A Baseline for XP Boot Changes

AAFS - 26 February 2010

Ben Livelsberger
NIST
Information Technology Laboratory
CFTT Project

Disclaimer

Certain trade names and company products are mentioned in the text or identified. In no case does such identification imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the products are necessarily the best available for the purpose.

Outline

- Introduction
- Methodology/Approach
- Expected Results
- Analysis/Findings
- Conclusion

Introduction

- Question: What changes on a hard drive when you boot a system?
- Answer:
  - Sector content of installed devices containing volumes
    - Accessed, write, created date and time metadata
    - Files created
    - Files deleted

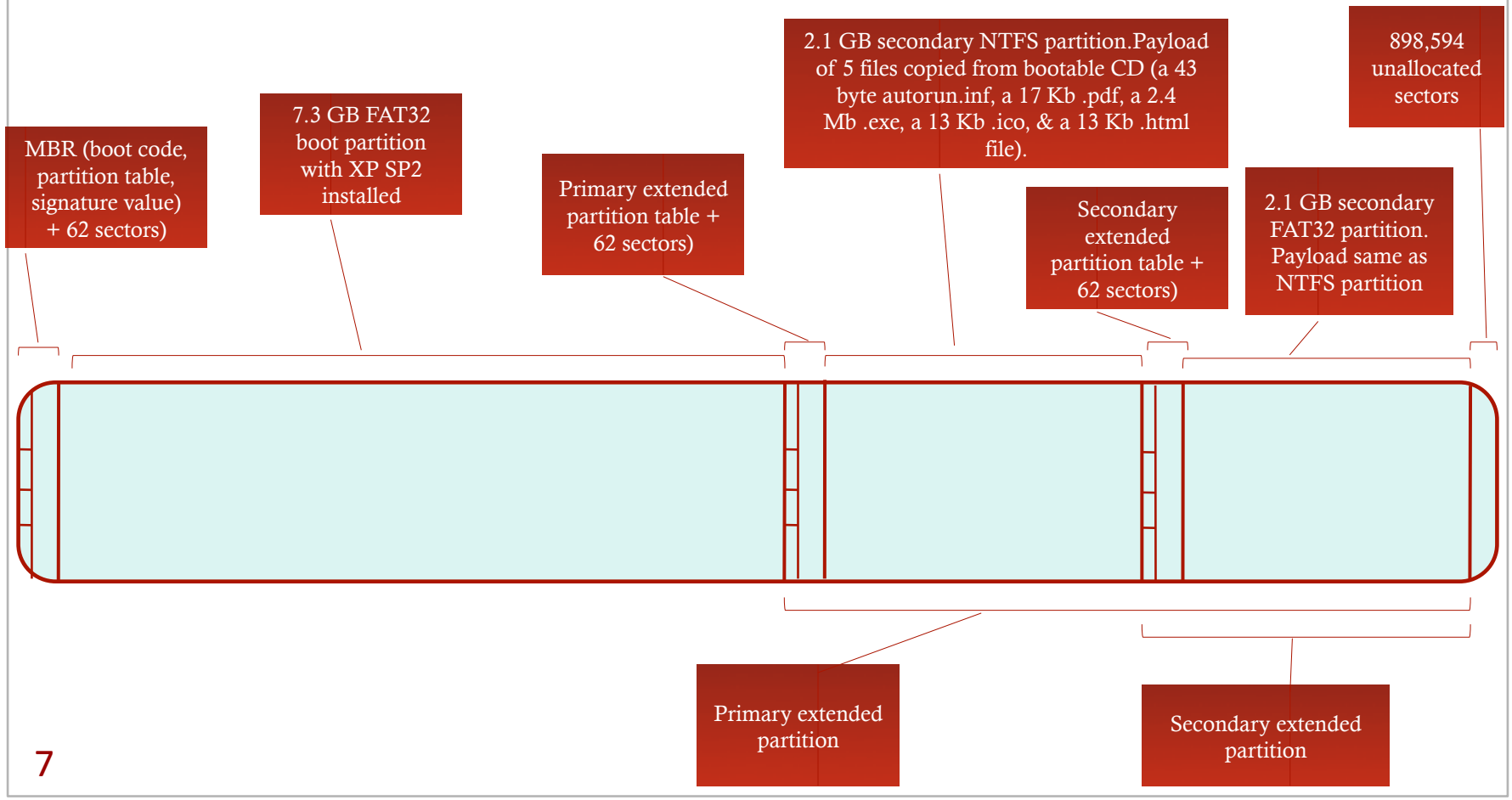
Methodology and Approach

- Build Vanilla XP system not networked
- Cycle through several boots and shutdowns
- Image with dd
- Boot, 2 minutes idle, shutdown, and reimage (5x)
- Compare images- Linux & perl
- Analyze differences- perl scripts and SleuthKit Tools

