**Lab 7: Recycle Bin and Anti-forensics**

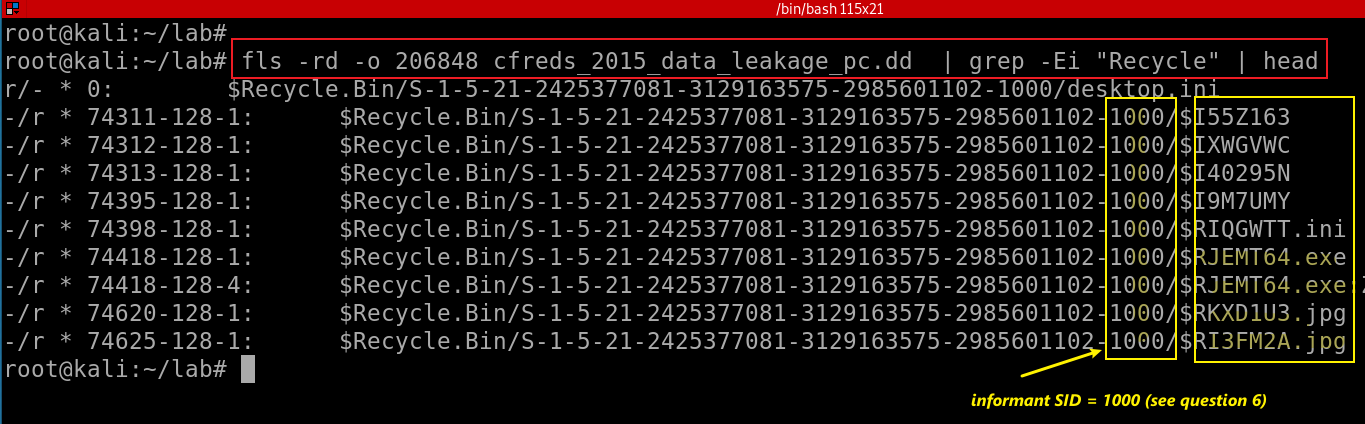
**What You Need for this lab**

* + 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+
  + Image “cfreds\_2015\_data\_leakage\_pc.dd” from Lab 5

1. **Recycle Bin**

**Step 1.**

* Examine ‘Recycle Bin’ data in PC.

