IBM 32 MB USB Memory Key
(P/N 22P5296)

Boot Sector Virus
Detection and Cleaning Algorithm

(for IBM internal use only)

Author: David Kang
Last Updated: 1/10/02

Windows 98 and Windows ME

1. Run utility to arrive at Initial Screen, Click "Fix"
2. Utility will call out "fdisk.exe" and scans screen printout to detect all physical drives
   - ?? If more than one 32 MB device detected, output "More than one 32 MB device…", remove the other 32 MB device, and run utility again with only memory key attached
3. If memory key is detected (both conditions 'a' and 'b' are met), utility will run "fdisk/cmbr" to replace the MBR and output "Memory key cleaned", utility will exit, system will restart
   a. 32 MB in capacity
   b. Master Boot Record (MBR) in partition

Limitations:

1. Falsely detect 32 MB device as memory key if conditions 'a' and 'b' are still met (unlikely):
   - ?? initial notice for user to remove all other removable storage media
   - ?? only if memory key is not plugged in, otherwise "More than one 32 MB device…"
   - ?? MBR will be replaced with generic MBR (harmless)
2. No method to detect if virus is actually present on key because OS does not allow read access to MBR to check for virus string – will proceed and replace MBR anytime key is detected
3. Must have fdisk.exe - likelihood of customer not having "fdisk.exe" is very low because standard on Win 98/ME OS
4. In Win 98 only, certain changes in configuration may cause the need for system restart to reinitialize "fdisk.exe", output "Error running utility" (see "Fdisk Configuration" below)

	Win 98/ME
No key plugged in	"Memory Key not detected" Comment: Condition 'a' not met.
Non-infected key	"Memory Key cleaned successfully" Limitation (2)
Infected key	"Memory Key cleaned successfully"
32MB device (w/ MBR)	"Memory Key cleaned successfully" Limitation (1)
More than one 32 MB device	"More than one 32 MB device detected"
Key in write protect mode	Currently working on implementing popup message to stop routine after running utility if key is in the write protect mode and warn user – only prevention now is the initial notice screen

Fdisk Configurations [Win 98 Only ,Win ME ok]

1. Any other 32MB device plugged in already ✍ run utility, "Memory Key not detected" --> remove device, plug in key, run utility ✍ "Error running utility" (initial screen indicate to remove all other devices before running utility)
2. Memory Key or any 32MB device plugged in already ---> remove that device, don't run utility ---> plug in memory key, run utility ✍ "Error running utility" (initial screen indicate to ensure memory key plugged in before running utility)

The likelihood of customer in any of the two configurations above is low. Most will be in the two configurations listed below. If customer follows instructions on initial screen correctly, they will not run into these situations above. If they do, the output message below will ask them to try again with the correct configuration.

1. No key plugged in, don't run utility --> Plug in key, run utility, OK (majority of customers)
2. Key already plugged in, run utility, OK (majority of customers)

Windows 2000 and Windows XP

1. Run utility to arrive at Initial Screen, Click "Fix"
2. Utility will check all physical drives to verify three conditions 'a', 'b', and 'c', if any condition not met, it will proceed to check the next physical drive
    a. Read first sector to check if bootable MBR exists (bootable "boot indicator" of MBR)
    b. Make sure the device is 32MB in size
    c. Compare physical drive's MBR vs. infected MBR to compare if virus string detected
        ?? if detected, infected MBR will be replaced by generic MBR

Limitations:

1. 32 MB device may be falsely detected as memory key by passing 'a' and 'b' but MBR will not be rewritten since 'c' will fail
    ?? rarely any 32 MB storage media have bootable partition
    ?? initial Screen asks user to remove any other removable storage media

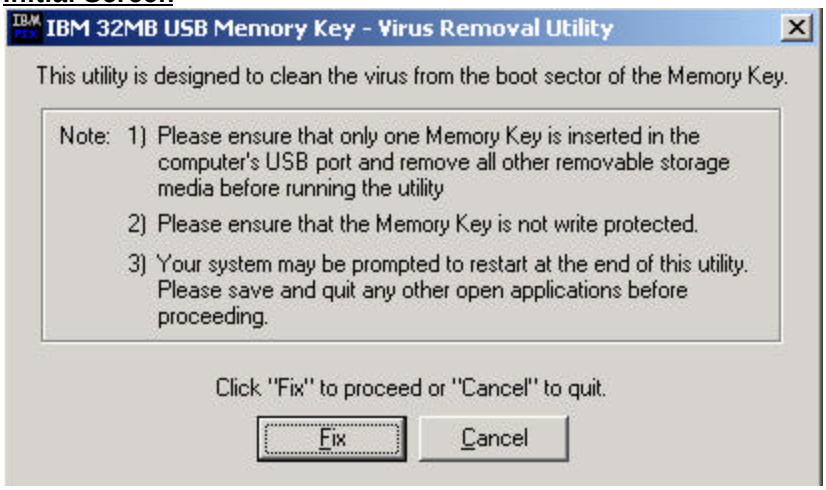
	Win 2000/XP
No key plugged	"Memory key not detected" Comment: Either condition 'a' or 'b' not met.
Non-infected key	"Memory key detected, but no virus found" Comment: Condition 'a' and 'b' met, but 'c' not met.
Infected key	"Memory Key cleaned sucessfully" Comment: Condition 'a', 'b', and 'c' met
32MB device (w/ MBR)	"Memory key detected, but no virus found" Limitation (1)
Key in write protect mode	Currently working on implementing popup message to stop routine after running utility if key is in the write protect mode and warn user – only prevention now is the initial notice screen

Other

How to determine which OS the user has? GetVersion( )
Where does utility search for fdisk.exe? Does not actually search for it, just calls it out.

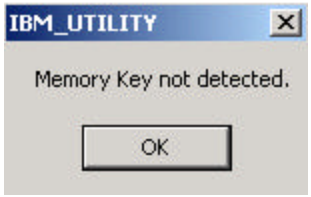
USER INTERFACE OUTPUT DISPLAY

Initial Screen

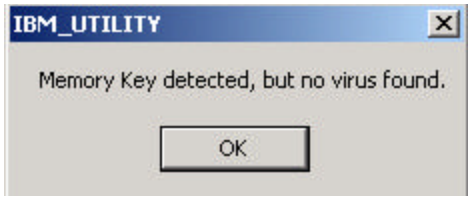


Detected and cleaned

No memory key inserted



Non-infected memory key [Win 2000/XP only]



More than one 32 MB device [Win 98/ME only]

Fdisk Limitiation [Win 98/ME only]

No Fdisk on system [Win 98/ME only]