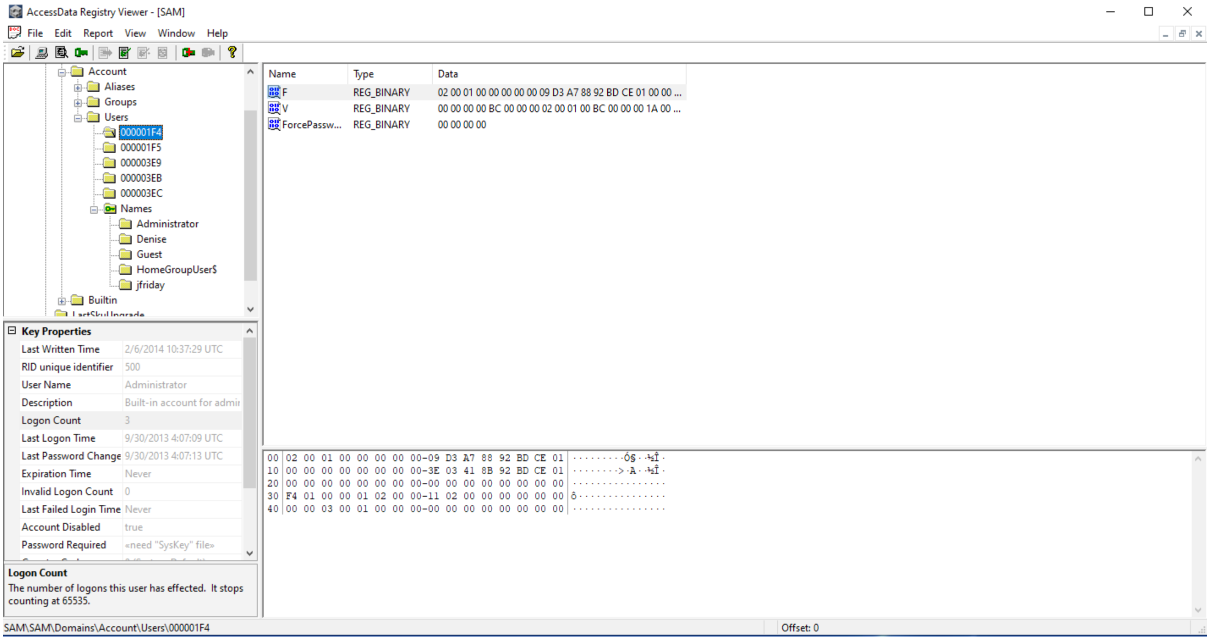
Khushi Gupta 000888120

DFSC 6410 Lab Assignment 2

PART 1

Lab 5.2: Examining the SAM Hive

1. The registry contains how many hives? **5**
2. How many user accounts are disabled? **2**
3. The SAM hive uses PIDs to store information on user accounts. True or False?
   False
4. Name two SID values that indicate whether an account was created automatically.
   500, 501 and 1000
5. The key properties pane in registry viewer shows user accounts have changed their passwords. True or False?
   True



Name	Type	Data
F	REG_BINARY	02 00 01 00 00 00 00 00 09 D3 A7 88 92 BD CE 01 00 00 ...
V	REG_BINARY	00 00 00 00 BC 00 00 00 02 00 01 00 BC 00 00 00 1A 00 ...
ForcePassw...	REG_BINARY	00 00 00 00

Key Properties	
Last Written Time	2/6/2014 10:37:29 UTC
RID unique identifier	500
User Name	Administrator
Description	Built-in account for admir
Logon Count	3
Last Logon Time	9/30/2013 4:07:09 UTC
Last Password Change	9/30/2013 4:07:13 UTC
Expiration Time	Never
Invalid Logon Count	0
Last Failed Login Time	Never
Account Disabled	true
Password Required	«need "SysKey" file»

