Student:	Email:
muhammad zahid	zahid1mz@cmich.edu

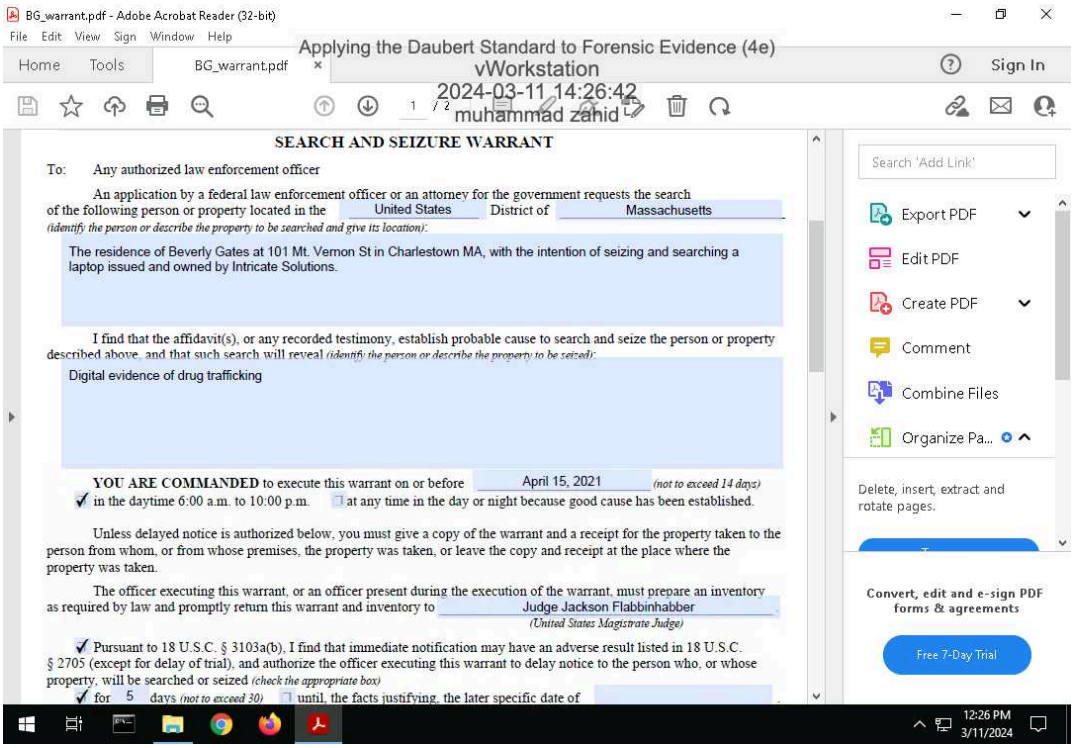
Time on Task:	Progress:
9 hours, 2 minutes	100%

