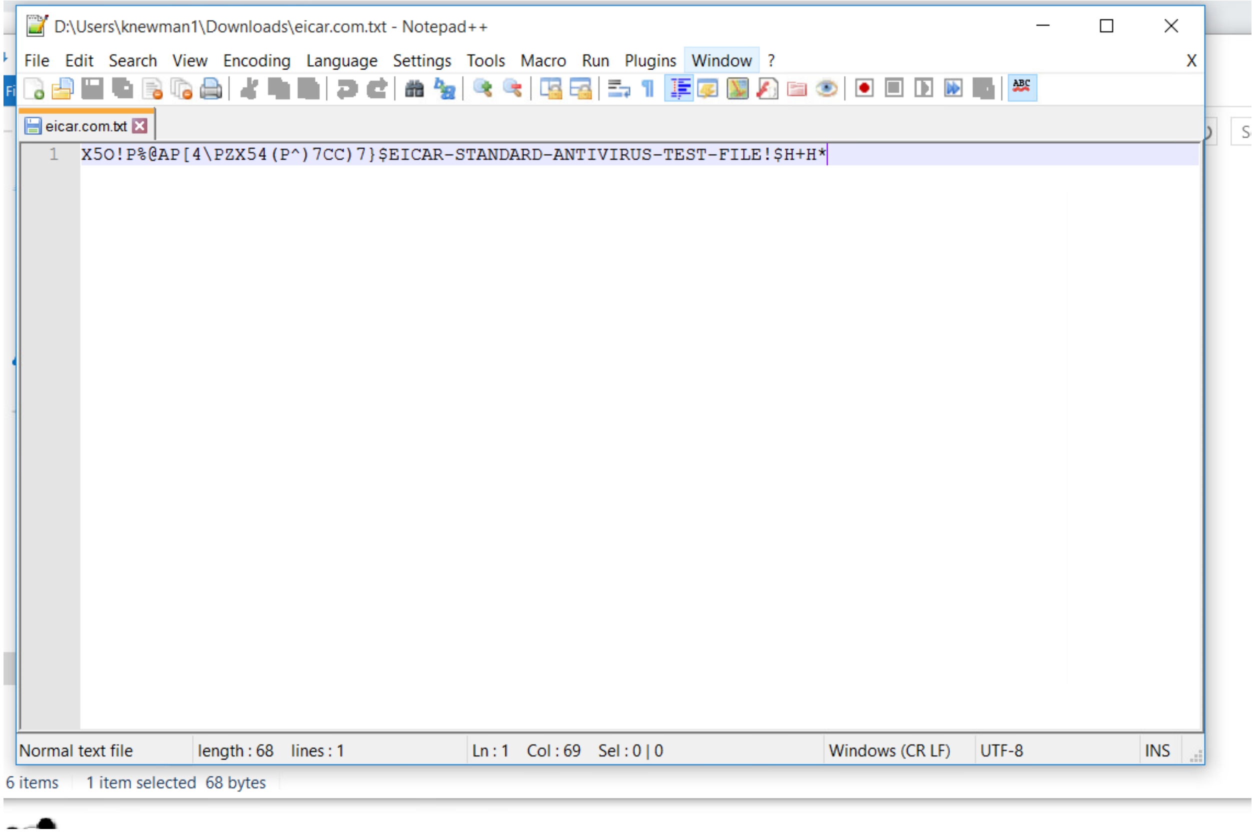
eicar.com 68 Bytes	eicar.com.txt 68 Bytes	eicar_com.zip 184 Bytes	eicarcom2.zip 308 Bytes

Download area using the secure, SSL enabled protocol https

eicar.com 68 Bytes	eicar.com.txt 68 Bytes	eicar_com.zip 184 Bytes	eicarcom2.zip 308 Bytes

How to delete the test file from your PC

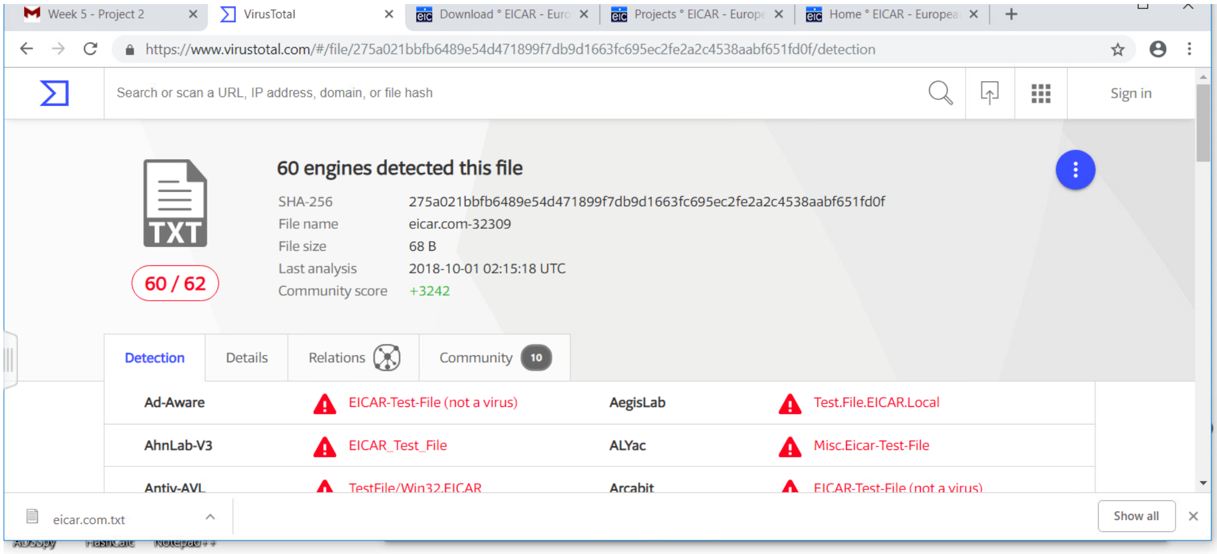
We understand (from the many emails we receive) that it might be difficult for you to delete the test file from your



```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Normal text file | length : 68 lines : 1 | Ln : 1 Col : 69 Sel : 0 | 0 | Windows (CR LF) | UTF-8 | INS

6 items 1 item selected 68 bytes



