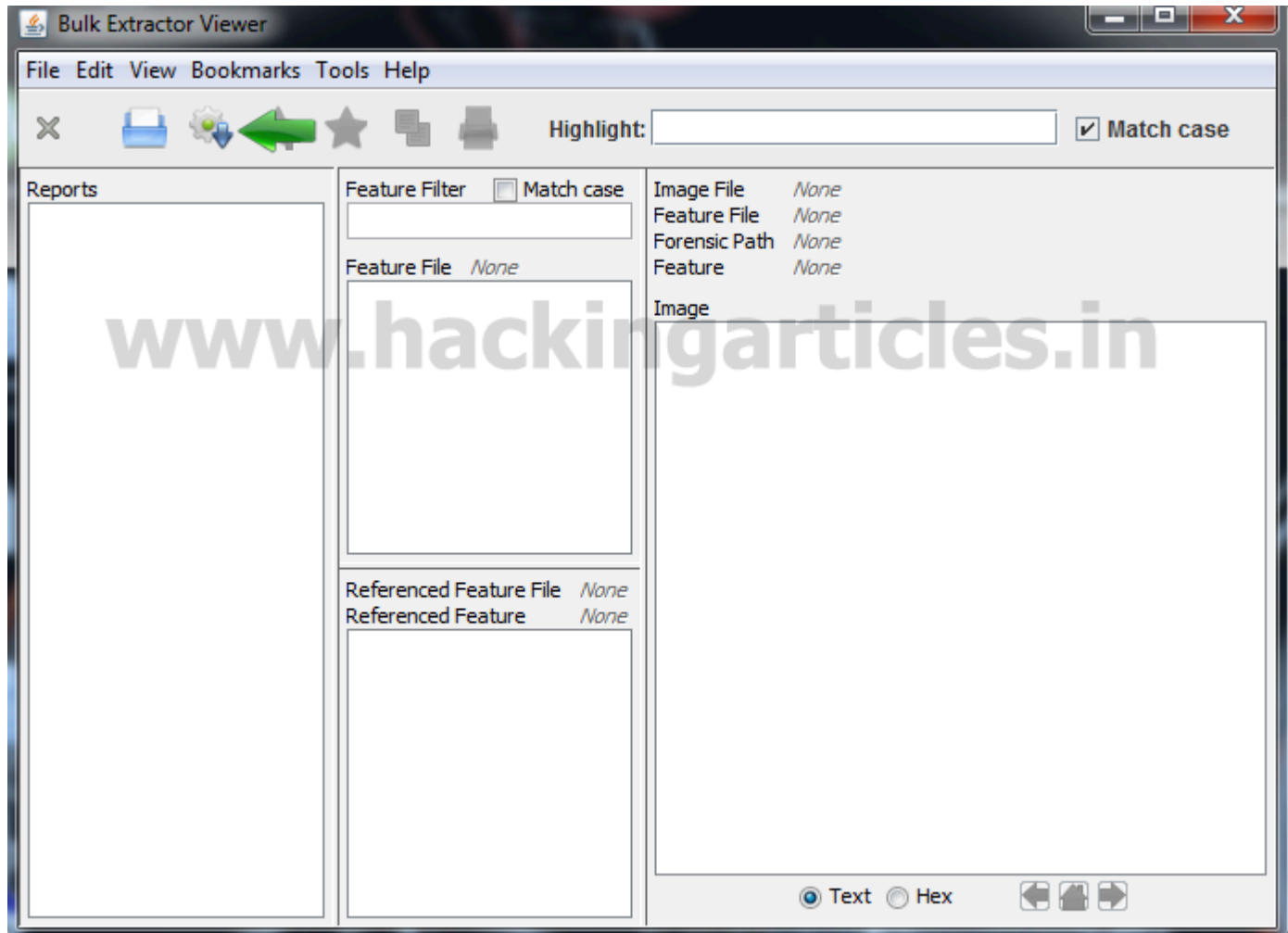# How to Collect Email Evidence in Victim PC (Email Forensics)

January 14, 2015   By Raj Chandel

First capture the victim's ram using dump it tool. (For details visit **here**)

Download bulk extractor viewer (from **here**) and install it in your PC.