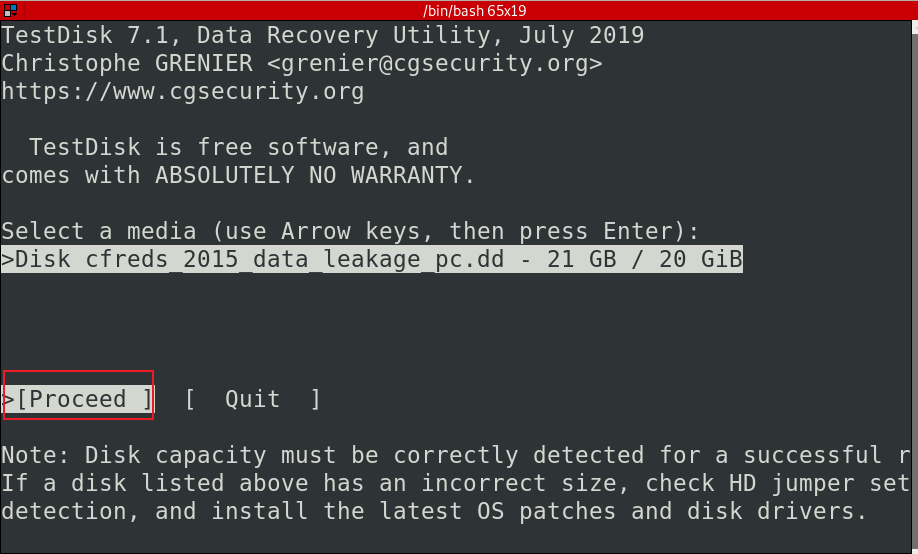


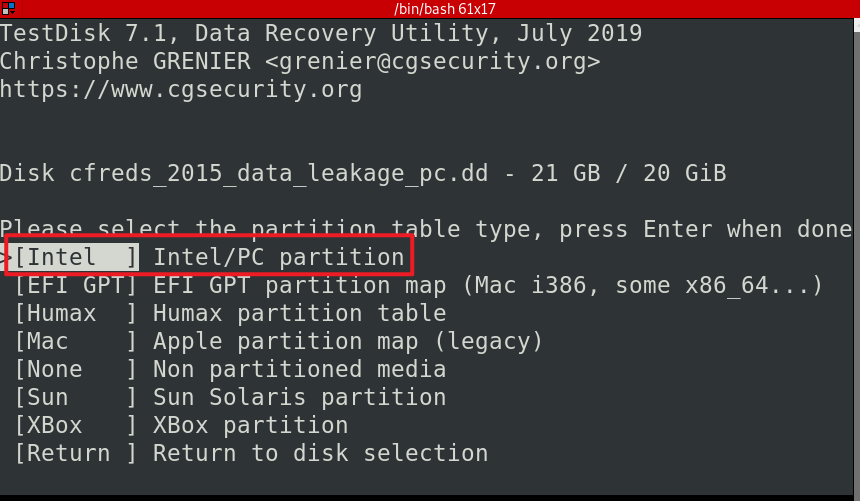
**Step 2.**

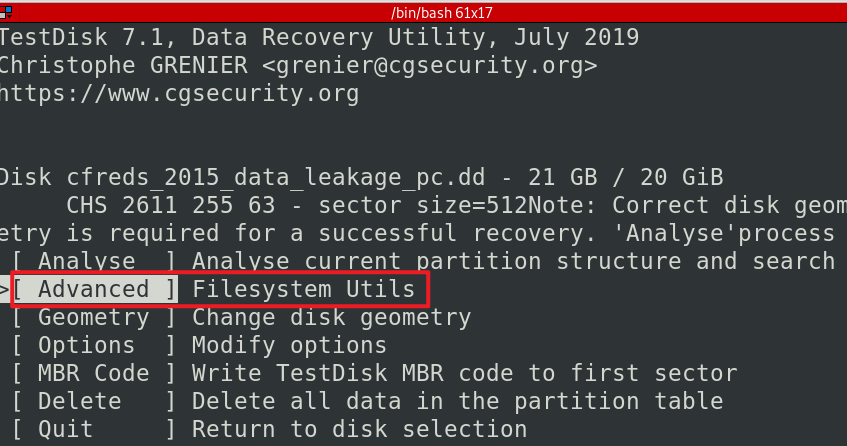
* Use *testdisk* to Recover *$Recyle.bin*

