Experiment No.: 13

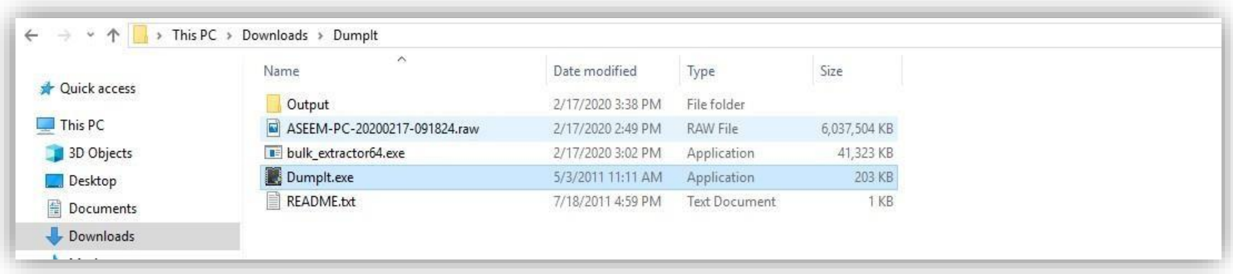
EMAIL FORENSICS

Aim of the Experiment: How to Collect Email Evidence in Victim PC

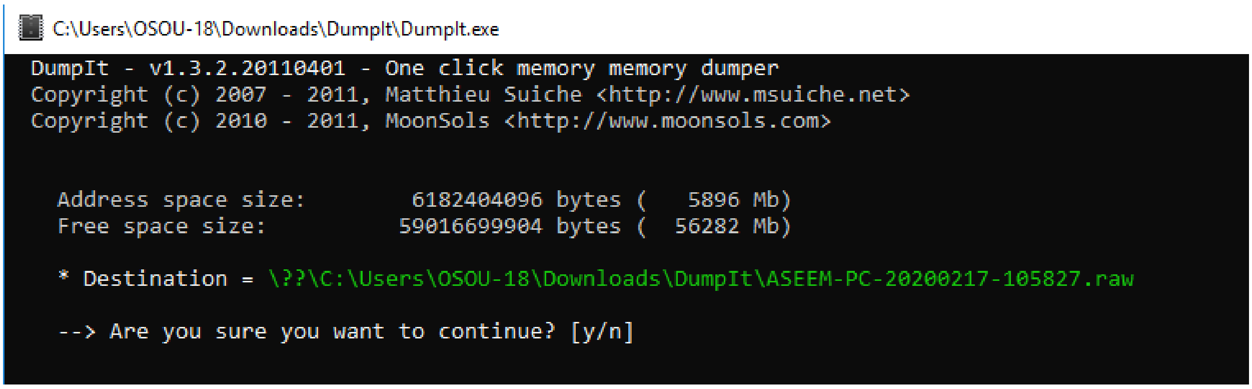
To collect email evidence from Victim PC the first step is to capture the victim's RAM. This can be possible using **dumpit** tool.

This utility is used to generate a physical memory dump of Windows machines. It works with both x86 (32-bits) and x64 (64-bits) machines. The raw memory dump isgenerated in the current directory, only a confirmation question is prompted before starting. Perfect to deploy the executable on USB keys, for quick incident responses needs.

Run **Dumpit.exe** file the raw memory dump will be generated and save to the same directory

