Understanding and Reading Mail Logs, Postfix Logs, Sendmail Logs, Qmail Logs
How do I read Mail Log?

Logs play a crucial role in identifying the issue may it be Basic Problem or a Big Problem heap, logs generated can make a System Admins life quite easy if you know what exactly they say. Understanding Mail Logs, Postfix Logs, Sendmail Logs or any other MTA are all the same. All the Mail Server Programs are Logging aware.

Lets get to work and understand the Logs generated by RSyslog Daemon. Sendmail Listens on Two ports
25 : MTA (Mail Transfer Agent)
587 : MSP (*Mail Submission Program/Port)

Example Log:

```
Feb 4 06:10:09 techy sendmail[5392]: o140e90B005392: from=,
size=2434, class=0, nrcpts=1,
msgid=<201002040040.o140e9Mi005380@techy.bounceme.net>, proto=ESMTP,
daemon=MTA, relay=localhost [127.0.0.1]
Feb 4 06:10:09 techy sendmail[5380]: o140e9Mi005380: to=root,
ctladdr=root (0/0), delay=00:00:00, xdelay=00:00:00, mailer=relay,
pri=32168, relay=[127.0.0.1] [127.0.0.1], dsn=2.0.0, stat=Sent
(o140e90B005392 Message accepted for delivery)
```

Feb 4 06:10:09 = Date of Mail received to the Mail Transfer Agent
techy = Hostname
sendmail[5392] = MTA or Application Name with PID for the Mail
o140e90B005392 = Queue ID
from= = Sender Address
to= Reciepient Address
Size=2434 = Size in Bytes
nrcpts=1 = Number of Recepients
msgid=<201002040040.o140e9Mi005380@www.linuxmaza.com> = Message ID (Unique of every Mail)
proto=ESMTP = Protocol Used
daemon=MTA = Application Handler In Sendmail it could be MSP or MTA
relay=localhost [127.0.0.1] = Mail relayed to the next Destination Server / Recipient Server
"delays=a/b/c/d"
where a=time before queue manager, including message transmission;
b=time in queue manager; c=connection setup time including DNS,
HELO and TLS; d=message transmission time. Numbers smaller than 0.01 seconds
are rounded to 0, to reduce the noise level in the logfile.

orig_to = This is omitted when the address did not change.
conn_use = This is omitted when a connection is used once.
ctladdr=root = Controlling user
dsn=2.0.0 = Delivery Status Notification, It can be 2.x.x, 4.x.x, 5.x.x Where 2.x.x is Successfully Sent, 4.x.x Is Mail Temporarily Deferred, 5.x.x stands for Permanent Failure
stat=Sent = Status of the Message. Values Sent,Deferred,Bounced

All the above parameters are almost same generated in Postfix Logs, Sendmail Logs, Qmail Logs also there could be some extra information about the mail added into the logs.