**School of Computing**
**IT8003 Digital Forensics and Investigation**

# Practical 2B: Email

## Introduction

In Digital Forensic analyzing on different artifacts and understand certain user behavior through analysis of the device belonging to the subject is crucial. Such as web browsing history we can tell what the subject searched during the period and interest. Another element to digital forensic analysis or investigation is Email communication, this will allow the forensic examiner to have greater insight of the subject as to who he/she has communicated with and parties involved in the matter. As well as what has the subject sent other personal email address or external parties.

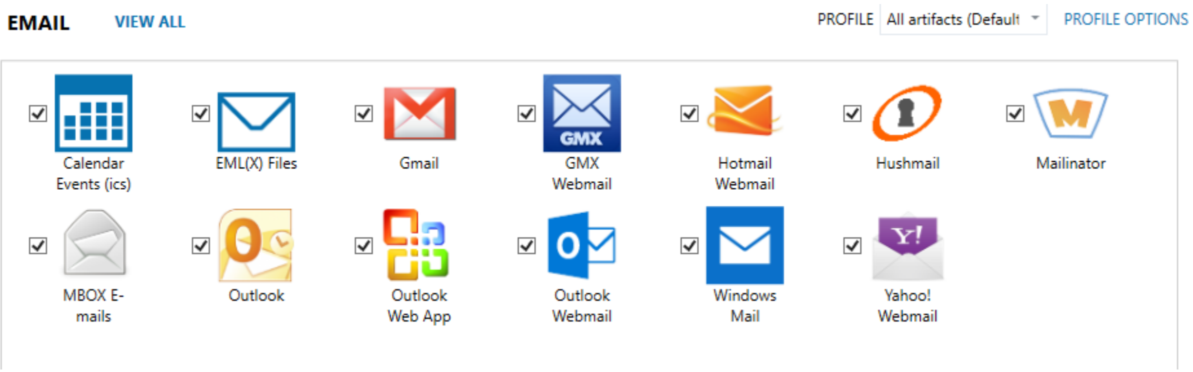
## Learning Objectives

In this lesson, students will take part in lectures, instructor led exercises, and student practical exercises to recover emails and email attachments from mail clients supported by Magnet AXIOM. At the conclusion of this lesson, students will be able to identify, discuss, and utilize Magnet AXIOM to review, sort and filter and report email and email attachments in of a successful investigation.

## Email Category

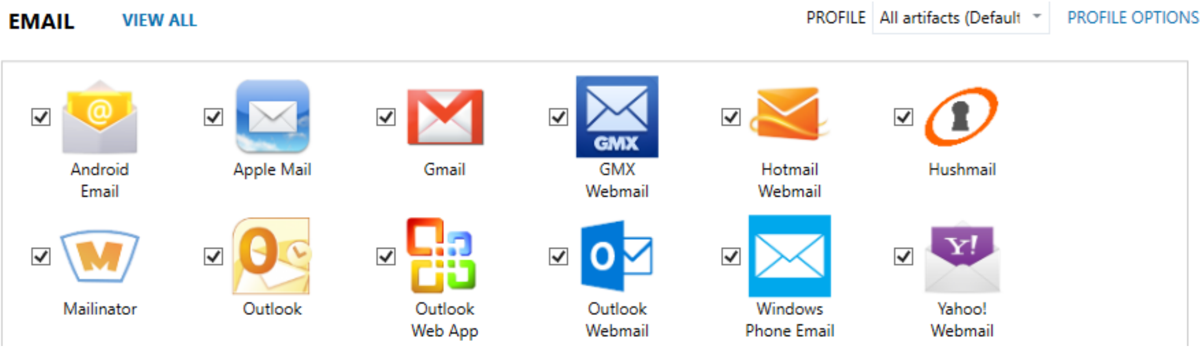
AXIOM Process will search for and categorize a variety of types of email into the Email artifact category. A screenshot of the choices for OS X / Windows is shown below. Email Options for mobile devices will vary somewhat. See the Artifact Reference Guide for a comprehensive list. It should be noted that AXIOM supports searching of both traditional email client artifacts (POP, IMAP protocols, etc.) and those from web-based email. This is useful since a user may access the same email account differently on different computers or devices.

Note: That the contents of compound mail structures such as found in Microsoft Outlook will also be parsed. This will include Appointments, Contacts, Journals, Notes and Tasks.



☑ Calendar Events (ics)
☑ EML(X) Files
☑ Gmail
☑ GMX Webmail
☑ Hotmail Webmail
☑ Hushmail
☑ Mailinator
☑ MBOX E-mails
☑ Outlook
☑ Outlook Web App
☑ Outlook Webmail
☑ Windows Mail
☑ Yahoo! Webmail

Figure 3-4-1: Supported Computer Email Artifacts In Magnet Axiom Process



EMAIL VIEW ALL

PROFILE All artifacts (Default PROFILE OPTIONS

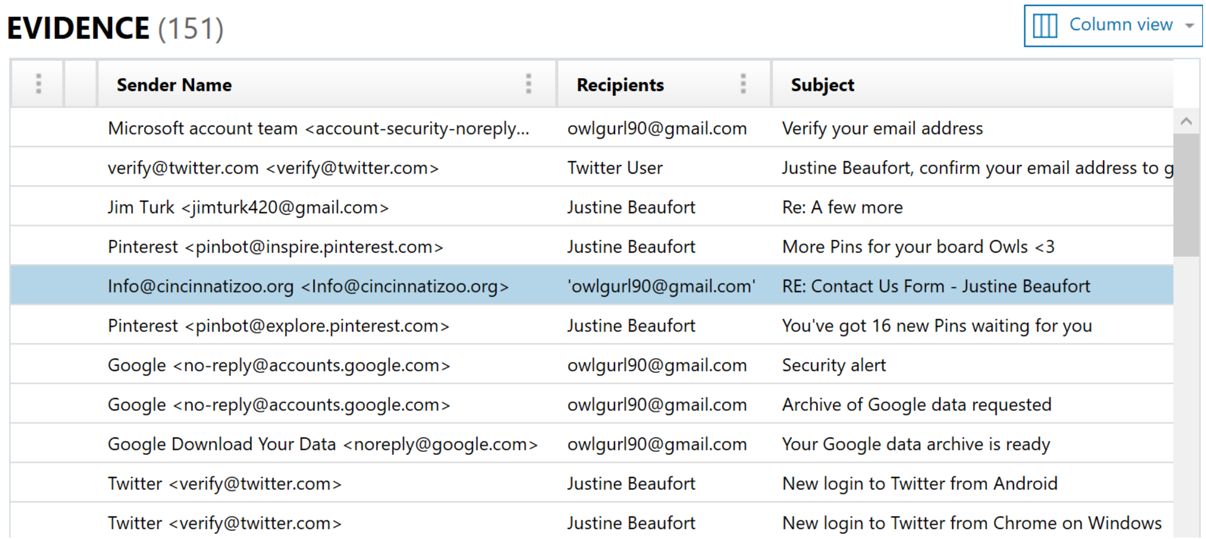
☑ Android Email ☑ Apple Mail ☑ Gmail ☑ GMX Webmail ☑ Hotmail Webmail ☑ Hushmail

