ITIS 4250 / 5250

Lab # 5

11/6/2019

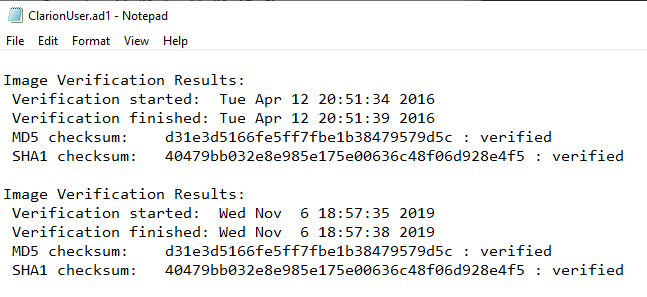
**Overview:**

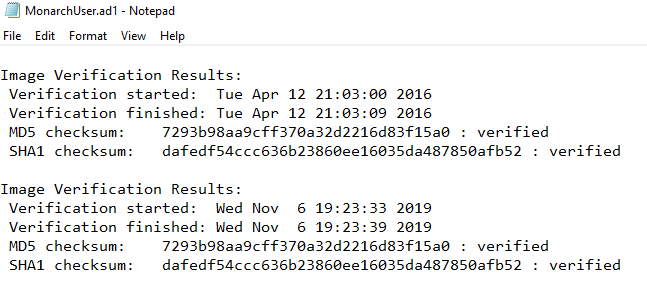
On November 6, 2019, Agent Sampson has asked me to provide the records of communication regarding email conversations between Monarch and Dr. Thaddeus Venture along with other scientists. I was asked to identify these communications, locations of these CGI members and any photographs, and any other evidence of explosives, drones, poisons, bombs and other deadly weapons. I have received proper permission to investigate these images that have been acquired.

**Forensic Acquisition & Exam Preparation**

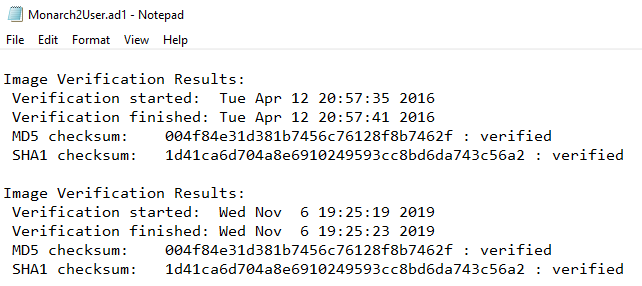
The first step was transferring the files ‘ClarionUser.ad1, ‘MonarchUser.ad1’ and ‘Monarch2User.ad1’ from Canvas into a fresh folder on my work machine. My machine is a Lenovo Yoga 13 with 8gb of ddr4 ram along with an i5-8500. After transferring files ‘ClarionUser.ad1, ‘MonarchUser.ad1’ and ‘Monarch2User.ad1’ on my machine I verified the hash to make sure the file hasn’t been tampered with.

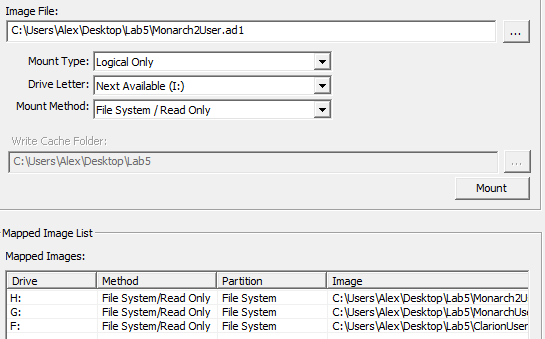
ClartionUser.ad1 MD5: d31e3d5166fe5ff7fbe1b38479579d5c



MonarchUser.ad1 MD5: 7293b98aa9cff370a32d2216d83f15a0 

Monarch2User.ad1 MD5: 004f84e31d381b7456c76128f8b7462f



After this I went upon loading the images into autopsy, since these files are .ad1 they are not supported by autopsy, so I mounted the files into FTK. 

