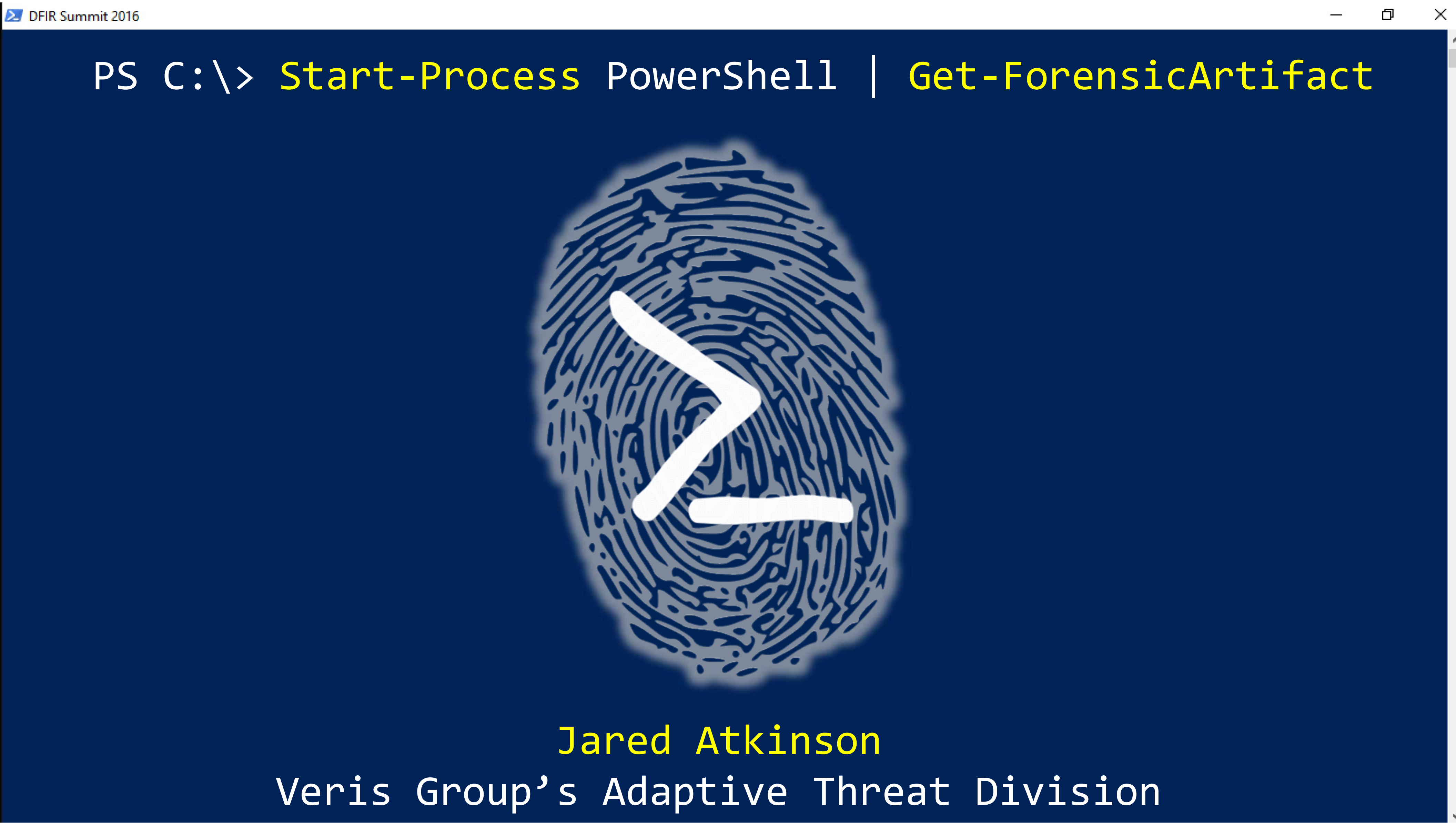


DFIR Summit 2016

```
PS C:\> Start-Process PowerShell | Get-ForensicArtifact
```

Jared Atkinson

Veris Group’s Adaptive Threat Division

VERIS GROUP

@jaredcatkinson

- Jared Atkinson
  - Defensive Services Technical Lead for Adaptive Threat Division
    - Leads the service line responsible for proactive detection and response to advanced threats in Fortune 100 commercial environments
  - Former
    - U.S. Air Force Hunt (2011 – 2015)
  - 2015 Black Hat Minesweeper Champion
  - Moderator of the PowerShell.com “Security Forum”
  - Open Source Developer
    - PowerForensics
    - Uproot IDS
    - WMIEventing
  - Researcher of forensic artifact file formats

