

DFRWS Forensics Challenge 2008

Ricci S. C. IEONG (ricci@ewalker.com.hk)

Lunar AU (lunar@ewalker.com.hk)

HC. LEUNG (chau@ewalker.com.hk)

Luky SIU (luky@ewalker.com.hk)

Kenneth TSE (kenneth@ewalker.com.hk)

Introduction

Summary of findings

DFRWS Forensics Challenge 2008 is a forensics challenge that covers review of network packets, browser history, cookies, form history analysis, email analysis and memory analysis. In this analysis, eWalker team performed various analysis and suspected that *Steve Vagon* has communicated with an external party *faatali* for selling company IT infrastructure information. Information may have been transferred through Windows Live Messenger, while the pricing negotiations were found in the Google spreadsheets.

Background

According to DFRWS 2008 Forensics Challenge introduction, an organization has become aware of external attempts to gain access to sensitive proprietary information on its computer systems. Through interviews and active monitoring, a single user was suspected of collaborating with an outside party. Then from the collected data 1) user home directory from suspect's machine, 2) Network traffic captured and 3) Full dump of memory from suspect's machine, participants have to analyze and determine if any evidence can be collected.

Preliminary Findings

After verifying the downloaded `dfrws2008-challenge.zip` against the sha1 checksum, eWalker team identified that within the zip file, the following evidence records could be extracted from the zip file:

File names	Description of the files
Suspect.pcap	Network packet capture file
Challenge.mem	Memory dump file
Other files	Files extracted from the user directory including the web history files

Table 1: List of major files in the dfrws2008-challenge.zip

Then time information was collected from the zip file modified time, web history record (after executing some web history extraction tool) as well as the network packet analysis tool. The identified the information from the evidence record were listed as follows:

Evidence Record	Time
Memory Dump	Unknown
User directory	2007-01-05 11:24:12 PM – 2007-12-16 11:58:30PM
Network traffic	2007-12-17 11:32:16.111289 – 2007-12-17 12:31:00.464157
Web History	2007-12-08 16:25:33 – 2007-12-17 12:57:27

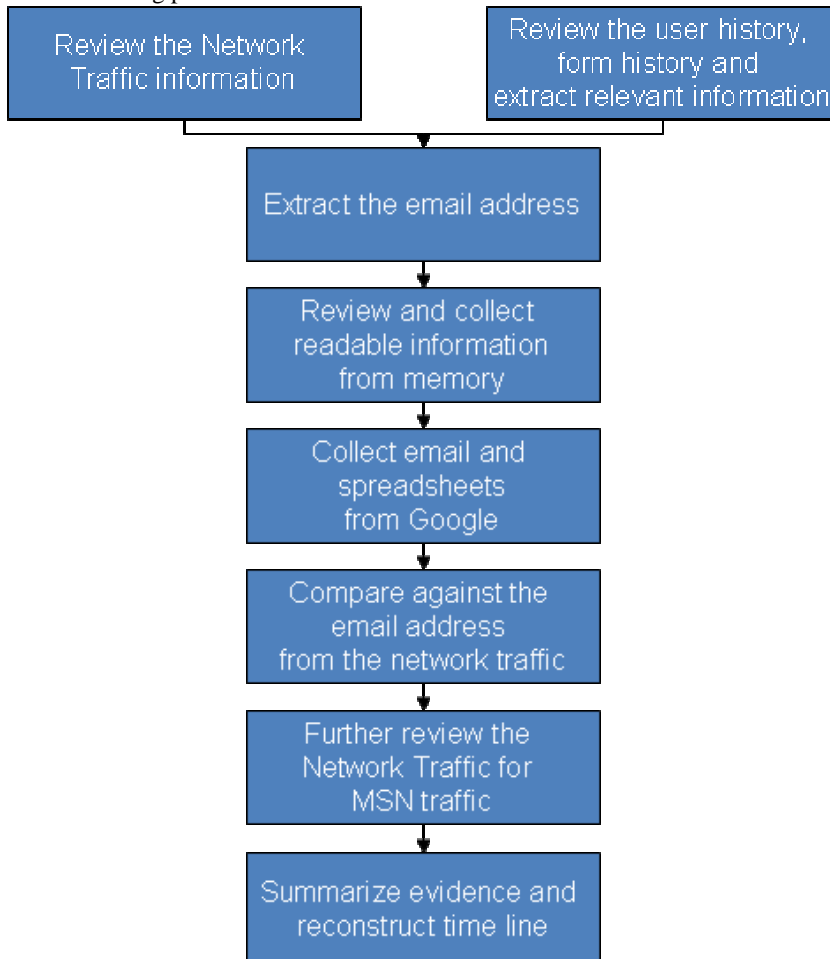
Table 2: Time stamps of major evidence records identified

It is observed that the time record of network traffic has some degree of overlap, while user directory files were collected either in different time zone or collected at some time earlier than the network traffic captured time.

Methodology & Tools

Methodology

After unzipping the evidence records from the zip file, eWalker team performed the analysis according to the following procedures:



At the beginning, the team first reviewed the network packets and analyzed the packets for useful information. Statistics, network traffic types analysis have also been performed.

At the same time, eWalker team also analyzed the information available in the user directories. The directory contains the Firefox browser history, cookie and form history. From the browser history, eWalker collected the list of web sites that have been recently visited.

From the visited web lists, email servers have been accessed. eWalker team searched and identified a list of email address from the network packets and web history. Besides, memory were also analyzed and reviewed for available readable information.

Based on the information collected from network packets, email account was accessed and emails were dumped to the local server. Relevant links to other places were also assessed and requested.

Email addresses and email content collected from Internet have been analyzed and compared against network packets, memory content and web history from the evidence record.

Network packets were further analyzed in order to specifically search for relevant network traffic – MSN traffic.

Finally, all the evidence records were reviewed and time line event have to be reconstructed.

Tools

Throughout the analysis, the eWalker team adopted the scheme to use existing tools before building any tools. It was observed most tools that the investigation required were already available on the Internet, so no specific tools have been built.

Name of the tool used	Role in this analysis	Function of the tool
Wireshark	Pcap file analysis	Parse the pcap file for network packet analysis and packet capturing
Chaoreaders.pl	Pcap file analysis	Parse the pcap file and separate network packets into pieces of streams. It automatically connects packets to streams.
Web Historian	History file analysis	Parse Firefox history data
dumpAutoComplete	Form history file analysis	Extract AutoComplete information stored in Firefox
DORK	History file analysis	Extract records from history.dat in Firefox (in MORK) format
Mork.pl	History file analysis	Parse files in MORK file format
MozillaCacheView	Cache file analysis	Extract information from Firefox cache
Strings	Memory analysis	Extract ASC readable characters from binary file
Bintext	Memory analysis	View ASC readable characters from binary file
Firefox	Web page analysis	Use for viewing web content from the Internet

Table 3: List of tools used in investigation

However, the team has also identified some deficiency in the existing tools. That will be outlined under the issue section in this paper.

Detail Findings

Network Package Analysis

The network packet capture file suspect.pcap was extracted from the Wireshark and totally 10243 packets were found to be generated between 2007-12-17 11:32:16.111289 – 2007-12-17 12:31:00.464157.

By generating the statistics of network traffic and reviewing the network traffic types based on Wireshark, it was determined that majority of the network packets are generated from TCP traffic.

Protocols	% of Packets
Transmission Control Protocol (TCP)	94.60%
User Datagram Protocol (UDP)	4.14%
Internet Control Message Protocol (ICMP)	0.13%

Address Resolution Protocol (ARP)	1.13%
-----------------------------------	-------

Table 4: Categorization of Protocols

Among these 10243 packets, the traffic break down was found to be:

Source Address	Destination Address	Number of packets
Vmware_c2:2f:0c	Broadcast	4 packets
Vmware_c2:2f:0c	vmware_e4:56:48	9 packets
Vmware_ed:9d:3c	Broadcast	11 packets
Vmware_c2:2f:0c	Vmware_c0:00:08	15 packets
Vmware_c2:2f:0c	Vmware_ed:9d:3c	10204 packets

Table 5: Categorization of packets based on Source MAC address

Based on the packet analyzed, it was observed that VMware_c2:2f:0c with the IP address of 192.168.151.130 should be the target IP address to be reviewed. While Vmware_ed:96:3c were usually mapped to 219.93.175.67. However, as this is not within the same Local Area Network, this MAC address is likely to be MAC address of the gateway of the Local Area Network.

