**Lab 7: Automating E-mail Evidence Discovery (E3)**

**By**

**Natnael Kebede**



**University of Dallas**

**2020**

This Paper Submitted in Partial Fulfillment of the Requirements for

CYBS 7359 – Digital Forensics

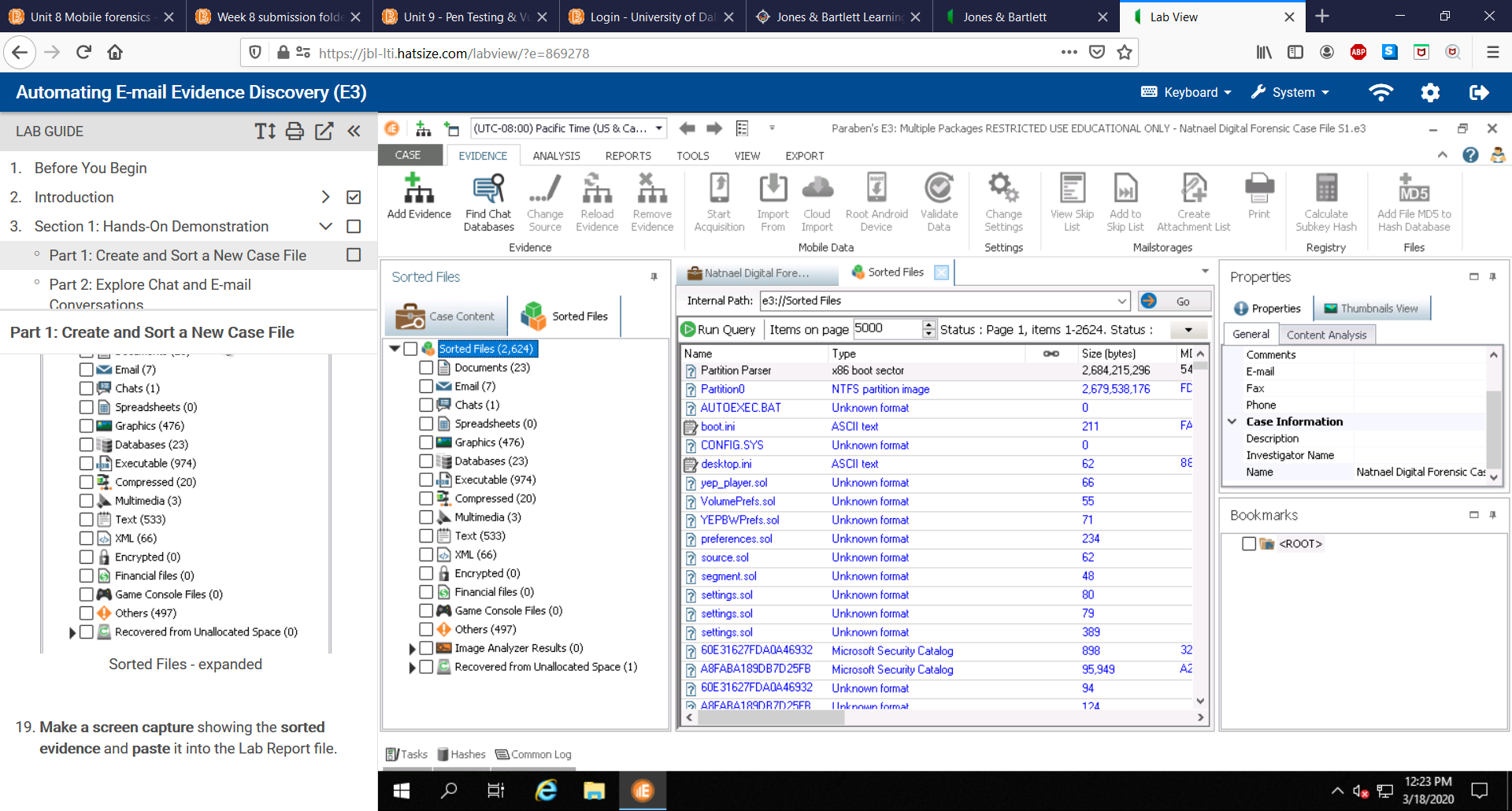
Spring 2020

Presented to Dr. Renita Murimi

**Section 1**

**Part 1**

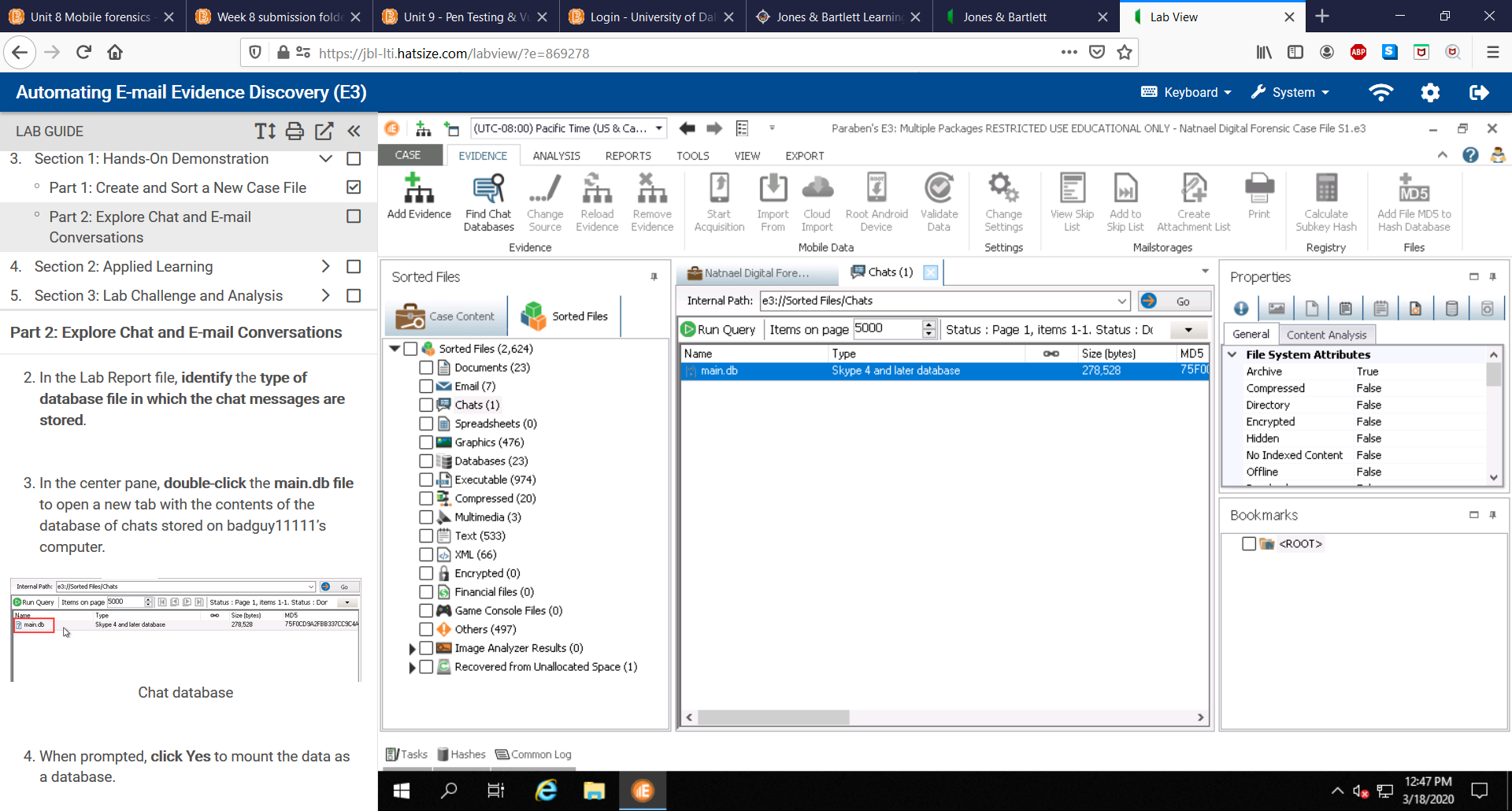
1. Make a screen capture showing the sorted evidence and paste it into the Lab Report file.



