# 

# ITT-306: Understanding Email Headers

**Purpose**

After examining the details of the headers of an email message, you will be able to identify products and protocols used to filter spam and ensure that messages are secure.

**Spam Experiment**

I decided to send myself a clearly “spammy” message from my university email account to my Google Gmail account. I thought the message would get filtered out by university or Google but instead both the initial message and the reply were delivered. It is a short message that contains a clear reference to a spam seller, but the message was delivered anyway. It turns out that the spam filters do not usually rely on identifying spam by reading the contents of a message. Instead, they rely on behind the scenes checks of trusted domains and mail servers. There is a huge amount of overhead text included in every message you send.

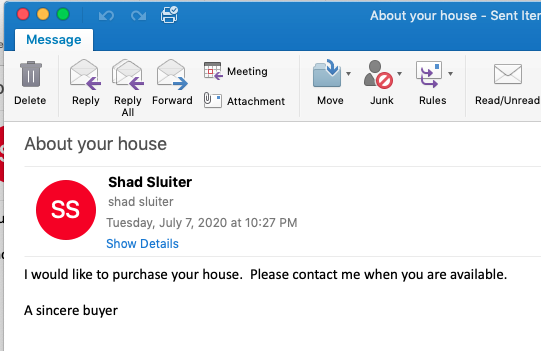
**Directions**

1. Examine the details of the initial message and the reply.
2. Read the explanations of each of the header lines.
3. Answer the questions in Part 3 of the assignment.

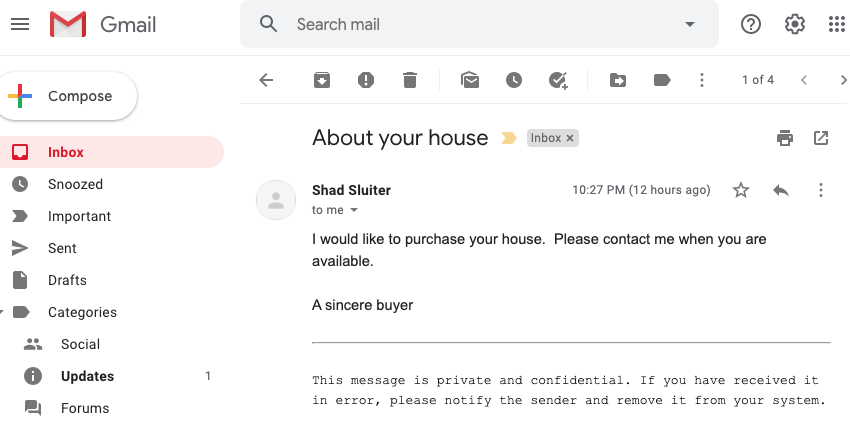
## Part 1: The Messages

The following message was sent from [shad.sluiter@gcu.edu](mailto:shad.sluiter@gcu.edu) to [shadsluiter@gmail.com](mailto:shadsluiter@gmail.com)

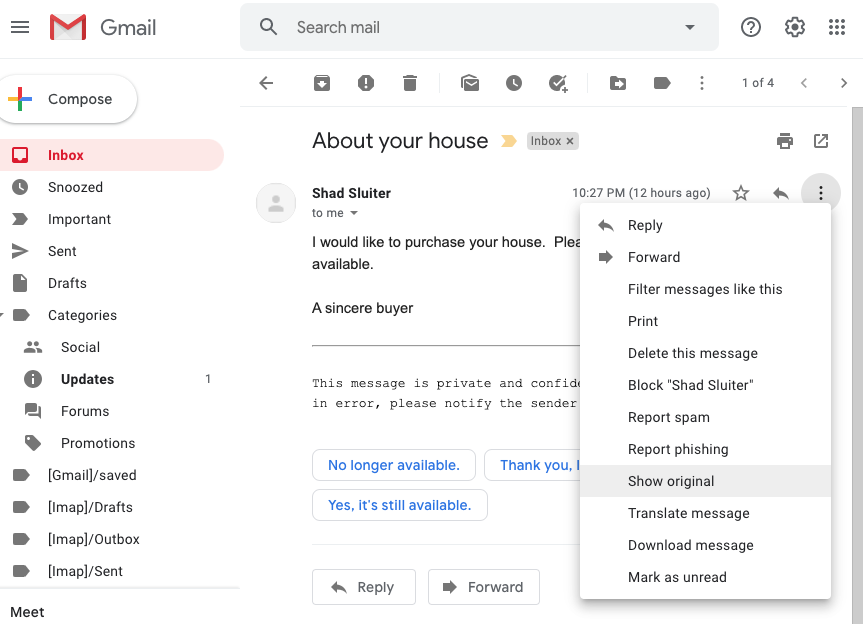
This is what the sent message looked like in Outlook.



This is what the received message looked like inside Gmail.



To show what the original text looks like choose the “Show Original” command from a setting menu.



