

# Applying the Daubert Standard to Forensic Evidence (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 01

Student:

Samman Chouhan

Email:

schouhan1@hawk.iit.edu

Time on Task:

2 hours, 39 minutes

Progress:

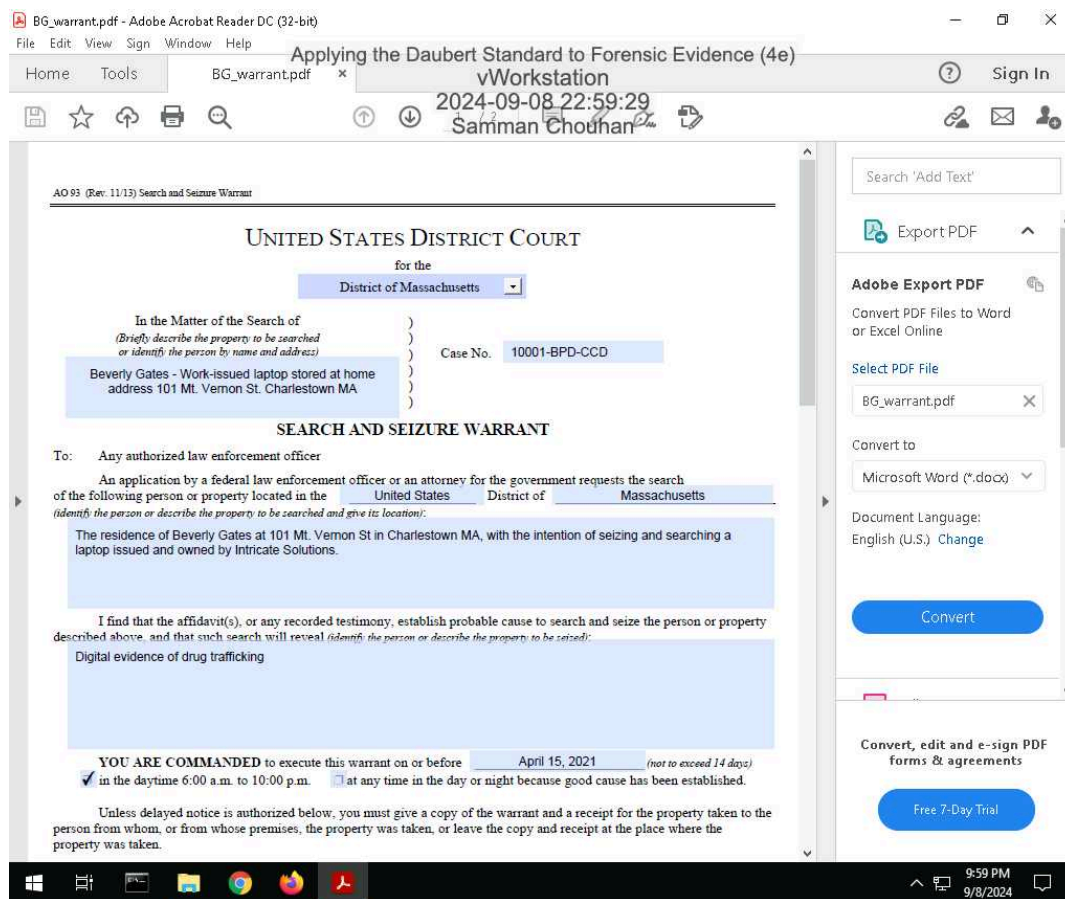
100%

Report Generated: Monday, September 9, 2024 at 2:32 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.



# Applying the Daubert Standard to Forensic Evidence (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 01

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

The screenshot shows the Adobe Acrobat Reader interface with a Chain of Custody form titled "Applying the Daubert Standard to Forensic Evidence (4e)". The form is filled out with the following information:

- Evidence collected by (name): Hannah Jones
- Date/Time collected: 1:30 PM, April 19, 2021
- Evidence description: 1 disk image taken from seized dell laptop
- Describe Collection method (include operating system, utility, commands, arguments, etc): disk image generated using FTK Imager from Windows 10 workstation
- What application software/utility is required to view the file?: FTK Imager, E3, Autopsy, Encase, or comparable
- Where is evidence initially stored?: Disk image is stored on BPD file server, source laptop stored in BPD police locker
- How is evidence initially secured?: Windows BitLocker Encryption
- Collector signature: [Redacted] Date: April 20, 2021

The form also includes a "Copy History" table and a "Transfer History" section.