While from the network packet address break down, it was observed that many network traffic originated from 192.168.151.130 were directed to 219.93.175.67. However based on packet analysis, it was observed that some network traffic with content of Google mail, Google spreadsheets also passed through this address. Thus, it seems that the 219.93.175.67 may be a proxy server.

By verifying the address using the whois service, it was identified that the address belongs to an address in Malaysia. Through Open Public Proxy list¹, it was identified that the IP address is one of the open proxy server, it was identified that the address 219.93.175.67 (cdn-jrc-c2100-02.tm.net.my) should be an open proxy server.

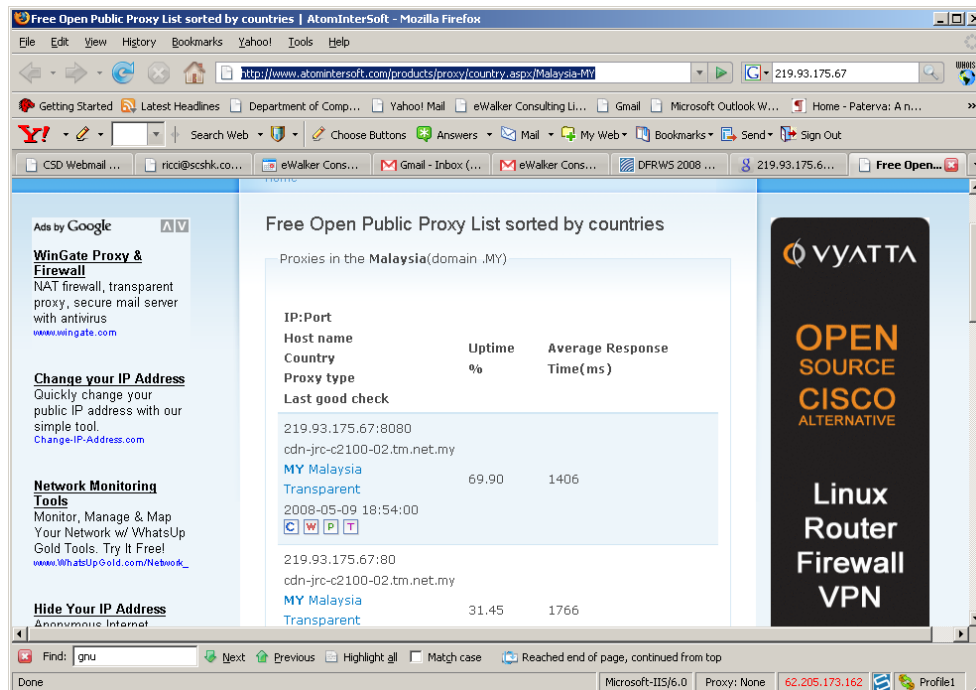


Figure 1: Free Open Proxy Lists output

¹ <http://www.atomintersoft.com/products/proxy/country.aspx/Malaysia-MY>

In further packet analysis, it was observed that the following addresses have been visited by the target machine (by analyzing the web history)

11:32:16 - 11:34:14 ----	http://youtube.com/
11:32:30 - 11:32:30 ----	http://travelocity.com
11:34:16 - 11:34:27 ----	http://www.noblebank.pl
11:34:28 - 11:34:59 ----	http://www.gmail.com (11:36:38) (should be gmail.com)
11:34:50 - 11:38:05 ----	http://www.gmail.com (may be Gmailchat)
11:36:00 -	http://www.idioma-software.com/pig/pig_latin.html
11:36:23 -	http://www.yahoo.com
11:37:03 - 11:37:04 ----	http://mail.yahoo.com
11:37:37 -	http://www.myspace.com
11:42:02 -	http://www.bankrate.com
11:42:05 -	http://m1.2mdn.net
11:43:40 -	http://www.kuro5hin.org
11:44:02 -	http://youtube.com
11:45:29 -	http://www.disney.com
11:45:45 -	http://youtube.com/watch?v=ZiRHyzjb5SI
11:48:36 -	http://youtube.com/watch?v=1RUFBGDvsy0
11:50:57 -	http://www.google.com
11:52:01 -	http://www.wrigley.com
11:52:50 -	http://www.amazon.com
11:54:05 -	http://www.facebook.com
11:54:28 -	http://www.live.com
11:56:48 -	http://www.ebay.com
12:18:48 -	http://en.wikipedia.org/wiki/Lee_Smith_%28baseball_player%29
12:24:22 -	http://ekiga.net

Table 6: List of URL accessed on 17 Dec 2007 extracted from web history

By observing the list of addresses, eWalker team determined that it would be more important to further review the email content from the network packet captured. Based on the web history information (which will be outlined in the following section), it is likely that only Gmail should be the core email communication channel. Thus by filtering to the Google mail, then the following communication has been extracted.

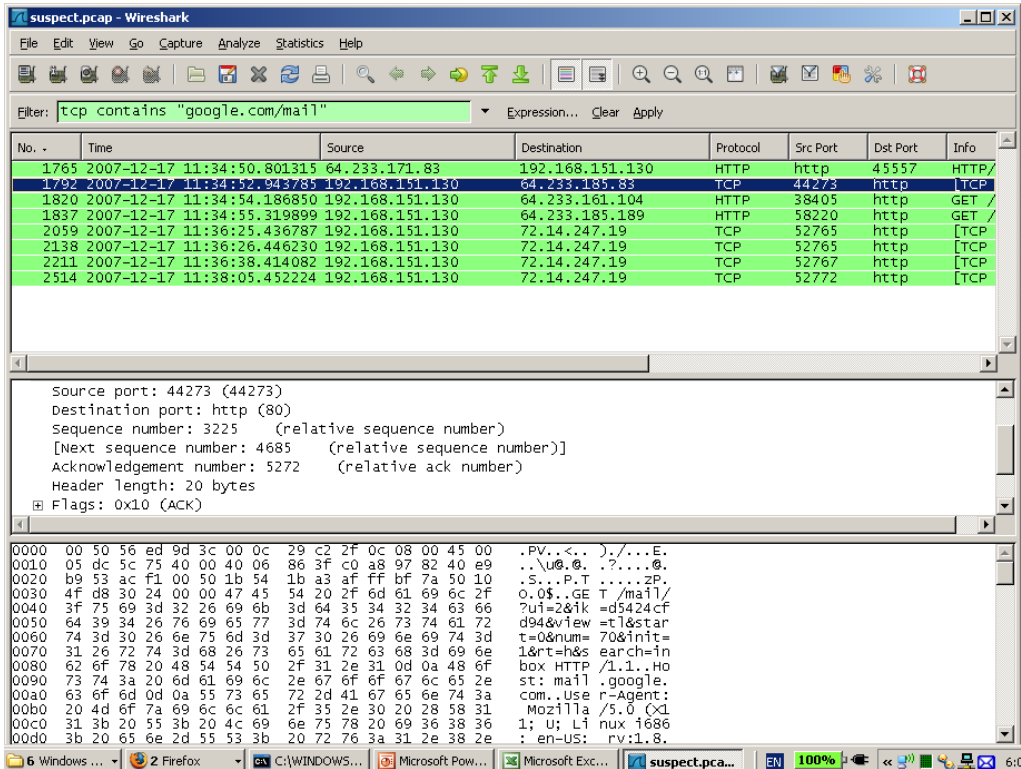


Figure 2: List of filtered network traffic for Google mail

Among the email content captured, it was observed that the following addresses were comparatively more relevant emails.

