CIA TECHNICAL HANDBOOK

TABLE OF CONTENTS

MISSION OBJECTIVES

- Understand new ways to check in clients and manage their expectations
- Understand new diagnostic processes and tools
- Troubleshoot and eradicate viruses effectively
- Understand what Adware/Spyware are and how to eradicate them
- Learn new, basic, and low level troubleshooting procedures
- Learn more effective ways of resolving advanced operating system issues, NOT just restoring
- Resolve advanced Winsock/Dial-up Networking issues

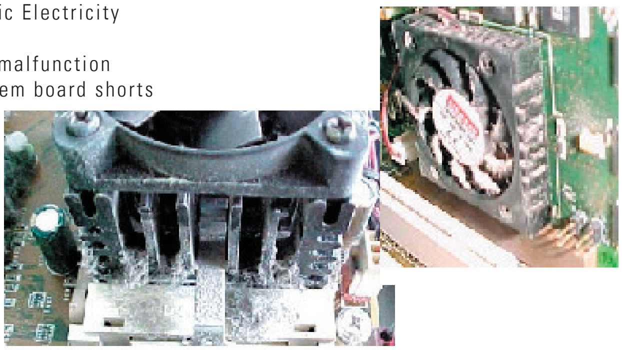
2.0 - LEVEL 1 – PRE-OPERATIONS (PRE-OP)

The following are steps that take only a moment andA be performed on every computer before it is checked into tech bench or at the begining of an on-site service call

- Replicate client's issue(s)
- Open the computer case:
- Check for dust
- Check for distended capacitors
- Check for unseated cards and unconnected cables
- Check fans for proper operation

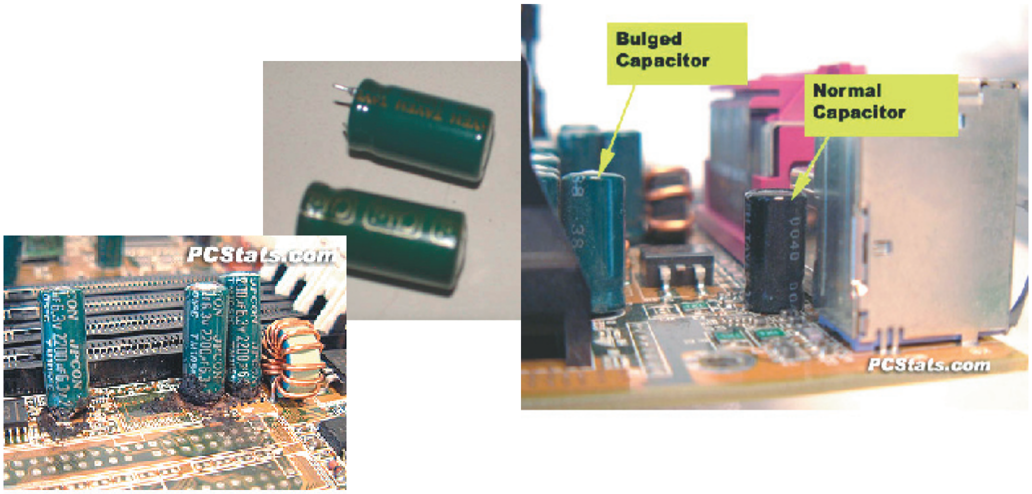
- Perform visual software inspection for viruses and spyware
- Check for rogue processes and startup applications

Check For Dust
The following are problems that can and will be caused by dust:
- Static Electricity
- Heat
- Fan malfunction
- System board shorts



Typically, you can use some type of pressured air tank (like the one used in Mobile Install) to effectively clean out computers. Because of the chemical residue that may accumulate on the system board, canned air is not recommended for performing this. Get authorization from the client for a System Cleaning before performing this task.

Distended Capacitors
A Distended Capacitor is an immediate service disqualifier. When a distended capacitor is found, you can deem the computer to have a defective system board. Look for either a bulge on the top side of the capacitor or an acid-like mark on the top or the bottom of the capacitor.



3.0 - COMPUTER CHECK-IN

* Perform the initial diagnosis for the product before creating a STAR Service Order

For all computers, administer the following:

Perform the Non-Negotiables

- Require the client to sign disclaimer form.
- Each computer is granted a five minute consultation. These five minutes should be used for "quick fixes" and the initial diagnostic. All steps of C.A.R.E. should be administered at this time as well.
- If the computer is able to be repaired in less than five minutes, perform repairs and send client on their way.
- If computer is not able to be repaired during initial consultation phase, inform the client that a full, in-depth diagnosis must be performed to determine the nature and extent of the problem(s).
- If the client's equipment is not covered by a warranty or PSP, inform client that a $59 diagnostic fee is necessary to perform the diagnostic procedures to determine the problem.
    - Inform client of anticipated total cost of service and also inform them that the $59 diagnostic fee is non-refundable and does not apply towards the cost of the repairs.
    - If product is covered under by a warranty or PSP the $59 diagnostic fee is waived.
- Create STAR tag at this time with detailed notes.
- Collect $59 Diagnostic Fee through P.O.S. and attach copy of receipt to signed STAR Tag.
- Inform client that they will be receiving a phone call with a quote for total cost of repairs within given time frame

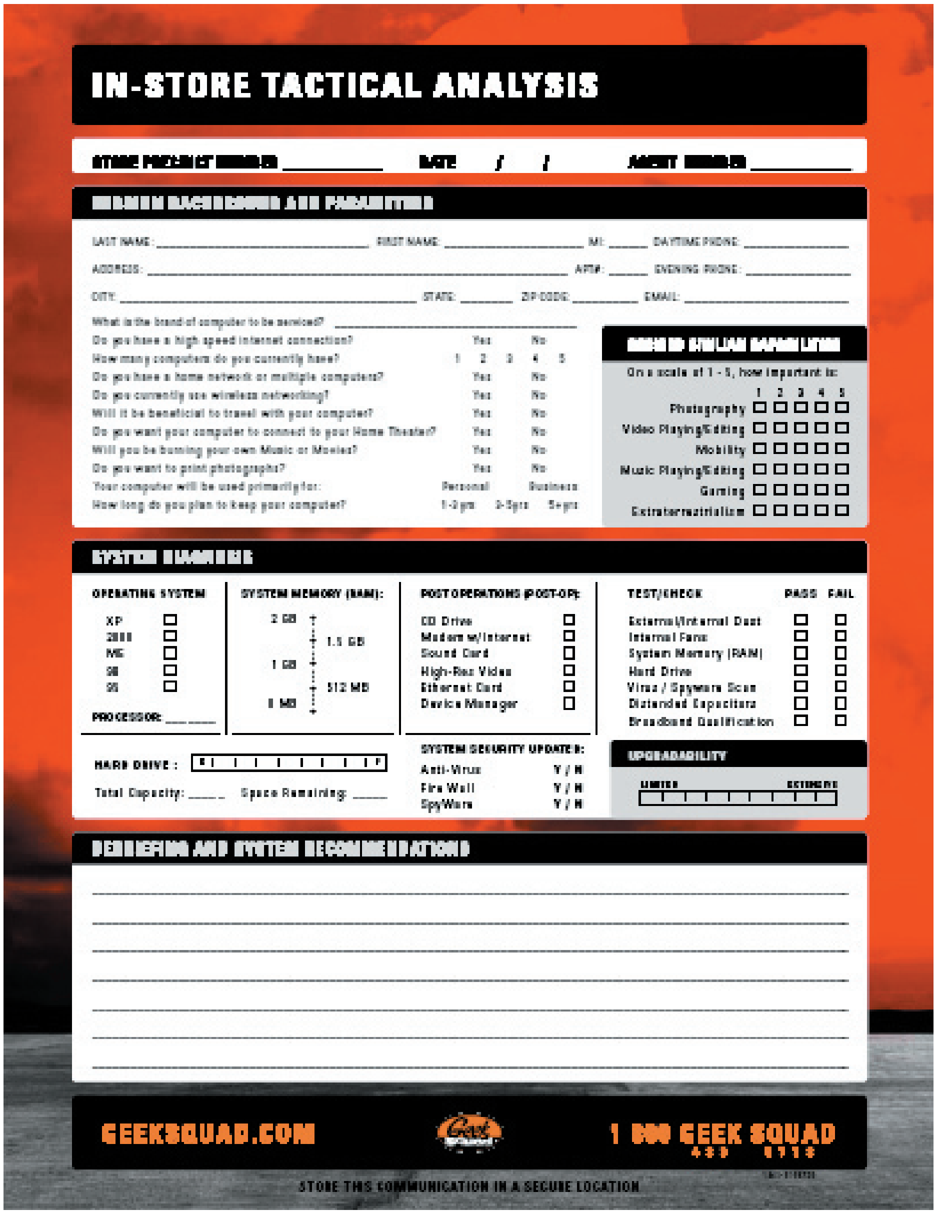
During the initial consolation phase a thorough examination of both hardware and software pieces should be performed to make a very knowledgeable and accurate rough estimate for total cost of repairs.

