

RONGGUANG OU

LAB 1

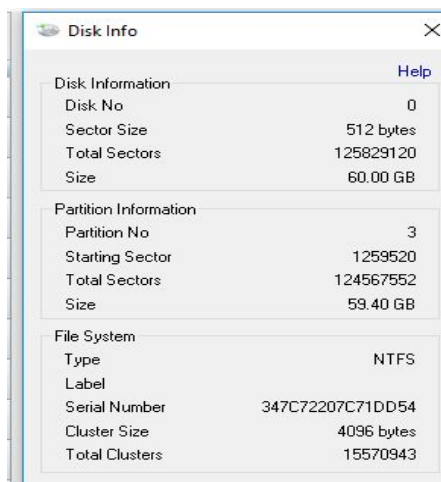
Objective : Practice the uses of modern forensics software to conduct a simple acquisition to reveal target computer information.

Note: Due to the sensitive information on my pc. I have used a VM to simulate this lab. Thank you for your understanding.

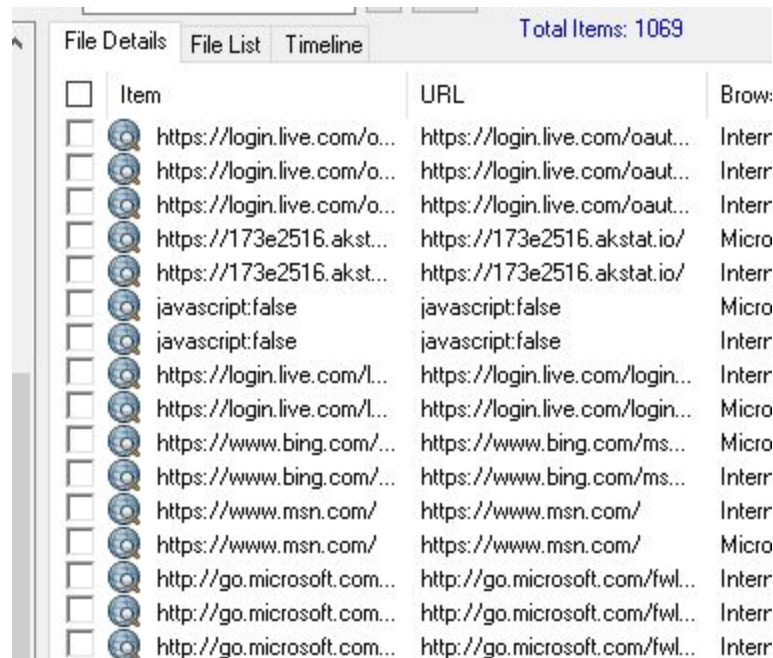
1. There are 5 text files, 2 compressed files, 29 executable files and 65 file composed of different types of configuration files. There are no image files and no deleted files.



2. There is 59.40GB unallocated space for use.



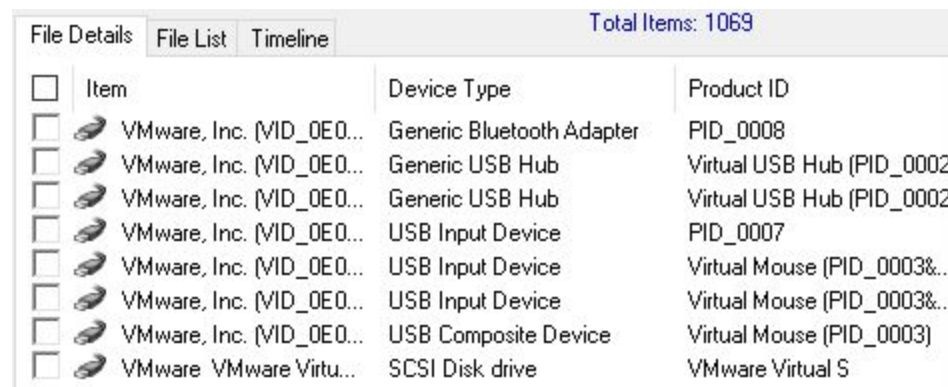
- The top 20 websites visited are login.live.com, 173e2516.akstat.io, bing.com, msn.com and microsoft.com



