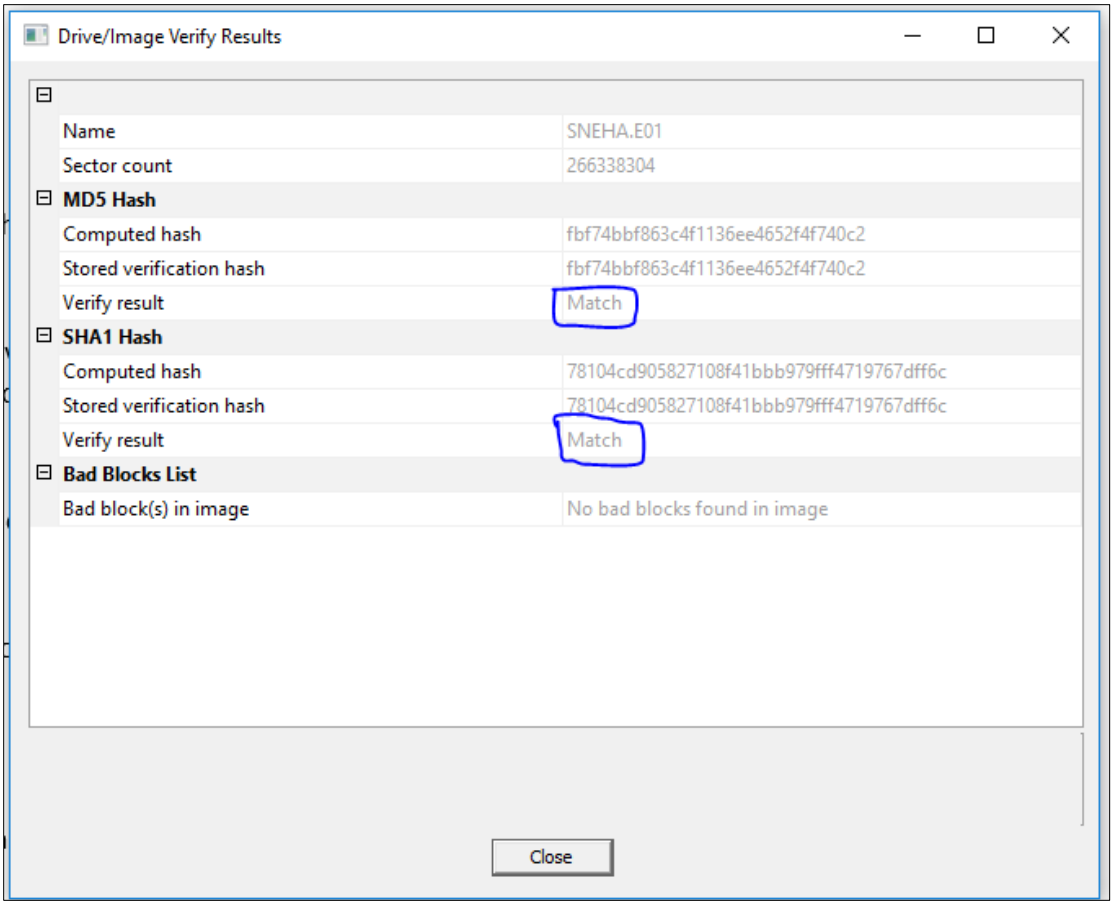
ITIS 5250
Sneha Rangari
Graduate Lab
12/04/2018

Overview:

In this Lab, I have created a case file and asked to verify it, once verified we perform the examination and find the deliverables required and try to identify the suspect. I have created scenario having: communications via text apps/email, pictures and records or and a general timeline of what will happen before the evidence is acquired into image file.
Thus I will be finding certain email conversations, photographs, encrypted files, etc. from the given image. Also, I will be looking for evidence such as, contacts, addresses and login attempts.

Forensic Acquisition & Exam Preparation

I am provided with the forensic image that was made by the police department which I loaded using FTK Imager to verify integrity of the image. Also, I used Belkasoft Evidence center, Autopsy, PRTK and ESE Database Viewer for evidence processing.

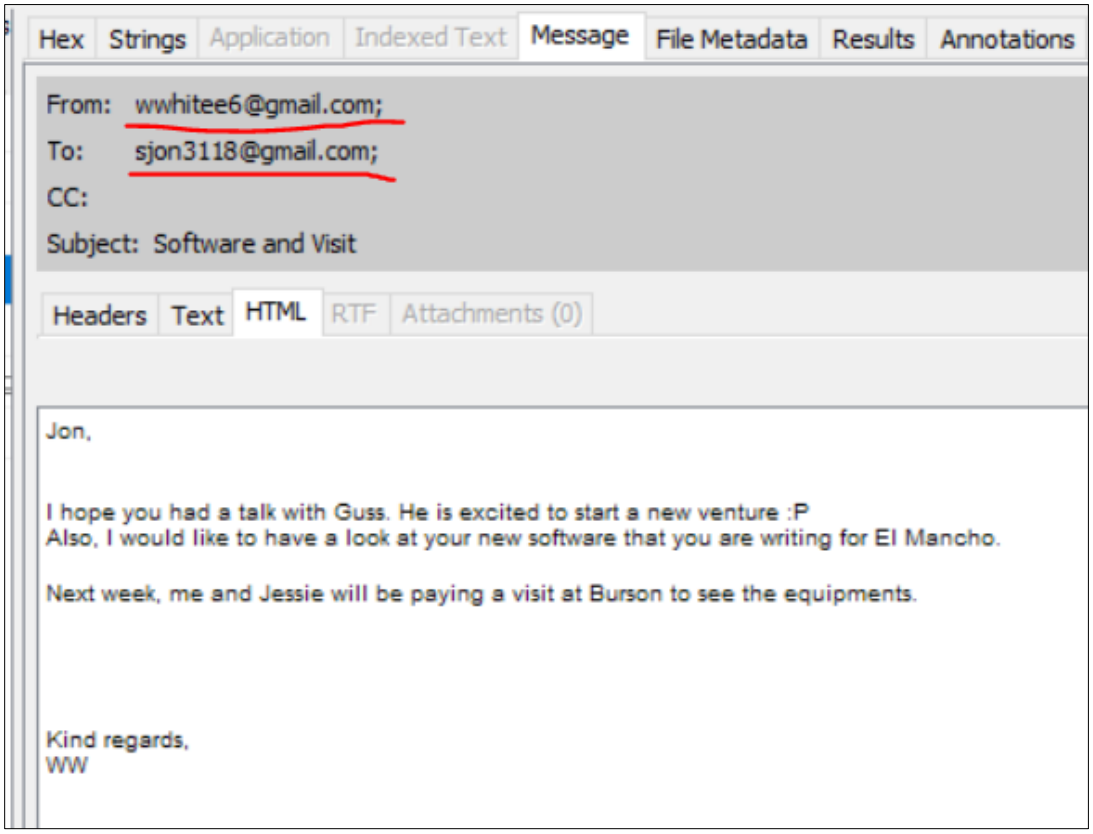


Both, the stored and computed hash matches.

