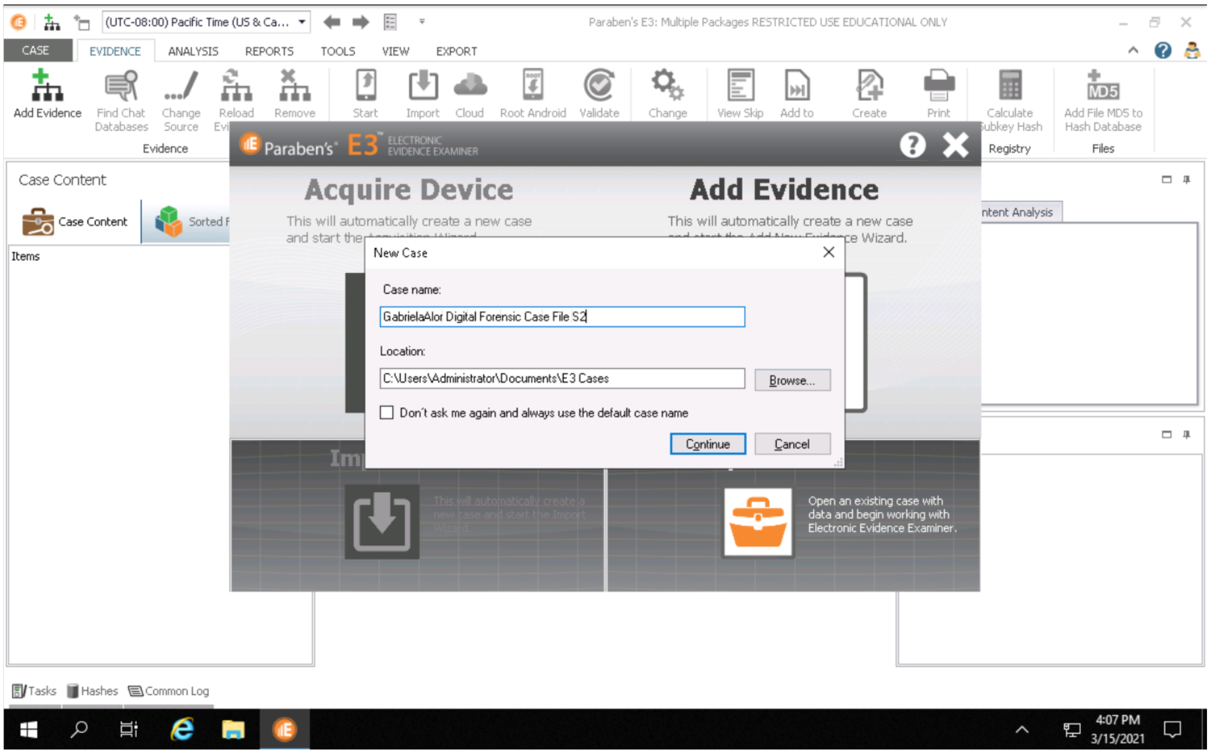
CIS4203.01 **Brandon Thompson**

Dr. Ashokkumar Patel Due: 2/23//21

Lab 6: Automated E-Mail Evidence Discovery

In this lab we will use Paraben's E3 tool to load and sort digital evidence to view suspicious chats and email messages.

Part 1: Create and Sort a New Case File


(UTC-08:00) Pacific Time (US & Ca...
Paraben's E3: Multiple Packages RESTRICTED USE EDUCATIONAL ONLY
CASE
EVIDENCE
ANALYSIS
REPORTS
TOOLS
VIEW
EXPORT
Add Evidence
Find Chat Databases
Change Source
Reload Evi
Remove
Start
Import
Cloud
Root Android
Validate
Change
View Skip
Add to
Create
Print
Calculate Subkey Hash
Add File MD5 to Hash Database
Evidence
Registry
Files
Case Content
Case Content
Sorted F
Items
ntent Analysis
Paraben's E3 ELECTRONIC EVIDENCE EXAMINER
Acquire Device
This will automatically create a new case and start the Acquisition Wizard.
Add Evidence
This will automatically create a new case and start the Add New Evidence Wizard.
Im
This will automatically create a new case and start the Import Wizard.
Open an existing case with data and begin working with Electronic Evidence Examiner.
Tasks
Hashes
Common Log
4:07 PM
3/15/2021

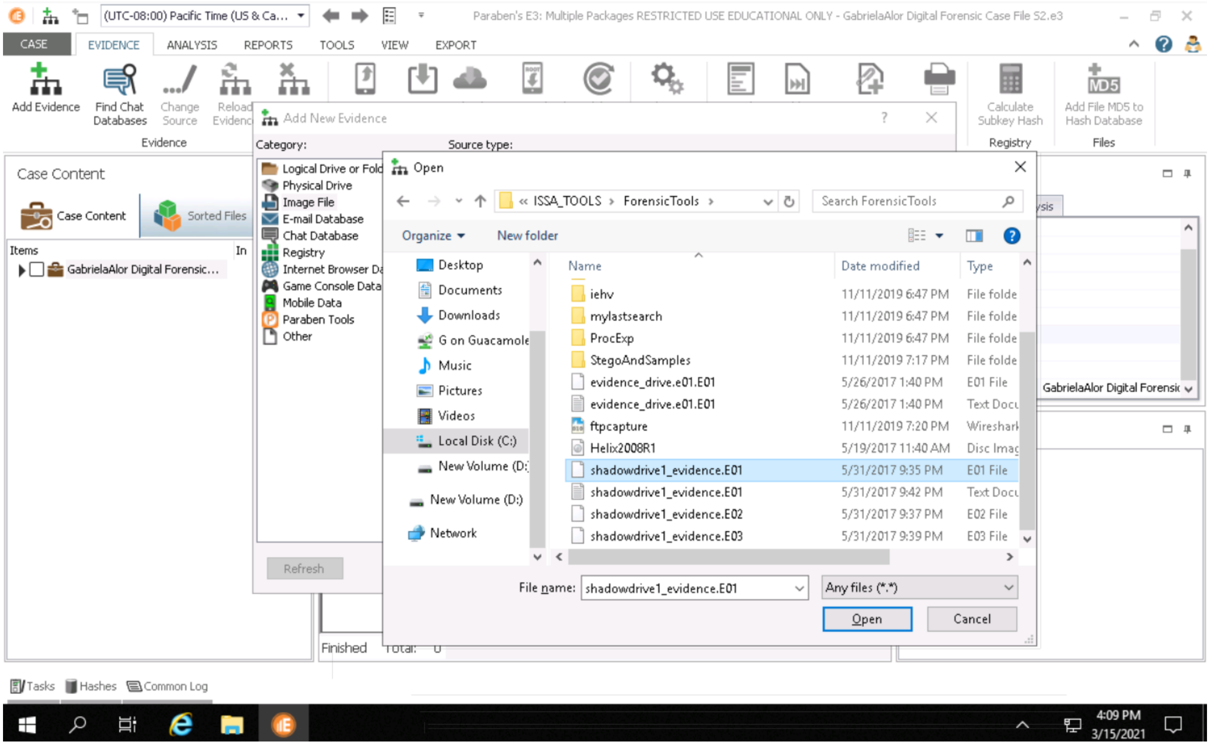
New Case

Case name: GabrielaAlor Digital Forensic Case File S2

Location: C:\Users\Administrator\Documents\E3 Cases

□ Don't ask me again and always use the default case name

Figure 1: Creation of evidence file.



Paraben's E3: Multiple Packages RESTRICTED USE EDUCATIONAL ONLY - GabrielaAlor Digital Forensic Case File 52.e3

GabrielaAlor Digital Forensic...

« ISSA_TOOLS › ForensicTools ›

Search ForensicTools

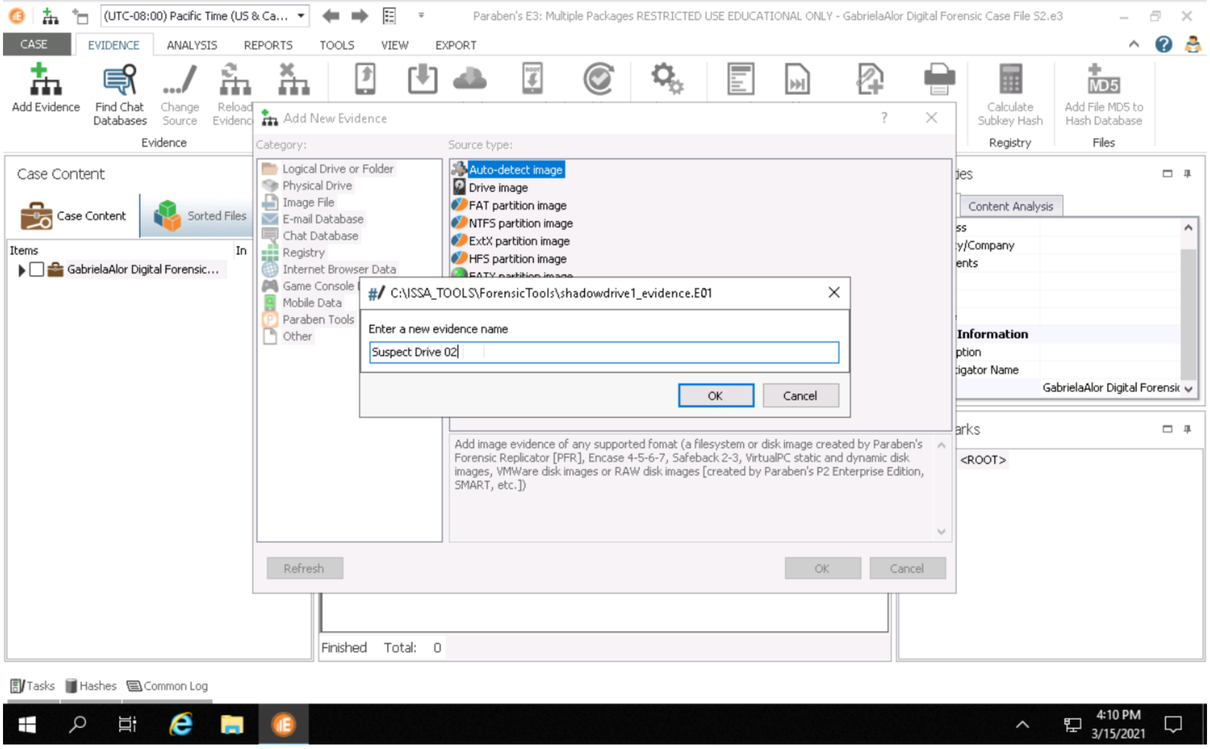
Name	Date modified	Type
iehv	11/11/2019 6:47 PM	File folde
mylastsearch	11/11/2019 6:47 PM	File folde
ProcExp	11/11/2019 6:47 PM	File folde
StegoAndSamples	11/11/2019 7:17 PM	File folde
evidence_drive.e01.E01	5/26/2017 1:40 PM	E01 File
evidence_drive.e01.E01	5/26/2017 1:40 PM	Text Docu
ftpcapture	11/11/2019 7:20 PM	Wireshark
Helix2008R1	5/19/2017 11:40 AM	Disc Imag
shadowdrive1_evidence.E01	5/31/2017 9:35 PM	E01 File
shadowdrive1_evidence.E01	5/31/2017 9:42 PM	Text Docu
shadowdrive1_evidence.E02	5/31/2017 9:37 PM	E02 File
shadowdrive1_evidence.E03	5/31/2017 9:39 PM	E03 File

File name: shadowdrive1_evidence.E01

Any files (*.*)

GabrielaAlor Digital Forensic

Figure 2: Adding digital drive image to the evidence file.