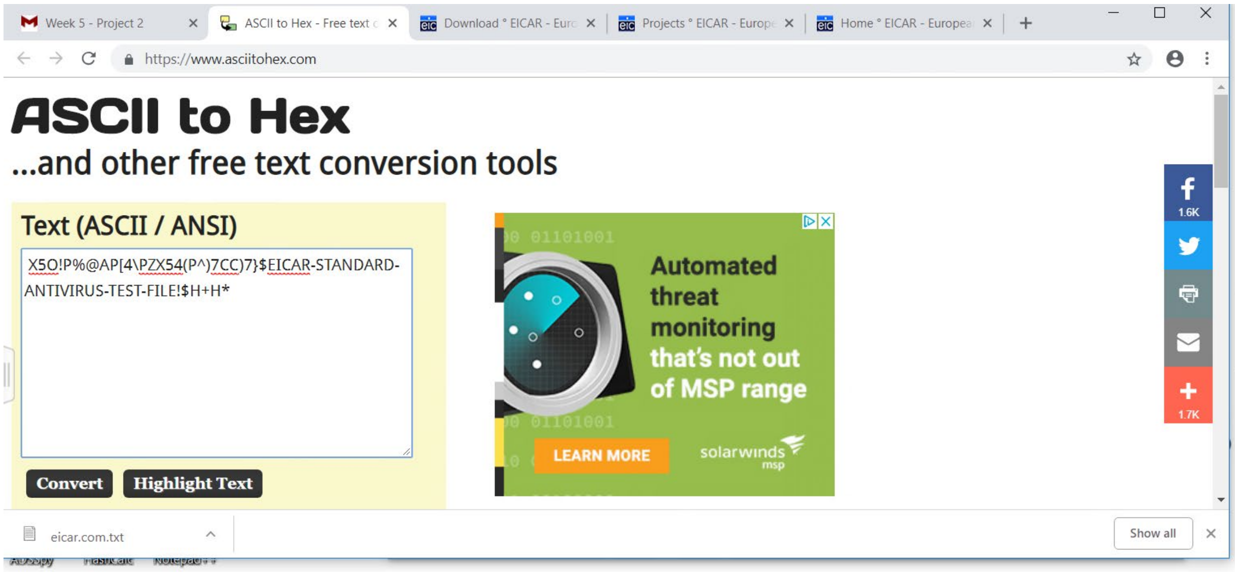
https://www.virustotal.com/#/file/275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f/detection

60 engines detected this file

60 / 62

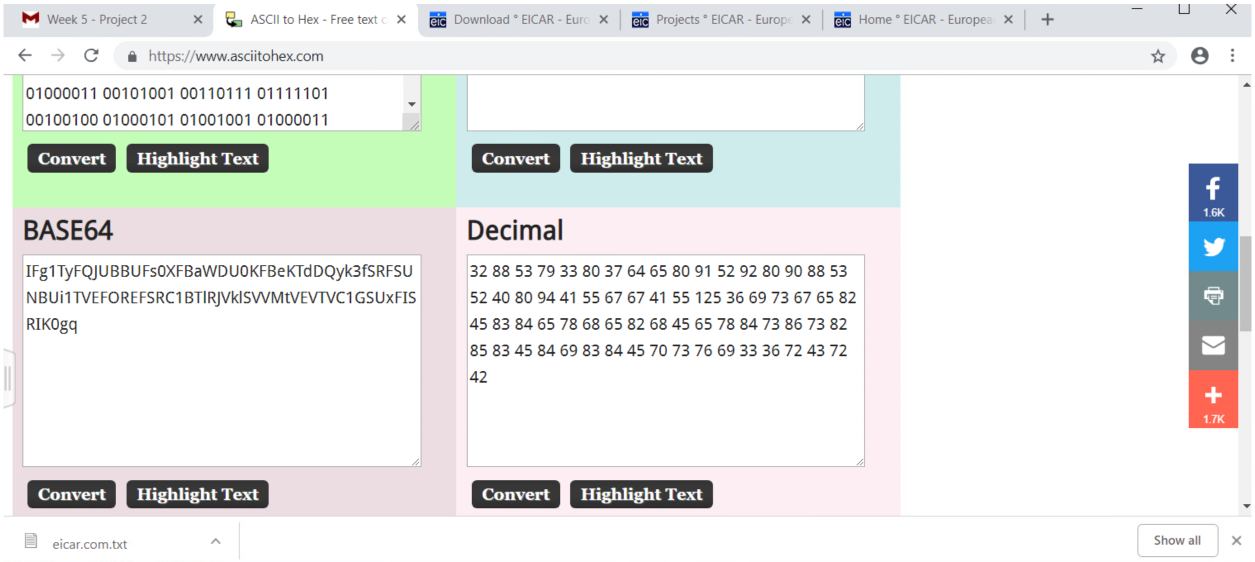
SHA-256 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f
File name eicar.com-32309
File size 68 B
Last analysis 2018-10-01 02:15:18 UTC
Community score +3242

Ad-Aware	EICAR-Test-File (not a virus)	AegisLab	Test.File.EICAR.Local
AhnLab-V3	EICAR_Test_File	ALYac	Misc.Eicar-Test-File
Antiy-AVL	TestFile/Win32.EICAR	Arcabit	EICAR-Test-File (not a virus)


Week 5 - Project 2
ASCII to Hex - Free text c
Download ° EICAR - Euro
Projects ° EICAR - Europe
