**University of Victoria**

**Engineering & Computer Science Co-op**

**Work Term Report**

**Term (Spring) 2018**

**Forensic Investigation Of E-Mail Headers**

**NOKIA**

**A000001803/4L AA EP Sec Threat Intel Lab Alcatel-Lucent**

**Kanata, Ontario, Canada**

**Maninder Singh**

**V00879900**

**Work Term Number-1**

**Masters in Telecommunication and Information Security**

[**manindersingh@uvic.ca**](mailto:manindersingh@uvic.ca)

**April 20, 2018**

**In partial fulfillment of the academic requirements of this co-op term**

**Supervisor's Approval: To be completed by Co-op Employer**

This report will be handled by UVic Co-op staff and will be read by one assigned report marker who may be a co-op staff member within the Engineering and Computer Science Co-operative Education Program, or a UVic faculty member or teaching assistant. The report will be either returned to the student or, subject to the student’s right to appeal a grade, held for one year after which it will be destroyed.

I approve the release of this report to the University of Victoria for evaluation purposes only.

Signature: Position: Date:

Name (print): E-Mail: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

For (Company Name)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Maninder Singh

383 Kinghorn Crescent

Kanata, Ontario, K2K 2R6

April 20, 2018

Dr. Kin Li

Dept. of Electrical & Computer Engineering

University of Victoria

P.O. Box 1700

Victoria, B.C. V8W 2Y2

Canada

Dear Dr. Kin Li

Please accept the accompanying Work Term Report entitled “Forensic Investigation Of E-Mail Headers.”

This report is the result of first work term completed at Nokia (formerly Alcatel-Lucent) Kanata, Ontario. I was working in the position of malware research assistant in Nokia’s Threat Intelligence Lab. As a Co-op student I was responsible to read research articles related to the latest malware attacks, then write signatures that alert in the field if that kind of malware is active, doing passive analysis for the existing signatures to make sure they alert on right kind of traffic with no false positives.

Through this course of the term, I got the opportunity to learn valuable concepts about malware, their working behaviour, how they spread, and strategies to stop them. I feel this knowledge will be very beneficial for me in the future co-op terms and further in my career.

I would like to thank my manager Mr. Paul Edwards, security engineer Mr. John, and Mr. Pierre for sharing their knowledge and experiences with me.

Sincerely,

Maninder Singh

NOKIA, Kanata, ON

Attachment: Forensic Investigation Of E-Mail Headers

**TABLE OF CONTENTS**

LIST OF FIGURES.….….………………………………………………………..…….………. iv

SUMMARY…….……………………………………………………………………..………… v

1.0 INTRODUCTION……..…………….……………………….……………………………… 1

2.0 EMAIL ARCHITECTURE…………………….………………………………...………….. 2

3.0 EMAIL FORENSIC TECHNIQUES…….………………………………………………….. 3

3.1 HEADER ANALYSIS…….…………………….……………………………..……….. 3

3.1.1 Sender’s Email Address: ….………………………………………………….. 5

3.1.2 Detecting Fake Email Addresses: ……………………………………………. 5

3.1.3 Examination by Message Initiation Protocol (HTTP vs SMTP): ………...….. 6

3.1.4 Scrutinizing Message ID: …………………………………………………….. 6

3.2 BAIT TACTICS …….…………………….……………………………………………. 7

3.3 SERVER INVESTIGATION …….………….…………………………………………. 7

3.4 NETWORK DEVICE INVESTIGATION …...……….………………………………... 8

4.0 EMAIL FORENSIC TOOLS …….………………………………………………………….. 8

4.1 eMailTrackerPro ..………………………………………………………………………..8

4.2 FORENSICS USING KALI LINUX TOOL- MALTEGO.…………………………… 13

5.0 CONCLUSION...……….…………………………………………………………………... 16

6.0 RECOMMENDATIONS...……….…………………………………………………...……. 17

Cited references…………………………………………………….……………………………17

**LIST OF FIGURES**

Figure 1: How email actually works ……………………………………………...……...……… 3

Figure 2: Header of fraud email …………………………………………….…………………... 4

Figure 3: Header of forged Email……………………………...………………………………... 4

Figure 4: eMailTrackerPro scan …………………………………………..…………………….. 6

Figure 5: Geographical trace route of email …………………………………………….………. 7

Figure 6: Maltego tool scan …………………………………….……………………………...... 7

Figure 7: Scattered tree scan of domain……………..………………………………………...... 11

Figure 8: Email verification using tree scan …………………………………………………… 13

**SUMMARY**

Over the last 10 years, email has emerged as the most imperative strategy over the web for the trading of messages, files, and different exchanges from the PCs as well as from other keen gadgets like cell phones and tablets. Because of this broad utilization of email for different exercises, email protocols have been secured through different strategies, however, cybercriminals are yet abusing it for different malicious exercises over the web. Email forensic includes the investigation of the source and header of the email message with the assistance of different software tools and strategies to explore the realness of the email. This examination will help to understand the basic architecture of email header and different email actors and segments engaged in the examination of email.

