

ITIS 5250
Parag Mhatre
Lab 6
11/25/2018

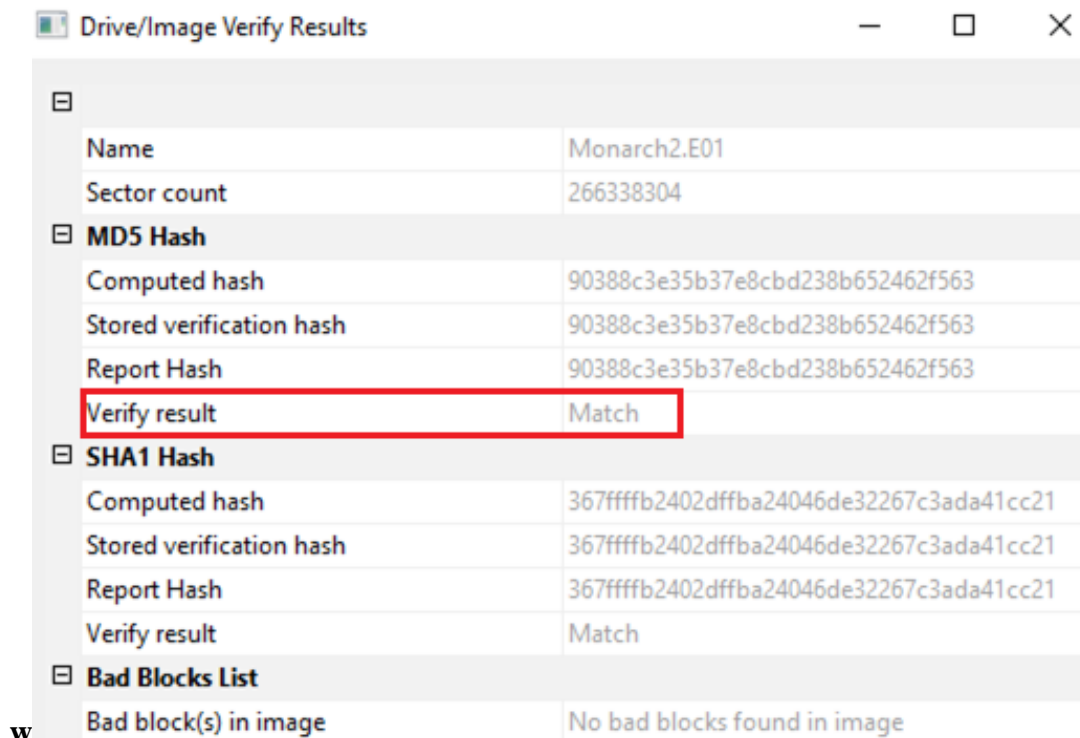
Overview:

In this case, I will be examining 6 files, viz. - MonarchUser.ad1, Monarch2User.ad1, ClarionUser.ad, Clarion.E01, Monarch.E01 and Monarch2.E01. The Monarch is a little-known super villain that is now gaining traction and whose costumed capers have attracted the attention of your police organization. I must investigate and find evidence where The Monarch, has discussed/planned to harm local super scientist Dr. Thaddeus Venture and others. Agent Sampson has asked me to identify any communications with the GCI (Guild of Calamitous Intent), the location of members of the GCI, photographs of the Monarch and his associates, communications with the GCI or any evidence of explosives, drones, poisons, bombs or other means to kill or injure the Monarch's intended targets.

Forensic Acquisition and Exam Preparation:

I moved the image files from the shared folder in the Forensics Lab, calculated and verified the Hash values of the files. The software used for accessing & extracting information from the images is FTK Imager 4.1.1.1, PRTK (Password Recovery Toolkit) and Forensic Toolkit 6.3

