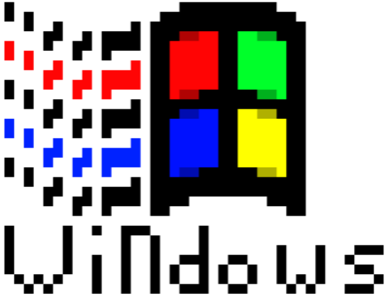
Cyber Defense Organization

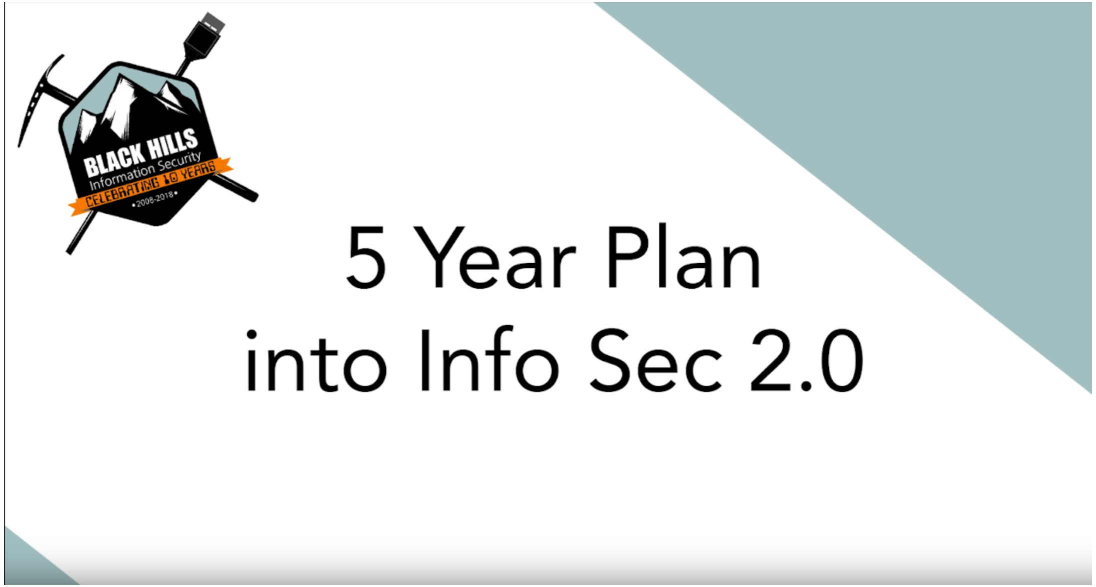
Fall 2019 - Intro to Windows Security



Term of the Week

Where do I get started?

5 Year Plan into InfoSec Part 2

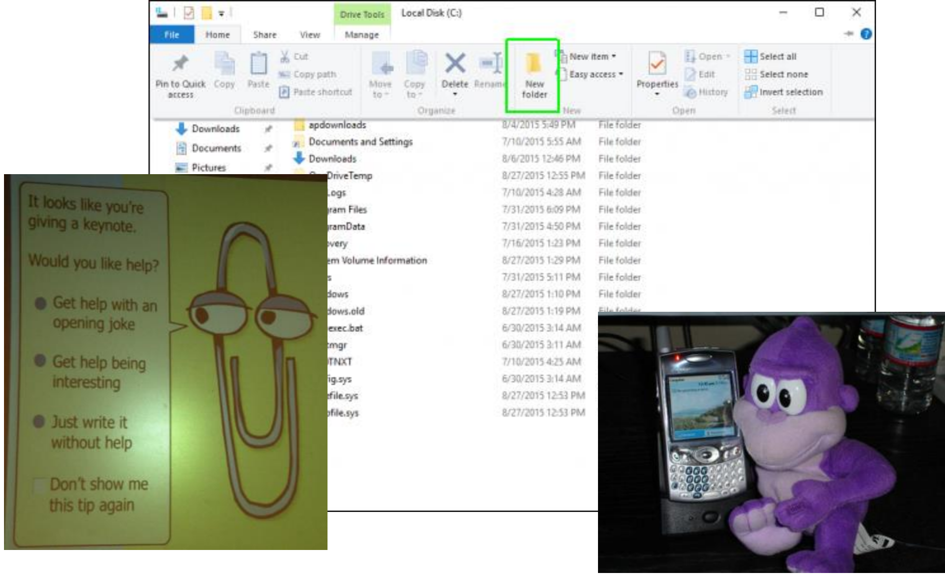


5 Year Plan
into Info Sec 2.0

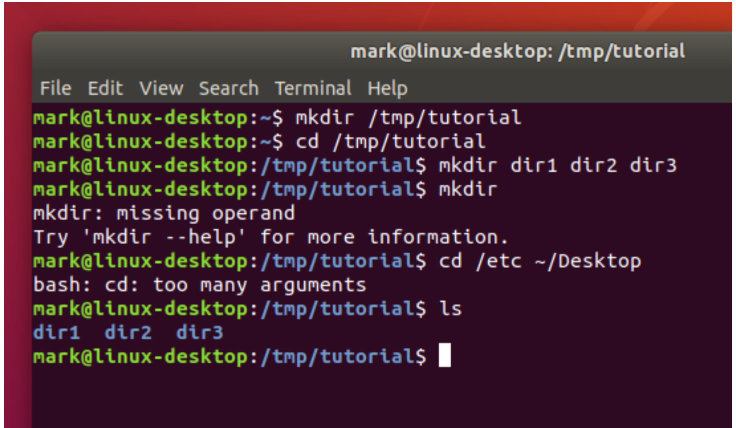
Lets Jump Right In

What is Windows?

- Windows is a GUI based OS
  - A Graphical based Operating System
- Windows server can host a variety of services…
  - AD, DNS, DHCP, IIS (Webserver), etc.
- Very popular in the enterprise environment



VS

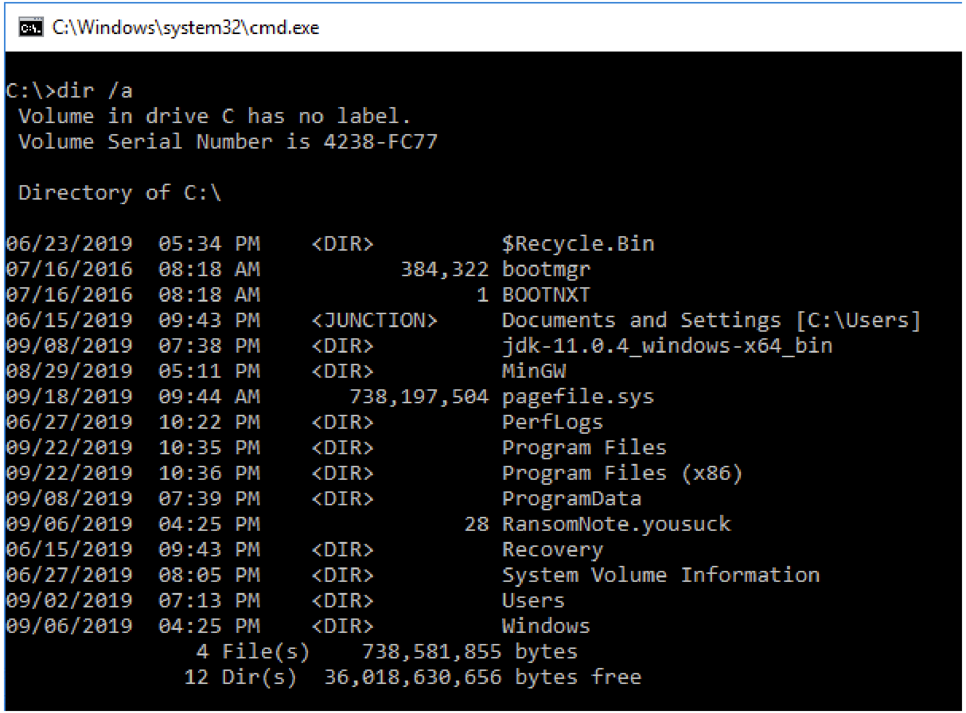

mark@linux-desktop: /tmp/tutorial
File Edit View Search Terminal Help

```
mark@linux-desktop:~$ mkdir /tmp/tutorial
mark@linux-desktop:~$ cd /tmp/tutorial
mark@linux-desktop:/tmp/tutorial$ mkdir dir1 dir2 dir3
mark@linux-desktop:/tmp/tutorial$ mkdir
mkdir: missing operand
Try 'mkdir --help' for more information.
mark@linux-desktop:/tmp/tutorial$ cd /etc ~/Desktop
bash: cd: too many arguments
mark@linux-desktop:/tmp/tutorial$ ls
dir1  dir2  dir3
mark@linux-desktop:/tmp/tutorial$ 
```

TL;DR Windows is a big subject. You can approach this from Forensics, Operations, Blue Team, Compliance, Development, Redteam etc. perspectives.