ATD

PowerForensics

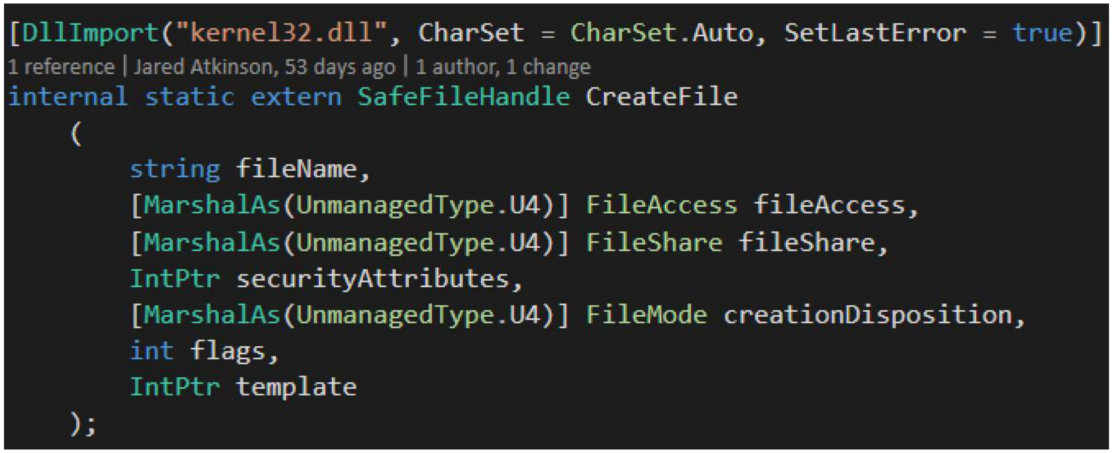
- PowerShell Module for Live Forensic Investigation
  - www.github.com/Invoke-IR/PowerForensics
- Binary Module (Compiled C# DLL)
- Minimizes Use of Windows APIs
- Currently Parses:
  - NTFS Data Structures
  - Windows Specific Data Structures
    - Windows Registry
    - Windows Event Log
    - Scheduled Jobs
    - Prefetch Files

Design Requirements

- **Forensically sound**
  - Parse raw disk structures
  - Don’t alter NTFS timestamps
- Can execute on a live (running) host
- Operationally fast
  - Collect forensic data in seconds or minutes
- Modular capabilities
  - Cmdlets perform discrete tasks and can be tied together for more complicated tasks
- Capable of working remotely
  - At the proof of concept stage

Reading a Disk/Volume’s Contents

- CreateFile API
  - Used to create a read handle to Physical Disk or Logical Volume
- FileStream Read Method
  - Used to read from the handle



```
[DllImport("kernel32.dll", CharSet = CharSet.Auto, SetLastError = true)]
1 reference | Jared Atkinson, 53 days ago | 1 author, 1 change
internal static extern SafeFileHandle CreateFile
    (
        string fileName,
        [MarshalAs(UnmanagedType.U4)] FileAccess fileAccess,
        [MarshalAs(UnmanagedType.U4)] FileShare fileShare,
        IntPtr securityAttributes,
        [MarshalAs(UnmanagedType.U4)] FileMode creationDisposition,
        int flags,
        IntPtr template
    );
```

MASTER BOOT RECORD

>_INVOKE-IR

BY: JARED ATKINSON
TEMPLATE BY: ANGE ALBERTINI

```
000: 33 C0 8E D0 BC 00 7C 8E C0 8E D8 BE 00 7C BF 00
010: 06 B9 00 02 FC F3 A4 50 68 1C 06 CB FB B9 04 00
020: BD BE 07 80 7E 00 00 7C 0B 0F 85 0E 01 83 C5 10
030: E2 F1 CD 18 88 56 00 55 C6 46 11 05 C6 46 10 00
040: B4 41 BB AA 55 CD 13 5D 72 0F 81 FB 55 AA 75 09
050: F7 C1 01 00 74 03 FE 46 10 66 60 80 7E 10 00 74
060: 26 66 68 00 00 00 00 66 FF 76 08 68 00 00 68 00
070: 7C 68 01 00 68 10 00 B4 42 8A 56 00 8B F4 CD 13
080: 9F 83 C4 10 9E EB 14 B8 01 02 BB 00 7C 8A 56 00
090: 8A 76 01 8A 4E 02 8A 6E 03 CD 13 66 61 73 1C FE
0A0: 4E 11 75 0C 80 7E 00 80 0F 84 8A 00 B2 80 EB 84
0B0: 55 32 E4 8A 56 00 CD 13 5D EB 9E 81 3E FE 7D 55
0C0: AA 75 6E FF 76 00 E8 8D 00 75 17 FA B0 D1 E6 64
0D0: E8 83 00 B0 DF E6 60 E8 7C 00 B0 FF E6 64 E8 75
0E0: 00 FB B8 00 BB CD 1A 66 23 C0 75 3B 66 81 FB 54
0F0: 43 50 41 75 32 81 F9 02 01 72 2C 66 68 07 BB 00
100: 00 66 68 00 02 00 00 66 68 08 00 00 00 66 53 66
110: 53 66 55 66 68 00 00 00 00 66 68 00 7C 00 00 66
120: 61 68 00 00 07 CD 1A 5A 32 F6 EA 00 7C 00 00 CD
130: 18 A0 B7 07 EB 08 A0 B6 07 EB 03 A0 B5 07 32 E4
140: 05 00 07 8B F0 AC 3C 00 74 09 BB 07 00 B4 0E CD
150: 10 EB F2 F4 EB FD 2B C9 E4 64 EB 00 24 02 E0 F8
160: 24 02 C3 49 6E 76 61 6C 69 64 20 70 61 72 74 69
170: 74 69 6F 6E 20 74 61 62 6C 65 00 45 72 72 6F 72
180: 20 6C 6F 61 64 69 6E 67 20 6F 70 65 72 61 74 69
190: 6E 67 20 73 79 73 74 65 6D 00 4D 69 73 73 69 6E
1A0: 67 20 6F 70 65 72 61 74 69 6E 67 20 73 79 73 74
1B0: 65 6D 00 00 00 63 7B 9A 82 D4 BA 7D 00 00 00 20
1C0: 21 00 07 FE FF FF 00 08 00 00 00 90 36 06 80 FE
1D0: FF FF 07 FE FF FF 00 A0 36 06 00 60 09 00 00 00
1E0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
1F0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 AA
```

