4. Implementation

4.1 Introduction

In this section, we shall discuss how the proposed solution was implemented, algorithms that are used and how this tool can be used by investigator. Investigator just needs to install our tool on his/her own system and run GUI.py file. In order to utilize various features of this tool; investigator have to follow some guideline which are provided in "Guidelines" section at the end of this chapter.

Our proposed tool has three independent modules - 1) Web Forensics 2) Network Forensics 3) Email forensics. User can choose any of the above based on his/her requirement. Evidences which are analyzed include pcap files, email content and chrome browser. Once the analysis is done, report is generated which can be saved on local system or can be viewed anytime.

Web Forensics module implicitly collects data from browser, analyze this data and generate independent report for cookies, history, downloads and time-liner. Network Forensics module takes pcap file as input, analyze all the packets, detect attacks and generate report. This module also captures live traffic from ethernet port. Email Forensics module takes email body as input and generate report based on whether the email content is malicious or not.

4.2 Environmental Setup

4.2.1 Hardware Requirement

1. System: Pentium IV 2.4 GHz.
2. Processor: 2 Physical CPU Cores
3. Ram: 512 Mb (Min.)
4. Hard Disk: 20 GB (Min.)
5. USB Port: 2.0
6. Mouse and keyboard

4.2.2 Software Requirement

1. Operating system: - Windows 7 or 7+
2. Coding Language: python, SQLite, mysql
3. Tool Used: - Spyder (Anaconda)

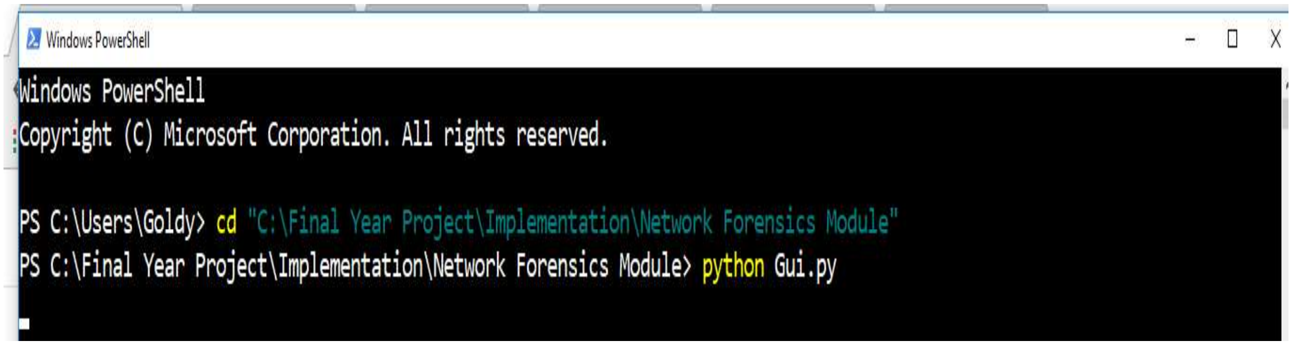
4.2.3 Software Specification

1. Operating System: Windows 7
2. Data Bases: Mysql, SQLite
3. Python: 2.7
4. Diagrams: https://www.draw.io
5. Libraries: os, sqlite3, csv, matplotlib.pyplot ,numpy, datetime, time, nltk, padas, re, pyshark, scipy, collection, tkinter, scrolltext, tkfinddialog, pymysql, tabulate, sys.

4.3 Screenshots

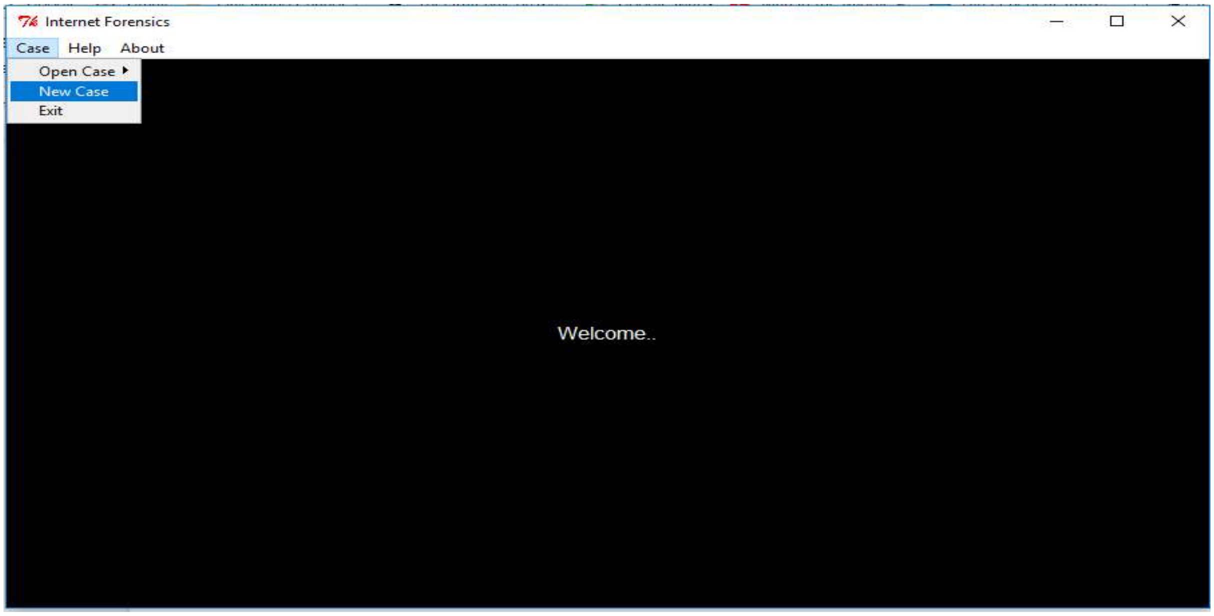
This section provides information about the tool and the steps for using our proposed tool along with the screenshots.

1) Open command prompt or windows power shell and type following command:
   cd "path_of_project"
   python GUI.py



