(Especially when the evidence has been hidden or eliminated)

1) Click on your **[Start]** button and then click on "**My Computer**"

2) When "**My Computer**" is open, Double-Click on your C: drive to open it. Then, Double-Click the **Documents and Settings** folder to open it.

Network Evaluation

Tutorials and Guides to help enhance the integrity and security of your systems

www.networkeval.com   (408) 395-3921
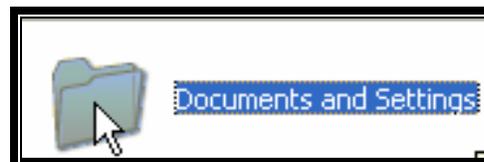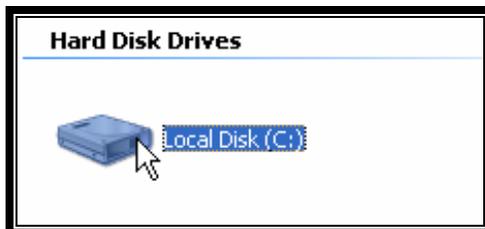
3) Open the **Tools** menu and click on **Folder Options**...
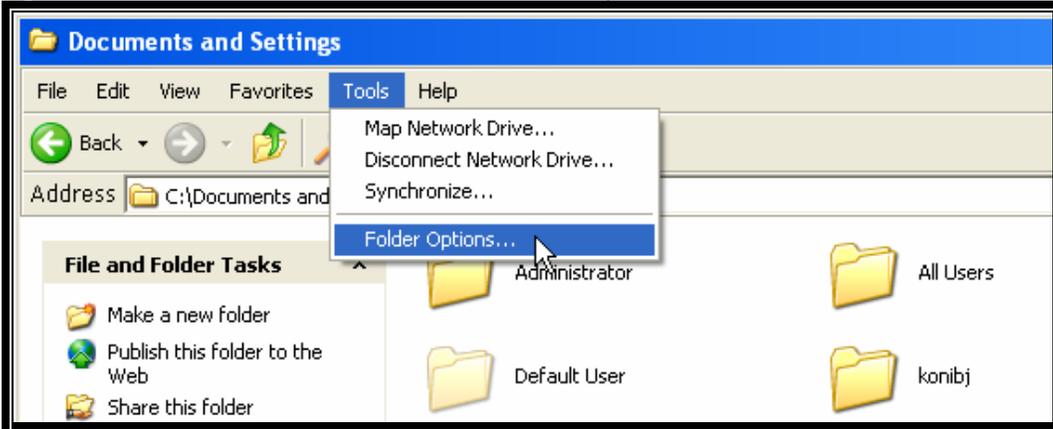
4) Click on the **View** folder tab
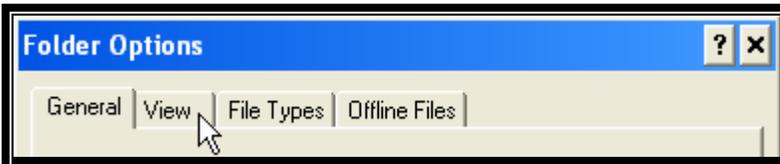
5) Click the radio button for "**Show hidden files and folders**" and then click on **OK**.

Network Evaluation

Tutorials and Guides to help enhance the integrity and security of your systems

We're Looking For Trouble

www.networkeval.com   (408) 395-3921
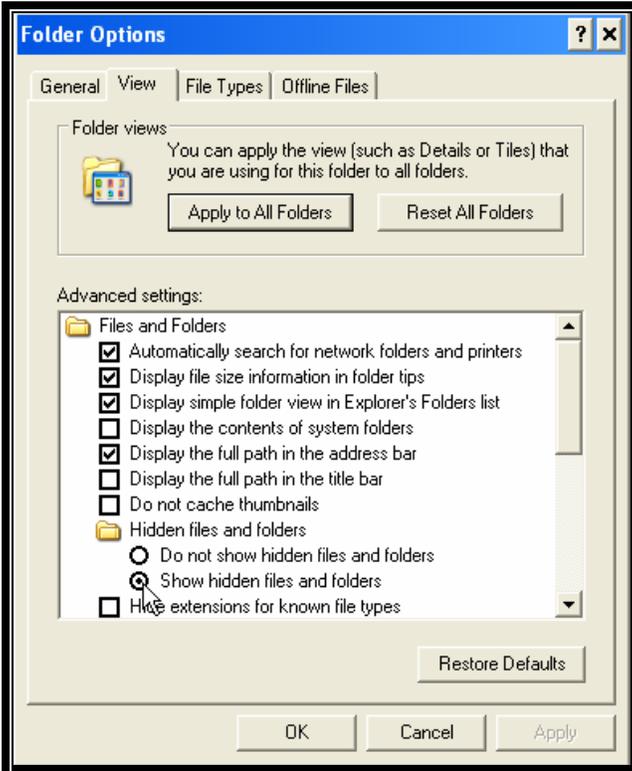
6) You should now see some "faded" folders in the Documents and Settings folder, along with the normal looking folders. These are referred to as "Hidden". In this case, we want to open up the one belonging to our "**Suspect_User**". Double-click on that to open it.

