**ITIS 4250/5250**

**Lab #Graduate Research Pooja Haridasyam**

**1st May 2023**

**Overview:**

Detective Anna Garcia handed you a case and a computer belonging to the subject.

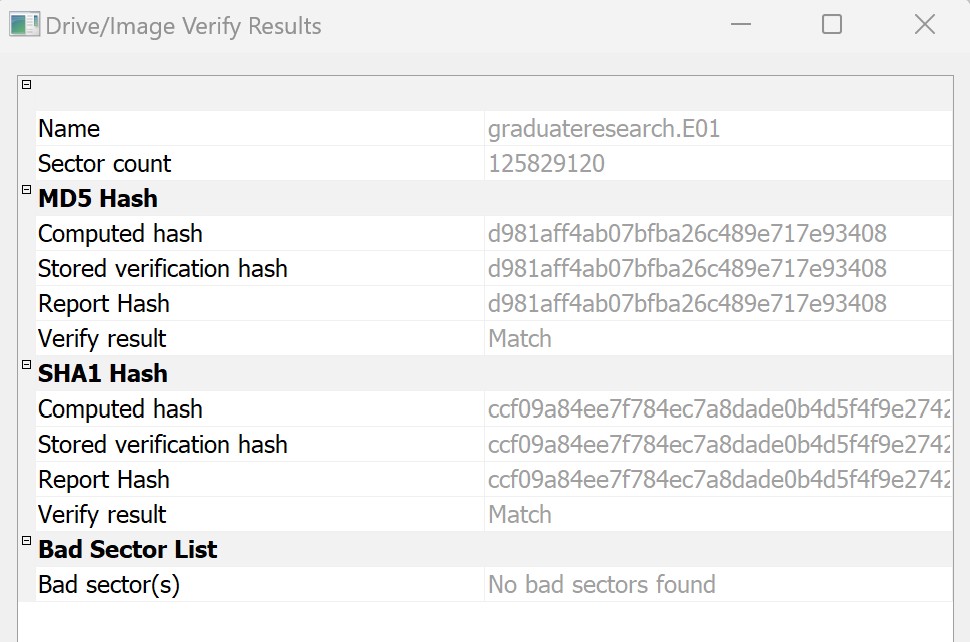
*Scenario:*

*There is an ongoing investigation regarding a series of fraudulent emails that appear to be from UPS, requesting payment for non-existent packages. Sarah Forfar received one of these emails and unknowingly opened it. The authorities suspect that the emails may be linked to an organized cybercrime group that is attempting to obtain sensitive information from unsuspecting individuals. As part of the investigation, Detective Anna Garcia visited Sarah to gather more information about the email and examine the computer for any potential security breaches.*

*Detective Anna seizes her computer for further investigation and warns her to be cautious of similar scams in the future.*

**Forensic Acquisition & Exam Preparation**

Use AccessDataFTKImager to load the image named graduateresearch.E01 and confirm its validity



*Figure: Verified Hash value*

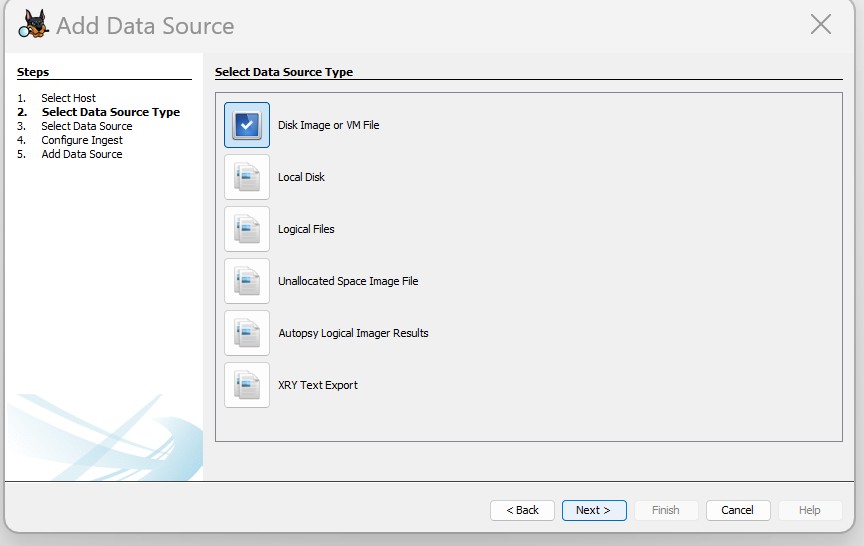
Verified Hash value: d981aff4ab07bfba26c489e717e93408

**Software used for examination of the task:**

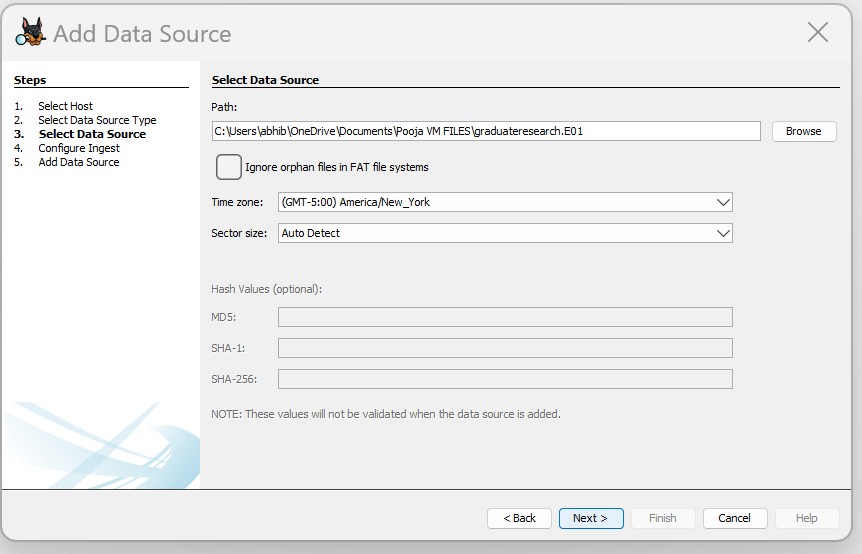
1. AccessData FTK Imager version 3.1.2.0 for 64-bit systems
2. Autopsy version 4.20.0 for 64-bit systems
3. An ASUSTek laptop running the Windows 11 operating system, AMD Ryzen 9 6900HS Processor with Radeon Graphics, 16GB RAM.
4. Win Prefetch Viewer v1.37 for 64-bit systems
5. Arsenal Image Mounter version 3.9.228
6. Access Data Registry Viewer version 2.0.0
7. Gephi 0.10.1
8. Wireshark 4.0.5
9. Microsoft Event Viewer

**Forensic Analysis:**

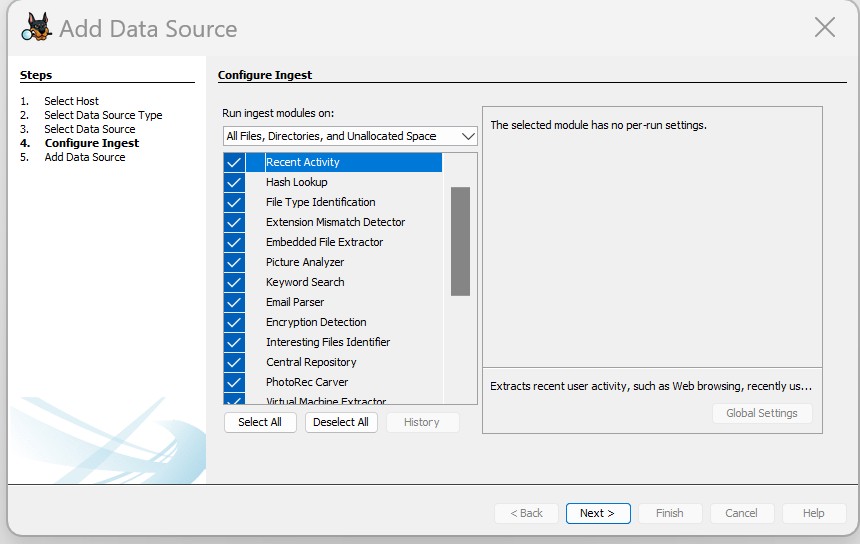
Launch Autopsy, then generate a new case and incorporate the graduateresearch.E01 file as the data source.



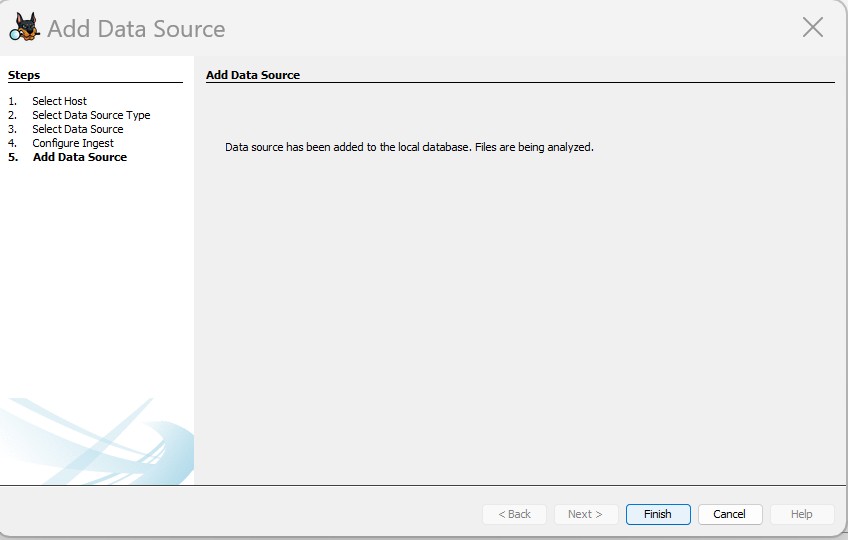
*Figure: Selecting datasource type*



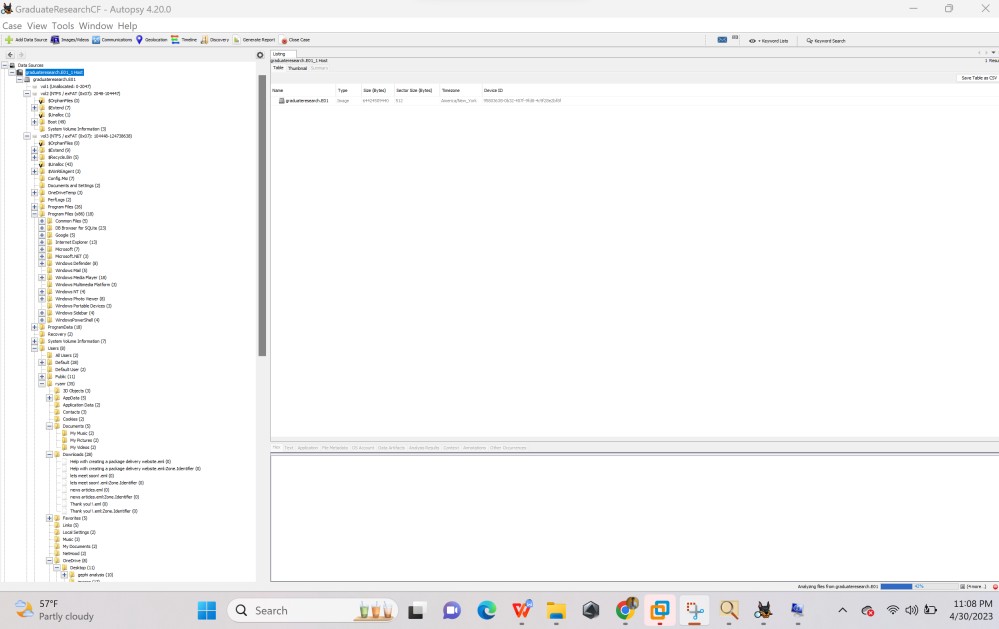
*Figure: Case information*



*Figure: Selecting the ingest modules*



*Figure: Adding data source*

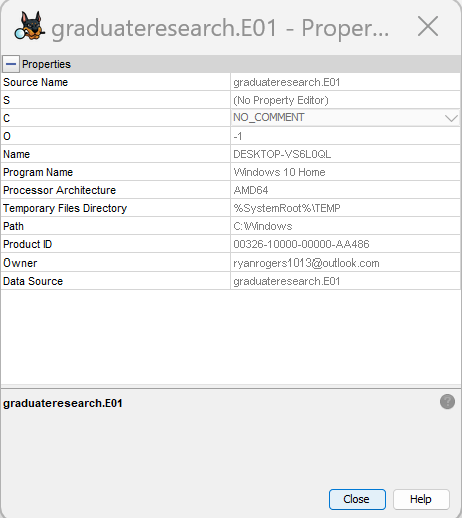


*Figure: Data sources*

By utilizing the previously mentioned tools, Autopsy and Registry Explorer, we can discover solutions to the following inquiries and carry out the analysis:

1. What was the name of the owner and the computer?

The information can be located under Data Artifacts -> Operating System Information -> SYSTEM -> Owner.

