Data Protection and the Management of Malware Using A WIM PE

Joseph Gentile

Seidenberg School of CSIS

Pace University

Pleasantville, NY 10570 USA

Gentilejoseph92@gmail.com

The Rise of Cyber Crimes

- Cyber crimes are growing exponentially
- The more secure, the more at risk
- Destruction, disruption, degradation, dos
- Considered more of a threat than terrorism
- More of a risk than physical theft
- Low apprehension rate

The Root of the Issue

- Money
- Time
- Constant Evolution
- The internet itself

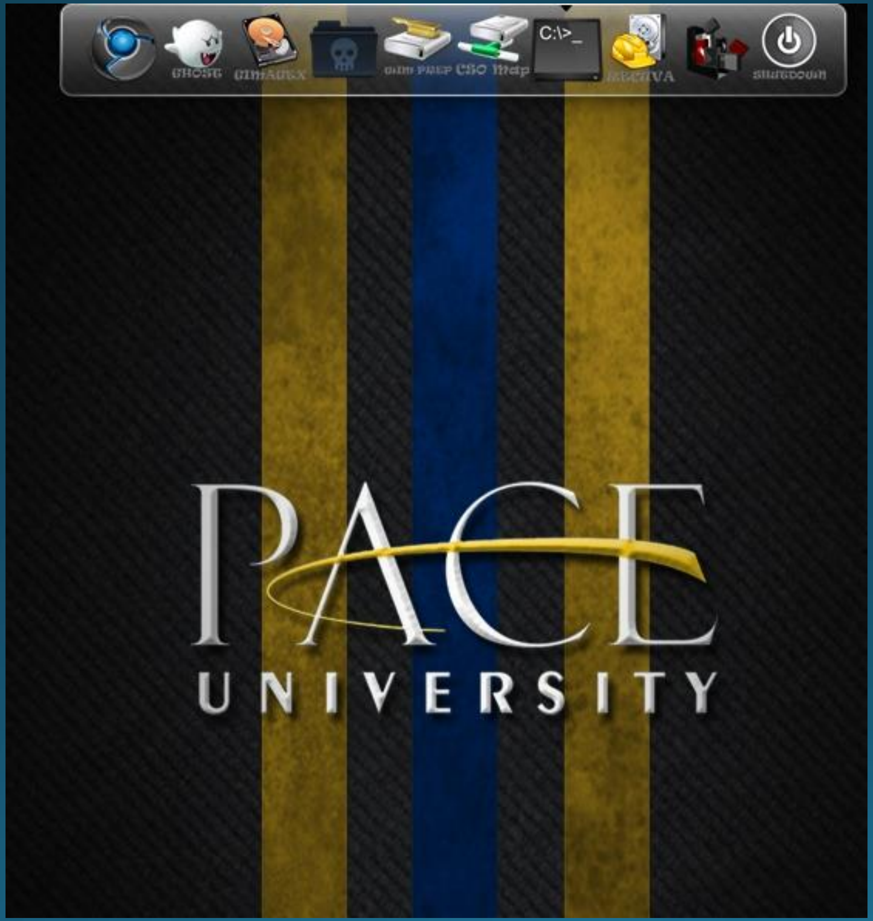
A New Threat

- “Crypto”-Viruses
- The risk of server infection
- Lack of a solution

An Alternate Solution

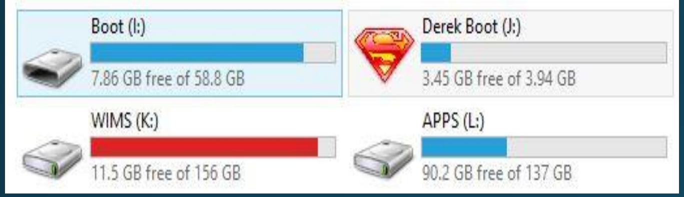
- Training Employees on Malware Management
- Using Windows PE Environments