PARTITION TYPES

0x00 - EMPTY	0x83 - LINUX
0x01 - FAT12	0x84 - HIBERNATION
0x04 - FAT16	0x85 - LINUX_EXTENDED
0x05 - MS_EXTENDED	0x86 - NTFS_VOLUME_SET
0x06 - FAT16	0x87 - NTFS_VOLUME_SET_1
0x07 - NTFS	0xa0 - HIBERNATION_1
0x0b - FAT32	0xa1 - HIBERNATION_2
0x0c - FAT32	0xa5 - FREEBSD
0x0e - FAT16	0xa6 - OPENBSD
0x0f - MS_EXTENDED	0xa8 - MACOSX
0x11 - HIDDEN_FAT12	0xa9 - NETBSD
0x14 - HIDDEN_FAT16	0xab - MAC_OSX_BOOT
0x16 - HIDDEN_FAT16	0xb7 - BSDI
0x1b - HIDDEN_FAT32	0xb8 - BSDI_SWAP
0x1c - HIDDEN_FAT32	0xee - EFI_GPT_DISK
0x1e - HIDDEN_FAT16	0xef - EFI_SYSTEM_PARTITION
0x42 - MS_MBR_DYNAMIC	0xfb - VMWARE_FILE_SYSTEM
0x82 - SOLARIS_X86	0xfc - VMWARE_SWAP
0x82 - LINUX_SWAP	

BOOT CODE

FIELDS	VALUES
jump to boot program	
disk parameters	
boot program code	
disk signature	82D4BA7D

CHS ADDRESSING

```
00100000 00100001 00000000
--------------------------
00100000 100001 0000000000
    Head - 1st byte
  Sector - 2nd byte (0-5 bits)
Cylinder - 2nd byte (6-7 bits)
           3rd byte
```

PARTITION TABLE

FIELDS	VALUES
status	0x00 - Non-Bootable
starting head	0x20
starting sector	0x21
starting cylinder	0x00
partition type	0x07 - NTFS
ending head	0xFE
ending sector	0x3F
ending cylinder	0x3FF
relative start sector	0x800
total sectors	0x6369000

FIELDS	VALUES
status	0x80 - Bootable
starting head	0xFE
starting sector	0x3F
starting cylinder	0x3FF
partition type	0x07 - NTFS
ending head	0xFE
ending sector	0x3F
ending cylinder	0x3FF
relative start sector	0x636A000
total sectors	0x96000

