Laboratory Report
IST602: Digital Forensics

Examination Number: 2 Date: 10/13/19
Examiner's Name: Akshay Chaurasia

Examination:

On 10/13/19, the corporate delivered a copy of the forensic image of a **.zip** file containing the registry files from Mark's computer and the imaged USB in EnCase **(.eo1)**

The corporate received an anonymous call. The caller informed the corporate security department that a trusted employee, Rodger Marks, has been selling the company's secrets to a corporate spy. The caller alleges that Marks has sent company proprietary and/or Trade Secret information to Turkey in return for a paid fishing trip.

Initially, the corporate security officers tried to find out the truth by examining the access logs and even by searching Mark's office but could not find any evidentiary value in document form that could connection mark with the corporate espionage. Even the corporate security department's digital forensic examiner conducted an examination on Mark's hard drive but did not find anything that indicated any connection between Mark's and Turkey.

Therefore, they requested me to conduct an examination and provide the company with relevant information concerning any participation by Mark in the unauthorized dissemination of proprietary or Trade Secret information.

Forensic Question(s): [Use Inman & Rudin Paradigm]

1. Identify relevant information concerning Rodger Mark, the corporate, and Turkey
2. Identify information regarding the paid fishing trip
3. Locate all document file
4. Recover and examine the files
5. Classify the information as unauthorized dissemination of Trade Secret
6. Locate any references to concerning Rodger Mark, the corporate, and Turkey
7. Associate files, media, computer, IP address with concerning Rodger Mark, the corporate, and Turkey
8. Re-construct the events/activities

Steps Taken:

1. The provided image file of the USB (forensic image #SU10132019), was loaded on the Forensic Toolkit version 1.81 and the image was indexed.
2. A search for the relevant files was conducted to find out any document related to Rodger Mark, the corporate, and Turkey

Laboratory Report
IST602: Digital Forensics

Examination Number: 2 Date: 10/13/19
Examiner's Name: Akshay Chaurasia

3. 3 e-mail threads with 4 messages were recovered from the "Overview" tab of the Forensic Toolkit
4. Sorted the emails by date
5. Then a ".html" file was recovered from the "Explore" tab
6. The recovered files were examined
7. The registry files were also examined using the Registry Viewer.

Results: After inspecting the image file of the USB using the Forensic toolkit, I found the following objects in the "Overview" tab. (Line number 3 of the Steps Taken)

- 3 email threads
- 4 email messages
- 1 .html file

After recovering these files, we found the following information/metadata (Line no 4 of the Steps Taken)

Name	File Type	Date
Message0001	Email	03/16/2007
Message0002	Email	03/17/2007
Message0003	Email	03/18/2007
Industrial Espionage File	.html	03/16/2007
Top Secret	PDF	03/17/2007

A review of the recovered emails reveals that the messages were exchanged between Rodger Mark and Tomas Turcano **(See appendix A, B and D).** It can also be seen that Mark provided Thomas some "Top Secret" file after which Thomas said that he would arrange a fishing trip for him. These files have been marked SUDF101382019" and provided to the corporate. A .html file named "Industrial Espionage" was also recovered from the provided image **(See appendix E)**

Conclusions:

The recovered files show that the messages were exchanged between Rodger Mark and Tomas Turcano. Tomas Turcano can be seen asking Rodger Mark about "Anything interesting happening at work". A PDF type file, named "Top Secret", which was sent to Tomas by Mark, was also recovered **(See appendix B and D)**. Finally, a .html file named Industrial espionage was was found in the image drive.

Laboratory Report
IST602: Digital Forensics

Examination Number: 2 Date: 10/13/19
Examiner's Name: Akshay Chaurasia

Opinions:

In my opinion, Rodger Mark did provide Thomas with some "Top Secret" information for a paid fishing trip, as informed by the anonymous caller.

