BNA, INC.

DIGITAL DISCOVERY & E-EVIDENCE

BNA Employee-Owned Since 1947

VOL. 11, NO. 8 REPORT APRIL 14, 2011

BNA INSIGHT

Exchange Message Tracking Logs—Message Forensics

BY JAMES R. SCARAZZO

With the ubiquity of e-mail comes the increased risk that corporate e-mail systems will be used for fraud. However, only the individual sending and receiving the messages knows the underlying meaning, and message flow occurs whether the intent is for the benefit, or contrary to, a company's interest. As a result, tools designed to monitor message flow for production and troubleshooting in an Exchange environment may also be applied to a forensic examination. This article discusses the use of one such tool, Microsoft's LogParser utility, for conducting investigations of unacceptable communications.

Brief History of Microsoft Exchange

Microsoft began its first proof of concept for its Exchange E-mail Server system in the early 1990's and, after considerable development time, shipped its first version of Exchange in June 1996. Although it was the earliest version of Exchange, it was externally shipped as Exchange 4.0, which was in line with Microsoft's marketing strategy to follow on the coattails of Microsoft Mail 3.5. For the next two years, Microsoft shipped newer versions, with Exchange 5.0 shipping in May 1997 and Exchange 5.5 shipping in February 1998.

In November 2000, Microsoft introduced Exchange 2000, which unlike its predecessors, integrated with Microsoft's Active Directory. Exchange 2000 was followed by Exchange 2003 in September 2003, Exchange 2007 in January 2007, and the latest version, Exchange 2010, which was released in November 2009.[1]

[1] History of Exchange: http://msexchangeteam.com/archive/2008/01/02/447806.aspx

At least as far back as Exchange 5.5, message logging was available, but not enabled by default on versions earlier than Exchange 2007. The message tracking features of Exchange create logs or records detailing message activity in an Exchange organization. In order to save space, the message tracking feature uses ''circular logging.'' Circular logging refers to the process by which older logs are overwritten by newer ones after a specified period of time.

Message Tracking Log Architecture

Generically, a message is an instance of data exchanged between running processes. It follows then, that the tracking of messages can be defined as ''logging,'' determining how and where such exchanges occurred and recording the messaging transactions for examination. The information tracked and logged varies from process to process.

The logging of data exchanges between processes is for the most part unknown to users, but in fact, records verification that the remote process has received the data or communication of other information that is necessary for the business processes to function properly. System administrators use message tracking for such things as troubleshooting, reviewing historic transactions, data mining, or performance evaluations. The forensic examiner can use this same information to determine what type of communication occurred and when (within the logging period).

It is the ability to mine or evaluate message activity which lends itself to a forensic examination of transactions. With respect to Exchange, the instances of data being tracked are electronic mail messages sent, received, and processed by the Exchange server.

Metadata. The logging process records information about the message event (the ''message metadata''), but does not store the message content.[2] Following is a partial list of the message metadata recorded in the Exchange message tracking log files:

- The date and time of the message event.
- The IP address of the messaging server or client that submitted the message.
- The name of the messaging server or messaging client that submitted the message.
- The IP address of the source or destination server running Microsoft Exchange.
- The name of the destination server.
- The message event type.
- An internal message identifier assigned by the Exchange server processing the message.
- A message ID found in the message header.
- Recipient address(es).
- The size of the message.
- The number of recipients receiving the message.
- The message subject.
- The sender address.

The message metadata is recorded in the tracking logs and persists until the log is overwritten, even if the actual e-mail message itself has been deleted, removed from the deleted items folder, and subsequently cleared from the Exchange Dumpster. (The Dumpster functions somewhat like the better-known Recycle Bin, and is described more fully below.) By default the logging period is 30 days but an administrator may set the period to a length of time more suited to specific business needs. Acceptable logging periods currently range from zero to 24,855 days.