The original content

Delivered-To: shadsluiter@gmail.com

Received: by 2002:a6b:d915:0:0:0:0:0 with SMTP id r21csp325820ioc;

Tue, 7 Jul 2020 22:27:51 -0700 (PDT)

X-Google-Smtp-Source: ABdhPJzBenPs22m7iFH7OlXgSRmDJen3fIFfo8jC2hDfufugnv7q7CE262mGkYF9NVDD3Ox3XWoY

X-Received: by 2002:a17:90b:488:: with SMTP id bh8mr8169248pjb.49.1594186071314;

Tue, 07 Jul 2020 22:27:51 -0700 (PDT)

ARC-Seal: i=1; a=rsa-sha256; t=1594186071; cv=none;

d=google.com; s=arc-20160816;

b=SlyXLsof/6reeaUcHXqUCDKglZ2Plq/9AM3b7oGwv0a9bkRMcna7nds4Vvfi6+IPx0

xng/a/HVf1qPSVyTUZpHZKQujFmIH53afwb4JckLq+GAxw35jxc6OA3beGGdlTxPgDcp

VmR2PrsscRhyE2ITpX/j255C645L9q5zLrcNJv1+ZzfBoM4Z275Lia65zwUBWvttCwTI

+VaD1R/eaiiAeGqBt4CzyMXbLOrkxjwLUKv1HRsYHyakYX5/eQ4UMsdJ4q9oR7kmti8R

xwa8ZR+APv6ftTayPMNob7h900VYYPw9cmQsC9dflr6P9ut8tVDv5/JVR8jh2f5CeL9J

Xq7g==

ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;

h=mime-version:content-language:accept-language:message-id:date

:thread-index:thread-topic:subject:to:from;

bh=58wOdAP7PWmZpCANTqdAlt7mOiutAz8PLSsTYtx9vkw=;

b=aUfih37MHovv35WxZZKpt3TY22X1W/pNDp2Y7qDnveP351Cl/f8DsgLvunWj1Ny7V7

dySftDY1U9u7n92nNmqmrsW7t4yRoFrloUsenJhNx5D03Xz9FOxp2Eu1OXNt0ZP1hwBB

tXN/+OIsS0FpshtkBM3XRsDEtQR/dC136ARMEMl/kPDHa9WH1n05SniupKe6TJ/P6kzX

YVORpvxBPaX8w9wa/jwXov6cNzbgabgu6gahZ0tWNBOFF/GnDxayydVfIfqUp2od15Lw

HpN3DrOGU2X9j6cMy9HcwSulrFgWMXJ4q37FK9ELjyGbKdhOdrFjVxdWM3ayG5vt/SUh

hqDQ==

ARC-Authentication-Results: i=1; mx.google.com;

spf=pass (google.com: domain of shad.sluiter@gcu.edu designates 205.220.162.148 as permitted sender) smtp.mailfrom=Shad.Sluiter@gcu.edu;

dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=gcu.edu

Return-Path: <Shad.Sluiter@gcu.edu>

Received: from mx0a-002bcc03.pphosted.com (mx0a-002bcc03.pphosted.com. [205.220.162.148])

by mx.google.com with ESMTPS id j8si16986463plk.311.2020.07.07.22.27.50

for <shadsluiter@gmail.com>

(version=TLS1\_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);

Tue, 07 Jul 2020 22:27:51 -0700 (PDT)

Received-SPF: pass (google.com: domain of shad.sluiter@gcu.edu designates 205.220.162.148 as permitted sender) client-ip=205.220.162.148;

Authentication-Results: mx.google.com;

spf=pass (google.com: domain of shad.sluiter@gcu.edu designates 205.220.162.148 as permitted sender) smtp.mailfrom=Shad.Sluiter@gcu.edu;

dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=gcu.edu

Received: from pps.filterd (m0196097.ppops.net [127.0.0.1]) by mx0a-002bcc03.pphosted.com (8.16.0.42/8.16.0.42) with SMTP id 0685IaXW012097 for <shadsluiter@gmail.com>; Tue, 7 Jul 2020 22:27:50 -0700

Received: from ppptagvs1001.gcu.edu (smtp02.gcu.edu [137.152.25.26]) by mx0a-002bcc03.pphosted.com with ESMTP id 322pdqc9sw-1 (version=TLSv1.2 cipher=ECDHE-RSA-AES256-GCM-SHA384 bits=256 verify=NOT) for <shadsluiter@gmail.com>; Tue, 07 Jul 2020 22:27:50 -0700

Received: from pps.filterd (PPPTAGVS1001.gcu.edu [127.0.0.1]) by PPPTAGVS1001.gcu.edu (8.16.0.42/8.16.0.42) with SMTP id 0683nYHS025135 for <shadsluiter@gmail.com>; Tue, 7 Jul 2020 22:27:49 -0700

Received: from pexhdbps1005.gcu.edu (PEXHDBPS1005.gcu.edu [10.254.53.112]) by PPPTAGVS1001.gcu.edu with ESMTP id 322qr47mf7-1 (version=TLSv1.2 cipher=AES128-SHA256 bits=128 verify=NOT) for <shadsluiter@gmail.com>; Tue, 07 Jul 2020 22:27:49 -0700