Date	Copied By	Copy Method	Disposition of original and all copies

**Transfer History:**

- Transferred from (print name, sign & date): Brendan O'Rourke
- Transferred to (print name, sign & date): Samman Chouhan 09/08/2024
- Where is evidence now stored?: vWorkstation
- How is evidence now secured?: Windows BitLocker Encryption
- Transferred from (print name, sign & date):
- Transferred to (print name, sign & date):
- Where is evidence now stored?:
- How is evidence now secured?:

## 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.

The screenshot shows a Notepad window titled "0002665\_hash - Notepad" with the following content:

```
MD5,SHA1,FileNames
"a2f4e5c365c0413bbf14cfe7ba48898","90fa188cd5ada2f64340961c240a24865b6e9c6","E:\vWorkstation\0002665\0002665"
```

# Applying the Daubert Standard to Forensic Evidence (4e)

Digital Forensics, Investigation, and Response, Fourth Edition - Lab 01

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.



# Applying the Daubert Standard to Forensic Evidence (4e)

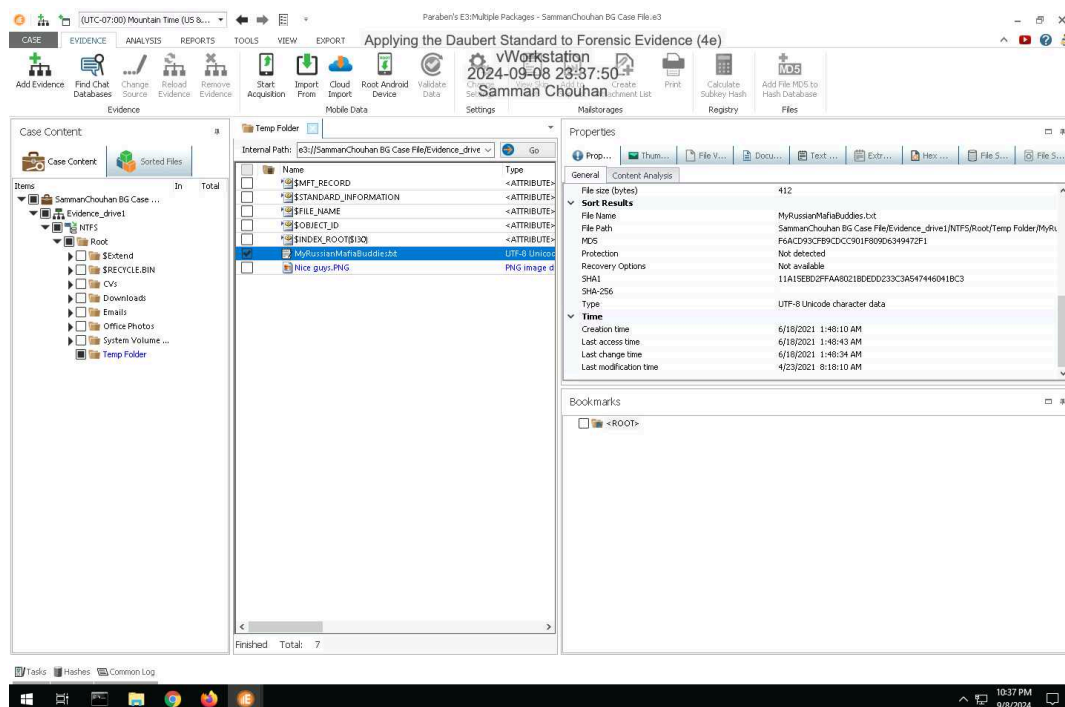
## Digital Forensics, Investigation, and Response, Fourth Edition - Lab 01

