

## **Bootable CD**

by

**Fung Wai Wa**

ISFS Council Member

While IBM-PC was first introduced in early 1980's, there was no hard-disk attached to the machine: PC at that time was booted up with a floppy disk (not the 3.5" floppy disk that we are using today, but the 5.25" bigger floppy disks). In mid-1980s, the price of hard-disks had reached to a level that most people can afford. Since then, hard-disk has become an indispensable component for a microcomputer system. With high-disks, bigger applications can be supported. More memory- and disk-hungry applications are created, and a major trend started: movement from command-line applications to GUI-based applications.

GUI-based applications greatly reduce the learning barrier of using computers by laymen, making more people be willing to use the PC applications. The number of PC users further increased when people saw the benefits of Internet in mid 1990s. It became a trend to surf the net.

Not all people are using the computer to perform legal activities. While more and more people, including the bad guys, are relying on the computer for their daily activities, computer systems can be a major source of evidence in case criminal activities are involved. For example, even though a file is deleted with normal Windows or DOS utilities, there is still chance for investigator to retrieve the content of the deleted files. Another example is the Internet cache files kept in the hard-disk while people are surfing the Web using browsers such as Internet Explorer (IE). Normal users might not be aware of its existence, but investigator might be using residual information to help the investigation. When people want to cover their tracks, they might need tools to wipe (instead of deleting) those files that they want to eliminate from being recovering, and they might need to clean up all temporary files used in their applications such as IE. This is a very tedious step and sometimes, some minor trace might still be left.

But the covering task can be easily done now -- using the bootable CD.

Current technology enables us to use bootable CD to boot to Linux and WinXP operating systems and to run completely from CD. Knoppix (<http://www.knoppix.net/>) is a free and open-source bootable CD distribution of Linux; while UBCD4Win (<http://ubcd4win.com/>) is a representative for open-source tool to create a WinXP bootable CD. Now, we can, like our good old days, boot up with a bootable CD and store our data to a USB disk. There would be no booting problem due to crashes in OS configuration settings. Moreover, there might be no trace on what we have done.

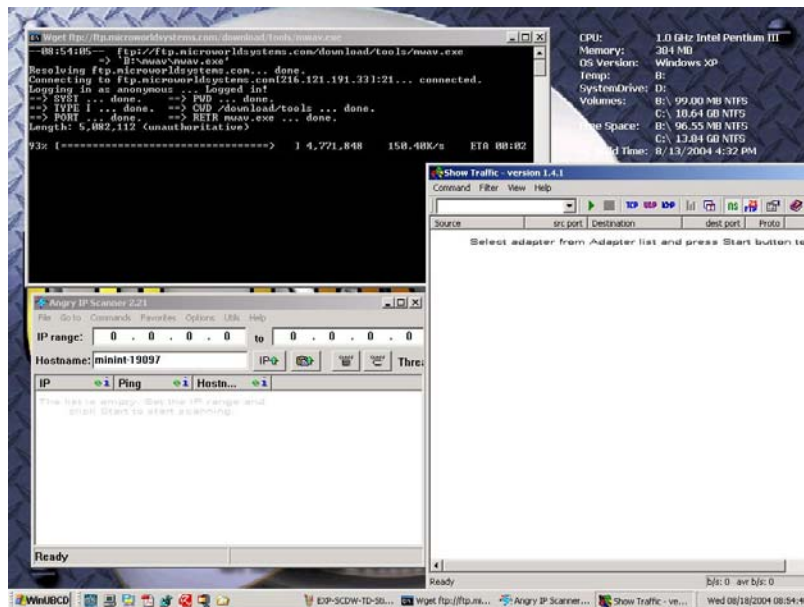
Knoppix is attractive because its excellent hardware detection, rich collection of programs, and feasibility to create one's own customized Knoppix CD. There have been a number of Linux distributions customized from Knoppix. Examples include Helix (<http://www.e-fense.com/helix/>) and Knoppix-STD (<http://www.knoppix-std.org>). The ISO images of these customized bootable CD can be downloaded from their respective web sites; and we can then burn the ISO image onto a CD for use. In addition to incident handling tools (including common attack and defense tools, virus scanning tools, forensics tools, etc), basic Linux tools including web browsers are also included. Consider a scenario of a bad guy to browse to child-porn web sites, all local evidence (e.g. web browser cache, temporary files, etc) would be completely lost when the machine is turned off. Traditional techniques on searching

for evidences in temporary directories would not give any evidence. The search for the Linux history / system log files would not give any clues on the previous commands used in the previous sessions. Probably the only evidence would be the ISP record that someone from the subscribed location might have ever visited the child porn sites.

For Windows users, UBCD4Win can be considered. When booted up, a Window desktop similar to the usual Windows XP environment is available. The UBCD4Win comes with a number of GUI applications, including a K-Meleon Internet browser. However, when compared to Knoppix distribution and its variants, UBCD4Win has the following troubles:

- (1) No ISO image is available for download due to license issue. As such, one need to build the ISO image himself / herself.
- (2) Not all GUI-based applications can be easily inserted / customized into the CD image. Plugins must be created for each GUI applications.

The following is an example screen shot that can be found in the UBCD4Win web site:



On the other hand, these bootable CD might help investigators or IT personnel to do preliminary analysis on a subject computer. In general, it is not expected that tools for incident handling would be pre-installed in the suspect's (or victim's) machine. While doing a preliminary analysis on the subject's machine, tools burned into these CD would be a good source of help, with no need to install anything into the subject machine. However, if you plan to use these bootable CD to boot up a subject PC, Knoppix-based bootable CD can be used, while it is reminded that UBCD4Win would tamper the local hard-disks and it cannot (yet) be used for this purpose.