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Goldy> cd "C:\Final Year Project\Implementation\Network Forensics Module"
PS C:\Final Year Project\Implementation\Network Forensics Module> python Gui.py
```

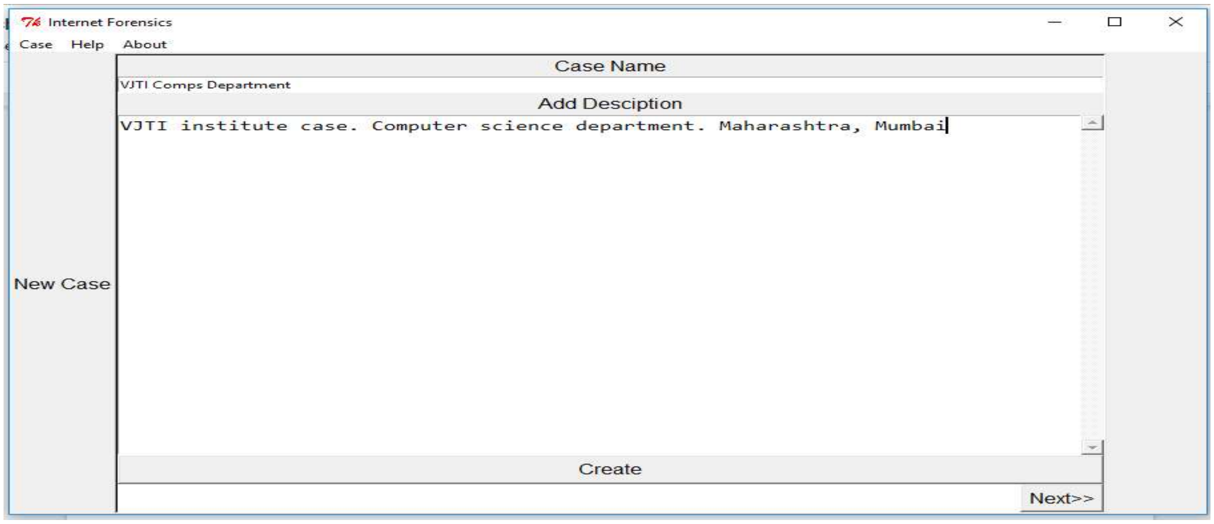
2) Following screen will display on the screen. Go to **Case** menu and select **new case**



Screen 4.1: Front Window

Screen 4.1 shows the tool window which contains three options: Case, Help and About. The case tab allows us to open an existing case or create a new case for forensic analysis and investigation. The Help tab provides help options to the user regarding the common problems he may face while using the tool. About provides information about the tool.

3) Write case name and Description and click on create button in order to create a new case.



Case Name

VJTI Comps Department

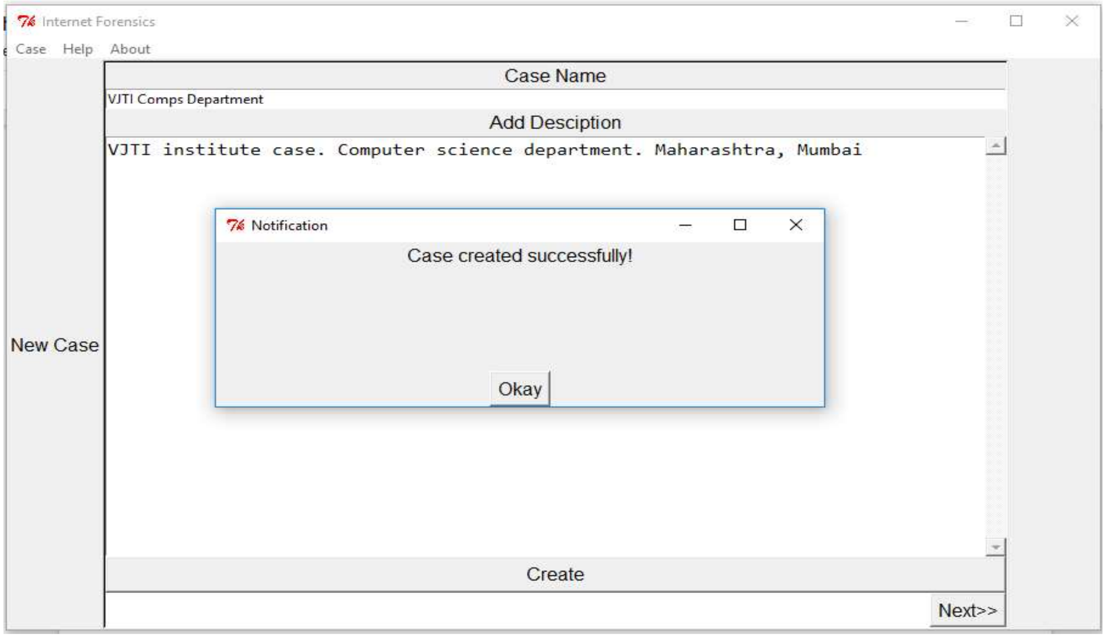
Add Desciption

VJTI institute case. Computer science department. Maharashtra, Mumbai

Screen 4.2: Creating New Case

Screen 4.2 shows the "Create New Case" window where the investigator can type in the name of the case, its description and click the next button to create the case.

4) Once case created successfully, click on next button



VJTI Comps Department

VJTI institute case. Computer science department. Maharashtra, Mumbai

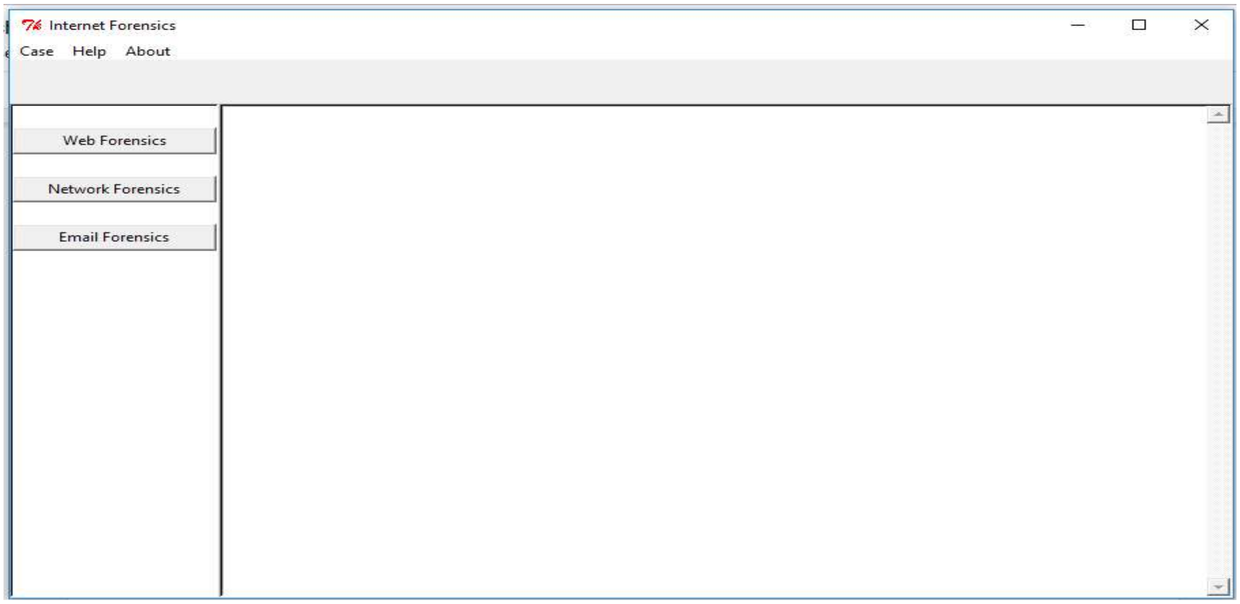
Case created successfully!

Screen 4.3: Screenshot showing successful creation of case

After successful Creation, a notification displaying the message "Case Created Successfully" is shown to the investigator as shown in Screen 4.3.

5) Select one of the three modules -
The tool provides the investigator with three modules to work with i.e. Web forensics, Network Forensics and Email Forensics. Web Forensics option allows to view the cookies, downloads and History data captured from the user's browser. The user can further do user timeline analysis to obtain refined result about the attacks and generate report.

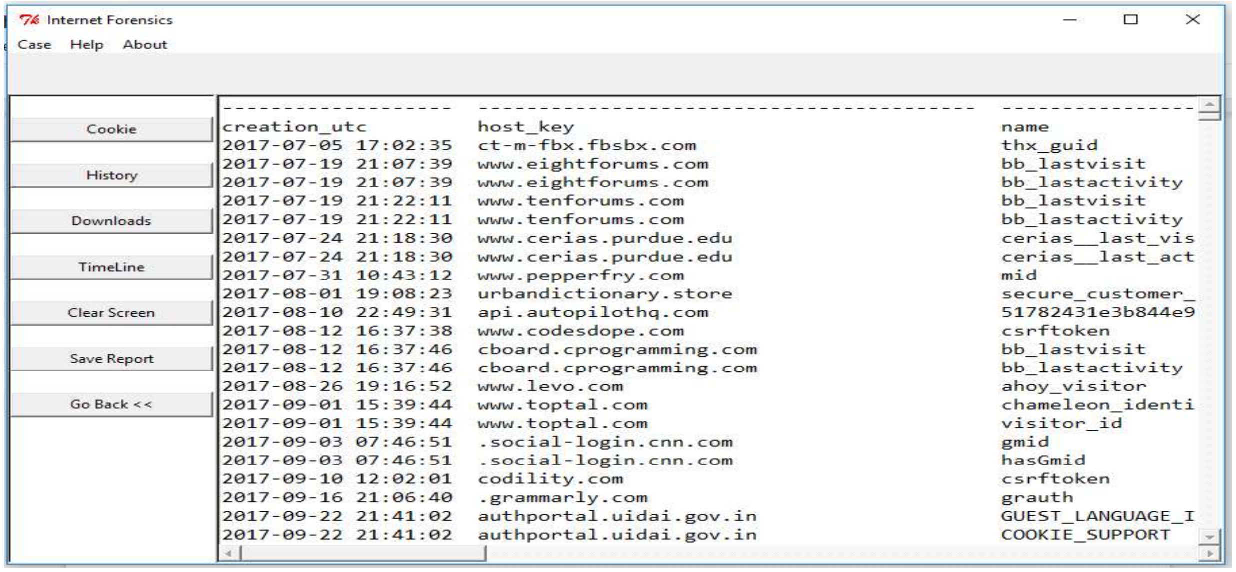
Network analysis option will help detect the four major types of attacks : Probing, Denial Of Service, R2L, U2R.
Email Forensics will help detect spam and non spam emails.



Screen 4.4: Selecting one of the three Modules

Screen 4.4 shows the tool window where the investigator can choose one of the three forensic modules from Web, Network and Network Forensics to start his/her investigation.

6) Web Forensics Module -Cookie

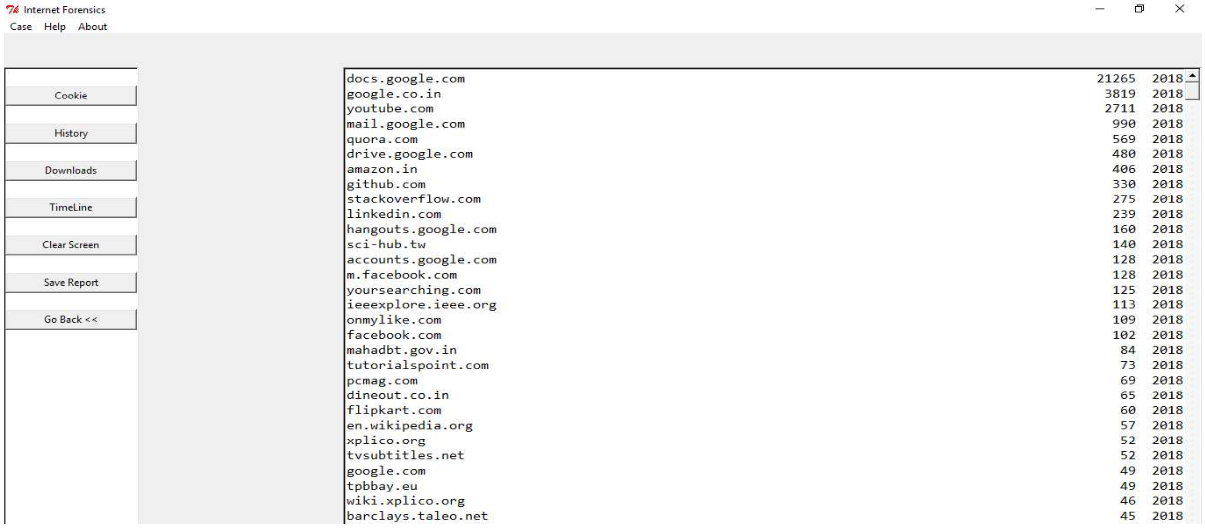