FIELDS	VALUES
partition type	0x00 - EMPTY

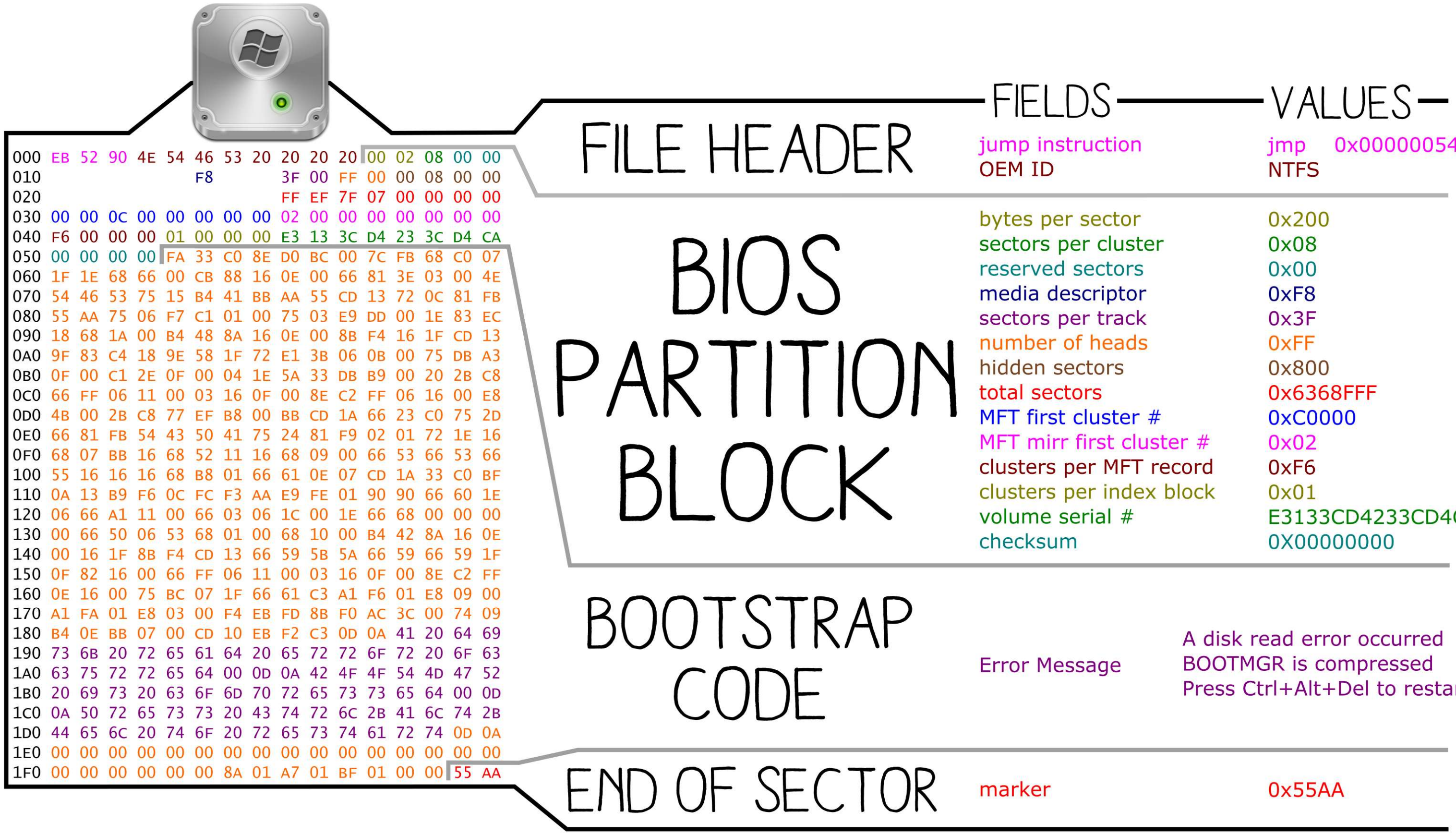
FIELDS	VALUES
partition type	0x00 - EMPTY

