



How to Customize Symantec Endpoint Recovery Tool

Efrain Ortiz
Distinguished Systems Engineer

Overview

This document provides step-by-step instructions to customize the Symantec Endpoint Recovery Tool. The Symantec Endpoint Recovery Tool is a bootable ISO image provided by Symantec, typically from the <http://fileconnect.symantec.com> site. A SEP product serial number or registered license will be required to download from Fileconnect. The SERT disk is used to boot from a CD-ROM drive and scan a system with the main Operating System in a non-running state in order to improve chances of detecting hard to find malware. Instructions in this whitepaper are not supported by Symantec. Instructions provided as-is.

The first objective of the document is to show how to create the SERT Disk with extra utilities for Malware Response. The second objective in this document is to make the customized SERT disk bootable from USB media.

Application	Description
Symantec AntiVirus	Symantec Anvirus Portable Executable Content
Microsoft Autoruns.exe	Microsoft Sysinternals autoruns.exe
Symantec Checksum.exe	Symantec tool for performing checksums and output to file.
AutoIT.exe	Customized AutoIT script to prompt user with questions.
SCP	Secure Copy Utility to provide means to copy files from PE environment to trusted system over SSH.

List of Tools

Legend:	
SERTWorkingDirectory	C:\SERTPROJ\
SERTWimMountDirectory	C:\SERTPROJ\Mount
SERTTargetISOLocation	C:\SERTPROJ\SertPE.iso
WinPEImage	C:\SERTPROJ\bootdisk
SERTSOURCE	C:\SERTPROJ\Symantec_Endpoint_Recovery_Tool_2.0.24_AllWin_EN

Step 1: Download the Symantec Endpoint Recovery Tool ISO from <http://fileconnect.symantec.com> using your serial number or after registering your license.

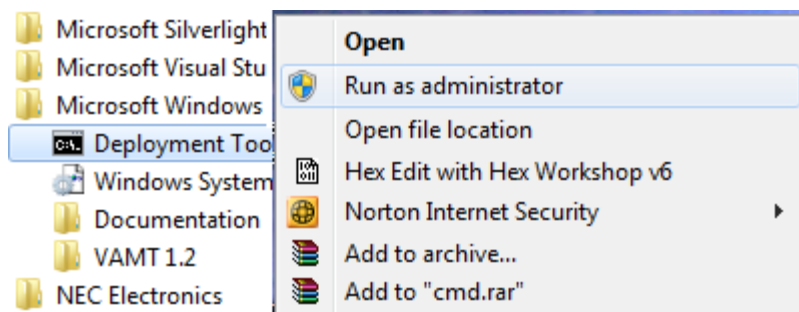
Step 2: Extract the BOOT.wim file from Symantec_Endpoint_Recovery_Tool_2.0.24_AllWin_EN.iso image using one of the following options:

- Mount the "Symantec_Endpoint_Recovery_Tool_2.0.24_AllWin_EN.iso" with an ISO mount utility such as Virtual CD and copy out \Sources\boot.wim to SERTWorkingDirectory.
- Burn the "Symantec_Endpoint_Recovery_Tool_2.0.24_AllWin_EN.iso" to CD-ROM and copy the \Sources\boot.wim to SERTWorkingDirectory.
- Extract "Symantec_Endpoint_Recovery_Tool_2.0.24_AllWin_EN.iso" contents with unzip utility that supports ISO's and copy out the \Sources\BOOT.WIM file to your SERTWorkingdirectory.

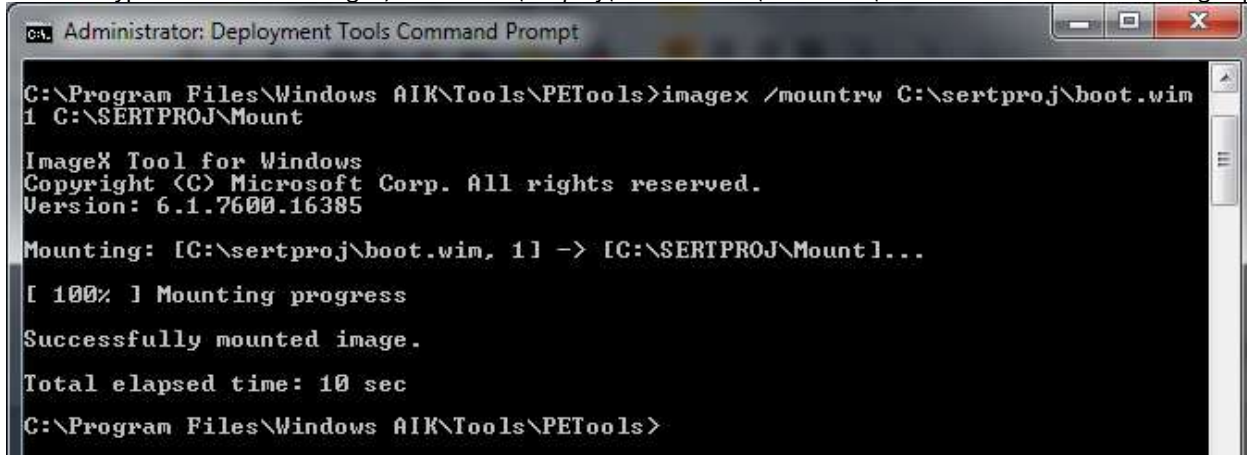
WIM Modification Instructions from Microsoft location: [http://technet.microsoft.com/en-us/library/cc709665\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc709665(WS.10).aspx)