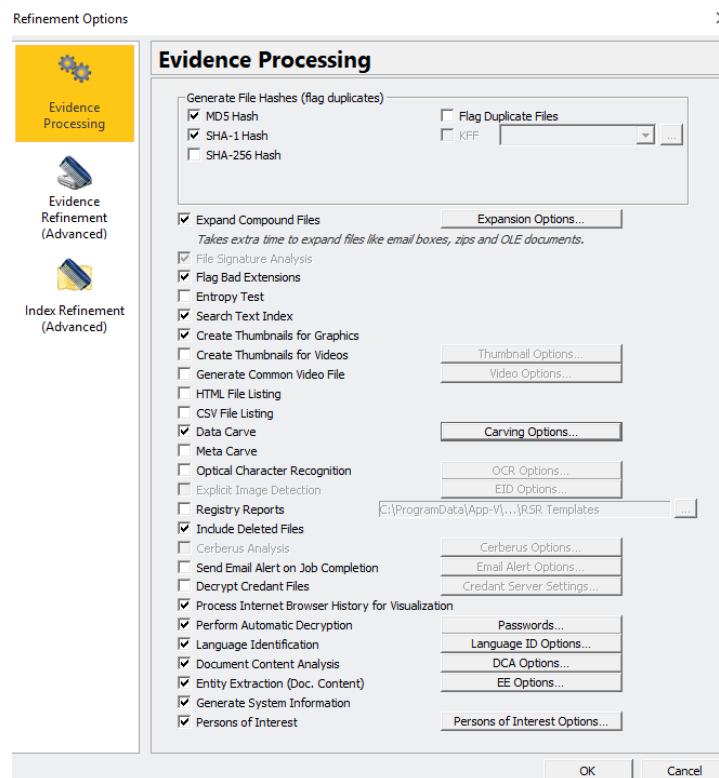
Hash Verifications:

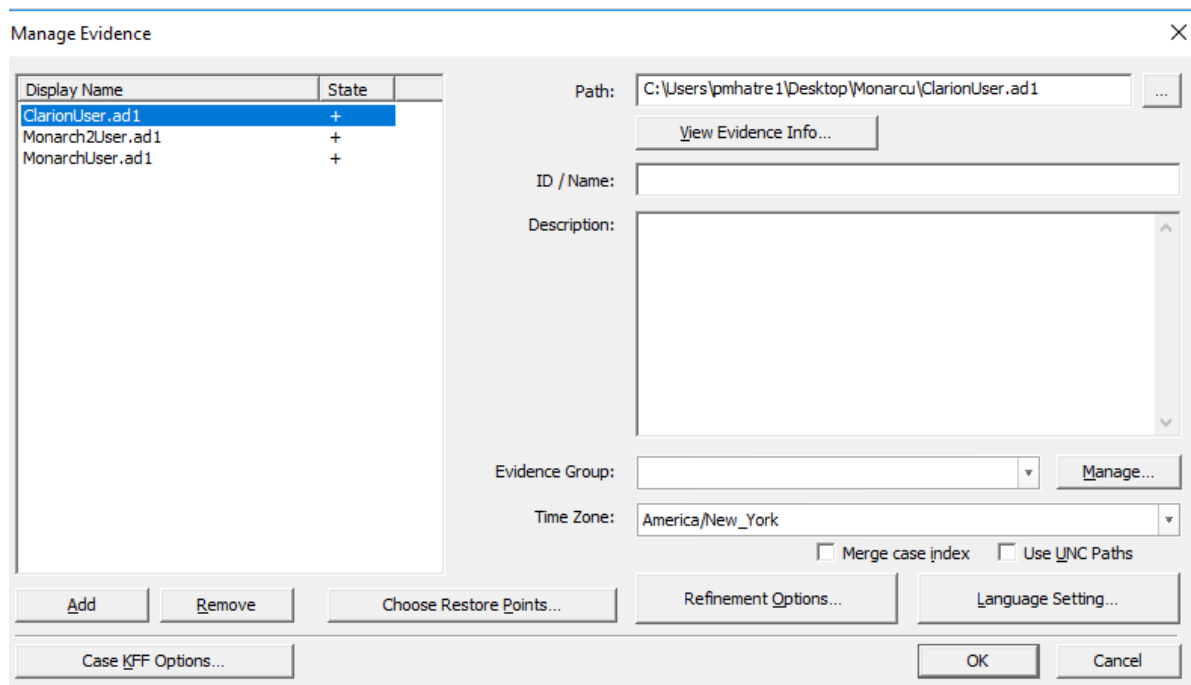
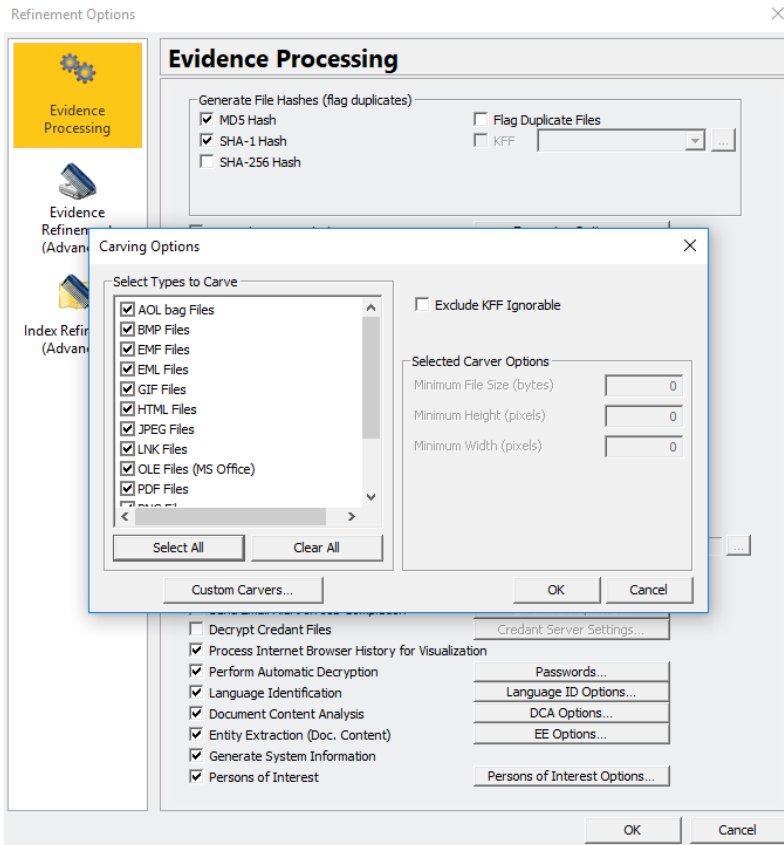


