ITIS 5250
Sneha Rangari
Lab 6
11/25/2018

Overview:

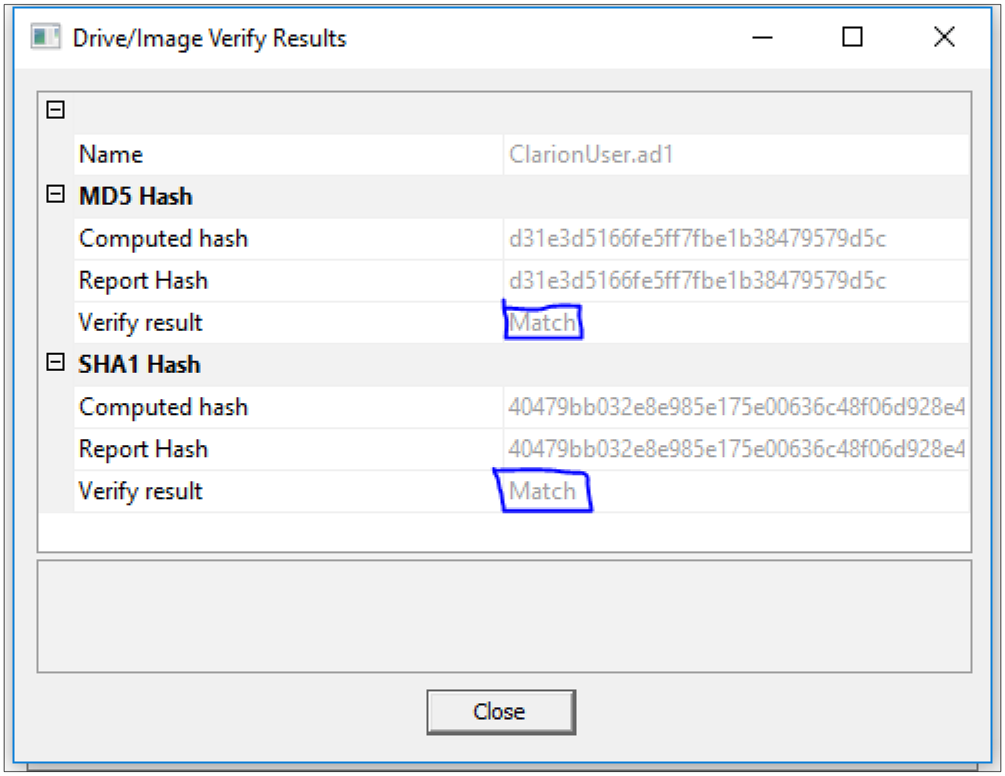
In this Lab, I have been given six files including three AD1 files namely MonarchUser.ad1, Monarch2User.ad1 and ClarionUser.ad1 and three e01 files namely Monarch.e01', 'Monarch2.e01', 'Clarion.e01'. I have been asked to make use of the "FTK Tool" along with "FTK Imager Tool" and "PRTK" and gather certain shreds of evidence such as email address, email conversations, passwords and photographs from the images provided. Also, I have been asked to find items like bombs, explosives, drones, etc.

Forensic Acquisition & Exam Preparation:

I accessed the Forensic images in the Shared Folder on the network from the Forensics Lab in Cone 169. I accessed images named 'Monarch.e01', 'Monarch2.e01', 'Clarion.e01', 'MonarchUser.ad1', 'Monarch2User.ad1' and 'ClarionUser.ad1'. Later, I loaded these images using FTK Imager. The software used for accessing & extracting information from the image is FTK Imager 4.1.1.1. The first step undertaken after accessing the image files was the Hash verification along with description of image from txt file and verified their integrity.

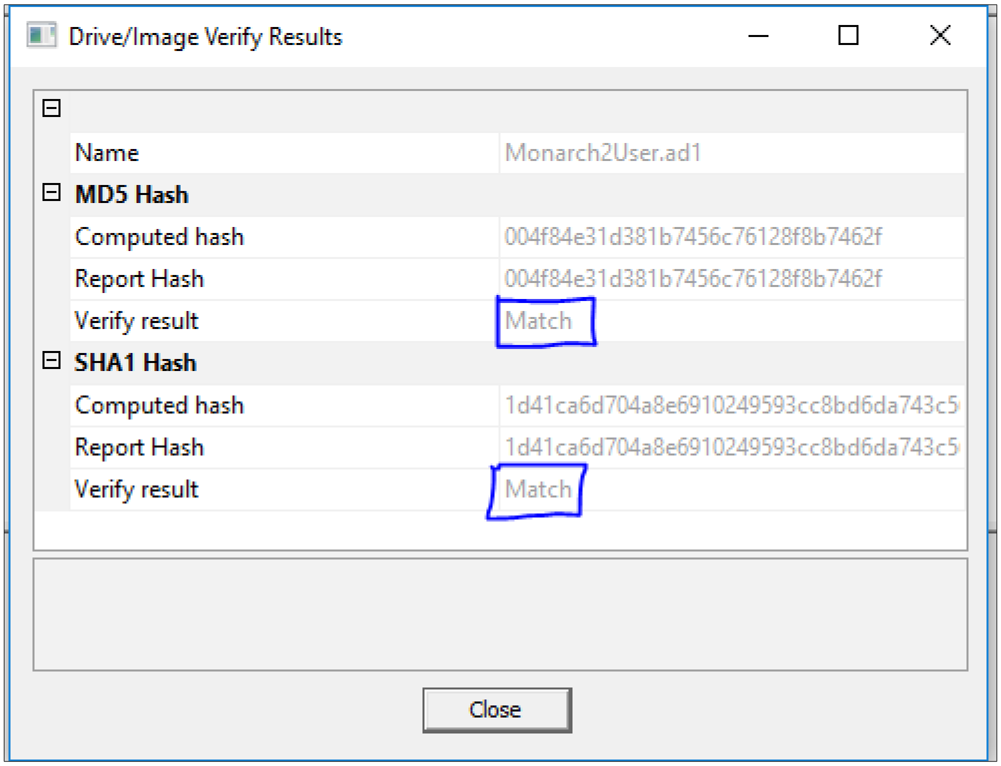
Later, I loaded these images using FTK Imager and verified their **integrity**.

For All AD1:



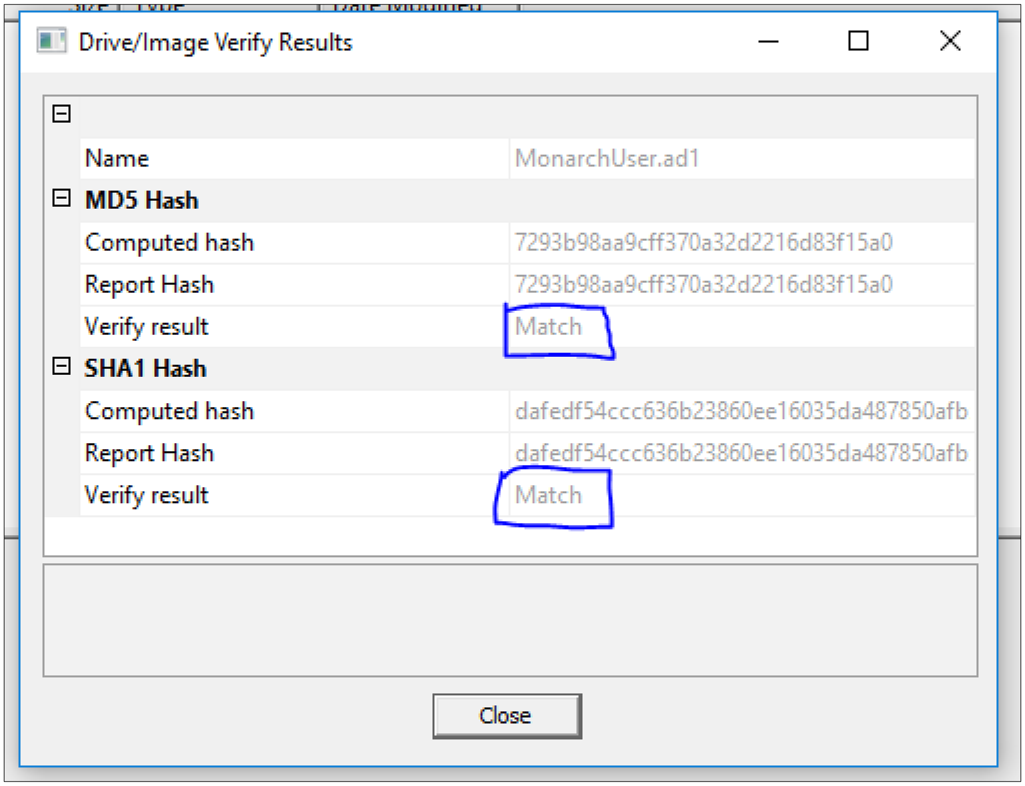
Drive/Image Verify Results

Name	ClarionUser.ad1
MD5 Hash	
Computed hash	d31e3d5166fe5ff7fbe1b38479579d5c
Report Hash	d31e3d5166fe5ff7fbe1b38479579d5c
Verify result	Match
SHA1 Hash	
Computed hash	40479bb032e8e985e175e00636c48f06d928e4
Report Hash	40479bb032e8e985e175e00636c48f06d928e4
Verify result	Match



Drive/Image Verify Results

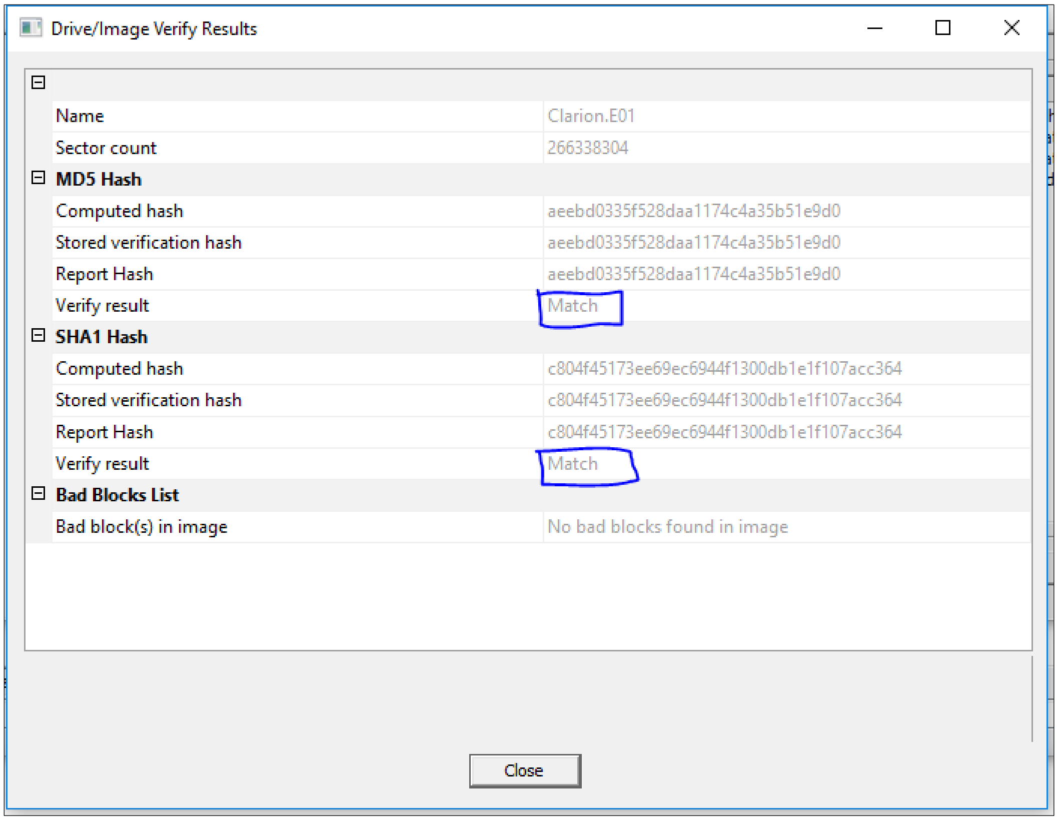
Name	Monarch2User.ad1
MD5 Hash	
Computed hash	004f84e31d381b7456c76128f8b7462f
Report Hash	004f84e31d381b7456c76128f8b7462f
Verify result	Match
SHA1 Hash	
Computed hash	1d41ca6d704a8e6910249593cc8bd6da743c5
Report Hash	1d41ca6d704a8e6910249593cc8bd6da743c5
Verify result	Match



Drive/Image Verify Results

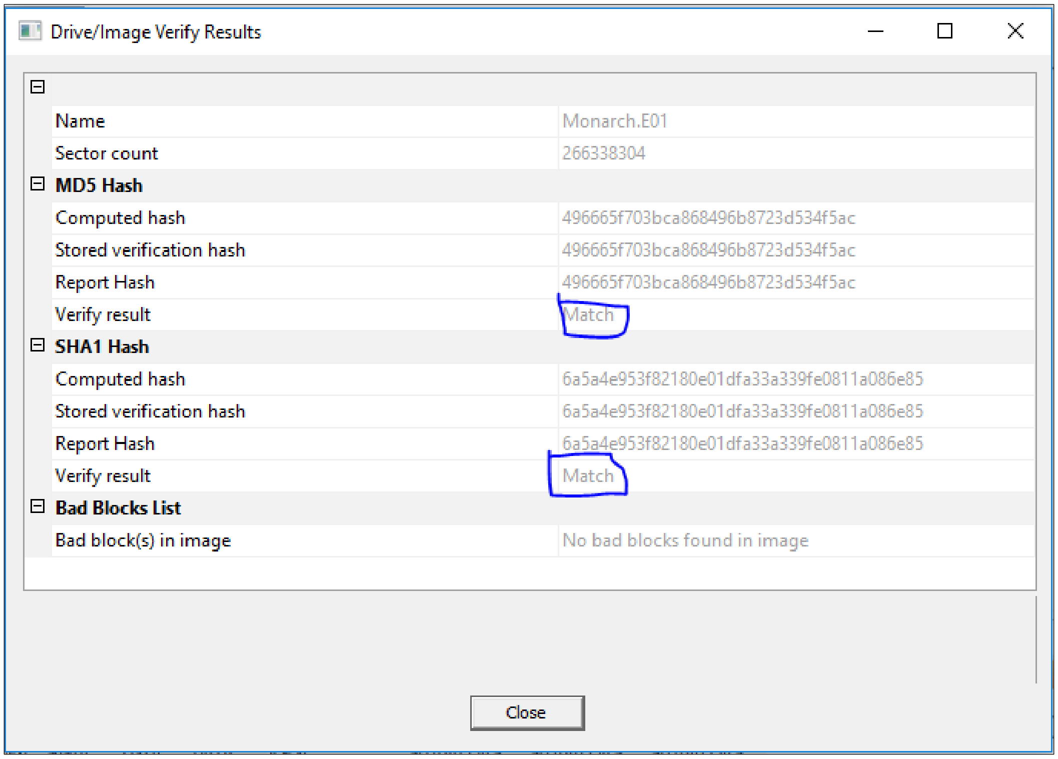
Name	MonarchUser.ad1
MD5 Hash	
Computed hash	7293b98aa9cff370a32d2216d83f15a0
Report Hash	7293b98aa9cff370a32d2216d83f15a0
Verify result	Match
SHA1 Hash	
Computed hash	dafedf54ccc636b23860ee16035da487850afb
Report Hash	dafedf54ccc636b23860ee16035da487850afb
Verify result	Match

For All E01:



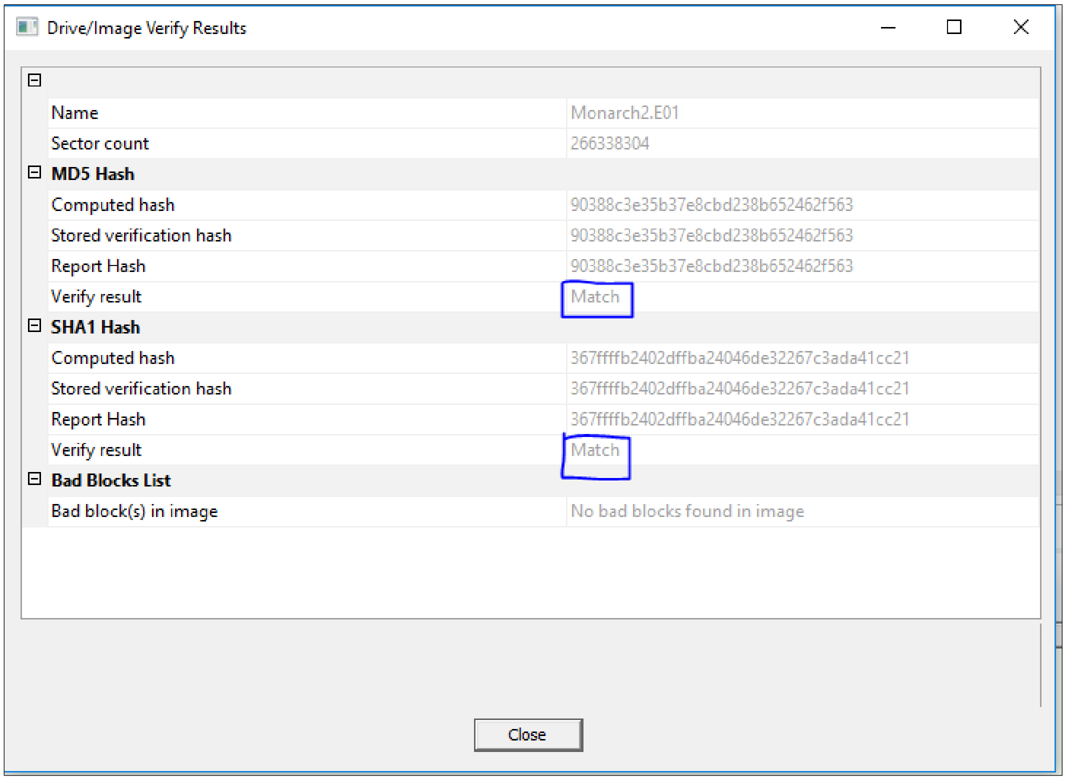
Drive/Image Verify Results

⊟	
Name	Clarion.E01
Sector count	266338304
⊟ **MD5 Hash**	
Computed hash	aeebd0335f528daa1174c4a35b51e9d0
Stored verification hash	aeebd0335f528daa1174c4a35b51e9d0
Report Hash	aeebd0335f528daa1174c4a35b51e9d0
Verify result	Match
⊟ **SHA1 Hash**	
Computed hash	c804f45173ee69ec6944f1300db1e1f107acc364
Stored verification hash	c804f45173ee69ec6944f1300db1e1f107acc364
Report Hash	c804f45173ee69ec6944f1300db1e1f107acc364
Verify result	Match
⊟ **Bad Blocks List**	
Bad block(s) in image	No bad blocks found in image



Drive/Image Verify Results

⊟	
Name	Monarch.E01
Sector count	266338304
⊟ **MD5 Hash**	
Computed hash	496665f703bca868496b8723d534f5ac
Stored verification hash	496665f703bca868496b8723d534f5ac
Report Hash	496665f703bca868496b8723d534f5ac
Verify result	Match
⊟ **SHA1 Hash**	
Computed hash	6a5a4e953f82180e01dfa33a339fe0811a086e85
Stored verification hash	6a5a4e953f82180e01dfa33a339fe0811a086e85
Report Hash	6a5a4e953f82180e01dfa33a339fe0811a086e85
Verify result	Match
⊟ **Bad Blocks List**	
Bad block(s) in image	No bad blocks found in image



Drive/Image Verify Results

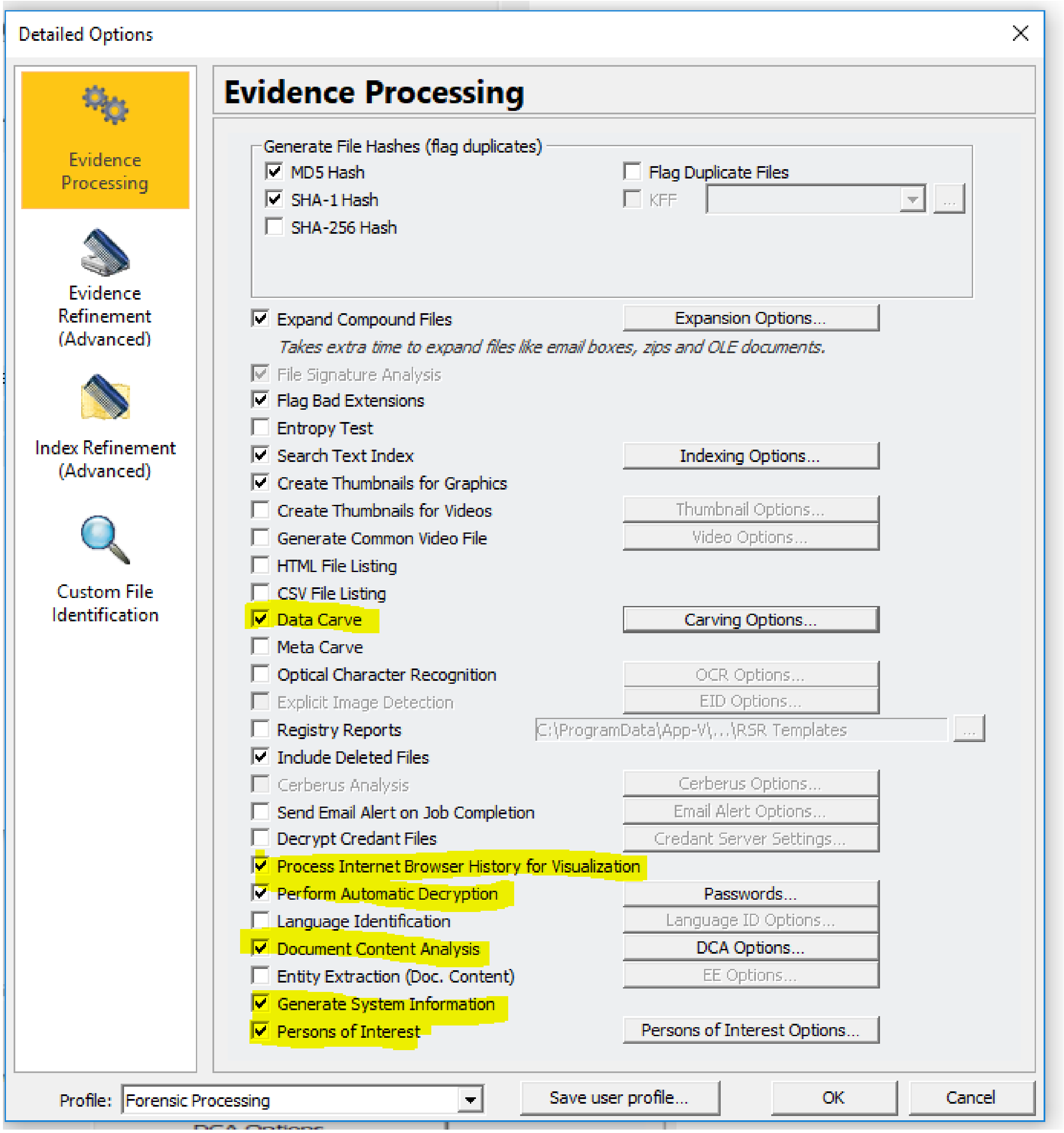
Name	Monarch2.E01
Sector count	266338304
MD5 Hash	
Computed hash	90388c3e35b37e8cbd238b652462f563
Stored verification hash	90388c3e35b37e8cbd238b652462f563
Report Hash	90388c3e35b37e8cbd238b652462f563
Verify result	Match
SHA1 Hash	
Computed hash	367ffffb2402dffba24046de32267c3ada41cc21
Stored verification hash	367ffffb2402dffba24046de32267c3ada41cc21
Report Hash	367ffffb2402dffba24046de32267c3ada41cc21
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

The above results show that these images were not tampered and then using FTK. I customized processing profile by adding options:

- Data Carve
- Process Internet Browser History for visualization
- Perform Automatic decryption
- Document content analysis
- Entity Extraction
- General System Information
- Persons of Interest

In Carving options, I selected all types to Carve.