Report Generated: Wednesday, March 13, 2024 at 1:04 AM

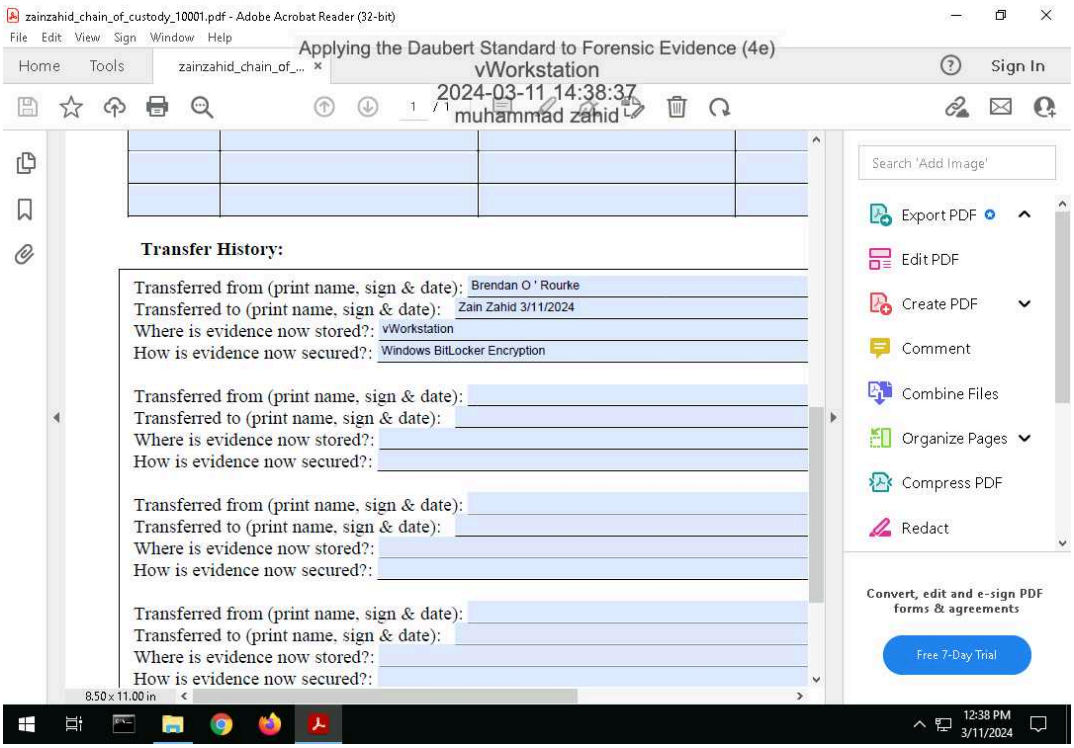
Section 1: Hands-On Demonstration

Part 1: Complete Chain of Custody Procedures

7. **Make a screen capture** showing the **contents of the search warrant in Adobe Reader**.

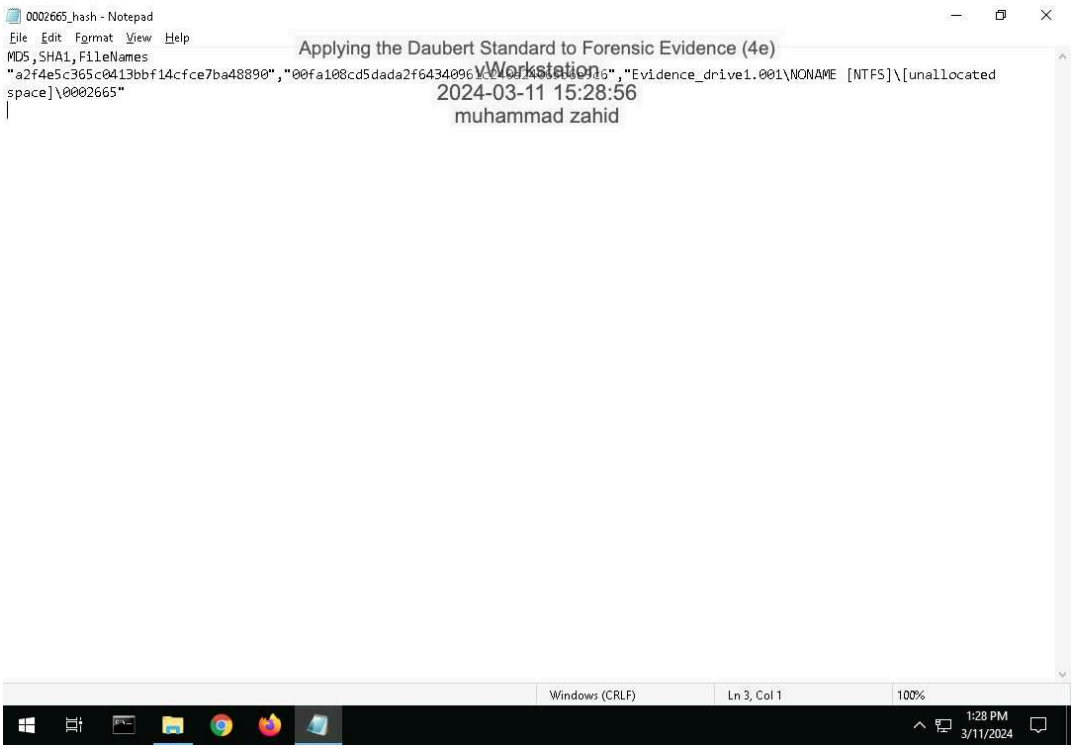


14. **Make a screen capture** showing the **completed Chain of Custody form in Adobe Reader.**

