IT IS 5250

Ruchira Pokhriyal

Lab 6

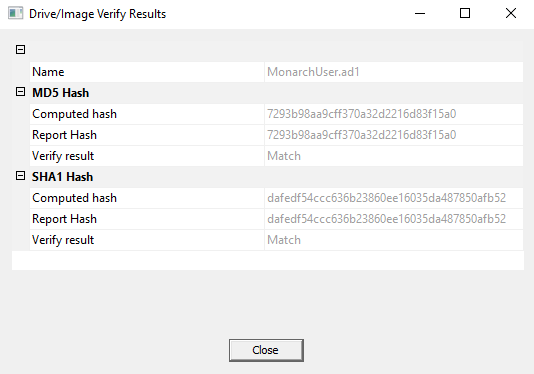
11/26/2018

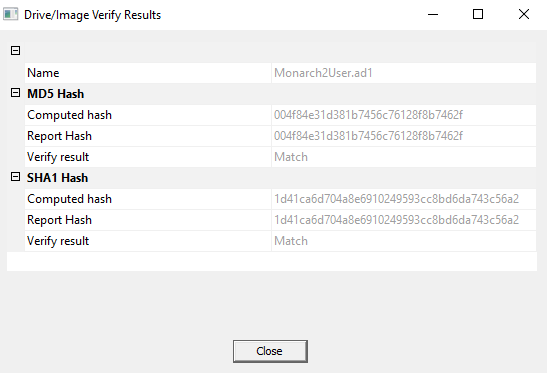
**Overview**

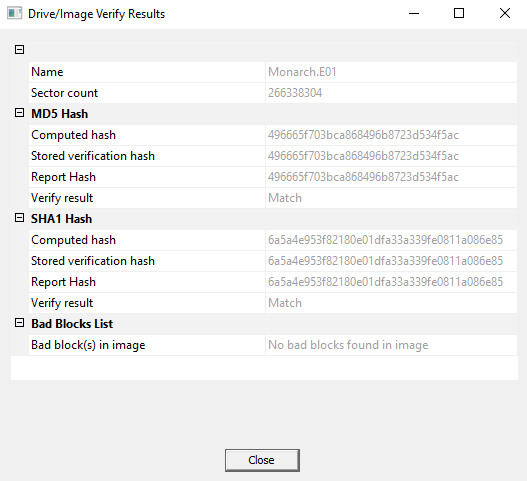
The Monarch is a little-known super villain that is gaining traction and whose costume capers have attracted the attention of the police organization. When Monarch provided his busted laptop to Conjectural Technologies for repairs, the technician alerted the law enforcement for the suspicious activity. In this case, I am provided with three AD1 files: MonarchUser.ad1, Monarch2User.ad1, ClarionUser.ad1 and three image files: Clarion.E01, Monarch.E01 and Monarch2.E01. I am asked by Agent Sampson to provide the records of communication regarding email conversations in which the Monarch has discussed ways to cause harm to local scientist Dr. Thaddeus Venture and others.

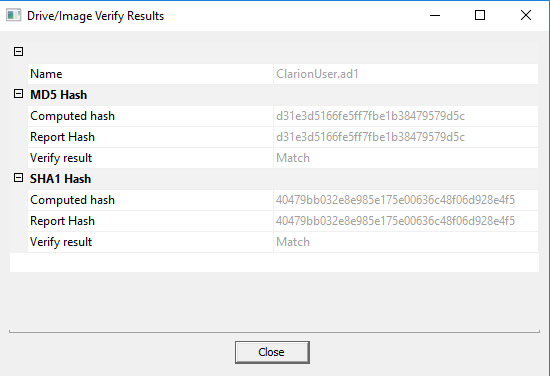
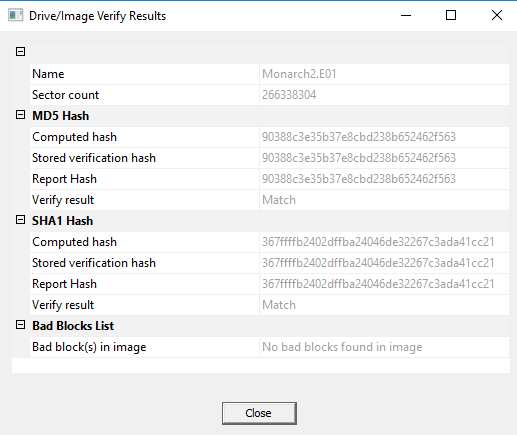
**Forensic Acquisition and Exam Preparation**

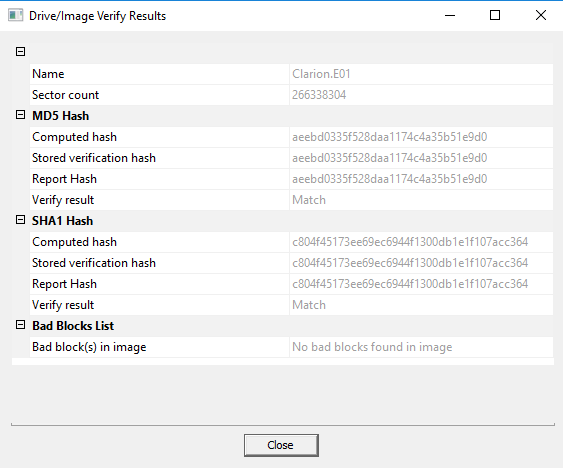
From the server’s shared directory, I accessed MonarchUser.ad1, Monarch2User.ad1, ClarionUser.ad1, Clarion.E01, Monarch.E01 and Monarch2.E01 and loaded into FTK Imager (Version 4.1.1.1) for hash verification. Additionally, I used FTK (Version 6.3.0.186) for evidence processing.