Drive/Image Verify Results	
[-] [X]	
[-]	
Name	Monarch2.E01
Sector count	266338304
[-] MD5 Hash	
Computed hash	90388c3e35b37e8cbd238b652462f563
Stored verification hash	90388c3e35b37e8cbd238b652462f563
Report Hash	90388c3e35b37e8cbd238b652462f563
Verify result	Match
[-] SHA1 Hash	
Computed hash	367ffffb2402dffba24046de32267c3ada41cc21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

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

I loaded up the images and files in FTK with custom processing options as follows:





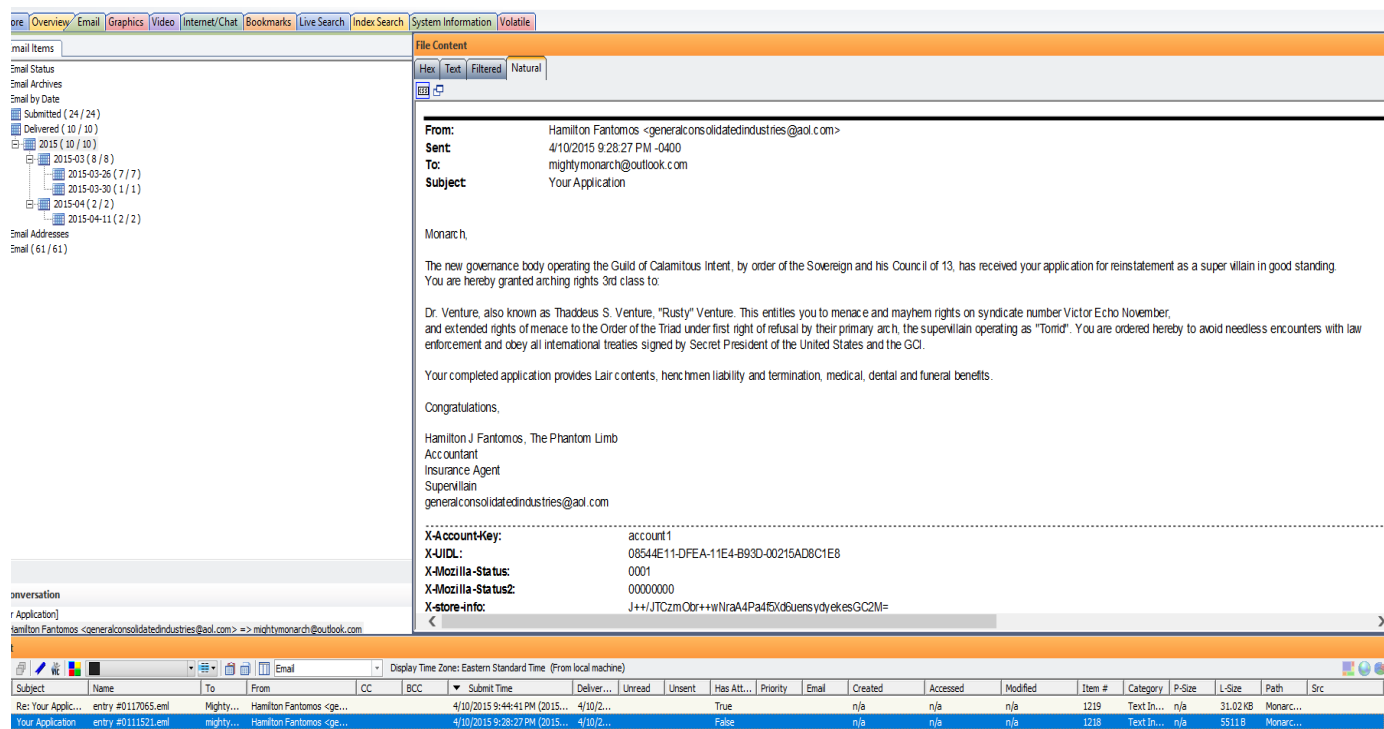
Findings and Report (Forensic Analysis)