Microsoft Exchange log files are written with a *.log extension but structurally are comma separated (CSV) text files. The files can be imported into a number of applications for review, parsed using third party tools, or as suggested here, analyzed using Microsoft's LogParser Utility.[3]

Background and Forensic Need

While message tracking is intended for an Exchange administrator's use for such things as collecting information about message flow, or gathering statistical information such as the number of messages sent or received, the message metadata contained in the logs can also be mined for forensic examination purposes.

Consider a scenario where suspicion arises that an individual or group of individuals is transmitting proprietary information to a competitor or an employee is e-mailing company information to a personal e-mail account. There are numerous instances where knowledge of what messages are being sent or received and when they are being sent or received, regardless of message content, might be of value.

A need may arise, for example, to know the top 10 persons with whom an individual communicates, as a basis for discerning which other employees or individuals are involved with an event. Examination of message tracking logs might provide or supplement information relevant to such questions.

Questions relative to subject content or dates and times of communications might be of interest. Tracking log message metadata might also provide insight into correspondence being sent from an employee to a competitor. Reviewing the metadata information captured by the tracking logs can identify valuable information about message traffic for further examination.

It is important to note, however, that the extent of the information available is contingent on

1) if logging is enabled;

2) when the event of interest occurred with respect to the retention time of the logs; and

3) whether the person of interest utilized the company's Exchange server as the means of communication.

Nevertheless, examination of message tracking logs should not be overlooked as a potential source of information.

Investigation Process

The logging process documents information being sent or received by an Exchange server. In a large organization with multiple Exchange servers, it might be necessary to collect the logs from all of the servers in order to fully understand the message flow.

If the Exchange server being examined is configured with Exchange 2003, message logging is disabled by default. To conduct the desired examination, message logging must be enabled on the Exchange server.

[2] http://technet.microsoft.com/en-us/library/cc539064.aspx

[3] Features of LogParser 2.2: http://technet.microsoft.com/en-us/library/ee692660.aspx

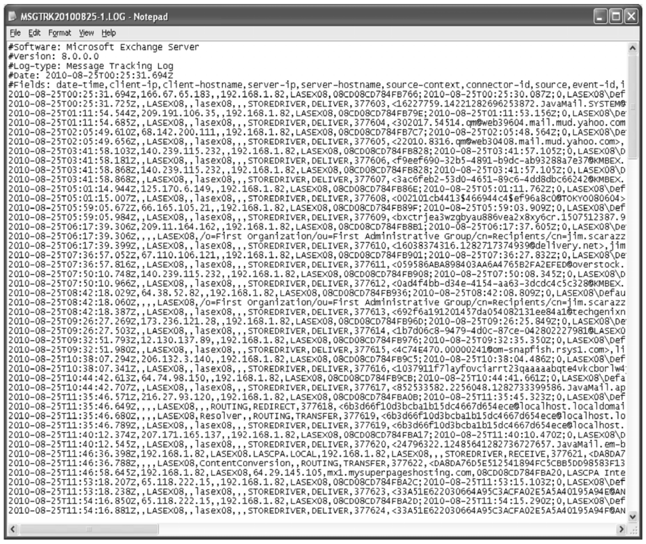
In an Exchange 2007 and Exchange 2010 environment, message tracking is enabled by default on servers having the Edge Transport, Hub Transport, or Mailbox roles installed. It is important to understand the Exchange configuration before proceeding. The examiner must also take precautions to document the validity of the copied logs and record the chain of custody for the electronic evidence. Consequently, the first step in the process is to determine if logging was enabled on the Exchange server(s) on which the mailbox(es) of interest is (are) stored.

Once a determination is made to collect the logs they may be copied from their location on the servers to external media. The log files should be hashed for evidentiary purposes, and a record of the collection should be made.

File Locators. The locations of the log files are configurable, but by default, message tracking logs are stored in the Exchange server installation location; specifically:
For Exchange 2003:
C:\Program Files\Exchsrvr\<ServerName>.log, where <ServerName> is the name of the host system on which Exchange 2003 was installed;
For Exchange 2007:
C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\MessageTracking.

