**Lab 1: Applying the Daubert Standard to Forensic Evidence (E3)**

**By**

**Natnael Kebede**



**University of Dallas**

**2020**

This Paper Submitted in Partial Fulfillment of the Requirements for

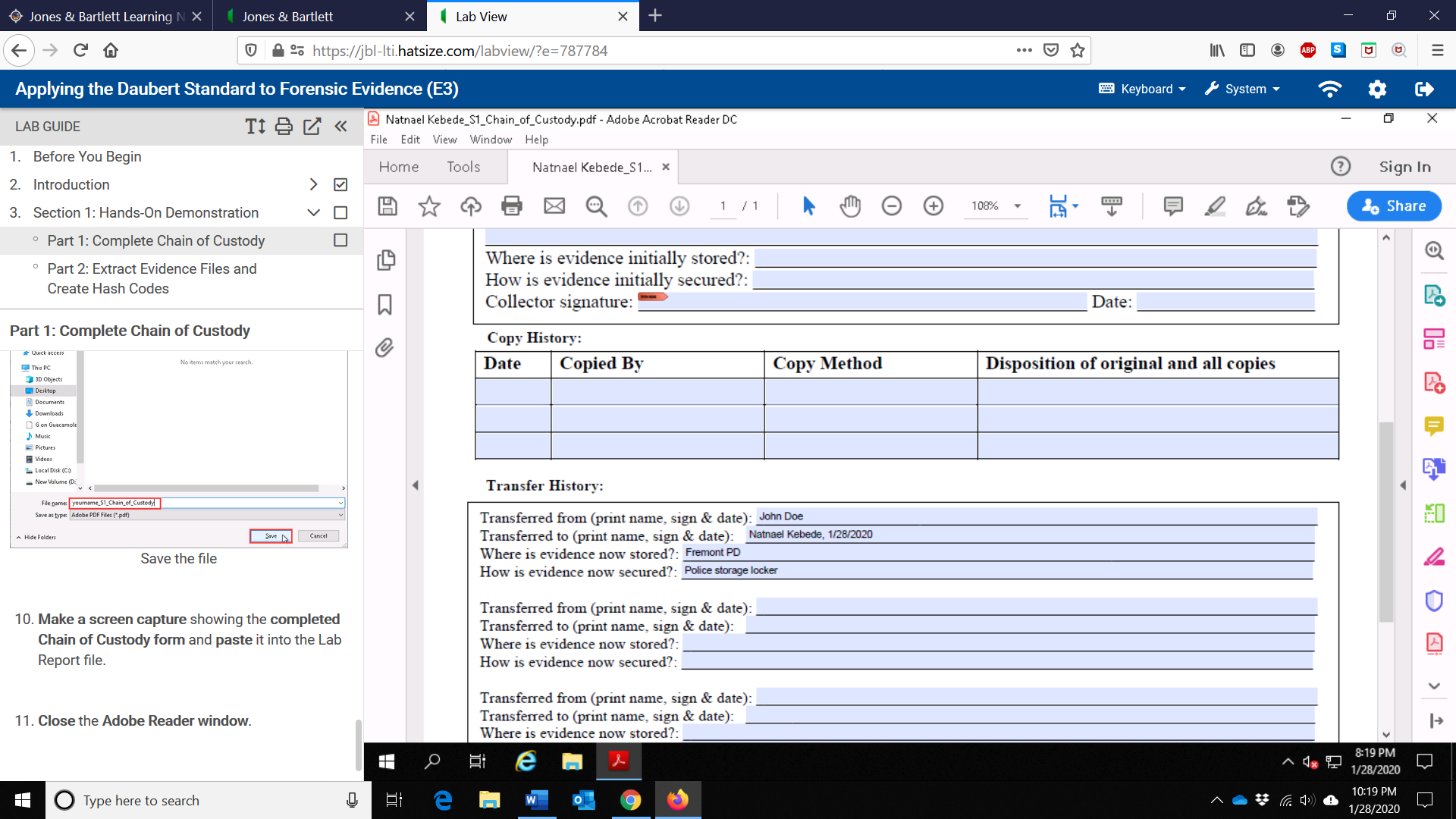
CYBS 7359 – Penetration Testing and Vulnerability Assessment