```
-------------------  -----------------------------------------  ----------------
creation_utc         host_key                                   name
2017-07-05 17:02:35  ct-m-fbx.fbsbx.com                         thx_guid
2017-07-19 21:07:39  www.eightforums.com                        bb_lastvisit
2017-07-19 21:07:39  www.eightforums.com                        bb_lastactivity
2017-07-19 21:22:11  www.tenforums.com                          bb_lastvisit
2017-07-19 21:22:11  www.tenforums.com                          bb_lastactivity
2017-07-24 21:18:30  www.cerias.purdue.edu                      cerias__last_vis
2017-07-24 21:18:30  www.cerias.purdue.edu                      cerias__last_act
2017-07-31 10:43:12  www.pepperfry.com                          mid
2017-08-01 19:08:23  urbandictionary.store                      secure_customer_
2017-08-10 22:49:31  api.autopilothq.com                        51782431e3b844e9
2017-08-12 16:37:38  www.codesdope.com                          csrftoken
2017-08-12 16:37:46  cboard.cprogramming.com                    bb_lastvisit
2017-08-12 16:37:46  cboard.cprogramming.com                    bb_lastactivity
2017-08-26 19:16:52  www.levo.com                               ahoy_visitor
2017-09-01 15:39:44  www.toptal.com                             chameleon_identi
2017-09-01 15:39:44  www.toptal.com                             visitor_id
2017-09-03 07:46:51  .social-login.cnn.com                      gmid
2017-09-03 07:46:51  .social-login.cnn.com                      hasGmid
2017-09-10 12:02:01  codility.com                               csrftoken
2017-09-16 21:06:40  .grammarly.com                             grauth
2017-09-22 21:41:02  authportal.uidai.gov.in                    GUEST_LANGUAGE_I
2017-09-22 21:41:02  authportal.uidai.gov.in                    COOKIE_SUPPORT
```

Screen 4.5: Screen showing details of cookie

Screen 4.5 shows the different basis upon which the investigator can do web forensics: cookies, downloads, History and time line analysis. In the screen above, we see the details of cookies stored in the user's web browser. Details such as the Date and time of the cookie creation, the name, host key of the cookie are displayed.

7) Web Forensics- History

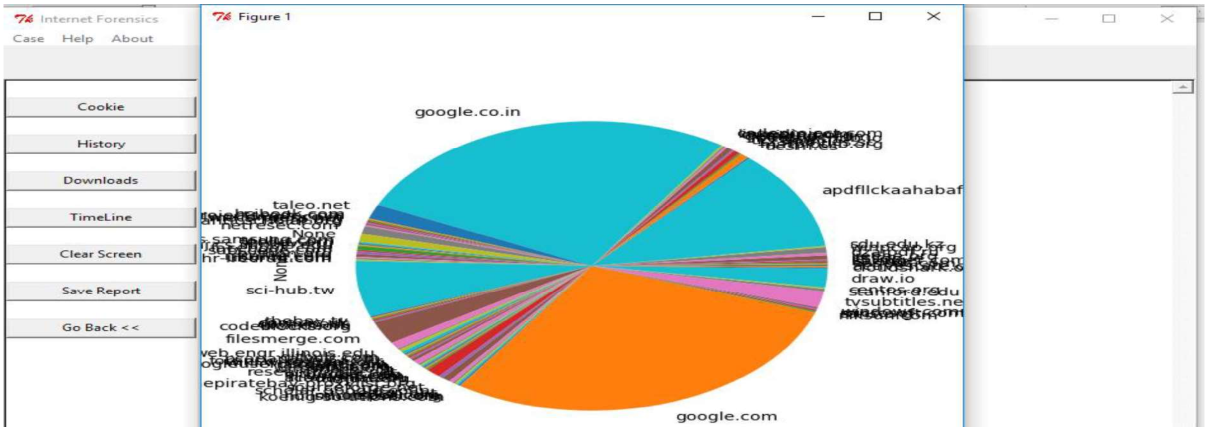


