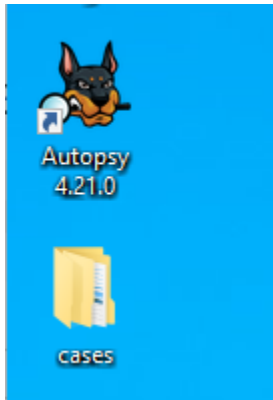


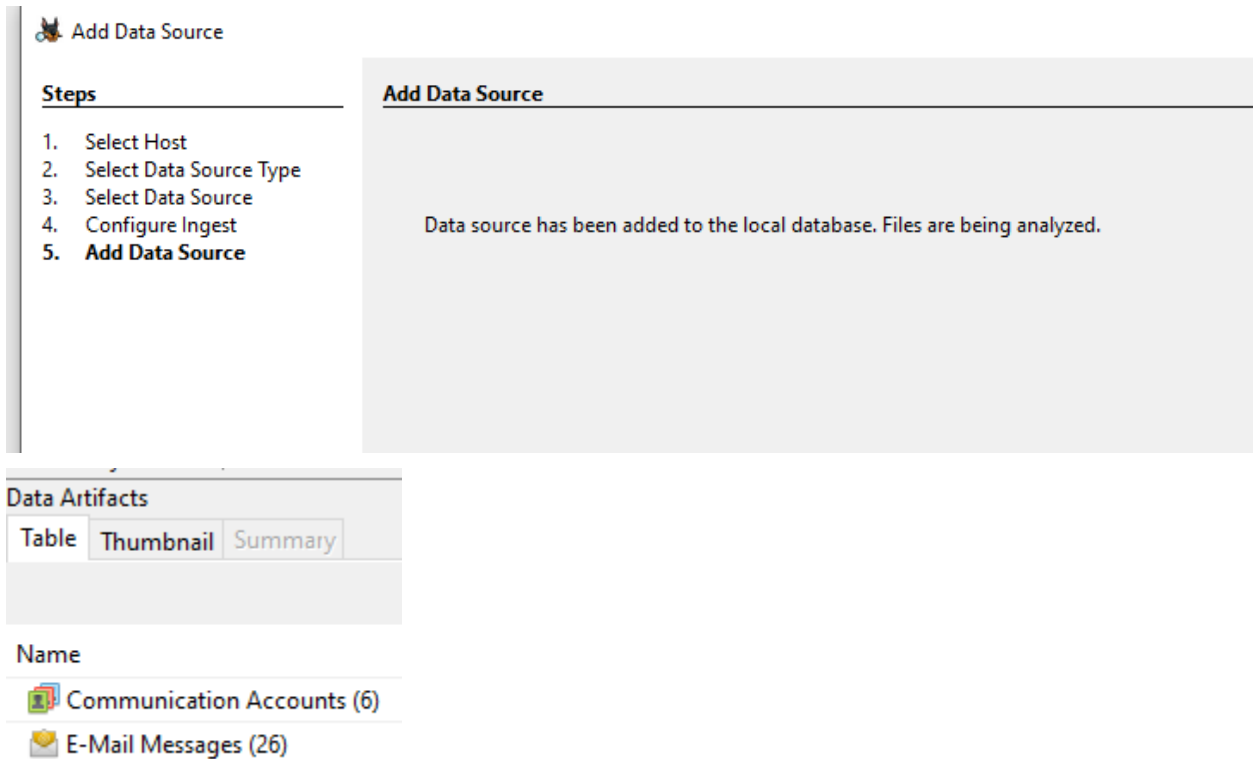
Task 1: Recover PST Emails

Step 1: Install Autopsy






Autopsy installed onto Windows VM from previous labs.