Spring 2020

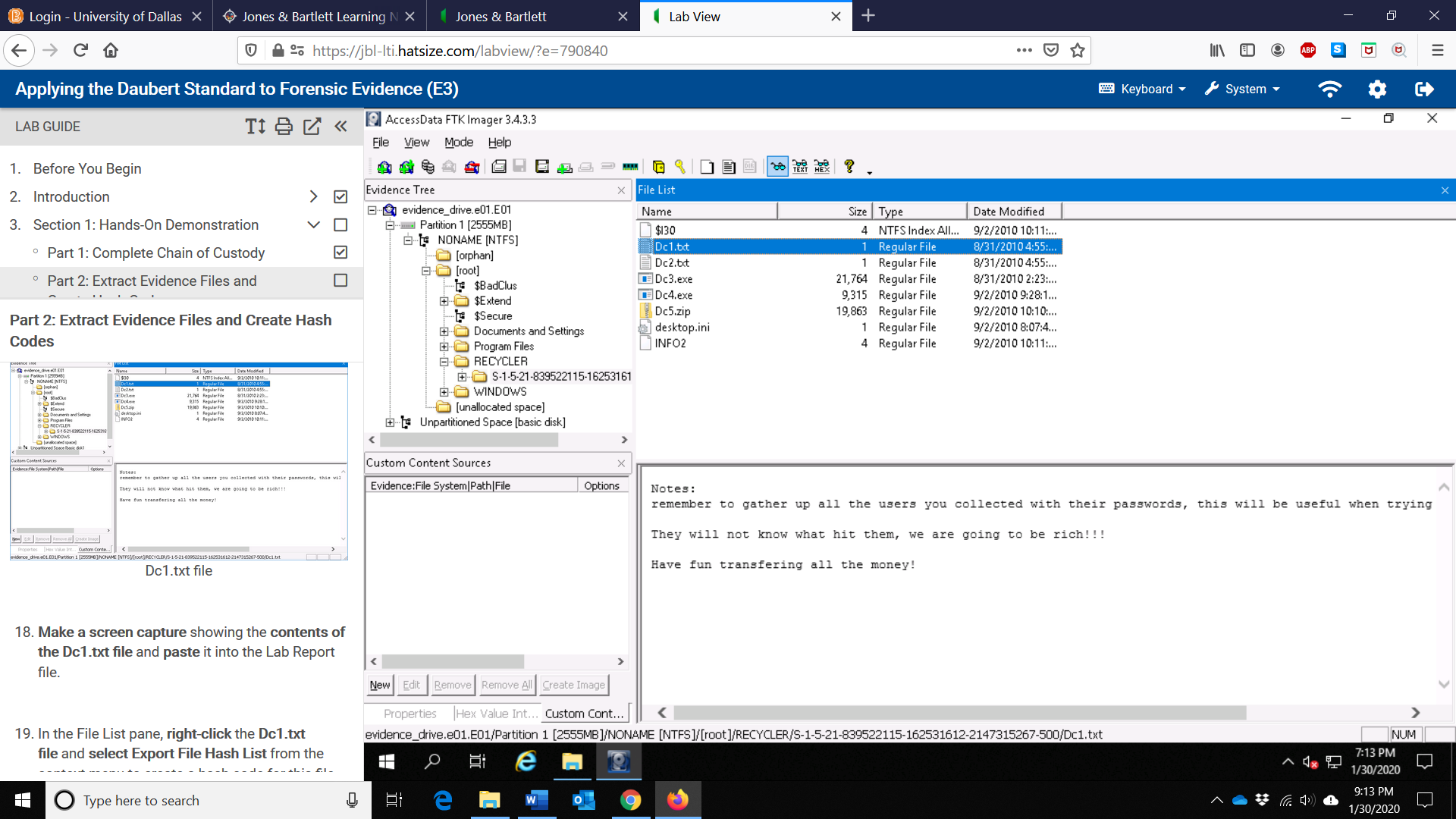
Presented to Dr. Renita Murimi

**Section 1**

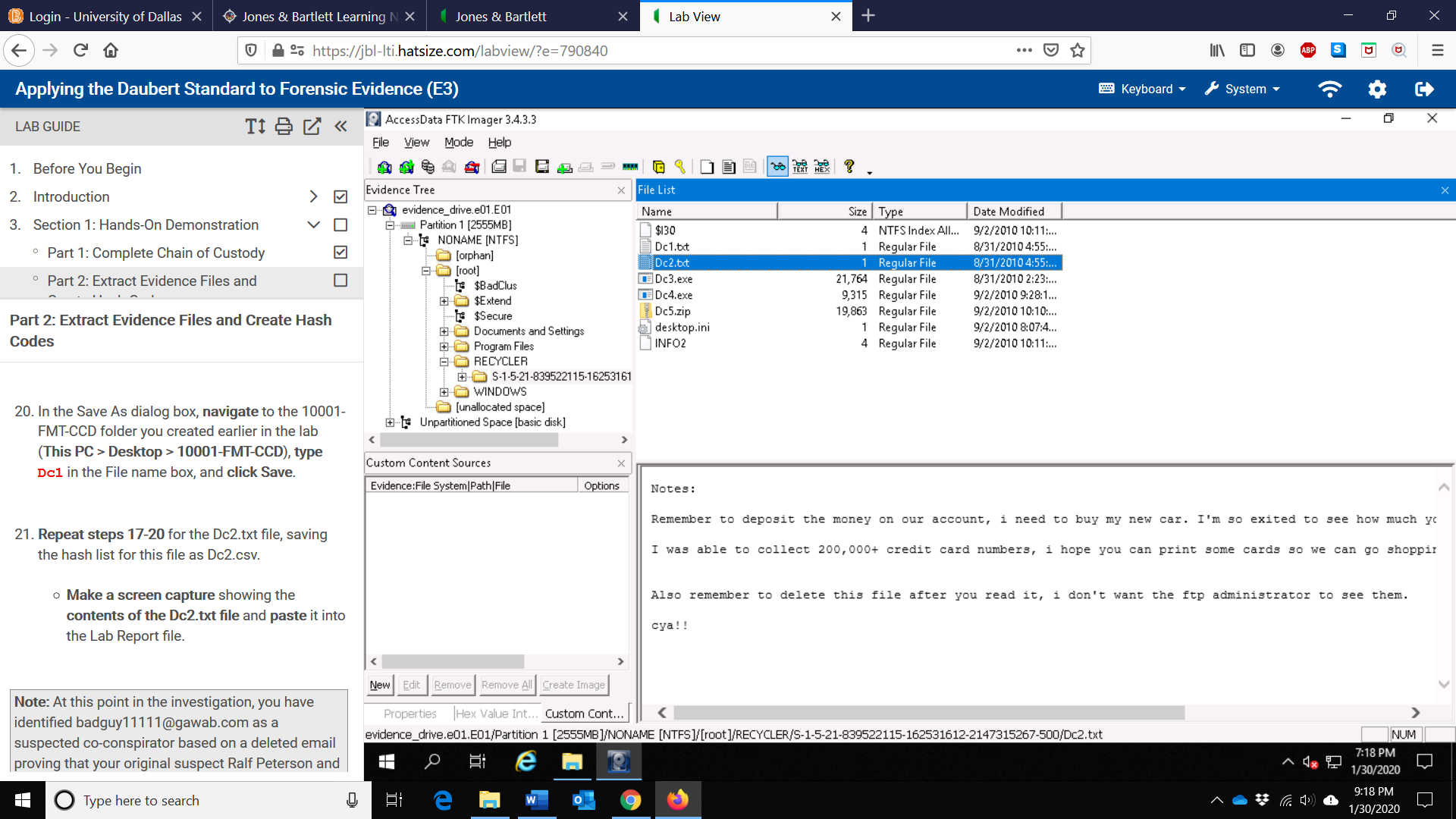
1. Make a screen capture showing the completed Chain of Custody form and paste it into the Lab Report file.



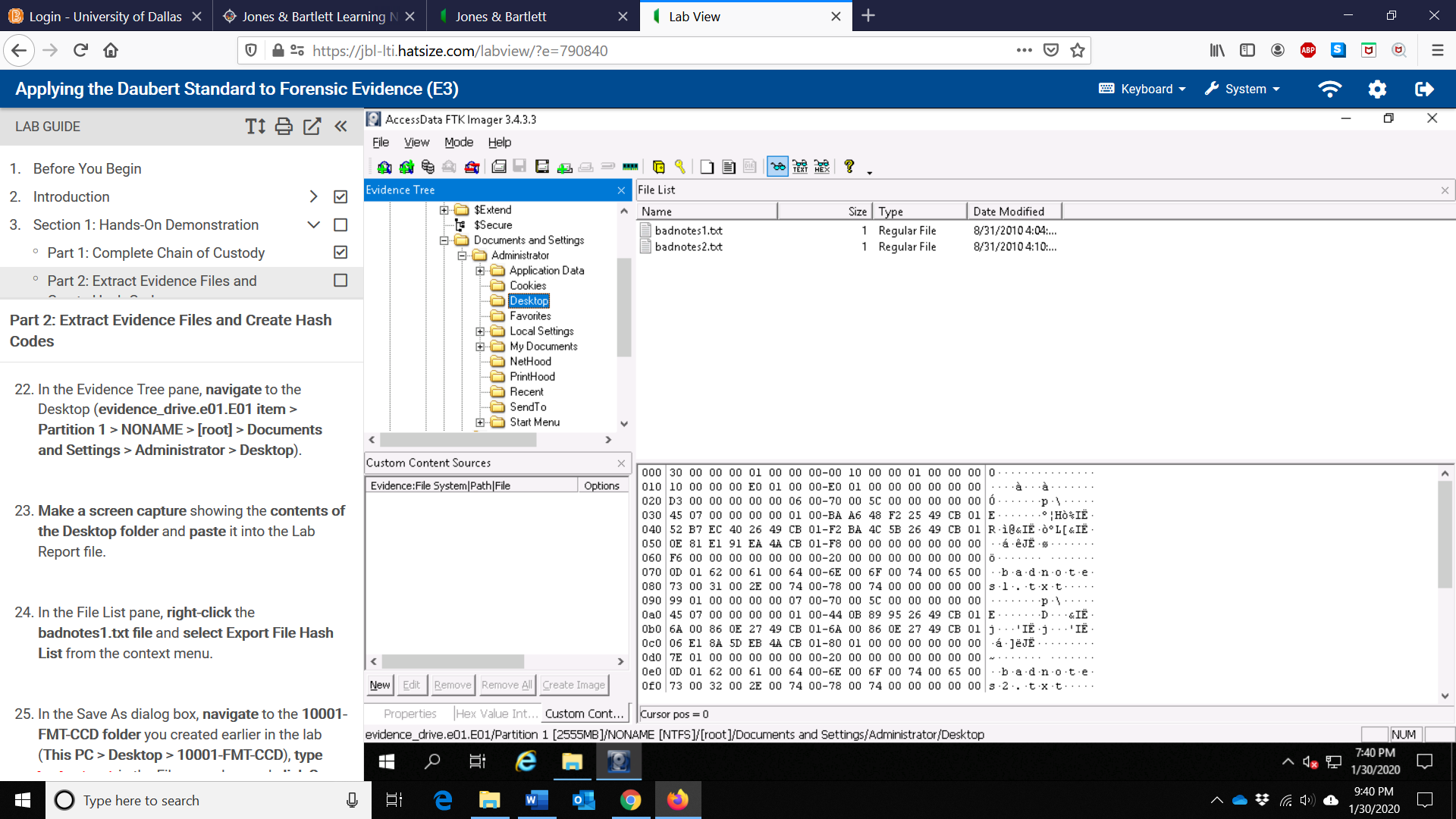
1. Make a screen capture showing the contents of the Dc1.txt file and paste it into the Lab Report file.



