Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 004.42:004.738.12
DOI: https://doi.org/10.24867/16BE36Ljubic

ФОРЕНЗИКА ЕЛЕКТРОНСКЕ ПОШТЕ

E-MAIL FORENSICS

Јанко Љубић, *Факултет техничких наука, Нови Сад*

Област – ЕЛЕКТРОТЕХНИКА И РАЧУНАРСТВО

Кратак садржај – *Рад представља истраживање у области дигиталне форензике електронске поште. Чињеница је да је значајан број електронских порука данас малициозног карактера и да често постоји потреба за утврђивањем идентитета и аутентичности учесника у конверзацији. Циљ рада био је преглед и поређење постојећих форензичких техника и алата. Анализирано је више техника и алата. Закључене су предности и недостаци форензике мејлова као и чињеница да постоји потреба за њеним унапређивањем.*

Кључне речи: *Форензика, дигитални докази, електронска пошта*

Abstract – *This work presents research in a field of the Digital Email Forensics. Today, it is a well-known fact that the significant number of emails are malicious in nature. There is often a need to identify and authenticate the conversation participants, which is being done by use of email forensics. The aim of this work is a presentation and comparison of existent forensics methods and tools. Multiple forensics techniques and tools were analyzed. In the end, the current advantages and disadvantages of email forensics were concluded, alongside with a fact of existing need for its improvement and further development.*

Keywords: *Forensics, digital evidence, email*

1. УВОД

Приличан број електронских порука данас јесте малициозног карактера. Пошиљаоци имају за циљ да се лажно представе или путем мејла инфилтрирају у систем примаоца и тиме нанесу штету.

Такође, често постоји потреба за утврђивањем аутентичности пошиљаоца. Одговоре на ова питања даје форензика електронске поште. У овом раду су упоређене релевантне технике и алати, приказане су њихове предности и мане као и услови у којима их ваља или не ваља користити.

2. ЕЛЕКТРОНСКА ПОШТА

Једна електронска порука (у даљем тексту мејл) се шаље од пошиљаоца примаоцу, или примаоцима и састоји се од више саставних делова од којих сваки носи информације корисне за одређивање садржаја поруке као и идентификације учесника у комуникацији или информације о самој поруци – мејлу. Главне делове мејла представљају заглавље и тело. Заглавље (табела 1) садржи информације у форми парова, кључ вредност, које указују на адресу пошиљаоца, адресу примаоца, информације о времену слања и слично. Тело садржи суштинску поруку мејла коју је креирао пошиљалац.

Табела 1. *Важнија поља у заглављу мејла*

Назив поља	Опис
From	Мејл адреса и опционо име аутора мејла.
To	Мејл адреса/адресе, и опционо име/имена прималаца мејла.
Cc	Carbon Copy – мејл адреса/адресе корисника који ће добити копију мејла.
Bcc	Blind Carbon Copy – мејл адреса/адресе корисника који су осталима невидљиви, а добиће своју копију мејла.
Subject	Кратки наслов мејла.
Date	Временски тренутак када је мејл креиран.
Reply-To	Мејл адреса на коју би требало послати одговор.
Message-ID	Аутоматски генерисано поље које представља јединствени идентификатор поруке.
Recieved	Информација генерисана од стране мејл сервера који су руковали поруком, у обрнутом редоследу, а која служи праћењу кретања поруке кроз мрежу.

Пут мејла од пошиљаоца до примаоца се може разликовати у зависности од архитектуре система електронске поште.

Тип 1 – архитектура у којој нема интернета већ су и пошиљалац и прималац повезани на исти, дељени систем који прослеђује поруке. Мејлови се креирају и читају уз помоћ агентских апликација.