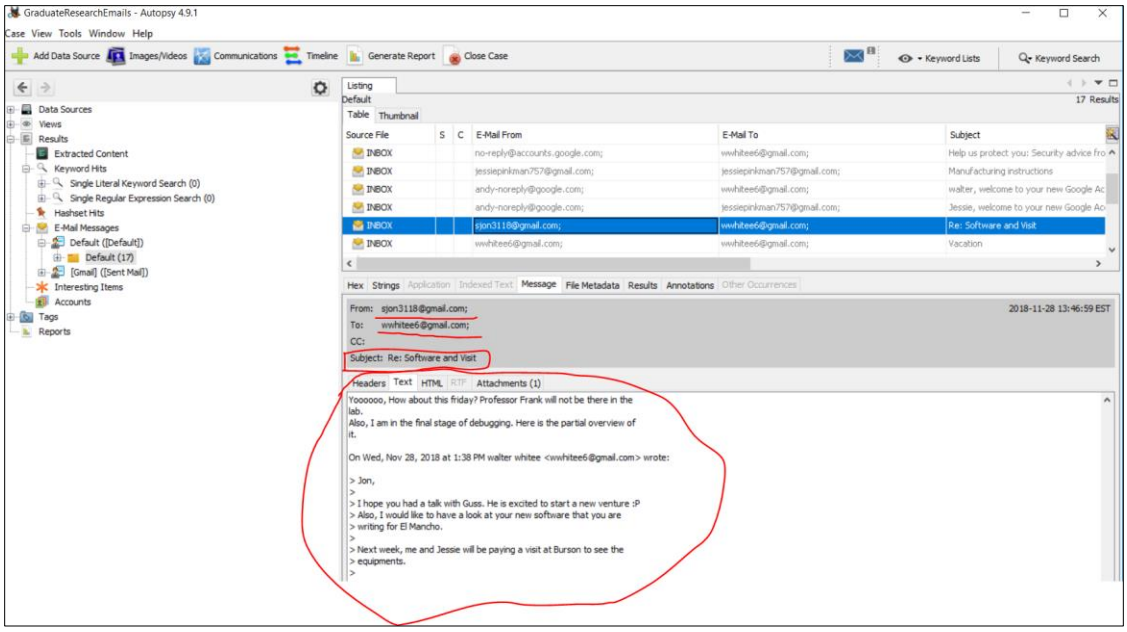
Findings and Report (Forensic Analysis)

1. Can you find any evidence that shows El Mancho members were talking to the students?

Using Autopsy tool and searching into E-Mail Messages I found this below screenshot showing one of the gang leader of El Mancho i.e White Walker is sending mail to Snow Jon who is the student, about the new software and visiting to Burson lab.

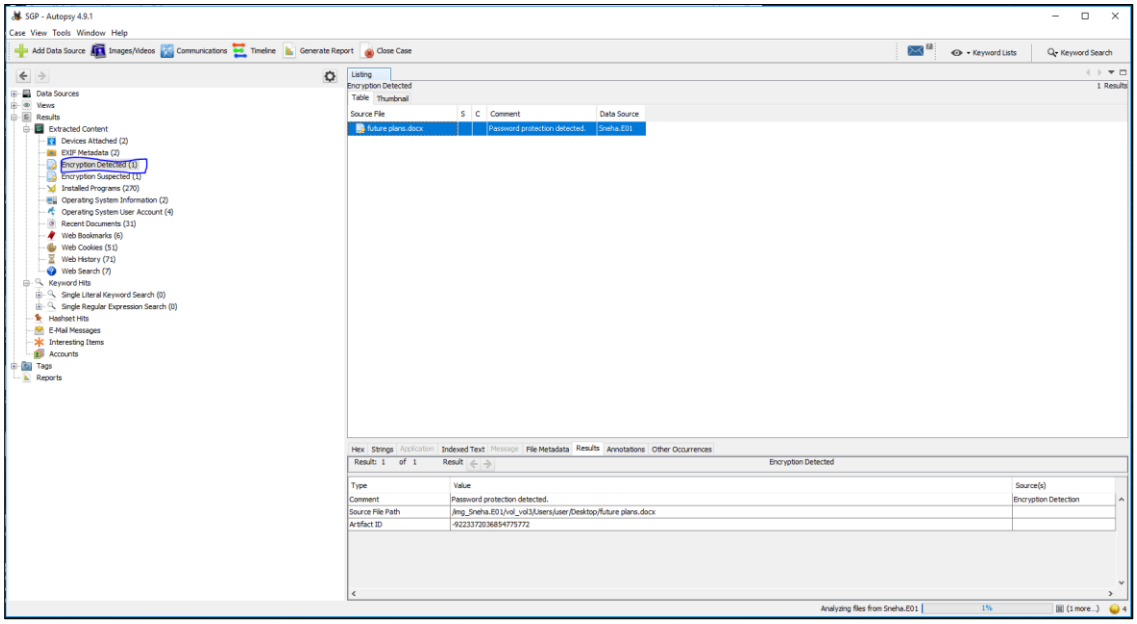


Below screenshot shows the reply message from Snow Jon to White Walker.