1. Who is Guild's Operative?

The Guild's Operative appears to be Hamilton Fantomos. There is an e-mail sent from Hamilton Fantomos to Monarch where information regarding Monarch's reinstatement as a Supervillain and other information including Dr. Venture and following international treaties is communicated. The e-mail is located in the following path:

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

A Screenshot of the e-mail is given below.



2. Can you identify any pictures of this person?

I found an e-mail in the path given below, which Hamilton has sent to Monarch saying that he was with one Sheila and that he's sent their photo as an attachment to the e-mail.

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

More Overview Email Graphics Video Internet/Chat Bookmarks Live Search Index Search System Information Volatile

Email Items

Email Status

Email Archives

Email by Date

- Submitted (24 / 24)
- Delivered (10 / 10)
- 2015 (10 / 10)
 - 2015-03 (8 / 8)
 - 2015-03-26 (7 / 7)
 - 2015-03-30 (1 / 1)
 - 2015-04 (2 / 2)
 - 2015-04-11 (2 / 2)

Email Addresses

Email (61 / 61)

File Content

Hex Text Filtered Natural

From: Hamilton Fantomos <generalconsolidatedindustries@aol.com>

Sent: 4/10/2015 9:44:41 PM -0400

To: mightymonarch@outlook.com

Subject: Re: Your Application

Attachments: venture2src.rent1.jpg

Monarch,

Here's a little photo from 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 glorified 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.

Conversation

ur Application]

Hamilton Fantomos <generalconsolidatedindustries@aol.com> => mightymonarch@outlook.com

st

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

Subject	Name	To	From	CC	BCC	Submit Time	Deliver...	Unread	Unsent	Has Att...	Priority	Email	Created	Accessed	Modified	Item #	Category	P-Size	L-Size	Path	Src
Re: Your Applic...	entry #0117065.enl	Mighty...	Hamilton Fantomos <ge...			4/10/2015 9:44:41 PM (2015...	4/10/2...			True		n/a	n/a	n/a	n/a	1219	Text In...	n/a	31.02 KB	Monarc...	

The attachment to the e-mail is given below shows one man and one woman sitting in a car. It is safe to assume that the man must be Hamilton.



3. Can you provide any pictures depicting the Monarch?

After searching the forensic images, I found the following pictures with their respective paths depicting the Monarch.

MonarchUser.ad1\Downloads\venture-bros-monarch.jpg



MonarchUser.ad1\Downloads\the_monarch_wants_you__again_by_petex-d2yvzlz.jpg



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



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

As seen from the e-mail communication between Monarch and the operative – Hamilton, it is found that the e-mail addresses are as follows:

Monarch's email address - mightymonarch@outlook.com

Operative's (Hamilton) email address - generalconsolidatedindustries@aol.com

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 "Tomic". 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.