☑ Mailinator ☑ Outlook ☑ Outlook Web App ☑ Outlook Webmail ☑ Windows Phone Email ☑ Yahoo! Webmail

Figure 3-4-2: Supported Mobile Email Artifacts In Magnet Axiom Process

## Email Content

In the Column View of the Evidence Pane, column data for selected email will be displayed. The columns shown will be email specific, such as To, From, Subject, Carbon Copy, etc. The exact columns shown will differ depending on the email client being displayed.

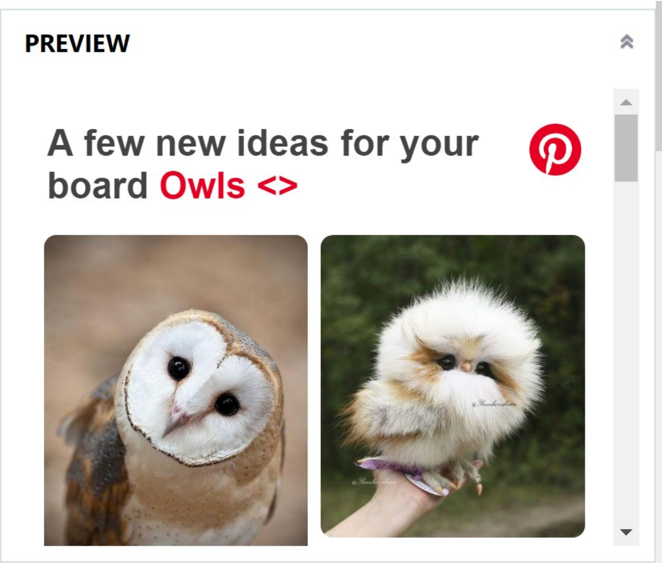


**EVIDENCE** (151)

| Sender Name | Recipients | Subject |
|---|---|---|
| Microsoft account team <account-security-noreply... | owlgurl90@gmail.com | Verify your email address |
| verify@twitter.com <verify@twitter.com> | Twitter User | Justine Beaufort, confirm your email address to g |
| Jim Turk <jimturk420@gmail.com> | Justine Beaufort | Re: A few more |
| Pinterest <pinbot@inspire.pinterest.com> | Justine Beaufort | More Pins for your board Owls <3 |
| Info@cincinnatizoo.org <Info@cincinnatizoo.org> | 'owlgurl90@gmail.com' | RE: Contact Us Form - Justine Beaufort |
| Pinterest <pinbot@explore.pinterest.com> | Justine Beaufort | You've got 16 new Pins waiting for you |
| Google <no-reply@accounts.google.com> | owlgurl90@gmail.com | Security alert |
| Google <no-reply@accounts.google.com> | owlgurl90@gmail.com | Archive of Google data requested |
| Google Download Your Data <noreply@google.com> | owlgurl90@gmail.com | Your Google data archive is ready |
| Twitter <verify@twitter.com> | Justine Beaufort | New login to Twitter from Android |
| Twitter <verify@twitter.com> | Justine Beaufort | New login to Twitter from Chrome on Windows |

Figure 3-4-3: Email Column View

The Contents Pane provides additional information for the Examiner. The Preview Card in this pane will provide a rendered view of the email content if available; this would be the case for mail with HTML content. Note that not all HTML content will render in an easily readable fashion in the Preview Card.

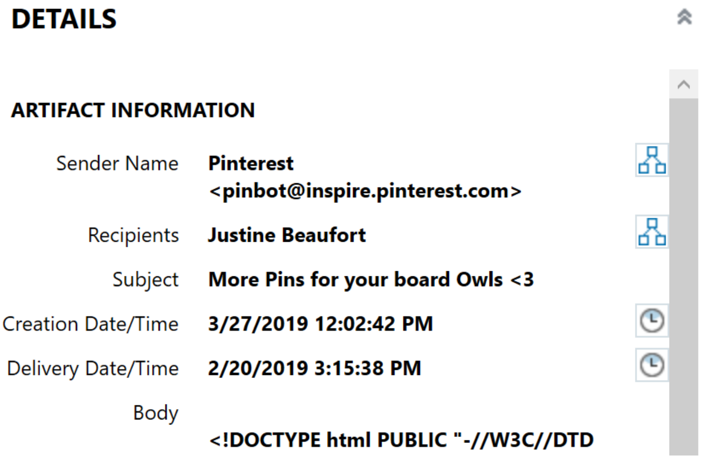


**PREVIEW**

A few new ideas for your board Owls <>

Figure 3-4-4: Email Preview

The Details card will contain some of the email-specific column data as well as normal Source and Location information.