This then allowed me to load them into autopsy.

**Findings and Report (Forensic Analysis)**

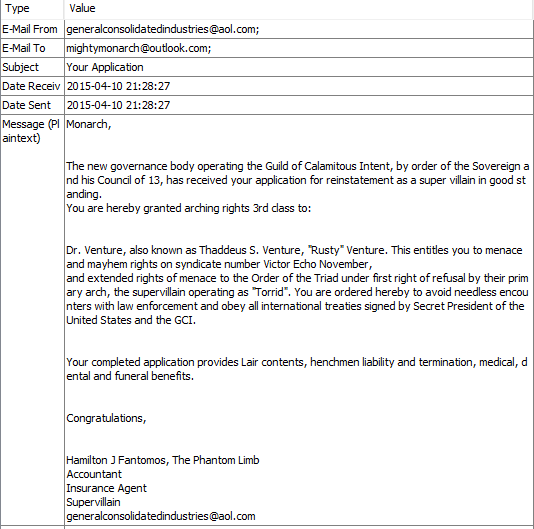
**Who is the Guild's operative?**

The Guild’s operative is the individual Hamilton J Fantomos, who goes by the supervillain name of The Phantom Limb. This was found by investigating emails that were found across the images I was given to investigate.

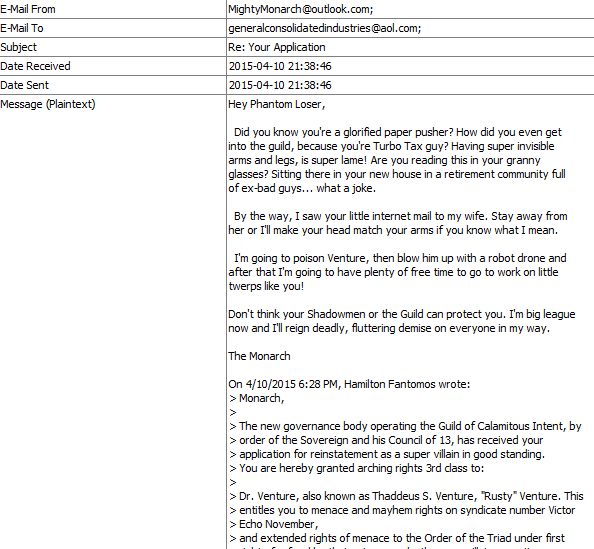
**Are there communications from this person?**

Yes, I have found numerous communications between Hamilton and Monarch, as well as a forwarded message from another individual Sheila Monarch that contains a conversation with Hamilton.

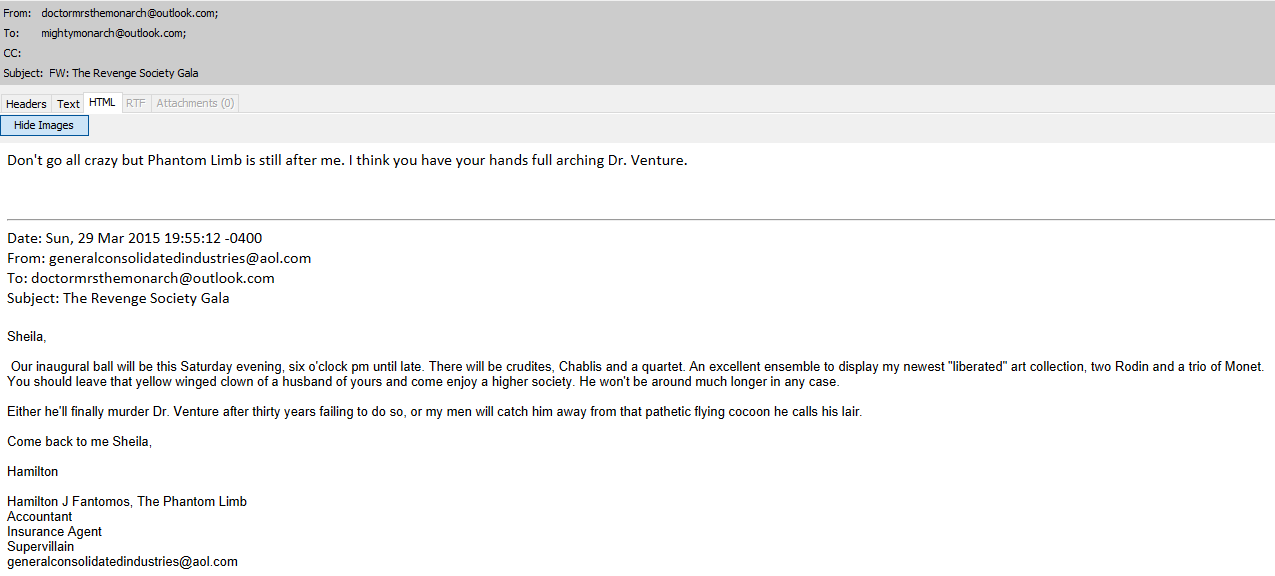
Below is the start of the first chain between Hamilton and Monarch that I was able to recover, within its Hamilton is informing Monarch about his application for being reinstated as a super villain, and how he is being granted arching rights 3rd class.