Examination points to consider, but not limited to:

- Open case to check for dust
- Proper operation of all fans
- Unseated cards and cables
- Distended capacitors
- Spyware and or Viruses
- Low system resources
- Amount of memory
- Any other applicable examinations that the technician feels necessary

3.1 - IN-STORE FORMS

In-Store Tactical Analysis (front)



IN-STORE TACTICAL ANALYSIS

STORE PRECINCT NUMBER ___________ DATE / / AGENT NUMBER ___________

MISSION BACKGROUND AND PARAMETERS

LAST NAME: ____________ FIRST NAME: ____________ MI: _____ DAYTIME PHONE: ____________

ADDRESS: ______________________ APT#: _____ EVENING PHONE: ____________

CITY: ____________ STATE: ______ ZIP CODE: ________ EMAIL: ____________

What is the brand of computer to be serviced? ____________________

Do you have a high speed internet connection?		Yes		No	
How many computers do you currently have?	1	2	3	4	5
Do you have a home network or multiple computers?		Yes		No	
Do you currently use wireless networking?		Yes		No	
Will it be beneficial to travel with your computer?		Yes		No	
Do you want your computer to connect to your Home Theater?		Yes		No	
Will you be burning your own Music or Movies?		Yes		No	
Do you want to print photographs?		Yes		No	
Your computer will be used primarily for:	Personal			Business	
How long do you plan to keep your computer?	1-2yrs		3-5yrs		5+yrs

DESIRED CIVILIAN CAPABILITIES

On a scale of 1 - 5, how important is:

	1	2	3	4	5
Photography	□	□	□	□	□
Video Playing/Editing	□	□	□	□	□
Mobility	□	□	□	□	□
Music Playing/Editing	□	□	□	□	□
Gaming	□	□	□	□	□
Extraterrestrialism	□	□	□	□	□

SYSTEM DIAGNOSIS

OPERATING SYSTEM

XP	□
2000	□
ME	□
98	□
95	□

PROCESSOR: ______

SYSTEM MEMORY (RAM):

2 GB
1.5 GB
1 GB
512 MB
0 MB

POST OPERATIONS (POST-OP):

CD Drive	□
Modem w/Internet	□
Sound Card	□
High-Res Video	□
Ethernet Card	□
Device Manager	□

TEST/CHECK	PASS	FAIL
External/Internal Dust	□	□
Internal Fans	□	□
System Memory (RAM)	□	□
Hard Drive	□	□
Virus / Spyware Scan	□	□
Distended Capacitors	□	□
Broadband Qualification	□	□

HARD DRIVE: E F

Total Capacity: _____ Space Remaining: _____

SYSTEM SECURITY UPDATES:

Anti-Virus	Y / N
Fire Wall	Y / N
SpyWare	Y / N

UPGRADABILITY

LIMITED EXTENSIVE

DEBRIEFING AND SYSTEM RECOMMENDATIONS

____
____
____
____
____
____
____

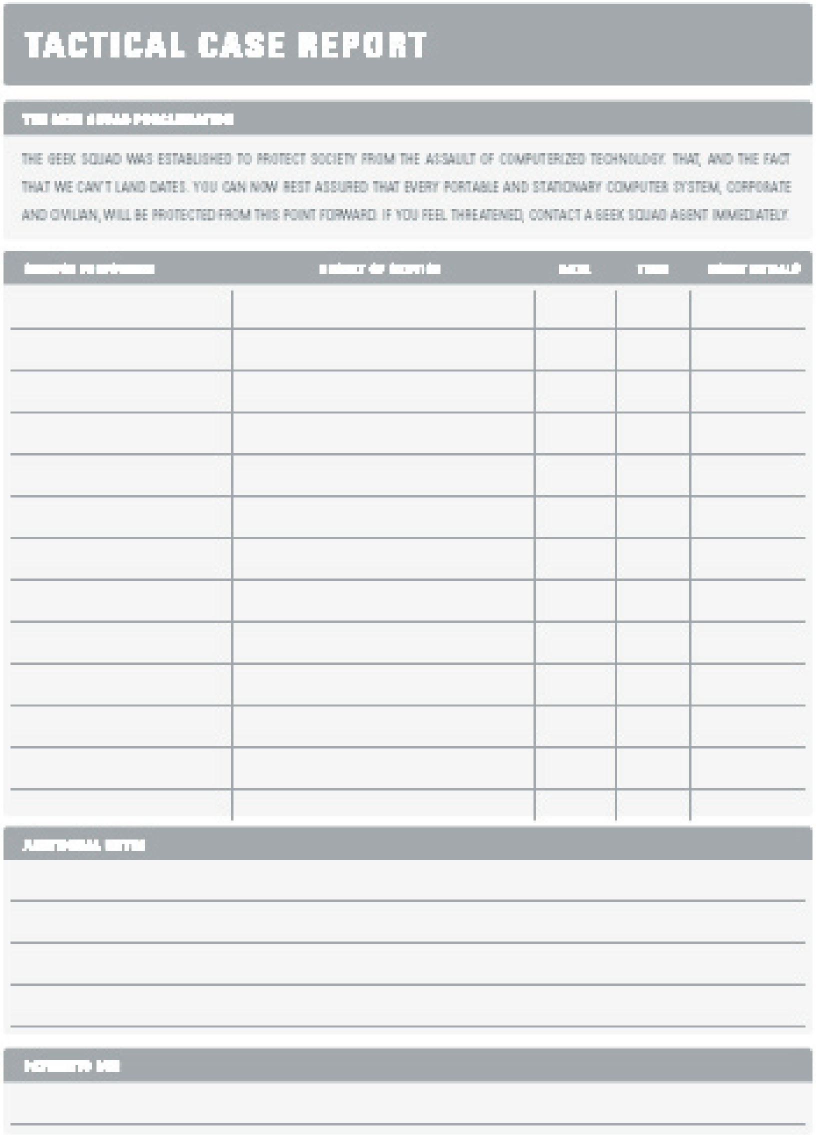
GEEKSQUAD.COM 1 800 GEEK SQUAD
433 7783

STORE THIS COMMUNICATION IN A SECURE LOCATION

Data collection points include
- Client’s personal: name, address, phone, computer habits
- Client’s computer information: OS version, CPU, RAM, HD
- Pre-Op checklits

Customer feedback information
- Debriefing and Recommendations: recommendations of what should/might be done to computer

Tactical Case Report



TACTICAL CASE REPORT

THE GEEK SQUAD PROCLAMATION

THE GEEK SQUAD WAS ESTABLISHED TO PROTECT SOCIETY FROM THE ASSAULT OF COMPUTERIZED TECHNOLOGY. THAT, AND THE FACT THAT WE CAN'T LAND DATES. YOU CAN NOW REST ASSURED THAT EVERY PORTABLE AND STATIONARY COMPUTER SYSTEM, CORPORATE AND CIVILIAN, WILL BE PROTECTED FROM THIS POINT FORWARD. IF YOU FEEL THREATENED, CONTACT A GEEK SQUAD AGENT IMMEDIATELY.

[illegible]	[illegible]	DATE	TIME	[illegible]

ADDITIONAL NOTES

PAYMENT DUE

- Technician’s note section
- Technician will document ALL work performed and the results here
- This will be shown to the client when they pick their machine up
- Additional notes about the client’s computer
- Payment due

4.0 - LEVEL 2 DIAGNOSTICS

- Run PC Doctor
- Run DFT
- Run virus scan
- Run spyware scan (reference section 6.8 for instructions)

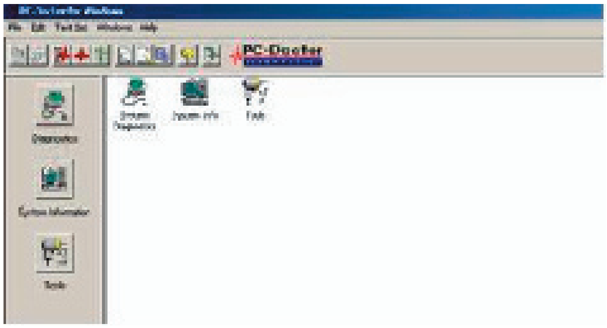
Document ALL Level 2 diagnostic findings. There are appropriate sections on the "In-Store Tactical Analysis" form for all of the Level 1 and Level 2 Diagnostic tests under the section labeled "System Diagnosis".

If possible hard drive failure is present, IMMEDIATELY STOP working on the client's machine and contact them with findings/solutions.

Once your Level 2 diagnostics are completed, stop working on the machine and contact the client for approval.

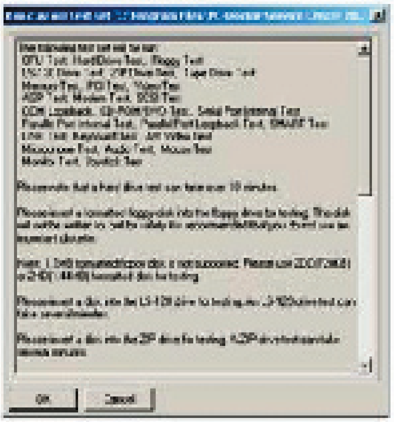
4.1 - PC-DOCTOR DIAGNOSTICS

- Start the PC into any version of Microsoft® Windows®
- Close all programs, INCLUDING anti-virus programs
- Insert the PC-Doctor CD into the CD-ROM
- Connect Parallel loop back Adaptor (program will not run without it)
- Select one of the install options from the Options menu
    - Install
    - Quick Install and Run
    - Create self-booting disk
    - Run PC-Doctor from CD
    - Uninstall
- Example (running within OS)
- Select Diagnostics from the menu



The program will ask you to select the tests to be run and then prompt you to this screen to confirm (this will also give you any special instructions for each test)

- Testing will commence and record parameters and status
- Note: Some tests (mouse, graphics, keyboard) will require interaction. Once again this will be noted as special instructions before the testing starts.
- Once testing is completed the results will be posted to view applicable issues. The details tab will also drill down into more information about each test.