Paraben's E3: Multiple Packages RESTRICTED USE EDUCATIONAL ONLY - GabrielaAlor Digital Forensic Case File 52.e3

GabrielaAlor Digital Forensic...

C:\ISSA_TOOLS\ForensicTools\shadowdrive1_evidence.E01

Enter a new evidence name

Suspect Drive 02

Add image evidence of any supported fomat (a filesystem or disk image created by Paraben's Forensic Replicator [PFR], Encase 4-5-6-7, Safeback 2-3, VirtualPC static and dynamic disk images, VMWare disk images or RAW disk images [created by Paraben's P2 Enterprise Edition, SMART, etc.])

ies

ss

y/Company

ents

Information

ption

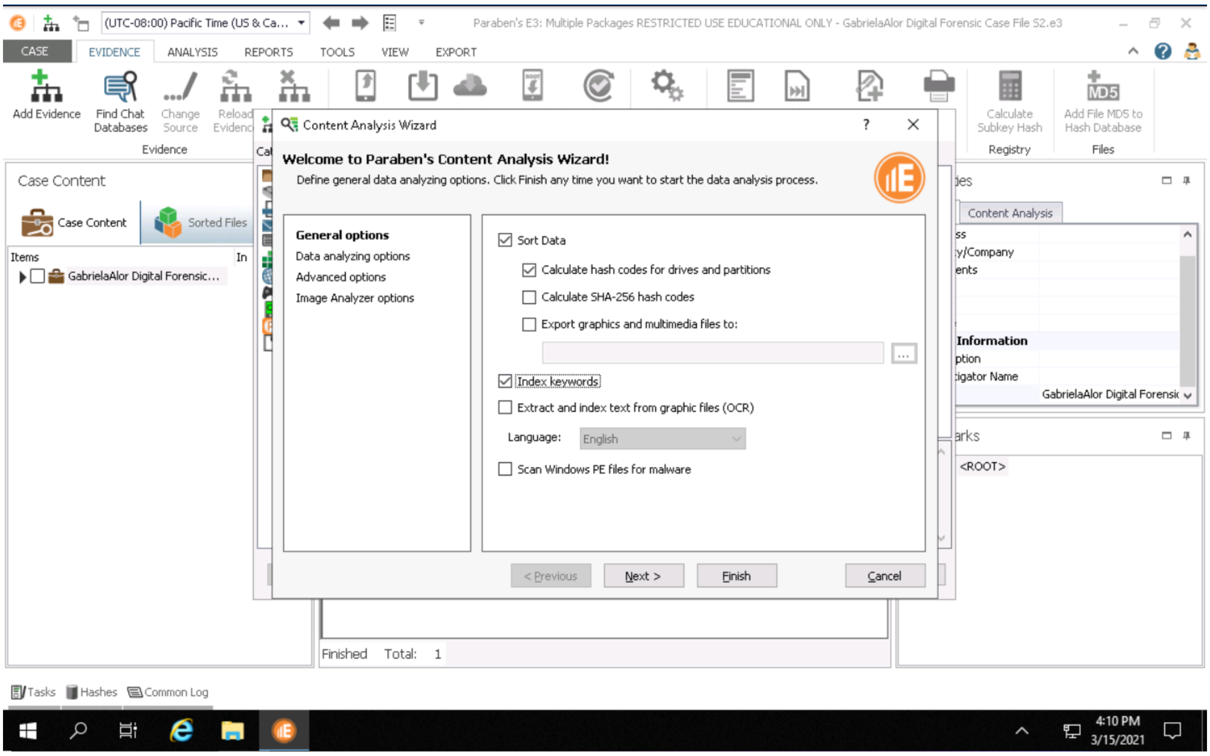
igator Name

GabrielaAlor Digital Forensic

arks

<ROOT>

Figure 3: Naming the evidence drive.



Content Analysis Wizard

Welcome to Paraben's Content Analysis Wizard!

Define general data analyzing options. Click Finish any time you want to start the data analysis process.

General options
Data analyzing options
Advanced options
Image Analyzer options

☑ Sort Data

☑ Calculate hash codes for drives and partitions

☐ Calculate SHA-256 hash codes

☐ Export graphics and multimedia files to:

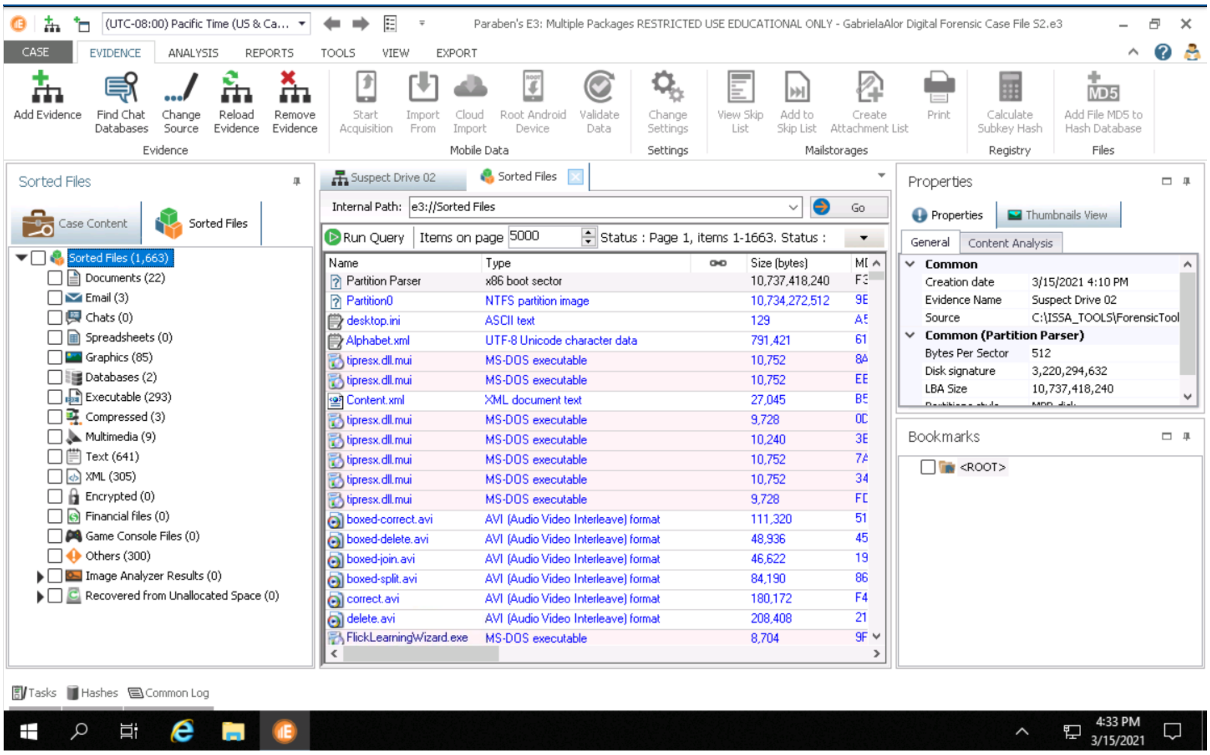
☑ Index keywords

☐ Extract and index text from graphic files (OCR)

Language: English

☐ Scan Windows PE files for malware

Figure 4: Calculating hash codes for drives and partitions.



☐ Sorted Files (1,663)
- ☐ Documents (22)
- ☐ Email (3)
- ☐ Chats (0)
- ☐ Spreadsheets (0)
- ☐ Graphics (85)
- ☐ Databases (2)
- ☐ Executable (293)
- ☐ Compressed (3)
- ☐ Multimedia (9)
- ☐ Text (641)
- ☐ XML (305)
- ☐ Encrypted (0)
- ☐ Financial files (0)
- ☐ Game Console Files (0)
- ☐ Others (300)
- ☐ Image Analyzer Results (0)
- ☐ Recovered from Unallocated Space (0)

Internal Path: e3://Sorted Files

Items on page 5000 Status : Page 1, items 1-1663. Status :

Name	Type		Size (bytes)	MI
Partition Parser	x86 boot sector		10,737,418,240	F3
Partition0	NTFS partition image		10,734,272,512	9E
desktop.ini	ASCII text		129	A5
Alphabet.xml	UTF-8 Unicode character data		791,421	61
tipresx.dll.mui	MS-DOS executable		10,752	8A
tipresx.dll.mui	MS-DOS executable		10,752	EE
Content.xml	XML document text		27,045	B5
tipresx.dll.mui	MS-DOS executable		9,728	0C
tipresx.dll.mui	MS-DOS executable		10,240	3E
tipresx.dll.mui	MS-DOS executable		10,752	7A
tipresx.dll.mui	MS-DOS executable		10,752	34
tipresx.dll.mui	MS-DOS executable		9,728	FC
boxed-correct.avi	AVI (Audio Video Interleave) format		111,320	51
boxed-delete.avi	AVI (Audio Video Interleave) format		48,936	45
boxed-join.avi	AVI (Audio Video Interleave) format		46,622	19
boxed-split.avi	AVI (Audio Video Interleave) format		84,190	86
correct.avi	AVI (Audio Video Interleave) format		180,172	F4
delete.avi	AVI (Audio Video Interleave) format		208,408	21
FlickLearningWizard.exe	MS-DOS executable		8,704	9F