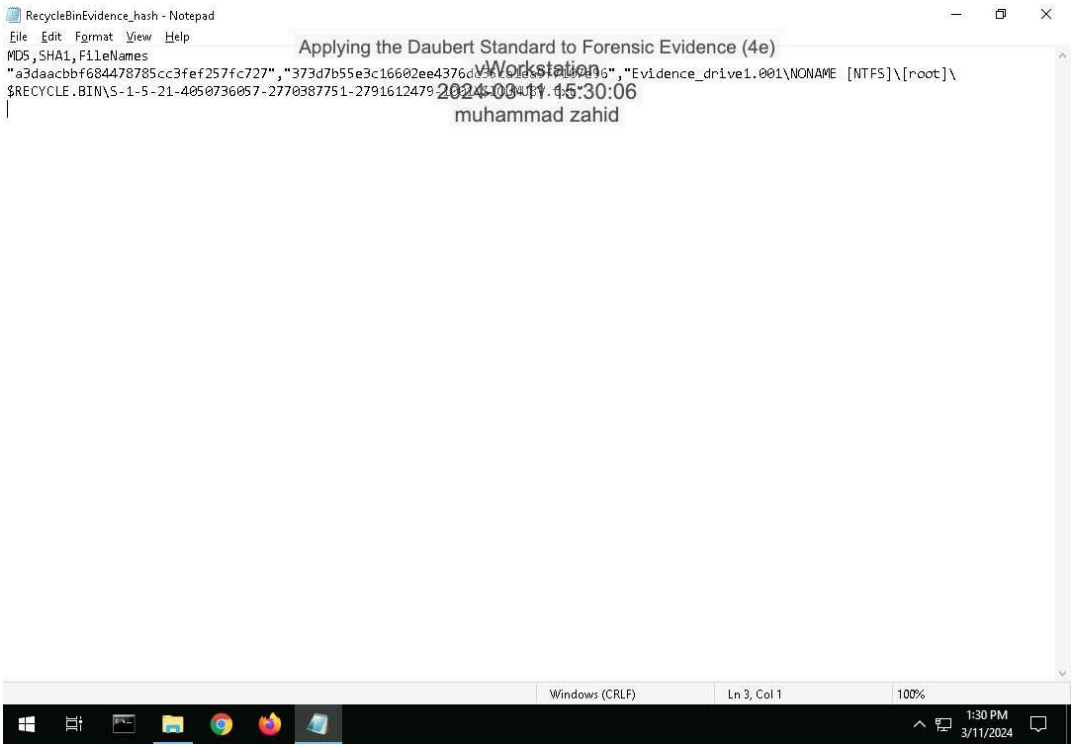


Part 2: Extract Evidence Files and Create Hash Codes with FTK Imager

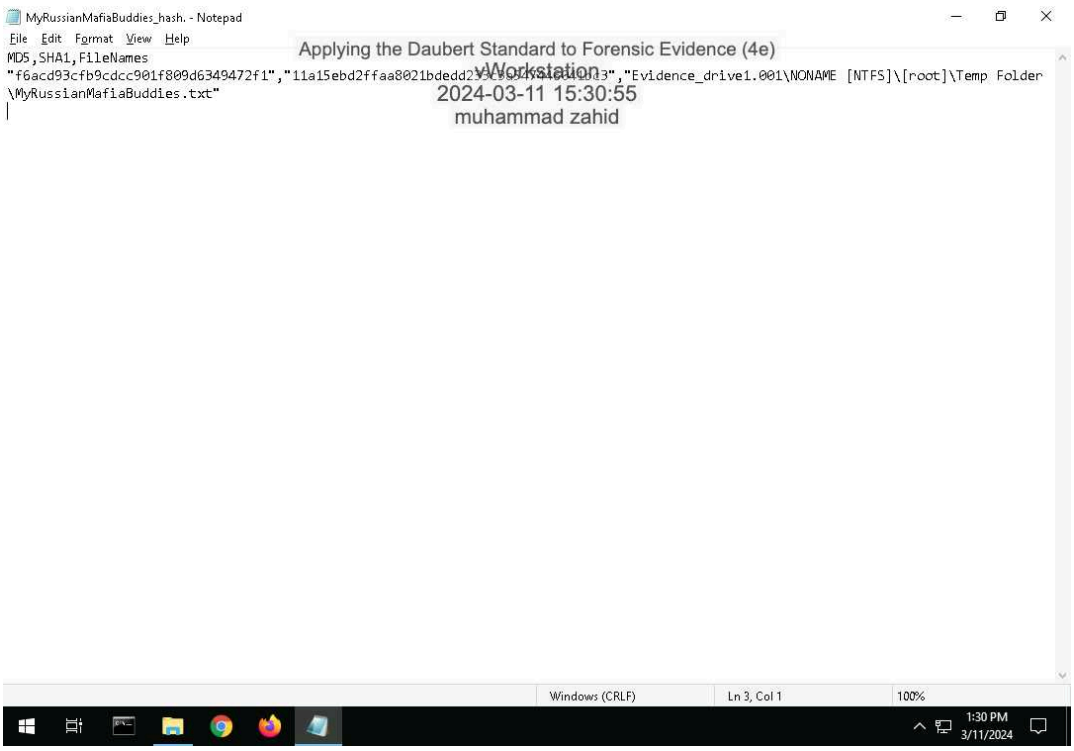
34. **Make a screen capture** showing the **contents of the 0002665_hash.csv file**.