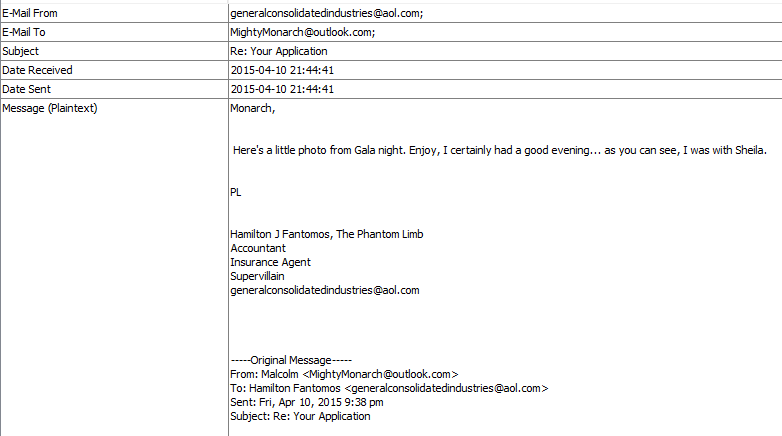
In response to that email monarch sent the following email. Threating Hamilton (Phantom Limb) to never talk to his wife again and that he is going to murder the scientist Venture and then maybe go after Hamilton himself.



This appears to be in response to an email that monarch received from Sheila ([doctormrsthemonarch@outlook.com](mailto:doctormrsthemonarch@outlook.com)) who forwarded an email between them and Hamilton. In this email he asks her to come to the inaugural ball that will be occurring Saturday evening without her husband.



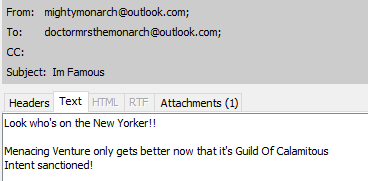
**Can you identify any pictures of this person?**

In the email thread regarding the application between Monarch and Hamilton there is a photo that is believed to contain Hamilton. He responds to Monarch by sending him an attached photo from the Gala which he describes that you can see that he was with Sheila.

The attached photo contains two individuals within a car. It can be assumed that the women on the right side of the car is indeed Sheila and the individual on the left can be assumed to be Hamilton.

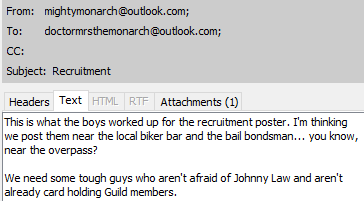


**Can you provide any images depicting the Monarch?**

In an email sent to [doctormrsthemonarch@outlook.com](mailto:doctormrsthemonarch@outlook.com) by Monarch he shows her that he is on the cover of the New Yorker and send the photo of him on it to her 



There is also another email that was sent to [doctormrsthemonarch@outlook.com](mailto:doctormrsthemonarch@outlook.com) by Monarch discussing recruitment posters. The attached poster depicts the monarch and appears to be a propaganda poster to recruit.