In a forensic investigation, it is likely that the transaction logs will be copied from the Exchange server for examination, rather than conducting the review on a live system. Such being the case, a UNC path or a local path designation must be used to identify where the logs are located in order to use LogParser to run queries against the logs. If the local path contains spaces in the path name, the entire path must be delimited by single quotes. This path information will be utilized in the FROM parameter of the search query. If a local path is used, it is best to place the log files in a folder to which there are no spaces in the path name.

Queries. LogParser utilizes a SQL engine to query the log files and therefore has considerable power to return information about the tracking log contents. Some of the more common queries include messages sent and/or received by an individual, messages sent or/received by a particular domain, and messages containing certain key words in the subject line. It may also be of interest to determine the top number of messages communicated to or from certain persons.

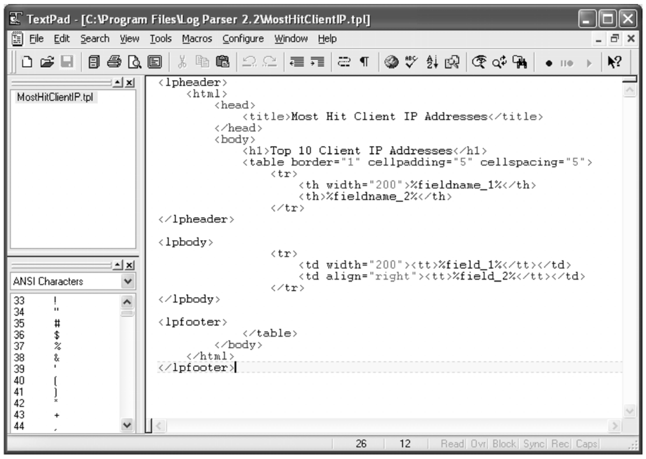


```
#Software: Microsoft Exchange Server
#Version: 8.0.0.0
#Log-type: Message Tracking Log
#Date: 2010-08-25T00:25:31.694Z
#Fields: date-time,client-ip,client-hostname,server-ip,server-hostname,source-context,connector-id,source,event-id,i
2010-08-25T00:25:31.694Z,166.67.65.183,,192.168.1.82,LASEX08,08CD08CD784FB766;2010-08-25T00:25:30.087Z;0,LASEX08\Def
2010-08-25T00:25:31.725Z,,LASEX08,,lasex08,,,STOREDRIVER,DELIVER,377603,<16227759.14221282696253872.JavaMail.SYSTEM@
2010-08-25T01:11:54.544Z,209.191.106.35,,192.168.1.82,LASEX08,08CD08CD784FB79E;2010-08-25T01:11:53.156Z;0,LASEX08\De
2010-08-25T01:11:54.685Z,,LASEX08,,lasex08,,,STOREDRIVER,DELIVER,377604,<302017.54514.qm@web39604.mail.mud.yahoo.com
2010-08-25T02:05:49.610Z,68.142.200.111,,192.168.1.82,LASEX08,08CD08CD784FB7C7;2010-08-25T02:05:48.564Z;0,LASEX08\De
2010-08-25T02:05:49.656Z,,LASEX08,,lasex08,,,STOREDRIVER,DELIVER,377605,<22010.8316.qm@web30408.mail.mud.yahoo.com>,
2010-08-25T03:41:58.103Z,140.239.115.232,,192.168.1.82,LASEX08,08CD08CD784FB828;2010-08-25T03:41:57.105Z;0,LASEX08\D
2010-08-25T03:41:58.181Z,,LASEX08,,lasex08,,,STOREDRIVER,DELIVER,377606,<f9eef690-32b5-4891-b9dc-ab93288a7e37@KMBEX.
2010-08-25T03:41:58.868Z,140.239.115.232,,192.168.1.82,LASEX08,08CD08CD784FB828;2010-08-25T03:41:57.105Z;0,LASEX08\D
2010-08-25T03:41:58.868Z,,LASEX08,,lasex08,,,STOREDRIVER,DELIVER,377607,<3ac6feb2-53d0-4651-89c6-4dd8dbc66242@KMBEX.
2010-08-25T05:01:14.944Z,125.170.6.149,,192.168.1.82,LASEX08,08CD08CD784FB86E;2010-08-25T05:01:11.762Z;0,LASEX08\Def
2010-08-25T05:01:15.007Z,,LASEX08,,lasex08,,,STOREDRIVER,DELIVER,377608,<002101cb4413$466944c4$ef96a8c0@TOKYO080604>
2010-08-25T05:59:05.672Z,66.165.105.21,,192.168.1.82,LASEX08,08CD08CD784FB89F;2010-08-25T05:59:03.909Z;0,LASEX08\Def
2010-08-25T05:59:05.984Z,,LASEX08,,lasex08,,,STOREDRIVER,DELIVER,377609,<bxctrjea3wzgbyau886vea2x8xy6cr.1507512387.9
2010-08-25T06:17:39.306Z,209.11.164.162,,192.168.1.82,LASEX08,08CD08CD784FB8B1;2010-08-25T06:17:37.605Z;0,LASEX08\De
2010-08-25T06:17:39.306Z,,,,LASEX08,/o=First Organization/ou=First Administrative Group/cn=Recipients/cn=jim.scarazz
2010-08-25T06:17:39.399Z,,LASEX08,,lasex08,,,STOREDRIVER,DELIVER,377610,<16038374316.1282717374939@delivery.net>,jim