Windows 8.1 PE



Setup

Partitions



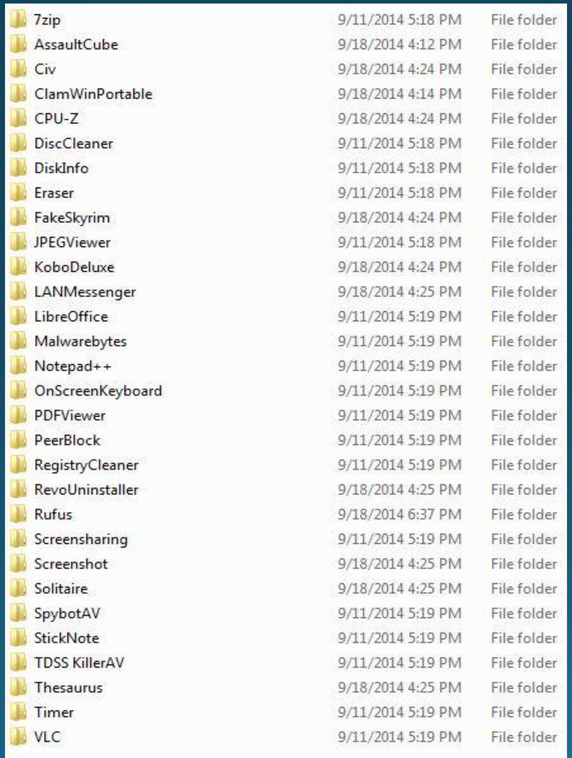
Boot (I:)
7.86 GB free of 58.8 GB

Derek Boot (J:)
3.45 GB free of 3.94 GB

WIMS (K:)
11.5 GB free of 156 GB

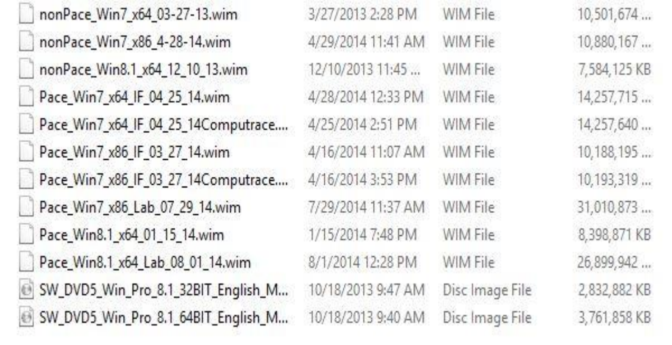
APPS (L:)
90.2 GB free of 137 GB

Portable Apps



7zip	9/11/2014 5:18 PM	File folder
AssaultCube	9/18/2014 4:12 PM	File folder
Civ	9/18/2014 4:24 PM	File folder
ClamWinPortable	9/18/2014 4:14 PM	File folder
CPU-Z	9/18/2014 4:24 PM	File folder
DiscCleaner	9/11/2014 5:18 PM	File folder
DiskInfo	9/11/2014 5:18 PM	File folder
Eraser	9/11/2014 5:18 PM	File folder
FakeSkyrim	9/18/2014 4:24 PM	File folder
JPEGViewer	9/11/2014 5:18 PM	File folder
KoboDeluxe	9/18/2014 4:24 PM	File folder
LANMessenger	9/18/2014 4:25 PM	File folder
LibreOffice	9/11/2014 5:19 PM	File folder
Malwarebytes	9/11/2014 5:19 PM	File folder
Notepad++	9/11/2014 5:19 PM	File folder
OnScreenKeyboard	9/11/2014 5:19 PM	File folder
PDFViewer	9/11/2014 5:19 PM	File folder
PeerBlock	9/11/2014 5:19 PM	File folder
RegistryCleaner	9/11/2014 5:19 PM	File folder
RevoUninstaller	9/18/2014 4:25 PM	File folder
Rufus	9/18/2014 6:37 PM	File folder
Screensharing	9/11/2014 5:19 PM	File folder
Screenshot	9/18/2014 4:25 PM	File folder
Solitaire	9/18/2014 4:25 PM	File folder
SpybotAV	9/11/2014 5:19 PM	File folder
StickNote	9/11/2014 5:19 PM	File folder
TDSS KillerAV	9/11/2014 5:19 PM	File folder
Thesaurus	9/18/2014 4:25 PM	File folder
Timer	9/11/2014 5:19 PM	File folder
VLC	9/11/2014 5:19 PM	File folder