**Can you find the Monarch’s email address or the email address of the operative?**

I have found the following email addresses that have the upmost importance to this case.

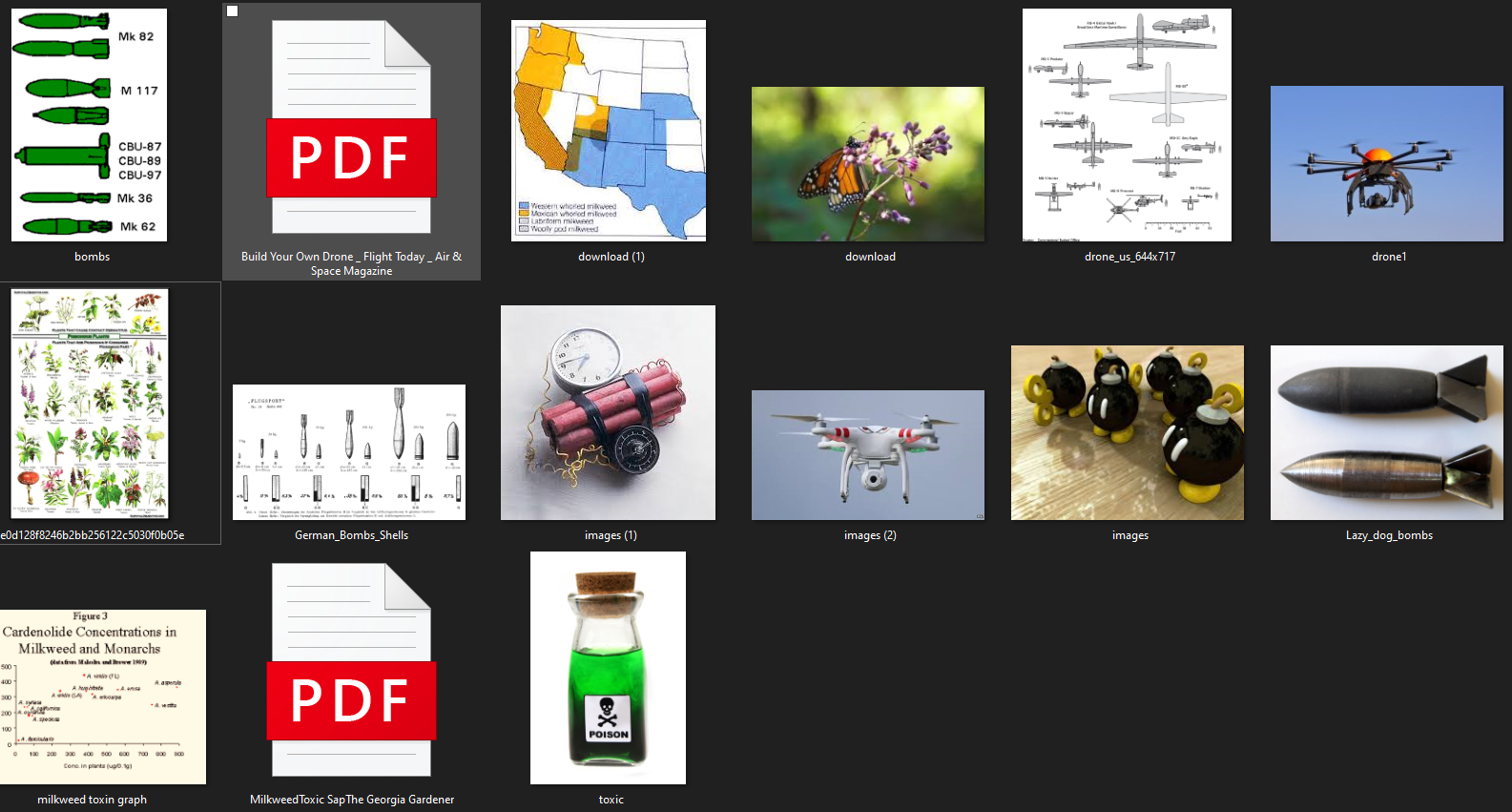
[mightymonarch@outlook.com](mailto:mightymonarch@outlook.com) – Monarch