**DETAILS**

**ARTIFACT INFORMATION**

Sender Name **Pinterest <pinbot@inspire.pinterest.com>**

Recipients **Justine Beaufort**

Subject **More Pins for your board Owls <3**

Creation Date/Time **3/27/2019 12:02:42 PM**

Delivery Date/Time **2/20/2019 3:15:38 PM**

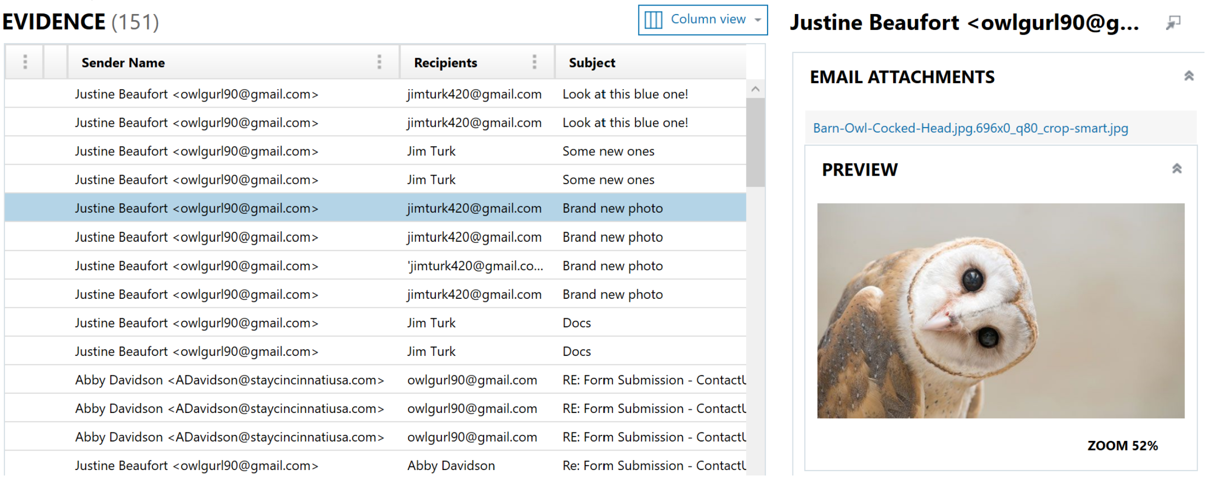
Body

**<!DOCTYPE html PUBLIC "-//W3C//DTD**

Figure 3-4-5: Email Details

## Email Attachments

If an artifact Email has a file attachment, it will be noted in the Attachments column in the Column View of the Evidence Pane. The file name of the attachment will be listed in the column; this information will also appear in the Details Card of the Content Pane. The attached file will normally not be viewable in the Preview Card; however a hyperlink to the file will appear instead and the content of the email itself will show in the preview pane. Email clients have varying methods and locations for storing file attachments. If the case being viewed has been built from an image file of an entire logical or physical drive, the attached files should be available in their normal artifact categories within AXIOM Examine – Documents, Pictures, Videos, etc.



**EVIDENCE** (151)

| Sender Name | Recipients | Subject |
|---|---|---|
| Justine Beaufort <owlgurl90@gmail.com> | jimturk420@gmail.com | Look at this blue one! |
| Justine Beaufort <owlgurl90@gmail.com> | jimturk420@gmail.com | Look at this blue one! |
| Justine Beaufort <owlgurl90@gmail.com> | Jim Turk | Some new ones |
| Justine Beaufort <owlgurl90@gmail.com> | Jim Turk | Some new ones |
| Justine Beaufort <owlgurl90@gmail.com> | jimturk420@gmail.com | Brand new photo |
| Justine Beaufort <owlgurl90@gmail.com> | jimturk420@gmail.com | Brand new photo |
| Justine Beaufort <owlgurl90@gmail.com> | 'jimturk420@gmail.co... | Brand new photo |
| Justine Beaufort <owlgurl90@gmail.com> | jimturk420@gmail.com | Brand new photo |
| Justine Beaufort <owlgurl90@gmail.com> | Jim Turk | Docs |
| Justine Beaufort <owlgurl90@gmail.com> | Jim Turk | Docs |
| Abby Davidson <ADavidson@staycincinnatiusa.com> | owlgurl90@gmail.com | RE: Form Submission - ContactU |
| Abby Davidson <ADavidson@staycincinnatiusa.com> | owlgurl90@gmail.com | RE: Form Submission - ContactU |
| Abby Davidson <ADavidson@staycincinnatiusa.com> | owlgurl90@gmail.com | RE: Form Submission - ContactU |
| Justine Beaufort <owlgurl90@gmail.com> | Abby Davidson | Re: Form Submission - ContactU |

**Justine Beaufort <owlgurl90@g...**

**EMAIL ATTACHMENTS**

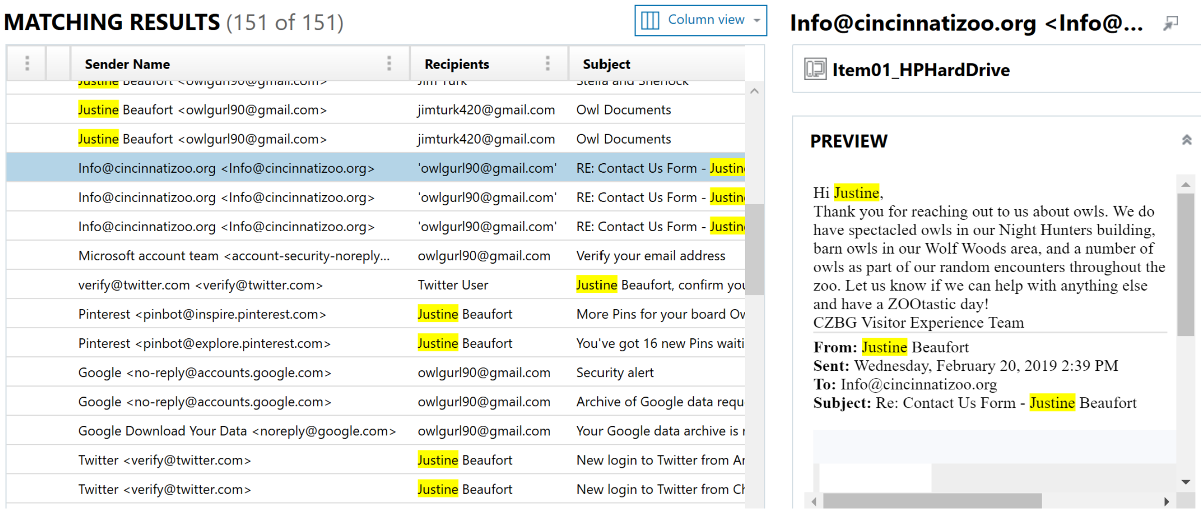
Barn-Owl-Cocked-Head.jpg.696x0_q80_crop-smart.jpg

**PREVIEW**

Figure 3-4-7: Email Body in The Preview Pane And Email Attachments

## Searching Email

Emails can be searched for keywords. Keyword searches are not case sensitive. Column data such as To, From, Subject and the message body itself will be included in searches. In the example shown below, a search was done for the term “justine.” As can be seen in the results, hits are highlighted in the column information about the email in addition to the body of the email.



