AN EMPIRICAL ANALYSIS OF EMAIL FORENSICS TOOLS

Ahmad Ghafarian, Ash Mady and Kyung Park

Department of Computer Science and Information Systems, Mike Cottrell College of Business, University of North Georgia, Dahlonega, GA, USA

ABSTRACT

Emails are the most common service on the Internet for communication and sending documents. Email is used not only from computers but also from many other electronic devices such as tablets; smartphones, etc. Emails can also be used for criminal activities. Email forensic refers to the study of email detail and content as evidence to identify the actual sender and recipient of a message, date/time of transmission, detailed record of email transaction, intent of the sender, etc. Email forensics involves investigation of metadata, keyword, searching, port scanning and generating report based on investigators need. Many tools are available for any investigation that involves email forensics. Investigators should be very careful of not violating user's privacy. To this end, investigators should run keyword searches to reveal only the relevant emails. Therefore, knowledge of the features of the tool and the search features is necessary for the tool selection. In this research, we experimentally compare the performance of several email forensics tools. Our aim is to help the investigators with the tool selection task. We evaluate the tools in terms of their keyword search, report generation, and other features such as, email format, size of the file accepted, whether they work online or offline, format of the reports, etc. We use Enron email dataset for our experiment.

KEYWORDS

Email forensic, digital forensic, report generation, keyword search, tools, Enron, filtering.

1. INTRODUCTION

Digital forensics refers to the acquisition and analysis of data from the memory of an electronic device such as laptop, smartphone, etc. [1]. A digital forensics investigation that involves analysis of emails is referred to as email forensics. This process involves retrieving email details including sender, receiver, content, date, time, and other details including the intention of the email sender [2]. However, the examination of the suspect's entire email transactions may violate the privacy of the person being under investigation. To avoid this privacy violation, the investigators use email forensics tools and perform keyword search for retrieving only those emails that are related to the current case [3, 4]. To do that, the investigators need to have a good knowledge of the email forensics tools including their keyword search and reporting capabilities.
There are many software tools, which may assist the forensics investigators. These tools provide easy use browser format, automated key search reports, and other features. Current forensic tools are designed to help examiners in finding specific pieces of evidence by tracing emails. Further, these tools are created for solving crimes committed against people where the evidence resides on the memory of a device. Selection of an email forensics tools that implements the visibility, filtering, keyword search and report generation would be the first logical step in this direction. Considering the existence of several email forensics tools, the selection process may not be trivial. In an effort to address this gap and assist forensics experts in selecting an appropriate tool,

we empirically evaluate the search and report generation capabilities of several contemporary email forensics tools. In the experiment, we use the Enron email dataset file that is maintained by MIT [5] and is provided to researchers. We import the email files to these tools, run the tools, and evaluate their keyword search filtering and the report generation features. We also evaluate other features, such as, the supported email format, size of the file they accept, format of the reports, and online or offline, etc.

The rest of this paper is organized as follows. Section 2 provides a literature review. Section 3 describes tools and technology. Section 4 covers the experiment methodology. Analysis of the results is covered in section 5. Section 6 covers the conclusion where we report our findings as well as the possible extension of this work for future research.

2. BACKGROUND

Email forensics is an integral part of many digital forensics investigations. Researchers and practitioners have studied various aspects of email forensics such as tool development [3, 6], technique [4], technologies [7], and methodologies [8] to assist forensics investigators. In this section, we present most of the relevant research results in this field.

The paper by Banday [3] illustrates email architecture from a forensics perspective. The author describes the roles and responsibilities of different email actors and components, itemizes metadata contained in email headers, and lists protocols and ports used in it. In addition, the author provides the details of various open source and proprietary email forensics tools and their capabilities. The paper by Meghanathan, et al [7] provides a comprehensive survey of email and network forensics tools as well as their specific features. Another paper by Paglierani, et al [8] defines a general methodology for email forensics and show proof of concept with evidence results. Other studies of the main characteristics of email forensics tools and techniques can be found in [1, 2]. Cohen [4] presents an automated technique for bulk-email analysis and presentation to aid in evidence interpretation. In another paper, Devendran, et al [9] theoretically have examined a set of common features of four popular email forensic tools.

Hajidj, et al [6] developed a new email analysis software tool by integrating existing statistical and machine learning techniques as well as data from social networking techniques. The authors proposed a framework that offers different functionalities ranging from email storing, editing, searching, and querying. However, we found no report on the widespread use of their framework. Stolfo and Hershkp [10] have developed an email visualization tool, which helps the investigators to visualize traces of emails. They have used data mining techniques in the development of their tool. The tool supports many different email formats. The authors claim that their tool may be leveraged in many applications. In similar research, Khan, et al [11] proposes a framework that employs data mining techniques to perform statistical analysis, email classification & clustering, author identification, and social network analysis. The researchers use Enron email dataset to evaluate their implementation.

Another study of privacy of email investigation can be found in [12]. The authors introduced a cryptographic scheme that allows encrypting the entire email set before handing them over for investigation. The major feature of this approach is that one can run keyword searches on the encrypted data. Once the tool identifies some emails as having the keyword search, then those emails will be decrypted for further processing. In the next section, we discuss the experiment process.

3. TOOLS AND TECHNOLOGY

The following subsections describe the email forensics tools, the technology and the environment of our experiment.

3.1. Email Forensics Software Tools

In this experiment, we used the following email forensics tools. The justification for selecting these tools are twofold. First, these are the most popular tools available in the market. Second, they offer trial versions for research and evaluation purposes.

- Aid4Mail v3.8 [13]
- eMailTrackerPro V10 [14]
- MailXamine V4 [15]
- Paraben's EMX V8.6.5277 [16]
- Autopsy V4.13.0 [17]
- OSForensics V7 [18]

3.2. Hardware

The experiment was performed on several laptops hosting Microsoft Windows 10 Ultimate 64 bits. The hardware specification includes Intel core 2Duo CPU, 2.5 GHz, 4GB RAM, and 320GB HDD (two partitions). To prepare for the experiment, we first reimaged the laptops. This process ensures that no applications exists on laptops and sound forensics process is followed. Then, we installed an email forensics tool on each laptop, imported the Enron email dataset file to each of the software tool ready for the experiment.

3.3. Email Dataset

To perform the experiment; we needed a set of email files for offline processing. We decided to use the Enron email dataset, which is maintained by MIT and contains hundreds of thousands of email files. Processing all those emails is time consuming and is beyond the scope and purpose of this study. In addition, the email forensics tools under this study impose limitations on the number of emails they can process for an input folder. Therefore, we selected three folders from the email dataset. The selected folders contain all types of emails including sent emails, received emails, deleted emails, etc. We made sure that the selected email folders are sufficient to demonstrate the behavior of the tools. The format of the Enron email dataset is called Maildir (See Figure 1). Some of the email forensics tools under this study do not accept this format. Therefore, we had to convert this format to a different format, which is acceptable by the tool.

