Lab 1: Forensics lab preparation

Ayman El Hajjar

March 5, 2018

Notes about this lab

Requirements

- This lab only require you to be using a linux machine.
- This can be a virtual machine such as Debian or Kali.
- **A USB is only needed for the Portfolio task 4**

0.1 Sleuthkit

Install sleuthkit tools

1. download Sleuthkit from the website `www.sleuthkit.org/sleuthkit/download.php`
   - The current version at the time of writing the lab is sleuthkit-4.6.0. If this changed, make sure your commands below reflect this change.
2. Open terminal
3. Type **cp sleuthkit-4.6.0.tar.gz /home/yourusername/Desktop/**
4. Go to your home director using the **cd** command. Use
5. We will now extract the compressed file in the Desktop
6. **tar -xvf sleuthkit-4.6.0.tar.gz**
7. go inside the sleuthkit folder using the **cd** command **cd sleuthkit-4.6.0**
8. Wen now need to build the sleuthkit application (install it)
   - **./configure**
   - **make**
   - **sudo make install**

1 Lab Preparation USB Drive

1.1 Format your usb

1. Open the Terminal (Ctrl + Alt + T)
2. type **lsblk -** using this command, you will be able to identify your usb drive.
3. unmount usb drive. Check your drives with **lsblk** again and mount your drive another time.
4. For the next step, make sure you identified the USB correctly as it is a powerful command and go format your computer.
5. erase everything using dd **sudo dd if=/dev/zero of=/dev/sdb bs=4k && sync**
6. **sudo fdisk /dev/sdb** and press **o** to create a new empty DOS partition table.
7. use **lsblk** to check naming of new partition
8. Format the new partition volume **dev/sdb1 -** In my computer it is sdb1, check with lsblk
   - **sudo mkfs.vfat /dev/sdb1**

- The next section, you will have to put some files and folder in your usb.
- DO NOT PUT ANYTHING PERSONAL
- Take a screenshot of your file structure (file explorer)
- Delete some files

1.2 DD your USB drive

sudo dd if=/dev/sdb1 of=/home/username/Desktop/usb.dd This command will take some time so be patient. I am calling the file usb.img you can call it any name you want (keep the extension name the same).