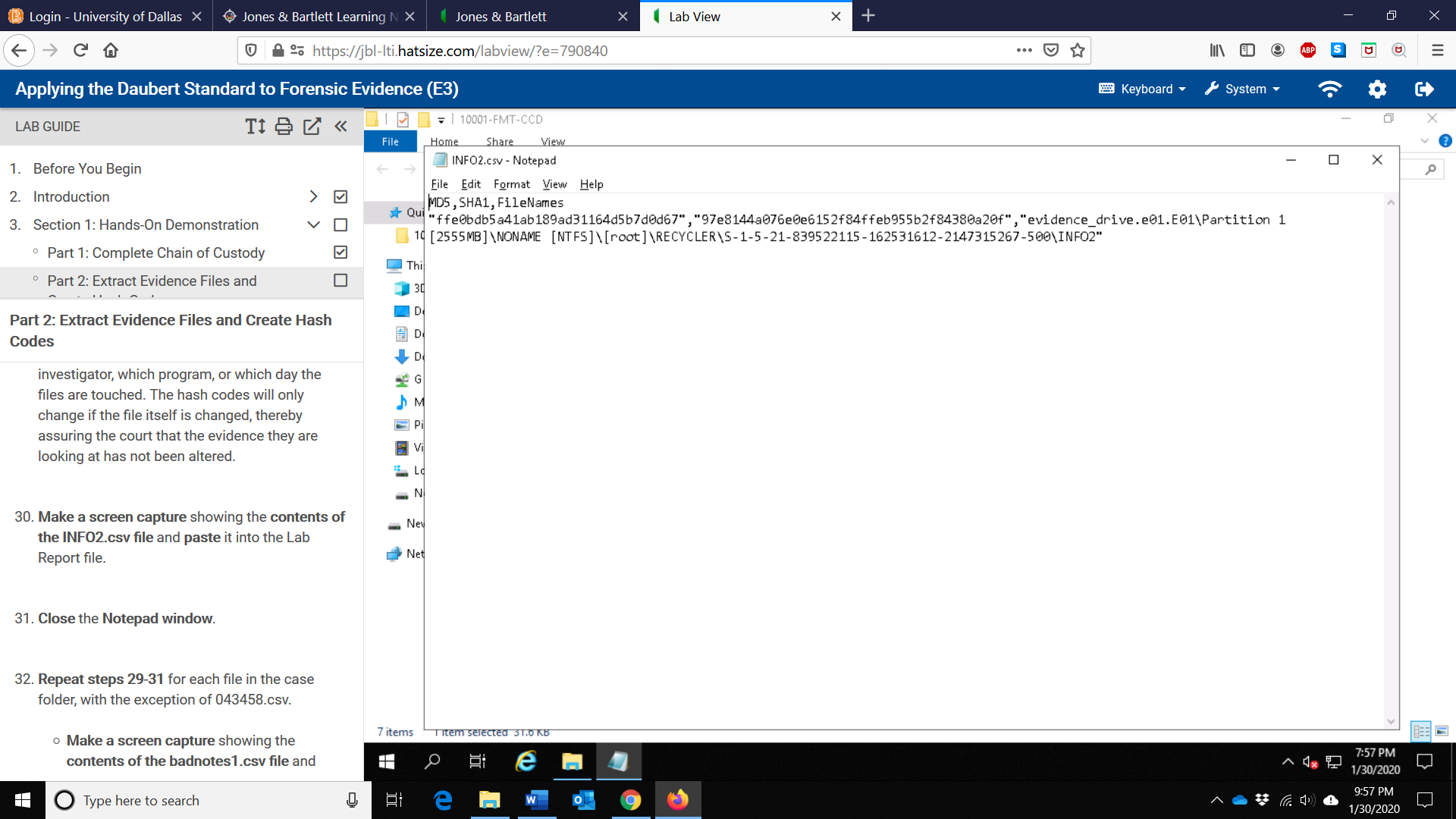
1. Make a screen capture showing the contents of the Dc2.txt file and paste it into the Lab Report file.



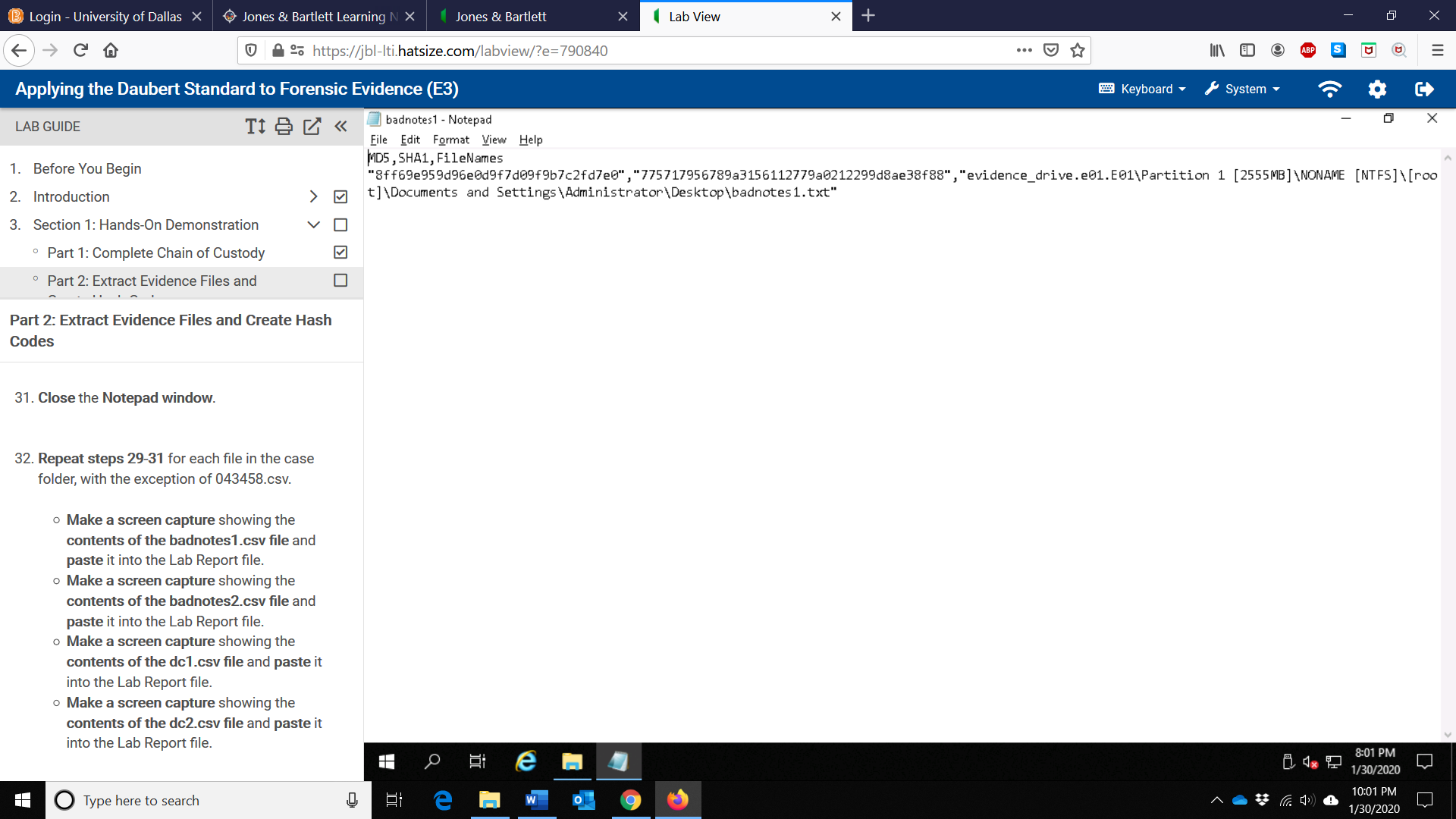
1. Make a screen capture showing the contents of the Desktop folder and paste it into the Lab Report file.