**1.0 Introduction**

Email is the most continuous strategy for trading data between two foundations. Email architecture comprises the different hardware and software components including clients for sender and receiver. Every Sender and receiver customer has services installed on it, which are required for communication. Both the sending and receiving servers are connected to the web, however, the sender's and receiver's client does not. In spite of the fact that, email communication has been designed as such to make things simple, powerful and efficient as it follows guaranteed delivery mechanism. In any case, we think that it's exceptionally normal that email has been the focal point of different malicious attacks. This incorporates spam, phishing, malicious attachments and others. Because of broad utilization of email from personal to business use, it has turned into the prime focus of attackers and other spammers. This questions the integrity and security of email.

In the most recent couple of years, numerous innovations have been created for investigating and securing the e-mails, which incorporates spam detection tools, phishing mail detectors, and other email filters. The significant purpose of building up this kind of advances is to direct a measurable examination of messages with the goal that the unauthentic sources are distinguished and the damage is avoided. The devices created in these years are built in a segregated way rather than working on the issues found in the past tools or upon earlier research. The greater part of tools are not intended to solve any specific cyber or crime related problem but they are mostly used to recover or gain information. This examination endeavors to compare the previous tools related to the forensic investigation and will try to recommend some new solution. The following couple of sections will define the architecture of email framework, followed by basic email headers and actors involved.

**2.0 E-MAIL ARCHITECTURE**

Email framework includes various hardware and software components, which help in guaranteed conveyance over the system. Ensured delivery implies if the email is sent to the specific target framework, it will be conveyed irrespective of the availability of the target system. The system compromises of the following objects:

1. Sender Client
2. Receiver Client
3. Sender Server
4. Receiver Server

The sending and receiving servers are always connected to the internet but same is not the case with sender and receiver client as they are connected to the internet whenever required.

Let us take an example of very popular Alice and Bob sending the mails to each other systems. Alice composes an email on her system, which is called client for Bob and sends it to her Sending server ‘smtp.a.org’. After this, the sending server does the lookup operation for the email exchange record of the receiving server called ‘b.org’ through DNS (Domain name system) protocol on DNS server ‘dns.b.org’. The work of DNS server here is to respond to the request with highest priority mail exchange server ‘mx.b.org’ for the domain ‘b.org’. Sender server establishes SMTP connection with the receiver server, does guaranteed delivery to the mailbox of receiver server, and further drops the mail on the local mailbox on client’s computer using IMAP and POP protocols. Bob Can read the message stored in his server mailbox without downloading it on the local mailbox using web application.

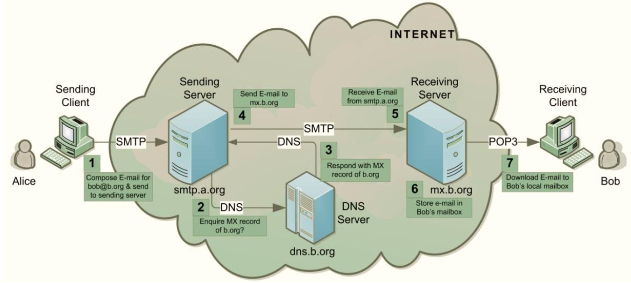


Figure 1: How email actually works[3]

**3.0 EMAIL FORENSICS TECHNIQUES**

Email forensics alludes to the investigation of email content and its source as to distinguish the genuine sender and recipient of the mail. Along the side, the data of transmission and including the time, detailed email transaction records, and the number of hops the email has experienced is additionally contained in the examination report depending upon the kind of Examination and email investigation method utilized. Different distinctive methodologies are considered and some of them are described underneath.

**3.1 HEADER ANALYSIS**

Emails are comprised of two primary parts; message header and message body. The header of the body comprises of routing information regarding the email and contains information for source and destination of email, the IP address and timeline of message.

