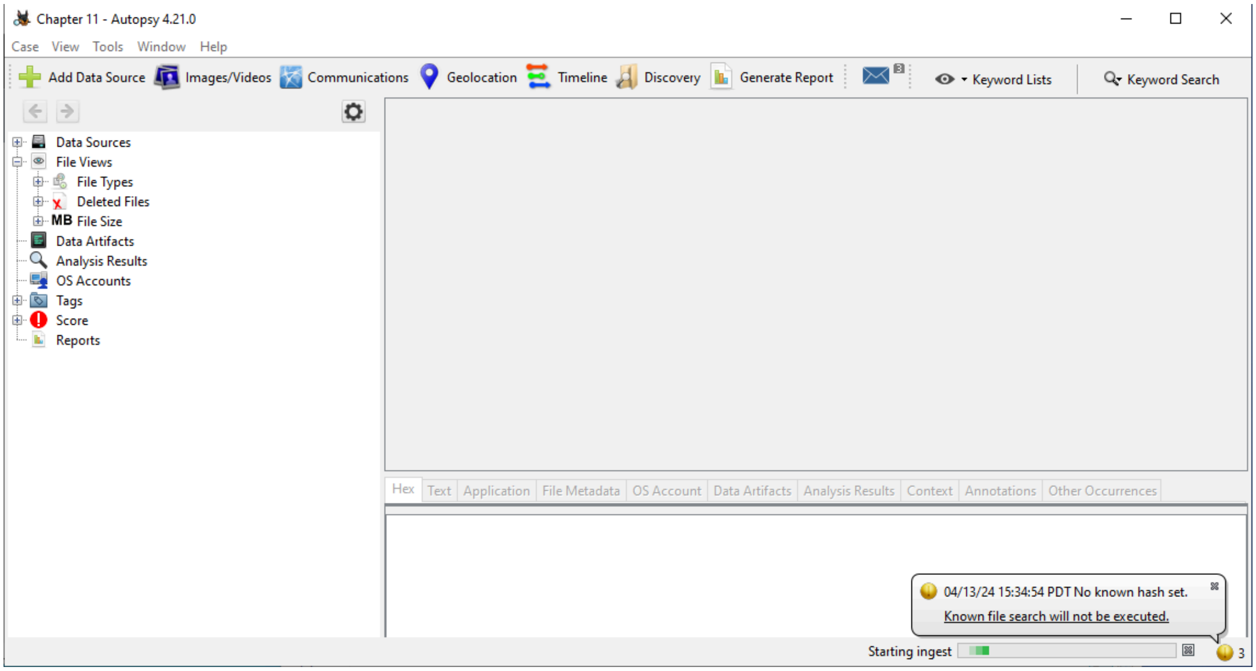
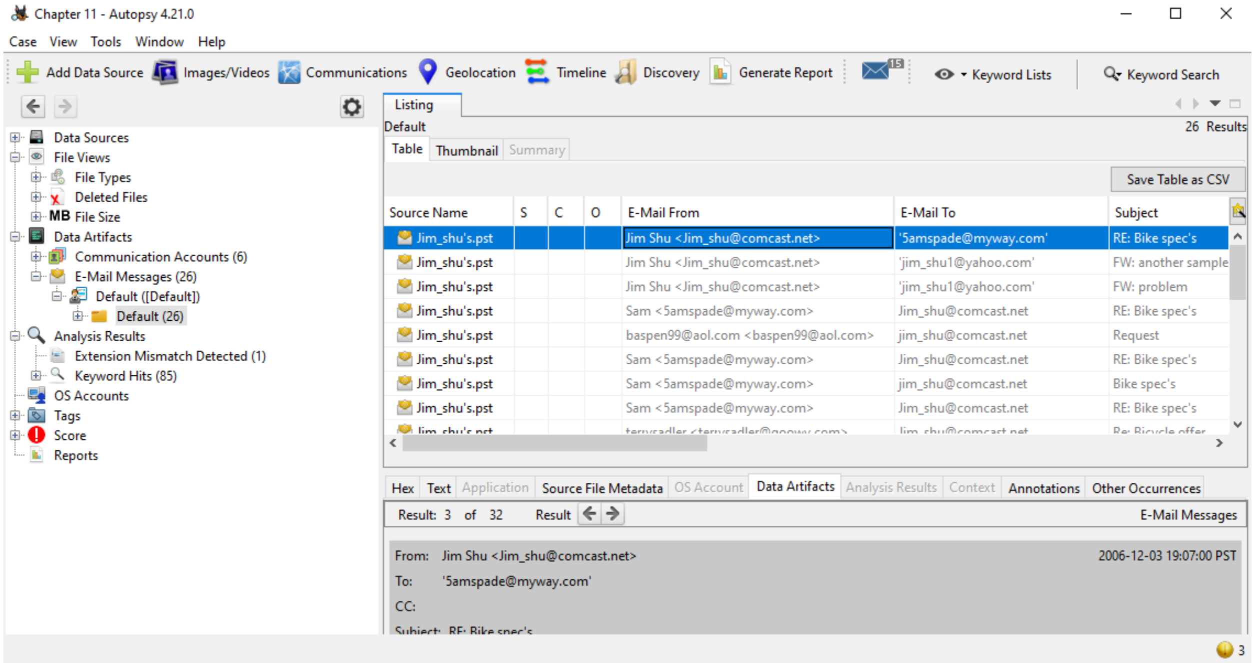
Task 1:



