

University of South Florida



[A-Z Index](#) - [Campus Directory](#) - [Calendars](#) - [Search](#)

| Main Menu |
|--|
| Home |
| Documentation |
| Security |
| Infrastructure |
| Official Policies |
| Standards and Procedures |
| Admin. Templates |
| DMCA Compliance |
| Software |
| Nessus |
| McAfee VirusScan |
| OSSEC |
| Other Tools |
| Suggested Software |
| Gramm-Leach-Bliley |
| Overview |
| PDF Flyer |
| Resources |
| Awareness Quiz |
| DShield Trends |
| Tips and How-To's |
| Copyright Info |
| Music |
| Movies |
| Software |
| Informative Videos |
| Legal Downloads |
| Links |
| USF Main Website |
| Get your NetID |
| myUSF |
| USF Network Statistics |
| Site Info |
| About This Site |
| Site News |
| Contact |

Security website

Looking at 'Full Headers' From an Email



When you read an email, you usually only see a few pieces of the information. You see the sender's address, sometimes his or her name, and the 'body' of the message. Much like the Post Office stamp tells you which Post Office was used to send you an envelope, the **Headers** of an email can tell you exactly where an email originated.

Here's an example of all the headers available on a piece of email:

```
Return-Path: <TDGSBZSP@dummy.com>
X-Original-To: me@spock.acomp.usf.edu
Delivered-To: me@spock.acomp.usf.edu
Received: from ritchie.acomp.usf.edu (ritchie.acomp.usf.edu
[131.247.100.10])
  by spock.acomp.usf.edu (Postfix) with ESMTTP id 4BE5141DE5
  for ; Wed, 3 Mar 2004 13:47:39 -0500 (EST)
Received: by ritchie.acomp.usf.edu (Postfix)
  id 93FF82ADE3; Wed, 3 Mar 2004 13:54:35 -0500 (EST)
Delivered-To: me@ritchie.acomp.usf.edu
Received: from c-67-172-14-146.client.comcast.net (c-67-172-14-
146.client.comcast.net [67.172.14.146])
  by ritchie.acomp.usf.edu (Postfix) with SMTP
  id 0C5562ADD4; Wed, 3 Mar 2004 13:54:32 -0500 (EST)
Received: from 86.224.7.64 by 67.172.14.146; Wed, 07 Jan 2004
14:36:43 +0600
Message-ID:
From: "Carey Quinones" <TDGSBZSP@dummy.com>
Reply-To: "Dummy User" <TDGSBZSP@dummy.com>
To: me@ritchie.acomp.usf.edu
```

```
Subject: Are you a junky? bml  
Date: Wed, 07 Jan 2004 12:30:43 +0400  
Content-Type: multipart/alternative;  
boundary="--89836586738176973240"
```

Your mail reader usually only displays the underlined, green headers: 'From,' 'Subject,' etc. Often administrators have to look at the 'Received' headers in order to track down a spam or a virus infection. While the 'From' information is easy to fake, 'Received' headers take a bit more work.

The procedure used to display all the headers on an email will vary depending on the software you are using to read your email. Here are some of the more popular readers.

Outlook Users

1. Highlight the email you want to investigate by selecting it from the list of emails.
2. Right click on the same email, and select **Options**
3. The headers will be displayed under **Internet Headers**. You can copy from this window by selecting the text you want to copy and hitting **Ctrl-C**

Mozilla Thunderbird Users

1. Highlight the email you want to investigate by selecting it from the list of emails.
2. Hit **Ctrl-U** on your keyboard.
3. A window will pop up with the raw code for your email. You can copy from this window by selecting the text you want to copy and hitting **Ctrl-C**

mailbox.acomp.usf.edu Users

1. From the list of emails, click on the message you want to see.
2. Once the message comes up, select **Message Source**
3. A window will pop up with the raw code for your email. You can copy from this window by selecting the text you want to copy and hitting **Ctrl-C**

© 2003-2008 USF Incident Response Team