**Objectives:**

- Use Access Data's FTK Imager to locate and export Windows Event Log Files
- Use Event Log Explorer to Examine the Event Logs and identify information relevant to this investigation
- Understand the general contents of Windows Event Logs

1. Open / Install Access Data's FTK Imager 3

2. Select File > Add Evidence Item > Select Image File > Browse to the Suspect image and add it.

3. Navigate to the Windows System Event Logs. They are in C:\Windows\System32\Config. Export the three event logs (AppEvent.evt, SecEvent.evt, & SysEvent.evt) to a new directory.

4. Open / Install Event Log Explorer (elex_setup.exe).

5. Select File > Open Log File > Direct > Select the log files that you exported from the suspect image. (Open all 3 log files)

6. Examine the SecEvent.Evt and answer the following questions:

    a. What user profile logged on 4/13/2014 at 4:42:12PM? What type of logon was it?

= ________________________________________________________________

    b. When was the user profile "Tiny_Tim" created?

= ________________________________________________________________

7. Examine the SysEvent.Evt log and answer the following questions:

    a. What occurred on 4/6/2014 at 3:35:37PM and how could it be relevant to your investigation?

= ________________________________________________________________

    b. We are concerned that the remote desktop tool, VNC, may have been used in this attack. Does the System Event log provide any indication of this?

= ________________________________________________________________

8. Examine the AppEvent.Evt log and answer the following questions:

   a. Does the application event log provide any further indications of how VNC was used in this attack and where the source of the attack may have come from?

      ______________________________________________________________________

      ______________________________________________________________________

      ______________________________________________________________________

      ______________________________________________________________________