4. THE EXPERIMENT METHODOLOGY

The email forensics experiment consists of the following orderly steps.

- Installed one email forensics tool on each laptop
- Launched the email forensics tool and created a case
- Imported email files from the selected dataset folders.
- Ran keyword search on email files and within an email content
- Generated reports
- Analyzed the generated reports

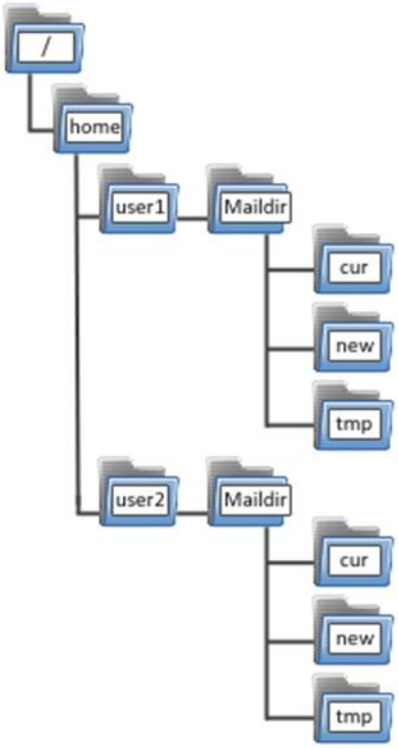


Figure 1. Enron Maildir internal structure

4.1. Add4Mail

Add4Mail is a proprietary suite of email conversion tools including email migration, email discovery, and email archiving. It allows users to process email data for various investigation purposes. During the experiment we observed that Add4Mail:

- Removes email-subjects from all reports and conversion process.
- Supports several popular email extension formats from various mail client programs.
- Can work on the email trash folder.
- Process large email files.
- Can search the machine for email file, folder name or identity name (this option not available when using Maildir format).
- Allows the investigator to select a folder and then search subfolders for specific email files.
- The tool has no dedicated search section or report section options. It converts an email details to a file and the converted files treated as reports.
- Can search all supported mail formats.
- Capable of filtering the emails based on several features including text, date/time, keywords, logical operators and regular expressions.

When you convert to specific file format, you can use some search and filter options before the conversion process. We generated the following reports for our selected emails.

- The name of the domain that emails are sent or received from them.
- Timeline of the email exchange (day and month).

- Pictures on these emails.
- PDF files on these emails.
- Email addresses that are typed in the body of the messages.
- Export emails metadata in these formats, CSV, TSV and XML.
- Converted email files to CSV and XML formats.

The report results for the domain name, day, and month are shown in Figure 2 a., b. and c. respectively.

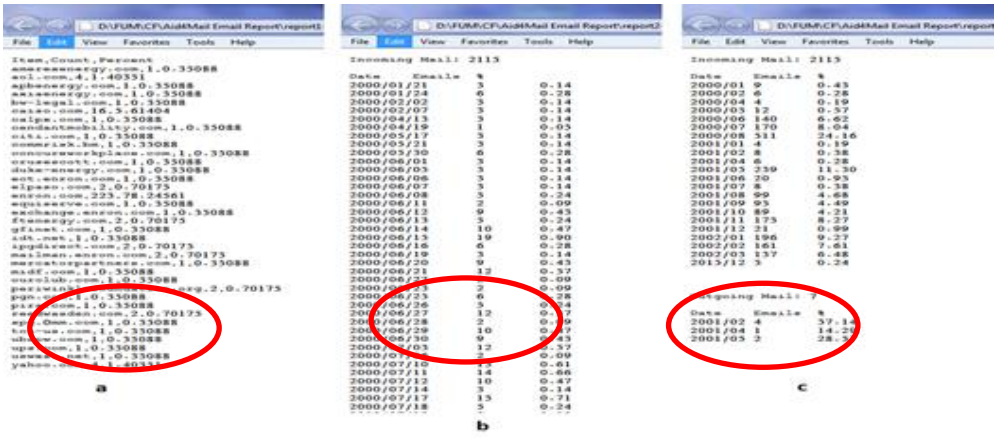


Figure 2. Report generated by Add4Mail

One of the useful functions of Aid4Mail is that we can use script or import new scripts into the software and use this script for filtering reports. Some of these scripts are export only emails from Gmail address, mails with JPG/MOV/AVI files, process deleted emails, skip duplicates on export, etc. We used these filters for searching emails that were sent from 04/14/2000 until 4/20/2000. Figure 3 shows the filters we used.

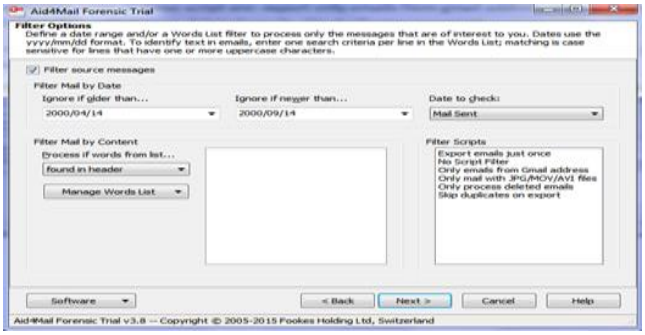


Figure 3. Filtered page for emails between 4/14/2000 and 4/20/2000

During the experiment, we observed additional limitations of Add4Mail. First, the Graphical User Interface (GUI) of the tool is very simple and offers no flexibility to the investigator. Second, we need other applications like web browsers; PDF readers, or MS Excel for analyzing and searching the results of the report. This is because these applications are not integrated into the tool.

4.2. Paraben Email Examiner (EMX)

Paraben E3 EMX is proprietary and allows us to analyze message headers, bodies, and attachments. It recovers email in the deleted folders. Paraben supports almost all major email formats and can generate keyword search reports. Our experiment demonstrated that the tool has the following major features.

- Can search all email files or whole database folders and generates reports.
- Has comprehensive keyword search features, bookmarking, advanced Boolean searching, and searching within attachments.
- Supports for various languages including Unicode.
- Capable of examining email headers and bodies and provides details report of search filters (including contents from attachments).
- Accepts Maildir format and several other formats
- Can show all the email files of a selected folder in a separate window.
- Shows the results of analysis of the selected emails within the Paraben
- Can convert Maildir email format to other formats like EML, EMX, MHT, PST. The conversion process supports filtering (based on text, hex search, locate code page, etc.) and the converted file represents a report. It has the option to define a scope for converting the email including subject, body, headers, etc.
- Allows selecting the information we want to be included in the reports. The output can be filtered by time, date, etc. This feature helps the investigator to preserve privacy.