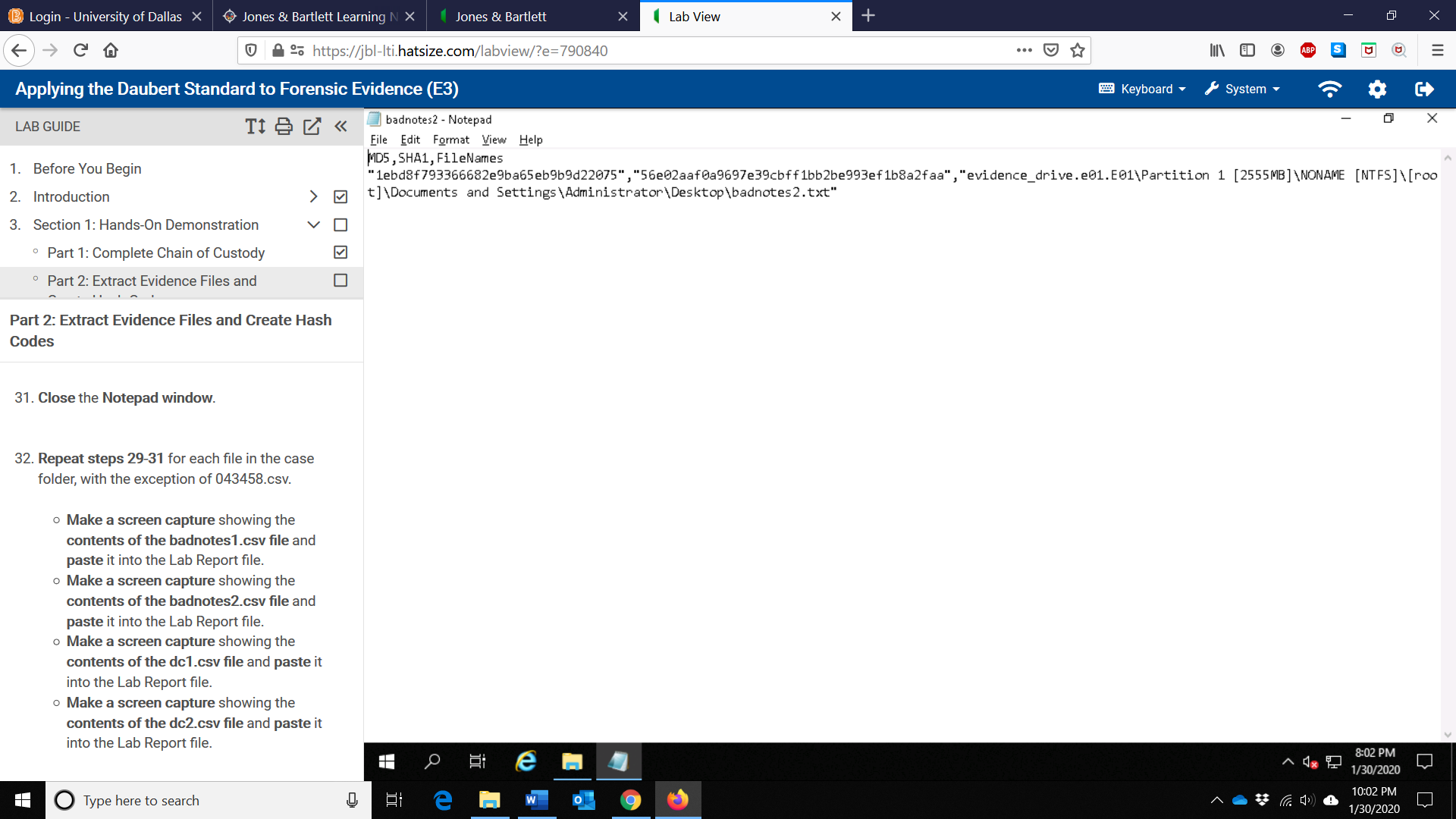
1. Make a screen capture showing the contents of the INFO2.csv file and paste it into the Lab Report file.



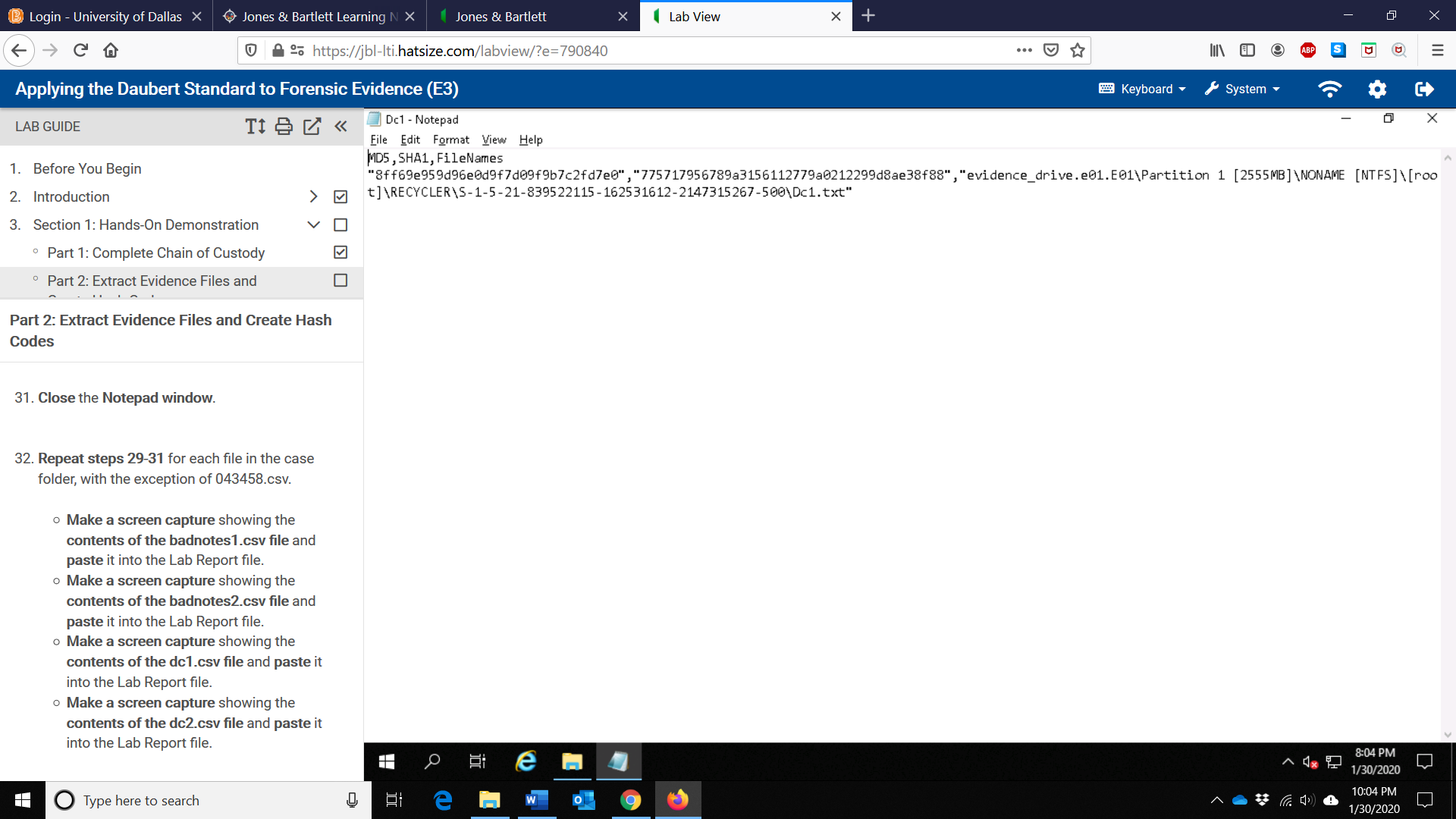
1. Make a screen capture showing the contents of the badnotes1.csv file and paste it into the Lab Report file.