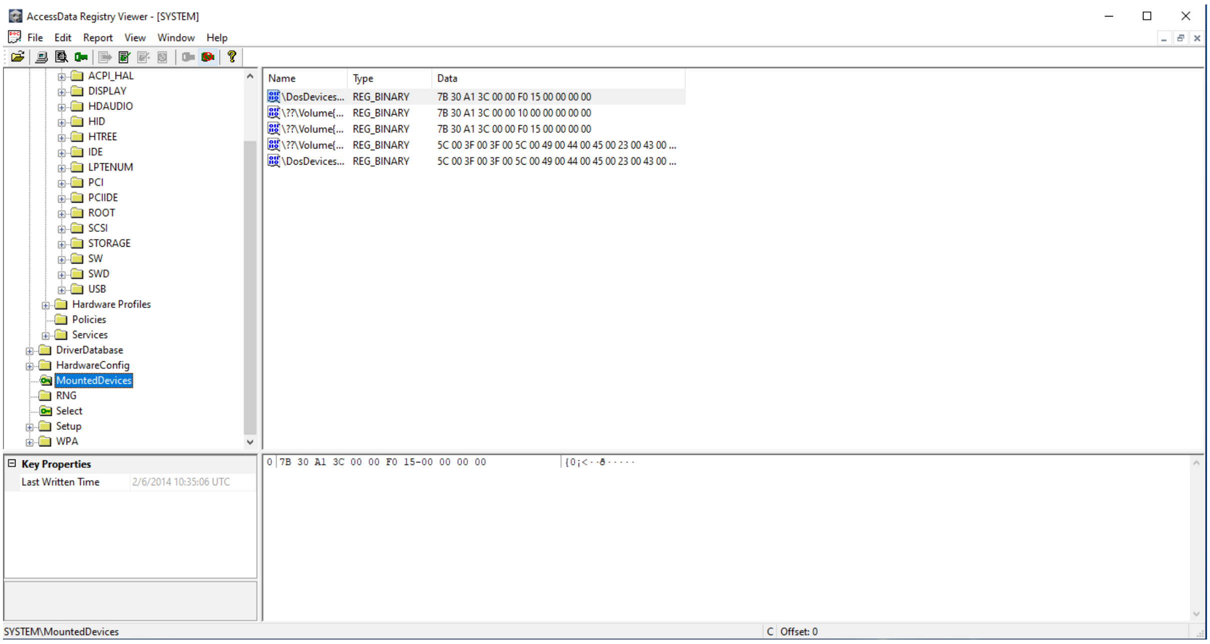
Logon Count
The number of logons this user has effected. It stops counting at 65535.

```
00 | 02 00 01 00 00 00 00 00-09 D3 A7 88 92 BD CE 01 | ········ÓS··½Î·
10 | 00 00 00 00 00 00 00 00-3E 03 41 8B 92 BD CE 01 | ········>·A··½Î·
20 | 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 | ················
30 | F4 01 00 00 01 02 00 00-11 02 00 00 00 00 00 00 | ô···············
40 | 00 00 03 00 01 00 00 00-00 00 00 00 00 00 00 00 | ················
```

SAM\SAM\Domains\Account\Users\000001F4   Offset: 0

Lab 5.3: Examining the SYSTEM Hive

1. What's the computer name of this system? **mnmsrv**
2. What's the time zone setting for this system? **UTC**
3. How many mounted devices on this system have assigned drive letters?
   2
4. What information is stored in the Enum folder?
   Hardware and Software values
5. The SYSTEM hive contains configuration data for passwords. True or False?
   False



Name	Type	Data
\DosDevices...	REG_BINARY	7B 30 A1 3C 00 00 F0 15 00 00 00 00
\??\Volume{...	REG_BINARY	7B 30 A1 3C 00 00 10 00 00 00 00 00
\??\Volume{...	REG_BINARY	7B 30 A1 3C 00 00 F0 15 00 00 00 00
\??\Volume{...	REG_BINARY	5C 00 3F 00 3F 00 5C 00 49 00 44 00 45 00 23 00 43 00 ...
\DosDevices...	REG_BINARY	5C 00 3F 00 3F 00 5C 00 49 00 44 00 45 00 23 00 43 00 ...

