DIGITAL FORENSICS II
EXPERIMENT 7

Submitted to: Mr. Keshav Kaushik
Submitted by: Kashish Srivastava
R134218079
500067405

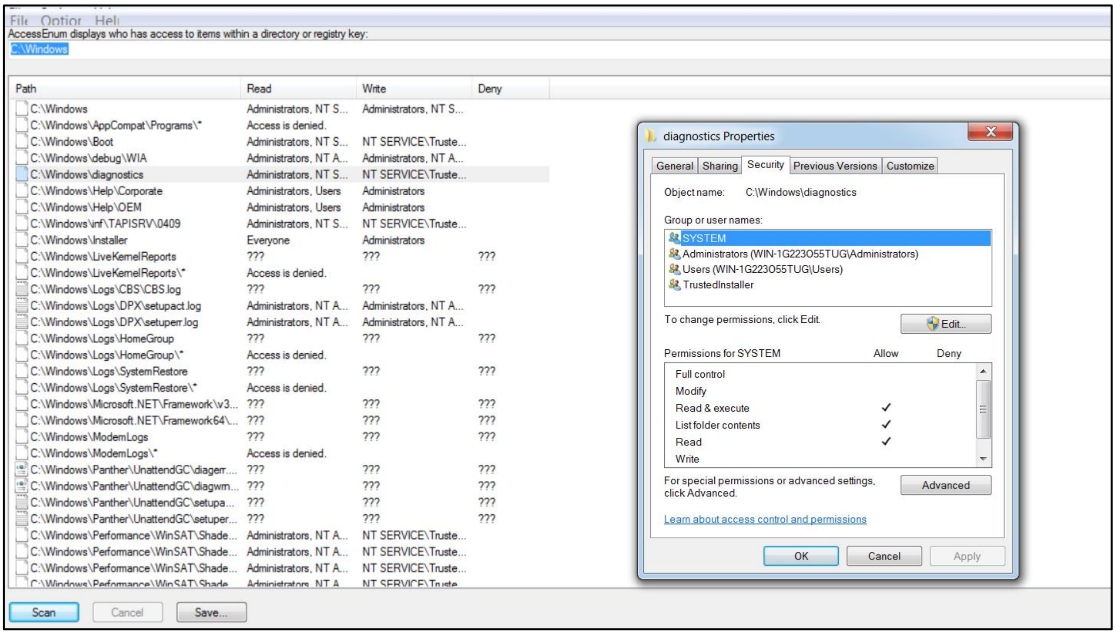
Aim: Forensics using SysInternals tool.

Tools Description: 10 tools of Sysinternals have been mentioned below -

- AccessEnum
- Cacheset
- Autologon
- PsLoglist
- Loadorder
- Bginfo
- TCPview
- CPU stres
- Disk2vhd
- PsService

❖ AccessEnum v1.32

AccessEnum gives us a full view of our file system and Registry security settings in seconds, making it the ideal tool for helping us find security holes and lock down permissions where necessary. It uses standard Windows security APIs to populate its listview with read, write and deny access information.



AccessEnum displays who has access to items within a directory or registry key:
C:\Windows

Path	Read	Write	Deny
C:\Windows	Administrators, NT S...	Administrators, NT S...	
C:\Windows\AppCompat\Programs\*	Access is denied.		
C:\Windows\Boot	Administrators, NT S...	NT SERVICE\Truste...	
C:\Windows\debug\WIA	Administrators, NT A...	Administrators, NT A...	
C:\Windows\diagnostics	Administrators, NT S...	NT SERVICE\Truste...	
C:\Windows\Help\Corporate	Administrators, Users	Administrators	
C:\Windows\Help\OEM	Administrators, Users	Administrators	
C:\Windows\inf\TAPISRV\0409	Administrators, NT S...	NT SERVICE\Truste...	
C:\Windows\Installer	Everyone	Administrators	
C:\Windows\LiveKernelReports	???	???	???
C:\Windows\LiveKernelReports\*	Access is denied.		
C:\Windows\Logs\CBS\CBS.log	???	???	???
C:\Windows\Logs\DPX\setupact.log	Administrators, NT A...	Administrators, NT A...	
C:\Windows\Logs\DPX\setuperr.log	Administrators, NT A...	Administrators, NT A...	
C:\Windows\Logs\HomeGroup	???	???	???
C:\Windows\Logs\HomeGroup\*	Access is denied.		
C:\Windows\Logs\SystemRestore	???	???	???
C:\Windows\Logs\SystemRestore\*	Access is denied.		
C:\Windows\Microsoft.NET\Framework\v3...	???	???	???
C:\Windows\Microsoft.NET\Framework64\...	???	???	???
C:\Windows\ModemLogs	???	???	???
C:\Windows\ModemLogs\*	Access is denied.		
C:\Windows\Panther\UnattendGC\diagerr....	???	???	???
C:\Windows\Panther\UnattendGC\diagwrn...	???	???	???
C:\Windows\Panther\UnattendGC\setupa...	???	???	???
C:\Windows\Panther\UnattendGC\setuper...	???	???	???
C:\Windows\Performance\WinSAT\Shade...	Administrators, NT A...	NT SERVICE\Truste...	
C:\Windows\Performance\WinSAT\Shade...	Administrators, NT A...	NT SERVICE\Truste...	
C:\Windows\Performance\WinSAT\Shade...	Administrators, NT A...	NT SERVICE\Truste...	
C:\Windows\Performance\WinSAT\Shade...	Administrators, NT A...	NT SERVICE\Truste...	

diagnostics Properties

General | Sharing | Security | Previous Versions | Customize

Object name: C:\Windows\diagnostics

Group or user names:
SYSTEM
Administrators (WIN-1G223O55TUG\Administrators)
Users (WIN-1G223O55TUG\Users)
TrustedInstaller

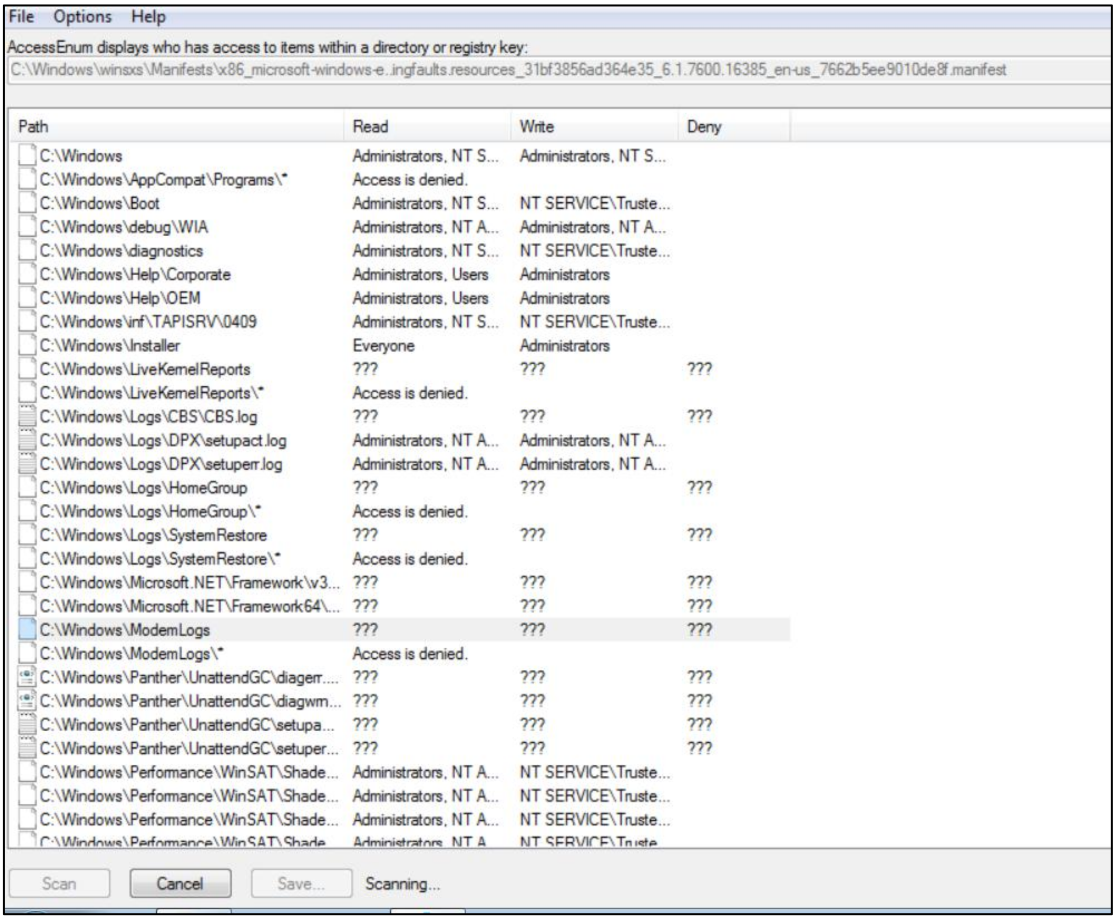
To change permissions, click Edit. [Edit...]