The following test set will be run:
CPU Test, HardDrive Test, Floppy Test
LS-120 Drive Test, ZIP Drive Test, Tape Drive Test
Memory Test, PCI Test, Video Test
AGP Test, Modem Test, SCSI Test
COM Loopback, CD-ROM/DVD Test, Serial Port Internal Test
Parallel Port Internal Test, Parallel Port Loopback Test, SMART Test
USB Test, Keyboard Test, [illegible]
Microphone Test, Audio Test, Mouse Test
Monitor Test, Joystick Test

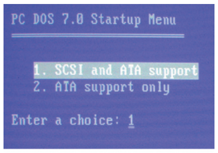
Please note that a hard disk test can take over 10 minutes.

Please insert a formatted floppy disk into the floppy drive for testing. [illegible]

Note: 1.2MB formatted floppy disk is not supported. Please use 2DD (720KB) or 2HD (1.44MB) formatted disk for testing.

Please insert a disk into the LS-120 drive for testing. [illegible]

Please insert a disk into the ZIP drive for testing. [illegible]

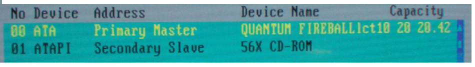


```
PC DOS 7.0 Startup Menu

  1. SCSI and ATA support
  2. ATA support only

Enter a choice: 1
```

4.2 - Hard Drive Sector Scan - DFT (Drive Fitness Test)

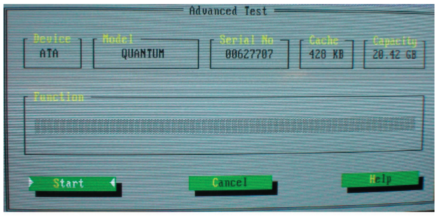
Choose ATA or SCSI support

- If running the test from a CD, choose Abort (A) when a message appears attempting to access the floppy drive for a log file. This message will not appear when running DFT from a floppy
- Agree to the license agreement
- Verify that all hard drives appear
- Run tests in 'Advanced' mode



```
No Device  Address          Device Name                  Capacity
00 ATA     Primary Master   QUANTUM FIREBALLlct10 20 20.42
01 ATAPI   Secondary Slave  56X CD-ROM
```

This software package runs only one Hard Drive at a time. Start testing one of the drives.



```
Advanced Test
Device   Model     Serial No   Cache    Capacity
ATA      QUANTUM   00627707    428 KB   20.42 GB
```

If the hard drive tests complete successfully the results screen will display with a green background. If the background color is red, the hard drive has failed a test. Proceed to match up the error code from the list that can be found on page 32 of the following PDF. Most of the time when this test fails the hard drive needs to be replaced.

http://www.hgst.com/hdd/support/dft32_userguide.pdf

REPLACE HD (Usually these codes mean HD replacement is necessary)

0x42 Drive temperature problem
0x70 Corrupt Sector [A general hard disk problem was detected. You can run the "Erase Disk" utility. If a subsequent test fails again, the drive is defective and should be replaced.
0x72 Device S.M.A.R.T. Error
0x73 Device damaged by shock
0x74 S.M.A.R.T. Self-test failed [An error was detected during S.M.A.R.T. self-test. You can run the "Erase Disk" utility of DFT. IF a subsequent test fails again, the drive is defective and should be replaced.
0x75 Defective Hard Disk Drive Component

OTHER ERROR CODES

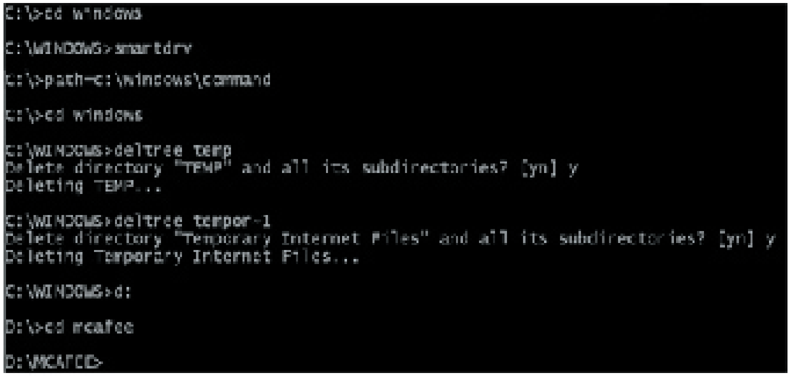
0x00 No Error
0x10 Test aborted by user
0x20 Selected drive not present
0x21 ATA Master device not present
0x22 Device protected
0x23 Format Degraded
0x30 Out of Memory
0x31 Wrong Parameter
0x33 Function cannot be executed on this device
0x40 System interrupts the current operation [smartdrv.exe can cause this error]
0x41 Bad Cable
0x43 Pending SCSI request
0x44 System Vibration
0x45 Low System Performance
0x71 Device not ready

4.3 - Virus Scan (McAfee Command Line)

Windows 95/98/SE/ME

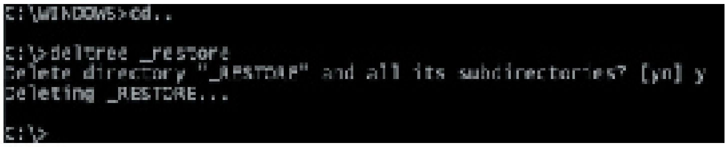
Follow these instructions for scanning for viruses.

- Boot from MRI or boot disk
- Go to CD drive and type in the following command: smartdrv
- Go to C drive (C:\)
- Precede to delete all temp/temp Internet/restore files



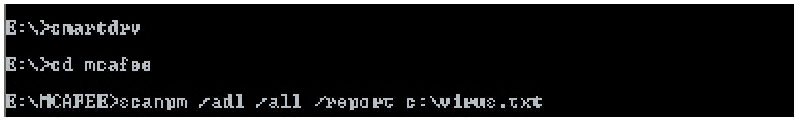
```
C:\>cd windows

C:\WINDOWS>smartdrv

C:\>path=c:\windows\command

C:\>cd windows

C:\WINDOWS>deltree temp
Delete directory "TEMP" and all its subdirectories? [yn] y
Deleting TEMP...

C:\WINDOWS>deltree tempor~1
Delete directory "Temporary Internet Files" and all its subdirectories? [yn] y
Deleting Temporary Internet Files...

C:\WINDOWS>d:

D:\>cd mcafee

D:\MCAFEE>
```

Note: If Win ME, perform the following command
   * It may be easier to remove temp/restore files from within Windows



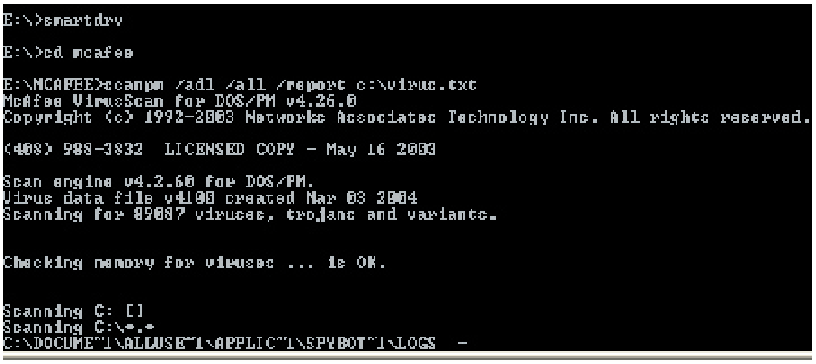
```
C:\WINDOWS>cd..

C:\>deltree _restore
Delete directory "_RESTORE" and all its subdirectories? [yn] y
Deleting _RESTORE...

C:\>
```

- Go to CD drive and type in the following commands:



```
E:\>smartdrv

E:\>cd mcafee

E:\MCAFEE>scanpm /adl /all /report c:\virus.txt
```

- The scan will commence

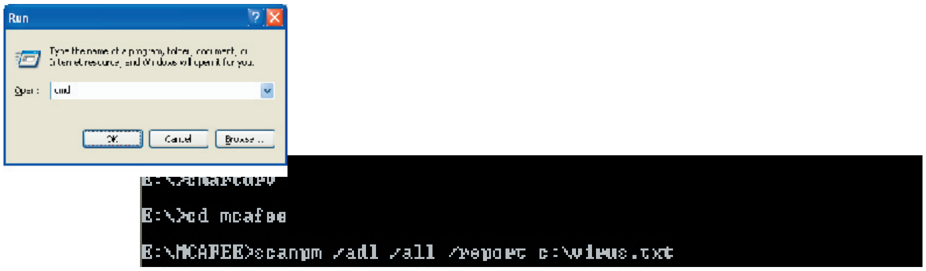


```
E:\>smartdrv

E:\>cd mcafee

E:\MCAFEE>scanpm /adl /all /report c:\virus.txt
McAfee VirusScan for DOS/PM v4.26.0
Copyright (c) 1992-2003 Networks Associates Technology Inc. All rights reserved.

(408) 988-3832  LICENSED COPY - May 16 2003

Scan engine v4.2.60 for DOS/PM.
Virus data file v4100 created Mar 03 2004
Scanning for 89087 viruses, trojans and variants.


Checking memory for viruses ... is OK.


Scanning C: []
Scanning C:\*.*
C:\DOCUME~1\ALLUSE~1\APPLIC~1\SPYBOT~1\LOGS  -
```

4.3 - Windows NT / 2000 / XP - (NTFS)

Each of these operating systems have the ability to run on the New Technology File Systems (NTFS) which cannot be accessed from a standard boot disk. You first need to boot into Windows Safe Mode. Then follow these instructions:

- Open the run command
- Type 'cmd' or 'command' – Command Prompt will open
- Go to CD drive and type in the following commands:

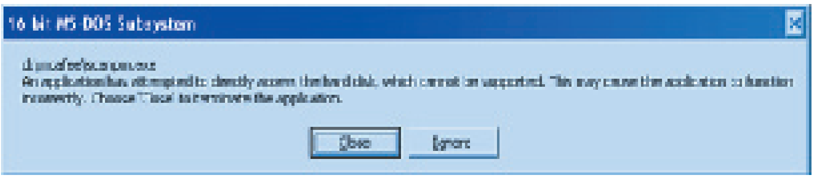


Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
OK
Cancel
Browse...