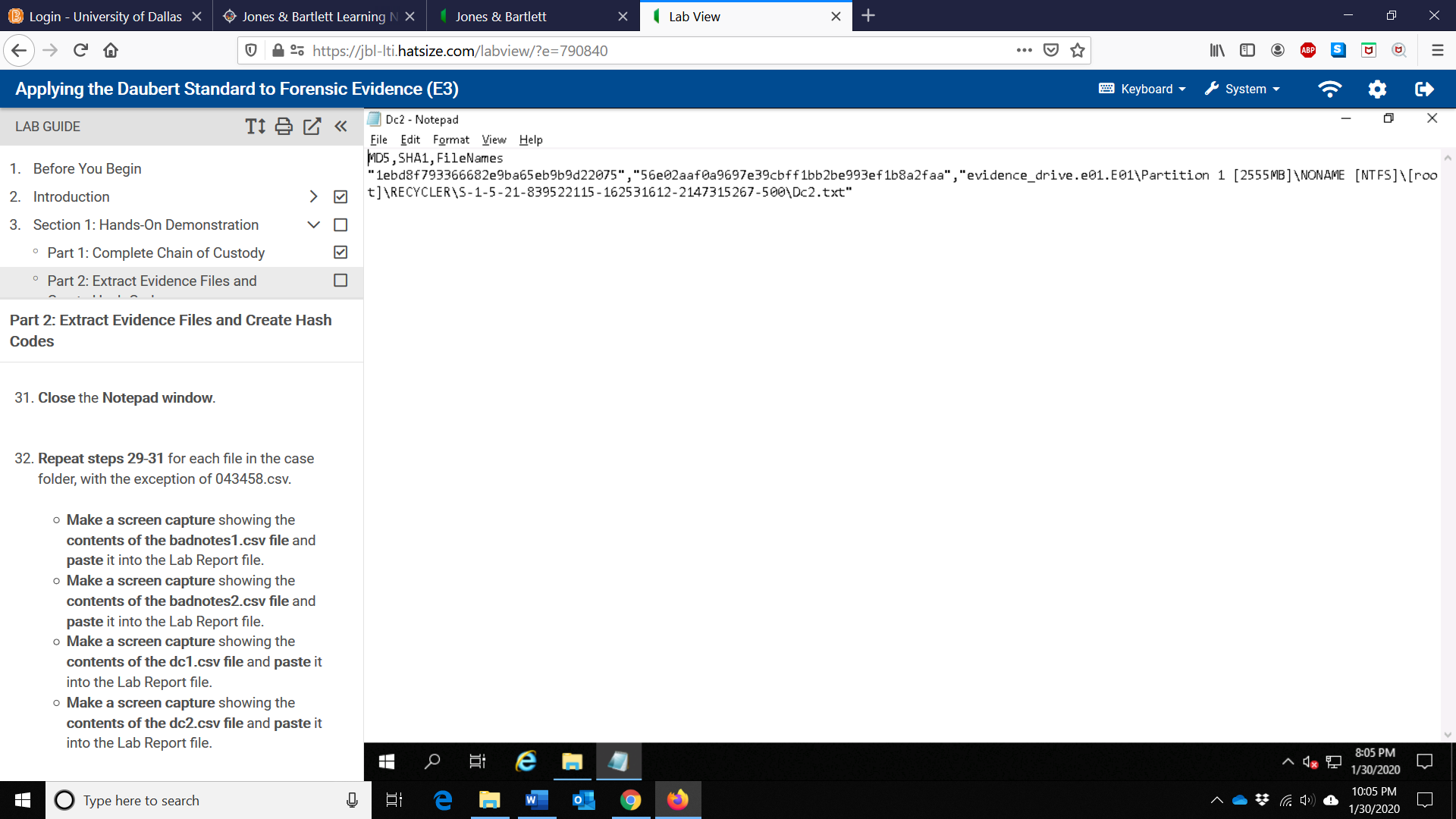
1. Make a screen capture showing the contents of the badnotes2.csv file and paste it into the Lab Report file.



1. Make a screen capture showing the contents of the dc1.csv file and paste it into the Lab Report file.

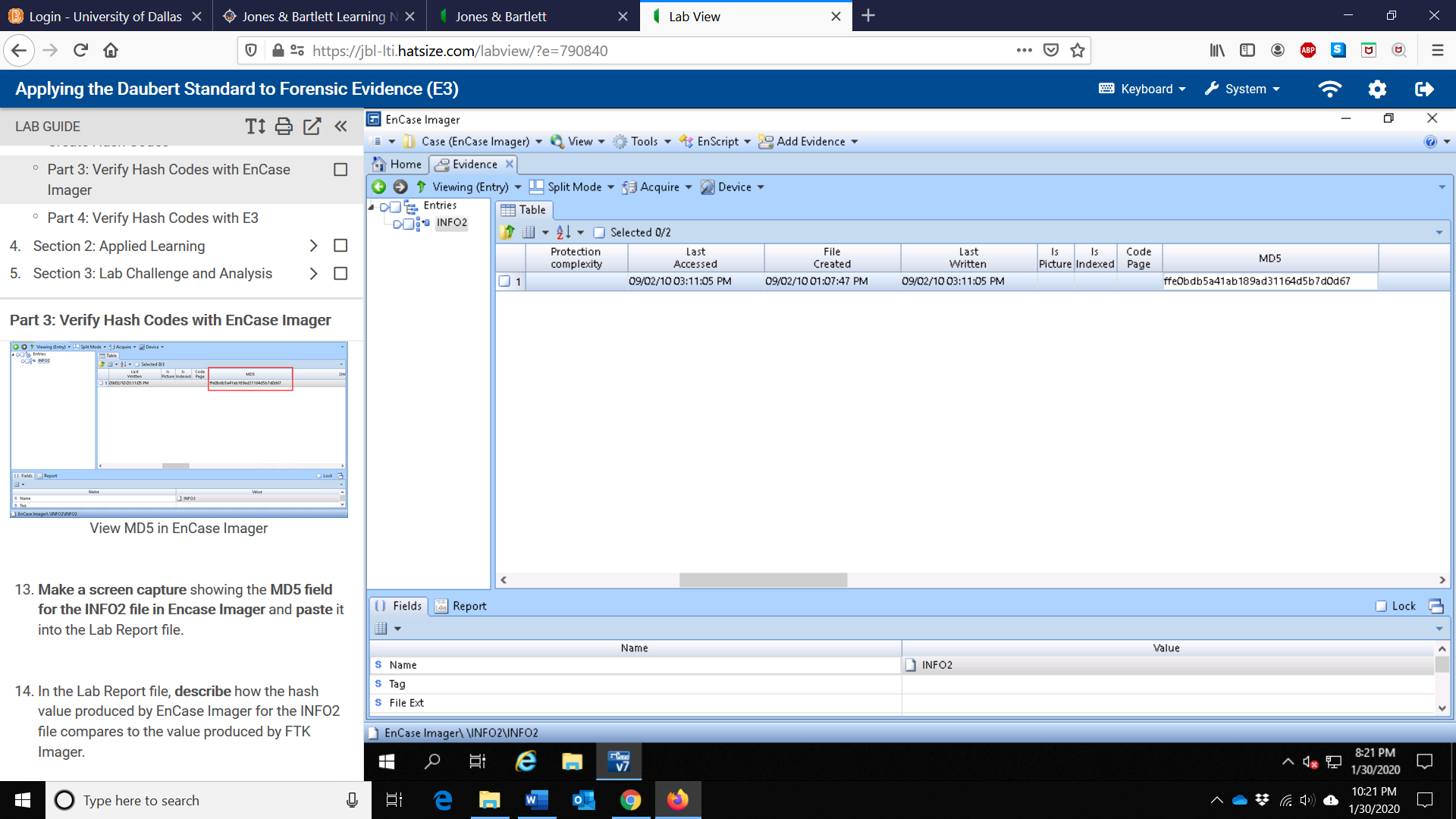


1. Make a screen capture showing the contents of the dc2.csv file and paste it into the Lab Report file.



1. Make a screen capture showing the MD5 field for the INFO2 file in Encase

Imager and paste it into the Lab Report file.