END OF MBR

FIELDS	VALUES
marker	0x55AA

NTFS
Volume Boot Record

BY: JARED ATKINSON
TEMPLATE BY: ANGE ALBERTINI



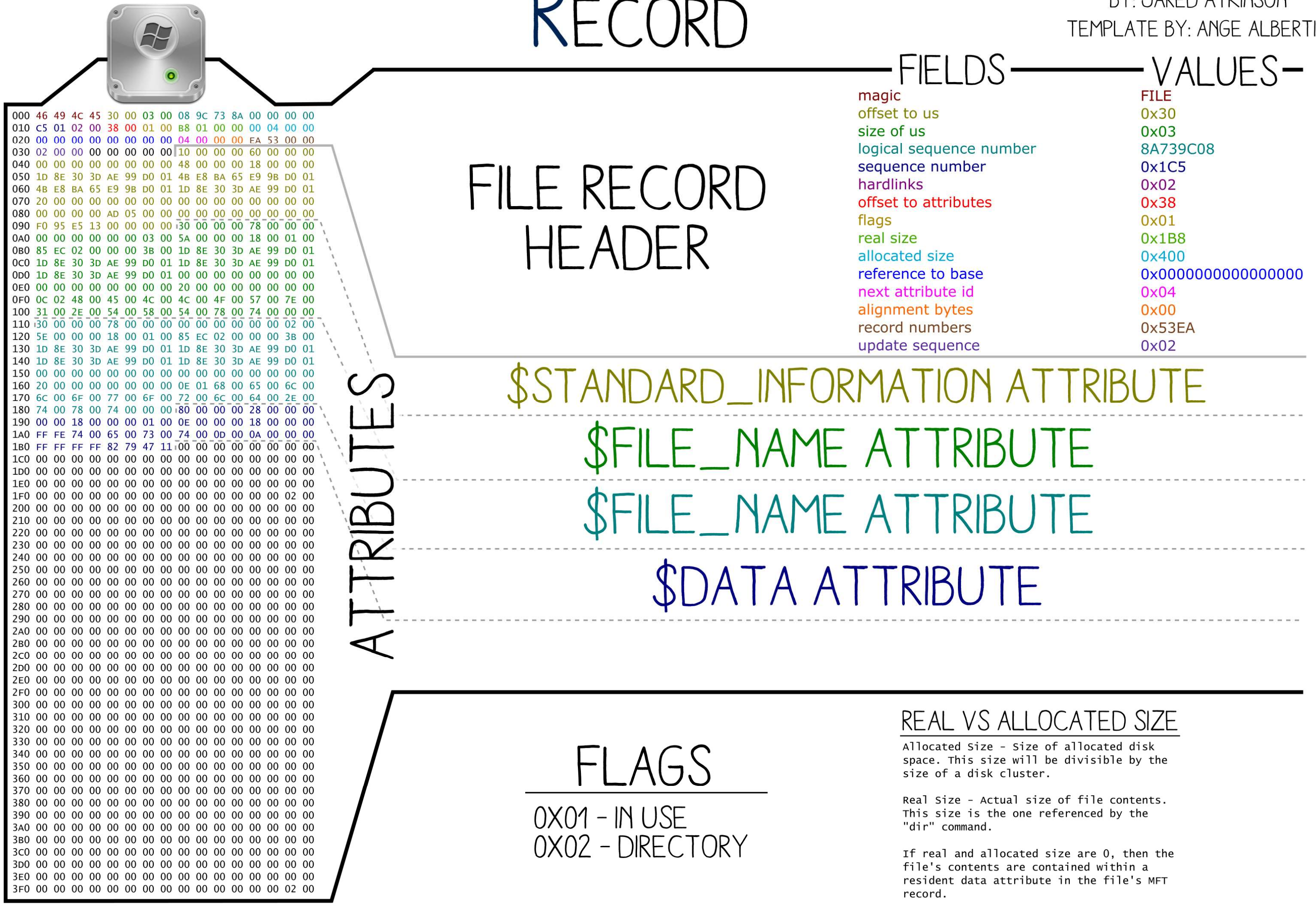
```
000 EB 52 90 4E 54 46 53 20 20 20 20 00 02 08 00 00
010                F8       3F 00 FF 00 00 08 00 00
020                         FF EF 7F 07 00 00 00 00
030 00 00 0C 00 00 00 00 00 02 00 00 00 00 00 00 00
040 F6 00 00 00 01 00 00 00 E3 13 3C D4 23 3C D4 CA
050 00 00 00 00 FA 33 C0 8E D0 BC 00 7C FB 68 C0 07
060 1F 1E 68 66 00 CB 88 16 0E 00 66 81 3E 03 00 4E
070 54 46 53 75 15 B4 41 BB AA 55 CD 13 72 0C 81 FB
080 55 AA 75 06 F7 C1 01 00 75 03 E9 DD 00 1E 83 EC
090 18 68 1A 00 B4 48 8A 16 0E 00 8B F4 16 1F CD 13
0A0 9F 83 C4 18 9E 58 1F 72 E1 3B 06 0B 00 75 DB A3
0B0 0F 00 C1 2E 0F 00 04 1E 5A 33 DB B9 00 20 2B C8
0C0 66 FF 06 11 00 03 16 0F 00 8E C2 FF 06 16 00 E8
0D0 4B 00 2B C8 77 EF B8 00 BB CD 1A 66 23 C0 75 2D
0E0 66 81 FB 54 43 50 41 75 24 81 F9 02 01 72 1E 16
0F0 68 07 BB 16 68 52 11 16 68 09 00 66 53 66 53 66
100 55 16 16 16 68 B8 01 66 61 0E 07 CD 1A 33 C0 BF
110 0A 13 B9 F6 0C FC F3 AA E9 FE 01 90 90 66 60 1E
120 06 66 A1 11 00 66 03 06 1C 00 1E 66 68 00 00 00
130 00 66 50 06 53 68 01 00 68 10 00 B4 42 8A 16 0E
140 00 16 1F 8B F4 CD 13 66 59 5B 5A 66 59 66 59 1F
150 0F 82 16 00 66 FF 06 11 00 03 16 0F 00 8E C2 FF
160 0E 16 00 75 BC 07 1F 66 61 C3 A1 F6 01 E8 09 00
170 A1 FA 01 E8 03 00 F4 EB FD 8B F0 AC 3C 00 74 09
180 B4 0E BB 07 00 CD 10 EB F2 C3 0D 0A 41 20 64 69
190 73 6B 20 72 65 61 64 20 65 72 72 6F 72 20 6F 63
1A0 63 75 72 72 65 64 00 0D 0A 42 4F 4F 54 4D 47 52
1B0 20 69 73 20 63 6F 6D 70 72 65 73 73 65 64 00 0D
1C0 0A 50 72 65 73 73 20 43 74 72 6C 2B 41 6C 74 2B
1D0 44 65 6C 20 74 6F 20 72 65 73 74 61 72 74 0D 0A
1E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
1F0 00 00 00 00 00 00 8A 01 A7 01 BF 01 00 00 55 AA
```

