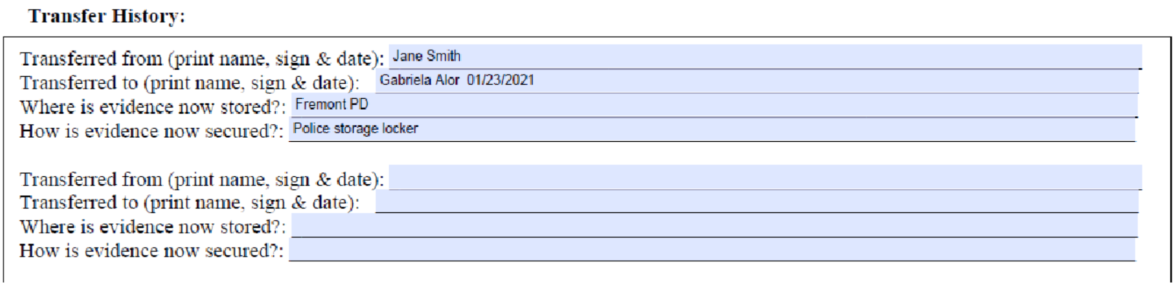
CIS4203.01 **Brandon Thompson**

Dr. Ashokkumar Patel Due: 1/24/21

Lab 1 Section 2: Applying the Daubert Standard



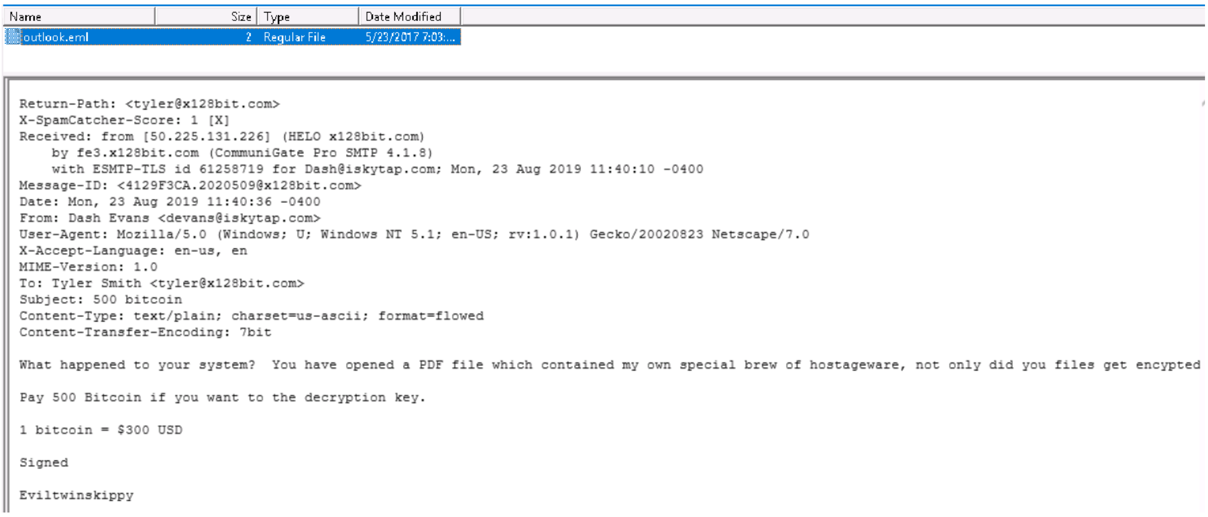
Transfer History:

Transferred from (print name, sign & date): Jane Smith
Transferred to (print name, sign & date): Gabriela Alor 01/23/2021
Where is evidence now stored?: Fremont PD
How is evidence now secured?: Police storage locker

Transferred from (print name, sign & date):
Transferred to (print name, sign & date):
Where is evidence now stored?:
How is evidence now secured?:

Figure 1: Chain of Custody PDF.

The chain of Custody file shows that we received evidence from Jane Smith on 1/23/2021 at the Fremont PD stored in a locker.

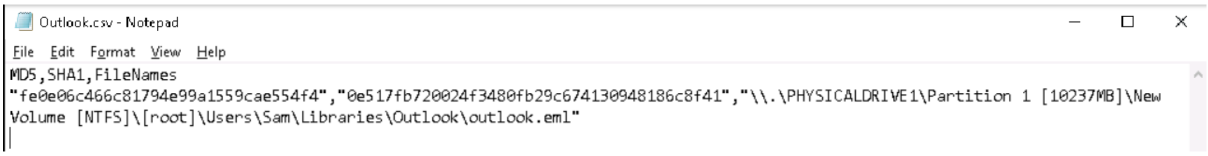


Name	Size	Type	Date Modified
outlook.eml	2	Regular File	5/23/2017 7:03:...

```
Return-Path: <tyler@x128bit.com>
X-SpamCatcher-Score: 1 [X]
Received: from [50.225.131.226] (HELO x128bit.com)
    by fe3.x128bit.com (CommuniGate Pro SMTP 4.1.8)
    with ESMTP-TLS id 61258719 for Dash@iskytap.com; Mon, 23 Aug 2019 11:40:10 -0400
Message-ID: <4129F3CA.2020509@x128bit.com>
Date: Mon, 23 Aug 2019 11:40:36 -0400
From: Dash Evans <devans@iskytap.com>
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.1) Gecko/20020823 Netscape/7.0
X-Accept-Language: en-us, en
MIME-Version: 1.0
To: Tyler Smith <tyler@x128bit.com>
Subject: 500 bitcoin
Content-Type: text/plain; charset=us-ascii; format=flowed
Content-Transfer-Encoding: 7bit

What happened to your system?  You have opened a PDF file which contained my own special brew of hostageware, not only did you files get encypted

Pay 500 Bitcoin if you want to the decryption key.

1 bitcoin = $300 USD

Signed

Eviltwinskippy
```