```
docs.google.com          21265  2018
google.co.in              3819  2018
youtube.com               2711  2018
mail.google.com            990  2018
quora.com                  569  2018
drive.google.com           480  2018
amazon.in                  406  2018
github.com                 330  2018
stackoverflow.com          275  2018
linkedin.com               239  2018
hangouts.google.com        160  2018
sci-hub.tw                 140  2018
accounts.google.com        128  2018
m.facebook.com             128  2018
yoursearching.com          125  2018
ieeexplore.ieee.org        113  2018
onmylike.com               109  2018
facebook.com               102  2018
mahadbt.gov.in              84  2018
tutorialspoint.com          73  2018
pcmag.com                   69  2018
dineout.co.in               65  2018
flipkart.com                60  2018
en.wikipedia.org            57  2018
xplico.org                  52  2018
tvsubtitles.net             52  2018
google.com                  49  2018
tpbbay.eu                   49  2018
wiki.xplico.org             46  2018
barclays.taleo.net          45  2018
```

Screen 4.6: Screen showing details of History

Screen 4.6 shows the history details extracted from the browser. It shows the websites and pages searched for, the number of times they were searched and the year of the search.

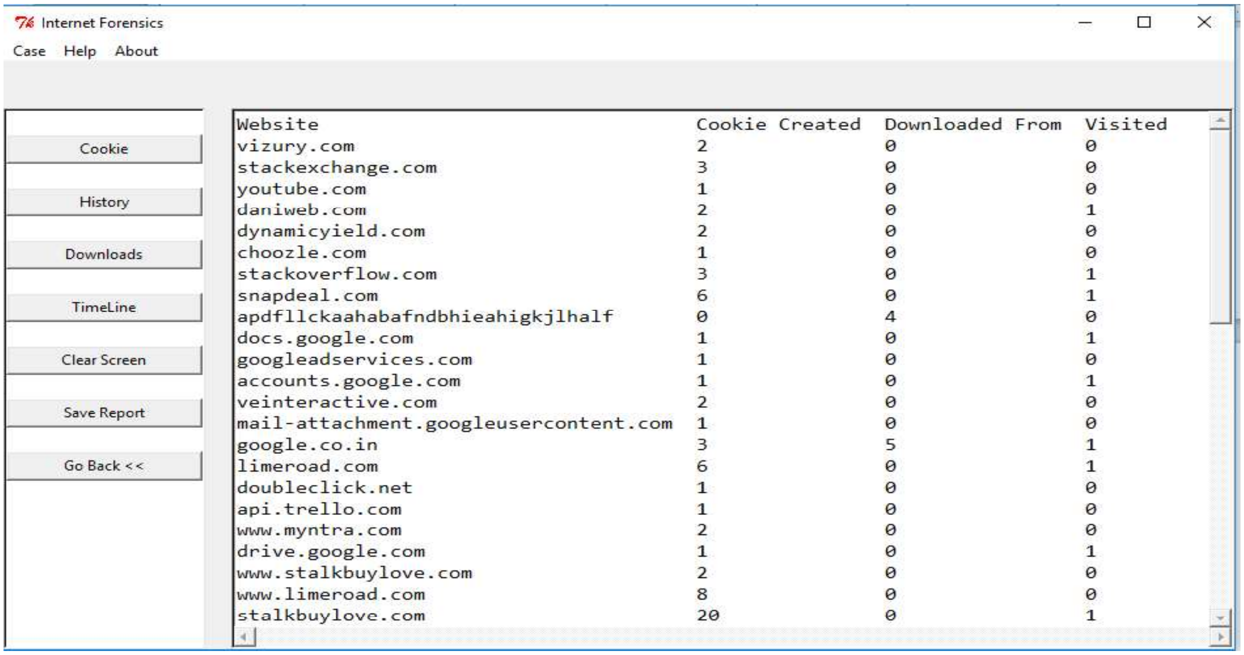
8) Web Forensics - Downloads



Screen 4.7: Screen showing downloads

Screen 4.7 shows a pie chart that depicts the number of downloads done from a particular website. In the screen, we see that the maximum downloads were done from google.co.in followed by google.com.

9) Web Forensics - Timeline Analysis



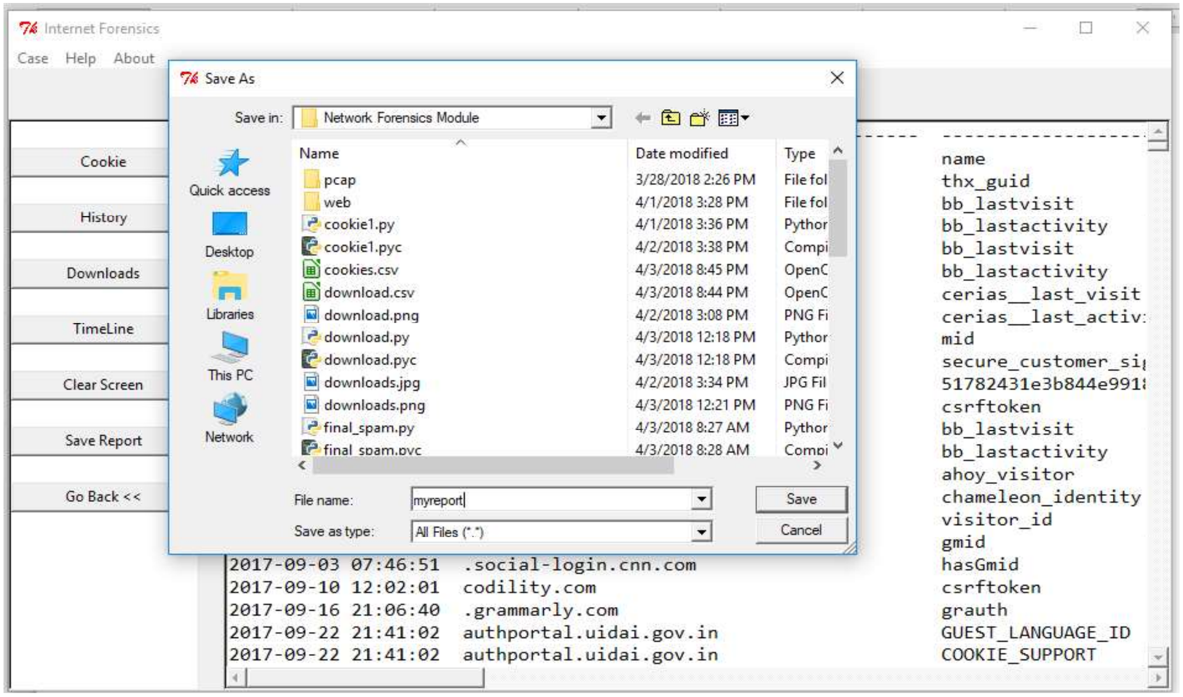
```
Website                               Cookie Created  Downloaded From  Visited
vizury.com                            2               0                0
stackexchange.com                     3               0                0
youtube.com                           1               0                0
daniweb.com                           2               0                1
dynamicyield.com                      2               0                0
choozle.com                           1               0                0
stackoverflow.com                     3               0                1
snapdeal.com                          6               0                1
apdfllckaahabafndbhieahigkjlhalf      0               4                0
docs.google.com                       1               0                1
googleadservices.com                  1               0                0
accounts.google.com                   1               0                1
veinteractive.com                     2               0                0
mail-attachment.googleusercontent.com 1               0                0
google.co.in                          3               5                1
limeroad.com                          6               0                1
doubleclick.net                       1               0                0
api.trello.com                        1               0                0
www.myntra.com                        2               0                0
drive.google.com                      1               0                1
www.stalkbuylove.com                  2               0                0
www.limeroad.com                      8               0                0
stalkbuylove.com                      20              0                1
```

Screen 4.8: Screen showing timeline analysis

Screen 4.8 shows the timeline analysis of the web browser details. It shows the website visited, the number of cookies created from the website, the number of files or items downloaded from the website, etc.

10) Click on Save Report to save report on your system

Screen 4.9 shows the ‘Save As’ window. It is displayed when the investigator clicks the save report button. The investigator is then prompted to save the report by the name and in the location of his/her choice.



Save in: Network Forensics Module

Name	Date modified	Type
pcap	3/28/2018 2:26 PM	File fol
web	4/1/2018 3:28 PM	File fol
cookie1.py	4/1/2018 3:36 PM	Pythor
cookie1.pyc	4/2/2018 3:38 PM	Compi
cookies.csv	4/3/2018 8:45 PM	OpenC
download.csv	4/3/2018 8:44 PM	OpenC
download.png	4/2/2018 3:08 PM	PNG Fi
download.py	4/3/2018 12:18 PM	Pythor
download.pyc	4/3/2018 12:18 PM	Compi
downloads.jpg	4/2/2018 3:34 PM	JPG Fil
downloads.png	4/3/2018 12:21 PM	PNG Fi
final_spam.py	4/3/2018 8:27 AM	Pythor
final_spam.pyc	4/3/2018 8:28 AM	Compi

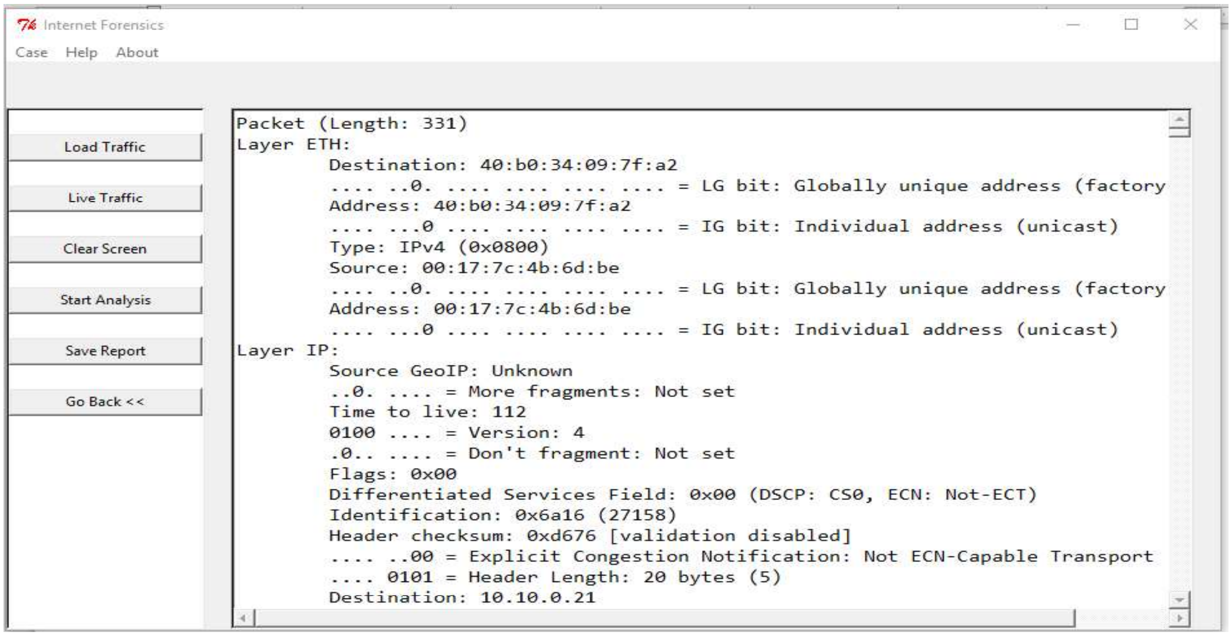
File name: myreport

Save as type: All Files (*.*)

