ELECTRONIC MAIL FORENSICS

Milorad S. Markagić
University of Defence in Belgrade, Military Academy,
Department of Telecommunications and Informatics,
Belgrade

DOI: 10.5937/vojtehg61-1434

FIELD: Telecommunications, IT
ARTICLE TYPE: Professional Paper

Abstract:

In general, digital forensics could be defined as a compilation of methods of collecting, analysing and presenting digital evidence that could be found on computers, servers, in networks, databases, mobile devices and all other electronic devices where data is stored. This paper explains the methods of collection of digital evidence in electronic mail and their analysis as well as taxonomy (classification) of digital forensics.

Key words: *digital forensics, computer forensics, electronic mail.*

Introduction

Electronic mail is becoming a part of evidence in a large number of both civil and criminal forensic investigations. Electronic mail and mail based on internet servers spread fast and thus easily and equally fast ends in a computer of a user for whom it is not intended. The first electronic message was sent by Ray Tomilson in 1971, and then, years later, with the use of personal computers and the Internet, it grew into a global means of communication, private and business alike (Swaminathan, et al, 2009). Furthermore, it is also used as a means of fun, besides information exchange, and as such represents an indispensable source of digital evidence when a computer security incident occurs.

milmarkag@yahoo.com

The mail, based on internet servers, is very useful during an investigation. If a suspect has an account on a certain mail server, it is possible, with the appropriate permission of the provider and a court order, to find even deleted messages as most providers in their user privacy policy do not guarantee deletion of data on backup systems.

Every electronic message is sent as a series of packages. During transport in the network, each of these packages has to contain the following elements:

Source address: IP address of the sender's computer, with the exception of certain cases when the address is hidden,

Destination address: IP address of the recipient's computer,

Payload: data or message that are actually the main purpose of exchange of electronic message.

Routers forward packages from the beginning position to the ending destination according to their routing tables.

From a forensic standpoint, client-server electronic mail systems are best for information search because all messages are downloaded to the user's local computer i.e. hard disk, making investigation easier as the forensic analyst has an access to the data storage medium.

Servers could be accessed as well, for the purpose of searching through their electronic mail activity records, as well as for possible new messages. It is not possible to switch off the electronic mail production server in order to perform a search. Rather, security copies are checked first and, should everything else fail, last resort would be to switch off the server (Carrier, 2009).

Electronic Mail Analysis

Every electronic message consists of two parts: header and message text. The source and destination addresses, the message sender and the intended recipient could be obtained from the header, and the message body contains the text of the message (Caloyannides, 2009).

Most electronic mail clients usually show only basic information in their header:

from whom – sender's address: this field could be disguised, i.e. sender identification could show another person, while the real IP sender's address is hidden,

for whom - recipient address: that could also be hidden, i.e. disguised,

subject (or title) – this field can sometimes be empty or could contain misleading and often encrypted information or a message with previously agreed upon methods of communication and procedures,

Date and time – obtained from the sender's computer, which may be incorrect if the clock on sender's computer is set wrongly, intentionally or accidentally.

As the basic header information cannot be taken for granted, search has to be extended to the information that is shown in it. The extended header contains far more information than the routers require to deliver a message to its final destination.

The most useful information in the extended header is the IP address of the source. This information makes it possible to track the sender. First, the electronic mail server picking up the message assigns to it a specific identification number. It is possible to follow it in actual and real time and its path through the network only if the investigator gains the access to the server logs before the information searched for is deleted.

In addition to viewing the header and the text of a message, it is necessary to check other potential sources of information:

– attachments with extensions (.doc, .xls, pictures...),

– addresses stated in CC and BCC fields (Carbon Copy or Blind Carbon Copy),

– names of people to whom the message is forwarded, and

– original message or a series of messages to which this is a response, or a response to a message being investigated.

It should by no means be assumed that the logged user has sent all messages because in any working environment the co-workers share computers and computer log-in passwords, and thus many gain access to the computer under investigation (Nolan, et al, 2005).

The process of forensic extraction of electronic messages in the client-server environment consists of common general steps. A vast number of electronic mail systems use one of the following three protocols:

– SMTP – Simple Mail Transfer Protocol,

– POP – Post Office Protocol, or

– IMAP – Internet Message Access Protocol.