Since Paraben accepts Maildir format we did not have to do any conversion. Figure 4 shows the result of report generation. The figure shows the email data and the header.

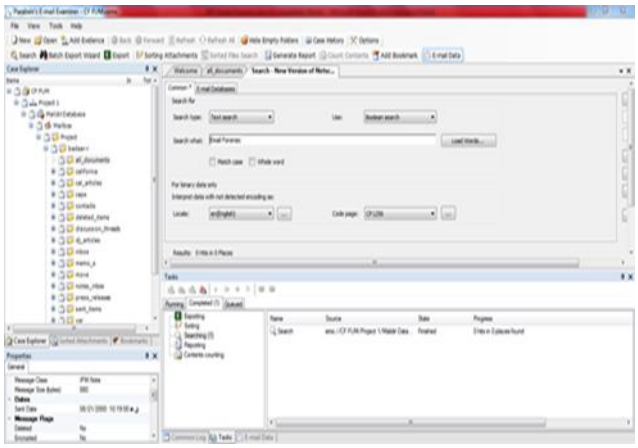


Figure 4. Search options in Paraben for emails dataset

In addition, we used several keyword searches and searched for the word “ENRON” in the three email folders we used in this research. The result is shown in Figure 5.

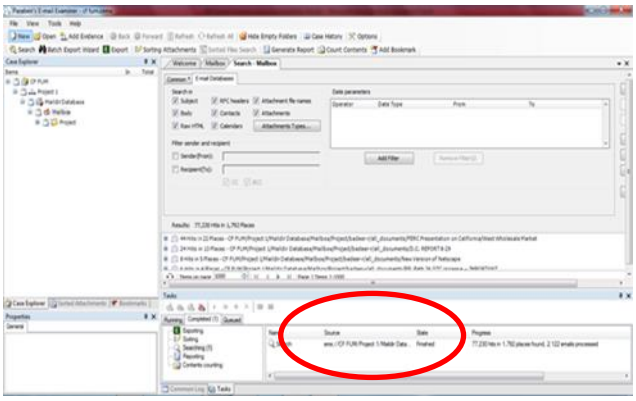


Figure 5. Result of Search for Word "ENRON"

Another search for the word "weekend". Generated the HTML report. EMX can generate reports in various formats including HTML Investigative, simple Text, CSV Text, evidence, and HTML email message. Figure 6 shows a CSV report created from the email database folder.

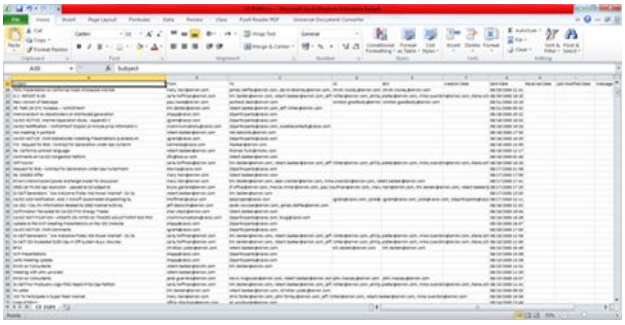


Figure 6. CSV Report Generated From Enron Emails

4.3. eMailTrackerPro

This proprietary tool can trace an email using the email header as well as filtering spam emails. Our experiment has shown that the has the following features.

- It is different from all the other tools in that there is no option for importing emails file, folder or database.
- It requires that we insert an email header manually, connect this software to your email account, or suspect's email account.
- It allows us to connect multiple accounts to this tool simultaneously.
- It requires connecting to a live email account, doing keyword filtering search, and generating support.

For this experiment, we created a Yahoo email account, i.e. FUM_CF@YAHOO.COM and incorporated this account to the tool (see Figure 9). If we want to trace an email that was received to this account, we can select that email and then trace it. After performing this task, we noticed that the results are shown in a separate popup windows and include information like Whois (Network Domain), sender and receiver name, IP address hop for this email and email header. For example, Figure 7 shows trace of an email origin by eMailTrackerPro. Similarly, Figure 8 shows filtering emails sent by a specific sender.

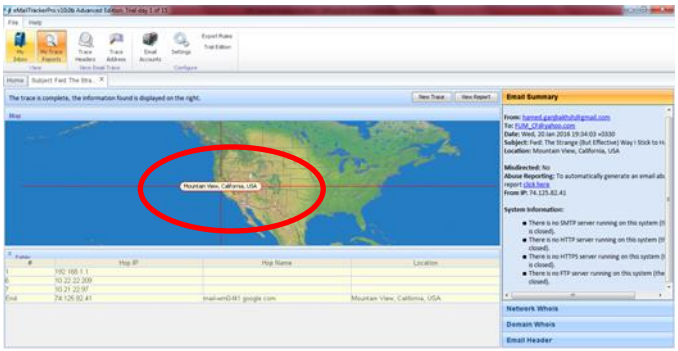


Figure 7. Trace of an email in eMailTrackerPro

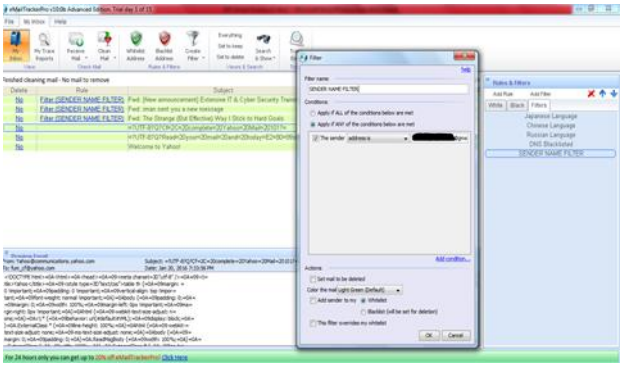


Figure 8. Filter email sent by a specific sender

We can filter by subject, sender's email address, To address, DNS blacklist, sender IP address, IP block, etc. For example, Figure 9 shows filtered Yahoo@communications.yahoo.com.