7) Within the Suspect_User's folder, there will be several familiar ones such as "**My Documents**", "**Desktop**", "**Favorites**" and such. The ones we're interested in are the "faded", or "Hidden" ones which are normally invisible.
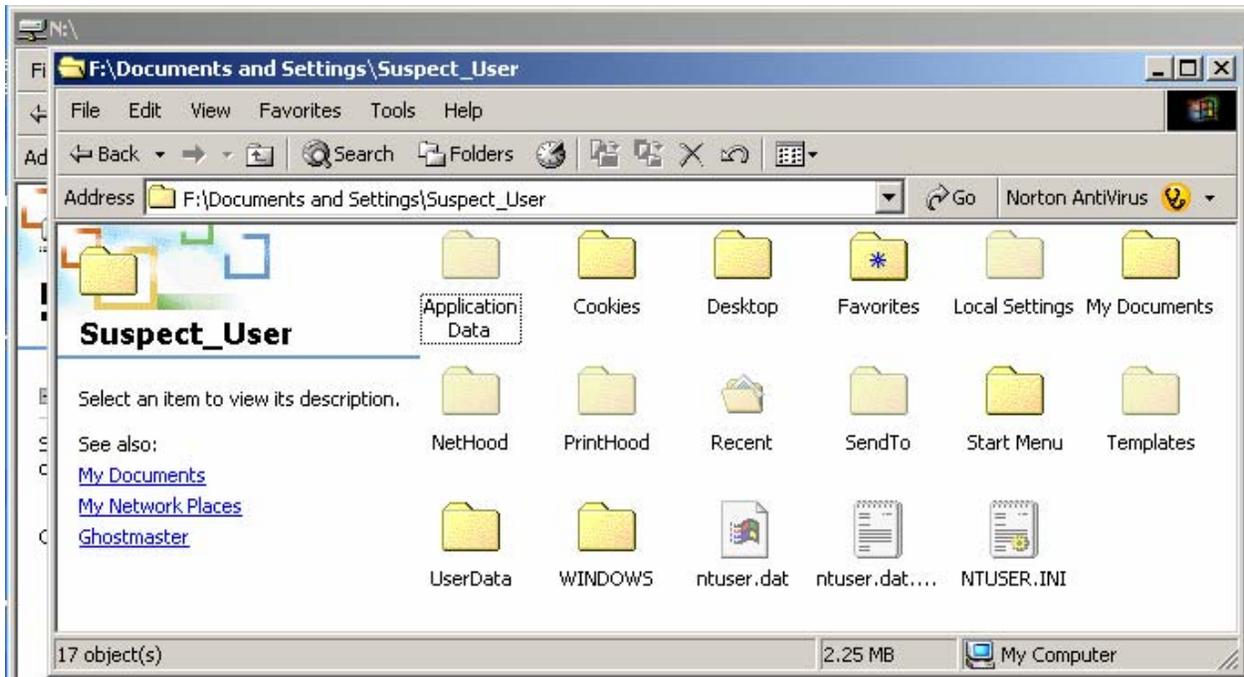
8) If there is a folder called "**Incomplete**", open that one first.
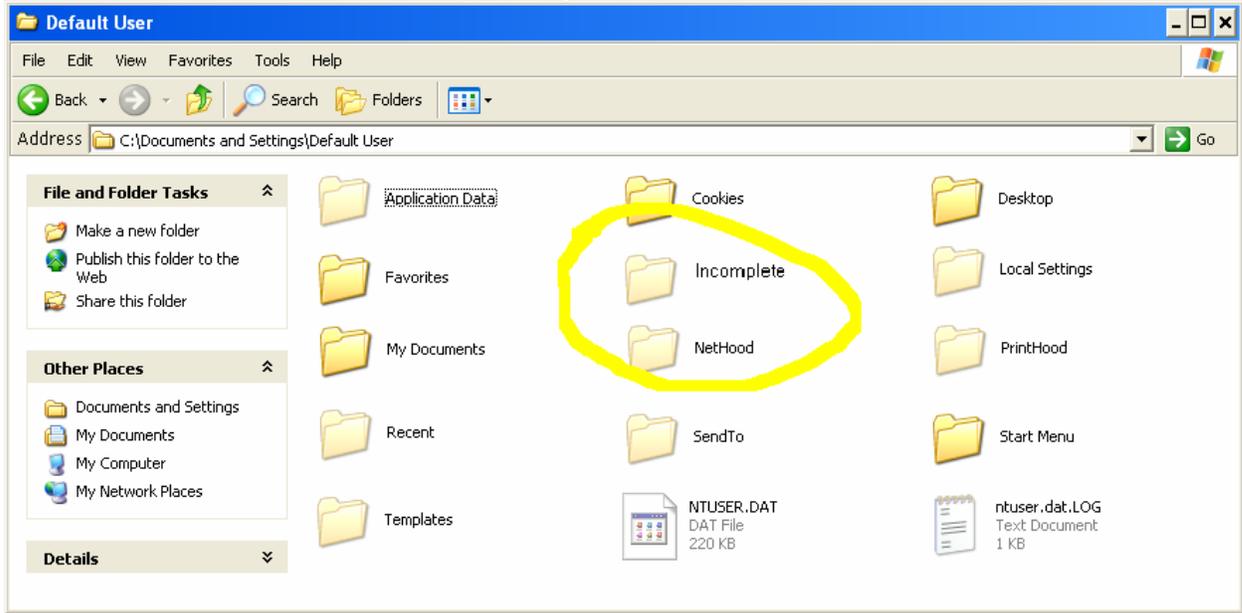
The "Incomplete" folder contains Internet downloads which failed to complete successfully. In the case of large/detailed images and videos, there are often remnants left here which most users are not aware of. This folder is not usually cleaned out by the "Remove temporary Internet Files", or "cleanup" programs like "Evidence Eliminator" which are used to hide evidence of surfing porn and such.