04/13/24 15:34:54 PDT No known hash set.
Known file search will not be executed.

Starting ingest

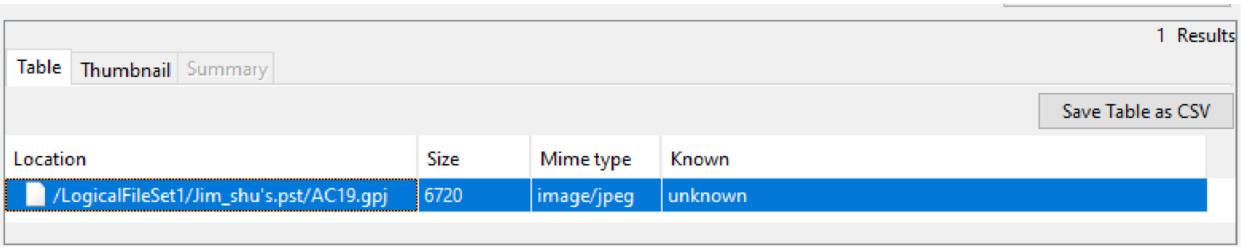
In this step, I am in autopsy and have created a new case.



Source Name	S	C	O	E-Mail From	E-Mail To	Subject
Jim_shu's.pst				Jim Shu <Jim_shu@comcast.net>	'5amspade@myway.com'	RE: Bike spec's
Jim_shu's.pst				Jim Shu <Jim_shu@comcast.net>	'jim_shu1@yahoo.com'	FW: another sample
Jim_shu's.pst				Jim Shu <Jim_shu@comcast.net>	'jim_shu1@yahoo.com'	FW: problem
Jim_shu's.pst				Sam <5amspade@myway.com>	Jim_shu@comcast.net	RE: Bike spec's
Jim_shu's.pst				baspen99@aol.com <baspen99@aol.com>	jim_shu@comcast.net	Request
Jim_shu's.pst				Sam <5amspade@myway.com>	Jim_shu@comcast.net	RE: Bike spec's
Jim_shu's.pst				Sam <5amspade@myway.com>	jim_shu@comcast.net	Bike spec's
Jim_shu's.pst				Sam <5amspade@myway.com>	Jim_shu@comcast.net	RE: Bike spec's
Jim_shu's.pst				terrysadler <terrysadler@gooway.com>	Jim_shu@comcast.net	Re: Bicycle offer

