The main purpose of Fedora 20 i686 Live AntiVirus Spin is of-course to clean your virus infected Windows computers /USB sticks / external drives, etc. Use this spin to boot your system in a clean state, remove the virus infected files, and get back to what you wanted to do with your Windows computer.

Download the ISO from the download section of www.wbitt.com .

How to use:
Of-course the first logical step would be to burn the ISO on a USB or a CDROM. Then, follow the step below to mitigate virus infection from the infected computer.

1. Boot the infected computer with this boot CD/USB and connect to Internet through some means. (Ethernet, Wireless/Wifi, Mobile BroadBand, etc)
2. Open a Text Terminal (Command Line Interface), and execute the command "**su -c freshclam** " . This will update the CLAMAV virus definitions. Leave the terminal open for later use.
3. Open File Manager and click/double-click/open the disk partition/device you want to run the antivirus scanner on. This will mount the volume under a specific mount point. Make a note of that as it will be used in a later step. You should be able to see the contents of this location in the file manager.
4. Start "ClamTK" AntiVirus Scanner GUI interface. It is shown on the desktop, and also appears in the "Accessories" menu.
5. Double-Click "Settings" in the "Configuration" section of the ClamTK GUI, and select/check mark "Scan Directories Recursively".
6. Select "Scan files larger than 20 MB" , and "Files beginning with a dot"
7. Double-Click "Scan a Directory" in the "Analysis" section of the ClamTK GUI.
8. Select the directory you want to run the scan on. You have already mounted/opened this directory in step 2.
9. Start the scan (of-course).
10. When the scan finishes, it may show you the number of threats and also show you the list of files with virus infection.
11. NOTE: **The ClamTK virus scanner will delete the files having virus infection**, as it is not able to "disinfect" any file.
12. You may want to take screen shots of the scan results and the actions you are performing.
13. When all infected files are "deleted", issue the "**sync**" command on the command / text terminal.
14. Now click the small "eject" button in the file manager, in front of the disk icon of the volume you were scanning.
15. Halt the system by using the "**halt**" command in the text terminal. NOTE: DO NOT SIMPLY SWITCH OFF THE COMPUTER. Do NOT pull out the AntiVirus USB / CD just yet.
16. When the system is halted, it is time to pull out the antivirus disk. You can now turn the system back on, and boot from the local hard disk.

Details about the AntiVirus Spin:

- The AntiVirus spin provides LXDE Desktop as the main desktop environment. LXDE is very lightweight and very fast/efficient.
- You can also select OpenBox Desktop instead of LXDE on the login screen, which is a minimalist window manager and uses even lesser resources than LXDE.
- The 32 bit version is able to work on both 32 and 64 bit machines/systems.
- This AntiVirus spin is also able to install itself on the hard drive, if you choose to do so. There is an icon on the desktop clearly labelled as "Install to Hard drive". Be very clear that this icon cannot be used to install the ClamAV/TK antivirus on the hard disk. In fact it will install the entire operating system ("Fedora 20 AntiVirus Spin" in this case) on the hard drive. It will erase your existing partitions and destroy your data if you don't know what you are doing. (Though it will give you options for partitioning, etc). On the other hand, this is an excellent spin to install on low powered (32 bit) computers, which need second life!!!

The following packages are added to pack more punch:-

clamtk - AntiVirus Scanner GUI
vim - Vim Editor
links - Text mode web browser
net-tools - Basic networking tools including: ifconfig, netstat, route, and others. Now obsolete.
iproute - Replacement for tools in the net-tools package.
bind-utils - Basic DNS tools (dig)
traceroute - Trace the route!
tcpdump - Packet Capture
ifstat - A little tool to report interface activity like vmstat/iostat.
iftop - iftop does for network usage what top(1) does for CPU usage.
hping3 - hping3 is a network tool able to send custom TCP/IP packets and to display target replies like ping do with ICMP replies.
NetPIPE - Protocol independent performance tool that visually represents the network performance under a variety of conditions.
nmap - Network / port scanning (and more!)
nc6 - NetCat (Swiss Army knife of network tools)
rkhunter - RootKit Hunter to search for rootkits on the infected disk/volume.
chkrootkit - Tool to locally check for signs of a rootkit.
unhide - A forensic tool to find processes and TCP/UDP ports hidden by rootkits, Linux kernel modules or by other techniques.
ddrescue - data recovery tool. It copies data from one file or block device (hard disc, cd-rom, etc) to another.
safecopy - data recovery tool which tries to extract as much data as possible from a problematic (i.e. damaged sectors) sources.
scrub - Scrub writes patterns on files or disk devices to make retrieving the data more difficult.
wipe - Command for securely erasing files from magnetic media.
parted - Partition Editor (create, destroy, resize, move, and copy hard disk partitions.)
gparted - GUI for parted .
partimage - Partition imaging utility, which saves partitions, having a supported filesystem, to an

image file.
gdisk - fdisk-like partitioning tool for GPT disks.
kpartx - Manages partition creation and removal for device-mapper devices.
testdisk - Tool to check and undelete partition. Works with FAT12/16/32, NTFS, ext2/3/4, Linux Raid, LVM, etc. Also recovers image files.
rsyslog - Remote Syslog.
mate-screenshot - Take Screenshots of your work.
Memtest86+ - A thorough stand-alone memory test for x86 and x86-64 architecture computers.

On behalf of the entire WBITT team, I thank you for using the Fedora AntiVirus Spin. We hope that you find it useful.
Muhammad Kamran Azeem (kamran at wbitt dot com)