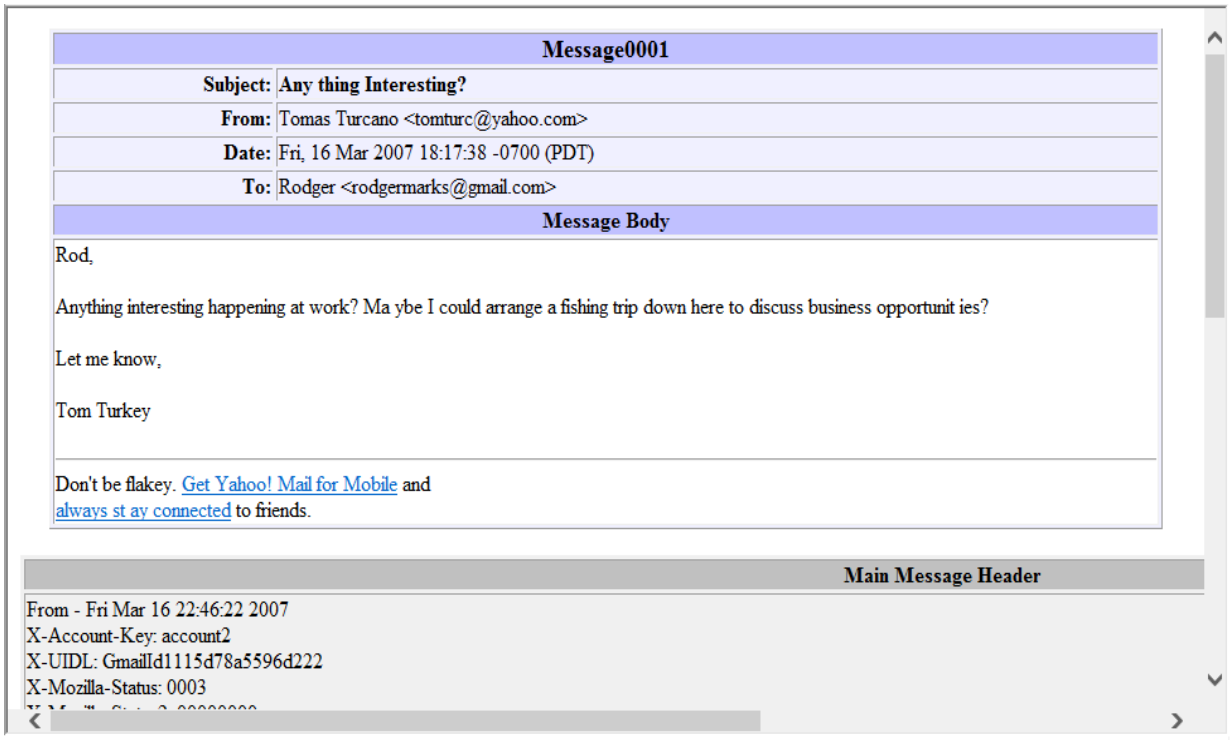
Certification:

I hereby certify that the work presented above was personally performed by me and the opinions and conclusions stated are my own and based upon the work that I performed.

Akshay Chaurasia
Signature

Appendix A

The recovered email, "Message0001" was sent by Tomas Turcano on Fri, 16 March 2007. It was addressed to Rodger Mark. It can be seen in the mail that Tomas was asking mark if "Anything Interesting was happening at work". Below is the screenshot of the content of Message0001.



Message0001

Subject:	**Any thing Interesting?**
From:	Tomas Turcano <tomturc@yahoo.com>
Date:	Fri, 16 Mar 2007 18:17:38 -0700 (PDT)
To:	Rodger <rodgermarks@gmail.com>

Message Body

Rod,

Anything interesting happening at work? Ma ybe I could arrange a fishing trip down here to discuss business opportunit ies?

Let me know,

Tom Turkey

Don't be flakey. Get Yahoo! Mail for Mobile and
always st ay connected to friends.

Main Message Header

From - Fri Mar 16 22:46:22 2007
X-Account-Key: account2
X-UIDL: GmailId1115d78a5596d222
X-Mozilla-Status: 0003

Appendix B

The recovered email, "Message0001" was sent by Rodger Mark on Sat, 17 March 2007. It was addressed to Tomas in response to his initial email. It can be seen in the mail that Mark had sent a "Top secret"file of the type .pdf to tomas. Below is the screenshot of the content of Message0001.