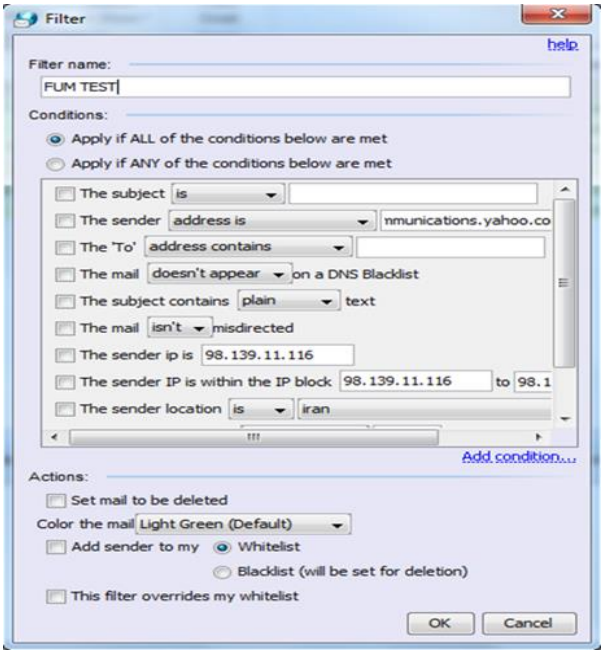


Figure 9. Filtering email with name "FUM TEST"

The tool also allows the investigator to send emails to blacklist or whitelist automatically. However, it does not support comprehensive keyword search, which means the investigators can only searches through the subject, from address, to address, and IP address of the sender (see Figure 10).

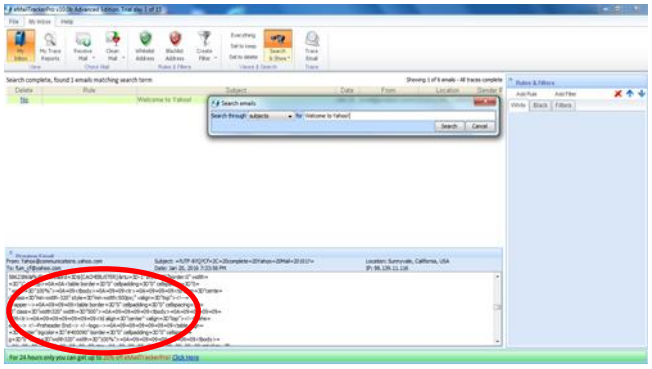


Figure 10. Search result for email subject.

4.4. MailXaminer

MailXaminer is a proprietary digital forensic software that allows the examination of email messages from both web and application-based email clients. The demo version allows fifty emails to export, which was enough for this research. Below is the major observations.

- Supports most email file formats (20+ file format, e.g. *.ost, *.pst *.olm ,EML/EMLX, Maildir, Mbox, .mbx, .edb, etc.)
- Facilitates both online and offline forensics (see Figure. 11).
- Allows previewing the details of all emails including mail body, HEX format of the email, properties, message header, MIME, email Hop, HTML format, RTF and attachments.
- Implements keyword search filtering and analysis as well as allowing us to insert a CSV file containing keyword search.

To be consistent, we used the offline feature of this tool. Similar to what we did with the other tools, we imported the file of the email into this tool and began the experiment. Figure 12 shows an example of a message preview in MailXaminer.

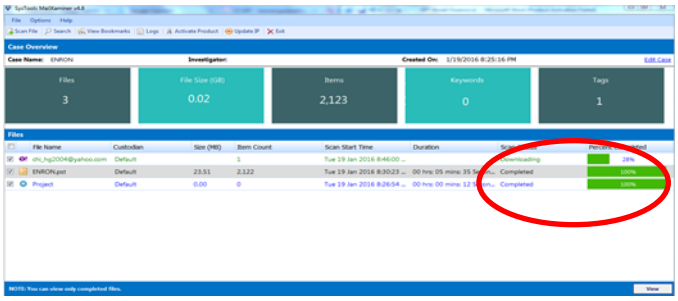


Figure 11. Offline/online Email Support in MailXaminer

The search feature works based on a name, keyword, and date search. MailXaminer allows searching of emails containing specific names or emails that have been exchanged between the

suspect and the other parties. Figure 13 shows the result of a search that we ran on our dataset for the word “Enron”.

Figure 12. Email preview on MailXaminer

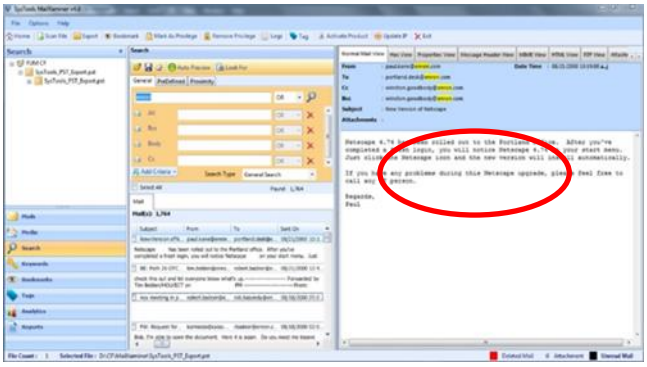


Figure 13. Search result of word "Enron" in our dataset.

Another feature of the MailXaminer is that it allows creating a date range for searching emails. This feature will help the investigators to narrow the range of emails that need to be examined. Fig. 14 shows the result of a search we performed for the name “bob” in the range of 1/21/2000 and 9/22/2000.

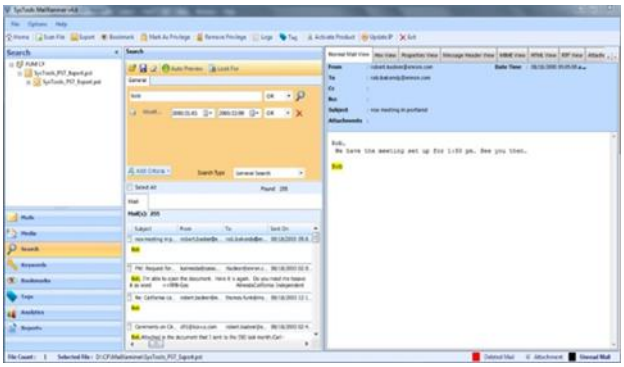


Figure 14. Search for emails that have word “bob” between 1/21/2000 and 9/22/2000.

This tool has a Predefined tab that can search for emails based on the Regular Expressions search algorithm. This search option helps the investigator to detect email message patterns with the use of category and subcategory searches such as phone numbers, URLs, addresses, postal code, and

country. In addition, the tool can bookmark a record of case related pieces of evidence. For example, Figure 15 shows emails related to CAISO Corporation that we bookmarked emails from that domain for further examination. See also [19] for similar results.