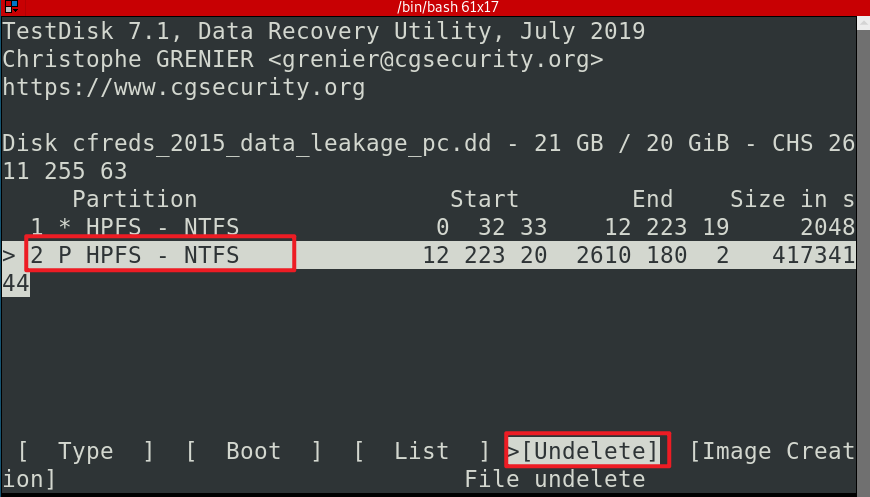
Recover the image



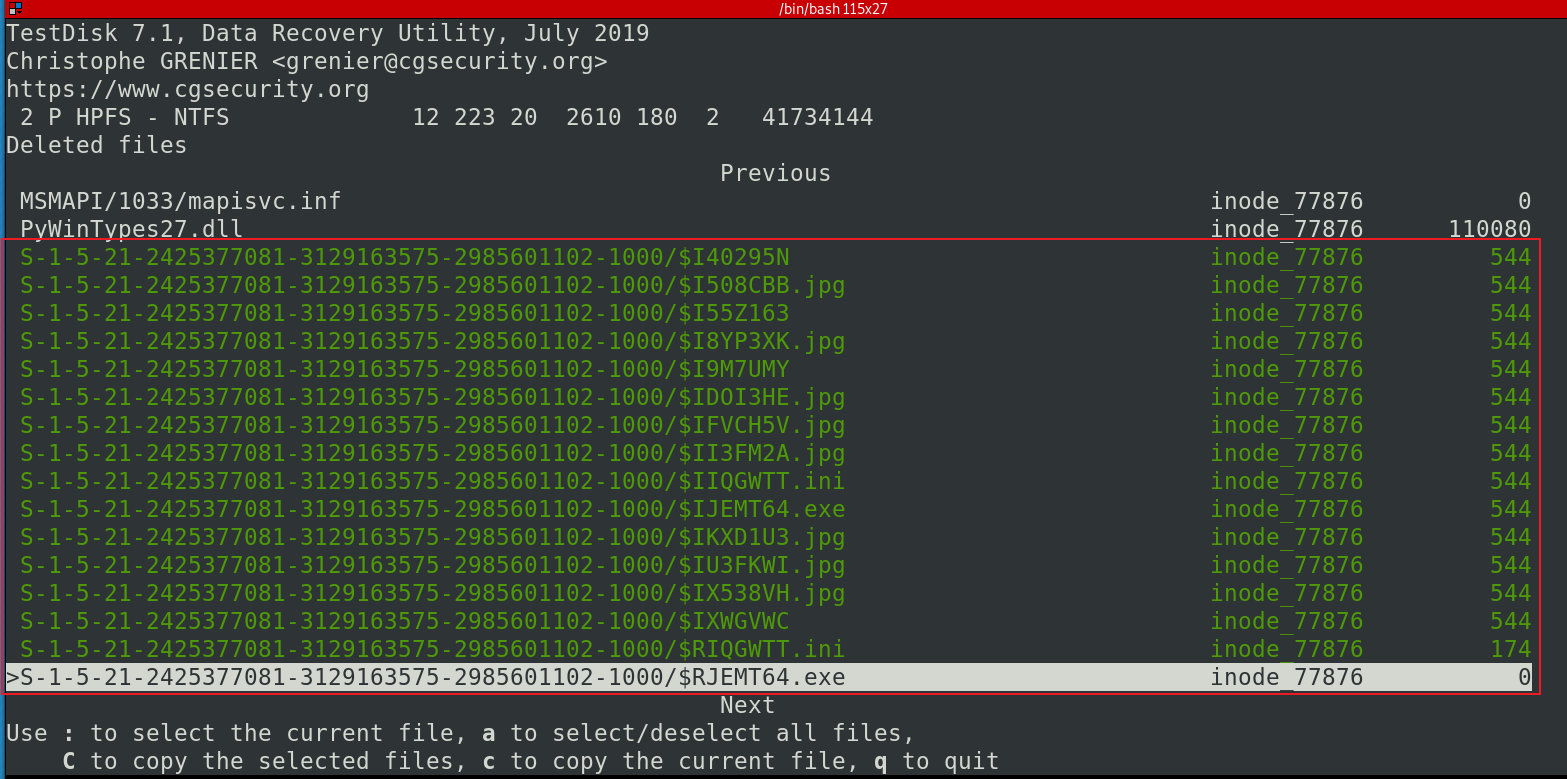
****

****

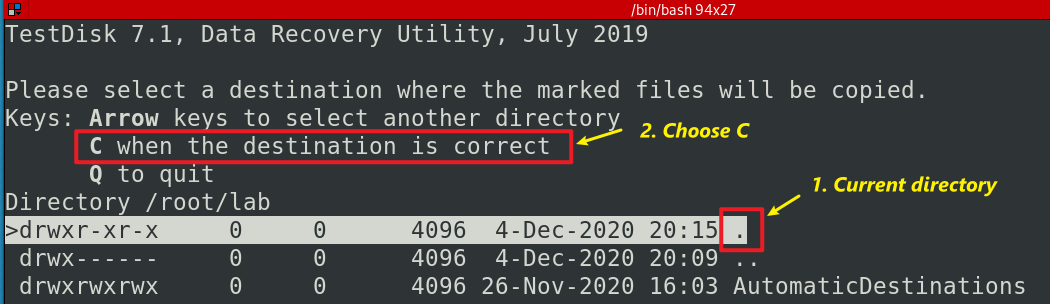
****

****

* Use testDisk to recover files

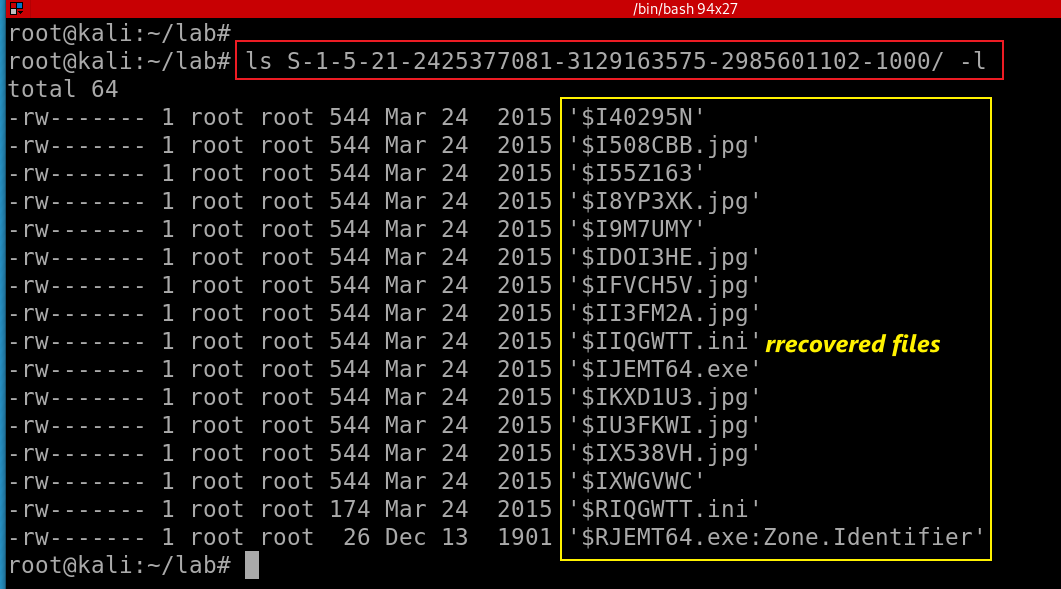
****

* Choose the destination and copy

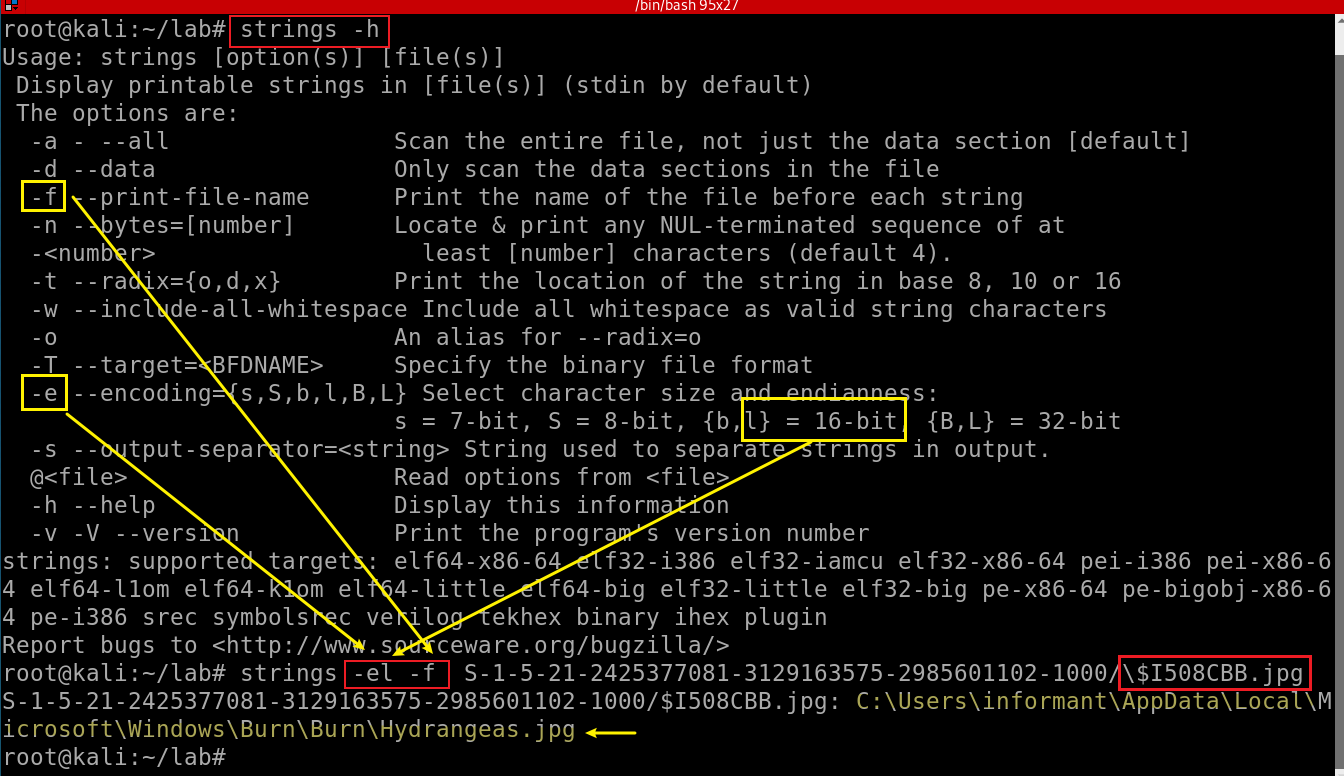
****

Quit all

*ls S-1-5-21-2425377081-3129163575-2985601102-1000/ -l*



* Match random file names with readable file names in the file



