Experiment No.8
To use bulk_extractor tool to detect Evidence related to email
Date of Performance:
Date of Submission:

Aim: To use bulk_extractor tool to detect Evidence related to email

Objective: To make use of the bulk_extractor tool to recover email related evidence from a disk image

Theory:

Bulk_extractor is a C++ program that scans a disk image, a file, or a directory of files and extracts useful information without parsing the file system or file system structures. The results are stored in feature files that can be easily inspected, parsed, or processed with automated tools. bulk_extractor also creates histograms of features that it finds, as features that are more common tend to be more important.

Bulk Email Extractor is also an email client manager. The software provides a streamlined extraction of email. It supports every online email service on the internet. This helps users process all email addresses in an efficient and automated manner.

Bulk Email Extractor is created to handle tons of emails addresses. Collecting email addresses is a monumental job for anyone. Piled-up messages from clients and accounts can be a good source of email addresses. Some of them could be not existing or fake and most users don't have the luxury of checking individual email addresses. It will take several hours until all email addresses are collected and sorted out. This software is capable of extracting large amounts of email addresses. It runs within minutes compared to the manual opening of contact addresses. Any online email services or business directory websites are supported by this software and it even supports websites with email listings.

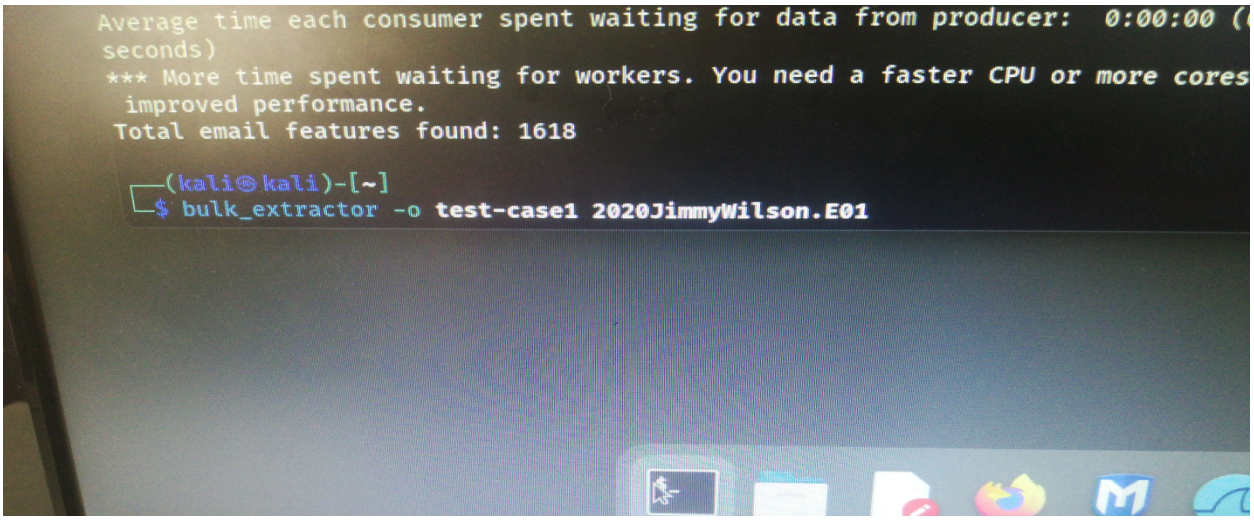


Fig. 8.1 View of Bulk_Extractor

Process:

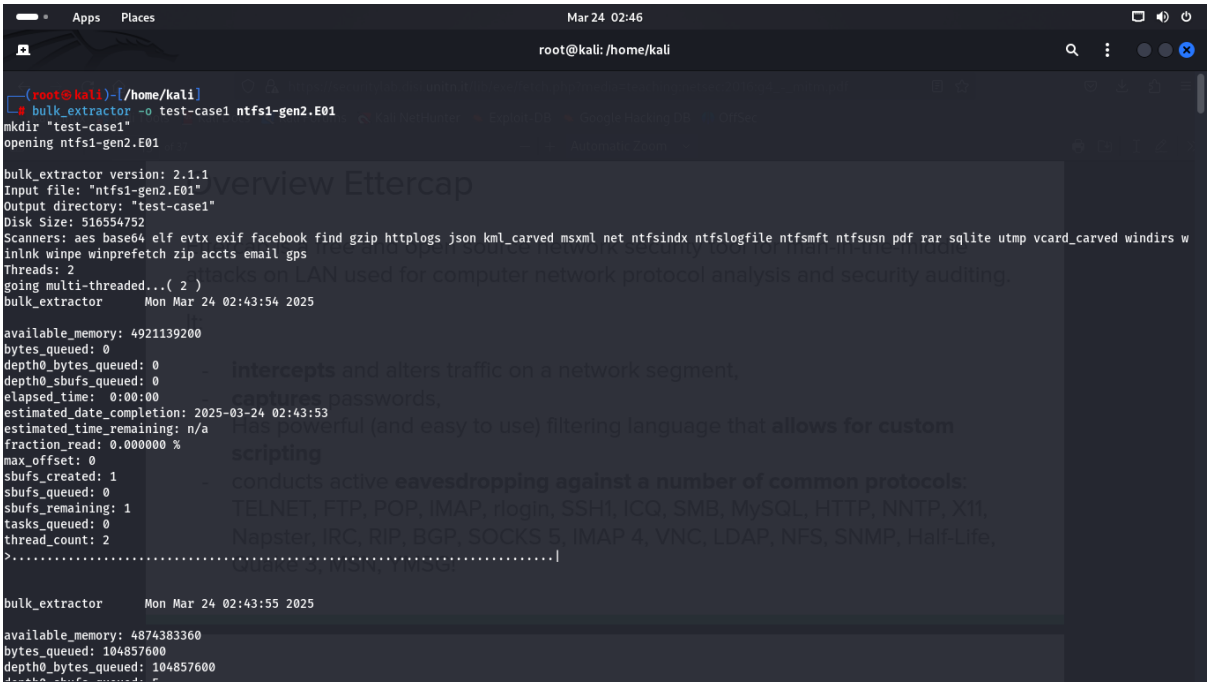
Step 1, open the Bulk_extractor tool in kali Linux

