3.3. Performing Remote Acquisition

Performing Remote Acquisitions

• Remote acquisitions are handy when you need to image the drive of a computer far away from your location

– Or when you don't want a suspect to be aware of an ongoing investigation

Remote Acquisitions with Runtime Software

- Runtime Software offers the following shareware programs for remote acquisitions:

  – DiskExplorer for FAT

  – DiskExplorer for NTFS

  – HDHOST

- Preparing DiskExplorer and HDHOST for remote acquisitions

  – Requires the Runtime Software, a portable media device (USB thumb drive or floppy disk), and two networked computers

- Making a remote connection with DiskExplorer

  – Requires running HDHOST on a suspect's computer

  – To establish a connection with HDHOST, the suspect's computer must be:

- Connected to the network

- Powered on

- Logged on to any user account with permission to run noninstalled applications

- HDHOST can't be run surreptitiously

Fig: Displaying the contents of the HDHOST folder in Windows Exp

Fig: Selecting a connection type

- Making a remote acquisition with DiskExplorer

– After you have established a connection with DiskExplorer from the acquisition workstation

- You can navigate through the suspect computer's files and folders or copy data
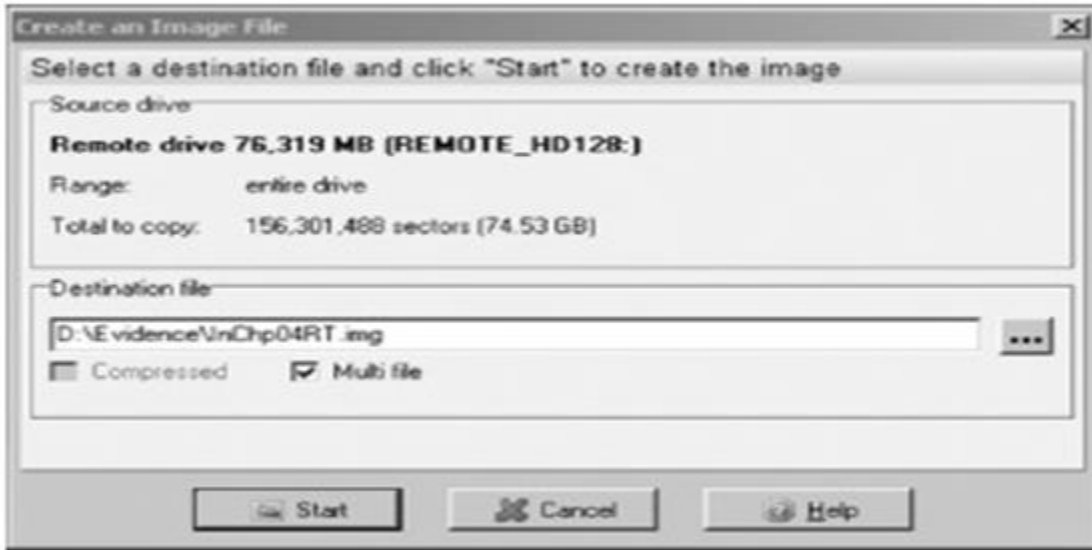
– The Runtime tools don't generate a hash for acquisitions

Fig: Create an Image file Dialog box