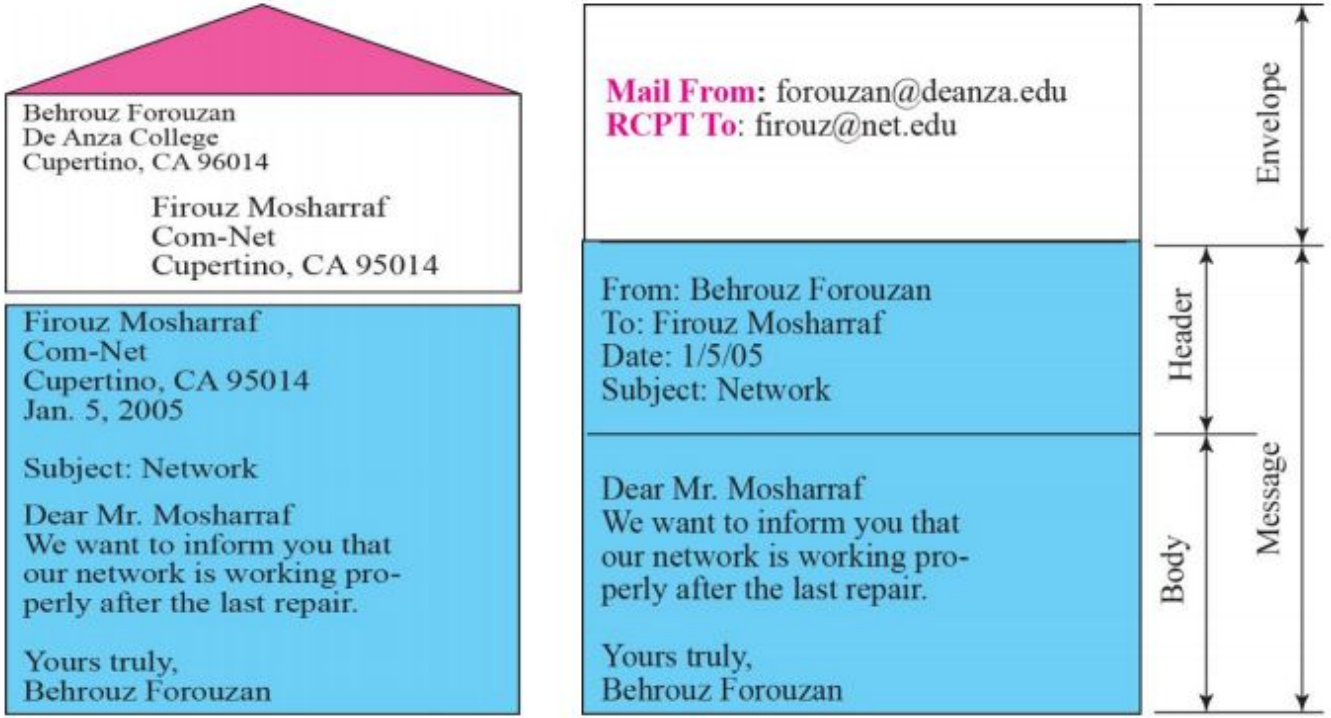
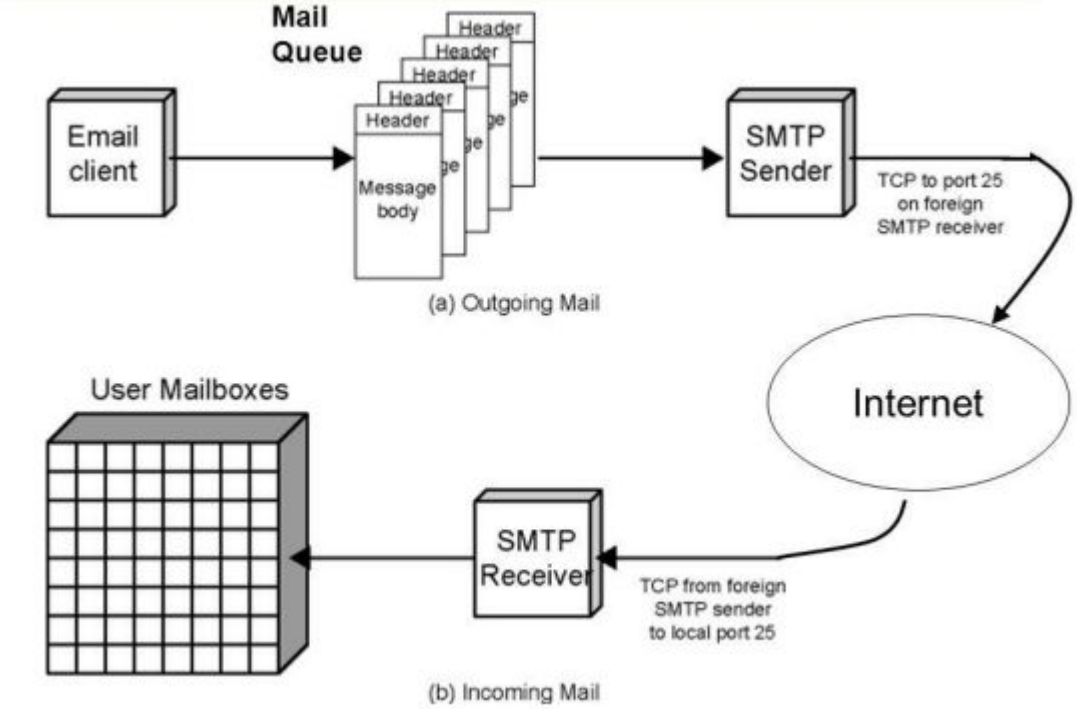
Dive Into Email Header