9) If you examined the "**Incomplete**" folder, click the "**Back**" button to return to the users "home" folder.. Then double-click on the "hidden" **Local Settings** folder to open it.

10) Open the "**Temporary Internet Files**" folder
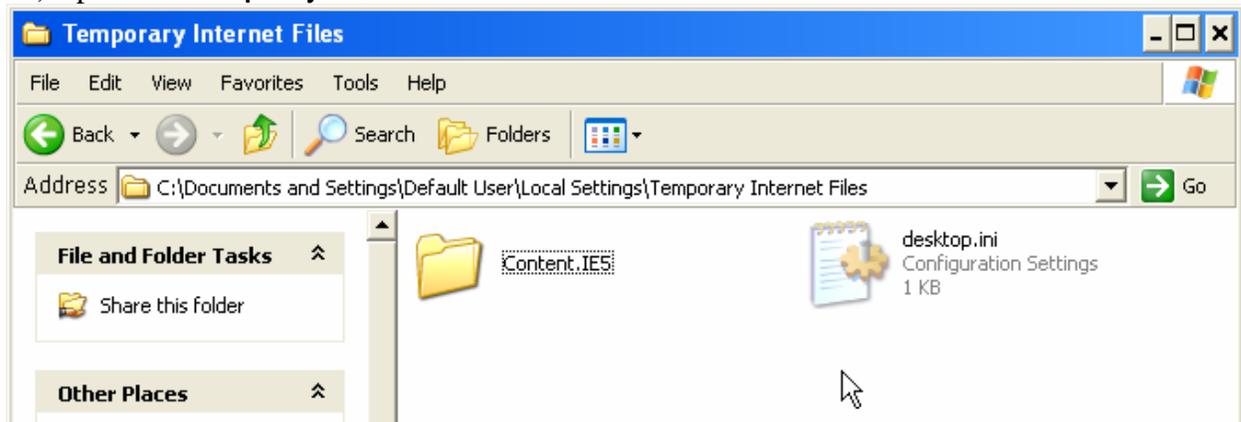
11) Open the "**Content.IE5**" folder
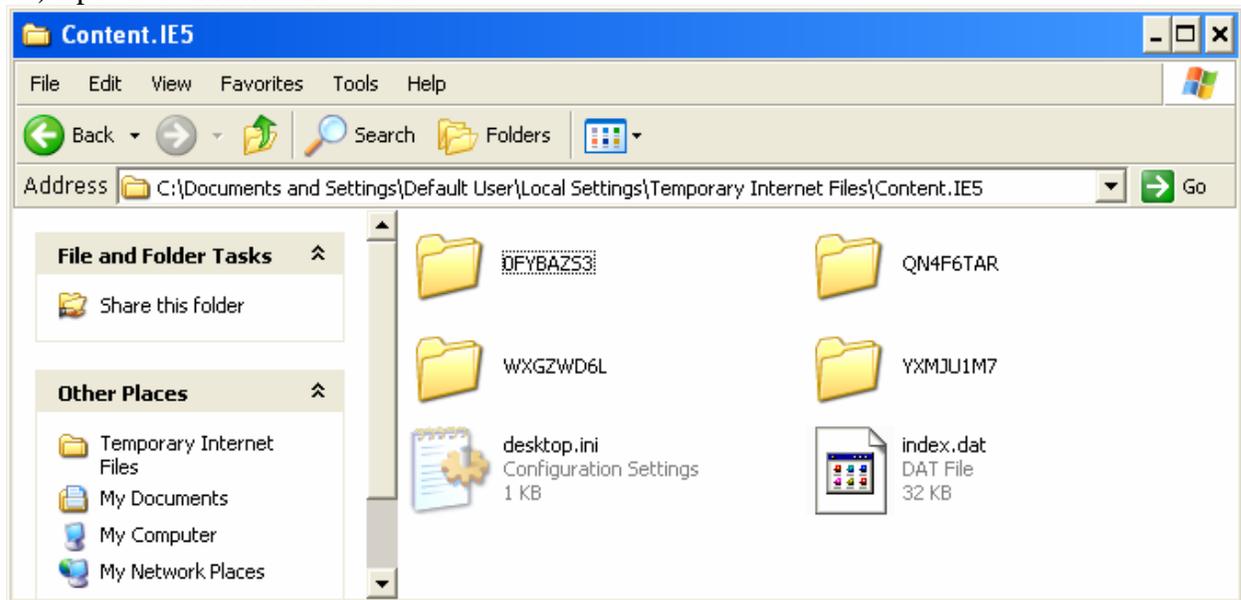
Inside this folder will be a number of folders with cryptic names, such as seen above. Each of these "cryptic" named folders contain the actual temporary Internet files downloaded during web surfing.