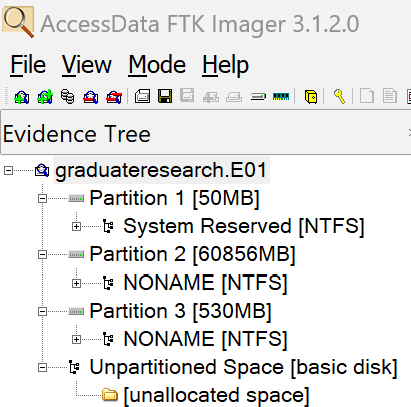


*Figure: Name of the computer*

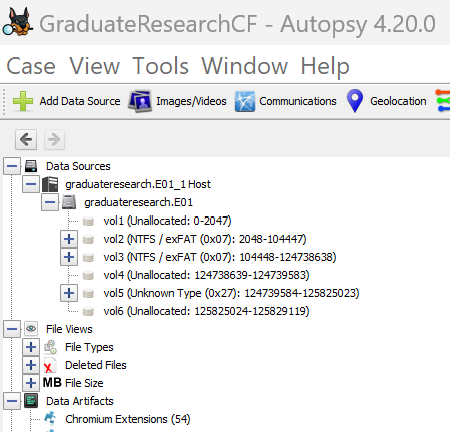
From the above picture we can say that the owner of the computer is Ryan Rogers.

1. Provide an explanation of how the entire hard drive space was utilized on the computer, including partitions and the amount of space that was used and free.

**In FTKImager** shows a total of **four partitions**, including an **Unpartitioned space** on the basic disk, **System Reserved Partition** of 1-50 MB, **Partition 2** with 60856 MB, and **Partition 3** with 530 MB



*Figure: Disk Partition in FTKimager*



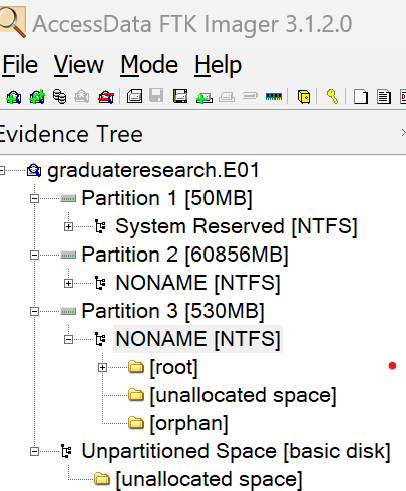
*Figure: Disk partition in Autopsy*

In Autopsy, we can see 6 Partitions

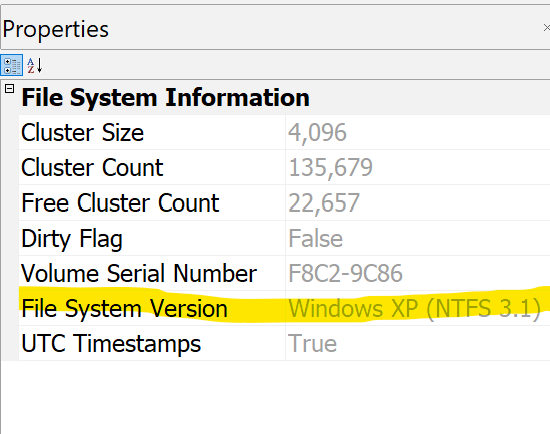
* + **Vol1(Unallocated)**
  + **Vol2(NTFS)**
  + **Vol3(NTFS)**
  + **Vol4(Unallocated)**
  + **Vol5(Unknown)**
  + **Vol6(Unallocated)**

1. Determine which file system is being utilized?

According to the properties tab in FTKImager, it was determined that the NTFS file system was being utilized on the subject's computer.



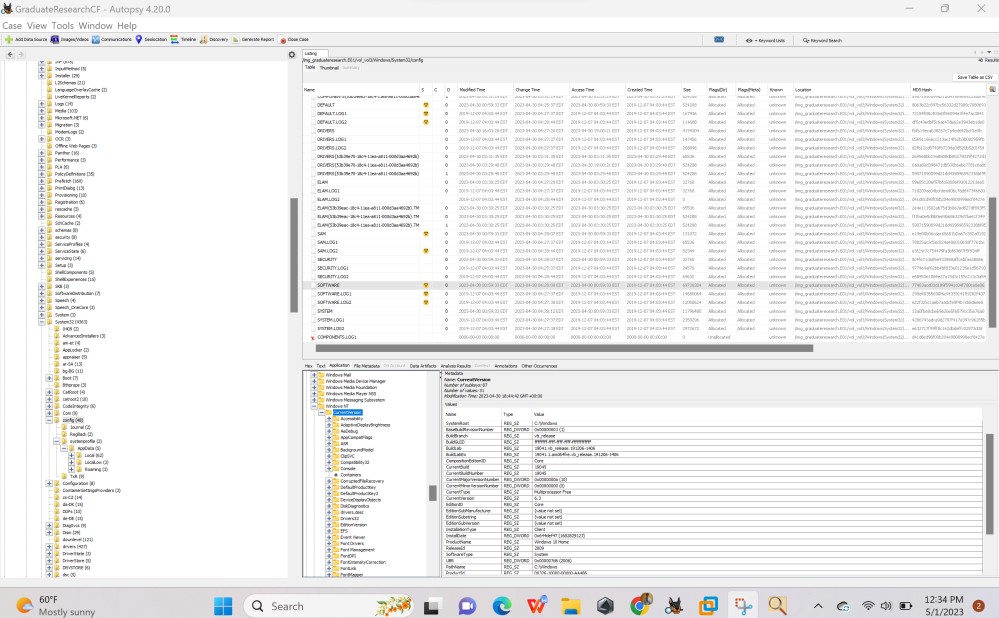
*Figure: Disk Partition in FTK imager*



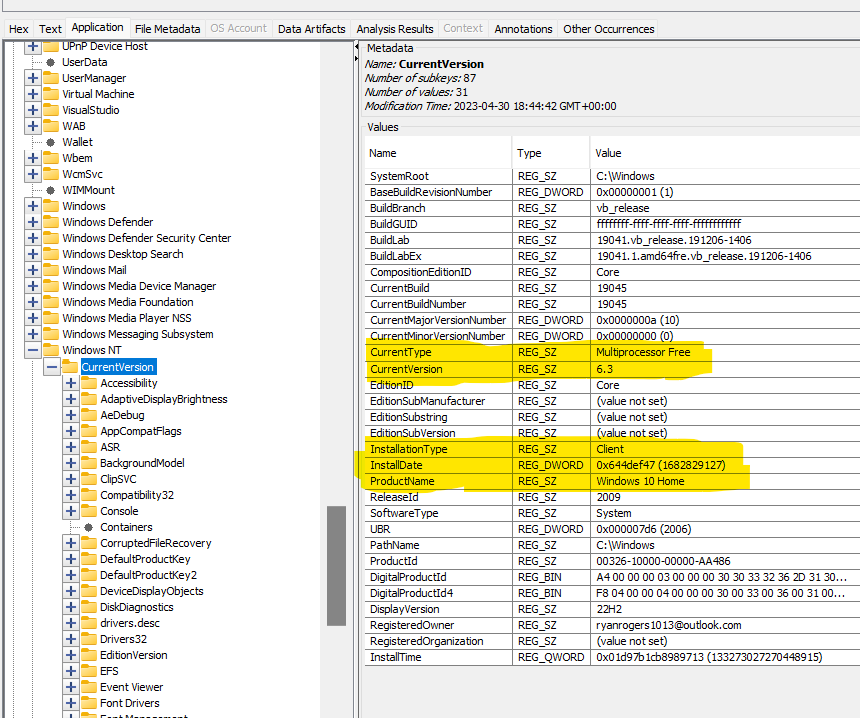
The NTFS file system was utilized on the computer in question, as per the details retrieved from the Properties tab in FTKImager.

1. Determine the operating system's version?

From the mentioned path we can confirm that the version of the windows OS is 6.3 . aduateresearch.E01 -> vol\_vol3 -> windows -> System32 -> Config



*Figure: System Configuration*

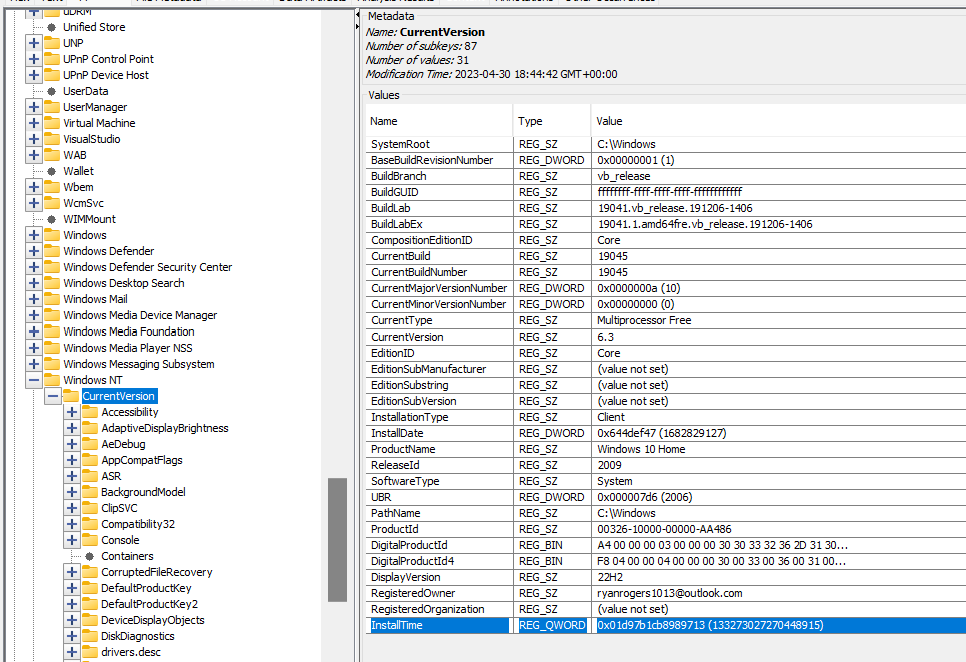


*Figure: Current version and type*

1. Locate the installation date of the operating system?

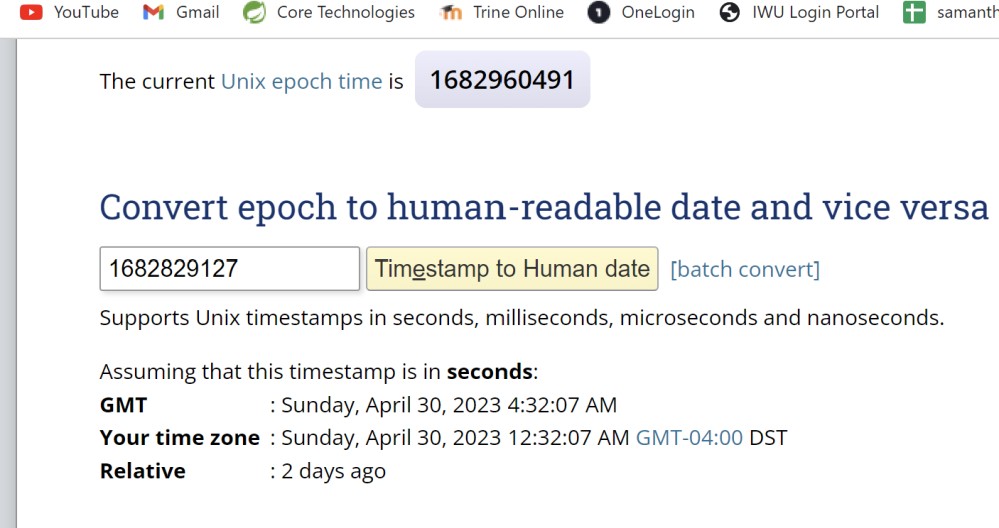
The OS was installed on Sunday, April 30, 2023 4:32:07 AM.