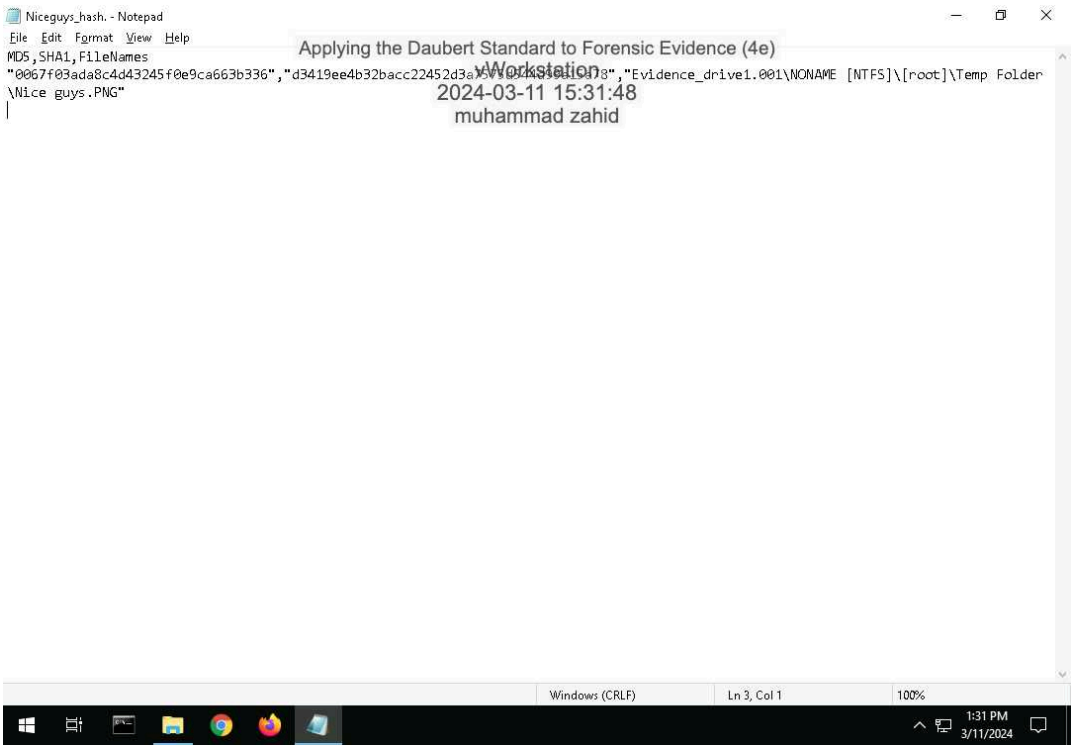
37. **Make a screen capture** showing the **contents of the RecycleBinEvidence_hash.csv file**.



38. **Make a screen capture** showing the **contents of the MyRussianMafiaBuddies_hash.csv file**.