2010-08-25T07:36:57.052Z,67.110.106.121,,192.168.1.82,LASEX08,08CD08CD784FB901;2010-08-25T07:36:27.832Z;0,LASEX08\De
2010-08-25T07:36:57.816Z,,LASEX08,,lasex08,,,STOREDRIVER,DELIVER,377611,<059586ABA898403AA6A4765B2FA2EFED@overstock.
2010-08-25T07:50:10.748Z,140.239.115.232,,192.168.1.82,LASEX08,08CD08CD784FB908;2010-08-25T07:50:08.345Z;0,LASEX08\D
2010-08-25T07:50:10.966Z,,LASEX08,,lasex08,,,STOREDRIVER,DELIVER,377612,<0ad4f4bb-d34e-4154-aa63-3dcdc4c5c328@KMBEX.
2010-08-25T08:42:18.029Z,64.38.52.82,,192.168.1.82,LASEX08,08CD08CD784FB936;2010-08-25T08:42:08.809Z;0,LASEX08\Defau
2010-08-25T08:42:18.060Z,,,,LASEX08,/o=First Organization/ou=First Administrative Group/cn=Recipients/cn=jim.scarazz
2010-08-25T08:42:18.387Z,,LASEX08,,lasex08,,,STOREDRIVER,DELIVER,377613,<692f6a191201457da054082131ee84a1@techgenixn
2010-08-25T09:26:27.269Z,173.236.121.28,,192.168.1.82,LASEX08,08CD08CD784FB96D;2010-08-25T09:26:25.849Z;0,LASEX08\De
2010-08-25T09:26:27.503Z,,LASEX08,,lasex08,,,STOREDRIVER,DELIVER,377614,<1b7d06c8-9479-4d0c-87ce-042802227981@LASEX0
2010-08-25T09:32:51.793Z,12.130.137.89,,192.168.1.82,LASEX08,08CD08CD784FB976;2010-08-25T09:32:35.350Z;0,LASEX08\Def
2010-08-25T09:32:51.980Z,,LASEX08,,lasex08,,,STOREDRIVER,DELIVER,377615,<4C74E470.00000241@om-snapfish.rsys1.com>,li
2010-08-25T10:38:07.294Z,206.132.3.140,,192.168.1.82,LASEX08,08CD08CD784FB9C5;2010-08-25T10:38:04.486Z;0,LASEX08\Def
2010-08-25T10:38:07.341Z,,LASEX08,,lasex08,,,STOREDRIVER,DELIVER,377616,<1037911f7layfovciarrt23qaaaaabqte4vkcborlw4
2010-08-25T10:44:42.613Z,64.74.98.150,,192.168.1.82,LASEX08,08CD08CD784FB9CB;2010-08-25T10:44:41.661Z;0,LASEX08\Defa
2010-08-25T10:44:42.707Z,,LASEX08,,lasex08,,,STOREDRIVER,DELIVER,377617,<852533582.2256048.1282733399586.JavaMail.ap
2010-08-25T11:35:46.571Z,216.27.93.120,,192.168.1.82,LASEX08,08CD08CD784FBA0B;2010-08-25T11:35:45.323Z;0,LASEX08\Def
2010-08-25T11:35:46.649Z,,,,LASEX08,,,ROUTING,REDIRECT,377618,<6b3d66f10d3bcba1b15dc4667d654ece@localhost.localdomai
2010-08-25T11:35:46.680Z,,,,LASEX08,Resolver,,ROUTING,TRANSFER,377619,<6b3d66f10d3bcba1b15dc4667d654ece@localhost.lo
2010-08-25T11:35:46.789Z,,LASEX08,,lasex08,,,STOREDRIVER,DELIVER,377619,<6b3d66f10d3bcba1b15dc4667d654ece@localhost.
2010-08-25T11:40:12.374Z,207.171.165.137,,192.168.1.82,LASEX08,08CD08CD784FBA17;2010-08-25T11:40:10.470Z;0,LASEX08\D
2010-08-25T11:40:12.545Z,,LASEX08,,lasex08,,,STOREDRIVER,DELIVER,377620,<24796322.12485641282736727657.JavaMail.em-b
2010-08-25T11:46:36.398Z,192.168.1.82,LASEX08.LASCPA.LOCAL,192.168.1.82,LASEX08,,,STOREDRIVER,RECEIVE,377621,<DA8DA7
2010-08-25T11:46:36.788Z,,,,LASEX08,ContentConversion,,ROUTING,TRANSFER,377622,<DA8DA76D5E512541894FC5CBB5DD98583F13
2010-08-25T11:46:58.645Z,192.168.1.82,LASEX08,64.29.145.105,mx1.mysuperpageshosting.com,08CD08CD784FBA20,LASCPA Inte
2010-08-25T11:53:18.207Z,65.118.222.15,,192.168.1.82,LASEX08,08CD08CD784FBA2C;2010-08-25T11:53:15.103Z;0,LASEX08\Def
2010-08-25T11:53:18.238Z,,LASEX08,,lasex08,,,STOREDRIVER,DELIVER,377623,<33A51E622030664A95C3ACFA02E5A5A40195A94E@AN
2010-08-25T11:54:16.850Z,65.118.222.15,,192.168.1.82,LASEX08,08CD08CD784FBA2D;2010-08-25T11:54:15.290Z;0,LASEX08\Def
2010-08-25T11:54:16.881Z,,LASEX08,,lasex08,,,STOREDRIVER,DELIVER,377624,<33A51E622030664A95C3ACFA02E5A5A40195A94F@AN
```