File Structure

Directory	Description
\PerfLogs	Windows performance logs.
\Program Files	Programs are installed in here.
\Program Files (x86)	On a 64-bit machine, 32-bit programs are placed here.
\ProgramData	Contains program data that are expected to be accessed by computer programs regardless of the user account in the context of which they run.
\Users	User Profile folders.
\Windows	Windows itself is installed into this folder.
\Windows\System32	Stores dynamic-link library (DLL) files that implement the core features of Windows and Windows API.

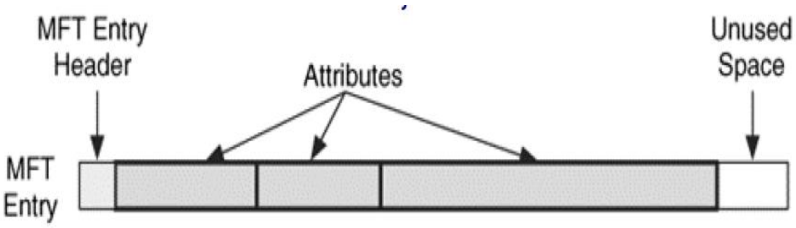


```
C:\>dir /a
 Volume in drive C has no label.
 Volume Serial Number is 4238-FC77

 Directory of C:\

06/23/2019  05:34 PM    <DIR>          $Recycle.Bin
07/16/2016  08:18 AM           384,322 bootmgr
07/16/2016  08:18 AM                 1 BOOTNXT
06/15/2019  09:43 PM    <JUNCTION>     Documents and Settings [C:\Users]
09/08/2019  07:38 PM    <DIR>          jdk-11.0.4_windows-x64_bin
08/29/2019  05:11 PM    <DIR>          MinGW
09/18/2019  09:44 AM       738,197,504 pagefile.sys
06/27/2019  10:22 PM    <DIR>          PerfLogs
09/22/2019  10:35 PM    <DIR>          Program Files
09/22/2019  10:36 PM    <DIR>          Program Files (x86)
09/08/2019  07:39 PM    <DIR>          ProgramData
09/06/2019  04:25 PM                28 RansomNote.yousuck
06/15/2019  09:43 PM    <DIR>          Recovery
06/27/2019  08:05 PM    <DIR>          System Volume Information
09/02/2019  07:13 PM    <DIR>          Users
09/06/2019  04:25 PM    <DIR>          Windows
               4 File(s)    738,581,855 bytes
              12 Dir(s)  36,018,630,656 bytes free
```

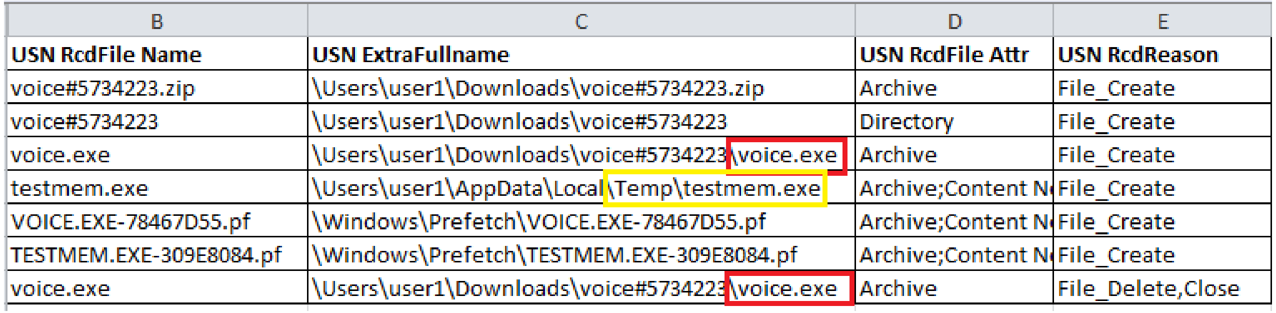
File System (NTFS) - MFT/$USNJRNL:$J

Master File Table ($MFT) is the heart of NTFS because it contains the information about all files and directories.

Every file and directory has at least one entry in the table, and the entries by themselves are very simple.



The change journal is a file that records when changes are made to files and directories. Video.



B	C	D	E
USN RcdFile Name	**USN ExtraFullname**	**USN RcdFile Attr**	**USN RcdReason**
voice#5734223.zip	\Users\user1\Downloads\voice#5734223.zip	Archive	File_Create
voice#5734223	\Users\user1\Downloads\voice#5734223	Directory	File_Create
voice.exe	\Users\user1\Downloads\voice#5734223\voice.exe	Archive	File_Create
testmem.exe	\Users\user1\AppData\Local\Temp\testmem.exe	Archive;Content N	File_Create
VOICE.EXE-78467D55.pf	\Windows\Prefetch\VOICE.EXE-78467D55.pf	Archive;Content N	File_Create
TESTMEM.EXE-309E8084.pf	\Windows\Prefetch\TESTMEM.EXE-309E8084.pf	Archive;Content N	File_Create
voice.exe	\Users\user1\Downloads\voice#5734223\voice.exe	Archive	File_Delete,Close

File System (NTFS) - Time Stamps

This is more into the forensics side. If interested read the book, File System Forensics. 10/10.

Every File has two sets of 4 Time Stamps

$STANDARD_INFO can be modified by user level processes like timestomp.

$FILE_NAME can only be modified by the system kernel. (There are no known anti-forensics utilities that can accomplish this.)*

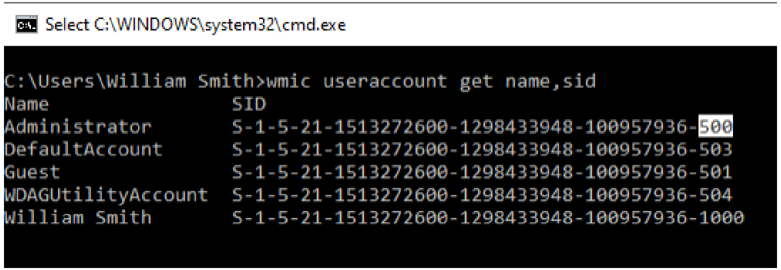
The MAC(b) times are derived from file system metadata and they stand for:

1. Modified
2. Accessed
3. Changed ($MFT Modified)
4. Birth (file creation time)

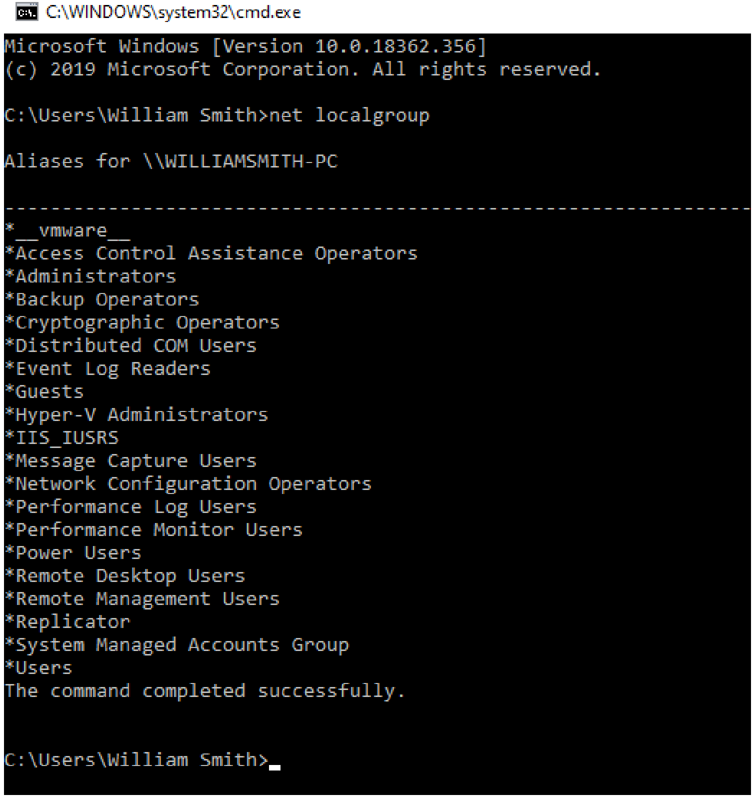
The (b) is in parentheses because not all file systems record a birth time.
*COUGH*EXT4*COUGH*