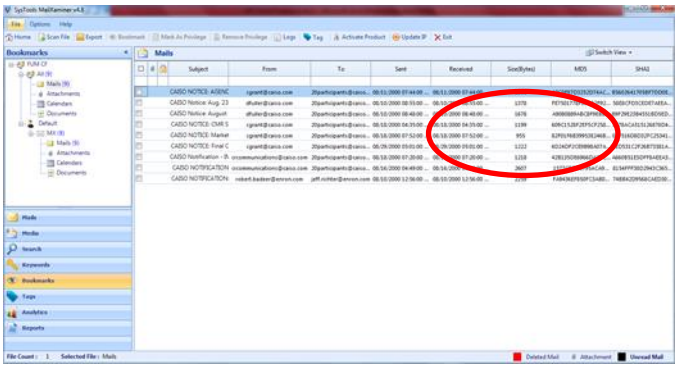


Figure 15. Bookmarked Emails under investigation.

During the investigation, we may find some important emails; we can export those emails to various different formats for analysis by other tools or create a report. The formats that are supported include Concordance ,CSV ,EML ,HTML ,HTML ,MSG ,PDF ,PRINT ,PST , TIFF. In this option, there is no filter or search option and the entire email file is exported as a report. Figure 16 shows the HTML report from emails that bookmarked in the previous step.

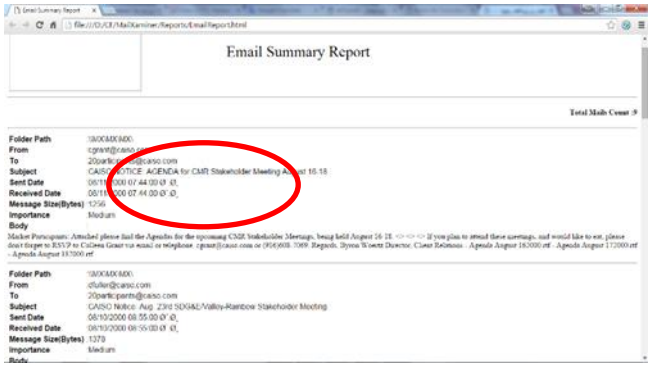


Figure 16. HTML report from bookmarked Emails

4.5. Autopsy

Autopsy is free general-purpose digital forensics software, which also has an email analysis feature. This tool also supports offline email processing. During our experiment, we identified the following properties.

- Supports offline and online files.
- The email file input does not require any specific extensions or email formats. This is because the application imports the plaintext of the email content as well as email attachments.
- Allows comprehensive keyword search
- Can generate reports of many application types such as PDF, CVS, XML, etc.
- Allows visualization of indexed files as text.

Autopsy has multiple exporting functionalities for its indexed data. We searched for the keyword "Enron" it returned 15932 results (see Figure 17). When you click on the returned files from the result, you can see the indexed text of the files with the word "Enron."

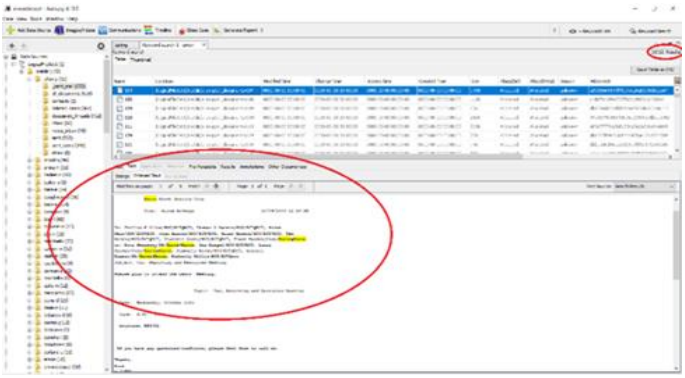


Figure 17. Keyword search results for "Enron"

Besides, a bulk search using a premade word list can be used to check for certain words in the emails. This method of searching allows the user to use a preconfigured list of related words. Figure 18 shows the application of premade word. The highlighted area shows the list of keywords.

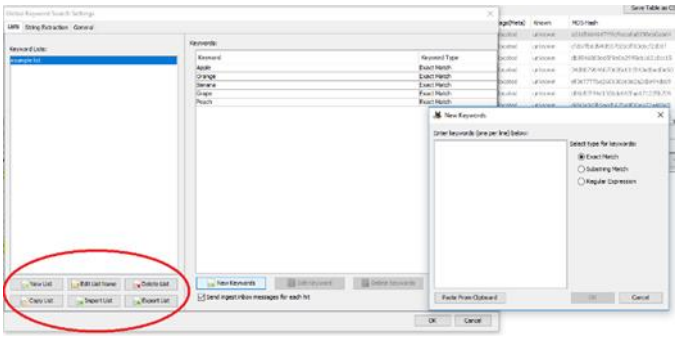


Figure 18. Example of keyword list

Autopsy allows configuration of a new list or importing preconfigured lists (xml or txt format), such as the lists of banned sports drugs, websites, chemicals, etc. (see Figure 19).

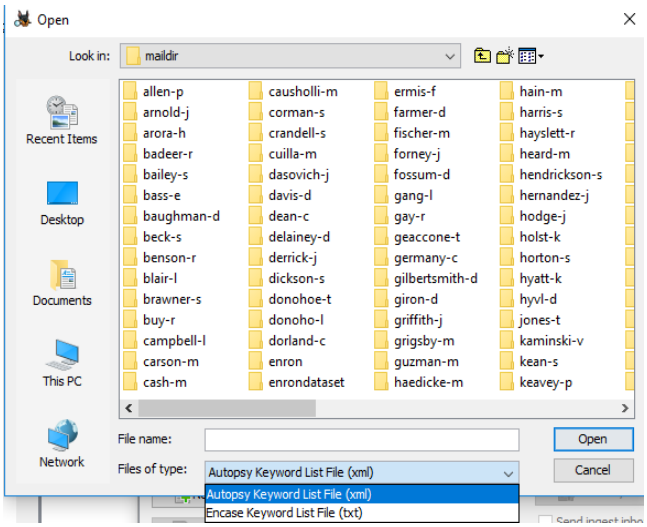


Figure 19. The keyword list import function and the supported file extensions

We can also view the Indexed email file as text (see Figure 20) The contents can also be viewed as Strings or Hex decimal (see Figure 21)

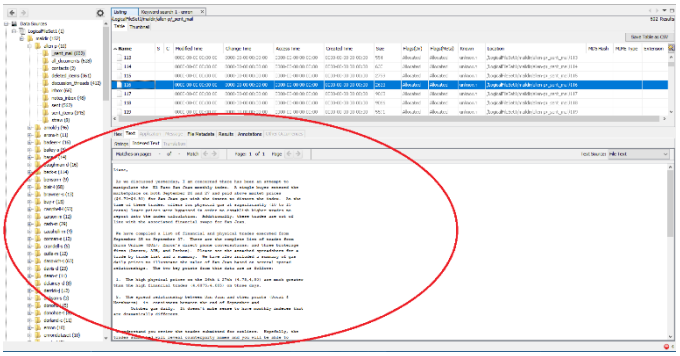


Figure 20. Text view of Autopsy index email file in Autopsy.

