**Lab 5: Examining the Registry**

**What You Need for this lab**

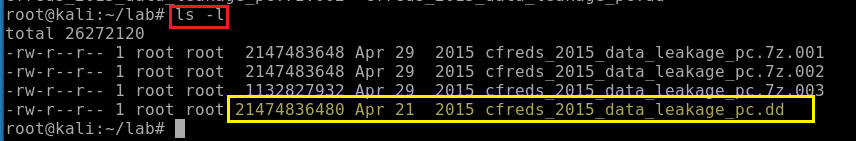
* + Install Virtualbox : <https://www.virtualbox.org/wiki/Downloads>
  + Install Kali 2021.4. : <https://old.kali.org/kali-images/kali-2021.4/>
    - Notes: Suggest You configure the disk size of Kali VM 80G because the size of each leakage cases image is 30G+
    - Add new virtual hardisk size 20 GB
  + Tools RegRipper 3.0
  + Download DD images
* <https://www.dropbox.com/s/u4axlx8eomgwfdc/cfreds_2015_data_leakage_pc.7z.001>
* <https://www.dropbox.com/s/pyq50s2cri6yftf/cfreds_2015_data_leakage_pc.7z.002>
* <https://www.dropbox.com/s/cxvzuiupmqc7l99/cfreds_2015_data_leakage_pc.7z.003>