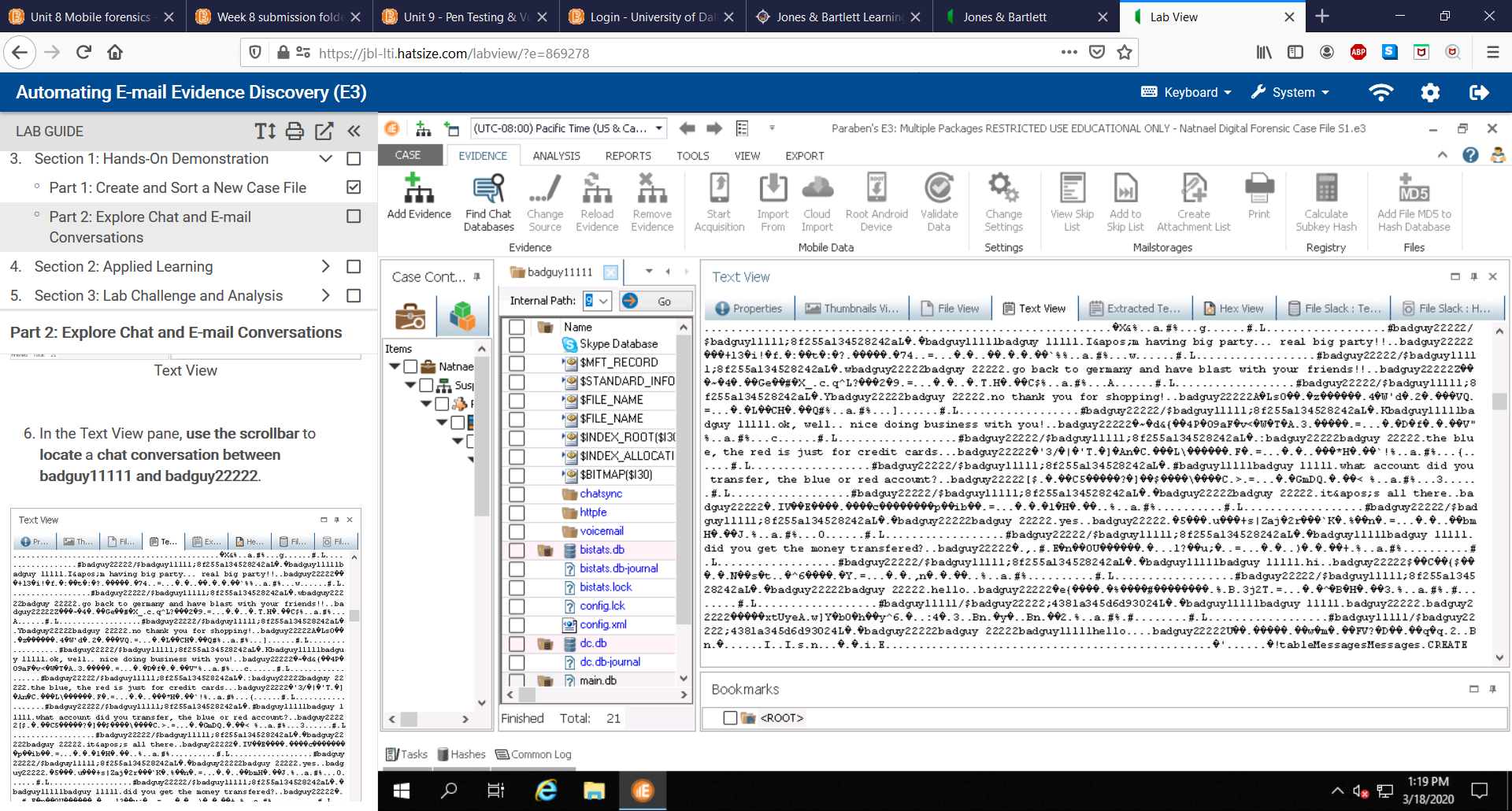
**Part 2**

1. In the Lab Report file, identify the type of database file in which chat messages are stored.

The type of database the chat messages are stored in is Skype 4 and later database as shown in the screenshot below.