12) Open the first one of these "cryptic" folders as an example. Right-Click on the open (white) space and click on the "**View**" menu item, and then the "**Thumbnails**" item. This will allow you to view miniature copies of many graphics files.

Network Evaluation

Tutorials and Guides to help enhance the integrity and security of your systems

www.networkeval.com   (408) 395-3921

If the folder is left with the (currently – Details) View option, then you'll see the full name of the temporary files, along with the web site they were downloaded from, and the time and date stamp (scroll to the far right for those).

Additional Notes

Some Internet temporary files can be found under the user's temp folder. A shortened version of the folder navigation is shown below, but similar to the more detailed examples above.
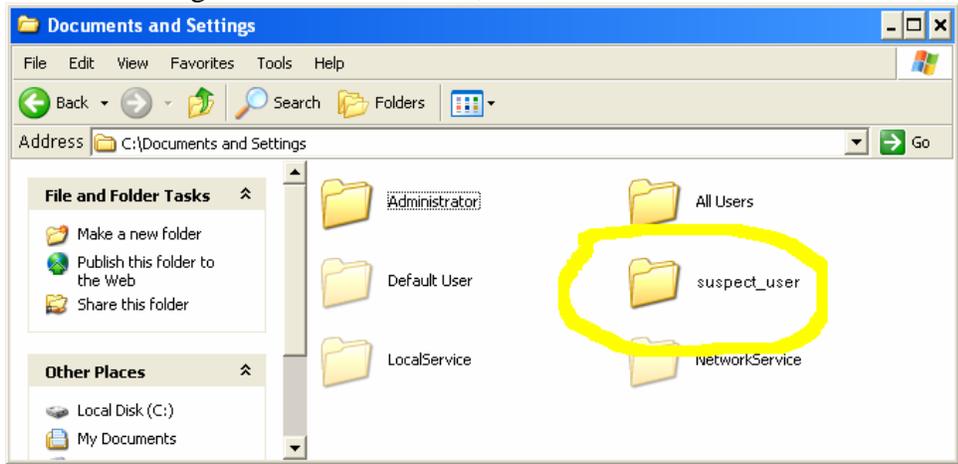
Network Evaluation

