Removing Viruses and Other Unwanted Files from a PC

NOTE: If it has been determined that there are definitely viruses on the workstation, the first course of action should always be to pull the hard drive from the system, attach it as a slave drive on another computer (such as the DV test computer), and then run a full system scan on the system (using NOD32 virus scanning software). The following steps are to be performed, in addition to the system scan, if the scan did not completely remove all viruses affecting the computer.

1) Login in to the workstation using one of the Windows (2000 or XP) profiles. NOTE: If there is more than one profile, each must be cleaned up separately. Therefore it is best to clean one profile completely, then begin the next, and so on.
2) Once it's been determined there are viruses on the workstation, ***for EACH USER PROFILE, complete SOME or ALL of the following*** *(depending upon what is necessary to get the system back in working order)* **…**

1. Preliminary Steps to Remove Viruses from a Workstation

1) Turn on the workstation.
   NOTE: If you CANNOT get the workstation to boot up, unplug/remove all non-essential cards -
   Such as the sound card, scanner and/or printer SCSI cards, etc.
2) Press the [F8] key to access the boot menu. Arrow down to "SAFE MODE – COMMAND PROMPT" and [ENTER].
3) Once the system has booted into safe mode, press [CTRL] + [ALT] + [DELETE]. From the upper menu of the pop-up *Windows Task Manager* window, click "File" and then select "New Task (Run …)."
4) From the *Create New Task* window, type **Explorer** in the empty field and click "OK." Answer "Yes" to any pop-ups.
5) From Windows Explorer, browse to C:\Windows and then double-click to open "regedit."
6) From the *Registry Editor*, browse to HKEY_LOCAL_MACHINE\system\CurrentControlSet\Services.
7) Browse down to the service named "Winsock." Right-click on it and select "Export." From the pop-up *Export Registry File* window, browse to C:\Backup\Registry (the Backup, Registry directories will need created first) and then click "Save" to back up the file. Repeat this step, this time selecting the "Winsock2" folder.
8) Next, select and then delete both the Winsock and Winsock2 folders in order to disable the system's TCP/IP.
9) Click the upper right-hand [X] to close the *Registry Editor*.
10) Next, from Windows Explorer, blow away ALL files in ALL Temp directories (C:\Windows\Temp and C:\Documents and Settings\EACH USER'S Temp directories) prior to running any scans. Close Windows Explorer.
11) Again, From the upper menu of the *Task Manager* window, click "File" and then select "New Task (Run …)."
12) From the *Create New Task* window, type **MSConfig** in the empty field and click "OK."
13) From MSConfig, disable EVERYTHING in the Startup & ALL non-Microsoft Services. (This is done to help determine which service(s) are bogging down the system.) Click "Apply" and "Close." From the pop-up window, click "Restart."
14) Once the system has been restarted and logged in to the appropriate user, from the pop-up window, check the "Don't show this window upon startup …" checkbox and click "OK."
15) From Internet Explorer, delete Temporary Internet Files, History, Cookies.
16) From the Programs tab of the *Internet Properties*, click "Manage Add ons." Scroll through the list of Add ons. Click to select and then click "Disable" to disable any unfamiliar or unwanted ones.
    NOTE: Some Add ons may automatically re-enable. This is a good indication that these particular Add ons are viruses. In such cases, write down the Add ons' names, determine where they are stored on the hard drive, and [SHIFT] + [DELETE] them. You might need to access the workstation using ERD Commander to be able to delete them.

2. Checking for Malicious Program Installations via the Control Panel and Startup Folder

1) From the Start menu of the workstation, select Settings -> "Control Panel."
2) From the *Control Panel*, double-click to open "Add/Remove Programs."
3) From the *Add/Remove Programs* window, scroll down the entire list of Currently installed programs.
4) For each program that should not be on the system (and was likely auto-installed by a sneaky website):
   - Jot down the name of the program on a piece of paper (all removed items will be written down).
   - Click to select the program. Click the "Change/Remove" button, answering "Yes" to any pop-up messages.
   - The program should unistall and return you to the *Add/Remove Programs* window.