Message0001	
Subject:	**Re: Any thing Interesting?**
From:	Rodger Marks <Rodgermarks@gmail.com>
Date:	Sat, 17 Mar 2007 17:30:58 -0400
To:	Tomas Turcano <tomturc@yahoo.com>

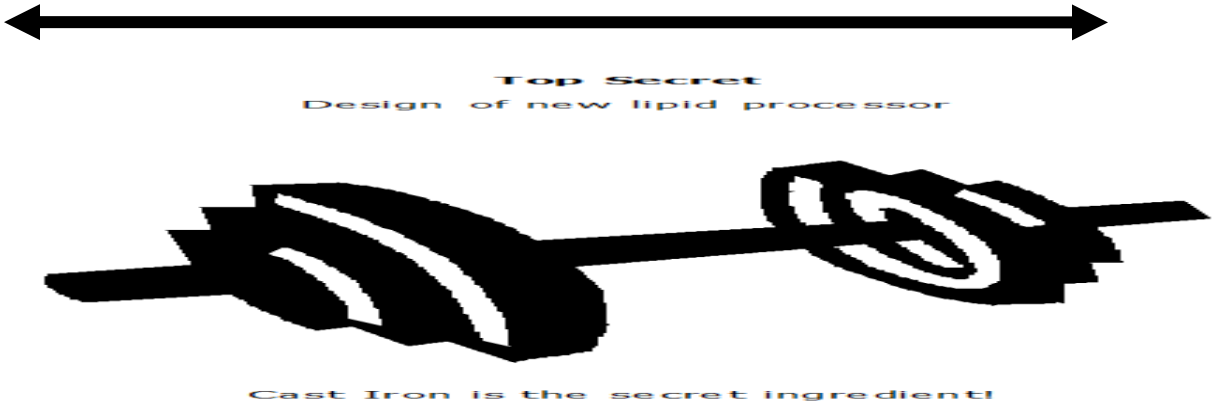
Message Body

Tomas Turcano wrote:
> Rod,
>
> Anything interesting happening at work? Maybe I could arrange a
> fishing trip down here to discuss business opportunities?
>
> Let me know,
>
> Tom Turkey
>
> ---
> Don't be flakey. Get Yahoo! Mail for Mobile
> <http://us.rd.yahoo.com/evt=43909/*http://mobile.yahoo.com/mail> and
> always stay connected
> <http://us.rd.yahoo.com/evt=43909/*http://mobile.yahoo.com/mail> to
> friends.
Do you think this would be enough for a week of bonefishing?

Rod

Attachment

-----Attachment1-----
File name = "Top Secret.pdf"



Appendix C

The recovered email, "Message0002" was sent by Sally Smith on Sat, 17 March 2007. It was addressed to Mark. Below is the screenshot of the content of Message0002.

Message0002	
Subject:	**Thinking of you....**
From:	"Sally Smith" <sallysmith645@hotmail.com>
Date:	Sat, 17 Mar 2007 21:43:55 +0000
To:	rodgermarks@gmail.com
Message Body	

When I saw this I thought of you. Hope your new venture give us lots of
money to enjoy life!

http://money.cnn.com/magazines/fortune/fortune_archive/2007/03/19/8402362/index.htm

Sally

---

i'm making a difference. Make every IM count for the cause of your choice.
Join Now.
http://clk.atdmt.com/MSN/go/msnnkwme0080000001msn/direct/01/?href=http://im.live.com/messenger/im/home/?source=hmtagline

Appendix D

The recovered email, "Message0003" was sent by Tomas on Sun, 18 March 2007. It was addressed to Mark in response to his initial email. It can be seen in the mail that Tomas is talking about a fishing trip that he has earned. Below is the screenshot of the content of Message0003.

Message0003	
Subject:	**Get Packing**
From:	Tomas Turcano <tomturc@yahoo.com>
Date:	Sun, 18 Mar 2007 07:17:14 -0700 (PDT)
To:	Rodger Marks <rodgermarks@gmail.com>
Message Body	
I think you earned your fishing trip! I'll call you at home to arrange. Turkey	
8:00? 8:25? 8:40? Find a flick in no time with the Yahoo! Search movie showtime shortcut.	

Appendix E

The recovered .html file, "Industrial Espionage" found in the image of the USB drive provided by the corporate. Below is the screenshot of the content of .html file.