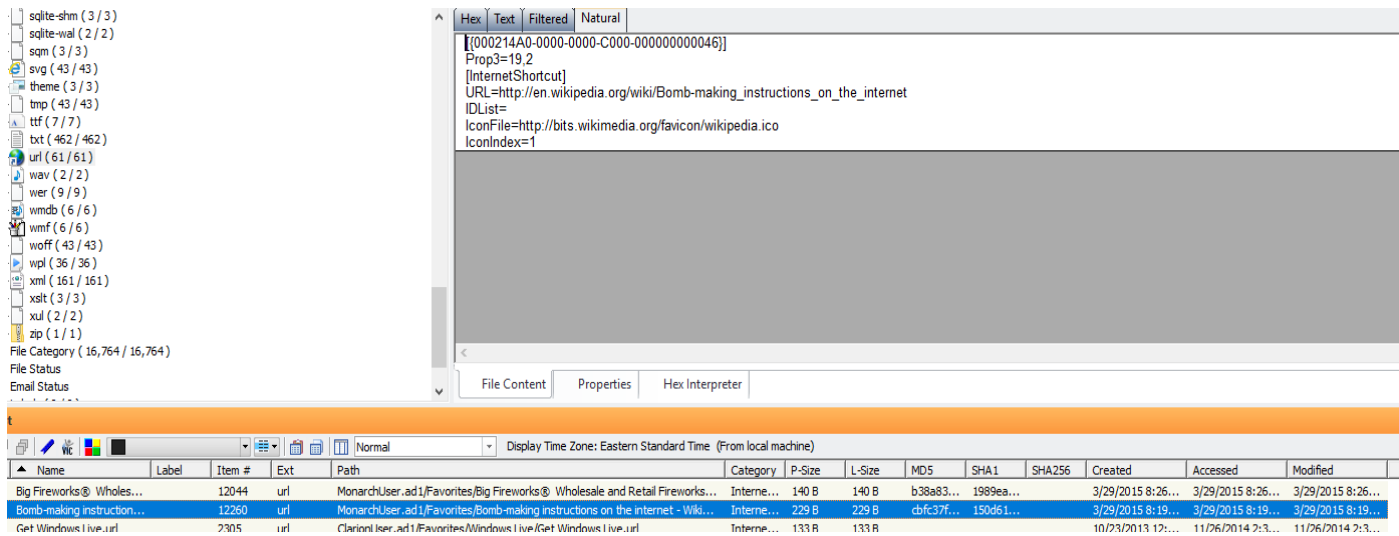
Congratulations,

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

5. Are there any items related to the Monarch's plans for violence?

While investigating, I found various items/evidence related to plans for violence. They are as follows:

1. Bomb making instructions Wikipedia page in Favorites.



The screenshot shows a file explorer window with a list of files on the left and a detailed view of a selected file on the right. The file list includes various file types such as sqlite-shm, sqlite-wal, sqm, svg, theme, tmp, ttf, txt, url, wav, wer, wmdb, wmf, woff, wpl, xml, xslt, xul, and zip. The selected file is 'url (61/61)'. The detailed view shows the file's properties, including its name, size, and a list of items. The file is a URL pointing to a Wikipedia page about bomb-making instructions.

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
Big Fireworks® Wholes...		12044	url	MonarchUser.ad1\Favorites\Big Fireworks® Wholesale and Retail Fireworks...	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...		12260	url	MonarchUser.ad1\Favorites\Bomb-making instructions on the internet - Wiki...	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		2305	url	MonarchUser.ad1\Favorites\Windows Live\Get Windows Live.url	Interne...	133 B	133 B				10/23/2013 12:...	11/26/2014 2:3...	11/26/2014 2:3...

2. An image of a crudely made hand grenadelike object.

MonarchUser.ad1\AppData\Local\Microsoft\Temporary Internet Files\Low\ Content.IE5\ KBIPEE3F\ FAEQMCJF68BAFNW.SQUARE2[1].jpg

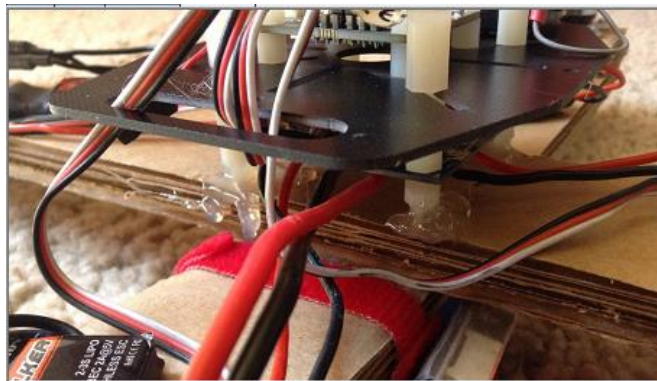


3. An image of Mousetrap Car step. A possible application of this is to use it to trigger something on a desired movement involving it.