Figure 1 – Sample Partial Message Tracking Log

LogParser provides the examiner with control of the output format and permits the use of templates to create, among other things, an html report. Figure 1, Message Tracking Log[4], shows a typical log file opened in its raw state—an almost continuous stream of comma separated values.

Formats. Exchange 2003 Exchange logs used the W3C format. However, there is not a specific format for Exchange 2007 and Exchange 2010 logs so one must use CSV as the input format. The LogParser utility accepts both formats. LogParser also provides control of output formats. A practical output format is HTM. HTM files are written as defined by a template file. Figure 2 shows an example of a Template File.


TextPad - [C:\Program Files\Log Parser 2.2\MostHitClientIP.tpl]
File Edit Search View Tools Macros Configure Window Help
MostHitClientIP.tpl
ANSI Characters
33 !
34 "
35 #
36 $
37 %
38 &
39 '
40 (
41)
42 *
43 +
44 ,
26
12
Read Ovr Block Sync Rec Caps

```
<lpheader>
    <html>
        <head>
            <title>Most Hit Client IP Addresses</title>
        </head>
        <body>
            <h1>Top 10 Client IP Addresses</h1>
            <table border="1" cellpadding="5" cellspacing="5">
                <tr>
                    <th width="200">%fieldname_1%</th>
                    <th>%fieldname_2%</th>
                </tr>
</lpheader>

<lpbody>
                <tr>
                    <td width="200"><tt>%field_1%</tt></td>
                    <td align="right"><tt>%field_2%</tt></td>
                </tr>
</lpbody>

<lpfooter>
            </table>
        </body>
    </html>
</lpfooter>
```