Properties

Properties | Thumbnails View

General | Content Analysis

Common

Creation date	3/15/2021 4:10 PM
Evidence Name	Suspect Drive 02
Source	C:\ISSA_TOOLS\ForensicTool

Common (Partition Parser)

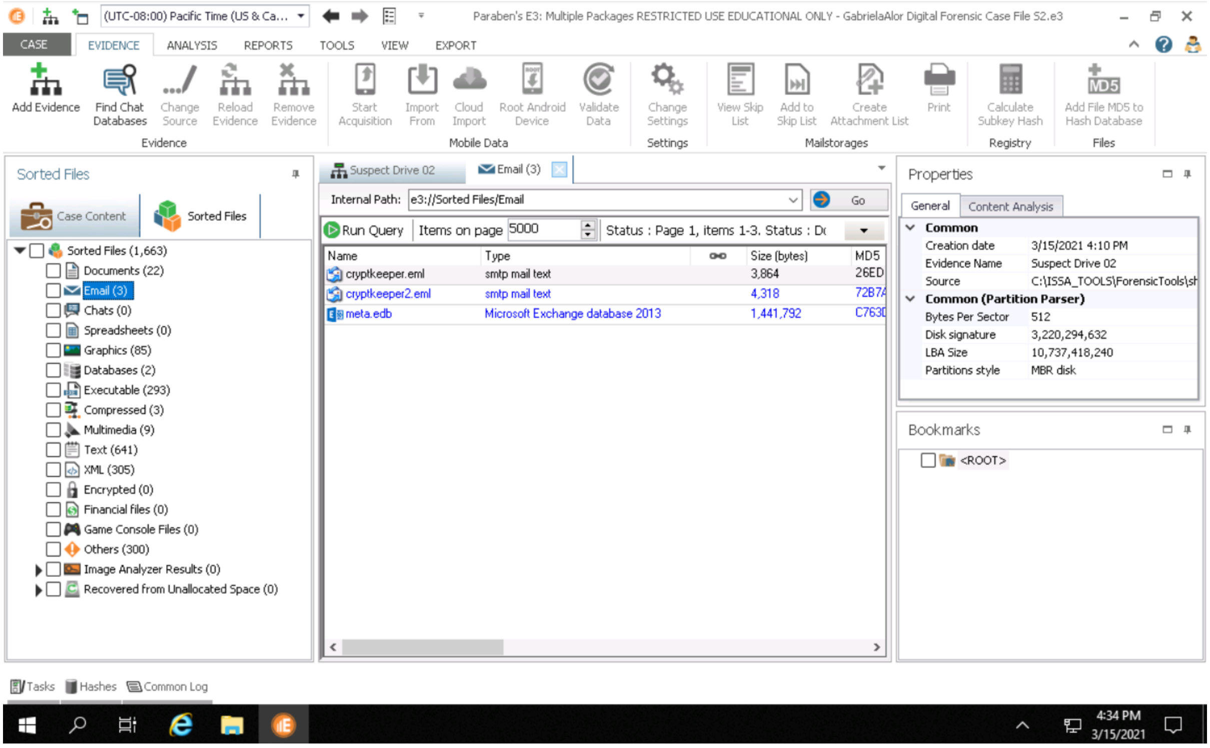
Bytes Per Sector	512
Disk signature	3,220,294,632
LBA Size	10,737,418,240

Bookmarks

☐ <ROOT>

Figure 5: Sorted evidence.

Part 2: Explore Chat and E-mail Conversations



- Sorted Files (1,663)
  - Documents (22)
  - Email (3)
  - Chats (0)
  - Spreadsheets (0)
  - Graphics (85)
  - Databases (2)
  - Executable (293)
  - Compressed (3)
  - Multimedia (9)
  - Text (641)
  - XML (305)
  - Encrypted (0)
  - Financial files (0)
  - Game Console Files (0)
  - Others (300)
  - Image Analyzer Results (0)
  - Recovered from Unallocated Space (0)

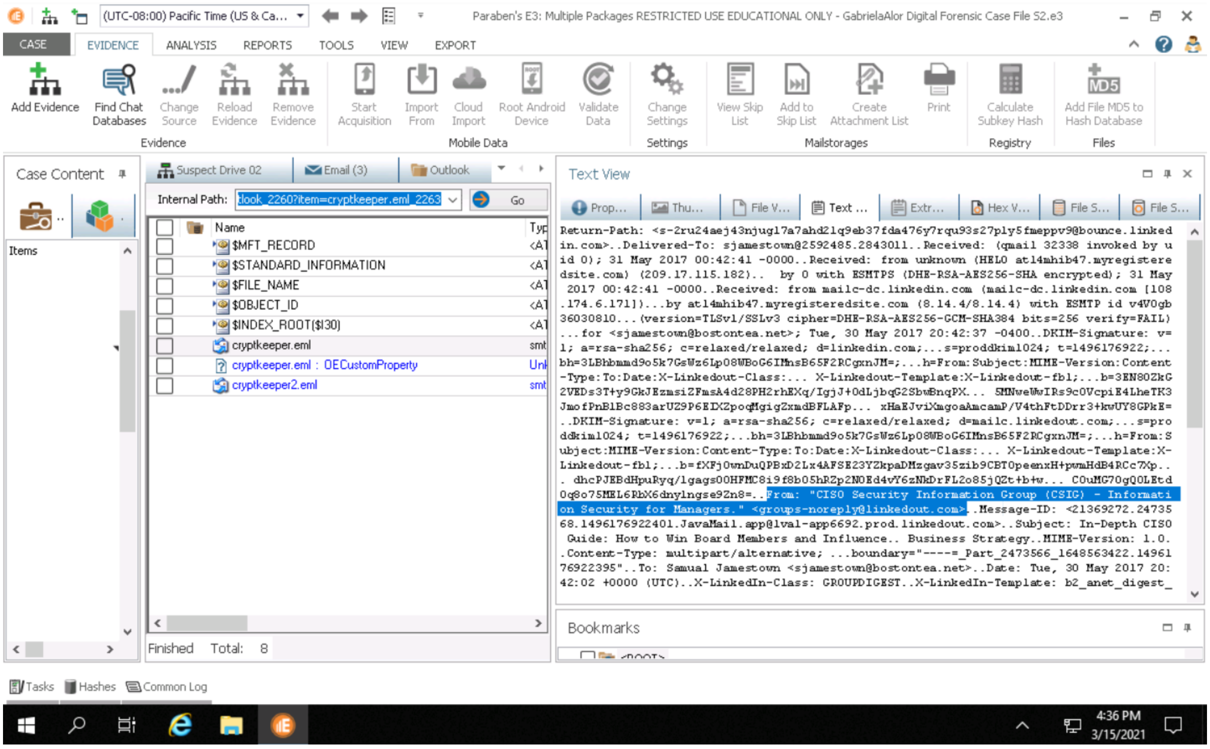
Internal Path: e3://Sorted Files/Email

Items on page 5000 | Status : Page 1, items 1-3. Status : D

Name	Type	Size (bytes)	MD5
cryptkeeper.eml	smtp mail text	3,864	26ED
cryptkeeper2.eml	smtp mail text	4,318	72B7
meta.edb	Microsoft Exchange database 2013	1,441,792	C763

Common	
Creation date	3/15/2021 4:10 PM
Evidence Name	Suspect Drive 02
Source	C:\ISSA_TOOLS\ForensicTools\sh
Common (Partition Parser)	
Bytes Per Sector	512
Disk signature	3,220,294,632
LBA Size	10,737,418,240
Partitions style	MBR disk

Figure 6: Email evidence category.



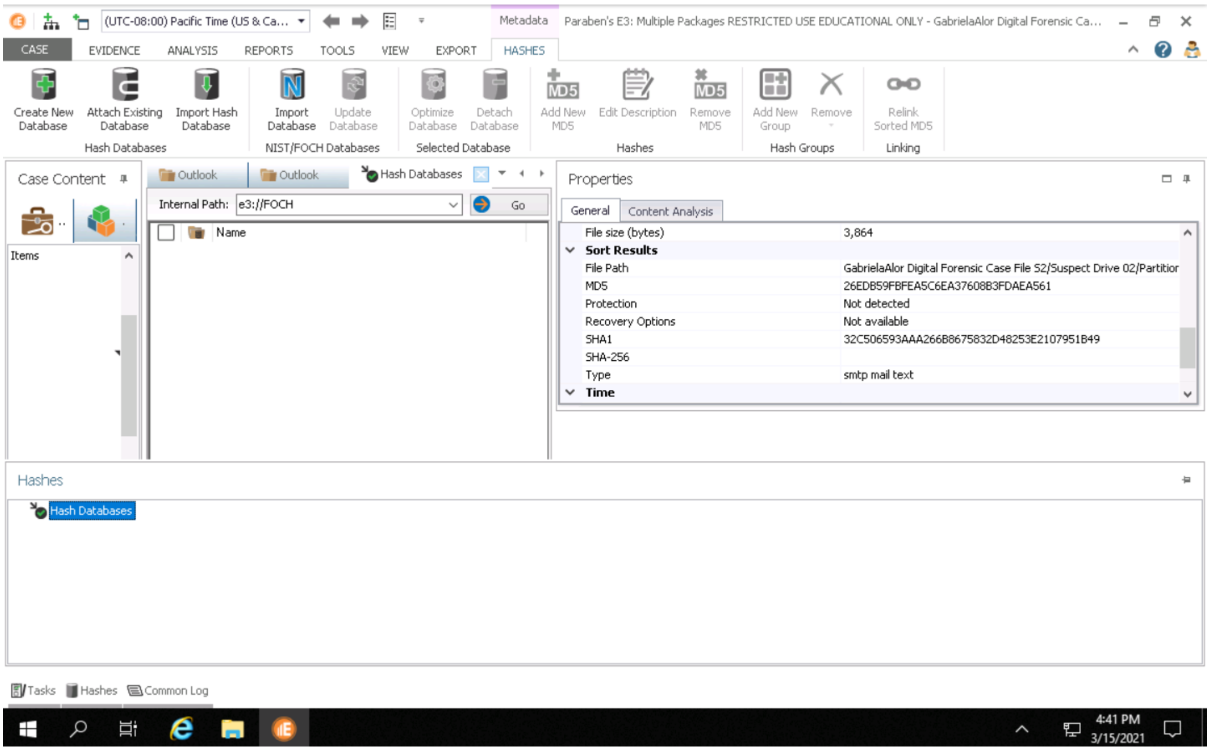
Internal Path: look_2260?item=cryptkeeper.eml_2263