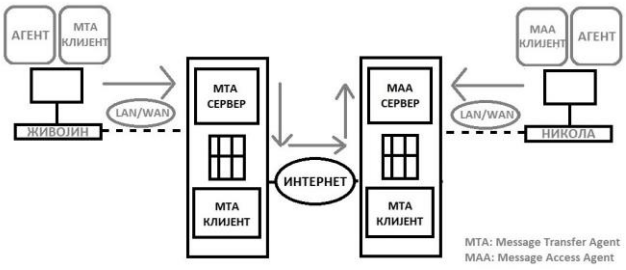
Тип 2 – пошиљалац и прималац више не деле исти систем већ се мејл шаље путем интернета од једног сервера до другог. Пошиљалац користи агентски програм да креира и пошаље мејл а прималац користи агентски програм да приступи мејловима који се

НАПОМЕНА:
Овај рад проистекао је из мастер рада чији ментор је био др Стеван Гостојић, ванр. проф.

налазе у поштанском сандучету његовог сервера електронске поште.

Тип 3 – прималац је и даље директно повезан на свој сервер електронске поште али је пошиљалац сада повезан преко LAN/WAN (LAN – Local Area Network, WAN – Wide Area Network) мреже.

Тип 4 – данас најчешће сретани тип архитектуре. И пошиљалац и прималац су на сервере електронске поште повезани путем LAN/WAN конекције [1] (слика 1).



Слика 1: Најчешћа архитектура мејл система

Протоколи размене мејлова представљају стандарде размене информација између корисничких агентских апликација и сервера електронске поште. Разликујемо више протокола по функционалности и месту примене, а као најзаступљенији истичу се SMTP, MIME, POP3, IMAP4, HTTP, Microsoft Exchange.

3. ТЕХНИКЕ ФОРЕНЗИКЕ ЕЛЕКТРОНСКЕ ПОШТЕ

Дигитална форензика представља процес коришћења ваљаних научних метода за идентификовање, прикупљање, чување, анализу и презентовање дигиталних доказа добијених из дигиталних извора а за потребе лакшег и бољег разумевања и реконструкције догађаја који могу представљати кривично дело [2]. Дигитална форензика се грана у различитим правцима па тако разликујемо форензику масовне и радне меморије, форензику оперативних система, форензику мобилних уређаја и тако даље. Једна од грана дигиталне форензике јесте и форензика рачунарских мрежа. У овом случају, дигитални докази преносе се путем рачунарских мрежа. Електронска порука, односно мејл, представља један од таквих дигиталних доказа.

3.1. Идентификовање доказа

Мејл се идентификује тако што се тражи свуда по мрежи, јер је могуће да је у локалу обрисан али да се његова копија и даље чува у мејл серверу, на пример. Поред мејла, дигитални доказ представљају и логови са уређаја мејл система.

3.2. Прикупљање доказа

Да би се докази обрадили морају се прикупити на ваљан начин који подразумева да ће стање на уређајима са којих се докази прикупљају бити неизмењено, као и да ће докази бити очувани и копирани у истом стању у ком су и пронађени. Такође је важно забележити сваку од радњи и идентификовати особе које су радњу преузеле како би се обезбедио ланац доказа и знало ко је, у ком тренутку и на који начин утицао на и прикупљао дигиталне доказе. Медиј на ком ће се чувати прикупљени подаци мора пре почетка фазе прикупљања и чувања бити форензички чист.

Када се посматра електронска порука и прикупља као доказ, мора се водити рачуна на то у ком се формату порука преузима. Порука се треба преузети у свом изворном формату, а не претварати у формат који одговара истражитељима. Често се прави копија целокупног сандучета за шта постоји више техника.

- Истраживање сервера - Мејлови који су обрисани са клијента (било пошиљаоца или примаоца) и чији опоравак није могућ, могу се затражити од мејл сервера пошто већина њих чува копије након што мејл доставе. Даље, логови сервера могу помоћи да се пронађе адреса рачунара одговорног за покретање мејл трансакције. Неки од сервера могу чувати информације о власнику поштанског сандучета као што је на пример број кредитне картице власника, што може много помоћи у проналажењу идентитета особе [3].
- Истраживање уређаја на мрежи - Рутери, свичеви или неки заштитни зидови и њихови логови.
- Тактика мамца - Уколико је мејл адреса са којег је примљена порука која се испитује права, истражитељи могу послати мамац мејл пошиљаоцу. Такав мејл садржи „img“ елемент чији се извор слике (енгл. source - src) налази на неком HTTP серверу.