Tutorials and Guides to help enhance the integrity and security of your systems

www.networkeval.com   (408) 395-3921

We're Looking For Trouble

PC Cleanup - Tracking "suspect" web surfing
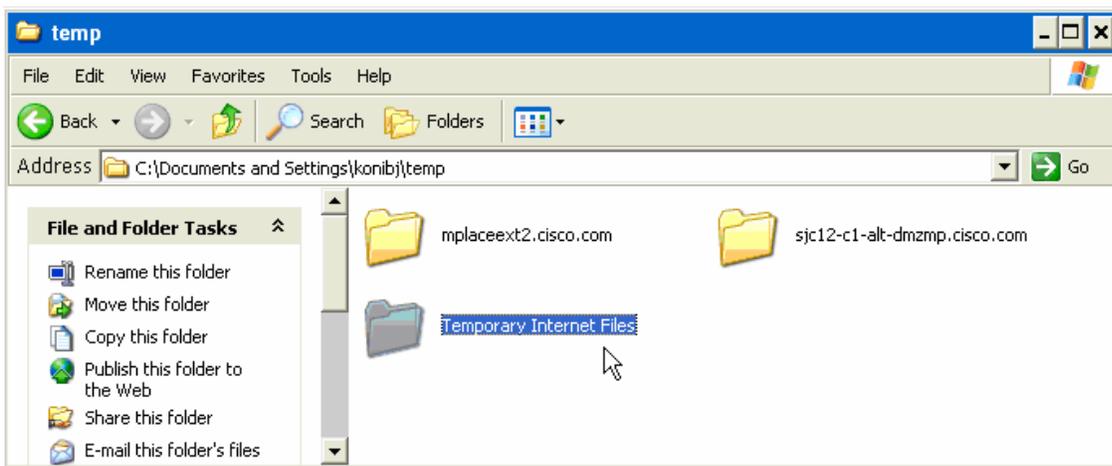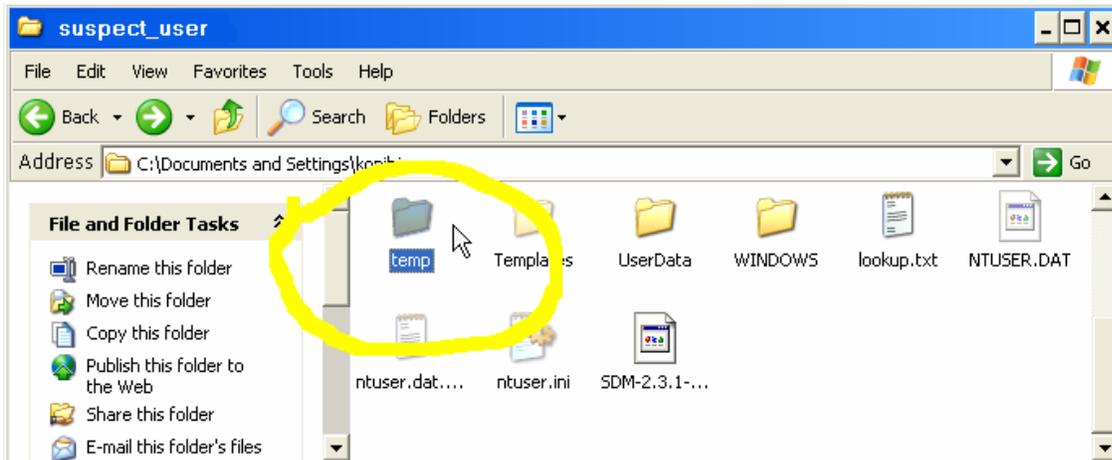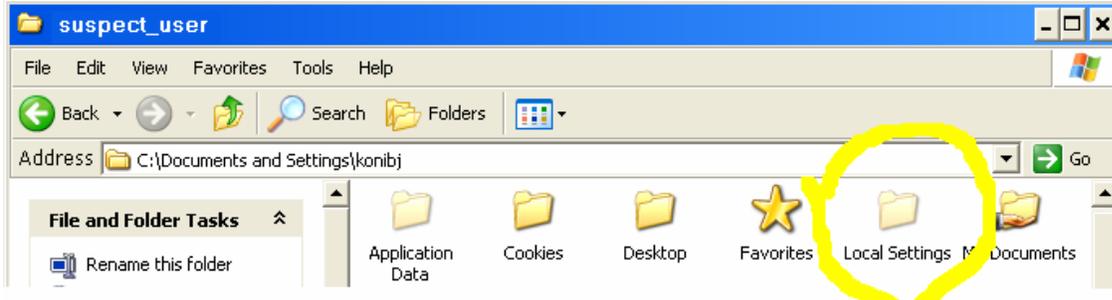
If the suspected user surfs with a different Internet Browser (Internet Explorer, Mozilla/Firefox, Netscape, Opera, Safari, etc.) then you may have to look in the **Application Data** folders for the Internet surfing content. Start from the **Documents and Settings** folder and work your way down.