**Step 1.**

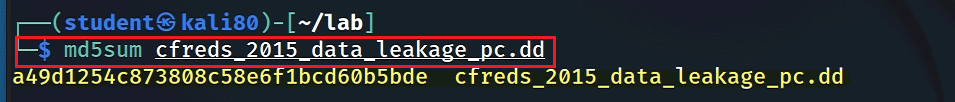
Unzipped the DD image



Verify the unzipped DD image

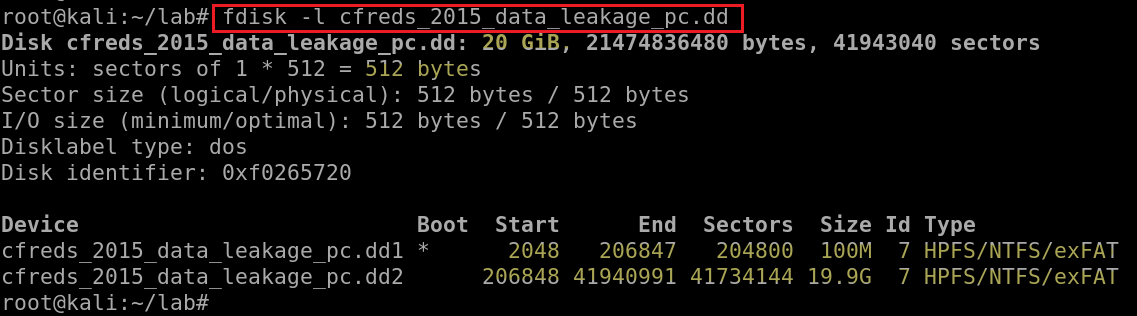


Verify the unzipped DD image with MD5

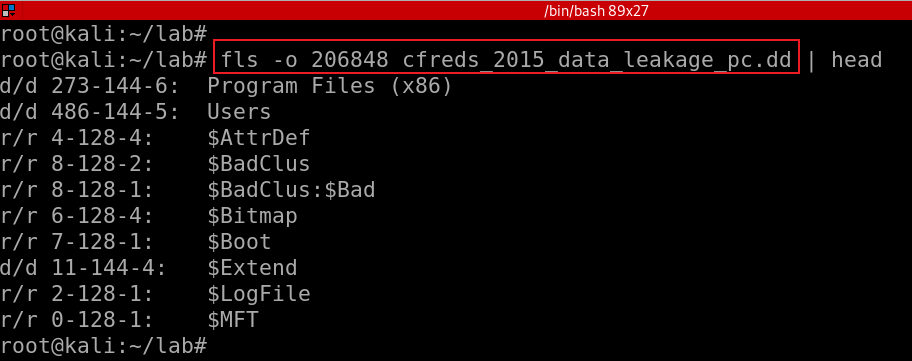
****

**Step 2.**

Exam partitions of the DD image using *fdisk*



List file/directory names of the system volume



If your VM doesn’t support auto-mounting

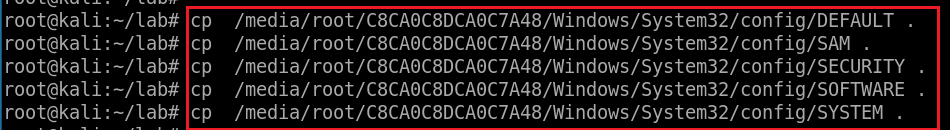
Create a folder as the mount point



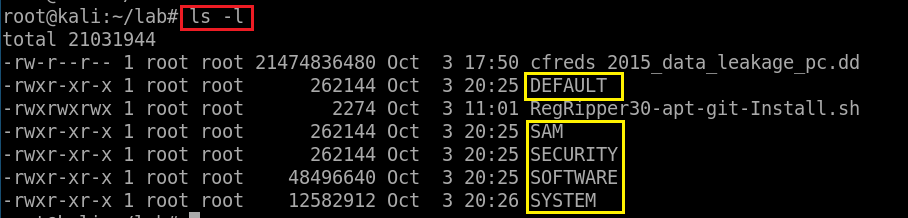
