



Name: Jesse Russell

Case Study 1 - Bob Jones, industrial espionage (read no action) Case description: Bob Jones works for Mr. Cookie (MRC) and has been a valued staff member in the finance division for twelve years. About 6 months ago, Mr. Jones began acting erratically different from his usual persona. He was noticed to quickly change his computer screen when anyone entered his office. He has purchased a new car that seems outside of his salary reach. He also has been noticed working late and on weekends. His manager, Kathy Stevens, reported this odd behavior to Human Resources so that Bob would have a person to talk with if he chooses to do so. When HR reached out to Bob and met in his office, they found him to be irritable, agitated, and angry. Additionally, upon first arriving, HR staff noticed Bob removing a flash drive from his computer and placing it in his pocket. As removable storage devices are not allowed at MRC, the HR staff asked Bob to turn over the flash drive and go home for the weekend (it was Friday at 2pm). Bob furnished the thumb drive and complained that MRC was invading his privacy, claiming that the thumb drive contained only family pictures. The thumb drive was taken with no discussion. Bob was so angry that he unplugged his machine on his way out. After Bob left, HR then put the thumb drive on the desk and sealed the room by contacting the IT security team who arrived and removed Bob's access from the pin code door. Security also removed all pins except for HR, Security, and Kathy Stevens. Security then acquired images from the computer, two found flash drives, and proceed to move all the original equipment to a highly secure locked area of the company. Bob's computing account is mrc42. Paul is a former administrator to the CEO. The images have now been passed on to you, a forensics expert within the security team. The hard drive hash and corresponding image hash have been proven to match. The thumb drive hash and corresponding image hash have been proven to match. The image files are in dd format and therefore can be used with many tools.



The information security policies in the company include the following: (read, remember as you process evidence)

1. Confidential paper documents and electronic files are the sole property of MRC and should not be distributed outside of the company. Examples – Patents, formulas, trade secrets, customer lists, unpublished financial information
2. Avoid transferring sensitive data (e.g. customer information, employee records, confidential) to other devices or accounts. When mass transfer of such data is needed, we request employees to ask our [Security Specialists] for help.
3. Remember passwords instead of writing them down.
4. No use of removable storage devices is permitted.
5. Share confidential data over the company network/ system and not over public Wi-Fi or private connection.
6. Ensure that the recipients of the data are properly authorized people or organizations and have adequate security policies.
7. Report scams, privacy breaches and hacking attempts.
8. MRC proprietary information stored on electronic and computing devices whether owned or leased by MRC, the employee or a third party, remains the sole property of MRC and can not be transferred or removed without written approval.
9. All MRC electronic and computing resources are the property of MRC and are not to be used for anything outside of company work. MRC reserves the right to investigate the equipment as needed for any purpose.
10. BYOD - any personal electronic device attached to MRC IT solutions (IE corporate WIFI, LAN, etc.) are subject to all MRC policy.
11. MRC email systems are for the sole purpose of MRC business.



1. Assignment: Formatting and Requirements

- The report should be thorough and professional. Assume someone who isn't in Information Security or Information Technology will be reading this report. Explain what how you got the evidence, and what that evidence means to the scenario.
- The report should be free of grammar, spelling, and other writing errors. Screenshots should be sized to be easier for reading (as shown in sample cases)
- Submit in PDF

2. Target System & Devices

- Suspect computer- running Windows 10, NTFS
- Suspect USB drive – 8gb NTFS
- The physical systems are locked securely and have not been touched by any person except the security team to make images. A hash value of the images taken from Bob's computer match the copy that is provided in this case study.

3. Initial evidence (list as found) **EVIDENCE MUST BE ALPHABETIC ORDER; ANALYSIS MUST FOLLOW SAME ORDER**

Item to analyze (File name)	Analyzed by	Completed on
Agenda.docx	Jesse Russell	3/5/21
Customer Reference List Template.xlsx	Jesse Russell	3/5/21
Family1.jpg	Jesse Russell	3/5/21
Family2.jpg	Jesse Russell	3/5/21
Family3.jpg	Jesse Russell	3/5/21
Family4.jpg	Jesse Russell	3/5/21
Family Picture.eml	Jesse Russell	3/5/21
IMG-1189.JPG	Jesse Russell	3/5/21
To do.txt	Jesse Russell	3/5/21



4. Tool listing

ProDiscover Basic, Version 8.2.0.2

ProDiscover is a tool used by investigators to find and analyze a drive's contents, even if they're deleted. See: <https://www.prodiscover.com/>

Hexed.it

Hexed.it is an online, browser-based tool that allows investigators to analyze and edit the hex values of any given file. See: <https://www.hexed.it/>

WinMD5 Free

WinMD5 is a free utility that allows investigators to calculate the MD5 hash value of any given file. See: <https://www.winmd5.com/>

1. Agenda.docx

- a. Found on USB2. This appears to be an agenda, detailing his agenda presumably for his work at MRC.

