Lab #12 – Registry Analysis

Objectives:

- Use Access Data's FTK Imager to locate and export Windows Event Log Files
- Use Registry Browser to access the suspect system's registry and extract evidence pertinent to the investigation.

1. Open / Install 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. Install and open Registry Browser. **Remember to run as Administrator if you are using Windows 7**
5. Select *File > Open Registry* and navigate to the mounted suspect image and select the *WINDOWS* folder on the root.
6. Within the registry, navigate to HKLM\System\CurrentControlSet\Enum\USBSTOR
    a. What is the Friendly name of the "Disk&Ven_Memorex&Prod_Mini&Rev_PMAP" thumb drive that was attached to this system?

_____

    b. What is the Parent Prefix ID for this device?

_____

7. Navigate to HKLM\System\Mounted Devices. Go to *DosDevices\F:*. Look at the Value Data, the number following the *\??\Storage#RemovableMedia#* is the Parent Prefix ID for the F: Volume . What is it?

_____

    a. Based on those two parent prefix ID's, what Drive letter was assigned to the Disk&Ven_Memorex&Prod_Mini&Rev_PMAP?

= **F:**

8. Navigate to the *HKEY_USERS\S-1-5-21-1715567821-308236825-725344543-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.bmp* path. What was the only .bmp file opened on this system?

---

9. Select *Tools > Generate Report*

   a. Go to the *Run, Run-, Runonce, RunOnceEX* section of the report. These are all autostarts. Do any of them look suspicious? What was the key name?

---

   a. Go to the *Network Interfaces*. What was the system's IP address?

---

   b. Go to *Windows Explorer - Recent Documents Cache by Extension.* What time and date was *Fake Light Saber Authenticity Papers.zip* last accessed?