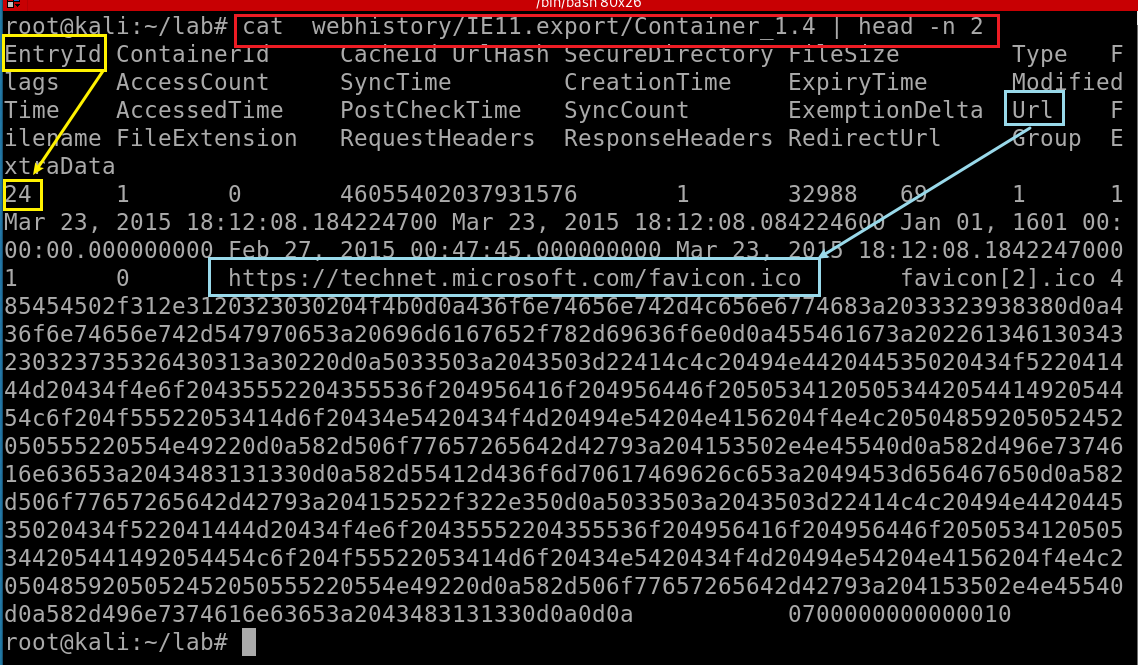
**Examine ‘Recycle Bin’ data in PC :**

|  |  |  |
| --- | --- | --- |
| $I Name | Timestamp Deleted | Original File (or Directory) Path |
| $I40295N | 2015-03-24 15:51:47 | C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\prop |
| ??? | ??? | ??? |
| ??? | ??? | ??? |

1. **What actions were performed for anti-forensics on PC at the last day ‘2015-03-25’?**