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



MonarchUser.ad1/AppData/Local/Microsoft/Windows/Temporary Internet files/Low/Content.IE5/2KH5I8Y3/IMG_0120-e1359677201327[1].jpg



I also found the image of a drone at the path given below,

MonarchUser.ad1/AppData/Local/Microsoft/Windows/Temporary Internet files/Low/Content.IE5/KBIPEE3F/31DYMixwkvL_AA160_(1).jpg

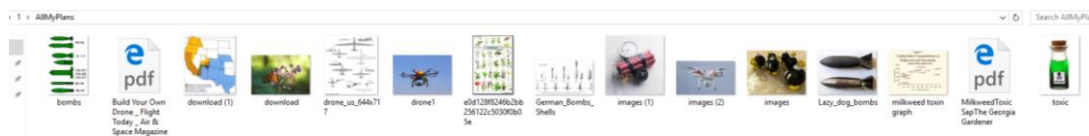


6. Can you recover any passwords?

I found a compressed file called “AllMyPlans.zip” which was password protected. I extracted this file and tried to crack the password using the PRTK (Password Recovery Toolkit). After some time, PRTK cracked the password which was “monarch”.

Properties	
Job Information	
Attack Type:	ZIP dictionary attack
Module:	ZIP Password Module
Profile:	English
Status:	Finished
Difficulty:	Difficult
Begin Time:	11/24/18 18:15:21
End Time:	11/24/18 18:15:35
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

In the extracted files, I found further evidence in the form of pictures, related to the Monarch’s plans for violence.



I also tried recovering passwords from the SAM file. The password found for the user account is “guest123”.

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 23:45:53

End Time: 11/17/18 23:46:32

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

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

I found map picture files, pictures of the Clarion hotel and extensive internet searches for the hotel from the forensic images were found when I checked the Browsing history. It can be said that the Monarch's stay at the hotel was pre-planned.

ClarionUser.AD1/AppData/Local/Microsoft/Windows/Temporary Internet Files/Low/Content.IE5/2KH5I8Y3/0320102211301010[1].png

Evidence Items

ClarionUser.ad1

Monarch2User.ad1

MonarchUser.ad1

File Content

Hex

Text

Filtered

Natural

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
	0320102211301003[1]...		6265	png	ClarionUser.ad1/AppDa...	PNG	12.00 KB	9179 B				4/10/2015 9:46...	4/10/2015 9:46...	4/10/2015 9:46...
	0320102211301010[1]...		4154	png	ClarionUser.ad1/AppDa...	PNG	16.00 KB	13,244 KB				4/10/2015 9:46...	4/10/2015 9:46...	4/10/2015 9:46...
	0320102211301011[1]...		6262	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]...		4282	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]...		4453	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]...		6521	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...
	0320102211301123[1]...		6559	png	ClarionUser.ad1/AppDa...	PNG	16.00 KB	13.18 KB	70e937...	8e75c2...		4/10/2015 9:46...	4/10/2015 9:46...	4/10/2015 9:46...
	0320102211301130[1]...		6519	png	ClarionUser.ad1/AppDa...	PNG	16.00 KB	13.11 KB	a06e6f...	090371...		4/10/2015 9:46...	4/10/2015 9:46...	4/10/2015 9:46...
	0320102211301302[1]...		6515	png	ClarionUser.ad1/AppDa...	PNG	12.00 KB	9868 B				4/10/2015 9:46...	4/10/2015 9:46...	4/10/2015 9:46...