	FIELDS	VALUES
FILE HEADER	jump instruction	jmp 0x00000054
	OEM ID	NTFS
BIOS PARTITION BLOCK	bytes per sector	0x200
	sectors per cluster	0x08
	reserved sectors	0x00
	media descriptor	0xF8
	sectors per track	0x3F
	number of heads	0xFF
	hidden sectors	0x800
	total sectors	0x6368FFF
	MFT first cluster #	0xC0000
	MFT mirr first cluster #	0x02
	clusters per MFT record	0xF6
	clusters per index block	0x01
	volume serial #	E3133CD4233CD4CA
	checksum	0X00000000
BOOTSTRAP CODE	Error Message	A disk read error occurred BOOTMGR is compressed Press Ctrl+Alt+Del to restart
END OF SECTOR	marker	0x55AA

Master File Table Record

>_INVOKE-IR

BY: JARED ATKINSON
TEMPLATE BY: ANGE ALBERTINI



```
000 46 49 4C 45 30 00 03 00 08 9C 73 8A 00 00 00 00
010 C5 01 02 00 38 00 01 00 B8 01 00 00 00 04 00 00
020 00 00 00 00 00 00 00 00 04 00 00 00 EA 53 00 00
030 02 00 00 00 00 00 00 00 10 00 00 00 60 00 00 00
040 00 00 00 00 00 00 00 00 48 00 00 00 18 00 00 00
050 1D 8E 30 3D AE 99 D0 01 4B E8 BA 65 E9 9B D0 01
060 4B E8 BA 65 E9 9B D0 01 1D 8E 30 3D AE 99 D0 01
070 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
080 00 00 00 00 AD 05 00 00 00 00 00 00 00 00 00 00
090 F0 95 E5 13 00 00 00 00 30 00 00 00 78 00 00 00
0A0 00 00 00 00 00 00 03 00 5A 00 00 00 18 00 01 00
0B0 85 EC 02 00 00 00 3B 00 1D 8E 30 3D AE 99 D0 01
0C0 1D 8E 30 3D AE 99 D0 01 1D 8E 30 3D AE 99 D0 01
0D0 1D 8E 30 3D AE 99 D0 01 00 00 00 00 00 00 00 00
0E0 00 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00
0F0 0C 02 48 00 45 00 4C 00 4C 00 4F 00 57 00 7E 00
100 31 00 2E 00 54 00 58 00 54 00 78 00 74 00 00 00
110 30 00 00 00 78 00 00 00 00 00 00 00 00 00 02 00
120 5E 00 00 00 18 00 01 00 85 EC 02 00 00 00 3B 00
130 1D 8E 30 3D AE 99 D0 01 1D 8E 30 3D AE 99 D0 01
140 1D 8E 30 3D AE 99 D0 01 1D 8E 30 3D AE 99 D0 01
150 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
160 20 00 00 00 00 00 00 00 0E 01 68 00 65 00 6C 00
170 6C 00 6F 00 77 00 6F 00 72 00 6C 00 64 00 2E 00
180 74 00 78 00 74 00 00 00 80 00 00 00 28 00 00 00
190 00 00 18 00 00 00 01 00 0E 00 00 00 18 00 00 00
1A0 FF FE 74 00 65 00 73 00 74 00 0D 00 0A 00 00 00
1B0 FF FF FF FF 82 79 47 11 00 00 00 00 00 00 00 00
1C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
1D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
1E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
1F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00
200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
210 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
220 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
230 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
240 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
250 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
260 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
270 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
280 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
290 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
2A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
2B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
2C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
2D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
2E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
2F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
300 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
310 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
320 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
330 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
340 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
350 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
360 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
370 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
380 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
390 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
3A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
3B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
3C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
3D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
3E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
3F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00
```

FILE RECORD HEADER

FIELDS	VALUES
magic	FILE
offset to us	0x30
size of us	0x03
logical sequence number	8A739C08
sequence number	0x1C5
hardlinks	0x02
offset to attributes	0x38
flags	0x01
real size	0x1B8
allocated size	0x400
reference to base	0x0000000000000000
next attribute id	0x04
alignment bytes	0x00
record numbers	0x53EA
update sequence	0x02

ATTRIBUTES

$STANDARD_INFORMATION ATTRIBUTE

$FILE_NAME ATTRIBUTE

$FILE_NAME ATTRIBUTE

$DATA ATTRIBUTE

FLAGS

0X01 - IN USE
0X02 - DIRECTORY

REAL VS ALLOCATED SIZE

Allocated Size - Size of allocated disk space. This size will be divisible by the size of a disk cluster.