Step 3: Mount the Symantec SERTWorkingDirectory\Boot.wim file for modification

Run "Deployment tools Command Line" as administrator. Start > "All Programs" > "Microsoft Windows AIK" > "Deployment Tools Command Line"



Type the command 'imagex /mountrw C:\sertproj\boot.wim 1 C:\SERTPROJ\Mount' <ENTER> minus the single quotes.



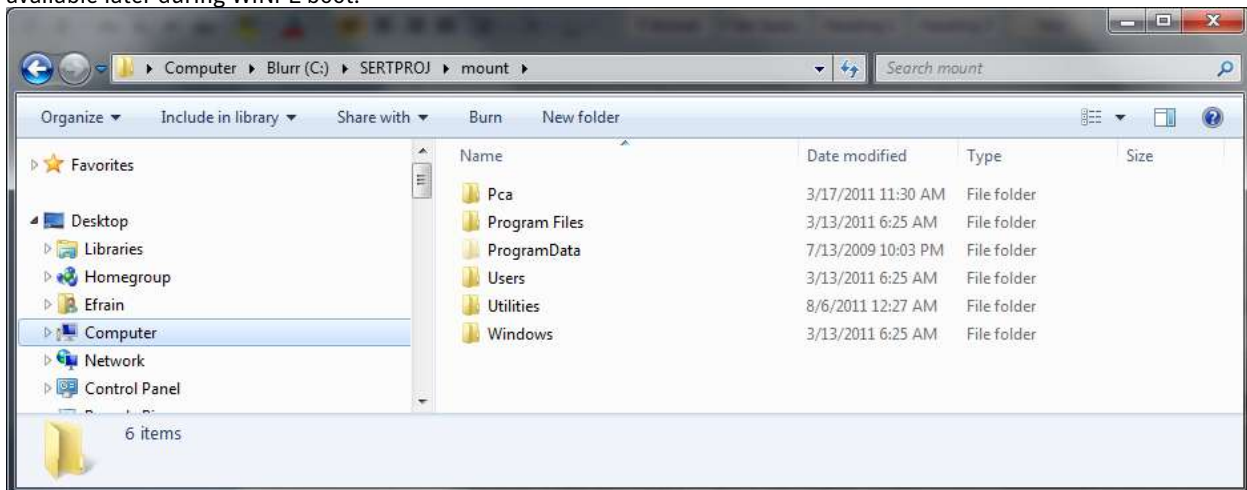
```
C:\Program Files\Windows AIK\Tools\PETools>imagex /mountrw C:\sertproj\boot.wim
1 C:\SERTPROJ\Mount

ImageX Tool for Windows
Copyright (C) Microsoft Corp. All rights reserved.
Version: 6.1.7600.16385

Mounting: [C:\sertproj\boot.wim, 1] -> [C:\SERTPROJ\Mount]...

[ 100% ] Mounting progress
Successfully mounted image.
Total elapsed time: 10 sec
C:\Program Files\Windows AIK\Tools\PETools>
```

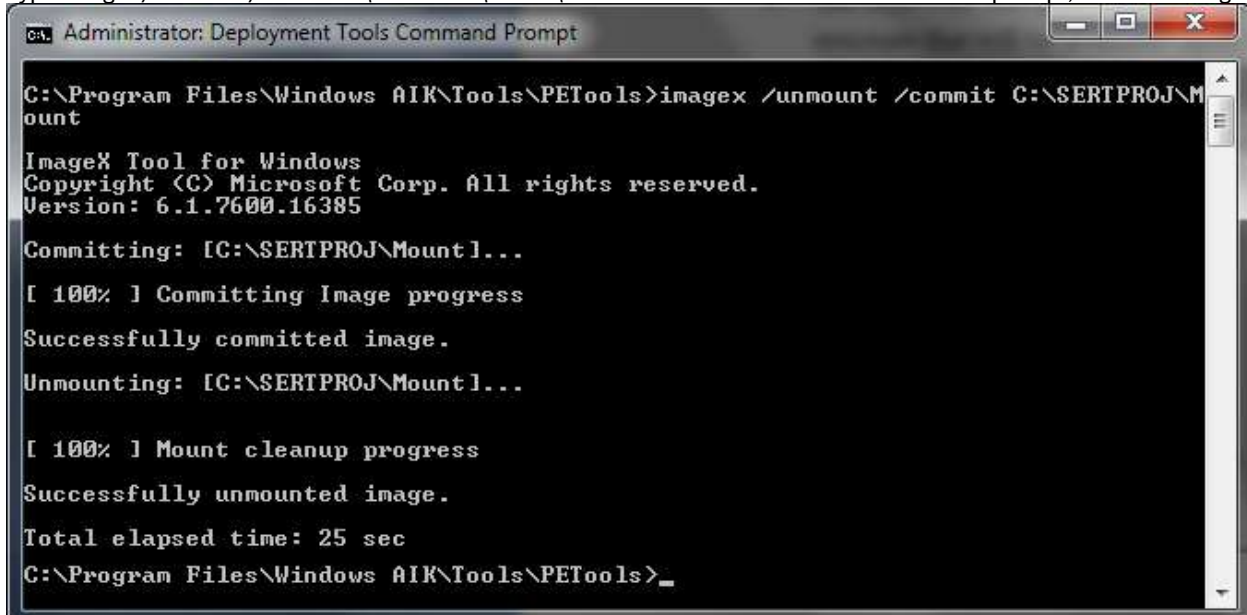
The boot.wim file is presented to the administrator under C:\SERTPROJ\Mount as the directory structure that will be available later during WINPE boot.