Transport of electronic messages becomes standardized with the usage of these protocols. The challenge is getting electronic messages from a variety of client electronic mail applications using forensic tools.

Two most commonly used client software packages are:

Outlook – Besides the standard options of an electronic mail application, it contains: Calendar, Tasks and Contact Manager. These provide a detailed insight into a daily routine of the suspect. Unlike Outlook Express, it stores all data within a single user identity, in a document with an extension .pst that could be accessed using the forensic tools FTK or EnCase.

Outlook Express – Stores data in a document with an extension .dbx. Viewing is possible with an appropriate viewer application. Every user account opened in Outlook Express is assigned a hexadecimal number sequ-

ence (hash) that Microsoft uses for account identification. These user account identity numbers are stored in sub-directories, either in Documents or in Settings, depending on the version of the operating system used.

Outlook Express, Outlook, AOL, Eudora and Thunderbird store electronic mail locally, on a computer, which remarkably simplifies viewing and search operations. In this way, as well as by viewing server mail logs, one can reach the information that links the server and the electronic message simply by viewing the identification message (Volonino, Anzaldua, 2008).

Electronic Mail Document Extensions

In the cases when only documents needed for the viewing of electronic messages are required to be found, or when specific documents stored within a message are required to be copied, it is possible to use a system on the investigated computer or expert software such as Outlook Extract Pro or Outlook Export.

Far more appropriate, safer and simpler is to use forensic tools such as EnCase or FTK with built-in browsers that permit viewing and recording database contents as well as their copying to other media for further analyses. Forensic tools automate the process of data downloading and copying, thus making it easier to analyze data and to generate log reports.

Document extensions for frequent electronic mail clients, and depending on a client, may be .abi, .arl, .aim, .bag, .mbx, .dbx, .dgr, .emb, .pab, .pst, .wab….

Computer forensics software can be used to open almost all electronic messages formats, thus clearing possibilities for the following:

– Detailed search of electronic messages,

– Reading/viewing message header information,

– Copying electronic messages in their entirety (header, address, text), and

– Grouping and classifying messages.

These activities are made on working copies of original data (Carrier, 2009).

Analysis of Electronic Mail based on Internet servers

Public web systems such as Google, Yahoo, Hotmail, gmail etc, are commonly used for personal communication by means of electronic mail. These systems are used without client software and represent a client-server system. The web mail system delivers electronic messages using

the SMTP protocol or applying POP or IMAP protocols. Web mail is not kept locally on a computer, unles the client explicitly requests otherwise, but is stored on a [public] server.

The access to an E-mail account on a server or collecting user account data by providers greatly reduces the work load of a forensic investigator. If the access is denied, a web mail message could be reached by accessing RAM and cache memory. When the user checks messages or is in a process of creating a new one, the operating system saves data from the screen onto the hard disk, especially if the user needs more time to complete composing the message.

Places where one could search for web mail messages on a local computer are: temporary file locations such as system swap partitions or cache memory and unallocated partitions following the deletion of temporary files and documents.

Downloading data from temporary files is a time-consuming process even if some forensic tools are used, because the reconstruction of the internet page is done from the nonformatted digital space.

Web mail on a local computer has a form of a web page and an E-mail functionality; therefore, one should look for documents with .html extensions. As the times/time stamps when the user has visited web pages could not be taken into consideration, i.e. cannot be accepted, As the user's web page view log cannot be valid after some time, their number could be significantly downsized if one takes into consideration the use of specific key words and checks for services the suspect has used.

Temporary Documents

Operating systems create temporary documents for applications that send and receive data through the network. These data are first stored in the RAM and, when it fills up, the operating system moves data lower on its data list of priorities that applications require and writes them on a hard disk. There is no particular and exclusive space where temporary documents are stored because some applications create additional temporary files to the ones created by the operating system.

Applications that do not have the means to temporarily store data leave it up to the operating system to store data using swap data files or virtual memory. If and when the application needs temporarily stored information, the operating system sends it to the application and erases it from the hard disk. Even though the swap databases could be deleted, it is possible to recover data because it still physically exists in the disk, i.e., until new data is written over it (Swaminathan, et al, 2009), (Nolan, et al, 2005).