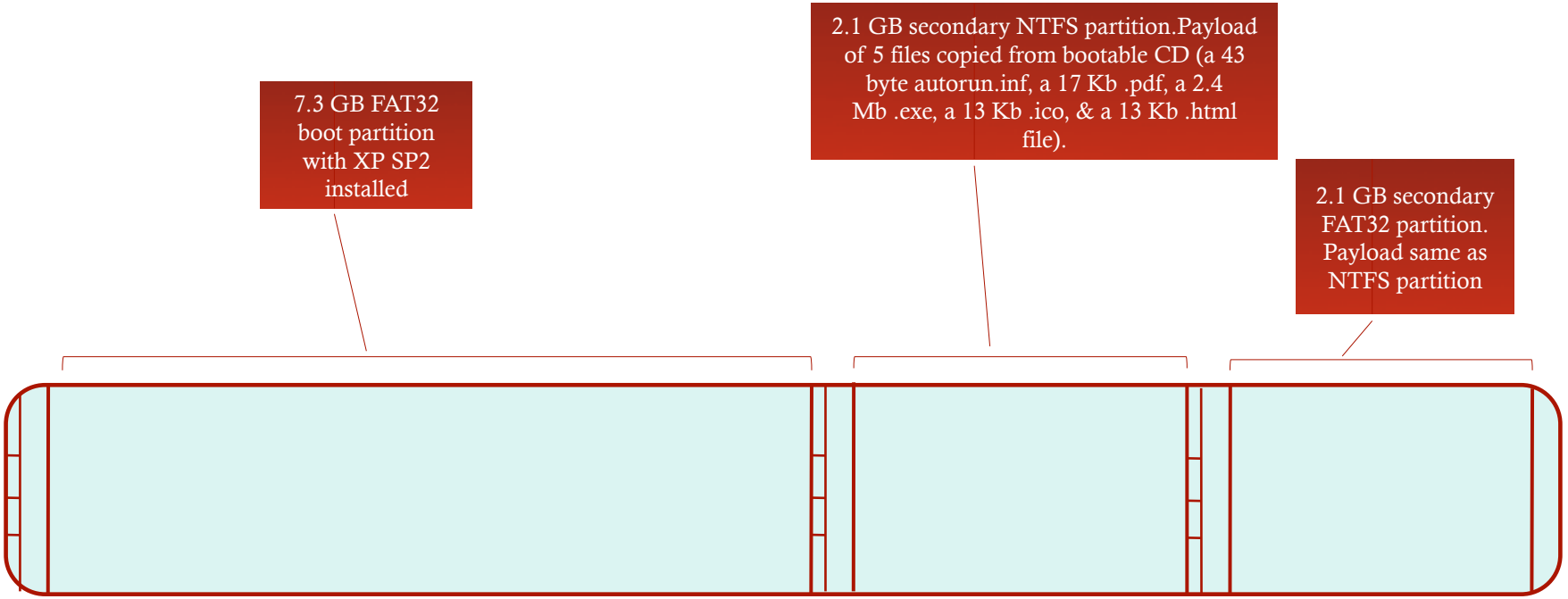
Methodology and Approach

- Build (vanilla) XP system
  - DCO drive to 12 GB
  - Partitioned
    - 7 GB primary FAT32
    - 2 GB secondary NTFS & 2 GB secondary FAT32
  - Windows XP Professional SP2
  - Add user files to secondary partitions
    - 5 files - 2.4 Mb
    - Types: .inf, .pdf, .exe, .ico, & .html

Expected Results



Analysis/Findings



- Changes confined to file system partitions
- Few changes to the secondary file system partitions

Analysis/Findings: Boot Volume

analyze_partitions.pl p0 Output (from run 1)