Open: cmd

```
E:\>[illegible]

E:\>cd mcafee

E:\MCAFEE>scanpm /adl /all /report c:\virus.txt
```

- When running a scan within Windows NT/2k/XP you may get an error. Click 'Ignore' and continue the scan process. This will not damage any files.



[illegible]
An application has attempted to directly access the hard disk, which cannot be supported. This may cause the application to function incorrectly. Choose 'Close' to terminate the application.

NOTE: If a virus is found, first, contact the client and approve (if not previously approved) the cost for removing a virus.

- This is a software issue and it is not covered under any warranty or PSP.
- This is also a great time to up-sell the installation of new anti-virus software if necessary.

Commonly Used Switches:

- /adl = all drives local
- /all = all files
- /report c:\<filename> = create a report file
- /append = appends report
- /clean = clean
- /? = help
- scanpm /? = help

5.0 - CONTACTING CLIENT

After the full diagnostic suite is completed, contact client with findings, appropriate solutions, and total cost of said solutions. It is very important that all repairs that are necessary to be made are noted on Tactical Case Report form so that the phone call and approval amount is accurate.

After making contact with the client and they approve/disapprove the cost, make sure that the conversation time, date and approvals/disapprovals are documented on the Tactical Case Report form. It is to your benefit to get the name of person approving/disapproving the repairs if it is not the client. If client approves/disapproves part of the service, but not all of it, make sure that there are notes on the Tactical Case Report form that reflect this. Also, if there are any parts that client needs to pay for this should be noted on the Tactical Case Report form.

If client is not available, leave a message informing them that they should contact the tech bench at the appropriate number and that you are looking for an approval for the estimate.

After getting approval perform necessary repairs and continue with service.

6.1 - Motherboard / Power-Related Service Diagnostics

NOTE: Pre-Op should have already taken place

If the system does not boot:

- Use power supply tester to verify that it is pushing out power.

- Test power supply and CMOS battery with a voltmeter.

- Power Supply - (DC: +/- 5, +/- 12)
- CMOS – (+/-3V)

NOTE: Settings will need to be entered in the BIOS afterwards

If power supply is functioning:
- Check all cables
- Pull/Reseat all cards, memory and processor
- If that doesn't work, it is probably a bad motherboard

If power supply is not functioning:
- Try a different power supply
- Pull all cards except video card and one stick of RAM
- If the computer turns on, use process of elimination to find out which card is preventing the computer from powering on.
- Try a test switch or jump motherboard

Lookup Beep Codes if you hear any:
Reference: http://www.computerhope.com/beep.htm

6.2 - BIOS Errors

Keyboard Errors:

- Check for stuck keys
- Try different keyboard otherwise it is probably a defective port
- Try another keyboard type (USB/PS2)

Checksum Error:

- Reboot system
- If it recurs verify settings in BIOS (system clock)
- If it recurs pull battery and power cable for 30 seconds
- If it recurs replace CMOS battery
- If it recurs re-flash CMOS using jumper on motherboard
- If it recurs it is a defective motherboard

No Hard Drive Recognized:

- Check all cables
- See if the Hard Drive is even spinning
- Volt-test the power cable to the hard drive
- Check IDE settings in the BIOS (Auto)
- Try different IDE cable and power cable
- Try other IDE channel (Secondary)
- Try client’s Hard Drive in test computer
- Try different Hard Drive in client’s computer

6.3 - STOP Errors / SU Errors

STOP ERRORS
STOP errors messages are software crashes or hardware malfunctions that cause the operating system to halt normal usage.

- Are similar to SU errors, although they don't always happen when installing / reinstalling the operating system. Again, reference the Microsoft Knowledge Base for details on why the error is occurring.
- Also, search by STOP error number (i.e. 0x0000000). Check Google.com (or Google Groups) using the SU error code to find the fix workaround.

SU ERRORS

- Usually appear when trying to install a new copy of Windows or when performing a Soft Install of Windows. There is a fix or workaround for all SU errors.
- When an SU error is encountered, reference the Microsoft Knowledge Base article Q129971 for detail on why this error is occurring.
- Also, check Google.com (or Google Groups), using the SU error code to find the fix or workaround.

ERROR SU0350 WINDOWS 9x INSTALLATION ISSUE

- Error SU0350 - Setup was unable to display the Nondisclosure Agreement. Setup will now close.
- This is a common error message seen when performing a soft installation of Windows 9x Operating Systems
- Boot to a Command Prompt with proper boot disk.
- At the command prompt, type the following line, and then press ENTER:
- Copy c:\windows\license.txt c:\windows\help
- When you are prompted to overwrite the file, press Y, and then press ENTER.
- Restart the computer and resume installation

6.4 - COMMON OPERATING SYSTEM ERRORS AND FIXES

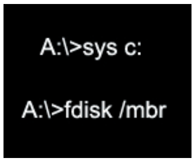
No Operating System Found/Invalid System Disk/Unmountable_Boot_Volume

Verify there is no floppy or CD is in the drive

Run DFT (if not run already) and if DFT passes:
* Do NOT run the following if Dynamic Drive Overlay (DDO) is being used [e.g. GoBack, MaxBLAST]

Windows 9X / ME

- Boot off of a boot disk, at the prompt:



```
A:\>sys c:

A:\>fdisk /mbr
```

If this does not resolve the problem proceed to a "Soft Install" of Windows.

Windows XP

- Boot off the client's ORIGINAL Windows XP CD
- Run the recovery console, command prompt run the commands:
  * If the admin password is not available or working, boot off a Win2k CD

  - C:\>chkdsk /r
  - C:\>fixboot

6.5 - WINDOWS REGISTRY

The Windows Registry is a central hierarchical database used to store information necessary to configure the system for one or more users, applications and hardware devices.

WARNING NOTE: It is possible to permanently corrupt Windows by changing the Registry. Any changes you make should be done with caution. By backing up before modification, you virtually eliminate the possibility of disaster. Many registry problems can be remedied by soft installing the operating system or installing certain updates (i.e. Windows Service Packs and/or Internet Explorer Updates).

The Registry is edited with a tool found in your Windows folder. That tool is the Registry Editor. It’s called Regedit.exe and is included with Windows for the purpose of viewing and editing the Registry.

EXPORTING REGISTRY KEYS (BACKUP)
Find and highlight the key you want to modify or delete.

On the File menu, click Export.

In the Save in box, select a location where you want to save the Registration Entries (.reg), in the File name box, type a file name, and then click Save.

You may now modify or delete the exported key. If you find this was not helpful or a part of Windows has become unstable, simply Double Click the exported Registration Entry (.reg) and select “Yes” when prompted, to restore the key to its original state.

ENUMERATOR KEY
The Enumerator key contains subkeys for the specific hardware components your computer uses. Removing individual keys will completely remove the device from the operating system.

Windows 9X / ME
- Location = HKEY_LOCAL_MACHINE\Enum

Windows 2000 / XP
- Location = HKEY_LOCAL_MACHINE\System\ControlSet001\Enum

Choose next level down = type of device

Right click on the device you would like to modify and click permissions

Select Allow Full Control

Export (Backup) the Key and Modify as needed

RUN KEYS
Programs in the Run keys start automatically each time that a user logs onto the OS

Locations:
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Programs that should not be starting up with Windows can be deleted.

EXEFile KEY

Location:
- HKEY_CLASSES_ROOT\exefile\shell\open\command

A virus may corrupt this key resulting in EXE files being opened by the virus.

The value in this string should only be- “%1” %* -clear out additional words, characters, or files.

6.6 - OPERATING SYSTEM SERVICE CHECKLIST

NOTE: Assume that Pre-Op has been preformed

- Attempt boot to normal Windows
- Replicate client's issue
- If cannot boot to normal Windows, boot to Safe Mode
- Check Device Manger for redundant, conflicted or unknown/uninstalled devices. (Windows 9x/ME only)
- Remove all redundant devices (ALL entries must be removed for the device) (Windows 9x/ME only)
- Remove all conflicted devices and unknown/uninstalled devices
- Check startup configuration with MSCONFIG
- Uncheck autoexec.bat and config.sys in Windows 9x Operating Systems
- Remove startup programs that are unnecessary for the function of the OS or peripherals. (Always leave Antivirus and Software Firewalls enabled)
- Reboot system and enter Normal mode
- Reinstall any drivers for removed devices
- Delete all Temp files and Temporary Internet Files
- See System Tune-Up portion of the System Tune-Up and Optimization for exact details
- Run Windows Update
- Install OS service packs and Internet Explorer updates
- Install all Critical Updates and selected other Updates
- Install DirectX updates

Proceed to Post-Op procedures

6.6.1 - SYSTEM TUNE-UP AND OPTIMIZATION

* This is a procedure that should be applied to ALL machines
(minus machines that have hardware or other issues that prevent basic OS functionality)

*This procedure will be applied in conjunction with other services
– it may end up being applied at different stages within said services

Tune-up

- Clean ALL of the temporary files on ALL accounts
  - o Make sure that you reboot the machine once into Normal Mode (in case temp files remain that need to be executed)
  - o Common temp file locations:
    C:\Documents and Settings\%user%\Local Settings\Temp
    C:\Documents and Settings\%user%\Local Settings\Temporary Internet Files
    C:\Documents and Settings\%user%\Local Settings\History
    C:\Documents and Settings\%user%\Cookies
    C:\Windows\Temp
    C:\Windows\Temporary Internet Files
    C:\Windows\Cookies
    Any c:\temp dir

Even though Cookies/TIF/History were cleaned, use IE's "Delete Cookies", "Delete Files", and "Clear History" options too.