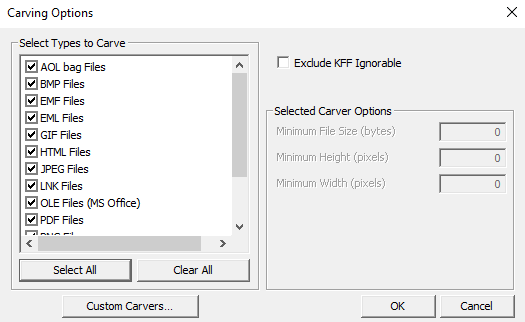




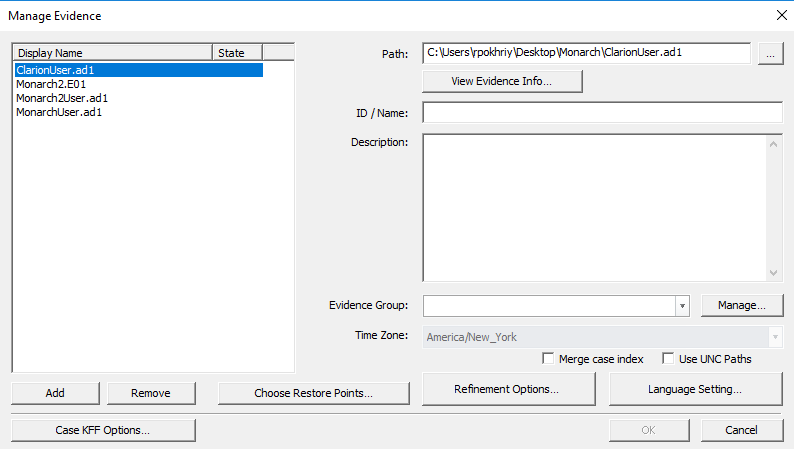


**The above results show that these images were not tampered and then using FTK, I processed them as shown.**

**Evidence Processing using FTK: Carving Options:**

**Adding Image:**

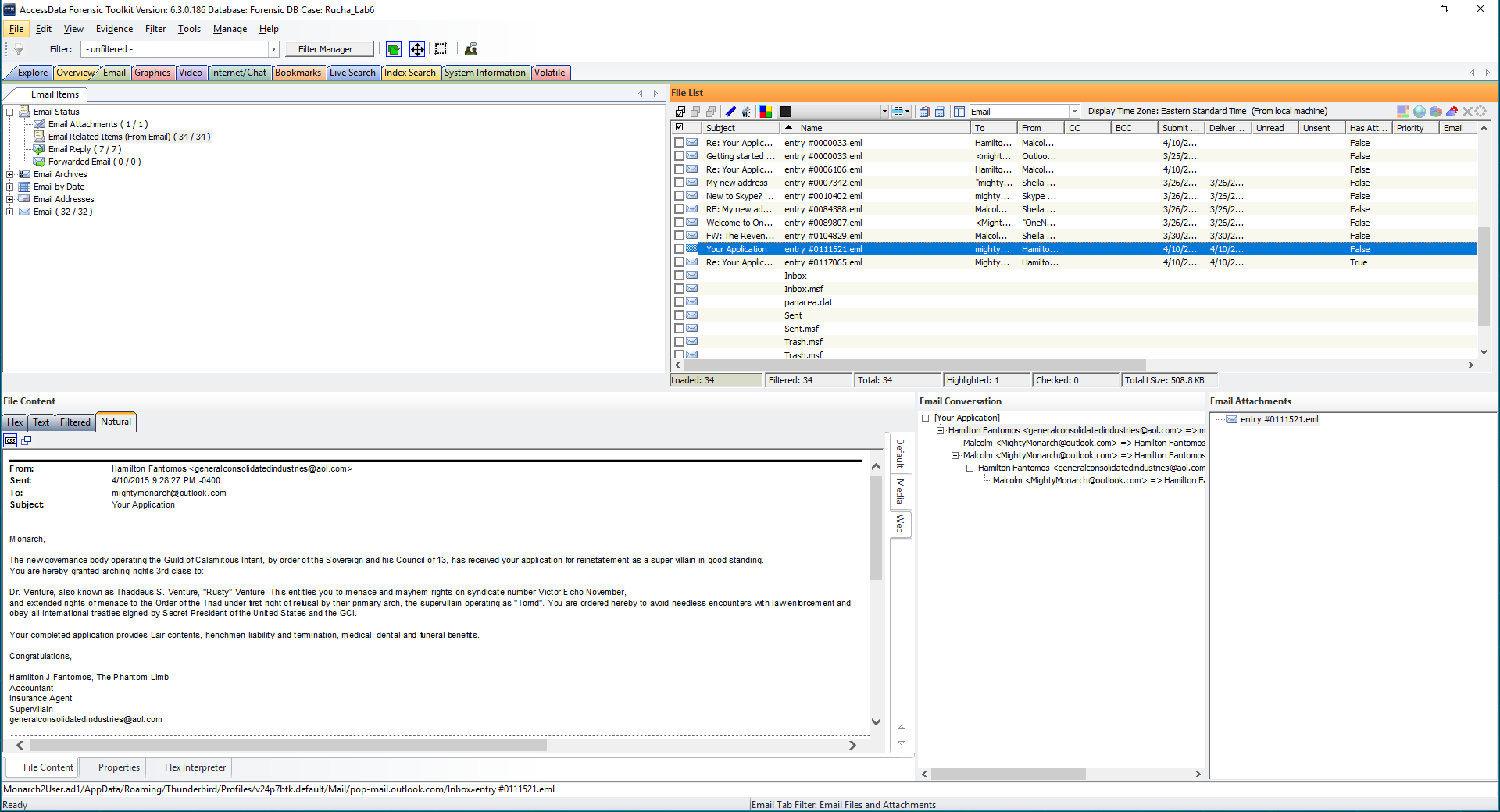


**Findings and Report (Forensic Analysis)**

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

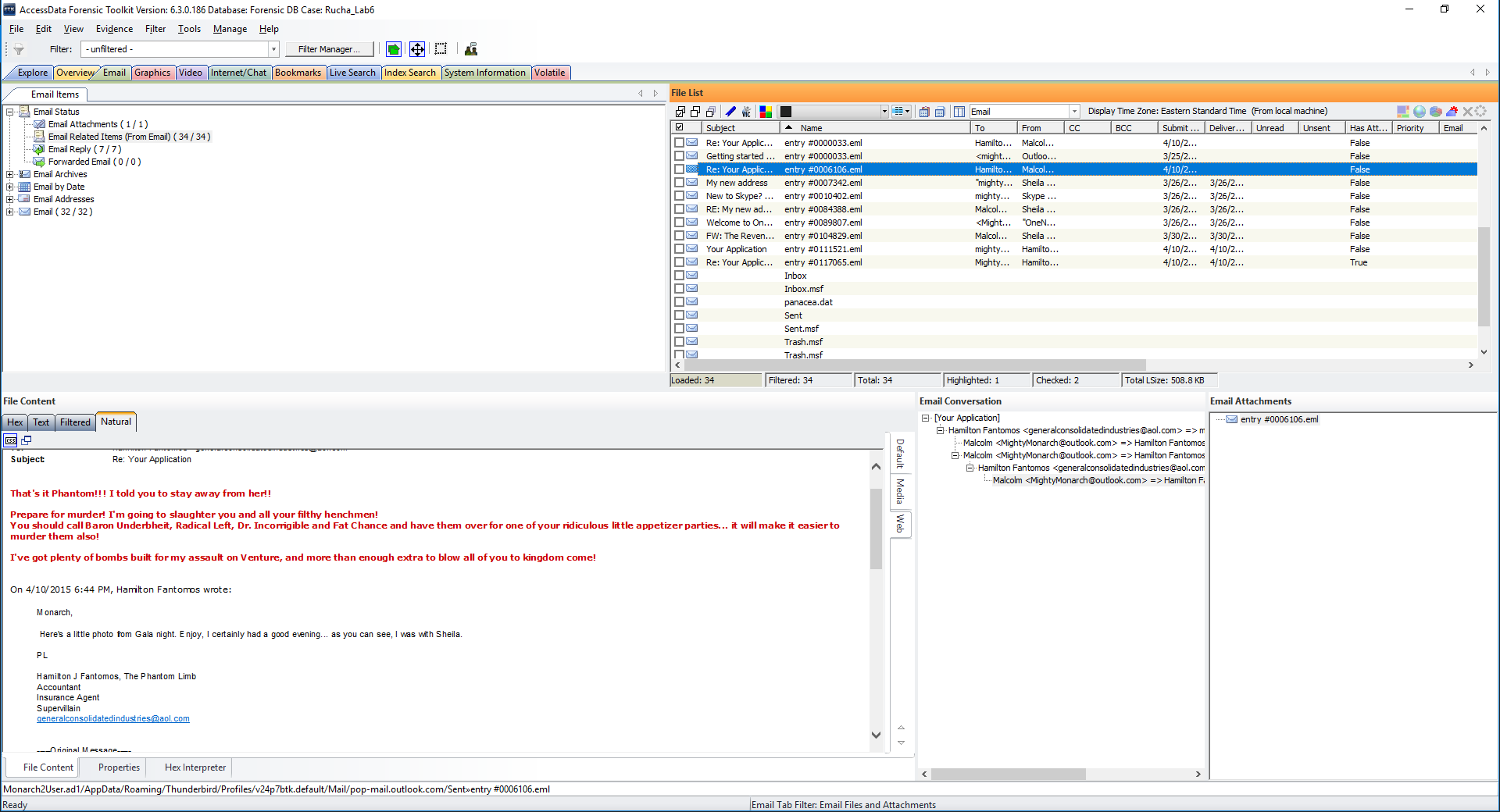
The below email conversation shows that the Guild’s operative is **Hamilton Fantomos**.

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

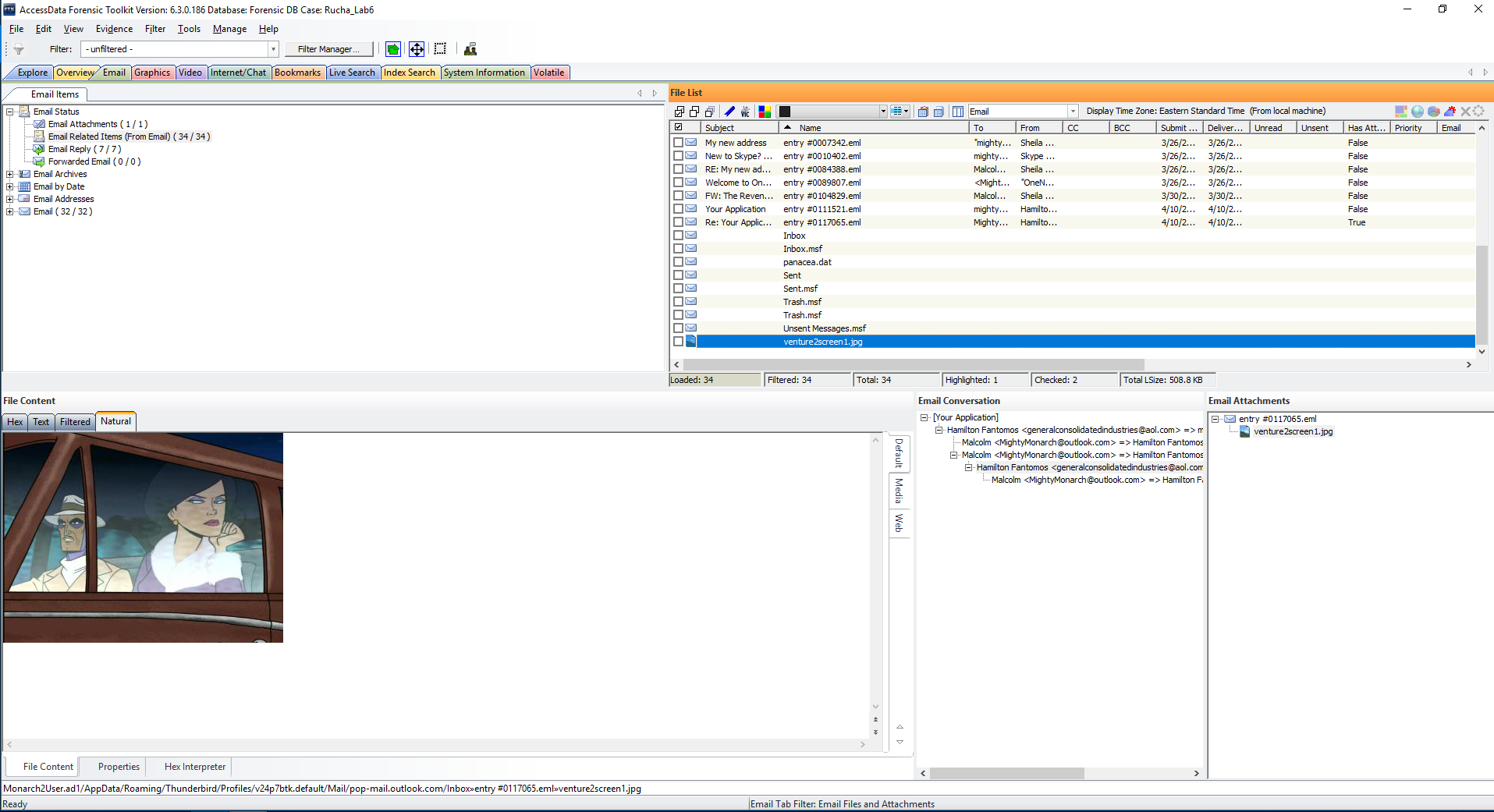


The following email along with its attachment displays Hamilton’s picture on the left.

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



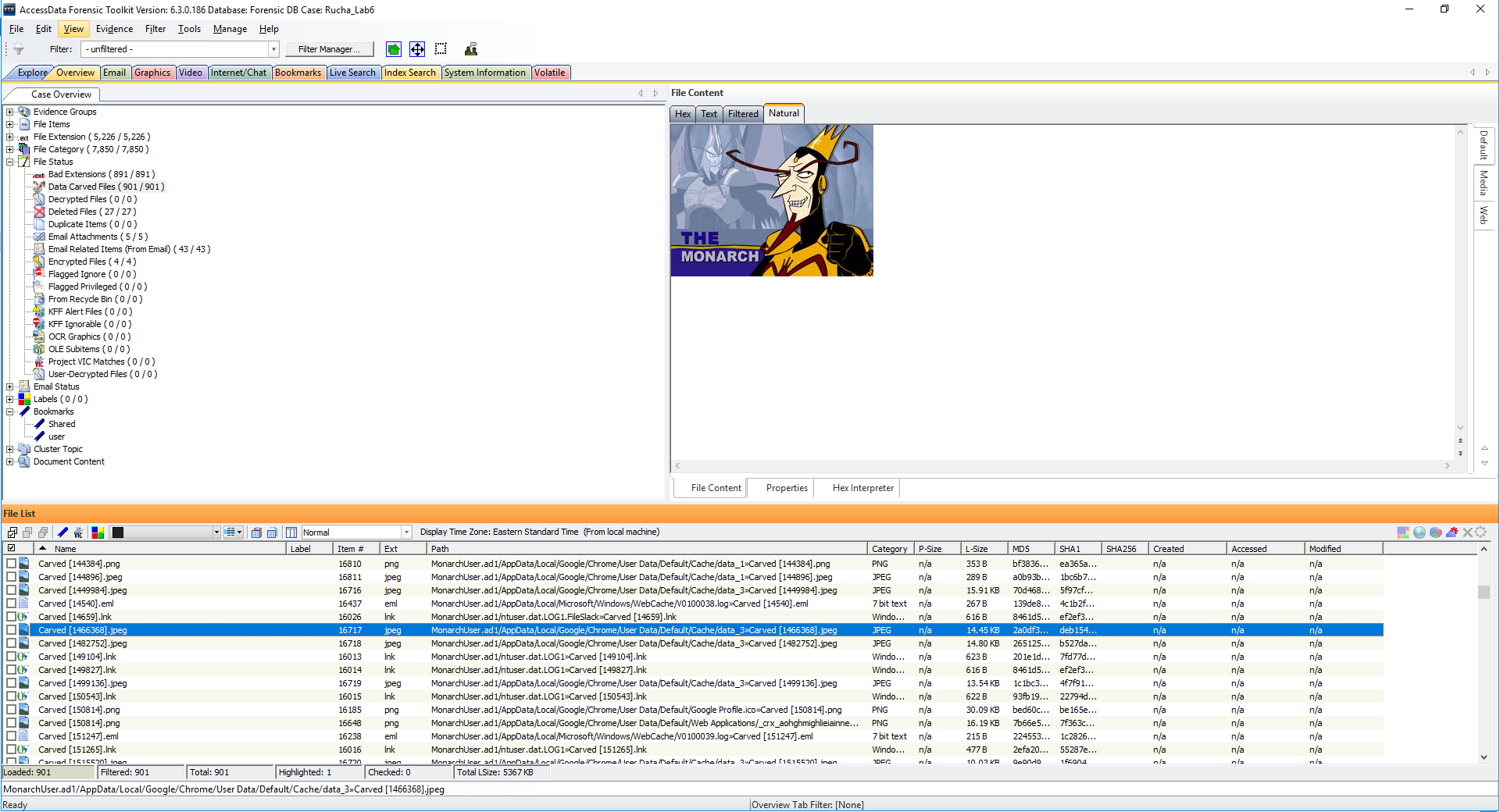
**Path: Monarch2User.ad1/AppData/Roaming/Thunderbird/Profiles/v24p7btk.default/Mail/pop-mail.outlook.com/Inbox>>entry #0117065.eml>>venture2screen1.jpg**



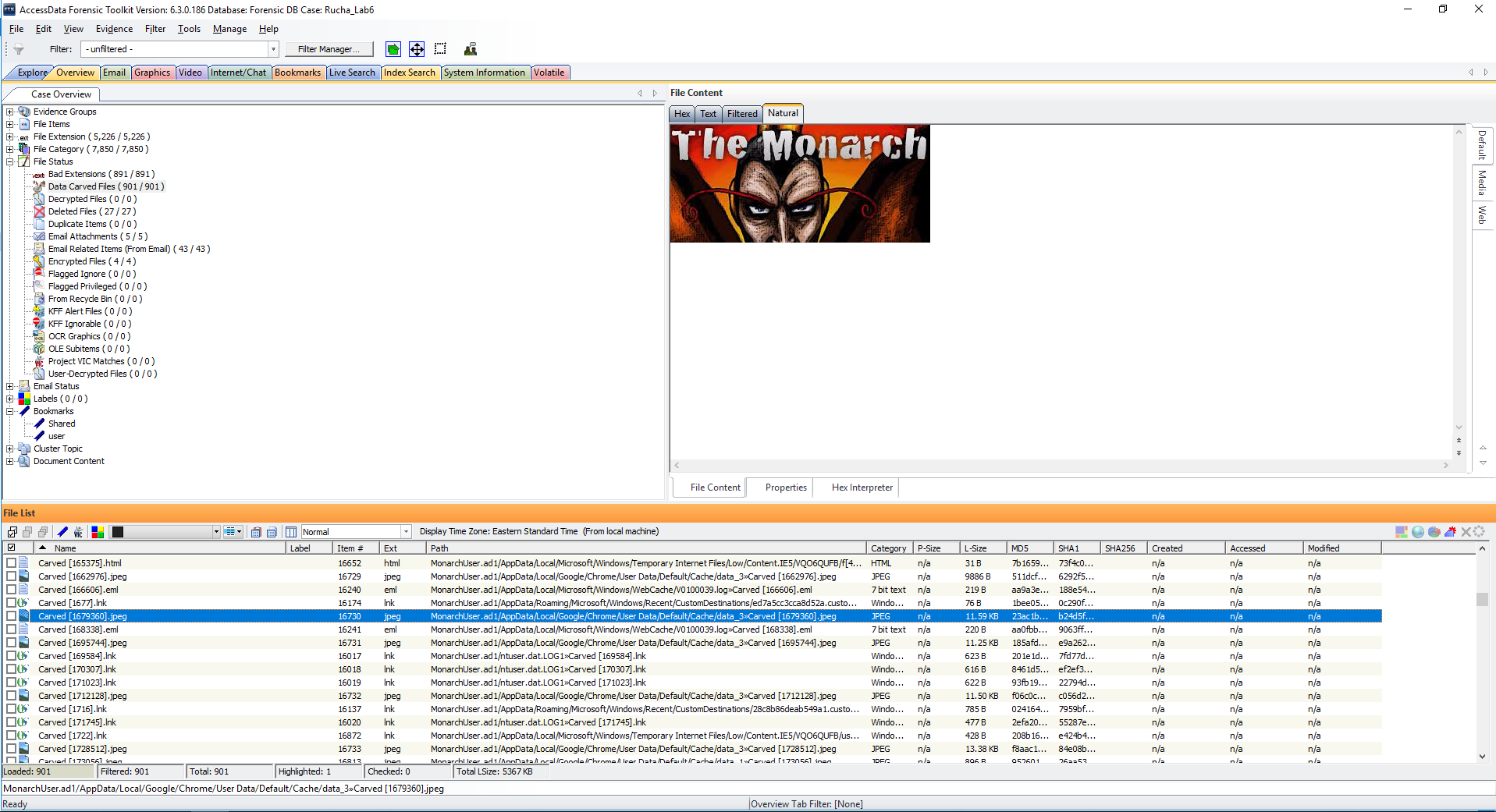
2. Can you provide any pictures depicting the Monarch?

