Exchange 2003 statistics with Logparser

Often when I try to get some information about customers current Exchange 2003 system they don't have a clue how much mail going through the system, other question that is unanswered is size of mail, when is mail delivered. Gathering this type of information is important since it can generate numbers to use as input when sizing your upcoming Exchange 2007 servers.

Activate Message tracking:
In these examples I use Exchange Message Tracking log files to run Logparser against. Other sources of information can be the SMTP protocol log files, but this is another story.
Most Exchange admins have activated Message Tracking but if you don't, start Exchange System Manager and drill down to the Server object, right click on it and select properties. Select the checkbox "Enable message tracking". This activation is per server basis and if you have multiple servers it's a good idea to activate it on all servers. It can be done with System server policy or by manually doing it on all servers. When activated; log files will be created in C:\Program Files\Exchsrvr\.log\ if you have installed Exchange in the default location.

Message tracking format:
When mail is sent in an Exchange server it goes through several steps before it actually arrives at the recipient inbox. Which steps involved also depends on where the message originates from and where it's sent to. Each event write a line in the message tracking log file and therefore every mail is logged several times with different Event-ID in the file. See Microsoft KB article 821905 for Message tracking event IDs in Exchange Server 2003. As stated in the KB article there is no single event that is logged a single time for each mail but the closest match is Event-ID 1019. Event-ID's is important depending on what information you want to get from log files.

Logparser:
What is Logparser? It's a very nice command line tool for parsing log files. Most log files are in some kind of text format such as CSV, W3C but it can also be eventlog and netmon trace files.
Start by download and install logparser from http://www.microsoft.com/downloads/details.aspx?FamilyID=890cd06b-abf8-4c25-91b2-f8d975cf8c07&DisplayLang=en. If you want results to be displayed as graphs you also need Office web components http://www.microsoft.com/downloads/details.aspx?FamilyID=7287252C-402E-4F72-97A5-E0FD290D4B76&displaylang=en. They only exists for office 2003 but can be used even if you run office 2007. Logparser is also available as a COM object so it can be used from scripts you write. http://msexchangeteam.com/files/12/attachments/entry445704.aspx
You don't need to install logparser on your Exchange server, simplest is to run it from your PC as long as you have access to the log files.

Running logparser:
Start by copy those message tracking log files you want to

examine from your Exchange server to a local directory on your PC. If you open a log file it will be opened with notepad which not do a great job of formatting it, my suggestion is to use wordpad if you want to open and read message tracking log files manually. Other important factors are from which server is log files copied, you would get different result if using log files from a mailbox server or from a server acting as a hub, also consider the Event-ID used when parsing log files.

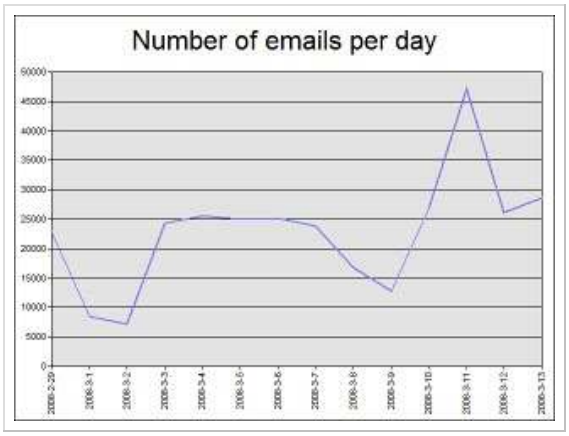
A common request is getting the number of email per day.
"C:\Program Files\Log Parser 2.2\LogParser.exe" "Select Date as Day,Count(*) as email from *.log where Event-ID = 1019 Group By Day" -i:W3C

Output will look like

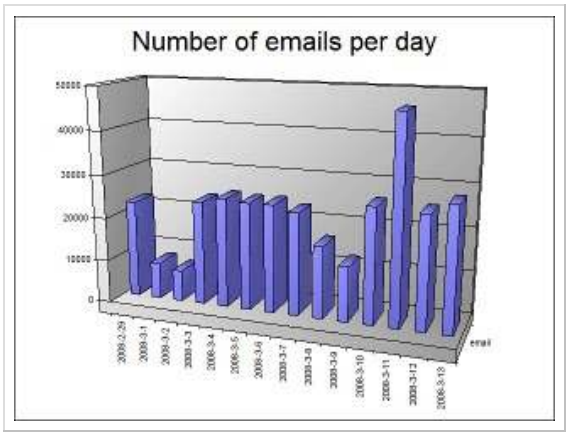
Day	email
2008-2-29	22869
2008-3-1	8479
2008-3-2	7234
2008-3-3	24290
2008-3-4	25504
2008-3-5	25020
2008-3-6	25096
2008-3-7	23806
2008-3-8	16864
2008-3-9	12754
2008-3-10	26683
2008-3-11	47088
2008-3-12	26132
2008-3-13	28605

What happens is that each logfile in the current directory is examined for rows where 'Event-ID = 1019'. The Date field is read and summed and then the output is grouped to get number of hits per day. In this example I have logfiles ranging from 29 Feb to 13 of Mar.