- Reserved Area: 1 (FS Info Sector)
- FAT Area:
  - FAT 0: 1105 1122 6170 10821 10823 10829
  - FAT 1: 15417 15434 20482 25133 25135 25141

Analysis/Findings: Boot Volume Data Area

- Total data area sectors changed:
  - 12,501-14,827 sectors, 6.2-7.4 MB
  - Average: 13,865 sectors (6.9 MB)
- Changes to content of:
  - 9,436 -11,931 (10,883 ave or 78%) allocated sectors, file content
  - 2,740-3,359 (2,923 ave or 21%) unallocated sectors
  - 34-149 sectors (1%) containing directory entries

Unallocated Space: File Growth

- File Growth:
  - Log Files & Prefetch Files
  - Collective growth: 10-609 sectors
  - 100-500+ sectors to prefetch boot trace file

# cycles file grew	Files that Grew
5	WINDOWS/Debug/UserMode/userenv.log
5	WINDOWS/system32/wbem/Logs/wbemess.log
5	WINDOWS/WindowsUpdate.log
2	WINDOWS/SchedLgU.Txt
3	WINDOWS/Prefetch/NTOSBOOT-B00DFAAD.pf
2	WINDOWS/Prefetch/WSCNTFY.EXE-1B24F5EB.pf

Unallocated Space: New & Temporary Files

- New Files
  - 5 restore point files
  - change.log cycled
- Temporary Files
  - WINDOWS/Temp/_sg034g7.TMP (616 KB) &
  - WINDOWS/SoftwareDistribution/DataStore/Logs/_mp.edb (65 KB)
- No Persistent Files Deleted
- Some changes to unallocated space not accounted for

New Files (paths abbreviated)
System Volume Information/_restore{ … }/RP1/change.log
System Volume Information/_restore{ … }/RP1/A0000052.INI
System Volume Information/_restore{ … }/RP1/A0000053.INI
System Volume Information/_restore{ … }/RP1/A0000054.INI
System Volume Information/_restore{ … }/RP1/A0000055.ini

Changes to File Content

- Changes to File Content
  - 39 common files every cycle
  - 40-45 Files
- Amount Changed
  - Average: 11,049 sectors
  - 95% were to PAGEFILE.SYS & SYSTEM files

Changes to File Content (by Directory)

- Documents and Settings & WINDOWS/system32/config
  - 22 registry files (Usrclass.dat, Ntuser.dat, DEFAULT, SAM, SECURITY, SOFTWARE, SYSTEM, .log files)
  - Average Total: 1322 sectors
- WINDOWS/system32/wbem
  - 7 WMI Files
  - Average Total: 30 sectors
- WINDOWS/Prefetch
  - 3 .pf Prefetch Files (NTOSBOOT-B00DFAAD.pf, WSCNTFY.EXE-1B24F5EB.pf, & WUAUCLT.EXE-399A8E72.pf)
  - Average Total: 651 sectors

Changes to File Content (Misc)

- Miscellaneous Other Files

# of cycles file chgd	ave # sectors chgd	Misc. Files that Changed
5	9284.4	PAGEFILE.SYS
5	1	System Volume Information/_restore {1E17E5A1-FE9A-4F64-AA4B-1C4617CFC305}/_driver.cfg
5	3	WINDOWS/system32/config/ AppEvent.Evt
5	7.8	WINDOWS/system32/config/ SysEvent.Evt
4	1	WINDOWS/system32/wpa.dbl
2	2	System Volume Information/_restore {1E17E5A1-FE9A-4F64-AA4B-1C4617CFC305}/drivetable.txt
1	2	WINDOWS/Tasks/SA.DAT
5	3	WINDOWS/Debug/UserMode/ userenv.log
5	1.6	WINDOWS/SchedLgU.Txt
5	6	WINDOWS/WindowsUpdate.log

Changes to File Content (Summary)