Loaded: 821

Filtered: 821

Total: 3,758

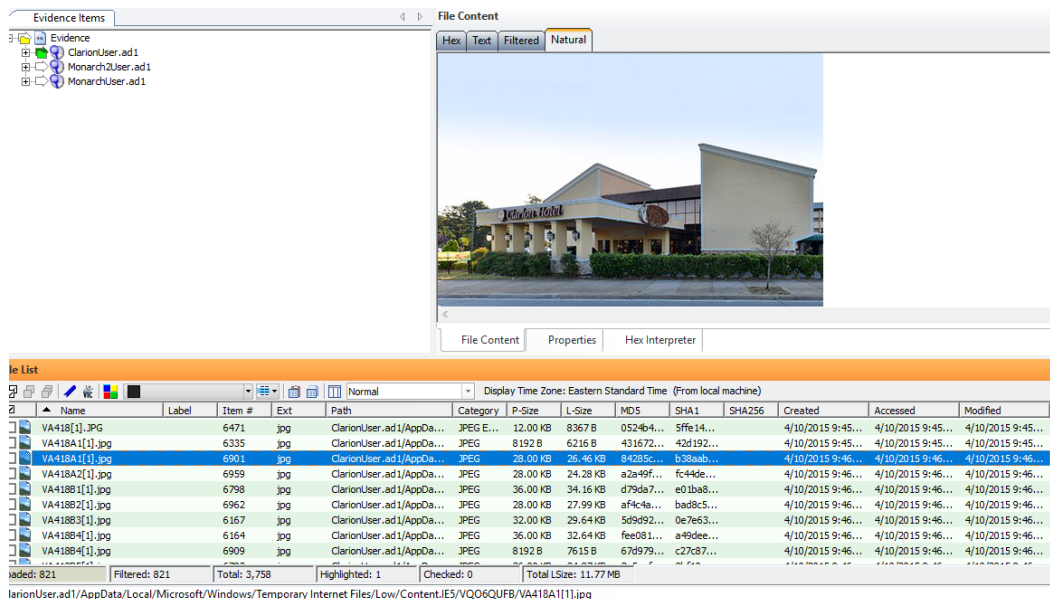
Highlighted: 1

Checked: 0

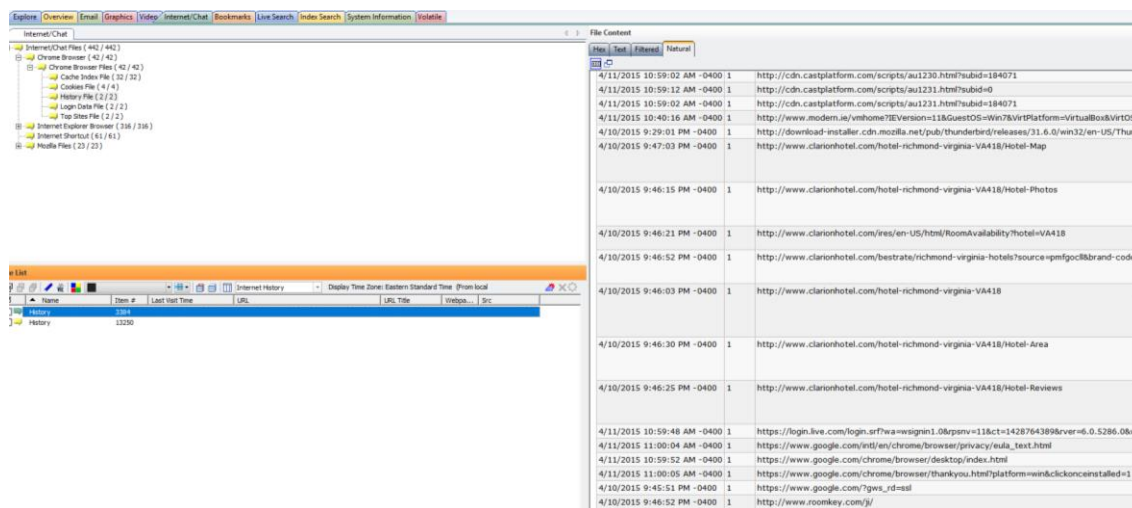
Total LSize: 11.77 MB

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

ClarionUser.AD1/AppData/Local/Microsoft/Windows/Temporary Internet Files/Low/Content.IE5/VQO6QUFB/VA418A1[1].jpg



Monarch2User.ad1/AppData/Local/Google/Chrome/UserData/Default/History



Conclusion:

I verified and examined the forensic images MonarchUser.ad1, Monarch2User.ad1, ClarionUser.ad1, Clarion.E01, Monarch.E01 and Monarch2.E01 using the Forensic Toolkit 6.3 and I found relevant email conversations between the Monarch and the operative named Hamilton. I also found the operative's and the Monarch's pictures and email addresses. In addition to this, I found evidence related to Monarch's plans of violence including recovering password for a zip file. Moreover, I found evidence that the Monarch's stay in the hotel was pre-planned.