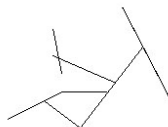
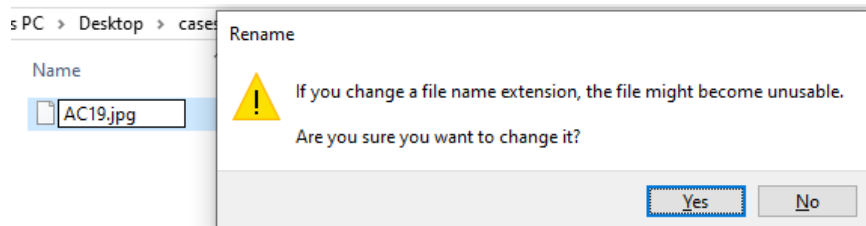
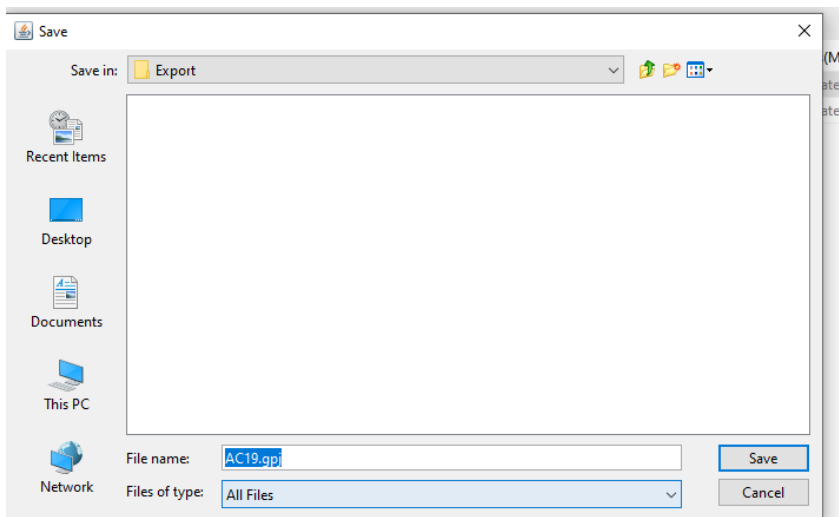
Step 2: Create Case



.pst files were added to the new case that was created. Email messages were found in the data artifacts section.

Step 3: Analyze Email Attachment

Directory tree		
Data Content		
/LogicalFileSet1/Jim_shu's.pst		
Table	Thumbnail	Summary
Name	S	C
 AC19.gpj		
 Tubing Materials.rtf		



Successfully located email attachment; extracted and renamed the file.

Step 4: Analyze Email Headers

From: baspen99@aol.com <baspen99@aol.com>
To: jim_shu@comcast.net
CC:
Subject: Request

Headers | Text | HTML | RTF | Attachments (0) | Accounts

```

-----HEADERS-----

Received: from imo-d04.mx.aol.com ([205.188.157.36])
    by rwcrmxc15.comcast.net (rwcrmxc15) with ESMTP
    id <20061204020424r1500jql9e>; Mon, 4 Dec 2006 02:04:24 +0000
X-Originating-IP: [205.188.157.36]
Received: from Baspen99@aol.com
    by imo-d04.mx.aol.com (mail_out_v38_r7.6) id i.ce5.478a666 (52373)
    for <jim_shu@comcast.net>; Sun, 3 Dec 2006 21:04:17 -0500 (EST)
Received: from FWM-D21 (fwm-d21.webmail.aol.com [205.188.160.213]) by ciao-m02.mx.a
To: jim_shu@comcast.net
Subject: Request
Date: Sun, 03 Dec 2006 21:04:15 -0500
X-MB-Message-Source: WebUI
MIME-Version: 1.0
From: baspen99@aol.com
X-MB-Message-Type: User
Content-Type: multipart/alternative;
    boundary="-----MB_8C8E55FA25FEDC7_F50_5BFC_FWM-D21.sysops.aol.com"
X-Mailer: AOL WebMail 22250
Received: from 24.18.24.250 by FWM-D21.sysops.aol.com (205.188.160.213) with HTTP (WebM
Message-Id: <8C8E55FA2625021-F50-310D@FWM-D21.sysops.aol.com>
X-AOL-IP: 205.188.160.213
X-Spam-Flag: NO

---END HEADERS---