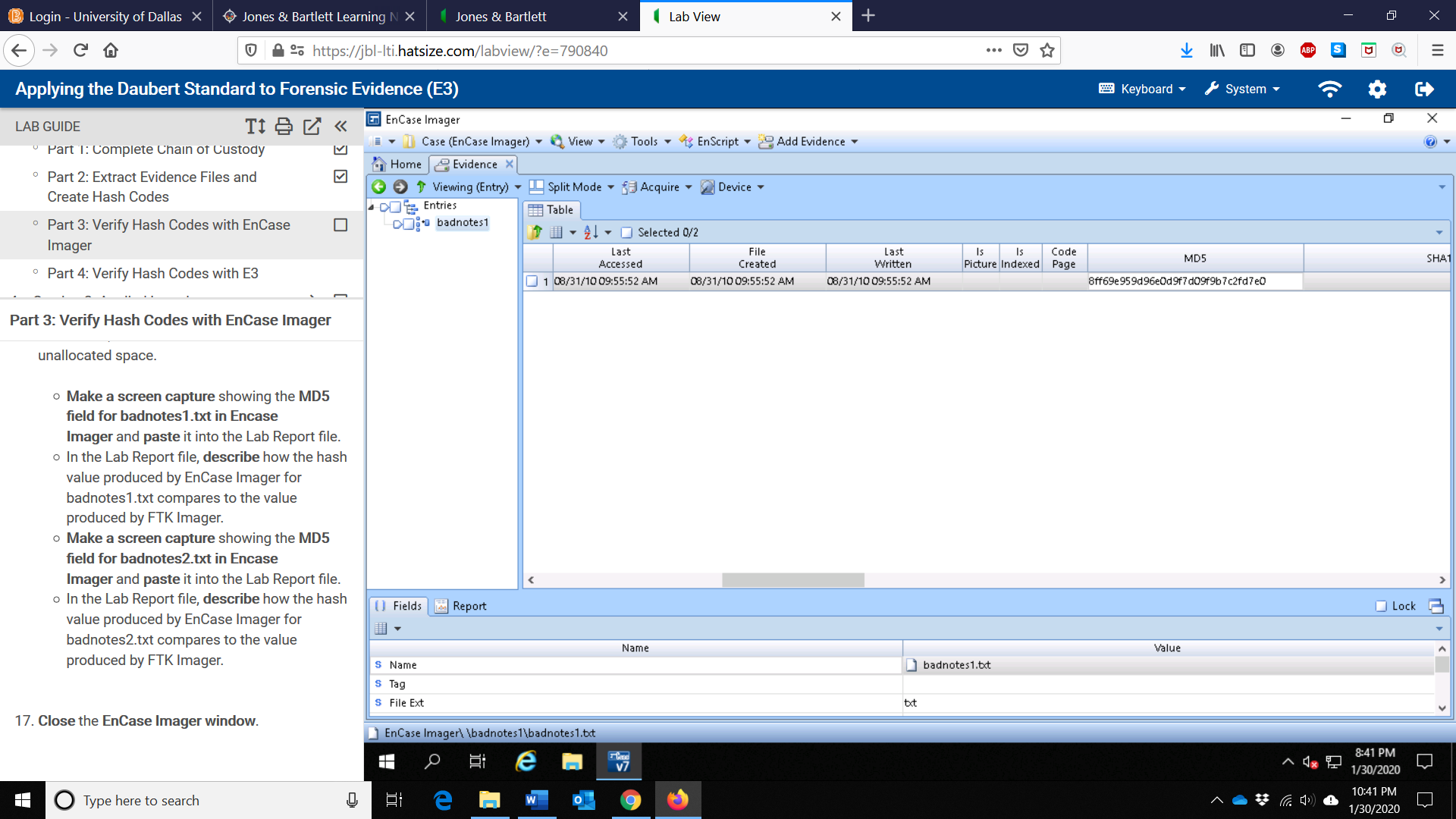
1. In the Lab Report file, describe how the hash value produced by the EnCase

Imager for the INFO2 file compares to the value produced by FTK Imager.

Comparing the MD5 hash value produced for the INFO2 file by the EnCase Imager and by FTK Imager, we can see that the hash value remains the same (ffe0bdb5a41ab189ad31164d5b7d0d67). This scenario also indicates that the files haven’t been altered and that no matter which investigator or which program we use, the hash code generated will remain the same. Furthermore, it also assures the court that the evidence they are looking at has not been changed.

1. Make a screen capture showing the MD5 field for the badnotes1.txt file in

Encase Imager and paste it into the Lab Report file.



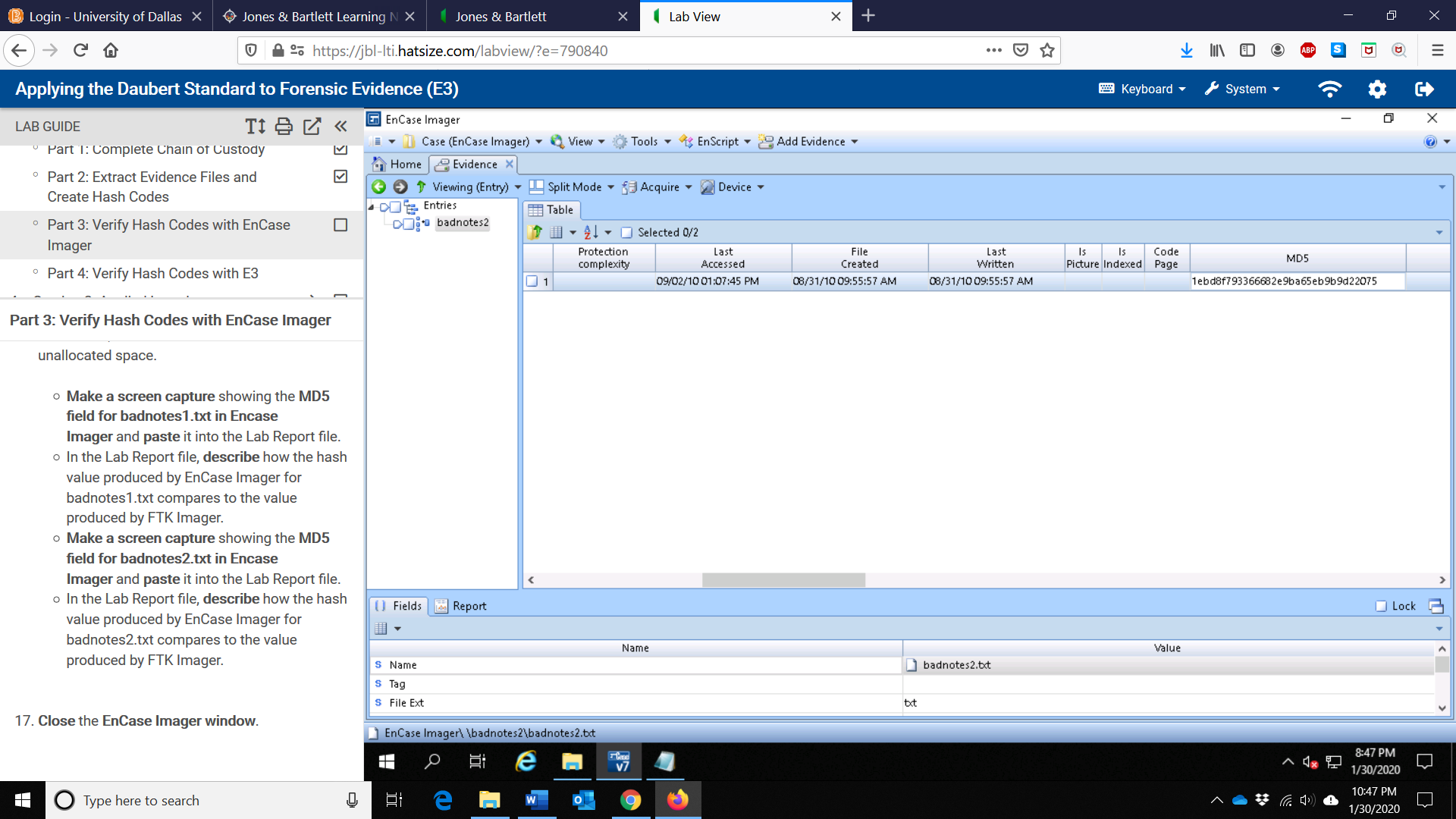
1. In the Lab Report file, describe how the hash value produced by the EnCase

Imager for the badnotes1.txt compares to the value produced by FTK Imager.