   NOTE: Remove Symantec Norton AntiVirus first, if it is to be replaced by NOD32 on the system. LiveReg and LiveSubscribe must also be removed, unless the system contains additional Norton programs, in which case they must remain installed on the system. NOTE: An easy way to uninstall all Norton virus utilities AT THE SAME TIME: From Internet Explorer, browse to **www.sarc.com/symnrt** and download and run the Norton Removal Tool on the PC. After restarting the computer, all Norton utilities will be gone.
5) Click to close the *Add/Remove Programs* window and the *Control Panel*.
6) From Windows Explorer, browse to C:\Documents and Settings**user**\Start Menu\Programs\Startup.
7) Select and press [DELETE] to remove all potentially malicious programs from the system and then close Explorer.
8) From the Start menu of the workstation, select "Shut Down …" Disconnect the workstation's modem or network cable!

3. Checking for Malicious Program Installations via the Registry

1) Upon reboot, press [F8] in order to boot the workstation in "Safe Mode – Command Prompt Only."
2) Wait a short while for the system to start up. From the resulting *Command Prompt* window, press [CTRL] + [ALT] + [DELETE]. From the Task Manager, click the "Task Manager" button. Next, from the upper menu of the pop-up window, click "File" and select "New Task."
   Type **regedit** in order to open the *Registry Editor*.
3) From *Registry Editor*, browse to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run.
4) From the upper menu, click "File" and select "Export the key." Browse to C:\Backup\Registry.
5) Look for any unexpected or unusual items in the Run menu list. (If uncertain about any of the items listed in this, or any of the other Run directories, use a separate computer and search the name of the file in Google to see if it should be kept or not.) Right-click all unexpected items and select "Delete." Answer "Yes" in response to the pop-up message.
6) Jot down the name of all deleted items on a piece of paper (along with where the item resides on the workstation).
7) Press [F5] and verify that none of the items reappear in the directory. NOTE: Any reappearing item is likely a nasty virus.
8) Repeat step 5 - 7 for each of the following folder locations: RunOnce and RunOnceEx.
9) From *Registry Editor*, browse to HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run.
10) Repeat steps 4 – 7. NOTE: The CURRENT_USER Run directories will contain different information, depending upon which profile the user is logged in with. The contents of the CURRENT_USER must be checked for **EACH USER**.
11) Click the upper righthand [X] to close the *Registry Editor*.
12) If any item reappears in any of the run directories, then complete the following …

A. Removing Viruses from the Registry with the Aid of ERD Commander

1) Restart the workstation. Place the ERD (Emergency Recovery Disk) Commander CD into the CD-ROM. (Verify that the system is set to boot from the CD-ROM drive first!)
2) From the pop-up window, click to skip network configuration. At the following window, click "OK."
3) From the ERD desktop (which resembles to Windows' desktop), go to Start -> Administrative Tools -> Regedit.
4) Return to the registry path location where the virus reappeared.
5) Select the virus and press [DELETE] in order to delete it. Press [F5] and verify that it doesn't reappear. NOTE: Any items deleted via the ERD Commander registry should never reappear.
6) Next, browse to HKEY_CURRENT_USER and, for each user folder, check in the user's Run, RunOnce, and RunOnceEx folders for all files that should be deleted. Jot down and delete all files deemed unnecessary to keep. NOTE: *In the ERD Commander Registry (versus the regular Windows Registry), all users' directories can be viewed without having to be logged into the workstation as that specific user!*

B. Removing Files from the ERD Commander Version of Windows Explorer

1) From the ERD desktop, open Explorer. Browse to C:\Program Files.
2) Jot down any program file folders that you determine are unnecessary, then delete these suspect folders.
3) Browse to C:\Windows\System32. Jot down and delete all suspect files.
4) For each user:
   - From Explorer, browse to C:\Documents and Settings**user**.
   - Select the "Cookies" folder and press [DELETE]. Answer "Yes" in response to the pop-up message.
   - Double-click to open "Local Settings." (Be certain that hidden files are viewable in the Folder options.)
   - Open the "History" folder, select all items and press [DELETE]. Answer "Yes" to the pop-up message. Browse up one directory level.
   - Open the "Temporary Internet Files" folder, select all items and press [DELETE]. Answer "Yes" in response to the pop-up message. Browse up one directory level.
   - Double-click to open "Temp." Select all files and press [DELETE]. Answer "Yes" in response to the pop-up message.
5) Browse to C:\Windows\Prefetch. Select all items and press [DELETE]. Answer "Yes" to the pop-up message.
6) Close Explorer. From the desktop, right-click on the Recycle Bin and select "Empty Recycle Bin."