Users & Group

- User groups work much different from a linux based system
  - Based off of SIDs (Security Identifiers)
- SIDs determine what permission groups, users, or even the current session has access too



```
C:\Users\William Smith>wmic useraccount get name,sid
Name                SID
Administrator       S-1-5-21-1513272600-1298433948-100957936-500
DefaultAccount      S-1-5-21-1513272600-1298433948-100957936-503
Guest               S-1-5-21-1513272600-1298433948-100957936-501
WDAGUtilityAccount  S-1-5-21-1513272600-1298433948-100957936-504
William Smith       S-1-5-21-1513272600-1298433948-100957936-1000
```



```
Microsoft Windows [Version 10.0.18362.356]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\William Smith>net localgroup

Aliases for \\WILLIAMSMITH-PC

-------------------------------------------------------------------------------
*__vmware__
*Access Control Assistance Operators
*Administrators
*Backup Operators
*Cryptographic Operators
*Distributed COM Users
*Event Log Readers
*Guests
*Hyper-V Administrators
*IIS_IUSRS
*Message Capture Users
*Network Configuration Operators
*Performance Log Users
*Performance Monitor Users
*Power Users
*Remote Desktop Users
*Remote Management Users
*Replicator
*System Managed Accounts Group
*Users
The command completed successfully.


C:\Users\William Smith>_
```

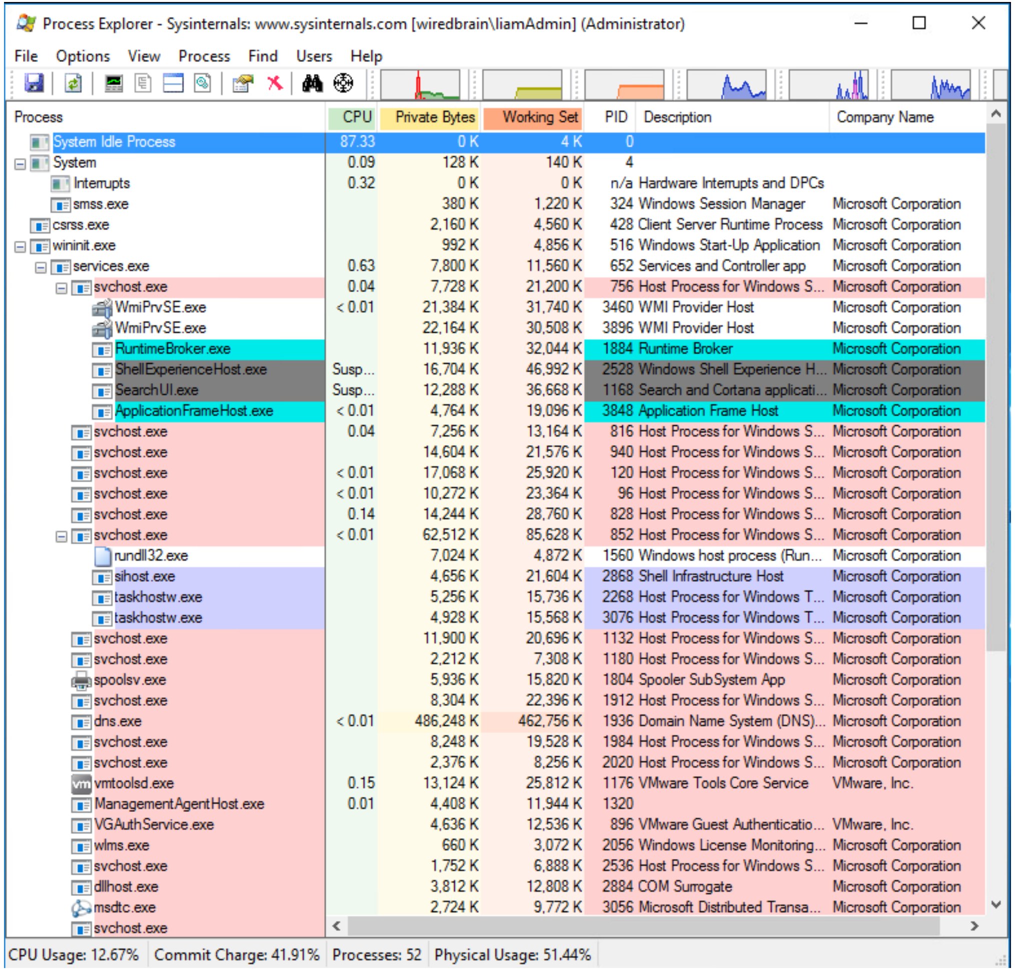
Processesses

An application consists of one or more processes.

A process, in the simplest terms, is an executing program.

One or more threads run in the context of the process.

A thread is something you use to sow a button. (basic unit to which the operating system allocates processor time).


Process Explorer - Sysinternals: www.sysinternals.com [wiredbrain\liamAdmin] (Administrator)
File
Options
View
Process
Find
Users
Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	87.33	0 K	4 K	0		
System	0.09	128 K	140 K	4		
Interrupts	0.32	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		380 K	1,220 K	324	Windows Session Manager	Microsoft Corporation
csrss.exe		2,160 K	4,560 K	428	Client Server Runtime Process	Microsoft Corporation
wininit.exe		992 K	4,856 K	516	Windows Start-Up Application	Microsoft Corporation
services.exe	0.63	7,800 K	11,560 K	652	Services and Controller app	Microsoft Corporation
svchost.exe	0.04	7,728 K	21,200 K	756	Host Process for Windows S...	Microsoft Corporation
WmiPrvSE.exe	< 0.01	21,384 K	31,740 K	3460	WMI Provider Host	Microsoft Corporation
WmiPrvSE.exe		22,164 K	30,508 K	3896	WMI Provider Host	Microsoft Corporation
RuntimeBroker.exe		11,936 K	32,044 K	1884	Runtime Broker	Microsoft Corporation
ShellExperienceHost.exe	Susp...	16,704 K	46,992 K	2528	Windows Shell Experience H...	Microsoft Corporation
SearchUI.exe	Susp...	12,288 K	36,668 K	1168	Search and Cortana applicati...	Microsoft Corporation
ApplicationFrameHost.exe	< 0.01	4,764 K	19,096 K	3848	Application Frame Host	Microsoft Corporation
svchost.exe	0.04	7,256 K	13,164 K	816	Host Process for Windows S...	Microsoft Corporation
svchost.exe		14,604 K	21,576 K	940	Host Process for Windows S...	Microsoft Corporation
svchost.exe	< 0.01	17,068 K	25,920 K	120	Host Process for Windows S...	Microsoft Corporation
svchost.exe	< 0.01	10,272 K	23,364 K	96	Host Process for Windows S...	Microsoft Corporation
svchost.exe	0.14	14,244 K	28,760 K	828	Host Process for Windows S...	Microsoft Corporation
svchost.exe	< 0.01	62,512 K	85,628 K	852	Host Process for Windows S...	Microsoft Corporation
rundll32.exe		7,024 K	4,872 K	1560	Windows host process (Run...	Microsoft Corporation
sihost.exe		4,656 K	21,604 K	2868	Shell Infrastructure Host	Microsoft Corporation
taskhostw.exe		5,256 K	15,736 K	2268	Host Process for Windows T...	Microsoft Corporation
taskhostw.exe		4,928 K	15,568 K	3076	Host Process for Windows T...	Microsoft Corporation
svchost.exe		11,900 K	20,696 K	1132	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,212 K	7,308 K	1180	Host Process for Windows S...	Microsoft Corporation
spoolsv.exe		5,936 K	15,820 K	1804	Spooler SubSystem App	Microsoft Corporation
svchost.exe		8,304 K	22,396 K	1912	Host Process for Windows S...	Microsoft Corporation
dns.exe	< 0.01	486,248 K	462,756 K	1936	Domain Name System (DNS)...	Microsoft Corporation
svchost.exe		8,248 K	19,528 K	1984	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,376 K	8,256 K	2020	Host Process for Windows S...	Microsoft Corporation
vmtoolsd.exe	0.15	13,124 K	25,812 K	1176	VMware Tools Core Service	VMware, Inc.
ManagementAgentHost.exe	0.01	4,408 K	11,944 K	1320		
VGAuthService.exe		4,636 K	12,536 K	896	VMware Guest Authenticatio...	VMware, Inc.
wlms.exe		660 K	3,072 K	2056	Windows License Monitoring...	Microsoft Corporation
svchost.exe		1,752 K	6,888 K	2536	Host Process for Windows S...	Microsoft Corporation
dllhost.exe		3,812 K	12,808 K	2884	COM Surrogate	Microsoft Corporation
msdtc.exe		2,724 K	9,772 K	3056	Microsoft Distributed Transa...	Microsoft Corporation
svchost.exe						