Internet Explorer has also an option of saving pages that have been accessed by the browser. And although the number of days Internet Explorer is to store this information is left to the user to adjust, it should be noted that they do not dissapear after being deleted. Internet Explorer uses the index.dat document for creating a database of accessed pages, cookies and other details related to the use of search engines.

It is possible to extract these data from index.dat documents and inversely reconstruct the user log-in history to the point when the user first accessed the Internet on that computer and browser. Mozilla, Google Chrome and Opera use similar methods of saving surf histories.

Instant Messages

In big organizations the communication with the users is often done by instant messaging. Employees within the company communicate between themselves by instant messaging, and these are also freequently used for personal conversation as well. People exchange messages that are going through servers and the work process in this case is almost identical to the work process of electronic mail, with the main difference being that it is taking place in real time.

Some instant messaging software packages provide options for recording conversation history, but very few users do choose this option. Parts of conversations could be found on servers, but whole conversations may be found only if the option of conversation history is switched on or if the network traffic of a computer from which instant messages are sent is recorded while the communication is in progress.

There are also real-time forensic methods. Tools such as Web Case offer partial forensic tracking of data in real time by storing IP addresses, chat sessions and other communication through internet connection (Volonino, Anzaldua, 2008).

Conclusion

The technology of today allows for change and manipulation of digital media in ways that have been impossible only a few years ago. The technology of the future will almost certainly bring about manipulations of digital media in ways that seem impossible today. As technology continues its evolution, it will be increasingly important that digital forensics keeps its pace with the developments and progress. And as techniques are developed, as well as methods for revealing computer frauds, newer and more sophisticated methods of forgeries and counterfeitting will emerge, ones that will be much harder to bring to light.

It is a neverending and continuous struggle between software developers and service providers on the one side, and malicious users and criminals on the other.

The field of digital forensics will continue to make the creation of convincing and plausible forgeries whose goals are to deceive and mislead an arduous and difficult task by developing new methods, althorithms and tools.

References

Caloyannides, M.A., 2009, "Forensics Is So Yesterday", IEEE Security & Privacy, Volume 7, Number 2,

Carrier, B.D., 2009. "Digital Forensics Works", IEEE Security & Privacy, Volume 7, Number 2,

Nolan, R., Branson, J., Wait, C., O'Sullivan, C., 2005. "First Responders Guide to Computer Forensics", CERT,

Swaminathan, A., Wu, M., Ray Liu, K.J. 2009. "Component Forensics", IEEE Signal Processing Magazine, Volume 26, Number 2,

Volonino, L., Anzaldua, R., 2008. "Computer Forensics", Wiley Publishing Inc.

FORENZIKA ELEKTRONSKE POŠTE

OBLAST: telekomunikacije, informacione tehnologije
VRSTA ČLANKA: stručni članak

Sažetak:

U najopštijem smislu digitalna forenzika može se definisati kao skup metoda za prikupljanje, analizu i prezentaciju digitalnih dokaza koji se mogu pronaći na računarima, serverima, u računarskim mrežama, bazama podataka, mobilnim uređajima i svim drugim elektronskim uređajima na kojima se čuvaju podaci. U ovom radu opisane su metode prikupljanja digitalnih dokaza u elektronskoj pošti i njihova analiza.

Uvod

Elektronska pošta se kao dokazni materijal pojavljuje u velikom broju kako građanskih, tako i kriminalnih forenzičkih istraga. Elektronska pošta i elektronska pošta zasnovana na internet serverima širi se veoma brzo, pa lako i brzo završi i na računaru korisnika kome nije namenjena.

Prvu elektronsku poruku poslao je Ray Tomilson 1971. godine, a deset godina kasnije, u kombinaciji sa personalnim računarima i internetom, prerasta u globalni način komuniciranja – i personalnog i poslovnog. Takođe, koristi se i radi zabave, načina razmene podataka, ali predstavlja i nezamenjiv izvor digitalnih dokaza, kada dođe do računarskog incidenta.

Analiza elektronske pošte

Svaka elektronska poruka sastoji se od dva dela: zaglavlja i teksta poruke. Iz zaglavlja je moguće saznati izvorišnu i odredišnu adresu pošiljaoca i namenjenog primaoca, a telo poruke sadrži tekst poruke.