**MATCHING RESULTS** (151 of 151)

| Sender Name | Recipients | Subject |
|---|---|---|
| Justine Beaufort <owlgurl90@gmail.com> | Jim Turk | Stella and Sherlock |
| Justine Beaufort <owlgurl90@gmail.com> | jimturk420@gmail.com | Owl Documents |
| Justine Beaufort <owlgurl90@gmail.com> | jimturk420@gmail.com | Owl Documents |
| Info@cincinnatizoo.org <Info@cincinnatizoo.org> | 'owlgurl90@gmail.com' | RE: Contact Us Form - Justin |
| Info@cincinnatizoo.org <Info@cincinnatizoo.org> | 'owlgurl90@gmail.com' | RE: Contact Us Form - Justin |
| Info@cincinnatizoo.org <Info@cincinnatizoo.org> | 'owlgurl90@gmail.com' | RE: Contact Us Form - Justin |
| Microsoft account team <account-security-noreply... | owlgurl90@gmail.com | Verify your email address |
| verify@twitter.com <verify@twitter.com> | Twitter User | Justine Beaufort, confirm you |
| Pinterest <pinbot@inspire.pinterest.com> | Justine Beaufort | More Pins for your board Ov |
| Pinterest <pinbot@explore.pinterest.com> | Justine Beaufort | You've got 16 new Pins waiti |
| Google <no-reply@accounts.google.com> | owlgurl90@gmail.com | Security alert |
| Google <no-reply@accounts.google.com> | owlgurl90@gmail.com | Archive of Google data requ |
| Google Download Your Data <noreply@google.com> | owlgurl90@gmail.com | Your Google data archive is r |
| Twitter <verify@twitter.com> | Justine Beaufort | New login to Twitter from Ar |
| Twitter <verify@twitter.com> | Justine Beaufort | New login to Twitter from Ch |

**Info@cincinnatizoo.org <Info@...**

**Item01_HPHardDrive**

**PREVIEW**

Hi Justine,
Thank you for reaching out to us about owls. We do have spectacled owls in our Night Hunters building, barn owls in our Wolf Woods area, and a number of owls as part of our random encounters throughout the zoo. Let us know if we can help with anything else and have a ZOOtastic day!
CZBG Visitor Experience Team

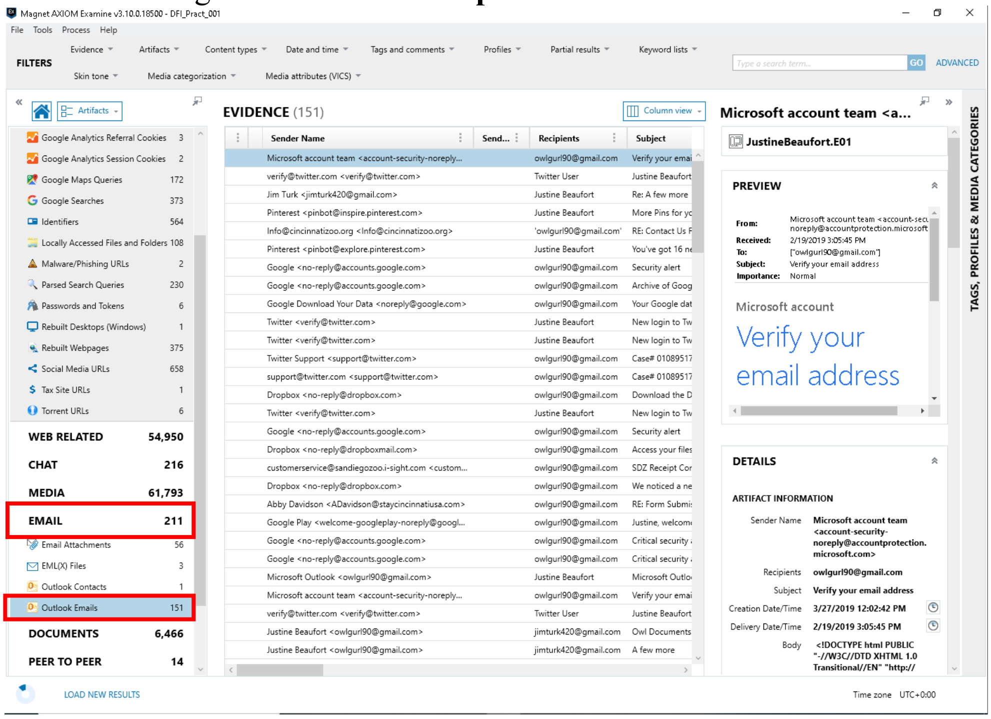
**From:** Justine Beaufort
**Sent:** Wednesday, February 20, 2019 2:39 PM
**To:** Info@cincinnatizoo.org
**Subject:** Re: Contact Us Form - Justine Beaufort

Figure 3-4-9: Searching Email

# Exercise 1. Searching Email

Start Magnet AXIOM in your Forensic VM. Click on "BROWSE TO A CASE" and open case "DFI_Practical_1_Case".

1. Go to "Case dashboard", select "Artifacts" then click on "**Email**" –> "**Outlook Emails**" and right click on the "**Recipients**" column


Magnet AXIOM Examine v3.10.0.18500 - DFI_Pract_001
File Tools Process Help
FILTERS
Evidence Artifacts Content types Date and time Tags and comments Profiles Partial results Keyword lists
Skin tone Media categorization Media attributes (VICS)
Type a search term...
GO
ADVANCED
Artifacts
Column view
TAGS, PROFILES & MEDIA CATEGORIES
LOAD NEW RESULTS
Time zone UTC+0:00

| | |
|---|---|
| Google Analytics Referral Cookies | 3 |
| Google Analytics Session Cookies | 2 |
| Google Maps Queries | 172 |
| Google Searches | 373 |
| Identifiers | 564 |
| Locally Accessed Files and Folders | 108 |
| Malware/Phishing URLs | 2 |
| Parsed Search Queries | 230 |
| Passwords and Tokens | 6 |
| Rebuilt Desktops (Windows) | 1 |
| Rebuilt Webpages | 375 |
| Social Media URLs | 658 |
| Tax Site URLs | 1 |
| Torrent URLs | 6 |
| WEB RELATED | 54,950 |
| CHAT | 216 |
| MEDIA | 61,793 |
| EMAIL | 211 |
| Email Attachments | 56 |
| EML(X) Files | 3 |
| Outlook Contacts | 1 |
| Outlook Emails | 151 |
| DOCUMENTS | 6,466 |
| PEER TO PEER | 14 |

