Email Header Example

Legend (mostly right!)

Received: from
Sending Server
Receiving Server
Message ID
Trace Headers
informational Headers
Body

Email Headers

```
Return-Path: <prvs=93188a193=SRS1@fsg.edu>
Delivered-To: steve@swaney.com
Received: (qmail 6338 invoked by uid 399); 14 Aug 2013 07:59:33 -
0000
X-Virus-Scan: Scanned by ClamAV 0.97.8 (no viruses);
 Wed, 14 Aug 2013 08:24:22 -0500
Received: from mta25.safeguardmail.net (184.172.50.186)
 by mail1.gohsphere.com with ESMTP; 14 Aug 2013 07:59:32 -0000
X-Originating-IP: 184.172.50.186
Received: from mta25.safeguardmail.net (localhost.localdomain
[127.0.0.1])
      by mta25.safeguardmail.net (8.13.8/8.13.8) with ESMTP id
r7ECjDpZ026369
      for <steve@swaney.com>; Wed, 14 Aug 2013 07:59:31 -0500
X-Haraka-RcptSummary: valid=1 invalid=0 unverified=0 relay=0
norelay=0
Received-SPF: None (mta25.safeguardmail.net: domain of jhu.edu
does not designate 166.129.8.141  as permitted sender)
receiver=mta25.safeguardmail.net; identity=mailfrom; client-
ip=166.129.8.141 ; helo=ipex1.fsg.edu; envelope-
from=<prvs=93188a193=SRS1@fsg.edu>
Received-SPF: None (mta25.safeguardmail.net: domain of
ipex1.fsg.edu does not designate 166.129.8.141  as permitted
sender) receiver=mta25.safeguardmail.net; identity=helo; client-
ip=166.129.8.141 ; helo=ipex1.fsg.edu; envelope-
from=<prvs=93188a193=SRS1@fsg.edu>
```

```
Received: from ipex1.fsg.edu (ipex1.fsg.edu [166.129.8.141 ])
      by mta25.safeguardmail.net (Haraka/2.1.4) with ESMTPS id
7B470838-3340-40DB-A8FE-0C227796FEF3.1
      envelope-from <prvs=93188a193=SRS1@fsg.edu>
      (version=TLSv1/SSLv3 cipher=RC4-SHA verify=OK);
      Wed, 14 Aug 2013 07:59:30 -0500
X-IronPort-AV: E=Sophos;i="4.89,876,1367985600";
  d="jpg'145?scan'145,208,217,145";a="295463734"
Received: from jhemtmwex3.win.ad.fsg.edu (HELO exchange.fsg.edu)
([10.181.198.38])
 by ipex1.fsg.edu with ESMTP/TLS/AES128-SHA; 14 Aug 2013 08:59:29
-0400
Received: from JHEMTMWEX2.win.ad.fsg.edu ([169.254.5.159]) by
JHEMTMWEX3.win.ad.fsg.edu ([168.25.6.206]) with mapi id
14.03.0123.003; Wed,
14 Aug 2013 08:59:28 -0400
From: Sharon Smith <SRS1@fsg.edu>
To: "steve@swaney.com" <steve@swaney.com>
Subject: Thanks
Thread-Topic: Thanks
Thread-Index: Ac6Y7g3f82K+pNHBTByN5jZc84A/bg==
Date: Wed, 14 Aug 2013 12:59:28 +0000
Accept-Language: en-US
Content-Language: en-US
X-MS-Has-Attach: yes
X-MS-TNEF-Correlator:
x-originating-ip: [10.181.39.184]
Content-Type: multipart/related;
      boundary="_004_6976DB235E1DE541BCB13748454B1884947838C8JHEMT
MWEX2winad_";
      type="multipart/alternative"
MIME-Version: 1.0
X-Haraka-Syntax: mail_case=upper mail_spaces=false
rcpt_case=upper rcpt_spaces=false
X-Haraka-GeoIP: US
X-Haraka-GeoIP-Received: 166.129.8.141 :US 10.181.198.38:UNKNOWN
169.254.5.159:UNKNOWN 10.181.39.184:UNKNOWN
X-Haraka-rDNS: ipex1.fsg.edu
X-Haraka-FCrDNS: ipex1.fsg.edu
X-Haraka-HostID: johnshopkins.edu
X-Haraka-SenderAuth: 166.129.8.141  jhu.edu
X-Haraka-Domain-Info: domain="jhu.edu" last_update=5
primary_ns="ens1.fsg.edu" serial=2013080901 refresh=3600
retry=900 expiration=1209600 minimum=3600 flags="SOA_UPDATE_7"
X-Haraka-DNSWL: white.ip.fslupdate.com:127.0.11.2
X-Haraka-NonLatin: 0
```

```
References:
<6976DB235E1DE541BCB13748454B1884947838C8@JHEMTMWEX2.win.ad.fsg.e
du>
Message-Id:
<WM!9f1c3dd20dd6422782878e577cfb170e3d1e60619b8f6c024af85b51d0010
ba448b0f53e6a229ba6f13ddb4f09926ce9!@mta25.safeguardmail.net>
X-SAFEGuardMail-Information: SafeGuardMail Service
X-SAFEGuardMail-MailScanner-ID: r7ECjDpZ026369
X-SAFEGuardMail: Found to be clean
X-SAFEGuardMail-SpamCheck: not spam, SpamAssassin (not cached,
score=-1.895,
     required 4, BAYES_00 -1.90, DI_SOA_UPDATE_7 0.00,
HARAKA_DNSWL 0.00,
     HARAKA_FCRDNS 0.00, HARAKA_SENDER_AUTH 0.00, HTML_MESSAGE
0.00)
X-Envelope-From: prvs=93188a193=SRS1@fsg.edu
X-SafeGuardMail-To: steve@swaney.com

--_004_6976DB235E1DE541BCB13748454B1884947838C8JHEMTMWEX2winad_
Content-Type: multipart/alternative;
     boundary="_000_6976DB235E1DE541BCB13748454B1884947838C8JHEMT
MWEX2winad_"

--_000_6976DB235E1DE541BCB13748454B1884947838C8JHEMTMWEX2winad_
Content-Type: text/plain; charset="us-ascii"
Content-Transfer-Encoding: quoted-printable

The pc was at our doorstep this morning.

Thank you very much

Sharon

Sharon Smith, M.B.A.
IT @ Enterprise Business Solutions
9001 Smith Avenue, Suite 3300
Washington DC 20007
```