Permissions for SYSTEM	Allow	Deny
Full control		
Modify		
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write		

For special permissions or advanced settings, click Advanced. [Advanced]

Learn about access control and permissions

[OK] [Cancel] [Apply]



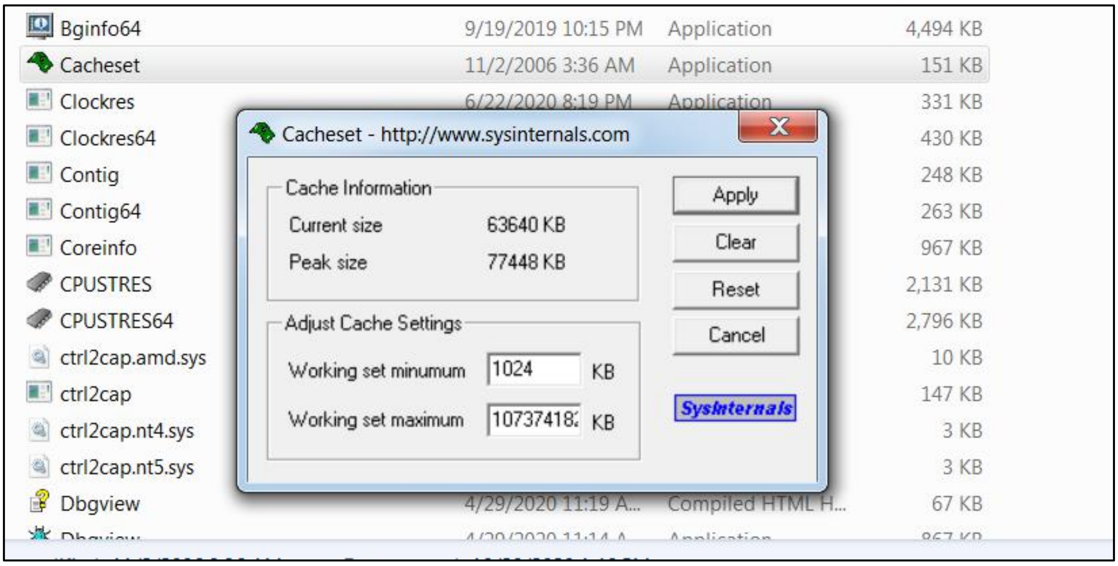
AccessEnum displays who has access to items within a directory or registry key:

C:\Windows\winsxs\Manifests\x86_microsoft-windows-e..ingfaults.resources_31bf3856ad364e35_6.1.7600.16385_en-us_7662b5ee9010de8f.manifest

Path	Read	Write	Deny
C:\Windows	Administrators, NT S...	Administrators, NT S...	
C:\Windows\AppCompat\Programs\*	Access is denied.		
C:\Windows\Boot	Administrators, NT S...	NT SERVICE\Truste...	
C:\Windows\debug\WIA	Administrators, NT A...	Administrators, NT A...	
C:\Windows\diagnostics	Administrators, NT S...	NT SERVICE\Truste...	
C:\Windows\Help\Corporate	Administrators, Users	Administrators	
C:\Windows\Help\OEM	Administrators, Users	Administrators	
C:\Windows\inf\TAPISRV\0409	Administrators, NT S...	NT SERVICE\Truste...	
C:\Windows\Installer	Everyone	Administrators	
C:\Windows\LiveKernelReports	???	???	???
C:\Windows\LiveKernelReports\*	Access is denied.		
C:\Windows\Logs\CBS\CBS.log	???	???	???
C:\Windows\Logs\DPX\setupact.log	Administrators, NT A...	Administrators, NT A...	
C:\Windows\Logs\DPX\setuperr.log	Administrators, NT A...	Administrators, NT A...	
C:\Windows\Logs\HomeGroup	???	???	???
C:\Windows\Logs\HomeGroup\*	Access is denied.		
C:\Windows\Logs\SystemRestore	???	???	???
C:\Windows\Logs\SystemRestore\*	Access is denied.		
C:\Windows\Microsoft.NET\Framework\v3...	???	???	???
C:\Windows\Microsoft.NET\Framework64\...	???	???	???
C:\Windows\ModemLogs	???	???	???
C:\Windows\ModemLogs\*	Access is denied.		
C:\Windows\Panther\UnattendGC\diagerr....	???	???	???
C:\Windows\Panther\UnattendGC\diagwrn...	???	???	???
C:\Windows\Panther\UnattendGC\setupa...	???	???	???
C:\Windows\Panther\UnattendGC\setuper...	???	???	???
C:\Windows\Performance\WinSAT\Shade...	Administrators, NT A...	NT SERVICE\Truste...	
C:\Windows\Performance\WinSAT\Shade...	Administrators, NT A...	NT SERVICE\Truste...	
C:\Windows\Performance\WinSAT\Shade...	Administrators, NT A...	NT SERVICE\Truste...	
C:\Windows\Performance\WinSAT\Shade...	Administrators, NT A...	NT SERVICE\Truste...	

❖ CacheSet v1.0

CacheSet is an applet that allows us to manipulate the working-set parameters of the system file cache. Unlike CacheMan, *CacheSet* runs on all versions of NT and will work without modifications on new Service Pack releases. In addition to providing us the ability to control the minimum and maximum working set sizes, it also allows us to reset the Cache's working set, forcing it to grow as necessary from a minimal starting point.