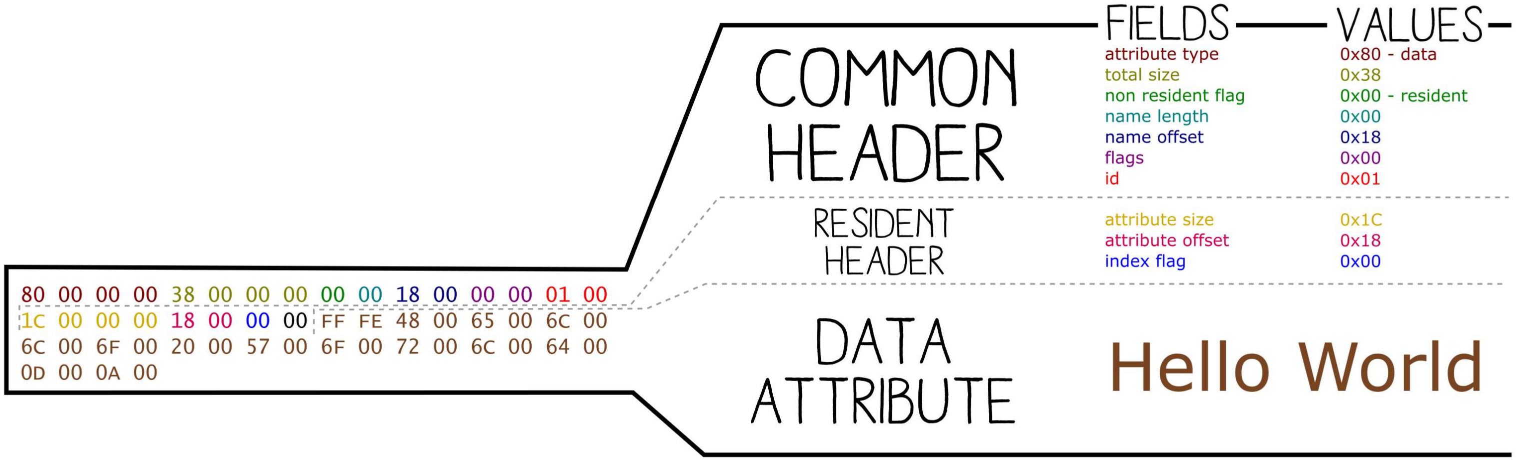
Real Size - Actual size of file contents. This size is the one referenced by the "dir" command.

If real and allocated size are 0, then the file's contents are contained within a resident data attribute in the file's MFT record.

$DATA ATTRIBUTE

INVOKE-IR

BY: JARED ATKINSON
TEMPLATE BY: ANGE ALBERTINI



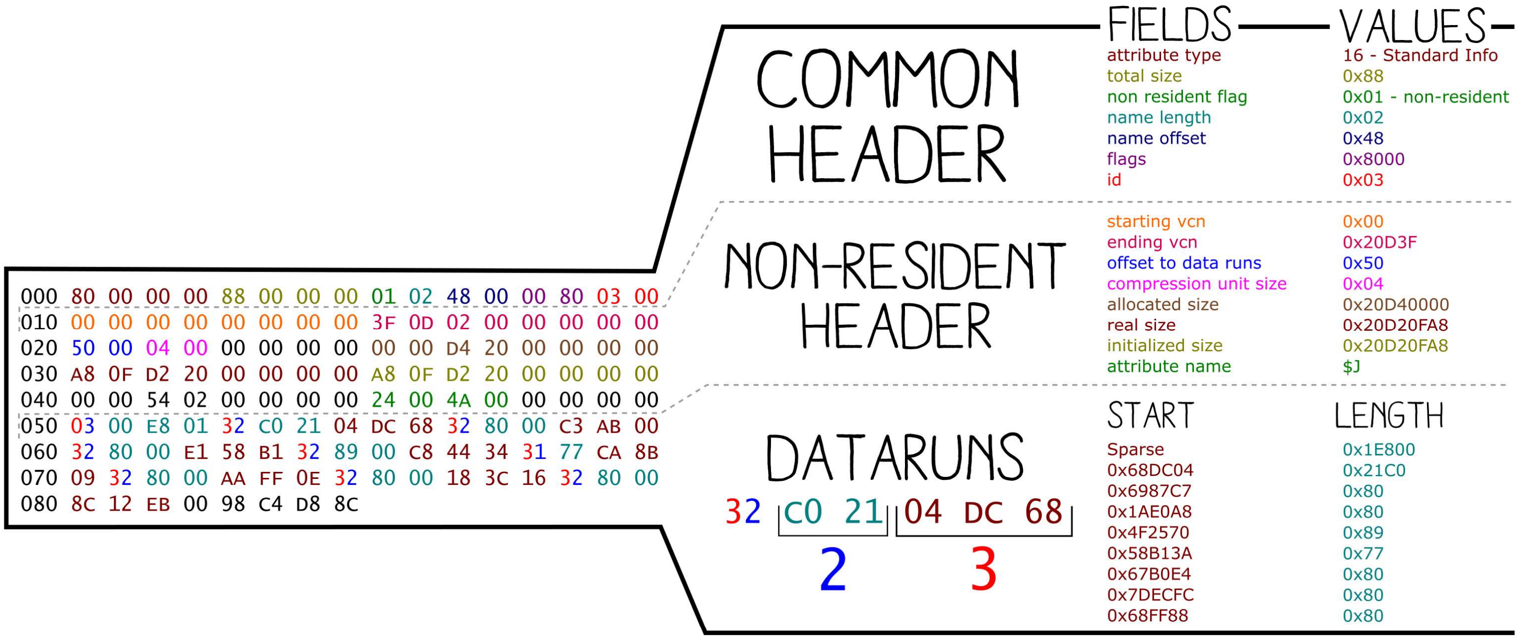
```
80 00 00 00 38 00 00 00 00 00 18 00 00 00 01 00
1C 00 00 00 18 00 00 00 FF FE 48 00 65 00 6C 00
6C 00 6F 00 20 00 57 00 6F 00 72 00 6C 00 64 00
0D 00 0A 00
```