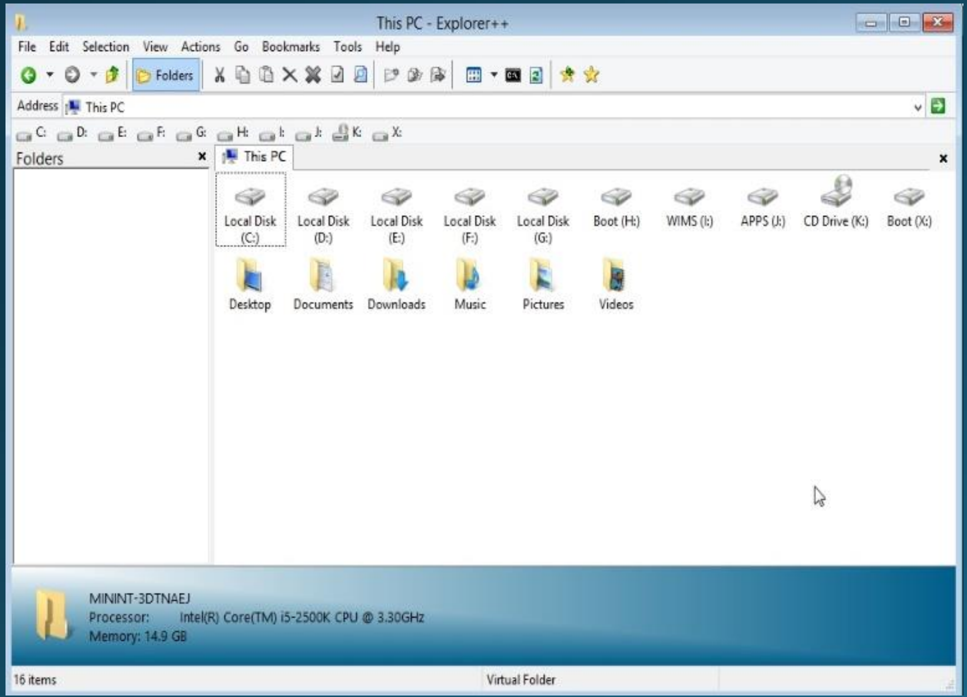
WIM Images



nonPace_Win7_x64_03-27-13.wim	3/27/2013 2:28 PM	WIM File	10,501,674 ...
nonPace_Win7_x86_4-28-14.wim	4/29/2014 11:41 AM	WIM File	10,880,167 ...
nonPace_Win8.1_x64_12_10_13.wim	12/10/2013 11:45 ...	WIM File	7,584,125 KB
Pace_Win7_x64_IF_04_25_14.wim	4/28/2014 12:33 PM	WIM File	14,257,715 ...
Pace_Win7_x64_IF_04_25_14Computrace....	4/25/2014 2:51 PM	WIM File	14,257,640 ...
Pace_Win7_x86_IF_03_27_14.wim	4/16/2014 11:07 AM	WIM File	10,188,195 ...
Pace_Win7_x86_IF_03_27_14Computrace....	4/16/2014 3:53 PM	WIM File	10,193,319 ...
Pace_Win7_x86_Lab_07_29_14.wim	7/29/2014 11:37 AM	WIM File	31,010,873 ...
Pace_Win8.1_x64_01_15_14.wim	1/15/2014 7:48 PM	WIM File	8,398,871 KB
Pace_Win8.1_x64_Lab_08_01_14.wim	8/1/2014 12:28 PM	WIM File	26,899,942 ...
SW_DVD5_Win_Pro_8.1_32BIT_English_M...	10/18/2013 9:47 AM	Disc Image File	2,832,882 KB
SW_DVD5_Win_Pro_8.1_64BIT_English_M...	10/18/2013 9:40 AM	Disc Image File	3,761,858 KB