11:34:50 – Login and download email

11:34:54 – Email accessed

11:34:56 – Email between steve and faatali (session_0081.part_01.gz)

11:36:25 – 11:36:38 – From steve to investors@noblebank.pl (session_0090.part_01.gz)

Some of the Gmail access content was found to be Gmail communication establishment or periodic new email checking only. Because Gmail is a Web2.0 design using AJAX technology, email received will not be transferred to the web browser every time user read the email. Instead, email content will be downloaded to the web browser when user first selected to update the email content. So email updates will only be performed once after login to Gmail or after explicit update of the email.

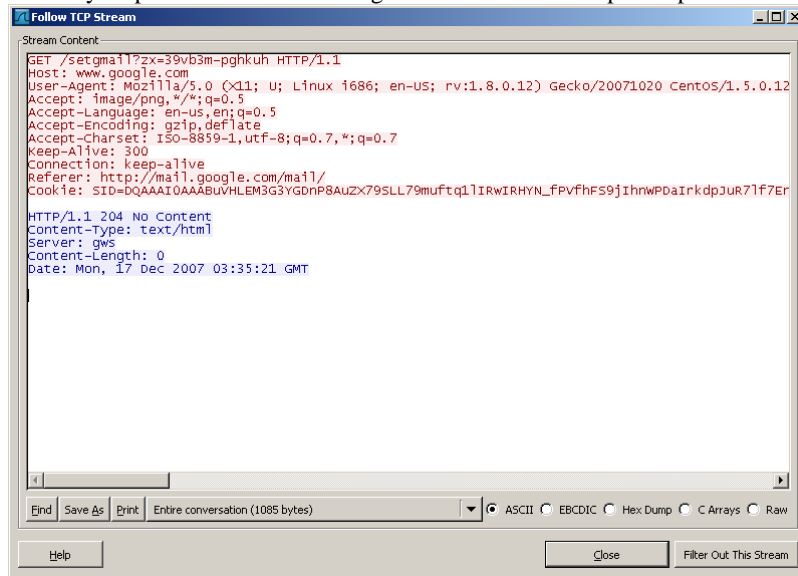


Figure 3: Sample of Gmail communication traffic

Gmailchat related content have also been identified, but there is no obvious traffic of Gmailchat being identified from the network packet. Therefore, it is assumed that Gmailchat may not be used but enabled in Gmail.

Because Gmail is usually encoded using GZIP between the browser and server, eWalker team parsed the pcap file through the Chaosreader.pl. Using this tool, network packets were categorized into streams and GZIP content of web traffic (or any other traffic) are automatically converted as gz file.

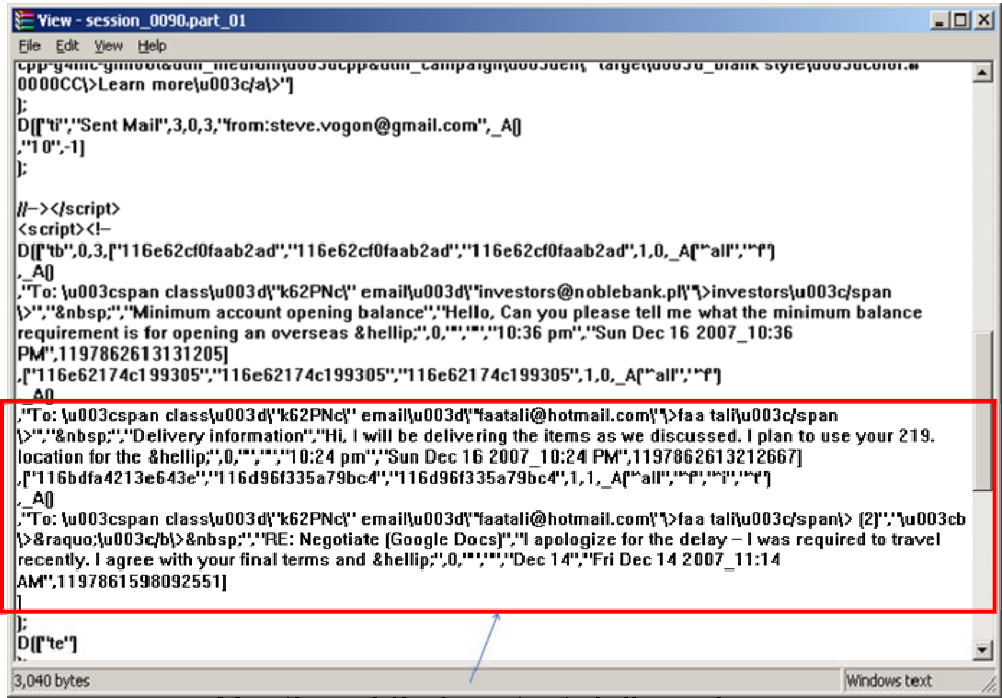
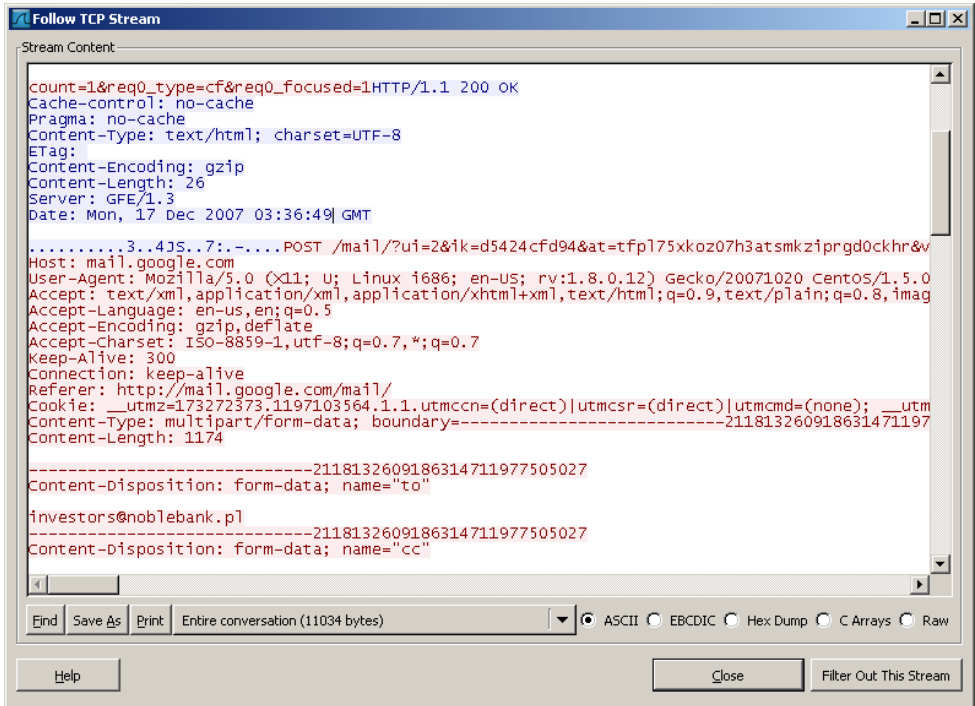
By further digging into the session_0081.part_01 content which was identified to be the network communication between Steve and Faatali, the following were identified.



Figure 4: Gmail communications extracted and decoded in Session_0081.part_01

Steve and Faatali may have transferred some important files through Windows Live (suspected to be Windows Live Messenger). But unfortunately, no trace of Windows Live Messenger could be observed by even searching the Windows Live Messenger connection protocol in the network content. So it is assumed Steve may be planning to transfer the file but not yet performed, or may have already transferred the file through from another machine or transferred before the network packet captured period.

While in the other of Gmail accessed, it was observed that Steve started to communicate with the Noblebank in Poland regarding to opening of account in that overseas bank.



Mentioned that content delivered

Figure 5: Gmail communications extracted and decoded in Session_0090.part_01

It was also found that Steve mentioned that he will deliver the information as discussed.