Name	Typ
$MFT_RECORD	<A
$STANDARD_INFORMATION	<A
$FILE_NAME	<A
$OBJECT_ID	<A
$INDEX_ROOT($I30)	<A
cryptkeeper.eml	smt
cryptkeeper.eml : OECustomProperty	Unk
cryptkeeper2.eml	smt

Finished Total: 8

```
Return-Path: <s-2ru24aej43njugl7a7ahd2lq9eb37fda476y7rqu93s27ply5fmeppv9@bounce.linked
in.com>..Delivered-To: sjamestown@2592485.2843011..Received: (qmail 32338 invoked by u
id 0); 31 May 2017 00:42:41 -0000..Received: from unknown (HELO atl4mhib47.myregistere
dsite.com) (209.17.115.182)..  by 0 with ESMTPS (DHE-RSA-AES256-SHA encrypted); 31 May
 2017 00:42:41 -0000..Received: from mailc-dc.linkedin.com (mailc-dc.linkedin.com [108
.174.6.171])...by atl4mhib47.myregisteredsite.com (8.14.4/8.14.4) with ESMTP id v4V0gb
36030810...(version=TLSv1/SSLv3 cipher=DHE-RSA-AES256-GCM-SHA384 bits=256 verify=FAIL)
...for <sjamestown@bostontea.net>; Tue, 30 May 2017 20:42:37 -0400..DKIM-Signature: v=
1; a=rsa-sha256; c=relaxed/relaxed; d=linkedin.com;...s=proddkim1024; t=1496176922;...
bh=3LBhbmmd9o5k7GsWz6Lp08WBoG6IMnsB65F2RCgxnJM=;...h=From:Subject:MIME-Version:Content
-Type:To:Date:X-Linkedout-Class:... X-Linkedout-Template:X-Linkedout-fbl;...b=3EN80ZkG
2VEDs3T+y9GkJEzmsiZFmsA4d28PH2rhEXq/IgjJ+0dLjbqG2SbwBnqPX... 5MNweWwIRs9c0VcpiE4LheTK3
JmofPnBlBc883arUZ9P6EIXZpoqMgigZxmdBFLAFp... xHaEJviXmgoaAmcamP/V4thFtDDrr3+kwUY8GPkE=
..DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=mailc.linkedout.com;...s=pro
ddkim1024; t=1496176922;...bh=3LBhbmmd9o5k7GsWz6Lp08WBoG6IMnsB65F2RCgxnJM=;...h=From:S
ubject:MIME-Version:Content-Type:To:Date:X-Linkedout-Class:... X-Linkedout-Template:X-
Linkedout-fbl;...b=fXFj0wnDuQPBxD2Lx4AFSE23YZkpaDMzgav35zib9CBT0peenxH+pwmHdB4RCc7Xp..
. dhcPJEBdHpuRyq/lgags00HFMC8i9f8b05hRZp2N0Ed4vY6zNkDrFL2o85jQZt+b+w... C0uMG70gQ0LEtd
0q8o75MEL6RbX6dnylngse9Zn8=..From: "CISO Security Information Group (CSIG) - Informati
on Security for Managers." <groups-noreply@linkedout.com>..Message-ID: <21369272.24735
68.1496176922401.JavaMail.app@lval-app6692.prod.linkedout.com>..Subject: In-Depth CISO
 Guide: How to Win Board Members and Influence.. Business Strategy..MIME-Version: 1.0.
.Content-Type: multipart/alternative; ...boundary="----=_Part_2473566_1648563422.14961
76922395"..To: Samual Jamestown <sjamestown@bostontea.net>..Date: Tue, 30 May 2017 20:
42:02 +0000 (UTC)..X-LinkedIn-Class: GROUPDIGEST..X-LinkedIn-Template: b2_anet_digest_
```

Figure 7: Contents of cryptkeeper.eml evidence.

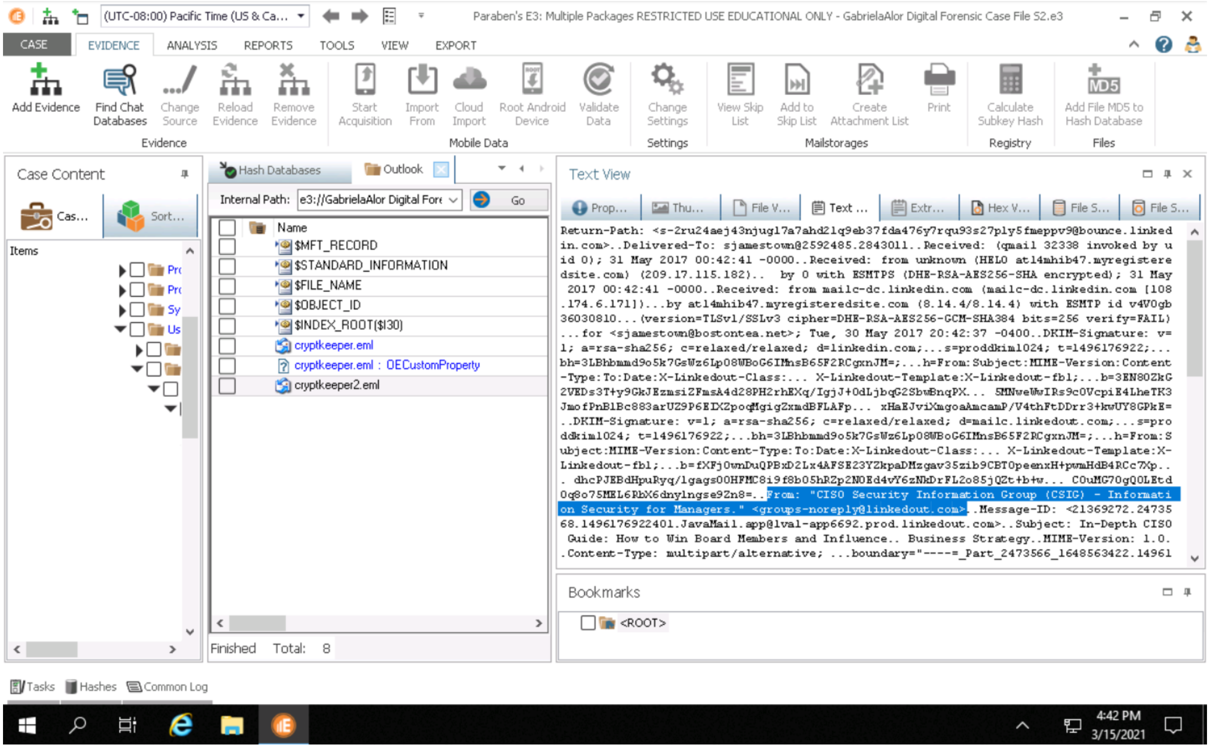


Properties

General | Content Analysis

File size (bytes)	3,864
Sort Results	
File Path	GabrielaAlor Digital Forensic Case File S2/Suspect Drive 02/Partitior
MD5	26EDB59FBFEA5C6EA37608B3FDAEA561
Protection	Not detected
Recovery Options	Not available
SHA1	32C506593AAA266B8675832D48253E2107951B49
SHA-256	
Type	smtp mail text
Time	

Figure 8: MD5 and SHA1 hashes for cryptkeeper.eml

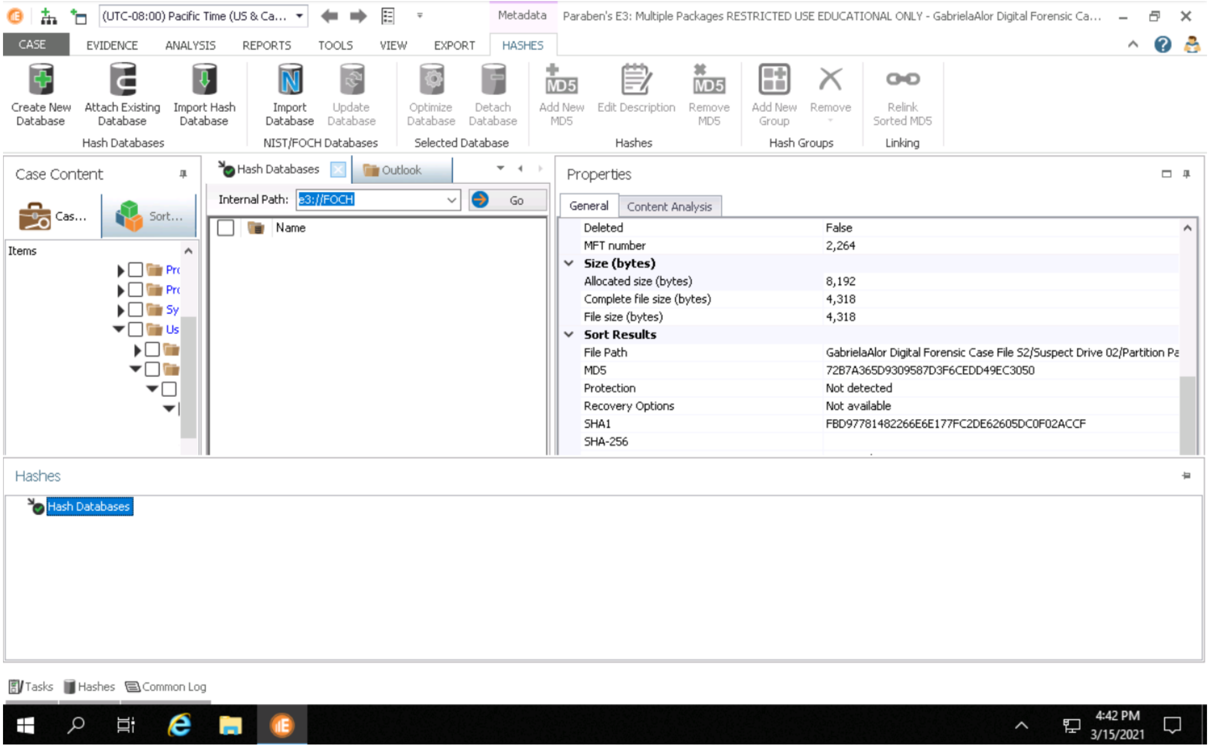


Name
- $MFT_RECORD
- $STANDARD_INFORMATION
- $FILE_NAME
- $OBJECT_ID
- $INDEX_ROOT($I30)
- cryptkeeper.eml
- cryptkeeper.eml : OECustomProperty
- cryptkeeper2.eml