Remember that some .dat's (specifically index.dat) located within these folders may not be able to be deleted using conventional deletion methods

6.7 - VIRUS REMOVAL

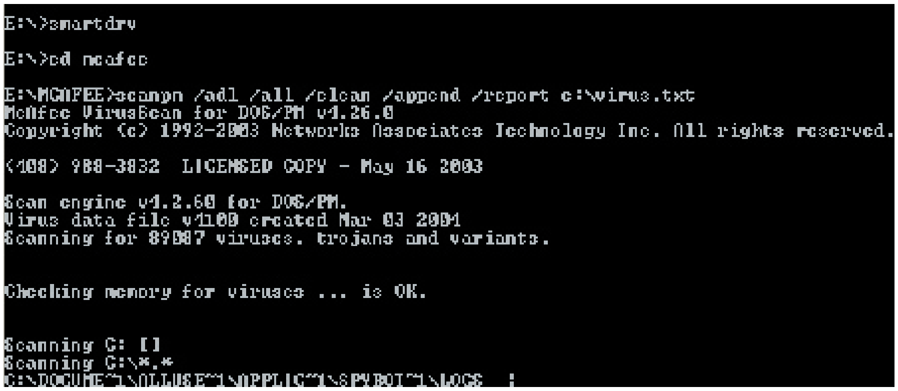
NOTE: For scanning instructions please reference section 4.3.

Add the </clean> and </append> switches to the command line. This will clean the viruses and append your virus.txt log file

Example of new command:

- scanpm /adl /all /clean /append /report c:\virus.txt

NOTE: If the virus has an official clean tool (Symantec Fix Utility) DO NOT attempt to clean using this command line method, use the Fix Utility. You may then run a command line virus scan to be sure the virus was eradicated.



```
E:\>smartdrv

E:\>cd mcafee

E:\MCAFEE>scanpm /adl /all /clean /append /report c:\virus.txt
McAfee VirusScan for DOS/PM v4.26.0
Copyright (c) 1992-2003 Networks Associates Technology Inc. All rights reserved.

(408) 988-3832  LICENSED COPY - May 16 2003

Scan engine v4.2.60 for DOS/PM.
Virus data file v4100 created Mar 03 2004
Scanning for 89087 viruses, trojans and variants.


Checking memory for viruses ... is OK.


Scanning C: []
Scanning C:\*.*
C:\DOCUME~1\ALLUSE~1\APPLIC~1\SPYBOT~1\LOGS  |
```

VIRUS ERADICATION ALTERNATIVES

Use fix/removal tools located on MRI \.\Virus Removal Tools

- If tool is not available/out-dated for specific virus you may download Symantec removal tools at http://www.symantec.com

Secondary Drive:

- A hard drive may also be mounted as a secondary drive in a system that has an active virus scanning software. Then run a manual scan of the secondary drive to remove viruses. Do note that using this method, a virus software may quarantine required operating system files. This would require a repair or Soft Install of the operating system before the computer will function properly. Do not perform this operation when removing the KLEZ virus, use the Symantec Fix Utility. Please also note that this method takes more manual Agent time as opposed to typing commands and letting the software take care of the rest.

Scanning and eradicating with NTFS

- Safe Mode with networking required for online scan/eradication

Online

- House Call at http://housecall.trendmicro.com/

Local

- BartPE (where available)

VIRUS RESEARCH

See McAfee's Virus Information List website for advanced manual virus removal instructions.

http://vil.mcafee.com

Other excellent virus information websites:

http://www.symantec.com

http://www.viruslist.com

NOTE: In Windows ME and Windows XP remember to disable the Restore function to prevent the Restore directory from re-infecting the system. Remember to enable afterwards.

If a client does not want viruses removed from their system you MUST make a notation of this denial of service in the service order notes.

Also, if the client does not want us to install new virus software, note that we do not cover virus re-infection if the computer leaves the store without proper virus protection. Notate this in the service order as well.

6.8 - ADWARE/SPYWARE REMOVAL

This procedure is to be used as a guide for removing adware/spyware. There are many, many ways of removing adware/spyware, but this is a proven way of eradicating a large percentage of most adware/spyware applications.

If the client requests that ANY adware/spyware application, file, etc be left on the machine our service cannot and will not carry a warranty

Boot the machine once into Normal Mode [in case temp files remain that need to be executed]
Client may provide vital information that tells you flat-out that there's spyware. Some of these could be but are not limited to:

- Internet slow
- Tons of pop-ups
- Homepage hijackings

Some keys signs to look for:

- KaZaA
- Toolbars within Internet Explorer
- Machine is extremely slow to boot

Common running processes

- Hbinst.exe
- Save.exe
- Msbb.exe
- AST.exe
- CMESys.exe

Certain applications (e.g. KaZaA, WeatherBug, Wild Tangent) will probably not work after you clean the machine.

- You MUST inform the client of this before proceeding

Boot into Safe Mode [with networking if applicable]

- Most spyware removal applications can be installed and updated within Safe Mode. If not (or no CD-ROM support), install/update via Normal Mode, then return to Safe Mode for cleaning.
- Delete ALL temp files on ALL accounts (see Tune-up portion of System Tune-up and Optimization for exact details). DO NOT remove adware/spyware applications via Add/ Remove Programs right now
- In Windows XP/ME – Disable the System Restore function

SPYBOT SEARCH & DESTROY

- Install SpyBot-S&D with all of the default settings selected.
- Apply all updates manually from MRI. Don't forget to change the path of installation for the updates (Usually <C:\Program Files\SpyBot - Search & Destroy\>).
- Launch "SpyBot-S&D (advanced mode)". If Internet is available, apply web updates via SpyBot S&D. Manual updates are also available at http://www.safer-networking.org You may have to change the mirror site as DDoS attacks are frequent.
- SpyBot S&D will automatically restart.
- If you're not in the main scan page, get there, and then "Check for problems". Record how many instances of spyware were found for your notes.
- The scan will take a few minutes or could even "freeze" for some time (e.g. c2.lop). This is normal so just let it finish
- While SpyBot is running, perform a system optimization (see Optimization portion of System Tune-up and Optimization for exact details).
- When SpyBot-S&D finishes, "Select all items" and "Fix selected problems". If "Select all items" is not available, go to Settings -> Settings -> then enable "Show expert buttons in results list" (option is at the bottom); then return to SpyBot-S&D tab and continue cleaning. Depending on infestation level, "Network fixes" may need to be applied; it will

automatically notify you of this, simply click "OK". During the fixing of problems the application may appear to freeze. This is normal so just let it finish

- Usually SpyBot will be able to fix most problems on the first attempt
  If it asks to be run at next startup, cancel this. If New.net was installed a second scan is necessary. Reboot into Safe Mode and scan again. Other problems can actually be removed on a second scan without a reboot.
- Continue cleaning with SpyBot-S&D until the machine is "clean" per its findings
  Some problems can NOT be removed by SpyBot-S&D (e.g. variants of i-lookup, VX2. BetterInternet, etc).These will have to be "skipped" at this point and cleaned with other tools

AD-AWARE

- Install Ad-Aware with all of the default settings selected
- Apply all updates manually from MRI. Extract the .zip – usually <C:\Program Files\Lavasoft\Ad-aware 6>. You can actually start the installation and scanning with this application during the latter stages of SpyBot-S&D to save time. However, be careful not to "cross-clean" infections found by both applications otherwise you'll be chasing a non-existing infection
- Launch Ad-Aware. If Internet is available, apply web updates via Ad-Aware. Manual updates are also available at http://www.lavasoftusa.com/support/download/.
- After updates are applied, Click "Start". Be sure to select "Customize" and enable the following:
  - "Scan within archives"
  - "Scan my IE Favorites for banned URLs"
  - "Scan my Hosts files" – then click "Proceed"
- Record how many instances of spyware were found for your notes. The scan will take a few minutes or could even "freeze" for some time at various locations. This is normal so just let it finish.
- When Ad-Aware finishes, "Select all objects" (right-click in results to get this option), click "Next", then "OK". During the quarantine process the application may appear to freeze. This is normal so just let it finish. Usually it will be able to fix most problems on the first attempt.
- If it asks to be run at next startup, cancel this. Other problems can actually be removed on a second scan without a reboot. Continue cleaning with Ad-Aware until the machine is "clean" per its findings. Some problems can NOT be removed by Ad-Aware (e.g. variants of i-lookup, VX2.BetterInternet, etc). These will have to be "skipped" at this point and cleaned with other tools

Depending on the level of infestation, other spyware removal applications may need to be used

- SpySweeper is a great tool. Not only for cleaning, but as a prevention tool – so attach it!

Once both above programs show the machine being "clean" move onto a deeper cleaning. This "Clean" may mean that 99% of the infestation was cleaned. Miscellaneous entries like VX2. BetterInternet, CoolWWWSearch, look2me, i-lookup may still exist and possibly cannot be cleaned by either program.

ADDITIONAL REMOVAL TOOLS

There are a few additional adware/spyware removal tools that will come in handy. They can be located on the MRI CD in the folder: \.\Spyware\Misc Removal Tools. Before you use any of these tools, please read the documentation for each application.