CPU Usage: 12.67% | Commit Charge: 41.91% | Processes: 52 | Physical Usage: 51.44%

Firewall

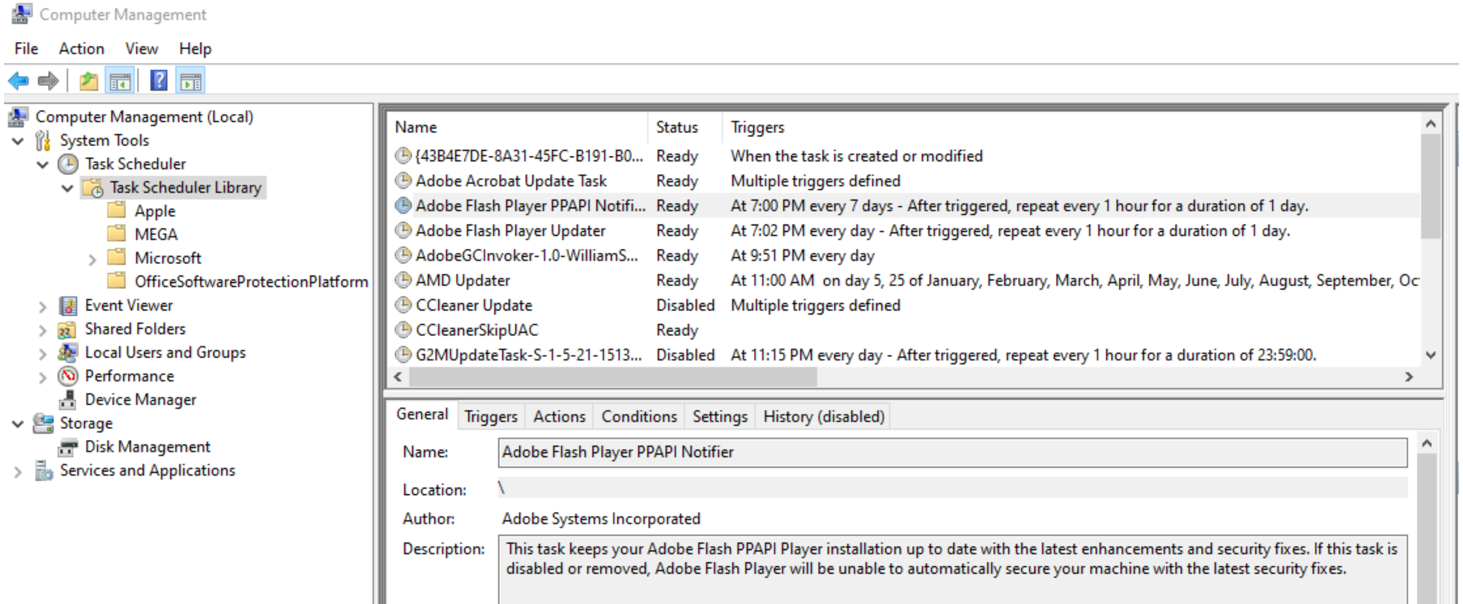
- The Windows firewall operates for just that machine
- You can create inbound and outbound rules through the GUI
- Good for blocking network traffic that you don't need

You can block traffic at the program level. Not just ports/protocols. (Kinda important in competitions).

Task Scheduler

Task Scheduler is a component of Microsoft Windows that provides the ability to schedule the launch of programs or scripts at pre-defined times or after specified time intervals: job scheduling (task scheduling).

You know all those annoying update things you 100% Ignore from Adobe once a week?



Name	Status	Triggers
{43B4E7DE-8A31-45FC-B191-B0...	Ready	When the task is created or modified
Adobe Acrobat Update Task	Ready	Multiple triggers defined
Adobe Flash Player PPAPI Notifi...	Ready	At 7:00 PM every 7 days - After triggered, repeat every 1 hour for a duration of 1 day.
Adobe Flash Player Updater	Ready	At 7:02 PM every day - After triggered, repeat every 1 hour for a duration of 1 day.
AdobeGCInvoker-1.0-WilliamS...	Ready	At 9:51 PM every day
AMD Updater	Ready	At 11:00 AM on day 5, 25 of January, February, March, April, May, June, July, August, September, Oc
CCleaner Update	Disabled	Multiple triggers defined
CCleanerSkipUAC	Ready	
G2MUpdateTask-S-1-5-21-1513...	Disabled	At 11:15 PM every day - After triggered, repeat every 1 hour for a duration of 23:59:00.

Name: Adobe Flash Player PPAPI Notifier

Location: \

Author: Adobe Systems Incorporated

Description: This task keeps your Adobe Flash PPAPI Player installation up to date with the latest enhancements and security fixes. If this task is disabled or removed, Adobe Flash Player will be unable to automatically secure your machine with the latest security fixes.

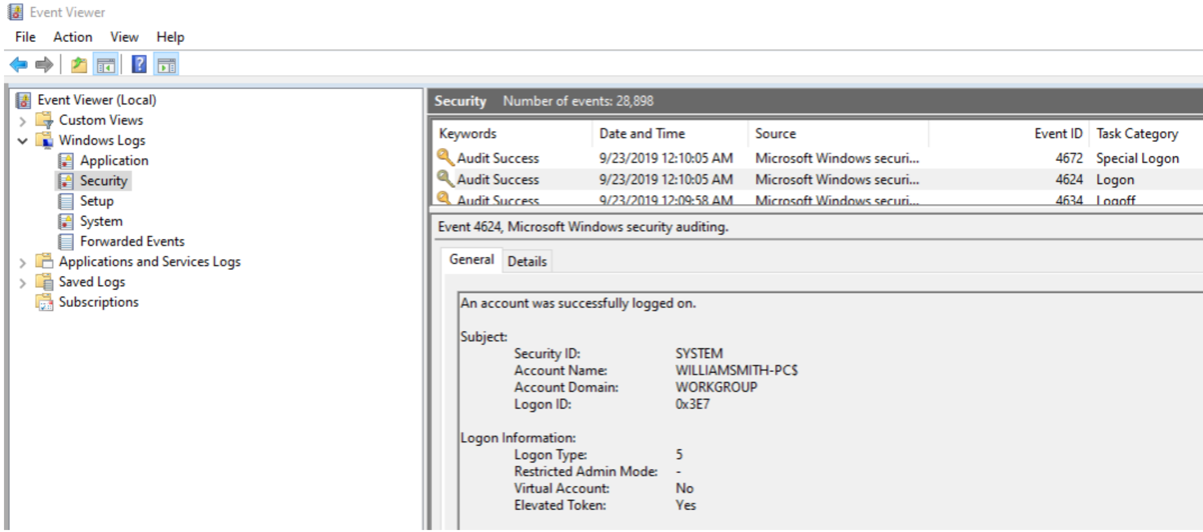
Event Viewer/Event Logs

Windows has logs.

The Event Viewer is a tool in Windows that displays detailed information about significant events on your computer.

No they are not that pretty. But they are beautiful in their own way. Mastery in understanding them will bring you far!

Logon types (5 = “Unlock” here) are important.

