17810
Systems Programmer, Heal Thy PC: Tuneup Time

Victor Freyer, Principal Solutions Architect

Lemon Bay Computer Service LLC

Previously with Southwestern Bell, Cisco Systems, Bank of America, Bank One and JP Morgan Chase

victor@LemonBayComputerService.com

Do-It-Yourself PC Tune-Up

- Why do it yourself?
  - Personal privacy
  - Can't live without your computer
  - Sense of accomplishment
  - Second career?
  - The Geek Squad™ wants to charge what!?

- What do you need?
  - A plan
  - A toolkit full of free tools

Simple 15-Step Process

- Boot to Windows
- Shutdown Windows
- Evaluate hard drive health
- Backup Windows partition
- Malware removal and cleanup
- Correct file system errors
- Windows System File Checker
- Uninstall unnecessary programs
- Remove unneeded programs from startup
- Remove Internet Explorer toolbars
- Remove temporary files
- Defragment Windows partition
- Update system BIOS
- Update programs
- Install anti-virus software

Boot and Shutdown

- Computer must not be Suspended or Hibernating
  - Likelihood of corrupting your file system
- Benchmark startup time
  - So you can compare when you're done
- Shutdown to insure a clean file system close
  - Save yourself from problems later

Evaluate Hard Drive Health

- Boot SystemRescueCD
  - Download the live Linux CD – www.sysresccd.org
  - Right-click the ISO file to burn to CD
- Review hard drive SMART statistics
  - smartctl -a /dev/sda
- Run SMART self test
  - smartctl -t short /dev/sda
  - smartctl -l selftest /dev/sda

SMART Statistics

- smartctl -a /dev/sda

```
Model Family:     Western Digital Scorpio family
Device Model:     WDC WD800BEVE-00UYT0
Serial Number:    WD-WXE408L96343
Firmware Version: 01.04A01
User Capacity:    80,026,361,856 bytes
...

SMART Attributes Data Structure revision number: 16
Vendor Specific SMART Attributes with Thresholds:
ID# ATTRIBUTE_NAME          FLAG     VALUE WORST THRESH TYPE      UPDATED  WHEN_FAILED RAW_VALUE
...
  5 Reallocated_Sector_Ct   0x0033   200   200   140    Pre-fail  Always       -       0
...
  9 Power_On_Hours          0x0032   095   095   000    Old_age   Always       -       3670
...
194 Temperature_Celsius     0x0022   111   100   000    Old_age   Always       -       32
196 Reallocated_Event_Count 0x0032   200   200   000    Old_age   Always       -       0
197 Current_Pending_Sector  0x0012   200   200   000    Old_age   Always       -       0
...

SMART Error Log Version: 1
No Errors Logged
```

SMART Self Test Results

- smartctl -t short /dev/sda – run the test
- smartctl -l selftest /dev/sda – view the results

```
smartctl version 5.38 [i486-pc-linux-gnu] Copyright (C) 2002-8 Bruce Allen
Home page is http://smartmontools.sourceforge.net/

=== START OF READ SMART DATA SECTION ===
SMART Self-test log structure revision number 1
Num  Test_Description    Status                  Remaining  LifeTime(hours)  LBA_of_first_error
# 1  Short offline       Completed without error       00%      3671         -
# 2  Short offline       Completed without error       00%      1783         -
```

Backup Windows Partition

- Still in Linux
  - Back up the MBR
    - dd if=/dev/sda of=mbr.bin bs=512 count=1
  - Back up the contents of the boot partition
    - partimage (NTFS and FAT)
    - ntfsclone (NTFS only)
      ntfsclone --save-image -o backup.image /dev/sda1
- Other backup software
  - DriveImage XML
  - Comodo Backup
  - Acronis True Image ($$)

Malware Removal Part 1

Offline Scanning Tools

- AVG Rescue CD
  http://www.avg.com/ww-en/download.prd-arl
- Kaspersky Rescue Disk
  http://support.kaspersky.com/4162
- Microsoft Safety Scanner
  http://www.microsoft.com/security/scanner/
- F-Secure Rescue CD
  https://www.f-secure.com/en/web/labs_global/rescue-cd

Malware Removal Part 2

Post-Removal Cleanup within Windows

- AdwCleaner by Xplode (thru Win 8.1)
  https://toolslib.net/downloads/viewdownload/1-adwcleaner/
- Malwarebytes Anti-Rootkit BETA
  https://www.malwarebytes.org/antirootkit/
- Malwarebytes Anti-Malware
  https://www.malwarebytes.org/mwb-download/
- Spybot Search and Destroy
  https://www.safer-networking.org/dl/
- HitmanPro 3
  http://www.surfright.nl/en/products/
- Windows Repair
  http://www.tweaking.com