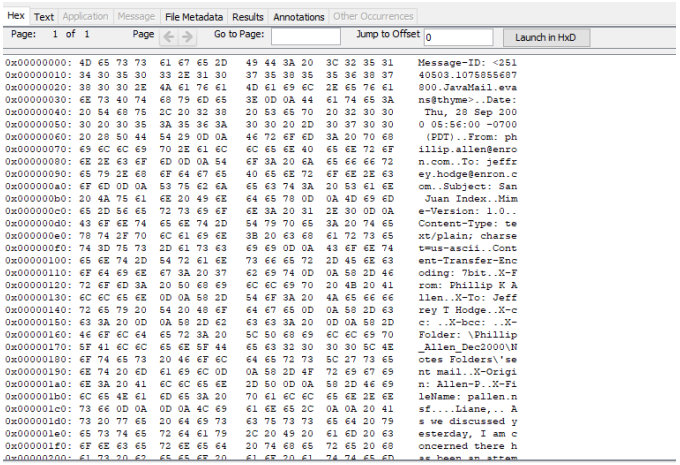


Figure 21. HEX view of indexed email file in Autopsy.

Moreover, we used the generate report function of Autopsy. Figure 22 shows the choice of a tab-delimited or a comma delimited file, querying the dataset into a table for visibility. Figure 23 shows the tab-delimited generated report. Autopsy has multiple exporting functions for its indexed data. Firstly, the user can save the table of the indexed metadata as a CSV file. Figure 24 shows the exported table, which includes metadata in CSV format for the "Enron" search.

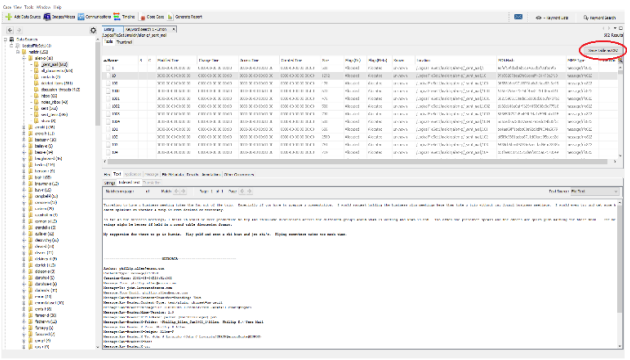


Figure 22. Shows Autopsy's save function saves table as CSV file

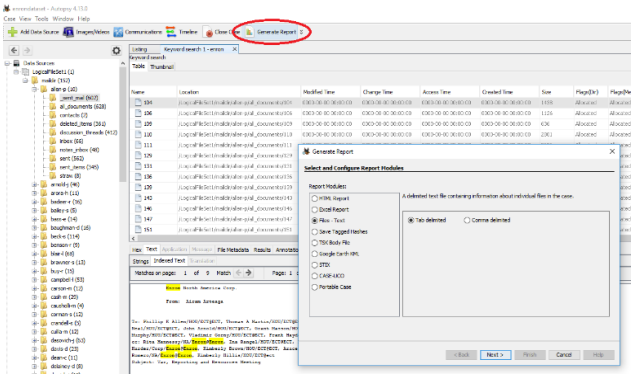


Figure 23. Shows Autopsy's Generated report function and the various report modules.

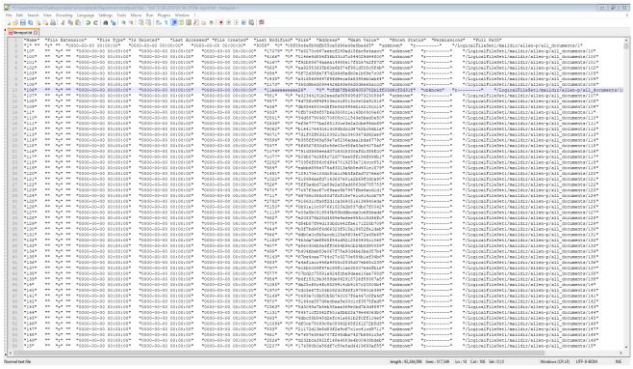


Figure 24. Generated tab delimited text report of the indexed Enron dataset files.

4.6. OSForensics

OSForensics is a proprietary digital forensics software that also has an email forensics feature. We used the free trial version. Below are the major email forensics features of this software.

- It only supports offline email file processing.
- The accepted file size and file count for indexing is restricted to the amount of available memory.
- The trial version of the product has a maximum index limit of 2500 files.
- It supports various email file formats for indexing including, .pst, .ost, .eml, .dbx, .mbox, .mbx, .eml, .msf, .msg (Mozilla, Thunderbird, Eudora, Unix mail).
- It can process the attached files.
- It has search and reporting capabilities.

We can search to filter indexed emails using the following fields: by term, from, fo/cc/bcc, date (from/to). As can be seen in Figure 25, we searched for the term "money" it returned all email results containing the word "money" in its content. In addition, we used a bulk search using a premade word list. Figure 26 shows the result of premade search lists. Similar to Autopsy, the example word lists included in the tool are a list of common words categorized by their topic, such as a list of banned sports drugs, websites, chemicals, and more. We can create more custom lists and add to the tool. The tool allows the user to sort the returned search results by score, name, date, filename, extension, and tag for easier viewing of filtered emails. This feature is extremely useful, as it saves investigator's time.

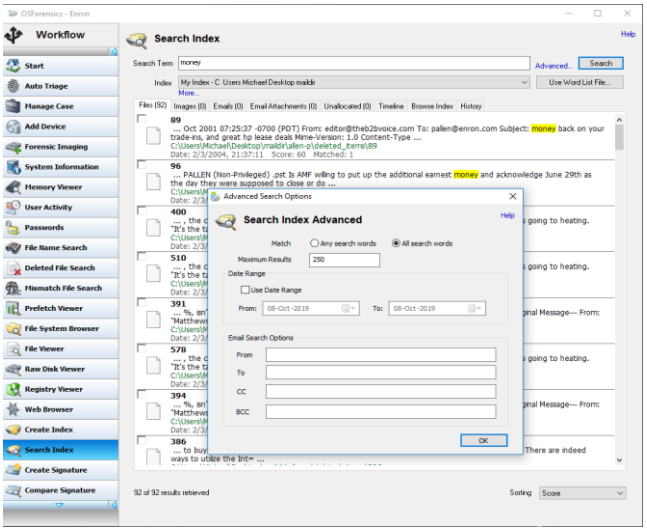


Figure 25. The search index function of OSForensics

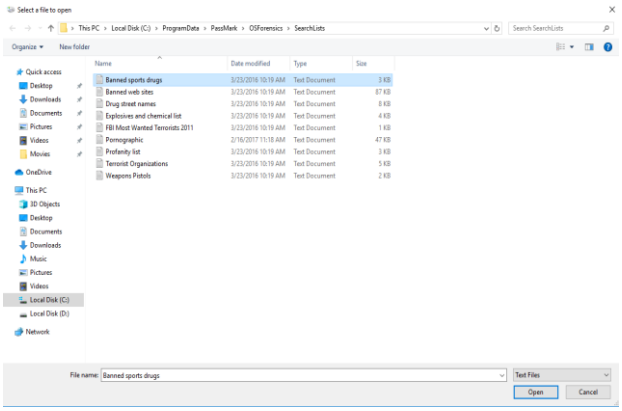


Figure. 26 The search list in OSForensics.