```
------   -------------------
         name
         thx_guid
         bb_lastvisit
         bb_lastactivity
         bb_lastvisit
         bb_lastactivity
         cerias__last_visit
         cerias__last_activ:
         mid
         secure_customer_si;
         51782431e3b844e991;
         csrftoken
         bb_lastvisit
         bb_lastactivity
         ahoy_visitor
         chameleon_identity
         visitor_id
         gmid
2017-09-03 07:46:51  .social-login.cnn.com        hasGmid
2017-09-10 12:02:01  codility.com                 csrftoken
2017-09-16 21:06:40  .grammarly.com               grauth
2017-09-22 21:41:02  authportal.uidai.gov.in      GUEST_LANGUAGE_ID
2017-09-22 21:41:02  authportal.uidai.gov.in      COOKIE_SUPPORT
```

Fig 4.9: Saving report on local system

11) Network Forensics - Click on **Load Traffic** button and choose a pcap file for analysis

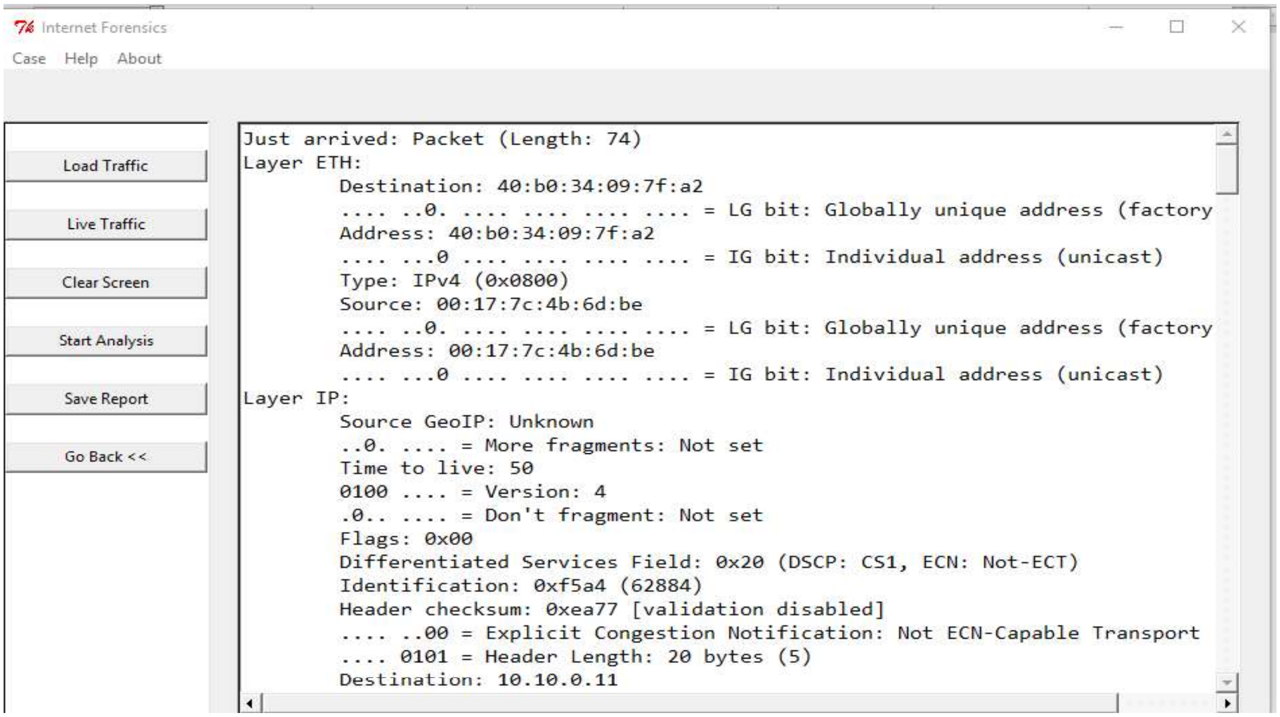