The below screenshots provide the photograph of the Monarch.

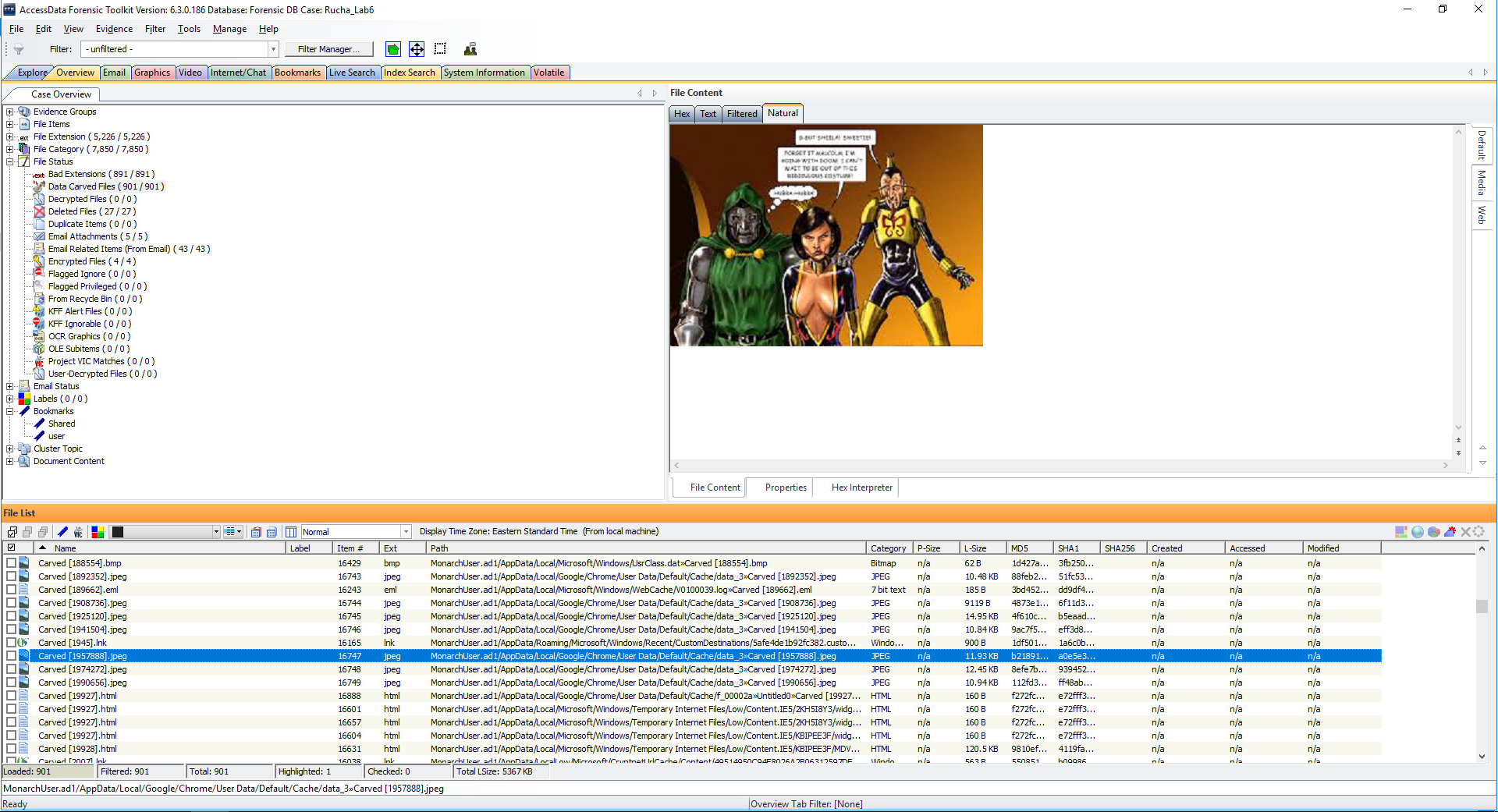
**Path: MonarchUser.ad1/AppData/Local/Google/Chrome/User Data /Default /Cache /data\_3 =Carved[1466368].jpeg**



**Path: MonarchUser.ad1/AppData/Local/Google/Chrome/User Data /Default /Cache /data\_3 =Carved[1679360].jpeg**



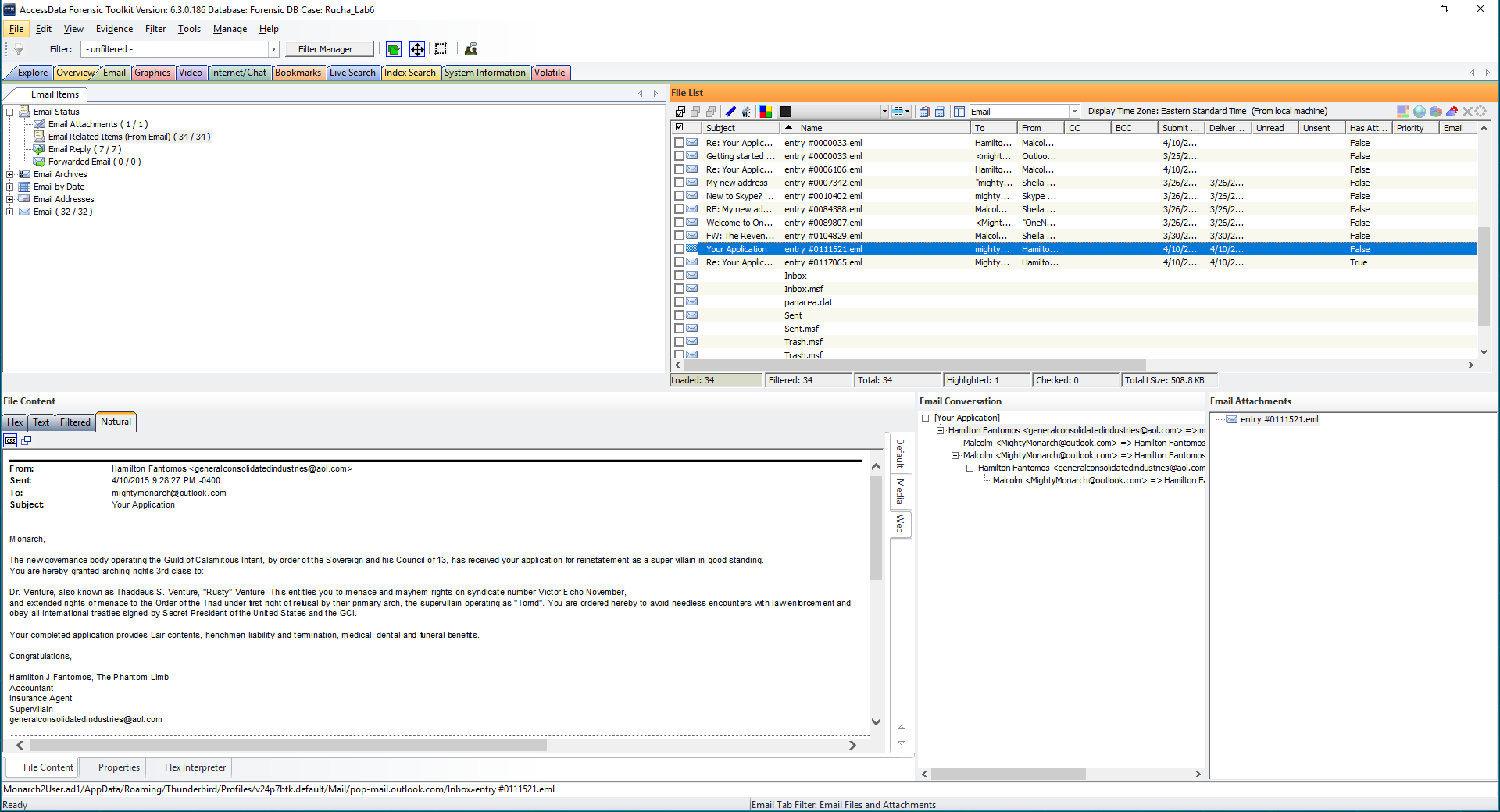
**Path: MonarchUser.ad1/AppData/Local/Google/Chrome/User Data /Default /Cache /data\_3 =Carved[1957888].jpeg**



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

It can be seen from the below screenshot that the Monarch’s email address is: [mightymonarch@outlook.com](mailto:mightymonarch@outlook.com) and the Operative’s email address is: [generalconsolidatedindustries@aol.com](mailto:generalconsolidatedindustries@aol.com)

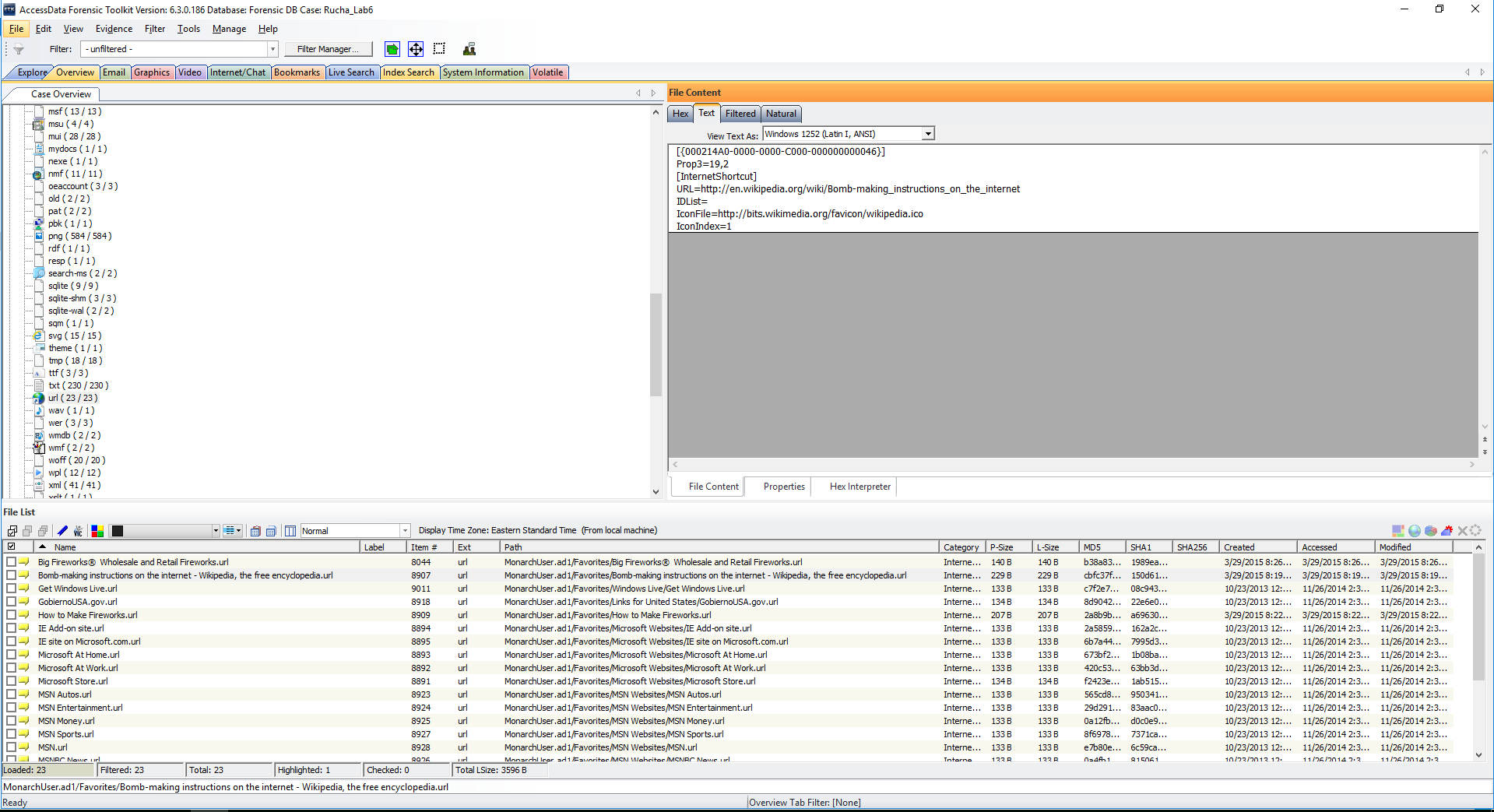
**Path: Monarch2User.ad1/AppData/Roaming/Thunderbird/Profiles/v24p7btk.default/Mail/pop-mail.outlook.com/Inbox>>entry#0111521.eml**