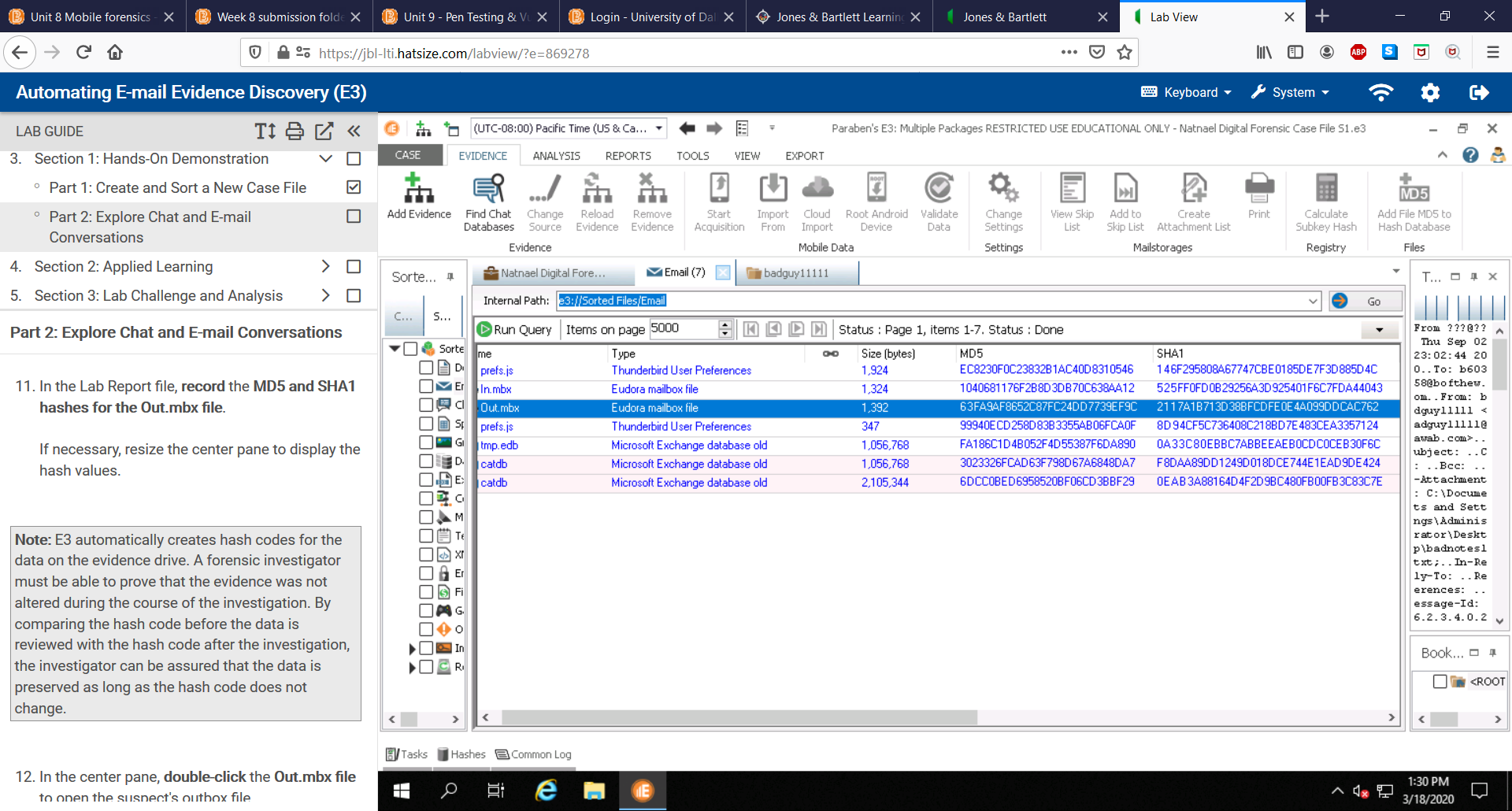


1. Make a screen capture showing the chat conversation and paste it into your Lab Report file.

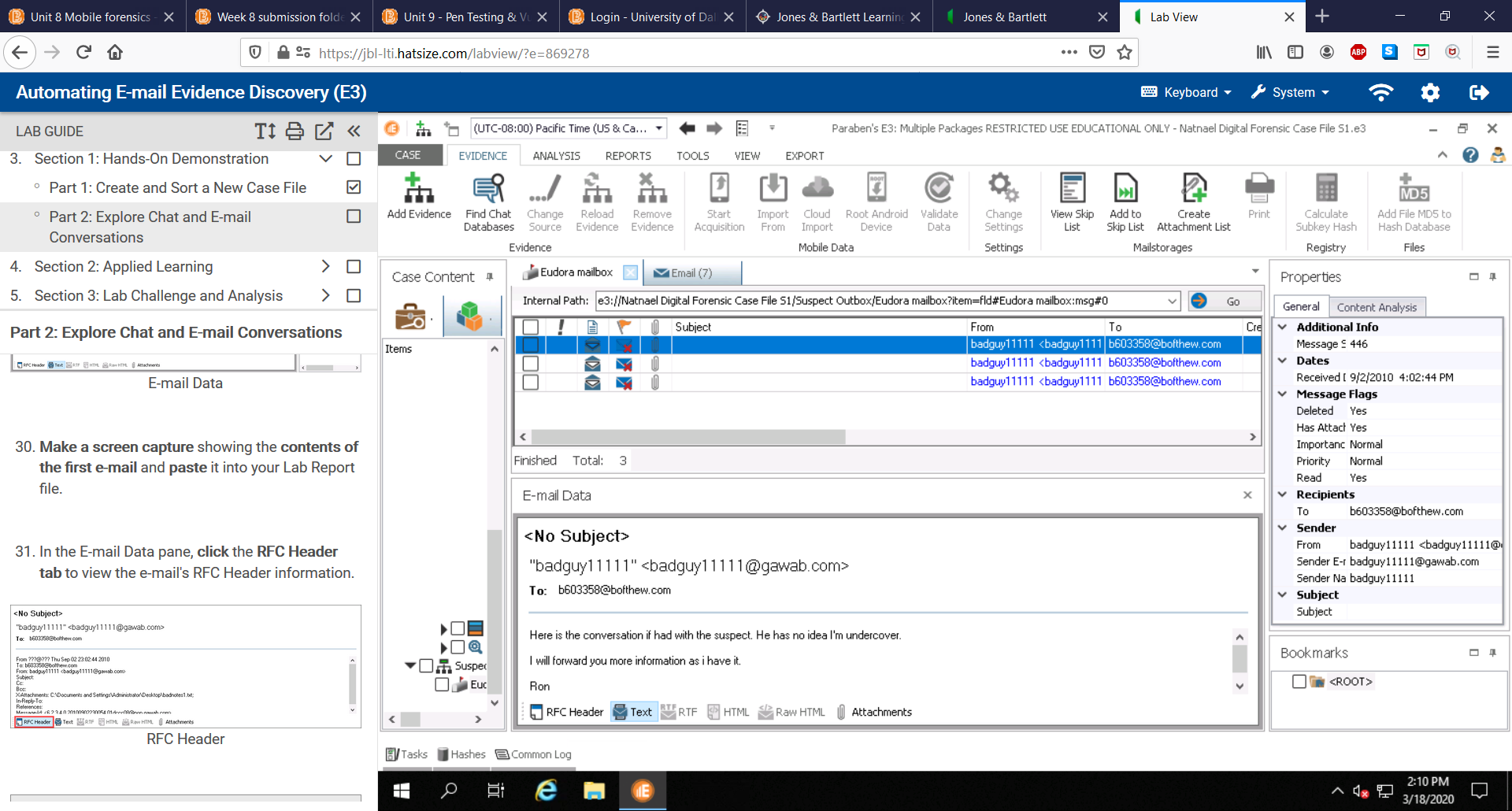