Received: from PEXHDBPS1006.gcu.edu (10.254.53.113) by PEXHDBPS1005.gcu.edu (10.254.53.112) with Microsoft SMTP Server (TLS) id 15.0.1497.2; Tue, 7 Jul 2020 22:27:49 -0700

Received: from PEXHDBPS1006.gcu.edu ([fe80::2159:81f:ba73:5bb5]) by PEXHDBPS1006.gcu.edu ([fe80::2159:81f:ba73:5bb5%25]) with mapi id 15.00.1497.006; Tue, 7 Jul 2020 22:27:49 -0700

From: Shad Sluiter <Shad.Sluiter@gcu.edu>

To: shad sluiter <shadsluiter@gmail.com>

Subject: About your house

Thread-Topic: About your house

Thread-Index: AQHWVOiEnVXWM7Uw5EWQNKDmCUu22w==

Date: Wed, 8 Jul 2020 05:27:48 +0000

Message-ID: <1C6FE75C-7FA9-4843-AA06-21108EAB6E60@gcu.edu>

Accept-Language: en-US

Content-Language: en-US

X-MS-Has-Attach:

X-MS-TNEF-Correlator:

x-ms-exchange-messagesentrepresentingtype: 1

x-ms-exchange-transport-fromentityheader: Hosted

x-originating-ip: [10.254.10.244]

Content-Type: multipart/alternative; boundary="\_000\_1C6FE75C7FA94843AA0621108EAB6E60gcuedu\_"

MIME-Version: 1.0

X-Proofpoint-Virus-Version: vendor=fsecure engine=2.50.10434:6.0.235,18.0.687 definitions=2020-07-08\_01:2020-07-08,2020-07-08 signatures=0

X-Proofpoint-Spam-Reason: safe

--\_000\_1C6FE75C7FA94843AA0621108EAB6E60gcuedu\_

Content-Type: text/plain; charset="utf-8"

Content-Transfer-Encoding: base64

SSB3b3VsZCBsaWtlIHRvIHB1cmNoYXNlIHlvdXIgaG91c2UuICBQbGVhc2UgY29udGFjdCBtZSB3

aGVuIHlvdSBhcmUgYXZhaWxhYmxlLg0KDQpBIHNpbmNlcmUgYnV5ZXINCg0KX19fX19fX19fX19f

X19fX19fX19fX19fX19fX19fX18NCg0KVGhpcyBtZXNzYWdlIGlzIHByaXZhdGUgYW5kIGNvbmZp

ZGVudGlhbC4gSWYgeW91IGhhdmUgcmVjZWl2ZWQgaXQgaW4gZXJyb3IsIHBsZWFzZSBub3RpZnkg

dGhlIHNlbmRlciBhbmQgcmVtb3ZlIGl0IGZyb20geW91ciBzeXN0ZW0uDQo=

--\_000\_1C6FE75C7FA94843AA0621108EAB6E60gcuedu\_

Content-Type: text/html; charset="utf-8"