### 39. Make a screen capture showing the contents of the Nice guys\_hash.csv file.



## Part 3: Verify Hash Codes with E3

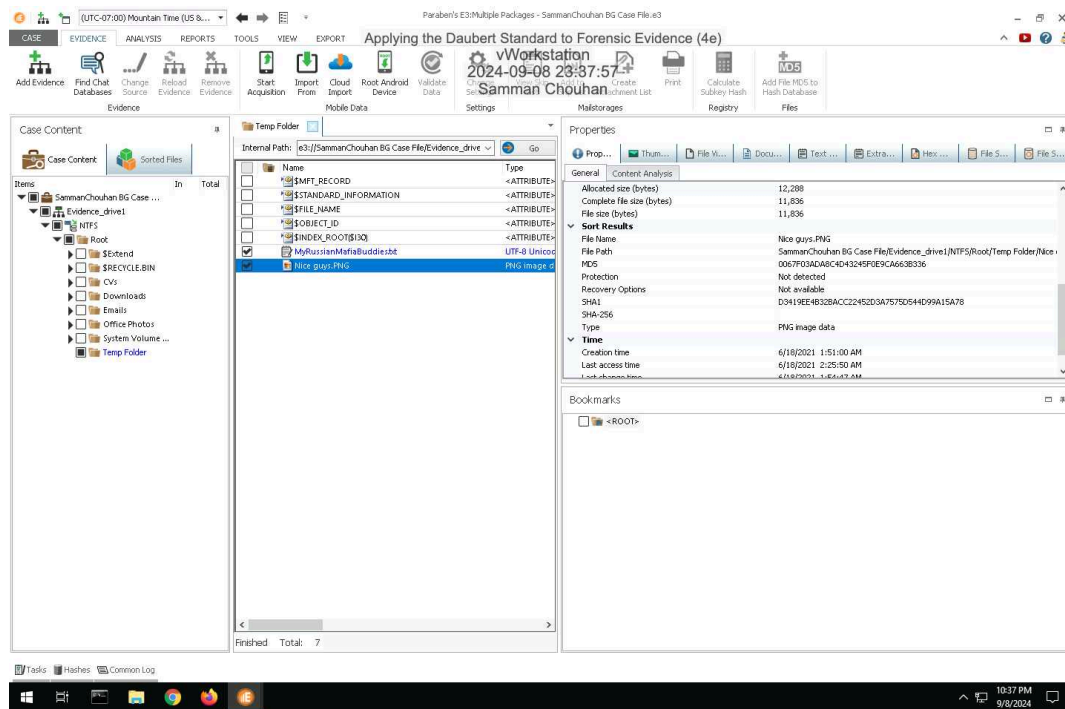
### 14. Make a screen capture showing the MD5 and SHA1 values for the MyRussianMafiaBuddies.txt file.