I processed them as shown:


Detailed Options
Evidence Processing
Evidence Refinement (Advanced)
Index Refinement (Advanced)
Custom File Identification

Evidence Processing

Generate File Hashes (flag duplicates)

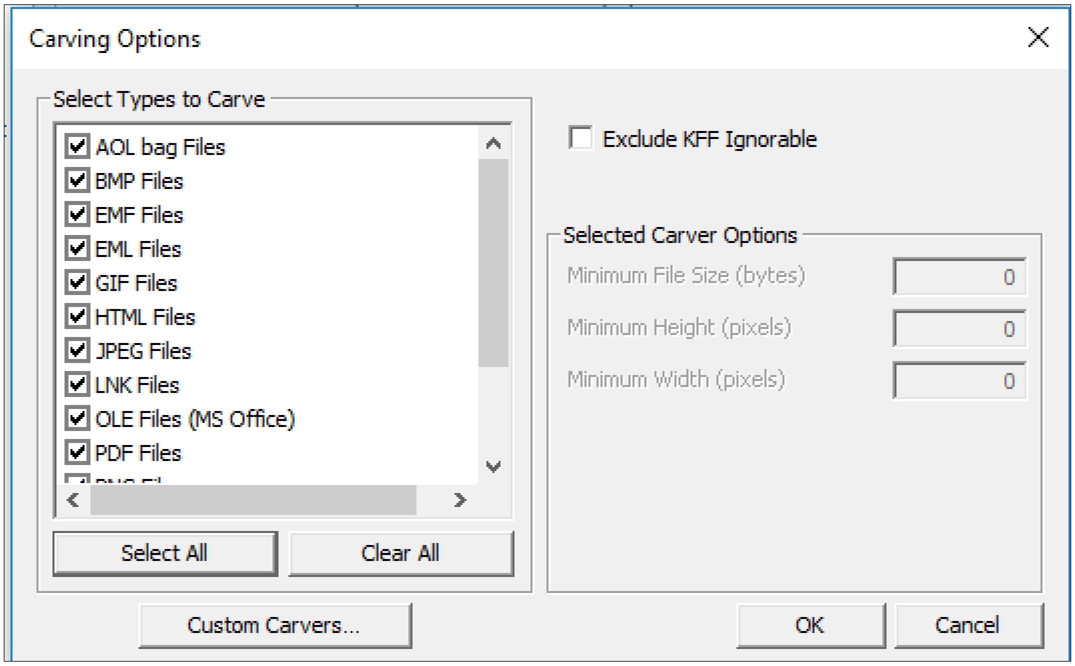
☑ MD5 Hash
☑ SHA-1 Hash
☐ SHA-256 Hash
☐ Flag Duplicate Files
☐ KFF

☑ Expand Compound Files

Takes extra time to expand files like email boxes, zips and OLE documents.

☑ File Signature Analysis
☑ Flag Bad Extensions
☐ Entropy Test
☑ Search Text Index
☑ Create Thumbnails for Graphics
☐ Create Thumbnails for Videos
☐ Generate Common Video File
☐ HTML File Listing
☐ CSV File Listing
☑ Data Carve
☐ Meta Carve
☐ Optical Character Recognition
☐ Explicit Image Detection
☐ Registry Reports — C:\ProgramData\App-V\...\RSR Templates
☑ Include Deleted Files
☐ Cerberus Analysis
☐ Send Email Alert on Job Completion
☐ Decrypt Credant Files
☑ Process Internet Browser History for Visualization
☑ Perform Automatic Decryption
☐ Language Identification
☑ Document Content Analysis
☐ Entity Extraction (Doc. Content)
☑ Generate System Information
☑ Persons of Interest

Profile: Forensic Processing



Carving Options

Select Types to Carve

☑ AOL bag Files
☑ BMP Files
☑ EMF Files
☑ EML Files
☑ GIF Files
☑ HTML Files
☑ JPEG Files
☑ LNK Files
☑ OLE Files (MS Office)
☑ PDF Files

☐ Exclude KFF Ignorable

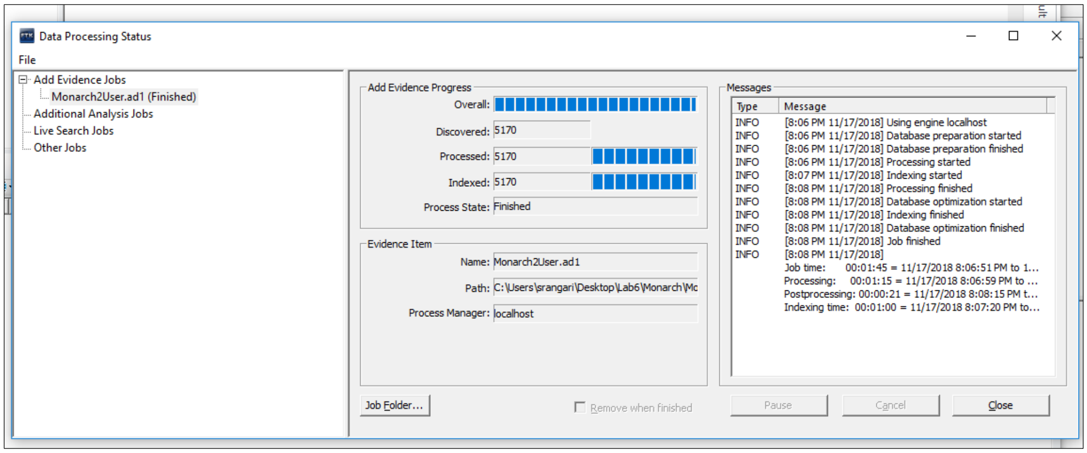
Selected Carver Options

Minimum File Size (bytes): 0
Minimum Height (pixels): 0
Minimum Width (pixels): 0

Findings and Report (Forensic Analysis)

1. Who is the Guild’s operative? Can you identify any pictures of this person?

From Monarch2User.ad1 file:



Data Processing Status

File

- Add Evidence Jobs
  - Monarch2User.ad1 (Finished)
- Additional Analysis Jobs
- Live Search Jobs
- Other Jobs

Add Evidence Progress

Overall:
Discovered: 5170
Processed: 5170
Indexed: 5170
Process State: Finished

Evidence Item

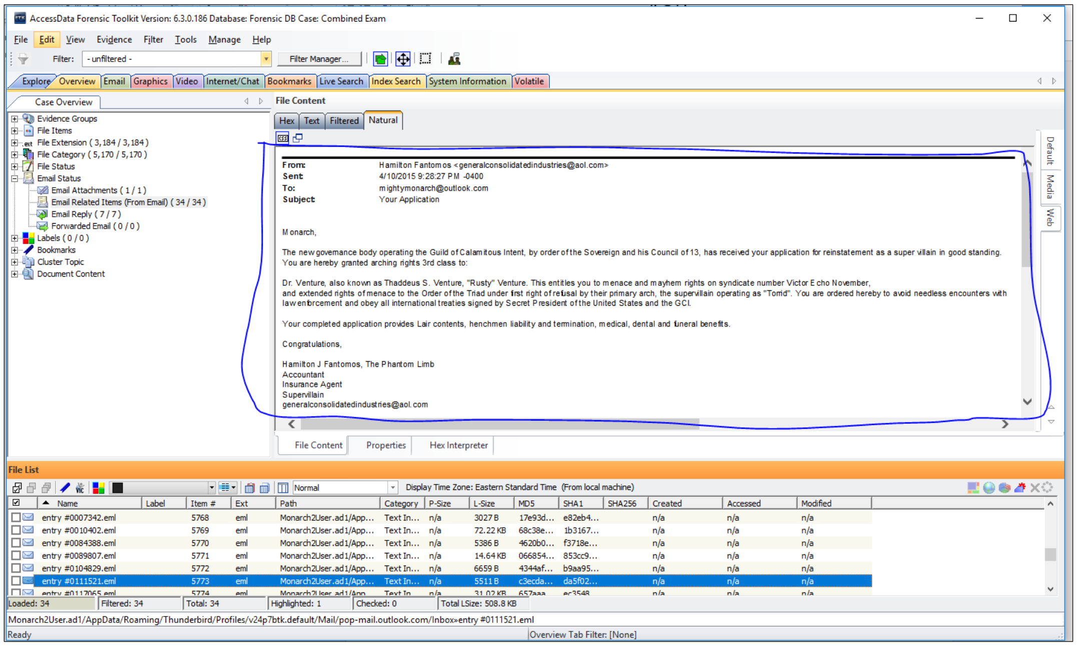
Name: Monarch2User.ad1
Path: C:\Users\srangari\Desktop\Lab6\Monarch\Mc
Process Manager: localhost

Messages

```
Type   Message
INFO   [8:06 PM 11/17/2018] Using engine localhost
INFO   [8:06 PM 11/17/2018] Database preparation started
INFO   [8:06 PM 11/17/2018] Database preparation finished
INFO   [8:06 PM 11/17/2018] Processing started
INFO   [8:07 PM 11/17/2018] Indexing started
INFO   [8:08 PM 11/17/2018] Processing finished
INFO   [8:08 PM 11/17/2018] Database optimization started
INFO   [8:08 PM 11/17/2018] Indexing finished
INFO   [8:08 PM 11/17/2018] Database optimization finished
INFO   [8:08 PM 11/17/2018] Job finished
INFO   [8:08 PM 11/17/2018]
       Job time:       00:01:45 = 11/17/2018 8:06:51 PM to 1...
       Processing:     00:01:15 = 11/17/2018 8:06:59 PM to ...
       Postprocessing: 00:00:21 = 11/17/2018 8:08:15 PM t...
       Indexing time:  00:01:00 = 11/17/2018 8:07:20 PM to...
```

☐ Remove when finished

In “Overview tab” in email status I found the email conversation showing that the Guild’s operative is **Hamilton Fantomos**.


AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Combined Exam
File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered -
Filter Manager...
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
Case Overview
Evidence Groups
File Items
File Extension (3,184 / 3,184)
File Category (5,170 / 5,170)
File Status
Email Status
Email Attachments (1 / 1)
Email Related Items (From Email) (34 / 34)
Email Reply (7 / 7)
Forwarded Email (0 / 0)
Labels (0 / 0)
Bookmarks
Cluster Topic
Document Content
File Content
Hex Text Filtered Natural
Default Media Web
File Content Properties Hex Interpreter
File List
Normal
Display Time Zone: Eastern Standard Time (From local machine)

From: Hamilton Fantomos <generalconsolidatedindustries@aol.com>
Sent: 4/10/2015 9:28:27 PM -0400
To: mightymonarch@outlook.com
Subject: Your Application

Monarch,

The new govemance body operating the Guild of Calamitous Intent, by order of the Sovereign and his Council of 13, has received your application for reinstatement as a super villain in good standing.
You are hereby granted arching rights 3rd class to:

Dr. Venture, also known as Thaddeus S. Venture, "Rusty" Venture. This entitles you to menace and mayhem rights on syndicate number Victor Echo November,
and extended rights of menace to the Order of the Triad under first right of refusal by their primary arch, the supervillain operating as "Torrid". You are ordered hereby to avoid needless encounters with law enforcement and obey all international treaties signed by Secret President of the United States and the GCI.

Your completed application provides Lair contents, henchmen liability and termination, medical, dental and funeral benefits.

Congratulations,

Hamilton J Fantomos, The Phantom Limb
Accountant
Insurance Agent
Supervillain
generalconsolidatedindustries@aol.com

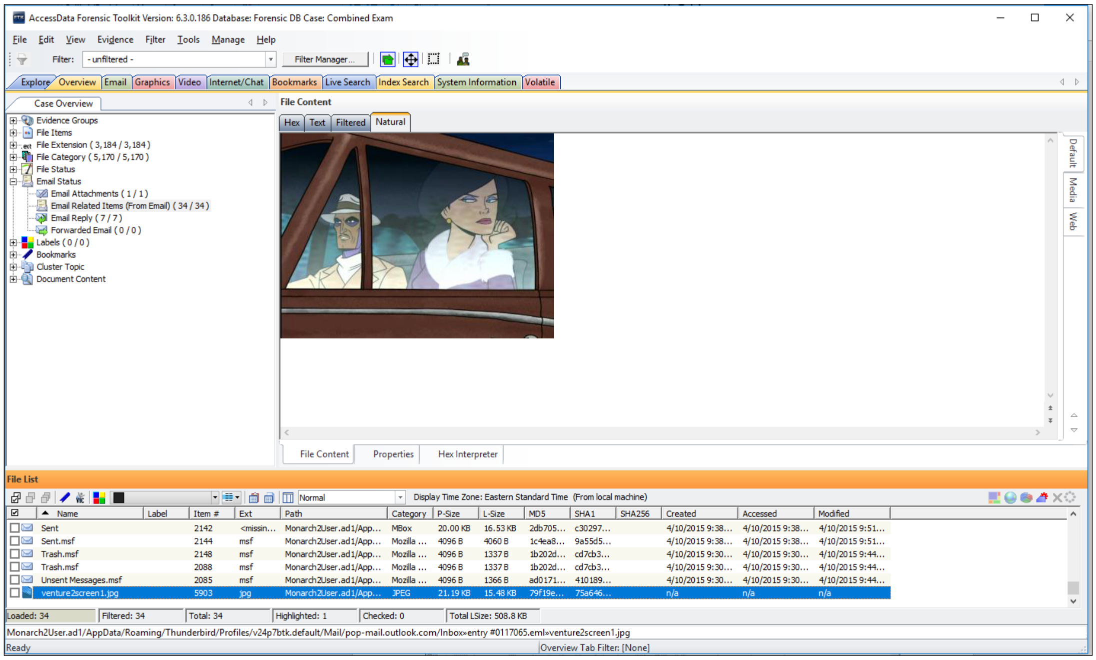
☑	Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
□	entry #0007342.eml		5768	eml	Monarch2User.ad1/App...	Text In...	n/a	3027 B	17e93d...	e82eb4...		n/a	n/a	n/a
□	entry #0010402.eml		5769	eml	Monarch2User.ad1/App...	Text In...	n/a	72.22 KB	68c38e...	1b3167...		n/a	n/a	n/a
□	entry #0084388.eml		5770	eml	Monarch2User.ad1/App...	Text In...	n/a	5386 B	4620b0...	f3718e...		n/a	n/a	n/a
□	entry #0089807.eml		5771	eml	Monarch2User.ad1/App...	Text In...	n/a	14.64 KB	066854...	853cc9...		n/a	n/a	n/a
□	entry #0104829.eml		5772	eml	Monarch2User.ad1/App...	Text In...	n/a	6659 B	4344af...	b9aa95...		n/a	n/a	n/a
□	entry #0111521.eml		5773	eml	Monarch2User.ad1/App...	Text In...	n/a	5511 B	c3ecda...	da5f02...		n/a	n/a	n/a
□	entry #0117065.eml		5774	eml	Monarch2User.ad1/App...	Text In...	n/a	31.02 KB	657aaa...	ec3548...		n/a	n/a	n/a

Loaded: 34 | Filtered: 34 | Total: 34 | Highlighted: 1 | Checked: 0 | Total LSize: 508.8 KB

Monarch2User.ad1/AppData/Roaming/Thunderbird/Profiles/v24p7btk.default/Mail/pop-mail.outlook.com/Inbox»entry #0111521.eml

Ready | Overview Tab Filter: [None]

The email along with its attachment displays Hamilton’s picture as below.


AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Combined Exam
File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered -
Filter Manager...
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
Case Overview
Evidence Groups
File Items
File Extension (3,184 / 3,184)
File Category (5,170 / 5,170)
File Status
Email Status
Email Attachments (1 / 1)
Email Related Items (From Email) (34 / 34)
Email Reply (7 / 7)
Forwarded Email (0 / 0)
Labels (0 / 0)
Bookmarks
Cluster Topic
Document Content
File Content
Hex Text Filtered Natural
Default Media Web
File Content Properties Hex Interpreter
File List
Normal
Display Time Zone: Eastern Standard Time (From local machine)

☑	Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
□	Sent		2142	<missin...	Monarch2User.ad1/App...	MBox	20.00 KB	16.53 KB	2db705...	c30297...		4/10/2015 9:38...	4/10/2015 9:38...	4/10/2015 9:51...
□	Sent.msf		2144	msf	Monarch2User.ad1/App...	Mozilla ...	4096 B	4060 B	1c4ea8...	9a55d5...		4/10/2015 9:38...	4/10/2015 9:38...	4/10/2015 9:51...
□	Trash.msf		2148	msf	Monarch2User.ad1/App...	Mozilla ...	4096 B	1337 B	1b202d...	cd7cb3...		4/10/2015 9:30...	4/10/2015 9:30...	4/10/2015 9:44...
□	Trash.msf		2088	msf	Monarch2User.ad1/App...	Mozilla ...	4096 B	1337 B	1b202d...	cd7cb3...		4/10/2015 9:30...	4/10/2015 9:30...	4/10/2015 9:44...
□	Unsent Messages.msf		2085	msf	Monarch2User.ad1/App...	Mozilla ...	4096 B	1366 B	ad0171...	410189...		4/10/2015 9:30...	4/10/2015 9:30...	4/10/2015 9:44...
□	venture2screen1.jpg		5903	jpg	Monarch2User.ad1/App...	JPEG	21.19 KB	15.48 KB	79f19e...	75a646...		n/a	n/a	n/a

Loaded: 34 | Filtered: 34 | Total: 34 | Highlighted: 1 | Checked: 0 | Total LSize: 508.8 KB

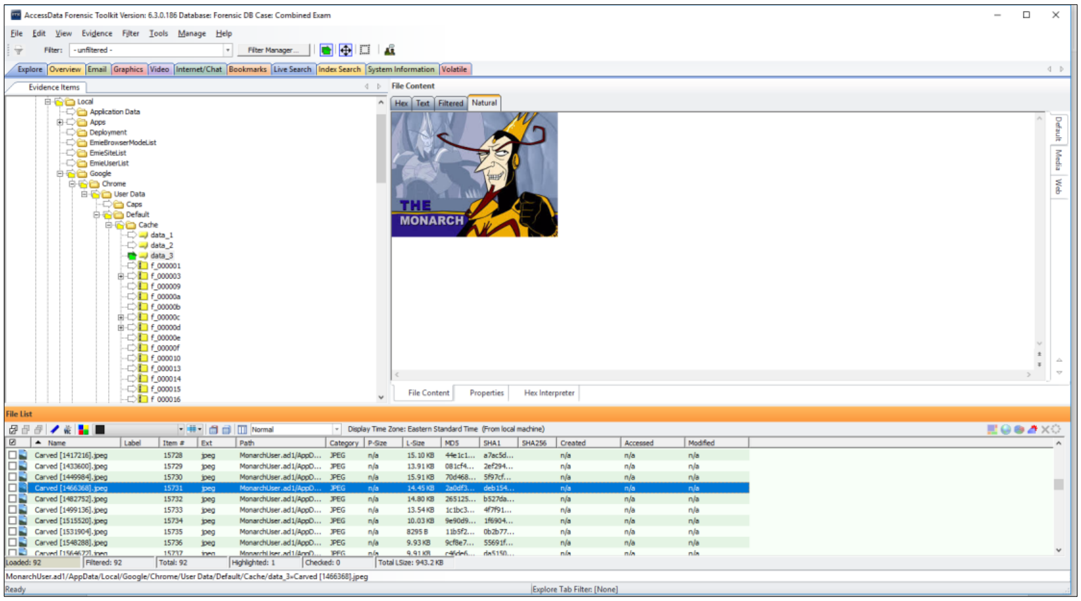
Monarch2User.ad1/AppData/Roaming/Thunderbird/Profiles/v24p7btk.default/Mail/pop-mail.outlook.com/Inbox»entry #0117065.eml»venture2screen1.jpg

Ready | Overview Tab Filter: [None]

2. Can you provide any pictures depicting the Monarch?

From MonarUser.ad1 File:

After performing data carving on MonarUser.ad1 file I found carved images showing pictures depicting the Monarch.