From the network packet captured, numbers of email addresses were identified. Many of them were simply email that appears on the web page downloaded during the web browsing activity. That may not be relevant to this case. Thus, email addresses that appeared in the email communication would definitely be more relevant to the case. The following email addresses have been identified and collected from the captured network packets:

steve.vogon@gmail.com
steve_vogon@hotmail.com
faatali@hotmail.com
investors@noblebank.pl

Based on the email communications, it is determined that Steve.vogon@gmail.com and steve_vogon@hotmail.com should be the email accounts owned by the person who used target machine for creating email.

In the network packet captured, it was identified that the user of the computer has also browsed some web pages other than Gmail and Google. Two relevant web sites included:
Travelocity (11:32:31 – 11:32:58)
NobleBank at (11:34:16 – 11:34:17)

While for the other web sites identified, as there is no obvious relationship with the case, no evidence has been collected:
youtube.com
Amazon.com
Facebook.com

Web History, Form History and Cookie Analysis

Network packet analysis identified some part of the information including the email, web address accessed. But detail information has to be identified from the target machine browser history.

Among the user directory, some files were extracted and determined to be relevant to the case². That includes:

history.dat
formhistory.dat
Cookies.txt
Firefox history files

Web History

From the directory structure and history file extension, it is assumed that the history file should be generated from the FireFox web browser in the target machine. FireFox web browser stored the browsing history record in the history.dat, autocomplete history record in the formhistory.dat and the cookies in the cookies.txt. So these files were extracted and passed to the relevant tools for interpretation.

Web history file history.dat is a binary file, but in known format. Web Historian and Dork, Mork.pl were used for analyzing the email.

According to the web history listed collected, it was observed that web history was first recorded from 08-Dec-2007.

The first web address that alerted the eWalker team was the access to vulnerability exploitation sites – milw0rm.com and metasploit.org. According to the web history, the user of the web browser has access to the following web sites and browsed for web vulnerabilities information from these web sites during 09-Dec-2007 14:29 – 15:34:

<http://milw0rm.com/>
<http://framework.metasploit.com/>
<http://metasploit.org/>

According to the URL link accessed to milw0rm.com, it was observed that the user has explicitly searched for Linux Kernel vulnerability, ELF vulnerability and X11 vulnerability.

² In the user directory, MidNight-Commander configuration file showed the artifact left behind by the DFRWS team, but that is not relevant to the case, so it will not be discussed in detail.

The most interesting findings were the identification of the Google Spreadsheets invitation page. From the web history, it was identified that

<http://spreadsheets.google.com/femail?id=o17742632304305298979.6904981162451457119.08953231559355367409.3362999466403390403&hl=en&to=%20%3Cfaatali%40hotmail.com%3E&cc=>

This URL link shown that faatali@hotmail.com invited the user Steve to access and review the spreadsheet. From the web history, it was confirmed that the web site was accessed in 2007-12-09 13:51:38 and last visited in 2007-12-09 13:52:11 by Steve. This also matched the records in the cookie file. In the Cookie file, the following information was identified:

id=o17742632304305298979.6904981162451457119.089532315593553674.htm
Where the last fetched was found to be 9 Dec 2007 13:51:37.

Cache information also shown the invitation email to accessed the spreadsheet content.

Invitation: Negotiate

From: Steve.Vogon@gmail.com
Collaborators: <faatali@hotmail.com>
Viewers:
Subject: Negotiate (Google Docs)
Message:

I've shared a document with you called "Negotiate":
<http://spreadsheets.google.com/ccc?key=pl958hhN-OvZf1K54yGvTxw>

It's not an attachment -- it's stored online at Google Docs. To open this document, just click the link above.

Add your message below: (optional)

Figure 6: Cached web page collected from the Web Cache files

While on 17-Dec-2007, user has no longer accessed to those exploitation web sites and the Google spreadsheets.

The list of web URL has been listed in Table 6. Among the list, user has accessed to many other web sites but as stated in the previous section, other than the Google, Gmail, NobleBank and Travelocity web site, other web sites should be less relevant to this investigation.

Form History

Another important piece of information is the web history information which was found from the form history file (user_files\.mozilla\firefox\n5q6tfua.default\formhistory.dat). This stores the auto-complete entries captured by the firefox browser when user filled in the forms.

By using the dumpAutoComplete tool, some interesting entries were identified.

Entries	Stored data	Web history
Answer to Google "Forget password" challenge:	IdentityAnswer: binky	
Web search history (?)	searchbar-history : CAN-2005-1263 extradition costa rica maldives non-extradition countries	

	overseas credit card payments panama extradition private banking privilege elevation 2.6.19	
Flight information (?):	firstNameForFlight1: Steve lastNameForFlight1: Vogon firstNameForFlight2: Catherine lastNameForFlight2: Lagrande goingTo: Costa Rica leavingDate : 12/30/2007 leavingFrom: Dulles	Assumed to be set to the server on 12/9/2007 – 15:48
Email subject (?):	subject: Account is set up Not identified in Gmail! Delivery information Minimum account opening balance Re: Negotiate (Google Docs	

Table 7: Relevant auto complete text dump from the Form History

According to the auto complete information, it was confirmed that the user Steve Vogon has planned to go for Trip from Dulles to Costa Rica on 30 Dec 2007. That matched the statement he stated in the email with Faatali.

Based on the Email subject highlighted, it was observed that “Account is set up”, “Not identified in Gmail!”, “Minimum account opening balance”, “Delivery information” and “Re: Negotiate (Google Docs)” were originally drafted in the browser.

The most interesting and important observation is the forget password answer to the Google account. With that information, eWalker team further collected some additional information directly from Steve’s Gmail account (Further details could be found in the Internet email analysis section).

Memory Analysis

Memory has been reviewed based on the strings and binary text viewer bintext.

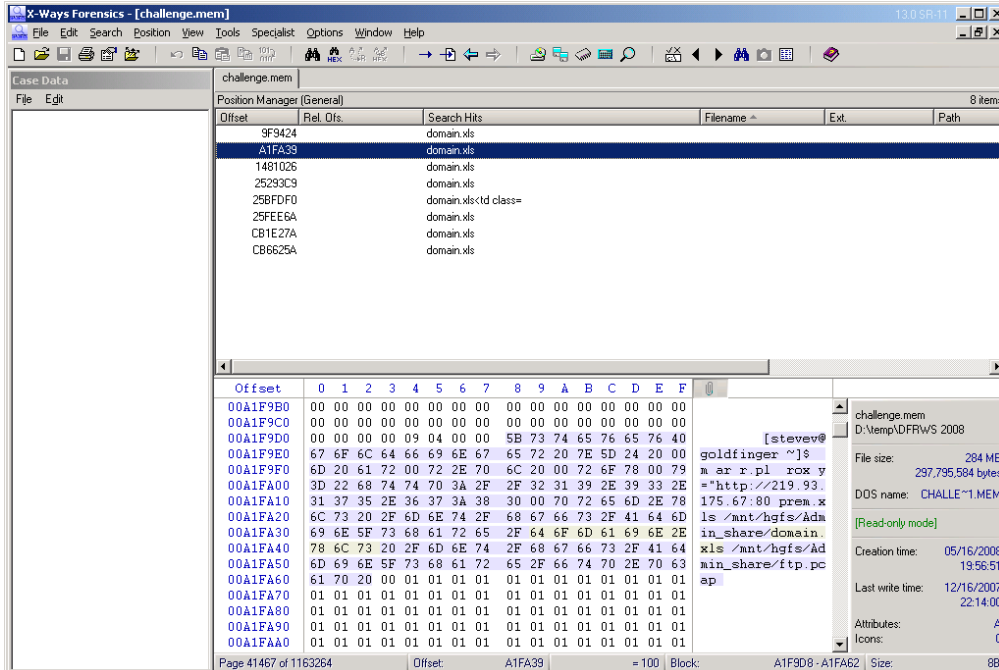
From the extracted text, Gmail access, mail content and web links were identified (http://www.google.com/support/accounts/bin/answer.py?answer=48598&hl=en&fpUrl=https%3A%2F%2Fwww.google.com%2Faccounts%2FForgotPasswd%3FfpOnly%3D1%26continue%3Dhttp%253A%252F%252Fdocs.google.com%252F%26followup%3Dhttp%253A%252F%252Fdocs.google.com%252F%26service%3Dwritely).