	FIELDS	VALUES
COMMON HEADER	attribute type	0x80 - data
	total size	0x38
	non resident flag	0x00 - resident
	name length	0x00
	name offset	0x18
	flags	0x00
	id	0x01
RESIDENT HEADER	attribute size	0x1C
	attribute offset	0x18
	index flag	0x00
DATA ATTRIBUTE	Hello World	

NON-RESIDENT ATTRIBUTE

>_ INVOKE-IR

BY: JARED ATKINSON
TEMPLATE BY: ANGE ALBERTINI



```
000 80 00 00 00 88 00 00 00 01 02 48 00 00 80 03 00
010 00 00 00 00 00 00 00 00 3F 0D 02 00 00 00 00 00
020 50 00 04 00 00 00 00 00 00 00 D4 20 00 00 00 00
030 A8 0F D2 20 00 00 00 00 A8 0F D2 20 00 00 00 00
040 00 00 54 02 00 00 00 00 24 00 4A 00 00 00 00 00
050 03 00 E8 01 32 C0 21 04 DC 68 32 80 00 C3 AB 00
060 32 80 00 E1 58 B1 32 89 00 C8 44 34 31 77 CA 8B
070 09 32 80 00 AA FF 0E 32 80 00 18 3C 16 32 80 00
080 8C 12 EB 00 98 C4 D8 8C
```

COMMON HEADER

FIELDS	VALUES
attribute type	16 - Standard Info
total size	0x88
non resident flag	0x01 - non-resident
name length	0x02
name offset	0x48
flags	0x8000
id	0x03

NON-RESIDENT HEADER

FIELDS	VALUES
starting vcn	0x00
ending vcn	0x20D3F
offset to data runs	0x50
compression unit size	0x04
allocated size	0x20D40000
real size	0x20D20FA8
initialized size	0x20D20FA8
attribute name	$J

DATARUNS

$$32\ \underbrace{C0\ 21}_{2}\ \underbrace{04\ DC\ 68}_{3}$$

START	LENGTH
Sparse	0x1E800
0x68DC04	0x21C0
0x6987C7	0x80
0x1AE0A8	0x80
0x4F2570	0x89
0x58B13A	0x77
0x67B0E4	0x80
0x7DECFC	0x80
0x68FF88	0x80

Demo:
Web Server Investigation

This demo is based on the @security4arabs Digital Forensics challenge by @binaryz0ne. To download a copy of the challenge please visit http://goo.gl/CVoEpo.

Situation

- Client does not provide much information:
  - Believes their Web Server has been compromised
  - Provides a forensic image to investigate
- Investigator must:
  - Find a temporal starting point
  - Determine if the web server has in fact been compromised
  - If compromised, provide leads for Incident Responders

Demo Video

https://youtu.be/Vh_UFnCgVkw

Initial Findings

- Time: 9/3/2015 6:49:23 AM
- Some sort of brute forcing (sqlmap?)
- Possible Attacker IP Address
    - 192.168.56.102
- Webshell Created
    - webshells.zip
    - c99.php
    - webshell.php
    - phpshell2.php

Demo
Timeline Visualization

This demo is based on Ryan Benson’s (@_RyanBenson) blog post (http://www.obsidianforensics.com/blog/finding-the-first-thread-with-visualization) where he describes leveraging Gource (http://gource.io/) to visualize a forensic timeline.

Timeline Visualization Demo

https://youtu.be/v5mYegFG1DA

The Future of PowerForensics

- Multiple File System Support
    - Extended File System (Ext2/3/4)
    - Hierarchical File System (HFS/HFS+)
    - File Allocation Table (FAT12/16/32)
- Additional Artifacts
    - SQLite
    - ESE Database
- WinPE + PowerForensics
- Remote Capabilities
    - PowerForensics Portable
- Community Involvement!