⊟ **Key Properties**

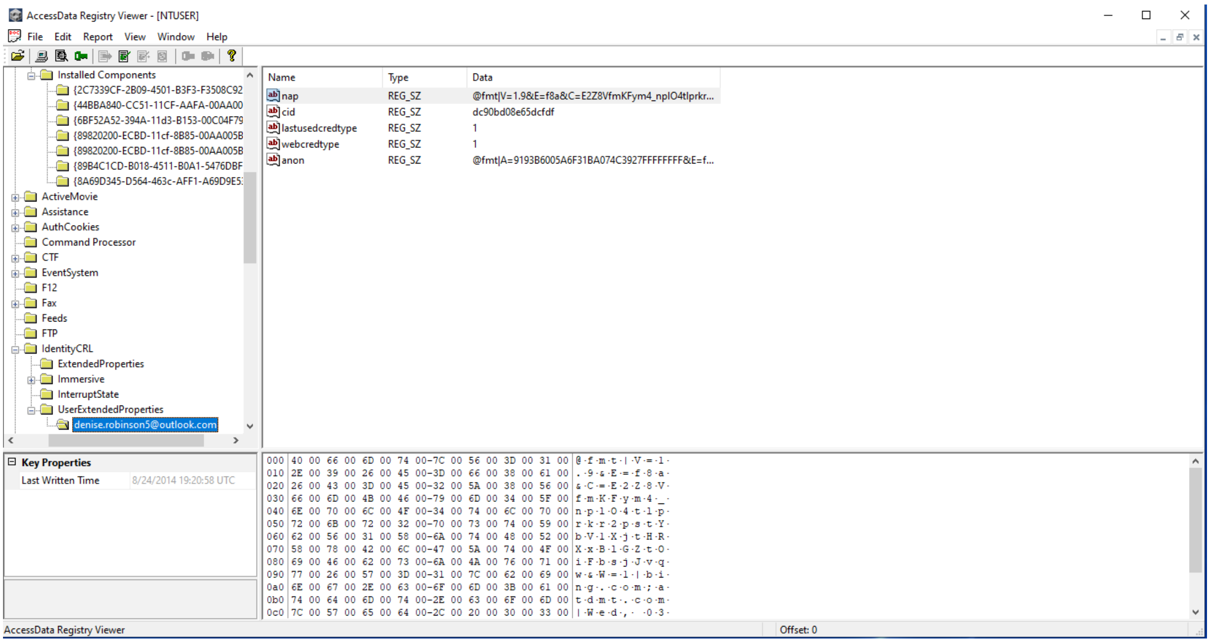
Last Written Time	2/6/2014 10:35:06 UTC

```
0 7B 30 A1 3C 00 00 F0 15-00 00 00 00          {0¡<··ð·····
```

SYSTEM\MountedDevices   C Offset: 0

Lab 5.4: Examining the ntuser.dat registry file

1. The ntuser.dat file contains information on multiple account holders. True or False?
   False
2. What's the email account for the Denise user?
   Denise.robinson5@outlook.com
3. The ntuser.dat file contains information on which of the following?
   Personalized desktop settings
4. Password decryption tools often need which of the following to retrieve user passwords?
   B,c
5. The ntuser.dat file is in which of the following paths?
   C:/Users/username


AccessData Registry Viewer - [NTUSER]
File Edit Report View Window Help

```
Installed Components
    {2C7339CF-2B09-4501-B3F3-F3508C92
    {44BBA840-CC51-11CF-AAFA-00AA00
    {6BF52A52-394A-11d3-B153-00C04F79
    {89820200-ECBD-11cf-8B85-00AA005B
    {89820200-ECBD-11cf-8B85-00AA005B
    {89B4C1CD-B018-4511-B0A1-5476DBF
    {8A69D345-D564-463c-AFF1-A69D9E5:
ActiveMovie
Assistance
AuthCookies
Command Processor
CTF
EventSystem
F12
Fax
Feeds
FTP
IdentityCRL
    ExtendedProperties
    Immersive
    InterruptState
    UserExtendedProperties
        denise.robinson5@outlook.com
```

Name	Type	Data
nap	REG_SZ	@fmt|V=1.9&E=f8a&C=E2Z8VfmKFym4_nplO4tlprkr...
cid	REG_SZ	dc90bd08e65dcfdf
lastusedcredtype	REG_SZ	1
webcredtype	REG_SZ	1
anon	REG_SZ	@fmt|A=9193B6005A6F31BA074C3927FFFFFFFF&E=f...