```

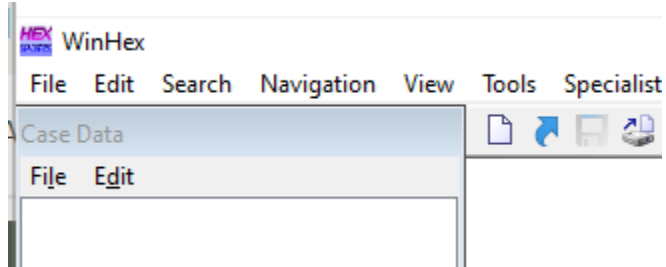
Headers Found

Header Name	Header Value
X-Originating-IP	[205.188.157.36]
To	jim_shu@comcast.net
Subject	Request
Date	Sun, 03 Dec 2006 21:04:15 -0500
X-MB-Message-Source	WebUI
MIME-Version	1.0
From	baspen99@aol.com
X-MB-Message-Type	User
Content-Type	multipart/alternative; boundary="-----MB_8C8E55FA25FEDC7_F50_5BFC_FWM-D21.sysops.aol.com"
X-Mailer	AOL WebMail 22250
Message-Id	<8C8E55FA2625021-F50-310D@FWM-D21.sysops.aol.com>
X-AOL-IP	205.188.160.213
X-Spam-Flag	NO

Successfully analyzed header of email from .pst file. We can see that this email was sent in 2006 in December and the originating IP address of the sender.

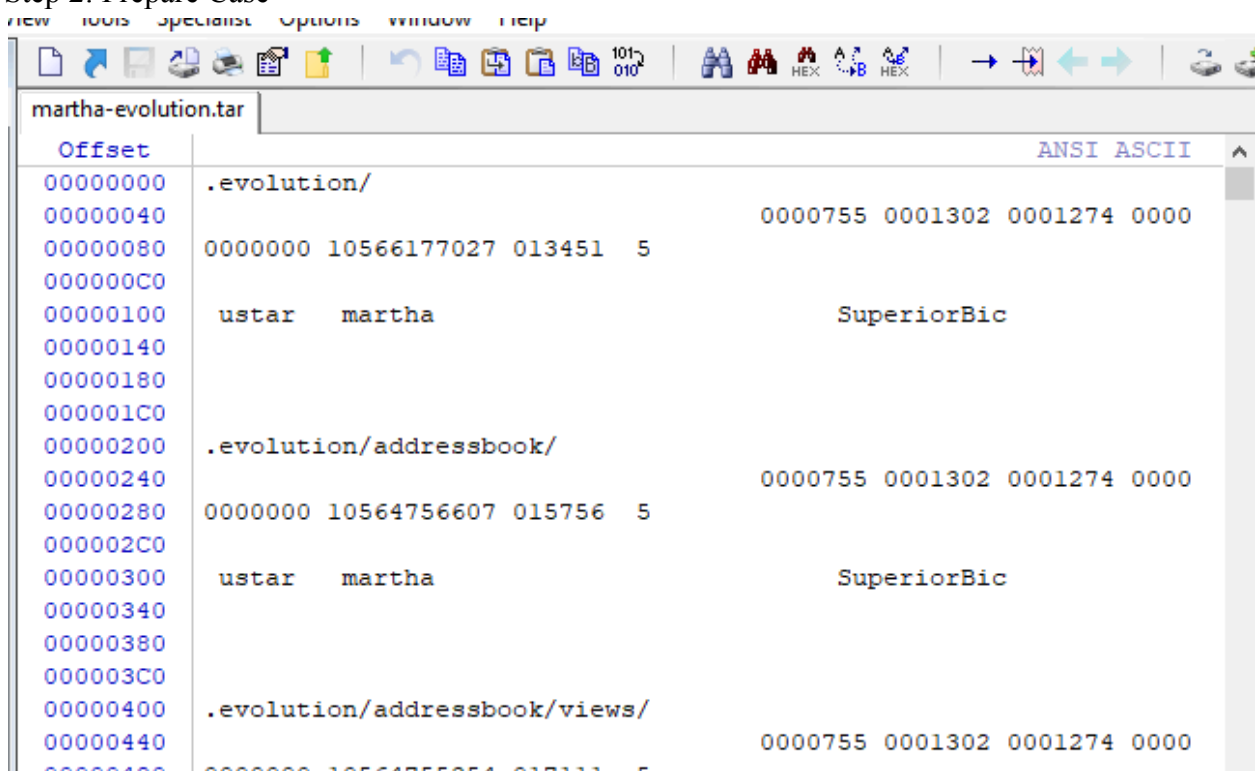
Task 2: Recover Other Emails

Step 1: Install Winhex



WinHex installed from previous labs.