Go to graduateresearch.E01 -> vol\_vol3 -> windows -> System32 -> Config.



*Figure: Install date and time*

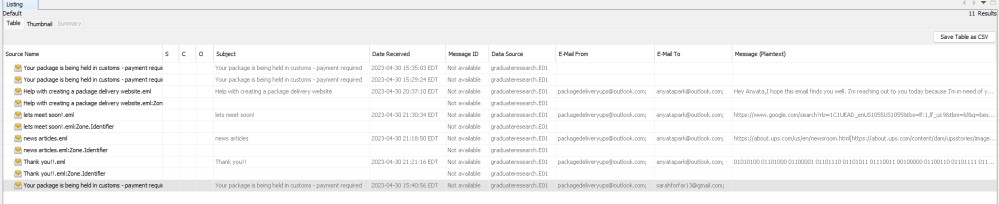
We can convert the installation date from epoch format to a human-readable format using an online converter.



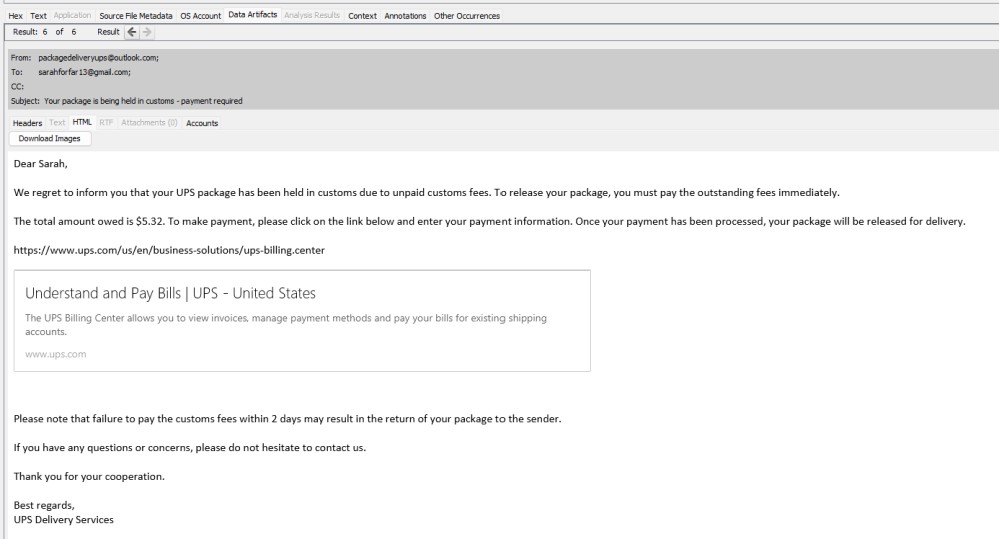
*Figure: Epoch to human readable converter*

1. Identify the email conversations related to the mentioned crime scene and provide the email addresses of the correspondents involved.

Go to Data Artifacts -> Email messages -> Default -> Default. From the mentioned path we can find the email conversations.



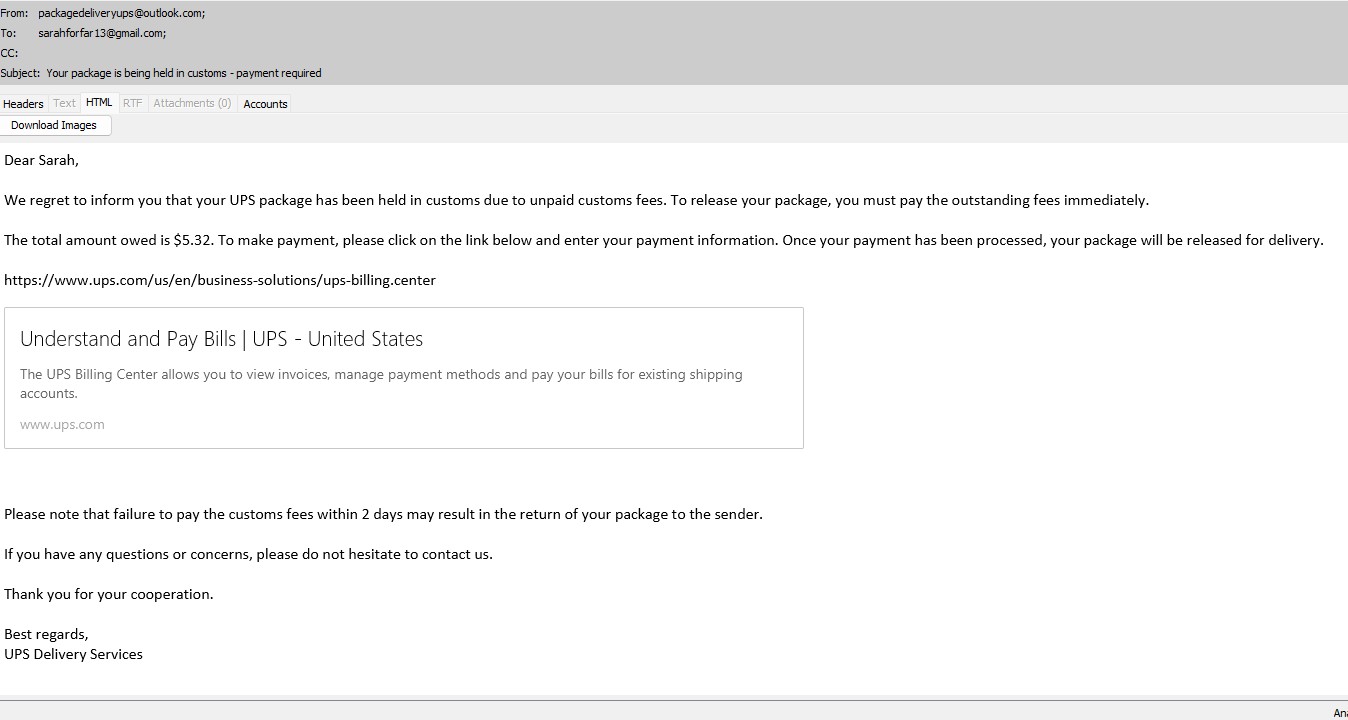
*Figure: email*



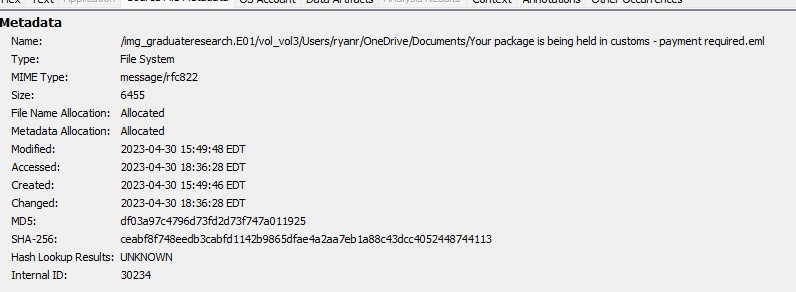
*Figure: Email header*

From the above picture we can see that the domain of the mail is outlook, and the mail id seems to be phony. The email correspondents include [packagedeliveryups@outlook.com,](mailto:packagedeliveryups@outlook.com) [sarahforfar@outlook.com](mailto:sarahtaylor@outlook.com)

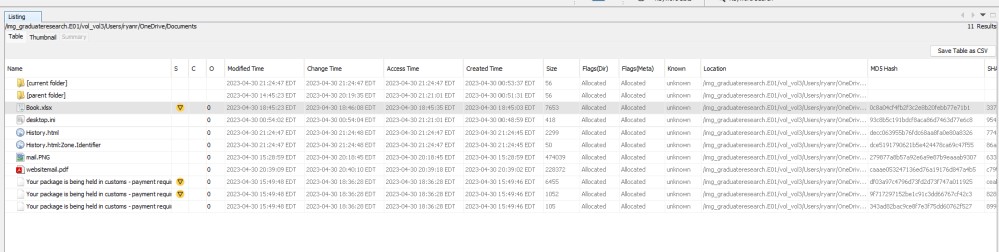
1. What are the contents of the phishing email?



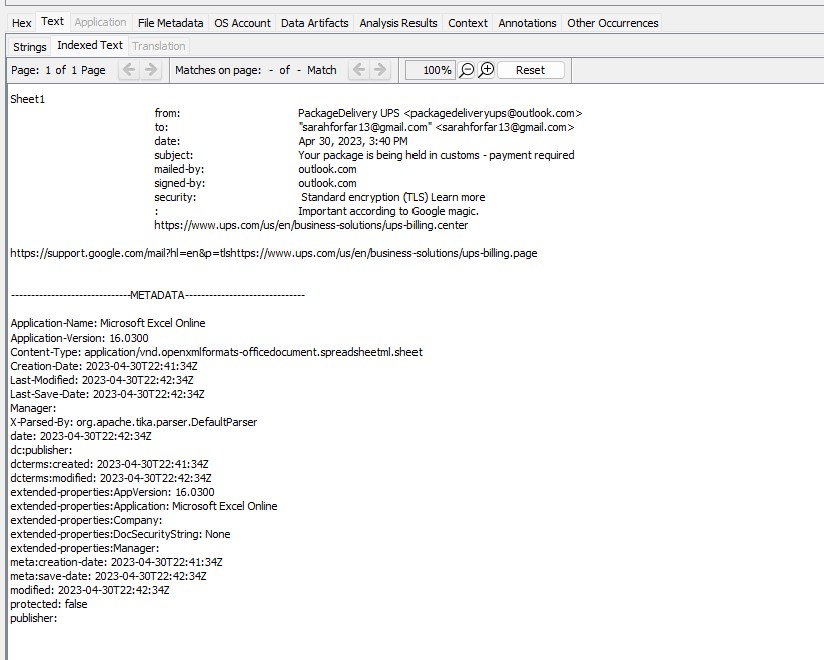
*Figure: Contents of email*



We can find that contents of email are stored in an Excel sheet in the following path. Got o Graduateresearch.E01 -> vol\_vol3 -> Users -> ryanr -> OneDrive -> Documents



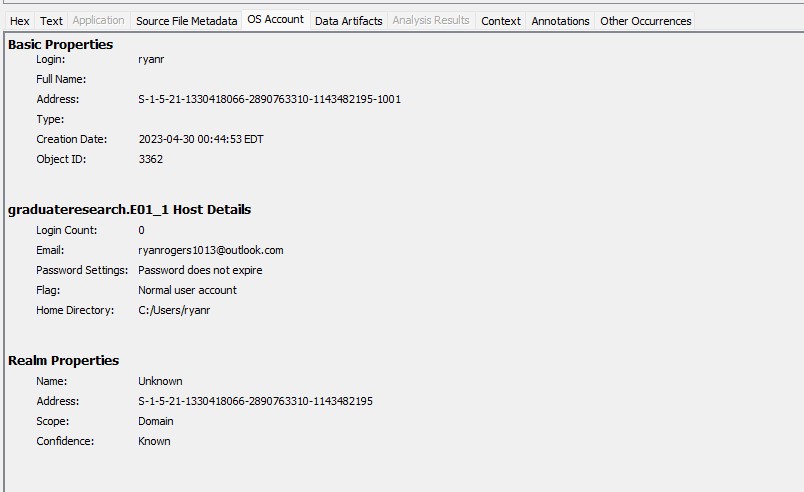
*Figure: Contents of email stored in Excel Sheet*



*Figure: Contents of Email*

1. What is the account used for the operating system?"

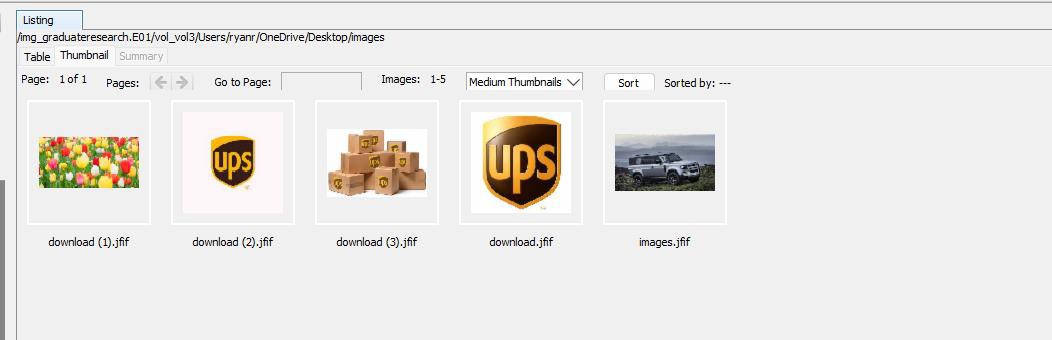
Goto Datta Artifacts -> Operating System information -> Right click and Properties.