Now open bulk extractor viewer and click on to generate report

Now select the dump it image file and select an output folder for the report and click on start bulk extractor as seen below
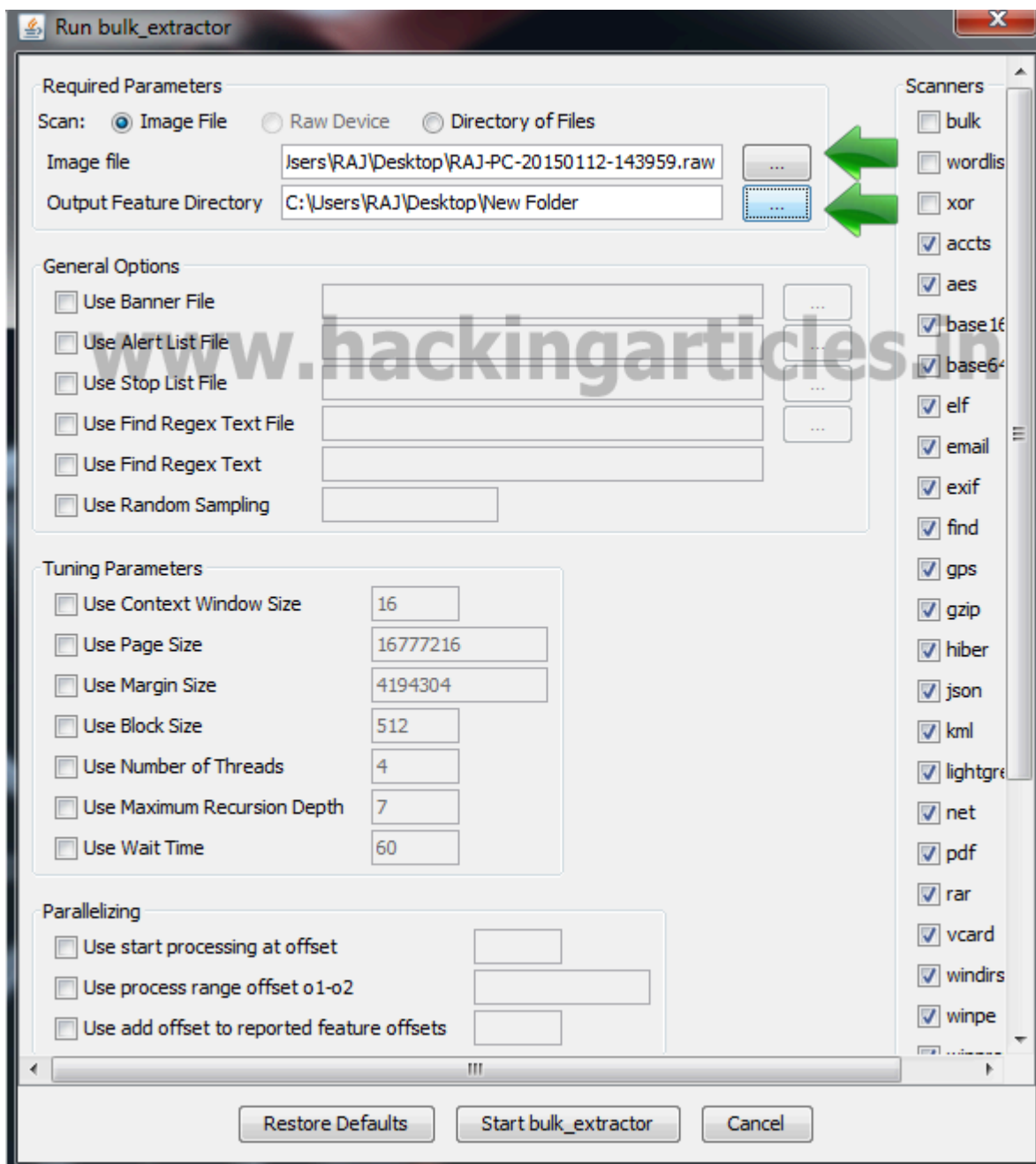
Now in order to investigate the victim saved information of Email ID Click on **email.txt** as seen below