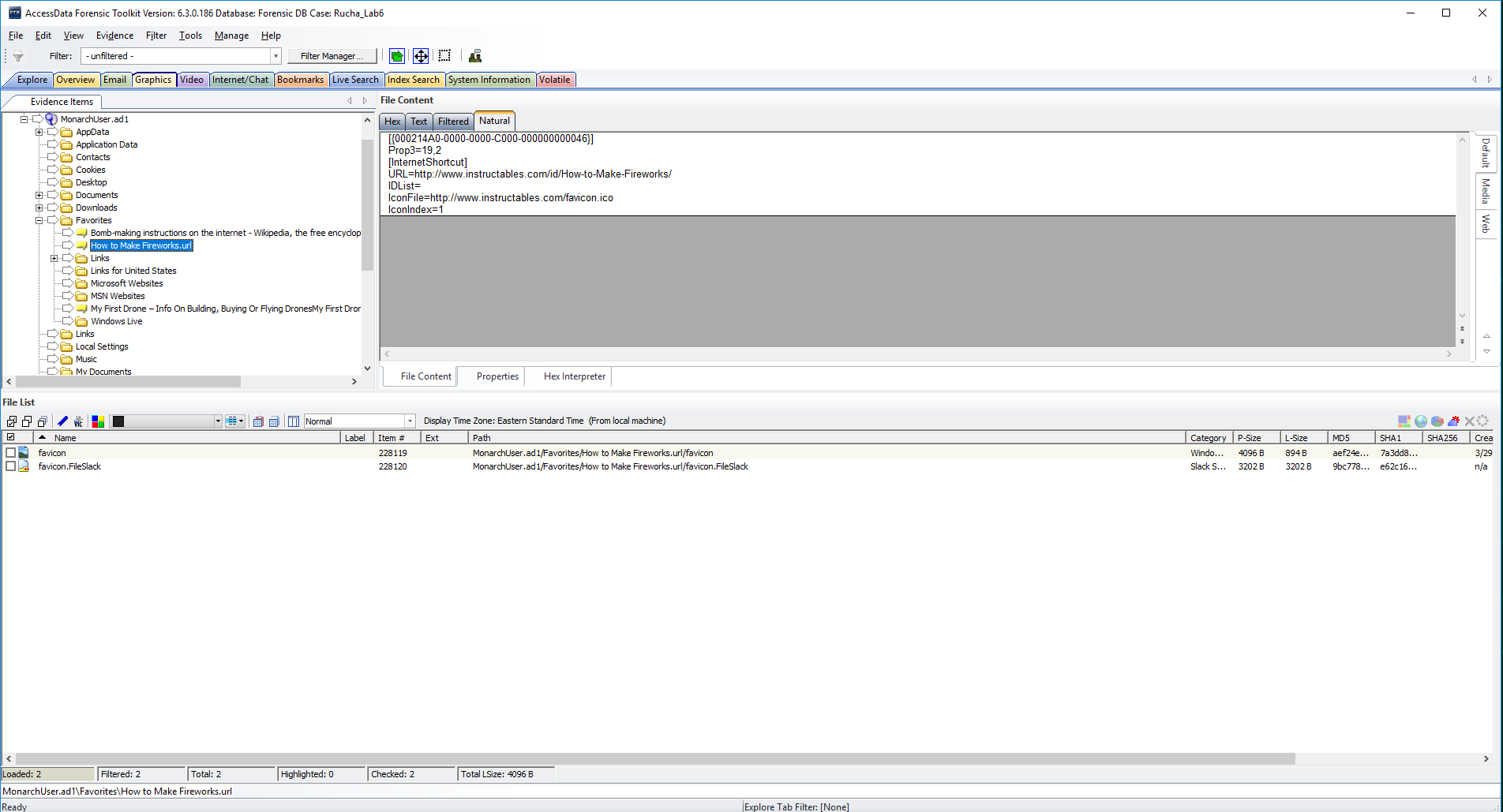
1. Are there any items related to the Monarch’s plans for violence?

Yes, as shown in below screenshots, several items were found related to Monarch’s plan for violence that includes URL’s and images.

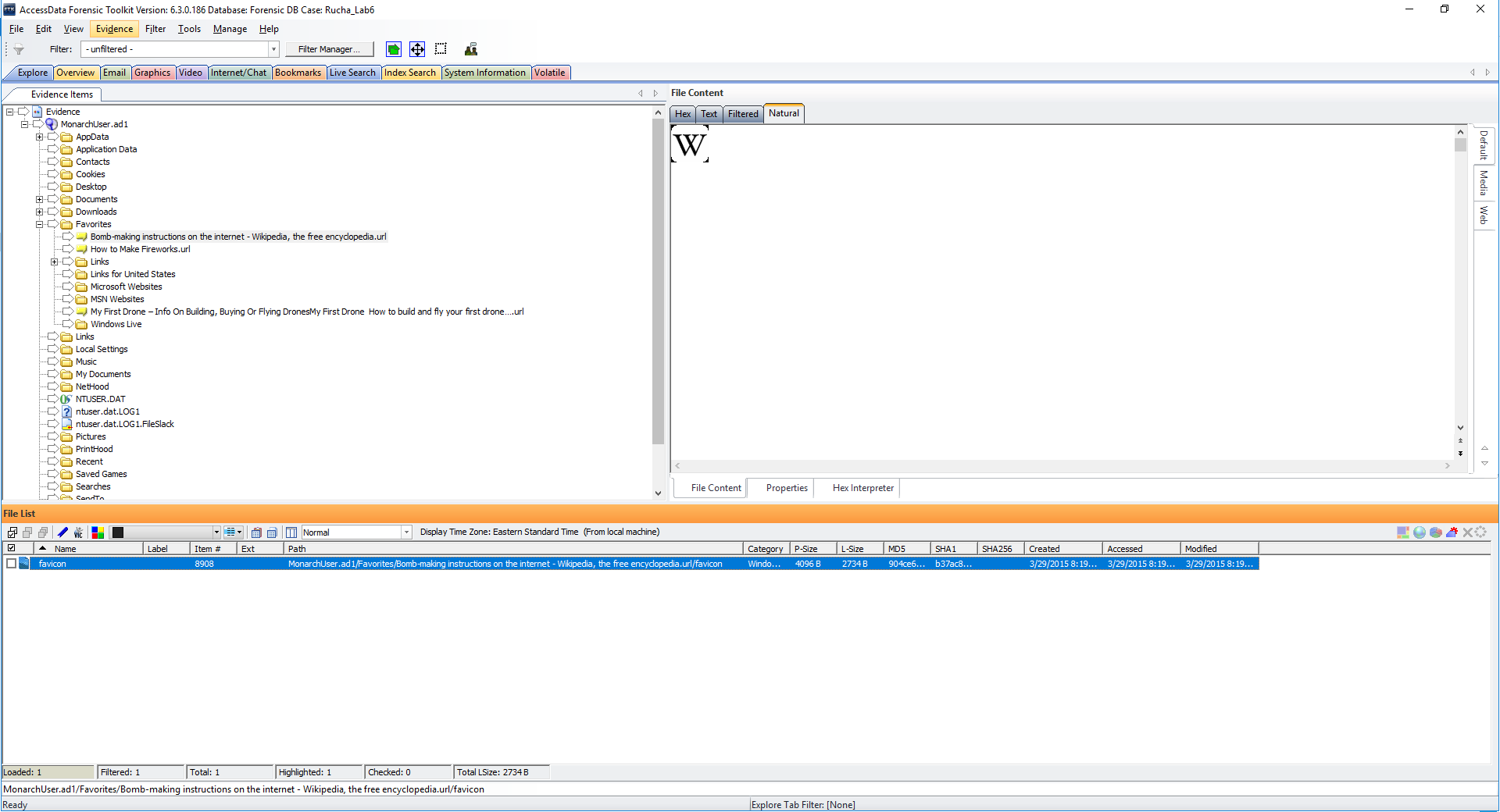
**Path: MonarchUser.ad1\Favorites\Bomb making instructions on the internet- Wikipedia, the free encyclopedia.url**



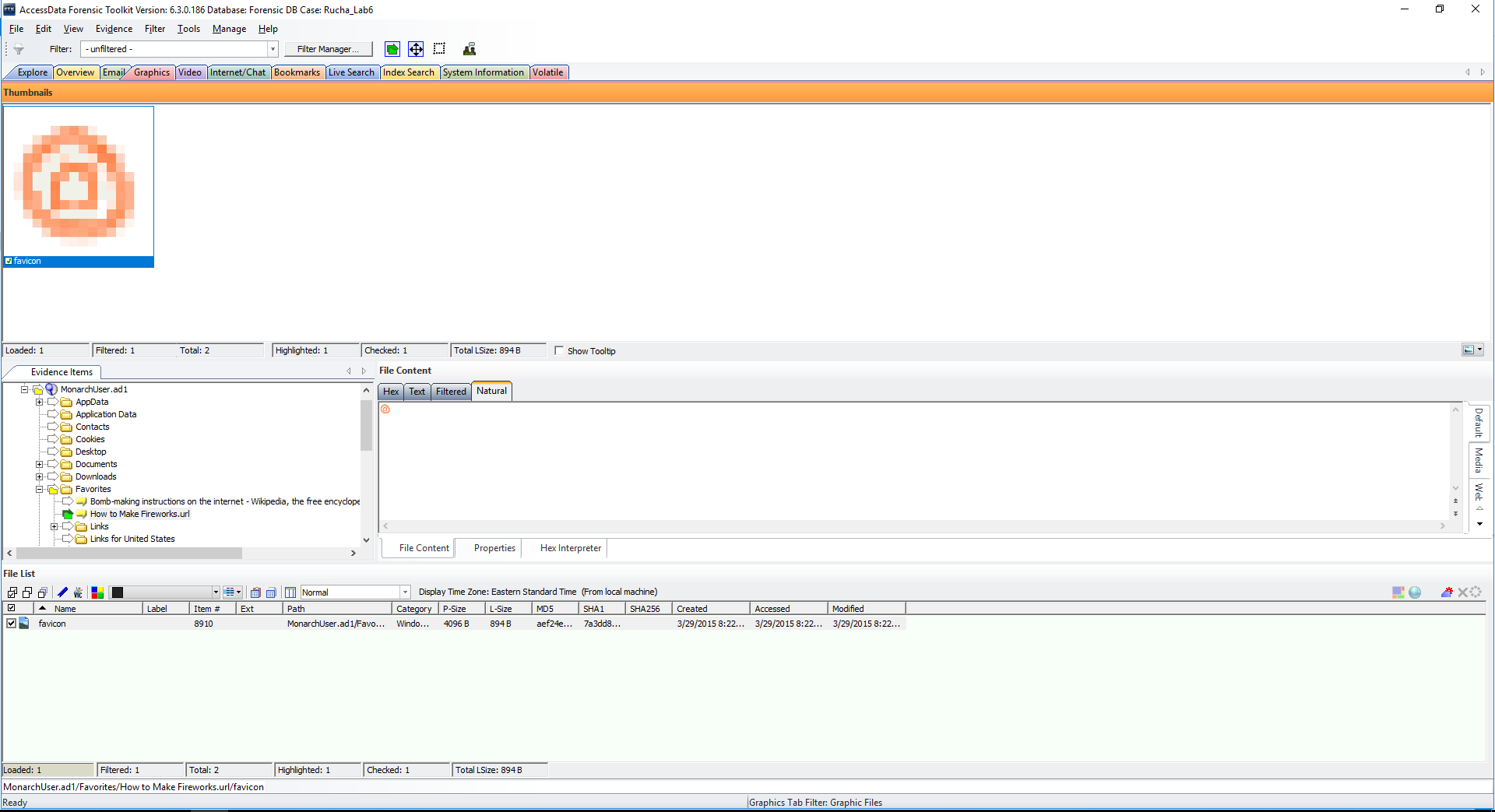
**Path: MonarchUser.ad1\Favorites\How to make Fireworks.url**