```
Packet (Length: 331)
Layer ETH:
        Destination: 40:b0:34:09:7f:a2
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory
        Address: 40:b0:34:09:7f:a2
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
        Type: IPv4 (0x0800)
        Source: 00:17:7c:4b:6d:be
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory
        Address: 00:17:7c:4b:6d:be
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Layer IP:
        Source GeoIP: Unknown
        ..0. .... = More fragments: Not set
        Time to live: 112
        0100 .... = Version: 4
        .0.. .... = Don't fragment: Not set
        Flags: 0x00
        Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        Identification: 0x6a16 (27158)
        Header checksum: 0xd676 [validation disabled]
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport
        .... 0101 = Header Length: 20 bytes (5)
        Destination: 10.10.0.21
```

Screen 4.10: Screen showing loaded traffic

Screen 4.10 shows the details of the loaded traffic. The loaded traffic button loads the pcap files stored in the host machine. The details of the loaded traffic included packet information stating the mac address of the source and destination, the, the header length, destination IP address, etc.

12) Network Forensics - Click on **Live Traffic** button to capture and display live traffic



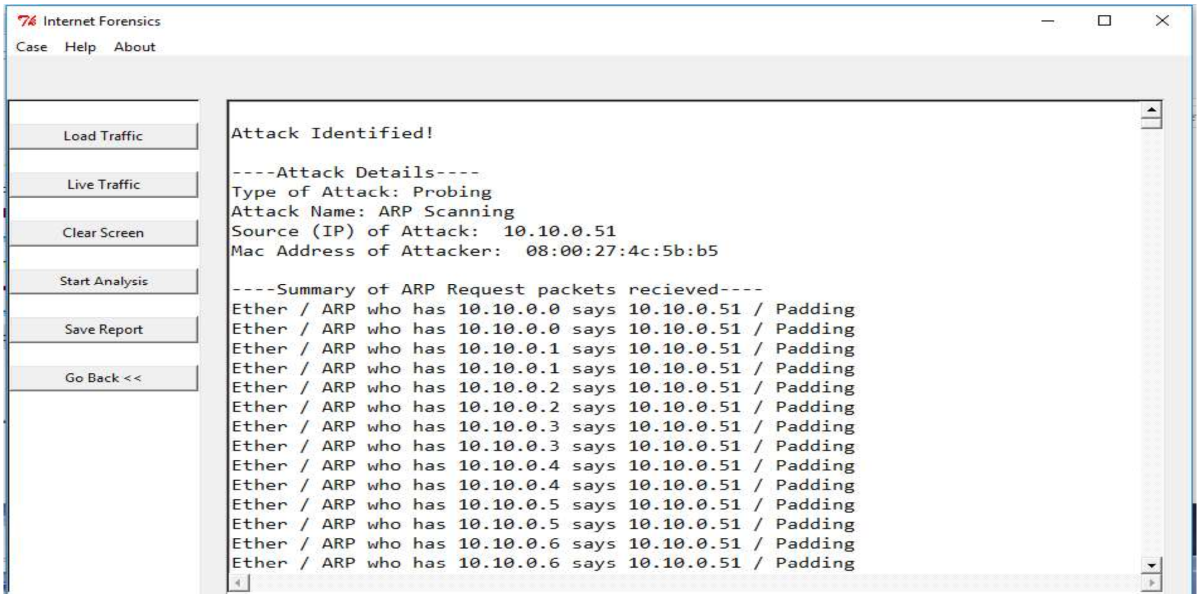
```
Just arrived: Packet (Length: 74)
Layer ETH:
        Destination: 40:b0:34:09:7f:a2
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory
        Address: 40:b0:34:09:7f:a2
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
        Type: IPv4 (0x0800)
        Source: 00:17:7c:4b:6d:be
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory
        Address: 00:17:7c:4b:6d:be
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Layer IP:
        Source GeoIP: Unknown
        ..0. .... = More fragments: Not set
        Time to live: 50
        0100 .... = Version: 4
        .0.. .... = Don't fragment: Not set
        Flags: 0x00
        Differentiated Services Field: 0x20 (DSCP: CS1, ECN: Not-ECT)
        Identification: 0xf5a4 (62884)
        Header checksum: 0xea77 [validation disabled]
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport
        .... 0101 = Header Length: 20 bytes (5)
        Destination: 10.10.0.11
```

Screen 4.11: Screen showing captured traffic

Screen 4.11 shows the packet details that are captured live. Live capture of packets involves displaying the details of those packets that are captured in real time.

13) Click on **Start Analysis** button. This will produce a brief report about the attack detected after analysis.

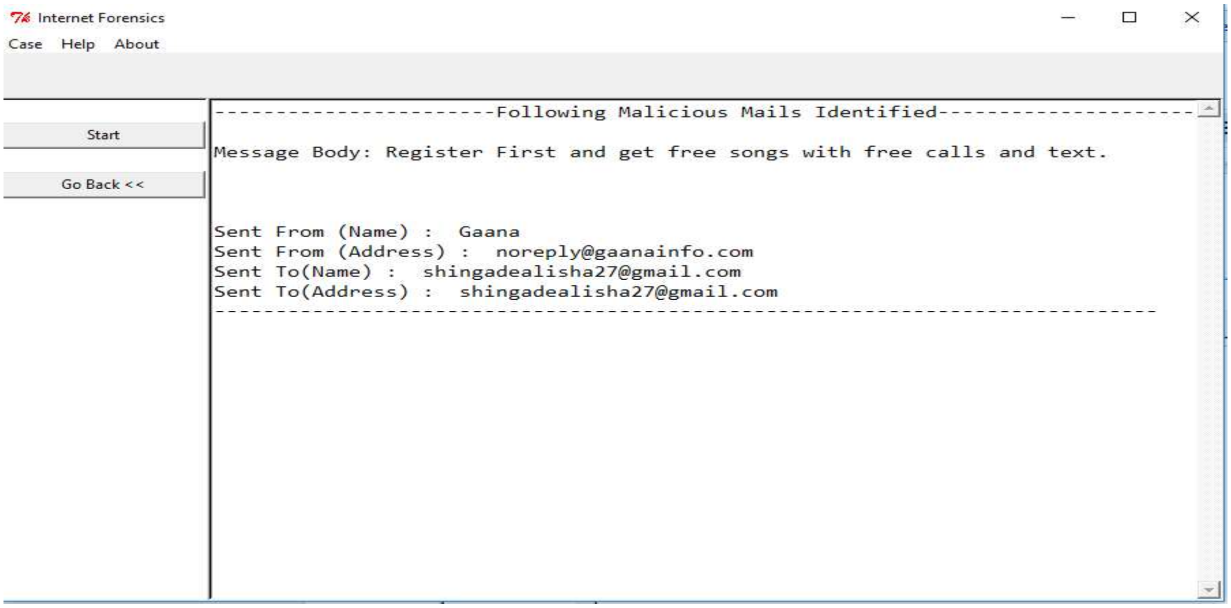
Screen 4.12 shows a window that displays the details when the investigator clicks the ‘Start Analysis’ button after loading the traffic.