Key Properties

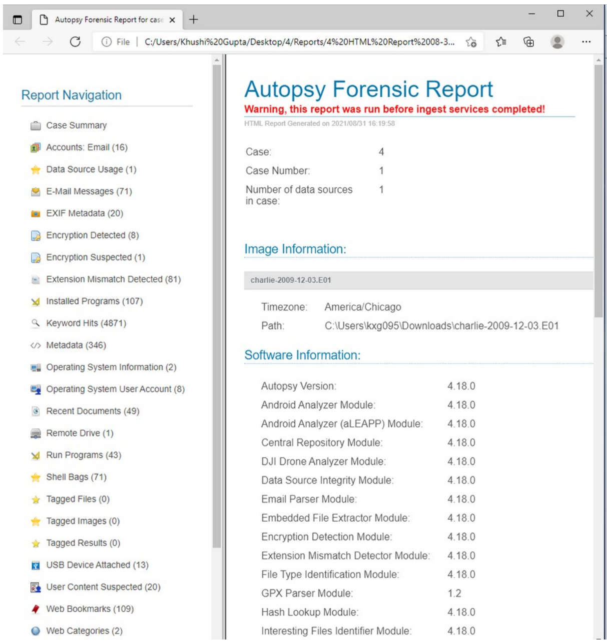
Last Written Time 8/24/2014 19:20:58 UTC

```
000 40 00 66 00 6D 00 74 00-7C 00 56 00 3D 00 31 00 @·f·m·t·|·V·=·1·
010 2E 00 39 00 26 00 45 00-3D 00 66 00 38 00 61 00 .·9·&·E·=·f·8·a·
020 26 00 43 00 3D 00 45 00-32 00 5A 00 38 00 56 00 &·C·=·E·2·Z·8·V·
030 66 00 6D 00 4B 00 46 00-79 00 6D 00 34 00 5F 00 f·m·K·F·y·m·4·_·
040 6E 00 70 00 6C 00 4F 00-34 00 74 00 6C 00 70 00 n·p·l·O·4·t·l·p·
050 72 00 6B 00 72 00 32 00-70 00 73 00 74 00 59 00 r·k·r·2·p·s·t·Y·
060 62 00 56 00 31 00 58 00-6A 00 74 00 48 00 52 00 b·V·1·X·j·t·H·R·
070 58 00 78 00 42 00 6C 00-47 00 5A 00 74 00 4F 00 X·x·B·l·G·Z·t·O·
080 69 00 46 00 62 00 73 00-6A 00 4A 00 76 00 71 00 i·F·b·s·j·J·v·q·
090 77 00 26 00 57 00 3D 00-31 00 7C 00 62 00 69 00 w·&·W·=·1·|·b·i·
0a0 6E 00 67 00 2E 00 63 00-6F 00 6D 00 3B 00 61 00 n·g·.·c·o·m·;·a·
0b0 74 00 64 00 6D 00 74 00-2E 00 63 00 6F 00 6D 00 t·d·m·t·.·c·o·m·
0c0 7C 00 57 00 65 00 64 00-2C 00 20 00 30 00 33 00 |·W·e·d·,· ·0·3·
```

PART 2

Lab 6.1: Using the Autopsy to Search an Image of a Hard Drive

1. How many e-mails did Charlie get? 10
2. How many e-mails did Charlie send? 24
3. What tools did Charlie search for on the web? Hex editor, python and steganography tool free
4. Did Charlie install any tools on this computer? Python
5. How many cameras can be identified by checking the Exif information?


Autopsy Forensic Report for case
File | C:/Users/Khushi%20Gupta/Desktop/4/Reports/4%20HTML%20Report%2008-3...

Report Navigation

- Case Summary
- Accounts: Email (16)
- Data Source Usage (1)
- E-Mail Messages (71)
- EXIF Metadata (20)
- Encryption Detected (8)
- Encryption Suspected (1)
- Extension Mismatch Detected (81)
- Installed Programs (107)
- Keyword Hits (4871)
- Metadata (346)
- Operating System Information (2)
- Operating System User Account (8)
- Recent Documents (49)
- Remote Drive (1)
- Run Programs (43)
- Shell Bags (71)
- Tagged Files (0)
- Tagged Images (0)
- Tagged Results (0)
- USB Device Attached (13)
- User Content Suspected (20)
- Web Bookmarks (109)
- Web Categories (2)

Autopsy Forensic Report

Warning, this report was run before ingest services completed!