Finished Total: 8

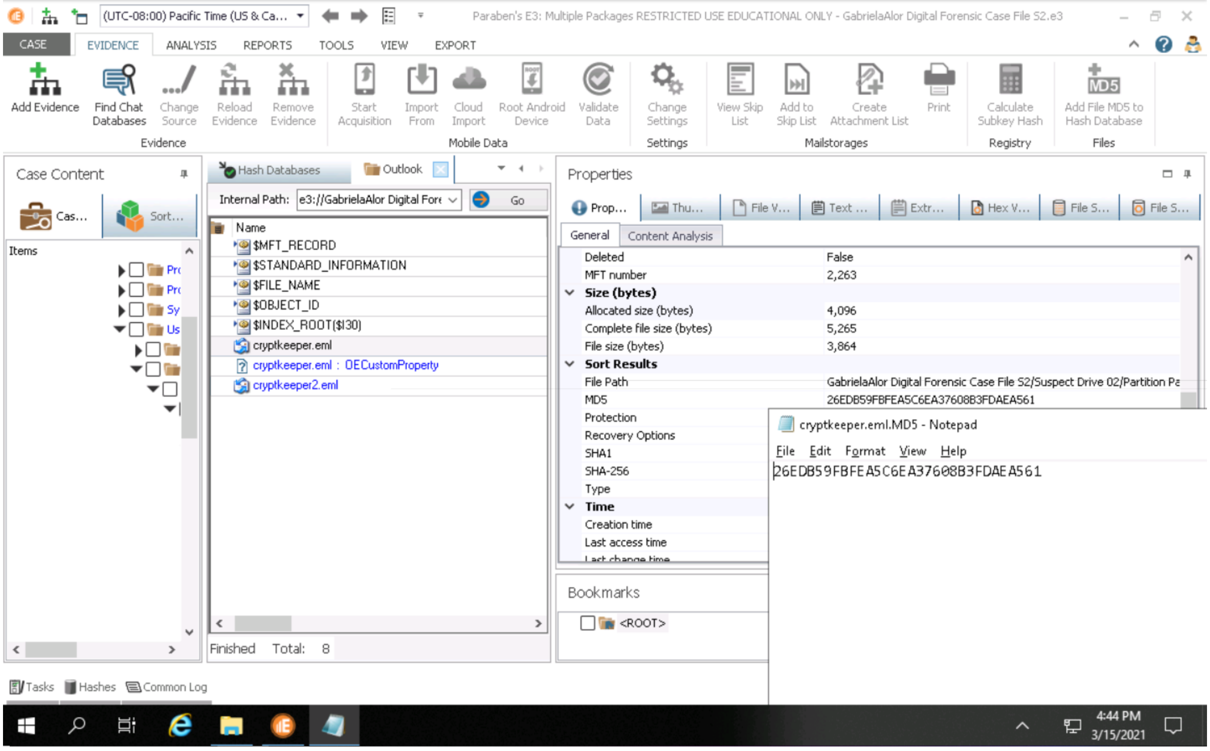
```
Return-Path: <s-2ru24aej43njugl7a7ahd2lq9eb37fda476y7rqu93s27ply5fmeppv9@bounce.linked
in.com>..Delivered-To: sjamestown@2592485.2843011..Received: (qmail 32338 invoked by u
id 0); 31 May 2017 00:42:41 -0000..Received: from unknown (HELO atl4mhib47.myregistere
dsite.com) (209.17.115.182)..  by 0 with ESMTPS (DHE-RSA-AES256-SHA encrypted); 31 May
 2017 00:42:41 -0000..Received: from mailc-dc.linkedin.com (mailc-dc.linkedin.com [108
.174.6.171])...by atl4mhib47.myregisteredsite.com (8.14.4/8.14.4) with ESMTP id v4V0gb
36030810...(version=TLSv1/SSLv3 cipher=DHE-RSA-AES256-GCM-SHA384 bits=256 verify=FAIL)
...for <sjamestown@bostontea.net>; Tue, 30 May 2017 20:42:37 -0400..DKIM-Signature: v=
1; a=rsa-sha256; c=relaxed/relaxed; d=linkedin.com;...s=proddkim1024; t=1496176922;...
bh=3LBhbmmd9o5k7GsWz6Lp08WBoG6IMnsB65F2RCgxnJM=;...h=From:Subject:MIME-Version:Content
-Type:To:Date:X-Linkedout-Class:... X-Linkedout-Template:X-Linkedout-fbl;...b=3EN80ZkG
2VEDs3T+y9GkJEzmsiZFmsA4d28PH2rhEXq/IgjJ+0dLjbqG2SbwBnqPX... 5MNweWwIRs9c0VcpiE4LheTK3
JmofPnB1Bc883arUZ9P6EIXZpoqMgigZxmdBFLAFp... xHaEJviXmgoaAmcamP/V4thFtDDrr3+kwUY8GPkE=
..DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=mailc.linkedout.com;...s=pro
ddkim1024; t=1496176922;...bh=3LBhbmmd9o5k7GsWz6Lp08WBoG6IMnsB65F2RCgxnJM=;...h=From:S
ubject:MIME-Version:Content-Type:To:Date:X-Linkedout-Class:... X-Linkedout-Template:X-
Linkedout-fbl;...b=fXFj0wnDuQPBxD2Lx4AFSE23YZkpaDMzgav35zib9CBT0peenxH+pwmHdB4RCc7Xp..
. dhcPJEBdHpuRyq/1gags00HFMC8i9f8b05hRZp2N0Ed4vY6zNkDrFL2o85jQZt+b+w... C0uMG70gQ0LEtd
0q8o75MEL6RbX6dnylngse9Zn8=..From: "CISO Security Information Group (CSIG) - Informati
on Security for Managers." <groups-noreply@linkedout.com>..Message-ID: <21369272.24735
68.1496176922401.JavaMail.app@lval-app6692.prod.linkedout.com>..Subject: In-Depth CISO
 Guide: How to Win Board Members and Influence.. Business Strategy..MIME-Version: 1.0.
.Content-Type: multipart/alternative; ...boundary="----=_Part_2473566_1648563422.14961
```

Figure 9: Contents of cryptkeeper2.eml evidence.



Deleted	False
MFT number	2,264
Size (bytes)	
Allocated size (bytes)	8,192
Complete file size (bytes)	4,318
File size (bytes)	4,318
Sort Results	
File Path	GabrielaAlor Digital Forensic Case File S2/Suspect Drive 02/Partition Pa
MD5	72B7A365D9309587D3F6CEDD49EC3050
Protection	Not detected
Recovery Options	Not available
SHA1	FBD97781482266E6E177FC2DE62605DC0F02ACCF
SHA-256	

Figure 10: MD5 and SHA1 values for cryptkeeper2.eml evidence file.



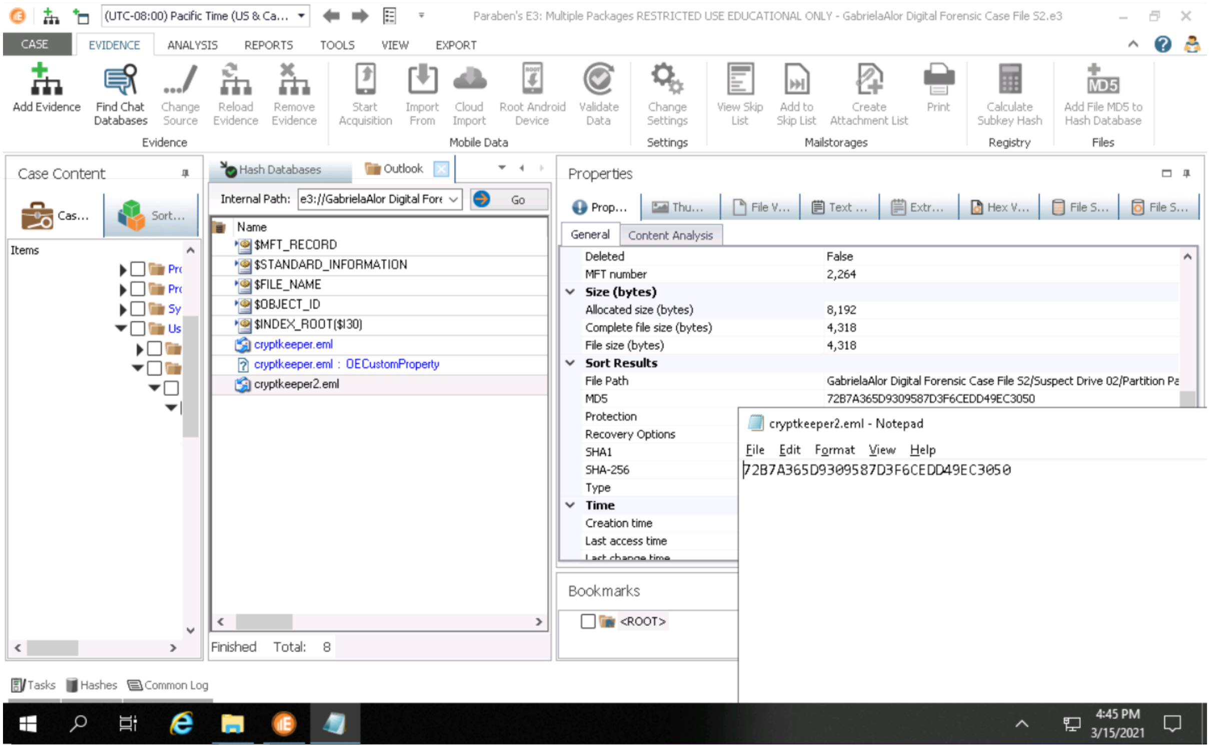
Name
$MFT_RECORD
$STANDARD_INFORMATION
$FILE_NAME
$OBJECT_ID
$INDEX_ROOT($I30)
cryptkeeper.eml
cryptkeeper.eml : OECustomProperty
cryptkeeper2.eml

Finished Total: 8

Deleted	False
MFT number	2,263
Size (bytes)	
Allocated size (bytes)	4,096
Complete file size (bytes)	5,265
File size (bytes)	3,864
Sort Results	
File Path	GabrielaAlor Digital Forensic Case File S2/Suspect Drive 02/Partition Pa
MD5	26EDB59FBFEA5C6EA37608B3FDAEA561
Protection	
Recovery Options	
SHA1	
SHA-256	
Type	
Time	
Creation time	
Last access time	
Last change time	

```
26EDB59FBFEA5C6EA37608B3FDAEA561
```

Figure 11: Comparison of cryptkeeper.eml MD5 values from step 7.