Content-ID: <8ED129678A88FB4AB95053274F3E5622@gcu.edu>

Content-Transfer-Encoding: base64

PGh0bWwgeG1sbnM6bz0idXJuOnNjaGVtYXMtbWljcm9zb2Z0LWNvbTpvZmZpY2U6b2ZmaWNlIiB4

bWxuczp3PSJ1cm46c2NoZW1hcy1taWNyb3NvZnQtY29tOm9mZmljZTp3b3JkIiB4bWxuczptPSJo

dHRwOi8vc2NoZW1hcy5taWNyb3NvZnQuY29tL29mZmljZS8yMDA0LzEyL29tbWwiIHhtbG5zPSJo

dHRwOi8vd3d3LnczLm9yZy9UUi9SRUMtaHRtbDQwIj4NCjxoZWFkPg0KPG1ldGEgaHR0cC1lcXVp

dj0iQ29udGVudC1UeXBlIiBjb250ZW50PSJ0ZXh0L2h0bWw7IGNoYXJzZXQ9dXRmLTgiPg0KPG1l

dGEgbmFtZT0iR2VuZXJhdG9yIiBjb250ZW50PSJNaWNyb3NvZnQgV29yZCAxNSAoZmlsdGVyZWQg

bWVkaXVtKSI+DQo8c3R5bGU+PCEtLQ0KLyogRm9udCBEZWZpbml0aW9ucyAqLw0KQGZvbnQtZmFj

ZQ0KCXtmb250LWZhbWlseToiQ2FtYnJpYSBNYXRoIjsNCglwYW5vc2UtMToyIDQgNSAzIDUgNCA2

IDMgMiA0O30NCkBmb250LWZhY2UNCgl7Zm9udC1mYW1pbHk6Q2FsaWJyaTsNCglwYW5vc2UtMToy

IDE1IDUgMiAyIDIgNCAzIDIgNDt9DQovKiBTdHlsZSBEZWZpbml0aW9ucyAqLw0KcC5Nc29Ob3Jt

YWwsIGxpLk1zb05vcm1hbCwgZGl2Lk1zb05vcm1hbA0KCXttYXJnaW46MGluOw0KCW1hcmdpbi1i

b3R0b206LjAwMDFwdDsNCglmb250LXNpemU6MTIuMHB0Ow0KCWZvbnQtZmFtaWx5OiJDYWxpYnJp

IixzYW5zLXNlcmlmO30NCmE6bGluaywgc3Bhbi5Nc29IeXBlcmxpbmsNCgl7bXNvLXN0eWxlLXBy

aW9yaXR5Ojk5Ow0KCWNvbG9yOiMwNTYzQzE7DQoJdGV4dC1kZWNvcmF0aW9uOnVuZGVybGluZTt9

DQphOnZpc2l0ZWQsIHNwYW4uTXNvSHlwZXJsaW5rRm9sbG93ZWQNCgl7bXNvLXN0eWxlLXByaW9y

aXR5Ojk5Ow0KCWNvbG9yOiM5NTRGNzI7DQoJdGV4dC1kZWNvcmF0aW9uOnVuZGVybGluZTt9DQpz

cGFuLkVtYWlsU3R5bGUxNw0KCXttc28tc3R5bGUtdHlwZTpwZXJzb25hbC1jb21wb3NlOw0KCWZv

bnQtZmFtaWx5OiJDYWxpYnJpIixzYW5zLXNlcmlmOw0KCWNvbG9yOndpbmRvd3RleHQ7fQ0KLk1z

b0NocERlZmF1bHQNCgl7bXNvLXN0eWxlLXR5cGU6ZXhwb3J0LW9ubHk7DQoJZm9udC1mYW1pbHk6

IkNhbGlicmkiLHNhbnMtc2VyaWY7fQ0KQHBhZ2UgV29yZFNlY3Rpb24xDQoJe3NpemU6OC41aW4g

MTEuMGluOw0KCW1hcmdpbjoxLjBpbiAxLjBpbiAxLjBpbiAxLjBpbjt9DQpkaXYuV29yZFNlY3Rp

b24xDQoJe3BhZ2U6V29yZFNlY3Rpb24xO30NCi0tPjwvc3R5bGU+DQo8L2hlYWQ+DQo8Ym9keSBs

YW5nPSJFTi1VUyIgbGluaz0iIzA1NjNDMSIgdmxpbms9IiM5NTRGNzIiPg0KPGRpdiBjbGFzcz0i

V29yZFNlY3Rpb24xIj4NCjxwIGNsYXNzPSJNc29Ob3JtYWwiPjxzcGFuIHN0eWxlPSJmb250LXNp

emU6MTEuMHB0Ij5JIHdvdWxkIGxpa2UgdG8gcHVyY2hhc2UgeW91ciBob3VzZS4mbmJzcDsgUGxl

YXNlIGNvbnRhY3QgbWUgd2hlbiB5b3UgYXJlIGF2YWlsYWJsZS48bzpwPjwvbzpwPjwvc3Bhbj48

L3A+DQo8cCBjbGFzcz0iTXNvTm9ybWFsIj48c3BhbiBzdHlsZT0iZm9udC1zaXplOjExLjBwdCI+

PG86cD4mbmJzcDs8L286cD48L3NwYW4+PC9wPg0KPHAgY2xhc3M9Ik1zb05vcm1hbCI+PHNwYW4g

c3R5bGU9ImZvbnQtc2l6ZToxMS4wcHQiPkEgc2luY2VyZSBidXllcjxvOnA+PC9vOnA+PC9zcGFu

PjwvcD4NCjwvZGl2Pg0KPGJyPg0KPGhyPg0KPGZvbnQgZmFjZT0iQ291cmllciBOZXciIGNvbG9y