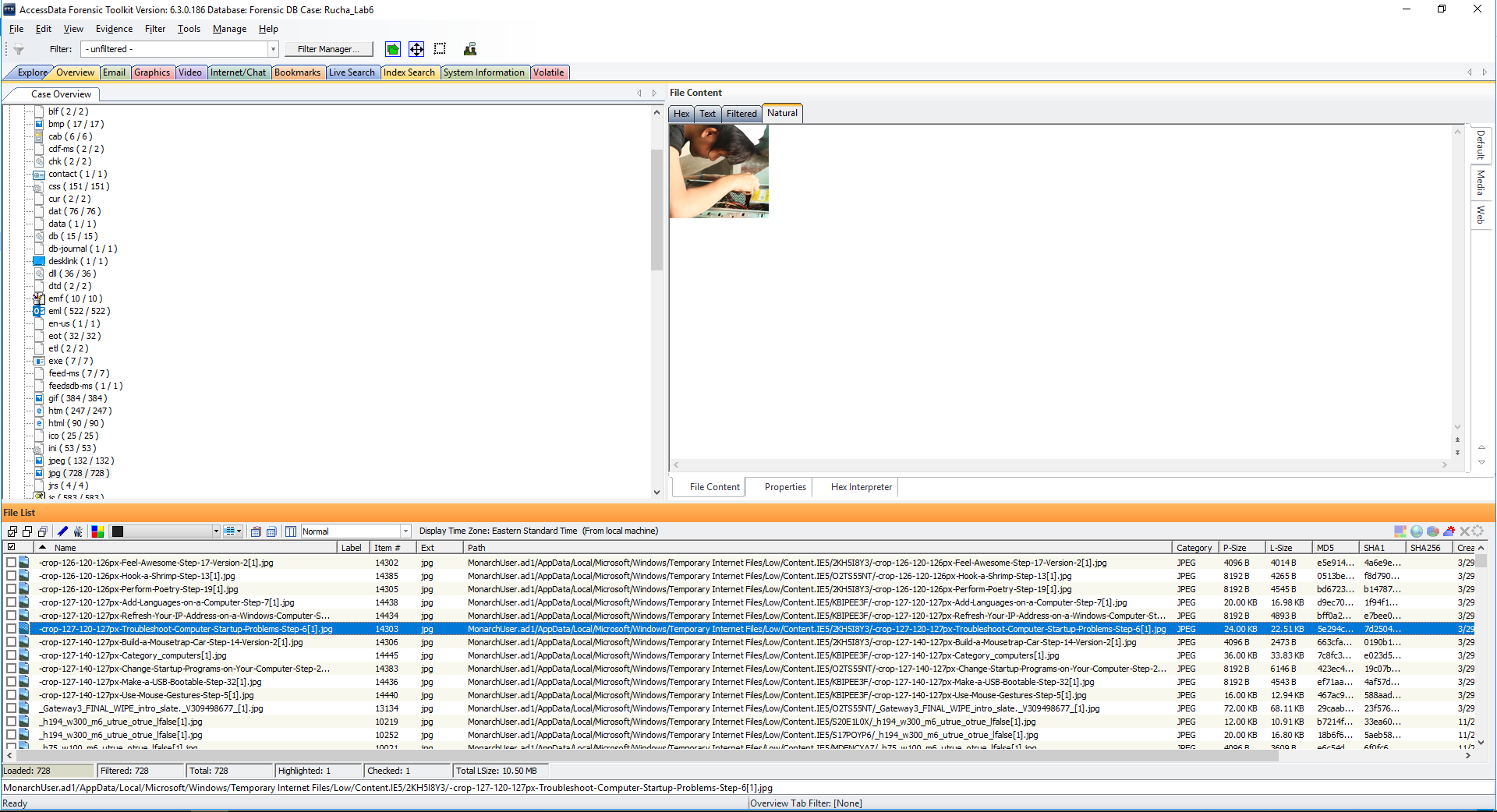
**Path: MonarchUser.ad1\Favorites\Bomb making instructions on the internet- Wikipedia, the free encyclopedia.url/favicon**



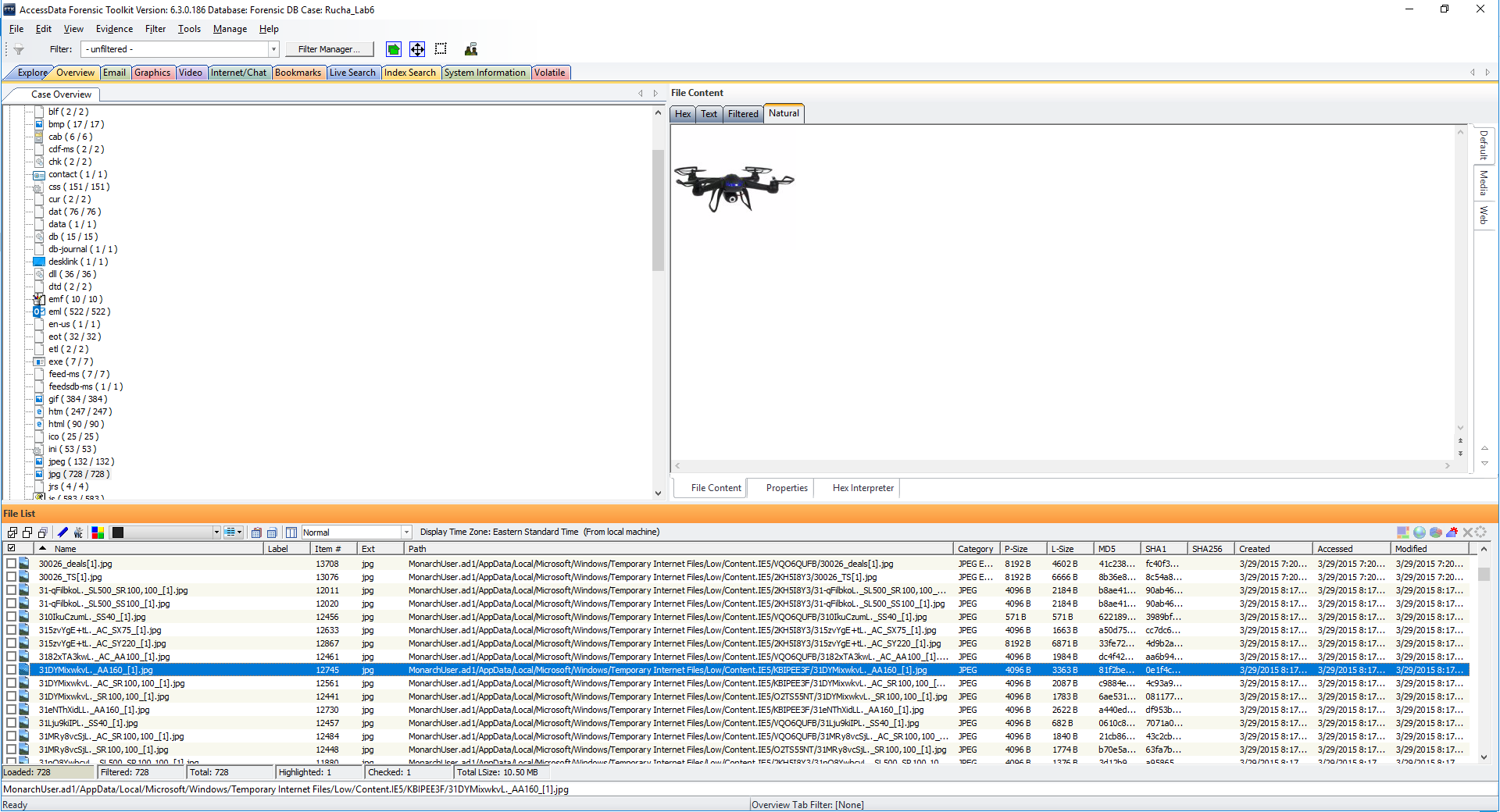
**Path: MonarchUser.ad1\Favorites\How to make Fireworks.url/favicon**



**Path: MonarchUser.ad1/AppData/Local/Microsoft/Windows/Temporary Internet files/Low/Content.IE5/2KH518Y3/-crop-127-120-127px-Troubleshoot-Computer-startup-Problems-Step-6[1].jpg**



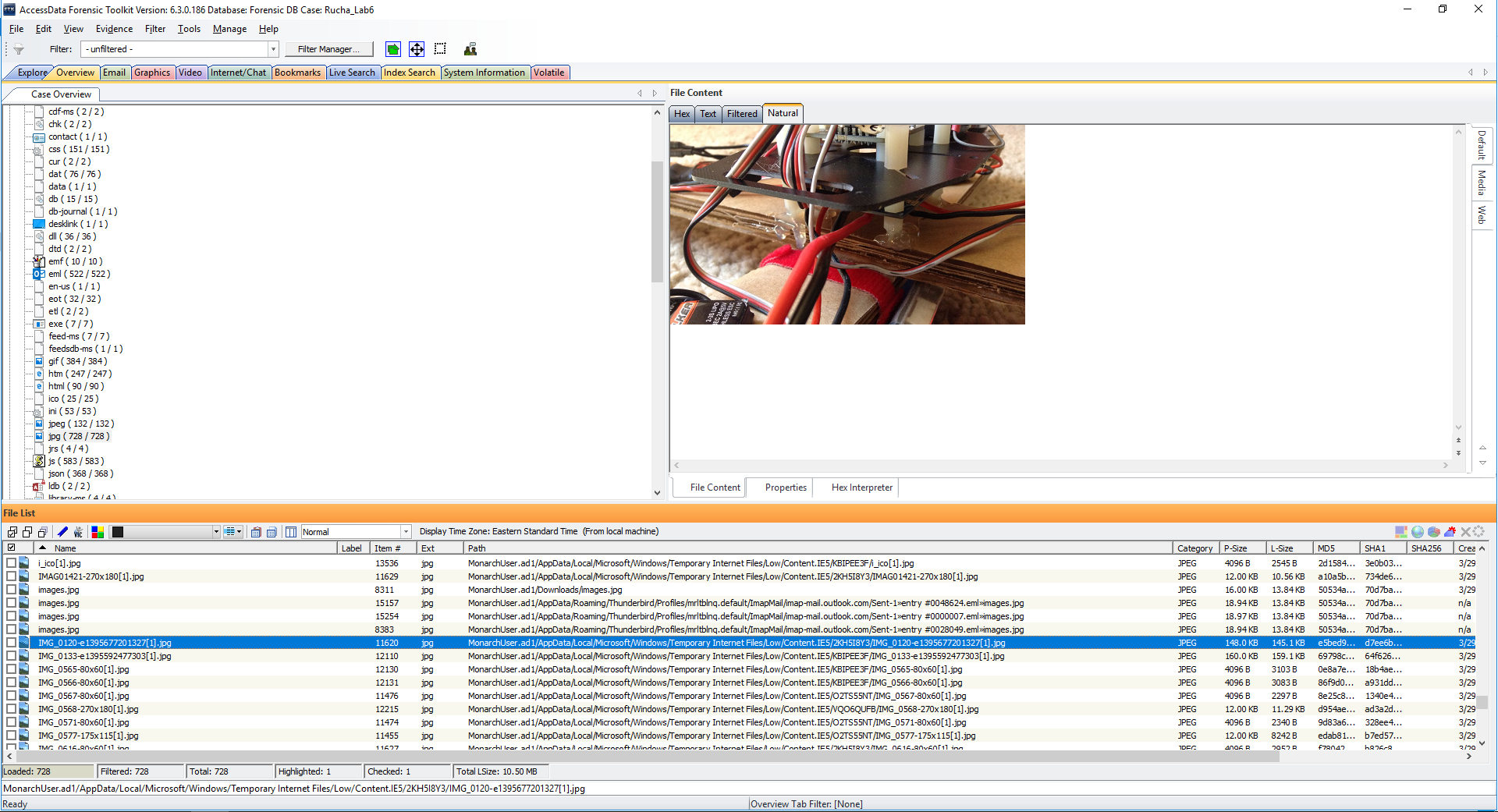
**Path: MonarchUser.ad1/AppData/Local/Microsoft/Windows/Temporary Internet files/Low/Content.IE5/KBIPEE3F/31DYMixwkvl\_AA160\_[1].jpg**