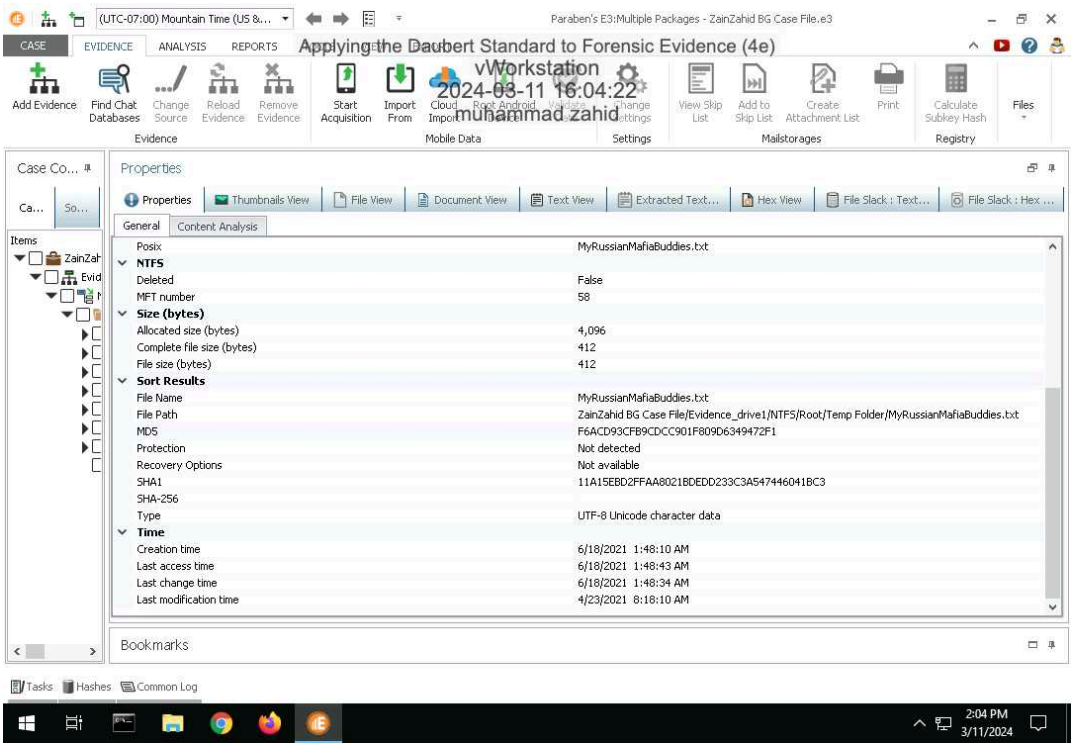


39. **Make a screen capture** showing the **contents of the Nice guys_hash.csv file**.

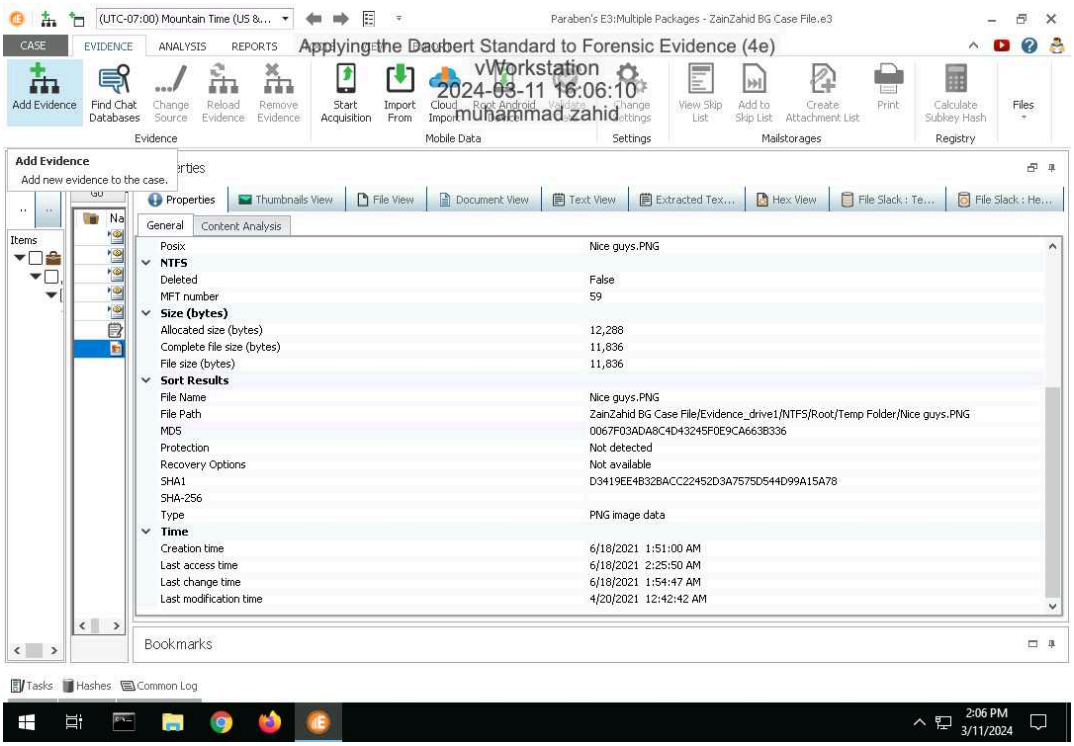


Part 3: Verify Hash Codes with E3

14. **Make a screen capture** showing the **MD5 and SHA1 values for the MyRussianMafiaBuddies.txt file**.



16. **Make a screen capture** showing the **MD5 and SHA1 values for the Nice Guys.png file**.