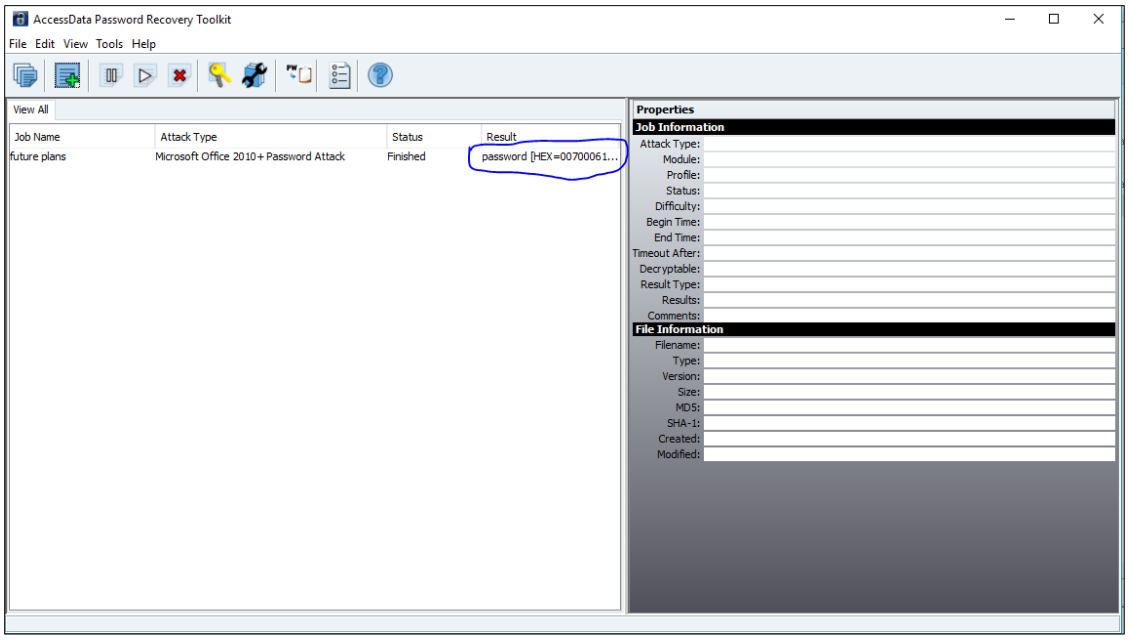


2. Can you find any encrypted files, passwords?

For this evidence I used Autopsy tool wherein under “Result” I found “Encryption Detected” file namely futureplans.docx which gives a description of password protection detected.

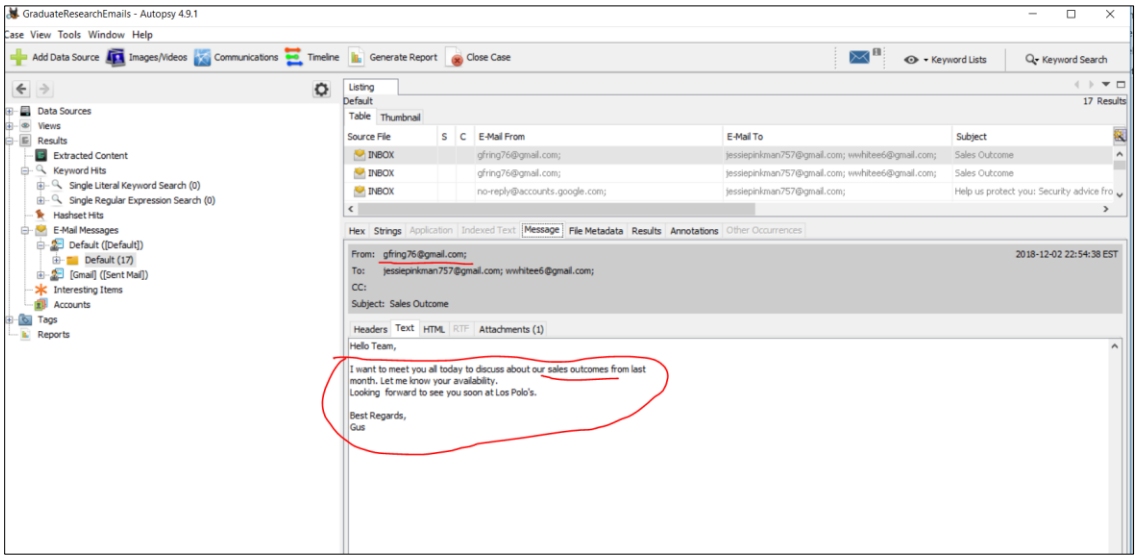


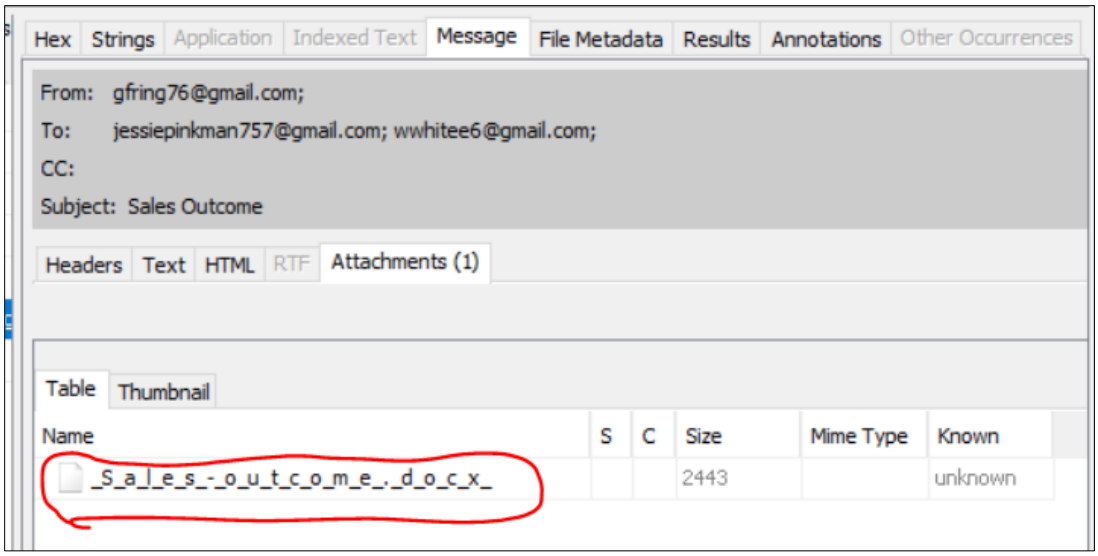
Using PRTK I cracked the password as “password” of the encrypted file as shown in below screenshot.



3. Find out any evidence that indicates Fring's plans to deploy money laundering.

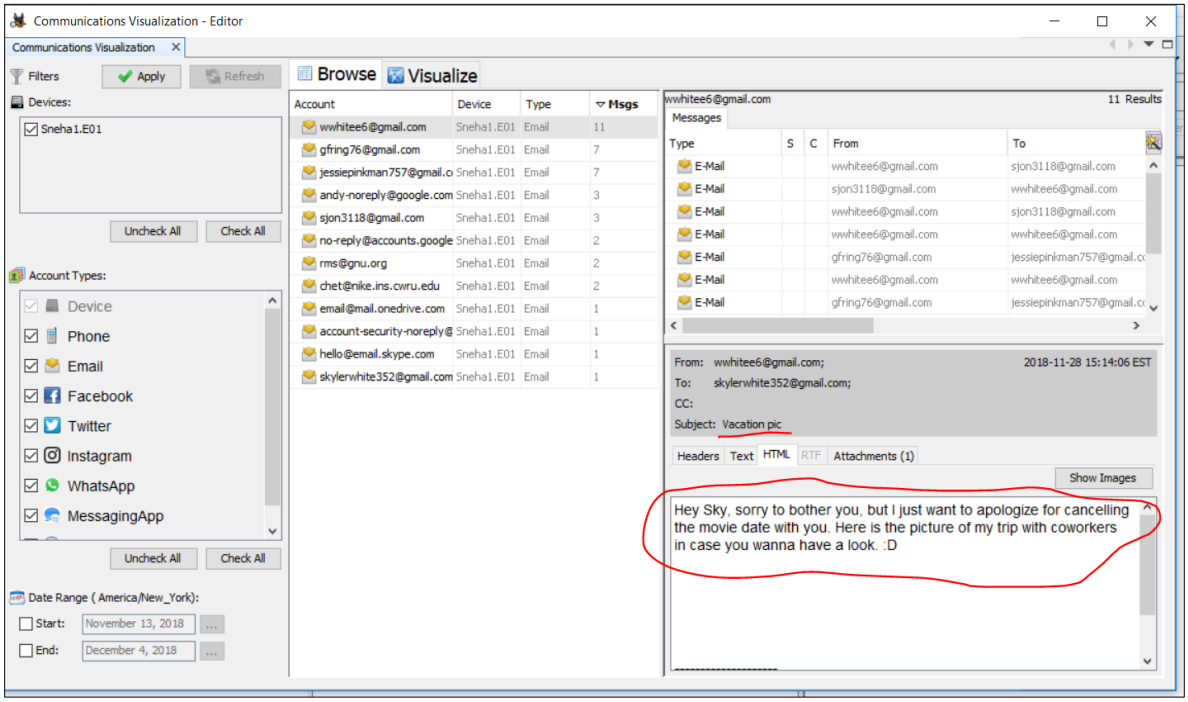
Using Autopsy tool and searching in E-Mail Messages I found conversation between Gus Fring and Jessie Pinkman discussing on sales outcome which actually comes from illegal drug selling.

