Southern New Hampshire University

# ISE 640 Module Three Assignment Worksheet Guidelines and Rubric
## Email Headers

Email headers provide important and valuable evidence. Email headers contain information not typically seen in a standard email, such as the source and destination of the IP address.

To complete this assignment, do the following:

1. Review the email, including headers, at the end of this document.
2. Answer the questions below.
3. Submit the completed Module Three Worksheet document.

Be sure to identify and describe the important pieces of evidence as directed in the questions provided.

**Answer the questions below:**

1. Who sent the email? Provide the name and email address. Why is this information important?

2. What is this IP address: 98.138.91.140? What does it represent? Why is this information important?

3. Identify the date and time the email was sent. Why is this information significant?

4. Identify the subject and body of the email. Why is this information important? Can you identify any suspicious or nefarious details?

5. What is the email address of the recipient? Why is this important evidence?

**Email**

```
Delivered-To: pbeddoe@gmail.com
Received: by 10.37.208.3 with SMTP id h3csp684694ybg;
        Sun, 24 Apr 2016 17:18:10 -0700 (PDT)
X-Received: by 10.107.2.70 with SMTP id 67mr15924779ioc.70.1461543490170;
        Sun, 24 Apr 2016 17:18:10 -0700 (PDT)
Return-Path: <dsmith@yahoo.com>
Received: from nm10-vm3.bullet.mail.ne1.yahoo.com (nm10-vm3.bullet.mail.ne1.yahoo.com. [98.138.91.140])
        by mx.google.com with ESMTPS id d42si20586415ioj.98.2016.04.24.17.18.09
        for <pbeddoe@gmail.com>
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
        Sun, 24 Apr 2016 17:18:10 -0700 (PDT)
Received-SPF: pass (google.com: domain of dsmith@yahoo.com designates 98.138.91.140 as permitted sender) client-
ip=98.138.91.140;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@yahoo.com;
       spf=pass (google.com: domain of dsmith@yahoo.com designates 98.138.91.140 as permitted sender)
smtp.mailfrom=dsmith@yahoo.com;
       dmarc=pass (p=REJECT dis=NONE) header.from=yahoo.com
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=yahoo.com; s=s2048; t=1461543489;
bh=1SRRIOY0Bz6C1j4m2i5gyIK96fLdKxHQRmzXxaDJ1TQ=; h=Date:From:Reply-To:To:Subject:References:From:Subject;
b=KqCQ8kZOA8TmBU54PvotdTtQwL/wuNzHPQ/r4Hbkl/U6ArimxubQWG0dbegBUAyDQWq4DTYCMai0VQB8FE3SKiKrXMJlWenMIWxrsQAp3lXEVr3YLxO04
K0cmhfpVBRs2MdEDIVYPtlE+8q75HbxHAr6a0G7gpILhdFztDGX47vTRgShhy+VWZAXNRsnoY6Zm0vQPM4GKQzo6uKUDhUnx48qstzZbUFFA49QFjTiLduD
DjYVvpKtromcu8pZ5HcAgF6QoXR+Nxme5c3Nht0KV8Uo21uS+h9/pcK3ToPBKDL+8OceT0t7er2UtleSa0bJAxUcW2f3YB39Vv4usIidxA==
Received: from [98.138.226.176] by nm10.bullet.mail.ne1.yahoo.com with NNFMP; 25 Apr 2016 00:18:09 -0000
Received: from [98.138.89.163] by tm11.bullet.mail.ne1.yahoo.com with NNFMP; 25 Apr 2016 00:18:09 -0000
Received: from [127.0.0.1] by omp1019.mail.ne1.yahoo.com with NNFMP; 25 Apr 2016 00:18:09 -0000
X-Yahoo-Newman-Property: ymail-3
X-Yahoo-Newman-Id: 564037.67553.bm@omp1019.mail.ne1.yahoo.com
X-YMail-OSG: s6c0BTYVM1niM3d.xvb7rmLBgStqvdGtAIZc9UJ090.Q.FafBuC8M1WZbUClDjD
 GcIBrHSq65NfxpW9cYX49d8fCmACFqA7C.lykcMvfiZgv7UUJW9v1TaGcDYcAM.yoo8k7oGBTBdJ
 .dNv92bigojeC7njhX5NlTTpeo_TI02_jyeM_E19wLzJErm3Y83vX22jRxp9Y78U0jpmFLnYQvZ1
 nknaui34uiVk04Xwc_zEopgE16smEGrMUYMjNdnHXPkNM5pZIrBNQZ7FQKyDfLs1_ZPPOe60SMcL