PSJCbGFjayIgc2l6ZT0iMiI+PGJyPg0KVGhpcyBtZXNzYWdlIGlzIHByaXZhdGUgYW5kIGNvbmZp

ZGVudGlhbC4gSWYgeW91IGhhdmUgcmVjZWl2ZWQgaXQgaW4gZXJyb3IsIHBsZWFzZSBub3RpZnkg

dGhlIHNlbmRlciBhbmQgcmVtb3ZlIGl0IGZyb20geW91ciBzeXN0ZW0uPGJyPg0KPC9mb250Pg0K

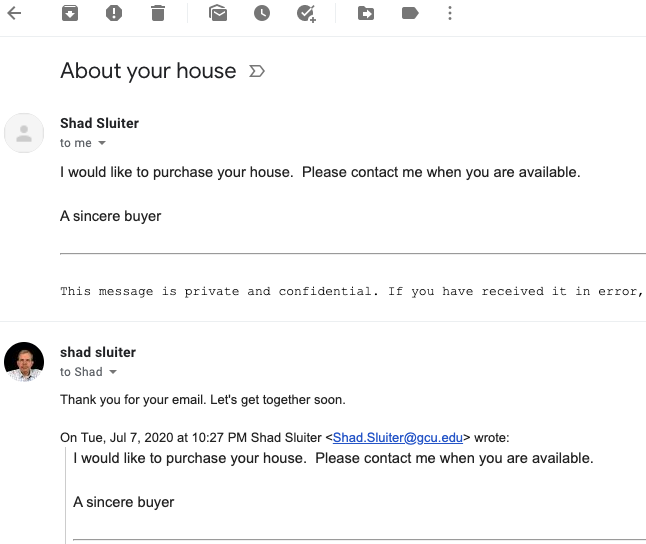
PC9ib2R5Pg0KPC9odG1sPg0K

--\_000\_1C6FE75C7FA94843AA0621108EAB6E60gcuedu\_--

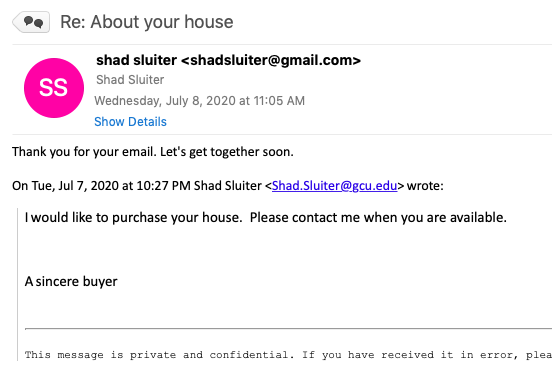
**The Reply:**

I replied to the university account from my Gmail account with a short message as shown.

**Gmail View:**



**Outlook View (University account that received the reply)**



Here are the email headers for the Google to GCU reply message.

Received: from PEXHDBPS1006.gcu.edu (10.254.53.113) by PEXHDBPS1006.gcu.edu

(10.254.53.113) with Microsoft SMTP Server (TLS) id 15.0.1497.2 via Mailbox

Transport; Wed, 8 Jul 2020 11:05:04 -0700

Received: from PPPTAGVS2001.gcu.edu (172.18.2.245) by PEXHDBPS1006.gcu.edu

(10.254.53.113) with Microsoft SMTP Server (TLS) id 15.0.1497.2; Wed, 8 Jul

2020 11:05:04 -0700

Received: from pps.filterd (PPPTAGVS2001.gcu.edu [127.0.0.1])

by PPPTAGVS2001.gcu.edu (8.16.0.42/8.16.0.42) with SMTP id 068I0LRo030474

for <Shad.Sluiter@gcu.edu>; Wed, 8 Jul 2020 11:05:04 -0700

Authentication-Results: gcu.edu;

spf=softfail smtp.mailfrom=shadsluiter@gmail.com;

dkim=pass header.s=20161025 header.d=gmail.com;

dmarc=pass header.from=gmail.com

Received: from mx0a-002bcc03.pphosted.com (mx0a-002bcc03.pphosted.com [205.220.162.148])

by PPPTAGVS2001.gcu.edu with ESMTP id 322qr2mufn-1

(version=TLSv1.2 cipher=ECDHE-RSA-AES256-GCM-SHA384 bits=256 verify=NOT)

for <Shad.Sluiter@gcu.edu>; Wed, 08 Jul 2020 11:05:04 -0700

Received: from pps.filterd (m0196097.ppops.net [127.0.0.1])

by mx0a-002bcc03.pphosted.com (8.16.0.42/8.16.0.42) with SMTP id 068HxZe3016558

for <Shad.Sluiter@gcu.edu>; Wed, 8 Jul 2020 11:05:03 -0700

Authentication-Results: ppops.net;

spf=pass smtp.mailfrom=shadsluiter@gmail.com

Received: from mail-il1-f172.google.com (mail-il1-f172.google.com [209.85.166.172])

by mx0a-002bcc03.pphosted.com with ESMTP id 325k1gr0px-1

(version=TLSv1.2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128 verify=NOT)

for <Shad.Sluiter@gcu.edu>; Wed, 08 Jul 2020 11:05:03 -0700

Received: by mail-il1-f172.google.com with SMTP id o3so22477253ilo.12

for <Shad.Sluiter@gcu.edu>; Wed, 08 Jul 2020 11:05:03 -0700 (PDT)