*Figure: OS account information.*

1. Is there any stored media on the computer that could be used to impersonate UPS?

Go to graduateresearch.E01->vol\_vol3->Onedrive->Users->images. We can find the logos of UPS and images related to packages.



*Figure: Images stored on the computer*



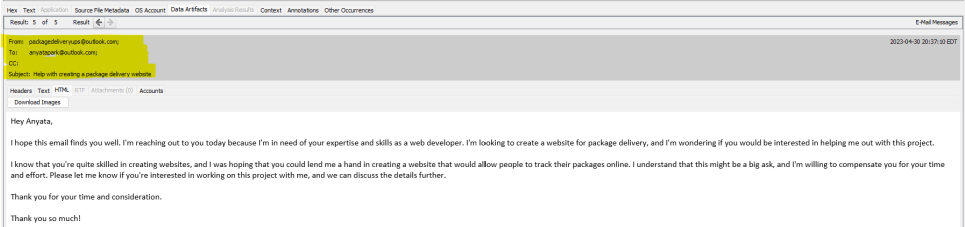
*Figure: UPS logo*



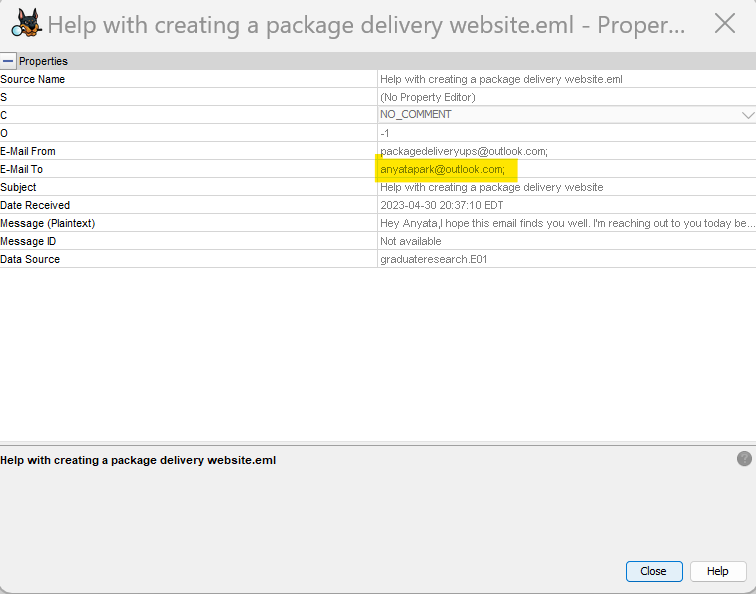
*Figure: UPS package image*

1. Identify if there is any evidence of the involvement of other individuals in the criminal activity, in addition to the suspect.

From the following emails, it appears that Ryan Rogers is associated with someone named Anyata Park, whose email address is [anyatapark@outlook.com](mailto:anyatapark@outlook.com).



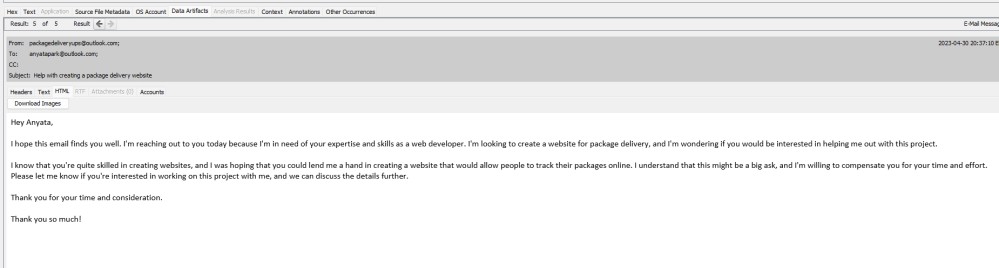
*Figure: Email Conversations*



*Figure: Associated person’s email address*

1. Provide any documented conversations involving the subject and their associates?

Go to Data Artifacts -> Email messages -> Default -> Default.



*Figure: Email Communications*

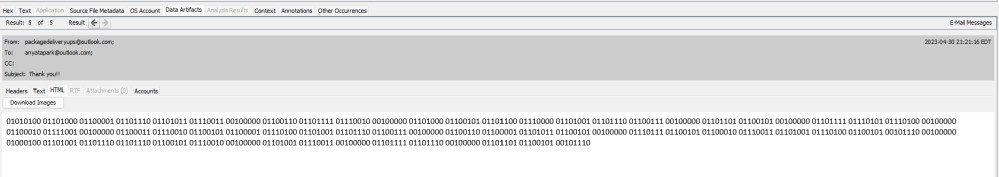


*Figure: Email Communications*

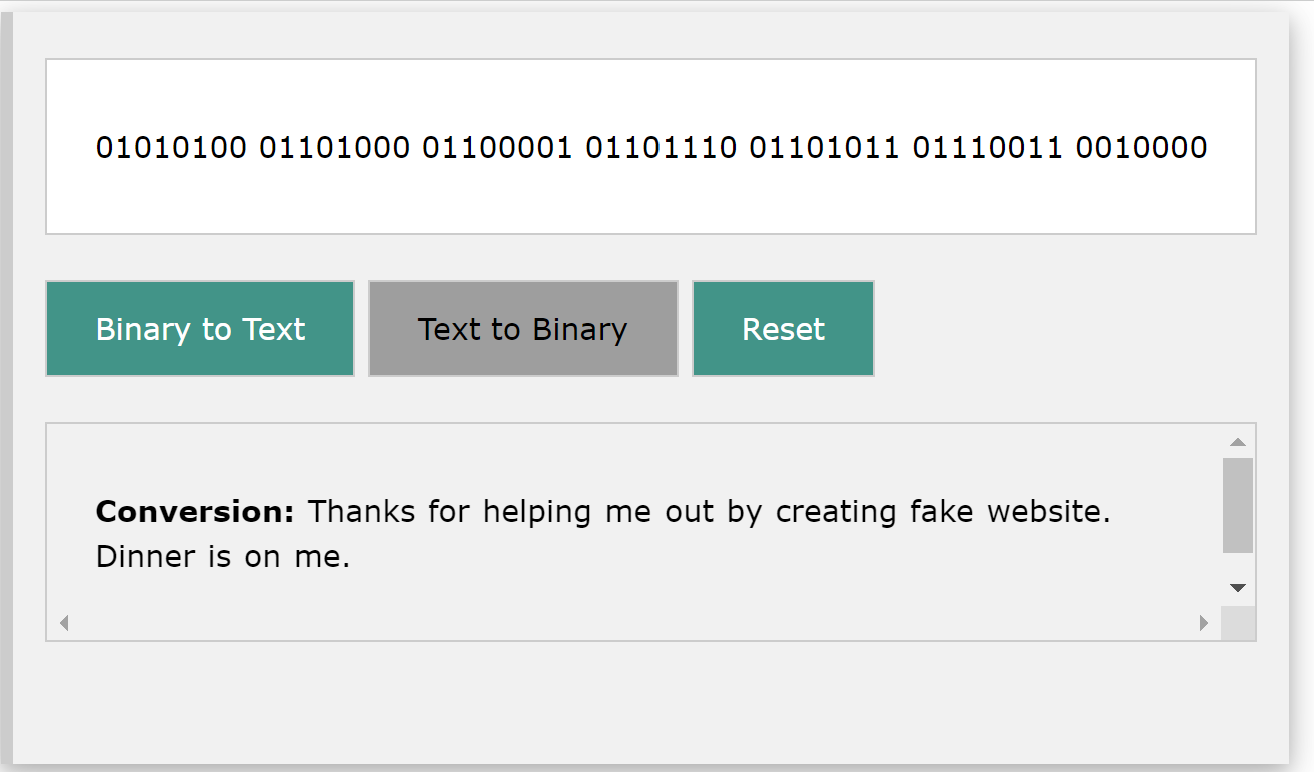
From the above images we can confirm that Ryan is communicating with Anyata in emails seeking help for creating a fake website.

1. Is any language or code mentioned in the communication be considered as evidence?

Go to Data Artifacts -> Email messages -> Default -> Default. We can find an email from [ryanrogers1013@outlook.com](mailto:ryanrogers1013@outlook.com) to [anyatapark@outlook.com](mailto:anyatapark@outlook.com) which is in binary code.



*Figure: Message sent in Binary format*

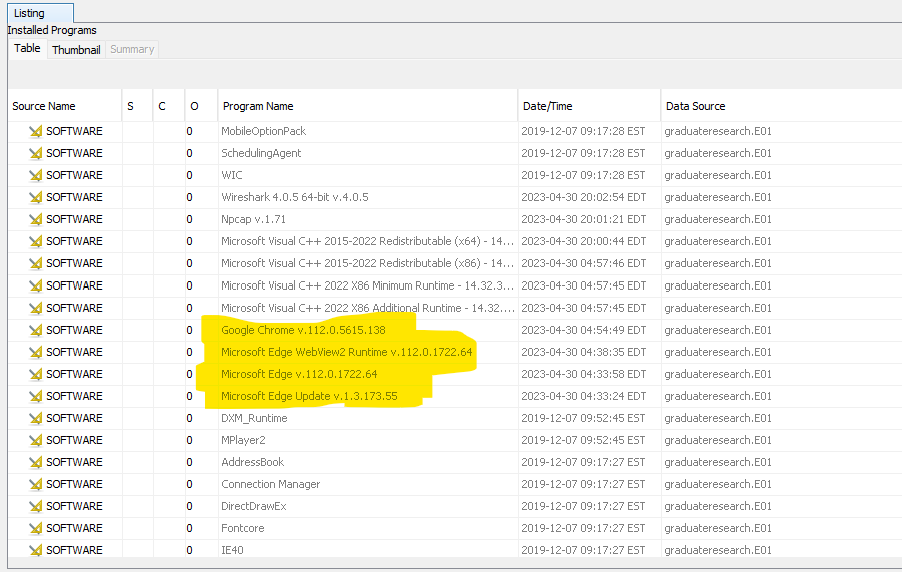


*Figure: Converting Binary to Text*

From the above pictures we can see that Ryan has attempted to use the binary format, after converting binary to text the message says “Thanks for helping me out by creating fake website. Dinner is on me.”