Bginfo64	9/19/2019 10:15 PM	Application	4,494 KB
Cacheset	11/2/2006 3:36 AM	Application	151 KB
Clockres	6/22/2020 8:19 PM	Application	331 KB
Clockres64			430 KB
Contig			248 KB
Contig64			263 KB
Coreinfo			967 KB
CPUSTRES			2,131 KB
CPUSTRES64			2,796 KB
ctrl2cap.amd.sys			10 KB
ctrl2cap			147 KB
ctrl2cap.nt4.sys			3 KB
ctrl2cap.nt5.sys			3 KB
Dbgview	4/29/2020 11:19 A...	Compiled HTML H...	67 KB
Dbgview	4/29/2020 11:14 A...	Application	867 KB

Cacheset - http://www.sysinternals.com

Cache Information

Current size 63640 KB

Peak size 77448 KB

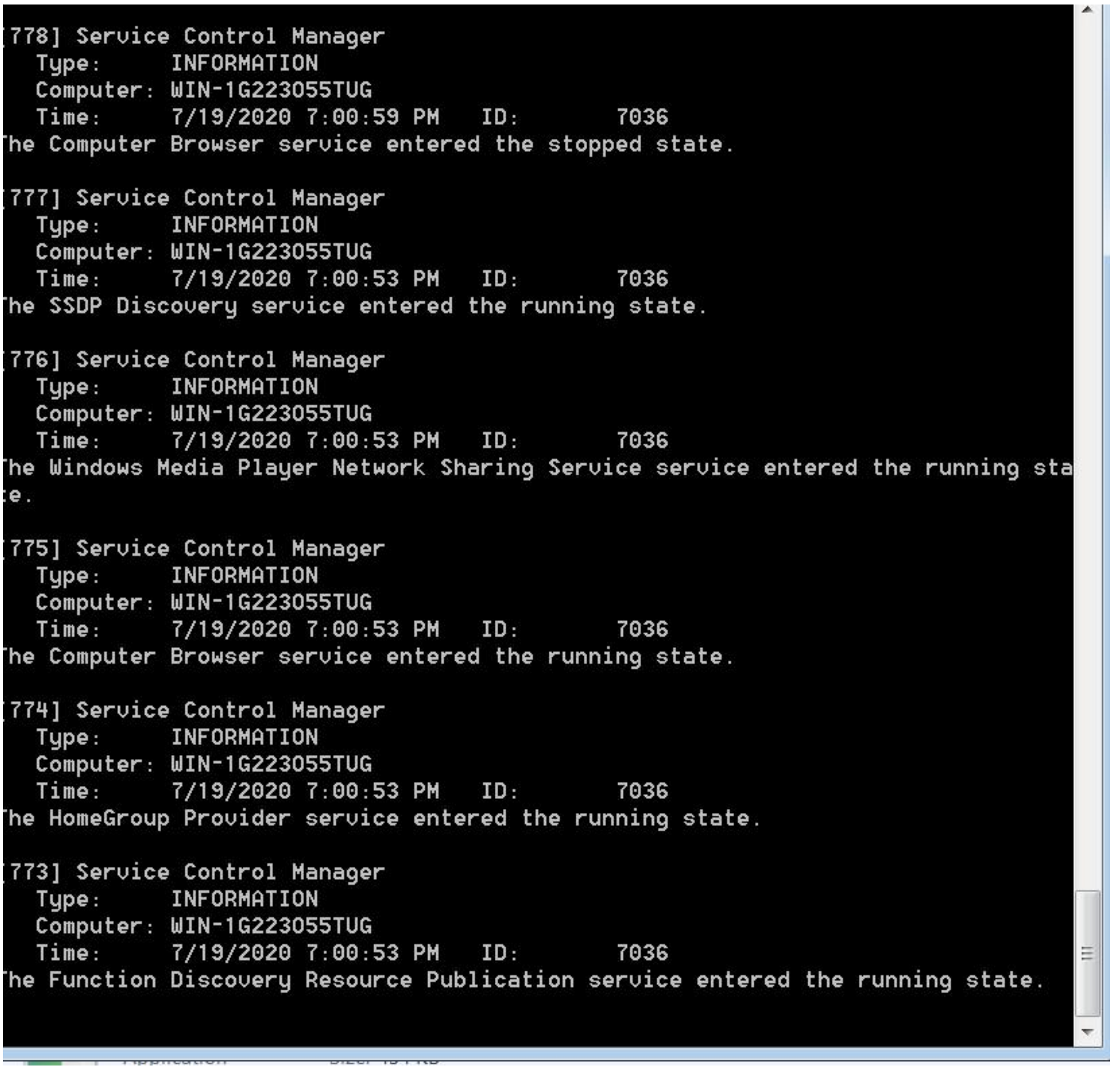
Adjust Cache Settings

Working set minumum 1024 KB

Working set maximum 10737418 KB

❖ PsLogList v2.81

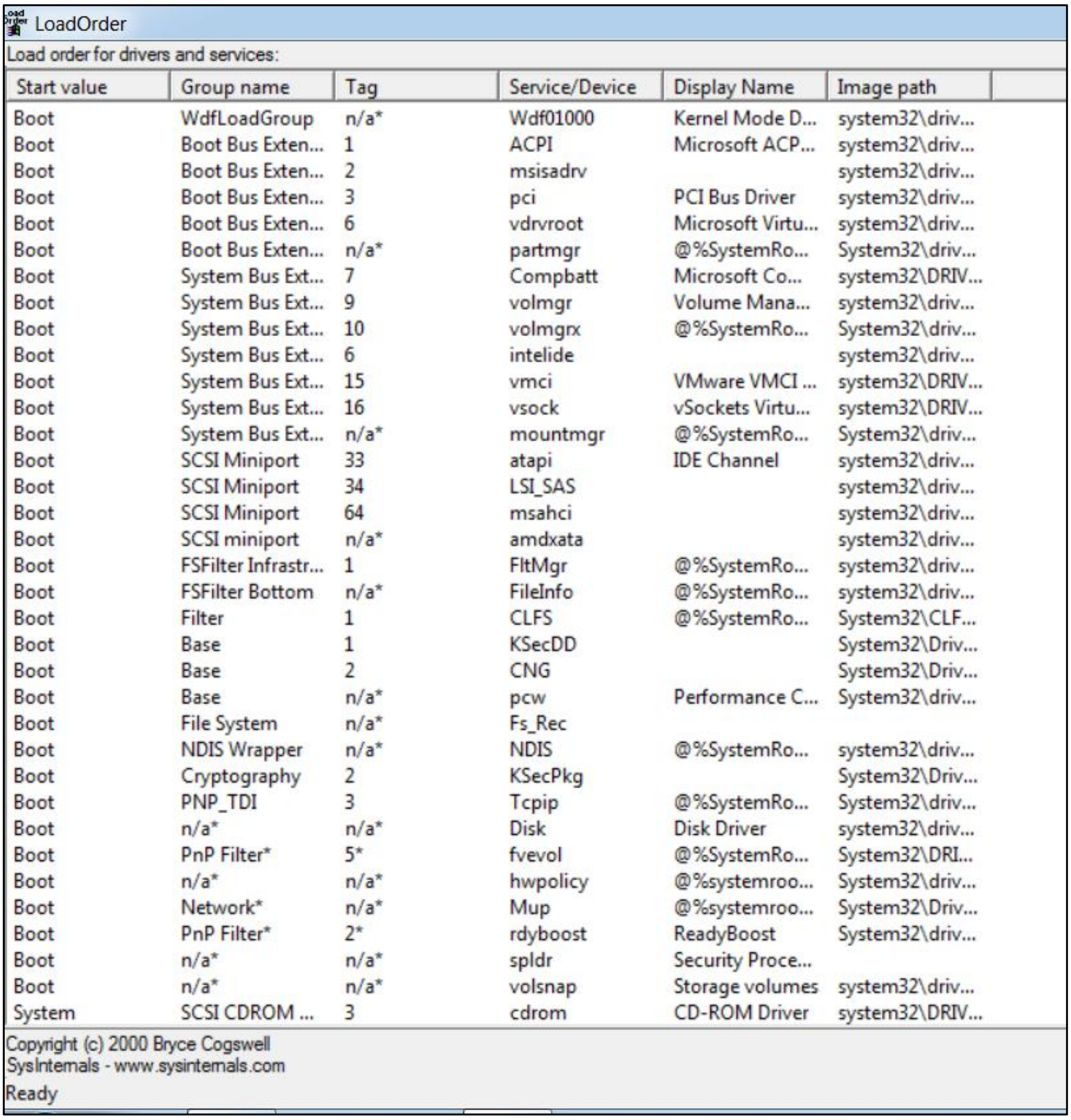
PsLogList is a clone of elogdump except that *PsLogList* lets us login to remote systems in situations usr current set of security credentials would not permit access to the Event Log, and *PsLogList* retrieves message strings from the computer on which the event log us view resides.



```
[778] Service Control Manager
  Type:     INFORMATION
  Computer: WIN-1G223O55TUG
  Time:     7/19/2020 7:00:59 PM   ID:      7036
he Computer Browser service entered the stopped state.

[777] Service Control Manager
  Type:     INFORMATION
  Computer: WIN-1G223O55TUG
  Time:     7/19/2020 7:00:53 PM   ID:      7036
he SSDP Discovery service entered the running state.

[776] Service Control Manager
  Type:     INFORMATION
  Computer: WIN-1G223O55TUG
  Time:     7/19/2020 7:00:53 PM   ID:      7036
he Windows Media Player Network Sharing Service service entered the running sta
e.

[775] Service Control Manager
  Type:     INFORMATION
  Computer: WIN-1G223O55TUG
  Time:     7/19/2020 7:00:53 PM   ID:      7036
he Computer Browser service entered the running state.

[774] Service Control Manager
  Type:     INFORMATION
  Computer: WIN-1G223O55TUG
  Time:     7/19/2020 7:00:53 PM   ID:      7036
he HomeGroup Provider service entered the running state.

[773] Service Control Manager
  Type:     INFORMATION
  Computer: WIN-1G223O55TUG
  Time:     7/19/2020 7:00:53 PM   ID:      7036
he Function Discovery Resource Publication service entered the running state.
```