C. Changing Computer Management Settings with the Aid of ERD Commander

1) From the ERD desktop, click Start -> Administrative Tools" and then select "Service and Driver Manager."
2) From the menu list of the *Computer Management* window, click "Services."
3) Locate "Messenger." Right-click on it and select "Properties."
4) Change the Startup type from "Automatic" to "Manual." From the Service status menu, click "Stop."
5) Click "Apply" then "OK" to accept settings changes and click [X] to close the *Computer Management* window.
6) From the Start Menu, select "Shut Down …" Select "Shut down" and click "OK."

4. Installing NOD32 and Running a System Scan

(Perform this procedure only when NOD32 is to be installed on the system, in place of former virus protection software.)

1) Insert the IT Flash Drive into the workstation's USB port.
2) From the pop-up Windows Explorer window, browse to the drive's NOD32 folder and then double-click "nentenst.exe."
3) Click "Next" at the *Welcome to NOD32* window with "Typical" bulleted.
4) Click the "I Agree" bullet at the *License Agreement* window and then click "Next."
5) Click "Next" at the *Internet Connection* window with "I don't use proxy server" bulleted.
6) Click "Next" at the following window with "Enable ThreatSense.Net" checked.
7) Click "Enable detection of potentially unwanted applications" and click "Next."
8) Click "Next" at the following window with "I want to start the file system monitor automatically" checked.
9) Click "Next" again to complete the installation and then click "Finish" with "Restart now" bulleted.
10) Once Windows is up, login as the **user**.
11) From the lower right-hand corner of the Windows toolbar, double-click the NOD32 icon to launch the program.
12) From the *NOD32 Control Center* window, click "Update." A large pop-up window will appear. Click "Update now."
13) Wait a few moments for NOD32 updates to download.

5. Scanning the System's Registry Using Registry Mechanic

1) Insert the IT Flash Drive into the workstation's USB port.
2) From the Windows Explorer window, browse to the drive's "Registry Mechanic" folder and double-click "rminstall.exe."
3) Click "Next" at the *Setup – Registry Mechanic* window.
4) Click the "I accept the agreement" bullet and click "Next."
5) Click "Next" at the *Select File Destination* window and then click "Next" again.
6) Uncheck "Install the free Google Toolbar" and click "Next."
7) Click "Finish" with the "Start Registry Mechanic and scan for problems" checkbox checked.
   Registry Mechanic will now open and scan the registry. Wait a few minutes for the scan to complete.
8) Once finished, click "Repair." NOTE: You will need to click the link to register prior to completing the system repair.
   From Explorer, browse to the USB's Registry Mechanic folder, open the text file, and then locate and "Copy/Paste"
   the account name and password information into the corresponding fields in Registry Mechanic.
9) Once the repair is finished, click "Continue" at the pop-up window.
10) Next, from the main window of Registry Mechanic, click "Optimize Your System."
11) Next, from the main window, click "Compact Registry."
12) From the *Registry compacting* pop-up window, check the "Create System Restore Point" and click "Yes."
    Wait a few minutes for the registry to prepare to compact. From the following window, click "Compact Now"
    and then click "Restart" in order to complete the compact process.
13) Once the workstation has restarted, log back in as the user.

6. Scanning for Embedded Pop-ups Using CWShredder Software

1) Upon reboot, remove the ERD Commander CD from the CD-ROM (and reset the workstation to boot from A: or C: first).
   NOTE: Jot down notes on any virus software (Norton or MacAfee) pop-up warning messages about viruses.
2) Insert the USB hard drive containing Pop-up Blocker software (CWShredder, HiJackThis, Ad-Aware, etc.).
   NOTE: CWShredder and HiJackThis are the two most important of these scans.
3) Login to the workstation using the same Windows (2000 or XP) profile that was utilized previously.
4) From Windows Explorer, browse to the USB hard drive location (oftentimes E:\).
5) Copy The CWShredder and HiJackThis folders. Browse to C:\ and paste the folders.
6) From C:\CWShredder, double-click to open "CWShredder.exe."
7) From the main window of CWShredder, uncheck the "Move bad files found to recycle bin" checkbox and click "Fix ->."
8) Click "OK" in response to the pop-up window. CWShredder will run and capture viruses (if any are found).
9) Once the scan is complete, click "Next ->" and then click "Exit."