[generalconsolidatedindustries@aol.com](mailto:generalconsolidatedindustries@aol.com) – Operative (Hamilton Fantomous)

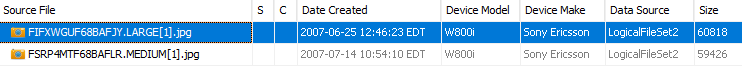
[doctormrsthemonarch@outlook.com](mailto:doctormrsthemonarch@outlook.com) – Sheila Monarch

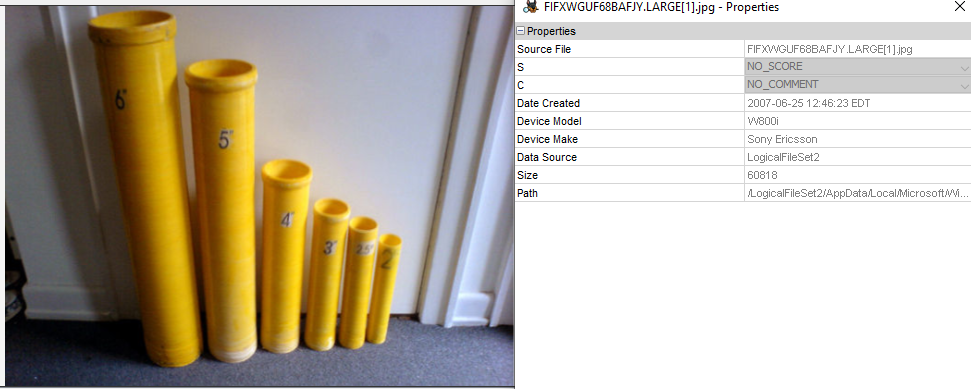
**Are there any items related to the Monarch’s plan for violence?**

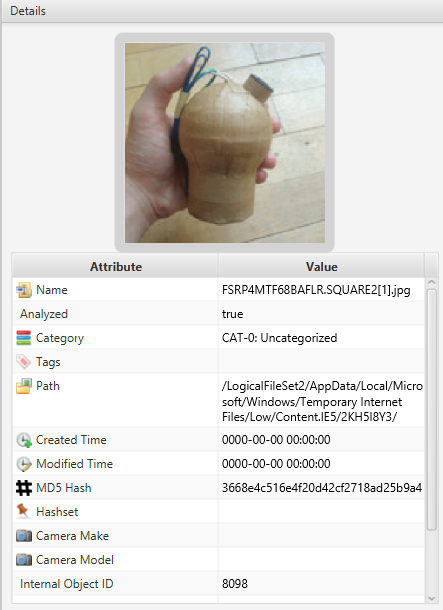
There are different examples of possible plans of violence. There is a zip file called AllMyPlans.zip that was found on the desktop of the MonarchUser2.ad1 Image. This zip file is passcode protected and after manual brute force I was able to get the password of this zip file which was ‘monarch’. After extracting the zip on my local machine, I was able to find that the zip file contained numerous resources to cause havoc and violence. Including images of bombs, drones, poisonous plants. There where also PDF guides to creating your own drone and pdfs about poison.

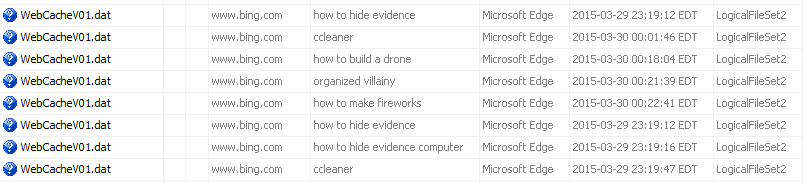


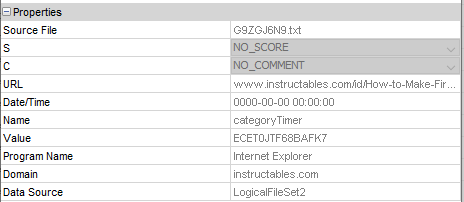
There are also deleted images that were able to be recovered with exif metadata depicting what appears to be a homemade bomb and a line of different size tubes with numbers on them. These were found on the MonarchUser.ad1 Image. These images where taken with a Sony Eriksson W880i.