Copy the files you are interested in moving into the new WinPE image to C:\SERTPROJ\mount\Program Files\NameYourOwnDirectory

Step 4: Write new files to the Boot.wim file by specifying the /commit command upon unmount.

Type 'imagex /unmount /commit C:\SERTPROJ\Mount\' <ENTER> at the Windows AIK command prompt, minus the single quotes.



```
C:\Program Files\Windows AIK\Tools\PETools>imagex /unmount /commit C:\SERTPROJ\M
ount

ImageX Tool for Windows
Copyright (C) Microsoft Corp. All rights reserved.
Version: 6.1.7600.16385

Committing: [C:\SERTPROJ\Mount]...

[ 100% ] Committing Image progress
Successfully committed image.

Unmounting: [C:\SERTPROJ\Mount]...

[ 100% ] Mount cleanup progress
Successfully unmounted image.
Total elapsed time: 25 sec
C:\Program Files\Windows AIK\Tools\PETools>
```

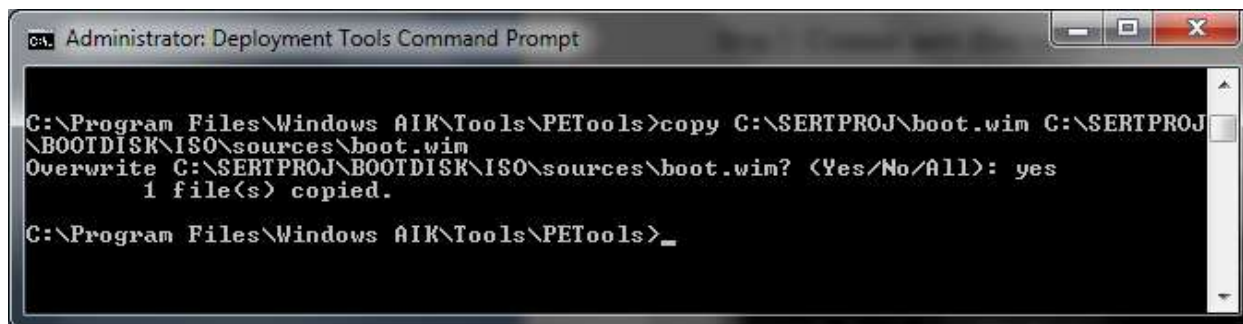
Step 5: Create a Bootdisk structure by using the Windows AIK copy command.

Type 'copytype x86 C:\sertproj\bootdisk' <ENTER> Please note, ensure C:\sertproj\bootdisk\ does not exist in C:\sertproj\ directory.

Step 6: Copy correct Boot.wim to WinPE Bootdisk.

Type 'del C:\SERTPROJ\bootdisk\winpe.wim' <ENTER>

Type 'copy C:\SERTPROJ\boot.wim C:\SERTPROJ\BOOTDISK\ISO\sources\boot.wim' <ENTER>



```
Administrator: Deployment Tools Command Prompt

C:\Program Files\Windows AIK\Tools\PETools>copy C:\SERTPROJ\boot.wim C:\SERTPROJ\
\BOOTDISK\ISO\sources\boot.wim
Overwrite C:\SERTPROJ\BOOTDISK\ISO\sources\boot.wim? (Yes/No/All): yes
1 file(s) copied.

C:\Program Files\Windows AIK\Tools\PETools>_
```

Step 7: Copy Network drivers and Symantec Software from

C:\SERTPROJ\Symantec_Endpoint_Recovery_Tool_2.0.24_AllWin_EN\SOURCES\DRIVERS\ directory.