7. Scanning for Embedded Pop-ups Using Ad-Aware Software

1) From the USB's "AdAware" folder, double-click to run "aawsepersonal.exe."
2) Follow the prompts in order to install AdAware. (NOTE: Do NOT check to store the program icon on the desktop.)
3) From the main window, click "Start."
4) Click "Next" with "Perform smart system-scan" bulleted. Ad-aware will now perform a system scan.
5) After a few minutes, a bug icon will flash, indicating that the scan is finished. click "Next."
6) From the menu, right-click on the Obj. checkbox and select "Select all objects." Next, click the "Quarantine" button.
7) From the pop-up window, type **1** for the File Name and click "OK" twice to quarantine the selected files.
8) Click "Next" and "OK" to remove the quarantined files from the system.
9) Click the upper-righthand [X] to close Ad-aware 6.

8. Scanning for Embedded Pop-ups Using Spybot – Search & Destroy

1) From the USB's "Spybot" folder, double-click to run "spybotsd13.exe."
2) Follow the prompts in order to install Spybot. (NOTE: Do NOT check to store the program icon on the desktop.)
3) From the main window of Spybot, click "Check for problems." The software will take a few minutes to scan the PC.
4) Upon scan completion, a message will appear.
5) If no threats were found … Click the upper righthand [X] to close *Spybot.*
6) If threats were found … From the lefthand menu of Spybot, click "Immunize." Click "OK" in response to the pop-up. After the immunization has finished, click [X] to close *Spybot.*

9. Scanning for Embedded Pop-ups Using HiJackThis

1) From C:\HiJackThis, double-click to open "HiJackThis."
2) Run HiJackThis. From the pop-up list, check to remove all items (many will be changes made to Internet Explorer, such as removing toolbars and extra buttons) that have altered Internet Explorer in any way.
3) Also, uncheck to remove any other suspicious items determined to be unimportant to the workstation (possible viruses).
   NOTE: To properly research unknown items appearing in the HiJackThis log, click and drag to highlight the entire log and then right-click on the highlighted text and select "Copy." Open an Internet Explorer window.
   From Internet Explorer, type **www.hijackthis.de** in the Address field and press [ENTER]. Scroll down the webpage and then right-click and "Paste" the log text into the webpage's Log file sub-window and then click "Analyze."
4) Once finished unchecking items, click "OK" in order to save changes. Answer "NO" at the pop-up (do not reboot).
5) From C:\CWShredder, double-click to run "CWShredder.exe" a second time.
   NOTE: If any viruses reappear, they are extra NASTY ones. To delete them permanently, rerun CWShredder using the Windows Safe Mode -> Command Prompt (or via the ERD Commander).
6) From C:\HiJackThis, double-click to run "HiJackThis" a second time.
7) For each item that was previously unchecked/deleted but has now reappeared:
   - Search for the item in Windows Explorer (searching also w/in hidden files and folders).
   - Once the item is located, delete it.
   - If the item is a service …
     - Right-click on "My Computer" and select "Manage."
     - From the menu list of the *Computer Management* window, click "Services and Applications."
     - From the window on the right, double-click to open "Services."
     - Locate the specific service item. Right-click on it and select "Properties."
     - Change the Startup type from "Automatic" to "Disabled."
     - Click "Apply" then "OK" to accept changes and click [X] to close the *Computer Management* window.
8) Continue to re-run CWShredder and HiJackThis until NONE of the previously deleted items reappears.
   NOTE: Some items may not be able to be deleted unless in Safe Mode (see step 8).
9) From the Start Menu, select "Shut Down …" Select "Shut down" and click "OK."

10. Deleting Files and Folders via Windows Safe Mode -> Command Prompt

NOTE: This particular series of steps will help you track down files that are listed in HiJackThis, Internet Explorer Add Ons, etc., but cannot be located via Windows Explorer.

1) Upon reboot, press [F8] in order to boot the workstation in "Safe Mode – Command Prompt Only."
2) Wait a short while for the system to start up. Login using the same Windows (2000 or XP) profile utilized previously.
3) From Windows Explorer, browse to the USB hard drive location (oftentimes E:\).
4) Using DOS via the Command Prompt, delete ALL suspect folders and files that could not be deleted in previous attempts (in Windows regular mode). *See jotted notes for specific files that still need to be deleted.*
   NOTE: Use **attrib *.*** to show all hidden files and folders located within a given dir.
5) From the upper menu of the pop-up window, click "File" and select "New Task."
6) Run HiJackThis again. All items that could not previously be deleted permanently should now be deleted.
7) From the Start Menu, select "Shut Down …" Select "Shut down" and click "OK."
8) Remove the USB drive containing the virus scanning software programs.