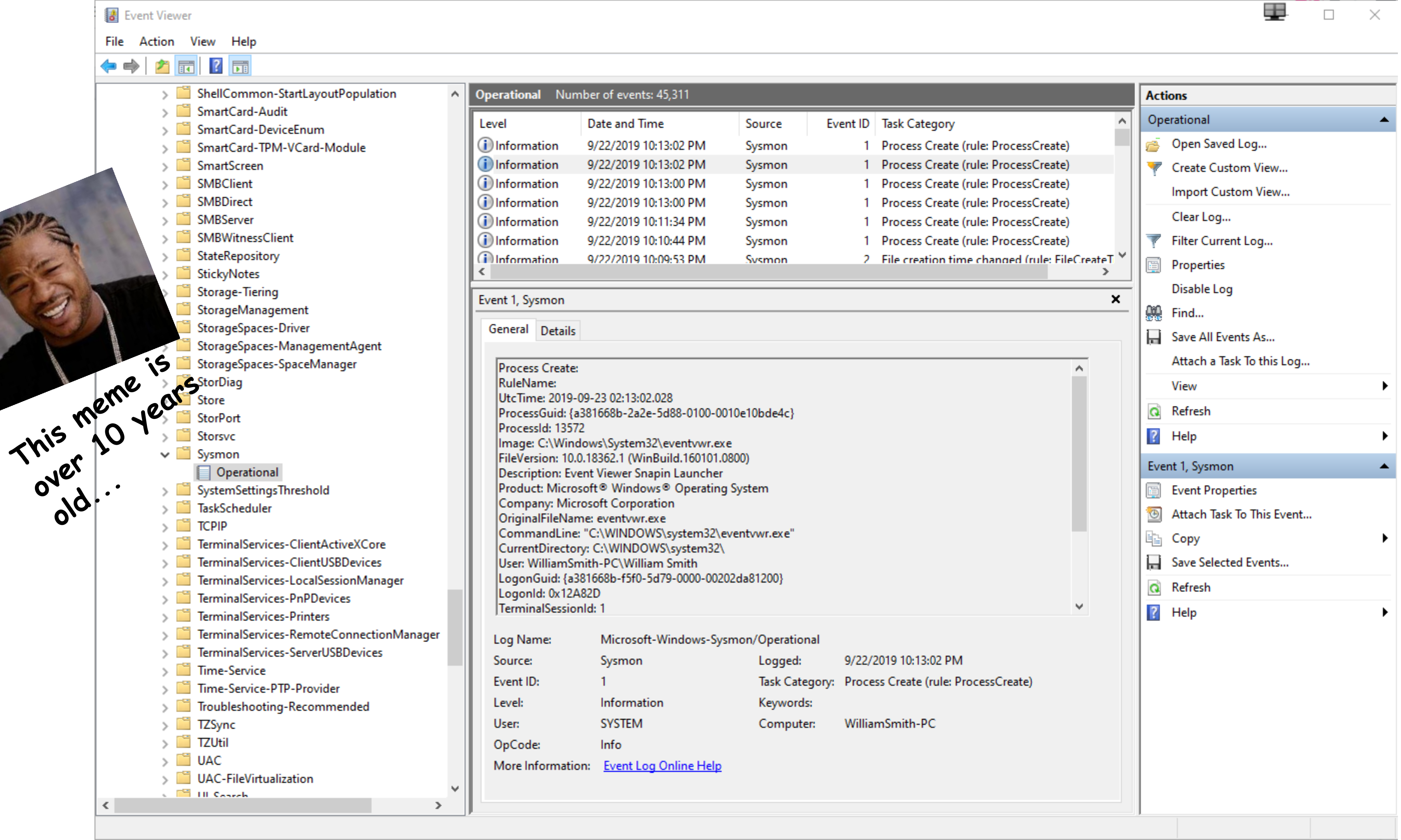


Number of events: 28,898

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	9/23/2019 12:10:05 AM	Microsoft Windows securi...	4672	Special Logon
Audit Success	9/23/2019 12:10:05 AM	Microsoft Windows securi...	4624	Logon
Audit Success	9/23/2019 12:09:58 AM	Microsoft Windows securi...	4634	Logoff

Event 4624, Microsoft Windows security auditing.

```
An account was successfully logged on.

Subject:
        Security ID:            SYSTEM
        Account Name:           WILLIAMSMITH-PC$
        Account Domain:         WORKGROUP
        Logon ID:               0x3E7

Logon Information:
        Logon Type:             5
        Restricted Admin Mode:  -
        Virtual Account:        No
        Elevated Token:         Yes
```



This meme is over 10 years old...

Operational   Number of events: 45,311

Level	Date and Time	Source	Event ID	Task Category
Information	9/22/2019 10:13:02 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	9/22/2019 10:13:02 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	9/22/2019 10:13:00 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	9/22/2019 10:13:00 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	9/22/2019 10:11:34 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	9/22/2019 10:10:44 PM	Sysmon	1	Process Create (rule: ProcessCreate)
Information	9/22/2019 10:09:53 PM	Sysmon	2	File creation time changed (rule: FileCreateT

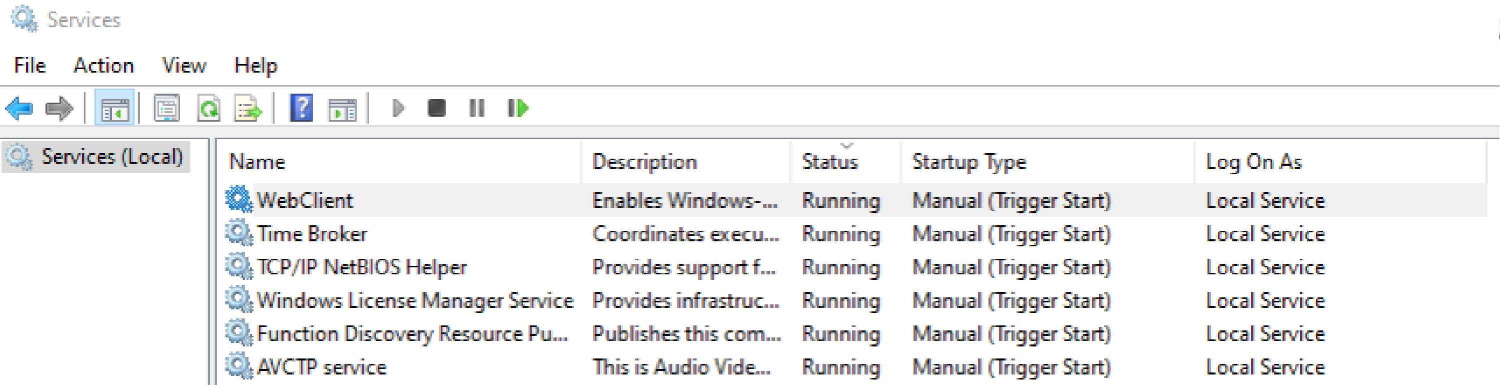
Event 1, Sysmon

```
Process Create:
RuleName:
UtcTime: 2019-09-23 02:13:02.028
ProcessGuid: {a381668b-2a2e-5d88-0100-0010e10bde4c}
ProcessId: 13572
Image: C:\Windows\System32\eventvwr.exe
FileVersion: 10.0.18362.1 (WinBuild.160101.0800)
Description: Event Viewer Snapin Launcher
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: eventvwr.exe
CommandLine: "C:\WINDOWS\system32\eventvwr.exe"
CurrentDirectory: C:\WINDOWS\system32\
User: WilliamSmith-PC\William Smith
LogonGuid: {a381668b-f5f0-5d79-0000-00202da81200}
LogonId: 0x12A82D
TerminalSessionId: 1
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	9/22/2019 10:13:02 PM
Event ID:	1	Task Category:	Process Create (rule: ProcessCreate)
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	WilliamSmith-PC
OpCode:	Info		
More Information:	Event Log Online Help		

Services

Microsoft Windows services, formerly known as NT services, enable you to create long-running executable applications that run in their own Windows sessions. These services can be automatically started when the computer boots, can be paused and restarted, and do not show any user interface. These features make services ideal for use on a server or whenever you need long-running functionality that does not interfere with other users who are working on the same computer.

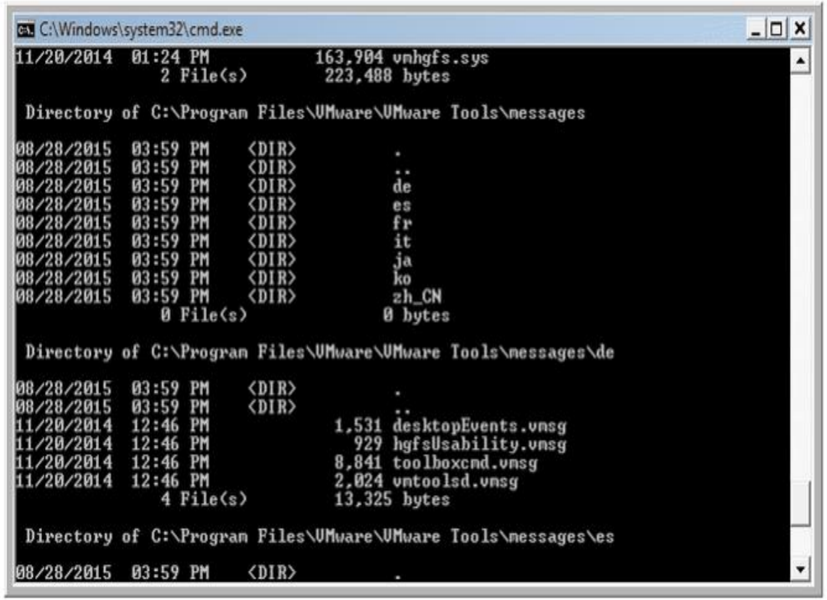


Name	Description	Status	Startup Type	Log On As
WebClient	Enables Windows-...	Running	Manual (Trigger Start)	Local Service
Time Broker	Coordinates execu...	Running	Manual (Trigger Start)	Local Service
TCP/IP NetBIOS Helper	Provides support f...	Running	Manual (Trigger Start)	Local Service
Windows License Manager Service	Provides infrastruc...	Running	Manual (Trigger Start)	Local Service
Function Discovery Resource Pu...	Publishes this com...	Running	Manual (Trigger Start)	Local Service
AVCTP service	This is Audio Vide...	Running	Manual (Trigger Start)	Local Service

Command Line/Prompt/CMD

Window’s own terminal

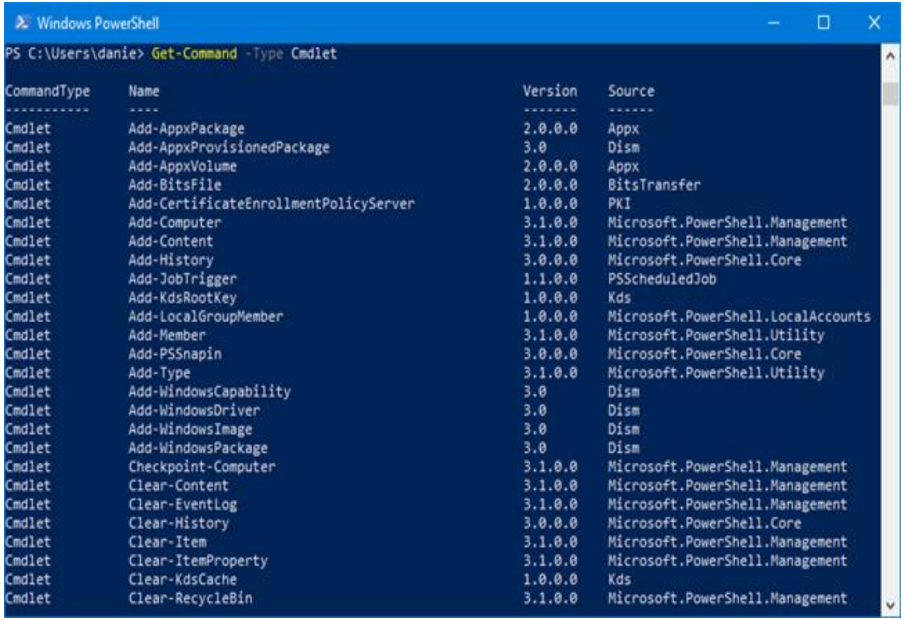
Command	Function
help	List of commands
systeminfo	High level overview of the system
ipconfig	Network configuration
netstat	Open connections (-ano)
net <>	A powerful suite of commands
ping	Test network communication
tracert	Trace a network communication
tasklist	List processes
taskkill	Kill a process



