Worcester Polytechnic Institute
Department of Computer Science

Lab 5-Module 5.1: Extracting unallocated clusters

Objectives

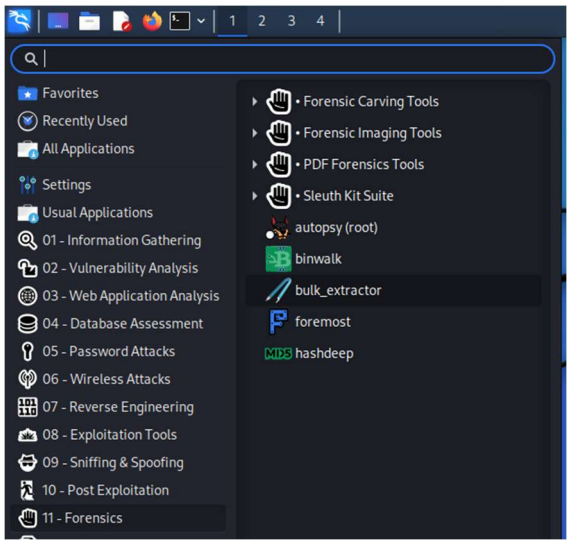
- File carving using Bulk Extractor

Task

Task 1. Software Preparation

1. Download the prepared image - m5t3demo.img to the desktop.

2. Kali linux has pre-installed Bulk Extractor, for other linux distributions, you may need to install Bulk Extractor



Task 2. Prepare configuration file

1. Open the terminal and enter **sudo su**
2. Enter to desktop directory by entering cd Desktop

3. Enter **bulk_extractor -h** to view the help menu
    - In the help menu, you can find the scanners which are enabled.

```
These scanners enabled; disable with -x:
   -x accts - disable scanner accts
     -S ssn_mode=0    0=Normal; 1=No `SSN' required; 2=No dashes required
     -S min_phone_digits=7    Min. digits required in a phone
   -x aes - disable scanner aes
     -S scan_aes_128=1    Scan for 128-bit AES keys; 0=No, 1=Yes
     -S scan_aes_192=0    Scan for 192-bit AES keys; 0=No, 1=Yes
     -S scan_aes_256=1    Scan for 256-bit AES keys; 0=No, 1=Yes
   -x base64 - disable scanner base64
   -x elf - disable scanner elf
   -x email - disable scanner email
   -x evtx - disable scanner evtx
   -x exif - disable scanner exif
     -S exif_debug=0    debug exif decoder
   -x facebook - disable scanner facebook
   -x find - disable scanner find
   -x gps - disable scanner gps
   -x gzip - disable scanner gzip
     -S gzip_max_uncompr_size=268435456    maximum size for decompressing GZIP objects
   -x httplogs - disable scanner httplogs
   -x json - disable scanner json
   -x kml_carved - disable scanner kml_carved
```

- You can also find the scanners which are disabled.

```
These scanners disabled; enable with -e:
   -e base16 - enable scanner base16
   -e hiberfile - enable scanner hiberfile
   -e outlook - enable scanner outlook
   -e wordlist - enable scanner wordlist
     -S word_min=6    Minimum word size
     -S word_max=16    Maximum word size
     -S max_output_file_size=100000000    Maximum size of the words output file
     -S strings=0    Scan for strings instead of words
   -e xor - enable scanner xor
     -S xor_mask=255    XOR mask value, in decimal
```

4. Enter **bulk_extractor -o bulkOutput m5t3demo.img** and wait for the process

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# bulk_extractor -o bulkOutput m5t3demo.img
mkdir "bulkOutput"
bulk_extractor version: 2.0.0
Input file: "m5t3demo.img"
Output directory: "bulkOutput"
Disk Size: 995470848
Scanners: aes base64 elf evtx exif facebook find gzip httplogs json kml_carved msxml net ntfsindx ntfslogfile ntfsmft ntfsusn pdf rar sqlite utmp vcard_carved windirs winlnk winpe winprefetch zip accts email gps
Threads: 8
going multi-threaded ... ( 8 )
bulk_extractor      Mon Nov 14 18:21:17 2022

available_memory: 7338909696
bytes_queued: 0
depth0_bytes_queued: 0
depth0_sbufs_queued: 0
elapsed_time:  0:00:00
estimated_date_completion: 2022-11-14 18:21:16
estimated_time_remaining: n/a
fraction_read: 0.000000 %
max_offset: 0
sbufs_created: 1
sbufs_queued: 0
sbufs_remaining: 1
tasks_queued: 0
thread_count: 8
```

5. If you see the lock icon next to the folder, in the terminal, enter **chmod -R 777 bulkOutput**