OSForensics allows viewing indexed emails as text in two ways, by double-clicking on search Windows and by using an email-viewing tool. For example, Figure 27 shows the text view of the indexed email file.

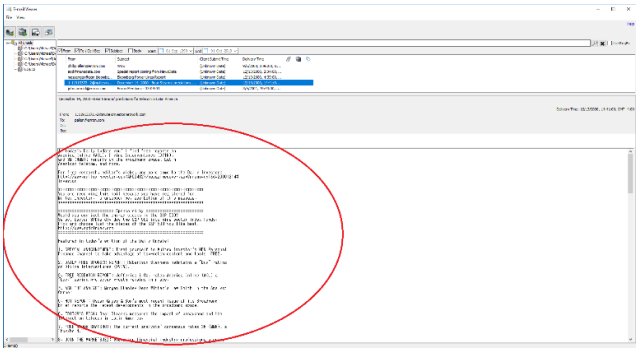


Figure 27. Text view of the indexed email file using email viewer tool.

The tool can use the result of the search to a generate report. This report can be exported in HTML or PDF format (see Figure. 28.) We should note that emails could be exported one by one using the Email Viewer Tool. Email files loaded into the Email Viewer Tool has only one export option: Base Name (ie.<base name>_index.html). As shown in Figure 29, this method of export creates five files in the export directory inlcuding <filename>.txt, which exports the email into text format. The other four files are the results of splitting the email into four different parts: header.txt, index.html, menu.html, and print.html.

To avoid the four different parts from being exported with the email, a workaround option is to export the file using the print functionality and save the file in PDF format, which creates just one PDF file in the export directory.

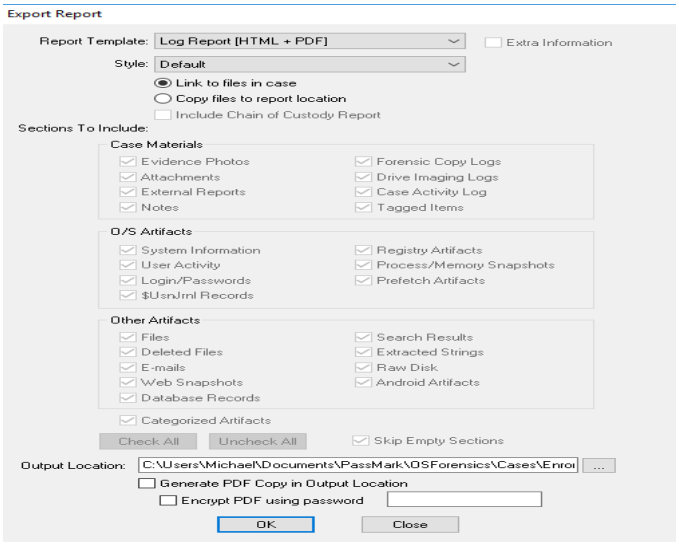


Figure 28. The export report feature of the OSForensics.

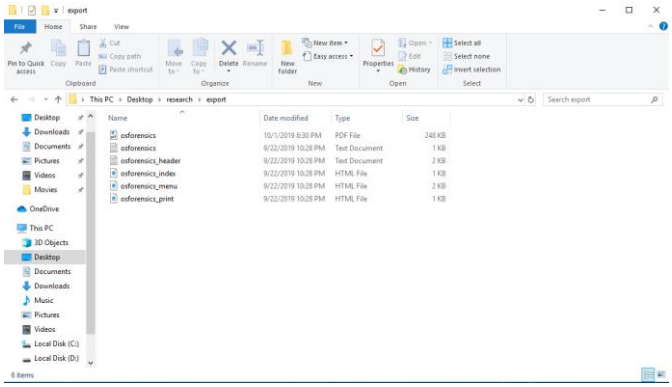


Figure 29. The export of index emails to a PDF file.

5. EXPERIMENT RESULT ANALYSIS

Aid4Mail is a suite of eight tools and supports almost all email formats. Our experiment shows that Aid4Mail can perform limited searches and can create reports based on those searches but cannot analyze the generated email reports. This is because other applications such as PDF reader; MS Word; CVS; etc. are not integrated into this tool. Moreover, the tool has a static and inflexiblee Graphical User Interface (GUI) and has no dedicated search or report generation option in the GUI.

Paraben accepts the Maildir format and has comprehensive keyword search features, bookmarking, advanced Boolean searching, and searching within attachments. We were able to analyze the search results within the tool and generate reports based on keyword search results. This is because other applications such as PDF reader, MS Word, etc. are integrated into the tool. It also has several search filters that help an investigator to find items of interests from the emails. In addition, the tool can examine email headers and bodies, provide information based on the search filter including contents from attachments. We found the GUI feature of this tool very helpful and easy to use.

MailXaminer supports most email file formats (36 file type) like: *.ost, *.pst , *.olm ,EML/EMLX ,*maildir* , MBOX , *.mbx ,*.edb etc. The tool supports both online and offline forensics. However, for consistency purpose we only used the offline feature of this tool. Using MailXaminer, we were able to import email files and perform keyboard search for name, email header, date, etc. Investigators can search for emails containing specific names or emails that have been exchanged between the suspect and receivers. Generating reports based on keyword search is relatively easy due applications, being integrated into the tool.

eMailTrackerPro is different from the above-mentioned tools in that it only supports live investigation. Due to the use of different email format, this tool does not support importing email files and folder. Therefore, we must connect the tool to the email accounts or import header of an email manually to analyze that email. The only offline feature available in this tool is importing email headers manually to the tool and trace the email path. It is a powerful tool for searching within the emails file online and can create report based on search results. The GUI feature of the tool is good but does not have all the features available in other tools.