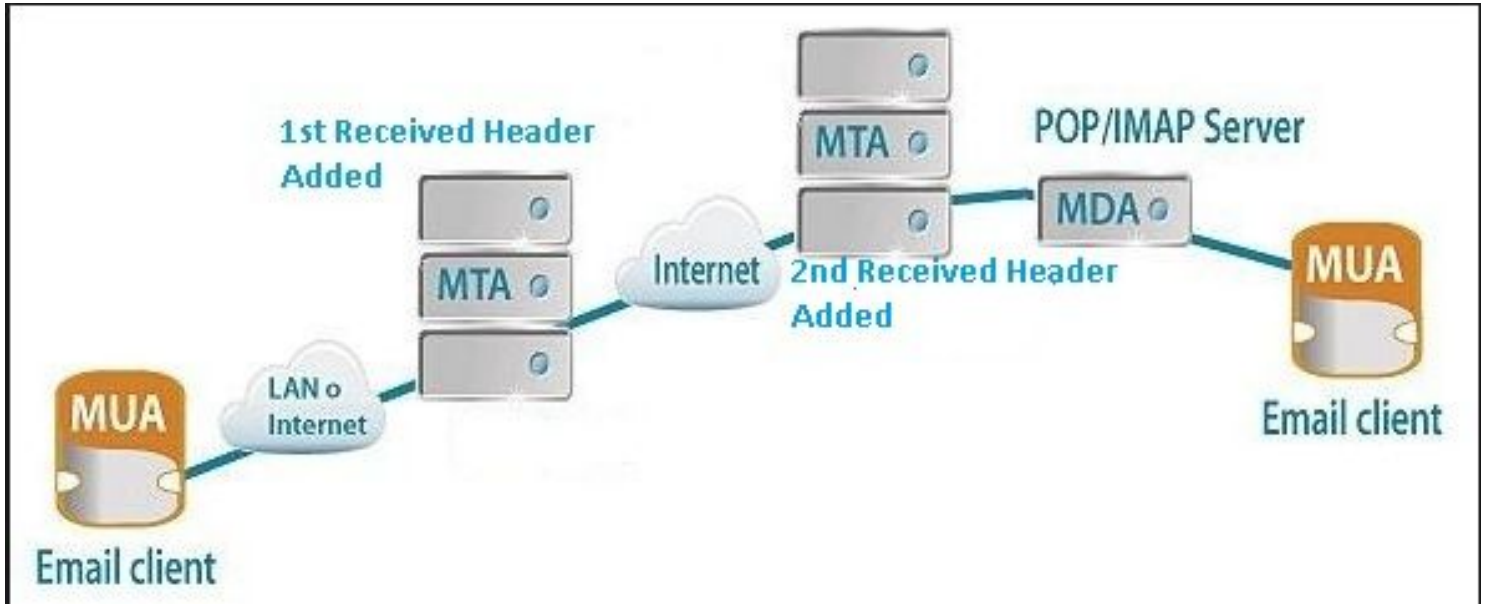
Format of an Email



SMTP Message Flow



SMTP Exchange Flow

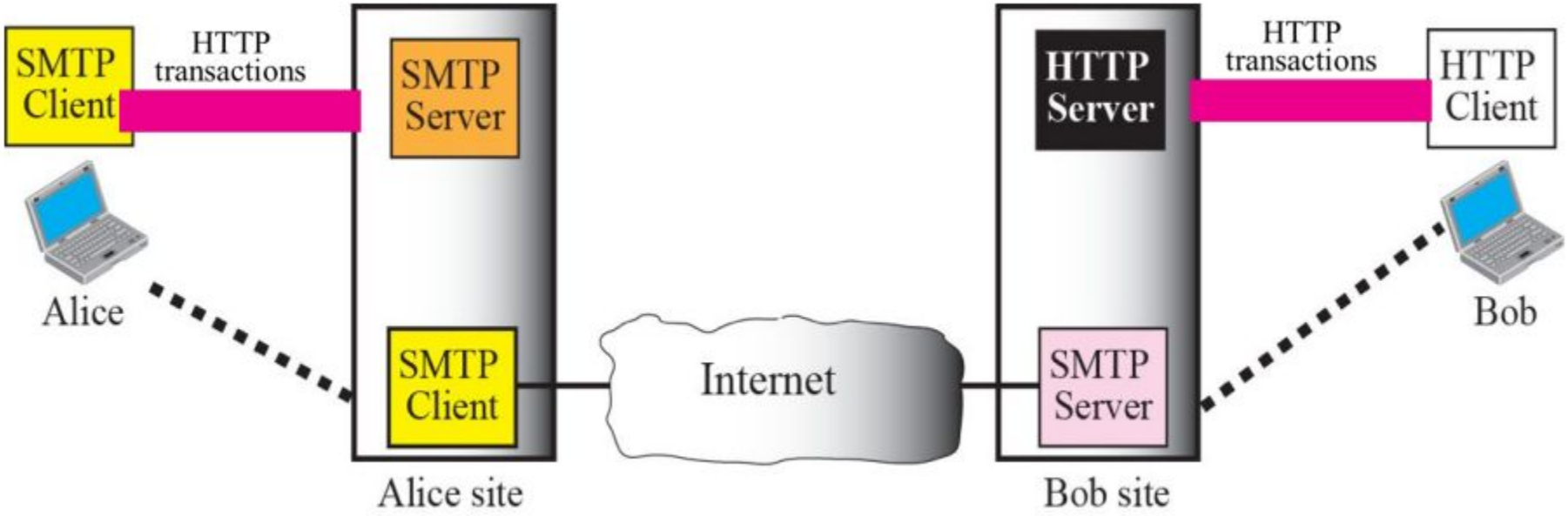


Components….

Several kinds of agents participate in SMTP exchanges:

- **MSA – Mail Submission Agent**
- **MTA – Mail Transfer Agent**
- **MDA – Mail Delivery Agent**
- **MUA – Mail User Agent**