File Details | File List | Timeline | Total Items: 1069

Item	URL	Brow:
https://login.live.com/o...	https://login.live.com/oauth...	Interr
https://login.live.com/o...	https://login.live.com/oauth...	Interr
https://login.live.com/o...	https://login.live.com/oauth...	Interr
https://173e2516.akst...	https://173e2516.akstat.io/	Micro
https://173e2516.akst...	https://173e2516.akstat.io/	Interr
javascript:false	javascript:false	Micro
javascript:false	javascript:false	Interr
https://login.live.com/l...	https://login.live.com/login...	Interr
https://login.live.com/l...	https://login.live.com/login...	Micro
https://www.bing.com/...	https://www.bing.com/ms...	Micro
https://www.bing.com/...	https://www.bing.com/ms...	Interr
https://www.msn.com/	https://www.msn.com/	Interr
https://www.msn.com/	https://www.msn.com/	Micro
http://go.microsoft.com...	http://go.microsoft.com/fwl...	Interr
http://go.microsoft.com...	http://go.microsoft.com/fwl...	Interr
http://go.microsoft.com...	http://go.microsoft.com/fwl...	Interr

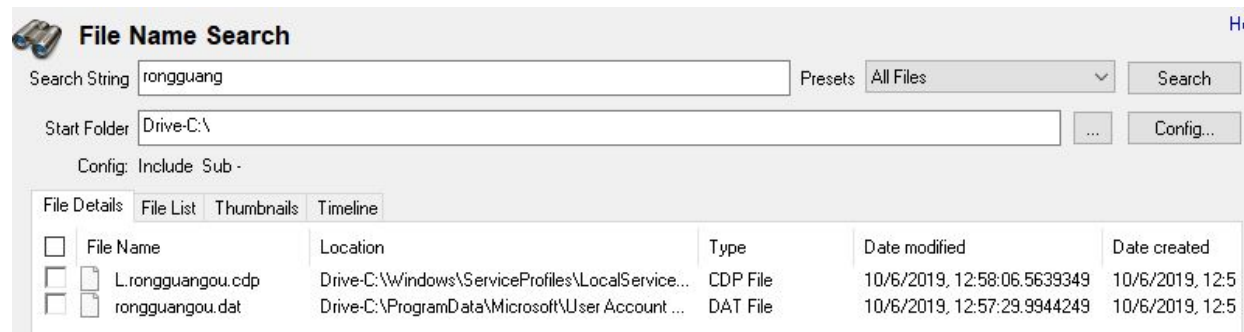
- The type of devices connected to pc is a bluetooth adaptor, generic usb and few usb input devices like mouse and keyboard.



File Details | File List | Timeline | Total Items: 1069

Item	Device Type	Product ID
VMware, Inc. (VID_0E0...	Generic Bluetooth Adapter	PID_0008
VMware, Inc. (VID_0E0...	Generic USB Hub	Virtual USB Hub (PID_0002)
VMware, Inc. (VID_0E0...	Generic USB Hub	Virtual USB Hub (PID_0002)
VMware, Inc. (VID_0E0...	USB Input Device	PID_0007
VMware, Inc. (VID_0E0...	USB Input Device	Virtual Mouse (PID_0003&..
VMware, Inc. (VID_0E0...	USB Input Device	Virtual Mouse (PID_0003&..
VMware, Inc. (VID_0E0...	USB Composite Device	Virtual Mouse (PID_0003)
VMware VMware Virtu...	SCSI Disk drive	VMware Virtual S

- A name search of my name yields two place. One is the service profile and another is user dat file.