Email Headers follows the bottom-up approach of the organization. This demonstrates the email was given from the source at the bottom of the header to the ones at the top of the header. Presently, these machines are called as Message Transfer Agents (MTAs) and they individually add a “got” section to the header of the email, which is sometimes referred to as “received header”, and are analogous to postmarks in conventional postal systems. “The received” sections will be in order like a pile of pancakes, with the individual receiving the email on top of the stack. In the figure underneath, we could see four received sections, this shows that the four MTAs were involved in the delivery of email message with the lower recipient segment from the

original sender.

Delivered-To: nagra.rurka@gmail.com

**Received: by 10.157.60.105 with SMTP id j38csp421875ote; Thu, 1 Feb 2018 21:53:24 -0800 (PST) X-Google-Smtp**-Source:

AH8x227IgICJjePLahY62IVVOX4WbMkaPJD5QfEwEaFaOu6XCSDXKMbWl2awThp3q6zyX8vI9A0w

**X-Received: by 2002:a17:902:4a0c:: with SMTP id w12v6mr25473303pld.17.1517550804324;**

Thu, 01 Feb 2018 21:53:24 -0800 (PST) ARC-Seal:

i=1; a=rsa-sha256; t=1517550804; cv=none; d=google.com; s=arc-20160816;

ARC-Authentication-Results: i=1; mx.google.com; dkim=pass header.i=@uvic.ca header.s=post header.b=nKm+IIBo; spf=pass (google.com: domain of gcmentor@uvic.ca designates 142.104.96.14 as permitted sender) smtp.mailfrom=gcmentor@uvic.ca; dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=uvic.ca

Return-Path: <gcmentor@uvic.ca > **Bottom Up Approach**

**Received: from hr.srvc.uvic.ca (hr.srvc.uvic.ca.**

**[142.104.96.14]) by mx.google.com with ESMTPS id s3v6si1151638plb.171.2018.02.01.21.53.24 for**

<nagra.rurka@gmail.com>

(version=TLS1\_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);

Thu, 01 Feb 2018 21:53:24 -0800 (PST)

**Received-SPF: pass (google.com: domain of gcmentor@uvic.ca designates**

**142.104.96.14 as permitted sender) client-ip=142.104.96.14;** AuthenticationResults: mx.google.com;

dkim=pass header.i=@uvic.ca header.s=post header.b=nKm+IIBo; spf=pass (google.com: domain of gcmentor@uvic.ca designates 142.104.96.14 as permitted sender) smtp.mailfrom=gcmentor@uvic.ca; dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=uvic.ca

Received: from localhost (localhost [127.0.0.1]) hr.srvc.uvic.ca

(Postfix) with ESMTP id F2989300082D for <nagra.rurka@gmail.com>; Thu,

1 Feb 2018 21:53:23 -0800 (PST)

X-Virus-Scanned: amavisd-new at uvic.ca

Received: from hr.srvc.uvic.ca ([127.0.0.1]) by localhost

(hr.srvc.uvic.ca [127.0.0.1]) (amavisd-new, port 10024) with ESMTP id 8rZas2QfDij for <nagra.rurka@gmail.com>; Thu,

1 Feb 2018 21:53:23 -0800 (PST)

**Received: from [192.168.11.116] (d173-183-76-60.bchsia.telus.net**

**[173.183.76.60]) by hr.srvc.uvic.ca (Postfix) with ESMTPSA id 6695F3000828 for <nagra.rurka@gmail.com>; Thu,**

1 Feb 2018 21:53:23 -0800 (PST)

DMARC-Filter: OpenDMARC Filter v1.3.2 post.engr.uvic.ca 6695F3000828

This header information is utilized to examine the header of the email message to determine its authenticity. For instance, to determine the source of the email, an examination ought to be finished by inspecting the received section at the bottom of the header and work the way up in bottom to top approach. In the case of emails, it is essential to look at the logs of all servers in the received chain at earliest. Since the logs are documented as often as possible by ISPs, time is a vital factor in email cases as HTTP and SMTP. Once the logs are archived, it takes effort and time both to decompress the log files which are needed to trace emails. Some of the emails have fake heads and fake “from” address to trap individuals into trusting that its an authenticated source, so alert and tight scrutiny shall be practiced in the investigation of the email header.

**3.1.1 Sender’s Email address:** The sender’s email address can be found after the “From’ section of header. Its not necessary that it is found only at that place but also can be found under other sections depending on the email client used. These sections can be one of the following:

• X-Originating E-mail

• X-sender

• Return-Path

The headers that start with a "X-" implies that they are X-Headers. X-headers are embedded by email clients or the applications, which uses it for processing the email and pass information to email handling programs. These can be presented by the large vendors and grabbed by others for use. This demonstrates that X headers can be considered as a true standard.