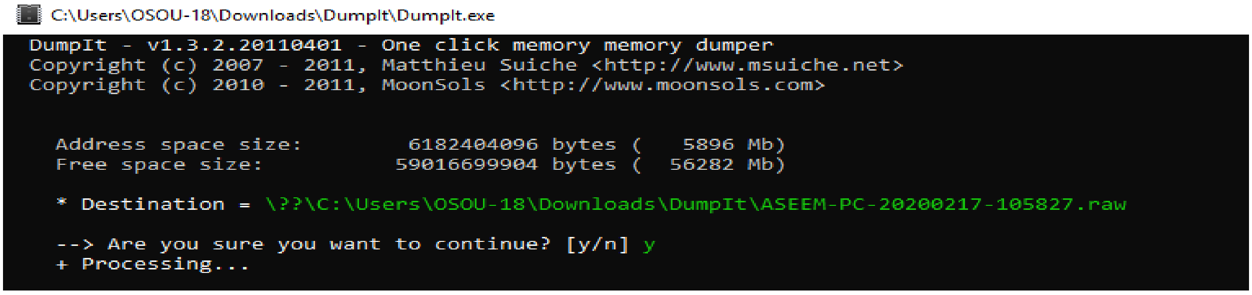


Name	Date modified	Type	Size
Output	2/17/2020 3:38 PM	File folder	
ASEEM-PC-20200217-091824.raw	2/17/2020 2:49 PM	RAW File	6,037,504 KB
bulk_extractor64.exe	2/17/2020 3:02 PM	Application	41,323 KB
DumpIt.exe	5/3/2011 11:11 AM	Application	203 KB
README.txt	7/18/2011 4:59 PM	Text Document	1 KB



```
DumpIt - v1.3.2.20110401 - One click memory memory dumper
Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msuiche.net>
Copyright (c) 2010 - 2011, MoonSols <http://www.moonsols.com>


  Address space size:        6182404096 bytes (   5896 Mb)
  Free space size:          59016699904 bytes (  56282 Mb)

  * Destination = \??\C:\Users\OSOU-18\Downloads\DumpIt\ASEEM-PC-20200217-105827.raw

  --> Are you sure you want to continue? [y/n]
```