Home ° EICAR - Europea
https://www.asciitohex.com
ASCII to Hex
...and other free text conversion tools
Automated threat monitoring that's not out of MSP range
LEARN MORE
solarwinds msp
1.6K
1.7K
eicar.com.txt
Show all

Text (ASCII / ANSI)

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```



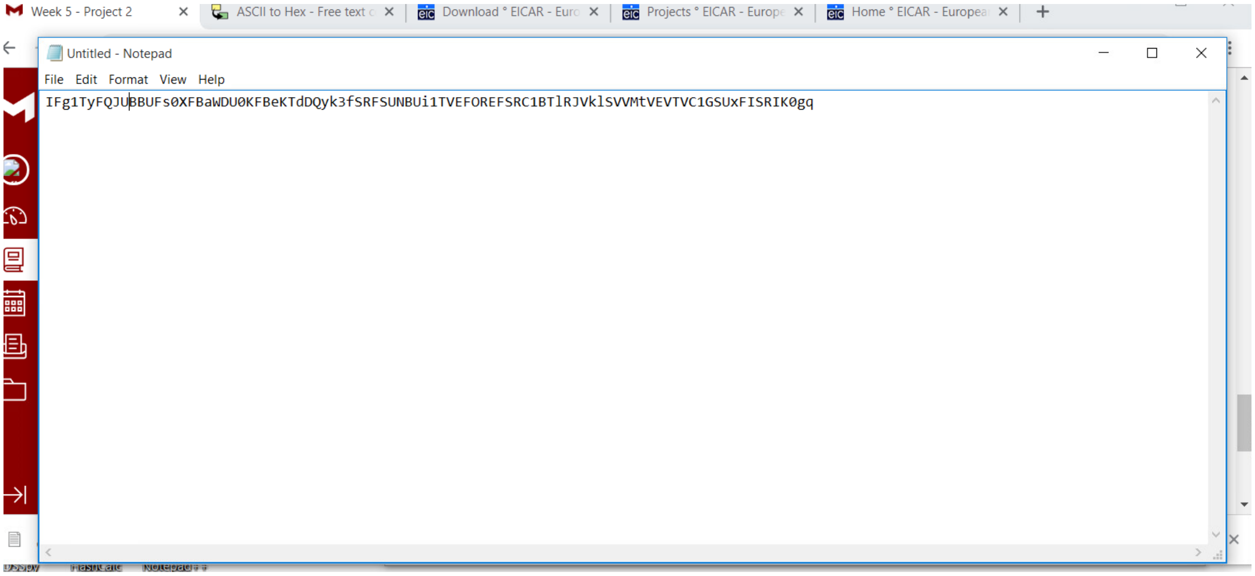
```
01000011 00101001 00110111 01111101
00100100 01000101 01001001 01000011
```

BASE64

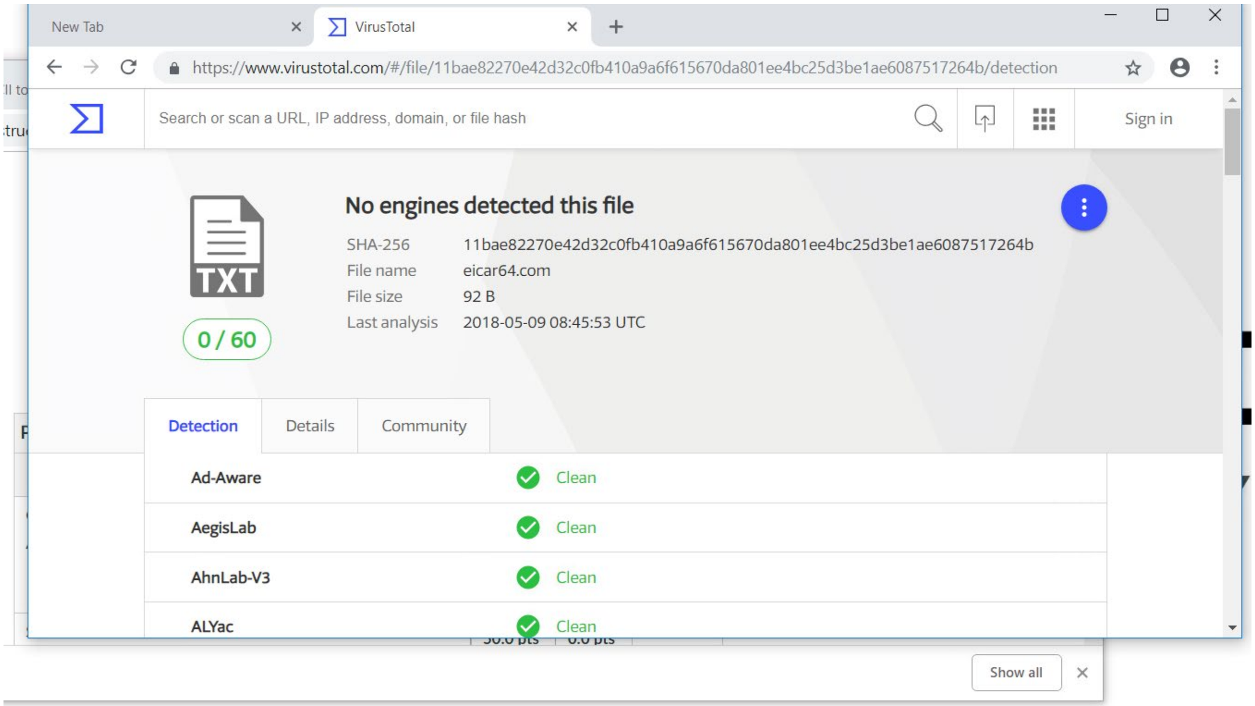
```
IFg1TyFQJUBBUFs0XFBaWDU0KFBeKTdDQyk3fSRFSU
NBUi1TVEFOREFSRC1BTlRJVklSVVMtVEVTVC1GSUxFIS
RIK0gq
```

Decimal

```
32 88 53 79 33 80 37 64 65 80 91 52 92 80 90 88 53
52 40 80 94 41 55 67 67 41 55 125 36 69 73 67 65 82
45 83 84 65 78 68 65 82 68 45 65 78 84 73 86 73 82
85 83 45 84 69 83 84 45 70 73 76 69 33 36 72 43 72
42
```



IFg1TyFQJUBBUFs0XFBaWDU0KFBeKTdDQyk3fSRFSUNBUi1TVEFOREFSRC1BTlRJVklSVVMtVEVTVC1GSUxFISRIK0gq


New Tab
VirusTotal
https://www.virustotal.com/#/file/11bae82270e42d32c0fb410a9a6f615670da801ee4bc25d3be1ae6087517264b/detection
Search or scan a URL, IP address, domain, or file hash
Sign in
TXT
Detection
Details
Community
Show all

No engines detected this file

0 / 60

SHA-256	11bae82270e42d32c0fb410a9a6f615670da801ee4bc25d3be1ae6087517264b
File name	eicar64.com
File size	92 B
Last analysis	2018-05-09 08:45:53 UTC

Ad-Aware	✓ Clean
AegisLab	✓ Clean
AhnLab-V3	✓ Clean
ALYac	✓ Clean