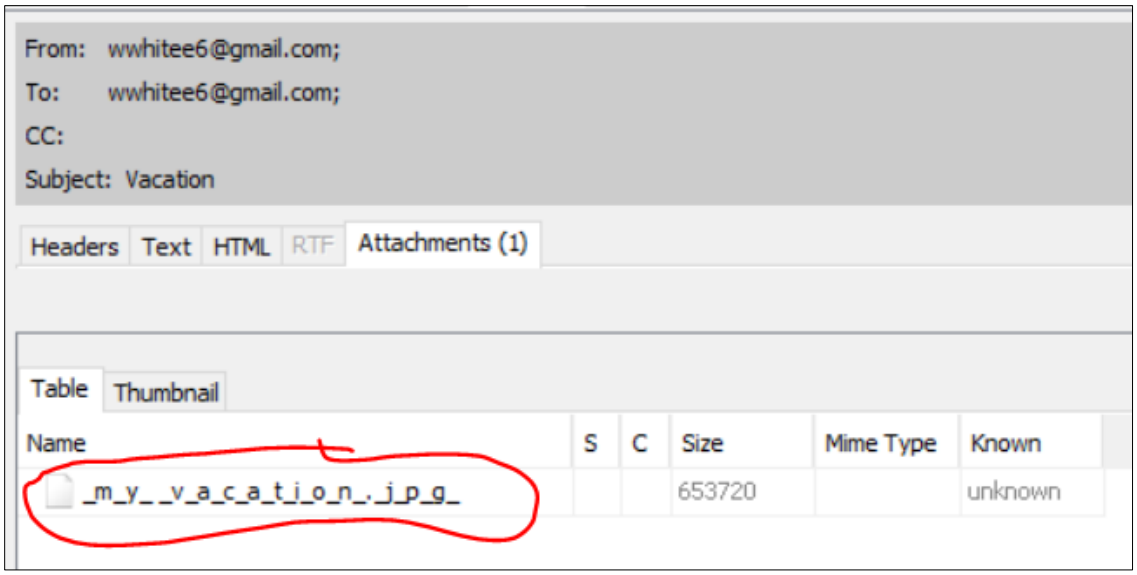




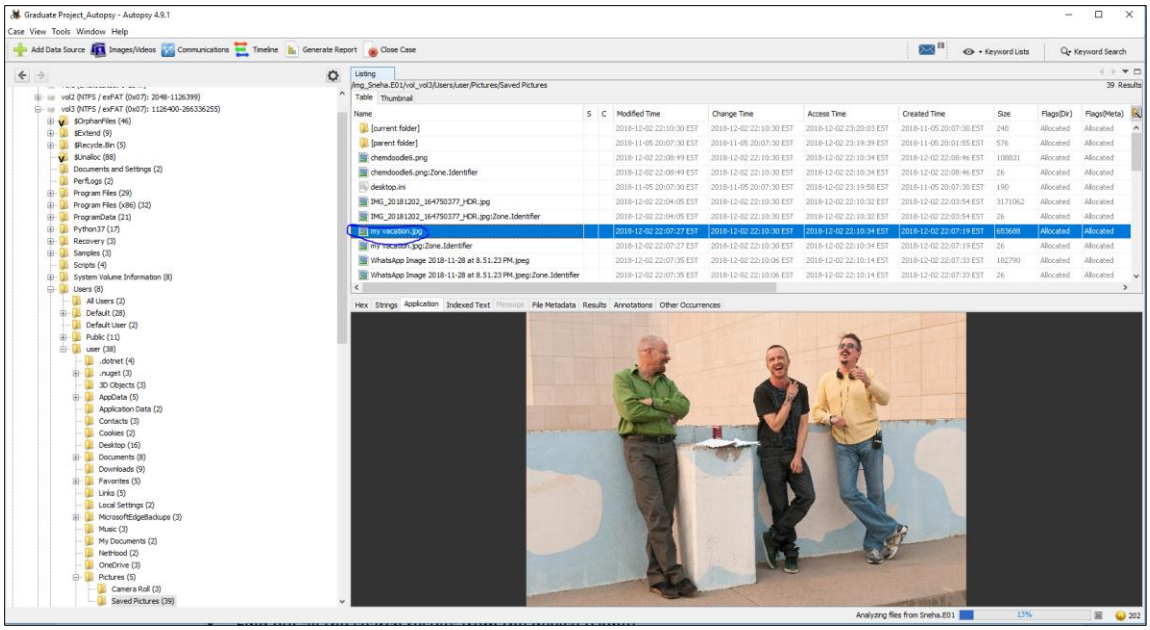
4. Can you find any pictures of El Mancho operatives?