❖ LoadOrder v1.0

This applet shows us the order that a Windows NT or Windows 2000 system loads device drivers. Note that on Windows 2000 plug-and-play drivers may actually load in a different order than the one calculated, because plug-and-play drivers are loaded on demand during device detection and enumeration.



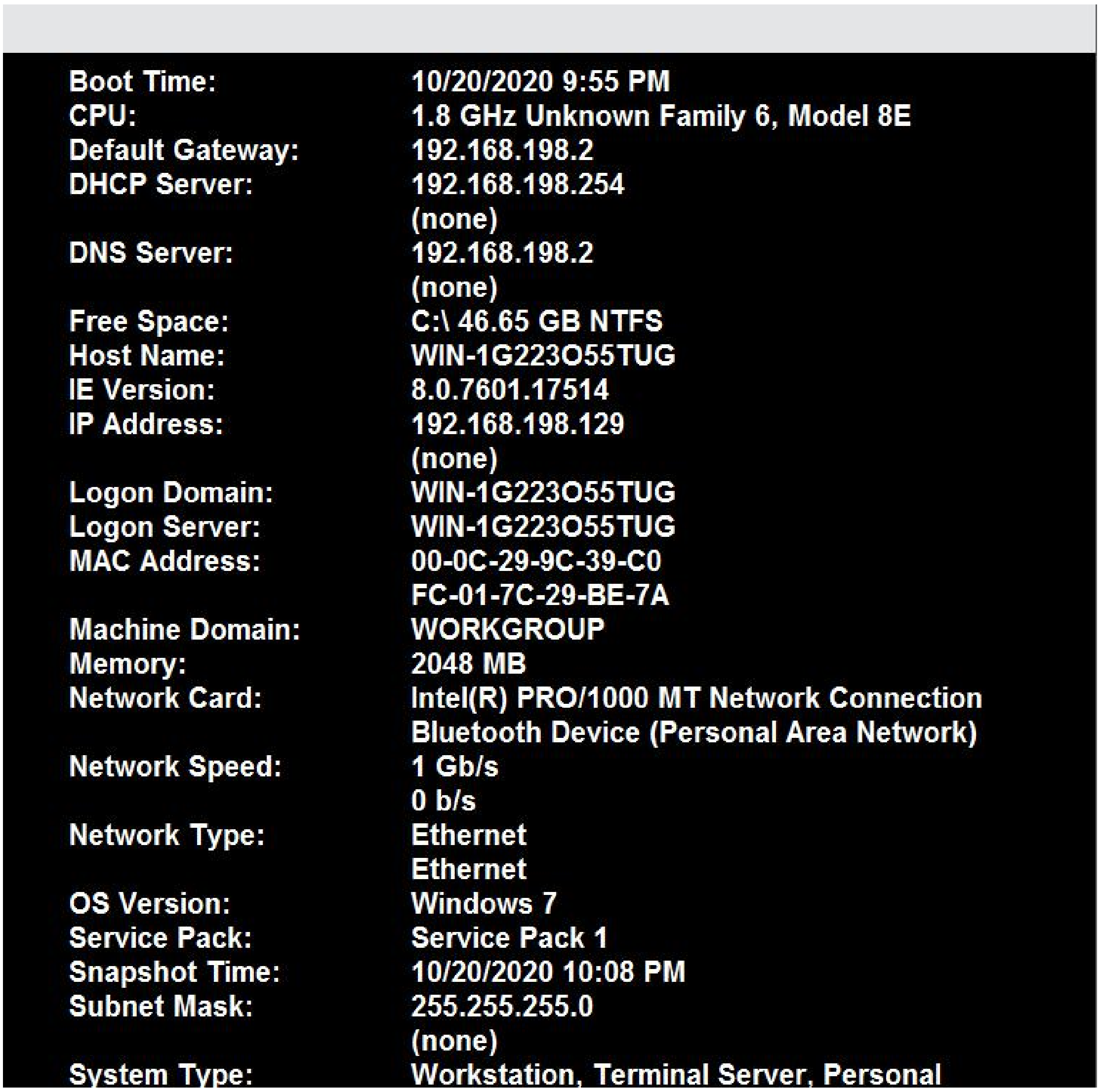
Load order for drivers and services:

Start value	Group name	Tag	Service/Device	Display Name	Image path
Boot	WdfLoadGroup	n/a*	Wdf01000	Kernel Mode D...	system32\driv...
Boot	Boot Bus Exten...	1	ACPI	Microsoft ACP...	system32\driv...
Boot	Boot Bus Exten...	2	msisadrv		system32\driv...
Boot	Boot Bus Exten...	3	pci	PCI Bus Driver	system32\driv...
Boot	Boot Bus Exten...	6	vdrvroot	Microsoft Virtu...	system32\driv...
Boot	Boot Bus Exten...	n/a*	partmgr	@%SystemRo...	System32\driv...
Boot	System Bus Ext...	7	Compbatt	Microsoft Co...	system32\DRIV...
Boot	System Bus Ext...	9	volmgr	Volume Mana...	system32\driv...
Boot	System Bus Ext...	10	volmgrx	@%SystemRo...	System32\driv...
Boot	System Bus Ext...	6	intelide		system32\driv...
Boot	System Bus Ext...	15	vmci	VMware VMCI ...	system32\DRIV...
Boot	System Bus Ext...	16	vsock	vSockets Virtu...	system32\DRIV...
Boot	System Bus Ext...	n/a*	mountmgr	@%SystemRo...	System32\driv...
Boot	SCSI Miniport	33	atapi	IDE Channel	system32\driv...
Boot	SCSI Miniport	34	LSI_SAS		system32\driv...
Boot	SCSI Miniport	64	msahci		system32\driv...
Boot	SCSI miniport	n/a*	amdxata		system32\driv...
Boot	FSFilter Infrastr...	1	FltMgr	@%SystemRo...	system32\driv...
Boot	FSFilter Bottom	n/a*	FileInfo	@%SystemRo...	system32\driv...
Boot	Filter	1	CLFS	@%SystemRo...	System32\CLF...
Boot	Base	1	KSecDD		System32\Driv...
Boot	Base	2	CNG		System32\Driv...
Boot	Base	n/a*	pcw	Performance C...	System32\driv...
Boot	File System	n/a*	Fs_Rec		
Boot	NDIS Wrapper	n/a*	NDIS	@%SystemRo...	system32\driv...
Boot	Cryptography	2	KSecPkg		System32\Driv...
Boot	PNP_TDI	3	Tcpip	@%SystemRo...	System32\driv...
Boot	n/a*	n/a*	Disk	Disk Driver	system32\driv...
Boot	PnP Filter*	5*	fvevol	@%SystemRo...	System32\DRI...
Boot	n/a*	n/a*	hwpolicy	@%systemroo...	System32\driv...
Boot	Network*	n/a*	Mup	@%systemroo...	System32\Driv...
Boot	PnP Filter*	2*	rdyboost	ReadyBoost	System32\driv...
Boot	n/a*	n/a*	spldr	Security Proce...	
Boot	n/a*	n/a*	volsnap	Storage volumes	system32\driv...
System	SCSI CDROM ...	3	cdrom	CD-ROM Driver	system32\DRIV...