```
11/20/2014  01:24 PM           163,904 vmhgfs.sys
               2 File(s)        223,488 bytes

 Directory of C:\Program Files\VMware\VMware Tools\messages

08/28/2015  03:59 PM    <DIR>          .
08/28/2015  03:59 PM    <DIR>          ..
08/28/2015  03:59 PM    <DIR>          de
08/28/2015  03:59 PM    <DIR>          es
08/28/2015  03:59 PM    <DIR>          fr
08/28/2015  03:59 PM    <DIR>          it
08/28/2015  03:59 PM    <DIR>          ja
08/28/2015  03:59 PM    <DIR>          ko
08/28/2015  03:59 PM    <DIR>          zh_CN
               0 File(s)              0 bytes

 Directory of C:\Program Files\VMware\VMware Tools\messages\de

08/28/2015  03:59 PM    <DIR>          .
08/28/2015  03:59 PM    <DIR>          ..
11/20/2014  12:46 PM             1,531 desktopEvents.vmsg
11/20/2014  12:46 PM               929 hgfsUsability.vmsg
11/20/2014  12:46 PM             8,841 toolboxcmd.vmsg
11/20/2014  12:46 PM             2,024 vmtoolsd.vmsg
               4 File(s)         13,325 bytes

 Directory of C:\Program Files\VMware\VMware Tools\messages\es

08/28/2015  03:59 PM    <DIR>          .
```

Powershell

- Powershell is a very powerful tool
- Amped up version of the CMD
- It can be used for…
  - Task automation
  - Scripting
- Has a simple command structure
  - Verb-noun



```
PS C:\Users\danie> Get-Command -Type Cmdlet

CommandType     Name                                               Version    Source
-----------     ----                                               -------    ------
Cmdlet          Add-AppxPackage                                    2.0.0.0    Appx
Cmdlet          Add-AppxProvisionedPackage                         3.0        Dism
Cmdlet          Add-AppxVolume                                     2.0.0.0    Appx
Cmdlet          Add-BitsFile                                       2.0.0.0    BitsTransfer
Cmdlet          Add-CertificateEnrollmentPolicyServer              1.0.0.0    PKI
Cmdlet          Add-Computer                                       3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Add-Content                                        3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Add-History                                        3.0.0.0    Microsoft.PowerShell.Core
Cmdlet          Add-JobTrigger                                     1.1.0.0    PSScheduledJob
Cmdlet          Add-KdsRootKey                                     1.0.0.0    Kds
Cmdlet          Add-LocalGroupMember                               1.0.0.0    Microsoft.PowerShell.LocalAccounts
Cmdlet          Add-Member                                         3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Add-PSSnapin                                       3.0.0.0    Microsoft.PowerShell.Core
Cmdlet          Add-Type                                           3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Add-WindowsCapability                              3.0        Dism
Cmdlet          Add-WindowsDriver                                  3.0        Dism
Cmdlet          Add-WindowsImage                                   3.0        Dism
Cmdlet          Add-WindowsPackage                                 3.0        Dism
Cmdlet          Checkpoint-Computer                                3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Clear-Content                                      3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Clear-EventLog                                     3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Clear-History                                      3.0.0.0    Microsoft.PowerShell.Core
Cmdlet          Clear-Item                                         3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Clear-ItemProperty                                 3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Clear-KdsCache                                     1.0.0.0    Kds
Cmdlet          Clear-RecycleBin                                   3.1.0.0    Microsoft.PowerShell.Management
```

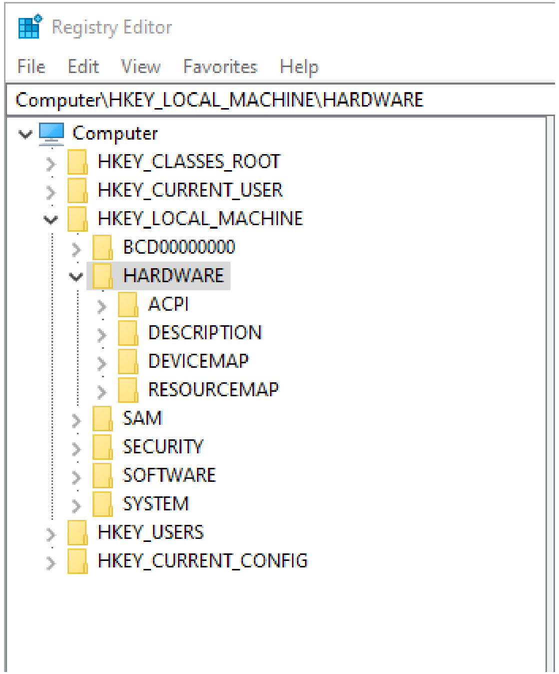
Its a shell…
and its blue.
Please laugh.

Registry

The Windows Registry is a hierarchical database that stores low-level settings for the Microsoft Windows operating system and for applications that opt to use the registry.

- HKEY_CLASSES_ROOT (HKCR)
- HKEY_CURRENT_USER (HKCU)
- HKEY_LOCAL_MACHINE (HKLM)
- HKEY_USER (HKU)
- HKEY_CURRENT_CONFIG (HKCC)

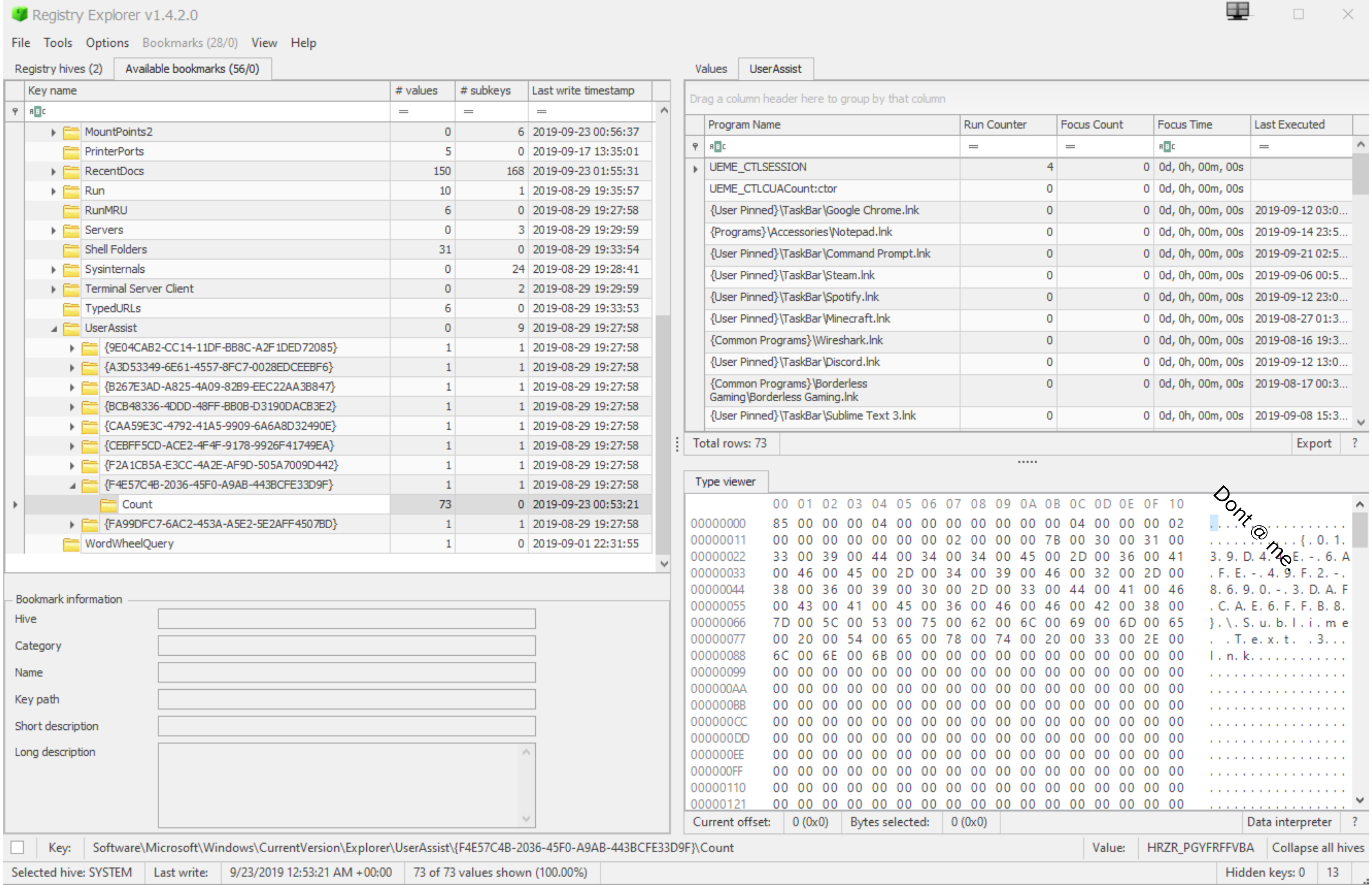
Look at it With RegEdit, or Registry Explorer.



Computer\HKEY_LOCAL_MACHINE\HARDWARE