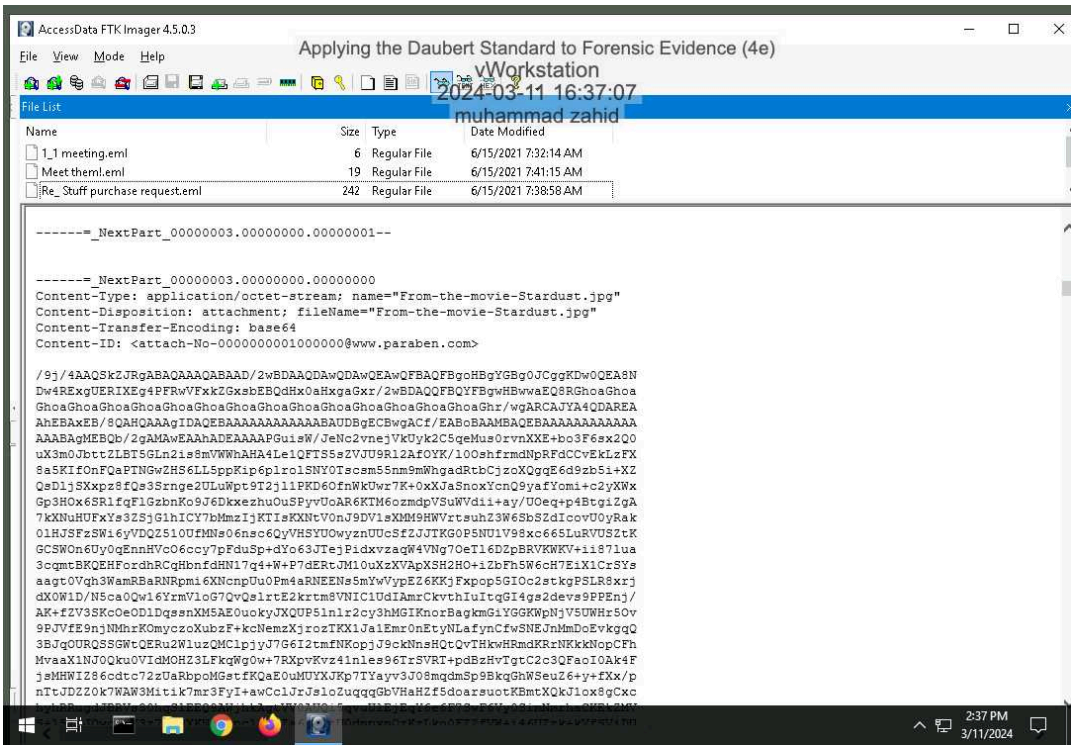
17. **Describe** how the hash values produced by E3 for the incriminating files compare to those produced by FTK. Do they match?

Yes they are the same values, the are corresponding to each other. They verify each other.

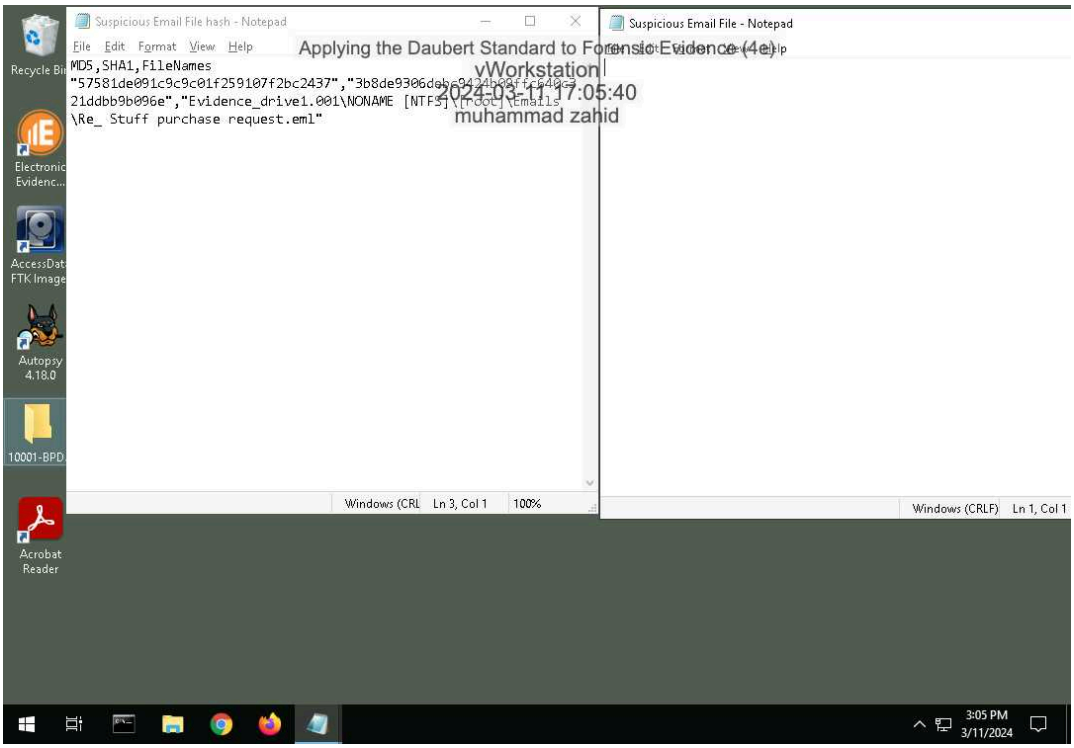
Section 2: Applied Learning

Part 1: Extract Evidence Files and Create Hash Codes with FTK Imager

5. **Make a screen capture** showing the **contents of the suspicious email file in the Display pane**.