**3.1.2 Detecting Fake Email Addresses:** The email address of the sender can be easily faked and can be extremely hard to identify. In the bottom-up approach of the header, if the “received” section does not coordinate the server of the email address, this suggests that the email is fake or has been manipulated in some way. An example of that is shown below:

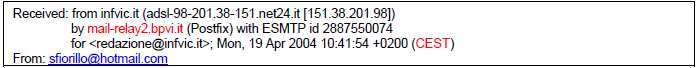


Figure 2: Header of the fraud email

The thing to notice in the above email address in the “from” field has “Hotmail.com” as a domain for the email while in the received segment of the header there is no Hotmail server mentioned. This clearly shows how there is a mismatch in the header information. What's more, the time stamp on the received segment for the header demonstrates the CEST time zone while there are no Hotmail servers in Europe.

**3.1.3 Examination by message initiation protocol (HTTP vs SMTP):** Whenever an email is sent from web-based email client utilizing “HTTP” or “HTTPS”, there is always a sign in the bottom-received section of the mail. If the header section shows “with SMTP” or “with ESMTP” used, it means that the email was sent either using manual means or through SMTP client software. So if so, it implies that the email is fashioned and not the genuine occurrence.

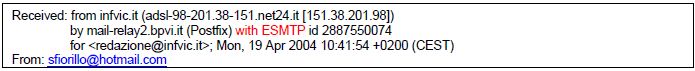


Figure 3: Header of the forged email

**3.1.4 Scrutinizing Message ID:** Message ID is a standout amongst the most vital thing which is utilized as a part of email investigation. Message IDs are made by the email customers and also the SMTP servers, which gets the message and pass it along to its destination. In the illustration given underneath, there are three email servers, which were associated with the conveyance of the message, and each of them assigned an ID to the message.

All these are some of the ways through which we dissect, look at the header of an email, and come to know whether the email has been satirized or not. These are the basics of header forensics, which is utilized alongside the machine learning algorithms to check it automatically. They come out as a product or software with these algorithms and strategies executed in them to assist innocent individuals with the email security issue.

**3.2 BAIT TACTICS**

In bait tactics examination, an email with a tag http:"<imgh src>", having a connection to a picture source at some other destination which is being monitored by the investigators, is sent to the sender of the email under scrutiny. At whatever point an email is clicked or opened, an entry is logged into the system containing the IP address of the recipient (sender of the email under investigation) is copied on the HTTP server, which is facilitating the picture, and this way attacker is followed. This does not work for the situation when the recipient (sender of the email under scrutiny) uses a proxy server. In that case, the IP address of the proxy server will be recorded as opposed to the real IP Address.

The Logs on a proxy server can be useful to track the sender of the email, which is under investigation. If the logs from the proxy server are not accessible because of some specific reason, then the investigators may send the tactic email, which can contain the following:

a) Embedded Java Applet that runs on the receiver’s computer

b) HTML page with ActiveX object.

These both can help to extract IP address of the receiver computer and email it to the investigators.

**3.3 SERVER INVESTIGATION**

In the server Investigation, different duplicates of conveyed emails and server audit logs are explored to recognize the source of an email message. Emails, which are not available from the sender or receiver client and is impossible to recover, can be asked for from the ISP servers as the majority of them stores the duplicate of all messages after their deliveries. Besides, the logs, which are kept up by the servers, can be studied in order to track the address of the PC responsible for making the email exchange. However, the server monitors the duplicates of email and server logs only for the time being periods and may not coordinate with the person who is examining. In addition, SMTP servers, which store essential information like Visa data and other sensitive data pertaining to the owner of the mailbox, can be utilized to recognize the individual behind an email address.

**3.4 NETWORK DEVICE INVESTIGATION**

This is another type of email examination in which logs kept up by the network devices, for example, switches, firewalls, and routers are utilized to research the source of an email message. This is a complex form of investigation and is only utilized when the logs of proxy or ISP server are unavailable because of some reasons. For example, when ISP server or proxy server has no logs with them as they don’t maintain it or there is lack of cooperation by ISPs.

