**Objectives:**

- Use FTK Imager to navigate a complete XP forensic image.
- Locate and extract suspect's Prefetch Files.
- Use WinPrefetch View to Parse the Prefetch files
- Understand the contents of the Prefetch File.

1. Open Access Data's FTK Imager 3
2. Select File > Image Mounting > Browse to the Suspect image and mount it to a local drive letter.
3. Confirm that you now have a local drive letter containing the suspect image's folder structure.
4. Use WinPrefetch View to parse the suspect system's prefetch Files.
    *a.* By default, WinPrefetchView will parse the prefetch files on the host computer. You are now looking at the programs that have been executed on the local computer.
    *b.* Select *Options > Advanced Options* and provide the path C:/Windows.
    *c.* What programs were executed most often on the suspect computer?

---

    *d.* When *was WINRAR.EXE* last executed on this system? Are there any indications as to what files WinRar was used to open?

---

---

    *e.* What was the first and last time that Wordpad.exe was run on this system?

---

    *f.* Is there any indication as to what files Wordpad may have been used to open? Could they have been related to the files that WinRar.exe was used to open?

---

g. Does any malware appear to have been executed on this system? If so, what was its name?

---

h. Based on the prefetch files, do you think the initial malware executed on the system could have dropped a second piece of malware on the system? If so, what was its name?

---

a. The attacker may have installed remote desktop capability using VNC. Can you confirm or deny this?

---

***Bonus:*** There may be a second version of the dropped malware. Do you know of any reason why this would be there? Hint: The attacker may have made a mistake when creating his malware, and had to fix it later. Any idea what the mistake was?)

---

---

---