Mail transaction over HTTP

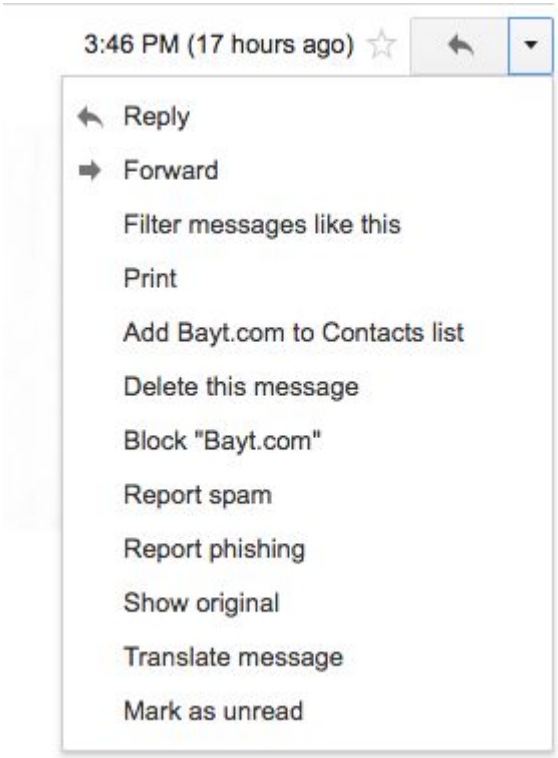


Find Email Header

Finding IP address in Gmail

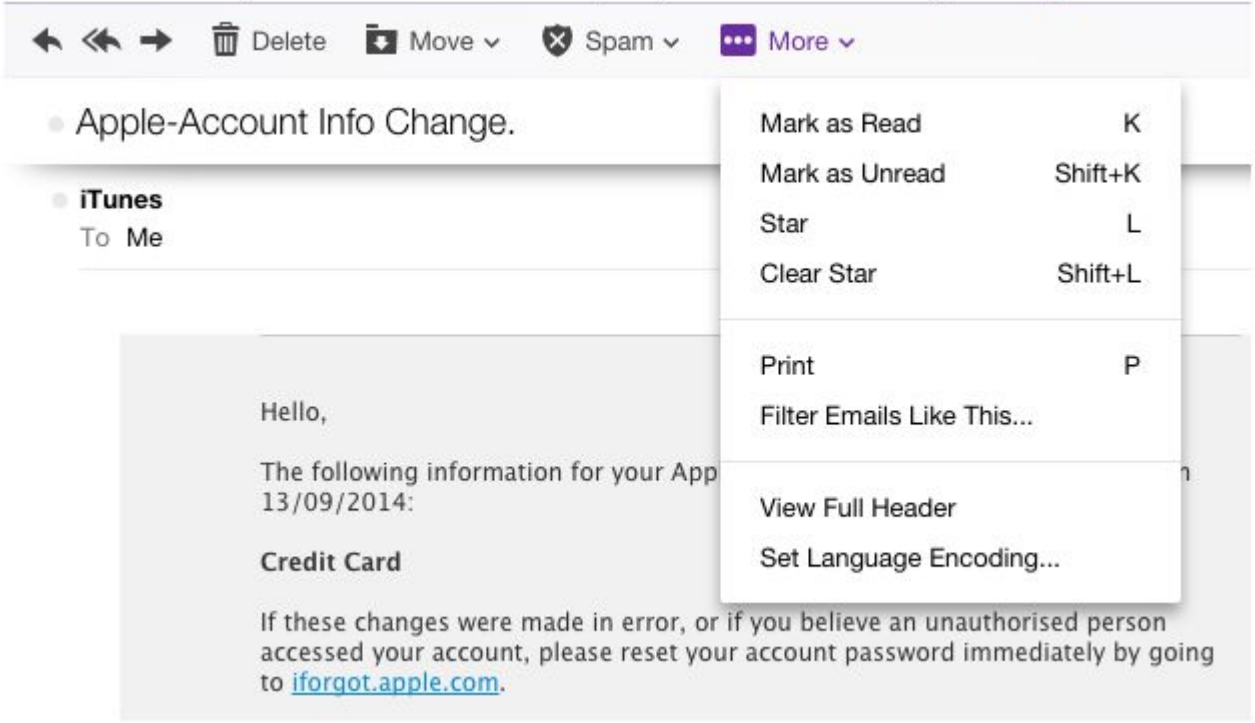
- Log into your Gmail account with your username and password.
- Open the mail.
- To display the email headers,

  Click on the inverted triangle beside **Reply**. Select **Show Orginal**.



YAHOO Email Header

- Log into your Yahoo! mail with your username and password.
- Click on **Inbox** or whichever folder you have stored your mail.
- Click on the email you want to track. When it opens, click on **More**. You'll get a dropdown menu.