Received Headers

Data is grouped into pairs (e.g. key value) except for data within brackets, which is treated like a comment.

```
from pex1.fsg.edu (ipex1.fsg.edu [166.129.8.141 ])
```
^^^ Usually the EHLO/HELO name that was used during the SMTP transaction.

```
(ipex1.fsg.edu [166.129.8.141 ])
 ^^^ rDNSf          ^^^ IP address literal

by mta25.safeguardmail.net (Haraka/2.1.4)
    ^^^ Hostname                ^^^ SMTP software

with ESMTPS
```

This describes the protocol used to receive the message. The most common are:

SMTP	Basic SMTP - no extensions (as RFC822). This means the connected client sent a HELO command after the initial SMTP banner.
ESMTP	Extended SMTP (as defined by RFC1869). This means the connected client sent an EHLO command after the initial SMTP banner.
ESMTPS	Extended SMTP with STARTTLS. The session was secured and encrypted with TLS.
ESMTPA	Extended SMTP with AUTH. The sender authenticated successfully via SMTP AUTH.
ESMTPSA	Extended SMTP with STARTTLS and AUTH.
mapi	Microsoft proprietary MAPI protocol.

```
id 7B470838-3340-40DB-A8FE-0C227796FEF3.1
```

The identifier assigned by the receiving server. Normally used to find a given session or transaction in the system logs.

And now look at the envelope-from line:

```
envelope-from prvs=93188a193=SRS1@fsg.edu
```

The SMTP envelope sender for this message. This is where a bounce message would be sent if the message could not be delivered for any reason. It will not necessarily correspond to the From: header (which is easily forged) but in this case, it does:

```
From: Sharon Smith SRS1@fsg.edu
```

```
(version=TLSv1/SSLv3 cipher=RC4-SHA verify=OK)
```

This is showing a comment which contains the TLS version and Cipher information. The verify=OK means that the common name supplied in the certificate matched the hostname of the machine and the certificate chain was trusted by the receiver. If the certificate chain could not be verified then this would show verify=FAIL - this is common in SMTP as most servers use self-signed certificates unless they are talking directly to MUAs which would otherwise display certificate warnings.