El Mancho has a leader Gustavo Fring with gang members Walter White and Jessie Pinkman. As per the email conversation of Gus with his wife about picture with his coworkers and having attachment as my_vacation.jpg



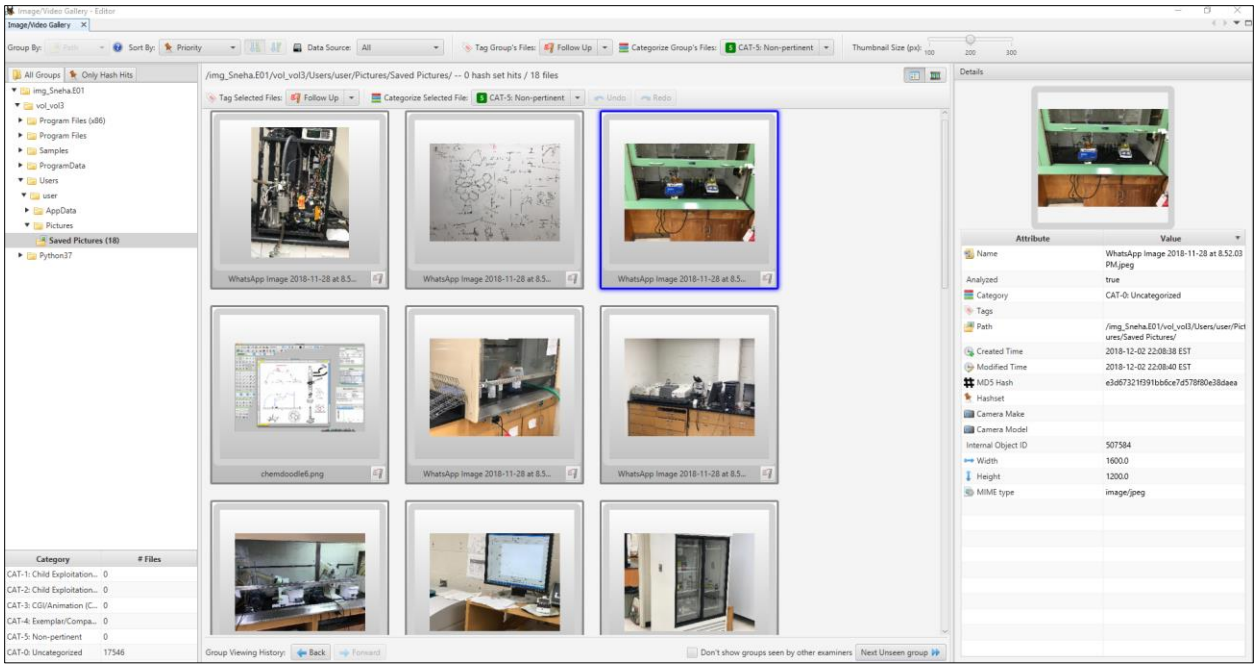


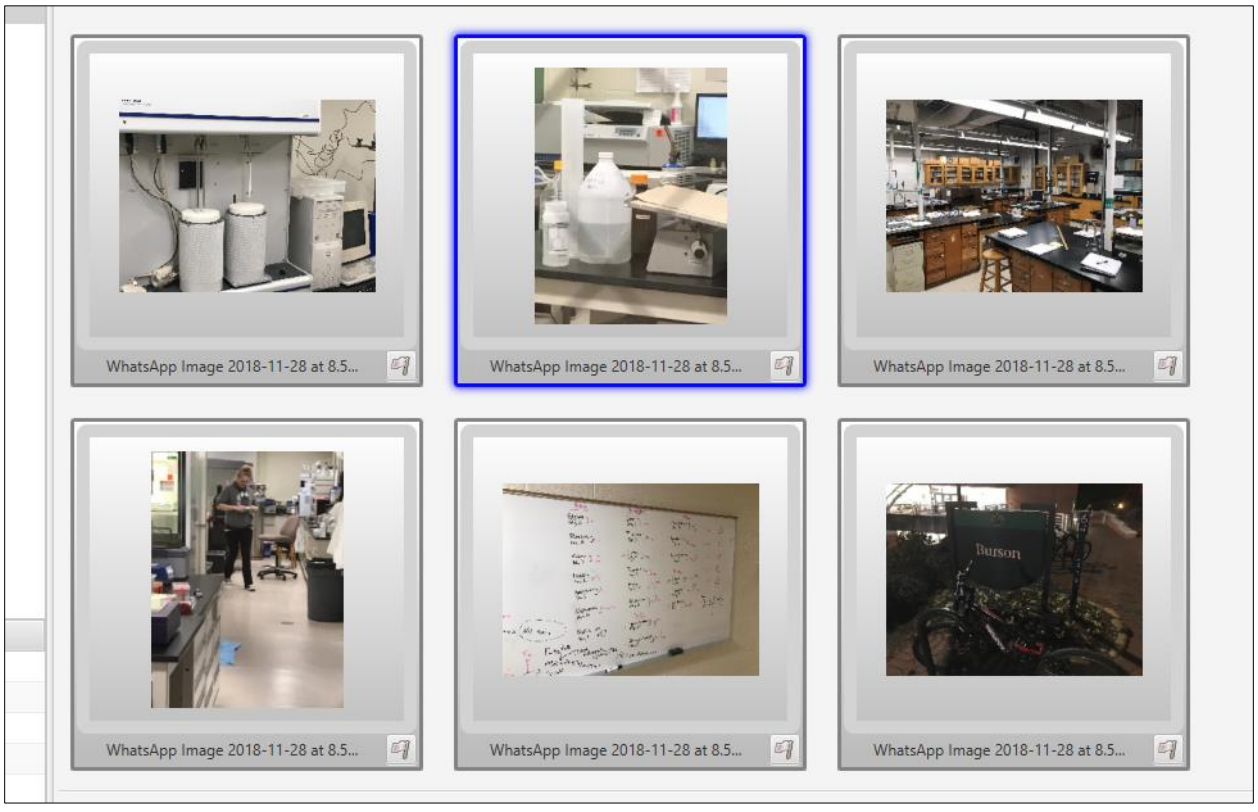
The below image of "my_vacation" shows this as picture of El Mancho operatives.



5. Evidence to show any suspicious activities inside the Burson lab?

From Autopsy tool, and going into Images/Videos tab I found images inside the Burson lab indicating some weird/ suspicious activities. Pictures showing chemical formulae, beaker, funnel indicate drugs are being manufactured here.