Ekstenzije dokumenata elektronske pošte

U slučajevima kada je potrebno otkriti samo dokumente potrebne za pregled elektronskih poruka, ili kopirati pojedinačni dokument sačuvan unutar elektronske pošte, moguće je koristiti sistem na istraživanom računaru ili specijalizovani softver kao što je Outlook Extract Pro ili Outlook Export.

Mnogo ispravniji, sigurniji i jednostavniji način je korišćenje forenzičkih alata, kao što su EnCase ili FTK, sa ugrađenim pregledačima koji omogućavaju pregled i snimanje sadržaja baze podataka, kao i njihovo kopiranje na druge medije za dalju analizu. Forenzički alati automatizuju proces skidanja i kopiranja podataka, pa ih je jednostavnije analizirati i generisati izveštaj.

Analiza elektronske pošte zasnovane na internet serverima

Za personalnu komunikaciju često se koriste Web servisi za elektronsku poštu: Google, Yahoo, Hotmail, Gmail.... Ovi se servisi koriste bez upotrebe softvera klijenata elektronske pošte i sačinjavaju klijent-server sistem. Web mail sistem predaje elektronsku poruku koristeći SMTP protokol i POP ili IMAP protokole. Web pošta se ne čuva na lokalnom računaru, osim ako to korisnik izričito ne zahteva, već ona ostaje memorisana na serveru.

Pristup nalogu elektronske pošte na serveru ili prikupljanje podataka o korisničkom nalogu od strane pružaoca usluga umnogome smanjuje količinu posla forenzičkom istražiocu. Ako pristup nije dozvoljen, do web mail poruka može se doći pregledom radne i keš memorije. Kada korisnik proverava poruke, ili sastavlja novu, operativni sistem sačuva podatke sa ekrana na hard disku, pogotovo ako korisniku treba više vreme da sastavi poruku.

Privremeni dokumenti

Operativni sistemi kreiraju privremene dokumente za aplikacije koje šalju i primaju podatke preko mreže. Ti se podaci prvo skladište u radnoj memoriji, a kada se ona popuni, operativni sistem pomera podatke niže na listu prioriteta podataka koji su potrebni aplikacijama i zapisuje ih na tvrdi disk. Ne postoji posebno i jedinstveno područje gde se čuvaju privremeni dokumenti, jer neke aplikacije stvaraju dodatne privremene datoteke uz one što ih stvara operativni sistem.

Aplikacije koje nemaju mogućnost privremenog čuvanja podataka prepuštaju operativnom sistemu da ih memoriše, koristeći swap datoteke ili virtualnu memoriju. Kada aplikaciji zatreba privremeno sačuvani

podatak, operativni sistem ga šalje aplikaciji i briše sa hard diska. Iako se swap datoteke brišu, do podataka je ipak moguće doći, jer još uvek fizički postoje na disku.

Instant poruke

U većim organizacijama komunikacija sa korisnicima se češće obavlja putem instant poruka. Radnici u okviru firme međusobno razgovaraju instant porukama, a veoma se često koriste i za lične međusobne razgovore. Osobe međusobno razmenjuju poruke koje putuju preko servera, a princip rada skoro je identičan kao princip rada elektronske pošte, sa osnovnom razlikom da se odvija u realnom vremenu.

Zaključak

Današnja tehnologija omogućava promenu i manipulaciju digitalnim medijem na načine koji su pre nekoliko godina bili nemogući. Buduća tehnologija gotovo će sigurno omogućiti manipulacije digitalnih medija na način koji se danas čini nemogućim. Kako tehnologija nastavlja svoju evoluciju, biće sve važnije da digitalna forenzika održi korak sa tim razvojem. Kako se razvijaju tehnike i metode za otkrivanje računarskih prevara, razvijaće se i nove sofisticiranije metode izrade falsifikata koje će biti teže otkriti.

Ključne reči: *digitalna forenzika, računarska forenzika, elektronska pošta.*

Datum prijema članka/Paper received on: 30. 01. 2012.
Datum dostavljanja ispravki rukopisa/Manuscript corrections submitted on: 20. 02. 2012.
Datum konačnog prihvatanja članka za objavljivanje/ Paper accepted for publishing on: 22. 02. 2012.