1. Identify applications used to download files from the internet.

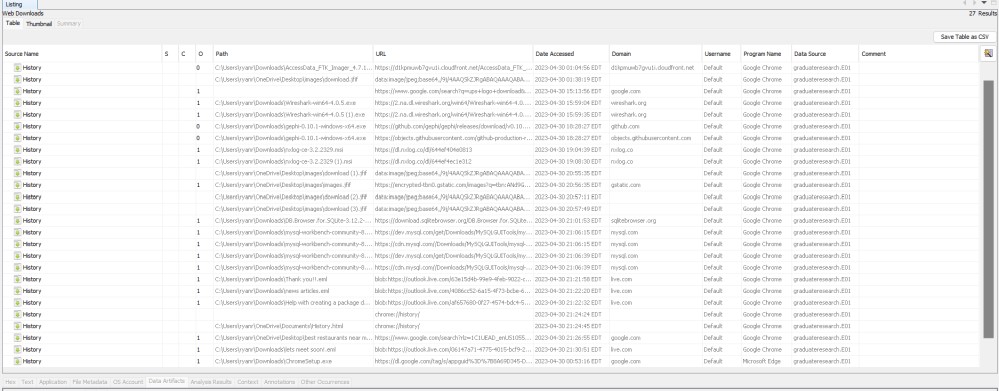
Go to Data Artifacts -> Installed Programs. From the below image we can confirm that “Google Chrome” and “Microsoft Edge” is used to download softwares.



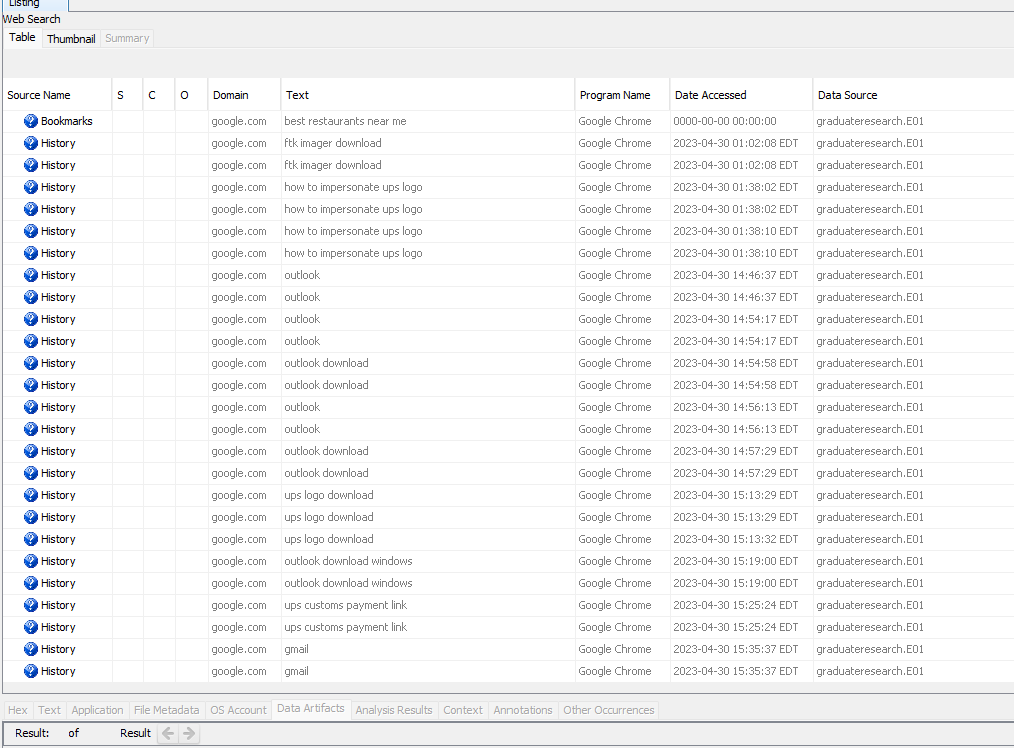
*Figure: Applications used to download software*

1. Is there any software installed on the computer that can be considered as evidence?"?

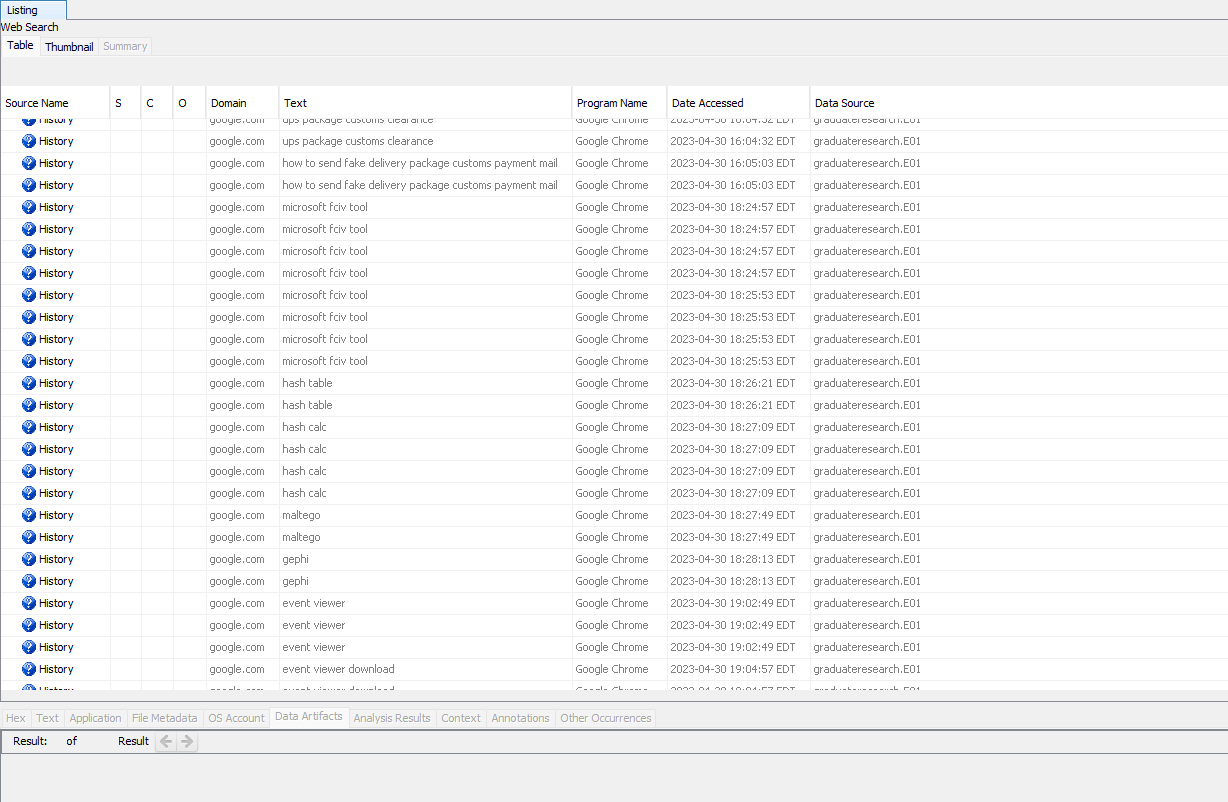
Goto Data Artifacts -> Web Downloads. We can see few softwares were installed on the computer.



*Figure: Software's installed*



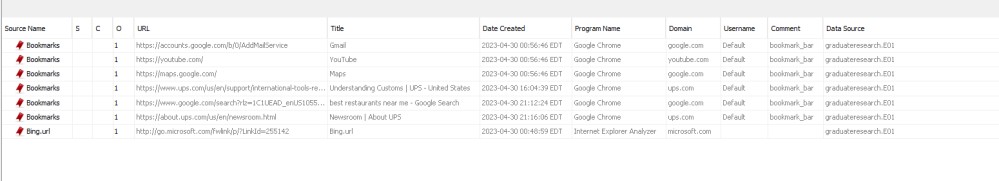
*Figure: Web History*



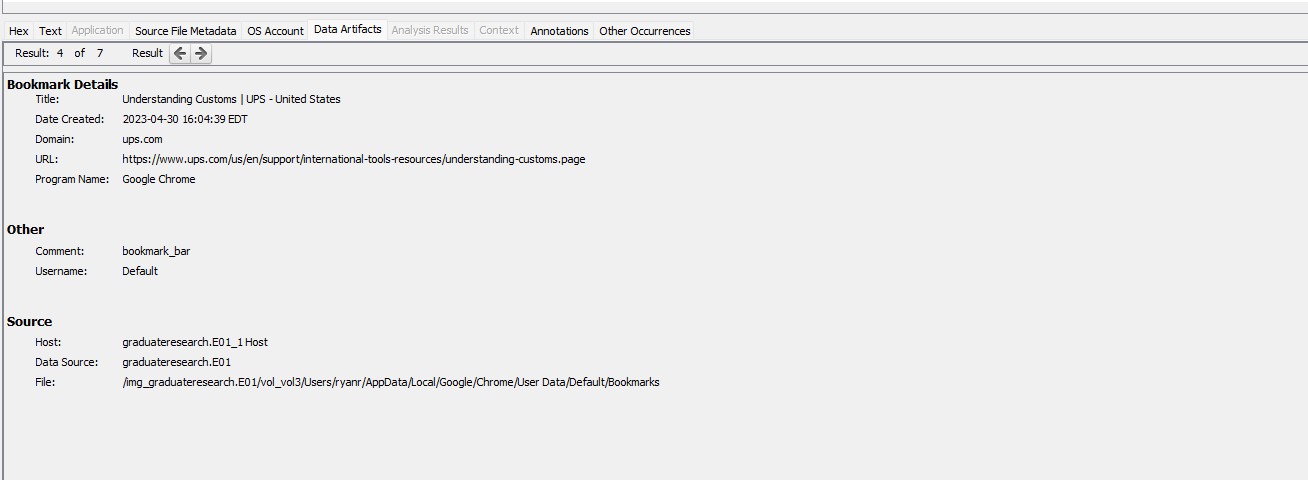
*Figure: web search of Ryan*

From history we can confirm that the attacker has installed few softwares and tried to search for the other software's.

1. Are there any bookmarks saved on the computer which can be useful for the analysis?



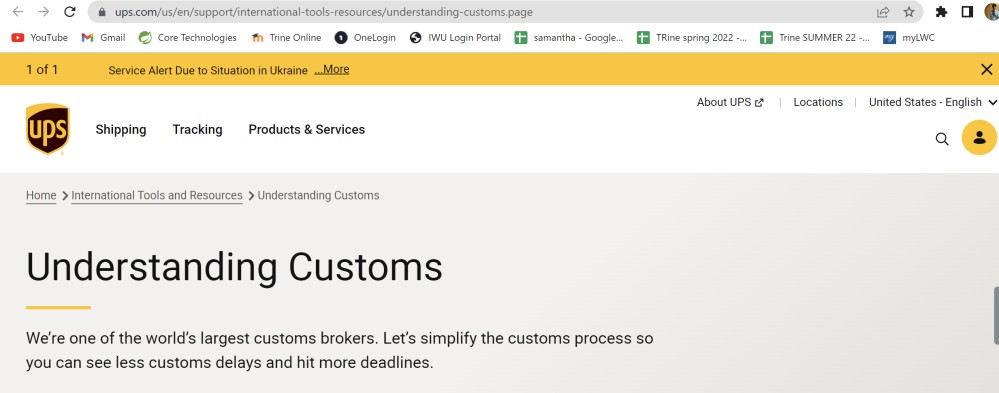
*Figure: Bookmarks on the computer*



*Figure: Bookmark of UPS official website.*

<https://www.ups.com/us/en/support/international-tools-resources/understanding-customs.page>

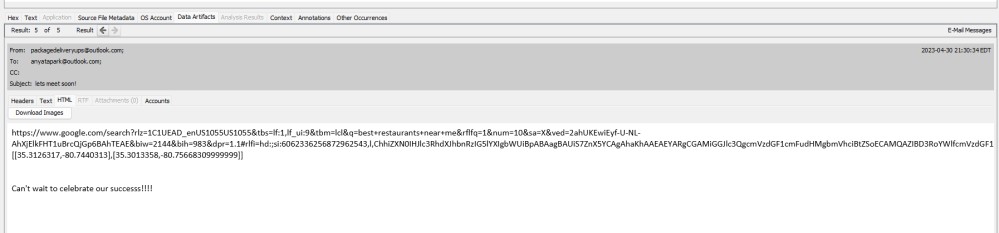
After confirming the link, it was discovered that the URL saved in the bookmarks belongs to the legitimate website for making customs payments for UPS.