EVIDENCE (151)

| Sender Name | Send... | Recipients | Subject |
|---|---|---|---|
| Microsoft account team <account-security-noreply... | | owlgurl90@gmail.com | Verify your emai |
| verify@twitter.com <verify@twitter.com> | | Twitter User | Justine Beaufort |
| Jim Turk <jimturk420@gmail.com> | | Justine Beaufort | Re: A few more |
| Pinterest <pinbot@inspire.pinterest.com> | | Justine Beaufort | More Pins for yo |
| Info@cincinnatizoo.org <Info@cincinnatizoo.org> | | 'owlgurl90@gmail.com' | RE: Contact Us F |
| Pinterest <pinbot@explore.pinterest.com> | | Justine Beaufort | You've got 16 ne |
| Google <no-reply@accounts.google.com> | | owlgurl90@gmail.com | Security alert |
| Google <no-reply@accounts.google.com> | | owlgurl90@gmail.com | Archive of Goog |
| Google Download Your Data <noreply@google.com> | | owlgurl90@gmail.com | Your Google dat |
| Twitter <verify@twitter.com> | | Justine Beaufort | New login to Tw |
| Twitter <verify@twitter.com> | | Justine Beaufort | New login to Tw |
| Twitter Support <support@twitter.com> | | owlgurl90@gmail.com | Case# 01089517 |
| support@twitter.com <support@twitter.com> | | owlgurl90@gmail.com | Case# 01089517 |
| Dropbox <no-reply@dropbox.com> | | owlgurl90@gmail.com | Download the D |
| Twitter <verify@twitter.com> | | Justine Beaufort | New login to Tw |
| Google <no-reply@accounts.google.com> | | owlgurl90@gmail.com | Security alert |
| Dropbox <no-reply@dropboxmail.com> | | owlgurl90@gmail.com | Access your files |
| customerservice@sandiegozoo.i-sight.com <custom... | | owlgurl90@gmail.com | SDZ Receipt Cor |
| Dropbox <no-reply@dropbox.com> | | owlgurl90@gmail.com | We noticed a ne |
| Abby Davidson <ADavidson@staycincinnatiusa.com> | | owlgurl90@gmail.com | RE: Form Submis |
| Google Play <welcome-googleplay-noreply@googl... | | owlgurl90@gmail.com | Justine, welcome |
| Google <no-reply@accounts.google.com> | | owlgurl90@gmail.com | Critical security a |
| Google <no-reply@accounts.google.com> | | owlgurl90@gmail.com | Critical security a |
| Microsoft Outlook <owlgurl90@gmail.com> | | Justine Beaufort | Microsoft Outlo |
| Microsoft account team <account-security-noreply... | | owlgurl90@gmail.com | Verify your emai |
| verify@twitter.com <verify@twitter.com> | | Twitter User | Justine Beaufort |
| Justine Beaufort <owlgurl90@gmail.com> | | jimturk420@gmail.com | Owl Documents |
| Justine Beaufort <owlgurl90@gmail.com> | | jimturk420@gmail.com | A few more |

Microsoft account team <a...

JustineBeaufort.E01

PREVIEW

From: Microsoft account team <account-secu noreply@accountprotection.microsoft
Received: 2/19/2019 3:05:45 PM
To: ["owlgurl90@gmail.com"]
Subject: Verify your email address
Importance: Normal

Microsoft account

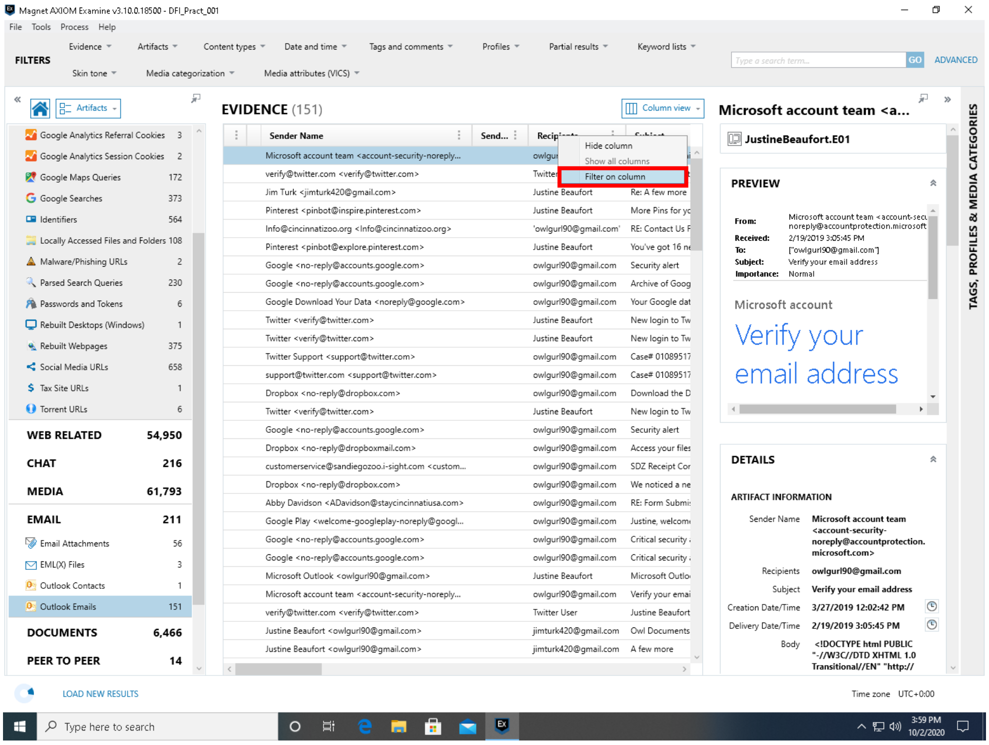
Verify your email address

DETAILS

ARTIFACT INFORMATION

| | |
|---|---|
| Sender Name | Microsoft account team <account-security-noreply@accountprotection.microsoft.com> |
| Recipients | owlgurl90@gmail.com |
| Subject | Verify your email address |
| Creation Date/Time | 3/27/2019 12:02:42 PM |
| Delivery Date/Time | 2/19/2019 3:05:45 PM |
| Body | <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http:// |