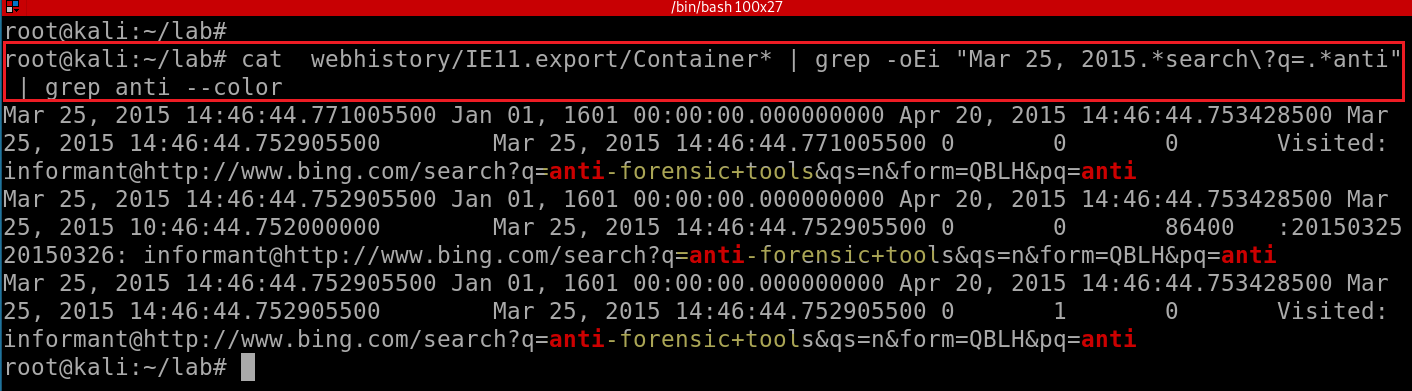
**Step 1.**

* Search IE anti-forensics using keyword



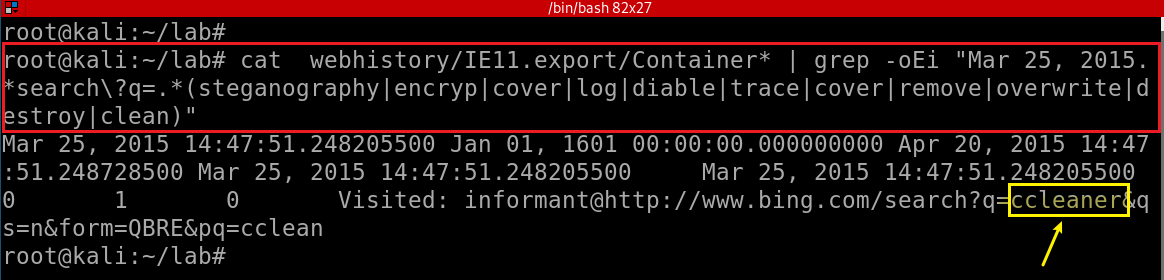
Three tasks:

1. Show all IE history
2. Grep date and with key word “anti”
3. Highlight anti in red



* Search a list of anti-forensic keywords :

***cat webhistory/IE11.export/Container\* | grep -oEi "Mar 25, 2015.\*search\?q=.\*(steganography|encryp|cover|log|diable|trace|cover|remove|overwrite|destroy|clean)"***

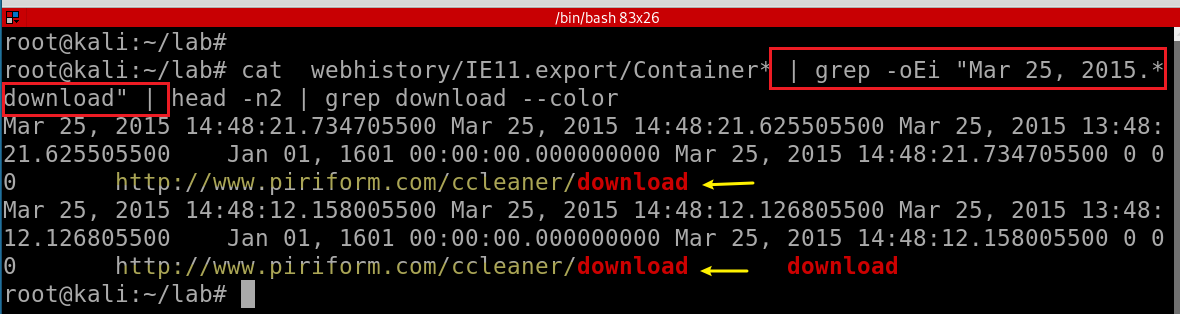


**Step 2.**

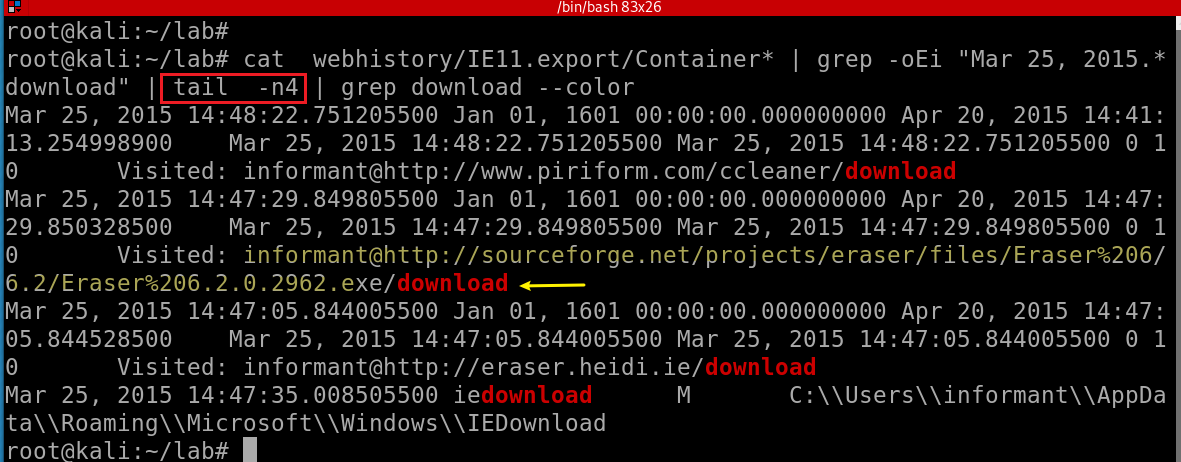
* Search IE download history

Search key word “*download*”, only show first two records for the demonstration purpose :