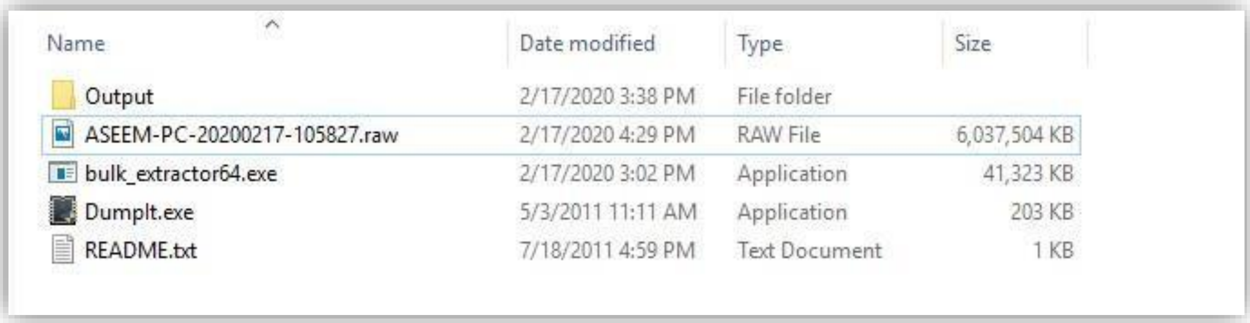
Write **'Y'** for processing



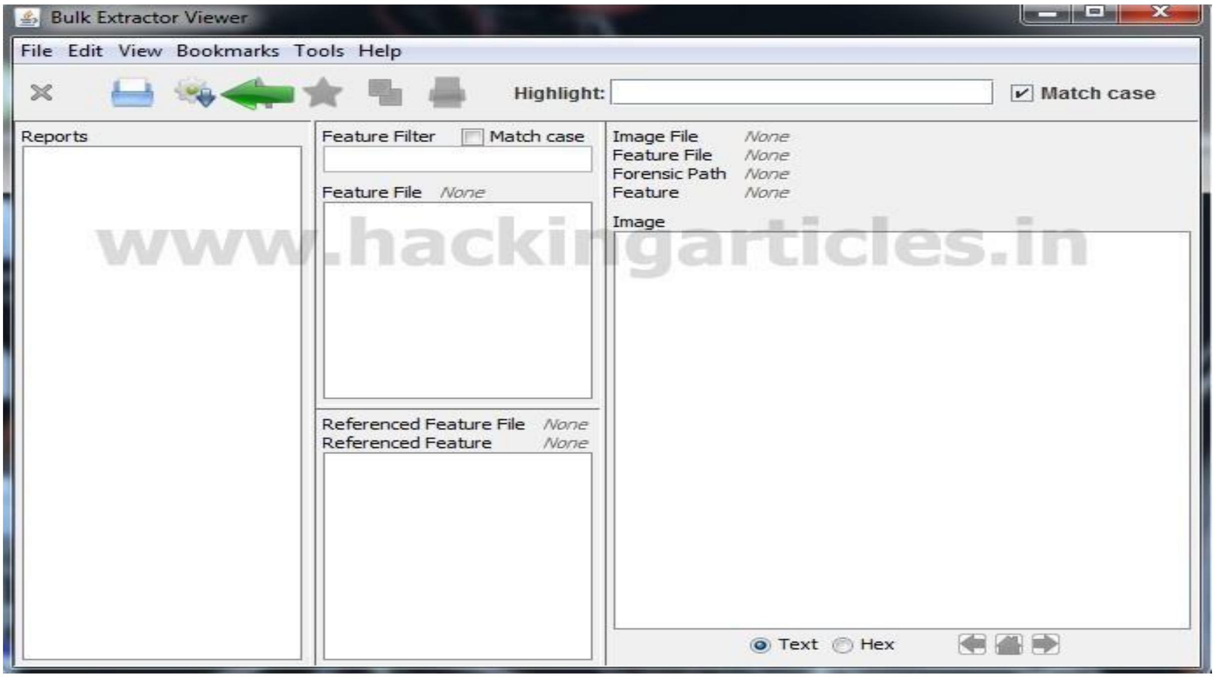
```
DumpIt - v1.3.2.20110401 - One click memory memory dumper
Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msuiche.net>
Copyright (c) 2010 - 2011, MoonSols <http://www.moonsols.com>


  Address space size:        6182404096 bytes (   5896 Mb)
  Free space size:          59016699904 bytes (  56282 Mb)

  * Destination = \??\C:\Users\OSOU-18\Downloads\DumpIt\ASEEM-PC-20200217-105827.raw

  --> Are you sure you want to continue? [y/n] y
  + Processing...
```

The output .RAW file will be as follows

Then Download **bulk extractor viewer** from GitHub and install it in your PC. Now open bulkextractor viewer and click on to **generate report**.



Name	Date modified	Type	Size
Output	2/17/2020 3:38 PM	File folder	
ASEEM-PC-20200217-105827.raw	2/17/2020 4:29 PM	RAW File	6,037,504 KB
bulk_extractor64.exe	2/17/2020 3:02 PM	Application	41,323 KB
DumpIt.exe	5/3/2011 11:11 AM	Application	203 KB
README.txt	7/18/2011 4:59 PM	Text Document	1 KB