3.3. Чување доказа

Да би се у било ком тренутку могло тврдити да су изнети докази веродостојни, мора се осигурати то да се у току процеса дигиталне форензике они ни на који начин не мењају, као и да се зна у ком тренутку су докази били предмет рада које особе (ланац доказа).

Неки од принципа којих се треба држати приликом обављања процеса дигиталне форензике су чување оригиналних доказа, фотографисање физичких доказа, фотографисање екрана приликом приступа дигиталним доказима, чување дупликата комплетних доказа, вршење хеш тест анализе са циљем утврђивања аутентичности претходно копираних доказа, чување ланца доказа (документовање датума, времена и свих осталих информација приликом пријема доказа на обраду).

3.4. Прегледање доказа

Докази прикупљени у претходној фази представљају сировину из које треба издвојити суштину. Суштину представљају докази који се из неког разлога сматрају релевантнијим извором информација за оповргавање или потврђивање кривичног тела, па се тако из скупине свих електронских порука из пријемног сандучета може издвојити секвенца око критичног мејла како би се извршила анализа њихових заглавља, серијских бројева и садржаја.

- Иницијално прегледање и предпроцесирање - Издвајање одређених мејлова из скупа

форматираног као ost или pst фајл може се обавити коришћењем различитих алата.

- Опоравак обрисаних података - Фаза прегледања доказа обухвата евентуалну реконструкцију обрисаних доказа, на пример мејлова који су обрисани у локалу али се и даље налазе на серверу. Обрисани мејлови су углавном доступни за опоравак у неком року. Након тог рока, опоравак је могућ уз помоћ неког од доступних алата који ће прегледати сачувани .ost, .pst или mbox фајл [4].
- Откључавање и дешифровање доказа

3.5. Анализа доказа

Фаза анализе подразумева процесуирање информација које се односе на објекат истраге са циљем одређивања чињеница о неком догађају, важност доказа и одговорност особе или особа.

- Претрага по тексту и шаблонима
- Анализа заглавља мејла - Срж форензичког истраживања електронске поште. Сваки мејл има тачно једно заглавље које је структурално подељено на поља у форми кључ-вредност. Заглавље мејла садржи главне информације које одређују ко је, коме, када, како (којим протоколом), са које адресе и шта послао. Нека од важнијих поља заглавља која се анализирају су *Recieved, X-Received, Received-SPF, Delivered-To, Return-Path, Authentication-Results, DKIM-Signature, Message-ID.*
- Утврђивање временског тока
- Визуализација

4. АЛАТИ ЗА ФОРЕНЗИКУ ЕЛЕКТРОНСКЕ ПОШТЕ

Од велике скупине алата издвојени су они за чије коришћење није било неопходно плаћање већ постоје верзије које је бесплатно могуће користити у ограниченом или неограниченом временском периоду. Такође, за алате за које је било неопходно издвојити новчана средства коришћене су информације из других истраживања, документација и слично.

4.1. Autopsy 4.19.1

Бесплатни алат отвореног кода који подржава рад и у интернет и у режиму без интернета. Врши аквизицију података са локалних дискова, фајлова и фолдера као и слика дискова. Подржава више мејл формата а функционише на више оперативних система. Може да анализира екстерне уређаје а подржава и напредне опције претраге и визуелизације, опоравка података и извоза у више различитих формата.

4.2. Aid4Mail Professional Trial 4.7

Бесплатна пробна верзија алата чији код није доступан јавности способан је да врши аквизицију података са локалног система, с тим што може да анализира искључиво *Windows* оперативни систем.