1. In the Lab Report file, record the MD5 and SHA1 hashes for the Out.mbx file.

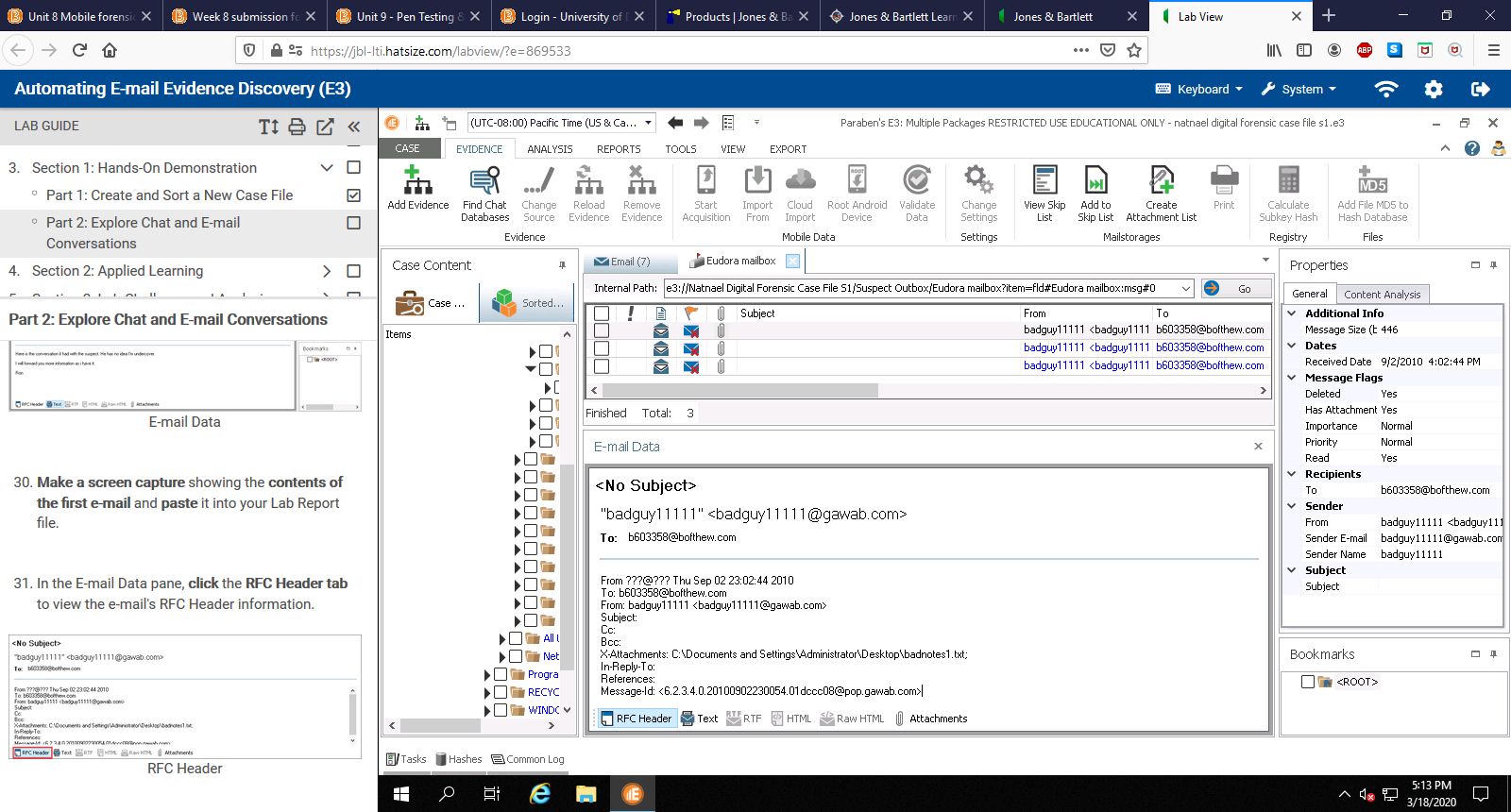
The MD5 and SHA1 hashes for the Out.mbx file is shown in the screenshot below.