*Figure: Official website of UPS Customs.*

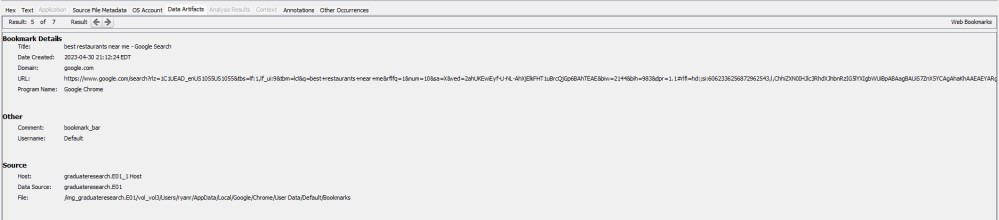
1. Is there any geolocation mentioned in any communication or on computer to confirm the address?

Goto Data Artifacts -> Email messages -> Default -> Default. An email has been found that contains a Google Maps location link showing the best restaurants near the sender's location. The email was sent to [anyatapark@outlook.com](mailto:anyatapark@outlook.com) .



*Figure: The email includes a link to a Google Maps location.*

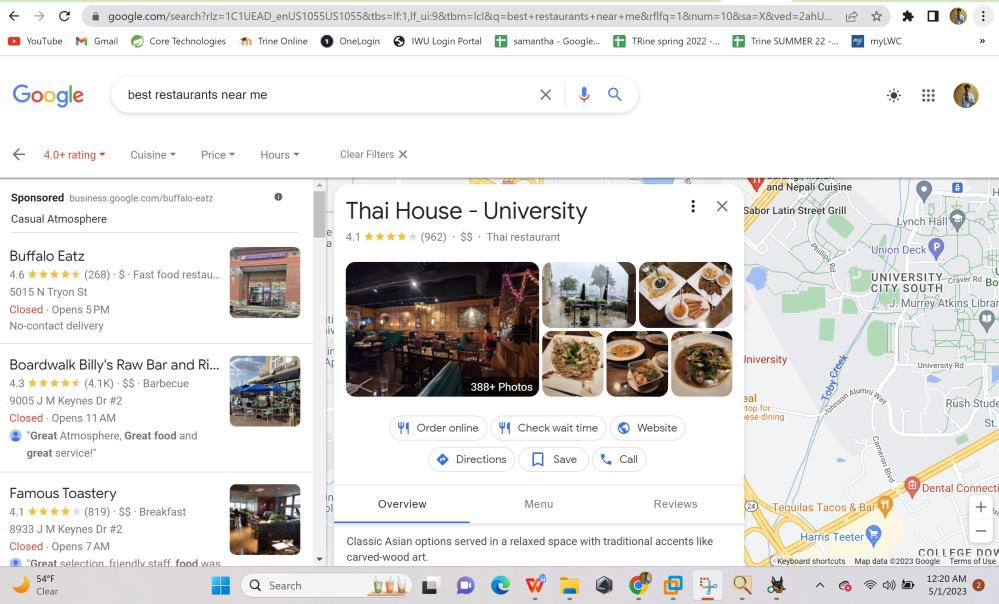
Furthermore, it can be observed that the Google Maps location link is saved as a bookmark.



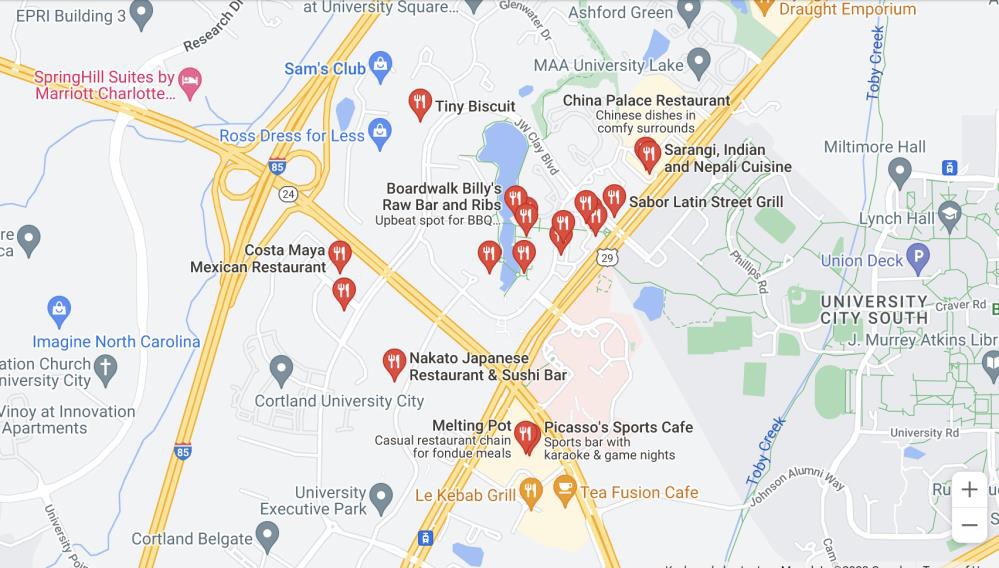
*Figure: Bookmark of google maps URL*

[https://www.google.com/search?rlz=1C1UEAD\_enUS1055US1055&tbs=lf:1,lf\_ui:9&tbm=lcl&](https://www.google.com/search?rlz=1C1UEAD_enUS1055US1055&tbs=lf%3A1%2Clf_ui%3A9&tbm=lcl&q=best%2Brestaurants%2Bnear%2Bme&rflfq=1&num=10&sa=X&ved=2ahUKEwiEyf-U-NL-AhXjElkFHT1uBrcQjGp6BAhTEAE&biw=2144&bih=983&dpr=1.1&rlfi=hd%3A%3Bsi%3A6062336256872962543%2Cl%2CChhiZXN0IHJlc3RhdXJhbnRzIG5lYXIgbWUiBpABAagBAUiS7ZnX5YCAgAhaKhAAEAEYARgCGAMiGGJlc3QgcmVzdGF1cmFudHMgbmVhciBtZSoECAMQAZIBD3RoYWlfcmVzdGF1cmFudJoBI0NoWkRTVWhOTUc5blMwVkpRMEZuU1VReWMyUnhOMUZCRUFFqgFWEAEqFCIQYmVzdCByZXN0YXVyYW50cygAMh4QASIawhQE_SE_DODINQoc__KDkSVGxkLE8zpKc0cyHBACIhhiZXN0IHJlc3RhdXJhbnRzIG5lYXIgbWXgAQA%2Cy%2CVi0zLJDWONw%3Bmv%3A%5B%5B35.3126317%2C-80.7440313%5D%2C%5B35.3013358%2C-80.75668309999999) [q=best+restaurants+near+me&rflfq=1&num=10&sa=X&ved=2ahUKEwiEyf-U-NL-](https://www.google.com/search?rlz=1C1UEAD_enUS1055US1055&tbs=lf%3A1%2Clf_ui%3A9&tbm=lcl&q=best%2Brestaurants%2Bnear%2Bme&rflfq=1&num=10&sa=X&ved=2ahUKEwiEyf-U-NL-AhXjElkFHT1uBrcQjGp6BAhTEAE&biw=2144&bih=983&dpr=1.1&rlfi=hd%3A%3Bsi%3A6062336256872962543%2Cl%2CChhiZXN0IHJlc3RhdXJhbnRzIG5lYXIgbWUiBpABAagBAUiS7ZnX5YCAgAhaKhAAEAEYARgCGAMiGGJlc3QgcmVzdGF1cmFudHMgbmVhciBtZSoECAMQAZIBD3RoYWlfcmVzdGF1cmFudJoBI0NoWkRTVWhOTUc5blMwVkpRMEZuU1VReWMyUnhOMUZCRUFFqgFWEAEqFCIQYmVzdCByZXN0YXVyYW50cygAMh4QASIawhQE_SE_DODINQoc__KDkSVGxkLE8zpKc0cyHBACIhhiZXN0IHJlc3RhdXJhbnRzIG5lYXIgbWXgAQA%2Cy%2CVi0zLJDWONw%3Bmv%3A%5B%5B35.3126317%2C-80.7440313%5D%2C%5B35.3013358%2C-80.75668309999999) [AhXjElkFHT1uBrcQjGp6BAhTEAE&biw=2144&bih=983&dpr=1.1#rlfi=hd:;si:606233625687](https://www.google.com/search?rlz=1C1UEAD_enUS1055US1055&tbs=lf%3A1%2Clf_ui%3A9&tbm=lcl&q=best%2Brestaurants%2Bnear%2Bme&rflfq=1&num=10&sa=X&ved=2ahUKEwiEyf-U-NL-AhXjElkFHT1uBrcQjGp6BAhTEAE&biw=2144&bih=983&dpr=1.1&rlfi=hd%3A%3Bsi%3A6062336256872962543%2Cl%2CChhiZXN0IHJlc3RhdXJhbnRzIG5lYXIgbWUiBpABAagBAUiS7ZnX5YCAgAhaKhAAEAEYARgCGAMiGGJlc3QgcmVzdGF1cmFudHMgbmVhciBtZSoECAMQAZIBD3RoYWlfcmVzdGF1cmFudJoBI0NoWkRTVWhOTUc5blMwVkpRMEZuU1VReWMyUnhOMUZCRUFFqgFWEAEqFCIQYmVzdCByZXN0YXVyYW50cygAMh4QASIawhQE_SE_DODINQoc__KDkSVGxkLE8zpKc0cyHBACIhhiZXN0IHJlc3RhdXJhbnRzIG5lYXIgbWXgAQA%2Cy%2CVi0zLJDWONw%3Bmv%3A%5B%5B35.3126317%2C-80.7440313%5D%2C%5B35.3013358%2C-80.75668309999999) [2962543,l,ChhiZXN0IHJlc3RhdXJhbnRzIG5lYXIgbWUiBpABAagBAUiS7ZnX5YCAgAhaKh](https://www.google.com/search?rlz=1C1UEAD_enUS1055US1055&tbs=lf%3A1%2Clf_ui%3A9&tbm=lcl&q=best%2Brestaurants%2Bnear%2Bme&rflfq=1&num=10&sa=X&ved=2ahUKEwiEyf-U-NL-AhXjElkFHT1uBrcQjGp6BAhTEAE&biw=2144&bih=983&dpr=1.1&rlfi=hd%3A%3Bsi%3A6062336256872962543%2Cl%2CChhiZXN0IHJlc3RhdXJhbnRzIG5lYXIgbWUiBpABAagBAUiS7ZnX5YCAgAhaKhAAEAEYARgCGAMiGGJlc3QgcmVzdGF1cmFudHMgbmVhciBtZSoECAMQAZIBD3RoYWlfcmVzdGF1cmFudJoBI0NoWkRTVWhOTUc5blMwVkpRMEZuU1VReWMyUnhOMUZCRUFFqgFWEAEqFCIQYmVzdCByZXN0YXVyYW50cygAMh4QASIawhQE_SE_DODINQoc__KDkSVGxkLE8zpKc0cyHBACIhhiZXN0IHJlc3RhdXJhbnRzIG5lYXIgbWXgAQA%2Cy%2CVi0zLJDWONw%3Bmv%3A%5B%5B35.3126317%2C-80.7440313%5D%2C%5B35.3013358%2C-80.75668309999999) [AAEAEYARgCGAMiGGJlc3QgcmVzdGF1cmFudHMgbmVhciBtZSoECAMQAZIBD3RoYW](https://www.google.com/search?rlz=1C1UEAD_enUS1055US1055&tbs=lf%3A1%2Clf_ui%3A9&tbm=lcl&q=best%2Brestaurants%2Bnear%2Bme&rflfq=1&num=10&sa=X&ved=2ahUKEwiEyf-U-NL-AhXjElkFHT1uBrcQjGp6BAhTEAE&biw=2144&bih=983&dpr=1.1&rlfi=hd%3A%3Bsi%3A6062336256872962543%2Cl%2CChhiZXN0IHJlc3RhdXJhbnRzIG5lYXIgbWUiBpABAagBAUiS7ZnX5YCAgAhaKhAAEAEYARgCGAMiGGJlc3QgcmVzdGF1cmFudHMgbmVhciBtZSoECAMQAZIBD3RoYWlfcmVzdGF1cmFudJoBI0NoWkRTVWhOTUc5blMwVkpRMEZuU1VReWMyUnhOMUZCRUFFqgFWEAEqFCIQYmVzdCByZXN0YXVyYW50cygAMh4QASIawhQE_SE_DODINQoc__KDkSVGxkLE8zpKc0cyHBACIhhiZXN0IHJlc3RhdXJhbnRzIG5lYXIgbWXgAQA%2Cy%2CVi0zLJDWONw%3Bmv%3A%5B%5B35.3126317%2C-80.7440313%5D%2C%5B35.3013358%2C-80.75668309999999) [lfcmVzdGF1cmFudJoBI0NoWkRTVWhOTUc5blMwVkpRMEZuU1VReWMyUnhOMUZCR](https://www.google.com/search?rlz=1C1UEAD_enUS1055US1055&tbs=lf%3A1%2Clf_ui%3A9&tbm=lcl&q=best%2Brestaurants%2Bnear%2Bme&rflfq=1&num=10&sa=X&ved=2ahUKEwiEyf-U-NL-AhXjElkFHT1uBrcQjGp6BAhTEAE&biw=2144&bih=983&dpr=1.1&rlfi=hd%3A%3Bsi%3A6062336256872962543%2Cl%2CChhiZXN0IHJlc3RhdXJhbnRzIG5lYXIgbWUiBpABAagBAUiS7ZnX5YCAgAhaKhAAEAEYARgCGAMiGGJlc3QgcmVzdGF1cmFudHMgbmVhciBtZSoECAMQAZIBD3RoYWlfcmVzdGF1cmFudJoBI0NoWkRTVWhOTUc5blMwVkpRMEZuU1VReWMyUnhOMUZCRUFFqgFWEAEqFCIQYmVzdCByZXN0YXVyYW50cygAMh4QASIawhQE_SE_DODINQoc__KDkSVGxkLE8zpKc0cyHBACIhhiZXN0IHJlc3RhdXJhbnRzIG5lYXIgbWXgAQA%2Cy%2CVi0zLJDWONw%3Bmv%3A%5B%5B35.3126317%2C-80.7440313%5D%2C%5B35.3013358%2C-80.75668309999999) [UFFqgFWEAEqFCIQYmVzdCByZXN0YXVyYW50cygAMh4QASIawhQE\_SE\_DODINQoc\_](https://www.google.com/search?rlz=1C1UEAD_enUS1055US1055&tbs=lf%3A1%2Clf_ui%3A9&tbm=lcl&q=best%2Brestaurants%2Bnear%2Bme&rflfq=1&num=10&sa=X&ved=2ahUKEwiEyf-U-NL-AhXjElkFHT1uBrcQjGp6BAhTEAE&biw=2144&bih=983&dpr=1.1&rlfi=hd%3A%3Bsi%3A6062336256872962543%2Cl%2CChhiZXN0IHJlc3RhdXJhbnRzIG5lYXIgbWUiBpABAagBAUiS7ZnX5YCAgAhaKhAAEAEYARgCGAMiGGJlc3QgcmVzdGF1cmFudHMgbmVhciBtZSoECAMQAZIBD3RoYWlfcmVzdGF1cmFudJoBI0NoWkRTVWhOTUc5blMwVkpRMEZuU1VReWMyUnhOMUZCRUFFqgFWEAEqFCIQYmVzdCByZXN0YXVyYW50cygAMh4QASIawhQE_SE_DODINQoc__KDkSVGxkLE8zpKc0cyHBACIhhiZXN0IHJlc3RhdXJhbnRzIG5lYXIgbWXgAQA%2Cy%2CVi0zLJDWONw%3Bmv%3A%5B%5B35.3126317%2C-80.7440313%5D%2C%5B35.3013358%2C-80.75668309999999)