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

d=gmail.com; s=20161025;

h=mime-version:references:in-reply-to:from:date:message-id:subject:to;

bh=LDPK46s7kgM8Wy/5aybK/eJJu/uVZhvZFeZGgyO1AL8=;

b=k8itwfm2VGDhQVbRU4N6KHC2JVBQyG93I368NQ7huDmdqhizroiZc4vHpf5Lb+joh2

GkG3OGP8K4Mix75GePxKIT7wivtKK9lf296ss9CUKUbgtY1AFS4nTpc6O8ncknsJYXTd

R774gY7Xcv0MdD6b651zKXkbwq2ODVQ9TU0TzcU0nvK18qZ1ZoR/zTX+G1B64wEb6B3I

P1MCuIrFFXweZKvs6xsUAu//LOyzLjIaMceQumBytVAZIwde+PsWE26jCkFOxF8TftHj

zMMtDN9v72IZvVtKmlCLm74CuNHMt2AHiVKPBlBbCOVVx2tvU65is3SYarmrGHD0wi44

c9dg==

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

d=1e100.net; s=20161025;

h=x-gm-message-state:mime-version:references:in-reply-to:from:date

:message-id:subject:to;

bh=LDPK46s7kgM8Wy/5aybK/eJJu/uVZhvZFeZGgyO1AL8=;

b=Fbl7Y2a8ftma08CZVDbe1+FYeltLUYldEF4lbMjcftDoC9+gJ1mX6+WSSQhoEIMXKh

oBRHO61dspYyZe6tmAaHFdrV9PNldxsZ3AXM16qJ6r1rBygPR60ntlSZ3wy5v9lkr7qd

ZT01t95t+Dro2YvYJgjXSvhkGvL2MhLwzDBpHwFgKrDH4qxktjpAIcuFA3vUR8kFEORg

KHCcq7hN3mJInPKDomYw5C0WaPhCycGHAKkeTStBgyure+m27URUv9npU+kNd99y32Ct

S/fe1ha7aJsy1O3gryqOuv9xNcS76fNbfqATxBAF1Qm2jzT4IyXvQmDpGS8KHPGJoHku

Y7MQ==

X-Gm-Message-State: AOAM531BKS7d2kirhlRL2etnFV0Fy/U8tE07QuId5Fqvp4WjtXsVPYw/

9MQRUTm/Cn+BUlEgcGTBHmmZ2HQPVNuQ++07qoIOgEKf

X-Google-Smtp-Source: ABdhPJwiLw3jSZMARxB3Xyy6REELZzkwzboXqLADhm56I9luDsveBXo3Q70ys+i+V/Md6MQs6yuFr9+Pdv3KYUZ0E+E=

X-Received: by 2002:a92:d84d:: with SMTP id h13mr45091136ilq.102.1594231502148;

Wed, 08 Jul 2020 11:05:02 -0700 (PDT)

MIME-Version: 1.0

References: <1C6FE75C-7FA9-4843-AA06-21108EAB6E60@gcu.edu>

In-Reply-To: <1C6FE75C-7FA9-4843-AA06-21108EAB6E60@gcu.edu>

From: shad sluiter <shadsluiter@gmail.com>

Date: Wed, 8 Jul 2020 11:04:50 -0700

Message-ID: <CANarGCR6i2NMwG71YbheW97NocK\_iM3JFxXBV3fU48K9B9okgw@mail.gmail.com>

Subject: Re: About your house

To: Shad Sluiter <Shad.Sluiter@gcu.edu>

X-CLX-Shades: Deliver

X-CLX-Response: 1TFkXGxoaHxEKTHoXGRsZEQpZRBd6fxl/Z1xof34acxEKWFgXYV54cmJBYUg dR2IRCnhOF2NTY2t7E1h+Gl9eEQp5TBdjW3tpBVlgWhhzZxEKeUMXZh1ya21NXGAeeV4RCkNIFx kYEQpDWRcHGxgZEQpDSRcaBBoaGhEKWU0Xbk9GQ1xPWBEKX1kXGB4cEQpfTRdnZnIRCllJFxpxG

hAadwYYGBxxGRwZEBp3BhgaBhoRClleF2hueREKSUYXTUlfdRh1QkVZXk9OEQpDThdsQB91chta XElueR1dB3gbS3p1H2JvaXsbSBhHU2VtSxEKWFwXHwQaBBgaHQUbGgQbGhoEHhIEGxMQGx4aHxo RCl5ZF31lHBNbEQpNXBcdEQpMWhdsa2tNaxEKTEYXYmtrEQpCTxdtbVJNa2xbb0hsbREKQ1oXGB

oTBBIfBBscHAQbHRgRCkJeFxsRCkJcFxoRCkJFF2kfWB9TQmdIXG5eEQpCThdjU2NrexNYfhpfX hEKQkwXYV54cmJBYUgdR2IRCkJsF2RvW0FJWlAfSGJCEQpCQBdhbUNPblp8XF5SQREKQlgXZBxn b0QSaRIFblIRCk1eFxsRClpYFxgRCllLFxMaExwRCnBoF2dBR0cZRVpafQFLEBkaEQpwaBdrYEx

pa0RacEhYXBAZGhEKcGgXekxnTFJeT2IYT24QHBwRCnBoF2FEeF1ZUgF9YF4aEBkaEQpwaBdjf3 BEYRp8ThlzARAZGhEKcGwXbUd7R1pFZBgYeHkQGRoRCnBMF2deb29aYR1OTFpTEBkaEQptfhcbE QpYTRdLESA=