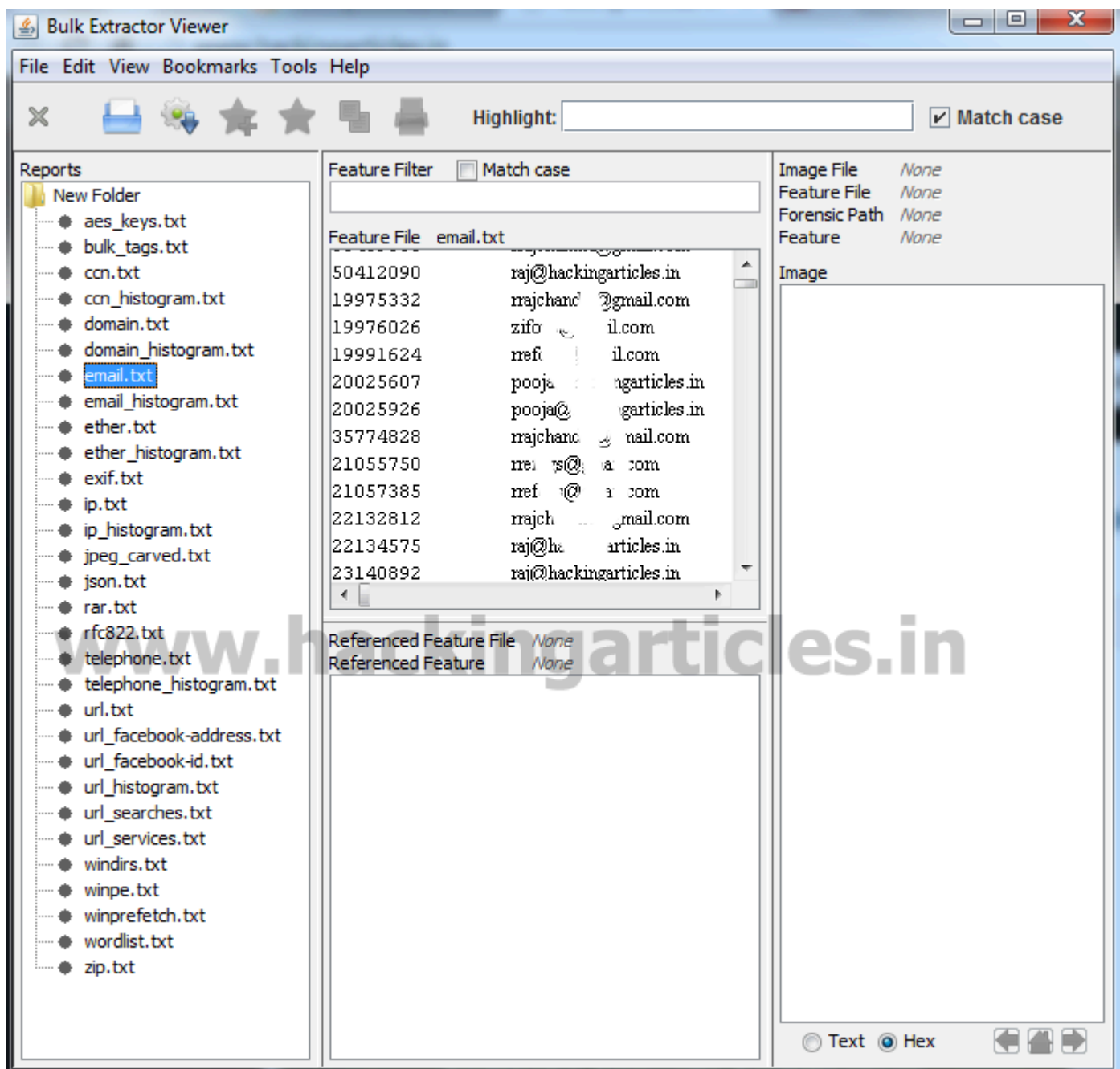And also click on **email_histogram.txt**

Bulk Extractor Viewer

File Edit View Bookmarks Tools Help

Highlight: [   ] ☑ Match case

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 Filter ☐ Match case
[   ]

Histogram File   email_histogram.txt

n=1190	rajchandel@gmail.com
n=847	zifovs@ ail.com
n=814	rrefog ail.com
n=813	raj@h articles.in
n=217	pooja garticles.in
n=167	cps-r verisign.com
n=159	kam .2. ail.com
n=69	http eve h @eff.org
n=62	prem s er thawte.com
n=58	olly@su om
n=31	sommayjain@gmail.com
n=27	daniel@veillard.com

www.hackingarticles.in

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	rrajch l@ ail.com
19004013	raj@ha ng cles.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*

Image

○ Text ● Hex