HTML Report Generated on 2021/08/31 16:19:58

Case:	4
Case Number:	1
Number of data sources in case:	1

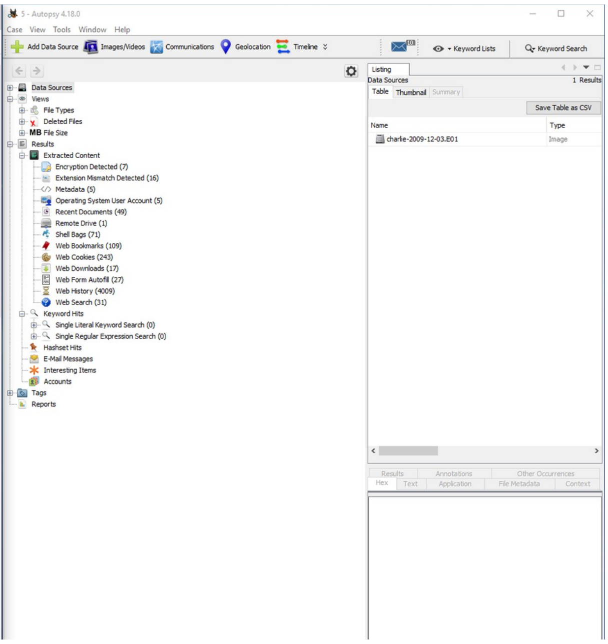
Image Information:

charlie-2009-12-03.E01

Timezone:	America/Chicago
Path:	C:\Users\kxg095\Downloads\charlie-2009-12-03.E01

Software Information:

Autopsy Version:	4.18.0
Android Analyzer Module:	4.18.0
Android Analyzer (aLEAPP) Module:	4.18.0
Central Repository Module:	4.18.0
DJI Drone Analyzer Module:	4.18.0
Data Source Integrity Module:	4.18.0
Email Parser Module:	4.18.0
Embedded File Extractor Module:	4.18.0
Encryption Detection Module:	4.18.0
Extension Mismatch Detector Module:	4.18.0
File Type Identification Module:	4.18.0
GPX Parser Module:	1.2
Hash Lookup Module:	4.18.0
Interesting Files Identifier Module:	4.18.0



```
Data Sources
Views
    File Types
    Deleted Files
    MB File Size
Results
    Extracted Content
        Encryption Detected (7)
        Extension Mismatch Detected (16)
        Metadata (5)
        Operating System User Account (5)
        Recent Documents (49)
        Remote Drive (1)
        Shell Bags (71)
        Web Bookmarks (109)
        Web Cookies (243)
        Web Downloads (17)
        Web Form Autofill (27)
        Web History (4009)
        Web Search (31)
    Keyword Hits
        Single Literal Keyword Search (0)
        Single Regular Expression Search (0)
    Hashset Hits
    E-Mail Messages
    Interesting Items
    Accounts
Tags
Reports
```