CWShredder

Utility specifically designed to remove CoolWWWSearch. (SpyBot/Ad-Aware sometimes can't removed all of the parts of this hijack – this does)

- If the error "'A required dll, MSVBVM60.DLL, was not found" appears, apply "Visual Basic 6.0 SP5 Run Time Files". Located on the MRI \.\Windows Tools.
- If CWS was on the machine and it infected any of the following, the specific .exe's will have to be replaced:
  wmplayer.exe, msconfig.exe, control.exe, rundll32, notepad.exe
  Replacement .exe's located on the MRI \.\Spyware\CWShredder\Additional CWS fixes
- If you tweak msconfig and have not rebooted the machine, CWShredder will say that it found the CWS.Msconfig
  This does not matter; System Configuration Utility will not prompt on next reboot

Hijackthis
Utility that assists in detecting and removing various hijacking entries
WARNING – Read ALL documentation about this application before using it
If run from a CD, backups of files you delete will NOT be made; copy the application to the desktop if needed.

KaZaABegone
Utility designed to fully removed KaZaA and all of its remnants
- Good to run this even if KaZaA was never installed as it finds other spyware applications associated with KaZaA

  WARNING – This utility will delete the "My Shared Folder" folder that contains the client's data that was downloaded via KaZaA. You MUST inform the client that this will be deleted BEFORE you run this utility
- If client wishes for KaZaA or content downloaded via KaZaA to remain on the machine, our service cannot and will not carry a warranty. Document this in your notes.

FixMsg117
Utility design to cure msg117.dll (ZestyFind) issues
- Good to use this "just in case" ZestyFind is on the machine
  Hard to tell if this hijacker is actually on the machine until it redirects you
- Depending on the level of infestation, other fixes may need to be applied
  It will notify you of this; usually winsock2 related

KillMsg118
Utility design to cure msg118.dll issues
- If the machine is "locking"/pausing for a long time a on the "Loading your personal settings…" display, run the following registry entry to show the file that is possibly causing this
- Located on MRI \.\Windows Tools\Registry Entries
  Enable - Show Verbose Security Status Messages.reg
  Disable - Undo Show Verbose Security Status Messages.reg

BHODemon
Breaks down Browser Helper Objects (BHO) for further troubleshooting

CoolWWWSearch.SmartKiller (v1.v2) MiniRemoval
Utility specifically designed to remove variants of CoolWWWSearch. You will know that the machine has this variant as most major adware/spyware removal tools will start, and then shutdown. Most major adware/spyware web sites will be inaccessible. If the machine has any of the below variants, this removal must be run FIRST to allow SpyBot and Ad-Aware to run.
- Variant 26: CWS.Smartsearch - Counter-counter-actions
- CWS.Smartsearch.2, CWS.Smartsearch.3, and CWS.Smartsearch.4

If you have multiple user accounts on the machine you must clean all accounts using the instructions above.

Manual Cleaning
After you "clean" the machine using all of the applicable applications, there will still be miscellaneous files/folders/icons that exist on the machine that are related to adware/spyware

- After the main [SpyBot, Ad-Aware] and miscellaneous [CWShredder, Hijackthis, KaZaABegone, etc] applications are run, the machine is probably technically "clean"

o Do you want your clients to see the mess left behind – no!
o This could freak them out and cause a "recall" on you – fix it the first time!

- Clean the Favorites folders

o C:\Documents and Settings\%user%\Favorites
o C:\Windows\Favorites

Do NOT delete all favorites – look for unusual entries

- Adult Links
- Gambling
- Casino

When these are created there are usually a few main folders and they all have the same modified date

Sometimes the Favorites are so infected you have to remove all of them; more effective than going through hundreds of shortcuts. Talk to your client if this happens.

Remove all spyware/adware entries from the Add/Remove Programs List. If it can't be removed, manually remove it

- Open Registry Editor to the following key: [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall]

This key is where the Add/Remove Program list is store. Some of the entries are plainly label and others are going to be in hexadecimal. For the hexadecimal entries you'll have to look in the right pane for the name corresponding to the entry in the Add/Remove Programs list that you want to remove. After the Add/Remove Programs List is clean, reboot into Normal Mode

Clean the [C:\Program Files] folder by removing the miscellaneous spyware/adware files/folders. Be sure to only delete files/folders that you know are related to adware/spyware.

If you recognize any installer that is used to install adware/spyware [most are in the root directory], delete them.

- Only delete executables that you know are adware/spyware

Clean [C:\WINDOWS\Downloaded Program Files] – may have already been done with Hijackthis

- Don't forget to remind the client that they'll will have to download Flash [or other similar] plug-ins if you deleted them

Delete the miscellaneous spyware/adware icons/shortcuts on the desktop and start menus

After ALL of this you have finally cleaned the machine so now it's time for testing.

(Re)Boot into Normal Mode and test Internet Explorer by visiting commonly used sites. It is also helpful to visit sites that use: Flash, SSL, ActiveX, or other similar technologies are good for testing. This will help prevent callbacks and recalls.

- http://www.google.com
- http://www.comcast.com
- http://mail.geeksquad.com/sts
- http://windowsupdate.microsoft.com

If you can't get to web sites, but you get an IP address, DNS, and can ping, winsock2 probably needs to be repaired. For instructions on how to do this please see the winsock2/DUN procedures.

Test random programs that may have been infected [WMP, msconfig, control.exe, etc] and preform this testing on ALL user accounts.

Reboot the machine a few times, test again. Testing should only take a few minutes and will help prevent recalls – so do it!!

If at any time during your testing spyware/adware appears (e.g. IE's redirecting you, random not normal pop-ups, etc), you may have to start the removal process all over again

Uninstall ALL spyware/adware applications used to performed the cleaning

Delete the Lavasoft folder in the Start Menu and [C:\program files]

Sometimes SpyBot will be here too; remove it if found

Clean the [%temp%] directory one more time; Hijackthis/other junk may be here

In Windows XP/ME – reenable System Restore

Reboot the machine a few more times just for good measure

Be sure that you document throughout your removal procedures – it's easy to jot down a few notes while you're doing the scans/cleaning instead of compiling it all at the end and missing vital points.

Documentation is not only for the client, but it's for the entire Geek Squad – so do it well!

EDUCATE, EDUCATE, and RE-EDUCATE the client – you'd be amazed how much this helps!!

6.9 - WINSOCK2 / DIAL-UP NETWORKING (DUN)

*If you are experiencing difficulty connecting to the internet or can connect to the internet but cannot access web pages, Winsock is damaged and must be reset to a working state. If these steps are followed in the correct order, many issues that are caused by Winsock being broken will be fixed.

*These issues may include a slow internet connection, the ability to connect to the internet but not browse web sites, the ability to ping a web site by IP address but not by name.

Windows 98/SE/ME

Remove TCP/IP in the network stack
- Start -> Settings -> Control Panel -> Networking
- Remove all TCP/IP settings in the box -> click "OK"
- DO NOT Reboot

Remove Dial-Up Networking
- Start -> Settings -> Control Panel -> Add/Remove Programs -> Windows Setup
- Click on Communications
- Uncheck Dial-Up Networking -> click "OK"
- DO NOT Reboot

Remove the Winsock2 registry key
- Start -> Run -> type regedit -> click "OK"
- Search for Winsock2 and delete all instances (should be two folders)
- Exit Windows Registry
- Reboot

Reinstall Dial-Up Networking
- Start -> Settings -> Control Panel -> Add/Remove Programs -> Windows Setup
- Click on Communications
- Check Dial-Up Networking -> click "OK"
- Reboot

WINDOWS 2000

Remove the Winsock2 registry key
- Start -> Run -> type regedit – click "OK"
- Follow the path HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
- Delete: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\winsock2

Uninstall TCP/IP
- Start -> Settings -> Network and Dial-Up connections
- Right-click Local Area Connection -> Properties
- Uncheck TCP/IP -> Click Uninstall
- Reboot

Re-install TCP/IP
- Start -> Settings -> Network and Dial-Up connections
- Right-click Local Area Connection -> Properties
- Click Install -> highlight Protocol -> click "Add"
- Install TCP/IP
- Reboot

Windows XP

Remove the Winsock and Winsock2 registry keys

- Start -> Run -> type regedit -> click "OK"
- Follow the path HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
- Delete:
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Winsock
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WinSock2

Make sure all files are shown

- Start, My Computer -> Tools -> Folder Options... -> View
- Enable <Show hidden files and folders>

Re-install TCP/IP

- Start -> Control Panel -> Network Connections
- Right-click the connect you wish to repair -> Properties
- Click "Install..." -> highlight Protocol -> click "Add..."
- Click "Have Disk..." -> click "Browse..." -> point to the <c:\windows\inf folder>
  * "Windows" folder may be named "Winnt"
- Click "Open" -> click "OK"
- Highlight "Internet Protocol (TCP/IP)" -> click "OK"

* Installation will pause for a few seconds -> when finished, close all open Windows

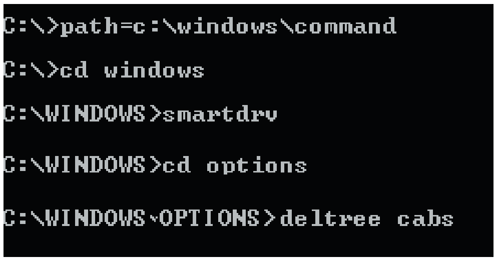
Note: In XP, it is not usually necessary to reboot after re-installing TCP/IP. Try to open Internet Explorer and see if you can browse. If you still cannot browse after completing the above steps, reboot. After rebooting you should be able to browse web sites.

6.10.1 - SOFT INSTALL OF WINDOWS 98/SE/ME

Any Internet Explorer upgrades should be uninstalled using add/remove programs before a soft install of Windows 98/ME is performed.