Mount partition 2 to the mounting point



Copy HKEY\_LOCAL\_MACHINE (Hive) files to \lab

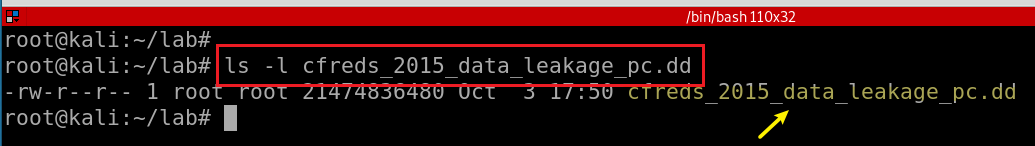


Verify five files

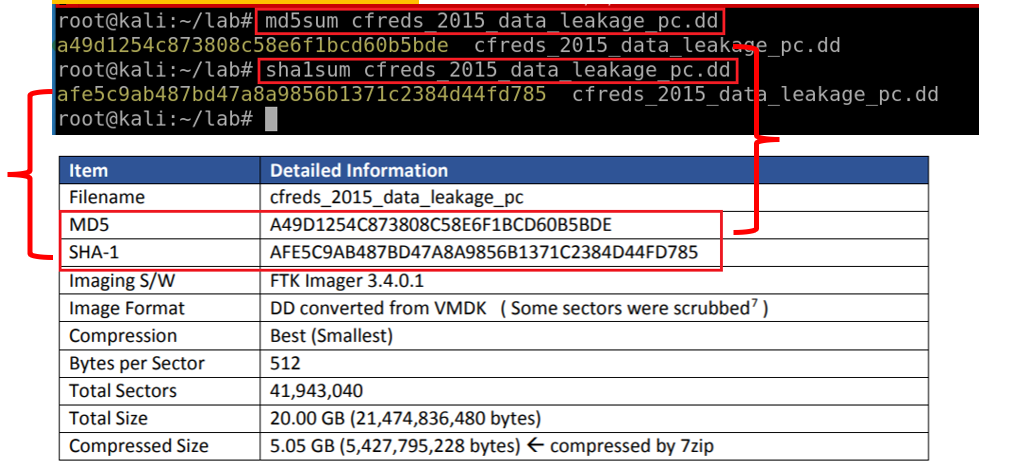


**Step 3.**

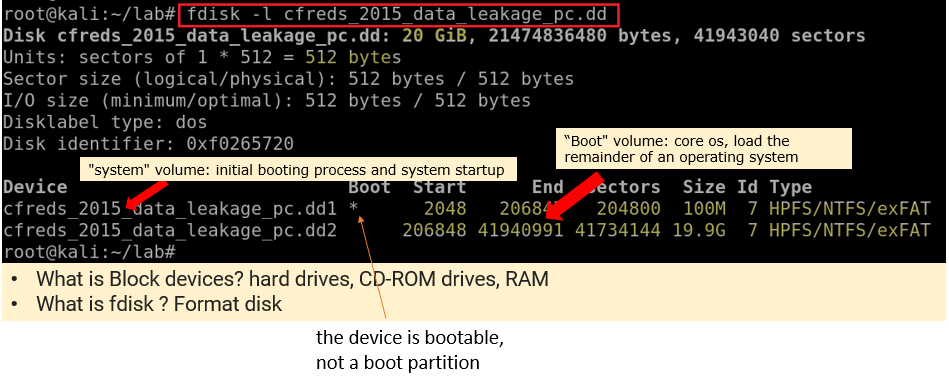
Verify you have the dd image



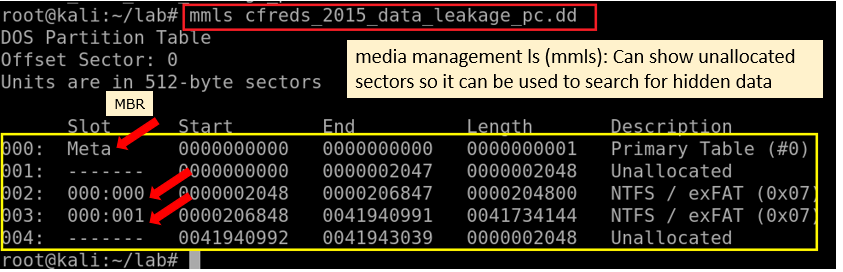
Compute MD5 and SHA1 of the DD image



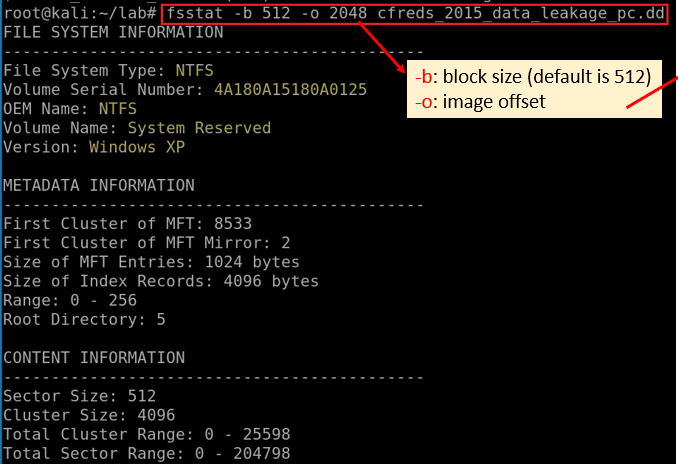
Show partitions of the image



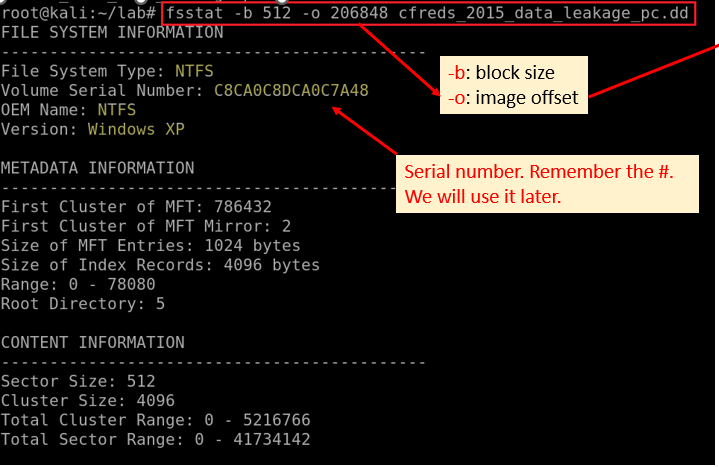
Show partitions and unallocated space using *mmls*