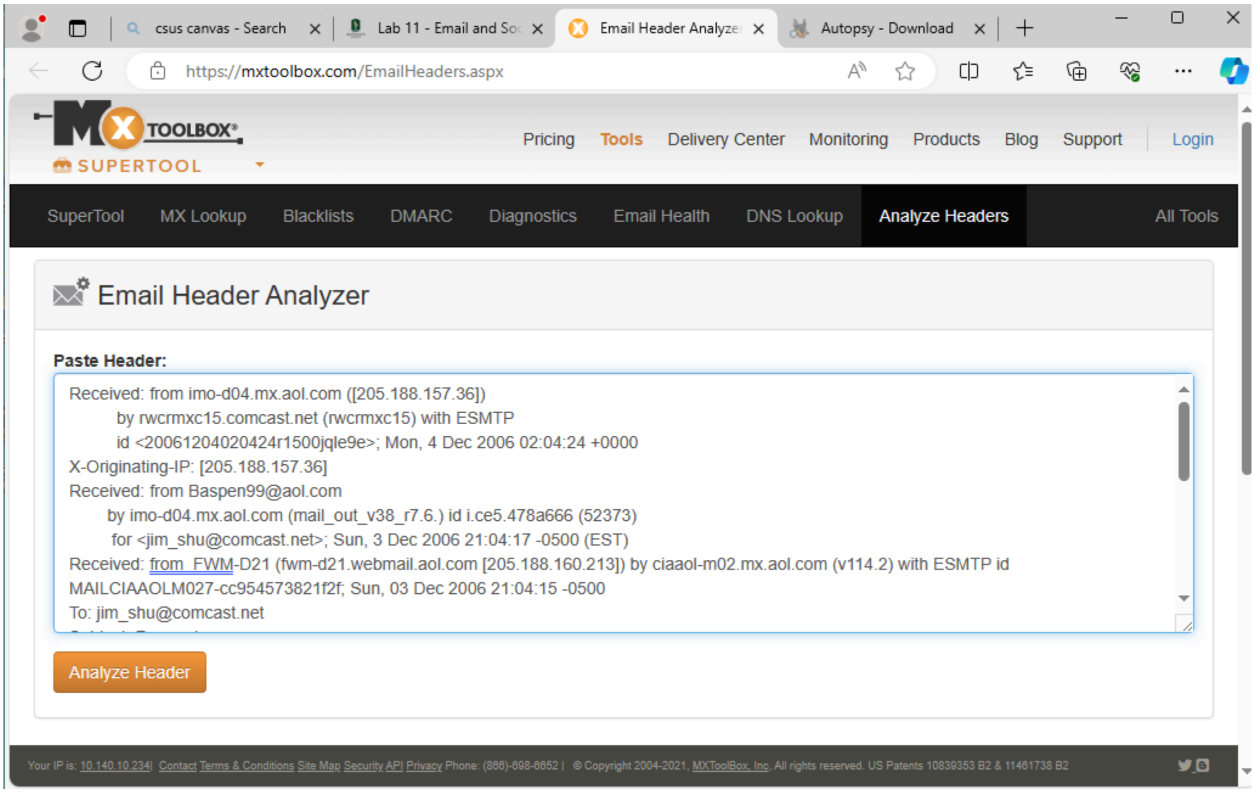
From: Jim Shu <Jim_shu@comcast.net> 2006-12-03 19:07:00 PST
To: '5amspade@myway.com'
CC:
Subject: RE: Bike spec's

Here I have found the Jim Shu email to 5amspade@myway.com.



Location	Size	Mime type	Known
/LogicalFileSet1/Jim_shu's.pst/AC19.gpj	6720	image/jpeg	unknown

Here we can see the attachment mime is image/jpeg.