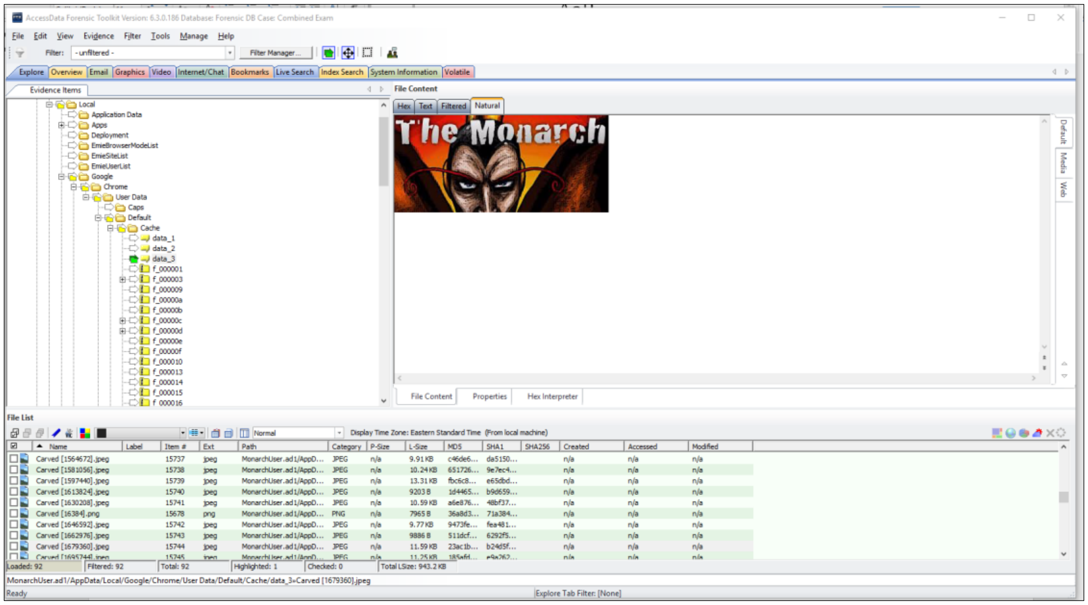
Display Time Zone: Eastern Standard Time (From local machine)

☑	Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
□	Carved [1417216].jpeg		15728	jpeg	MonarchUser.ad1/AppD...	JPEG	n/a	15.10 KB	44e1c1...	a7ac5d...		n/a	n/a	n/a
□	Carved [1433600].jpeg		15729	jpeg	MonarchUser.ad1/AppD...	JPEG	n/a	13.91 KB	081cf4...	2ef294...		n/a	n/a	n/a
□	Carved [1449984].jpeg		15730	jpeg	MonarchUser.ad1/AppD...	JPEG	n/a	15.91 KB	70d468...	5f97cf...		n/a	n/a	n/a
□	Carved [1466368].jpeg		15731	jpeg	MonarchUser.ad1/AppD...	JPEG	n/a	14.45 KB	2a0df3...	deb154...		n/a	n/a	n/a
□	Carved [1482752].jpeg		15732	jpeg	MonarchUser.ad1/AppD...	JPEG	n/a	14.80 KB	265125...	b527da...		n/a	n/a	n/a
□	Carved [1499136].jpeg		15733	jpeg	MonarchUser.ad1/AppD...	JPEG	n/a	13.54 KB	1c1bc3...	4f7f91...		n/a	n/a	n/a
□	Carved [1515520].jpeg		15734	jpeg	MonarchUser.ad1/AppD...	JPEG	n/a	10.03 KB	9e90d9...	1f6904...		n/a	n/a	n/a
□	Carved [1531904].jpeg		15735	jpeg	MonarchUser.ad1/AppD...	JPEG	n/a	8295 B	11b5f2...	0b2b77...		n/a	n/a	n/a
□	Carved [1548288].jpeg		15736	jpeg	MonarchUser.ad1/AppD...	JPEG	n/a	9.93 KB	9cf8e7...	55691f...		n/a	n/a	n/a
□	Carved [1564672].jpeg		15737	jpeg	MonarchUser.ad1/AppD...	JPEG	n/a	9.91 KB	c46de6...	da5150...		n/a	n/a	n/a

Loaded: 92 | Filtered: 92 | Total: 92 | Highlighted: 1 | Checked: 0 | Total LSize: 943.2 KB

MonarchUser.ad1/AppData/Local/Google/Chrome/User Data/Default/Cache/data_3»Carved [1466368].jpeg

Ready Explore Tab Filter: [None]



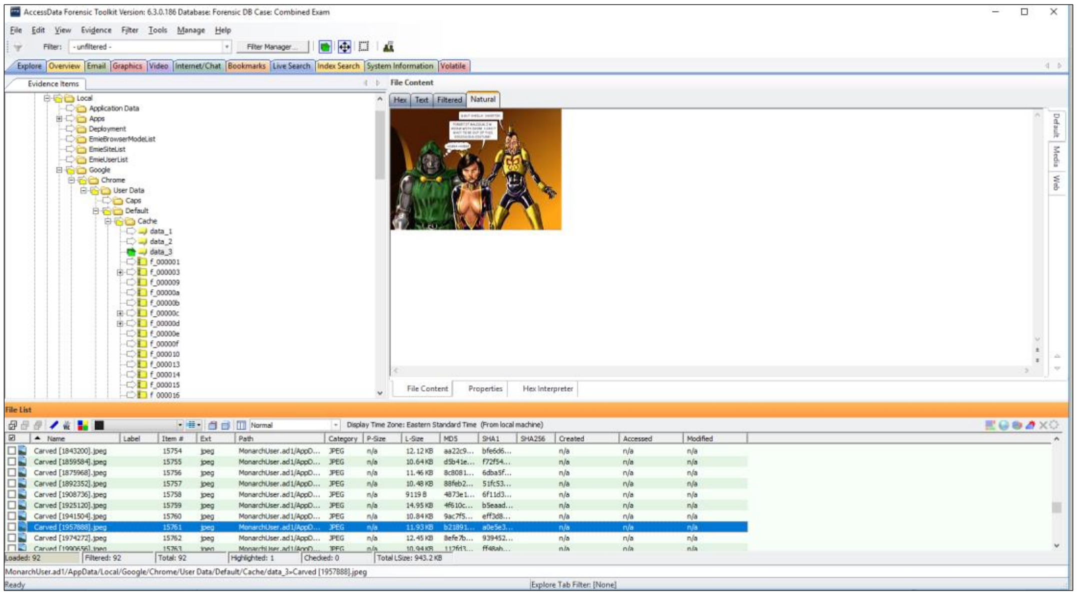
Display Time Zone: Eastern Standard Time (From local machine)

☑	Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
□	Carved [1564672].jpeg		15737	jpeg	MonarchUser.ad1/AppD...	JPEG	n/a	9.91 KB	c46de6...	da5150...		n/a	n/a	n/a
□	Carved [1581056].jpeg		15738	jpeg	MonarchUser.ad1/AppD...	JPEG	n/a	10.24 KB	651726...	9e7ec4...		n/a	n/a	n/a
□	Carved [1597440].jpeg		15739	jpeg	MonarchUser.ad1/AppD...	JPEG	n/a	13.31 KB	fbc6c8...	e65dbd...		n/a	n/a	n/a
□	Carved [1613824].jpeg		15740	jpeg	MonarchUser.ad1/AppD...	JPEG	n/a	9203 B	1d4465...	b9d659...		n/a	n/a	n/a
□	Carved [1630208].jpeg		15741	jpeg	MonarchUser.ad1/AppD...	JPEG	n/a	10.59 KB	a6e876...	48bf37...		n/a	n/a	n/a
□	Carved [16384].png		15678	png	MonarchUser.ad1/AppD...	PNG	n/a	7965 B	36a8d3...	71a384...		n/a	n/a	n/a
□	Carved [1646592].jpeg		15742	jpeg	MonarchUser.ad1/AppD...	JPEG	n/a	9.77 KB	9473fe...	fea481...		n/a	n/a	n/a
□	Carved [1662976].jpeg		15743	jpeg	MonarchUser.ad1/AppD...	JPEG	n/a	9886 B	511dcf...	6292f5...		n/a	n/a	n/a
□	Carved [1679360].jpeg		15744	jpeg	MonarchUser.ad1/AppD...	JPEG	n/a	11.59 KB	23ac1b...	b24d5f...		n/a	n/a	n/a
□	Carved [1695744].jpeg		15745	jpeg	MonarchUser.ad1/AppD...	JPEG	n/a	11.25 KB	185afd...	e9a262...		n/a	n/a	n/a

Loaded: 92 | Filtered: 92 | Total: 92 | Highlighted: 1 | Checked: 0 | Total LSize: 943.2 KB

MonarchUser.ad1/AppData/Local/Google/Chrome/User Data/Default/Cache/data_3»Carved [1679360].jpeg

Ready Explore Tab Filter: [None]



AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Combined Exam

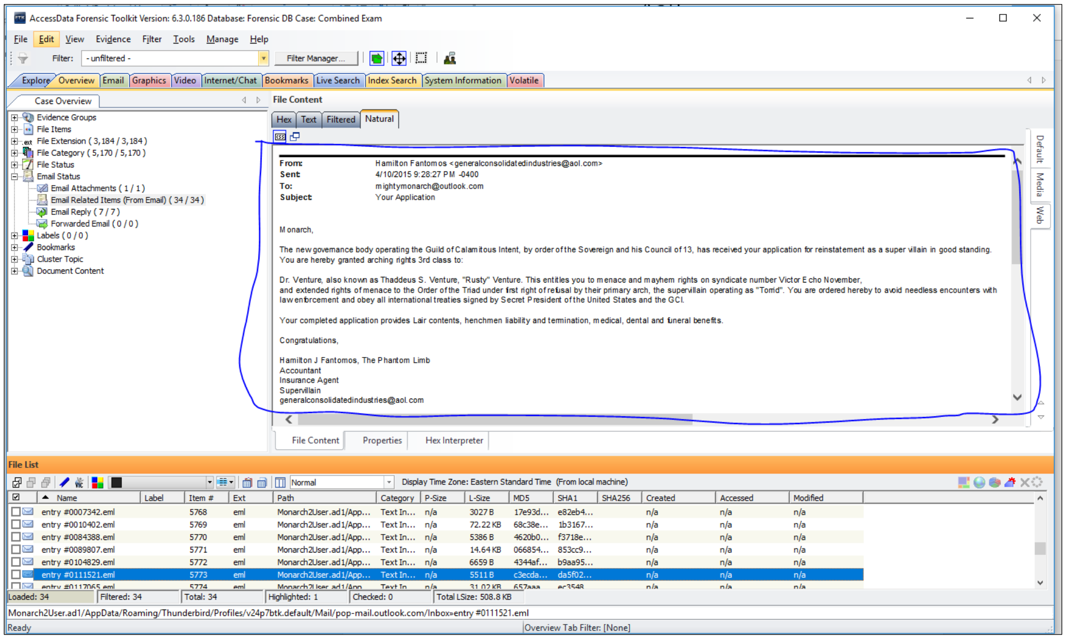
MonarchUser.ad1/AppData/Local/Google/Chrome/User Data/Default/Cache/data_3»Carved [1957888].jpeg

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
Carved [1843200].jpeg		15754	jpeg	MonarchUser.ad1/AppD...	JPEG	n/a	12.12 KB	aa22c9...	bfe6d6...		n/a	n/a	n/a
Carved [1859584].jpeg		15755	jpeg	MonarchUser.ad1/AppD...	JPEG	n/a	10.64 KB	d5b41e...	f72f54...		n/a	n/a	n/a
Carved [1875968].jpeg		15756	jpeg	MonarchUser.ad1/AppD...	JPEG	n/a	11.46 KB	8c8081...	6dba5f...		n/a	n/a	n/a
Carved [1892352].jpeg		15757	jpeg	MonarchUser.ad1/AppD...	JPEG	n/a	10.48 KB	88feb2...	51fc53...		n/a	n/a	n/a
Carved [1908736].jpeg		15758	jpeg	MonarchUser.ad1/AppD...	JPEG	n/a	9119 B	4873e1...	6f11d3...		n/a	n/a	n/a
Carved [1925120].jpeg		15759	jpeg	MonarchUser.ad1/AppD...	JPEG	n/a	14.95 KB	4f610c...	b5eaad...		n/a	n/a	n/a
Carved [1941504].jpeg		15760	jpeg	MonarchUser.ad1/AppD...	JPEG	n/a	10.84 KB	9ac7f5...	eff3d8...		n/a	n/a	n/a
Carved [1957888].jpeg		15761	jpeg	MonarchUser.ad1/AppD...	JPEG	n/a	11.93 KB	b21891...	a0e5e3...		n/a	n/a	n/a
Carved [1974272].jpeg		15762	jpeg	MonarchUser.ad1/AppD...	JPEG	n/a	12.45 KB	8efe7b...	939452...		n/a	n/a	n/a
Carved [1990656].jpeg		15763	jpeg	MonarchUser.ad1/AppD...	JPEG	n/a	10.94 KB	112fd3...	ff48ab...		n/a	n/a	n/a

Loaded: 92 | Filtered: 92 | Total: 92 | Highlighted: 1 | Checked: 0 | Total LSize: 943.2 KB

3. Can you find the Monarch's email address or the email address of the operative?

In overview tab, in email status I found the email conversation and thus found the Monarch's and operative's email address.
The Monarch's email address is **mightymonarch@outlook.com** and the email address of the operative is **generalconsolidateindustries@aol.com** .



AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Combined Exam

From:	Hamilton Fantomos <generalconsolidatedindustries@aol.com>
Sent:	4/10/2015 9:28:27 PM -0400
To:	mightymonarch@outlook.com
Subject:	Your Application

Monarch,

The new governance body operating the Guild of Calamitous Intent, by order of the Sovereign and his Council of 13, has received your application for reinstatement as a super villain in good standing. You are hereby granted arching rights 3rd class to:

Dr. Venture, also known as Thaddeus S. Venture, "Rusty" Venture. This entitles you to menace and mayhem rights on syndicate number Victor Echo November,
and extended rights of menace to the Order of the Triad under first right of refusal by their primary arch, the supervillain operating as "Torrid". You are ordered hereby to avoid needless encounters with law enforcement and obey all international treaties signed by Secret President of the United States and the GCI.

Your completed application provides Lair contents, henchmen liability and termination, medical, dental and funeral benefits.

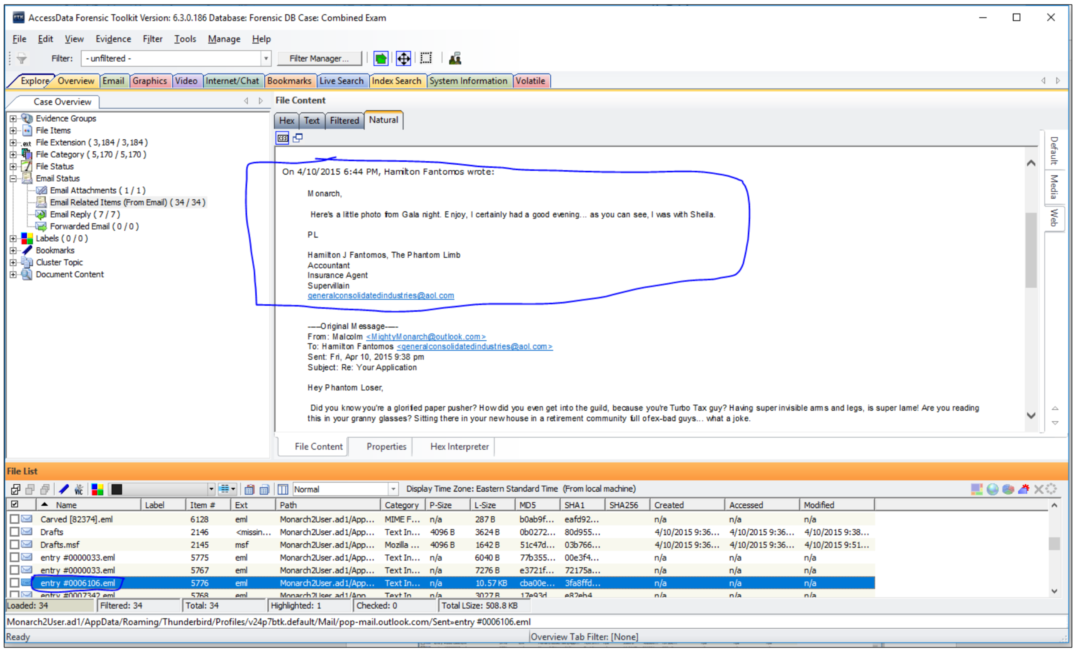
Congratulations,

Hamilton J Fantomos, The Phantom Limb
Accountant
Insurance Agent
Supervillain
generalconsolidatedindustries@aol.com

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
entry #0007342.eml		5768	eml	Monarch2User.ad1/App...	Text In...	n/a	3027 B	17e93d...	e82eb4...		n/a	n/a	n/a
entry #0010402.eml		5769	eml	Monarch2User.ad1/App...	Text In...	n/a	72.22 KB	68c38e...	1b3167...		n/a	n/a	n/a
entry #0084388.eml		5770	eml	Monarch2User.ad1/App...	Text In...	n/a	5386 B	4620b0...	f3718e...		n/a	n/a	n/a
entry #0089807.eml		5771	eml	Monarch2User.ad1/App...	Text In...	n/a	14.64 KB	066854...	853cc9...		n/a	n/a	n/a
entry #0104829.eml		5772	eml	Monarch2User.ad1/App...	Text In...	n/a	6659 B	4344af...	b9aa95...		n/a	n/a	n/a
entry #0111521.eml		5773	eml	Monarch2User.ad1/App...	Text In...	n/a	5511 B	c3ecda...	da5f02...		n/a	n/a	n/a
entry #0117065.eml		5774	eml	Monarch2User.ad1/App...	Text In...	n/a	31.02 KB	657aaa...	ec3548...		n/a	n/a	n/a

Loaded: 34 | Filtered: 34 | Total: 34 | Highlighted: 1 | Checked: 0 | Total LSize: 508.8 KB

Monarch2User.ad1/AppData/Roaming/Thunderbird/Profiles/v24p7btk.default/Mail/pop-mail.outlook.com/Inbox»entry #0111521.eml


AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Combined Exam
File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered -
Filter Manager...
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
Case Overview
Evidence Groups
File Items
File Extension (3,184 / 3,184)
File Category (5,170 / 5,170)
File Status
Email Status
Email Attachments (1 / 1)
Email Related Items (From Email) (34 / 34)
Email Reply (7 / 7)
Forwarded Email (0 / 0)
Labels (0 / 0)
Bookmarks
Cluster Topic
Document Content
File Content
Hex Text Filtered Natural
Default Media Web
File Content Properties Hex Interpreter
File List

On 4/10/2015 6:44 PM, Hamilton Fantomos wrote:

Monarch,

Here's a little photo fom Gala night. Enjoy, I certainly had a good evening... as you can see, I was with Sheila.

PL

Hamilton J Fantomos, The Phantom Limb
Accountant
Insurance Agent
Supervillain
generalconsolidatedindustries@aol.com

-----Original Message-----
From: Malcolm <MightyMonarch@outlook.com>
To: Hamilton Fantomos <generalconsolidatedindustries@aol.com>
Sent: Fri, Apr 10, 2015 9:38 pm
Subject: Re: Your Application

Hey Phantom Loser,

Did you know you're a glorifed paper pusher? How did you even get into the guild, because you're Turbo Tax guy? Having super invisible arms and legs, is super lame! Are you reading this in your granny glasses? Sitting there in your new house in a retirement community full of ex-bad guys... what a joke.