**4.0 EMAIL FORENSIC TOOLS**

There are a variety of tools, which may help you in the investigation of source and content of email message to examine the attack or the malicious intent of the intrusion. These tools help in finding the real sender with the assistance of investigation algorithms and tries to discover the sender IP and number of hops it has taken while reaching the destination. This additionally incorporates the way navigated by the message and distinguishes the spam and phishing systems. Some of the tools, which are utilized in the investigation as a part of the examination, are given as below:

**4.1 eMailTrackerPro**

This tool helps in analyzing the headers of the email and recognizes the IP address of the machine that sent the message so that the sender can be tracked down. It also helps in examining the way navigated by the email and shows the location and number of hops taken by the email once it left the sender client pc and reached the receiver client pc. Alongside, this tool also helps in verifying the actual IP address of the sender with the message id and Hop name. Various emails can be traced with this software and can monitor them effectively. The Geographical area of the IP address is really the location vector, which helps in deciding the threat level or legitimacy of an email message. Moreover, it pinpoints the city, where the most emails originated from. In addition, it identifies the network provider or ISP of the sender and provides the contact information for the investigation.

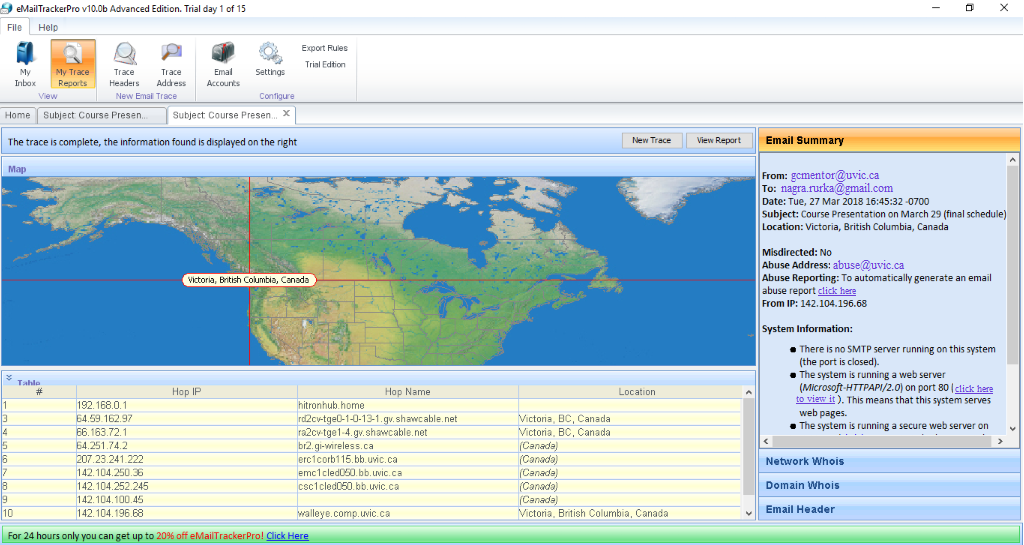


Figure 4: eMailTrackerPro scan

The actual path of the Sender’s IP address is reported in a routing table, which provides the additional location information that further aides in determining the sender’s true location. There is also an abuse reporting feature in it that can be used to make further investigation easier. It does another work of checking the email against the popular DNS blacklists, for example, Spamcop, which additionally helps in shielding against the spam and malicious emails. The highlight feature of this tool is abuse reporting which can create a report that can be sent to the Internet Service Provider(ISP) of the sender. The ISP can further take steps to prosecute the account holder and put a full stop to spam messages.

Below is the example of the email, which was traced and investigated . This email was received from an organization in Victoria, Canada and shows the email header used for the investigation. The second screenshot shows the number of hops it took after leaving sender system and before reaching it to receiver. The below screenshots are not taken from third party so no reference could be added. Here is the full report:

Computer 142.104.196.68 has been found. It is almost certainly located in Victoria, British Columbia, Canada as it has an exact match in the eMailTrackerPro database.

The sender's IP was - 142.104.196.68

The sender of this email appeared to have the address gcmentor@uvic.ca. This information is easily faked so should not be treated as conclusive.

The following map shows the route between sender and the entity to which he traced. A solid line represents a hop to a known location, and a dotted line represents a hop to a guessed location.



Figure 5: Geographical trace of route of email

|  |  |  |
| --- | --- | --- |
| **Address of Hop** | **Name of Hop** | **Location** |
| 206.87.191.253 |  | *Canada* |
| 142.104.252.65 |  | *Canada* |
| 142.104.100.45 |  | *Canada* |
| 142.104.196.68 | walleye.comp.uvic.ca | **Victoria, British Columbia, Canada** |