***cat webhistory/IE11.export/Container\* | grep -oEi "Mar 25, 2015.\*download" | head -n2 | grep download --color***



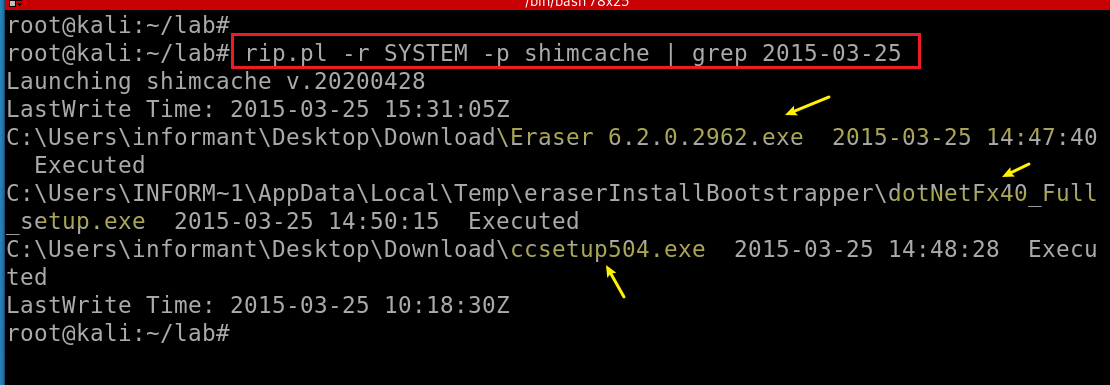
* Search key word “*download*”, only show last four records for the demonstration purpose



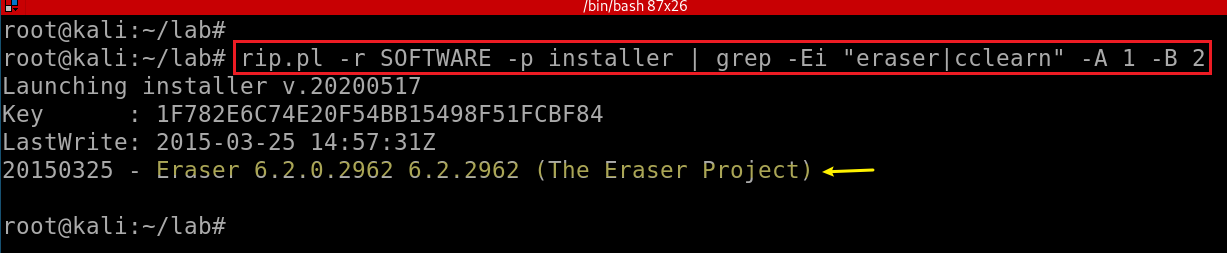
**Step 3.**

* Install download programs- *shimcache*

Check *shimcache* to monitor executed programs



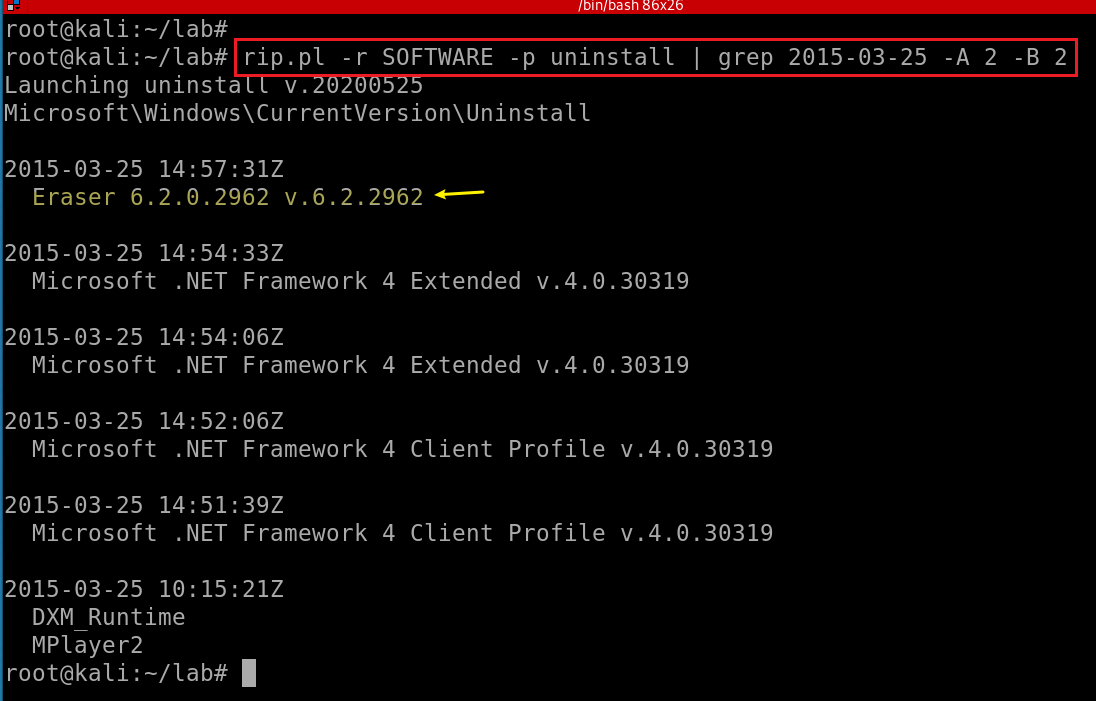
* Check if *eraser* or *cclearner* is managed by Win installer