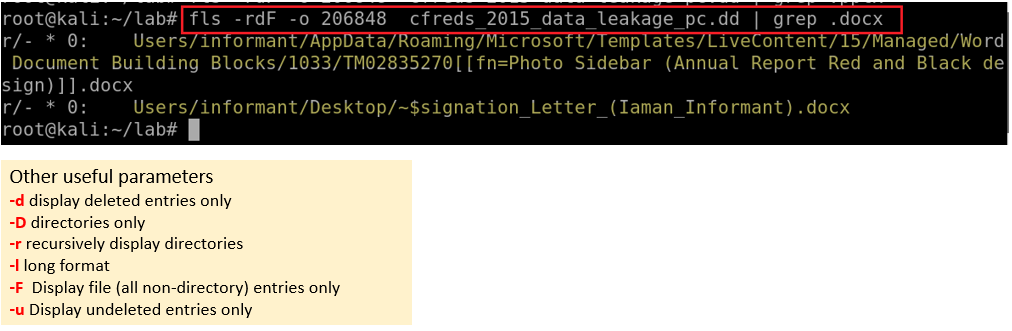
Display file system statistics and metadata information from a disk image (first partition)



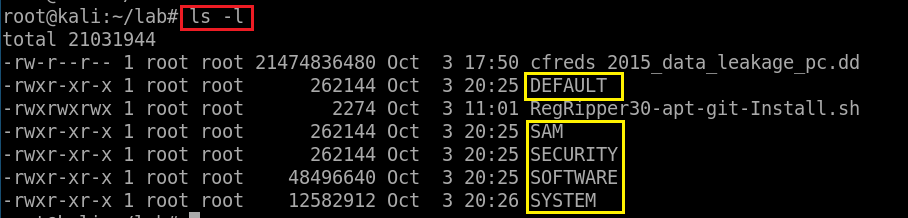
List the second partition details



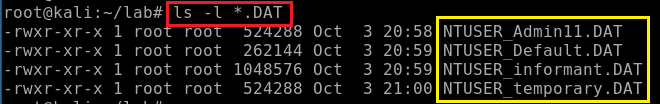
List all deleted *.docx* files in the whole partition?