```
Attack Identified!

----Attack Details----
Type of Attack: Probing
Attack Name: ARP Scanning
Source (IP) of Attack:  10.10.0.51
Mac Address of Attacker:  08:00:27:4c:5b:b5

----Summary of ARP Request packets recieved----
Ether / ARP who has 10.10.0.0 says 10.10.0.51 / Padding
Ether / ARP who has 10.10.0.0 says 10.10.0.51 / Padding
Ether / ARP who has 10.10.0.1 says 10.10.0.51 / Padding
Ether / ARP who has 10.10.0.1 says 10.10.0.51 / Padding
Ether / ARP who has 10.10.0.2 says 10.10.0.51 / Padding
Ether / ARP who has 10.10.0.2 says 10.10.0.51 / Padding
Ether / ARP who has 10.10.0.3 says 10.10.0.51 / Padding
Ether / ARP who has 10.10.0.3 says 10.10.0.51 / Padding
Ether / ARP who has 10.10.0.4 says 10.10.0.51 / Padding
Ether / ARP who has 10.10.0.4 says 10.10.0.51 / Padding
Ether / ARP who has 10.10.0.5 says 10.10.0.51 / Padding
Ether / ARP who has 10.10.0.5 says 10.10.0.51 / Padding
Ether / ARP who has 10.10.0.6 says 10.10.0.51 / Padding
Ether / ARP who has 10.10.0.6 says 10.10.0.51 / Padding
```

Screen 4.12: Screen showing report generated

14) Email Forensics - Click on Start to classify emails

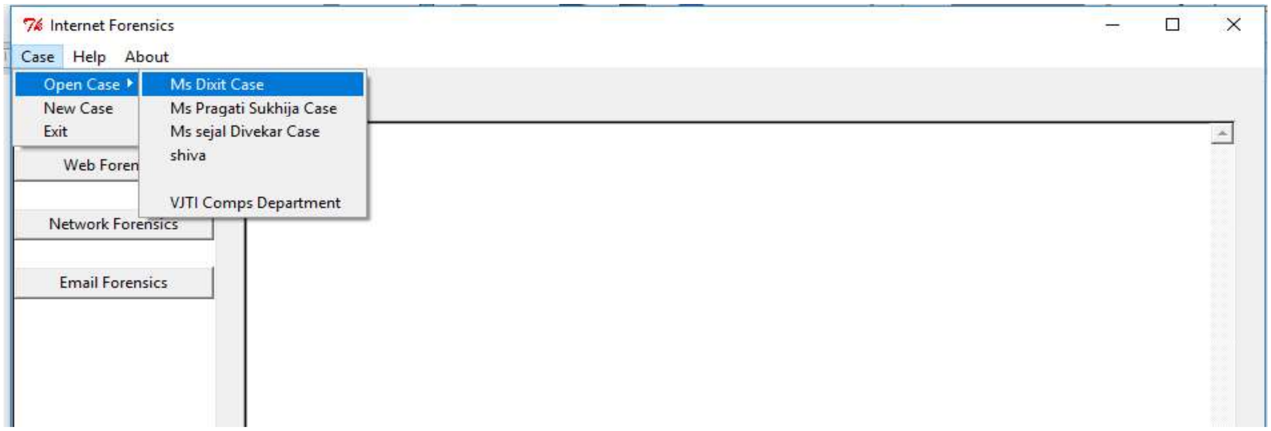


```
-----------------------Following Malicious Mails Identified---------------------
Message Body: Register First and get free songs with free calls and text.