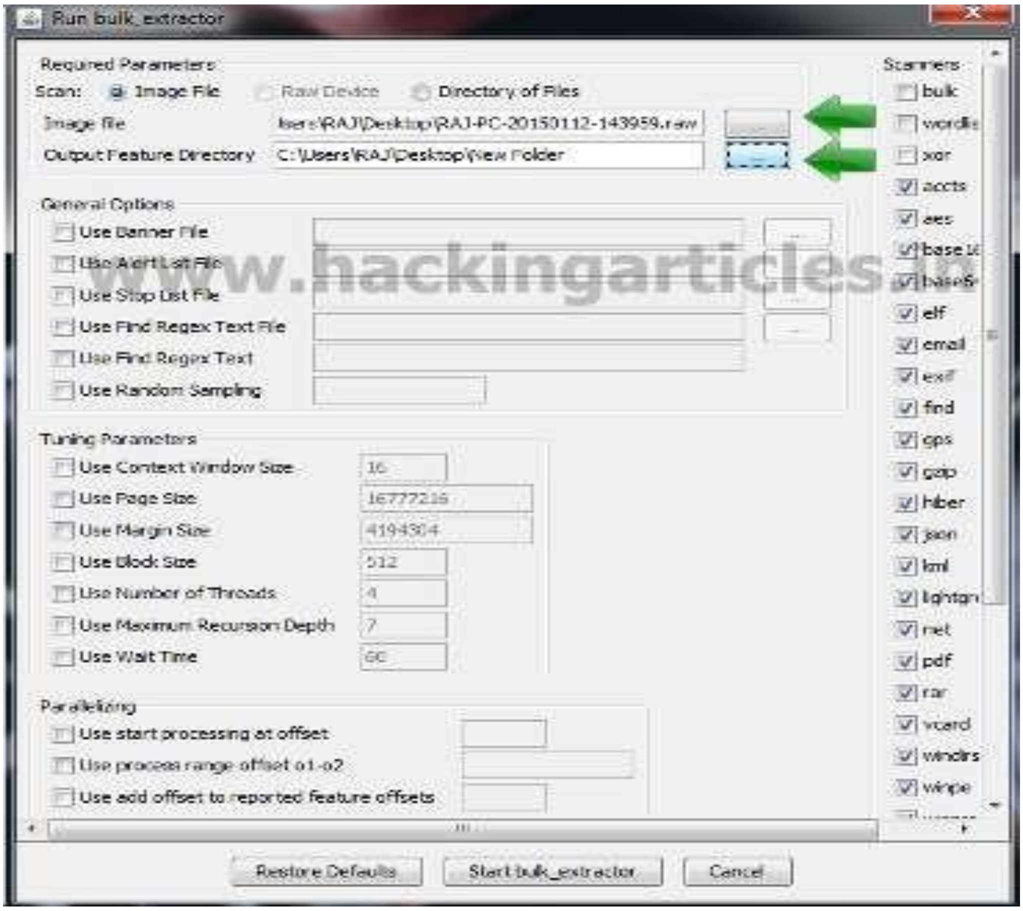


Feature File None

Image File None
Feature File None
Forensic Path None
Feature None
Image

Referenced Feature File None
Referenced Feature None

Now select the dump it image file and select an output folder for the report and click on startbulk extractor as seen below



Required Parameters

Scan: ● Image File ○ Raw Device ○ Directory of Files

Image file: lsers\RAJ\Desktop\RAJ-PC-20150112-143959.raw

Output Feature Directory: C:\Users\RAJ\Desktop\New Folder

General Options

- □ Use Banner File
- □ Use Alert List File
- □ Use Stop List File
- □ Use Find Regex Text File
- □ Use Find Regex Text
- □ Use Random Sampling

Tuning Parameters

- □ Use Context Window Size 16
- □ Use Page Size 16777216
- □ Use Margin Size 4194304
- □ Use Block Size 512
- □ Use Number of Threads 4
- □ Use Maximum Recursion Depth 7
- □ Use Wait Time 60

Parallelizing

- □ Use start processing at offset
- □ Use process range offset o1-o2
- □ Use add offset to reported feature offsets

Scanners

- □ bulk
- □ wordlis
- □ xor
- ☑ accts
- ☑ aes
- ☑ base16
- ☑ base64
- ☑ elf
- ☑ email
- ☑ exif
- ☑ find
- ☑ gps
- ☑ gzip
- ☑ hiber
- ☑ json
- ☑ kml
- ☑ lightgr
- ☑ net
- ☑ pdf
- ☑ rar
- ☑ vcard
- ☑ windirs
- ☑ winpe

Now in order to investigate the victim saved information of Email ID Click on email.txt as seenbelow