```
Computer
  HKEY_CLASSES_ROOT
  HKEY_CURRENT_USER
  HKEY_LOCAL_MACHINE
    BCD00000000
    HARDWARE
      ACPI
      DESCRIPTION
      DEVICEMAP
      RESOURCEMAP
    SAM
    SECURITY
    SOFTWARE
    SYSTEM
  HKEY_USERS
  HKEY_CURRENT_CONFIG
```

I can't stress enough how important it is for Windows Forensics. Check out this link for Liam's Windows Forensics Intro.


Registry Explorer v1.4.2.0
File
Tools
Options
Bookmarks (28/0)
View
Help
Registry hives (2)
Available bookmarks (56/0)
Values
UserAssist
Drag a column header here to group by that column

Key name	# values	# subkeys	Last write timestamp
MountPoints2	0	6	2019-09-23 00:56:37
PrinterPorts	5	0	2019-09-17 13:35:01
RecentDocs	150	168	2019-09-23 01:55:31
Run	10	1	2019-08-29 19:35:57
RunMRU	6	0	2019-08-29 19:27:58
Servers	0	3	2019-08-29 19:29:59
Shell Folders	31	0	2019-08-29 19:33:54
Sysinternals	0	24	2019-08-29 19:28:41
Terminal Server Client	0	2	2019-08-29 19:29:59
TypedURLs	6	0	2019-08-29 19:33:53
UserAssist	0	9	2019-08-29 19:27:58
{9E04CAB2-CC14-11DF-BB8C-A2F1DED72085}	1	1	2019-08-29 19:27:58
{A3D53349-6E61-4557-8FC7-0028EDCEEBF6}	1	1	2019-08-29 19:27:58
{B267E3AD-A825-4A09-82B9-EEC22AA3B847}	1	1	2019-08-29 19:27:58
{BCB48336-4DDD-48FF-BB0B-D3190DACB3E2}	1	1	2019-08-29 19:27:58
{CAA59E3C-4792-41A5-9909-6A6A8D32490E}	1	1	2019-08-29 19:27:58
{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}	1	1	2019-08-29 19:27:58
{F2A1CB5A-E3CC-4A2E-AF9D-505A7009D442}	1	1	2019-08-29 19:27:58
{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}	1	1	2019-08-29 19:27:58
Count	73	0	2019-09-23 00:53:21
{FA99DFC7-6AC2-453A-A5E2-5E2AFF4507BD}	1	1	2019-08-29 19:27:58
WordWheelQuery	1	0	2019-09-01 22:31:55

Program Name	Run Counter	Focus Count	Focus Time	Last Executed
UEME_CTLSESSION	4	0	0d, 0h, 00m, 00s	
UEME_CTLCUACount:ctor	0	0	0d, 0h, 00m, 00s	
{User Pinned}\TaskBar\Google Chrome.lnk	0	0	0d, 0h, 00m, 00s	2019-09-12 03:0...
{Programs}\Accessories\Notepad.lnk	0	0	0d, 0h, 00m, 00s	2019-09-14 23:5...
{User Pinned}\TaskBar\Command Prompt.lnk	0	0	0d, 0h, 00m, 00s	2019-09-21 02:5...
{User Pinned}\TaskBar\Steam.lnk	0	0	0d, 0h, 00m, 00s	2019-09-06 00:5...
{User Pinned}\TaskBar\Spotify.lnk	0	0	0d, 0h, 00m, 00s	2019-09-12 23:0...
{User Pinned}\TaskBar\Minecraft.lnk	0	0	0d, 0h, 00m, 00s	2019-08-27 01:3...
{Common Programs}\Wireshark.lnk	0	0	0d, 0h, 00m, 00s	2019-08-16 19:3...
{User Pinned}\TaskBar\Discord.lnk	0	0	0d, 0h, 00m, 00s	2019-09-12 13:0...
{Common Programs}\Borderless Gaming\Borderless Gaming.lnk	0	0	0d, 0h, 00m, 00s	2019-08-17 00:3...
{User Pinned}\TaskBar\Sublime Text 3.lnk	0	0	0d, 0h, 00m, 00s	2019-09-08 15:3...

Total rows: 73