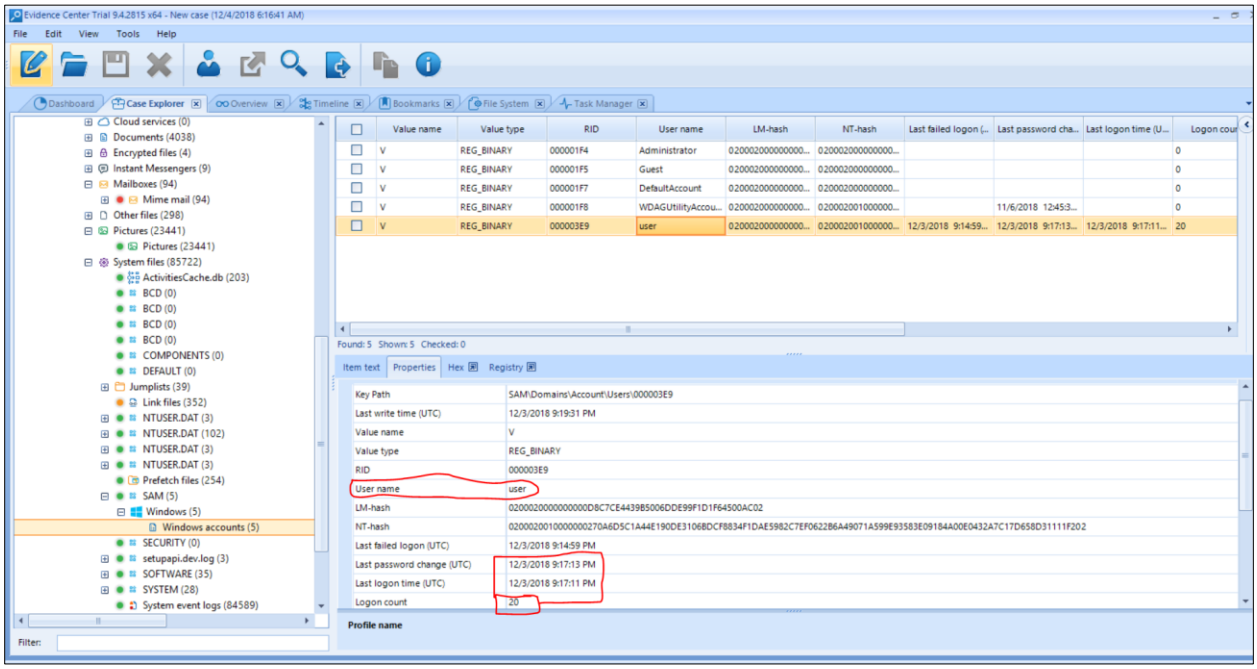


6. Who is the user of machine and find its last login time and last login date.

Using Belkasoft Evidence Center software, in case explorer tab and going into system files wherein SAM file shows the windows account. Here the most logon count is of user name as "user" who is "Gustavo Fring" as Officer hank seized the laptop device from the restaurant where he was about to meet one of his operatives.

Thus Logon count is 20.

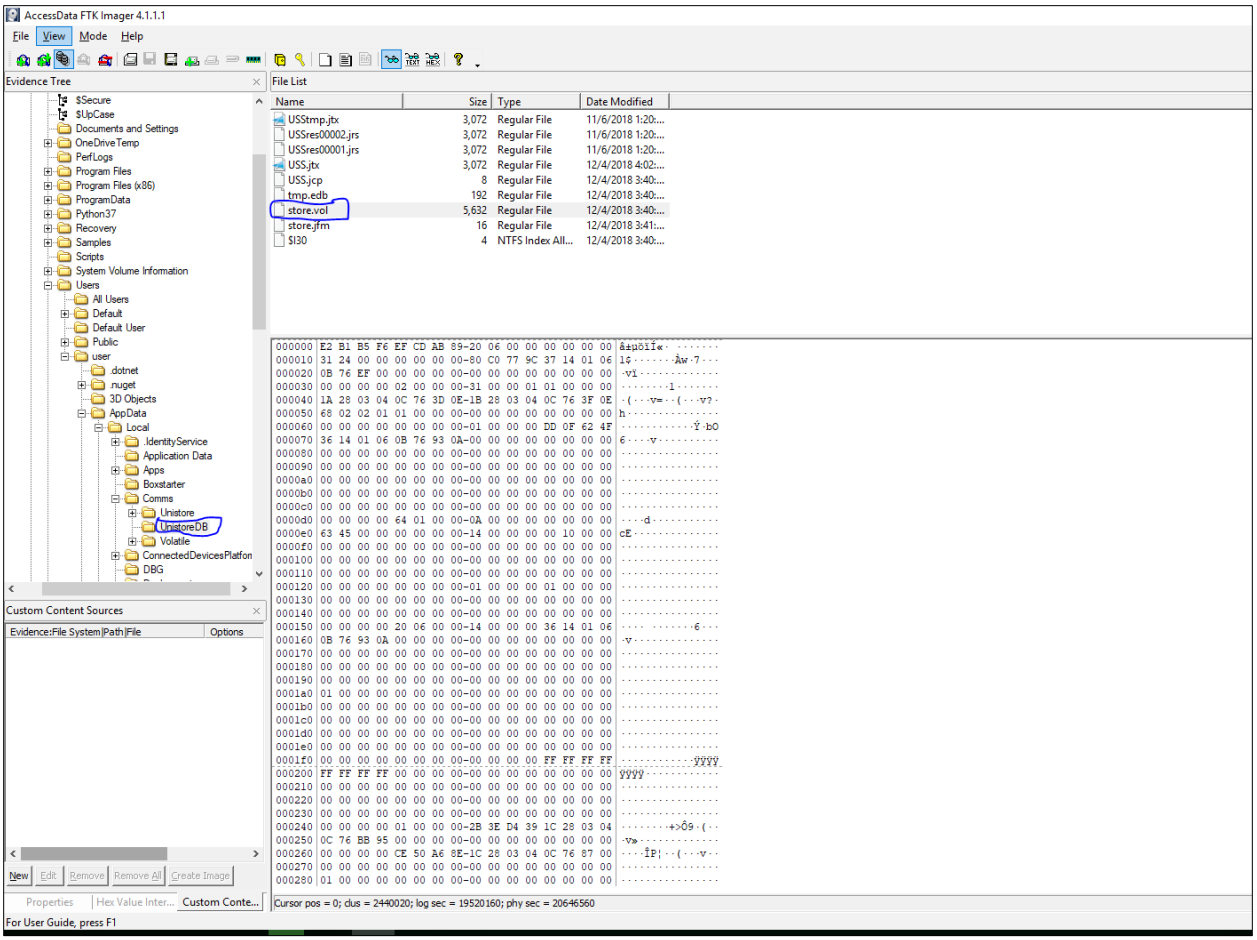
Last logon time and date: 12/3/2018 9:17:11 PM



7. Can you find out any contact/address information of the members of the Cartel?

After loading the image in FTK Imager and going into Users – user –AppData – Local – UnistoreDB

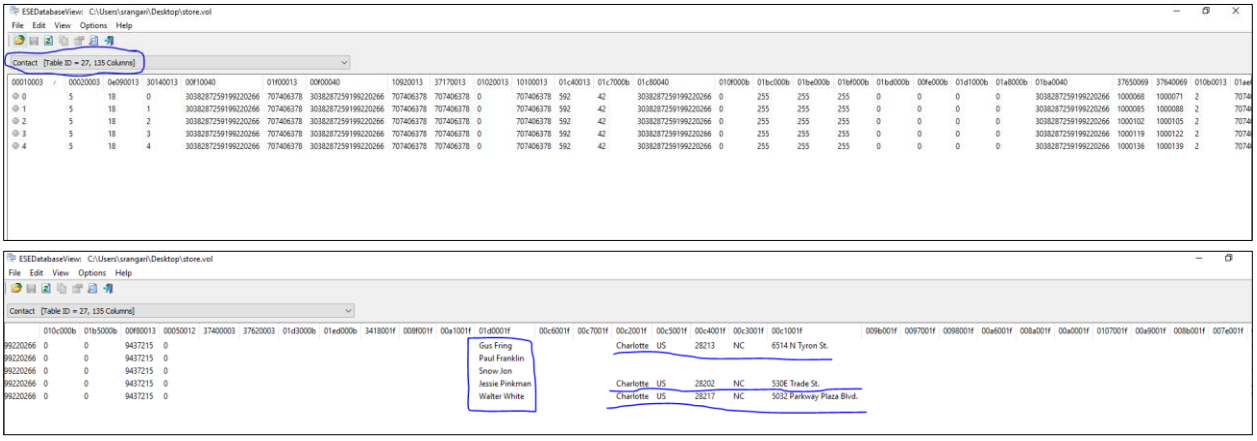
In file list I extracted store.vol as shown in below screenshot.