2. Select "**Filter on Column**"


Magnet AXIOM Examine v3.10.0.18500 - DFI_Pract_001
File Tools Process Help
FILTERS
Evidence Artifacts Content types Date and time Tags and comments Profiles Partial results Keyword lists
Skin tone Media categorization Media attributes (VICS)
Type a search term...
GO
ADVANCED
Artifacts
Column view
Hide column
Show all columns
Filter on column
TAGS, PROFILES & MEDIA CATEGORIES
LOAD NEW RESULTS
Time zone UTC+0:00
Type here to search
3:59 PM
10/2/2020

| | |
|---|---|
| Google Analytics Referral Cookies | 3 |
| Google Analytics Session Cookies | 2 |
| Google Maps Queries | 172 |
| Google Searches | 373 |
| Identifiers | 564 |
| Locally Accessed Files and Folders | 108 |
| Malware/Phishing URLs | 2 |
| Parsed Search Queries | 230 |
| Passwords and Tokens | 6 |
| Rebuilt Desktops (Windows) | 1 |
| Rebuilt Webpages | 375 |
| Social Media URLs | 658 |
| Tax Site URLs | 1 |
| Torrent URLs | 6 |
| WEB RELATED | 54,950 |
| CHAT | 216 |
| MEDIA | 61,793 |
| EMAIL | 211 |
| Email Attachments | 56 |
| EML(X) Files | 3 |
| Outlook Contacts | 1 |
| Outlook Emails | 151 |
| DOCUMENTS | 6,466 |
| PEER TO PEER | 14 |

EVIDENCE (151)

| Sender Name | Send... | Recipients | Subject |
|---|---|---|---|
| Microsoft account team <account-security-noreply... | | owlgu | |
| verify@twitter.com <verify@twitter.com> | | Twitter | |
| Jim Turk <jimturk420@gmail.com> | | Justine Beaufort | Re: A few more |
| Pinterest <pinbot@inspire.pinterest.com> | | Justine Beaufort | More Pins for yo |
| Info@cincinnatizoo.org <Info@cincinnatizoo.org> | | 'owlgurl90@gmail.com' | RE: Contact Us F |
| Pinterest <pinbot@explore.pinterest.com> | | Justine Beaufort | You've got 16 ne |
| Google <no-reply@accounts.google.com> | | owlgurl90@gmail.com | Security alert |
| Google <no-reply@accounts.google.com> | | owlgurl90@gmail.com | Archive of Goog |
| Google Download Your Data <noreply@google.com> | | owlgurl90@gmail.com | Your Google dat |
| Twitter <verify@twitter.com> | | Justine Beaufort | New login to Tw |
| Twitter <verify@twitter.com> | | Justine Beaufort | New login to Tw |
| Twitter Support <support@twitter.com> | | owlgurl90@gmail.com | Case# 01089517 |
| support@twitter.com <support@twitter.com> | | owlgurl90@gmail.com | Case# 01089517 |
| Dropbox <no-reply@dropbox.com> | | owlgurl90@gmail.com | Download the D |
| Twitter <verify@twitter.com> | | Justine Beaufort | New login to Tw |
| Google <no-reply@accounts.google.com> | | owlgurl90@gmail.com | Security alert |
| Dropbox <no-reply@dropboxmail.com> | | owlgurl90@gmail.com | Access your files |
| customerservice@sandiegozoo.i-sight.com <custom... | | owlgurl90@gmail.com | SDZ Receipt Cor |
| Dropbox <no-reply@dropbox.com> | | owlgurl90@gmail.com | We noticed a ne |
| Abby Davidson <ADavidson@staycincinnatiusa.com> | | owlgurl90@gmail.com | RE: Form Submis |
| Google Play <welcome-googleplay-noreply@googl... | | owlgurl90@gmail.com | Justine, welcome |
| Google <no-reply@accounts.google.com> | | owlgurl90@gmail.com | Critical security a |
| Google <no-reply@accounts.google.com> | | owlgurl90@gmail.com | Critical security a |
| Microsoft Outlook <owlgurl90@gmail.com> | | Justine Beaufort | Microsoft Outlo |
| Microsoft account team <account-security-noreply... | | owlgurl90@gmail.com | Verify your emai |
| verify@twitter.com <verify@twitter.com> | | Twitter User | Justine Beaufort |
| Justine Beaufort <owlgurl90@gmail.com> | | jimturk420@gmail.com | Owl Documents |
| Justine Beaufort <owlgurl90@gmail.com> | | jimturk420@gmail.com | A few more |

Microsoft account team <a...

JustineBeaufort.E01

PREVIEW

From: Microsoft account team <account-secu noreply@accountprotection.microsoft
Received: 2/19/2019 3:05:45 PM
To: ["owlgurl90@gmail.com"]
Subject: Verify your email address
Importance: Normal

Microsoft account

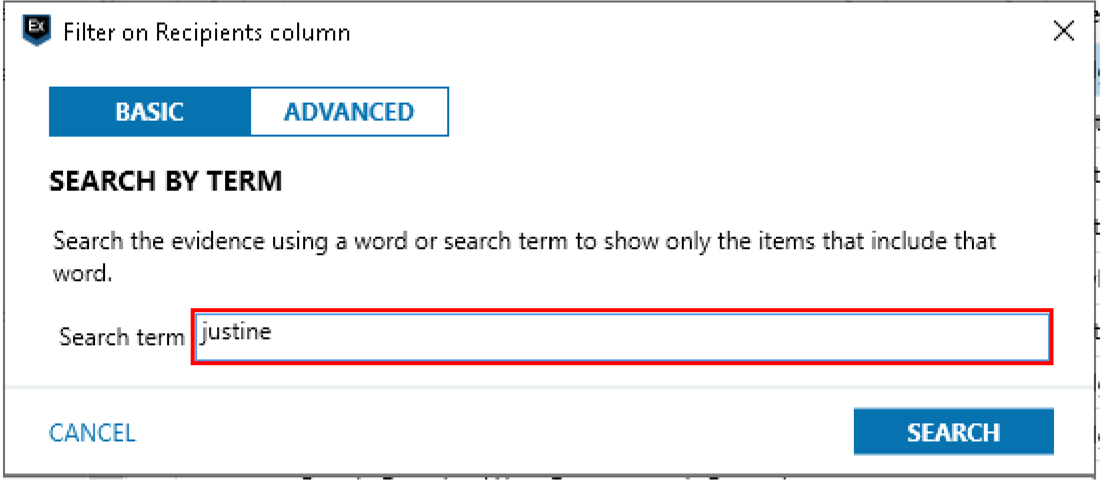
Verify your email address

DETAILS

ARTIFACT INFORMATION

| | |
|---|---|
| Sender Name | Microsoft account team <account-security-noreply@accountprotection.microsoft.com> |
| Recipients | owlgurl90@gmail.com |
| Subject | Verify your email address |
| Creation Date/Time | 3/27/2019 12:02:42 PM |
| Delivery Date/Time | 2/19/2019 3:05:45 PM |
| Body | <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http:// |

3. Key in "**Justine**" on the "**Search term**" bar



SEARCH BY TERM

Search the evidence using a word or search term to show only the items that include that word.