$MFT_RECORD
$STANDARD_INFORMATION
$FILE_NAME
$OBJECT_ID
$INDEX_ROOT($I30)
cryptkeeper.eml
cryptkeeper.eml : OECustomProperty
cryptkeeper2.eml

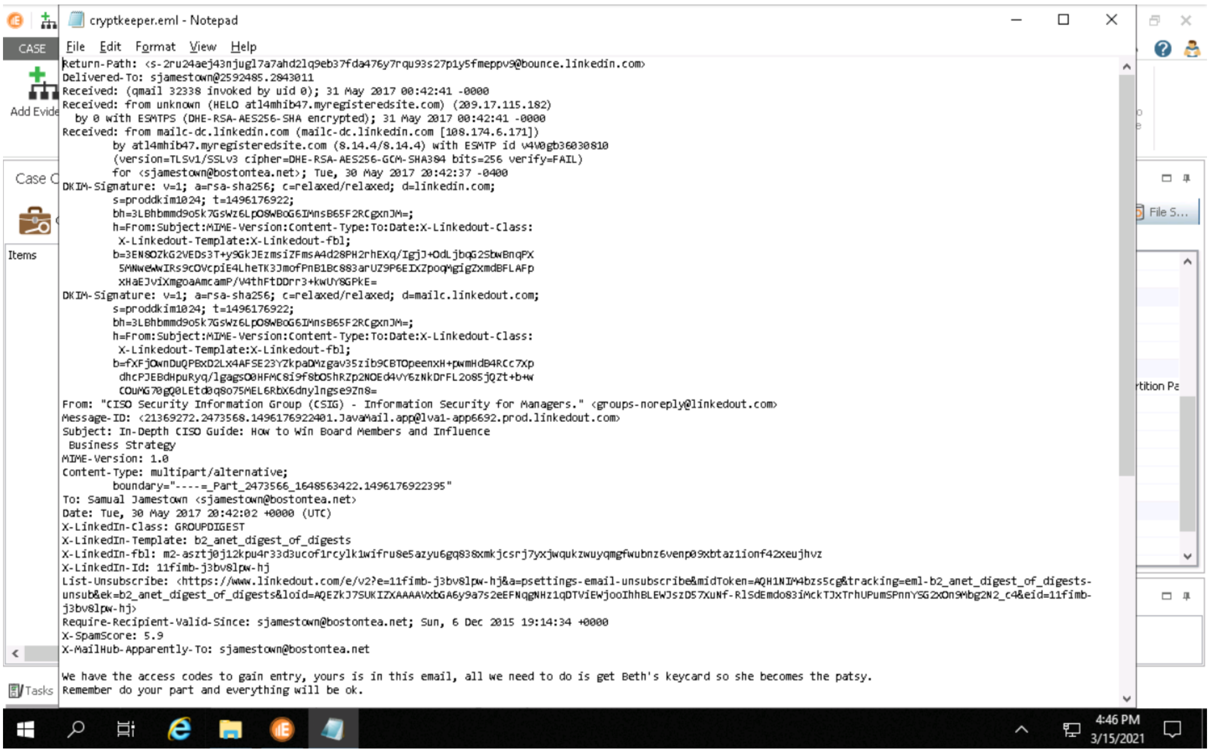
Deleted	False
MFT number	2,264
Size (bytes)	
Allocated size (bytes)	8,192
Complete file size (bytes)	4,318
File size (bytes)	4,318
Sort Results	
File Path	GabrielaAlor Digital Forensic Case File S2/Suspect Drive 02/Partition Pa
MD5	72B7A365D9309587D3F6CEDD49EC3050
Protection	
Recovery Options	
SHA1	
SHA-256	
Type	
Time	
Creation time	
Last access time	

cryptkeeper2.eml - Notepad

File Edit Format View Help

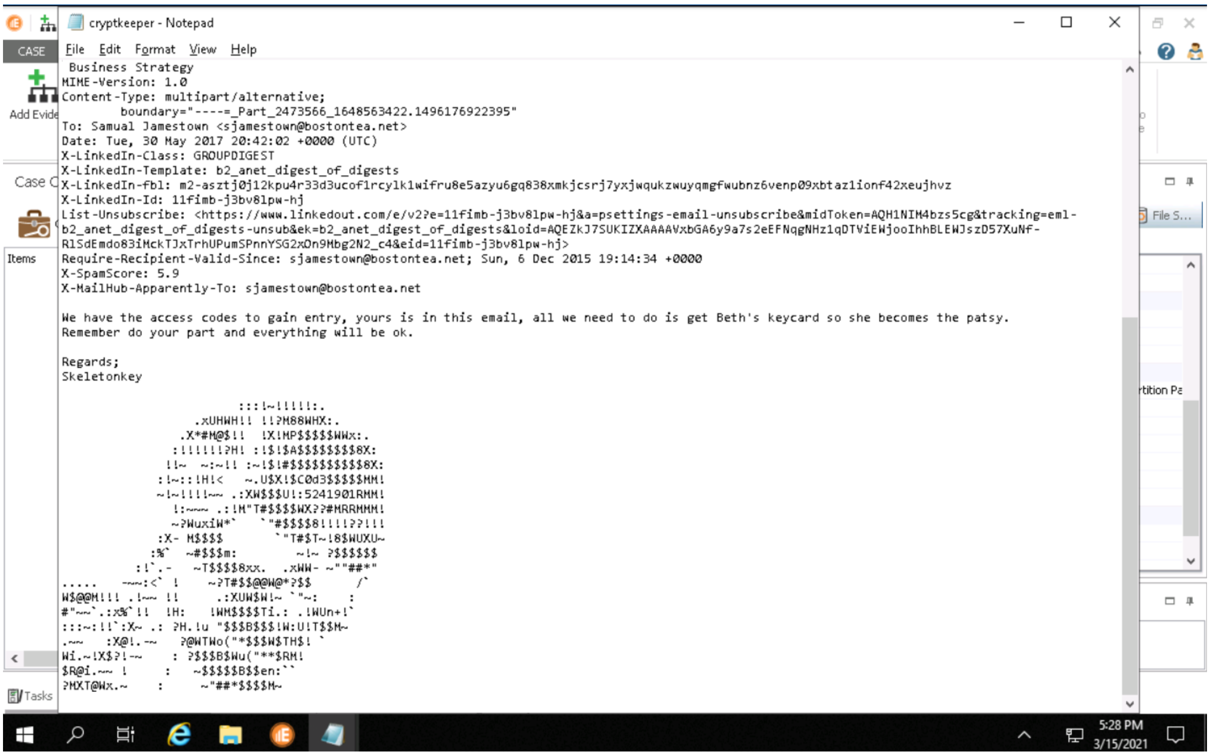
```
72B7A365D9309587D3F6CEDD49EC3050
```

Figure 12: Comparison of cryptkeeper2.eml MD5 hash values from step 7.