Comparing the MD5 hash value produced for the badnotes1.txt file by the EnCase Imager and by FTK Imager, we can see that the hash value remains the same (8ff69e959d96e0d9f7d09f9b7c2fd7e0). This scenario also indicates that the files haven’t been altered and that no matter which investigator or which program we use, the hash code generated will remain the same. Furthermore, it also assures the court that the evidence they are looking at has not been changed.

1. Make a screen capture showing the MD5 field for the badnotes2.txt file in

Encase Imager and paste it into the Lab Report file.

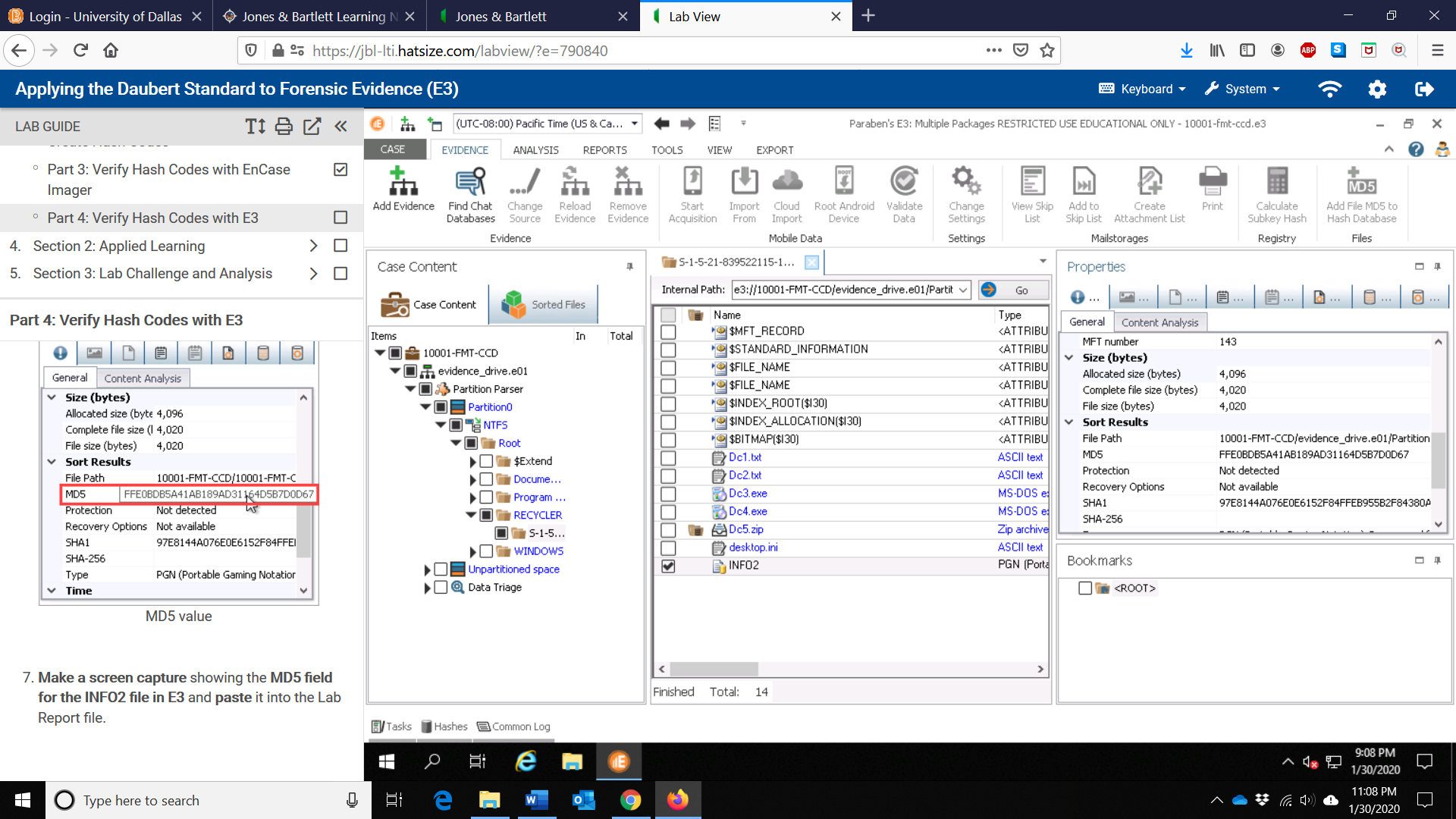


1. In the Lab Report file, describe how the hash value produced by the EnCase

Imager for the badnotes2.txt compares to the value produced by FTK Imager.

Comparing the MD5 hash value produced for the badnotes2.txt file by the EnCase imager and by FTK Imager, we can see that the hash value remains the same (1ebd8f793366682e9ba65eb9b9d22075). This scenario also indicates that the files haven’t been altered and that no matter which investigator or which program we use, the hash code generated will remain the same. Furthermore, it also assures the court that the evidence they are looking at has not been changed.

1. Make a screen capture showing the MD5 field for the INFO2 file in E3 and paste it into the Lab Report file.

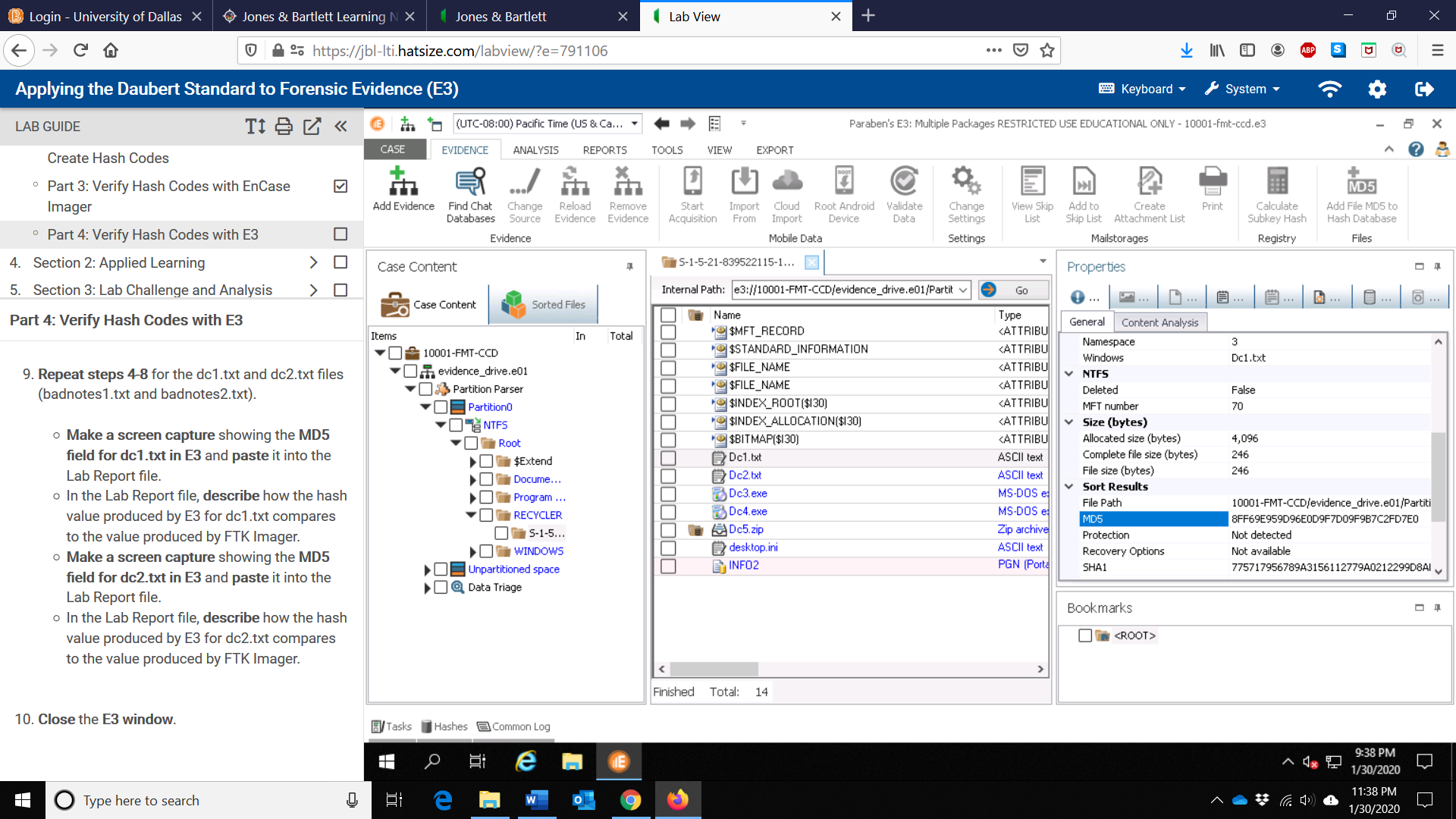


1. In the Lab Report file, describe how the hash value produced by E3 for the

INFO2 file compares to the value produce by FTK Imager.