Step 2: Prepare Case



Successfully removed Hex Display and loaded .tar file onto WinHex.

Step 3: Carve Email from Terry

```

00071000 : <robert.swartz@superiorbicycles.biz> Sent: Wednesday, February
00071040 14, 2007 6:03 PM Subject: Audits > Chris, > > We will need
00071080 to prepare for the annual board meeting. Can you coordinate > wi
000710C0 th Bob those special projects? > > Martha > From terrysadler@
00071100 goowy.com Sat Feb 17 15:15:45 2007 Received: from smtp-sjt-01.vi
00071140 vidround.com ([199.249.224.252]) by mail.vividround.com with Mi
00071180 crosoft SMTPSVC(6.0.3790.1830); Sat, 17 Feb 2007 15:15:45 -0600
000711C0 Received: from smtp1.goowy.com (smtp1.goowy.com [209.126.247.20
00071200 5]) by smtp-sjt-01.vividround.com (8.12.11/8.12.11) with ESMTP

```

File name:

Save as type:

 martha-evolution - Notepad

```

File Edit Format View Help
From terrysadler@goowy.com Sat Feb 17 15:15:45 2007
Received: from smtp-sjt-01.vividround.com ([199.249.224.252]) by
    mail.vividround.com with Microsoft SMTPSVC(6.0.3790.1830); Sat, 17 Feb 2007
    15:15:45 -0600
Received: from smtp1.goowy.com (smtp1.goowy.com [209.126.247.205]) by
    smtp-sjt-01.vividround.com (8.12.11/8.12.11) with ESMTP id 11HLAcgD060105
    for <martha.dax@superiorbicycles.biz>; Sat, 17 Feb 2007 15:10:38 -0600 (CST)
Received: (qmail 2864 invoked from network); 17 Feb 2007 21:01:53 -0000
Received: by simscan 1.1.0 ppid: 2857, pid: 2859, t: 0.1710s scanners:
    attach: 1.1.0 clamav: 0.88.4/m:38/d:1506 spam: 3.1.2
X-Spam-Checker-Version: SpamAssassin 3.1.2 (2006-05-25) on smtp1.goowy.com
X-Spam-Level:
X-Spam-Status: No, score=0.5 required=4.5 tests=ALL_TRUSTED,BIZ_TLD,
    HTML_50_60,HTML_MESSAGE autolearn=disabled version=3.1.2
Received: from unknown (HELO webserver002) ([192.168.25.102])
    (envelope-sender <terrysadler@goowy.com>) by smtp1.goowy.com
    (qmail-ldap-1.03) with SMTP for <martha.dax@superiorbicycles.biz>; 17 Feb
    2007 21:01:53 -0000
goowy: id: : 520051
From: terrysadler <terrysadler@goowy.com>
Reply-To: terrysadler <terrysadler@goowy.com>
To: martha.dax@superiorbicycles.biz
Date: Sat, 17 Feb 2007 21:15:44 GMT
Message-ID: <2af031584b5c460e95b36ddd6719529f@webserver002>
Subject: Investors
MIME-Version: 1.0
X-Mailer: goowy mail - http://www.goowy.com
Priority: Normal
X-Priority: 3
Content-Type: multipart/alternative; boundary="-----_EDNP_0000_6acd7458-decb-4ef6-bc8c-d4788e09019b"
X-ePrism-Trap: Default Trap
X-eGuard-Score: () 0.6 BIZ_TLD,HTML_50_60,HTML_MESSAGE

```

Saving the information from Terry's email into a new .txt file for further analysis after searching for Terry's name and finding a hit.