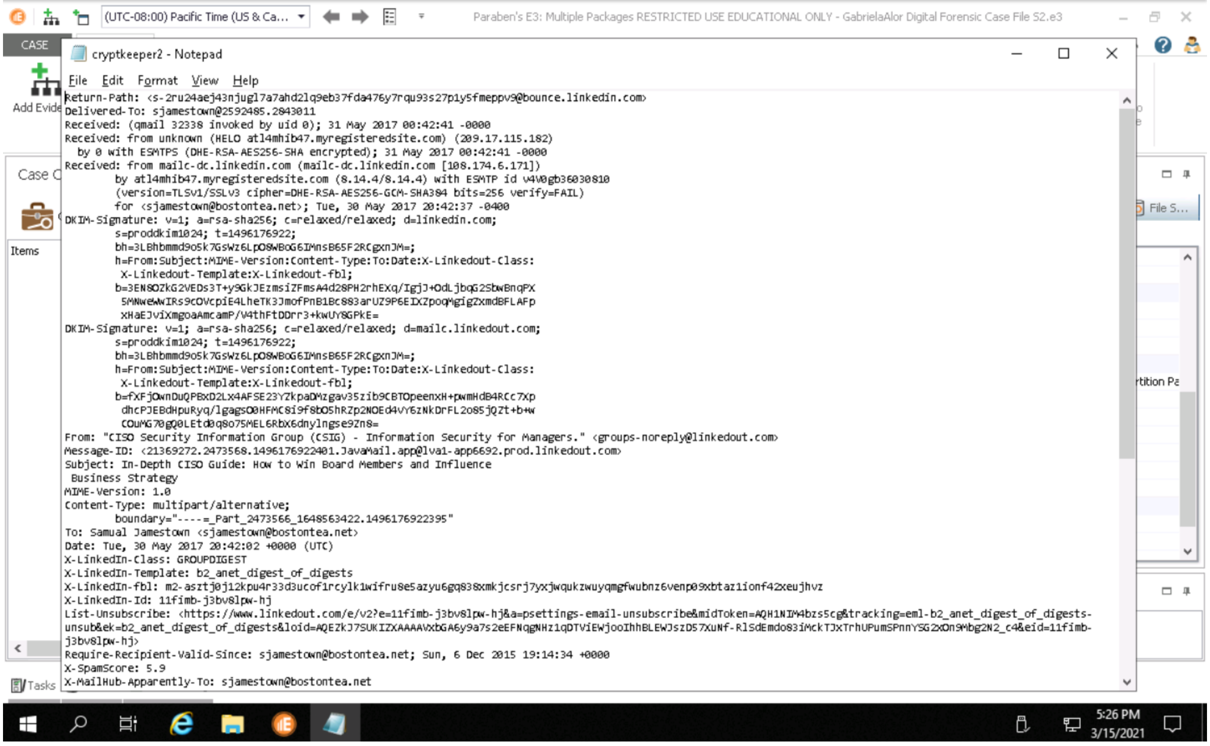
```
Return-Path: <s-2ru24aej43njugl7a7ahd2lq9eb37fda476y7rqu93s27p1y5fmeppv9@bounce.linkedin.com>
Delivered-To: sjamestown@2592485.2843011
Received: (qmail 32338 invoked by uid 0); 31 May 2017 00:42:41 -0000
Received: from unknown (HELO atl4mhib47.myregisteredsite.com) (209.17.115.182)
  by 0 with ESMTPS (DHE-RSA-AES256-SHA encrypted); 31 May 2017 00:42:41 -0000
Received: from mailc-dc.linkedin.com (mailc-dc.linkedin.com [108.174.6.171])
        by atl4mhib47.myregisteredsite.com (8.14.4/8.14.4) with ESMTP id v4V0gb36030810
        (version=TLSv1/SSLv3 cipher=DHE-RSA-AES256-GCM-SHA384 bits=256 verify=FAIL)
        for <sjamestown@bostontea.net>; Tue, 30 May 2017 20:42:37 -0400
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=linkedin.com;
        s=proddkim1024; t=1496176922;
        bh=3LBhbmmd9o5k7GsWz6LpO8WBoG6IMnsB65F2RCgxnJM=;
        h=From:Subject:MIME-Version:Content-Type:To:Date:X-Linkedout-Class:
         X-Linkedout-Template:X-Linkedout-fbl;
        b=3EN8OZkG2VEDs3T+y9GkJEzmsiZFmsA4d28PH2rhEXq/IgjJ+OdLjbqG2SbwBnqPX
         5MNweWwIRs9cOVcpiE4LheTK3JmofPnB1Bc883arUZ9P6EIXZpoqMgigZxmdBFLAFp
         xHaEJviXmgoaAmcamP/V4thFtDDrr3+kwUY8GPkE=
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=mailc.linkedout.com;
        s=proddkim1024; t=1496176922;
        bh=3LBhbmmd9o5k7GsWz6LpO8WBoG6IMnsB65F2RCgxnJM=;
        h=From:Subject:MIME-Version:Content-Type:To:Date:X-Linkedout-Class:
         X-Linkedout-Template:X-Linkedout-fbl;
        b=fXFjOwnDuQPBxD2Lx4AFSE23YZkpaDMzgav35zib9CBTOpeenxH+pwmHdB4RCc7Xp
         dhcPJEBdHpuRyq/lgagsO0HFMC8i9f8bO5hRZp2NOEd4vY6zNkDrFL2o85jQZt+b+w
         COuMG70gQ0LEtd0q8o75MEL6RbX6dnylngse9Zn8=
From: "CISO Security Information Group (CSIG) - Information Security for Managers." <groups-noreply@linkedout.com>
Message-ID: <21369272.2473568.1496176922401.JavaMail.app@lva1-app6692.prod.linkedout.com>
Subject: In-Depth CISO Guide: How to Win Board Members and Influence
 Business Strategy
MIME-Version: 1.0
Content-Type: multipart/alternative;
        boundary="----=_Part_2473566_1648563422.1496176922395"
To: Samual Jamestown <sjamestown@bostontea.net>
Date: Tue, 30 May 2017 20:42:02 +0000 (UTC)
X-LinkedIn-Class: GROUPDIGEST
X-LinkedIn-Template: b2_anet_digest_of_digests
X-LinkedIn-fbl: m2-asztj0j12kpu4r33d3ucof1rcylk1wifru8e5azyu6gq838xmkjcsrj7yxjwqukzwuyqmgfwubnz6venp09xbtaz1ionf42xeujhvz
X-LinkedIn-Id: 11fimb-j3bv8lpw-hj
List-Unsubscribe: <https://www.linkedout.com/e/v2?e=11fimb-j3bv8lpw-hj&a=psettings-email-unsubscribe&midToken=AQH1NIM4bzs5cg&tracking=eml-b2_anet_digest_of_digests-
unsub&ek=b2_anet_digest_of_digests&loid=AQEZkJ7SUKIZXAAAAVxbGA6y9a7s2eEFNqgNHz1qDTViEWjooIhhBLEWJszD57XuNf-RlSdEmdo83iMckTJxTrhUPumSPnnYSG2xOn9Mbg2N2_c4&eid=11fimb-
j3bv8lpw-hj>
Require-Recipient-Valid-Since: sjamestown@bostontea.net; Sun, 6 Dec 2015 19:14:34 +0000
X-SpamScore: 5.9
X-MailHub-Apparently-To: sjamestown@bostontea.net

We have the access codes to gain entry, yours is in this email, all we need to do is get Beth's keycard so she becomes the patsy.
Remember do your part and everything will be ok.
```

Figure 13: Contents of cryptkeeper.eml.



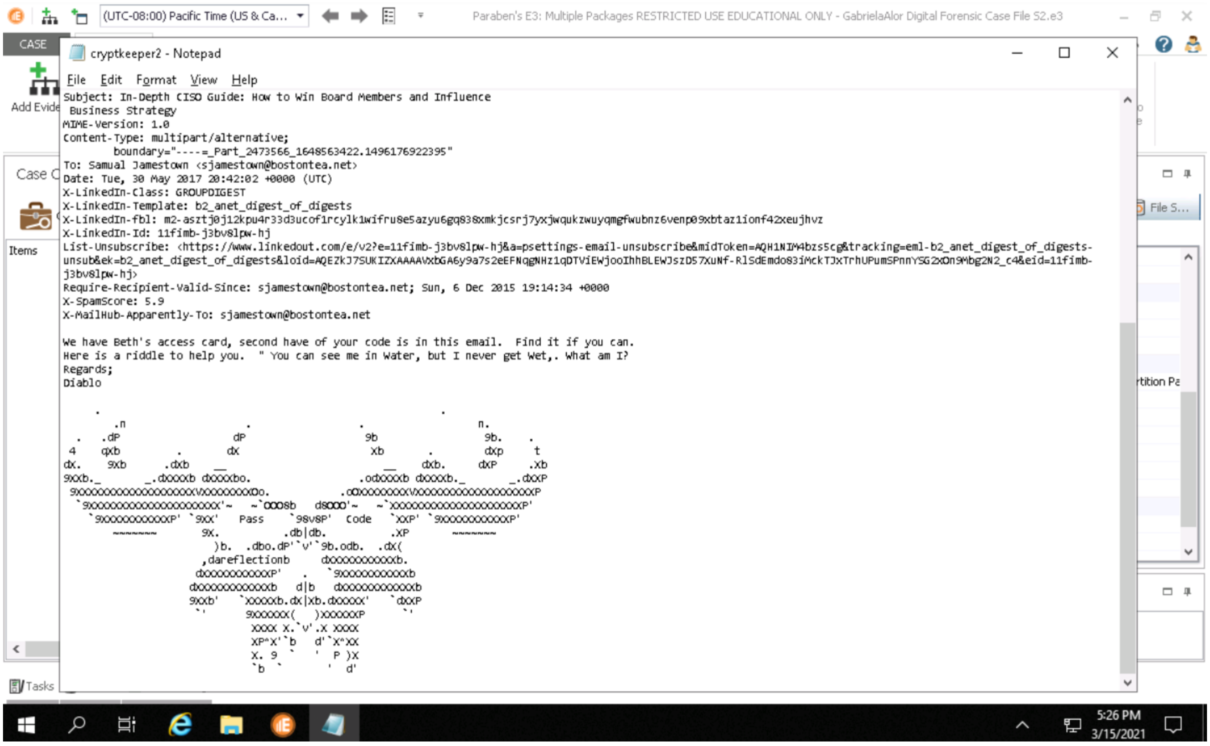
```
 Business Strategy
MIME-Version: 1.0
Content-Type: multipart/alternative;
        boundary="----=_Part_2473566_1648563422.1496176922395"
To: Samual Jamestown <sjamestown@bostontea.net>
Date: Tue, 30 May 2017 20:42:02 +0000 (UTC)
X-LinkedIn-Class: GROUPDIGEST
X-LinkedIn-Template: b2_anet_digest_of_digests
X-LinkedIn-fbl: m2-asztj0j12kpu4r33d3ucof1rcylk1wifru8e5azyu6gq838xmkjcsrj7yxjwqukzwuyqmgfwubnz6venp09xbtaz1ionf42xeujhvz
X-LinkedIn-Id: 11fimb-j3bv8lpw-hj
List-Unsubscribe: <https://www.linkedout.com/e/v2?e=11fimb-j3bv8lpw-hj&a=psettings-email-unsubscribe&midToken=AQH1NIM4bzs5cg&tracking=eml-
b2_anet_digest_of_digests-unsub&ek=b2_anet_digest_of_digests&loid=AQEZkJ7SUKIZXAAAAVxbGA6y9a7s2eEFNqgNHz1qDTViEWjooIhhBLEWJszD57XuNf-
R1SdEmdo83iMckTJxTrhUPumSPnnYSG2xOn9Mbg2N2_c4&eid=11fimb-j3bv8lpw-hj>
Require-Recipient-Valid-Since: sjamestown@bostontea.net; Sun, 6 Dec 2015 19:14:34 +0000
X-SpamScore: 5.9
X-MailHub-Apparently-To: sjamestown@bostontea.net

We have the access codes to gain entry, yours is in this email, all we need to do is get Beth's keycard so she becomes the patsy.
Remember do your part and everything will be ok.

Regards;
Skeletonkey

                        :::!~!!!!!:.
                  .xUHWH!! !!?M88WHX:.
                .X*#M@$!!  !X!MP$$$$$WWx:.
               :!!!!!!?H! :!$!$A$$$$$$$$8X:
              !!~  ~:~!! :~!$!#$$$$$$$$$$8X:
             :!~::!H!<   ~.U$X!$C0d3$$$$$MM!
             ~!~!!!!~~ .:XW$$$U!:5241901RMM!
               !:~~~ .:!M"T#$$$$WX??#MRRMMM!
               ~?WuxiW*`   `"#$$$$8!!!!??!!!
             :X- M$$$$       `"T#$T~!8$WUXU~
            :%`  ~#$$$m:        ~!~ ?$$$$$$
          :!`.-   ~T$$$$8xx.  .xWW- ~""##*"
.....   -~~:<` !    ~?T#$$@@W@*?$$      /`
W$@@M!!! .!~~ !!     .:XUW$W!~ `"~:    :
#"~~`.:x%`!!  !H:   !WM$$$$Ti.: .!WUn+!`
:::~:!!`:X~ .: ?H.!u "$$$B$$$!W:U!T$$M~
.~~   :X@!.-~   ?@WTWo("*$$$W$TH$! `
Wi.~!X$?!-~    : ?$$$B$Wu("**$RM!
$R@i.~~ !     :   ~$$$$$B$$en:``
?MXT@Wx.~    :     ~"##*$$$$M~
```

Figure 14: Contents of cryptkeeper.eml continued.