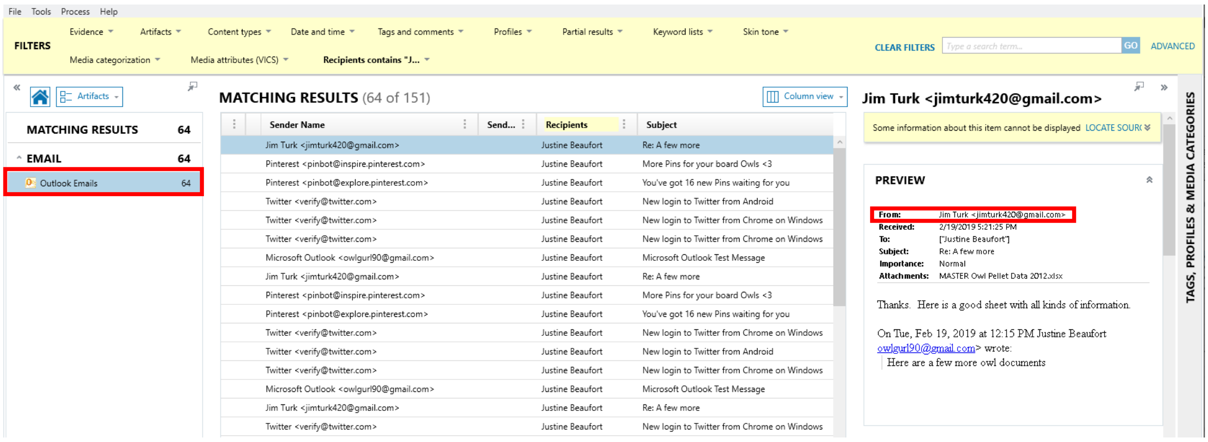
Search term: justine

**Exercise Question 1**

a) How many records appeared within Outlook Emails? 64

b) Who is the sender (Name and Email) of the email with the title of "Re: A few more"

Jim Turk <jimturk420@gmail.com>



| | |
|---|---|
| MATCHING RESULTS | 64 |
| EMAIL | 64 |
| Outlook Emails | 64 |

MATCHING RESULTS (64 of 151)

| Sender Name | Send... | Recipients | Subject |
|---|---|---|---|
| Jim Turk <jimturk420@gmail.com> | | Justine Beaufort | Re: A few more |
| Pinterest <pinbot@inspire.pinterest.com> | | Justine Beaufort | More Pins for your board Owls <3 |
| Pinterest <pinbot@explore.pinterest.com> | | Justine Beaufort | You've got 16 new Pins waiting for you |
| Twitter <verify@twitter.com> | | Justine Beaufort | New login to Twitter from Android |
| Twitter <verify@twitter.com> | | Justine Beaufort | New login to Twitter from Chrome on Windows |
| Twitter <verify@twitter.com> | | Justine Beaufort | New login to Twitter from Chrome on Windows |
| Microsoft Outlook <owlgurl90@gmail.com> | | Justine Beaufort | Microsoft Outlook Test Message |
| Jim Turk <jimturk420@gmail.com> | | Justine Beaufort | Re: A few more |
| Pinterest <pinbot@inspire.pinterest.com> | | Justine Beaufort | More Pins for your board Owls <3 |
| Pinterest <pinbot@explore.pinterest.com> | | Justine Beaufort | You've got 16 new Pins waiting for you |
| Twitter <verify@twitter.com> | | Justine Beaufort | New login to Twitter from Chrome on Windows |
| Twitter <verify@twitter.com> | | Justine Beaufort | New login to Twitter from Android |
| Twitter <verify@twitter.com> | | Justine Beaufort | New login to Twitter from Chrome on Windows |
| Microsoft Outlook <owlgurl90@gmail.com> | | Justine Beaufort | Microsoft Outlook Test Message |
| Jim Turk <jimturk420@gmail.com> | | Justine Beaufort | Re: A few more |
| Twitter <verify@twitter.com> | | Justine Beaufort | New login to Twitter from Chrome on Windows |

Jim Turk <jimturk420@gmail.com>

Some information about this item cannot be displayed

PREVIEW

| | |
|---|---|
| **From:** | Jim Turk <jimturk420@gmail.com> |
| **Received:** | 2/19/2019 5:21:25 PM |
| **To:** | ["Justine Beaufort"] |
| **Subject:** | Re: A few more |
| **Importance:** | Normal |
| **Attachments:** | MASTER Owl Pellet Data 2012.xlsx |

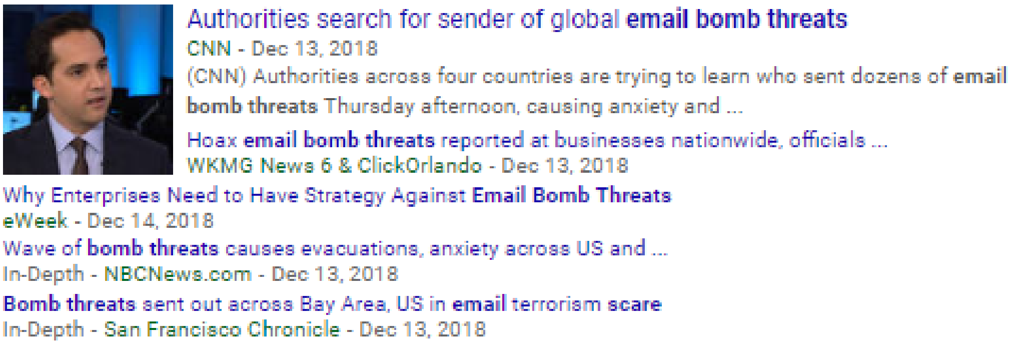
Thanks. Here is a good sheet with all kinds of information.

On Tue, Feb 19, 2019 at 12:15 PM Justine Beaufort owlgurl90@gmail.com> wrote:

> Here are a few more owl documents

## Exercise 2. Tracing Email

On December 13, 2018, thousands of bomb threats were received via email by businesses, schools, and governmental agencies throughout the United States.



Authorities search for sender of global email bomb threats
CNN - Dec 13, 2018
(CNN) Authorities across four countries are trying to learn who sent dozens of email bomb threats Thursday afternoon, causing anxiety and ...