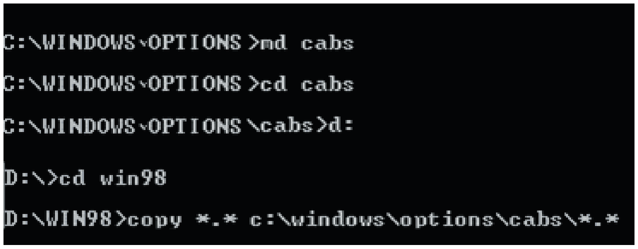
Boot from Windows boot disk to a DOS prompt.
* Try performing a Soft Install using their CABS first

A. Delete current CAB files and go to the C: drive.



```
C:\>path=c:\windows\command
C:\>cd windows
C:\WINDOWS>smartdrv
C:\WINDOWS>cd options
C:\WINDOWS\OPTIONS>deltree cabs
```

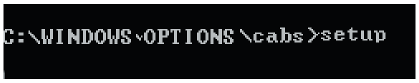
B. Create a new CABS directory, and copy cab files from the client's operating system CD to the new "cabs" directory.



```
C:\WINDOWS\OPTIONS>md cabs
C:\WINDOWS\OPTIONS>cd cabs
C:\WINDOWS\OPTIONS\cabs>d:

D:\>cd win98
D:\WIN98>copy *.* c:\windows\options\cabs\*.*
```

C. The process for ME is exactly the same except on the CD the folder that contains the cab files is D:\win9x instead of D:\win98

D. After the copy is complete switch back to the C: drive and run Windows 98/ME installation by typing "setup".



```
C:\WINDOWS\OPTIONS\cabs>setup
```

E. Run a Windows install as you normally would. Make sure when it is completed that all programs and devices are working properly and that the post-op procedure is performed.

6.10.2 - CLEAN/PARALLEL INSTALL OF WINDOWS 98/SE/ME

Client MUST BE NOTIFIED before a Clean/Parallel Install is done to any Operating System.

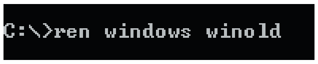
No data will be lost. However, the CLIENT must reinstall ALL of their programs for their data to work, or have us install their software at an additional fee.

A system restore must be done from the Restore CDs if the computer is an OEM computer that did not come with program disks. All data would be lost in this case. (see format install of Windows 98/ME)

A Clean/Parallel Install of Windows is very similar to a Soft Install of Windows. The main difference is that you rename the entire Windows directory and then create the new folders for the cabs. You run the setup exactly the same way as you do in a soft install.

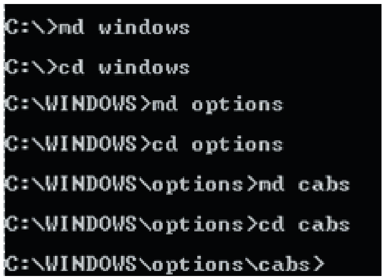
Boot from Windows boot disk to DOS prompt.

A. Rename current Windows directory to winold



```
C:\>ren windows winold
```

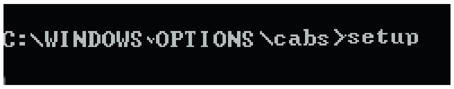
B. Create new Windows directory and copy cabs from Windows 98/ME disk



```
C:\>md windows
C:\>cd windows
C:\WINDOWS>md options
C:\WINDOWS>cd options
C:\WINDOWS\options>md cabs
C:\WINDOWS\options>cd cabs
C:\WINDOWS\options\cabs>
```

C. The process for ME is exactly the same except on the CD the folder that contains the cab files is D:\win9x instead of D:\win98

D. After the copy is complete switch back to the C: drive and run Windows 98/ME installation by typing “setup”.



```
C:\WINDOWS\OPTIONS\cabs>setup
```

You may need to reinstall some drivers after a Clean/Parallel Install of Windows. Download the proper drivers from the internet.

- Computer Manufacturer’s website
- Device Manufacturer’s website
- www.driverguide.com (Username: drivers Password: all)
- www.google.com/groups.google.com

Look for model numbers on device Printed Circuit Board (PCB) and major Integrated Circuits (IC) for search criteria.

After a Clean/Parallel Install, verify that the initial problem has been resolved and can’t be recreated.

If the problem can’t be recreated, proceed and complete post-op procedures.

If the problem still occurs, try updates (Windows, Internet Explorer), then proceed to a Format Install of Windows (contact the client before proceeding).

6.10.3 - FORMAT INSTALL OF WINDOWS 98/SE/ME

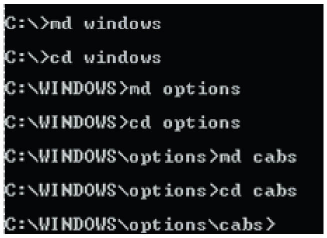
A Format Install of Windows 98/ME DELETES ALL DATA ON THE HARD DRIVE. The client must know that ALL DATA WILL BE DELETED FROM THE DRIVE. All programs will have to be reinstalled by the client, or we can install them for an additional fee. A Format Install of Windows 98/ME should only be used as a last resort after all other options have been tried.

Boot from Windows boot disk to DOS prompt.

A. Format C: drive

```
a:\>format c:
```

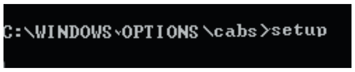
B. After format completes create new Windows directory and copy cabs from Windows 98/ME disk



```
C:\>md windows
C:\>cd windows
C:\WINDOWS>md options
C:\WINDOWS>cd options
C:\WINDOWS\options>md cabs
C:\WINDOWS\options>cd cabs
C:\WINDOWS\options\cabs>
```

C. The process for ME is exactly the same except on the CD the folder that contains the cab files is D:\win9x instead of D:\win98

D. After the copy is complete switch back to the C: drive and run Windows 98/ME installation by typing “setup”.



```
C:\WINDOWS\OPTIONS\cabs>setup
```

You will need to reinstall some drivers after a Format Install of Windows. Download the proper drivers from the internet, or use driver disks that came with the computer.

- Computer Manufacturer’s website
- Device Manufacturer’s website
- www.driverguide.com (Username: drivers Password: all)
- www.google.com/groups.google.com

Look for model numbers on device Printed Circuit Board (PCB) and major Integrated Circuits (IC) for search criteria.

Make sure Windows, programs, and devices are working properly. Proceed with post-op procedure.

6.10.4 - WINDOWS 2000 & XP REPAIR METHODS

- Soft Installs (Repair Installation)
- Clean/Parallel Installs
- Format and Installs

There are three ways you can attempt to resolve more severe technical issues that require at least a partial reinstallation of the operating system. The best practice is to do the least intrusive fix possible (don't amputate an arm to fix a broken fingernail). The Geek Squad always tries to leave a computer "the way it used to be", because clients are used to the way they do things. They like to have the solitaire icon in the upper right corner, and the adorable puppy wallpaper. Typically, when you need to reinstall the OS, you will find that clients have their restore CD buried in a closet somewhere. If you're lucky, they have an actual XP or 2000 CD. More recently, some manufacturers have stopped giving out CDs and are either putting the OS and restore information on a hidden hard drive partition, or putting images on the hard drive that can be burned to CDs. There is a potential for data corruption when performing any sort of install, especially when there is file system or partition corruption. It is very important to back up data before attempting any re-installation, as catastrophe can strike at any time. Don't get caught in the headlights of an empty directory tree, inform the client of potential risks, and suggest backing up any important data files "just in case". Below are the best ways to perform each type of installation.

OEM SOFTWARE DISC

SOFT INSTALL

A soft installation is the least intrusive way to repair an OS with corrupt files and/or missing or damaged portions of the OS. Once you're done with a soft install, very little has changed cosmetically, leaving the client happy as a clam. Even though the soft install leaves things visibly untouched, there is always a chance for massive data corruption, usually when a corrupt file system is involved - so inform client of any potential risks before starting work.

OEM XP and Win2k cds give you two options for installation – a repair install (soft install), or a clean install. To attempt a Soft install (or repair installation):

1.) Select the first menu option: "To setup Windows XP now, Press Enter".

2.) Setup will search for previous installations on the drive.

3.) If an installation is found, it will give you the option to either repair the installation that was found, or to install a fresh copy of the Operating System.

4.) Select the repair option "To repair the selected Windows XP installation, press R". Setup will then go through a series of checks and will begin repairing any corrupt or missing system files, and will continue through setup as if it was a standard installation.

CLEAN/PARALLEL INSTALL

Sometimes a soft install does not resolve the issue you are trying to repair. A clean/parallel install is necessary when there is extreme OS corruption, corrupt registry, etc. A clean or parallel install is installing a fresh copy of windows on the system in a different directory than the current copy of windows. The advantage to doing this rather than formatting is that although you are "starting from scratch" with windows, the client's data is not lost. Be sure to inform the client that ALL applications and peripherals will need to be reinstalled (that means Word, Quicken, Scrabble, etc…) after the windows reinstallation has finished. The client's data SHOULD not be lost, however be sure to warn them of the risk of data loss, and strongly suggest backing up all important data before proceeding with the installation.

Although data should not be lost, information like e-mail and quicken data may need to be imported after the respective programs are reinstalled.

1.) If possible, rename the client's Windows, Program Files, and Documents and Settings directory before proceeding with the installation. This will reduce the risk of data loss during the reinstall.

2.) Boot to the OEM Win2k or Windows XP CD and select "To setup Windows XP now, Press Enter".

3.) Select the option to install a fresh copy of Windows.

4.) Setup will prompt you for the new installation location.

5.) If you were not able to rename the current windows directory before starting the clean install, change the installation directory from "Windows" to "Windows2" or "WinXP". This will be your new windows directory

6.) Proceed through install as normal.

FORMAT AND INSTALLATION

A format and install is the most intrusive fix possible, and should only be used in extreme cases of partition or file system corruption. This method causes all data on the client's hard drive to be erased and a clean and fresh copy of windows to be installed. This is a *LAST RESORT*.