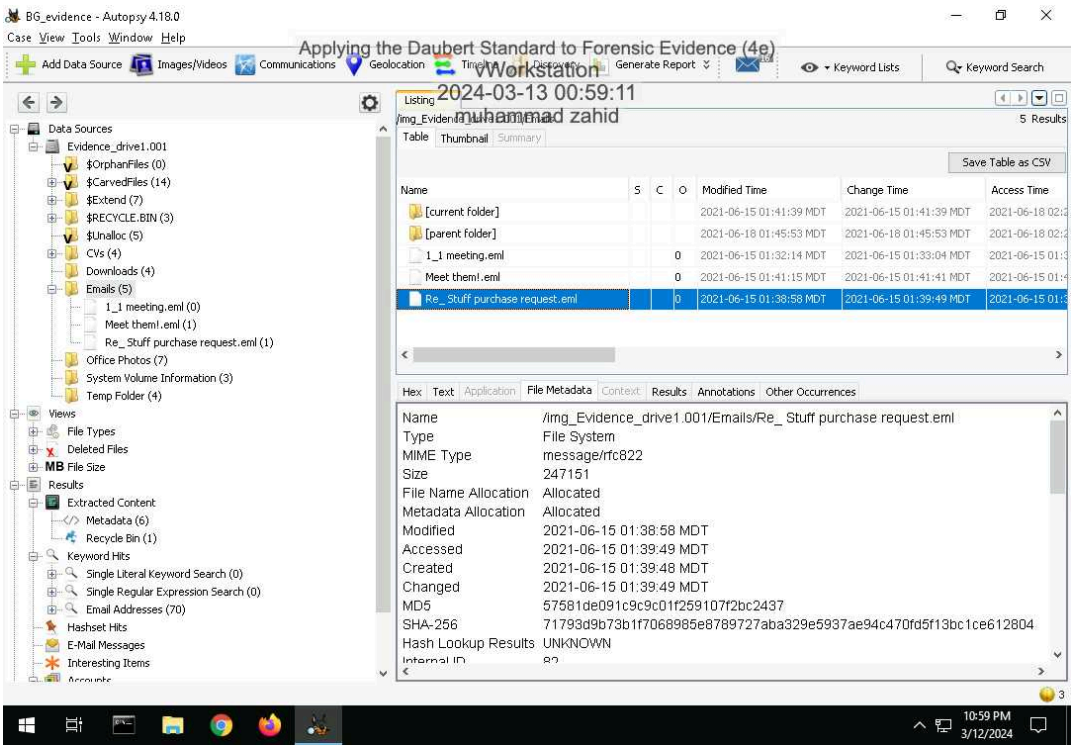


16. **Make a screen capture** showing the **two hash values for the suspicious email file**.



Part 2: Verify Hash Codes with Autopsy

11. **Make a screen capture** showing the **MD5 field in the Result Viewer**.