[\_KDkSVGxkLE8zpKc0cyHBACIhhiZXN0IHJlc3RhdXJhbnRzIG5lYXIgbWXgAQA,y,Vi0zLJ](https://www.google.com/search?rlz=1C1UEAD_enUS1055US1055&tbs=lf%3A1%2Clf_ui%3A9&tbm=lcl&q=best%2Brestaurants%2Bnear%2Bme&rflfq=1&num=10&sa=X&ved=2ahUKEwiEyf-U-NL-AhXjElkFHT1uBrcQjGp6BAhTEAE&biw=2144&bih=983&dpr=1.1&rlfi=hd%3A%3Bsi%3A6062336256872962543%2Cl%2CChhiZXN0IHJlc3RhdXJhbnRzIG5lYXIgbWUiBpABAagBAUiS7ZnX5YCAgAhaKhAAEAEYARgCGAMiGGJlc3QgcmVzdGF1cmFudHMgbmVhciBtZSoECAMQAZIBD3RoYWlfcmVzdGF1cmFudJoBI0NoWkRTVWhOTUc5blMwVkpRMEZuU1VReWMyUnhOMUZCRUFFqgFWEAEqFCIQYmVzdCByZXN0YXVyYW50cygAMh4QASIawhQE_SE_DODINQoc__KDkSVGxkLE8zpKc0cyHBACIhhiZXN0IHJlc3RhdXJhbnRzIG5lYXIgbWXgAQA%2Cy%2CVi0zLJDWONw%3Bmv%3A%5B%5B35.3126317%2C-80.7440313%5D%2C%5B35.3013358%2C-80.75668309999999) [DWONw;mv:[[35.3126317,-80.7440313],[35.3013358,-80.75668309999999](https://www.google.com/search?rlz=1C1UEAD_enUS1055US1055&tbs=lf%3A1%2Clf_ui%3A9&tbm=lcl&q=best%2Brestaurants%2Bnear%2Bme&rflfq=1&num=10&sa=X&ved=2ahUKEwiEyf-U-NL-AhXjElkFHT1uBrcQjGp6BAhTEAE&biw=2144&bih=983&dpr=1.1&rlfi=hd%3A%3Bsi%3A6062336256872962543%2Cl%2CChhiZXN0IHJlc3RhdXJhbnRzIG5lYXIgbWUiBpABAagBAUiS7ZnX5YCAgAhaKhAAEAEYARgCGAMiGGJlc3QgcmVzdGF1cmFudHMgbmVhciBtZSoECAMQAZIBD3RoYWlfcmVzdGF1cmFudJoBI0NoWkRTVWhOTUc5blMwVkpRMEZuU1VReWMyUnhOMUZCRUFFqgFWEAEqFCIQYmVzdCByZXN0YXVyYW50cygAMh4QASIawhQE_SE_DODINQoc__KDkSVGxkLE8zpKc0cyHBACIhhiZXN0IHJlc3RhdXJhbnRzIG5lYXIgbWXgAQA%2Cy%2CVi0zLJDWONw%3Bmv%3A%5B%5B35.3126317%2C-80.7440313%5D%2C%5B35.3013358%2C-80.75668309999999)]]

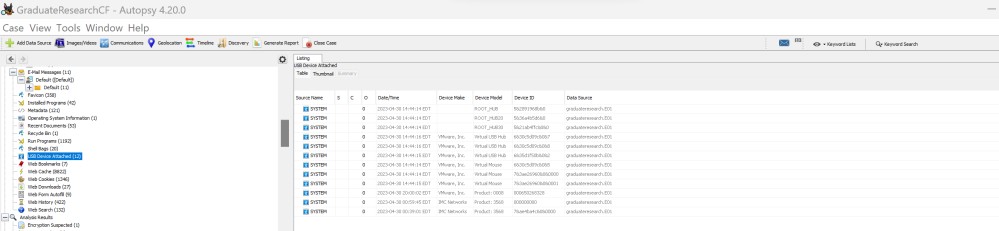


*Figure: Google maps location*



From the above image we can tell that the person is from Charlotte and near the University of North Carolina at Charlotte.

1. How many external storage devices were connected to the computer? Goto Data Artifacts -> USB devices attached.

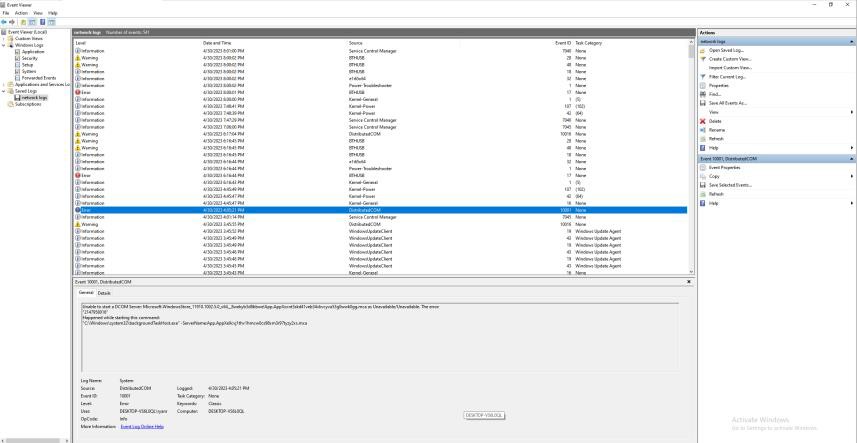


*Figure: USB devices attached.*

From the above image we can see there are total of 12 devices attached.

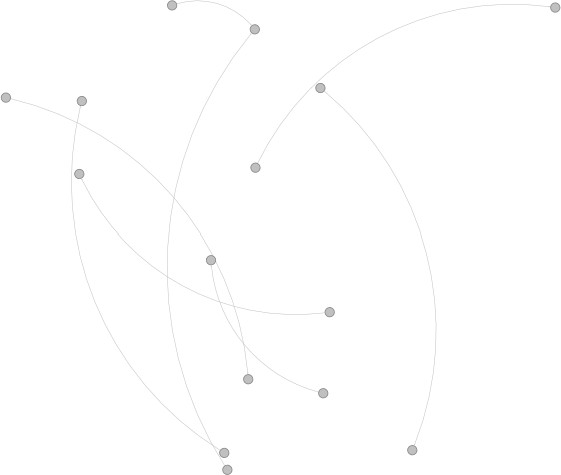
1. Can you conduct a network analysis on the network logs?

Using Microsoft Event Viewer, we can check the network logs. Export the network logs from Event viewer and the import them in Gephi to draw the graph based on the nodes and edges and run it.