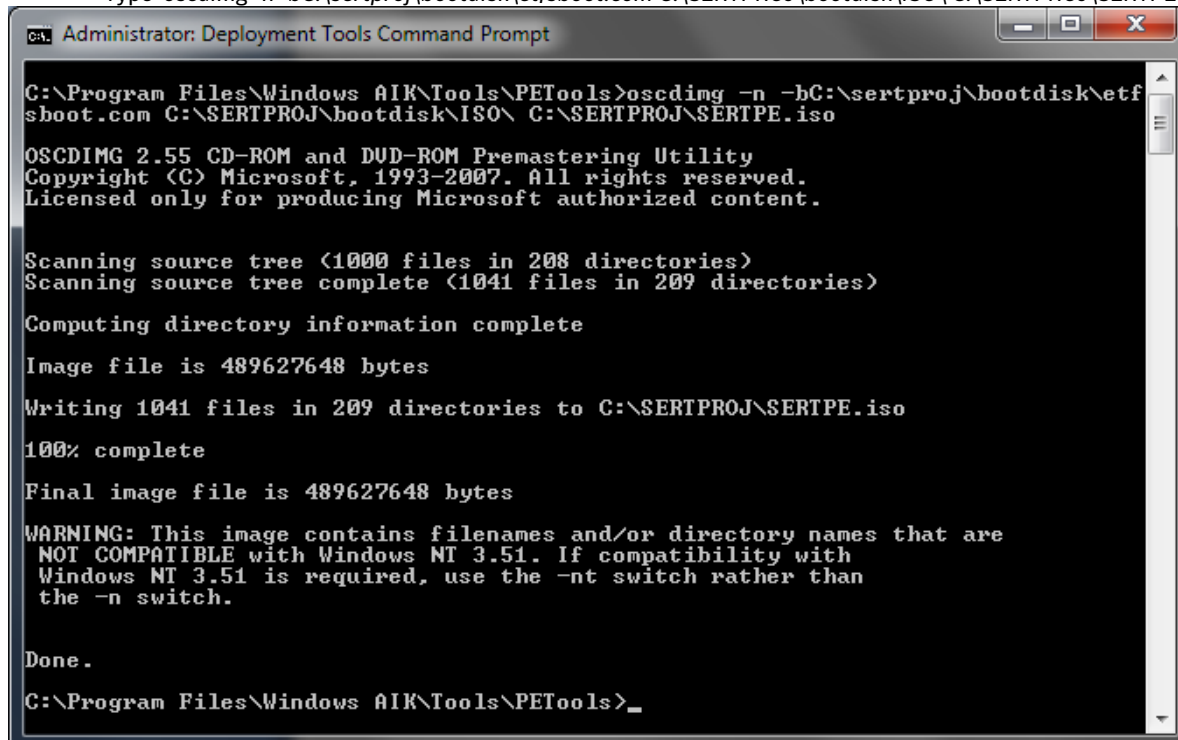
Type 'xcopy /E C:\SERTPROJ\Symantec_Endpoint_Recovery_Tool_2.0.24_AllWin_EN\SOURCES\DRIVERS
C:\SERTPROJ\bootdisk\ISO\sources\DRIVERS\' <ENTER>

Step 8: Copy the Symantec Software to the C:\SERTPROJ\bootdisk\ISO\sources\SYMANTEC_NBRT\

Type 'xcopy /E C:\SERTPROJ\Symantec_Endpoint_Recovery_Tool_2.0.24_AllWin_EN\SOURCES\SYMANTEC_NBRT
C:\SERTPROJ\bootdisk\ISO\sources\SYMANTEC_NBRT\' <ENTER>

Step 9: Create the bootable ISO Image with the included boot.wim changes.

Type 'oscdimg -n -bC:\sertproj\bootdisk\etfsboot.com C:\SERTPROJ\bootdisk\ISO\ C:\SERTPROJ\SERTPE.iso' <ENTER>



```
Administrator: Deployment Tools Command Prompt

C:\Program Files\Windows AIK\Tools\PETools>oscdimg -n -bC:\sertproj\bootdisk\etf
sboot.com C:\SERTPROJ\bootdisk\ISO\ C:\SERTPROJ\SERTPE.iso

OSCDIMG 2.55 CD-ROM and DUD-ROM Premastering Utility
Copyright (C) Microsoft, 1993-2007. All rights reserved.
Licensed only for producing Microsoft authorized content.

Scanning source tree (1000 files in 208 directories)
Scanning source tree complete (1041 files in 209 directories)

Computing directory information complete

Image file is 489627648 bytes

Writing 1041 files in 209 directories to C:\SERTPROJ\SERTPE.iso
100% complete

Final image file is 489627648 bytes

WARNING: This image contains filenames and/or directory names that are
NOT COMPATIBLE with Windows NT 3.51. If compatibility with
Windows NT 3.51 is required, use the -nt switch rather than
the -n switch.

Done.

C:\Program Files\Windows AIK\Tools\PETools>_
```

How to make a bootable USB Symantec Endpoint Recovery Tool

In this section instructions are provided to manually prepare a USB stick to become a bootable SERT disk. The process involves making the partition on the disk, formatting and making the primary USB partition “Active”.