Autopsy does not support Maildir format. However, we imported the Enron email files into the Autopsy without an extension, using the logical files data source input. The logical file input does not require specific extensions or email formats for the file input as the application imports

the plaintext of the file data. It has a comprehensive keyword search feature and wordlist for a bulk word search. The keyword search feature returns the search result in a table, which can be sued to generate reports. It has comprehensive features to process and analyze large sets of data and a feature to handle and store multiple cases, The GUI in Autopsy is friendly.

OSForensics tool supports various email file formats for indexing. It is a powerful tool can accept a large dataset of emails. The tool is capable of indexing. Its search function has comprehensive features such as date range, email headers, and email body to filter the search results. It can also utilize a preconfigure lists of words for filtering. However, a major weakness of this tool is that it does not allow mass exporting the filtered emails, which is necessary in processing large datasets of emails. Moreover, the tool lacks any report generation or analysis features to handle the data based on the search results. This is because the tool is not a dedicated email forensics tool.

6. CONCLUSION AND FUTURE WORK

In this research, we experimentally examined several email forensic tools and evaluated the features such as, whether the tool supports online or offline files, filtering, search, report generation, and thier graphical user interface. We used the Enron email dataset file as input to each tool. We evaluated the above features of the tools. The results demonstrate that the selection of a tool should be done with extreme care. This is because, although the tools have some common features but they also may lack some of the desired features. Therefore, the investigator should carefully examine the email forensics tools before they commit to a particular one. If necessary, they may use two different tools with diverse features. In summary, the selection of a tool depends on the needs of the investigators and the circumstances of the case under investigation.

This research can be extended in several ways: 1) Repeat the same experiment with a Proprietry version of the tools to examine full strength of the email forensics tools. 2) Use additional tools such as EmailTracer, Adcomplain, Internet Evidence Finder (IEF), FINALeMAIL, etc. 3) Compare the performance of the online features of the tools. 4) Use more email files from the dataset and on machines with different operating systems.

REFERENCES

[1] G. Chabra, and Dilpreet Singh Bajwa (2015). "Review of E-mail System, Security Protocols and Email Forensics." *International Journal of Computer Science and Communication Networks*, Vol 5, No. 3, pp. 201-211.

[2] P.P. Hatole, and Shobha K. Bawiskar (2017). "Literature Review of Email Forensics." *Imperial Journal of Interdisciplinary Research (IJIR)*, Vol. 3, No. 4, pp. 1436-1439.

[3] M. T. Banday (2011). "Techniques and Tools for Forensics Investigation of Emails." *International Journal of Network Security & Its Applications* (IJNSA), Vol. 3, No. 6, pp. 227-241.

[4] F. Cohen (2009). "Bulk Email Forensics." *IFIP International Conference on Digital Forensics. Springer*, chapter 4, pp. 51-67.

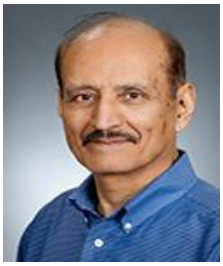
[5] Enron Dataset. https://www.cs.cmu.edu/~enron/

[6] R. Hadjidj, Mourad Debbabi, Hakim Lounis, Farkhund Iqbal, Adam Szporer, and Djamel Benredjem (2009). "Towards an integrated e-mail forensic analysis framework." *Digital Investigation* Vol. 5, pp. 124-137.

[7] N. Meghanathan, Sumanth Reddy Allam and Loretta A. Moore (2009). "Tools and Techniques for Network Forensics." *International Journal of Network Security & Its Applications (IJNSA)*, Vol, 1, No. 1, pp. 14-25.

[8] J. Paglierani, Mike Mabey and Gail-Joon Ahn (2013). "Towards Comprehensive and Collaborative Forensics on Email Evidence.". *9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing*. pp. 11-20.
[9] V. K. Devendran, Hossain Shahriar, Victor Clincy (2015). "A Comparative Study of Email Forensic Tools." *Journal of Information Security*. Vol. 6, No. 2, pp. 111-117.
[10] S. J. Stolfo, Shlomo Hershkop (2005). "Email Mining Toolkit Supporting Law Enforcement Forensic Analyzes." *National Conference on Digital Government Research, Atlanta, Georgia*, pp. 1-2.
[11] S. R. Khan, Smita M. Nirkhi, R. V. Dharaskar (2013). "E-mail Data Analysis for Application to Cyber Forensic Investigation using Data Mining." *International Journal of Applied Information Systems*, pp. 1-4.
[12] F. Armknecht and Dewald, A. (2015). "Privacy Preserving Email Forensics." *Digital Investigation*, Vol. 4, pp. 127-136.
[13] Aid4Mail, Email Forensic. http://www.aid4mail.com/
[14] EMailTrackerPro. http://www.emailtrackerpro.com/
[15] MailXaminer. http://www.mailxaminer.com
[16] Paraben (Network) E-mail Examiner. http://www.paraben.com/email-examiner.html
[17] Autopsy. Open Source Digital Forensics. http://sleuthkit.org/index.php
[18] OSForensics. https://www.osforensics.com/
[19] A. Ghafarian (2019). "Capabilities of email forensics tools." *Proceedings of the Computing Conference*. London, UK, pp. 514-528.

AUTHORS



Ahmad Ghafarian is a Professor of Computer Science and cybersecurity at the University of North Georgia. He received his Ph.D. and Msc. in computer science from University of Glasgow and his B.sc. in Mathematics from Mashhad University. He alos obtained a Postdoctoral fellowship in information security. His teaching and research interests lie primarily in the area of cybersecurity, inlcuding, various aspects of digital forensics, social media privacy and security, ransomware analysis, security of connected cars and internet of things. He has over twenty five years of teaching and research experience and about fourty peer reviewed publications. He secured several rsearch grants and involves students in his research activities.

Ash Mady, Ph.D., Department Head - Computer Science & Information Systems. Mike Cottrell College of Business. University of North Georgia. Mady received his Ph.D. degree in business administration with a research focus in information security from Kennesaw State University. He also has degrees in Computer Science, Physics, and Chemistry. His research interest and active projects are in the areas of Cybersecurity, Artificial Intelligence, and Financial Technology or Fintech. He has led several projects and awarded grants in work related to blockchain, technology adoption, cybersecurity and artificial intelligence. He is a member of the Special Interest Group on Information Security and Privacy. He has over twenty-five years of professional experience in academia, management, and software engineering.

Kyung Park is an undergraduate research assistant majoring in computer science with a concentration in Information Assurance and Security, and a minor in mathematics at the University of North Georgia. He is interested in researching and learning about all aspects of Cybersecurity.