Comparing the MD5 hash value produced for the INFO2 file by E3 and by FTK Imager, we can see that the hash value remains the same (ffe0bdb5a41ab189ad31164d5b7d0d67) since hexadecimal string output is case insensitive. This scenario also indicates that the files haven’t been altered and that no matter which investigator or which program we use, the hash code generated will remain the same. Furthermore, it also assures the court that the evidence they are looking at has not been changed.

1. Make a screen capture showing the MD5 field for dc1.txt in E3 and paste it into the Lab Report file.



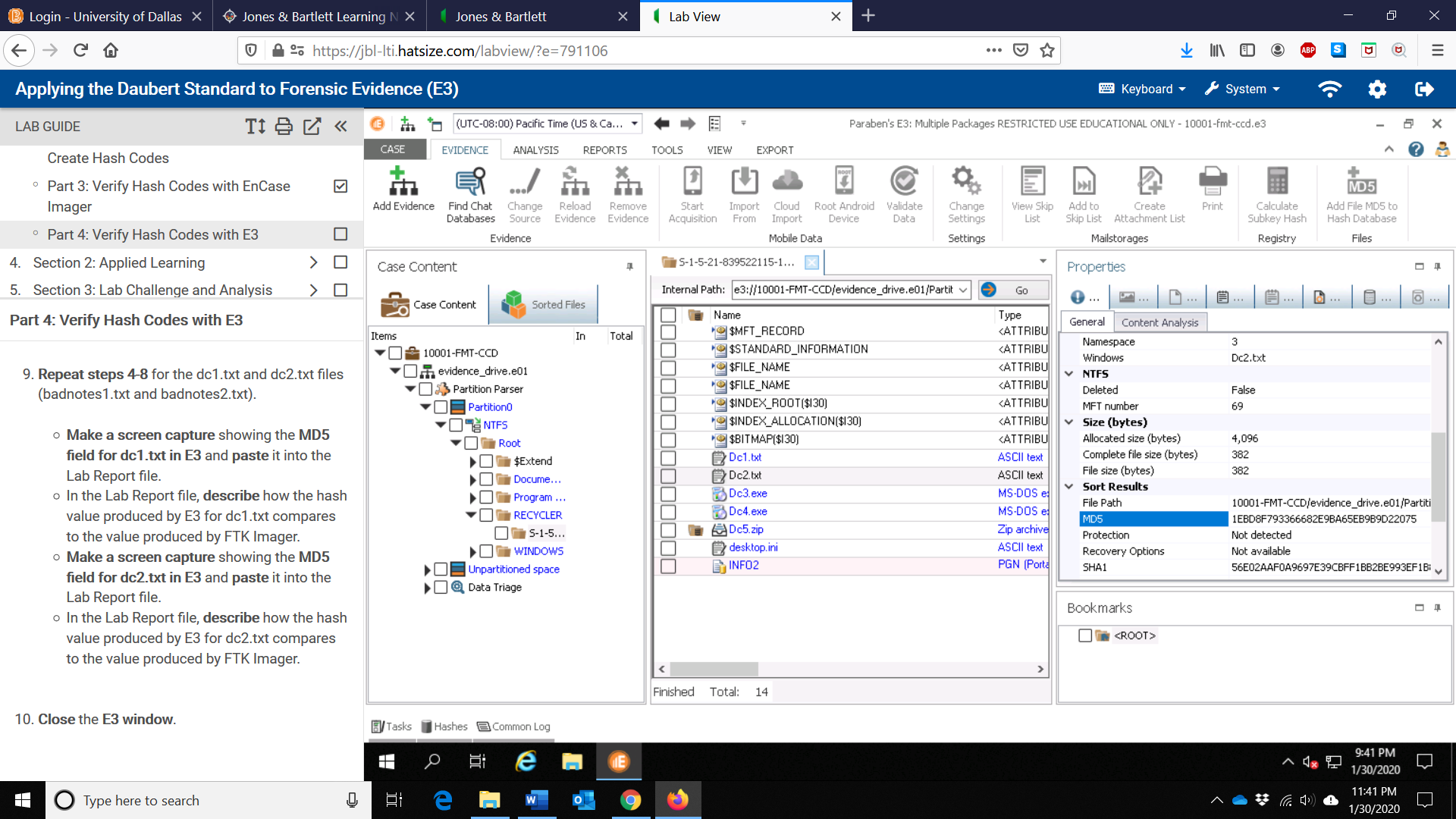
1. In the Lab Report file, describe how the hash value produced by E3 for dc1.txt

file compares to the value produce by FTK Imager.

Comparing the MD5 hash value produced for the dc1.txt file by the E3 and by FTK Imager, we can see that the hash value remains the same (8ff69e959d96e0d9f7d09f9b7c2fd7e0) since hexadecimal string output is case insensitive. This scenario also indicates that the files haven’t been altered and that no matter which investigator or which program we use, the hash code generated will remain the same. Furthermore, it also assures the court that the evidence they are looking at has not been changed.

1. Make a screen capture showing the MD5 field for dc2.txt in E3 and paste it into

the Lab Report file.



1. In the Lab Report file, describe how the hash value produced by E3 for dc2.txt file compares to the value produce by FTK Imager.

Comparing the MD5 hash value produced for the dc2.txt file by the E3 and by FTK Imager, we can see that the hash value remains the same (1ebd8f793366682e9ba65eb9b9d22075). since hexadecimal string output is case insensitive. This scenario also indicates that the files haven’t been altered and that no matter which investigator or which program we use, the hash code generated will remain the same. Furthermore, it also assures the court that the evidence they are looking at has not been changed.

**Lab #1 - Assessment Worksheet**

|  |
| --- |
| ***Lab Assessment Questions & Answers***  1. Why is the unallocated space of a Windows system so important to a forensic investigator?  In Windows system deleted files are not actually deleted. They are retained in the unallocated space on the hard drive. This is often a very evidence-rich area of the drive for a forensic investigator as deleted files always lead investigators to explore motives. |
| 2. From where were the badnotes1.txt and badnotes2.txt files recovered?  The badnotes1.txt and badnotes2.txt files deleted from the downloads folder were recovered form recyclers Dc1.txt and Dc2.txt respectively. |
| 3. What is the INFO2 file used for?  The INFO2 file is used for containing the original file name and location of the deleted files that are stored as Dcx in the Recycler.  4. How do you generate a hash file in FTK Imager?  To generate a hash file In FTK Imager, go to the File List pane, right-click the specific file you want and select the Export File Hash List from the context menu.  5. What was the MD5 hash value in 043458.csv, the deleted e-mail file?  The MD5 hash value in 043458.csv, the deleted e-mail file was 4d88b734fef2fc0ea51077c18e37cd20  6. What is the Daubert standard?  The Daubert standard is a legal standard that is key to forensics and used by a trial judge to make a preliminary assessment of whether an expert’s scientific testimony is based on reasoning or methodology that is scientifically valid and properly be to the facts at issue.  7. Why must a forensic investigator be familiar with emerging technologies?  A forensic investigator be familiar with emerging technologies because the Daubert standard requires that scientific evidence presented in court to be generally accepted. This scenario indicates that it is unlikely that new tools would be immediately approved for use in court. |