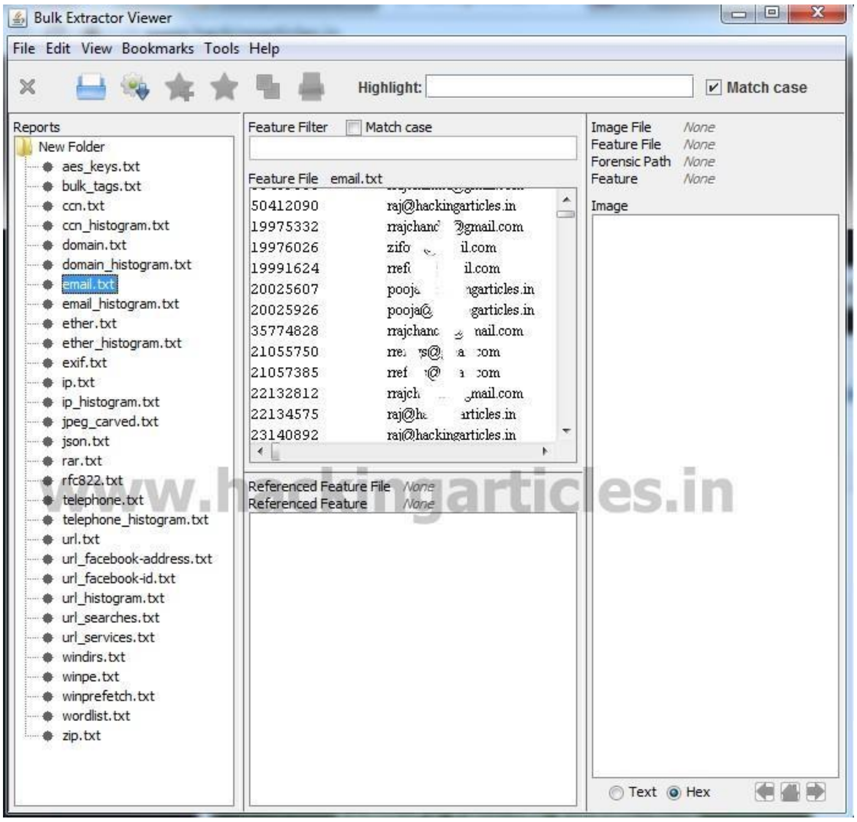


Image File None
Feature File None
Forensic Path None
Feature None

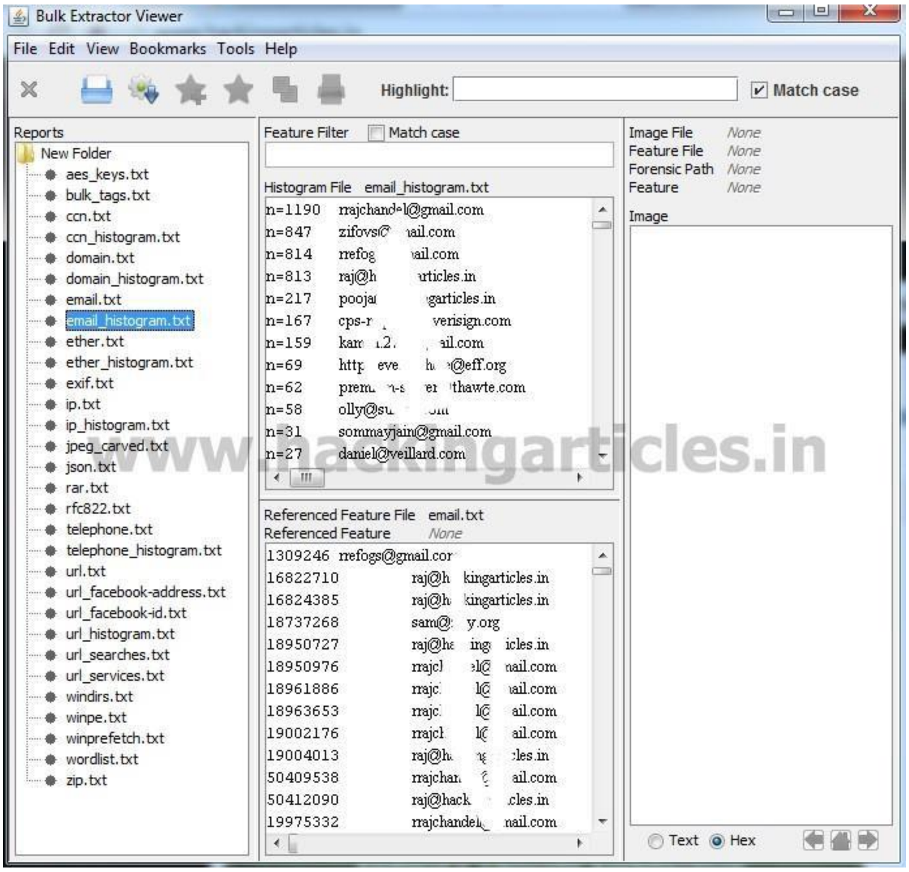
Reports

- New Folder
  - aes_keys.txt
  - bulk_tags.txt
  - ccn.txt
  - ccn_histogram.txt
  - domain.txt
  - domain_histogram.txt
  - email.txt
  - email_histogram.txt
  - ether.txt
  - ether_histogram.txt
  - exif.txt
  - ip.txt
  - ip_histogram.txt
  - jpeg_carved.txt
  - json.txt
  - rar.txt
  - rfc822.txt
  - telephone.txt
  - telephone_histogram.txt
  - url.txt
  - url_facebook-address.txt
  - url_facebook-id.txt
  - url_histogram.txt
  - url_searches.txt
  - url_services.txt
  - windirs.txt
  - winpe.txt
  - winprefetch.txt
  - wordlist.txt
  - zip.txt

Feature File email.txt

```
50412090    raj@hackingarticles.in
19975332    rrajchanc  @gmail.com
19976026    zifo      il.com
19991624    rrefi     il.com
20025607    pooja     ngarticles.in
20025926    pooja@    garticles.in
35774828    rrajchanc   nail.com
21055750    rre  s@   a  com
21057385    rref  @   a  com
22132812    rrajch     mail.com
22134575    raj@ha    articles.in
23140892    raj@hackingarticles.in
```

And also click on email_histogram.txt



```
New Folder
  aes_keys.txt
  bulk_tags.txt
  ccn.txt
  ccn_histogram.txt
  domain.txt
  domain_histogram.txt
  email.txt
  email_histogram.txt
  ether.txt
  ether_histogram.txt
  exif.txt
  ip.txt