Normal Display Time Zone: Eastern Standard Time (From local machine)

☑	Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
☐	Carved [82374].eml		6128	eml	Monarch2User.ad1/App...	MIME F...	n/a	287 B	b0ab9f...	eafd92...		n/a	n/a	n/a
☐	Drafts		2146	<missin...	Monarch2User.ad1/App...	Text In...	4096 B	3624 B	0b0272...	80d955...		4/10/2015 9:36...	4/10/2015 9:36...	4/10/2015 9:38...
☐	Drafts.msf		2145	msf	Monarch2User.ad1/App...	Mozilla ...	4096 B	1642 B	51c47d...	03b766...		4/10/2015 9:36...	4/10/2015 9:36...	4/10/2015 9:51...
☐	entry #0000033.eml		5775	eml	Monarch2User.ad1/App...	Text In...	n/a	6040 B	77b355...	00e3f4...		n/a	n/a	n/a
☐	entry #0000033.eml		5767	eml	Monarch2User.ad1/App...	Text In...	n/a	7276 B	e3721f...	72175a...		n/a	n/a	n/a
☐	entry #0006106.eml		5776	eml	Monarch2User.ad1/App...	Text In...	n/a	10.57 KB	cba00e...	3fa8ffd...		n/a	n/a	n/a
☐	entry #0007342.eml		5768	eml	Monarch2User.ad1/App...	Text In...	n/a	3027 B	17e93d...	e82eb4...		n/a	n/a	n/a

Loaded: 34 | Filtered: 34 | Total: 34 | Highlighted: 1 | Checked: 0 | Total LSize: 508.8 KB

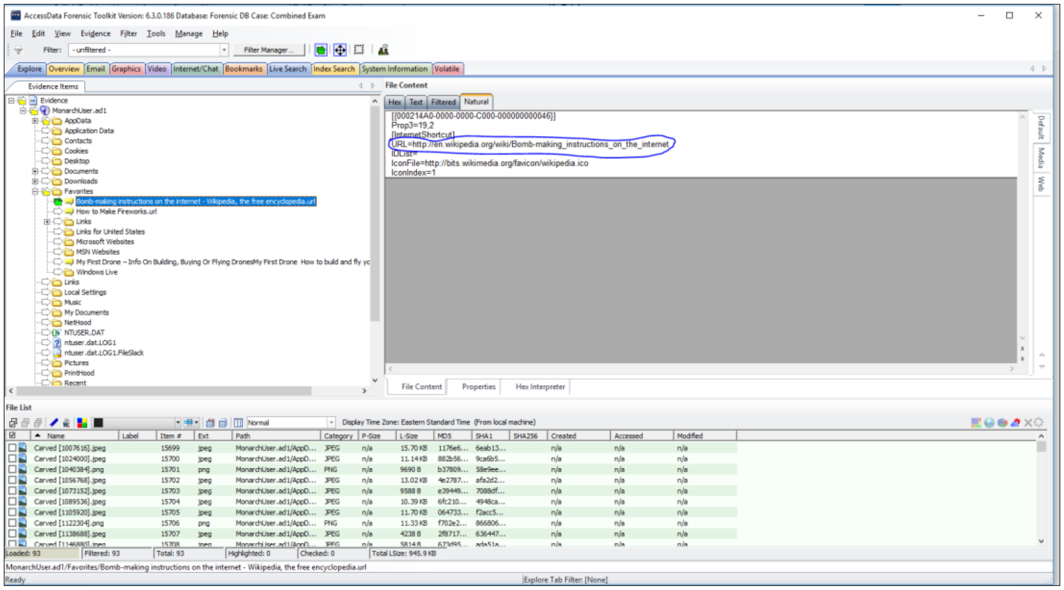
Monarch2User.ad1/AppData/Roaming/Thunderbird/Profiles/v24p7btk.default/Mail/pop-mail.outlook.com/Sent»entry #0006106.eml

Ready Overview Tab Filter: [None]

4. Are there any items related to monarch's plan for violence?

Following are the items showing URL and photographs.

As per the URL titled as Bomb making instructions on the internet, I got evidence of monarch's plan for voilance.


AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Combined Exam
File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered -
Filter Manager...
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
Evidence Items
Evidence
MonarchUser.ad1
AppData
Application Data
Contacts
Cookies
Desktop
Documents
Downloads
Favorites
Bomb-making instructions on the internet - Wikipedia, the free encyclopedia.url
How to Make Fireworks.url
Links
Links for United States
Microsoft Websites
MSN Websites
My First Drone – Info On Building, Buying Or Flying DronesMy First Drone How to build and fly yc
Windows Live
Links
Local Settings
Music
My Documents
NetHood
NTUSER.DAT
ntuser.dat.LOG1
ntuser.dat.LOG1.FileSlack
Pictures
PrintHood
Recent
File Content
Hex Text Filtered Natural
Default Media Web
File Content Properties Hex Interpreter
File List

```
[{000214A0-0000-0000-C000-000000000046}]
Prop3=19,2
[InternetShortcut]
URL=http://en.wikipedia.org/wiki/Bomb-making_instructions_on_the_internet
IDList=
IconFile=http://bits.wikimedia.org/favicon/wikipedia.ico
IconIndex=1
```

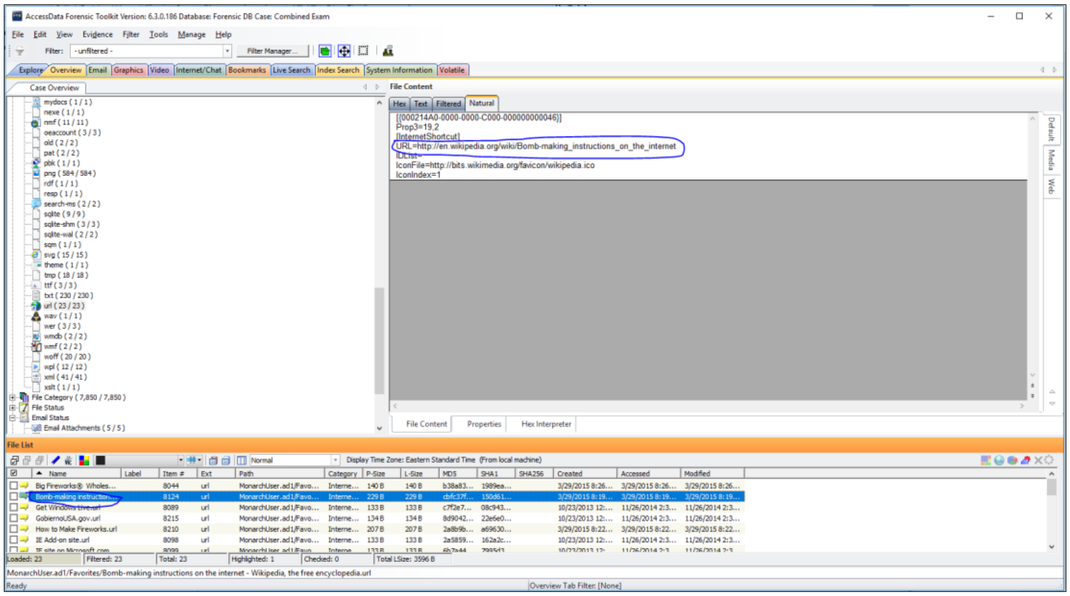
Normal Display Time Zone: Eastern Standard Time (From local machine)

☑	Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
☐	Carved [1007616].jpeg		15699	jpeg	MonarchUser.ad1/AppD...	JPEG	n/a	15.70 KB	1176e6...	6eab13...		n/a	n/a	n/a
☐	Carved [1024000].jpeg		15700	jpeg	MonarchUser.ad1/AppD...	JPEG	n/a	11.14 KB	882b56...	9ca6b5...		n/a	n/a	n/a
☐	Carved [1040384].png		15701	png	MonarchUser.ad1/AppD...	PNG	n/a	9690 B	b37809...	58e9ee...		n/a	n/a	n/a
☐	Carved [1056768].jpeg		15702	jpeg	MonarchUser.ad1/AppD...	JPEG	n/a	13.02 KB	4e2787...	afa2d2...		n/a	n/a	n/a
☐	Carved [1073152].jpeg		15703	jpeg	MonarchUser.ad1/AppD...	JPEG	n/a	9588 B	e39449...	7088df...		n/a	n/a	n/a
☐	Carved [1089536].jpeg		15704	jpeg	MonarchUser.ad1/AppD...	JPEG	n/a	10.39 KB	6fc210...	4948ca...		n/a	n/a	n/a
☐	Carved [1105920].jpeg		15705	jpeg	MonarchUser.ad1/AppD...	JPEG	n/a	11.70 KB	064733...	f2acc5...		n/a	n/a	n/a
☐	Carved [1122304].png		15706	png	MonarchUser.ad1/AppD...	PNG	n/a	11.33 KB	f702e2...	866806...		n/a	n/a	n/a
☐	Carved [1138688].jpeg		15707	jpeg	MonarchUser.ad1/AppD...	JPEG	n/a	4238 B	2f8717...	636447...		n/a	n/a	n/a
☐	Carved [1146880].jpeg		15708	jpeg	MonarchUser.ad1/AppD...	JPEG	n/a	5814 B	673d95...	ada51a...		n/a	n/a	n/a

Loaded: 93 | Filtered: 93 | Total: 93 | Highlighted: 0 | Checked: 0 | Total LSize: 945.9 KB

MonarchUser.ad1/Favorites/Bomb-making instructions on the internet - Wikipedia, the free encyclopedia.url

Ready Explore Tab Filter: [None]


AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Combined Exam
File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered -
Filter Manager...
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
Case Overview
File Content
Hex Text Filtered Natural
File Content Properties Hex Interpreter
File List
Default Media Web

mydocs (1 / 1)
nexe (1 / 1)
nmf (11 / 11)
oeaccount (3 / 3)
old (2 / 2)
pat (2 / 2)
pbk (1 / 1)
png (584 / 584)
rdf (1 / 1)
resp (1 / 1)
search-ms (2 / 2)
sqlite (9 / 9)
sqlite-shm (3 / 3)
sqlite-wal (2 / 2)
sqm (1 / 1)
svg (15 / 15)
theme (1 / 1)
tmp (18 / 18)
ttf (3 / 3)
txt (230 / 230)
url (23 / 23)
wav (1 / 1)
wer (3 / 3)
wmdb (2 / 2)
wmf (2 / 2)
woff (20 / 20)
wpl (12 / 12)
xml (41 / 41)
xslt (1 / 1)
File Category (7,850 / 7,850)
File Status
Email Status
Email Attachments (5 / 5)

```
[{000214A0-0000-0000-C000-000000000046}]
Prop3=19,2
[InternetShortcut]
URL=http://en.wikipedia.org/wiki/Bomb-making_instructions_on_the_internet
IDList=
IconFile=http://bits.wikimedia.org/favicon/wikipedia.ico
IconIndex=1
```

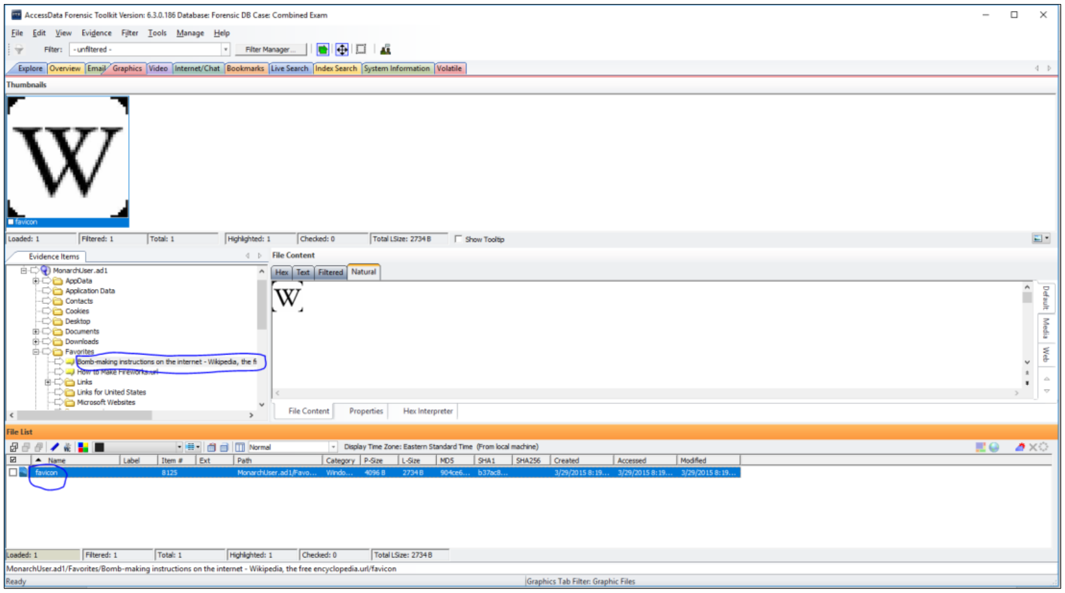
Normal   Display Time Zone: Eastern Standard Time (From local machine)

☑	Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
□	Big Fireworks® Wholes...		8044	url	MonarchUser.ad1/Favo...	Interne...	140 B	140 B	b38a83...	1989ea...		3/29/2015 8:26...	3/29/2015 8:26...	3/29/2015 8:26...
□	Bomb-making instruction...		8124	url	MonarchUser.ad1/Favo...	Interne...	229 B	229 B	cbfc37f...	150d61...		3/29/2015 8:19...	3/29/2015 8:19...	3/29/2015 8:19...
□	Get Windows Live.url		8089	url	MonarchUser.ad1/Favo...	Interne...	133 B	133 B	c7f2e7...	08c943...		10/23/2013 12:...	11/26/2014 2:3...	11/26/2014 2:3...
□	GobiernoUSA.gov.url		8215	url	MonarchUser.ad1/Favo...	Interne...	134 B	134 B	8d9042...	22e6e0...		10/23/2013 12:...	11/26/2014 2:3...	11/26/2014 2:3...
□	How to Make Fireworks.url		8210	url	MonarchUser.ad1/Favo...	Interne...	207 B	207 B	2a8b9b...	a69630...		3/29/2015 8:22...	3/29/2015 8:22...	3/29/2015 8:22...
□	IE Add-on site.url		8098	url	MonarchUser.ad1/Favo...	Interne...	133 B	133 B	2a5859...	162a2c...		10/23/2013 12:...	11/26/2014 2:3...	11/26/2014 2:3...
□	IE site on Microsoft.com		8099	url	MonarchUser.ad1/Favo...	Interne...	133 B	133 B	6b7a44	7995d3		10/23/2013 12:	11/26/2014 2:3	11/26/2014 2:3

Loaded: 23 | Filtered: 23 | Total: 23 | Highlighted: 1 | Checked: 0 | Total LSize: 3596 B

MonarchUser.ad1/Favorites/Bomb-making instructions on the internet - Wikipedia, the free encyclopedia.url

Ready   Overview Tab Filter: [None]


AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Combined Exam
File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered -
Filter Manager...
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
Thumbnails
W
favicon
Show Tooltip
Evidence Items
File Content
Hex Text Filtered Natural
W
File Content Properties Hex Interpreter
File List
Default Media Web

Loaded: 1 | Filtered: 1 | Total: 1 | Highlighted: 1 | Checked: 0 | Total LSize: 2734 B

MonarchUser.ad1
AppData
Application Data
Contacts
Cookies
Desktop
Documents
Downloads
Favorites
Bomb-making instructions on the internet - Wikipedia, the fi
How to Make Fireworks.url
Links
Links for United States
Microsoft Websites

Normal   Display Time Zone: Eastern Standard Time (From local machine)

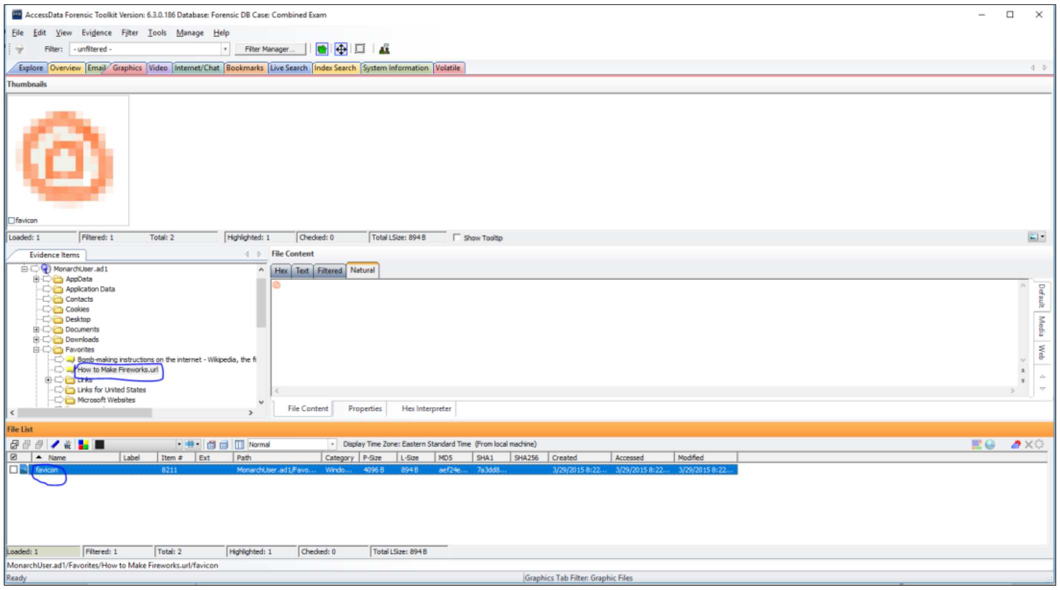
☑	Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
□	favicon		8125		MonarchUser.ad1/Favo...	Windo...	4096 B	2734 B	904ce6...	b37ac8...		3/29/2015 8:19...	3/29/2015 8:19...	3/29/2015 8:19...

Loaded: 1 | Filtered: 1 | Total: 1 | Highlighted: 1 | Checked: 0 | Total LSize: 2734 B

MonarchUser.ad1/Favorites/Bomb-making instructions on the internet - Wikipedia, the free encyclopedia.url/favicon

Ready   Graphics Tab Filter: Graphic Files

Below image shows evidence on how to make fireworks:


AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Combined Exam
File Edit View Evidence Filter Tools Manage Help
Filter Manager...
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
Thumbnails
File Content
Hex Text Filtered Natural
File Content Properties Hex Interpreter
Default Media Web
File List

Filter: - unfiltered -

□ favicon

Loaded: 1 | Filtered: 1 | Total: 2 | Highlighted: 1 | Checked: 0 | Total LSize: 894 B | □ Show Tooltip

Evidence Items

- MonarchUser.ad1
  - AppData
  - Application Data
  - Contacts
  - Cookies
  - Desktop
  - Documents
  - Downloads
  - Favorites
    - Bomb-making instructions on the internet - Wikipedia, the fi
    - How to Make Fireworks.url
    - Links
    - Links for United States
    - Microsoft Websites

Normal | Display Time Zone: Eastern Standard Time (From local machine)

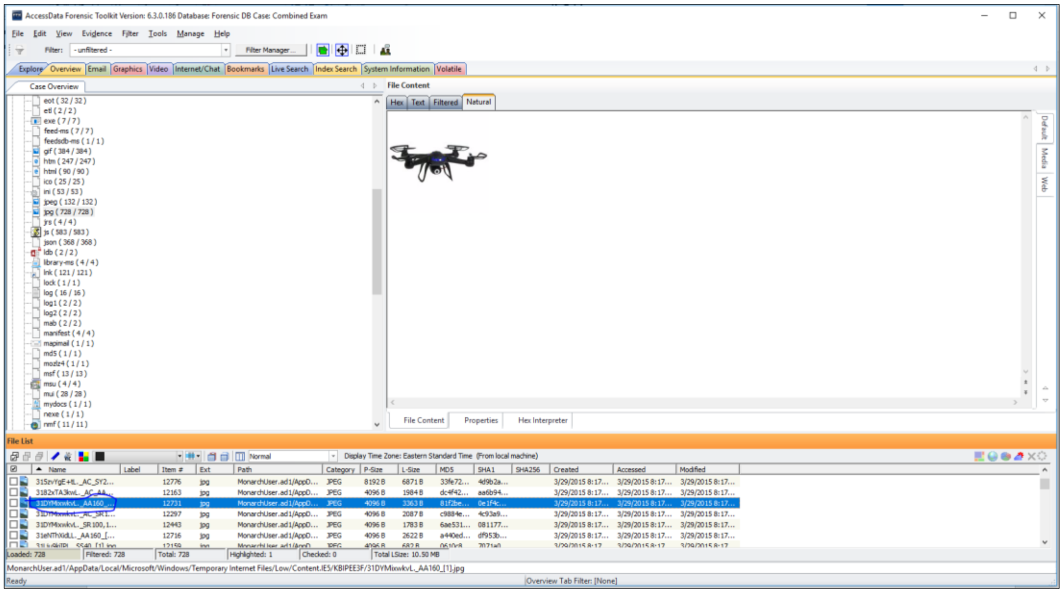
☑	Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
□	favicon		8211		MonarchUser.ad1/Favo...	Windo...	4096 B	894 B	aef24e...	7a3dd8...		3/29/2015 8:22...	3/29/2015 8:22...	3/29/2015 8:22...