# Applying the Daubert Standard to Forensic Evidence (4e)

## Digital Forensics, Investigation, and Response, Fourth Edition - Lab 01

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



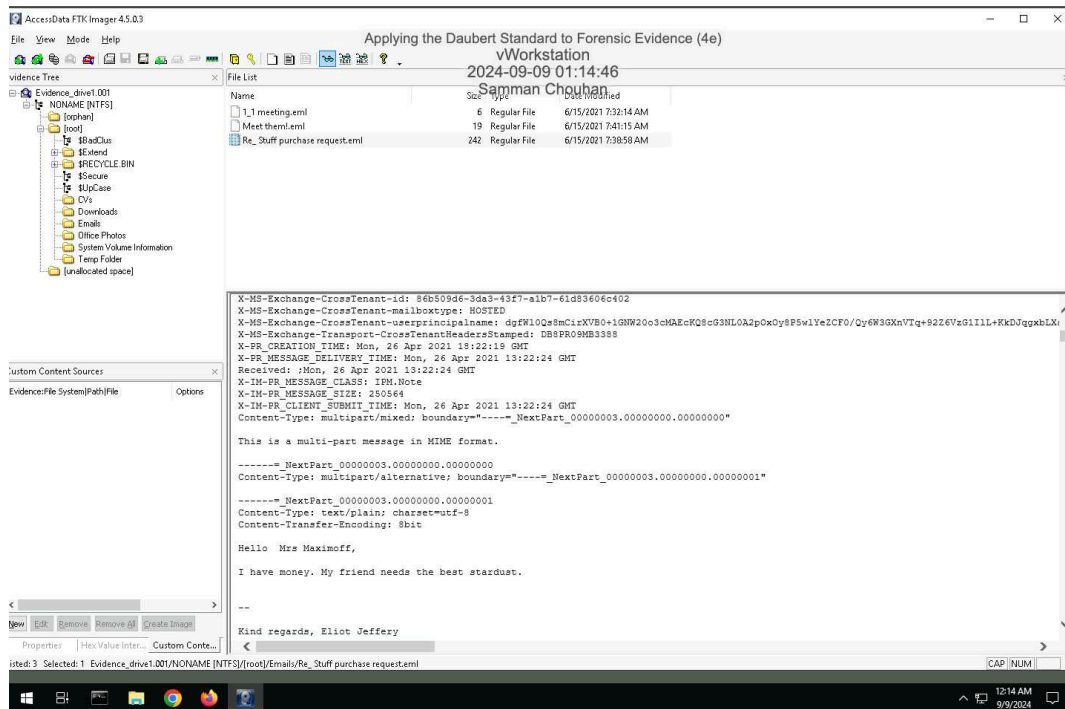
17. Describe how the hash values produced by E3 for the incriminating files compare to those produced by FTK. Do they match?