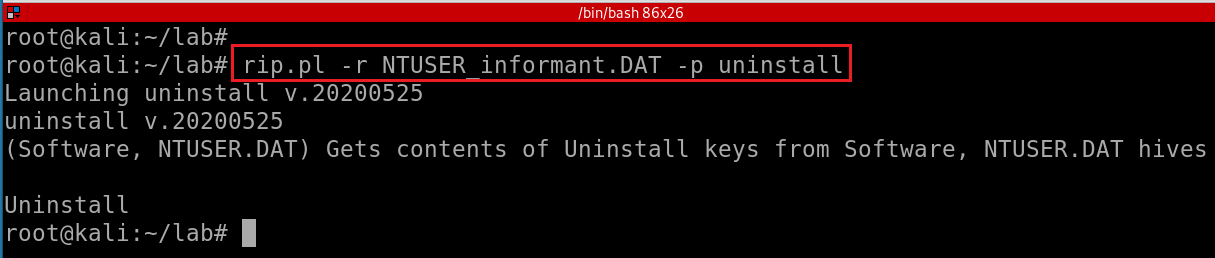
* Check Software registry hive

*rip.pl -r SOFTWARE -p uninstall | grep 2015-03-25 -A 2 -B 2*

*rip.pl -r NTUSER\_informant.DAT -p uninstall | grep 2015-03-25 -A 2 -B 2*



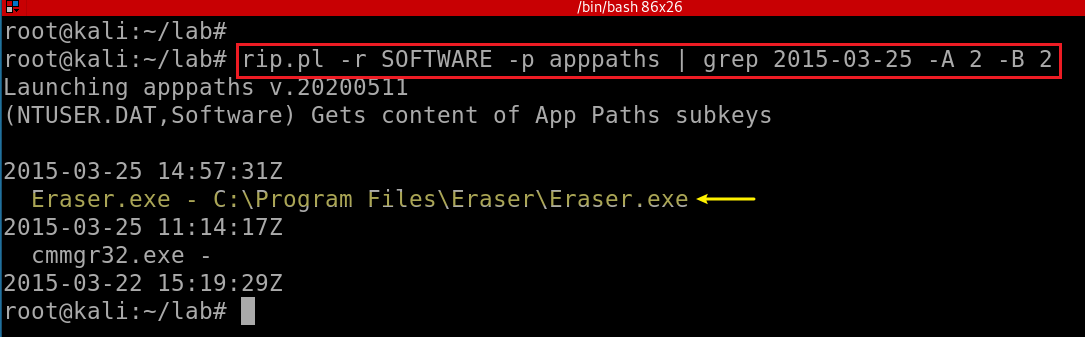
* Check *NTUSER\_informant.DAT* registry hive