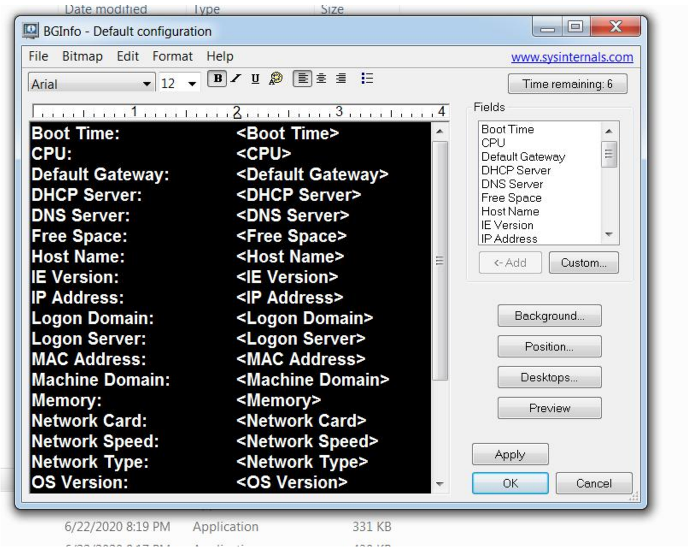
Copyright (c) 2000 Bryce Cogswell
SysInternals - www.sysinternals.com
Ready

- BgInfo v4.28

It automatically displays relevant information about a Windows computer on the desktop's background, such as the computer name, IP address, service pack version, and more. us can edit any field as well as the font and background colors, and can place it in usr startup folder so that it runs every boot, or even configure it to display as the background for the logon screen.



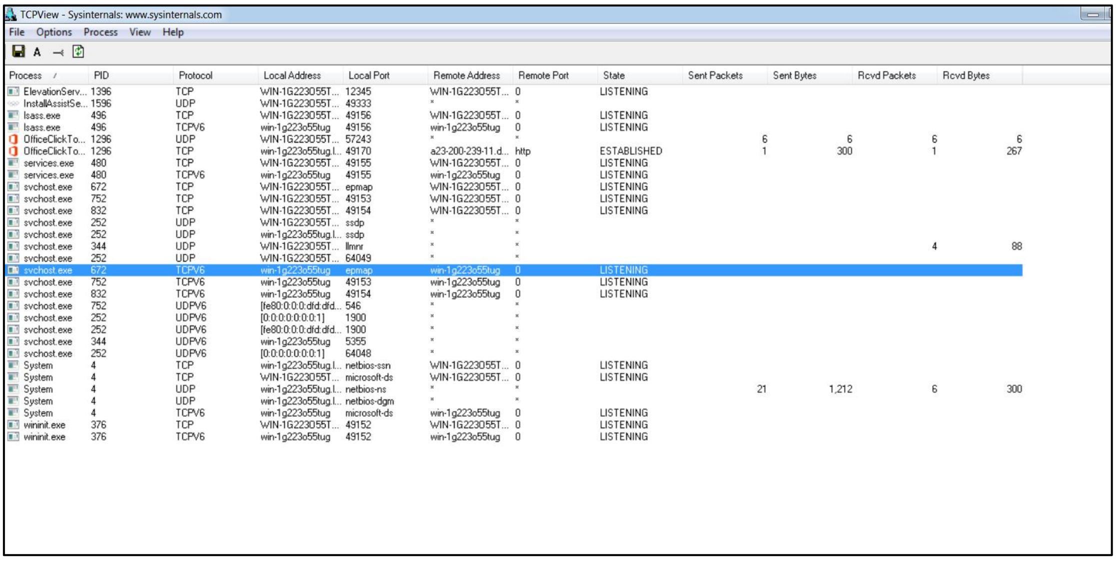
```
Boot Time:          10/20/2020 9:55 PM
CPU:                1.8 GHz Unknown Family 6, Model 8E
Default Gateway:    192.168.198.2
DHCP Server:        192.168.198.254
                    (none)
DNS Server:         192.168.198.2
                    (none)
Free Space:         C:\ 46.65 GB NTFS
Host Name:          WIN-1G223O55TUG
IE Version:         8.0.7601.17514
IP Address:         192.168.198.129
                    (none)
Logon Domain:       WIN-1G223O55TUG
Logon Server:       WIN-1G223O55TUG
MAC Address:        00-0C-29-9C-39-C0
                    FC-01-7C-29-BE-7A
Machine Domain:     WORKGROUP
Memory:             2048 MB
Network Card:       Intel(R) PRO/1000 MT Network Connection
                    Bluetooth Device (Personal Area Network)
Network Speed:      1 Gb/s
                    0 b/s
Network Type:       Ethernet
                    Ethernet
OS Version:         Windows 7
Service Pack:       Service Pack 1
Snapshot Time:      10/20/2020 10:08 PM
Subnet Mask:        255.255.255.0
                    (none)
System Type:        Workstation, Terminal Server, Personal
```



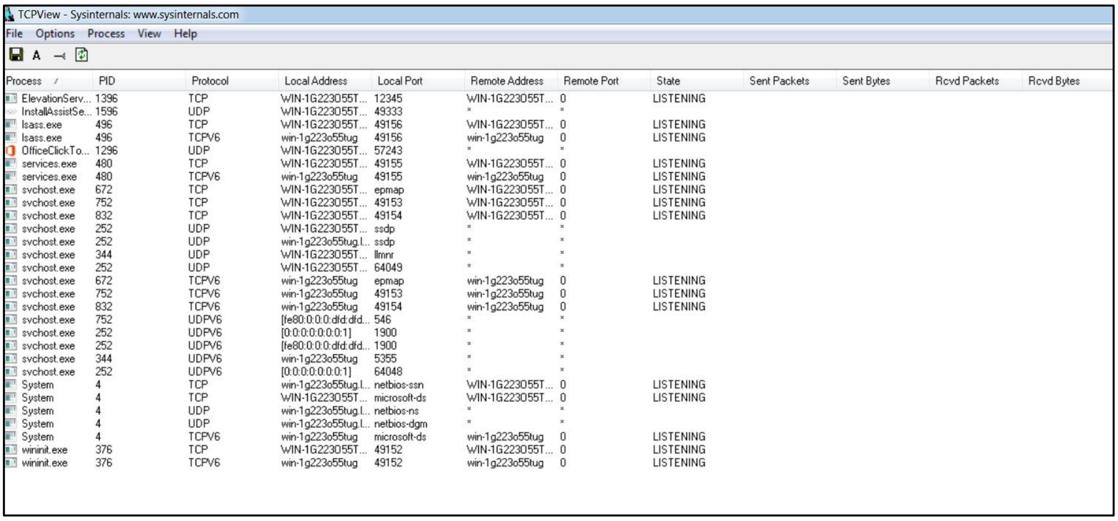
```
Boot Time:          <Boot Time>
CPU:                <CPU>
Default Gateway:    <Default Gateway>
DHCP Server:        <DHCP Server>
DNS Server:         <DNS Server>
Free Space:         <Free Space>
Host Name:          <Host Name>
IE Version:         <IE Version>
IP Address:         <IP Address>
Logon Domain:       <Logon Domain>
Logon Server:       <Logon Server>
MAC Address:        <MAC Address>
Machine Domain:     <Machine Domain>
Memory:             <Memory>
Network Card:       <Network Card>
Network Speed:      <Network Speed>
Network Type:       <Network Type>
OS Version:         <OS Version>
```