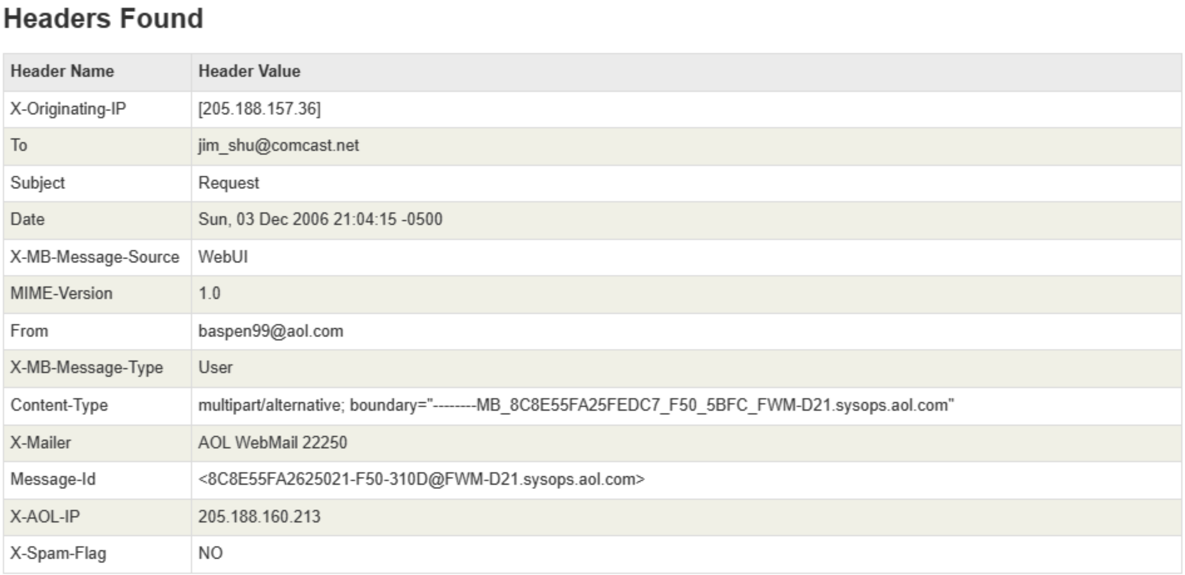
Email Header Analyzer

Paste Header:

```
Received: from imo-d04.mx.aol.com ([205.188.157.36])
        by rwcrmxc15.comcast.net (rwcrmxc15) with ESMTP
        id <20061204020424r1500jqle9e>; 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 ciaaol-m02.mx.aol.com (v114.2) with ESMTP id
MAILCIAAOLM027-cc954573821f2f; Sun, 03 Dec 2006 21:04:15 -0500
To: jim_shu@comcast.net
```

Your IP is: 10.140.10.234| Contact Terms & Conditions Site Map Security API Privacy Phone: (866)-698-6652 | © Copyright 2004-2021, MXToolBox, Inc. All rights reserved. US Patents 10839353 B2 & 11461738 B2

In this step, I have found the email from baspen99@aol.com to jim. I have copied the email header and pasted it in mxtoolbox.com.