yes they match

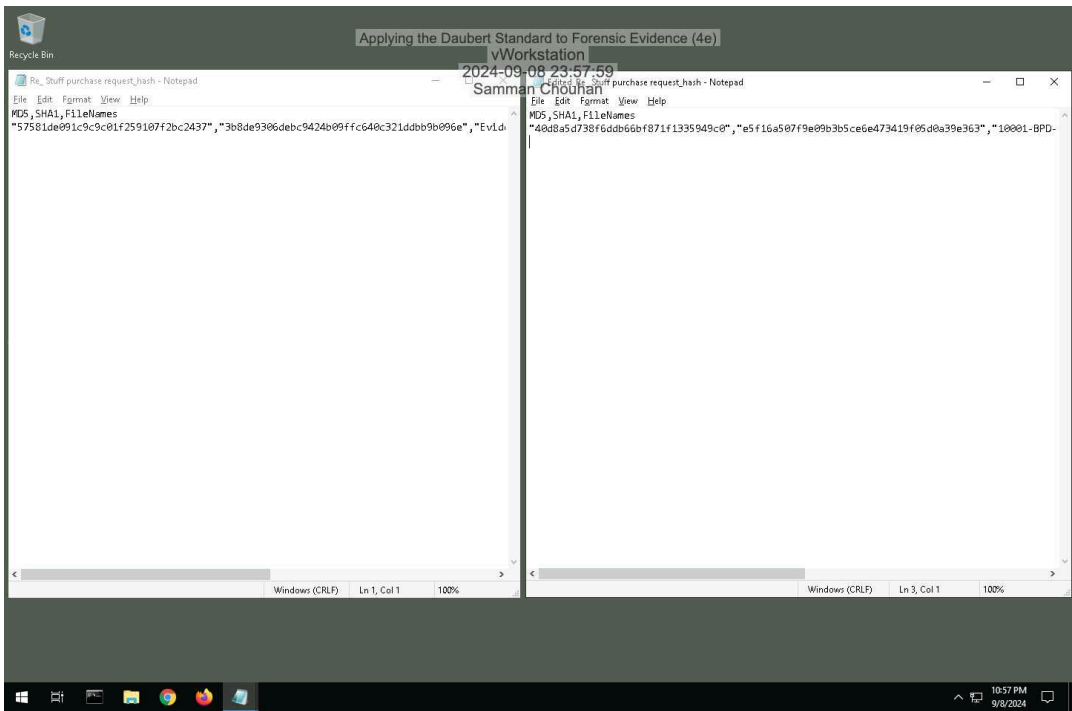
### Section 2: Applied Learning

#### 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.

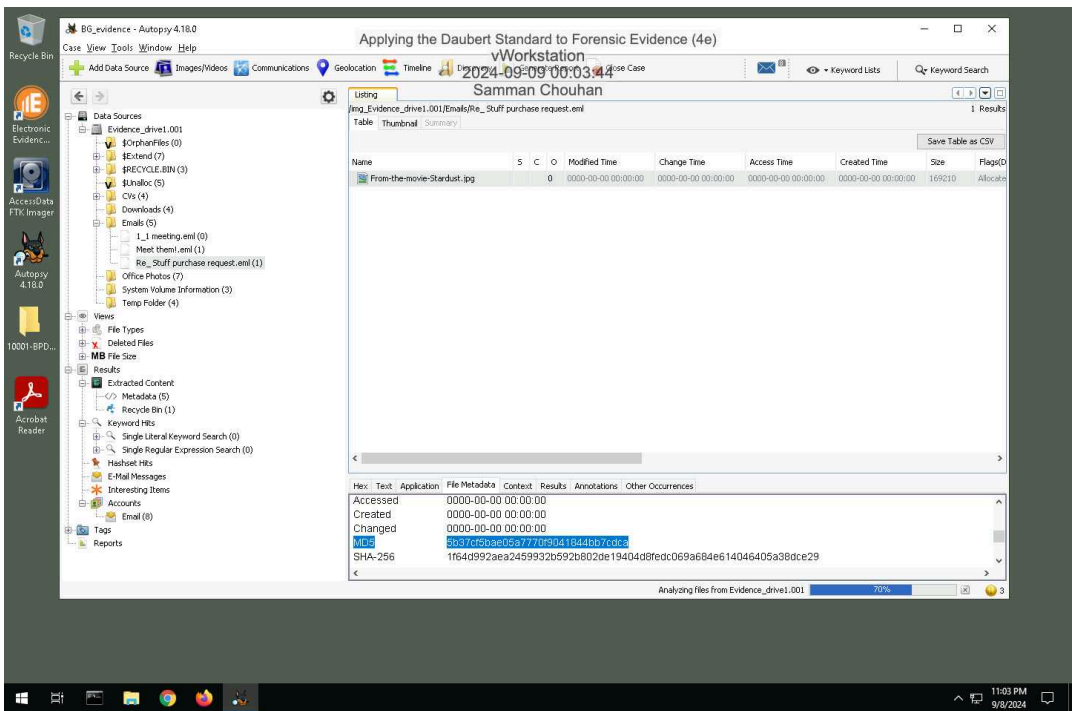


16. Make a screen capture showing the **two hash values** for the suspicious email file.



Part 2: Verify Hash Codes with Autopsy

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



## Applying the Daubert Standard to Forensic Evidence (4e)

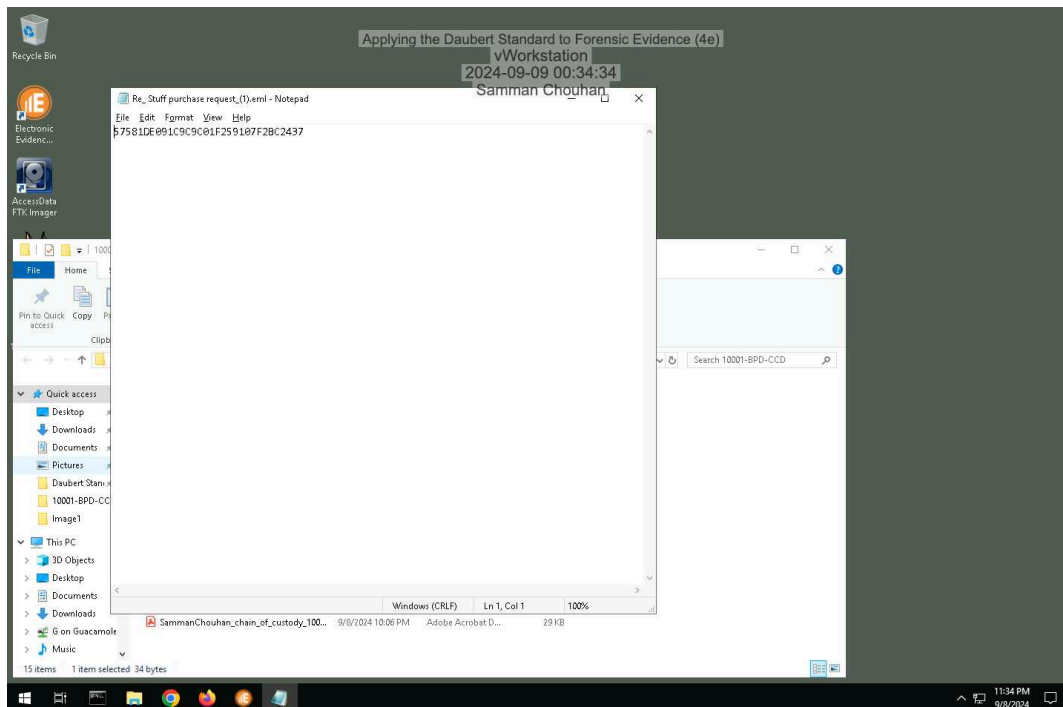
Digital Forensics, Investigation, and Response, Fourth Edition - Lab 01