  ip_histogram.txt
  jpeg_carved.txt
  json.txt
  rar.txt
  rfc822.txt
  telephone.txt
  telephone_histogram.txt
  url.txt
  url_facebook-address.txt
  url_facebook-id.txt
  url_histogram.txt
  url_searches.txt
  url_services.txt
  windirs.txt
  winpe.txt
  winprefetch.txt
  wordlist.txt
  zip.txt
```

Histogram File   email_histogram.txt

```
n=1190   rrajchandel@gmail.com
n=847    zifovs@    ail.com
n=814    rrefog      ail.com
n=813    raj@h       rticles.in
n=217    pooja        garticles.in
n=167    cps-r          verisign.com
n=159    kam  1.2.      ail.com
n=69     http  eve    h   @eff.org
n=62     prem.  n-s   er  thawte.com
n=58     olly@su
n=31     sommayjain@gmail.com
n=27     daniel@veillard.com
```

Referenced Feature File   email.txt
Referenced Feature   None

```
1309246  rrefogs@gmail.cor
16822710          raj@h   kingarticles.in
16824385          raj@h   kingarticles.in
18737268          sam@    y.org
18950727          raj@ha   ing   icles.in
18950976          rrajcl     el@   nail.com
18961886          rrajc       l@   ail.com
18963653          rrajc       l@    ail.com
19002176          rrajcl      l@    ail.com
19004013          raj@h.           les.in
50409538          rrajchan          ail.com
50412090          raj@hack        cles.in
19975332          rrajchandel     nail.com
```

Image File   None
Feature File   None
Forensic Path   None
Feature   None