

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.

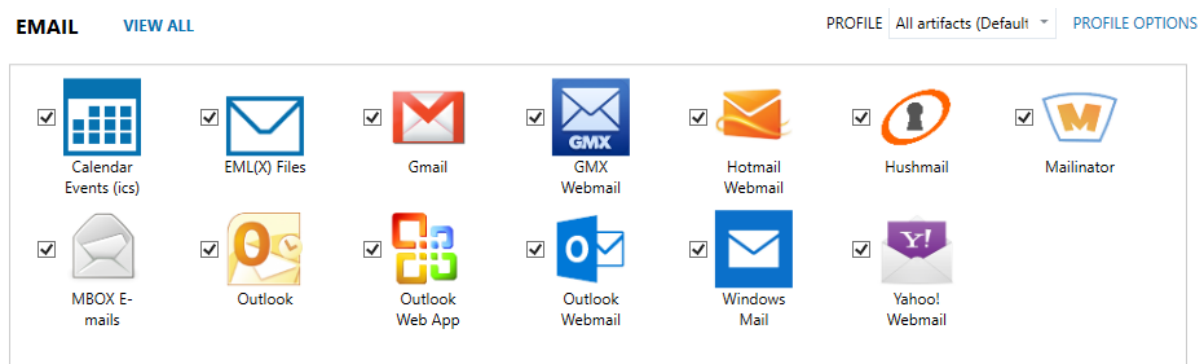


Figure 3-4-1: Supported Computer Email Artifacts In Magnet Axiom Process

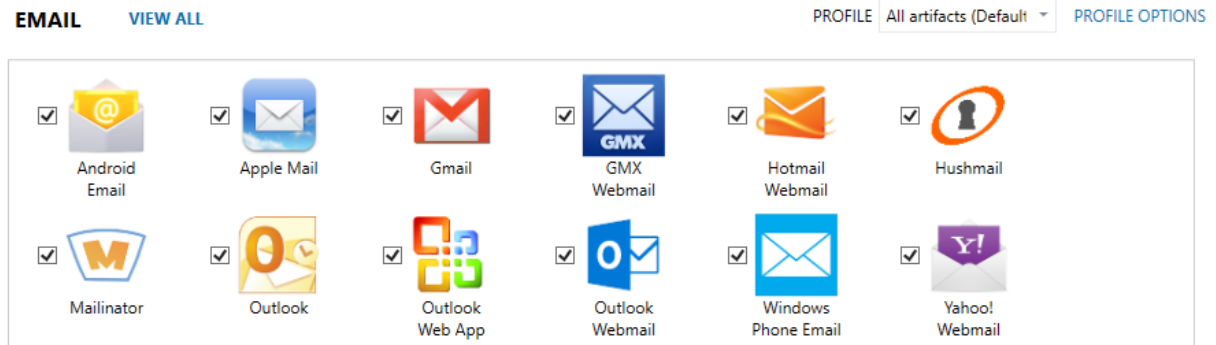


Figure 3-4-2: Supported Mobile Email Artifacts In Magnet Axiom Process

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)

Column view

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.



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.

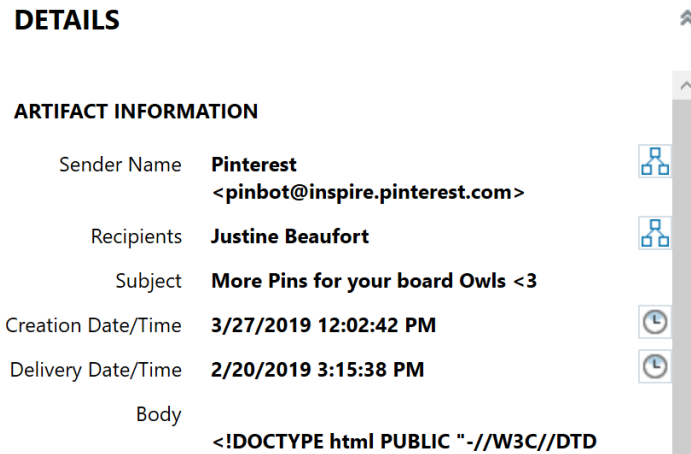


Figure 3-4-5: Email Details

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) Column view **Justine Beaufort <owlgurl90@g...>**