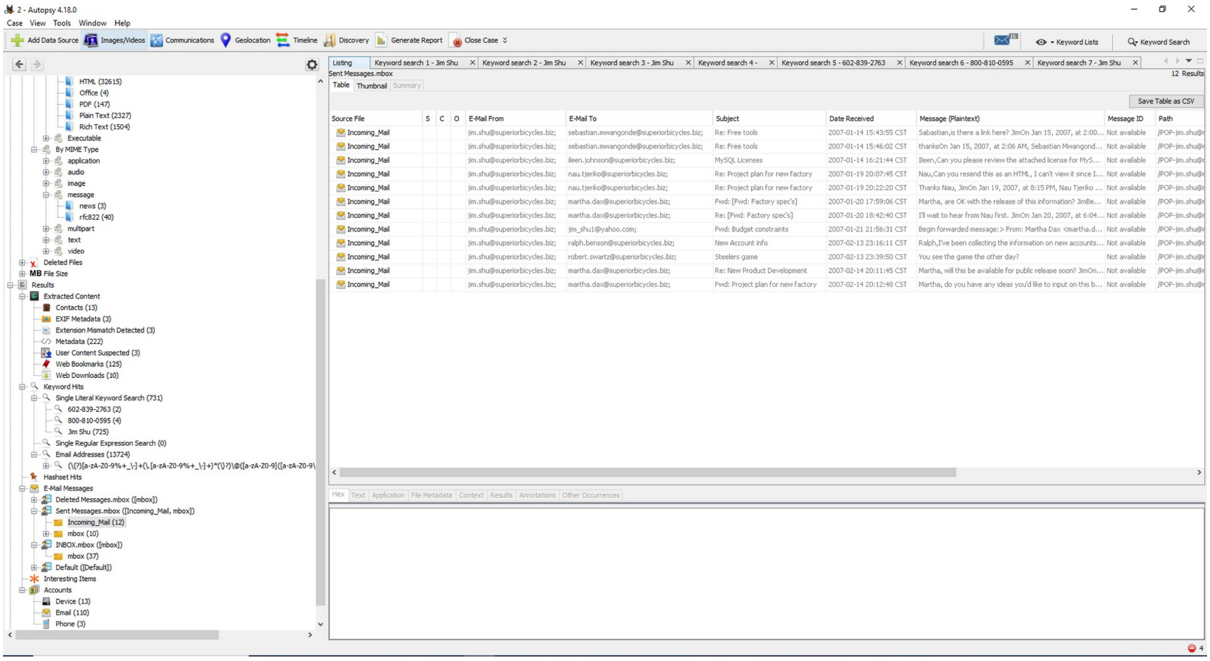
Data Sources 1 Results

Name	Type
charlie-2009-12-03.E01	Image

Khushi Gupta 000888120

Lab 7.1: Using Autopsy to process a Mac OS X Image

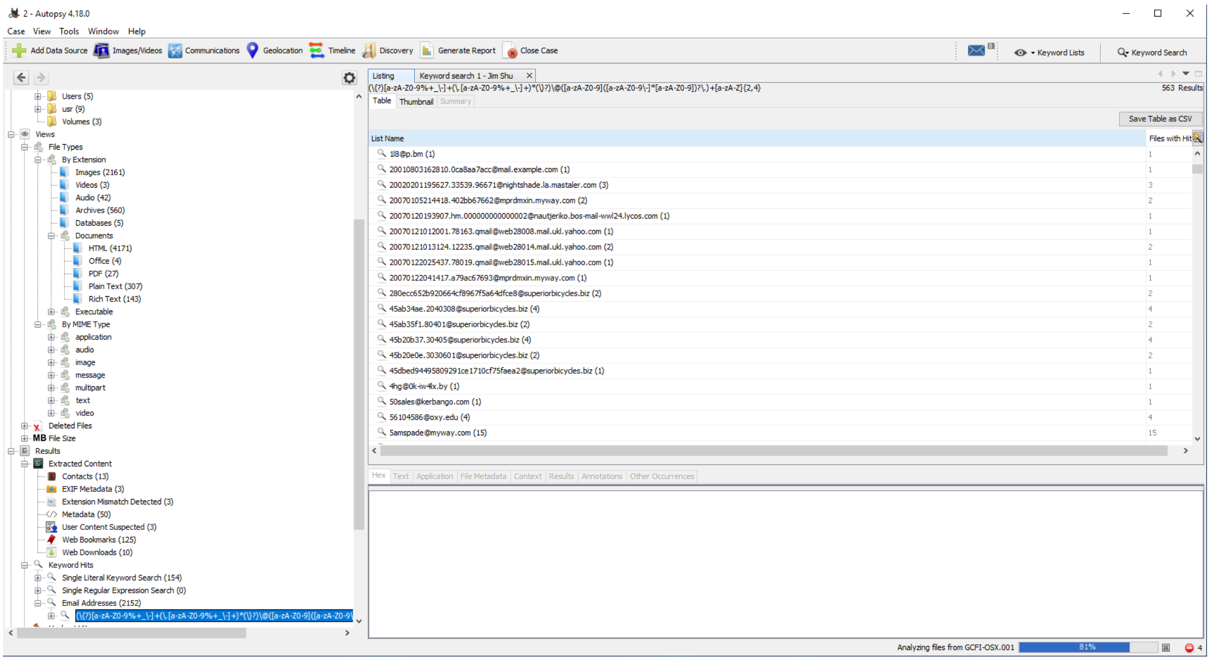
1. How many Word files are in the image? 4
2. What or who is the subject of the first message from Jim Shu? D
3. What phone number had the most search results? B
4. The Ext3 file system is used in Mac OS X. True or False? False
5. Who sent the last e-mail to Jim Shu? A