Figure 2 Example Template Document

Examination

Any message flow examination, whether conducted for forensic or Exchange administrative purposes, is done to determine how, when, and to what extent communications occurred. Such queries might include determining the most frequent communications, if a particular individual was sending or receiving messages from an outside third party, if messages were sent containing a subject of interest, or examination for a number of other criteria. Since the log files persist for the specified logging period even if the messages themselves are purged, examination of the logs might provide evidence of communication when searching for the messages themselves does not.

The Exchange server has a feature referred to as ''the Dumpster.'' This feature retains messages for a set period of time (after a user removes them from the deleted items folder) to allow for recovery of deleted items, much as the recycle bin on a computer holds information until it emptied. By default, messages are retained

[4] All figures were created specifically for this article on a set of test data developed for illustrative purposes and do not represent any specific source or target any specific incident. They are intended purely to illustrative the points being discussed. Any association or identification of actual names or IP addresses is coincidental.

in the dumpster for seven days, after which they are purged from the Exchange database. On the other hand, also by default, the Exchange tracking logs are maintained for a period of 30 days. Therefore, it may be possible to discover evidence of communication by examining the tracking logs for several weeks after the actual message has been deleted from a user's mailbox and subsequently purged from the Exchange dumpster.

Examination of the tracking logs might also provide for a preliminary assessment before a more detailed review is undertaken. Likewise, inspection of the tracking logs may supplement and support the actual e-mail message review.

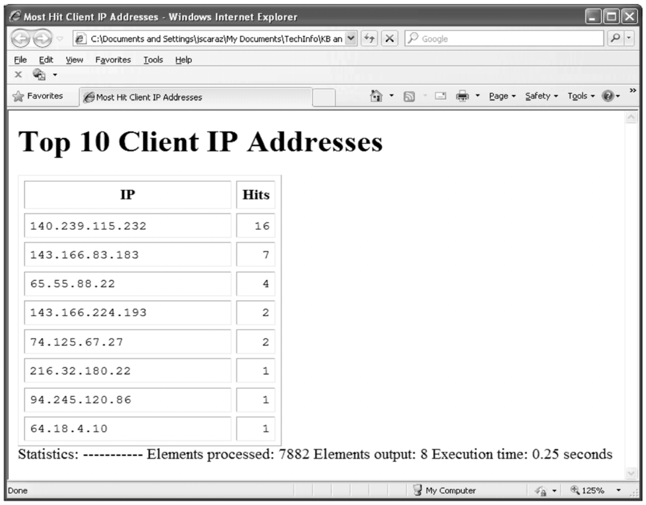
LogParser is a command line tool and can be installed on any Windows based machine. As noted above, the log files can be copied from the Exchange server to external media and examined outside of the Exchange environment. This provides for considerable flexibility.

Examples of Message Tracking Log Queries

Get Top 10 Addresses Sent by a Specific User. Examination for communications between internal and external individuals, the following query might be run:

```
LogParser ''SELECT TOP 10 server-ip as IP, COUNT(server-ip) AS Hits FROM \\\\<Path>\*.log Where ((source='SMTP') AND (event-id = 'SEND') AND (sender-address like'<Sender Address>')) GROUP BY server-ip ORDER BY Hits DESC'' -i:CSV -nSkipLines:4 -o:tpl -tpl mosthitClientIP.tpl > MostHitsSent.htm
```

The syntax of this query requests the top 10 addresses targeted by ''<Sender Address>'', counts the numbers of hits or times messages were sent, and exports the results to an HTM document named MostHits.htm. <Path> is the UNC or local path to where the logs are stored.