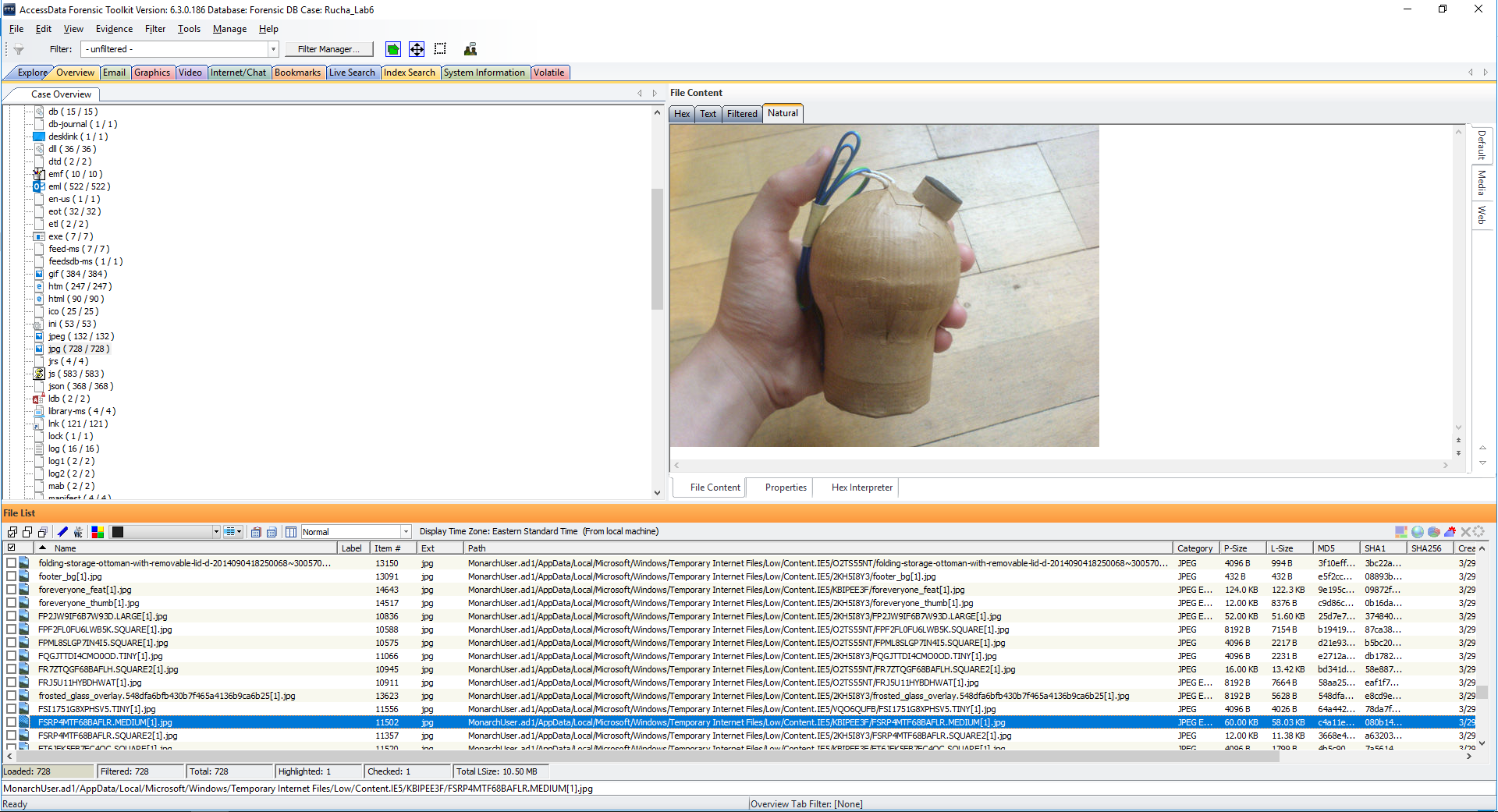
**Path: MonarchUser.ad1/AppData/Local/Microsoft/Windows/Temporary Internet files/Low/Content.IE5/2KH518Y3/31nZiagb2Wl\_AA160\_[1].jpg**



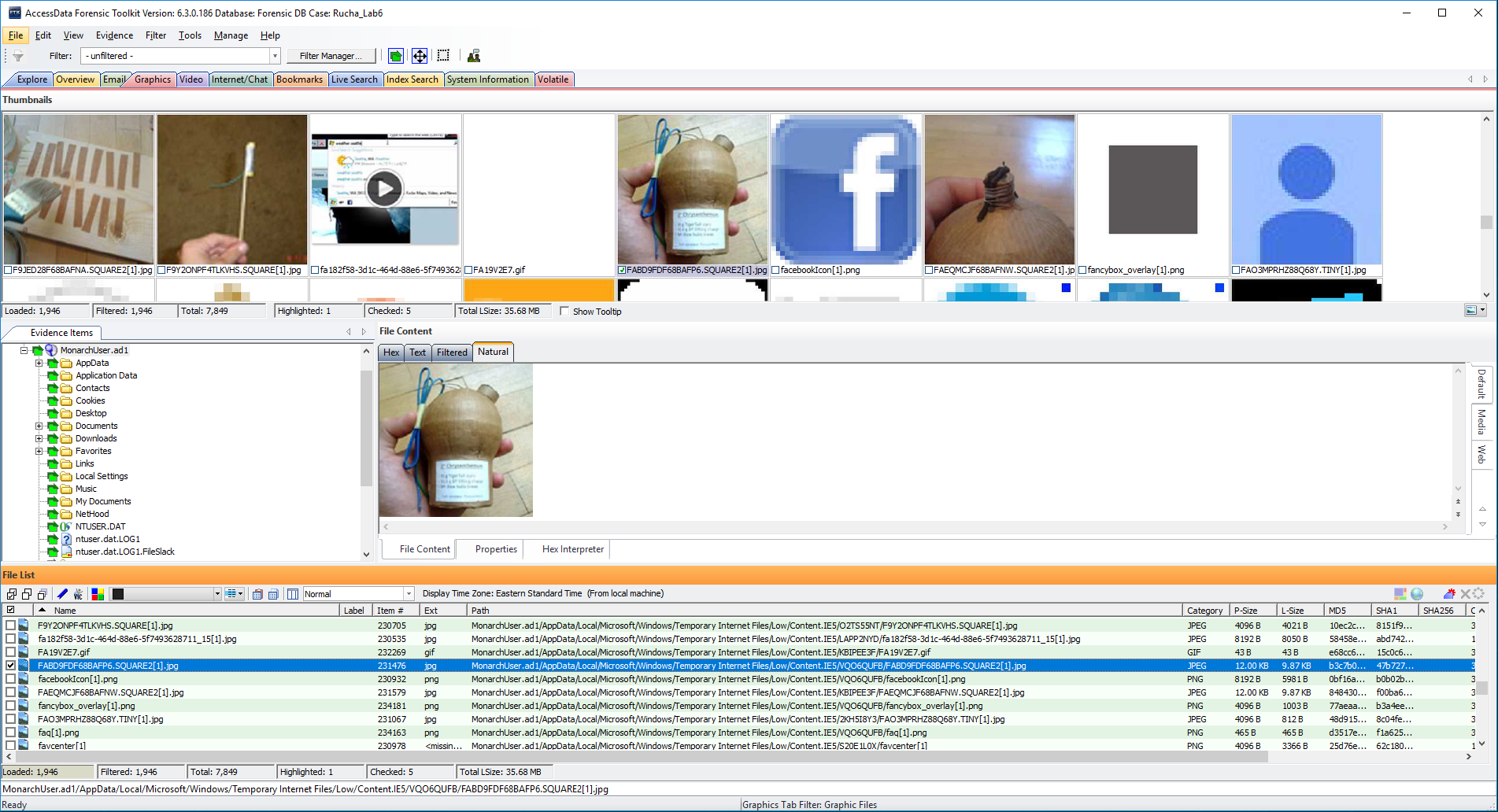
**Path: MonarchUser.ad1/AppData/Local/Microsoft/Windows/Temporary Internet files/Low/Content.IE5/2KH518Y3/IMG\_0120-e1359677201327[1].jpg**



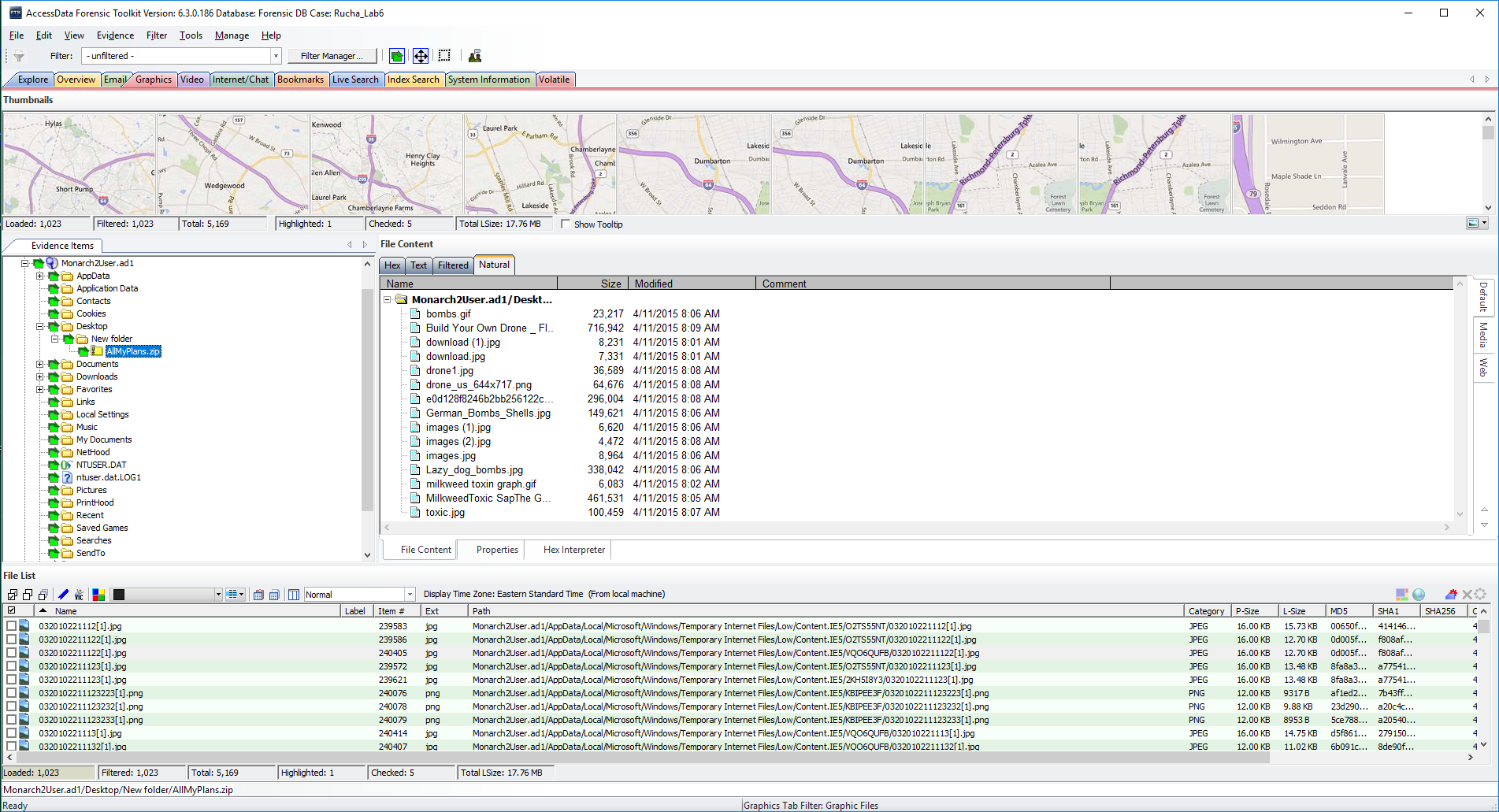
**Path: MonarchUser.ad1/AppData/Local/Microsoft/Windows/Temporary Internet files/Low/Content.IE5/KBIPEE3F/FSRP4MTF688AFLR.MEDIUM[1].jpg**



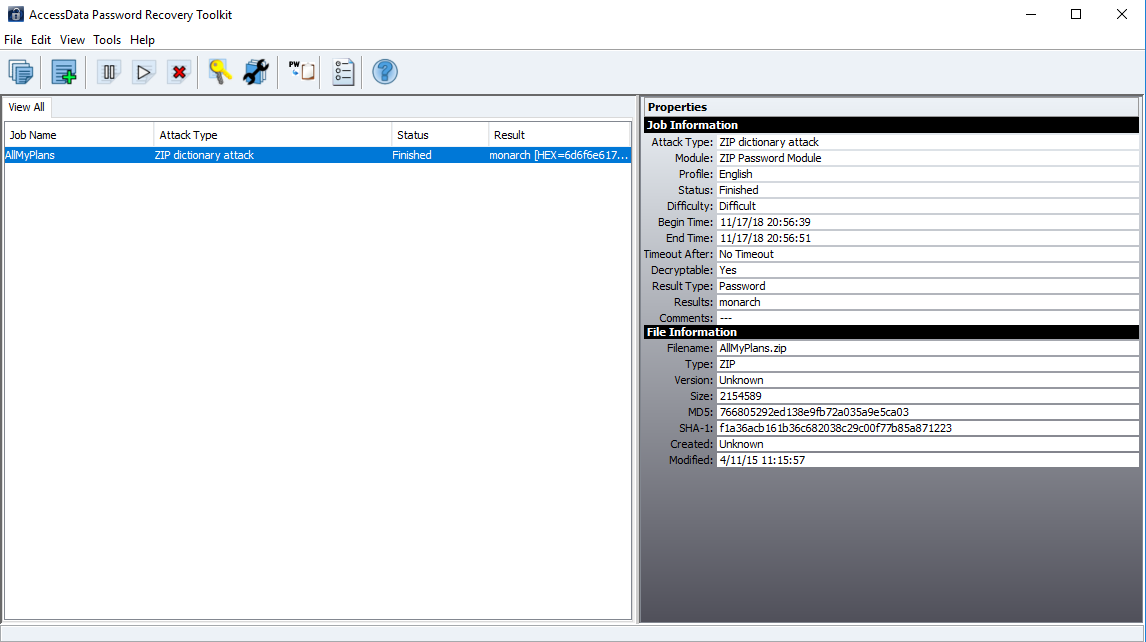
**Path: MonarchUser.ad1/AppData/Local/Microsoft/Windows/Temporary Internet files/Low/Content.IE5/VQO6QUF/FABD9FDF68BAFP6.SQUARE21.jpg**