Check NTFS and Windows Files

- Run “cmd.exe” as administrator to execute these commands

- Correct NTFS errors
  - CHKDSK C: /F
  - Repeat until a run has no errors

- Refresh Windows system files
  - SFC /SCANNOW

Clean Up Programs and Files

- Uninstall unnecessary programs
  - Run appwiz.cpl
- Clean up startup programs and browser toolbars
  - Windows Sysinternals: autoruns http://technet.microsoft.com/sysinternals
  - Microsoft: msconfig.exe
- Clean up files
  - Windows file cleanup: cleanmgr.exe
  - Piriform CCleaner http://www.piriform.com/ccleaner

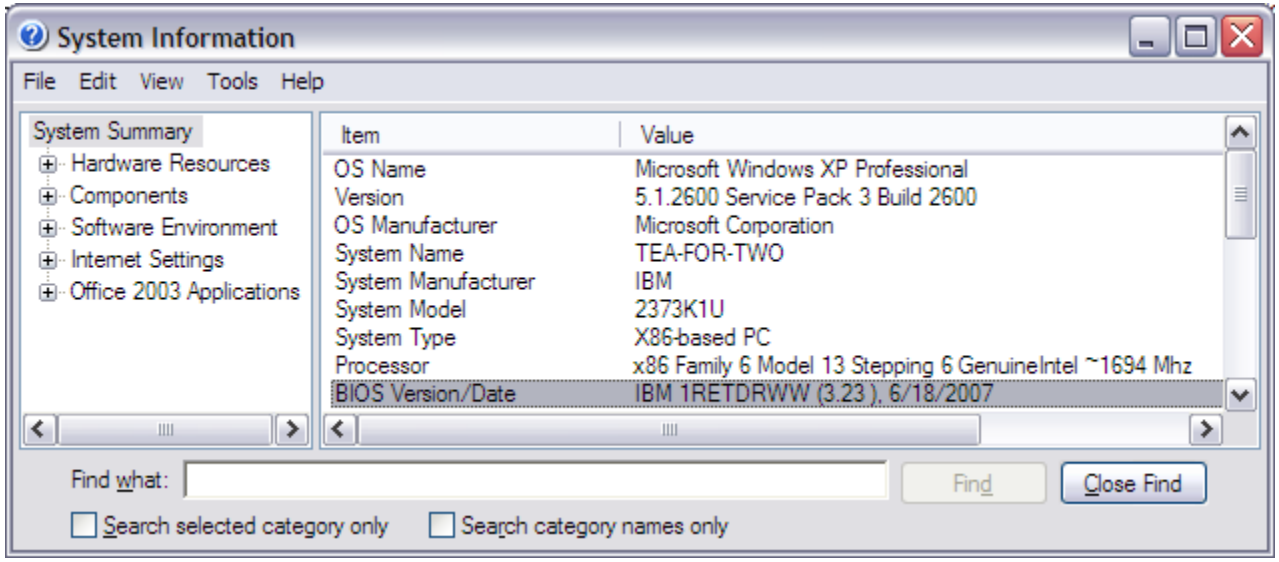
Defragment Windows Partition

- Windows Vista and later defragment automatically in the middle of the night – providing your computer is on!

- Minimize computer activity
  - Start -> Run-> msconfig.exe
    - Deselect all Startup items and all non-Microsoft services
  - Reboot
  - Start -> Run -> dfrgui.exe
  - Rerun msconfig
    - Re-enable all Startup and services
  - Reboot

Update System BIOS

- Check current BIOS – msinfo32.exe



- Get new BIOS from system/motherboard manufacturer

Update Programs

- Apply Service Packs (Windows and Office)
- Enable and apply Microsoft updates
- Update Internet Explorer to 11

- Update common programs
  - Acrobat Reader
  - Adobe Flash Player
  - Java runtime environment
  - Alternate browsers (Firefox, Chrome, Opera…)

Install a Lighter-Weight Antivirus

- If you're paying for an antivirus program, discontinue it
- Recommendations – free for individual use
  - AVG AntiVirus Free Edition – free.avg.com
  - Microsoft Security Essentials – windows.microsoft.com/mse
    - Included in Windows 8 and later
  - Avast Essential – www.avast.com

- It's good to have a second opinion
  - Malwarebytes Anti-Malware

- Uninstall your old antivirus program first!
  - Windows uninstall
  - Vendor-provided removal tool

Thank You!

- Session 17810 - Please evaluate this session!

- The best virus prevention
  - *Healthy paranoia*

victor@LemonBayComputerService.com