```
          00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10
00000000  85 00 00 00 04 00 00 00 00 00 00 00 04 00 00 00 02   . . . . . . . . . . . . . . . . .
00000011  00 00 00 00 00 00 00 02 00 00 00 7B 00 30 00 31 00   . . . . . . . . . . . { . 0 . 1 .
00000022  33 00 39 00 44 00 34 00 34 00 45 00 2D 00 36 00 41   3. 9. D. 4. 4. E. - . 6. A
00000033  00 46 00 45 00 2D 00 34 00 39 00 46 00 32 00 2D 00   . F. E. - . 4. 9. F. 2. - .
00000044  38 00 36 00 39 00 30 00 2D 00 33 00 44 00 41 00 46   8. 6. 9. 0. - . 3. D. A. F
00000055  00 43 00 41 00 45 00 36 00 46 00 46 00 42 00 38 00   . C. A. E. 6. F. F. B. 8.
00000066  7D 00 5C 00 53 00 75 00 62 00 6C 00 69 00 6D 00 65   } . \ . S. u. b. l . i . m e
00000077  00 20 00 54 00 65 00 78 00 74 00 20 00 33 00 2E 00   .   . T. e. x. t.   . 3. . .
00000088  6C 00 6E 00 6B 00 00 00 00 00 00 00 00 00 00 00 00   l . n. k. . . . . . . . . . . .
00000099  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   . . . . . . . . . . . . . . . . .
000000AA  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   . . . . . . . . . . . . . . . . .
000000BB  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   . . . . . . . . . . . . . . . . .
000000CC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   . . . . . . . . . . . . . . . . .
000000DD  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   . . . . . . . . . . . . . . . . .
000000EE  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   . . . . . . . . . . . . . . . . .
000000FF  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   . . . . . . . . . . . . . . . . .
00000110  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   . . . . . . . . . . . . . . . . .
00000121  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   . . . . . . . . . . . . . . . . .
```

Dont @ me.

Current offset: 0 (0x0) Bytes selected: 0 (0x0)

Hive

Category

Name

Key path

Short description

Long description

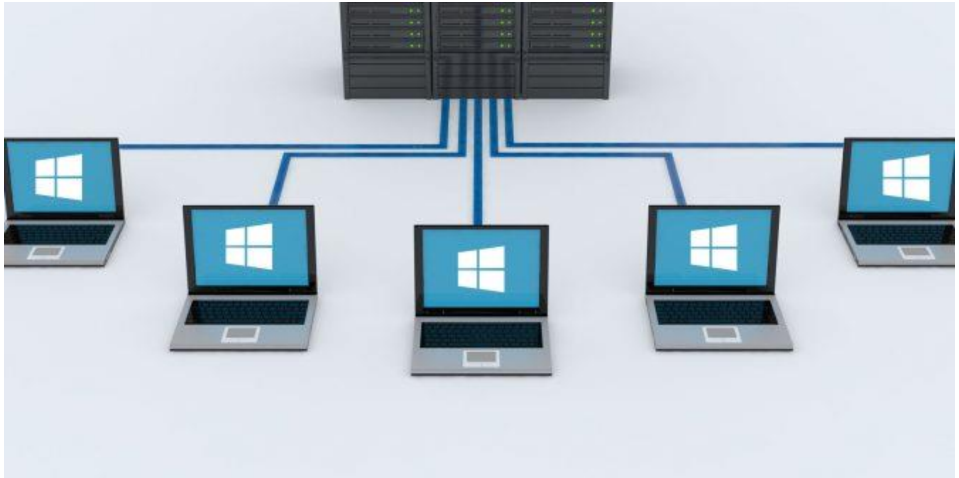
Key: Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}\Count

Value: HRZR_PGYFRFFVBA

Selected hive: SYSTEM Last write: 9/23/2019 12:53:21 AM +00:00 73 of 73 values shown (100.00%) Hidden keys: 0 13

Active Directory (AD)

- Very important… but it does a lot
    - Too much to cover right now!
- TL;DR A domain controller and it enforces security policies, authenticates, and authorized users across a domain



This is the best video I have ever seen on Active Directory: A Cat Explains Active Directory.

Sysinternals

The Sysinternals tool set was created in 1996 by Mark Russinovich were so good that Microsoft bought it and said “yo” just keep working on this this is great. The Windows system internals suite is used just about everywhere.

Tool Name	Function
procexp.exe	Process explorer; basically a better task manager.
autoruns.exe	See all of the activities that run automagically.
Tcpview.exe	See all connections. A better netstat.
sysmon.exe	A program to monitor and log additional events. Highly customizable.
Procmon.exe	Process Monitor, very advanced tool, can see *nearly* everything the machine is doing.

Zimmerman's Tools

When Eric Zimmerman was a Special Agent with the FBI, one of his responsibilities was managing on-scene triage. He started to make tools to parse common forensic artifacts.

They are good. Play with them.

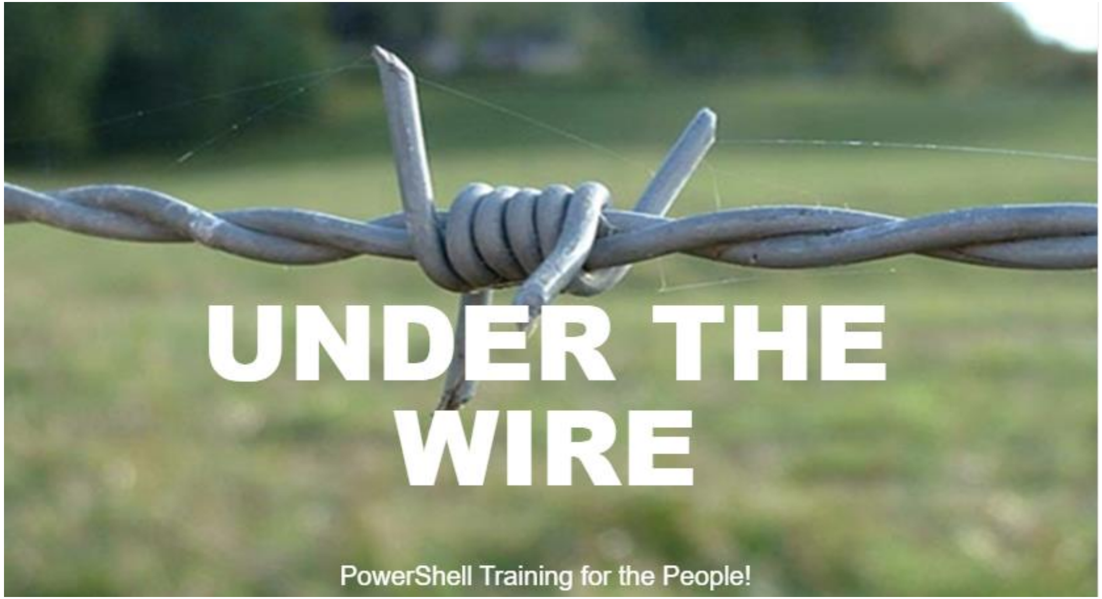
Tool Name	Function
get-zimmermantools	Powershell Script to grab them all
EvtxECmd	Event Log to CSV
MFTECmd	$MFT, $Boot, $J, $SDS To CSV
Registry Explorer	Registry Viewer with bookmarks.
ShellBags Explorer	View ShellBags.

Top 10 Power Rangers Villains | WatchMojo.com

Activity Time!

Here you go! =D

tinyurl.com/**CDOFall19WindowsPrimer**



Additional Resources

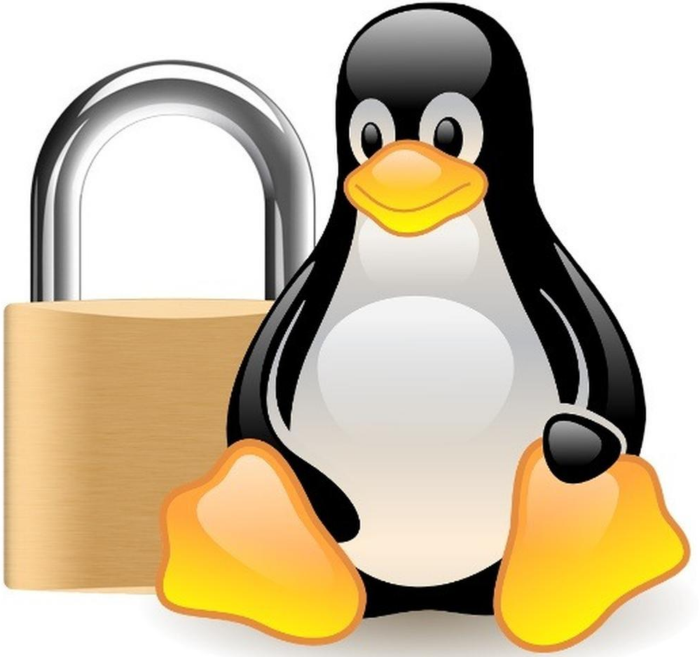
13 Cubed - Intro To Windows Forensics.

Troubleshooting with the Windows Sysinternals Tools - Book for Nerds

IppSec.

Cya Next Time!

Next Week's Workshop will be an Intro to **Linux Security** taught by **Tyler Ritchie**!



Other Student Groups

BB125; 7:15pm.

Certifications Open Forum

Security+

CISA

CRISC

CISSP

Security+

AWS Cloud Security

ISACA®

Student Group

Add us on Social Media!

Twitter: **@ualbanyCDO**

Instagram: **ualbany_cdo**

Website: **uacyber.org**

Myinvolvement: **Cyber Defense Org**

We have a discord!