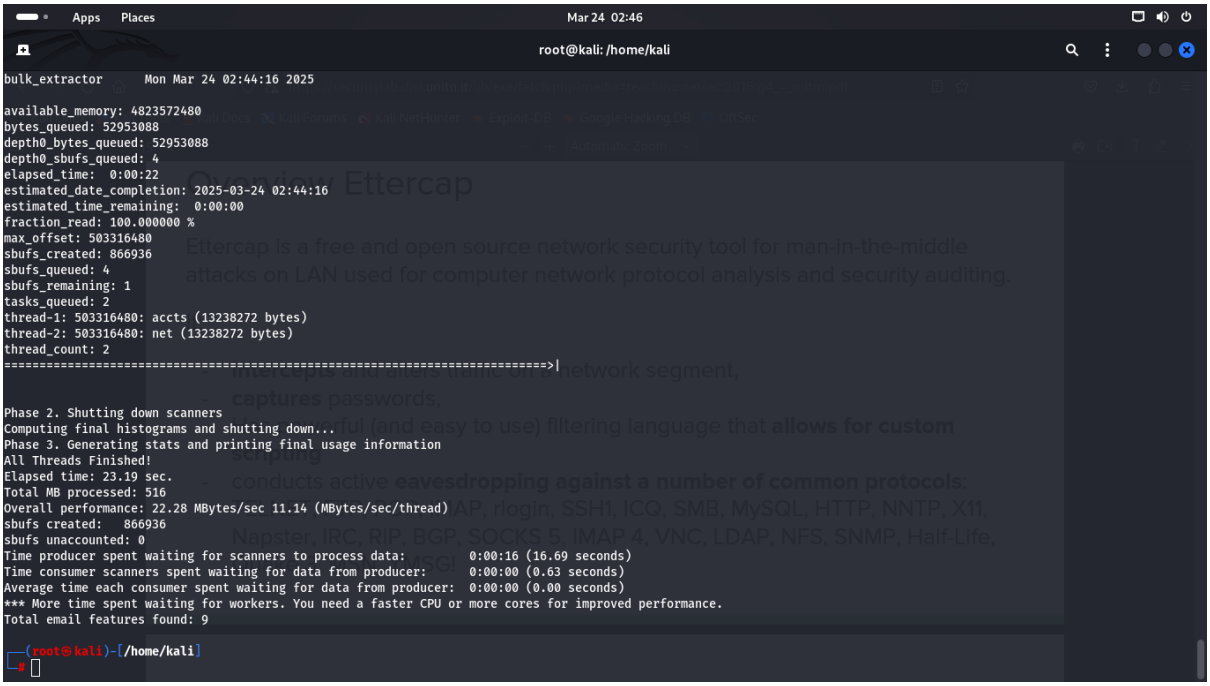
Step 2. create or download the mirror image of the hard disk

Step 3. use the command as shown in figure 8.1

Step 4. open the output file to see email evidence

Output:






```
# BANNER FILE NOT PROVIDED (-b option)
# BULK_EXTRACTOR-Version: 2.1.1
# Feature-Recorder: email
# Filename: ntfs1-gen2.E01
# Feature-File-Version: 1.1
47346547        xL6@3ov.KE      ^g\214\007t\344g'DF'\230\230\364F\264\204xL6@3ov.KE\343\341#\275\231\014\357&\213&u\226\203\350&\227
239767510-PDF-392       btinfo@bottomline.com   .bottomline.com btinfo@bottomline.com  Paybase Allows
239767510-PDF-1681      info@entegrity.com      w.entegrity.com info@entegrity.com Equifax E-Banki
239772263-PDF-1084      paul.wrenn@hicor.net    4 www.hicor.net paul.wrenn@hicor.net Mellon Global C
239772263-PDF-1296      gcm_direct_pgh@mellon.com       n.com/inst/gcm/ gcm_direct_pgh@mellon.com National City C
239772263-PDF-1673      mark_d_schulte@national-city.com        14 216-222-3633 mark_d_schulte@national-city.com \134(continued\134
239776426-PDF-437       gigiw@paytec.com        55 717-506-2200 gigiw@paytec.com Politzer & Hane
239776426-PDF-1747      ed_armstrong@stercomm.com       ingcommerce.com ed_armstrong@stercomm.com \134(continued\134
239780882-PDF-812       patricia.engelage@umb.com       045 www.umb.com patricia.engelage@umb.com
```

Conclusion:

The Bulk_extractor tool is highly significant in digital forensic investigations, especially for extracting email-related evidence. Its ability to scan raw disk images without relying on file system structures allows investigators to recover hidden or deleted email addresses and communication traces efficiently. By automatically parsing through large volumes of data and generating feature-rich output files, Bulk_extractor simplifies the process of identifying communication patterns, contacts, and potential leads. This makes it a valuable asset in cases involving email fraud, identity theft, cyberstalking, or any scenario where email communication plays a crucial role.