# of cydes file chgd	ave # sectors chgd	file
5	2	Documents and Settings/lab/Local Settings/Application Data/Microsoft/Windows/UsrClass.dat
5	1.6	Documents and Settings/lab/Local Settings/Application Data/Microsoft/Windows/UsrClass.dat.LOG
5	24	Documents and Settings/lab/NTUSER.DAT
5	1.6	Documents and Settings/lab/ntuser.dat.LOG
5	2	Documents and Settings/LocalService/Local Settings/Application Data/Microsoft/Windows/UsrClass.dat
5	1.8	Documents and Settings/LocalService/Local Settings/Application Data/Microsoft/Windows/UsrClass.dat.LOG
5	7	Documents and Settings/LocalService/NTUSER.DAT
5	1.8	Documents and Settings/LocalService/ntuser.dat.LOG
5	2	Documents and Settings/NetworkService/Local Settings/Application Data/Microsoft/Windows/UsrClass.dat
5	1.8	Documents and Settings/NetworkService/Local Settings/Application Data/Microsoft/Windows/UsrClass.dat.LOG
5	7	Documents and Settings/NetworkService/NTUSER.DAT
5	1.8	Documents and Settings/NetworkService/ntuser.dat.LOG
5	9284.4	PAGEFILE.SYS
5	1	System Volume Information/_restore{1E17E5A1-FE9A-4F64-AA4B-1C4617CFC305}/_driver.cfg
5	3	WINDOWS/Debug/UserMode/userenv.log
5	1.6	WINDOWS/SchedLgU.Txt
5	2	WINDOWS/SoftwareDistribution/DataStore/DataStore.edb
5	2	WINDOWS/SoftwareDistribution/DataStore/Logs/edb.chk
5	3.6	WINDOWS/SoftwareDistribution/DataStore/Logs/edb.log
5	3	WINDOWS/system32/config/AppEvent.Evt
5	4	WINDOWS/system32/config/DEFAULT
5	1.8	WINDOWS/system32/config/default.LOG
5	4	WINDOWS/system32/config/SAM
5	1.6	WINDOWS/system32/config/SAM.LOG
5	3.4	WINDOWS/system32/config/SECURITY
5	1.4	WINDOWS/system32/config/SECURITY.LOG
5	31.6	WINDOWS/system32/config/SOFTWARE
5	1	WINDOWS/system32/config/software.LOG
5	7.8	WINDOWS/system32/config/SysEvent.Evt
5	1207.2	WINDOWS/system32/config/SYSTEM
5	1	WINDOWS/system32/config/system.LOG
5	9.2	WINDOWS/system32/wbem/Logs/wbemess.log
5	6	WINDOWS/system32/wbem/Repository/FS/INDEX.BTR
5	1	WINDOWS/system32/wbem/Repository/FS/INDEX.MAP
5	2	WINDOWS/system32/wbem/Repository/FS/MAPPING1.MAP
5	2	WINDOWS/system32/wbem/Repository/FS/MAPPING2.MAP
5	9	WINDOWS/system32/wbem/Repository/FS/OBJECTS.DATA
5	1	WINDOWS/system32/wbem/Repository/FS/OBJECTS.MAP
5	6	WINDOWS/WindowsUpdate.log
4	1	WINDOWS/system32/wpa.dbl
3	608.7	WINDOWS/Prefetch/NTOSBOOT-B00DFAAD.pf
3	12.3	WINDOWS/Prefetch/WSCNTFY.EXE-1B24F5EB.pf
3	30.7	WINDOWS/Prefetch/WUAUCLT.EXE-399A8E72.pf
2	2	System Volume Information/_restore{1E17E5A1-FE9A-4F64-AA4B-1C4617CFC305}/drivetable.txt
1	2	WINDOWS/Tasks/SA.DAT

Conclusion

- The boot process creates new files.
- Some files grew, notably log files.
- Some temporary files were created and then deleted.
- No system files were deleted.
- If an XP SP2 PC is booted an average of 13,873 sectors will change in 40-45 files, metadata, and unallocated space.

Future Research

- Use of an NTFS boot partition
- Investigate changes in secondary partitions
- Use of other OSes- Vista, Windows 7
- Pulling plug vs. proper shut down
- Directory entry/meta data analysis
- Investigate prefetch file change variance

Project Sponsors (aka Steering Committee)

- National Institute of Justice (Major funding)
- FBI (Additional funding)
- Department of Defense, DCCI (Equipment and support)
- Homeland Security (Major funding)
- State & Local agencies (Technical input)
- Internal Revenue, IRS (Technical input)
- NIST/OLES (Program management)

Contacts

Ben Livelsberger

livebe01@nist.gov

Jim Lyle

www.cftt.nist.gov

cftt@nist.gov

Sue Ballou, Office of Law Enforcement Standards

susan.ballou@nist.gov