Sent From (Name) :  Gaana
Sent From (Address) :  noreply@gaanainfo.com
Sent To(Name) :  shingadealisha27@gmail.com
Sent To(Address) :  shingadealisha27@gmail.com
-----------------------------------------------------------------------------
```

Screen 4.13: Screen showing classification

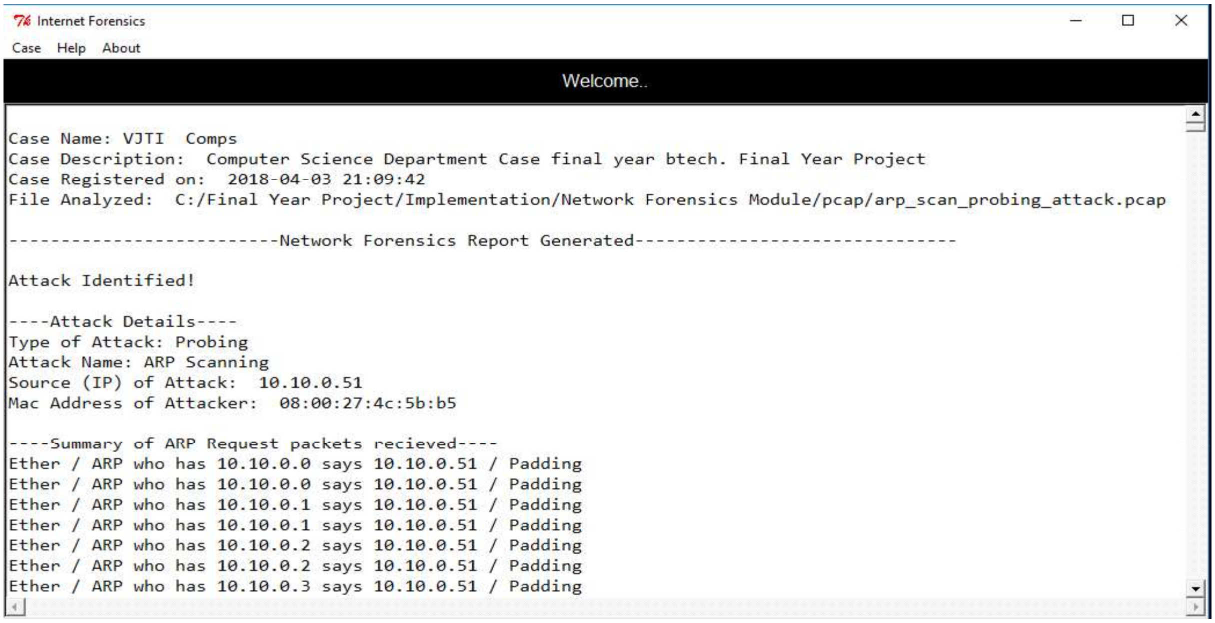
Screen 4.13 shows the email forensic screen which displays the spam emails found in an email account. The screen shows a report which displays the message body, the sender name and sender email address, the recipient name and recipient email address.

15) Click on **Case → Open case → case_name** to open existing cases.



Screen 4.14: Open existing cases

Screen 4.14 shows the 'Open Existing case' submenus that displays the cases already stored and saved in the host machine.



```
Case Name: VJTI  Comps
Case Description:  Computer Science Department Case final year btech. Final Year Project
Case Registered on:  2018-04-03 21:09:42
File Analyzed:  C:/Final Year Project/Implementation/Network Forensics Module/pcap/arp_scan_probing_attack.pcap

-------------------------Network Forensics Report Generated------------------------------

Attack Identified!

----Attack Details----
Type of Attack: Probing
Attack Name: ARP Scanning
Source (IP) of Attack:  10.10.0.51
Mac Address of Attacker:  08:00:27:4c:5b:b5

----Summary of ARP Request packets recieved----
Ether / ARP who has 10.10.0.0 says 10.10.0.51 / Padding
Ether / ARP who has 10.10.0.0 says 10.10.0.51 / Padding
Ether / ARP who has 10.10.0.1 says 10.10.0.51 / Padding
Ether / ARP who has 10.10.0.1 says 10.10.0.51 / Padding
Ether / ARP who has 10.10.0.2 says 10.10.0.51 / Padding
Ether / ARP who has 10.10.0.2 says 10.10.0.51 / Padding
Ether / ARP who has 10.10.0.3 says 10.10.0.51 / Padding
```

Screen 4.15: Screen showing existing case summary

Screen 4.15 shows the Existing Case summary. The report includes the case name, its description, date and time of the case registration, the attack name and its details. Here we see that the attack detected is ARP Scanning and the attack is a Probing type of network attack.

4.4 Conclusion

The user interface of Internet Forensics Tool is clear, concise, responsive. The user interface provide ease of navigation from one page to another. All the cases registered are stored in database which can viewed by analyst. This provide good knowledge of pre-existing cases with their results. The report generated provide good visualization of results which is obtained from analysis of case. This reduces analyst’s work and time.

5. Conclusion and Future Work

From related work we analyzed different tools and we integrated three domains together to determine the best features amongst all the existing tools to include them in our forensic tool.
Web activity on a system is recorded in various locations in several forms. When closely observed, the activity done by the user is understood. The digital evidence is used for forensic investigations and to undo some activities which are offensive or malicious or improperly terminated (for example System Restore). To trace an activity with respect to Web, the areas that were looked for evidences are history, cache, cookies, browser specific data, browser specific preferences and the registry.

All these areas reflected the expected changes in the system state and hence were helpful in reconstructing the whole activity. But deleting any of the evidences would seriously disturb the process of investigation. Google chrome is a light weight browser. It was found that chrome is very good for regular browsing. It has become popular very soon after it came into existence. Live Web forensics can be done to provide robust approach for forensics. Support of advanced string filtering algorithms such as the bloom filter, which is already being deployed in most application level firewalls should be adopted and research on more advanced algorithms should be done. To avoid harmful activities in private mode traces should be searched on hard disk for evidences.

Network forensics module in our proposed solution, is design to capture live traffic from ethernet. As soon as packets arrive, it captures them; divide details according to layer at which it was received and displays them on screen. Also, it allows user to provide his own input by capturing packets from crime scene in the form of pcap file. This pcap file is analyse by packet analyzer for attacks and report is generated and displayed on the screen. Investigator has to do nothing but give a pcap file as input and sit and relax, tool will do the rest of the processing. Also, investigator can save the generated report by pressing save button. This report gets saved on local machine and also in the database, Investigator can anytime go back and see saved reports.

Our tool is currently able to detect few of the network attacks. In future, we plan to train our tool for more attacks so that these attacks can be identified effectively, giving investigator a detail