Email Header

Return-Path: <suman@dhakacom.com>
X-Original-To: suman@amberit.com.bd
Delivered-To: suman@amberit.com.bd
Received: from antispam.amberit.net (antispam.amberit.net [202.4.96.35])
by mail.amberit.com.bd (Postfix) with ESMTPS id D7AC33860FD2
for <suman@amberit.com.bd>; Wed, 22 Mar 2017 09:09:49 +0600 (BDT)
X-ASG-Debug-ID: 1490152158-0a53fa7d2a89280001-lzhGtb
Received: from mail.dhakacom.com (www.dhakacom.com [202.4.96.5]) by antispam.amberit.net with ESMTP id T0DFBA77JotExORH
for <suman@amberit.com.bd>; Wed, 22 Mar 2017 09:09:18 +0600 (BDT)
X-Barracuda-Envelope-From: suman@dhakacom.com
X-Barracuda-Effective-Source-IP: www.dhakacom.com[202.4.96.5]
X-Barracuda-Apparent-Source-IP: 202.4.96.5
Received: by mail.dhakacom.com (Postfix, from userid 33)
id 137628003EC; Wed, 22 Mar 2017 09:08:48 +0600 (BDT)
To: suman@amberit.com.bd
Subject: How r you
X-PHP-Originating-Script: 501:rcmail.php
X-ASG-Orig-Subj: How r you
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="=_a886dd8b80748dca965c64ca9b39248d"
Date: Wed, 22 Mar 2017 09:08:48 +0600
From: Suman Kumar Saha <suman@dhakacom.com>
Reply-To: suman@dhakacom.com
Mail-Reply-To: suman@dhakacom.com
Message-ID: <f2cebde839d683746c86842ae7f10433@dhakacom.com>
X-Sender: suman@dhakacom.com
User-Agent: Roundcube Webmail/0.9.4

EMAIL Header

Return-Path: <sumansaha.bd@gmail.com>

X-Original-To: suman@amberit.com.bd

Delivered-To: suman@amberit.com.bd

Received: from antispam.amberit.net (antispam.amberit.net [202.4.96.35])
by mail.amberit.com.bd (Postfix) with ESMTPS id 412613860FC5
for <suman@amberit.com.bd>; Wed, 22 Mar 2017 09:04:30 +0600 (BDT)

X-ASG-Debug-ID: 1490151835-0a53fa7d2b88f70001-lzhGtb

Received: from mail-pf0-f193.google.com (mail-pf0-f193.google.com [209.85.192.193]) by antispam.amberit.net with ESMTP id uAFdMGf1OBS3uUHw (version=TLSv1.2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128 verify=NO) for <suman@amberit.com.bd>; Wed, 22 Mar 2017 09:03:57 +0600 (BDT)

X-Barracuda-Envelope-From: sumansaha.bd@gmail.com

X-Barracuda-Effective-Source-IP: mail-pf0-f193.google.com[209.85.192.193]

X-Barracuda-Apparent-Source-IP: 209.85.192.193

Received: by mail-pf0-f193.google.com with SMTP id r137so20834460pfr.3
for <suman@amberit.com.bd>; Tue, 21 Mar 2017 20:03:57 -0700 (PDT)

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;

X-Google-DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;

Email Header

x-Received: by 10.98.105.134 with SMTP id e128mr42229725pfc.19.1490151834448;
Tue, 21 Mar 2017 20:03:54 -0700 (PDT)
Received: from [192.168.20.38] ([202.126.123.53])
by smtp.gmail.com with ESMTPSA id z27sm89660pfg.38.2017.03.21.20.03.53
for <suman@amberit.com.bd>
(version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
Tue, 21 Mar 2017 20:03:53 -0700 (PDT)
From: Suman Saha <sumansaha.bd@gmail.com>
Content-Type: text/plain;
charset=us-ascii
Content-Transfer-Encoding: 7bit
Mime-Version: 1.0 (1.0)
Date: Wed, 22 Mar 2017 09:03:51 +0600
Subject: Hello
Message-Id: <38C99B49-140E-481B-A35C-D8DE9FBABA37@gmail.com>
X-ASG-Orig-Subj: Hello
To: Suman Amber IT <suman@amberit.com.bd>
X-Mailer: iPhone Mail (14D27)

Email Phishing Incident :Worth $40000

Received: from langtang.mos.com.np (langtang.mos.com.np [202.52.255.59])

Date: Wed, 09 Jul 2014 13:40:39 +0200

From: AbuL Hasan <abchasan@abc.com.bd>

To: <smforhad@abc.com.bd>

Organization: AbuL Hasan

Reply-To: <abchasan@outlook.com>

Mail-Reply-To: <abcsshasan@outlook.com>

Message-ID: <410f2b58efe0679d041a465a404b864f@mos.com.np>

X-Sender: abchasan@abc.com.bd

User-Agent: Roundcube Webmail/0.8.5

Paste your email header Here

http://www.iptrackeronline.com/email-header-analysis.php

Thanks!

Any questions?