X-Proofpoint-Virus-Version: vendor=fsecure engine=2.50.10434:6.0.235,18.0.687

definitions=2020-07-08\_16:2020-07-08,2020-07-08 signatures=0

X-Proofpoint-Spam-Reason: safe

Return-Path: shadsluiter@gmail.com

X-MS-Exchange-Organization-Network-Message-Id: d2a962a9-7d92-4f63-f2c5-08d8236970d8

X-MS-Exchange-Organization-AVStamp-Enterprise: 1.0

X-MS-Exchange-Organization-AuthSource: PEXHDBPS1006.gcu.edu

X-MS-Exchange-Organization-AuthAs: Anonymous

Content-type: multipart/alternative;

boundary="B\_3677051251\_1966378133"

> This message is in MIME format. Since your mail reader does not understand

this format, some or all of this message may not be legible.

--B\_3677051251\_1966378133

Content-type: text/plain;

charset="UTF-8"

Content-transfer-encoding: 7bit

Thank you for your email. Let's get together soon.

On Tue, Jul 7, 2020 at 10:27 PM Shad Sluiter <Shad.Sluiter@gcu.edu> wrote:

I would like to purchase your house. Please contact me when you are available.

A sincere buyer

This message is private and confidential. If you have received it in error, please notify the sender and remove it from your system.--B\_3677051251\_1966378133Content-type: text/html; charset="UTF-8"Content-transfer-encoding: quoted-printable<html>

<head>

<meta http-equiv=3D"Content-Type" content=3D"text/html; charset=3Dutf-8">

</head>

<body>

<div dir=3D"ltr">Thank you for your email. Let's get together soon.</div>

<br>

<div class=3D"gmail\_quote">

<div dir=3D"ltr" class=3D"gmail\_attr">On Tue, Jul 7, 2020 at 10:27 PM Shad Slui=

ter &lt;<a href=3D"mailto:Shad.Sluiter@gcu.edu">Shad.Sluiter@gcu.edu</a>&gt; w=

rote:<br>

</div>

<blockquote class=3D"gmail\_quote" style=3D"margin:0px 0px 0.8ex;border-left=

:1px solid rgb(204,204,204);padding-left:1ex">

<div lang=3D"EN-US">

<div class=3D"gmail-m\_-5750473745824511718WordSection1">

<p class=3D"MsoNormal"><span style=3D"font-size:11pt">I would like to purchase =

your house.&nbsp; Please contact me when you are available.<u></u><u></u></s=

pan></p>

<p class=3D"MsoNormal"><span style=3D"font-size:11pt"><u></u>&nbsp;<u></u></spa=

n></p>

<p class=3D"MsoNormal"><span style=3D"font-size:11pt">A sincere buyer<u></u><u>=

</u></span></p>

</div>

<br>

<hr>

<font face=3D"Courier New" color=3D"Black" size=3D"2"><br>

This message is private and confidential. If you have received it in error,=

please notify the sender and remove it from your system.<br>

</font></div>

</blockquote>

</div>

</body>

</html>

--B\_3677051251\_1966378133--

## Part 2 - Understanding Email Headers

The following is a brief explanation of some of the header sections of each email message. The tools and protocols used in the examples above are typical of most email communication online. However, there are likely differences in systems outside of Microsoft Exchange and Gmail’s servers.

From

* The return address of the sender. The user can override the default settings. This is as unreliable as the actual return address a sender can affix to a post office envelope.

Date

* Time stamp provided by the email client.

To

* Destination address.

Delivery Date

* Time stamp created by the mail transfer service.

Thread-Topic:

* Allows the email client to organize related emails into a single view.

Received

* These lines are generated by the email server and not the user composing the message. Read these lines from the bottom to top to see a reverse chronological order of the email transfer process. There is a variety of formats used by different email servers.

Message-id

* A unique string assigned by the mail system when the message is first created. These can be easily forged.

SPF (Sender Policy Framework)

* SPF allows the receiving mail server to check during mail delivery that mail claiming to come from a specific domain is submitted by an IP address authorized by that domain's administrators. This prevents a sender using Gmail’s servers (domain = google.com) from assigning a fake return address. The list of authorized sending hosts and IP addresses for a domain is published in the [DNS](https://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions) records for that domain.

ARC-Seal

ARC-Message-Signature

ARC-Authentication-Results

* These three ARC entries show the results of an authentication chain. An email message may pass through multiple servers before arriving at the final destination. If email server “A” sends to server “B” who forwards the message on to server “C”, then “C” must have a way to ensure that both “A” and “B” did not modify the message. At each point in the chain of transmission a hashed value of the email message is recorded, ensuring that the contents of the message have not be modified in an unauthorized manner. The ARC messages you see in the example below include hash results from the algorithm rsa-sha256.