Most Hit Client IP Addresses - Windows Internet Explorer
C:\Documents and Settings\jscaraz\My Documents\TechInfo\KB an
Google
File Edit View Favorites Tools Help
Favorites
Most Hit Client IP Addresses
Page Safety Tools
Done
My Computer
125%

Top 10 Client IP Addresses

IP	Hits
140.239.115.232	16
143.166.83.183	7
65.55.88.22	4
143.166.224.193	2
74.125.67.27	2
216.32.180.22	1
94.245.120.86	1
64.18.4.10	1

Statistics: ----------- Elements processed: 7882 Elements output: 8 Execution time: 0.25 seconds

Figure 3 – Example of Query Results for Top 10 Addresses Targeted by an Individual

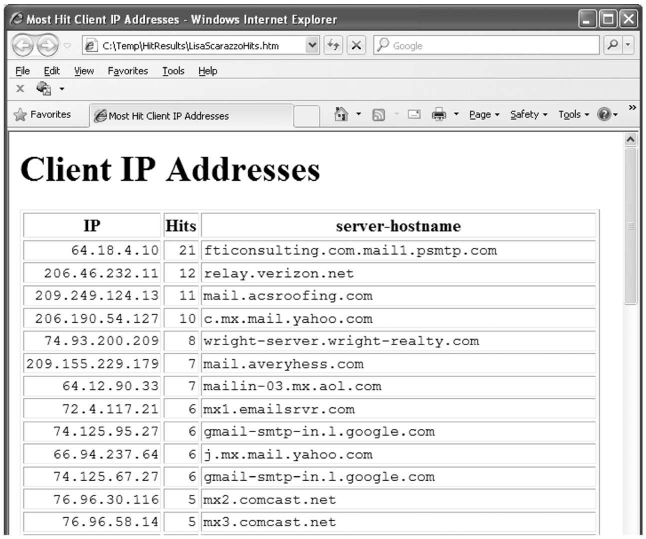
Figure 3 shows the results of such a query. The value of this examination is: it provides a documented method to determine if communications occurred between a given individual and outside sources, and identifies the frequency at which those communications occurred. The use of the Source-SMTP parameter signifies communications outside the company network. Internal communications could be evaluated by changing the source STOREDRIVER.

While this example was run on a small data set for demonstration purposes, the process is the same regardless of number of transactions recorded in the log files. This assessment might be conducted on several individuals and a target server IP address where the results are collated and reviewed for commonality and frequency. The results of such an examination might also provide some insight into a social network.

The query might be modified to target specific recipients as well as document if and how often communication occurred between individuals during the logging period. A slight modification, changing event-id = 'Receive' and sender-address to recipient-address would produce results of external communications delivered to a specific company employee.

Resolve Server Host Name. The tracking logs record a value for ''server-hostname.'' This field in the log file stores the name value of the server processing the request. With respect to outbound SMTP mail, this value is the name of the server receiving the message for the target domain. By including the server-host name as a field to select from the log, the receiving server name can be resolved:

```
SELECT server-ip as IP, COUNT(server-ip) AS Hits, server-hostname FROM <path> where ((source='SMTP') AND (event-id = 'SEND') AND (sender-address like <Sender Address>)) GROUP BY server-ip, server-hostname ORDER BY Hits DESC
```


Most Hit Client IP Addresses - Windows Internet Explorer
C:\Temp\HitResults\LisaScarazzoHits.htm
Google
File Edit View Favorites Tools Help
Favorites
Most Hit Client IP Addresses
Page Safety Tools

Client IP Addresses

IP	Hits	server-hostname
64.18.4.10	21	fticonsulting.com.mail1.psmtp.com
206.46.232.11	12	relay.verizon.net
209.249.124.13	11	mail.acsroofing.com
206.190.54.127	10	c.mx.mail.yahoo.com
74.93.200.209	8	wright-server.wright-realty.com
209.155.229.179	7	mail.averyhess.com
64.12.90.33	7	mailin-03.mx.aol.com
72.4.117.21	6	mx1.emailsrvr.com
74.125.95.27	6	gmail-smtp-in.l.google.com
66.94.237.64	6	j.mx.mail.yahoo.com
74.125.67.27	6	gmail-smtp-in.l.google.com
76.96.30.116	5	mx2.comcast.net
76.96.58.14	5	mx3.comcast.net

Figure 4 Sample of Results of a Host Server Name Query

Figure 4 shows the results of this query exported to HTM format. Resolution of a particular server name is more readable by humans and provides easy insight into where communications were being sent.