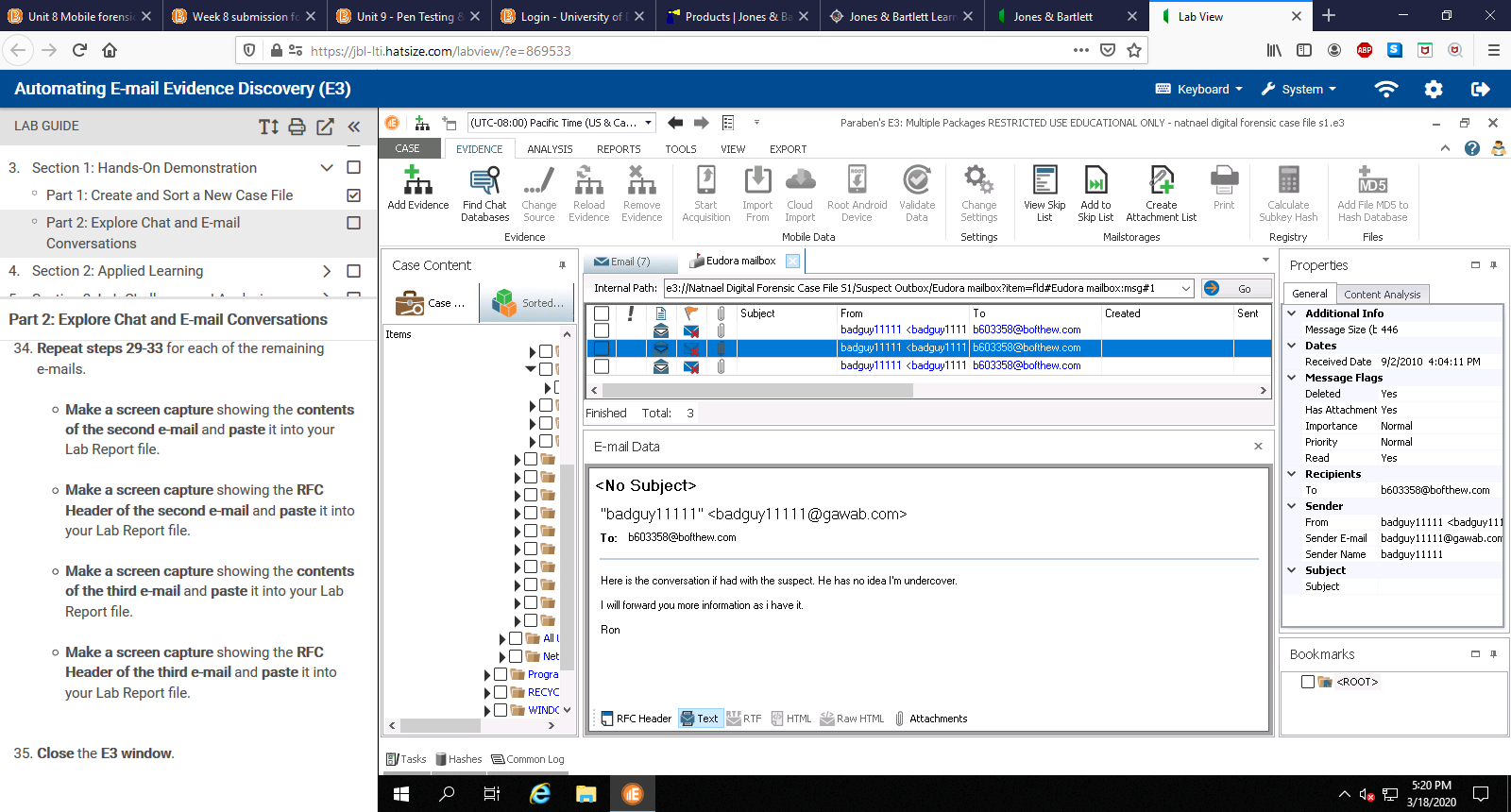
1. Make a screen capture showing the contents of the first email and paste it into your Lab Report file.



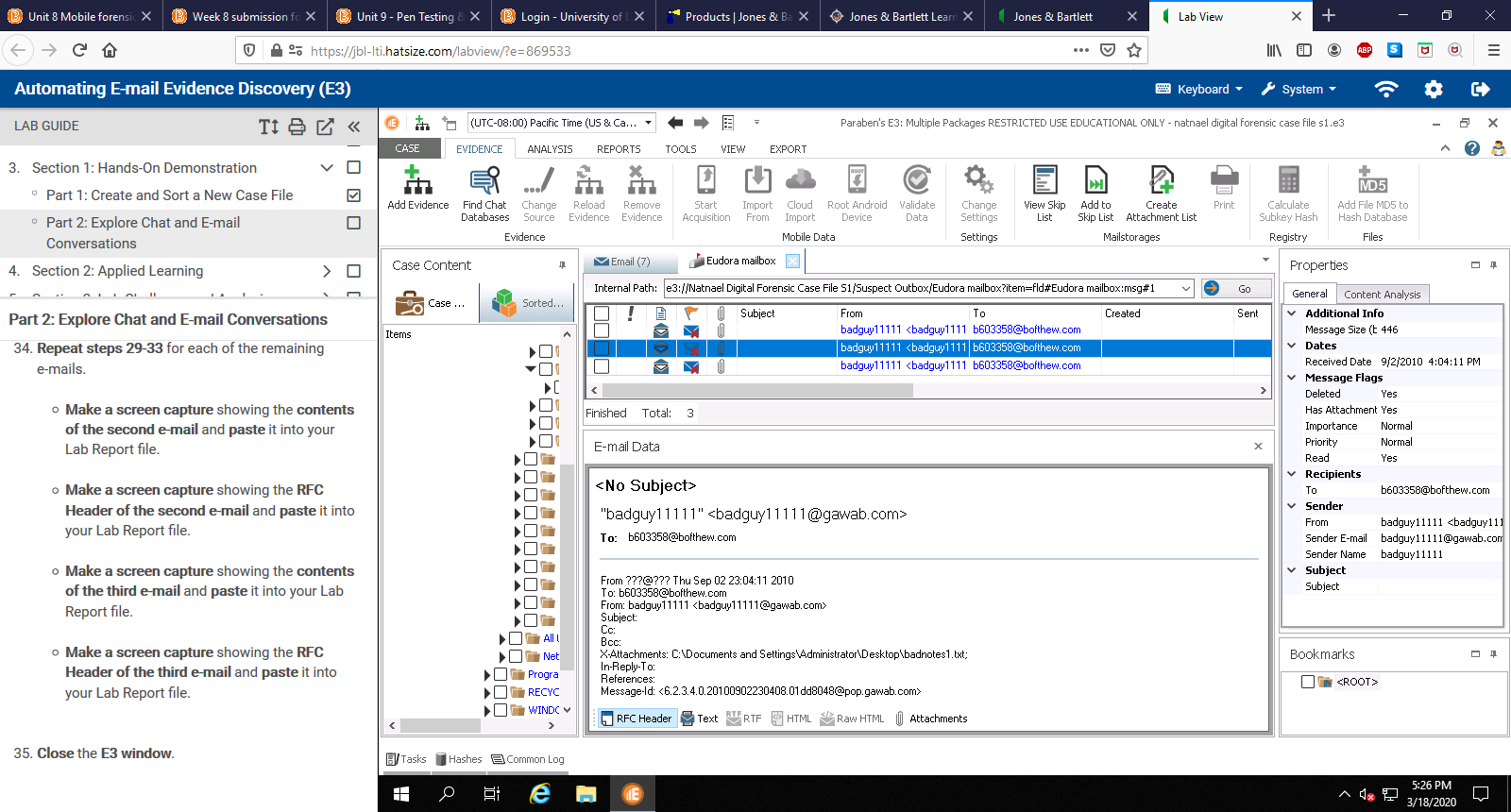
1. Make a screen capture showing the RFC Header of the first e-mail and paste it into your Lab Report file.