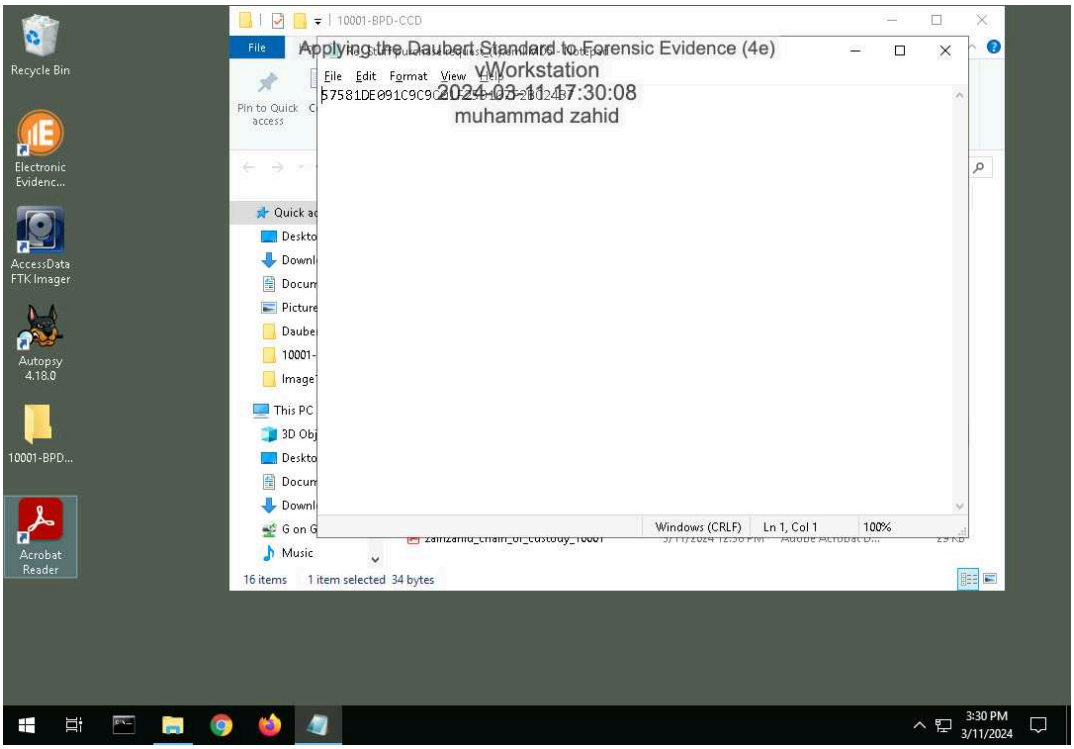


12. **Describe** how the hash value produced by Autopsy compares to the values produced by FTK Imager for the two .eml files.

Hash value produced by E3 compares to the values produced by the FTK imager for the Re_stuff purchase request.eml files and the value produced by Autopsy has same values. the Values of Re_stuff Purchase request 1.eml is different.

Part 3: Verify Hash Codes with E3

7. **Make a screen capture** showing the **MD5 value produced by E3**.



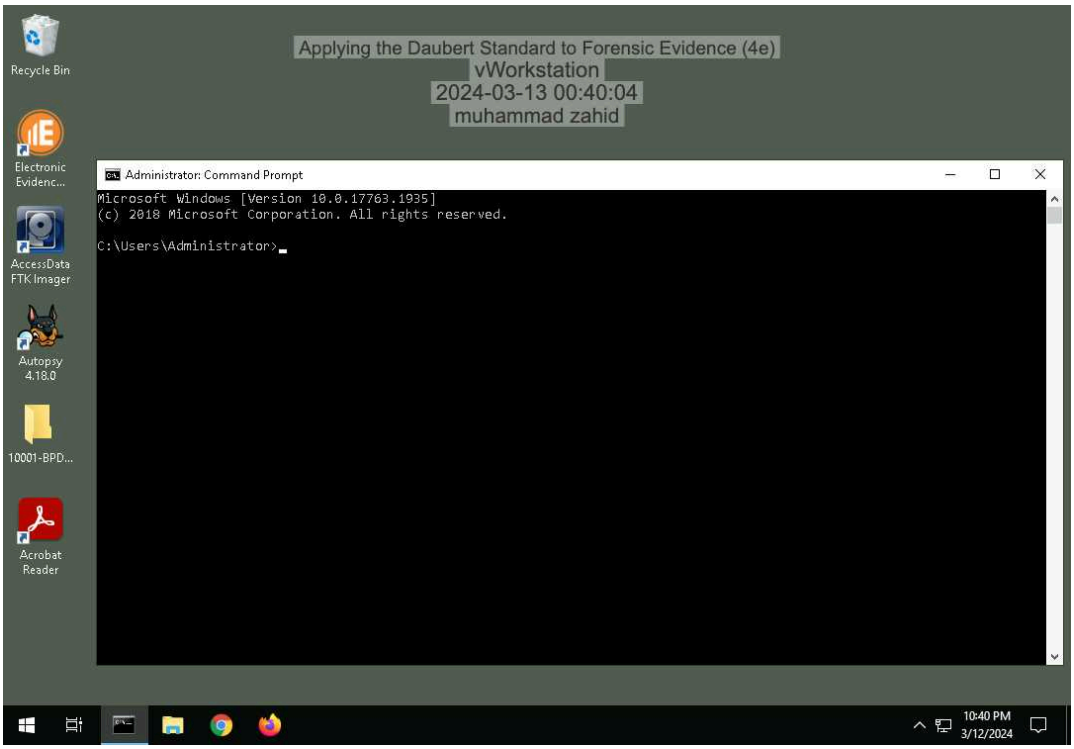
8. **Describe** how the hash value produced by E3 compares to the values produced by FTK Imager for the two .eml files and the value produced by Autopsy.

If you compare the original hash values in the two programs before the deleted and edited version then the hash values are the same, but if you compare to the deleted edited version then they would be different.

Section 3: Challenge and Analysis

Part 1: Verify Hash Codes on the Command Line

Make a screen capture showing the **hash values for the Evidence_drive1.001 file**.



Part 2: Locate Additional Evidence

Define the original file names and file paths for each of the three files.

Under Evidence Tree -> root -> ($Recycle.Bin). Full three files with their content are available there.