|  |  |
| --- | --- |
| **Network Owner Information** | **Domain Owner Information** |
| *The following information refers to the network on which this system lies.*     # The following results may also be obtained via:  # https://whois.arin.net/rest/nets;handle=NET-142-104-0-0-1?showDetails=true&showARIN=false&showNonArinTopLevelNet=false&ext=netref2  ##  # ARIN WHOIS data and services are subject to the Terms of Use  # available at: https://www.arin.net/whois\_tou.html  #  # If you see inaccuracies in the results, please report at  # https://www.arin.net/public/whoisinaccuracy/index.xhtml  #  **From:** [**gcmentor@uvic.ca**](mailto:gcmentor@uvic.ca ) **To: nagra.rurka@gmail.com**  **From IP:142.104.196.68**  NetRange: 142.104.0.0 - 142.104.255.255  CIDR: 142.104.0.0/16  NetName: UVIC  NetHandle: NET-142-104-0-0-1  Parent: NET142 (NET-142-0-0-0-0)  NetType: Direct Assignment  OriginAS:   Organization: University of Victoria (UNIVER-183-Z)  RegDate: 1992-01-29  Updated: 2012-04-02  Ref: https://whois.arin.net/rest/net/NET-142-104-0-0-1      OrgName: University of Victoria  OrgId: UNIVER-183-Z  Address: Network Services, P.O. Box 3045  City: Victoria  StateProv: BC  PostalCode: V8W-3P4  Country: CA  RegDate: 2008-06-30  Updated: 2009-10-30  Ref: https://whois.arin.net/rest/org/UNIVER-183-Z      OrgTechHandle: NETAD28-ARIN  OrgTechName: NetAdmin  OrgTechPhone: +1-250-721-7654   OrgTechEmail: netadmin@uvic.ca  OrgTechRef: https://whois.arin.net/rest/poc/NETAD28-ARIN    OrgAbuseHandle: ABUSE427-ARIN  OrgAbuseName: Abuse  OrgAbusePhone: +1-250-721-7687   OrgAbuseEmail: abuse@uvic.ca  OrgAbuseRef: https://whois.arin.net/rest/poc/ABUSE427-ARIN    RTechHandle: NETAD28-ARIN  RTechName: NetAdmin  RTechPhone: +1-250-721-7654   RTechEmail: netadmin@uvic.ca  RTechRef: https://whois.arin.net/rest/poc/NETAD28-ARIN    #  # ARIN WHOIS data and services are subject to the Terms of Use  # available at: https://www.arin.net/whois\_tou.html  #  # If you see inaccuracies in the results, please report at  # https://www.arin.net/public/whoisinaccuracy/index.xhtml  # | *The following information describes the organization or individual who registered the domain name****uvic.ca****. There can be many domain contacts however Corporate and Administrator are usually the best contact references.*  Domain name: uvic.ca  Domain status: registered  Creation date: 2000/10/02  Expiry date: 2020/04/07  Updated date: 2018/01/26  DNSSEC: Unsigned    Registrar:  Name: Webnames.ca Inc.  Number: 70    Registrant:  Name: University of Victoria    **Administrative contact:**  **Name: Jane Godfrey**  **Postal address: 3045 Network Services Clearihue Building**  **Victoria BC V8W3P4 Canada**  **Phone: +1.2507217673**  Fax: +1.2507218778  Email: jgodfrey@uvic.ca        Name servers:  dns1.uvic.ca 142.104.6.1  dns2.uvic.ca 142.104.80.2  ns4.uvic.ca 206.12.58.50  ns5.uvic.ca 206.12.58.52 |

Full Report for Header analysis of your email

* The system is running a mail server on port 25. This means that this system can be used to send email.
* The system is running a web server (Microsoft-HTTPAPI/2.0) on port 80. This means that this system serves web pages.
* The system is running a secure web server on port 443. This means that this system serves encrypted web pages. It therefore probably handles sensitive data, such as credit card information.
* There is no FTP server running on this system (the port is closed).

The above report shows everything the tools can get from the email header giving in the beginning. It uncovers exceptionally valuable data, which can help the specialist to check if the message is validated, or not. It incorporates the server's name as well which cannot be spoofed by anyone. It includes the location and the number of hops it has done in order to fetch the traceroute and verify authenticity. All the data gives a conclusion that the above follow from an email header was legitimate.

**4.2 FORENSICS USING KALI LINUX TOOL- MALTEGO**

The previous tool explained was not a professional tool and has constrained work which it can do. Numerous professional companies and Computer forensics investigators do not use such tools as they can be utilized by anyone and has limited functionality..

Kali Linux is a Linux based environment used for Digital Forensics and penetration testing. This is the official environment used in the big organizations such as Nokia, Microsoft, Fortinet for their advanced digital forensics investigation and Ethical Hacking. It has various tools incorporated into it which run from the Kali command line. One of the tools, which is utilized for email investigation, is Maltego.