Type 'diskpart' <ENTER>

Type 'list disk' <ENTER>

```
C:\Program Files\Windows AIK\Tools\PETools>diskpart

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

DISKPART> list disk

   Disk ###  Status              Size               Free              Dyn  Gpt
   -----  -
   Disk 0    Online             465 GB             3072 KB
   Disk 1    Online             1961 MB              0 B

DISKPART> _
```

Ensure you pick the correct drive. **WARNING!: Failure to select the correct drive will render your computer unusable.** In this example, the 1961MB drive is obviously the USB stick and it is designated Disk 1. Type 'select disk 1' <ENTER>

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

DISKPART> list disk

   Disk ###  Status              Size               Free              Dyn  Gpt
   -----  -
   Disk 0    Online             465 GB             3072 KB
   Disk 1    Online             1961 MB              0 B

DISKPART> select disk 1

Disk 1 is now the selected disk.

DISKPART>
```

Type 'clean' <ENTER>

```
C:\Windows\system32\diskpart.exe

DISKPART> clean

DiskPart succeeded in cleaning the disk.
```

Type 'create partition primary' <ENTER>

```
C:\Windows\system32\diskpart.exe

DISKPART> create partition primary

DiskPart succeeded in creating the specified partition.
```

Type 'select partition 1' <ENTER>

```
C:\Windows\system32\diskpart.exe

DISKPART> select partition 1
Partition 1 is now the selected partition.
```

Type 'active' <ENTER>

```
C:\Windows\system32\diskpart.exe

DISKPART> active
DiskPart marked the current partition as active.
```

Type 'format fs=fat32 quick' <ENTER>

```
C:\Windows\system32\diskpart.exe

DISKPART> format fs=fat32 quick
100 percent completed
DiskPart successfully formatted the volume.
DISKPART>
```

Type 'assign' <ENTER>

```
C:\Windows\system32\diskpart.exe

DISKPART> assign
DiskPart successfully assigned the drive letter or mount point.
DISKPART> _
```

Type 'exit' <ENTER>