(UTC-08:00) Pacific Time (US & Ca...
Paraben's E3: Multiple Packages RESTRICTED USE EDUCATIONAL ONLY - GabrielaAlor Digital Forensic Case File S2.e3
cryptkeeper2 - Notepad
File Edit Format View Help
CASE
Add Evide
Items
Tasks
5:26 PM
3/15/2021

```
Return-Path: <s-2ru24aej43njugl7a7ahd2lq9eb37fda476y7rqu93s27p1y5fmeppv9@bounce.linkedin.com>
Delivered-To: sjamestown@2592485.2843011
Received: (qmail 32338 invoked by uid 0); 31 May 2017 00:42:41 -0000
Received: from unknown (HELO atl4mhib47.myregisteredsite.com) (209.17.115.182)
  by 0 with ESMTPS (DHE-RSA-AES256-SHA encrypted); 31 May 2017 00:42:41 -0000
Received: from mailc-dc.linkedin.com (mailc-dc.linkedin.com [108.174.6.171])
        by atl4mhib47.myregisteredsite.com (8.14.4/8.14.4) with ESMTP id v4V0gb36030810
        (version=TLSv1/SSLv3 cipher=DHE-RSA-AES256-GCM-SHA384 bits=256 verify=FAIL)
        for <sjamestown@bostontea.net>; Tue, 30 May 2017 20:42:37 -0400
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=linkedin.com;
        s=proddkim1024; t=1496176922;
        bh=3LBhbmmd9o5k7GsWz6LpO8WBoG6IMnsB65F2RCgxnJM=;
        h=From:Subject:MIME-Version:Content-Type:To:Date:X-Linkedout-Class:
         X-Linkedout-Template:X-Linkedout-fbl;
        b=3EN8OZkG2VEDs3T+y9GkJEzmsiZFmsA4d28PH2rhEXq/IgjJ+OdLjbqG2SbwBnqPX
         5MNweWwIRs9cOVcpiE4LheTK3JmofPnB1Bc883arUZ9P6EIXZpoqMgigZxmdBFLAFp
         xHaEJviXmgoaAmcamP/V4thFtDDrr3+kwUY8GPkE=
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=mailc.linkedout.com;
        s=proddkim1024; t=1496176922;
        bh=3LBhbmmd9o5k7GsWz6LpO8WBoG6IMnsB65F2RCgxnJM=;
        h=From:Subject:MIME-Version:Content-Type:To:Date:X-Linkedout-Class:
         X-Linkedout-Template:X-Linkedout-fbl;
        b=fXFjOwnDuQPBxD2LX4AFSE23YZkpaDMzgav35zib9CBTOpeenxH+pwmHdB4RCc7Xp
         dhcPJEBdHpuRyq/lgagsO0HFMC8i9f8bO5hRZp2NOEd4vY6zNkDrFL2o85jQZt+b+w
         COuMG70gQ0LEtd0q8o75MEL6RbX6dnylngse9Zn8=
From: "CISO Security Information Group (CSIG) - Information Security for Managers." <groups-noreply@linkedout.com>
Message-ID: <21369272.2473568.1496176922401.JavaMail.app@lva1-app6692.prod.linkedout.com>
Subject: In-Depth CISO Guide: How to Win Board Members and Influence
 Business Strategy
MIME-Version: 1.0
Content-Type: multipart/alternative;
        boundary="----=_Part_2473566_1648563422.1496176922395"
To: Samual Jamestown <sjamestown@bostontea.net>
Date: Tue, 30 May 2017 20:42:02 +0000 (UTC)
X-LinkedIn-Class: GROUPDIGEST
X-LinkedIn-Template: b2_anet_digest_of_digests
X-LinkedIn-fbl: m2-asztj0j12kpu4r33d3ucof1rcylk1wifru8e5azyu6gq838xmkjcsrj7yxjwqukzwuyqmgfwubnz6venp09xbtaz1ionf42xeujhvz
X-LinkedIn-Id: 11fimb-j3bv8lpw-hj
List-Unsubscribe: <https://www.linkedout.com/e/v2?e=11fimb-j3bv8lpw-hj&a=psettings-email-unsubscribe&midToken=AQH1NIM4bzs5cg&tracking=eml-b2_anet_digest_of_digests-
unsub&ek=b2_anet_digest_of_digests&loid=AQEZkJ7SUKIZXAAAAVxbGA6y9a7s2eEFNqgNHz1qDTViEWjooIhhBLEWJszD57XuNf-R1SdEmdo83iMckTJxTrhUPumSPnnYSG2xOn9Mbg2N2_c4&eid=11fimb-
j3bv8lpw-hj>
Require-Recipient-Valid-Since: sjamestown@bostontea.net; Sun, 6 Dec 2015 19:14:34 +0000
X-SpamScore: 5.9
X-MailHub-Apparently-To: sjamestown@bostontea.net
```

Figure 15: Contents of cryptkeeper2.eml.


(UTC-08:00) Pacific Time (US & Ca...
Paraben's E3: Multiple Packages RESTRICTED USE EDUCATIONAL ONLY - GabrielaAlor Digital Forensic Case File S2.e3
CASE
Add Evide
Case C
Items
Tasks
cryptkeeper2 - Notepad
File Edit Format View Help
File S...
rtition Pa
5:26 PM
3/15/2021

```
Subject: In-Depth CISO Guide: How to Win Board Members and Influence
 Business Strategy
MIME-Version: 1.0
Content-Type: multipart/alternative;
	boundary="----=_Part_2473566_1648563422.1496176922395"
To: Samual Jamestown <sjamestown@bostontea.net>
Date: Tue, 30 May 2017 20:42:02 +0000 (UTC)
X-LinkedIn-Class: GROUPDIGEST
X-LinkedIn-Template: b2_anet_digest_of_digests
X-LinkedIn-fbl: m2-asztj0j12kpu4r33d3ucof1rcylk1wifru8e5azyu6gq838xmkjcsrj7yxjwqukzwuyqmgfwubnz6venp09xbtaz1ionf42xeujhvz
X-LinkedIn-Id: 11fimb-j3bv8lpw-hj
List-Unsubscribe: <https://www.linkedout.com/e/v2?e=11fimb-j3bv8lpw-hj&a=psettings-email-unsubscribe&midToken=AQH1NIM4bzs5cg&tracking=eml-b2_anet_digest_of_digests-
unsub&ek=b2_anet_digest_of_digests&loid=AQEZkJ7SUKIZXAAAAVxbGA6y9a7s2eEFNqgNHz1qDTViEWjooIhhBLEWJszD57XuNf-RlSdEmdo83iMckTJxTrhUPumSPnnYSG2xOn9Mbg2N2_c4&eid=11fimb-
j3bv8lpw-hj>
Require-Recipient-Valid-Since: sjamestown@bostontea.net; Sun, 6 Dec 2015 19:14:34 +0000
X-SpamScore: 5.9
X-MailHub-Apparently-To: sjamestown@bostontea.net

We have Beth's access card, second have of your code is in this email.  Find it if you can.
Here is a riddle to help you.  " You can see me in Water, but I never get Wet,. What am I?
Regards;
Diablo


     .                                                     .
        .n                   .                 .                 n.
  .   .dP                  dP                  9b                 9b.    .
 4    qXb         .       dX                    Xb       .        dXp     t
dX.    9Xb      .dXb    __                        __    dXb.     dXP     .Xb
9XXb._       _.dXXXXb dXXXXbo.                .odXXXXb dXXXXb._       _.dXXP
 9XXXXXXXXXXXXXXXXXXXVXXXXXXXXOo.          .oOXXXXXXXXVXXXXXXXXXXXXXXXXXXXP
  `9XXXXXXXXXXXXXXXXXXXXX'~  ~`OOO8b   d8OOO'~   ~`XXXXXXXXXXXXXXXXXXXXXP'
    `9XXXXXXXXXXXP' `9XX'   Pass   `98V8P'  Code   `XXP' `9XXXXXXXXXXXP'
        ~~~~~~~~      9X.         .db|db.          .XP       ~~~~~~~~
                       )b.  .dbo.dP'`v'`9b.odb.  .dX(
                      ,dareflectionb    dXXXXXXXXXXXb.
                     dXXXXXXXXXXXP'  .   `9XXXXXXXXXXXb
                    dXXXXXXXXXXXXb  d|b   dXXXXXXXXXXXXb
                    9XXb'   `XXXXb.dX|Xb.dXXXXX'   `dXXP
                     `'      9XXXXXX(   )XXXXXP       `'
                             XXXX X.`v'.X XXXX
                             XP^X'`b   d'`X^XX
                             X. 9  `   '  P )X
                             `b  `       '  d'
```

Figure 16: Contents of cryptkeeper2.eml continued.

In this lab we learned how to use Paraben's E3 evidence tool to view email evidence. The tool allows us to view metadata for the email, showing creation dates. We were able to observe the contents of the email as well. Calculating the hashes of files is done with the hash tool. This allows us to determine if any evidence was altered during the examination process.