❖ TCPView v3.05

TCPView is a Windows program that will show us detailed listings of all TCP and UDP endpoints on usr system, including the local and remote addresses and state of TCP connections. On Windows Server 2008, Vista, and XP, TCPView also reports the name of the process that owns the endpoint. TCPView provides a more informative and conveniently presented subset of the Netstat program that ships with Windows. The TCPView download includes Tcpvcon, a command-line version with the same functionality.



Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
ElevationServ...	1396	TCP	WIN-1G223055T...	12345	WIN-1G223055T...	0	LISTENING				
InstallAssistSe...	1596	UDP	WIN-1G223055T...	49333	*	*					
lsass.exe	496	TCP	WIN-1G223055T...	49156	WIN-1G223055T...	0	LISTENING				
lsass.exe	496	TCPV6	win-1g223o55tug	49156	win-1g223o55tug	0	LISTENING				
OfficeClickTo...	1296	UDP	WIN-1G223055T...	57243	*	*		6	6	6	6
OfficeClickTo...	1296	TCP	win-1g223o55tug.l...	49170	a23-200-239-11.d...	http	ESTABLISHED	1	300	1	267
services.exe	480	TCP	WIN-1G223055T...	49155	WIN-1G223055T...	0	LISTENING				
services.exe	480	TCPV6	win-1g223o55tug	49155	win-1g223o55tug	0	LISTENING				
svchost.exe	672	TCP	WIN-1G223055T...	epmap	WIN-1G223055T...	0	LISTENING				
svchost.exe	752	TCP	WIN-1G223055T...	49153	WIN-1G223055T...	0	LISTENING				
svchost.exe	832	TCP	WIN-1G223055T...	49154	WIN-1G223055T...	0	LISTENING				
svchost.exe	252	UDP	WIN-1G223055T...	ssdp	*	*					
svchost.exe	252	UDP	win-1g223o55tug.l...	ssdp	*	*					
svchost.exe	344	UDP	WIN-1G223055T...	llmnr	*	*				4	88
svchost.exe	252	UDP	WIN-1G223055T...	64049	*	*					
svchost.exe	672	TCPV6	win-1g223o55tug	epmap	win-1g223o55tug	0	LISTENING				
svchost.exe	752	TCPV6	win-1g223o55tug	49153	win-1g223o55tug	0	LISTENING				
svchost.exe	832	TCPV6	win-1g223o55tug	49154	win-1g223o55tug	0	LISTENING				
svchost.exe	752	UDPV6	[fe80:0:0:0:dfd:dfd...	546	*	*					
svchost.exe	252	UDPV6	[0:0:0:0:0:0:0:1]	1900	*	*					
svchost.exe	252	UDPV6	[fe80:0:0:0:dfd:dfd...	1900	*	*					
svchost.exe	344	UDPV6	win-1g223o55tug	5355	*	*					
svchost.exe	252	UDPV6	[0:0:0:0:0:0:0:1]	64048	*	*					
System	4	TCP	win-1g223o55tug.l...	netbios-ssn	WIN-1G223055T...	0	LISTENING				
System	4	TCP	WIN-1G223055T...	microsoft-ds	WIN-1G223055T...	0	LISTENING				
System	4	UDP	win-1g223o55tug.l...	netbios-ns	*	*		21	1,212	6	300
System	4	UDP	win-1g223o55tug.l...	netbios-dgm	*	*					
System	4	TCPV6	win-1g223o55tug	microsoft-ds	win-1g223o55tug	0	LISTENING				
wininit.exe	376	TCP	WIN-1G223055T...	49152	WIN-1G223055T...	0	LISTENING				
wininit.exe	376	TCPV6	win-1g223o55tug	49152	win-1g223o55tug	0	LISTENING				



Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
ElevationServ...	1396	TCP	WIN-1G223055T...	12345	WIN-1G223055T...	0	LISTENING				
InstallAssistSe...	1596	UDP	WIN-1G223055T...	49333	*	*					
lsass.exe	496	TCP	WIN-1G223055T...	49156	WIN-1G223055T...	0	LISTENING				
lsass.exe	496	TCPV6	win-1g223o55tug	49156	win-1g223o55tug	0	LISTENING				
OfficeClickTo...	1296	UDP	WIN-1G223055T...	57243	*	*					
services.exe	480	TCP	WIN-1G223055T...	49155	WIN-1G223055T...	0	LISTENING				
services.exe	480	TCPV6	win-1g223o55tug	49155	win-1g223o55tug	0	LISTENING				
svchost.exe	672	TCP	WIN-1G223055T...	epmap	WIN-1G223055T...	0	LISTENING				
svchost.exe	752	TCP	WIN-1G223055T...	49153	WIN-1G223055T...	0	LISTENING				
svchost.exe	832	TCP	WIN-1G223055T...	49154	WIN-1G223055T...	0	LISTENING				
svchost.exe	252	UDP	WIN-1G223055T...	ssdp	*	*					
svchost.exe	252	UDP	win-1g223o55tug.l...	ssdp	*	*					
svchost.exe	344	UDP	WIN-1G223055T...	llmnr	*	*					
svchost.exe	252	UDP	WIN-1G223055T...	64049	*	*					
svchost.exe	672	TCPV6	win-1g223o55tug	epmap	win-1g223o55tug	0	LISTENING				
svchost.exe	752	TCPV6	win-1g223o55tug	49153	win-1g223o55tug	0	LISTENING				
svchost.exe	832	TCPV6	win-1g223o55tug	49154	win-1g223o55tug	0	LISTENING				
svchost.exe	752	UDPV6	[fe80:0:0:0:dfd:dfd...	546	*	*					
svchost.exe	252	UDPV6	[0:0:0:0:0:0:0:1]	1900	*	*					
svchost.exe	252	UDPV6	[fe80:0:0:0:dfd:dfd...	1900	*	*					
svchost.exe	344	UDPV6	win-1g223o55tug	5355	*	*					
svchost.exe	252	UDPV6	[0:0:0:0:0:0:0:1]	64048	*	*					
System	4	TCP	win-1g223o55tug.l...	netbios-ssn	WIN-1G223055T...	0	LISTENING				
System	4	TCP	WIN-1G223055T...	microsoft-ds	WIN-1G223055T...	0	LISTENING				
System	4	UDP	win-1g223o55tug.l...	netbios-ns	*	*					
System	4	UDP	win-1g223o55tug.l...	netbios-dgm	*	*					
System	4	TCPV6	win-1g223o55tug	microsoft-ds	win-1g223o55tug	0	LISTENING				
wininit.exe	376	TCP	WIN-1G223055T...	49152	WIN-1G223055T...	0	LISTENING				
wininit.exe	376	TCPV6	win-1g223o55tug	49152	win-1g223o55tug	0	LISTENING				