Step 4: Carve Email Involving Jim Shu

```

0005D280 PIMADCPAAJyAAAsgwAMI8AACPIAADyDAAwJwAAI8gAAPIMAD CPAAJyAAAsgwA
0005D2C0 MIOl8fCcegyqOBdwTkAAAAASUVORK5CYII= ---t4dRE6cqcdSBHOrMdTQl Co
0005D300 ntent-Transfer-Encoding: 8bit ---t4dRE6cqcdSBHOrMdTQl From jim
0005D340 .shu@superiorbicycles.biz Wed Feb 14 20:11:38 2007 Received: fro
0005D380 m [192.168.1.106] ([24.18.24.250]) by mail.vividround.com with
0005D3C0 Microsoft SMTPSVC(6.0.3790.1830); Wed, 14 Feb 2007 20:11:38 -0600
0005D400 0 In-Reply-To: <1170648496.28879.9.camel@localhost.localdomain>
0005D440 References: <1170648496.28879.9.camel@localhost.localdomain> Mim
0005D480 e-Version: 1.0 (Apple Message framework v624) Content-Type: text
0005D4C0 /plain; charset=US-ASCII; format=flowed Message-Id: <1b5698a2329
0005D500 b3dc9e557394f3a74f916@superiorbicycles.biz> Content-Transfer-Enc
0005D540 oding: 7bit Cc: Bob Swartz <robert.swartz@superiorbicycles.biz>,
0005D580 Bart Jones <bart.jones@superiorbicycles.biz>, Nau Tjeriko <nau.
0005D5C0 tjeriko@superiorbicycles.biz>, Ralph Benson <ralph.benson@superi
0005D600 orbicycles.biz>, Ileen Johnson <ileen.johnson@superiorbicycles.b
0005D640 iz>, Sebastian Mwaqngonde <sebastian.mwaqngonde@superiorbicycles.
0005D680 biz>, Chris Murphy <chris.murphy@superiorbicycles.biz>, Sam Clem
0005D6C0 ens <sam.clemens@superiorbicycles.biz> From: Jim Shu <jim.shu@su
0005D700 periorbicycles.biz> Subject: Re: New Product Development Date: W
0005D740 ed, 14 Feb 2007 20:11:45 -0600 To: Martha Dax <martha.dax@superi
0005D780 orbicycles.biz> X-Mailer: Apple Mail (2.624) Return-Path: jim.sh
0005D7C0 u@superiorbicycles.biz X-OriginalArrivalTime: 15 Feb 2007 02:11:
0005D800 38.0281 (UTC) FILETIME=[A004C990:01C750A6] X-Evolution-Source:

```

```

jim - Notepad
File Edit Format View Help
From jim.shu@superiorbicycles.biz Wed Feb 14 20:11:38 2007
Received: from [192.168.1.106] ([24.18.24.250]) by mail.vividround.com with
Microsoft SMTPSVC(6.0.3790.1830); Wed, 14 Feb 2007 20:11:38 -0600
In-Reply-To: <1170648496.28879.9.camel@localhost.localdomain>
References: <1170648496.28879.9.camel@localhost.localdomain>
Time-Version: 1.0 (Apple Message framework v624)
Content-Type: text/plain; charset=US-ASCII; format=flowed
Message-Id: <1b5698a2329b3dc9e557394f3a74f916@superiorbicycles.biz>
Content-Transfer-Encoding: 7bit
Cc: Bob Swartz <robert.swartz@superiorbicycles.biz>, Bart Jones <bart.jones@superiorbicycles.biz>,
From: Jim Shu <jim.shu@superiorbicycles.biz>
Subject: Re: New Product Development
Date: Wed, 14 Feb 2007 20:11:45 -0600
To: Martha Dax <martha.dax@superiorbicycles.biz>
X-Mailer: Apple Mail (2.624)
Return-Path: jim.shu@superiorbicycles.biz
X-OriginalArrivalTime: 15 Feb 2007 02:11:38.0281 (UTC)
FILETIME=[A004C990:01C750A6]
X-Evolution-Source: pop://martha.dax@mail.superiorbicycles.biz/
X-Evolution: 00000003-0011

```

Martha, will this be available for public release soon? Jim

On Feb 4, 2007, at 10:08 PM, Martha Dax wrote:

- Hello everybody!
-
- We have a new announcement to make that is very sensitive regarding a new business venture for us. It is the manufacturing of Kayaks in addition to our bicycle line of products. Our advertising people are excited about this new addition to our line of fine products.
-
- For security purposes this is competitive sensitive information. Do not tell anyone outside our executive staff about this new

I was able to find email correspondence between Martha and Jim. This one of multiple email they're involved with together. In this email, Jim is speaking of starting a new business venture, regarding bicycles and advertising products related to that. He wants to keep these conversations secret for the sake of competition and other companies.