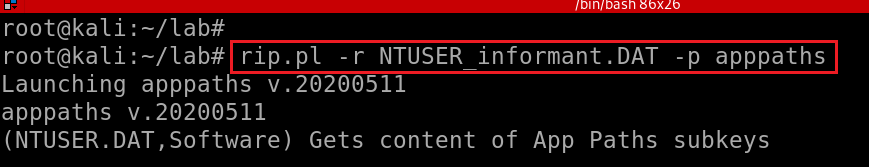
Nothing found

* Check app paths registry

Check Software apppaths

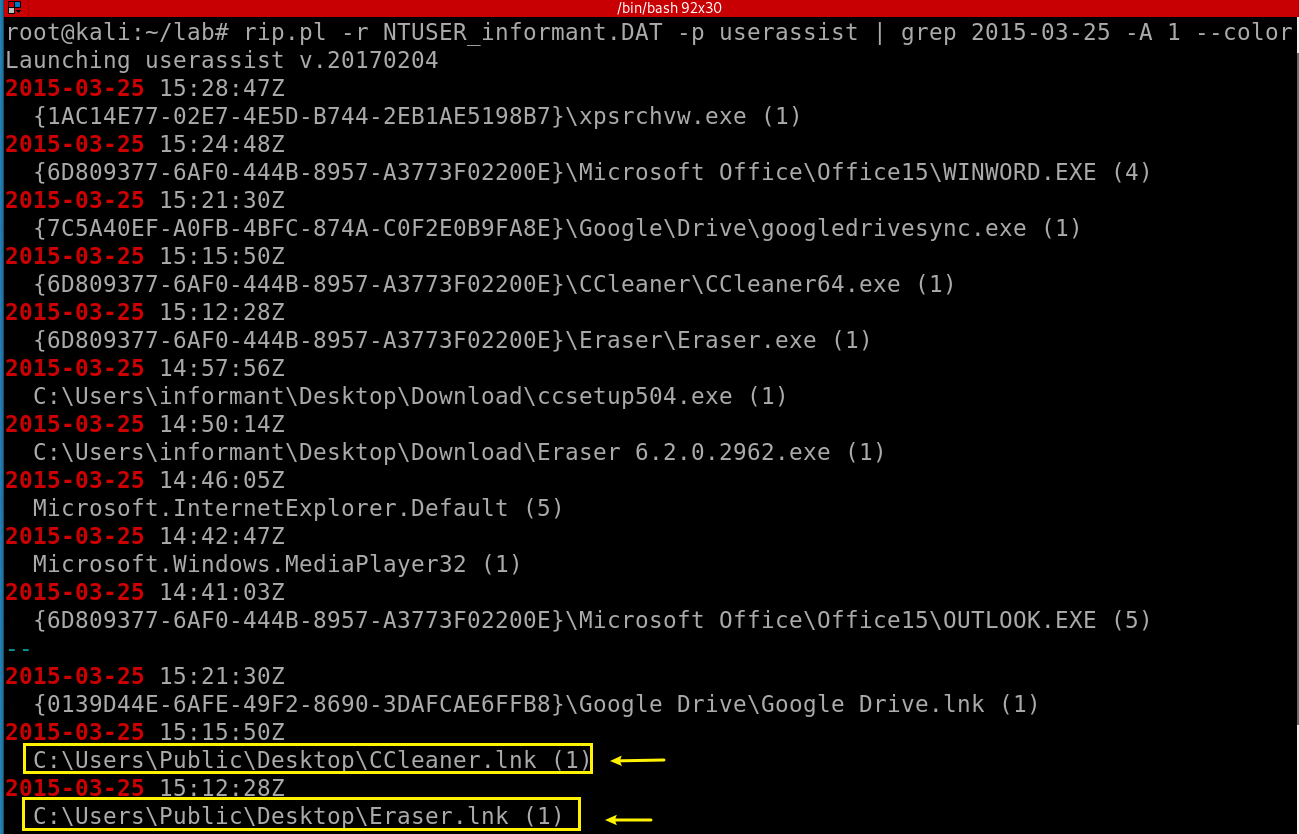


Check NTUSER\_informant apppaths



**Step 4**

* Execute two programs : *userassist*

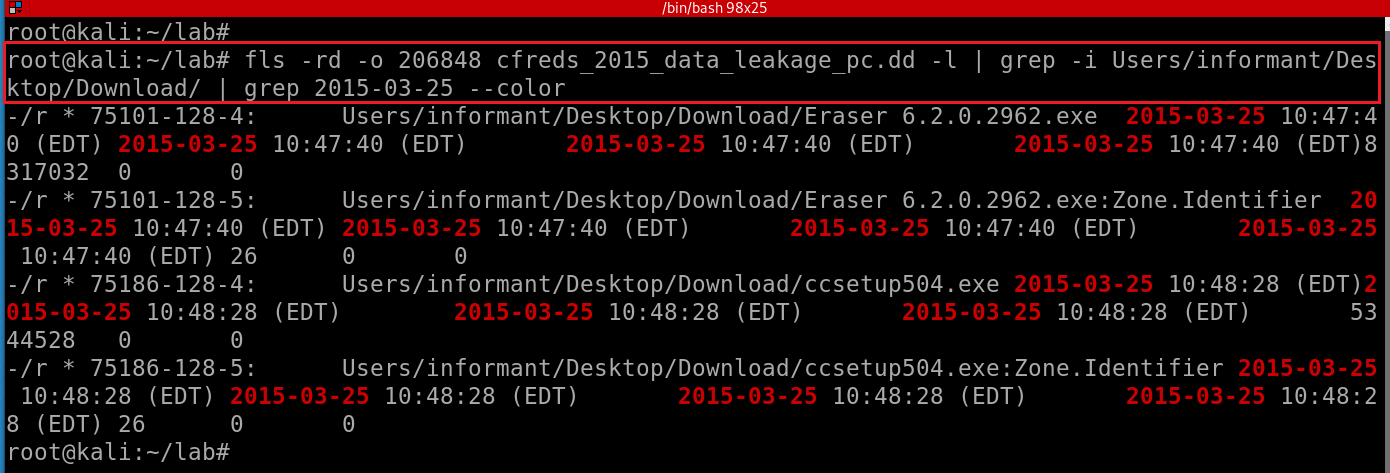


**Step 5**

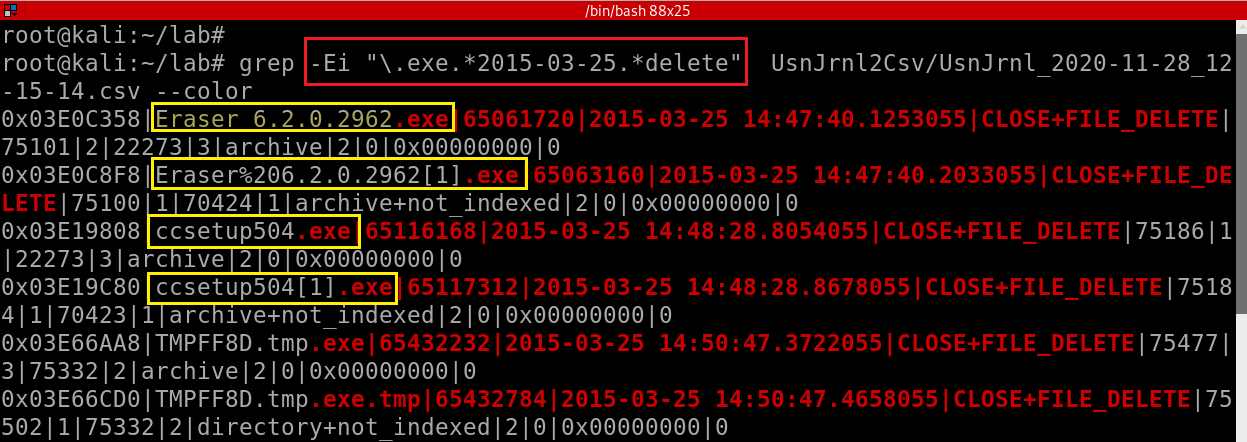
Search for deleted *.exe* files

Only search for 2015-03-25 from Download folder

*fls -rd -o 206848 cfreds\_2015\_data\_leakage\_pc.dd -l | grep -i Users/informant/Desktop/Download/ | grep 2015-03-25 --color*



* Only search for deleted .*exe* from *$UsnJrnl* on 2015-03-25



#### **What actions were performed for anti-forensics on PC at the last day ‘2015-03-25’?**

|  |  |  |
| --- | --- | --- |
| Timestamp | Behavior | Description |
| 2015-03-25 10:46:44 | Search  anti-forensic methods | anti-forensic tools |
| ??? | ??? | ??? |
| ??? | ??? | ??? |

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

Save the document with the filename "**YOUR NAME Lab 7.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 7 From YOUR NAME**", replacing "YOUR NAME" with your real name.