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 - ContactL
Abby Davidson <ADavidson@staycincinnatiusa.com>	owlgurl90@gmail.com	RE: Form Submission - ContactL
Abby Davidson <ADavidson@staycincinnatiusa.com>	owlgurl90@gmail.com	RE: Form Submission - ContactL
Justine Beaufort <owlgurl90@gmail.com>	Abby Davidson	Re: Form Submission - ContactL

EMAIL ATTACHMENTS

[Barn-Owl-Cocked-Head.jpg.696x0_q80_crop-smart.jpg](#)

PREVIEW

ZOOM 52%

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)

Column view

▼

Info@cincinnati.org <Info@...>

Sender Name	Recipients	Subject
Justine Beaufort <owlgurl90@gmail.com>	jimturk420@gmail.com	Owl Documents
Justine Beaufort <owlgurl90@gmail.com>	jimturk420@gmail.com	Owl Documents
Info@cincinnati.org <Info@cincinnati.org>	'owlgurl90@gmail.com'	RE: Contact Us Form - Justine
Info@cincinnati.org <Info@cincinnati.org>	'owlgurl90@gmail.com'	RE: Contact Us Form - Justine
Info@cincinnati.org <Info@cincinnati.org>	'owlgurl90@gmail.com'	RE: Contact Us Form - Justine
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 Cl

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 ZOOfastic day!

CZBG Visitor Experience Team

From: Justine Beaufort
Sent: Wednesday, February 20, 2019 2:39 PM
To: Info@cincinnati.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”.

- Go to “Case dashboard”, select “Artifacts” then click on “Email” → “Outlook Emails” and right click on the “Recipients” column

The screenshot shows the Magnet AXIOM interface. On the left, the 'FILTERS' pane lists various artifacts, with 'EMAIL' highlighted in red and showing 211 items. Below it, 'Outlook Emails' is also highlighted in red. The main 'EVIDENCE' pane displays a table of 151 items. The 'Recipients' column is highlighted, and a context menu is open with 'Filter on column' selected. The right pane shows a preview of an email from 'Microsoft account team' with the subject 'Verify your email address'.

- Select “Filter on Column”

This screenshot is identical to the one above, showing the Magnet AXIOM interface with the 'Filter on column' context menu open over the 'Recipients' column in the evidence table.

3. Key in “Justine” on the “Search term” bar

Filter on Recipients column

BASIC **ADVANCED**

SEARCH BY TERM

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

Search term

CANCEL **SEARCH**

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

File Tools Process Help

Evidence Artifacts Content types Date and time Tags and comments Profiles Partial results Keyword lists Skin tone

FILTERS Media categorization Media attributes (VICS) Recipients contains "J..."

CLEAR FILTERS Type a search term... **GO** **ADVANCED**

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 <venfy@twitter.com>		Justine Beaufort	New login to Twitter from Android
Twitter <venfy@twitter.com>		Justine Beaufort	New login to Twitter from Chrome on Windows
Twitter <venfy@twitter.com>		Justine Beaufort	New login to Twitter from Chrome on Windows
Microsoft Outlook <owlgun90@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 <venfy@twitter.com>		Justine Beaufort	New login to Twitter from Chrome on Windows
Twitter <venfy@twitter.com>		Justine Beaufort	New login to Twitter from Android
Twitter <venfy@twitter.com>		Justine Beaufort	New login to Twitter from Chrome on Windows
Microsoft Outlook <owlgun90@gmail.com>		Justine Beaufort	Microsoft Outlook Test Message
Jim Turk <jimturk420@gmail.com>		Justine Beaufort	Re: A few more
Twitter <venfy@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. [LOCATE SOURCE](#)

PREVIEW

From: Jim Turk <jimturk420@gmail.com>

Received: 2/19/2019 5:01:25 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 <owlgun90@gmail.com> wrote:

Here are a few more owl documents

TAGS, PROFILES & MEDIA CATEGORIES

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 ESMTTP 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/KT7dg30v52xog79EG4Lu7nIpe1UeneR8VJRkWD51M=;
b=c8MzT0Z60rEvUYJz8dMg8cIbiYNjDc+CK83PdCw4gX0djN+CHorPyx1f1vM0qKTNC91qhIyRZi4P
i035VZKDB+HdPw1k9h/McGSDPpxuGPsVxR065Ly8tn+qvsbU9p/XKb2taz713tnurEHawWlMwT8sr
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.

Unitas Global

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

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 --