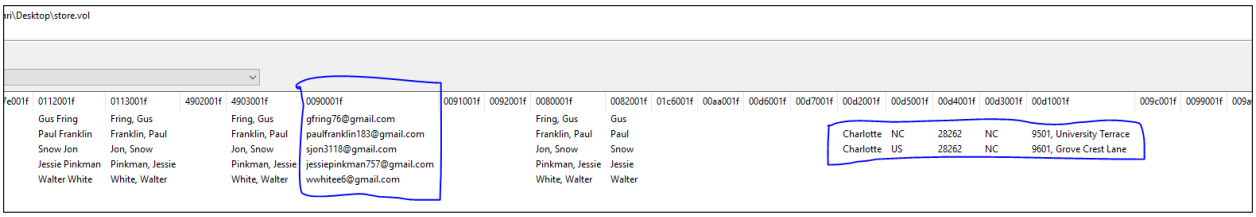


Using ESEDatabaseView and going to Contact [Table ID =27,135 Columns].

Cartel members includes Gus Fring (a leader), Jessie Pinkman (as Gang member), Walter White (as Gang member), Snow Jon (as a student) and Paul Franklin (as a student).

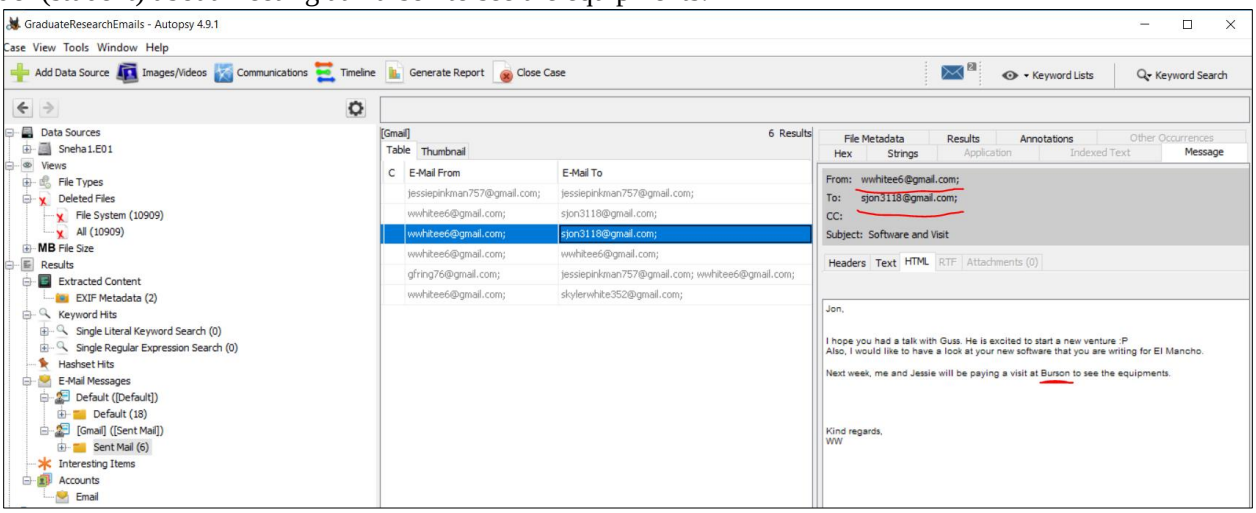
I am able to find contact/address information of the members of the Cartel as shown below.



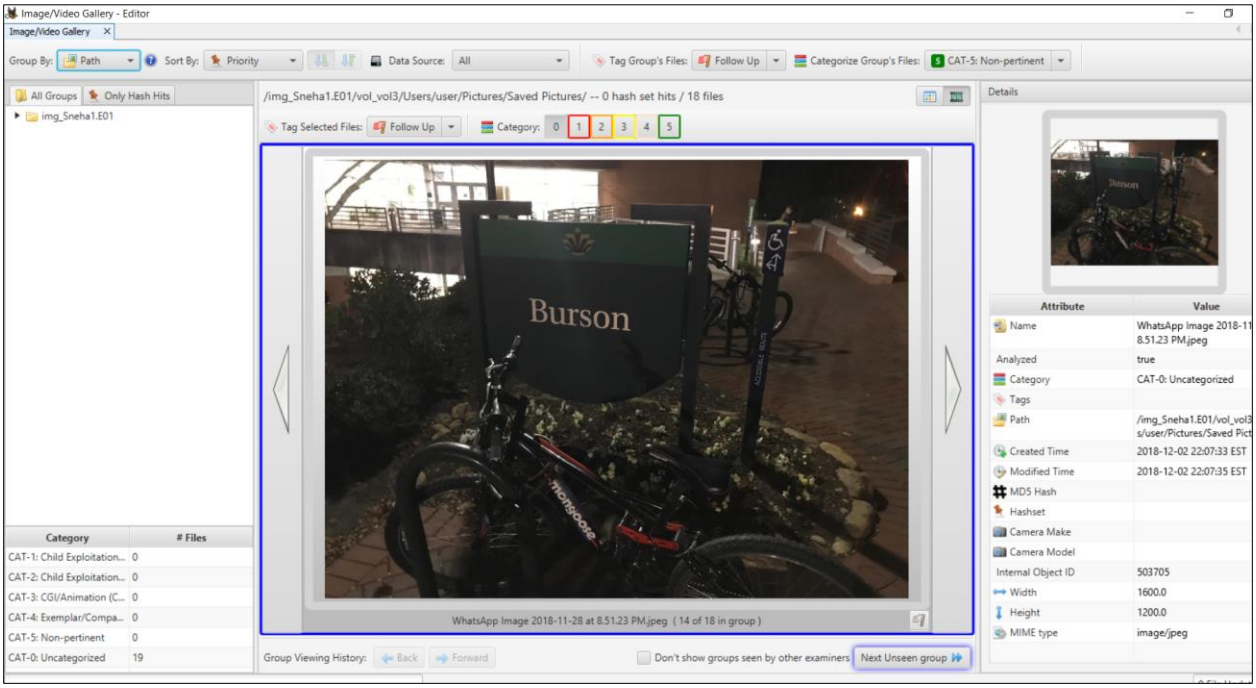


8. Can you find any picture of the meeting place which was discussed between gang leaders and student?

Using Autopsy tool and from email conversation between Walter White (gang leader) and Snow Jon(student) about meeting at Burson to see the equipments.