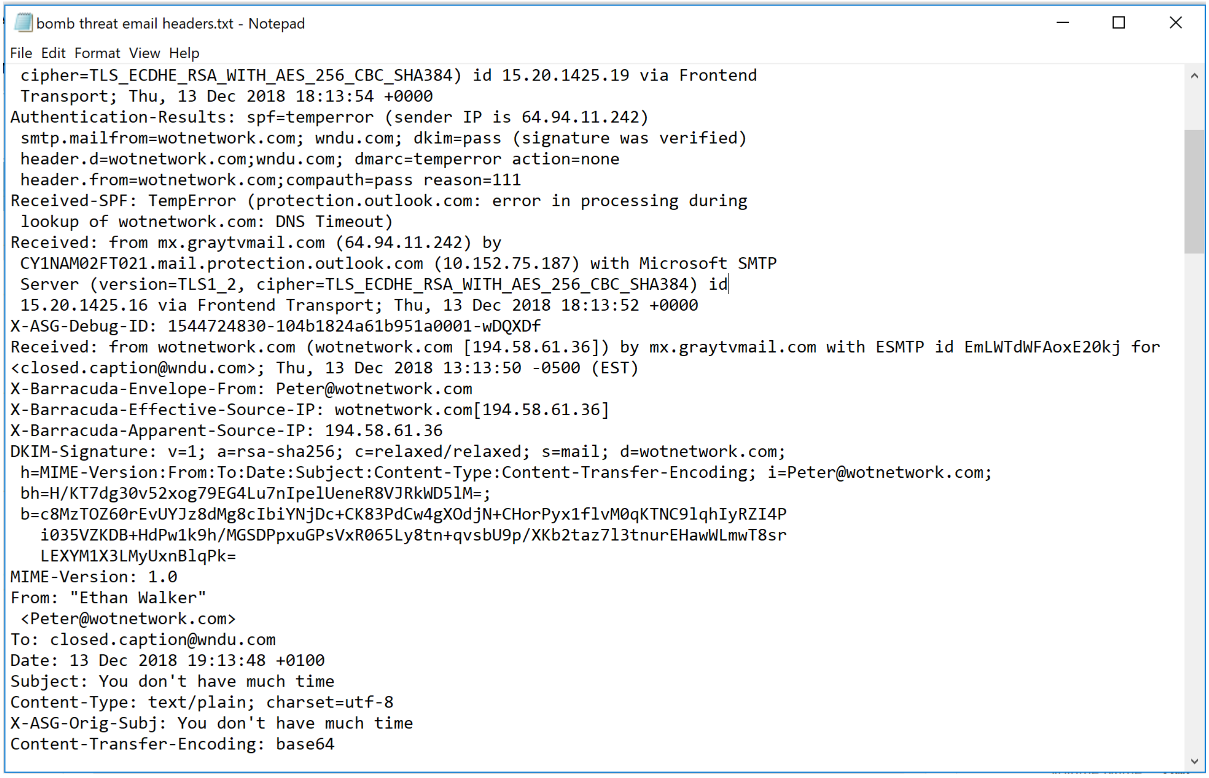
Hoax email bomb threats reported at businesses nationwide, officials ...
WKMG News 6 & ClickOrlando - Dec 13, 2018

Why Enterprises Need to Have Strategy Against Email Bomb Threats
eWeek - Dec 14, 2018

Wave of bomb threats causes evacuations, anxiety across US and ...
In-Depth - NBCNews.com - Dec 13, 2018

Bomb threats sent out across Bay Area, US in email terrorism scare
In-Depth - San Francisco Chronicle - Dec 13, 2018

Here is header information from one of those emails:



bomb threat email headers.txt - Notepad
File Edit Format View Help

```
 cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384) id 15.20.1425.19 via Frontend
 Transport; Thu, 13 Dec 2018 18:13:54 +0000
Authentication-Results: spf=temperror (sender IP is 64.94.11.242)
 smtp.mailfrom=wotnetwork.com; wndu.com; dkim=pass (signature was verified)
 header.d=wotnetwork.com;wndu.com; dmarc=temperror action=none
 header.from=wotnetwork.com;compauth=pass reason=111
Received-SPF: TempError (protection.outlook.com: error in processing during
 lookup of wotnetwork.com: DNS Timeout)
Received: from mx.graytvmail.com (64.94.11.242) by
 CY1NAM02FT021.mail.protection.outlook.com (10.152.75.187) with Microsoft SMTP
 Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384) id
 15.20.1425.16 via Frontend Transport; Thu, 13 Dec 2018 18:13:52 +0000
X-ASG-Debug-ID: 1544724830-104b1824a61b951a0001-wDQXDf
Received: from wotnetwork.com (wotnetwork.com [194.58.61.36]) by mx.graytvmail.com with ESMTP id EmLWTdWFAoxE20kj for
<closed.caption@wndu.com>; Thu, 13 Dec 2018 13:13:50 -0500 (EST)
X-Barracuda-Envelope-From: Peter@wotnetwork.com
X-Barracuda-Effective-Source-IP: wotnetwork.com[194.58.61.36]
X-Barracuda-Apparent-Source-IP: 194.58.61.36
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; s=mail; d=wotnetwork.com;
 h=MIME-Version:From:To:Date:Subject:Content-Type:Content-Transfer-Encoding; i=Peter@wotnetwork.com;
 bh=H/KT7dg30v52xog79EG4Lu7nIpelUeneR8VJRkWD5lM=;
 b=c8MzTOZ60rEvUYJz8dMg8cIbiYNjDc+CK83PdCw4gXOdjN+CHorPyx1flvM0qKTNC9lqhIyRZI4P
   i035VZKDB+HdPw1k9h/MGSDPpxuGPsVxR065Ly8tn+qvsbU9p/XKb2taz7l3tnurEHawWLmwT8sr
   LEXYM1X3LMyUxnBlqPk=
MIME-Version: 1.0
From: "Ethan Walker"
 <Peter@wotnetwork.com>
To: closed.caption@wndu.com
Date: 13 Dec 2018 19:13:48 +0100
Subject: You don't have much time
Content-Type: text/plain; charset=utf-8
X-ASG-Orig-Subj: You don't have much time
Content-Transfer-Encoding: base64
```

### Exercise Question 2

a) What is the origin IP address of the email? 64.94.11.242

b) Who is the registrant of that IP address? Hint: Arin.net.

Internap Holding LLC

c) What is the geographical location of that IP address: Hint: iplocation.com.

Latitude: 33.4125, Longitude: -84.3012, Country: United States, Region: Georgia
City: Hampton, Organization: Internap Corporation

Please answer all the above questions, exercise 1 to exercise 2 and submit your answers to blackboard / Learning Resources, "Lab Exercise Folder" for class participation marks. You document should be named as "<Name><StudentID>Lab2B". Example: John123456Lab2B.

-- End --