```
C:\Windows\system32\diskpart.exe

DISKPART>
DISKPART>
DISKPART> exit
```

The next step is to copy the prepared files/directories to the target USB drive.

Type 'xcopy /E C:\SERTPROJ\bootdisk\ISO*. * F:\' <ENTER> where F:\ is the recently created USB drive.

Type '"xcopy /E C:\SERTPROJ\bootdisk\etfsboot.com F:\etfsboot.com' <ENTER> where F:\ is the recently created USB drive letter. Ensure F:\ is the recently created USB assigned drive letter.

How to update virus definitions on SERT disk

This section provides instructions on how to download the latest rapid release definitions for inclusion in the SERT Boot disk. The downloaded definitions have to be decompressed and 2 files modified in order to make the definitions easily discoverable during the SERT AntiVirus execution procedure. If time is limited to update definitions properly, simply copying all the extracted files to the SERT destination folder will work, but will require manual navigation during the commencement of AntiVirus scanning. There are numerous ways to obtain the latest virus definitions. In this section we will discuss two of those options.

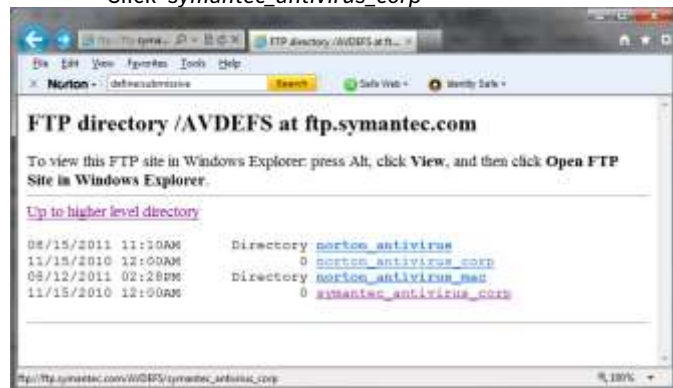
There are numerous ways to obtain the latest virus definitions. In this section we will discuss two of those options. Both options require that the JDB file be renamed to zip after download, in order to extract the contents. The first option requires manual download of the latest virus definitions from:

ftp://ftp.symantec.com/AVDEFS/symantec_antivirus_corp/rapidrelease/

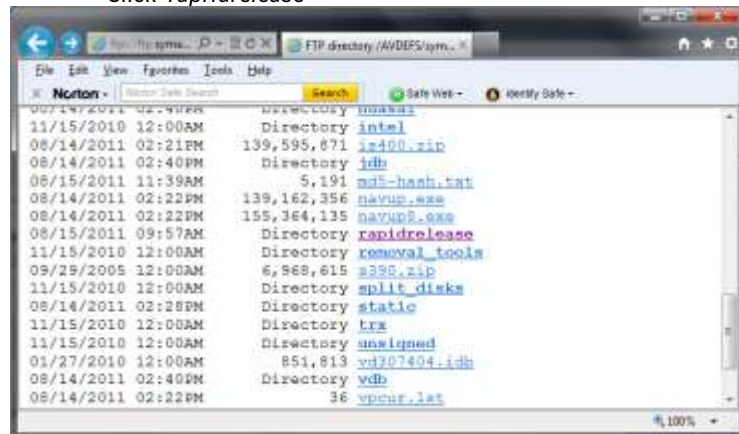
Click 'AVDEFS'



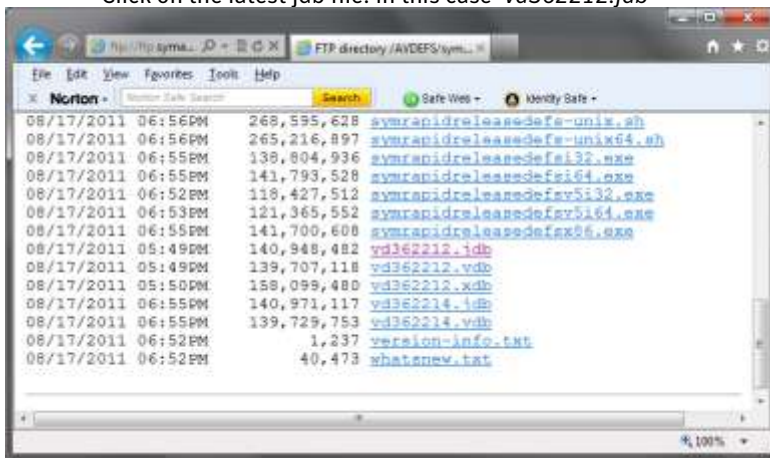
Click 'symantec_antivirus_corp'



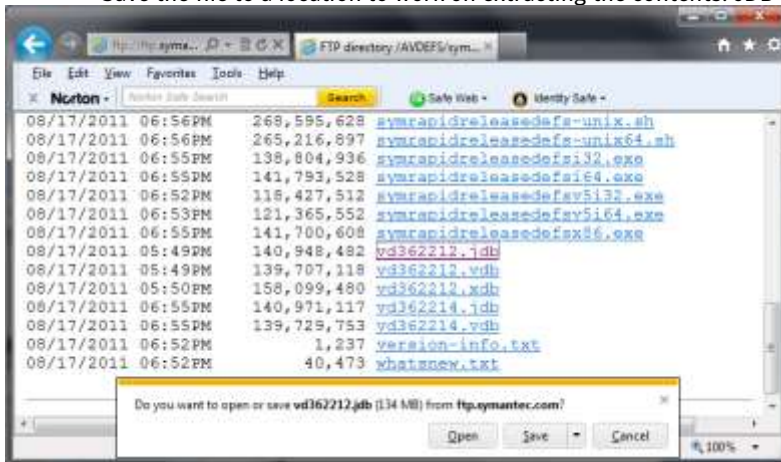
Click '*rapridrelease*'



Click on the latest jdb file. In this case 'vd362212.jdb'

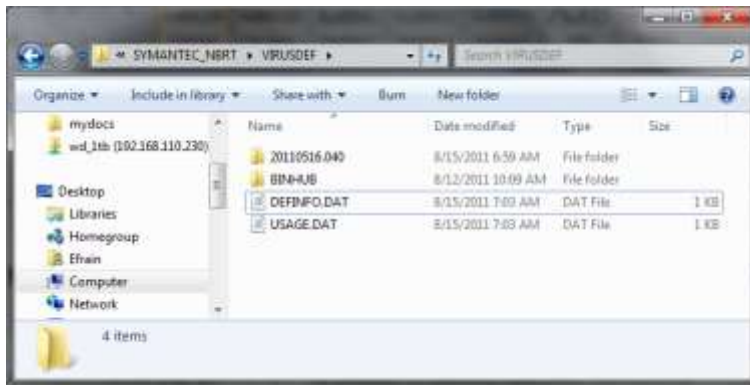


Save the file to a location to work on extracting the contents. JDB contents are in .zip format.

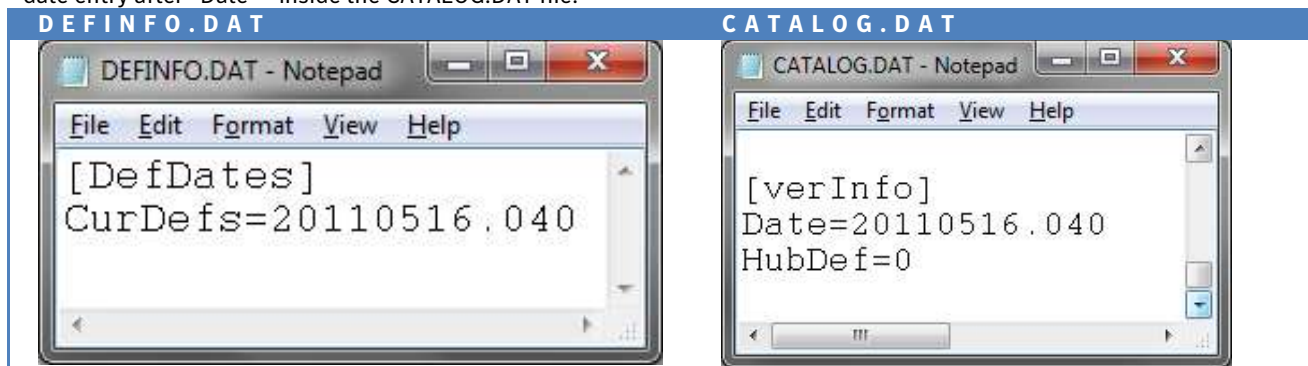


The second option requires the use of the cegetter.bat file included in Appendix A. The cegetter.bat file is required to be launched by a Task Scheduler for automatic downloads, command line execution or by double-clicking. The cegetter.bat file automatically downloads the latest rapid release definition file in the form of a #####.jdb file. Regardless of the method used to download the JDB file, the next step is to unzip the .JDB file. The uncompressed content is the content that needs to be copied to the WinPEImage \ISO\sources\SYMANTEC_NBRT\VIRUSDEF\VIRUSDEFS\20110516.040, where 20110516.040 is the virus definition revision number indicated inside the CATALOG.DAT file located inside \ISO\sources\SYMANTEC_NBRT\VIRUSDEF\VIRUSDEFS\20110516.040\catalog.dat.

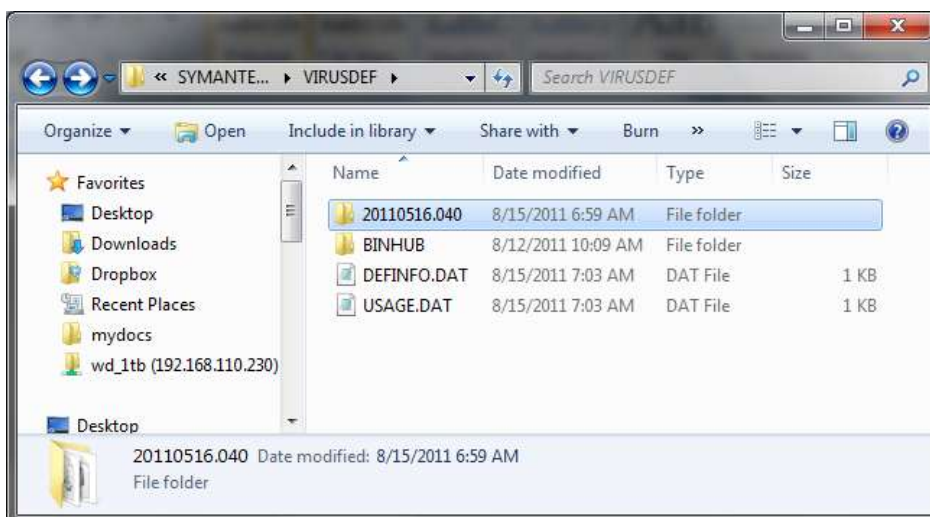
The following section is optional. If the CURDEFS variable is not set, later upon bootup of the winpe image, a manual action to point to the virus definitions will need to be performed.



After the files have been downloaded, open the DEFINFO.DAT and replace the “CurDefs=DATE” text to match the virus definition date entry after “Date=” inside the CATALOG.DAT file.



The date after CurDefs= should match the date after Date=.



Ensure the directory name is equal to the same date string in CATALOG.DAT file: i.e 20110516.040.
Burn your CD or make your USB drive and you should be ready to boot from removable media and scan for malware.

Appendix A: Rapid Release Automatic Download Script