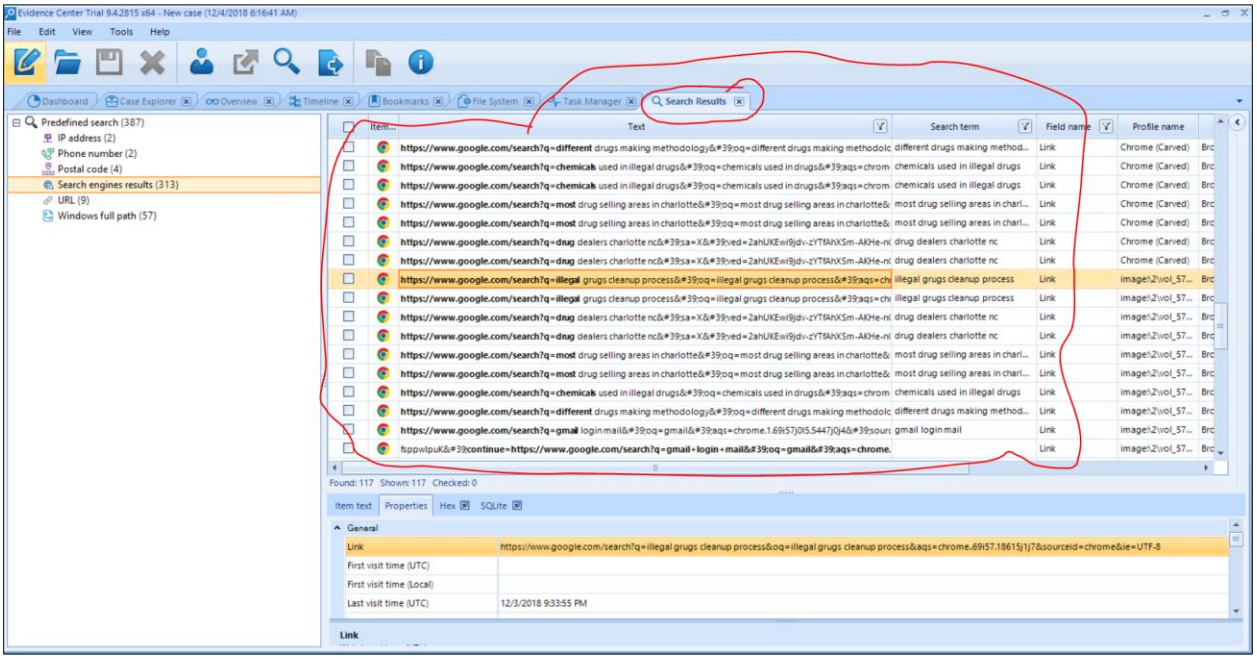


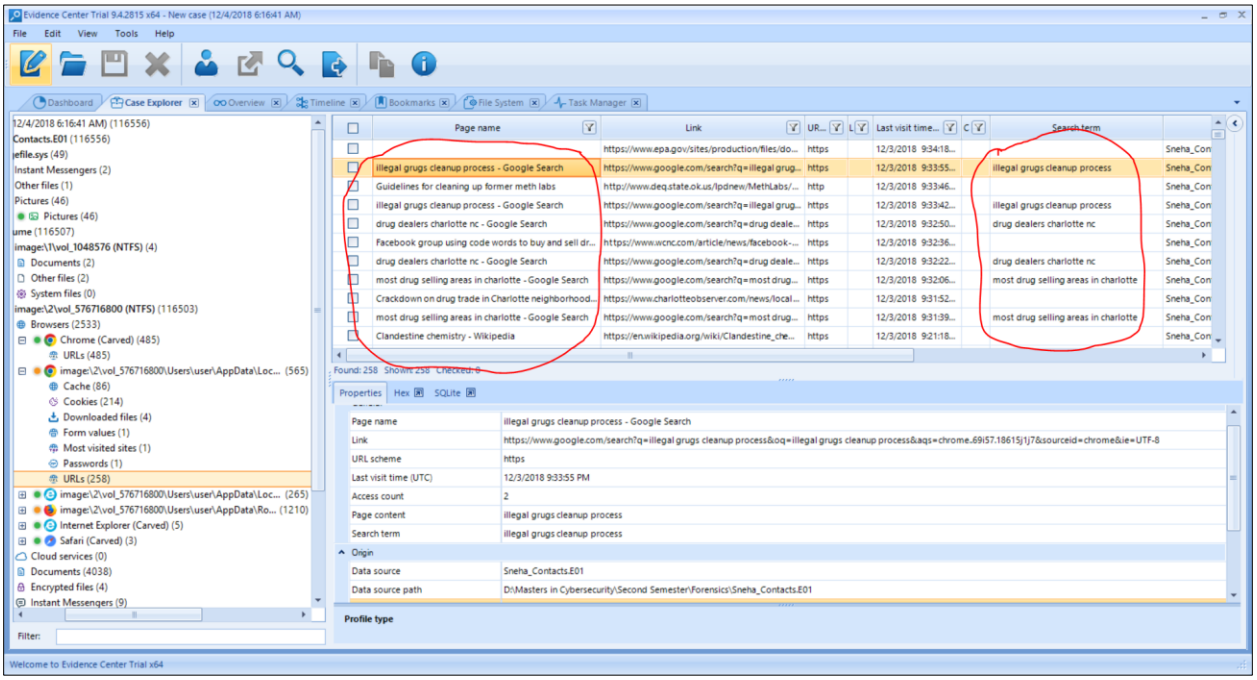
Below image shows the picture of Burson entrance.



9. Find out all the search results from the device.

Belkasoft's evidence center shows search results like place and address location showing that user has searched for some suspicious activities like illegal drugs cleanup, most drug selling areas in Charlotte, drugs making methodology, chemical used in drugs, etc.
Below screenshots show these search results from the device.





Conclusion

I examined the given image and using tools like FTK Imager, Belkasoft Evidence Center and Autopsy, I was able to find out evidence such as:

1. Email conversations between Gang leaders and students,
2. Certain photographs,
3. Passwords using PRTK tool,
4. Contact and address information along with location,
5. Attachments such as sales outcome, future plans
6. Browser history

Thus I examined the provided image and found out information relating in the image from multiple locations.