Loaded: 1 | Filtered: 1 | Total: 2 | Highlighted: 1 | Checked: 0 | Total LSize: 894 B

MonarchUser.ad1/Favorites/How to Make Fireworks.url/favicon

Ready | Graphics Tab Filter: Graphic Files

Below images shown evidences related to drone and other harmful plans.


AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Combined Exam
File Edit View Evidence Filter Tools Manage Help
Filter Manager...
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
Case Overview
File Content
Hex Text Filtered Natural
File Content Properties Hex Interpreter
Default Media Web
File List

Filter: - unfiltered -

- eot (32 / 32)
- etl (2 / 2)
- exe (7 / 7)
- feed-ms (7 / 7)
- feedsdb-ms (1 / 1)
- gif (384 / 384)
- htm (247 / 247)
- html (90 / 90)
- ico (25 / 25)
- ini (53 / 53)
- jpeg (132 / 132)
- jpg (728 / 728)
- jrs (4 / 4)
- js (583 / 583)
- json (368 / 368)
- ldb (2 / 2)
- library-ms (4 / 4)
- lnk (121 / 121)
- lock (1 / 1)
- log (16 / 16)
- log1 (2 / 2)
- log2 (2 / 2)
- mab (2 / 2)
- manifest (4 / 4)
- mapimail (1 / 1)
- md5 (1 / 1)
- mozlz4 (1 / 1)
- msf (13 / 13)
- msu (4 / 4)
- mui (28 / 28)
- mydocs (1 / 1)
- nexe (1 / 1)
- nmf (11 / 11)

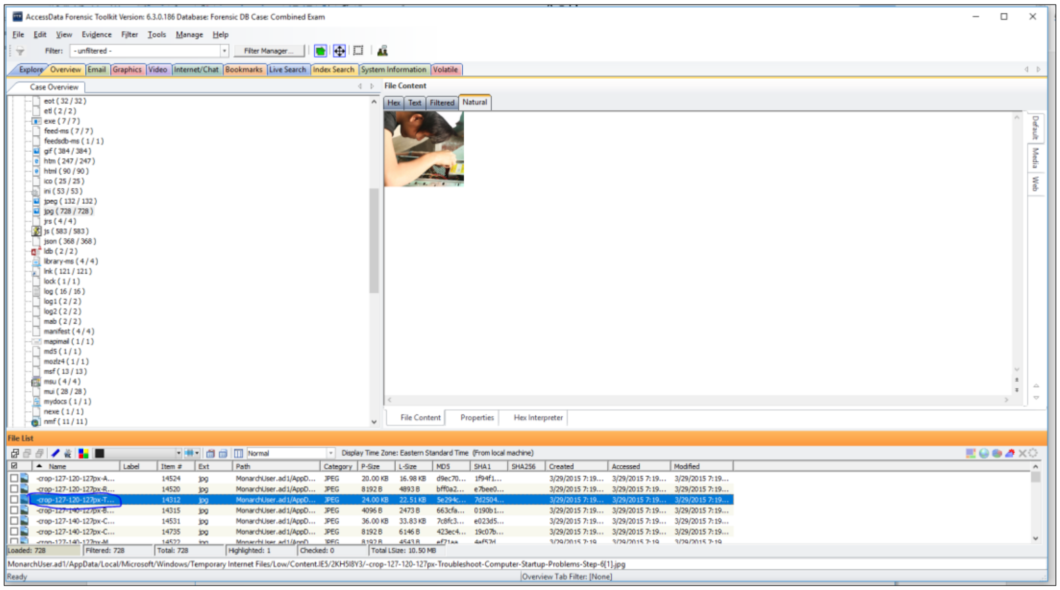
Normal | Display Time Zone: Eastern Standard Time (From local machine)

☑	Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
□	315zvYgE+tL._AC_SY2...		12776	jpg	MonarchUser.ad1/AppD...	JPEG	8192 B	6871 B	33fe72...	4d9b2a...		3/29/2015 8:17...	3/29/2015 8:17...	3/29/2015 8:17...
□	3182xTA3kwL._AC_AA...		12163	jpg	MonarchUser.ad1/AppD...	JPEG	4096 B	1984 B	dc4f42...	aa6b94...		3/29/2015 8:17...	3/29/2015 8:17...	3/29/2015 8:17...
□	31DYMixwkvL._AA160_...		12731	jpg	MonarchUser.ad1/AppD...	JPEG	4096 B	3363 B	81f2be...	0e1f4c...		3/29/2015 8:17...	3/29/2015 8:17...	3/29/2015 8:17...
□	31DYMixwkvL._AC_SR1...		12297	jpg	MonarchUser.ad1/AppD...	JPEG	4096 B	2087 B	c9884e...	4c93a9...		3/29/2015 8:17...	3/29/2015 8:17...	3/29/2015 8:17...
□	31DYMixwkvL._SR100,1...		12443	jpg	MonarchUser.ad1/AppD...	JPEG	4096 B	1783 B	6ae531...	081177...		3/29/2015 8:17...	3/29/2015 8:17...	3/29/2015 8:17...
□	31eNThXidLL._AA160_[...		12716	jpg	MonarchUser.ad1/AppD...	JPEG	4096 B	2622 B	a440ed...	df953b...		3/29/2015 8:17...	3/29/2015 8:17...	3/29/2015 8:17...
□	31Liu9kIPL._SS40_[1].jpg		12159	jpg	MonarchUser.ad1/AppD...	JPEG	4096 B	682 B	0610c8	7071a0		3/29/2015 8:17	3/29/2015 8:17	3/29/2015 8:17

Loaded: 728 | Filtered: 728 | Total: 728 | Highlighted: 1 | Checked: 0 | Total LSize: 10.50 MB

MonarchUser.ad1/AppData/Local/Microsoft/Windows/Temporary Internet Files/Low/Content.IE5/KBIPEE3F/31DYMixwkvL._AA160_[1].jpg

Ready | Overview Tab Filter: [None]


AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Combined Exam
File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered - Filter Manager...
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
Case Overview
File Content
Hex Text Filtered Natural
Default Media Web
File Content Properties Hex Interpreter
File List
Normal

eot (32 / 32)
etl (2 / 2)
exe (7 / 7)
feed-ms (7 / 7)
feedsdb-ms (1 / 1)
gif (384 / 384)
htm (247 / 247)
html (90 / 90)
ico (25 / 25)
ini (53 / 53)
jpeg (132 / 132)
jpg (728 / 728)
jrs (4 / 4)
js (583 / 583)
json (368 / 368)
ldb (2 / 2)
library-ms (4 / 4)
lnk (121 / 121)
lock (1 / 1)
log (16 / 16)
log1 (2 / 2)
log2 (2 / 2)
mab (2 / 2)
manifest (4 / 4)
mapimail (1 / 1)
md5 (1 / 1)
mozlz4 (1 / 1)
msf (13 / 13)
msu (4 / 4)
mui (28 / 28)
mydocs (1 / 1)
nexe (1 / 1)
nmf (11 / 11)

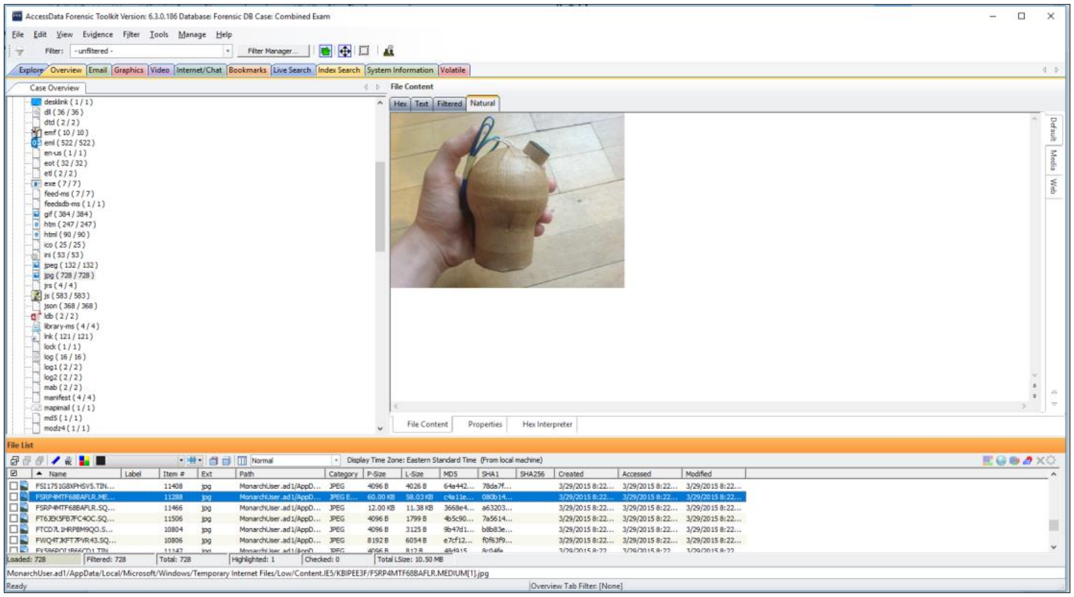
Display Time Zone: Eastern Standard Time (From local machine)

☑	Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
□	-crop-127-120-127px-A...		14524	jpg	MonarchUser.ad1/AppD...	JPEG	20.00 KB	16.98 KB	d9ec70...	1f94f1...		3/29/2015 7:19...	3/29/2015 7:19...	3/29/2015 7:19...
□	-crop-127-120-127px-R...		14520	jpg	MonarchUser.ad1/AppD...	JPEG	8192 B	4893 B	bff0a2...	e7bee0...		3/29/2015 7:19...	3/29/2015 7:19...	3/29/2015 7:19...
□	-crop-127-120-127px-T...		14312	jpg	MonarchUser.ad1/AppD...	JPEG	24.00 KB	22.51 KB	5e294c...	7d2504...		3/29/2015 7:19...	3/29/2015 7:19...	3/29/2015 7:19...
□	-crop-127-140-127px-B...		14315	jpg	MonarchUser.ad1/AppD...	JPEG	4096 B	2473 B	663cfa...	0190b1...		3/29/2015 7:19...	3/29/2015 7:19...	3/29/2015 7:19...
□	-crop-127-140-127px-C...		14531	jpg	MonarchUser.ad1/AppD...	JPEG	36.00 KB	33.83 KB	7c8fc3...	e023d5...		3/29/2015 7:19...	3/29/2015 7:19...	3/29/2015 7:19...
□	-crop-127-140-127px-C...		14735	jpg	MonarchUser.ad1/AppD...	JPEG	8192 B	6146 B	423ec4...	19c07b...		3/29/2015 7:19...	3/29/2015 7:19...	3/29/2015 7:19...

Loaded: 728 | Filtered: 728 | Total: 728 | Highlighted: 1 | Checked: 0 | Total LSize: 10.50 MB

MonarchUser.ad1/AppData/Local/Microsoft/Windows/Temporary Internet Files/Low/Content.IE5/2KH5I8Y3/-crop-127-120-127px-Troubleshoot-Computer-Startup-Problems-Step-6[1].jpg

Ready | Overview Tab Filter: [None]


AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Combined Exam
File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered - Filter Manager...
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
Case Overview
File Content
Hex Text Filtered Natural
Default Media Web
File Content Properties Hex Interpreter
File List
Normal

desklink (1 / 1)
dll (36 / 36)
dtd (2 / 2)
emf (10 / 10)
eml (522 / 522)
en-us (1 / 1)
eot (32 / 32)
etl (2 / 2)
exe (7 / 7)
feed-ms (7 / 7)
feedsdb-ms (1 / 1)
gif (384 / 384)
htm (247 / 247)
html (90 / 90)
ico (25 / 25)
ini (53 / 53)
jpeg (132 / 132)
jpg (728 / 728)
jrs (4 / 4)
js (583 / 583)
json (368 / 368)
ldb (2 / 2)
library-ms (4 / 4)
lnk (121 / 121)
lock (1 / 1)
log (16 / 16)
log1 (2 / 2)
log2 (2 / 2)
mab (2 / 2)
manifest (4 / 4)
mapimail (1 / 1)
md5 (1 / 1)
mozlz4 (1 / 1)

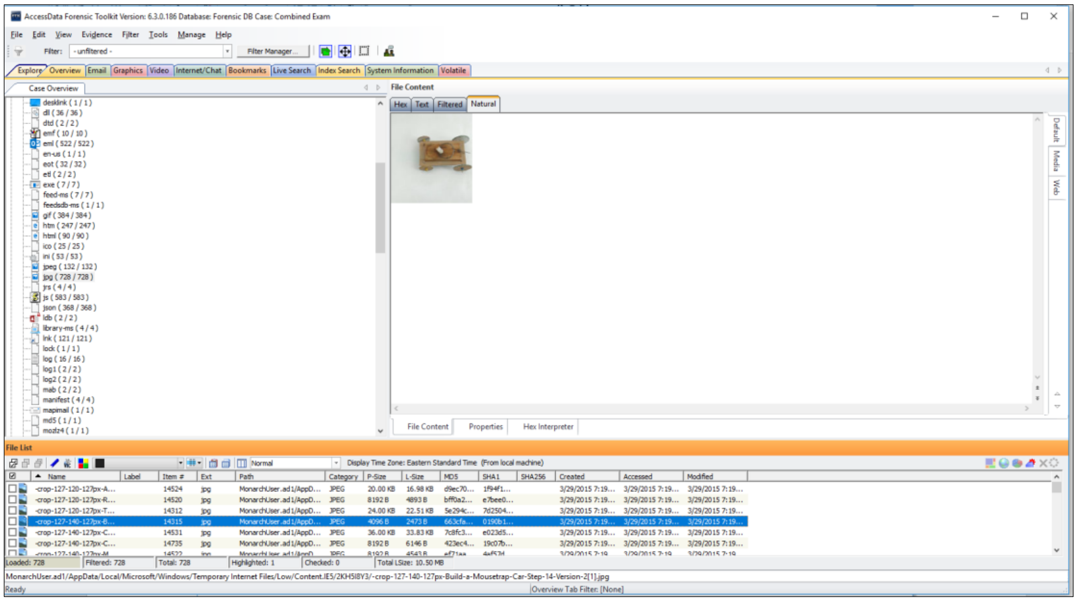
Display Time Zone: Eastern Standard Time (From local machine)

☑	Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
□	FSI1751G8XPHSV5.TIN...		11408	jpg	MonarchUser.ad1/AppD...	JPEG	4096 B	4026 B	64a442...	78da7f...		3/29/2015 8:22...	3/29/2015 8:22...	3/29/2015 8:22...
□	FSRP4MTF68BAFLR.ME...		11288	jpg	MonarchUser.ad1/AppD...	JPEG E...	60.00 KB	58.03 KB	c4a11e...	080b14...		3/29/2015 8:22...	3/29/2015 8:22...	3/29/2015 8:22...
□	FSRP4MTF68BAFLR.SQ...		11466	jpg	MonarchUser.ad1/AppD...	JPEG	12.00 KB	11.38 KB	3668e4...	a63203...		3/29/2015 8:22...	3/29/2015 8:22...	3/29/2015 8:22...
□	FT6JEK5FB7FC4OC.SQ...		11506	jpg	MonarchUser.ad1/AppD...	JPEG	4096 B	1799 B	4b5c90...	7a5614...		3/29/2015 8:22...	3/29/2015 8:22...	3/29/2015 8:22...
□	FTCD7L1HRPBM9QO.S...		10804	jpg	MonarchUser.ad1/AppD...	JPEG	4096 B	3125 B	9b47d1...	b8b83e...		3/29/2015 8:22...	3/29/2015 8:22...	3/29/2015 8:22...
□	FWQ4TJKFT7PVR43.SQ...		10806	jpg	MonarchUser.ad1/AppD...	JPEG	8192 B	6054 B	e7cf12...	f0f63f9...		3/29/2015 8:22...	3/29/2015 8:22...	3/29/2015 8:22...

Loaded: 728 | Filtered: 728 | Total: 728 | Highlighted: 1 | Checked: 0 | Total LSize: 10.50 MB

MonarchUser.ad1/AppData/Local/Microsoft/Windows/Temporary Internet Files/Low/Content.IE5/KBIPEE3F/FSRP4MTF68BAFLR.MEDIUM[1].jpg

Ready | Overview Tab Filter: [None]



AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Combined Exam

File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered -
Filter Manager...
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
Case Overview
File Content
Hex Text Filtered Natural
Default Media Web
File Content Properties Hex Interpreter
File List
Normal

- desktlnk (1 / 1)
- dll (36 / 36)
- dtd (2 / 2)
- emf (10 / 10)
- eml (522 / 522)
- en-us (1 / 1)
- eot (32 / 32)
- etl (2 / 2)
- exe (7 / 7)
- feed-ms (7 / 7)
- feedsdb-ms (1 / 1)
- gif (384 / 384)
- htm (247 / 247)
- html (90 / 90)
- ico (25 / 25)
- ini (53 / 53)
- jpeg (132 / 132)
- jpg (728 / 728)
- jrs (4 / 4)
- js (583 / 583)
- json (368 / 368)
- ldb (2 / 2)
- library-ms (4 / 4)
- lnk (121 / 121)
- lock (1 / 1)
- log (16 / 16)
- log1 (2 / 2)
- log2 (2 / 2)
- mab (2 / 2)
- manifest (4 / 4)
- mapimail (1 / 1)
- md5 (1 / 1)
- mozlz4 (1 / 1)

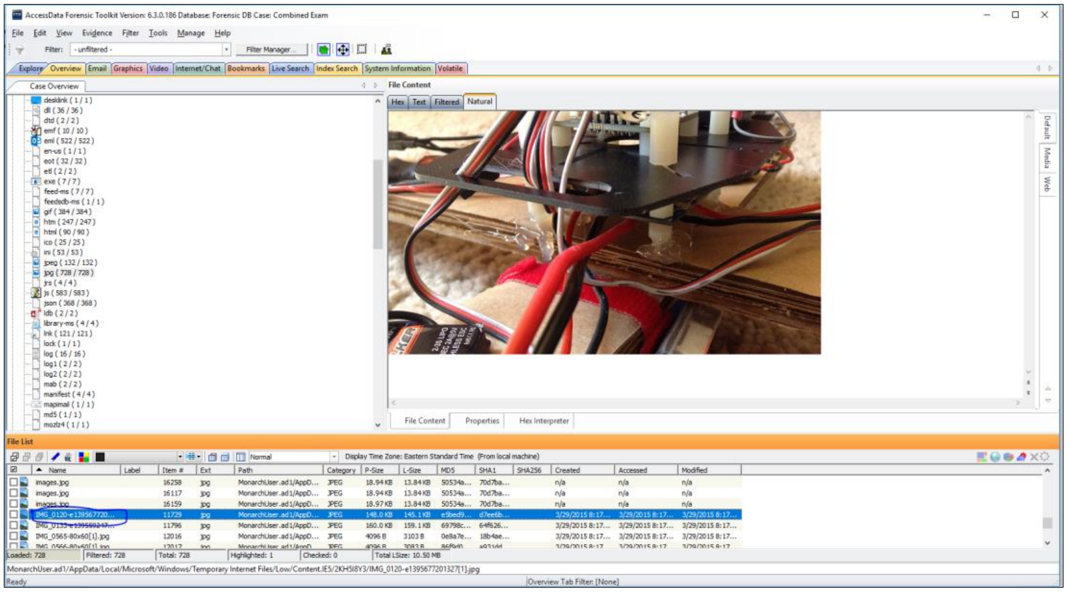
Display Time Zone: Eastern Standard Time (From local machine)

☑	Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
□	-crop-127-120-127px-A...		14524	jpg	MonarchUser.ad1/AppD...	JPEG	20.00 KB	16.98 KB	d9ec70...	1f94f1...		3/29/2015 7:19...	3/29/2015 7:19...	3/29/2015 7:19...
□	-crop-127-120-127px-R...		14520	jpg	MonarchUser.ad1/AppD...	JPEG	8192 B	4893 B	bff0a2...	e7bee0...		3/29/2015 7:19...	3/29/2015 7:19...	3/29/2015 7:19...
□	-crop-127-120-127px-T...		14312	jpg	MonarchUser.ad1/AppD...	JPEG	24.00 KB	22.51 KB	5e294c...	7d2504...		3/29/2015 7:19...	3/29/2015 7:19...	3/29/2015 7:19...
□	-crop-127-140-127px-B...		14315	jpg	MonarchUser.ad1/AppD...	JPEG	4096 B	2473 B	663cfa...	0190b1...		3/29/2015 7:19...	3/29/2015 7:19...	3/29/2015 7:19...
□	-crop-127-140-127px-C...		14531	jpg	MonarchUser.ad1/AppD...	JPEG	36.00 KB	33.83 KB	7c8fc3...	e023d5...		3/29/2015 7:19...	3/29/2015 7:19...	3/29/2015 7:19...
□	-crop-127-140-127px-C...		14735	jpg	MonarchUser.ad1/AppD...	JPEG	8192 B	6146 B	423ec4...	19c07b...		3/29/2015 7:19...	3/29/2015 7:19...	3/29/2015 7:19...
□	-crop-127-140-127px-M...		14522	jpg	MonarchUser.ad1/AppD...	JPEG	8192 B	4543 B	ef71aa...	4af57d...		3/29/2015 7:19...	3/29/2015 7:19...	3/29/2015 7:19...