```
@Set COPY_jdb_TO="C:\temp\"
@set RAPIDRELEASE=1
@set jdbTEMP=%temp%

@rem
=====
==
@rem Set RAPIDRELEASE=1 to download rapidrelease definitions, RAPIDRELEASE=0 for fully QA'd definitions (standard).
@rem Change COPY_jdb_TO= to point to the SEP server directory (or where you want the jdb file copied)
@rem you can also run the script directly from the SEP incoming folder and it will copy the definitions there.
@rem jdbTEMP is the temp folder the script will use while downloading definitions, set to %temp% to use system default
@rem
=====
==
@rem Script for downloading virus and spyware definition updates for
@rem Symantec Endpoint Protection version 11.xx
@rem
=====
==
@echo off
rem ===== check that OS is win2k or better =====
if not "%OS%" == "Windows_NT" goto BADOS
if "%APPDATA%" == "" goto BADOS

rem ===== make sure to be in script directory =====
if exist rtvscan.exe set COPY_jdb_TO=%CD%
for %%i in (%0) do @%%~di
for %%i in (%0) do @cd %%~pi
if exist rtvscan.exe set COPY_jdb_TO=%CD%

rem ===== get name/size of last file from "jdbdown.lastfile" =====
if not exist jdbdown.lastfile goto NOLAST
for /f "tokens=1" %%f in (jdbdown.lastfile) do set lastfile=%%f
for /f "tokens=2" %%f in (jdbdown.lastfile) do set lastsize=%%f