It was observed that Steve Vogon may have accessed the live.msn.com (.login.live.com TRUE /FALSE 2145801539 MSPPre steve_vogon@hotmail.com) but no further trace was picked up.

eWalker team has also attempted to use idetect to parse the linux dumped memory. However, because the team could not proper successfully parse the memory dump using that program, so no further identification could be found.

Digital certificate have also been spotted in the memory. However, because that may not be directly affecting the results, eWalker team decided to focus on the Internet content exploration.

After collecting the negotiation email content from the Gmail account, eWalker noticed that faatali actually would like to collect the domain.xls, intranet.vsd, acct_prem.xls and [ftp.pcap](#) files from Steve (further detailed will be explained in the following sections). Switching back to memory analysis, the team searched and identified the existence of the domain.xls, intranet.vsd, [ftp.pcap](#). From the identified format,



[steve@goldfinger ~]\$ m ar r.pl rox y =\"http://219.93.175.67:80 prem.xls /mnt/hgfs/Admin_share/domain.xls mnt/hgfs/Admin_share/ftp.pcap.

Figure 7: Extracted memory dump suspected to be containing file transfer information

It is likely Steve has planned and verified the location of the files. Those files were stored in the /mnt/hgfs/Admin_share folder of the target machine which has not been archived together in the user directory.

Then from another location in the memory, it is likely that Steve may have archived all the files to be sent into the archive.zip file.

```
zip archive.zip /mnt/hgfs/Admin_share/acct_prem.xls /mnt/hgfs/Admin_share/domain.xls /mnt/hgfs/Admin_share/ftp.pcap
```

Timestamps of the archive.zip file:

```
-rw-r--r-- 1 steve steve 21K Dec 16 22:28 archive.zip
```

Steve then transfer the file using a perl script:

```
steve@goldfinger:~.[steve@goldfinger ~]$ ./xfer.pl archive.zip ..Preparing archive.zip for transmission .....Sending now. Patience please .....Data transmission complete. Exiting.....]0
```

The potential source of the perl script is likely to be /mnt/hgfs/software/

```
[steve@goldfinger ~]$ cp /mnt/hgfs/software/xfer.pl .
```

Timestamp of the perl script:

```
-rwxrw-r-- 1 steve steve 3.2K Dec 16 22:28 xfer.pl
```

Internet Analysis

As highlighted in the previous section, only after eWalker team successfully viewed and collected the email from the Gmail account, the list of files can be confirmed.

Gmail

The first attempt to Steve's Gmail account was performed by using the formhistory challenge answer – *binky* to Steve's account. By submitting this answer, eWalker then changed the password and viewed the email content as well as accessed the spreadsheet in Google as Steve.

eWalker team noticed that after breaking into Steve's account, the evidence became vulnerable to the investigator. Any attempt may change the content of the evidence. However, before accessing to the Gmail account, eWalker team considered that action is similar to the activity performed in the live memory system. Therefore, investigator documented and recorded all actions performed and collected the necessary information as rapid as possible.

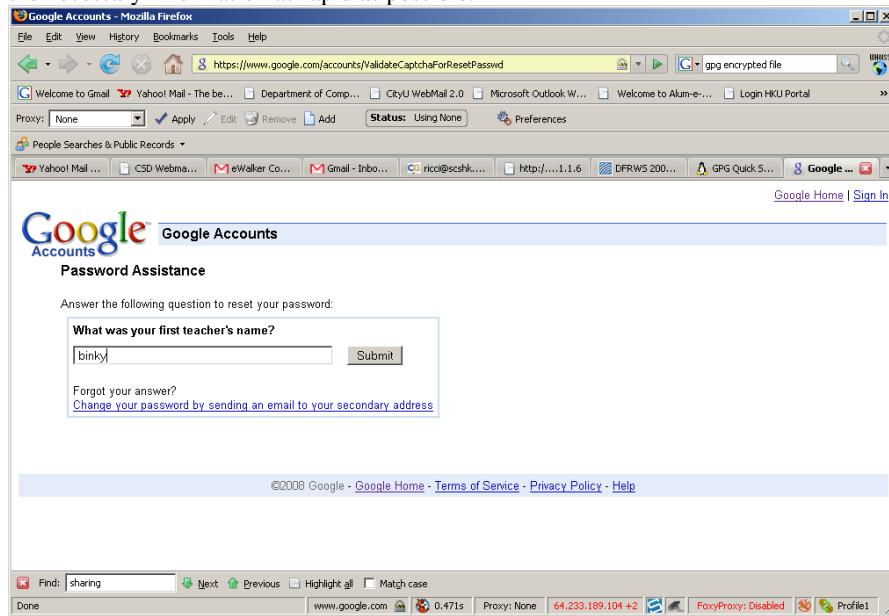


Figure 8: Accessing Steve's account using forget password challenge

After breaking into Steve account, following emails were found remaining in the mail box. Before eWalker team entered into the Gmail account of Steve, someone may have accessed or changed the content, eWalker cannot confirm that the emails listed in Gmail were the full list of emails possessed by Steve.

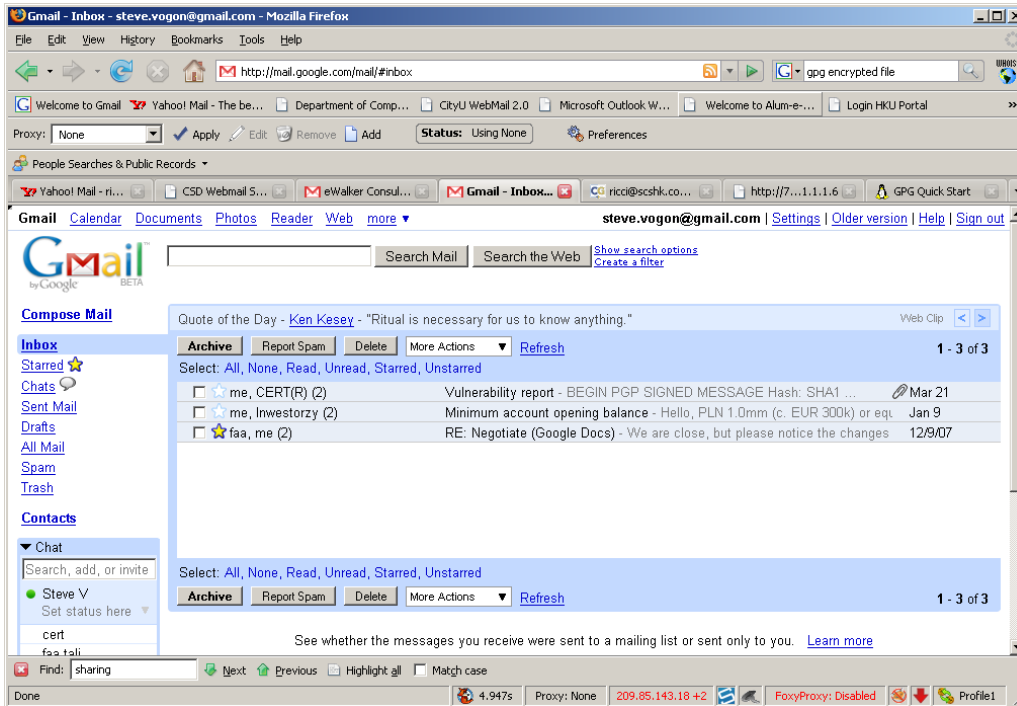


Figure 9: Email lists of Steve's Gmail account

Besides, trashed email may not exist in trash box for more than 30 days (defined by Gmail), therefore, at the time when eWalker team accessed to the mailbox, some trashed email may already been removed.