DMARC

* DMARC (Domain-based Message Authentication, Reporting, and Conformance) is an email authentication protocol. It is designed to give email domain owners the ability to protect their domain from email spoofing and phishing.
* DMARC allows a sender's domain to indicate that their emails are protected by one or both of two commonly used authentication methods, SPF or DKIM. The example emails shown below indicate that Google is using SPF and GCU is using DKIM.
* You will notice that the status of this DMARC record is p = “none,” meaning that there are no restrictions on this particular domain, gcu.edu.

MX

* A mail exchanger record (MX record) specifies the mail server responsible for accepting email messages on behalf of a domain name. It is a resource record in the Domain Name System (DNS). It is possible to configure several MX records, typically pointing to an array of mail servers for load balancing and redundancy.

Content-Type

* The format of the message, such as plain text or html.
* Many Content-Types which could usefully be transported via email are represented, in their "natural" format, as 8-bit character or binary data. Such data cannot be transmitted over some transport protocols. For example, RFC 821 restricts mail messages to 7-bit US-ASCII data with 1000 character lines.
* It is necessary, therefore, to define a standard mechanism for re-encoding such data into a 7-bit short-line format.

Mime-Version

* Multipurpose Internet Mail Extensions (MIME) is an Internet standard that extends the character set other than plain text ASCII of email. This allows an email message to properly encode all types of attachments such as: jpge, gif, mp3, mp4, Word, Excel, PDF and others.

Message Body

* This is the actual content of the email itself, written by the sender. You will notice that in the first email, there is no message body. Instead there is a large section of encoded text. Although the subject line is in plain text, the body of the email is encrypted. The reply message is not encrypted.

X-Proofpoint-Virus-Version

X-Proofpoint-Spam-Reason

X-CLX-Shades:

* These lines are results of a spam filter and virus checking service. ProofPoint is used for granular email filtering controls spam, bulk "graymail," and other unwanted email.

pphosted.com

* This is the domain name of the email server at Proofpoint, a third party email spam filtering company. The second email was routed through Proofpoint before being delivered to GCU. Their analysis of the likelihood of spam of the message is recorded in the headers.

## Part 3: Analyze the Headers of an email Message

Based on the information from Parts 1 and 2, complete the following:

1. Who sent this email message?
   1. The email was sent by [Shad.Slutier@gcu.edu](mailto:Shad.Slutier@gcu.edu). It is clear that this message was not actually sent by professor Sluiter, but that the original sender wanted to hide the actual sender of the message by manipulating the encoded message before sending it. This message was able to pass through multiple filters because GCU’s filters recognized it as a GCU email. I found this information in the original message text provided:

From: Shad Sluiter <Shad.Sluiter@gcu.edu>

To: shad sluiter <shadsluiter@gmail.com>

1. Who received it?
   1. The email was received by [shadslutier@gmail.com](mailto:shadslutier@gmail.com). I found this information in the original message text provided:

From: Shad Sluiter <Shad.Sluiter@gcu.edu>

To: shad sluiter [shadsluiter@gmail.com](mailto:shadsluiter@gmail.com)

1. How much time elapsed between the moment the sender pushed the “send” button, and when it was delivered to the recipient?
   1. Received: Tue, 7 Jul 2020 22:27:51 -0700 (PDT)
   2. Sent: Wed, 8 Jul 2020 05:27:48 +0000
   3. According to the original text that is provided at the beginning of the worksheet, the message took 7 hours to pass through the filters.
2. What MIME version is this email? What versions of MIME encoding exist?
   1. According to the text, there is a line that states, “MIME-Version: 1.0”
   2. There are multiple versions of MIME, but most email services only read MIME 1.0. The text also notes that the email may not be the correct MIME format, which should raise a red flag. This could mean that the encoding of the email has been altered for the use of the spammer.
3. About what percentage of this email text (in number of characters) is actually the body message?
   1. Body message: 227 characters
   2. Entire email: 6949
   3. Percentage of message that is body text: ~3.266%
4. What is an ARC-Seal, ARC-Message-Signature, and ARC-Authentication-Results?
   1. ARC-Seal: an instance number, DKIM signature to track past headers in the conversation and track security and changes of past messages in the correspondence. The purpose of ARC-Seal is to ensure that messages are tracked through the email system and are kept unchanged. The email may still send through the email providers system filters, but the user is able to view if changes are made.
   2. ARC-Message-Signature: an instance number followed by a DKIM signature that does not include the ARC-Seal headers. This signature tracks the changes made to the encoding of a message.
   3. ARC-Authentication-Results: an instance number followed by the SPF, DKIM, and the DMAIC validation. This step helps to track where the email has been and what filters it has passed through. Using DKIM and DMAIC, the email can pass through domain-specific filters that automatically filter out emails that are sent by unwanted senders. As an example, some secure organizations only allow for emails to be received form senders within the organization. DKIM and DMAIC allow for this functionality.
5. How is ARC related to rsa-sha256?
   1. The code, “rsa-sha256” refers to the ARC-Seal of the message. Within correspondences and conversation over email, this code should not change. If the code does change throughout the email conversation, the email may have been altered in a reply. Furthermore, this code identifies how the email has passed through different filters to reach its destination.