 IQ81gnnxdDOckGqLSZwoePaaqgPLufvCnNhxJ7AjydyKWma4QeZ8GX8SNVxjC9QKhW0o0FDyvjF4
 cwRXROcEsl3NFJ3rHW83nlfhahNGXv_D2.0ybEP.wKRSVV6LtrV2uHOYpd97vBvwlcwpv6NEaNtS
 Nc82xZ9Yvz6wFb8C05cWhfAgKS1JYicNmLSNSGXyTNtAOCHsuEBaL6Wm31Ir590tXrQsD9wdYkN4
 PnMi.eFMjQXMgd8A9.S1yjlr5JFhB_O0HFBoCa1vhdA--
Received: by 98.138.101.166; Mon, 25 Apr 2016 00:18:09 +0000
Date: Mon, 25 Apr 2016 00:18:08 +0000 (UTC)
From: "Denise Smith" <dsmith@yahoo.com>
Reply-To: "Denise Smith" <dsmith@yahoo.com>
To: "pbeddoe@gmail.com" <pbeddoe@gmail.com>
Message-ID: <1536143509.1086879.1461543488808.JavaMail.yahoo@mail.yahoo.com>
```

```
Subject: Payment Details
MIME-Version: 1.0
Content-Type: multipart/alternative;
        boundary="----=_Part_1086878_2084986636.1461543488806"
References: <1536143509.1086879.1461543488808.JavaMail.yahoo.ref@mail.yahoo.com>
Content-Length: 1198

------=_Part_1086878_2084986636.1461543488806
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: quoted-printable

Thank you for sending the money. =C2=A0As promised here are 2,500 credit ca=
rd numbers attached to this email. =C2=A0When I receive the final payment f=
rom you I will send the reaming 2,500. =C2=A0Talk to you soon, pleasure doi=
ng business with you.
Denise
------=_Part_1086878_2084986636.1461543488806
Content-Type: text/html; charset=UTF-8
Content-Transfer-Encoding: 7bit

<html><head></head><body><div style="color:#000; background-color:#fff; font-family:HelveticaNeue, Helvetica Neue,
Helvetica, Arial, Lucida Grande, sans-serif;font-size:12px"><div id="yui_3_16_0_ym19_1_1461543337762_2717"
dir="ltr">Thank you for sending the money. &nbsp;As promised here are 2,500 credit card numbers attached to this email.
&nbsp;When I receive the final payment from you I will send the reaming 2,500. &nbsp;Talk to you soon, pleasure doing
business with you.</div><div id="yui_3_16_0_ym19_1_1461543337762_2717" dir="ltr"><br></div><div
id="yui_3_16_0_ym19_1_1461543337762_2717" dir="ltr">Denise</div></div></body></html>
------=_Part_1086878_2084986636.1461543488806--
```

Southern New Hampshire University

| Question Number | Minimal or No Errors (100%) | Significant Errors (75%) | Not Evident (0%) | Value |
|---|---|---|---|---|
| **1** | Identifies the sender of the email and why it is important | Identifies the sender of the email but does not identify why this is important, or answer is illogical or incorrect | Does not answer the question | 15 |
| **2** | Identifies the source of the given IP address and why it is important | Identifies the source of the given IP address but does not identify why it is important, or answer is illogical or incorrect | Does not answer the question | 20 |
| **3** | Identifies the date and time the email was sent and why the information is significant | Identifies the date and time the email was sent but not why it is significant, or explanation is illogical | Does not answer the question | 20 |
| **4** | Identifies the content of the body of the email and possible nefarious intentions | Identifies the content of the body of the email but does not make a connection with the content and possible nefarious intentions | Does not answer the question | 25 |
| **5** | Identifies the recipient of the email and why it is important | Identifies the recipient of the email but does not identify why this is important, or answer is illogical or incorrect | Does not answer the question | 20 |
| | | | **Total** | **100%** |