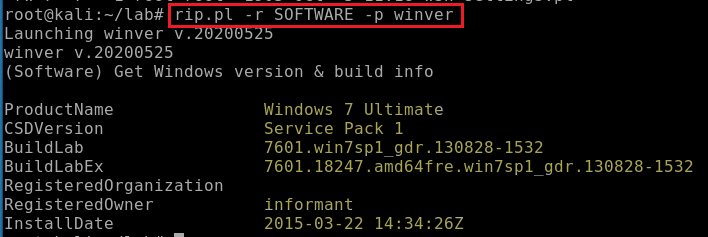
Verify system information



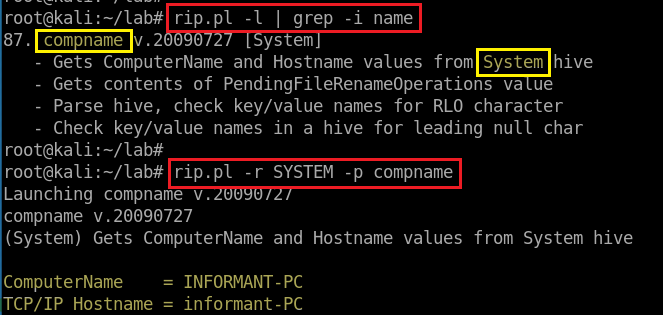
Verify Users’ information

****

**What is the installed OS information in detail?**

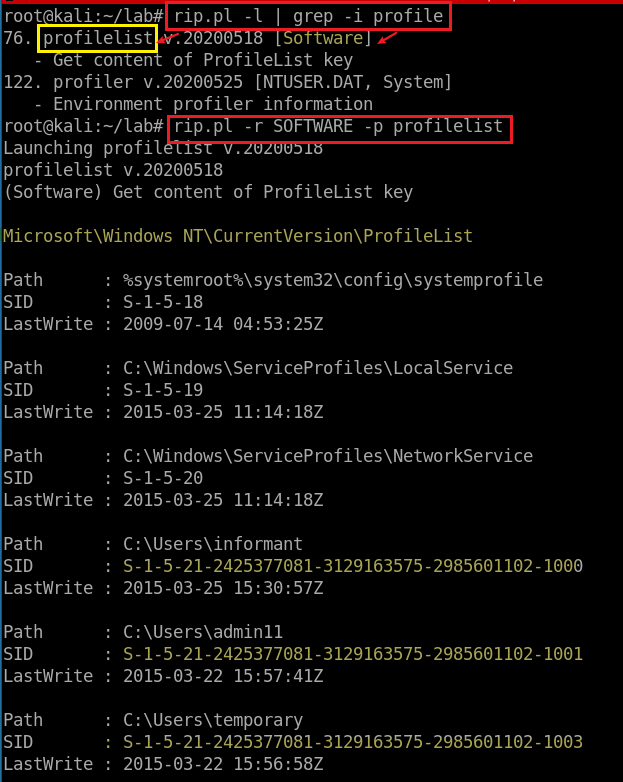
****

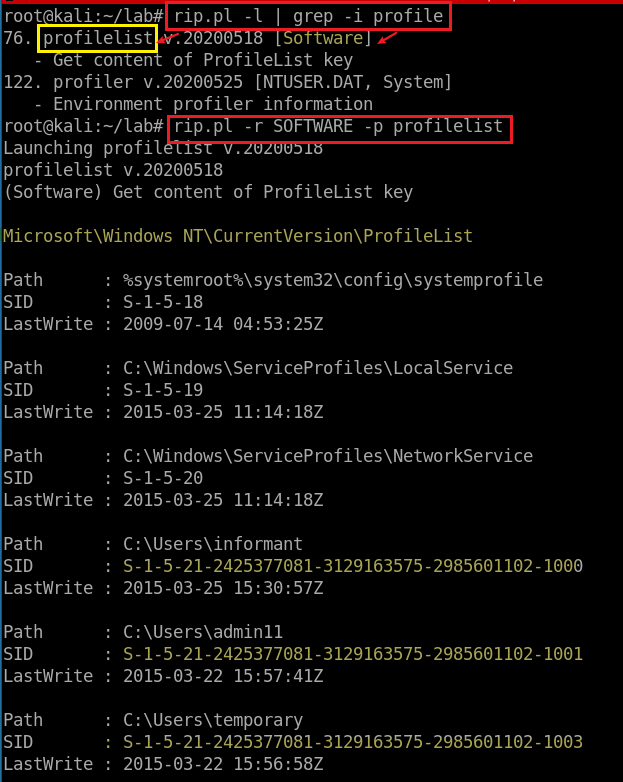
**What is the computer name?**

****

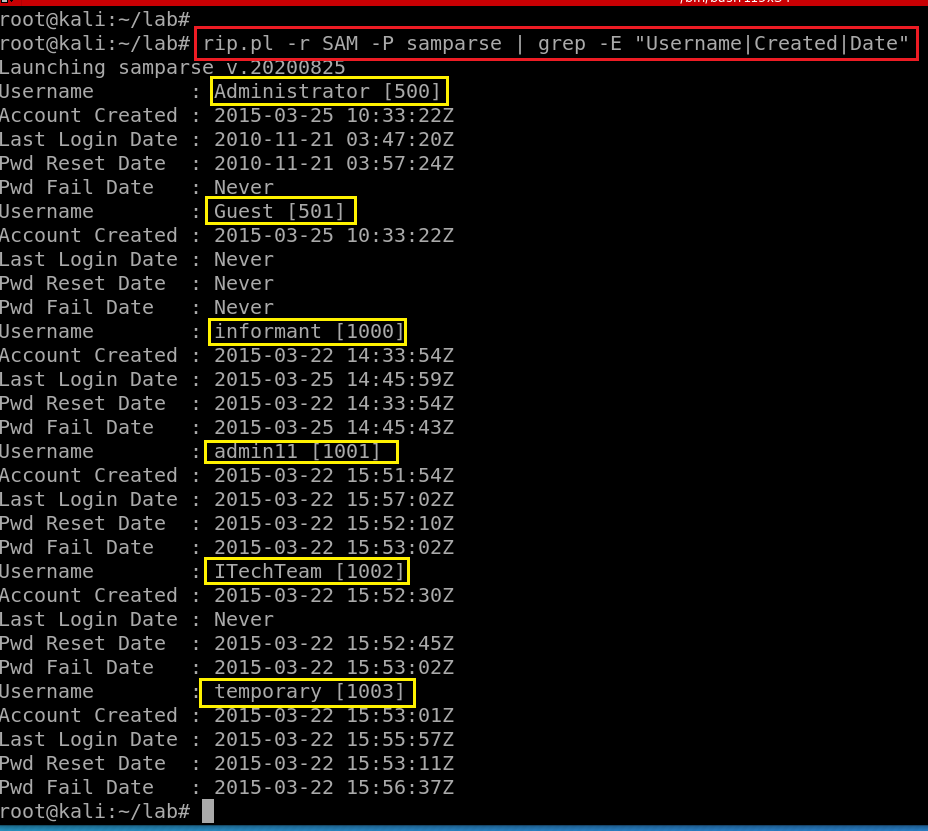
**How many accounts does the system have?**