Then eWalker team read all the emails. Summarized email content was listed below:

1. Minimum account opening balance
 - steve.vogon@gmail.com ◇ investors@noblebank.pl: Mon, Dec 17, 2007 at 11:36 AM
 - investors@noblebank.pl ◇ steve.vogon@gmail.com: Wed, Jan 9, 2008 at 1:03 AM
2. RE: Negotiate (Google Docs)
 - faatali@hotmail.com ◇ steve.vogon@gmail.com: Sun, Dec 9, 2007 at 4:15 PM
 - steve.vogon@gmail.com ◇ faatali@hotmail.com: Sat, Dec 15, 2007 at 12:14 AM
 - Linked with the Google Spreadsheet: Negotiate
 - Starred

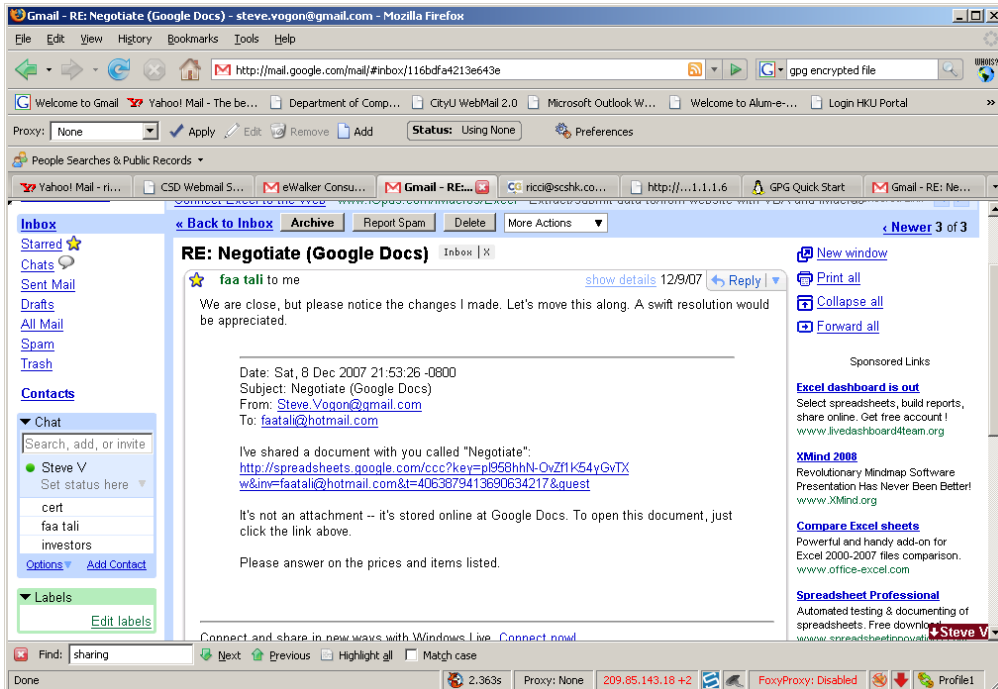


Figure 10: Negotiate (Google Docs) email with links to spreadsheets.google.com

3. Vulnerability report

- steve.vogon@gmail.com \diamond cert@cert.org: Fri, Mar 21, 2008 at 5:31 AM
- cert@cert.org \diamond steve.vogon@gmail.com: Fri, Mar 21, 2008 at 5:31 AM
- Attachment : vuln-report.zip.asc

4. Composed email: Delivery information

- steve.vogon@gmail.com \diamond faatali@hotmail.com: Mon, Dec 17, 2007 at 11:24 AM

According to the contact lists in Steve Gmail account, the following email addresses were identified and that matched with the email addresses identified in email communication channel.

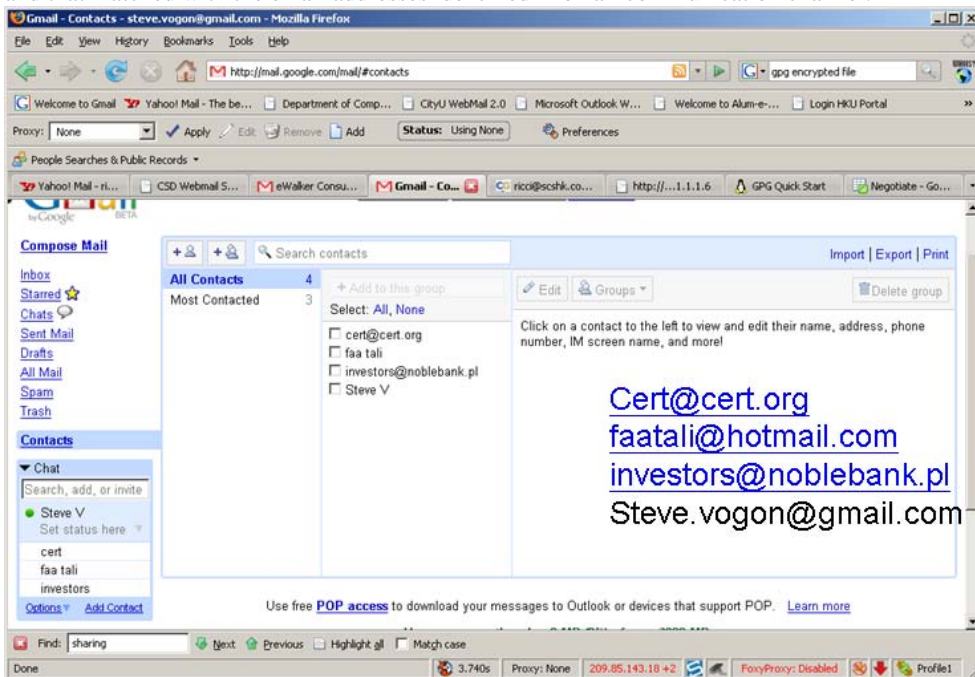


Figure 11: List of all contacts in Steve's Gmail account.

Spreadsheets

After collecting necessary evidence record, the team accessed to the spreadsheets.google.com – negotiate spreadsheet. The spreadsheet was located in Google Docs. Based on the conversation, it is likely that the document was created directly in Google Spreadsheets.

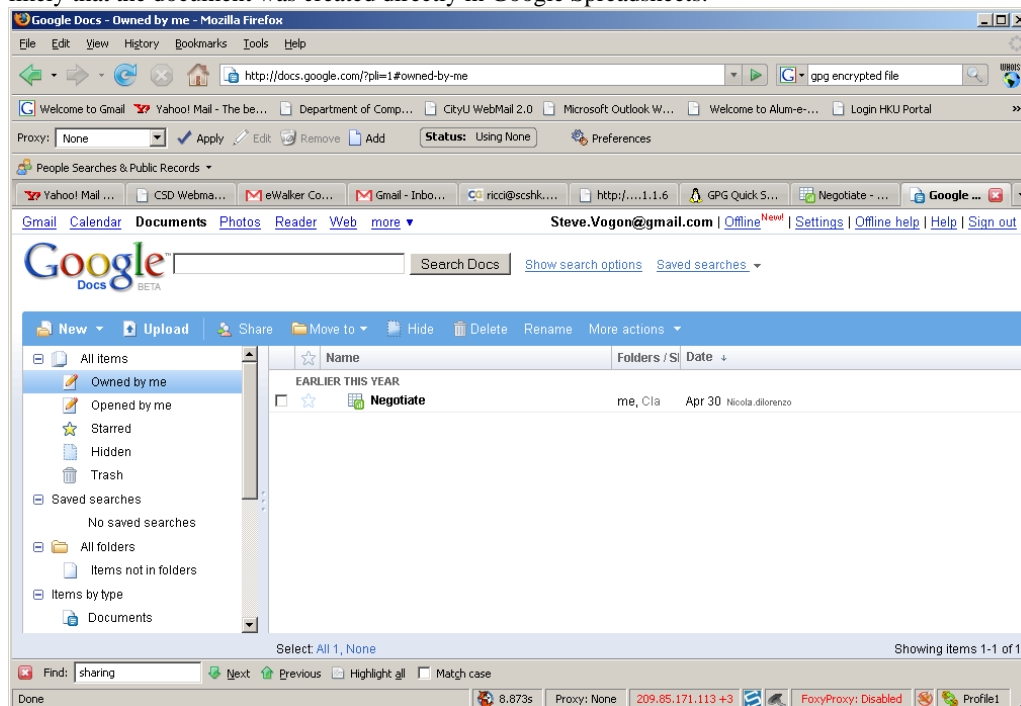


Figure 12: Google Docs listing the Negotiate spreadsheet.