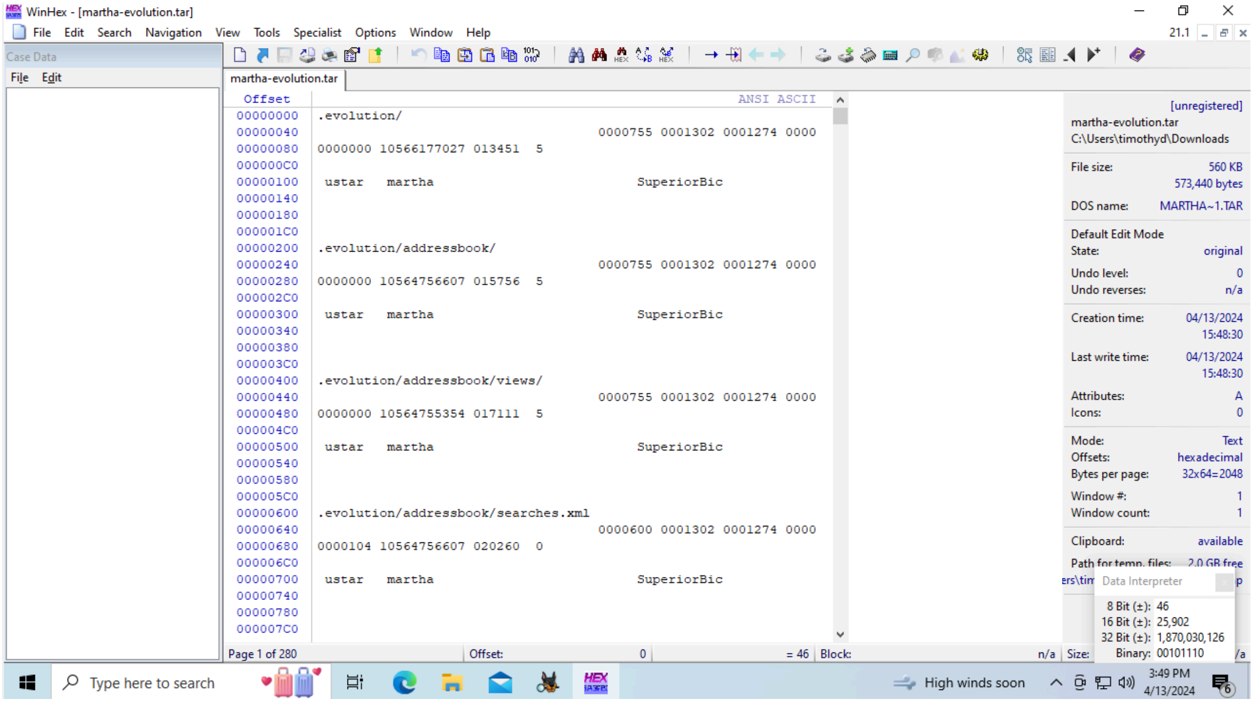


Headers Found

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

Here we can see the headers found information.

Task 2:



WinHex - [martha-evolution.tar]
File Edit Search Navigation View Tools Specialist Options Window Help
21.1
Case Data
File Edit
martha-evolution.tar
Type here to search
High winds soon
3:49 PM
4/13/2024

```
Offset                                                          ANSI ASCII
00000000  .evolution/
00000040                                       0000755 0001302 0001274 0000
00000080  0000000 10566177027 013451  5
000000C0
00000100   ustar   martha                          SuperiorBic
00000140
00000180
000001C0
00000200  .evolution/addressbook/
00000240                                       0000755 0001302 0001274 0000
00000280  0000000 10564756607 015756  5
000002C0
00000300   ustar   martha                          SuperiorBic
00000340
00000380
000003C0
00000400  .evolution/addressbook/views/
00000440                                       0000755 0001302 0001274 0000
00000480  0000000 10564755354 017111  5
000004C0
00000500   ustar   martha                          SuperiorBic
00000540
00000580
000005C0
00000600  .evolution/addressbook/searches.xml
00000640                                       0000600 0001302 0001274 0000
00000680  0000104 10564756607 020260  0
000006C0
00000700   ustar   martha                          SuperiorBic
00000740
00000780
000007C0
```