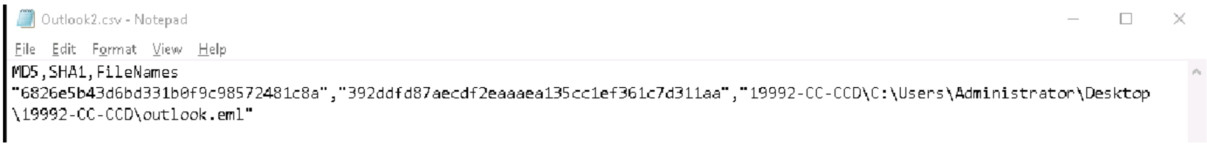
Figure 2: Contents of incriminating email.

The email shows extortion using ransomware to encrypt files, with the exchange of bitcoins for the decryption key.



```
MD5,SHA1,FileNames
"fe0e06c466c81794e99a1559cae554f4","0e517fb720024f3480fb29c674130948186c8f41","\\.\PHYSICALDRIVE1\Partition 1 [10237MB]\New
Volume [NTFS]\[root]\Users\Sam\Libraries\Outlook\outlook.eml"
```

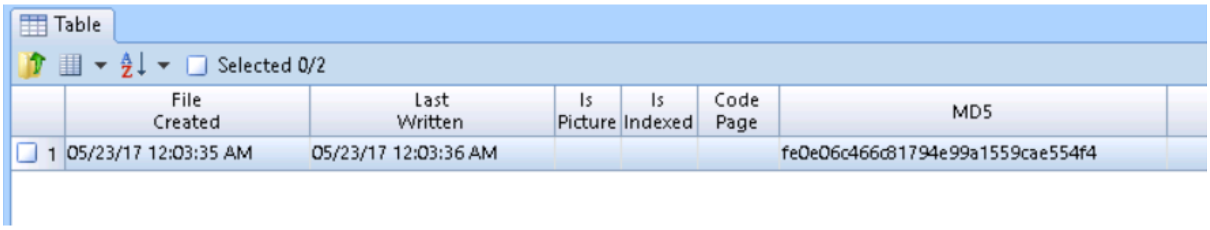
Figure 3: Hash value of the original Outlook file.



```
MD5,SHA1,FileNames
"6826e5b43d6bd331b0f9c98572481c8a","392ddfd87aecdf2eaaaea135cc1ef361c7d311aa","19992-CC-CCD\C:\Users\Administrator\Desktop
\19992-CC-CCD\outlook.eml"
```

Figure 4: Hash value of the altered Outlook file.

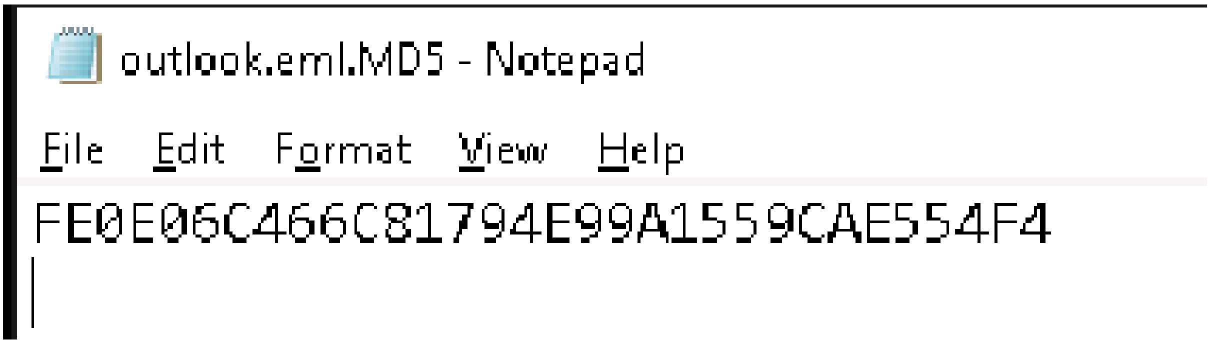
The hash values of these two files are different. This indicates that the contents of these files are not the same.



	File Created	Last Written	Is Picture	Is Indexed	Code Page	MD5
□ 1	05/23/17 12:03:35 AM	05/23/17 12:03:36 AM				fe0e06c466c81794e99a1559cae554f4

Figure 5: EnCase MD5 hash value for the Outlook file.

14. Question: Describe how the hash value produced by EnCase Imager compares to the values produced by FTK Imager for the two Outlook files.
The EnCase MD5 hash value is the same as the MD5 produced by FTK Imager for the original Outlook file.



```
FE0E06C466C81794E99A1559CAE554F4
```

Figure 6: E3 MD5 hash value for the Outlook file.

8. Question: Describe how the hash value produced by E3 compares to the values produced by FTK Imager for the two Outlook files and the value produced by EnCase.
The hash produced by E3 is the same as the hash produced by FTK Imager for the first Outlook file and the MD5 generated by EnCase.

In this lab we learned about how warrants are issued and the documentation of chain of custody to track who handles evidence. We used three different evidence viewing programs, FTK Imager, Encase Imager and E3 to view evidence data and generate hash values. Data can be pulled from many sources, including unallocated space on physical drives. Because this unallocated space is used to store deleted files, this is typically a good place to check for evidence. Hash values are used to validate that the evidence was not altered during the extraction process. The Daubert standard states that the evidence files gathered were not altered by the forensic process. In this case the hash of the original email matches the final hash generated, whereas the hash of the altered email is different.