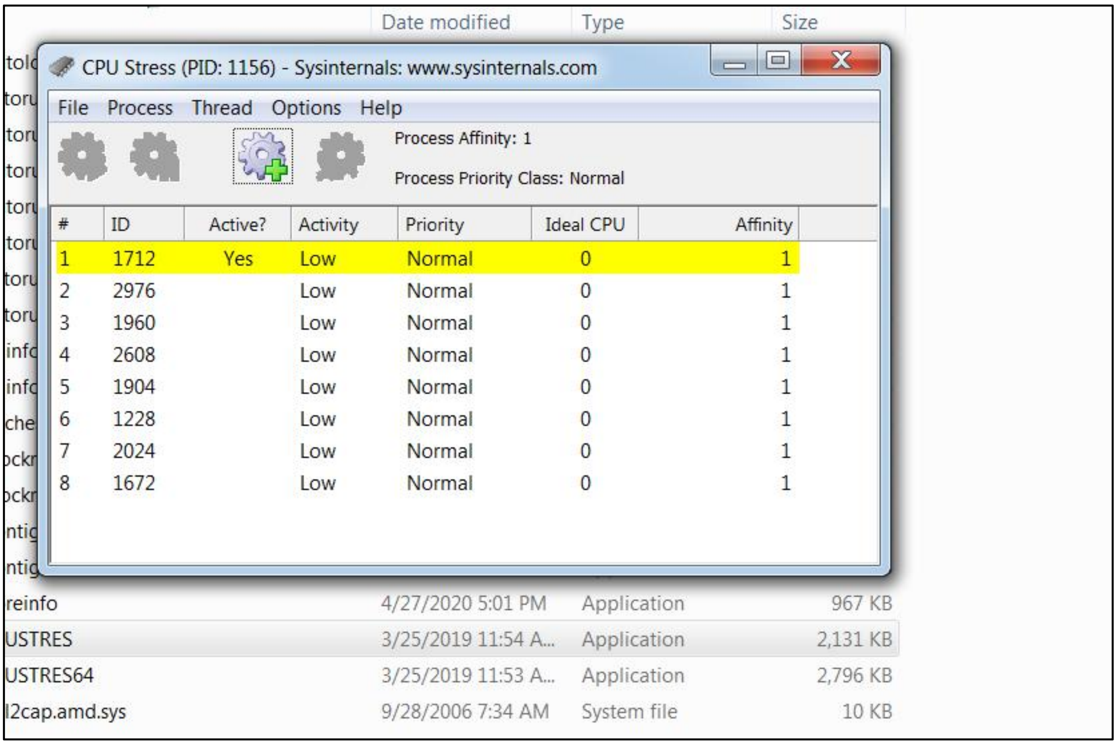
❖ CPUstres v2.0

CpuStres is a utility that can be used to simulate CPU activity by running up to 64 threads in a tight loop.

Each thread can be started, paused or stopped independently and can be configured with the following parameters:

Activity Level This can be Low, Medium, Busy or Maximum which controls how long the thread sleepss betusen cycles. Setting this value to Maximum causes the thread to run continuously.

Priority This controls the thread priority. Refer to Windows Internals by Mark Russinovich for details on thread priorities



CPU Stress (PID: 1156) - Sysinternals: www.sysinternals.com

Process Affinity: 1

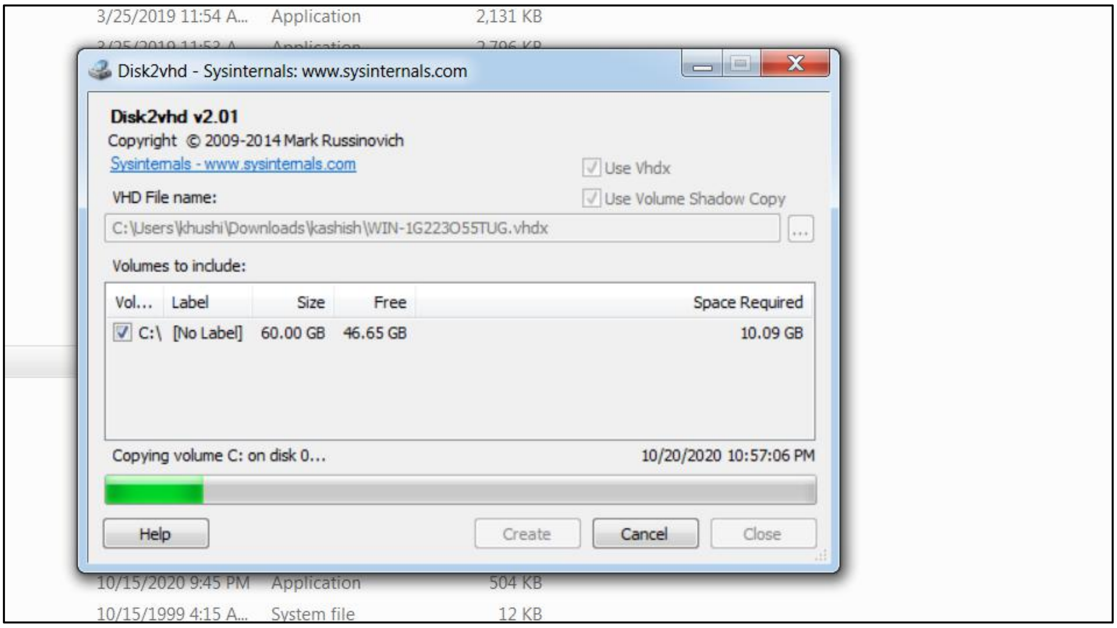
Process Priority Class: Normal

#	ID	Active?	Activity	Priority	Ideal CPU	Affinity
1	1712	Yes	Low	Normal	0	1
2	2976		Low	Normal	0	1
3	1960		Low	Normal	0	1
4	2608		Low	Normal	0	1
5	1904		Low	Normal	0	1
6	1228		Low	Normal	0	1
7	2024		Low	Normal	0	1
8	1672		Low	Normal	0	1

	Date modified	Type	Size
reinfo	4/27/2020 5:01 PM	Application	967 KB
USTRES	3/25/2019 11:54 A...	Application	2,131 KB
USTRES64	3/25/2019 11:53 A...	Application	2,796 KB
l2cap.amd.sys	9/28/2006 7:34 AM	System file	10 KB

❖ Disk2vhd v2.01

Disk2vhd is a utility that creates VHD (Virtual Hard Disk - Microsoft's Virtual Machine disk format) versions of physical disks for use in Microsoft Virtual PC or Microsoft Hyper-V virtual machines (VMs). The difference betusen Disk2vhd and other physical-to-virtual tools is that us can run Disk2vhd on a system that's online. Disk2vhd uses Windows' Volume Snapshot capability, introduced in Windows XP, to create consistent point-in-time snapshots of the volumes us want to include in a conversion.