[unregistered]
martha-evolution.tar
C:\Users\timothyd\Downloads

File size: 560 KB
573,440 bytes

DOS name: MARTHA~1.TAR

Default Edit Mode
State: original
Undo level: 0
Undo reverses: n/a

Creation time: 04/13/2024 15:48:30
Last write time: 04/13/2024 15:48:30

Attributes: A
Icons: 0

Mode: Text
Offsets: hexadecimal
Bytes per page: 32x64=2048

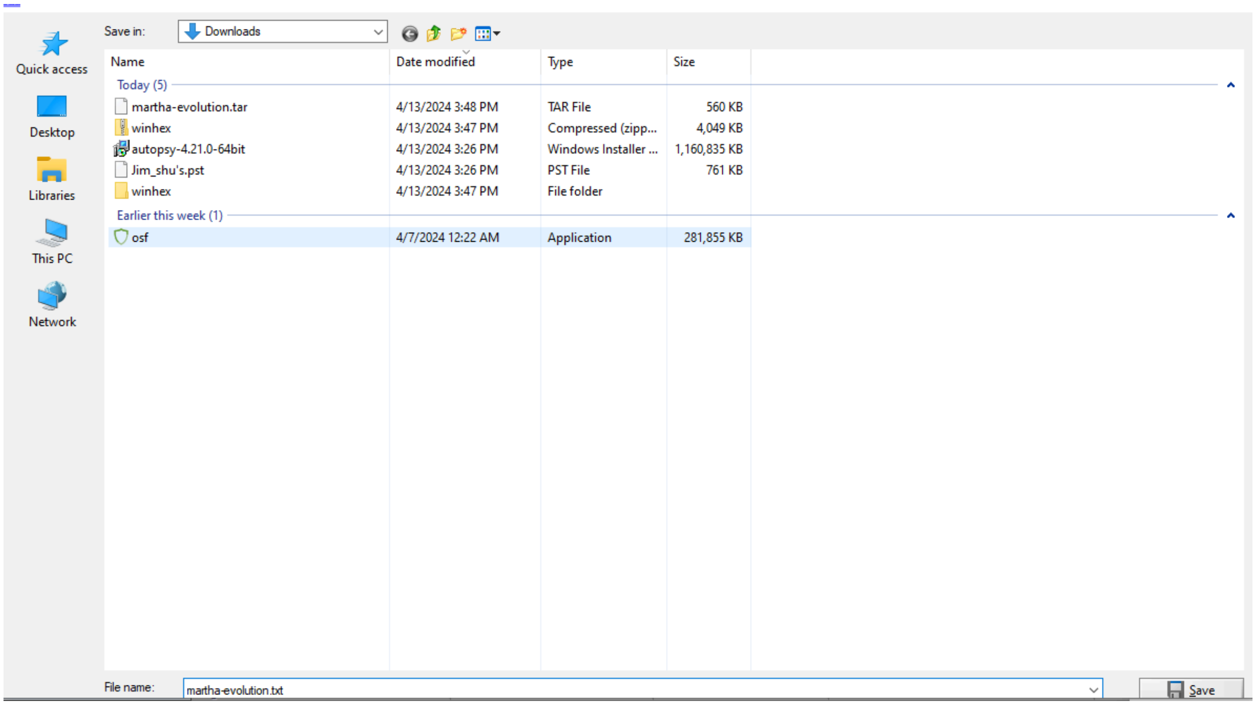
Window #: 1
Window count: 1

Clipboard: available
Path for temp. files: 2.0 GB free

Data Interpreter
8 Bit (±): 46
16 Bit (±): 25,902
32 Bit (±): 1,870,030,126
Binary: 00101110

Page 1 of 280 | Offset: 0 | = 46 | Block: n/a | Size:

In this step, I have downloaded the martha.tar file and opened it in WInhex. I then removed the Hex view.