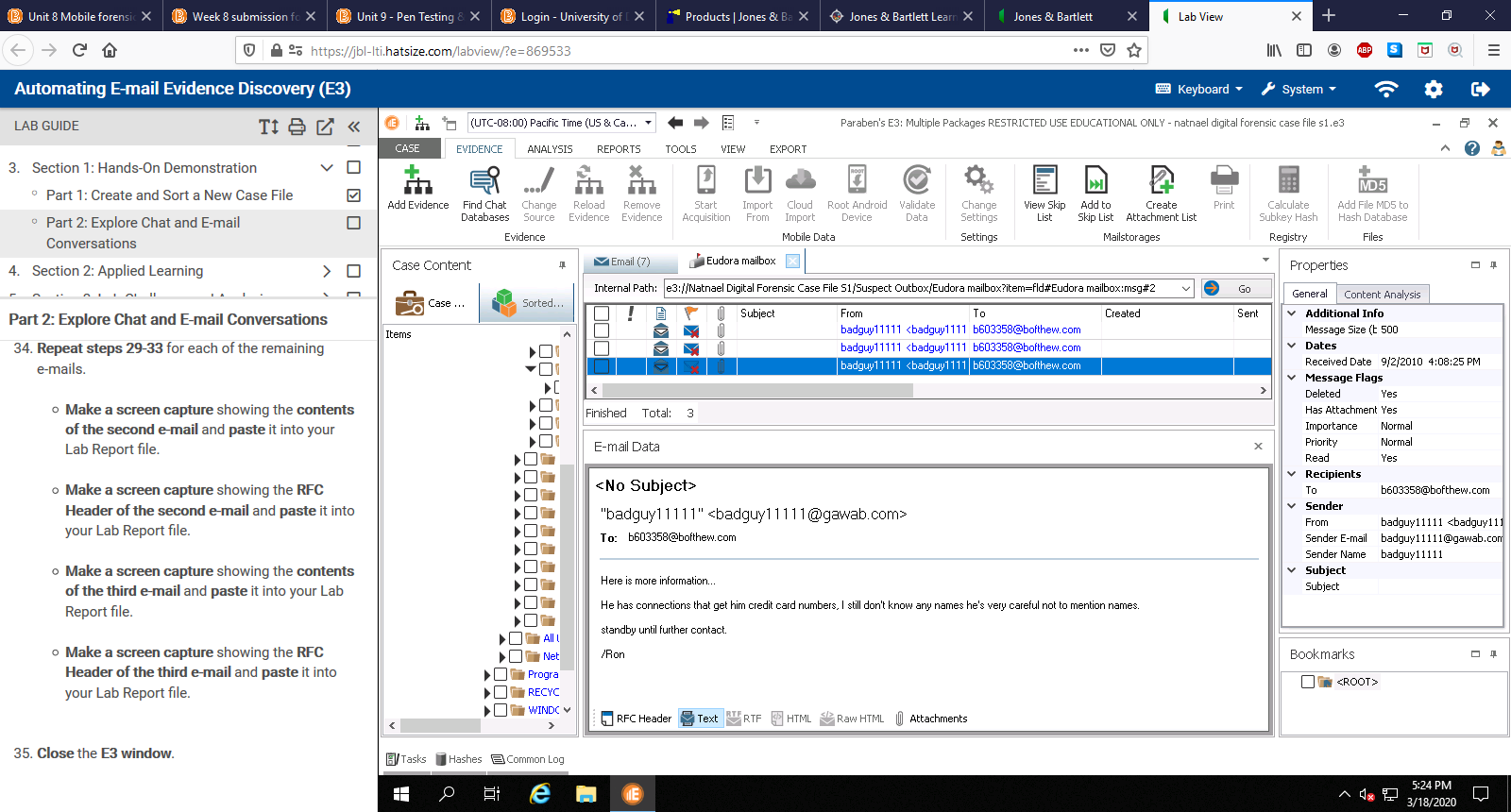
1. Make a screen capture showing the contents of the second email and paste it into your Lab Report file.