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

both applications provide the same MD5 hashes

### 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.

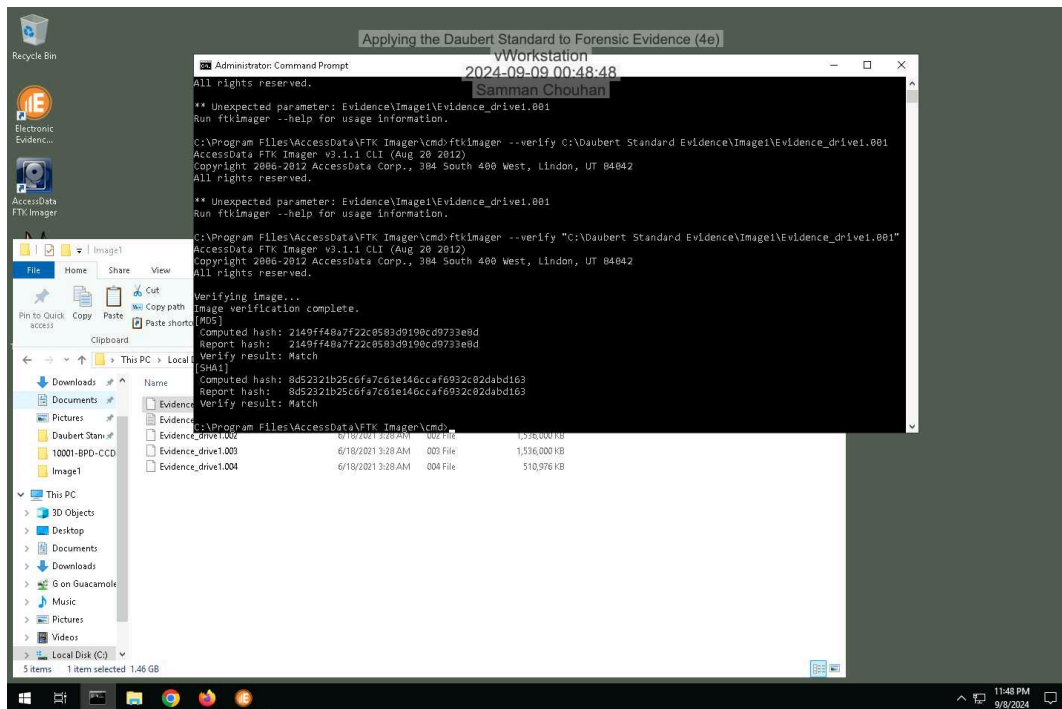
same hashes produced by all three applications



### 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.

\$R354ELH.xlsx G:\VIP Info21DrugSales.xlsx\$RBQEOTL.doc G:\Students>manual-testing-fresher-resume-1.doc\$RX3177E.pdf G:\Work Doc\hr letter for visa.pdf