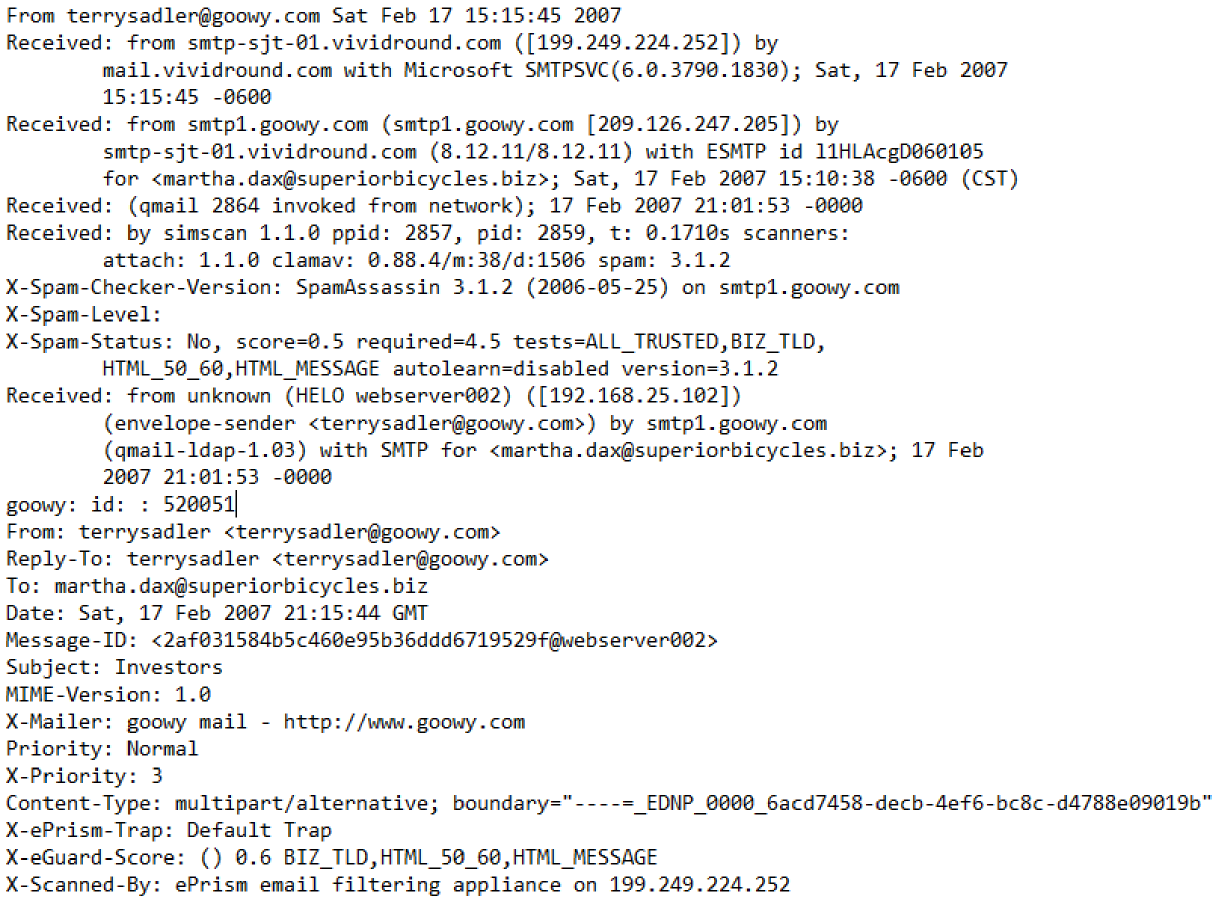


Save in: Downloads

Name	Date modified	Type	Size
Today (5)			
martha-evolution.tar	4/13/2024 3:48 PM	TAR File	560 KB
winhex	4/13/2024 3:47 PM	Compressed (zipp...	4,049 KB
autopsy-4.21.0-64bit	4/13/2024 3:26 PM	Windows Installer ...	1,160,835 KB
Jim_shu's.pst	4/13/2024 3:26 PM	PST File	761 KB
winhex	4/13/2024 3:47 PM	File folder	
Earlier this week (1)			
osf	4/7/2024 12:22 AM	Application	281,855 KB

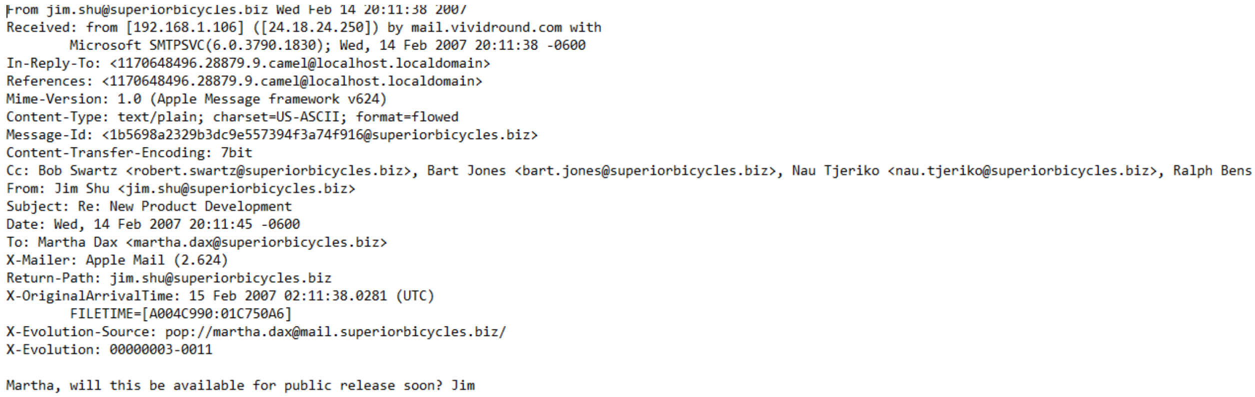
File name: martha-evolution.txt

Here I have copied the email from terrysadler and am saving it to a text file.



```
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 l1HLAcgD060105
        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
X-Scanned-By: ePrism email filtering appliance on 199.249.224.252
```

Here we can see the contents of the txt file.



```
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>
Mime-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>, Nau Tjeriko <nau.tjeriko@superiorbicycles.biz>, Ralph Bens
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
```

Here I have found an email from Jim Shu to Martha. He is asking here if the new product will be released to the public soon. He also seems to have a couple people CC'd.