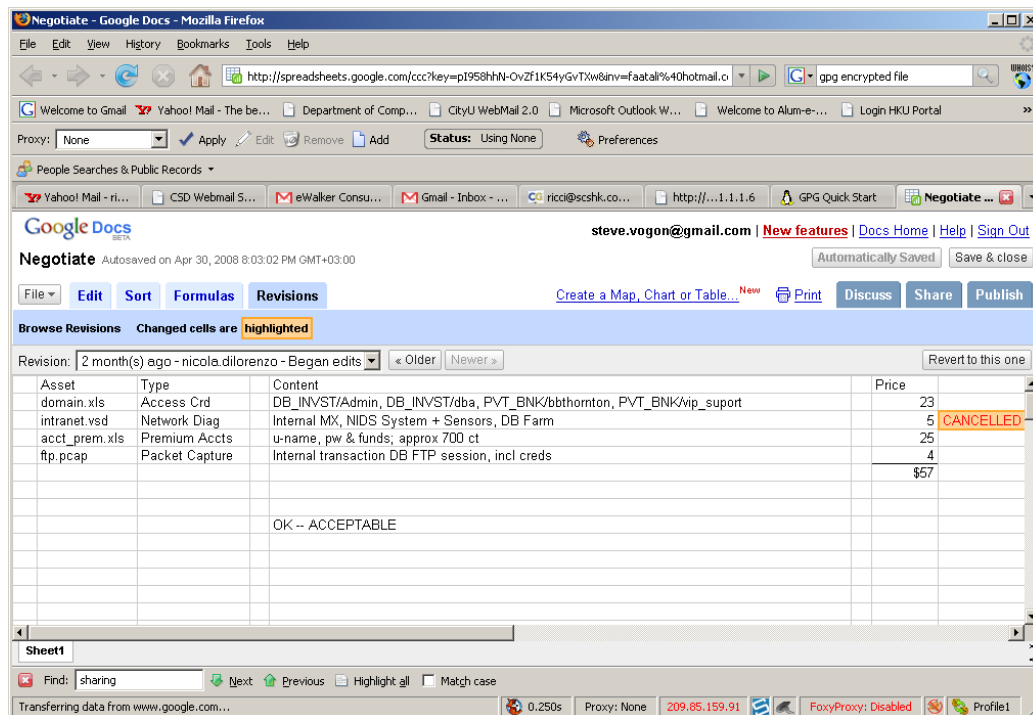


Figure 13: Access of Negotiate spreadsheets with highlighted enabled.

By enabling the view with highlights, modifications of the content were highlighted and the author of particular entries was shown. (but for entries entered over a period of time, they were no longer listed)

with detailed modification date). The modification dates to the spreadsheets were found below (further details of the spreadsheet content can be found in the screenshot kept in the attached presentation file).

- 6 months ago: Steve.Vogon created the document
- 6 months ago : Steve.Vogon added column text
- 6 months ago : Steve.Vogon pasted column text 'Content'
- 6 months ago : faatali added information about the 4 documents
- 6 months ago : Steve.Vogon decreased the prices³
- 6 months ago : Steve.Vogon added "OK -- ACCEPTABLE"
- Apr 30, 2008 8:03:02 PM GMT+03:00, nicola.dilorenzo added "CANCELLED" in the row of intranet.vsd

This listed out clearly which files and the requested content from Faatali.

Asset	Type	Content
domain.xls	Access Crd	DB_INVST/Admin, DB_INVST/dba, PVT_BNK/bbthornton, PVT_BNK/vip_suport
intranet.vsd	Network Diag	Internal MX, NIDS System + Sensors, DB Farm
acct_prem.xls	Premium Accts	u-name, pw & funds; approx 700 ct
ftp.pcap	Packet Capture	Internal transaction DB FTP session, incl creds

Table 8: The extracted content from the negotiate spreadsheet in Google Docs

As Nicola put down the cancelled in the spreadsheet, it is assumed that Nicola did not need Steve to send the Visio intranet diagram⁴.

Finally, the spreadsheet should be shared among 6 users.

- claudiogre@gmail.com
- desantis.fabrizio@gmail.com
- faatali@gmail.com
- kzsnow@gmail.com
- nicola.dilorenzo@gmail.com
- wietse@gmail.com

³ Steve should be the person selling the information, but it was found during the negotiation that the seller reduced the price. That was an unexpected action performed by a seller.

⁴ The date when Nicola revised the template is comparatively new, it is not known whether faatali really did not look for intranet.vsd.

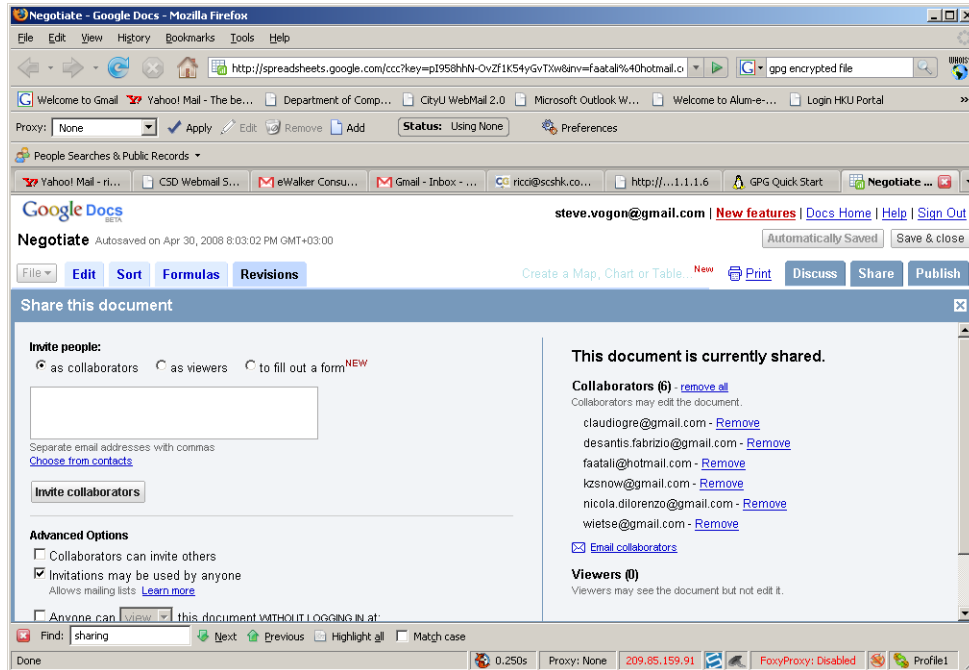


Figure 14: List of collaborators of the negotiate spreadsheets in Google Docs.

Time Analysis

As most information has already been explored and collected, it is necessary to determine the time line between the time of the network packet, local web history/web cache and the Gmail account dates before the event time line can be reconstructed.

eWalker used a methodology by picking one incident to correlate the time of all incidents. Firstly, from the Gmail content search and select for email heading and title. Then eWalker team searched through the network packet captured to identify the Gmail with the same title. Afterwards, history file was also searched and reviewed.

Throughout the investigation, it was observed that “Minimum account opening balance” appeared in network packet captured, Internet Gmail account and also web history. Thus, it was selected.

Source	Time	Time
Gmail with subject “Minimum account opening balance”	Dec 17 2007	11:36 AM
Network packet captured	Dec 17 2007	11:36:25
Gmail Server response message to the email	Dec 17 2007	03:36:53 GMT
Web History	Dec 17 2007	11:36:00 AM

Table 9: Timestamp of same email message

From the above information, it was confirmed that the Network packet captured time was only slightly deviated from the web history in the same machine. Also the time information matches closely with the time on the Gmail account. However, the server response time to the message did not match with the time zone of the sender “GMT +3 Qatar”.