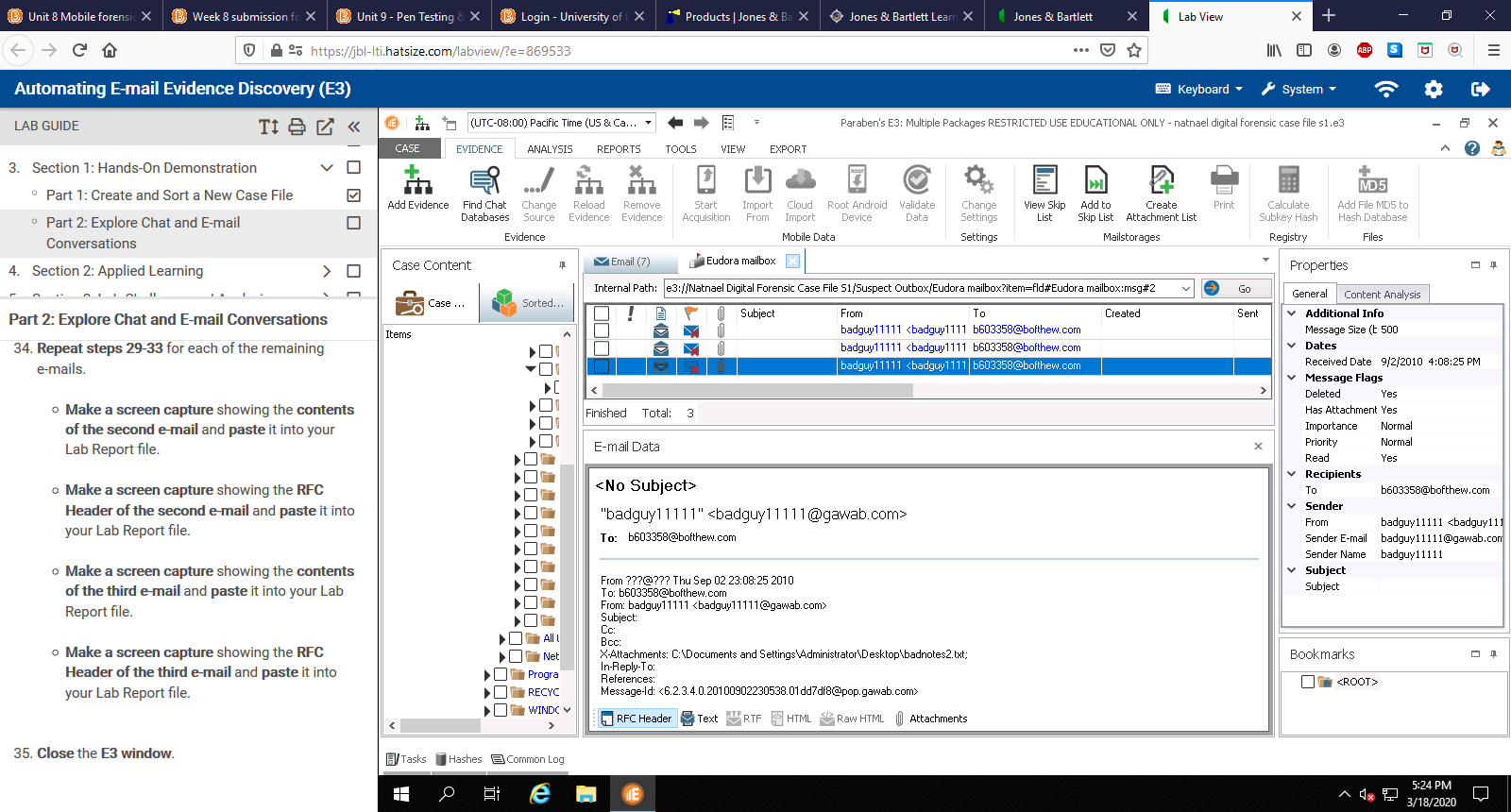
1. Make a screen capture showing the RFC Header of the second e-mail and paste it into your Lab Report file.



1. Make a screen capture showing the contents of the third email and paste it into your Lab Report file.



1. Make a screen capture showing the RFC Header of the third e-mail and paste it into your Lab Report file.



1. In the Lab Report document, compare the hash code with the MD5 value you recorded in step 11. Do they match?

Comparing the hash codes of these two as shown below, we can see that the values match. This indicates that the integrity of the data is still intact, and that chain of custody was kept.