Loaded: 728 | Filtered: 728 | Total: 728 | Highlighted: 1 | Checked: 0 | Total LSize: 10.50 MB

MonarchUser.ad1/AppData/Local/Microsoft/Windows/Temporary Internet Files/Low/Content.IE5/2KH5I8Y3/-crop-127-140-127px-Build-a-Mousetrap-Car-Step-14-Version-2[1].jpg

Ready | Overview Tab Filter: [None]



AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Combined Exam

File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered -
Filter Manager...
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
Case Overview
File Content
Hex Text Filtered Natural
Default Media Web
File Content Properties Hex Interpreter
File List
Normal

- desktlnk (1 / 1)
- dll (36 / 36)
- dtd (2 / 2)
- emf (10 / 10)
- eml (522 / 522)
- en-us (1 / 1)
- eot (32 / 32)
- etl (2 / 2)
- exe (7 / 7)
- feed-ms (7 / 7)
- feedsdb-ms (1 / 1)
- gif (384 / 384)
- htm (247 / 247)
- html (90 / 90)
- ico (25 / 25)
- ini (53 / 53)
- jpeg (132 / 132)
- jpg (728 / 728)
- jrs (4 / 4)
- js (583 / 583)
- json (368 / 368)
- ldb (2 / 2)
- library-ms (4 / 4)
- lnk (121 / 121)
- lock (1 / 1)
- log (16 / 16)
- log1 (2 / 2)
- log2 (2 / 2)
- mab (2 / 2)
- manifest (4 / 4)
- mapimail (1 / 1)
- md5 (1 / 1)
- mozlz4 (1 / 1)

Display Time Zone: Eastern Standard Time (From local machine)

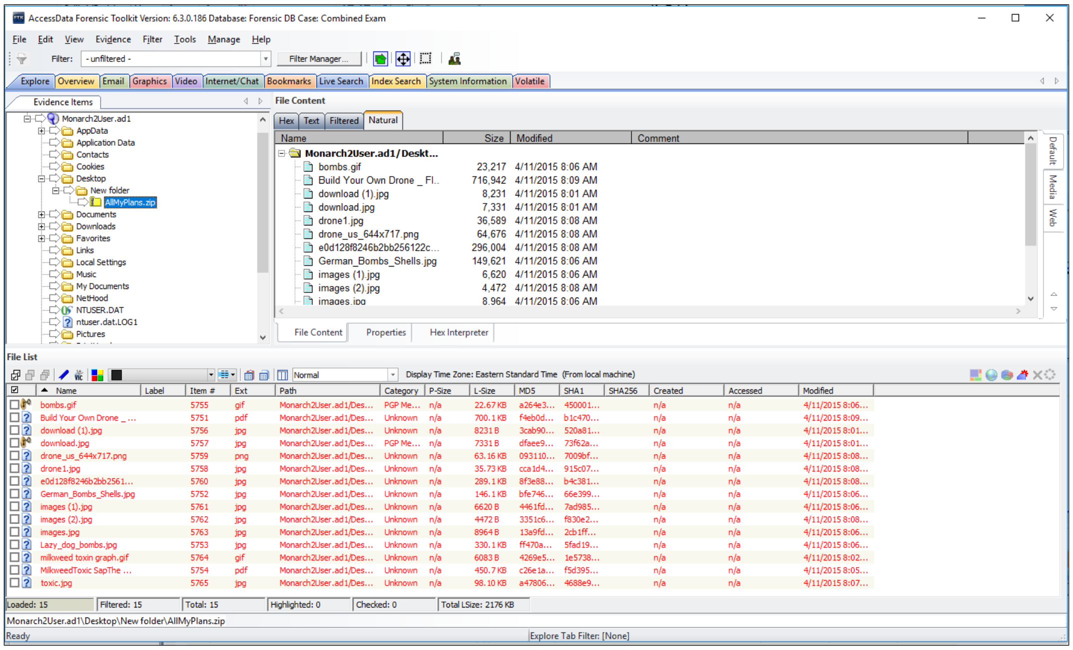
☑	Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
□	images.jpg		16258	jpg	MonarchUser.ad1/AppD...	JPEG	18.94 KB	13.84 KB	50534a...	70d7ba...		n/a	n/a	n/a
□	images.jpg		16117	jpg	MonarchUser.ad1/AppD...	JPEG	18.94 KB	13.84 KB	50534a...	70d7ba...		n/a	n/a	n/a
□	images.jpg		16159	jpg	MonarchUser.ad1/AppD...	JPEG	18.97 KB	13.84 KB	50534a...	70d7ba...		n/a	n/a	n/a
□	IMG_0120-e139567720...		11729	jpg	MonarchUser.ad1/AppD...	JPEG	148.0 KB	145.1 KB	e5bed9...	d7ee6b...		3/29/2015 8:17...	3/29/2015 8:17...	3/29/2015 8:17...
□	IMG_0135-e139559247...		11796	jpg	MonarchUser.ad1/AppD...	JPEG	160.0 KB	159.1 KB	69798c...	64f626...		3/29/2015 8:17...	3/29/2015 8:17...	3/29/2015 8:17...
□	IMG_0565-80x60[1].jpg		12016	jpg	MonarchUser.ad1/AppD...	JPEG	4096 B	3103 B	0e8a7e...	18b4ae...		3/29/2015 8:17...	3/29/2015 8:17...	3/29/2015 8:17...
□	IMG_0566-80x60[1].jpg		12017	jpg	MonarchUser.ad1/AppD...	JPEG	4096 B	3083 B	86f9d0...	a931dd...		3/29/2015 8:17...	3/29/2015 8:17...	3/29/2015 8:17...

Loaded: 728 | Filtered: 728 | Total: 728 | Highlighted: 1 | Checked: 0 | Total LSize: 10.50 MB

MonarchUser.ad1/AppData/Local/Microsoft/Windows/Temporary Internet Files/Low/Content.IE5/2KH5I8Y3/IMG_0120-e1395677201327[1].jpg

Ready | Overview Tab Filter: [None]

In explorer tab, I exported zip folder of MyPlans.



AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Combined Exam
File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered - Filter Manager...
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
Evidence Items
Monarch2User.ad1
AppData
Application Data
Contacts
Cookies
Desktop
New folder
AllMyPlans.zip
Documents
Downloads
Favorites
Links
Local Settings
Music
My Documents
NetHood
NTUSER.DAT
ntuser.dat.LOG1
Pictures
File Content
Hex Text Filtered Natural
File Content Properties Hex Interpreter
Default Media Web
File List
Normal
Display Time Zone: Eastern Standard Time (From local machine)

Name	Size	Modified	Comment
Monarch2User.ad1/Deskt...			
bombs.gif	23,217	4/11/2015 8:06 AM	
Build Your Own Drone _ Fl..	716,942	4/11/2015 8:09 AM	
download (1).jpg	8,231	4/11/2015 8:01 AM	
download.jpg	7,331	4/11/2015 8:01 AM	
drone1.jpg	36,589	4/11/2015 8:08 AM	
drone_us_644x717.png	64,676	4/11/2015 8:08 AM	
e0d128f8246b2bb256122c...	296,004	4/11/2015 8:08 AM	
German_Bombs_Shells.jpg	149,621	4/11/2015 8:06 AM	
images (1).jpg	6,620	4/11/2015 8:06 AM	
images (2).jpg	4,472	4/11/2015 8:08 AM	
images.jpg	8.964	4/11/2015 8:06 AM	

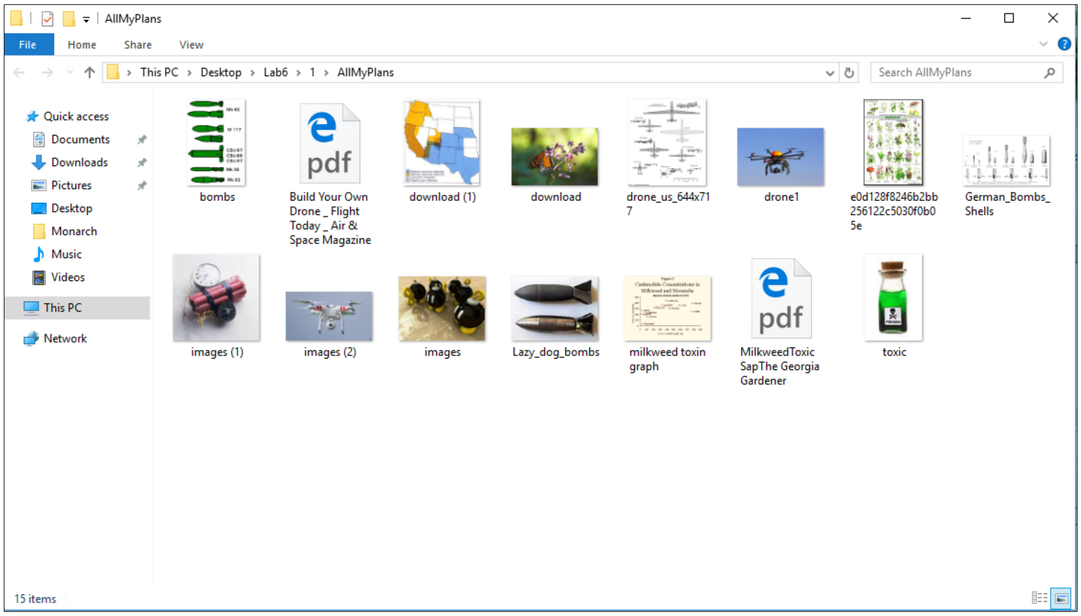
☑	Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
☐	bombs.gif		5755	gif	Monarch2User.ad1/Des...	PGP Me...	n/a	22.67 KB	a264e3...	450001...		n/a	n/a	4/11/2015 8:06...
☐	Build Your Own Drone _ ...		5751	pdf	Monarch2User.ad1/Des...	Unknown	n/a	700.1 KB	f4eb0d...	b1c470...		n/a	n/a	4/11/2015 8:09...
☐	download (1).jpg		5756	jpg	Monarch2User.ad1/Des...	Unknown	n/a	8231 B	3cab90...	520a81...		n/a	n/a	4/11/2015 8:01...
☐	download.jpg		5757	jpg	Monarch2User.ad1/Des...	PGP Me...	n/a	7331 B	dfaee9...	73f62a...		n/a	n/a	4/11/2015 8:01...
☐	drone_us_644x717.png		5759	png	Monarch2User.ad1/Des...	Unknown	n/a	63.16 KB	093110...	7009bf...		n/a	n/a	4/11/2015 8:08...
☐	drone1.jpg		5758	jpg	Monarch2User.ad1/Des...	Unknown	n/a	35.73 KB	cca1d4...	915c07...		n/a	n/a	4/11/2015 8:08...
☐	e0d128f8246b2bb2561...		5760	jpg	Monarch2User.ad1/Des...	Unknown	n/a	289.1 KB	8f3e88...	b4c381...		n/a	n/a	4/11/2015 8:08...
☐	German_Bombs_Shells.jpg		5752	jpg	Monarch2User.ad1/Des...	Unknown	n/a	146.1 KB	bfe746...	66e399...		n/a	n/a	4/11/2015 8:06...
☐	images (1).jpg		5761	jpg	Monarch2User.ad1/Des...	Unknown	n/a	6620 B	4461fd...	7ad985...		n/a	n/a	4/11/2015 8:06...
☐	images (2).jpg		5762	jpg	Monarch2User.ad1/Des...	Unknown	n/a	4472 B	3351c6...	f830e2...		n/a	n/a	4/11/2015 8:08...
☐	images.jpg		5763	jpg	Monarch2User.ad1/Des...	Unknown	n/a	8964 B	13a9fd...	2cb1ff...		n/a	n/a	4/11/2015 8:06...
☐	Lazy_dog_bombs.jpg		5753	jpg	Monarch2User.ad1/Des...	Unknown	n/a	330.1 KB	ff470a...	5fad19...		n/a	n/a	4/11/2015 8:06...
☐	milkweed toxin graph.gif		5764	gif	Monarch2User.ad1/Des...	Unknown	n/a	6083 B	4269e5...	1e5738...		n/a	n/a	4/11/2015 8:02...
☐	MilkweedToxic SapThe ...		5754	pdf	Monarch2User.ad1/Des...	Unknown	n/a	450.7 KB	c26e1a...	f5d395...		n/a	n/a	4/11/2015 8:05...
☐	toxic.jpg		5765	jpg	Monarch2User.ad1/Des...	Unknown	n/a	98.10 KB	a47806...	4688e9...		n/a	n/a	4/11/2015 8:07...

Loaded: 15 | Filtered: 15 | Total: 15 | Highlighted: 0 | Checked: 0 | Total LSize: 2176 KB

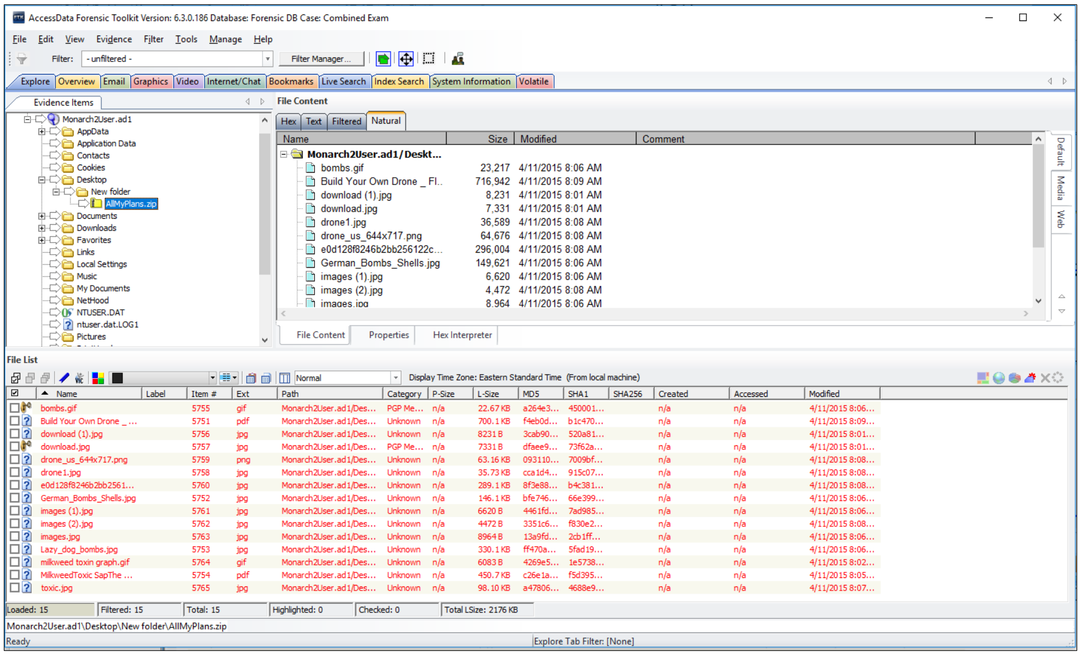
Monarch2User.ad1\Desktop\New folder\AllMyPlans.zip

Ready | Explore Tab Filter: [None]

After decrypting the above file using Password Recovery Toolkit, I found items like explosives, drones, poisons and bombs as shown below.



5. Can you recover any passwords?


AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Combined Exam
File Edit View Evidence Filter Tools Manage Help
Filter: - unfiltered -
Filter Manager...
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
Evidence Items
Monarch2User.ad1
AppData
Application Data
Contacts
Cookies
Desktop
New folder
AllMyPlans.zip
Documents
Downloads
Favorites
Links
Local Settings
Music
My Documents
NetHood
NTUSER.DAT
ntuser.dat.LOG1
Pictures
File Content
Hex Text Filtered Natural
File Content Properties Hex Interpreter
Default Media Web
File List
Normal

Name	Size	Modified	Comment
Monarch2User.ad1/Deskt...			
bombs.gif	23,217	4/11/2015 8:06 AM	
Build Your Own Drone _ Fl..	716,942	4/11/2015 8:09 AM	
download (1).jpg	8,231	4/11/2015 8:01 AM	
download.jpg	7,331	4/11/2015 8:01 AM	
drone1.jpg	36,589	4/11/2015 8:08 AM	
drone_us_644x717.png	64,676	4/11/2015 8:08 AM	
e0d128f8246b2bb256122c...	296,004	4/11/2015 8:08 AM	
German_Bombs_Shells.jpg	149,621	4/11/2015 8:06 AM	
images (1).jpg	6,620	4/11/2015 8:06 AM	
images (2).jpg	4,472	4/11/2015 8:08 AM	
images.jpg	8.964	4/11/2015 8:06 AM	

Display Time Zone: Eastern Standard Time (From local machine)

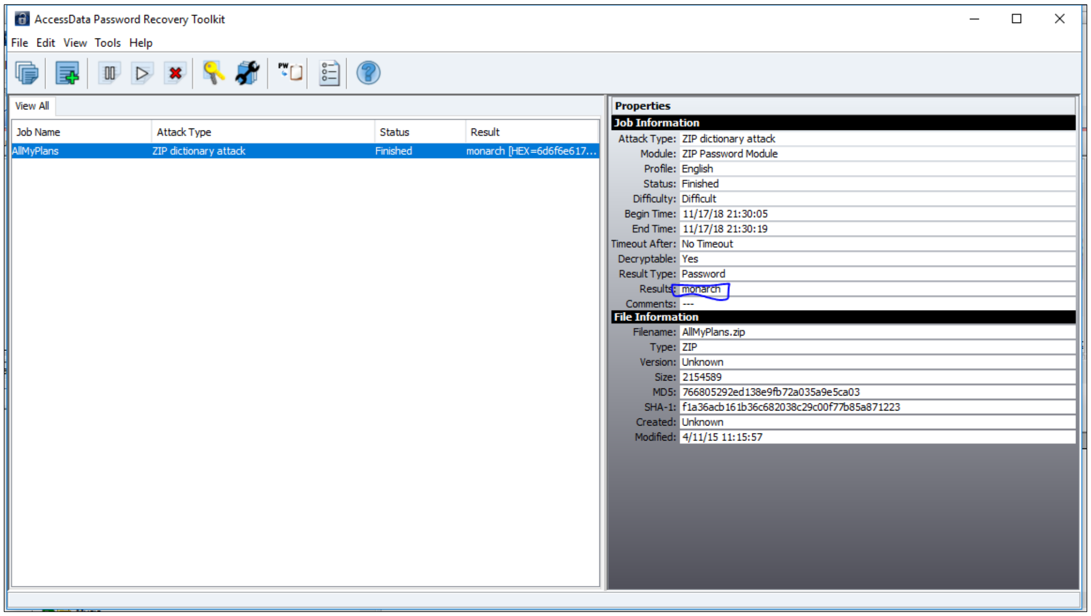
☑	Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
☐	bombs.gif		5755	gif	Monarch2User.ad1/Des...	PGP Me...	n/a	22.67 KB	a264e3...	450001...		n/a	n/a	4/11/2015 8:06...
☐	Build Your Own Drone _ ...		5751	pdf	Monarch2User.ad1/Des...	Unknown	n/a	700.1 KB	f4eb0d...	b1c470...		n/a	n/a	4/11/2015 8:09...
☐	download (1).jpg		5756	jpg	Monarch2User.ad1/Des...	Unknown	n/a	8231 B	3cab90...	520a81...		n/a	n/a	4/11/2015 8:01...
☐	download.jpg		5757	jpg	Monarch2User.ad1/Des...	PGP Me...	n/a	7331 B	dfaee9...	73f62a...		n/a	n/a	4/11/2015 8:01...
☐	drone_us_644x717.png		5759	png	Monarch2User.ad1/Des...	Unknown	n/a	63.16 KB	093110...	7009bf...		n/a	n/a	4/11/2015 8:08...
☐	drone1.jpg		5758	jpg	Monarch2User.ad1/Des...	Unknown	n/a	35.73 KB	cca1d4...	915c07...		n/a	n/a	4/11/2015 8:08...
☐	e0d128f8246b2bb2561...		5760	jpg	Monarch2User.ad1/Des...	Unknown	n/a	289.1 KB	8f3e88...	b4c381...		n/a	n/a	4/11/2015 8:08...
☐	German_Bombs_Shells.jpg		5752	jpg	Monarch2User.ad1/Des...	Unknown	n/a	146.1 KB	bfe746...	66e399...		n/a	n/a	4/11/2015 8:06...
☐	images (1).jpg		5761	jpg	Monarch2User.ad1/Des...	Unknown	n/a	6620 B	4461fd...	7ad985...		n/a	n/a	4/11/2015 8:06...
☐	images (2).jpg		5762	jpg	Monarch2User.ad1/Des...	Unknown	n/a	4472 B	3351c6...	f830e2...		n/a	n/a	4/11/2015 8:08...
☐	images.jpg		5763	jpg	Monarch2User.ad1/Des...	Unknown	n/a	8964 B	13a9fd...	2cb1ff...		n/a	n/a	4/11/2015 8:06...
☐	Lazy_dog_bombs.jpg		5753	jpg	Monarch2User.ad1/Des...	Unknown	n/a	330.1 KB	ff470a...	5fad19...		n/a	n/a	4/11/2015 8:06...
☐	milkweed toxin graph.gif		5764	gif	Monarch2User.ad1/Des...	Unknown	n/a	6083 B	4269e5...	1e5738...		n/a	n/a	4/11/2015 8:02...
☐	MilkweedToxic SapThe ...		5754	pdf	Monarch2User.ad1/Des...	Unknown	n/a	450.7 KB	c26e1a...	f5d395...		n/a	n/a	4/11/2015 8:05...
☐	toxic.jpg		5765	jpg	Monarch2User.ad1/Des...	Unknown	n/a	98.10 KB	a47806...	4688e9...		n/a	n/a	4/11/2015 8:07...