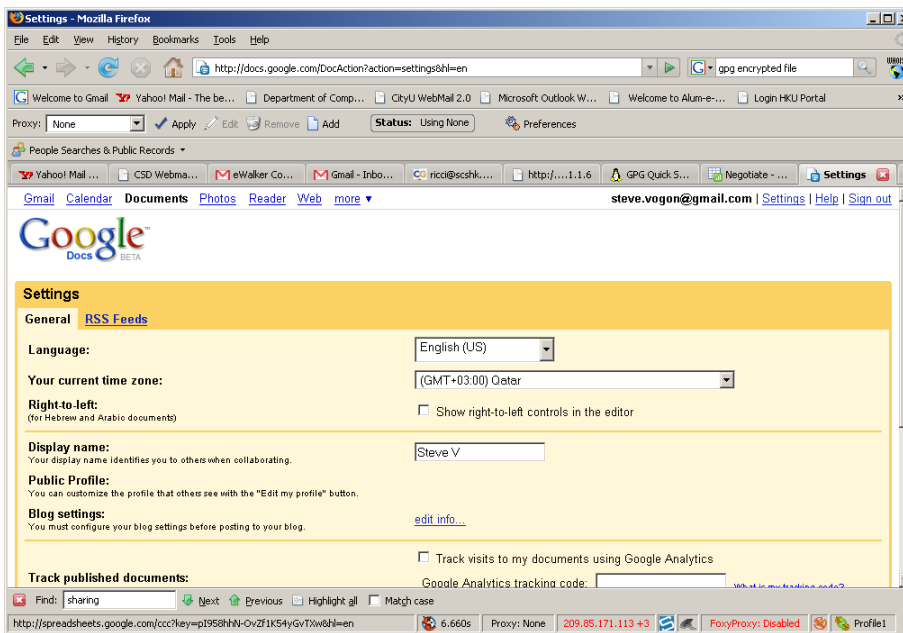
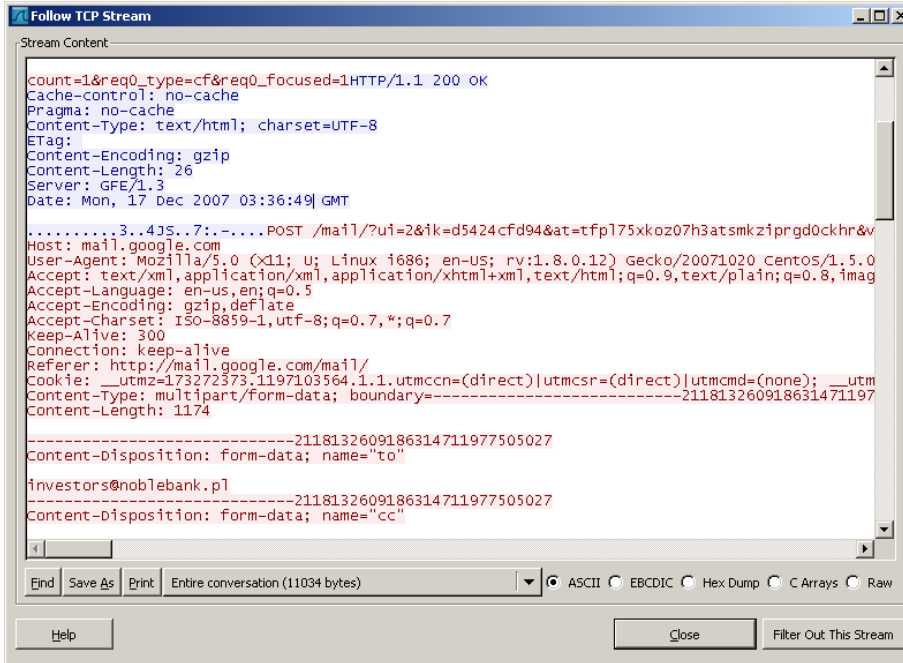


Figure 15: The top figure shows the Gmail server response time and the bottom figure shows the time zone set to the Gmail account.

Conclusions

After the thorough analysis, eWalker team concluded that based on the collected web history, it was observed that Steve Vogon started negotiated with Faatali through email.

Steve started to communicate with Faatali by setting up a spreadsheet on Google on or slightly around 8 Dec 2007 sensitive information negotiation. Faatali that provided the list of information required including IT infrastructure related information, network packet of internal transaction DB FTP session, including credentials, premium user accounts and access credentials as well as the price of those information.

After some pricing negotiation, Steve considered the price was reasonable and started to collect the information. The collected information should be kept in the target machine. He also searched the Internet on 9 Dec 2007 to see if there is any local vulnerability that can be utilized to gain root access to the server.

However, no evidence could be found from the provided information whether Steve actually performed any exploitation to the server. It can only confirm that Steve has ultimately collected some information and planned to send that information to Faatali.

Steve also planned to open an overseas account in Noble Bank of Poland. He also asked Faatali to transfer money to him through SWIFT.

According to the email communications captured in the network, it seems that Steve has or might plan to send the sensitive information through Windows Live Messenger.

Questions

1. What relevant user activity can be reconstructed from the data and what does it show? From the captured Gmail content, and the network traffic, it confirmed that Steve Vogon (steve.vogon@gmail.com) has contact Faatali (faatali@hotmail.com)

From the spreadsheets.google.com web site, it was observed that some other users may have participated in the negotiation process. Faatali has listed the pricing and the sensitive files he/she wanted Steve to collect. Steve has also negotiated with Faatali on the pricing before collecting the information.

Faatali and Steve agreed to use SWIFT for transfer of money and Steve asked Noble Bank to see if there is any method to transfer money to their offshore bank accounts.

According to email, it was observed that steve.vogon suggested using Windows Live Messenger for file transfer.

However, no trace of files transfer through live messenger could be successfully identified or recovered from the captured network packet or from the memory dump.

2. Is there evidence of inappropriate or suspicious activity on the system related to the user?

Some relevant information was found in the Spreadsheets.google.com and the Gmail content. Those could be verified from the browser history and cache files.

3. Is there evidence of collaboration with an outside party? If so, what can be determined about the identity of the outside party? How was any collaboration conducted?

Based on the content in the Spreadsheets.google.com, the history record in the Google Docs server confirmed that Faatali listed the information he/she would like to collect from the Steve.

The list of the collaborators in the Google Docs listed the email account of the collaborators. However, from the collected information, no evidence can lead back to the real name and identity of the person.

The collaboration was found to be performing through Gmail, spreadsheets.google.com. It is likely that the content of the sensitive files may be or may have been sent through Windows Live Messenger.

4. Is there evidence that sensitive data was copied? If so, what can be determined about that data and the manner of transfer?

The sensitive data being copied includes domain access credentials (DB_INVST/Admin, DB_INVST/dba, PVT_BNK/bbthornton, PVT_BNK/vip_support) in domain.xls, Premium Accts (u-

name, pw & funds; approx 700 ct) in acct_prem.xls, and Network packet captured from internal ftp server (Internal transaction DB FTP session, incl creds) in [ftp.pcap](#).

Those should be located in Steve machine and Steve planned to send that information to Faatali through Windows Live Messenger. According to the memory, the file may have been transferred using a script xfer.pl. However, no trace of file transfer was collected from the network packet.

Pending questions

After this review, some addition questions were spotted by the team.

1. As Steve negotiate with Faatali for information to be shared, why Steve lower the price instead of increasing the price during negotiation.
2. During the investigation, our team accessed to the web server for emails in Steve's Gmail account. Because, anyone who accessed into the Gmail account can change the content, it is not 100% sure that no one has changed the content of Gmail account after Dec 17, 2007
3. Any one who accessed to the Gmail account or spreadsheets can change the content. Tool should be developed to capture the access of the web site and prevent accidental access or modification of the Gmail content

<End of this document>