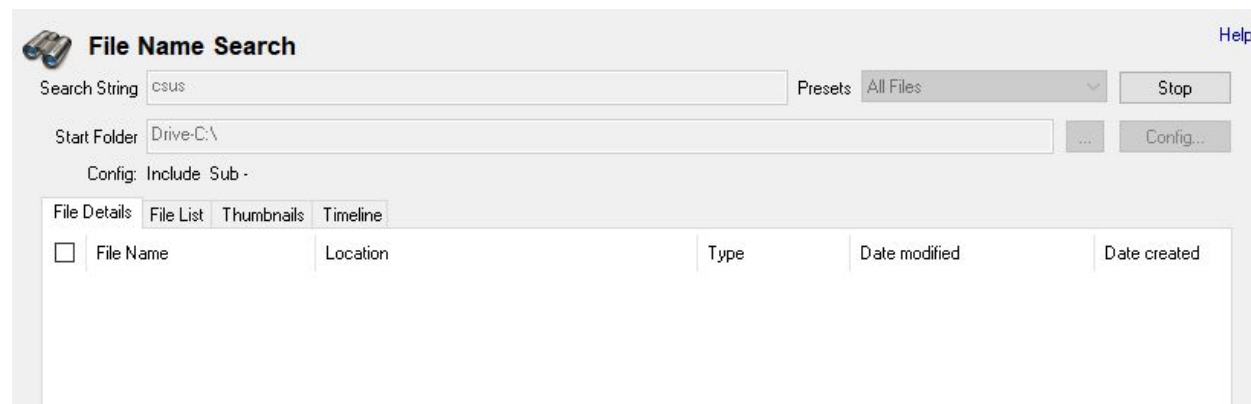
File Name Search

Search String: rongguang | Presets: All Files | Search

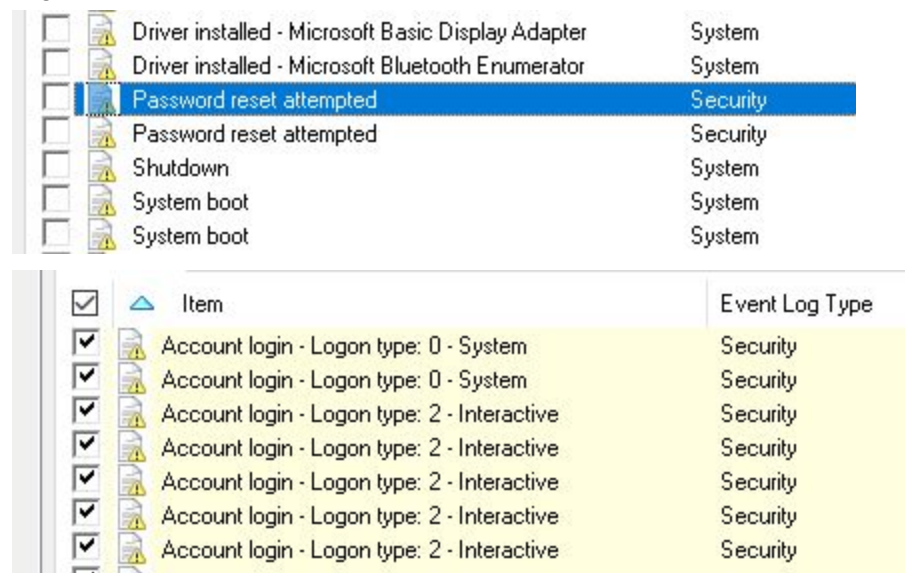
Start Folder: Drive-C:\ | Config: Include Sub -

File Name	Location	Type	Date modified	Date created
L.rongguangou.cdp	Drive-C:\Windows\ServiceProfiles\LocalService...	CDP File	10/6/2019, 12:58:06.5639349	10/6/2019, 12:5
rongguangou.dat	Drive-C:\ProgramData\Microsoft\User Account ...	DAT File	10/6/2019, 12:57:29.9944249	10/6/2019, 12:5

6. A name search of csus contains nothing.



7. The least expected thing I found is that the software can record security logs like account logins, shutdown, bootup log. All which give some status info about what might have happened.



In this lab, I have experienced different types of information can be revealed from OSForensics and I believe other similar types of software will generate similar results. I have a better understanding of user activities like what's in user activities and what kind of information will be logged. Many of the information are highly sensitive and this raise my awareness of the importance of protecting my data.