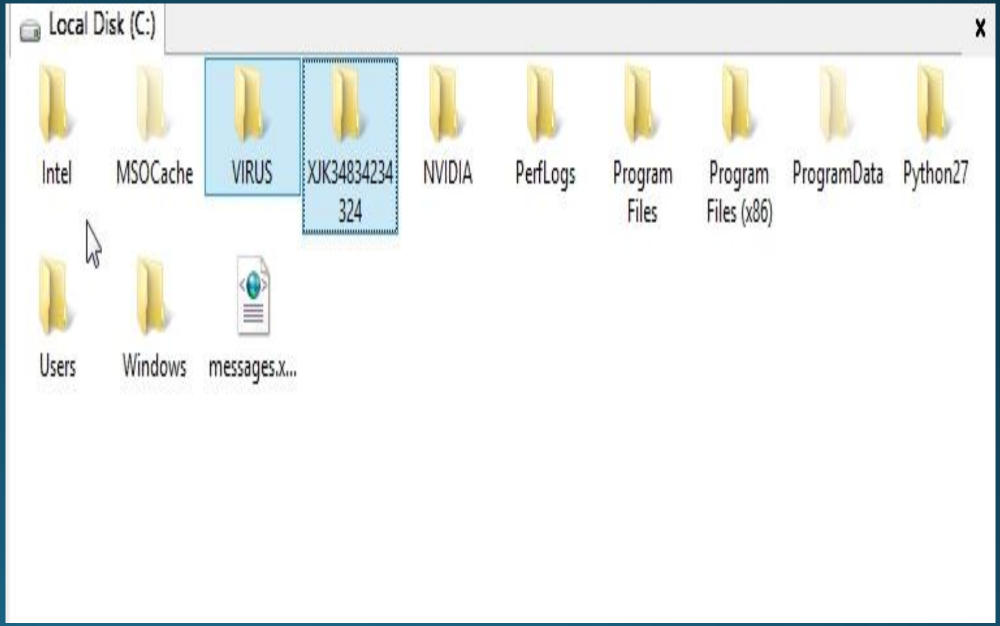
File Explorer

- Allows for document access / backup

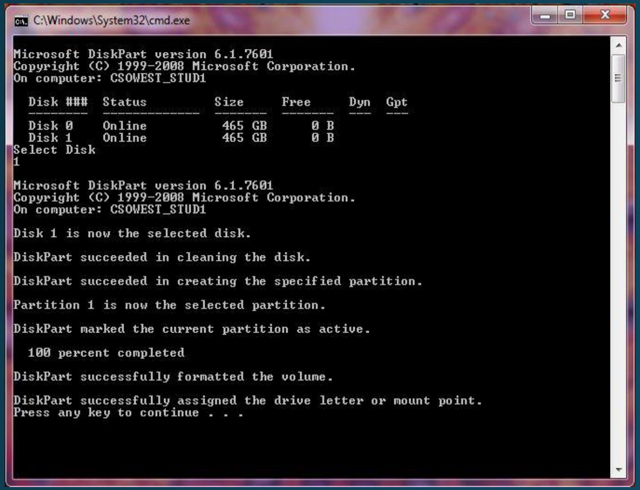


MININT-3DTNAEJ
Processor: Intel(R) Core(TM) i5-2500K CPU @ 3.30GHz
Memory: 14.9 GB

16 items | Virtual Folder

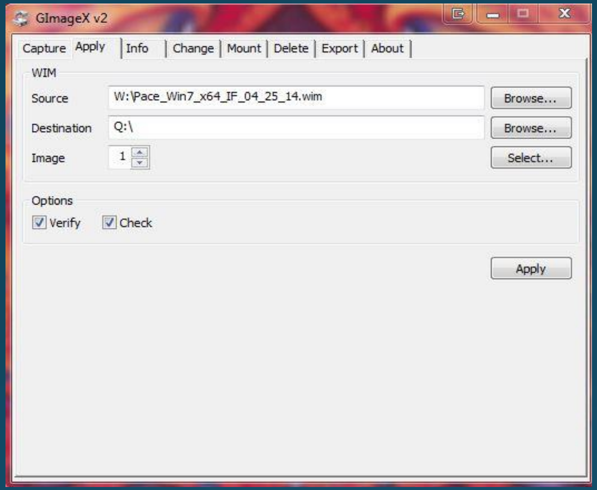


Using a PE for re-imaging



```
Microsoft DiskPart version 6.1.7601
Copyright (C) 1999-2008 Microsoft Corporation.
On computer: CSOWEST_STUD1

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online          465 GB      0 B
  Disk 1    Online          465 GB      0 B
Select Disk
1

Microsoft DiskPart version 6.1.7601
Copyright (C) 1999-2008 Microsoft Corporation.
On computer: CSOWEST_STUD1

Disk 1 is now the selected disk.

DiskPart succeeded in cleaning the disk.

DiskPart succeeded in creating the specified partition.

Partition 1 is now the selected partition.

DiskPart marked the current partition as active.

  100 percent completed

DiskPart successfully formatted the volume.

DiskPart successfully assigned the drive letter or mount point.
Press any key to continue . . .
```

Wim Prep

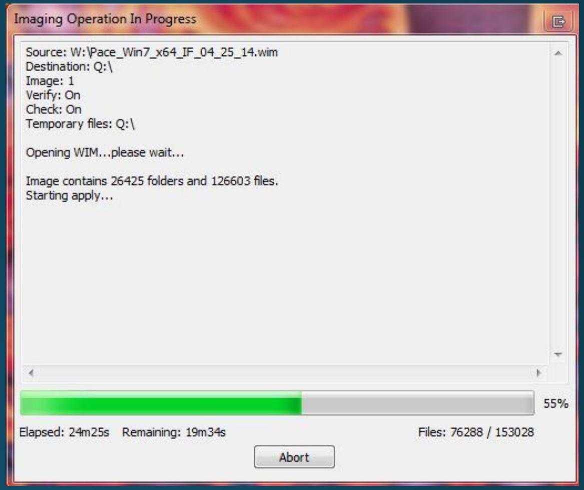


Source: W:\Pace_Win7_x64_IF_04_25_14.wim

Destination: Q:\

Image: 1

☑ Verify ☑ Check



```
Source: W:\Pace_Win7_x64_IF_04_25_14.wim
Destination: Q:\
Image: 1
Verify: On
Check: On
Temporary files: Q:\

Opening WIM...please wait...

Image contains 26425 folders and 126603 files.
Starting apply...
```

55%

Elapsed: 24m25s Remaining: 19m34s Files: 76288 / 153028

GImageX

Conclusions

- Trained Employees
- Lower Costs
- Lowered Risk