:NOLAST
rem ===== jump to temp dir =====
if not exist "%jdbTEMP%\jdbtmp" md "%jdbTEMP%\jdbtmp"
if exist "%jdbTEMP%\jdbtmp\*.jdb" del "%jdbTEMP%\jdbtmp\*.jdb"
pushd "%jdbTEMP%\jdbtmp"

rem ===== make ftp script for checking jdb directory on ftp =====
echo open ftp.symantec.com> check.txt
echo anonymous>> check.txt
echo email@address.com>> check.txt
set jdbfolder=jdb

if "%RAPIDRELEASE%" == "1" set jdbfolder=rapidrelease

echo cd /public/english_us_canada/antivirus_definitions/symantec_antivirus_corp/%jdbfolder%>> check.txt
echo dir *.jdb chk.lst>> check.txt
echo bye>> check.txt

rem ===== get filename and size from ftp =====

if exist chk.lst del chk.lst
ftp -s:check.txt
if not exist chk.lst goto ERROR
for /f "tokens=9" %%f in (chk.lst) do set jdbfile=%%f
for /f "tokens=5" %%f in (chk.lst) do set jdbsize=%%f
if "%jdbfile%" == "" goto ERROR
if "%jdbsize%" == "" goto ERROR

rem ===== compare ftp name/size to local =====

if not "%jdbfile%" == "%lastfile%" goto DOWNLOAD
if not "%jdbsize%" == "%lastsize%" goto DOWNLOAD
```

```

popd
echo.
echo Already downloaded latest %jdbfolder% file: %jdbfile% - size %jdbsize%
echo %date% %time% Already downloaded latest %jdbfolder% file: %jdbfile% - size %jdbsize% >> jdbdown.log
goto END

:DOWNLOAD
rem ===== make ftp script for downloading new jdb file =====
echo open ftp.symantec.com> down.txt
echo anonymous>> down.txt
echo email@address.com>> down.txt
echo cd public/english_us_canada/antivirus_definitions/norton_antivirus/%jdbfolder%>> down.txt
echo bin>> down.txt
echo hash>> down.txt
echo get %jdbfile%>> down.txt
echo bye>> down.txt

rem ===== download new file =====

ftp -s:down.txt
for %%i in (%jdbfile%) do @set newsiz=%%~zi
if not "%newsiz%" == "%jdbsize%" goto ERROR
move %jdbfile% %COPY_jdb_TO%
if exist %jdbfile% goto ERRORMOVE
popd

echo.
echo %jdbfile% %jdbsize% > jdbdown.lastfile
echo Downloaded new %jdbfolder% file: %jdbfile% - size %jdbsize%
echo %date% %time% Downloaded new %jdbfolder% file: %jdbfile% - size %jdbsize% >> jdbdown.log
goto END

:ERROR
popd
echo.
echo ERROR: problem downloading %jdbfolder% definition file. jdbfile=%jdbfile% jdbsize=%jdbsize% newsiz=%newsiz%
(lastfile=%lastfile% lastsize=%lastsize%).
echo %date% %time% ERROR: problem downloading %jdbfolder% definition file. jdbfile=%jdbfile% jdbsize=%jdbsize%
newsiz=%newsiz% (lastfile=%lastfile% lastsize=%lastsize%). >> jdbdown.log
type "%jdbTEMP%\jdbtmp\chk.lst" >> jdbdown.log
echo. >> jdbdown.log
goto END

:ERRORMOVE
popd
echo.
echo ERROR: problem moving definition file to SAV folder. COPY_jdb_TO=%COPY_jdb_TO% newsiz=%newsiz%
(lastfile=%lastfile% lastsize=%lastsize%).
echo %date% %time% ERROR: problem moving definition file to SAV folder. COPY_jdb_TO=%COPY_jdb_TO%
newsiz=%newsiz% (lastfile=%lastfile% lastsize=%lastsize%). >> jdbdown.log
goto END

:BADOS
echo.
echo ERROR: this script needs Windows 2000 or better.
echo %date% %time% ERROR: this script needs Windows 2000 or better. >> jdbdown.log
goto END

:END
if exist "%jdbTEMP%\jdbtmp\check.txt" del "%jdbTEMP%\jdbtmp\check.txt"
if exist "%jdbTEMP%\jdbtmp\down.txt" del "%jdbTEMP%\jdbtmp\down.txt"
if exist "%jdbTEMP%\jdbtmp\chk.lst" del "%jdbTEMP%\jdbtmp\chk.lst"
rd "%jdbTEMP%\jdbtmp"

set COPY_jdb_TO=
set RAPIDRELEASE=
set lastsize=
set lastfile=
set newsiz=
set jdbsize=
set jdbfile=
set jdbfolder=
set jdbtemp=

```

About Symantec Symantec is a global leader in providing security, storage and systems management solutions to help businesses and consumers secure and manage their information. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com

Copyright © 2011 Symantec Corporation. All rights reserved. Symantec and the Symantec logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.
08/11