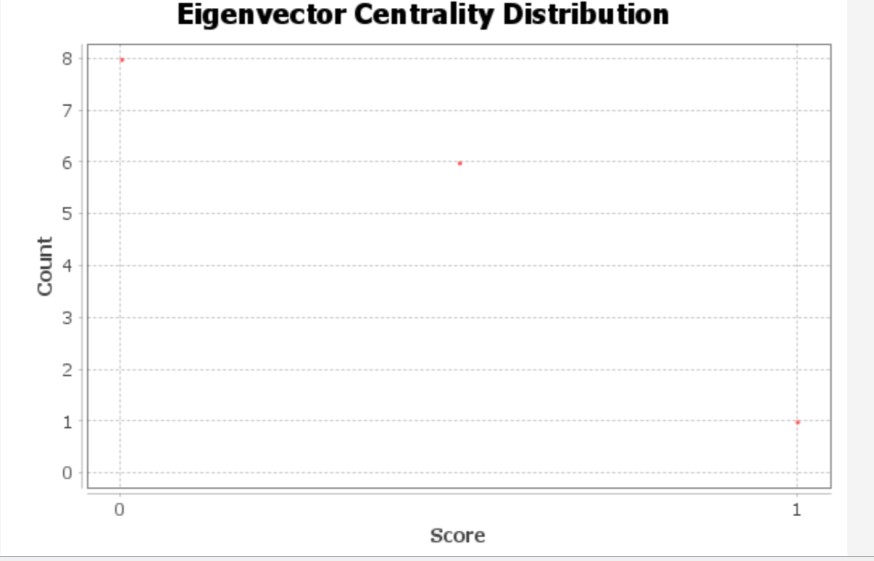


*Figure: Network logs from Event viewer*

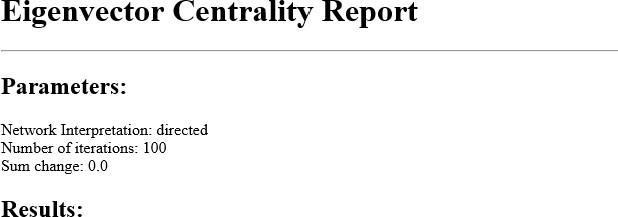
**Results from the Network log analysis:**



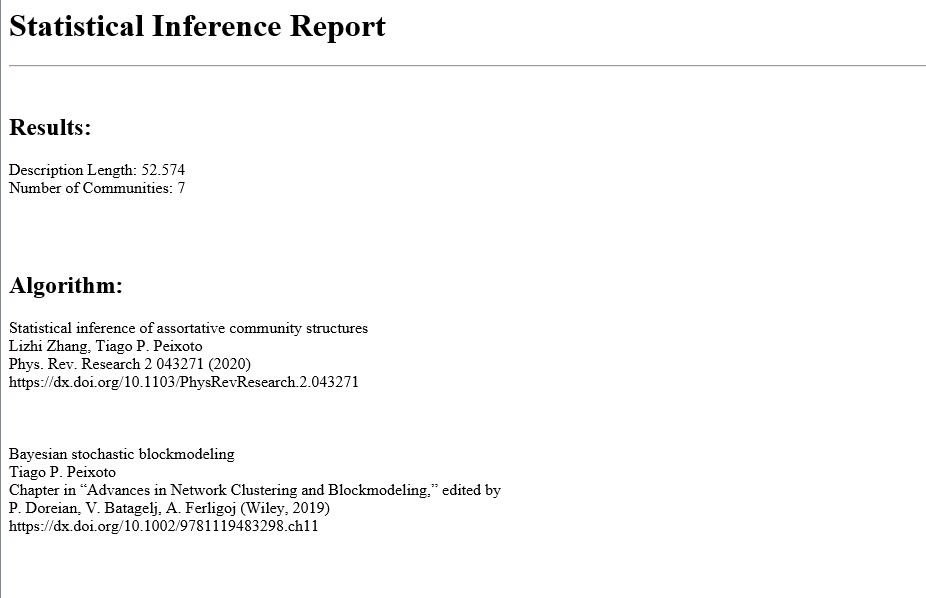
*Figure: Gephi Graph from the network logs*



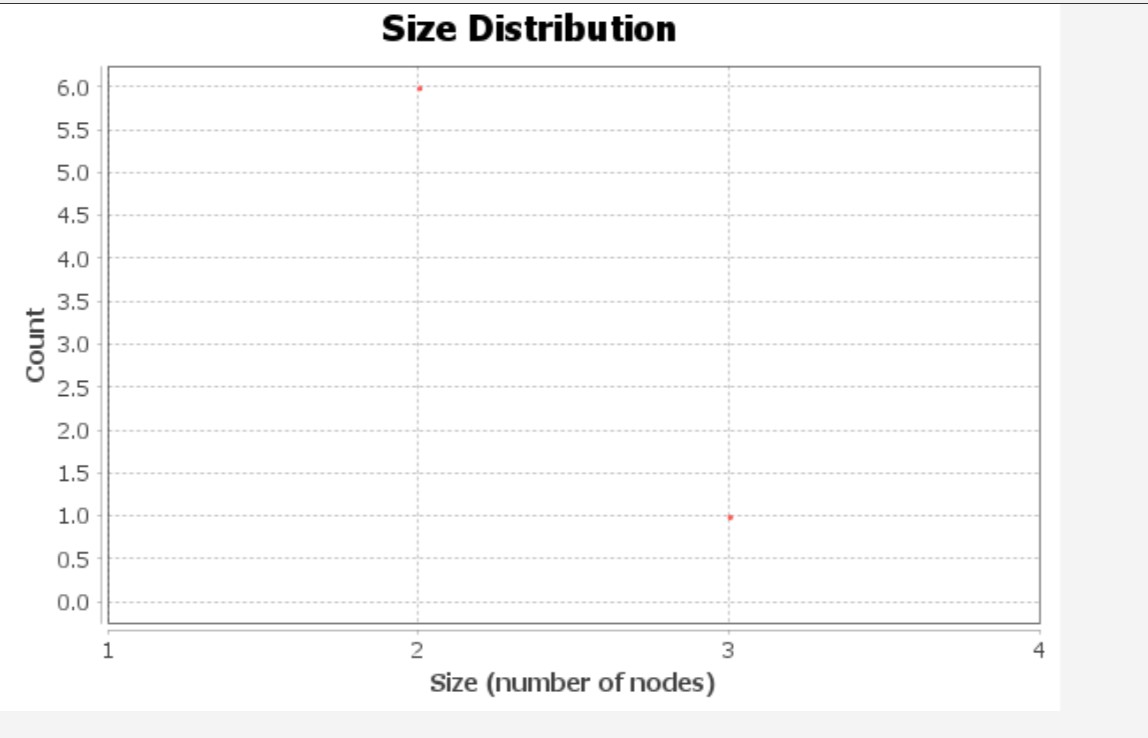
*Figure: Eigenvector Centrality distribution*



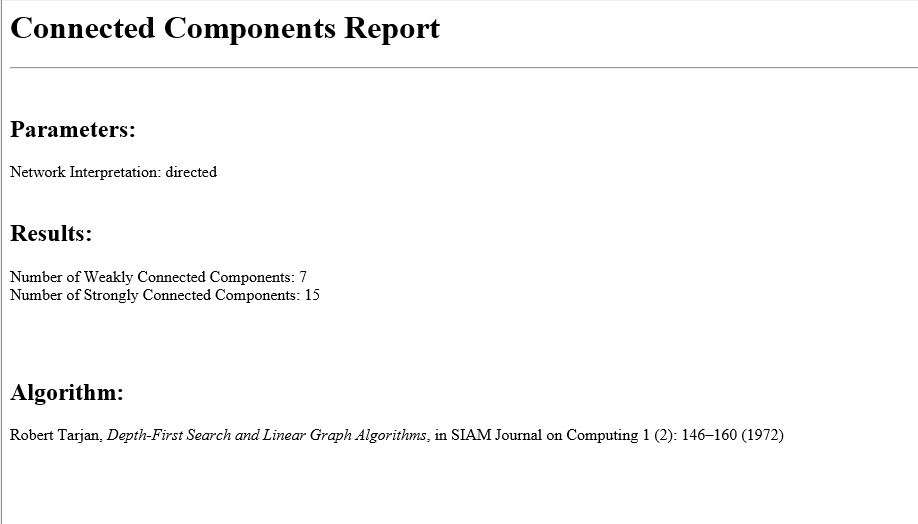
*Figure: Report of Eigenvector Centrality from Gephi*



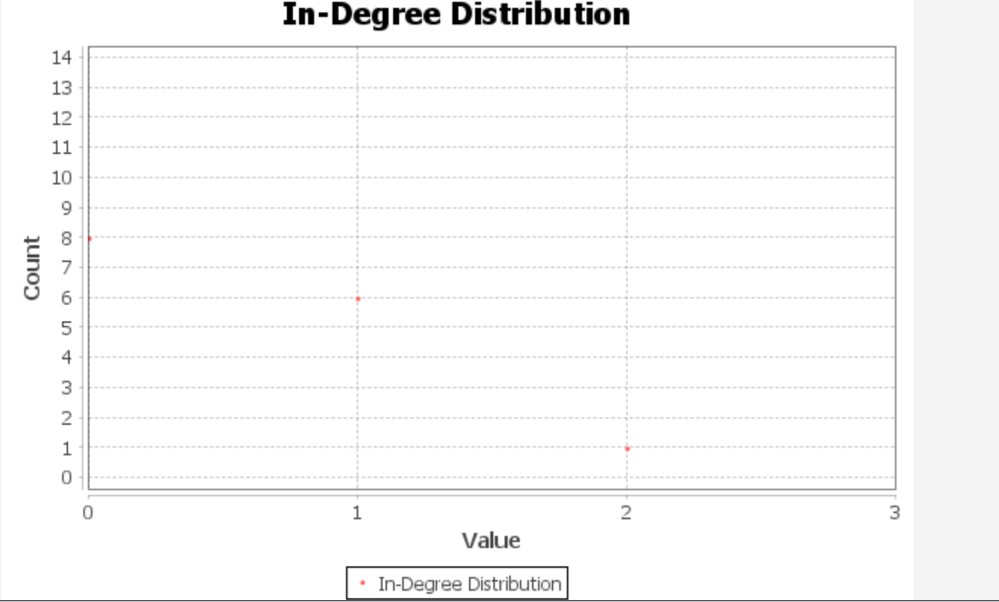
*Figure: Report of Statistical Inference from Gephi*



*Figure: Size distribution count*



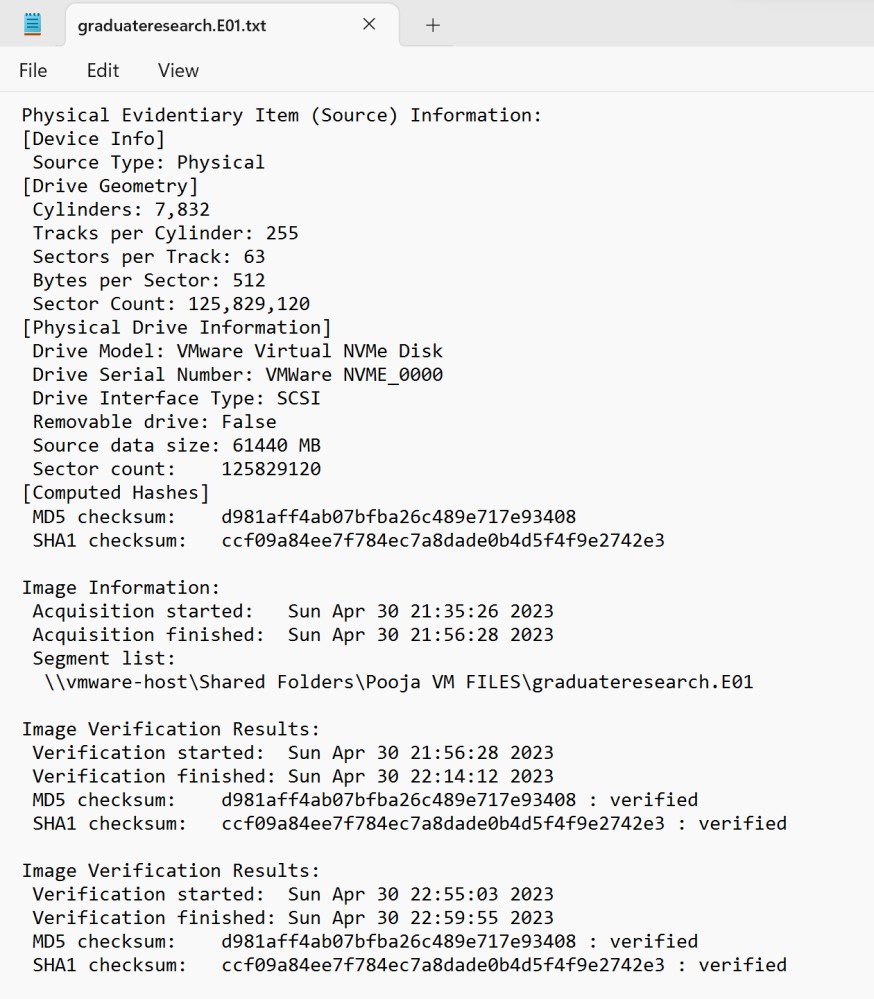
*Figure: Report of Connected Components*



*Figure: In-Degree distribution chart*



*Figure: Weighted Degree Report*



*Figure: graduateresearch.E01.txt*

**Conclusion:**

The investigation of the individual's computer is examined, and we have successfully collected and extracted all pertinent evidence as per our investigative requirements. The extracted evidence encompasses various types of data, such as images, emails, software usage, and connections to individuals linked to the case. After careful evaluation of the gathered evidence, it has been determined that there is currently no need for further analysis.