Подржава велики број формата мејлова које може проналазити и на екстерним уређајима и извозити у више различитих формата. Постоји опција опоравка података и претраге али не и нарочите визуелизације.

4.3. MailXaminer 4.9.3

Бесплатна пробна верзија чији је код такође задржан од стране произвођача нуди аквизицију података и са локалне машине и са интернета уз подршку мноштва мејл формата. Функционише искључиво на *Windows* оперативном систему с тим што може анализирати и екстерне уређаје. Подржава претрагу, визуализацију и опоравак података. Функционалност извоза података одлично је покривена.

4.4. AccessData FTK Imager 4.5.0.3

Алат који функционише само у режиму без интернета и може да врши аквизицију података са локалне машине али и са екстерних уређаја. Подржава доста мејл формата и покрива остале важније функционалности укључујући и претрагу, опоравак, визуализацију и извоз.

4.5. BitCurator Environment

Линукс дистрибуција отвореног кода који врши аквизицију локалне машине и свих типова мејл архива. Ради са екстерним уређајима и омогућава претрагу, визуализацију, опоравак и извоз података.

4.6. Paraben E-Mail Examiner

Затворени алат који се наплаћује и пружа офлајн услуге обраде преко 750 мејл формата на *Windows* оперативном систему. Не подржава рад са екстерним уређајима али омогућава визуализацију, опоравак и извоз података.

4.7. EnCase

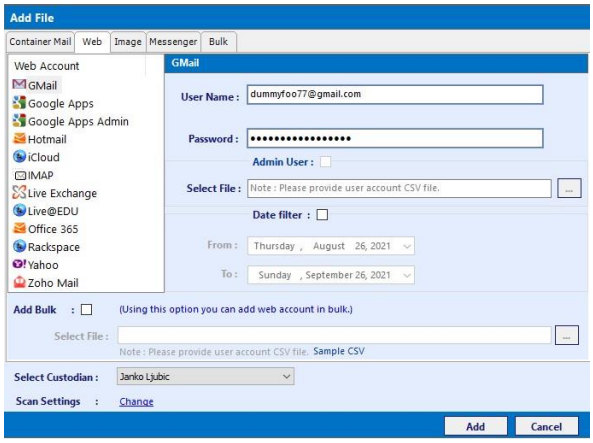
Затворени алат који се наплаћује и омогућава рад у режиму са и без интернета. Аквизиција података се обавља са интернета или локалне машине а подржано је преко 600 различитих формата мејлова које је могуће претраживати, опорављати, визуализовати и извозити у склопу више различитих оперативних система.

5. СТУДИЈА СЛУЧАЈА

Неке од ових техника и алата демонстрирани су на хипотетичком случају. Замислимо да постоји сумња да је са налога „dummyfoo77@gmail.com“ послата електронска порука чија садржина представља средство преваре и покушај лажног представљања. Задатак је извршити вештачење приложеног рачунара тако што ће се утврдити: да ли је преко уређаја остварен приступ налогу са адресом „dummyfoo77@gmail.com“, да ли се на том налогу налазе електронске поруке, садржај тих порука, да ли су поруке аутентичне, адресе на које су поруке послате и друге околности у вези настанка тих порука.

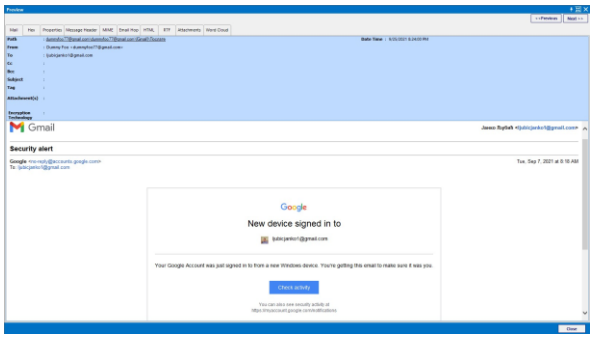
Идентификован је лаптоп уређај и забележен његов модел, изглед као и стање. Прикупљени су докази тако што се уз помоћ алата *SysTools MailXaminer v4.9.3* приступило мејл налогу осумњиченог (слика 2). Прикупљени докази сачувани су у непромењеном

облику на екстерној меморији која је претходно форензички очишћена.