Search for profiles





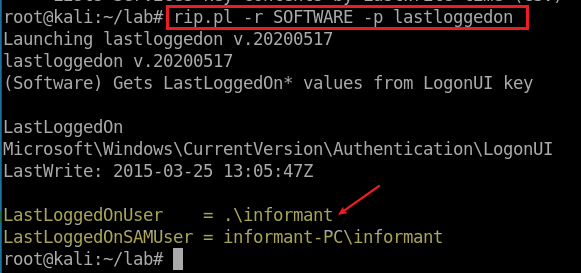
**Find and search for Security Accounts Manager (SAM) information**

****

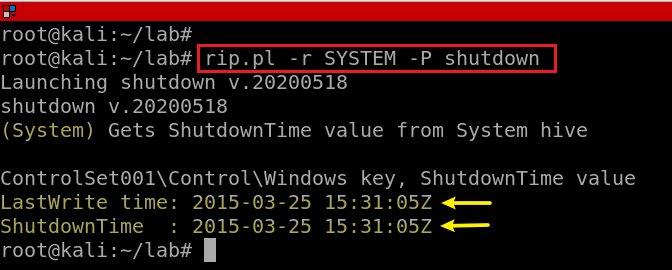
**How many accounts does the system have?**

**When is the login time?**

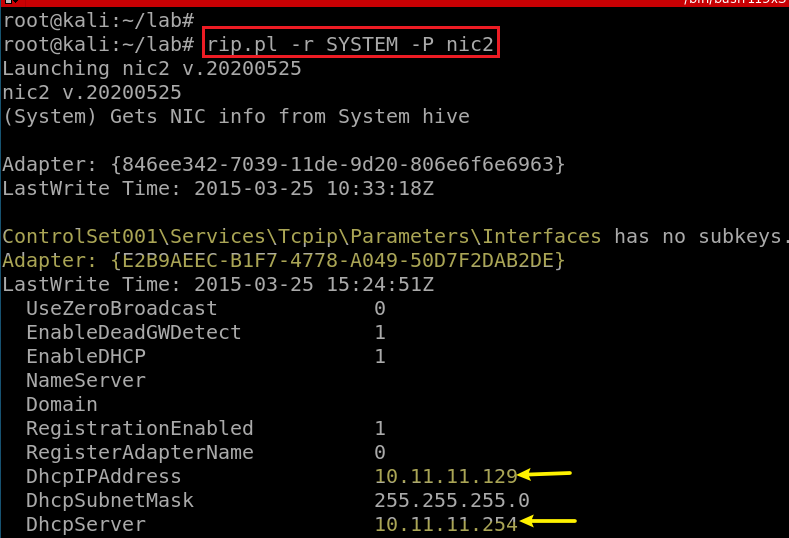
**Who was the last user to logon into PC?**

****

**When was the last recorded shutdown date/time?**

****

**Explain the information of network interface(s) with an IP address assigned by DHCP.**

****

**YOU MUST SUBMIT A FULL-SCREEN IMAGE FOR FULL CREDIT!**

Save the document with the filename "**YOUR NAME Lab 5.pdf**", replacing "YOUR NAME" with your real name.

Email the image to the instructor as an attachment to an e-mail message. Send it to: **xxx@fe.edu.vn** with a subject line of "**Lab 5 From YOUR NAME**", replacing "YOUR NAME" with your real name.