Maltego is an intelligent data mining and penetration-testing tool, which has a capacity of confirming an email as well as to break into the email database and check the authenticity. It begins with data assembling in which the email address can be entered from which the mail arrived. It then goes and checks in the database if there are any available matches in the database for the email address. Once we find the email address, it can be attacked and compromised. It can be utilized for network information gathering simply like eMailTrackerPro yet in a considerably more secure environment and has substantially more features as opposed to any open source accessible devices.

As the following tools can be used for Ethical purpose only and not for personal reasons, here trying to show gathered target information and the requested email map from the database. Due to confidentiality and ethical reasons, not going to exploit the email address, as it is not within the scope of the report.

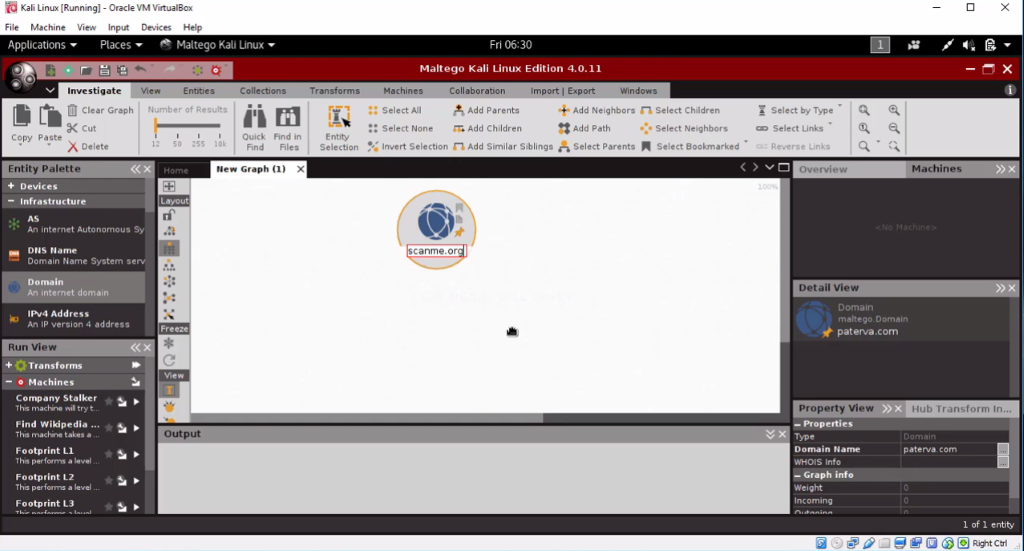


Figure 6: Maltego tool scan start

Suppose we got an email from the source called scanme.org (used this name as it is used for research purpose). We will find the below map and email addresses related to it to check what all information we gather form this tool.

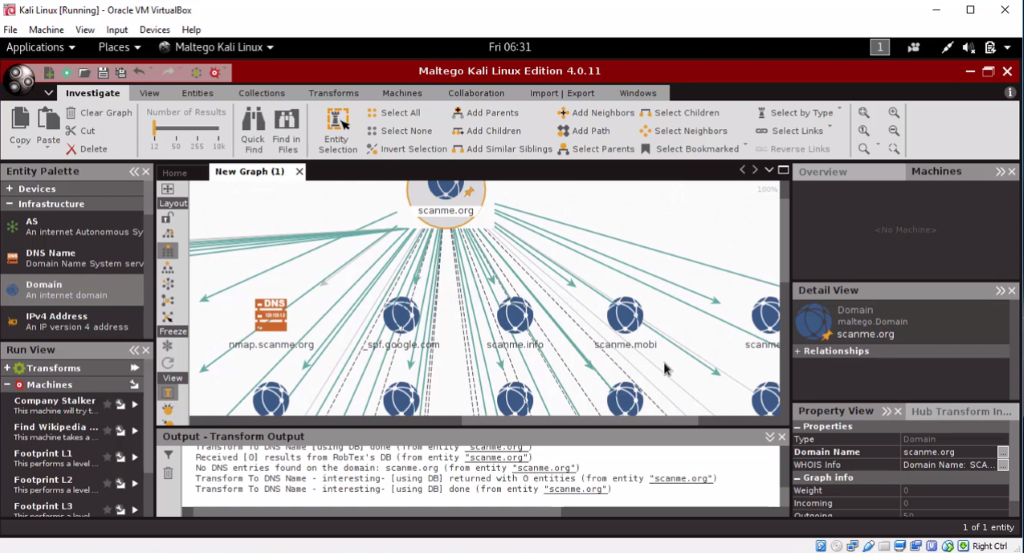


Figure 7: Scattered tree scan of domain

The map created for the scanme.org and all the related links and emails available on the internet is shown in the tree format in the above picture.