Sent Messages.mbox

12 Results

Source File	S	C	O	E-Mail From	E-Mail To	Subject	Date Received	Message (Plaintext)	Message ID	Path
Incoming_Mail				jim.shu@superiorbicycles.biz;	sebastian.mwangonde@superiorbicycles.biz;	Re: Free tools	2007-01-14 15:43:55 CST	Sabastian,is there a link here? JimOn Jan 15, 2007, at 2:00...	Not available	/POP-jim.shu@
Incoming_Mail				jim.shu@superiorbicycles.biz;	sebastian.mwangonde@superiorbicycles.biz;	Re: Free tools	2007-01-14 15:46:02 CST	thanksOn Jan 15, 2007, at 2:06 AM, Sebastian Mwangond...	Not available	/POP-jim.shu@
Incoming_Mail				jim.shu@superiorbicycles.biz;	ileen.johnson@superiorbicycles.biz;	MySQL Licenses	2007-01-14 16:21:44 CST	Ileen,Can you please review the attached license for MyS...	Not available	/POP-jim.shu@
Incoming_Mail				jim.shu@superiorbicycles.biz;	nau.tjeriko@superiorbicycles.biz;	Re: Project plan for new factory	2007-01-19 20:07:45 CST	Nau,Can you resend this as an HTML, I can't view it since I...	Not available	/POP-jim.shu@
Incoming_Mail				jim.shu@superiorbicycles.biz;	nau.tjeriko@superiorbicycles.biz;	Re: Project plan for new factory	2007-01-19 20:22:20 CST	Thanks Nau, JimOn Jan 19, 2007, at 8:15 PM, Nau Tjeriko ...	Not available	/POP-jim.shu@
Incoming_Mail				jim.shu@superiorbicycles.biz;	martha.dax@superiorbicycles.biz;	Fwd: [Fwd: Factory spec's]	2007-01-20 17:59:06 CST	Martha, are OK with the release of this information? JimBe...	Not available	/POP-jim.shu@
Incoming_Mail				jim.shu@superiorbicycles.biz;	martha.dax@superiorbicycles.biz;	Re: [Fwd: Factory spec's]	2007-01-20 18:42:40 CST	I'll wait to hear from Nau first. JimOn Jan 20, 2007, at 6:04...	Not available	/POP-jim.shu@
Incoming_Mail				jim.shu@superiorbicycles.biz;	jim_shu1@yahoo.com;	Fwd: Budget constraints	2007-01-21 21:56:31 CST	Begin forwarded message:> From: Martha Dax <martha.d...	Not available	/POP-jim.shu@
Incoming_Mail				jim.shu@superiorbicycles.biz;	ralph.benson@superiorbicycles.biz;	New Account info	2007-02-13 23:16:11 CST	Ralph,I've been collecting the information on new accounts...	Not available	/POP-jim.shu@
Incoming_Mail				jim.shu@superiorbicycles.biz;	robert.swartz@superiorbicycles.biz;	Steelers game	2007-02-13 23:39:50 CST	You see the game the other day?	Not available	/POP-jim.shu@
Incoming_Mail				jim.shu@superiorbicycles.biz;	martha.dax@superiorbicycles.biz;	Re: New Product Development	2007-02-14 20:11:45 CST	Martha, will this be available for public release soon? JimOn...	Not available	/POP-jim.shu@
Incoming_Mail				jim.shu@superiorbicycles.biz;	martha.dax@superiorbicycles.biz;	Fwd: Project plan for new factory	2007-02-14 20:12:48 CST	Martha, do you have any ideas you'd like to input on this b...	Not available	/POP-jim.shu@



(\{?)[a-zA-Z0-9%+_\-]+(\.[a-zA-Z0-9%+_\-]+)*(\}?)\@([a-zA-Z0-9]([a-zA-Z0-9\-]*[a-zA-Z0-9])?\.)+[a-zA-Z]{2,4}