When performing a format and install, there are 3 things you must do before proceeding with the work.

1.) Inform the client that all of their data is going to be lost, and why it is necessary to take such harsh action to resolve their problem (partition table is corrupt, etc...)

2.) Inform the client that they will not have any of their data after you format the system

3.) Inform the client that their data will be gone when you are done. This means e-mails, bookmarks, photos, documents, quicken data. Gone, never going to see it again. Reiterate this point over and over until you are sure the client understands.

To perform a format and install:

1.) Boot to the OEM CD. Select the option "To setup Windows XP now, Press Enter".

2.) Setup will find the previous installation and will ask if you want to repair it or "continue installing a fresh copy of Windows XP without repairing"

3.) Press ESC.

4.) Delete the current partition and follow setup's instructions to create and format a new one. BEFORE you do delete the partition, it is crucial that you explain to the client that ALL of their data is going to be erased. Tell them this at least 3 times before formatting the drive. Explain to them what data is - most people don't know that their data is "all of their MP3 files", or "all of their pictures from the lake cabin". Only after the client understands and agrees to losing all of their data, continue deleting the partition and recreating a new one.

5.) Setup will walk you through the rest of the install. After the installation is complete, it is your responsibility to install all needed drivers and to make sure everything is working as it should be. You should make sure they can get online and check their e-mail. This does not mean you have to reinstall all the applications that were installed before. Reinstalling applications and importing data is an additional service and should be billed accordingly.

NOTE: It would be wise to note any errors you run across during installation and research the cause and possible effect of said errors. It is also important to make sure that the OS is totally patched and the newest service packs are installed.

SOFT INSTALL WITH RECOVER CD

Some recovery CDs give you the option for a destructive repair or a non-destructive repair. If you encounter a machine that was shipped with W2K or XP and it came with recovery CDs, it is wise to investigate what options are available for that specific recovery disc. After you have examined your options, inform the client of your recommendation. If a non-destructive repair option exists, read through any warnings that the recovery CD’s displays and make sure to relay that information to the client in words they can understand.

Once you have educated the client and they understand what is going to happen to their system (and why it is necessary), run the non-destructive repair. The steps to perform this operation will vary from machine to machine and you should read everything VERY carefully before proceeding.

If the only option that the recovery CD has to offer is a destructive install, a soft install is not possible. At this point, you should stop, look at all available options, and present the least intrusive option to resolve the problem to the client. It is up to them to decide how they want to proceed from there.

FORMAT AND INSTALL WITH RECOVER CD

This is the standard recovery option for most PCs. Restore CDs are very straightforward and generally format and re-image the client’s hard drive, returning it to the state the system was in when it came off the shelf. It is crucial to stress the importance of informing the client about what formatting really means and making sure that the client understands the result before doing any work that could possibly result in data loss. Again, this should be a LAST RESORT.

NOTE: Not only is it very important to explain risks and reasons for your suggestions to clients in all situations, it is also extremely important to document EVERYTHING in the notes!

6.11 - COMMON FILE EXTENSIONS FOR DATA BACK-UP

The following is a list of programs that are commonly backed up and the relevant files and typical locations.

This is not all inclusive so it is important to consult the client as to any specific needs they may have.

'My Documents' directory

- Usually best to back up everything in this directory
- Some common extensions found here:
  *.doc - MS Word documents
  *.xls – MS Excel spreadsheet
  *.jpg – image files

'Favorites' directory

- Win 2K/XP – C:\ Documents and Settings\%user%\Favorites
- Win 9x/ME – C:\Windows\Favorites

Microsoft Outlook

- *.pst – Outlook data file
  Win 2k/XP: C:\Documents and Settings\%user%\Local Settings\Application Data\Microsoft\Outlook
  Win 9x/ME: C:\Windows\Profiles\%user%\Local Settings\Application Data\Microsoft\Outlook

Microsoft Outlook Express

- *.dbx - Outlook Express data file (most commonly)
  Win 2k/XP: C:\Documents and Settings\%user%\Local Settings\Application Data\Identities\{%}\Microsoft\Outlook Express
  Win 9x/ME: C:\Windows\Application Data\Identities\{%}\Microsoft\Outlook Express
- *.wab – Windows Address Book
  Win 2K/XP – C:\Documents and Settings\%user%\Application Data\Microsoft\Address Book
  Win 9x/ME - C:\Windows\Application Data\Microsoft\Address Book
- *.csv – Comma Separated Values
  A more reliable way to export/back-up address book entries
  To Export: File>Export>Address Book>Text File>Export
  To Import: File>Import>Other Address Book>Text File>Import

Quicken

- *.qdf - Quicken data file
  Stores all transactional data for the account
  Typical location - C:\Program Files\QuickenW\Backup
  If the data has not been backed up recently, the entire QuickenW directory should be copied

QuickBooks

- *.qbb - QuickBooks company file
  Stores all company-specific information
  Typical location – C:\Program Files\Intuit\QuickBooks

Microsoft Money

- *.mny
  Stores all transactional data for the account
  Typical location – C:\Program Files\Microsoft Money

6.12 - GENERIC/QUICK FIXES

These are some speedy fixes that are often used.

Microsoft Word will not open
- Enable “Show hidden files and folders”
- Normal.dot is probably corrupt and needs to be placed.
- Simply search for normal.dot and delete; Word will recreate this file next time it’s opened
- C:\Documents and Settings\%user%\Application Data\Microsoft\Templates
- C:\Program Files\Microsoft Office\Templates
- You must inform the client that their customizations will be lost

Paging file is set to 0 MB and won’t stay set when you manually try to set it
- Apply the Intel Application Accelerator v2.3; if applicable
- Located on the MRI \.\Intel

Can’t access any web sites, but you get an IP, DNS, and can ping
- Winsock2 may need to be repaired; see winsock2/DUN fixes
- You can perform this manually or there are a few tools on the MRI
- \.\Spyware\Winsock2 Utilities

Windows 2000/XP Only
User accounts are taking a long time to load/pausing at the “Loading Your Personal Settings...“ message – use this .reg to show you what file is possibly causing this
- Apply Show Verbose Security Status Messages.reg
- Located on the MRI \.\Windows Tools\Registry Entries
- Don’t forget to apply the undo to return the machine back to displaying the default message

Outlook Express 6 not allowing attachments
- If Service Pack 1 was installed, “Do not allow attachments to be saved or opened that could potentially be a virus” was automatically enabled; simply uncheck this option

You can’t access the following sites:
- Secured Sockets Layer (SSL)
- ActiveX is working partially/not at all
- Windows Update is not working properly (web site displays an ActiveX error)
- AOL versions greater than 7.0 (specifically 9.0 Optimized) won’t access most sites, specifically SSL
- Apply the Cryptographic service and ActiveX fixes v3.bat
- Located on the MRI \.\Windows Tools\Batch Files

If network shares are taking a long time to display, try this tweak
- When applied this tells the computer not to look at the shares folder, therefore speeding up your sharing
- Apply Speed up file.print sharing tweak.reg
- Located on the MRI \.\Windows Tools\Registry Entries

There is a folder on the MRI with a few helpful links to various web sites
- \.\Helpful Links

7.0 - Post-Operations (Post-Op)

After completing any type of computer service, post-op each system to verify that all of the following items are properly functioning. This is done to catch any issues that may still be occurring. By taking less than 5 minutes you may save a client the inconvenience of having to bring their computer back for what could have been an easy fix.

- Reboot the system a minimum of three times
- Watch for shutdown problems

- Test all Floppy and CD drives
- Test sound, modem/NIC, and video (i.e. higher than 16-bit 800x600)
- Check Device Manager in Normal Mode
- Check for multiple extraneous devices in Safe Mode Device Manager (Win9x only)
- Make sure Windows recognizes all the RAM in the system

- Load web pages (try to use client's account if possible)
- Open a sampling of applications on the desktop that the client likely uses (e.g. Microsoft Word, Microsoft Excel, QuickBooks, Quicken, etc.)
- Test their major applications whether you worked on them or not.

This has turned up many little issues in the past that may have become potential recalls. A satisfied client means a potential repeat client!

- Educate, educate, and re-educate the client on what was done with their system!

Check-Out

- Pull up client's service order through STAR
- Verify product is complete
- Get product, paperwork, and all parts
- Explain in detail what was wrong and what service was performed
- Make sure the client is fully aware of EVERYTHING you did to their machine
- Make recommendations as to how to prevent it from happening again
- Close service order in STAR
- Process payment through P.O.S.
- Parts and Labor
- Get client's signature on closed service order
- Lastly, thank the client for their business!

8.0 - COMPUTER CHECK-OUT

When the client returns to pick up their serviced product, perform the following:

1. Greet the client.
2. Use STAR to identify the unit; use the Service Order number or the client's phone number and last name to pull up their Service Order.
3. Show the client the Tactical Case Report form (on reverse side of In-Store Tactical Analysis form) and explain any applicable instructions regarding the product
4. Close the Service Order in STAR to print out copies of the Service Order.

a. Ring out the balance due in P.O.S. even of there is a $0 balance due. Collect payment as applicable. It is extremely important that all services and hardware pieces are processed through P.O.S. as to prevent shrink and to not miss out on any labor charges.

b. Have the client sign a copy of the Service Order; technician should sign it as well. Keep signed copy for the store file.

c. Give the unsigned copy of the Service Order and the unit to the client.

If repairs were completed and verified using the full diagnostic suite and the post-op was performed and noted then there is no reason to power on the computer and show the client that it is functioning appropriately. If client requests to have unit powered up at that time power up the machine and demonstrate proper operation.