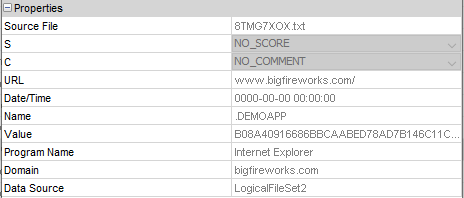






There is also is web browser evidence on MonarchUser.ad1 that shows that Monarch was researching how to build fireworks along with other evidence that he was trying to cover his web tracks by googling how to do so 



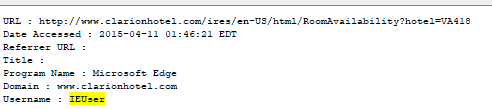


**Can you recover any passwords?**

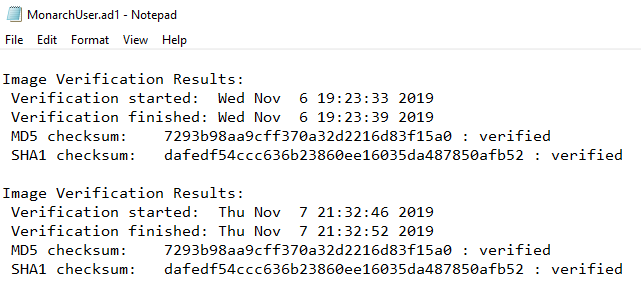
In the proccess of investigating the images I was able to brute force the password of the zip file containing evidence of violent items. Other than that I was not able to find any other passwords.

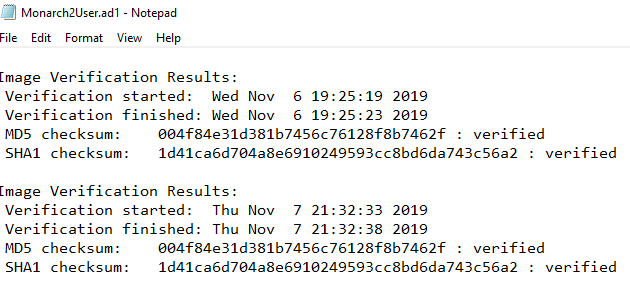
**Is there any evidence the Monarch planned to stay in the particular hotel?**

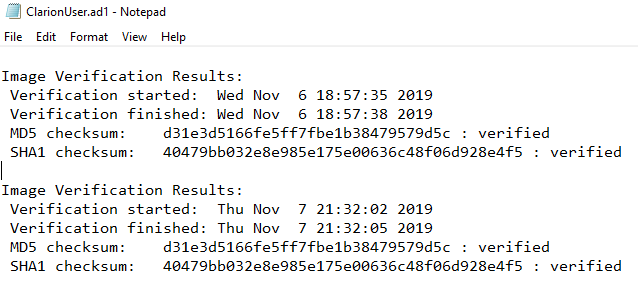
There are web records found that show that he was on the clarionhotel webpage looking for room avaliabilty. This hotel is a quality inn located at 3207 N. Arthur Ashe BoulevardBuilding A, Richmond, VA, 23230, US. This evidence was found on MonarchUser2.ad1 Image.



I re-verfied all the hashes to make sure that they were not altered.







**Conclusion:**

During this investigation I was able to find email conversations between Monarch and Hamilton the assumed operative. Within these emails he threatens to kill Dr. Venture and Hamilton himself. Found within the images there is also evidence of weapons and other means of doing harm found. These evidence items are found in pictures, how to guides and web-searches. It is also shown that Monarch is planning on staying at a quality inn in Richmond.