11. Reestablishing TCP/IP

1) Restart the workstation. Login to the workstation using the same Windows (2000 or XP) profile that was used previously.
2) From the Start Menu, select "Control Panel -> Network Connections." Right-click on the "Local Area Connection" and select "Properties." NOTE: TCP/IP will ALREADY APPEAR in the LAN Properties list, even though it is DISABLED.
3) Install a new "Protocol." Click "Have Disk …" Type C:\Windows\inf and click "OK."
4) Select "Microsoft -> Internet Protocol TCP/IP" and then click "OK" in order to reinstall TCP/IP (Winsock and Winsock2 will now reappear in the registry).
5) Next, from the *Protocols* window, uncheck all unnecessary protocols (leave only the primary protocols) and click "OK."
6) From the Start Menu, select "Shut Down …" Select "Shut down" and click "OK."
7) Upon restart, connect the workstation (via a modem or network cable).
8) Restart the workstation. Login to the workstation using the same Windows (2000 or XP) profile that was used previously.

12. Testing Internet Accessibility and Deleting Files from Internet Explorer

1) Test to see if the internet is working by opening Internet Explorer and browsing to a few websites. NOTE: It may be necessary to click "File" and then "Work Offline" to uncheck the Work offline feature. Close Internet Explorer.
2) From the desktop, right-click on "Internet Explorer" and select "Properties."
3) From the General tab of the *Internet Options* window, click "Delete Cookies …" Click "OK" in response to the pop-up.
4) Next, click "Delete Files …" Click "OK" in response to the pop-up.
5) Click "Clear History" and click "Yes" in response to the pop-up.
6) Click the "Use Blank" button to re-route the default home page.
7) Click "Settings …" From the *Settings* window, reduce the Amount of disk space to use to **50** MB. Click "OK."
8) Change the "Days to keep pages in history" to **3**.
9) From the Security tab, click the "Default" button.
10) From the Trusted Sites section, verify there are no illegitimate sites set as trusted. Click the "Restore Defaults" button.
11) Click "Apply" then "OK", and then close Internet Explorer.
12) From the desktop, double-click to open "Internet Explorer."
13) Verify that the system can access the internet. (This can also be tested by opening the Command Prompt and typing the command **ping** (**a specific webpage or IPaddress**).
14) If no access was established, check the network/modem connection. If still no access can be established, From the Start Menu, select "Control Panel -> Network Connections." Right-click on "TCP/IP" and then select "Renew configuration." (Winsock and Winsock2 will now be reconfigured in the registry).
    NOTE: Another way to reestablish Winsock and Winsock2 is to browse to C:\Backup\Registry, then double-click on the backed up "Winsock" and "Winsock2." (This will automatically cause these files to overwrite the existing registry files.)

13. Reinstalling AOL *(ONLY WHEN NECESSARY)*

(NOTE: If a system is running REALLY slow, check the Task Manager to determine if AOL components are taxing the CPU Sometimes AOL will need to be reinstalled, in order to greatly improve system performance… The same goes for Norton.)

1) From Explorer, browse to C:\Documents and Settings\All Users\Application Data\AOL\Organize.
2) Highlight all files in the Organize folder and then right-click and select "Copy."
3) Browse to C:\Backup. Right-click and create a new folder named "AOL." Open it and create another new folder named "Organize." Open this folder. Within this folder, right-click and "Paste" in order to paste the user's important AOL data.
4) Close Explorer, and then, from the From the Start menu of the workstation, select Settings -> "Control Panel."
5) From the *Control Panel*, double-click to open "Add/Remove Programs."
6) From the *Add/Remove Programs* window, select and click to uninstall ALL AOL-related software.
7) Once all have been removed, click to close the *Add/Remove Programs* window and the *Control Panel*.

14. Reinstalling MSConfig Services

1) From the left-hand portion of the Windows toolbar, click "Start" and then click "Run …"
2) From the Open field of the *Run* window, type **MSConfig** and click "OK."
3) From MSConfig, re-enable EVERYTHING in the Services section that is determined to be integral to the user's PC.
4) Click "Apply" and "Close." From the pop-up window, click "Restart."
5) Once the system has been restarted and logged in to the appropriate user, from the pop-up window, check the "Don't show this window upon startup …" checkbox and click "OK."