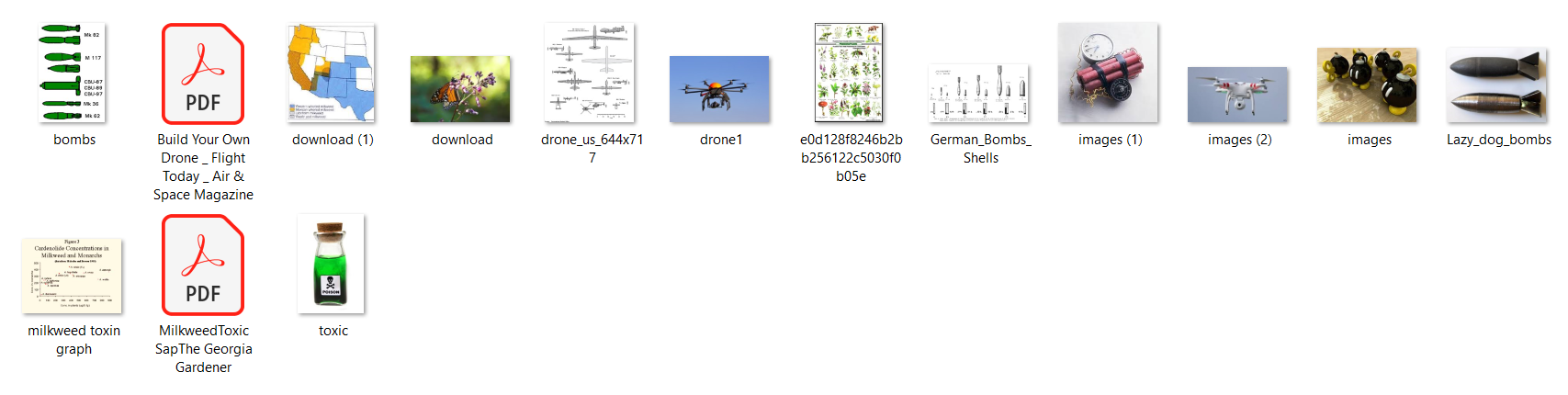


**Path: Monarch2user.ad1\Desktop\Newfolder\AllMyPlans.zip**



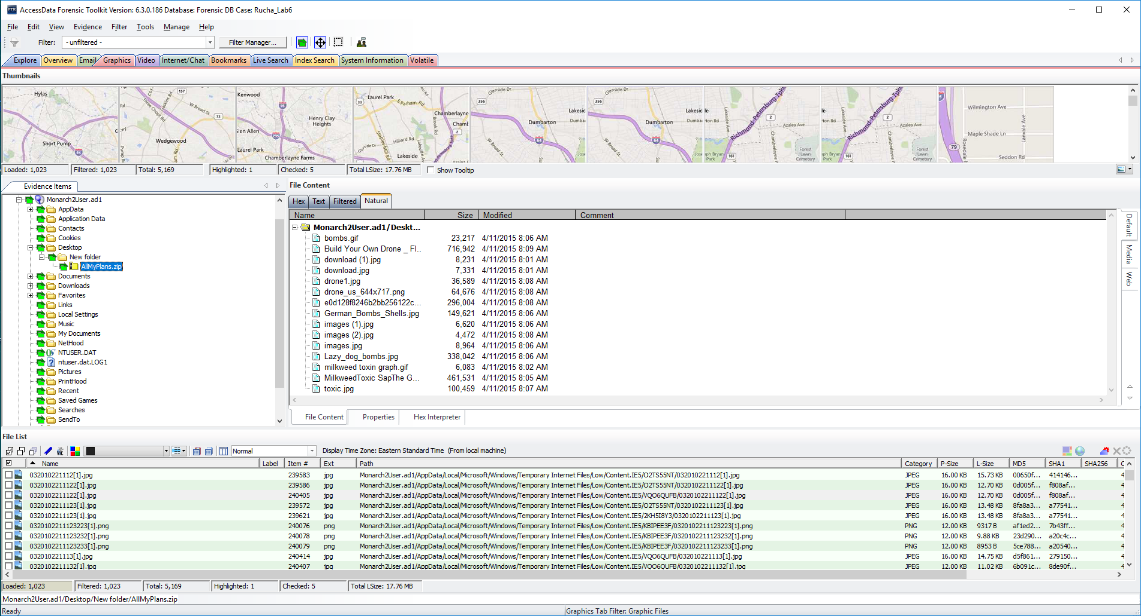
In order to decrypt the above file-**‘AllMyPlans.zip’**, I used Password Recovery Toolkit (PRTK) and found many items like explosives, poisons, drones, and bombs:

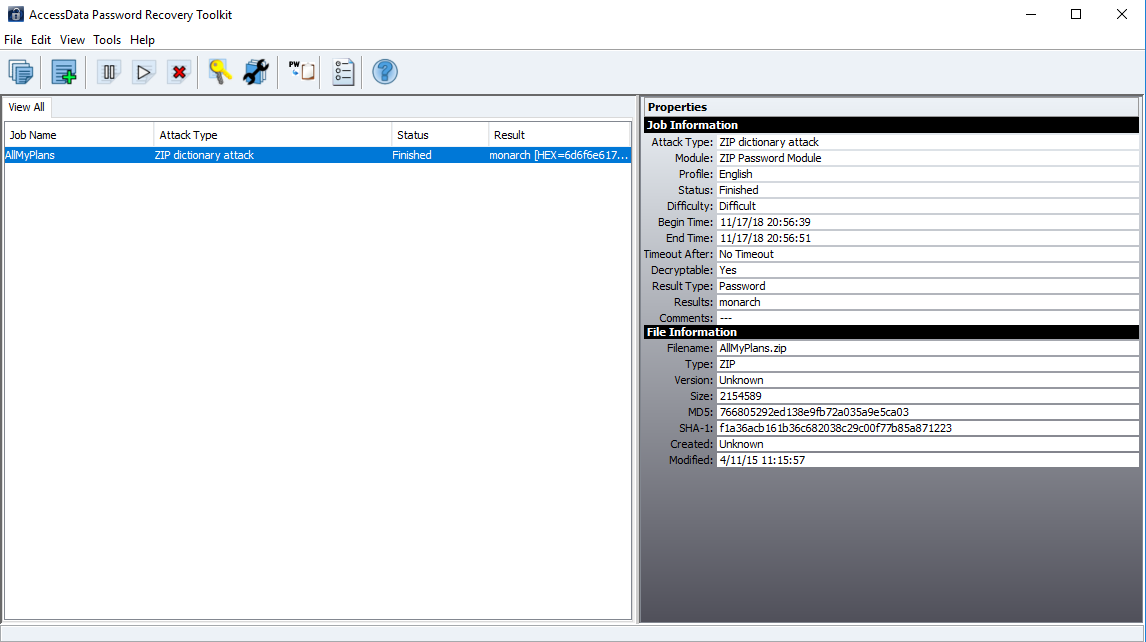




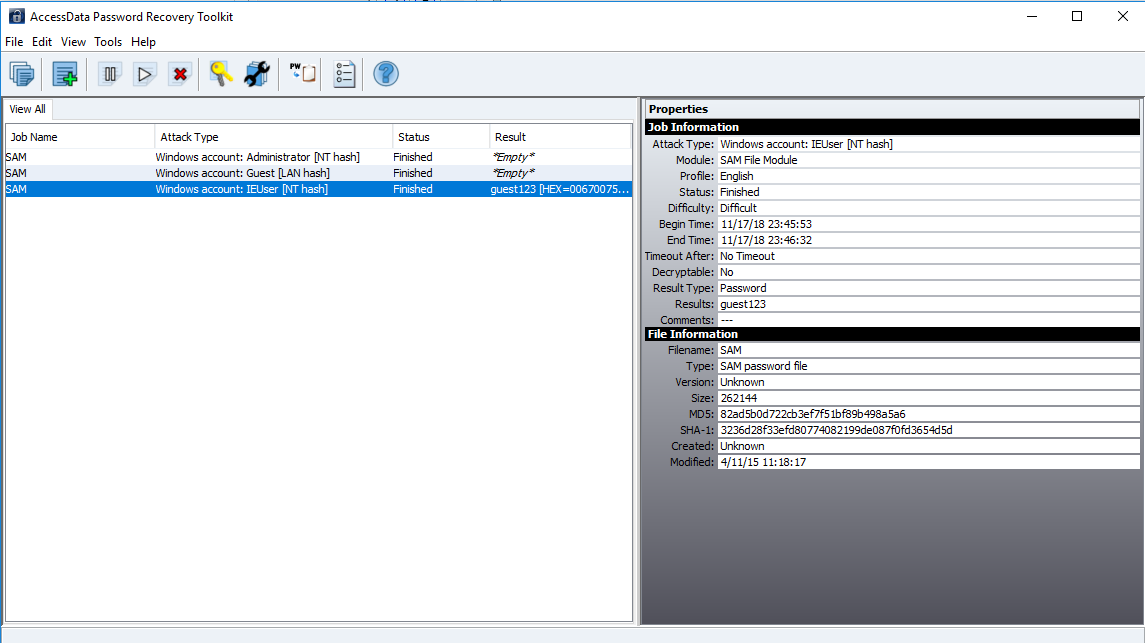
1. Can you recover any passwords?

To recover the passwords, I extracted the file ‘AllMyPlans.zip’ and load it into PRTK. The password of **AllMyPlans.zip** was found to be ‘**monarch**’ as shown below:





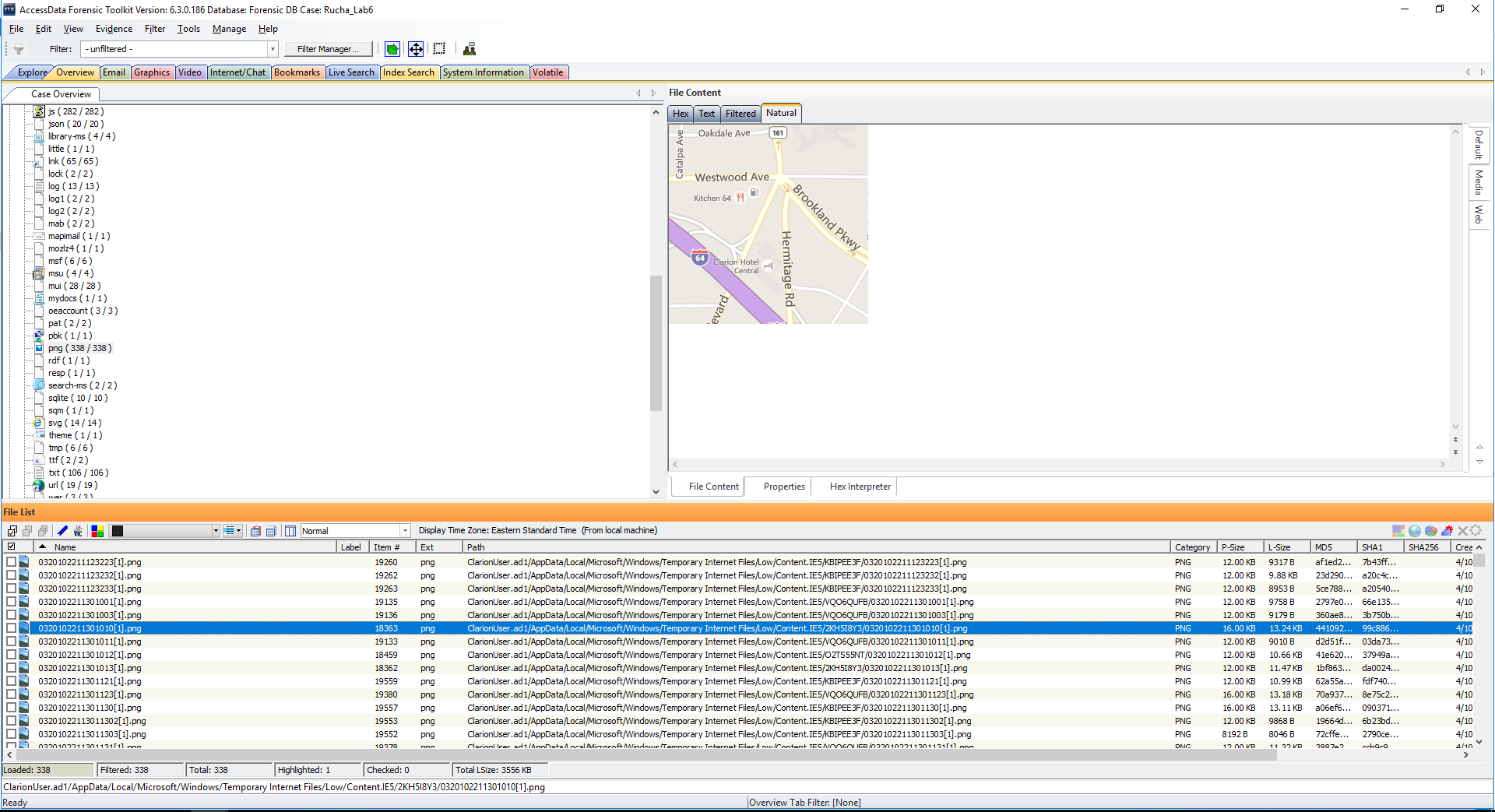
Additionally, I filtered the Registry files using Filter Manager and after exporting the ‘SAM’ and ‘SYSTEM’ files from ‘Monarch.E01’, I then loaded them into PRTK to crack the user account password. The password for the user account was found to be: **‘guest123’.**