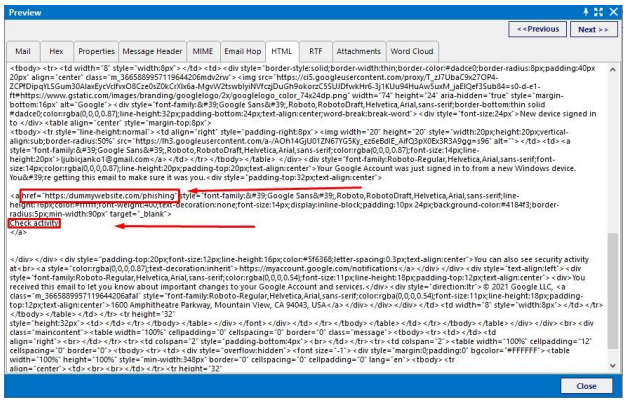
Слика 2: Приступање налогу из алата

Приликом прегледања доказа издвојен је мејл са карактеристикама које одговарају опису датом у хипотетичком случају (слика 3).



Слика 3: Пронађени мејл

Порука је анализирана и примећено је да порука садржи дугме које шаље корисника на нежељену и лажну локацију са циљем крађе података (слика 4). Такође је утврђен идентитет пошиљаоца.



Слика 4: Анализирани садржај мејла

Докази су презентовани у виду налаза који се прилаже суду.

6. ЗАКЉУЧАК

Са растом броја корисника електронске поште, расте и број потенцијалних жртава, али и број потенцијалних починилаца кривичних дела која се извршавају уз помоћ или преко електронских порука. Постоји потреба да се починиоци на научно важан начин пронађу и повежу са кривичним делом да би се могли санкционисати.

Коришћење проверених и устаљених техника смањује могућност прављења грешака које у правном или неком другом смислу могу да омету истрагу и долажење до истине.

Проблем већине постојећих техника и алата је тај што су артефакти које они анализирају опште познати и због тога погодни као тачке којима би у будућности могло бити манипулисано, поготово уколико се узме у обзир брзина развоја антифорензичких и криминалних алата и техника. Тиме би се могла довести у питање веродостојност тврдњи које су у претходном периоду важиле за истините, што у правној пракси није прихватљиво.

Како би се умањио утицај растуће гране антифорензике, неопходно је константно унапређивати и осавремењавати постојеће форензичке технике и алате, као и системе електронске поште који у многим случајевима допуштају манипулацију која може бити малициозног карактера.

7. ЛИТЕРАТУРА

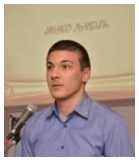
[1] G Chhabra, D Bajwa, Review of E-mail System, Security Protocols and Email Forensics. International Journal of Computer Science & Communication Networks (IJCSCN), Vol.5, Issue 3, pp.201-211, 2015.

[2] Andre Arnes, Digital Forensics, Norweigan University of Technology and Science, Norway, 2018.

[3] M. Tariq Banday, Techniques and Tools for Forensic Investigation of E-mail, University of Kashmir India, 2011.

[4] Tracy King, "How to Retrieve Emails from Gmail, Outlook, Hotmail, and Yahoo", 2021. Доступно на https://www.easeus.com/file-recovery/recover-deleted-email-files.html [посећено 05. септембра 2021.]

Кратка биографија:



Јанко Љубић рођен је 02.02.1998. године у Врању. Мастер рад на Факултету техничких наука из области Дигиталне форензике одбранио је 2021. године. контакт: janko.ljubic@uns.ac.com