15. Running Windows Updates

1) From the Start Menu, click "All Programs" then "Windows Update."
2) Click "Custom" at the *Keep Your Computer Up to Date* screen. The site will again scan the system for necessary updates.
3) Once the list of updates appears, from each left-hand menu, select the checkbox/bullet for all files that need installed.
4) After compiling all necessary files, click the "Review and install updates" link and then "Install Updates."
5) From the installation pop-up, click "I Accept" (and/or "Next") in order to download and install the update files.
6) Once update installation is complete, click "Restart Now."
7) Repeat steps 1 – 6, until all necessary Windows XP updates have been installed.

Assuming that the workstation is now "happy" (ALL viruses have been removed) and now has internet access…

16. Scanning for System Viruses Using AntiVirus Software (NOD32, for example)

1) From the lower right-hand corner of the Windows toolbar, double-click the NOD32 icon to launch the program.
2) From the *NOD32 Control Center* window, click "NOD32" (located in the Threat Protection Modules list). A large pop-up window will appear.
3) Click "Local (Scan local disks)" in order to begin a scan of the system's hard drive.
4) Wait a few moments for the NOD32 scan to complete.
5) Once the scan has finished, click "Quit."
6) If there is adequate time available, click "In-depth analysis" in order to begin a deep scan of the system's hard drive. Wait awhile for the NOD32 scan to complete. Once the scan has finished, click "Quit."
7) Next, from the right-hand window, click "Hide."
8) From the upper right-hand corner of the *NOD32 Control Center* window, click the down arrow to minimize the program.

17. Verifying Hard Drive and Memory Free Space

1) From the desktop, double-click to open "My Computer."
2) Right-click on "Local Disk (C:)" and then select "Properties."
3) From the General tab of the *Local Disk Properties* window, look at the Free Space and Used Space numbers in order to help determine if the drive needs replaced (for instance, if its free space is precariously close to running out, etc.).
4) Click "OK" to close the *Local Disk Properties* window.
5) Ensure that NO programs are open/running on the system.
6) Press [CTRL] + [ALT] + [DELETE]. From the *Windows Security* window, click "Task Manager."
7) From the bottom of the *Task Manager*, look at the system's CPU Usage amount. If the number is high, browse through the list of processes to determine which is demanding a large chunk of resources. Fix as necessary.
8) Also, from the bottom menu of the *Task Manager*, look at the system's Commit Charge in order to help determine if the Amount of memory needs to be increased (for instance, if the first amount is close to or above the second (total memory) – Example: 496 / 512).

TWO ADDITIONAL STEPS TO PERFORM, WHICH HELP WITH WORKSTATION PERFORMANCE:
(Perform these steps ONLY if there is lots of time available to work on the system)

18a. Run Scandisk

1) From the desktop, double-click to open "My Computer."
2) Right-click on "Local Disk (C:)" and select "Properties."
3) From the *Local Disk (C:) Properties* window, click the Tools tab and then click "Check Now …" to run Scandisk.
4) From the pop-up window, check the "Automatically fix file system errors" and "Scan for and attempt recovery of sectors" checkboxes and click "Start."
5) Answer "Yes" in response to the "Disk check could not be performed. Do you want to check at next startup?" message.
6) Click "OK" to close the *Local Disk (C:)* window.
7) Click the upper righthand [X] to close *My Computer*.
8) From the Start Menu, select "Shut Down …" Select "Restart" and click "OK."
9) Verify that Scandisk runs on the system.
10) After the scan has finished, log on to the system.

18b. Run Disk Defragmenter

(This step is performed not in order to remove viruses, but to enhance system performance.)

1) From the desktop, double-click to open "My Computer."
2) Right-click on "Local Disk (C:)" and select "Properties."
3) From the *Local Disk (C:) Properties* window, click the Tools tab and then click "Defragment Now …"
4) From the menu list, click to highlight "(C:)" and click "Defragment." (The defragment process will take a while.)
5) Click "Close" to close the pop-up window that appears once the defragment process has finished.
6) Click the upper righthand [X] to close *Disk Defragmenter*.
7) Click the upper righthand [X] to close *My Computer*.