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

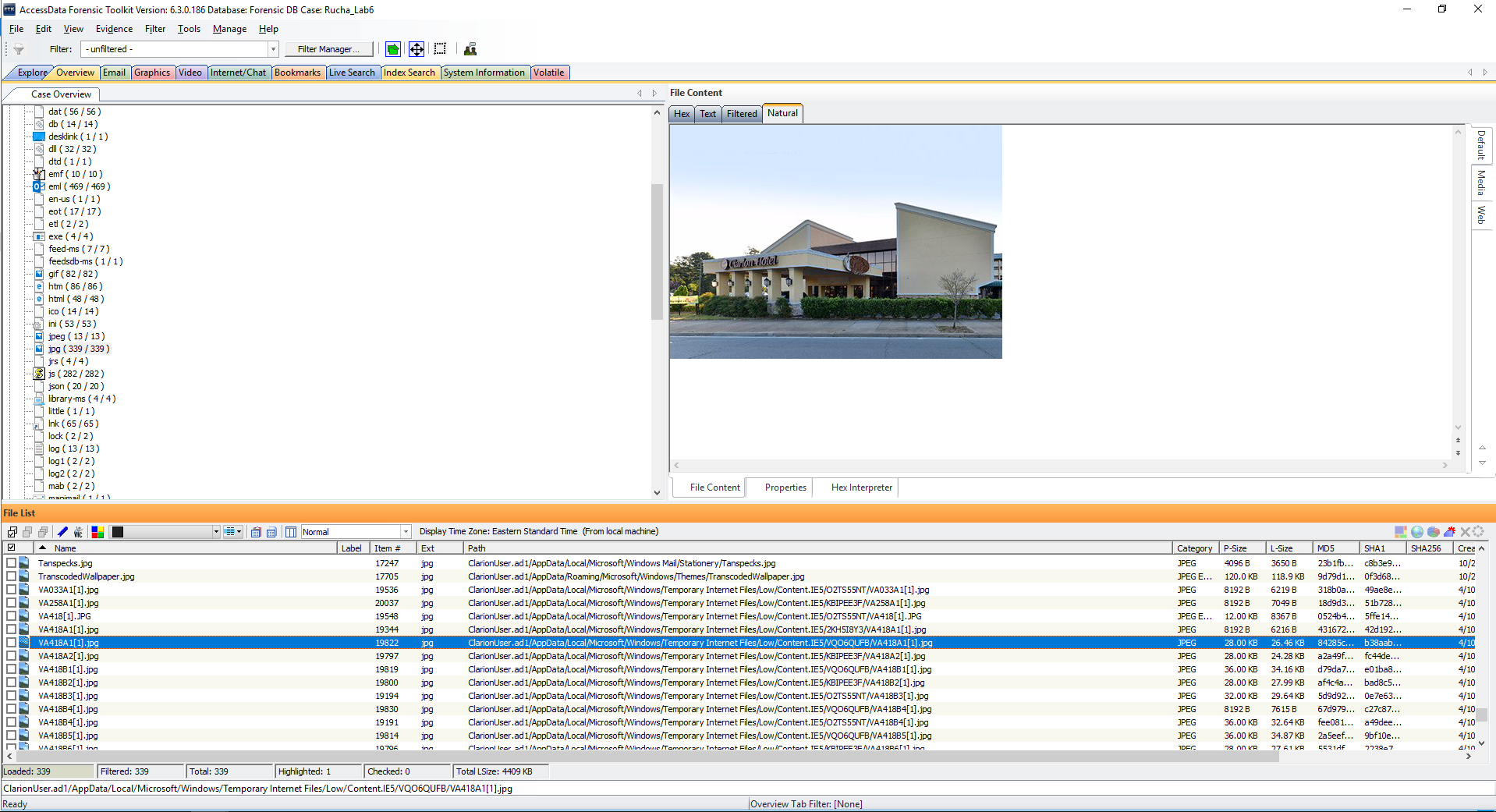
I found the following image in **‘ClarionUser.ad1’** which shows the location of a hotel named **‘Clarion’**.

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



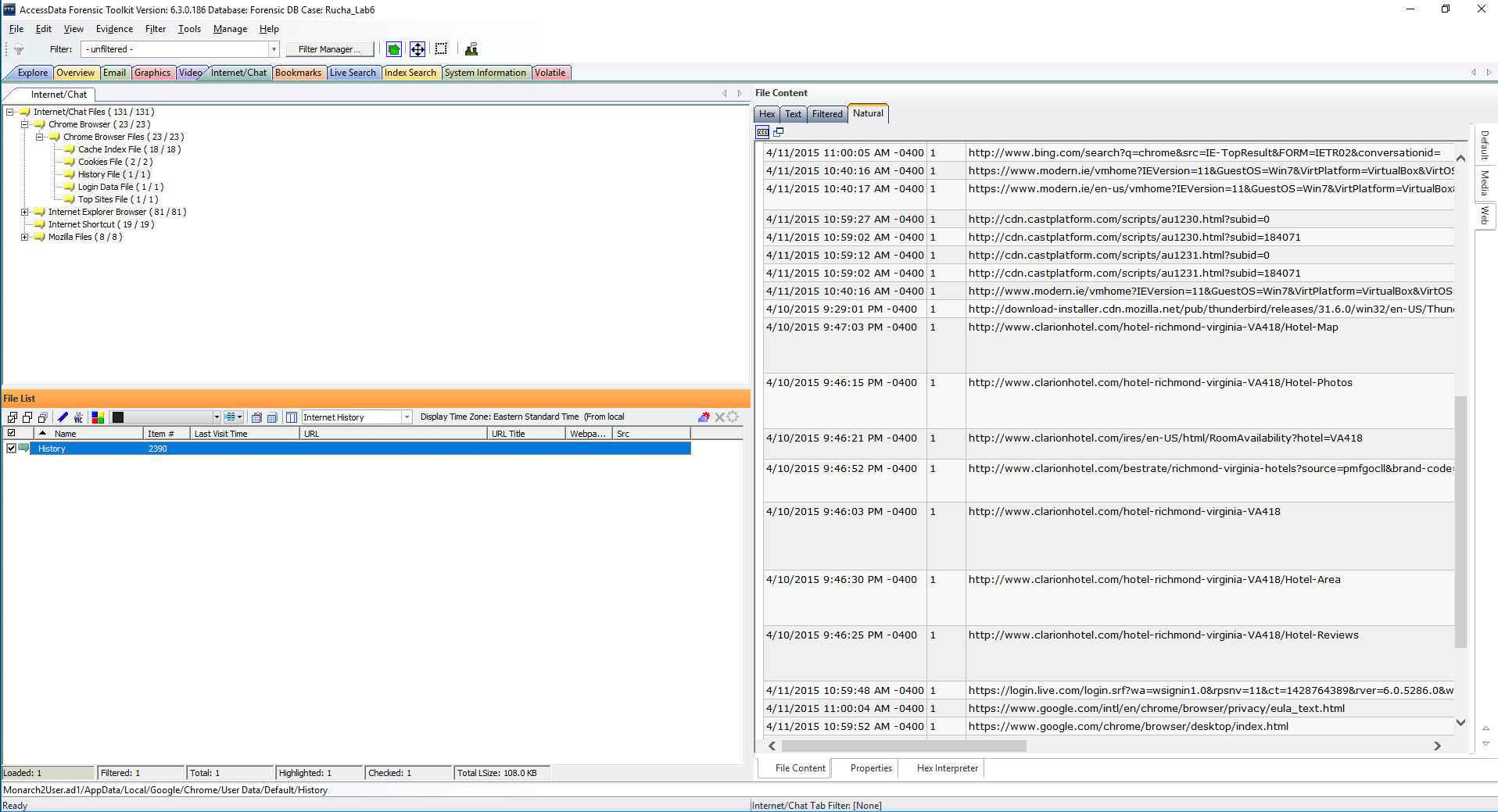
Below is a picture of Clarion Hotel which I found:

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



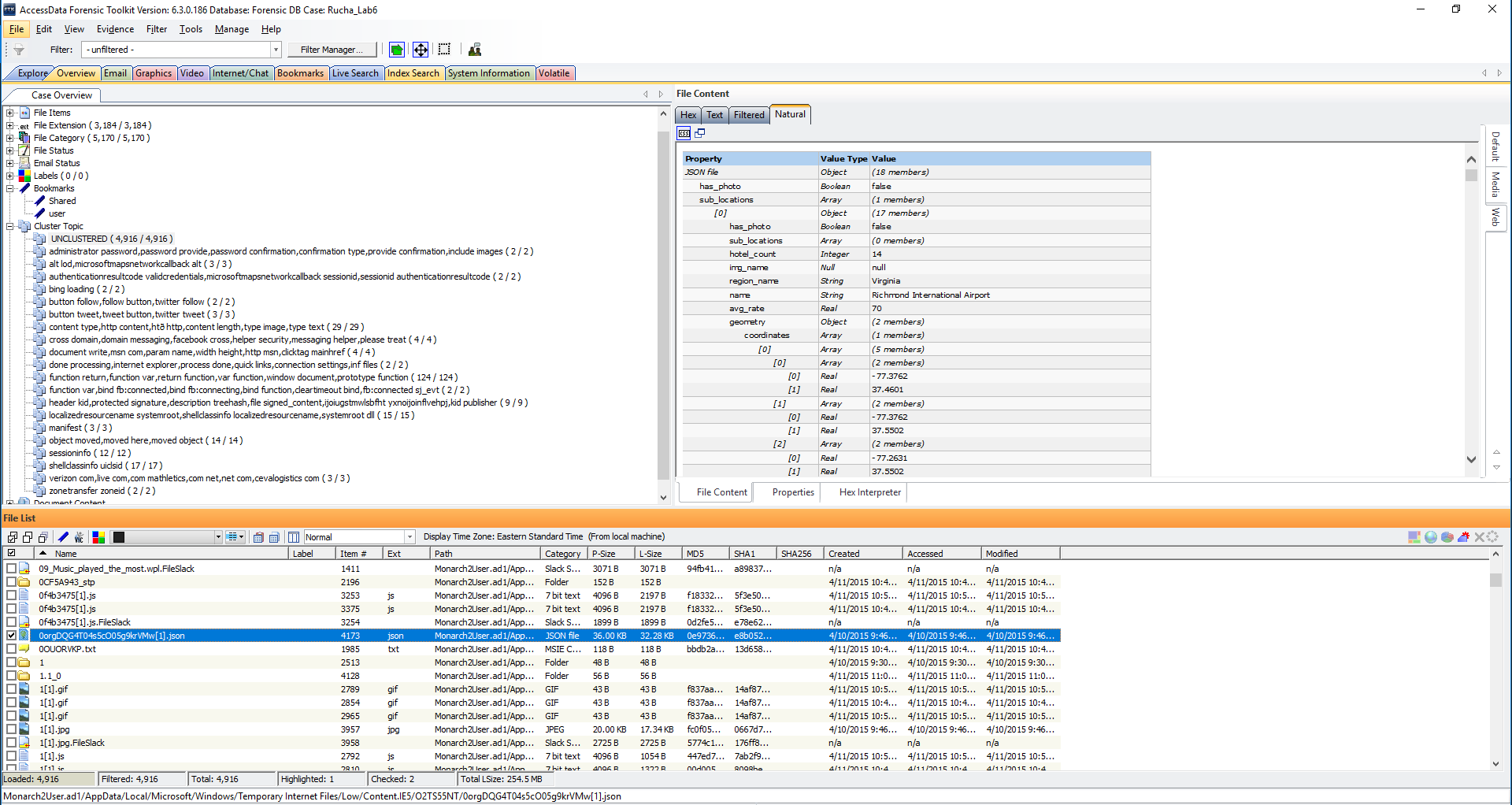
Additionally, in the “Internet/chat” tab, in the history file, I found the above search results of “Clarion Hotel”.

**Path: Monarch2User.ad1/AppData/Local/Google/Chrome/UserData/Default/History**



Also, In the JSON file, the property “hotel\_count” value was found to be 14 indicating that ‘Clarion Hotel’ was searched about several times.

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



**Conclusion**

In this lab, I examined the images Monarch.E01, Monarch2.E01, MonarchUser.ad1, Monarch2User.ad1, ClarionUser.ad1 and Clarion.E01, using FTK and found certain relevant email conversations, email addresses of Monarch and the Guild operative and images of Monarch. Additionally, I found the location of the Clarion hotel by examining the browser history in FTK. I used Password Recovery Toolkit to recover passwords of the encrypted file and user account and also found certain suspicious items like bombs, poisons, explosives, drones etc.