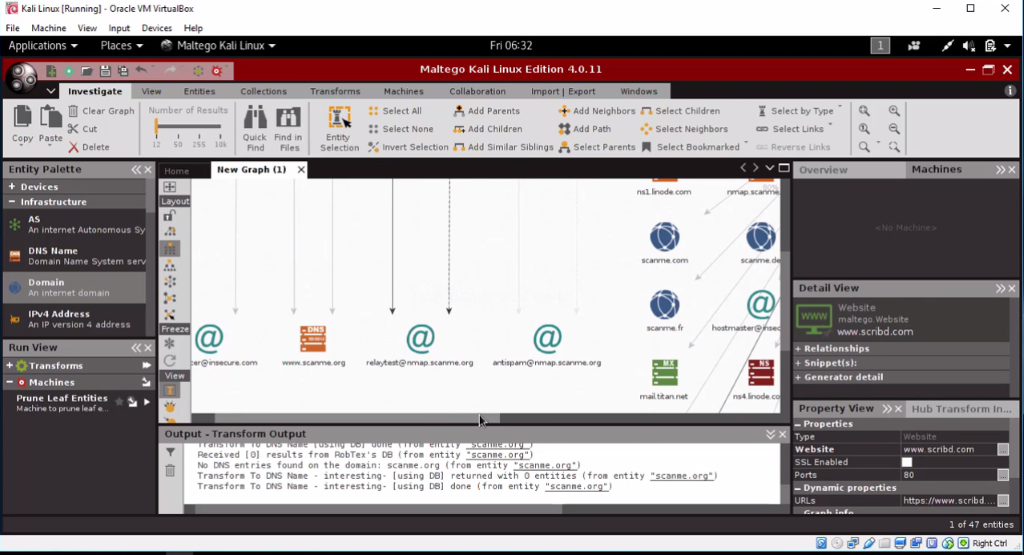


Figure 8: Email verification using tree scan

The above screenshot from Kali Linux shows the email addresses related to the search done for scanme.org. Now each of this email address can be exploited and used for email forensics purpose. Due to security reasons, it can not be done, as it will be unethical. This is how the Kali Linux can be used for Ethical Hacking of various email addresses to verify their authenticity.

**5.0 CONCLUSION**

From the set of tools available in the market for email forensics uses header analysis, location-based analysis, network devices evaluation and so on to perceive the birthplace of the email. Since the SMTP server logs and other data required for the examination is not effortlessly accessible from the ISPs, means until now a perfect solution has no longer been developed. Likewise, there is no smart mechanism which can sense the origin of the sender from different locations of the world if the sender is traveling means they do not learn through themselves and serves the purpose of insignificant classification without additionally learning.

**6.0 RECOMMENDATIONS**

The email framework is extremely utilized and complex distributed web application having a range of hardware and software segments including services, protocols, server, and agents. Numerous threats are met by the user due to vulnerabilities present in the system. So there is essential to make it more secure by defeating the present security flaws. Further, there is also a requirement to approve proactive forensics and to make our system to accept forensic readiness.

**CITED REFERENCES**

[1] https://pdfs.semanticscholar.org/47d6/b06d97e9955060b45e563f82fb5d193b9fee.pdf

[2] <https://abm-website-assets.s3.amazonaws.com/forensicmag.com/s3fs->

public/JIS\_2015041015341322.pdf

[3] https://pdfs.semanticscholar.org/8625/a3b17d199e5cabbb796bad0df56a7979c77c.pdf

[4] <https://www.hacker-arise.com/single-post/2017/03/31/Maltego-4-Part-2-Reconnaissance-on->

a-Person-Boris-Epshteyn

[5] https://kevinzakka.github.io/2016/07/13/k-nearest-neighbor/

[6] https://www.aid4mail.com//email-forensics.php

[7] http://www.emailtrackerpro.com/support/headerstutorial.html

[8] https://fenix.tecnico.ulisboa.pt/downloadFile/1970943312267438/csf-13.pdf

[9] http://www.ijcscn.com/Documents/Volumes/vol5issue3/ijcscn2015050311.pdf

[10] https://arxiv.org/ftp/arxiv/papers/1004/1004.0570.pdf

[11] http://emailheaders.net/gmail.html

[12] https://pdfs.semanticscholar.org/3f1c/20b2c3b28a0328bfc5db19b02621e5874cee.pdf