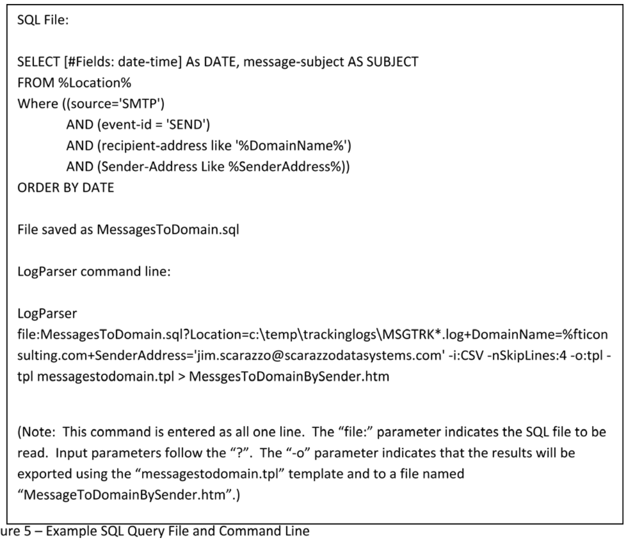
Again, a combination of queries might be run to examine commonalities with respect to communications.

Additional Considerations and Notes

All of the fields in the tracking logs can be queried depending on need. In addition to the queries outlined above, LogParser can be used to examine the logs for such things as subject keywords, dates of messages, events, or the source of the message. The results of the queries can be viewed on-line in the command prompt or exported to various formats for additional review.

Situations requiring examination for multiple parties might require the use of a batch file, exporting the results to individual HTM reports. LogParser query results can be exported to CSV file format, which might subsequently be imported to a database application for examination. LogParser allows for the import of query files so that complicated queries might be saved and certain parameters read in as variables. By creating SQL files, the examiner can be assured of reproducible results. Figure 5 provides an example of a SQL file and the associate LogParser command line. The SQL file is called from the LogParser command using the ''file:'' parameter.

In conclusion, LogParser is a powerful command line tool with considerable flexibility, permitting extensive examination of Exchange tracking logs for a number of items of interest and allows for the export of that information in multiple formats.



SQL File:

```
SELECT [#Fields: date-time] As DATE, message-subject AS SUBJECT
FROM %Location%
Where ((source='SMTP')
          AND (event-id = 'SEND')
          AND (recipient-address like '%DomainName%')
          AND (Sender-Address Like %SenderAddress%))
ORDER BY DATE
```

File saved as MessagesToDomain.sql

LogParser command line:

```
LogParser
file:MessagesToDomain.sql?Location=c:\temp\trackinglogs\MSGTRK*.log+DomainName=%fticon
sulting.com+SenderAddress='jim.scarazzo@scarazzodatasystems.com' -i:CSV -nSkipLines:4 -o:tpl -
tpl messagestodomain.tpl > MessgesToDomainBySender.htm
```

(Note: This command is entered as all one line. The "file:" parameter indicates the SQL file to be read. Input parameters follow the "?". The "-o" parameter indicates that the results will be exported using the "messagestodomain.tpl" template and to a file named "MessageToDomainBySender.htm".)

Figure 5 – Example SQL Query File and Command Line

Jim Scarazzo is a Director in the Technology practice of FTI, specializing in computer forensics. Mr. Scarazzo has extensive experience in computer systems, hardware, networks, and has performed numerous acquisitions and forensic analyses. Mr. Scarazzo has also provided testimony in matters involving electronic evidence and computer forensic examinations.

The views expressed in the article are held by the author and are not necessarily representative of FTI Consulting, Inc. or its other professionals. The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual, entity or transaction. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.