3/25/2019 11:54 A... Application 2,131 KB

Disk2vhd - Sysinternals: www.sysinternals.com

Disk2vhd v2.01
Copyright © 2009-2014 Mark Russinovich
Sysinternals - www.sysinternals.com

☑ Use Vhdx
☑ Use Volume Shadow Copy

VHD File name: C:\Users\khushi\Downloads\kashish\WIN-1G223O55TUG.vhdx

Volumes to include:

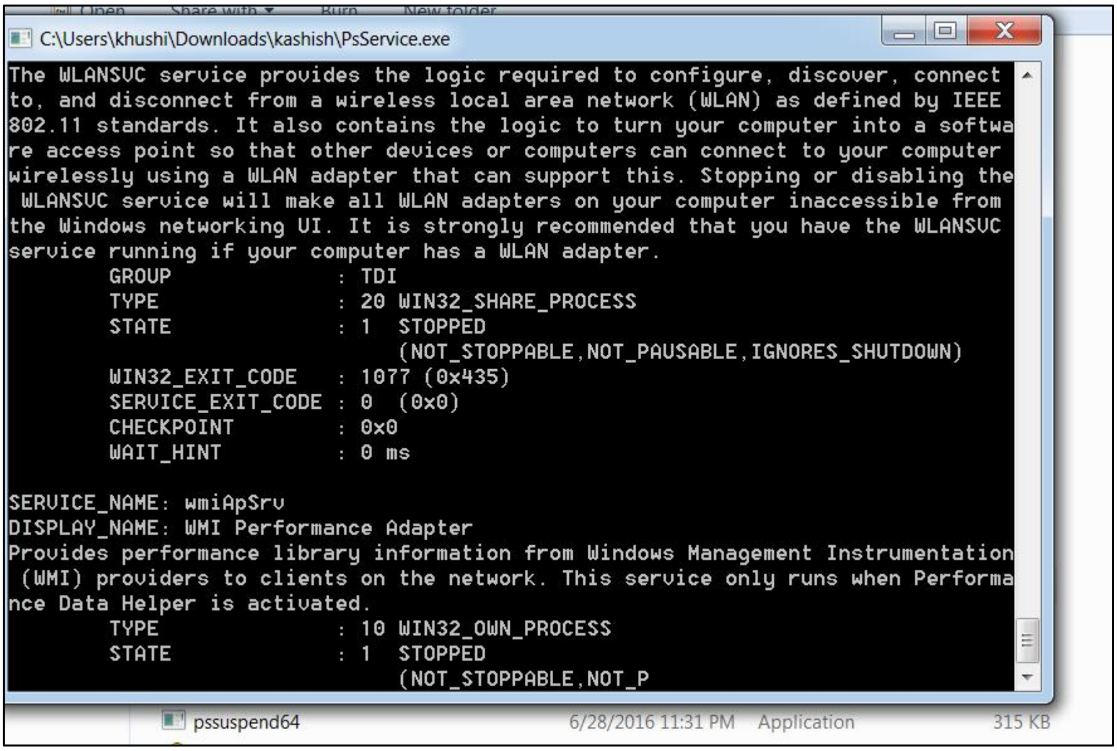
Vol...	Label	Size	Free	Space Required
☑ C:\	[No Label]	60.00 GB	46.65 GB	10.09 GB

Copying volume C: on disk 0... 10/20/2020 10:57:06 PM

10/15/2020 9:45 PM Application 504 KB
10/15/1999 4:15 A... System file 12 KB

- ❖ PsService v2.25

PsService is a service vieusr and controller for Windows. Like the SC utility that's included in the Windows NT and Windows 2000 Resource Kits, *PsService* displays the status, configuration, and dependencies of a service, and allows us to start, stop, pause, resume and restart them. Unlike the SC utility, *PsService* enables us to logon to a remote system using a different account, for cases when the account from which us run it doesn't have required permissions on the remote system.



C:\Users\khushi\Downloads\kashish\PsService.exe

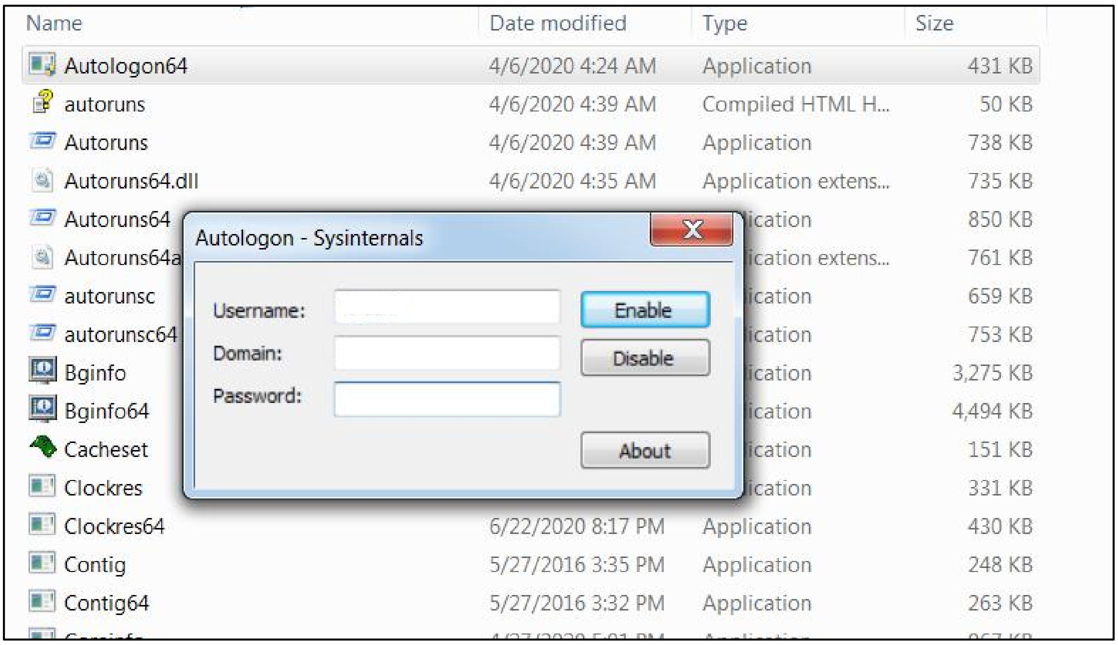
```
The WLANSVC service provides the logic required to configure, discover, connect
to, and disconnect from a wireless local area network (WLAN) as defined by IEEE
802.11 standards. It also contains the logic to turn your computer into a softwa
re access point so that other devices or computers can connect to your computer
wirelessly using a WLAN adapter that can support this. Stopping or disabling the
 WLANSVC service will make all WLAN adapters on your computer inaccessible from
the Windows networking UI. It is strongly recommended that you have the WLANSVC
service running if your computer has a WLAN adapter.
        GROUP              : TDI
        TYPE               : 20 WIN32_SHARE_PROCESS
        STATE              : 1  STOPPED
                                (NOT_STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 1077 (0x435)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0 ms

SERVICE_NAME: wmiApSrv
DISPLAY_NAME: WMI Performance Adapter
Provides performance library information from Windows Management Instrumentation
 (WMI) providers to clients on the network. This service only runs when Performa
nce Data Helper is activated.
        TYPE               : 10 WIN32_OWN_PROCESS
        STATE              : 1  STOPPED
                                (NOT_STOPPABLE,NOT_P
```

pssuspend64 6/28/2016 11:31 PM Application 315 KB

❖ Autologon v3.10

Autologon enables us to easily configure Windows' built-in autologon mechanism. Instead of waiting for a user to enter their name and password, Windows uses the credentials us enter with Autologon, which are encrypted in the Registry, to log on the specified user automatically.

Autologon is easy enough to use. Just run autologon.exe, fill in the dialog, and hit Enable. To turn off auto-logon, hit *Disable*. Also, if the shift key is held down before the system performs an autologon, the autologon will be disabled for that logon. us can also pass the username, domain and password as command-line arguments



Name	Date modified	Type	Size
Autologon64	4/6/2020 4:24 AM	Application	431 KB
autoruns	4/6/2020 4:39 AM	Compiled HTML H...	50 KB
Autoruns	4/6/2020 4:39 AM	Application	738 KB
Autoruns64.dll	4/6/2020 4:35 AM	Application extens...	735 KB
Autoruns64		ication	850 KB
Autoruns64a		ication extens...	761 KB
autorunsc		ication	659 KB
autorunsc64		ication	753 KB
Bginfo		ication	3,275 KB
Bginfo64		ication	4,494 KB
Cacheset		ication	151 KB
Clockres		ication	331 KB
Clockres64	6/22/2020 8:17 PM	Application	430 KB
Contig	5/27/2016 3:35 PM	Application	248 KB
Contig64	5/27/2016 3:32 PM	Application	263 KB