Loaded: 15 | Filtered: 15 | Total: 15 | Highlighted: 0 | Checked: 0 | Total LSize: 2176 KB

Monarch2User.ad1\Desktop\New folder\AllMyPlans.zip

Ready | Explore Tab Filter: [None]

To crack the password of the above file named ‘AllMyPlans.zip’, I used **PRTK**. The password of ‘AllMyPlans.zip’ is “monarch”.


AccessData Password Recovery Toolkit
File Edit View Tools Help
View All

Job Name	Attack Type	Status	Result
AllMyPlans	ZIP dictionary attack	Finished	monarch [HEX=6d6f6e617...

Properties

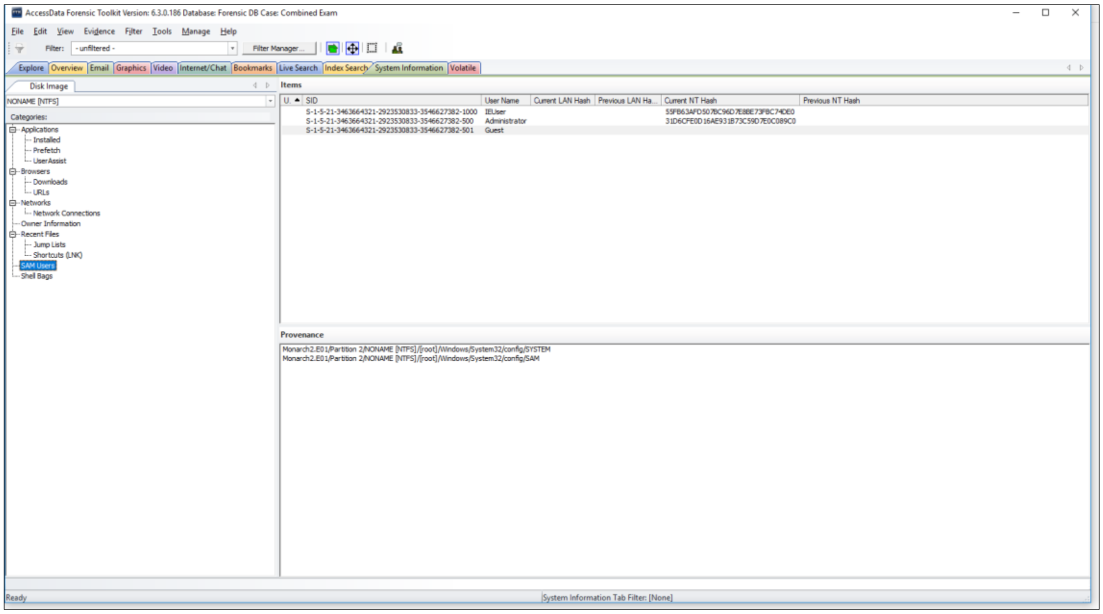
Job Information

Attack Type:	ZIP dictionary attack
Module:	ZIP Password Module
Profile:	English
Status:	Finished
Difficulty:	Difficult
Begin Time:	11/17/18 21:30:05
End Time:	11/17/18 21:30:19
Timeout After:	No Timeout
Decryptable:	Yes
Result Type:	Password
Results:	monarch
Comments:	---

File Information

Filename:	AllMyPlans.zip
Type:	ZIP
Version:	Unknown
Size:	2154589
MD5:	766805292ed138e9fb72a035a9e5ca03
SHA-1:	f1a36acb161b36c682038c29c00f77b85a871223
Created:	Unknown
Modified:	4/11/15 11:15:57

After exporting ‘SAM’ and ‘SYSTEM’ files from ‘ Monarch2.E01’, I cracked the user account password using PRTK as shown below. The password for the user account is “guest123”.



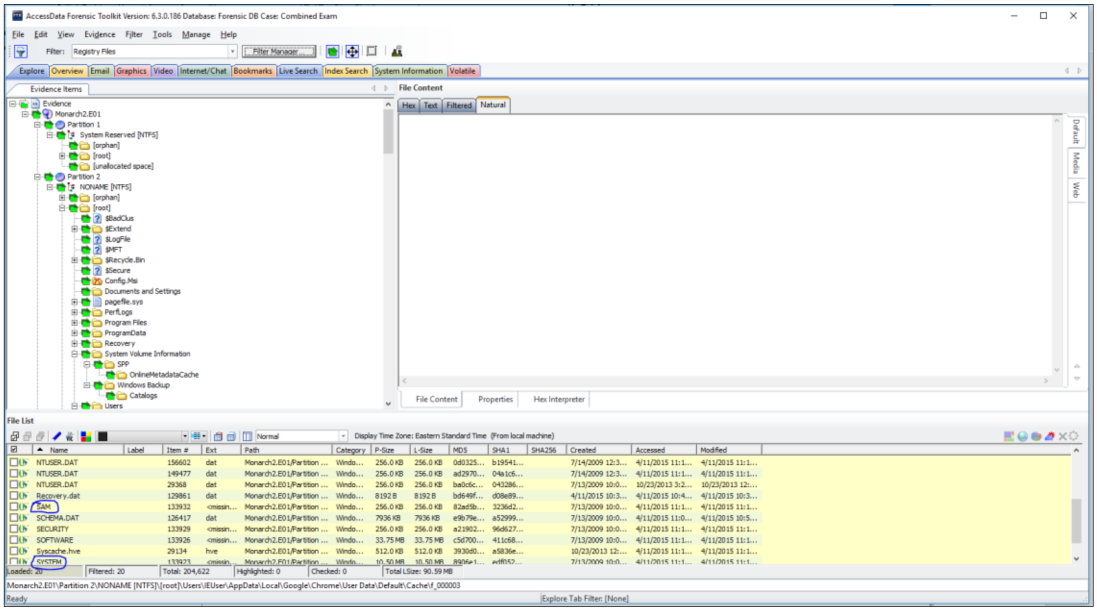
AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Combined Exam

U.	SID	User Name	Current LAN Hash	Previous LAN Ha...	Current NT Hash	Previous NT Hash
	S-1-5-21-3463664321-2923530833-3546627382-1000	IEUser			55FB63AFD507BC96D7E8BE73FBC74DE0	
	S-1-5-21-3463664321-2923530833-3546627382-500	Administrator			31D6CFE0D16AE931B73C59D7E0C089C0	
	S-1-5-21-3463664321-2923530833-3546627382-501	Guest				

Provenance

```
Monarch2.E01/Partition 2/NONAME [NTFS]/[root]/Windows/System32/config/SYSTEM
Monarch2.E01/Partition 2/NONAME [NTFS]/[root]/Windows/System32/config/SAM
```

Ready | System Information Tab Filter: [None]



AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Combined Exam

Display Time Zone: Eastern Standard Time (From local machine)

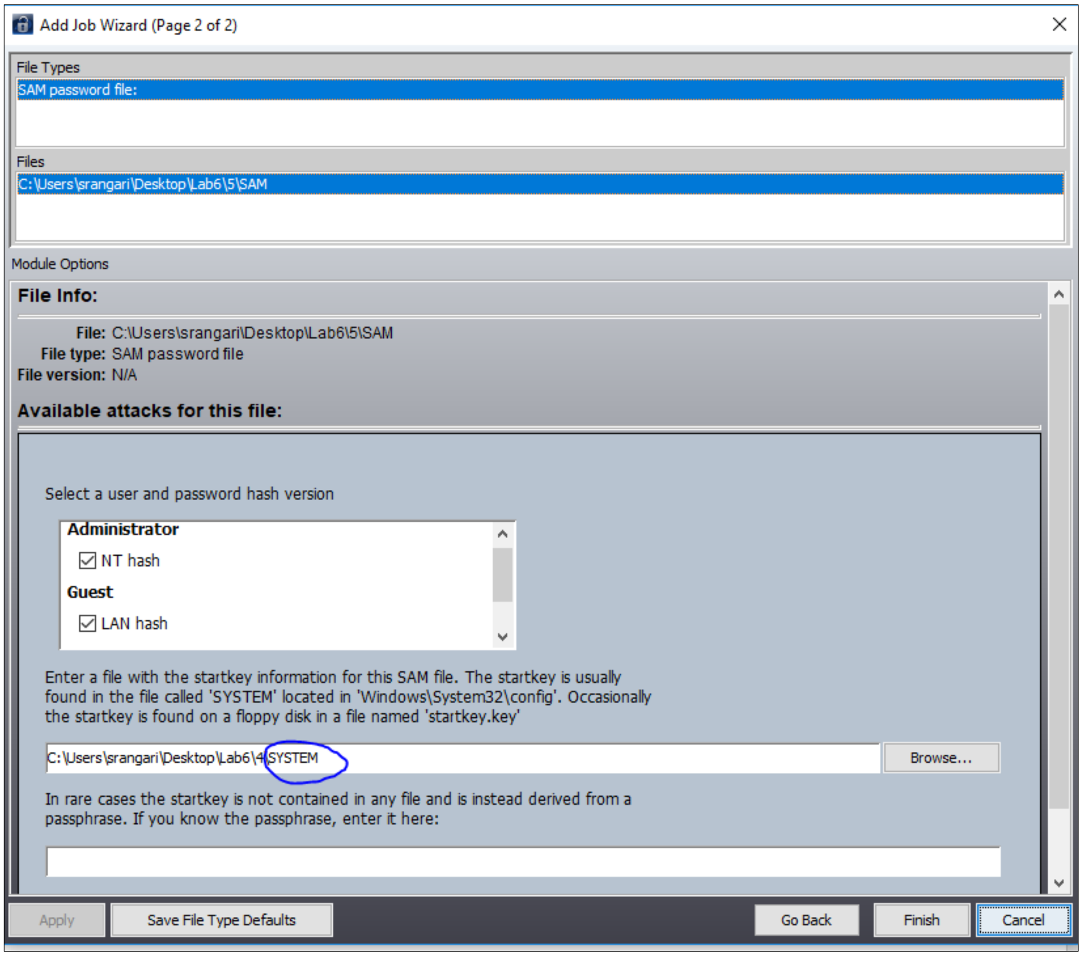
☑	Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
□	NTUSER.DAT		156602	dat	Monarch2.E01/Partition ...	Windo...	256.0 KB	256.0 KB	0d0325...	b19541...		7/14/2009 12:3...	4/11/2015 11:1...	4/11/2015 11:1...
□	NTUSER.DAT		149477	dat	Monarch2.E01/Partition ...	Windo...	256.0 KB	256.0 KB	ad2970...	04a1c6...		7/14/2009 12:3...	4/11/2015 11:1...	4/11/2015 11:1...
□	NTUSER.DAT		29368	dat	Monarch2.E01/Partition ...	Windo...	256.0 KB	256.0 KB	ba0c6c...	043286...		7/13/2009 10:0...	10/23/2013 3:2...	10/23/2013 12:...
□	Recovery.dat		129861	dat	Monarch2.E01/Partition ...	Windo...	8192 B	8192 B	bd649f...	d08e89...		4/11/2015 10:3...	4/11/2015 10:4...	4/11/2015 10:3...
□	SAM		133932	<missin...	Monarch2.E01/Partition ...	Windo...	256.0 KB	256.0 KB	82ad5b...	3236d2...		7/13/2009 10:0...	4/11/2015 11:1...	4/11/2015 11:1...
□	SCHEMA.DAT		126417	dat	Monarch2.E01/Partition ...	Windo...	7936 KB	7936 KB	e9b79e...	a52999...		7/13/2009 10:0...	4/11/2015 11:0...	4/11/2015 10:5...
□	SECURITY		133929	<missin...	Monarch2.E01/Partition ...	Windo...	256.0 KB	256.0 KB	a21902...	96d627...		7/13/2009 10:0...	4/11/2015 11:1...	4/11/2015 11:1...
□	SOFTWARE		133926	<missin...	Monarch2.E01/Partition ...	Windo...	33.75 MB	33.75 MB	c5d700...	411c68...		7/13/2009 10:0...	4/11/2015 11:1...	4/11/2015 11:1...
□	Syscache.hve		29134	hve	Monarch2.E01/Partition ...	Windo...	512.0 KB	512.0 KB	3930d0...	a5836e...		10/23/2013 12:...	4/11/2015 11:1...	4/11/2015 11:1...
□	SYSTEM		133923	<missin...	Monarch2.E01/Partition ...	Windo...	10.50 MB	10.50 MB	8906e1...	edf052...		7/13/2009 10:0...	4/11/2015 11:1...	4/11/2015 11:1...

Loaded: 20 | Filtered: 20 | Total: 204,622 | Highlighted: 0 | Checked: 0 | Total LSize: 90.59 MB

Monarch2.E01\Partition 2\NONAME [NTFS]\[root]\Users\IEUser\AppData\Local\Google\Chrome\User Data\Default\Cache\f_000003

Ready | Explore Tab Filter: [None]

In PRTK:



File Types

SAM password file:

Files

C:\Users\srangari\Desktop\Lab6\5\SAM

Module Options

File Info:

File: C:\Users\srangari\Desktop\Lab6\5\SAM
File type: SAM password file
File version: N/A

Available attacks for this file:

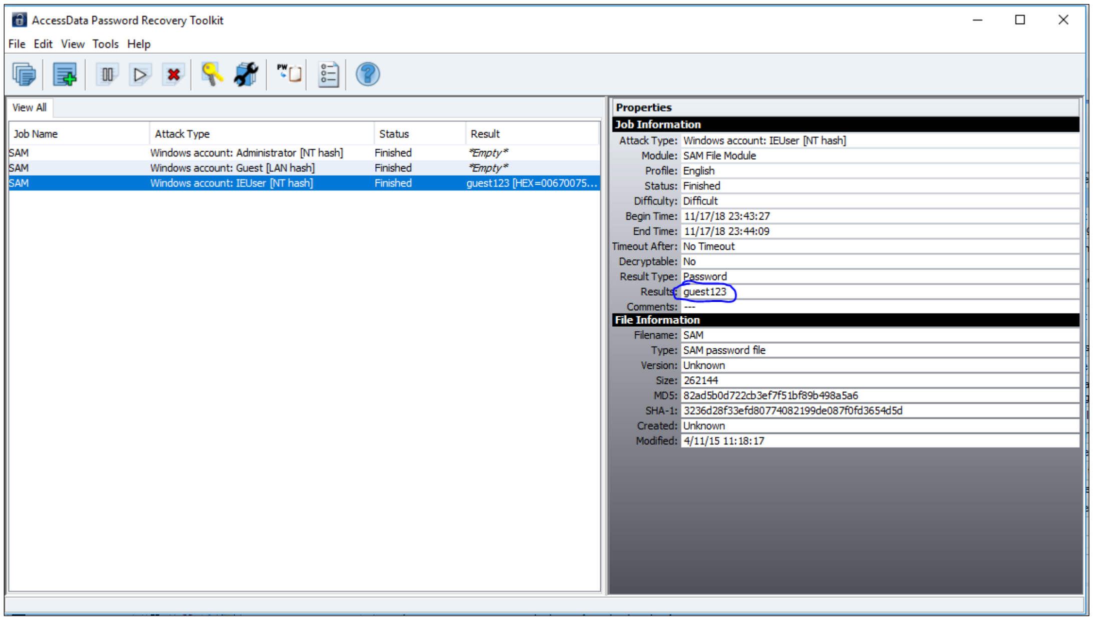
Select a user and password hash version

Administrator
☑ NT hash
Guest
☑ LAN hash

Enter a file with the startkey information for this SAM file. The startkey is usually found in the file called 'SYSTEM' located in 'Windows\System32\config'. Occasionally the startkey is found on a floppy disk in a file named 'startkey.key'

C:\Users\srangari\Desktop\Lab6\4\SYSTEM

In rare cases the startkey is not contained in any file and is instead derived from a passphrase. If you know the passphrase, enter it here:


AccessData Password Recovery Toolkit
File Edit View Tools Help
View All

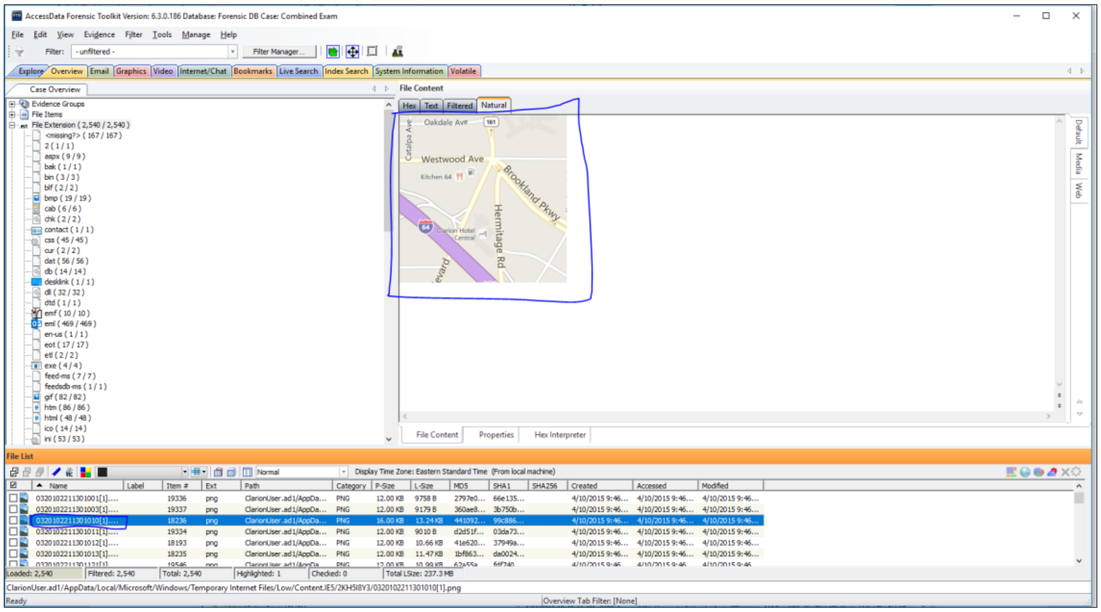
Job Name	Attack Type	Status	Result
SAM	Windows account: Administrator [NT hash]	Finished	*Empty*
SAM	Windows account: Guest [LAN hash]	Finished	*Empty*
SAM	Windows account: IEUser [NT hash]	Finished	guest123 [HEX=00670075...

Properties

Job Information	
Attack Type:	Windows account: IEUser [NT hash]
Module:	SAM File Module
Profile:	English
Status:	Finished
Difficulty:	Difficult
Begin Time:	11/17/18 23:43:27
End Time:	11/17/18 23:44:09
Timeout After:	No Timeout
Decryptable:	No
Result Type:	Password
Results:	guest123
Comments:	---
File Information	
Filename:	SAM
Type:	SAM password file
Version:	Unknown
Size:	262144
MD5:	82ad5b0d722cb3ef7f51bf89b498a5a6
SHA-1:	3236d28f33efd80774082199de087f0fd3654d5d
Created:	Unknown
Modified:	4/11/15 11:18:17

6. Is there any evidence the Monarch planned to stay in the particular hotel?

In the image 'ClarionUser.ad1', I found the following location of the 'Clarion Hotel'.



AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Combined Exam

Filter: - unfiltered -

- Evidence Groups
- File Items
- File Extension (2,540 / 2,540)
  - <missing?> (167 / 167)
  - 2 (1 / 1)
  - aspx (9 / 9)
  - bak (1 / 1)
  - bin (3 / 3)
  - blf (2 / 2)
  - bmp (19 / 19)
  - cab (6 / 6)
  - chk (2 / 2)
  - contact (1 / 1)
  - css (45 / 45)
  - cur (2 / 2)
  - dat (56 / 56)
  - db (14 / 14)
  - desklink (1 / 1)
  - dll (32 / 32)
  - dtd (1 / 1)
  - emf (10 / 10)
  - eml (469 / 469)
  - en-us (1 / 1)
  - eot (17 / 17)
  - etl (2 / 2)
  - exe (4 / 4)
  - feed-ms (7 / 7)
  - feedsdb-ms (1 / 1)
  - gif (82 / 82)
  - htm (86 / 86)
  - html (48 / 48)
  - ico (14 / 14)
  - ini (53 / 53)

Normal | Display Time Zone: Eastern Standard Time (From local machine)

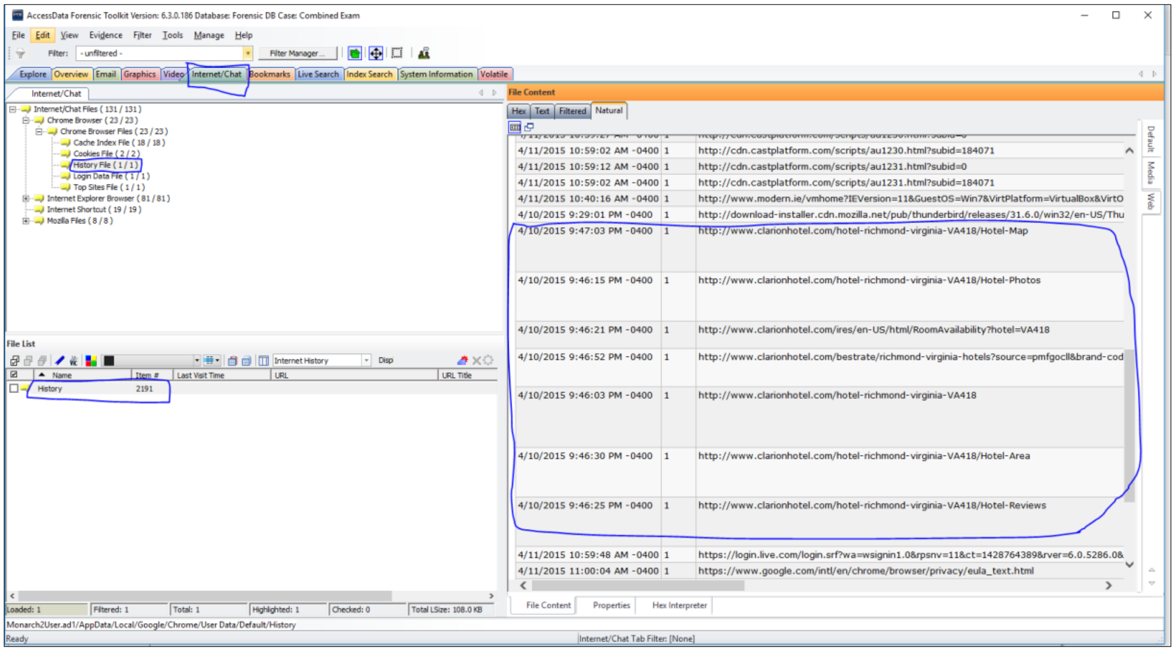
☑	Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
□	0320102211301001[1]....		19336	png	ClarionUser.ad1/AppDa...	PNG	12.00 KB	9758 B	2797e0...	66e135...		4/10/2015 9:46...	4/10/2015 9:46...	4/10/2015 9:46...
□	0320102211301003[1]....		19337	png	ClarionUser.ad1/AppDa...	PNG	12.00 KB	9179 B	360ae8...	3b750b...		4/10/2015 9:46...	4/10/2015 9:46...	4/10/2015 9:46...
□	0320102211301010[1]....		18236	png	ClarionUser.ad1/AppDa...	PNG	16.00 KB	13.24 KB	441092...	99c886...		4/10/2015 9:46...	4/10/2015 9:46...	4/10/2015 9:46...
□	0320102211301011[1]....		19334	png	ClarionUser.ad1/AppDa...	PNG	12.00 KB	9010 B	d2d51f...	03da73...		4/10/2015 9:46...	4/10/2015 9:46...	4/10/2015 9:46...
□	0320102211301012[1]....		18193	png	ClarionUser.ad1/AppDa...	PNG	12.00 KB	10.66 KB	41e620...	37949a...		4/10/2015 9:46...	4/10/2015 9:46...	4/10/2015 9:46...
□	0320102211301013[1]....		18235	png	ClarionUser.ad1/AppDa...	PNG	12.00 KB	11.47 KB	1bf863...	da0024...		4/10/2015 9:46...	4/10/2015 9:46...	4/10/2015 9:46...
□	0320102211301121[1]		19546	png	ClarionUser.ad1/AppDa	PNG	12.00 KB	10.99 KB	62a55a	fdf740		4/10/2015 9:46	4/10/2015 9:46	4/10/2015 9:46

Loaded: 2,540 | Filtered: 2,540 | Total: 2,540 | Highlighted: 1 | Checked: 0 | Total LSize: 237.3 MB

ClarionUser.ad1/AppData/Local/Microsoft/Windows/Temporary Internet Files/Low/Content.IE5/2KH5I8Y3/0320102211301010[1].png

Ready | Overview Tab Filter: [None]

Additionally, in the "Internet/chat" tab, in the history file, I found the various search results of " Clarion Hotel" as shown below.



AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Combined Exam

Filter: - unfiltered -

- Internet/Chat Files (131 / 131)
  - Chrome Browser (23 / 23)
    - Chrome Browser Files (23 / 23)
      - Cache Index File (18 / 18)
      - Cookies File (2 / 2)
      - History File (1 / 1)
      - Login Data File (1 / 1)
      - Top Sites File (1 / 1)
  - Internet Explorer Browser (81 / 81)
  - Internet Shortcut (19 / 19)
  - Mozilla Files (8 / 8)

Internet History

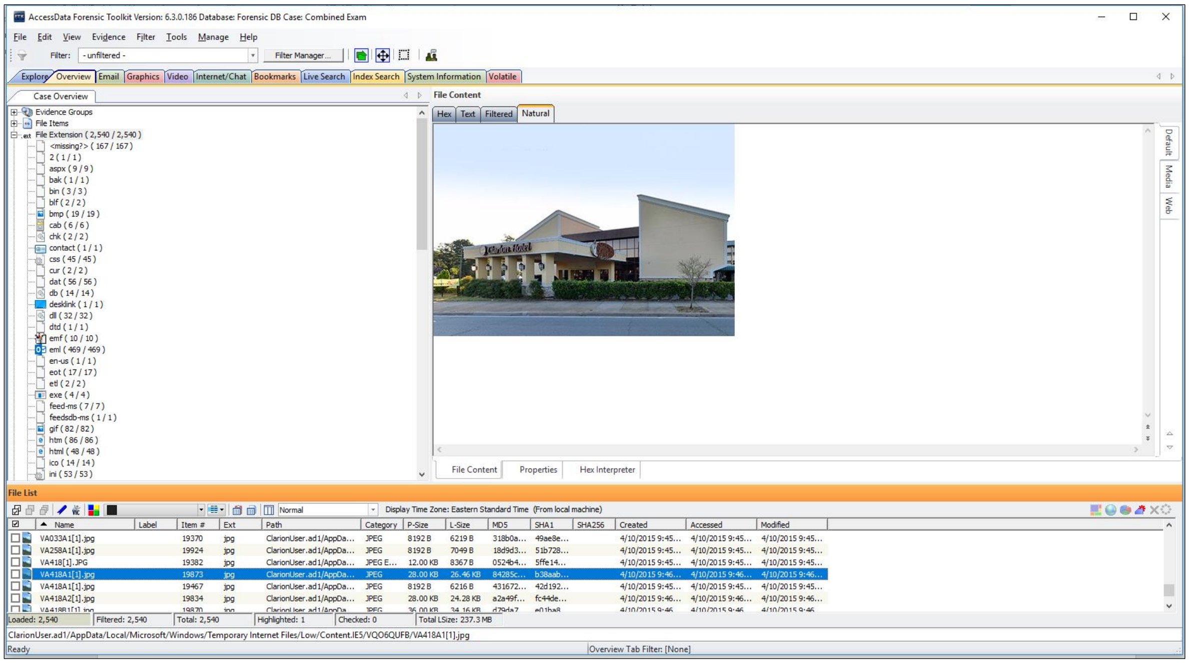
☑	Name	Item #	Last Visit Time	URL	URL Title
□	History	2191			

Loaded: 1 | Filtered: 1 | Total: 1 | Highlighted: 1 | Checked: 0 | Total LSize: 108.0 KB

Monarch2User.ad1/AppData/Local/Google/Chrome/User Data/Default/History

Ready | Internet/Chat Tab Filter: [None]

4/11/2015 10:59:27 AM -0400	1	http://cdn.castplatform.com/scripts/au1230.html?subid=0
4/11/2015 10:59:02 AM -0400	1	http://cdn.castplatform.com/scripts/au1230.html?subid=184071
4/11/2015 10:59:12 AM -0400	1	http://cdn.castplatform.com/scripts/au1231.html?subid=0
4/11/2015 10:59:02 AM -0400	1	http://cdn.castplatform.com/scripts/au1231.html?subid=184071
4/11/2015 10:40:16 AM -0400	1	http://www.modern.ie/vmhome?IEVersion=11&GuestOS=Win7&VirtPlatform=VirtualBox&VirtO
4/10/2015 9:29:01 PM -0400	1	http://download-installer.cdn.mozilla.net/pub/thunderbird/releases/31.6.0/win32/en-US/Thu
4/10/2015 9:47:03 PM -0400	1	http://www.clarionhotel.com/hotel-richmond-virginia-VA418/Hotel-Map
4/10/2015 9:46:15 PM -0400	1	http://www.clarionhotel.com/hotel-richmond-virginia-VA418/Hotel-Photos
4/10/2015 9:46:21 PM -0400	1	http://www.clarionhotel.com/ires/en-US/html/RoomAvailability?hotel=VA418
4/10/2015 9:46:52 PM -0400	1	http://www.clarionhotel.com/bestrate/richmond-virginia-hotels?source=pmfgocll&brand-cod
4/10/2015 9:46:03 PM -0400	1	http://www.clarionhotel.com/hotel-richmond-virginia-VA418
4/10/2015 9:46:30 PM -0400	1	http://www.clarionhotel.com/hotel-richmond-virginia-VA418/Hotel-Area
4/10/2015 9:46:25 PM -0400	1	http://www.clarionhotel.com/hotel-richmond-virginia-VA418/Hotel-Reviews
4/11/2015 10:59:48 AM -0400	1	https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=11&ct=1428764389&rver=6.0.5286.0&
4/11/2015 11:00:04 AM -0400	1	https://www.google.com/intl/en/chrome/browser/privacy/eula_text.html


File Edit View Evidence Filter Tools Manage Help
Filter Manager...
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
Hex Text Filtered Natural
Default Media Web
File Content Properties Hex Interpreter

AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Combined Exam

Filter: - unfiltered -

Case Overview

- Evidence Groups
- File Items
- File Extension (2,540 / 2,540)
  - <missing?> (167 / 167)
  - 2 (1 / 1)
  - aspx (9 / 9)
  - bak (1 / 1)
  - bin (3 / 3)
  - blf (2 / 2)
  - bmp (19 / 19)
  - cab (6 / 6)
  - chk (2 / 2)
  - contact (1 / 1)
  - css (45 / 45)
  - cur (2 / 2)
  - dat (56 / 56)
  - db (14 / 14)
  - desklink (1 / 1)
  - dll (32 / 32)
  - dtd (1 / 1)
  - emf (10 / 10)
  - eml (469 / 469)
  - en-us (1 / 1)
  - eot (17 / 17)
  - etl (2 / 2)
  - exe (4 / 4)
  - feed-ms (7 / 7)
  - feedsdb-ms (1 / 1)
  - gif (82 / 82)
  - htm (86 / 86)
  - html (48 / 48)
  - ico (14 / 14)
  - ini (53 / 53)

File Content

File List

Normal   Display Time Zone: Eastern Standard Time (From local machine)

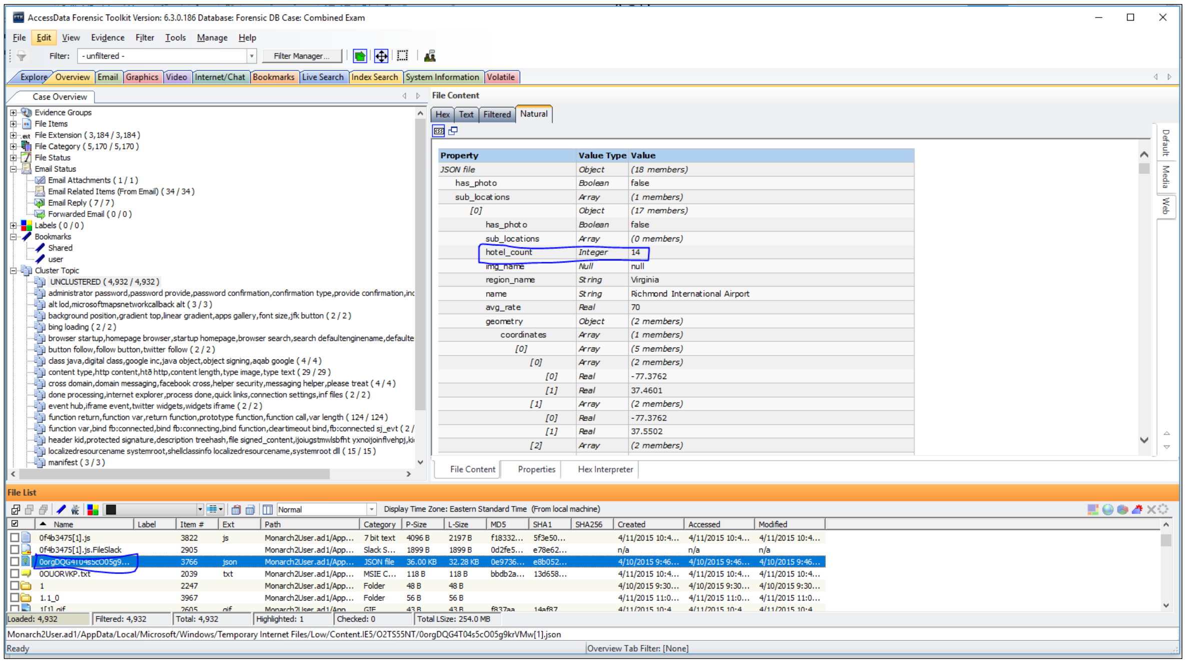
☑	Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
☐	VA033A1[1].jpg		19370	jpg	ClarionUser.ad1/AppDa...	JPEG	8192 B	6219 B	318b0a...	49ae8e...		4/10/2015 9:45...	4/10/2015 9:45...	4/10/2015 9:45...
☐	VA258A1[1].jpg		19924	jpg	ClarionUser.ad1/AppDa...	JPEG	8192 B	7049 B	18d9d3...	51b728...		4/10/2015 9:45...	4/10/2015 9:45...	4/10/2015 9:45...
☐	VA418[1].JPG		19382	jpg	ClarionUser.ad1/AppDa...	JPEG E...	12.00 KB	8367 B	0524b4...	5ffe14...		4/10/2015 9:45...	4/10/2015 9:45...	4/10/2015 9:45...
☐	VA418A1[1].jpg		19873	jpg	ClarionUser.ad1/AppDa...	JPEG	28.00 KB	26.46 KB	84285c...	b38aab...		4/10/2015 9:46...	4/10/2015 9:46...	4/10/2015 9:46...
☐	VA418A1[1].jpg		19467	jpg	ClarionUser.ad1/AppDa...	JPEG	8192 B	6216 B	431672...	42d192...		4/10/2015 9:45...	4/10/2015 9:45...	4/10/2015 9:45...
☐	VA418A2[1].jpg		19834	jpg	ClarionUser.ad1/AppDa...	JPEG	28.00 KB	24.28 KB	a2a49f...	fc44de...		4/10/2015 9:46...	4/10/2015 9:46...	4/10/2015 9:46...
☐	VA418B1[1].jpg		19870	jpg	ClarionUser.ad1/AppDa...	JPEG	36.00 KB	34.16 KB	d79da7	e01ba8		4/10/2015 9:46	4/10/2015 9:46	4/10/2015 9:46

Loaded: 2,540 | Filtered: 2,540 | Total: 2,540 | Highlighted: 1 | Checked: 0 | Total LSize: 237.3 MB

ClarionUser.ad1/AppData/Local/Microsoft/Windows/Temporary Internet Files/Low/Content.IE5/VQO6QUFB/VA418A1[1].jpg

Ready   Overview Tab Filter: [None]

Also, in “overview” tab, exploring the json file shows various details related hotel.


File Edit View Evidence Filter Tools Manage Help
Filter Manager...
Explore Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile
Hex Text Filtered Natural
Default Media Web
File Content Properties Hex Interpreter

AccessData Forensic Toolkit Version: 6.3.0.186 Database: Forensic DB Case: Combined Exam

Filter: - unfiltered -

Case Overview

- Evidence Groups
- File Items
- File Extension (3,184 / 3,184)
- File Category (5,170 / 5,170)
- File Status
- Email Status
  - Email Attachments (1 / 1)
  - Email Related Items (From Email) (34 / 34)
  - Email Reply (7 / 7)
  - Forwarded Email (0 / 0)
- Labels (0 / 0)
- Bookmarks
  - Shared
  - user
- Cluster Topic
  - UNCLUSTERED (4,932 / 4,932)
  - administrator password,password provide,password confirmation,confirmation type,provide confirmation,inc
  - alt lod,microsoftmapsnetworkcallback alt (3 / 3)
  - background position,gradient top,linear gradient,apps gallery,font size,jfk button (2 / 2)
  - bing loading (2 / 2)
  - browser startup,homepage browser,startup homepage,browser search,search defaultenginename,defaulte
  - button follow,follow button,twitter follow (2 / 2)
  - class java,digital class,google inc,java object,object signing,aqab google (4 / 4)
  - content type,http content,htā http,content length,type image,type text (29 / 29)
  - cross domain,domain messaging,facebook cross,helper security,messaging helper,please treat (4 / 4)
  - done processing,internet explorer,process done,quick links,connection settings,inf files (2 / 2)
  - event hub,iframe event,twitter widgets,widgets iframe (2 / 2)
  - function return,function var,return function,prototype function,function call,var length (124 / 124)
  - function var,bind fb:connected,bind fb:connecting,bind function,cleartimeout bind,fb:connected sj_evt (2 /
  - header kid,protected signature,description treehash,file signed_content,ijoiugstmwlsbfht yxnoijoinflvehpj,ki
  - localizedresourcename systemroot,shellclassinfo localizedresourcename,systemroot dll (15 / 15)
  - manifest (3 / 3)

File Content

Property	Value Type	Value
JSON file	Object	(18 members)
has_photo	Boolean	false
sub_locations	Array	(1 members)
[0]	Object	(17 members)
has_photo	Boolean	false
sub_locations	Array	(0 members)
hotel_count	Integer	14
img_name	Null	null
region_name	String	Virginia
name	String	Richmond International Airport
avg_rate	Real	70
geometry	Object	(2 members)
coordinates	Array	(1 members)
[0]	Array	(5 members)
[0]	Array	(2 members)
[0]	Real	-77.3762
[1]	Real	37.4601
[1]	Array	(2 members)
[0]	Real	-77.3762
[1]	Real	37.5502
[2]	Array	(2 members)

File List

Normal   Display Time Zone: Eastern Standard Time (From local machine)

☑	Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
☐	0f4b3475[1].js		3822	js	Monarch2User.ad1/App...	7 bit text	4096 B	2197 B	f18332...	5f3e50...		4/11/2015 10:4...	4/11/2015 10:4...	4/11/2015 10:4...
☐	0f4b3475[1].js.FileSlack		2905		Monarch2User.ad1/App...	Slack S...	1899 B	1899 B	0d2fe5...	e78e62...		n/a	n/a	n/a
☐	0orgDQG4T04s5cO05g9...		3766	json	Monarch2User.ad1/App...	JSON file	36.00 KB	32.28 KB	0e9736...	e8b052...		4/10/2015 9:46...	4/10/2015 9:46...	4/10/2015 9:46...
☐	0OUORVKP.txt		2039	txt	Monarch2User.ad1/App...	MSIE C...	118 B	118 B	bbdb2a...	13d658...		4/11/2015 10:4...	4/11/2015 10:4...	4/11/2015 10:4...
☐	1		2247		Monarch2User.ad1/App...	Folder	48 B	48 B				4/10/2015 9:30...	4/10/2015 9:30...	4/10/2015 9:30...
☐	1.1_0		3967		Monarch2User.ad1/App...	Folder	56 B	56 B				4/11/2015 11:0...	4/11/2015 11:0...	4/11/2015 11:0...
☐	1[1].gif		2605	gif	Monarch2User.ad1/App	GIF	43 B	43 B	f837aa	14af87		4/11/2015 10:4	4/11/2015 10:4	4/11/2015 10:4

Loaded: 4,932 | Filtered: 4,932 | Total: 4,932 | Highlighted: 1 | Checked: 0 | Total LSize: 254.0 MB

Monarch2User.ad1/AppData/Local/Microsoft/Windows/Temporary Internet Files/Low/Content.IE5/O2TS55NT/0orgDQG4T04s5cO05g9krVMw[1].json

Ready   Overview Tab Filter: [None]

In the JSON file, the property “hotel_count” has value 14.

Conclusion

After obtaining and verifying the forensic images, I performed operation using FTK Imager Tool to verify the integrity. In this lab I used PRTK which is used to access password-protected files or system passwords.

The information I found was as follows:

1) Certain email conversations relevant to the case indicating Guild's operative.
2) Performed carving on images and able to found pictures depicting the Guild’s operative and Monarch.
3) Through email conversation I found Monarch's email address and the email address of the operative.
4) After exploring and decrypting the files I found out certain suspicious items like poisons, bombs, etc. indicating Monarch’s plan of violence.
5) Using Password Recovery Toolkit, I recovered a password of an encrypted file as well as of the user account.
6) I found the location of the ‘Clarion Hotel’.

Thus I examined the provided images and found out information relating in the images.