563 Results

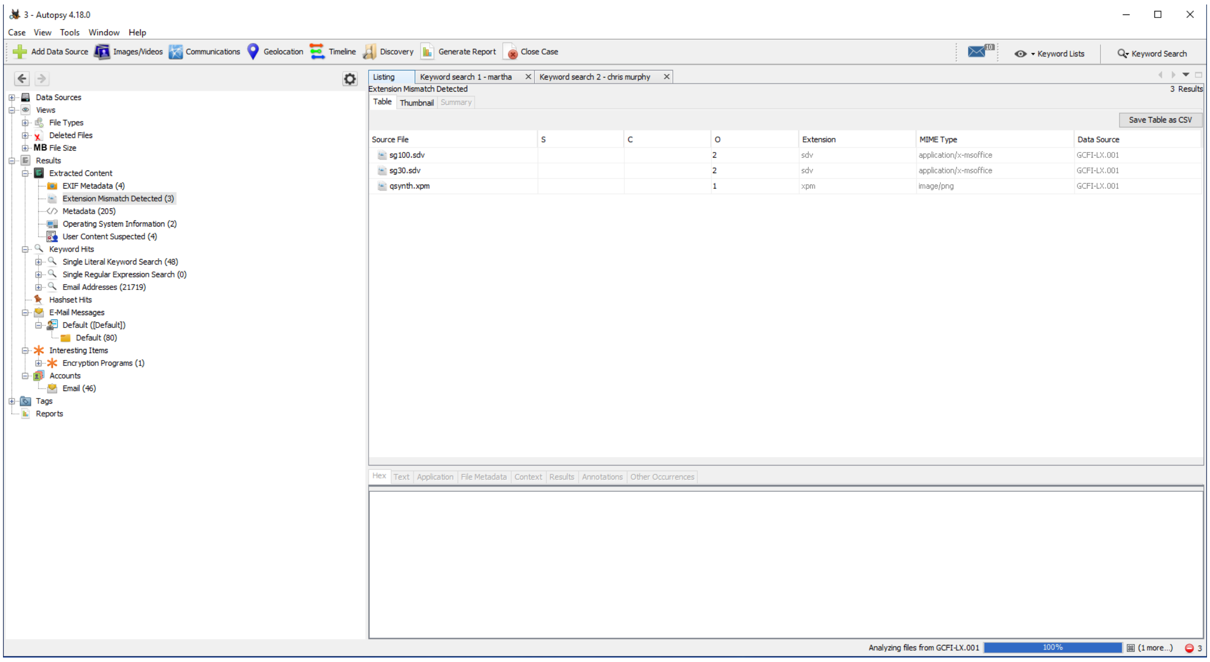
List Name	Files with Hit
1l8@p.bm (1)	1
20010803162810.0ca8aa7acc@mail.example.com (1)	1
20020201195627.33539.96671@nightshade.la.mastaler.com (3)	3
20070105214418.402bb67662@mprdmxin.myway.com (2)	2
20070120193907.hm.000000000000002@nautjeriko.bos-mail-wwl24.lycos.com (1)	1
20070121012001.78163.qmail@web28008.mail.ukl.yahoo.com (1)	1
20070121013124.12235.qmail@web28014.mail.ukl.yahoo.com (2)	2
20070122025437.78019.qmail@web28015.mail.ukl.yahoo.com (1)	1
20070122041417.a79ac67693@mprdmxin.myway.com (1)	1
280ecc652b920664cf8967f5a64dfce8@superiorbicycles.biz (2)	2
45ab34ae.2040308@superiorbicycles.biz (4)	4
45ab35f1.80401@superiorbicycles.biz (2)	2
45b20b37.30405@superiorbicycles.biz (4)	4
45b20e0e.3030601@superiorbicycles.biz (2)	2
45dbed94495809291ce1710cf75faea2@superiorbicycles.biz (1)	1
4hg@0k-iw4lx.by (1)	1
50sales@kerbango.com (1)	1
56104586@oxy.edu (4)	4
5amspade@myway.com (15)	15

Analyzing files from GCFI-OSX.001 81%

Lab 7.3: Using Autopsy to process a Linux Image

1. How many emails were recovered from the inbox? 80
2. How many word and excel files were recovered in this image? 13
3. Martha communicated via email only with Chris Murphy. True or False? False

4. What executable file was recovered in this image? 33
5. How many matches were found for the Martha Keyword? 38



Data Sources
Views
File Types
Deleted Files
MB File Size
Results
Extracted Content
EXIF Metadata (4)
Extension Mismatch Detected (3)
Metadata (205)
Operating System Information (2)
User Content Suspected (4)
Keyword Hits
Single Literal Keyword Search (48)
Single Regular Expression Search (0)
Email Addresses (21719)
Hashset Hits
E-Mail Messages
Default ([Default])
Default (80)
Interesting Items
Encryption Programs (1)
Accounts
Email (46)
Tags
Reports

Extension Mismatch Detected

3 Results

Source File	S	C	O	Extension	MIME Type	Data Source
sg100.sdv			2	sdv	application/x-msoffice	GCFI-LX.001
sg30.sdv			2	sdv	application/x-msoffice	GCFI-LX.001
qsynth.xpm			1	xpm	image/png	GCFI-LX.001

Analyzing files from GCFI-LX.001 100% (1 more...) 3