You can also output the result to jpg file
"C:\Program Files\Log Parser 2.2\LogParser.exe" "Select Date as Day,Count(*) as email Into chart.jpg from *.log where Event-ID = 1019 Group By Day" -i:W3C -o:Chart -Charttype:Line -Charttitle:"Number of emails per day" -View:on



or to a little more fancy 3D graph
"C:\Program Files\Log Parser 2.2\LogParser.exe" "Select Date as Day,Count(*) as email Into chart.jpg From *.log where Event-ID = 1019 Group By Day" -i:W3C -o:Chart -Charttype:Column3D -Charttitle:"Number of emails per day" -View:on



There are many different chart types available. If you run 'logparser.exe –h –o:Chart' you get a list of what charttype's is available.
Line,LineMarkers, LineStacked,LineStackedMarkers, LineStacked100,LineStacked100Markers, Line3D,LineOverlapped3D, LineStacked3D,LineStacked1003D, SmoothLine,SmoothLineMarkers, SmoothLineStacked, SmoothLineStackedMarkers,SmoothLineStacked100, SmoothLineStacked100Markers, BarClustered,BarStacked, BarStacked100, Bar3D,BarClustered3D, BarStacked3D,BarStacked1003D, ColumnClustered,ColumnStacked, ColumnStacked100,Column3D, ColumnClustered3D,ColumnStacked3D, ColumnStacked1003D,Pie, PieExploded, PieStacked, Pie3D,PieExploded3D, ScatterMarkers,ScatterSmoothLine, ScatterSmoothLineMarkers, ScatterLine, ScatterLineMarkers, ScatterLineFilled, Bubble,BubbleLine, Area, AreaStacked,AreaStacked100, Area3D, AreaOverlapped3D, AreaStacked3D, AreaStacked1003D, Doughnut, DoughnutExploded,RadarLine, RadarLineMarkers,RadarLineFilled, RadarSmoothLine,RadarSmoothLineMarkers, StockHLC,StockOHLC, PolarMarkers, PolarLine,PolarLineMarkers, PolarSmoothLine,PolarSmoothLineMarkers

When examining this statistic we can see that there is low volume on 1,2,8,9 of Mars and that should not be a surprise since those days are weekends. On the 11th we can see a higher volume.

Number of emails per hour:
"C:\Program Files\Log Parser 2.2\LogParser.exe" "Select Quantize(To_Timestamp(To_String(Extract_Prefix(Time,0,' ')),'h:m:s'),3600) as Hour,count(*) as email Into chart.jpg from 20080311.log where Event-ID = 1019 GROUP BY Hour ORDER

20080311.log where Event-ID = 1019 GROUP BY Hour ORDER BY Hour ASC" -i:W3C -o:Chart -Charttype:Line -Charttitle:"Number of emails per hour" -View:on

We can see that there is a high volume of email between 9 and 12 AM.
This logparser command reads the Time field and manipulates it to be in timestamp format in order for the Quantize parameter to work. Result from Quantize parameter is then summarized per hour and displayed in a line graph.

Or by adding all email from all log files per hour.
"C:\Program Files\Log Parser 2.2\LogParser.exe" "Select Quantize(To_Timestamp(To_String(Extract_Prefix(Time,0,' ')),'h:m:s'),3600) as Hour,count(*) as email Into chart.jpg from *.log where Event-ID = 1019 GROUP BY Hour ORDER BY Hour ASC" -i:W3C -o:Chart -Charttype:Line -Charttitle:"Number of emails per hour" -View:on

Other useful information is who is receiving most mail.
"C:\Program Files\Log Parser 2.2\LogParser.exe" "Select Top 10 Recipient-Address as Recipient,Count(*) as hits From *.log Where Event-ID = 1019 Group By Recipient Order By hits DESC" -i:W3C

Who is sending most email.
"C:\Program Files\Log Parser 2.2\LogParser.exe" "Select Top 10 Sender-Address as Sender,Count(*) as hits From *.log Where Event-ID = 1019 Group By Sender Order By hits DESC" -i:W3C

Which domain is receiving most email.

```
"C:\Program Files\Log Parser 2.2\LogParser.exe" "Select Top 10
Extract_SUFFIX(Recipient-Address,0,'@') as Recipient,Count(*)
as Hits from *.log Where Event-ID = 1019 Group By Recipient
Order By Hits DESC" -i:W3C
```

Avarage size on email per day.

```
"C:\Program Files\Log Parser 2.2\LogParser.exe" "Select
Date,AVG(total-bytes) From *.log Where Event-ID = 1019 Group
By Date" -i:W3C
```

```
Date AVG(ALL total-bytes)
--------- --------------------
2008-2-29 156344
2008-3-1 53003
2008-3-2 104991
2008-3-3 158491
2008-3-4 190721
2008-3-5 178313
2008-3-6 188157
2008-3-7 168273
2008-3-8 25809
2008-3-9 46874
2008-3-10 170719
2008-3-11 89262
2008-3-12 180671
2008-3-13 181731
```

Or just the average size of email in all log files.

```
"C:\Program Files\Log Parser 2.2\LogParser.exe" "Select
AVG(total-bytes) From *.log Where Event-ID = 1019 " -i:W3C
```

```
AVG(ALL total-bytes)
--------------------
144804
```

This gives us an average message size of 141KB