- b. Hash: 190a67f38707d2c97fba8c65133fd1a3

To do for meeting:

- 1. Prepare financial statements
- 2. Meet with Marketing Dept about new cookie launch
- 3. Have fresh samples ready from Corp Kitchen

- c. Image:

2. Family1.jpg

- a. Found of flash drive seized from Bob. This appears to be a picture of a family. The does not seem to be evidence of steganography in this file.

- b. Hash: 179271095bf7c95e1aef0887463b4f43



- c. Image:

3. Family2.jpg

- a. Found on flash drive seized from Bob. This appears to be an innocent picture of a family. However, steganography was used to hide other files inside this file.


- b. Hash: 2e363996fc1a2e5d7c5dc44cfe5598f3



- c. Image:

i. Espresso.pdf

1. This file was found hidden inside family.jpg using reverse steganography. It looks to be a PDF of a cookie recipe.
2. Hash: aa6ee1e52fc46a150041d490a1f8a842
3. Image:



Walmart

Walmart
2515 Ellsworth Rd
YPSILANTI, MI 48197
Sponsored

Cardamom and Espresso Chocolate Chip Cookies

★★★★★

Prep

35 m

Cook

10 m

Ready In

45 m

Recipe By: Kim

"Add some zing to your chocolate chip cookies with a bit of espresso and cardamom flavor! These are somewhat thin and chewy cookies, which makes them perfect for dunking into your morning cup of coffee."

Ingredients

3 1/4 cups all-purpose flour
1 teaspoon baking powder
1 teaspoon baking soda
1 teaspoon ground cardamom
1/2 teaspoon ground cinnamon
1/2 teaspoon salt
1 1/2 cups brown sugar, firmly packed

1 cup unsalted butter, softened
1/2 cup white sugar
2 large eggs, at room temperature
2 tablespoons instant espresso powder
1 tablespoon vanilla extract
1 (12 ounce) bag semisweet chocolate chips

Directions

- Preheat the oven to 350 degrees F (175 degrees C). Line 2 baking sheets with parchment paper.
- Whisk flour, baking powder, baking soda, cardamom, cinnamon, and salt together in a bowl.
- Cream brown sugar, butter, and white sugar together in a bowl until fluffy. Beat in eggs 1 at a time until thoroughly combined. Mix in instant espresso powder and vanilla extract.
- Mix flour mixture into the butter mixture until just combined; do not overmix. Fold in chocolate chips.
- Drop dough by the tablespoon onto the prepared baking sheets about 2 inches apart.
- Bake in the preheated oven until edges of cookies are set, 10 to 15 minutes. Cool cookies on the pans 2 to 3 minutes before transferring to a wire rack to cool completely.

ALL RIGHTS RESERVED © 2019 Allrecipes.com
Printed From Allrecipes.com 3/4/2019

Pete and Gerry's – Organic Eggs
Organic Cage Free Large Grade AA Eggs 12 Ct
\$4.74 for 1 item - expires in 5 days

McCormick Pure Vanilla Extract 2 Fl Oz
\$6.83 for 1 item - expires in 5 days

C&H Pure Cane Granulated Sugar 4 Lb
\$1.78 for 1 item - expires in a month

ii. Oatmeal.pdf

1. This file was found hidden inside family.jpg using reverse steganography. It looks to be a PDF of a cookie recipe.
2. Hash: b6e56a00dc94c43547510e2d07b76da6
3. Image:



Soft Oatmeal Cookies

★★★★★

Prep	Cook	Ready In
15 m	10 m	2 h



Walmart
2515 Ellsworth Rd
YPSILANTI, MI 48197
Sponsored

Recipe By: BITTERSWEET1

"These oatmeal cookies are very moist with a good flavor. Add a cup of raisins or nuts if you desire."

Ingredients

1 cup butter, softened	2 cups all-purpose flour
1 cup white sugar	1 teaspoon baking soda
1 cup packed brown sugar	1 teaspoon salt
2 eggs	1 1/2 teaspoons ground cinnamon
1 teaspoon vanilla extract	3 cups quick cooking oats

Directions

- 1 In a medium bowl, cream together butter, white sugar, and brown sugar. Beat in eggs one at a time, then stir in vanilla. Combine flour, baking soda, salt, and cinnamon; stir into the creamed mixture. Mix in oats. Cover, and chill dough for at least one hour.
- 2 Preheat the oven to 375 degrees F (190 degrees C). Grease cookie sheets. Roll the dough into walnut sized balls, and place 2 inches apart on cookie sheets. Flatten each cookie with a large fork dipped in sugar.
- 3 Bake for 8 to 10 minutes in preheated oven. Allow cookies to cool on baking sheet for 5 minutes before transferring to a wire rack to cool completely.

ALL RIGHTS RESERVED © 2019 Allrecipes.com
Printed From Allrecipes.com 3/4/2019


Pete and Gerry's –
Organic Eggs
Organic Cage
Free Large Grade
AA Eggs 12 Ct
\$4.74 for 1 item -
expires in 5 days


McCormick 
Pure Vanilla
Extract 2 Fl Oz
\$6.83 for 1 item -
expires in 5 days

C&H Pure Cane 
Granulated
Sugar 4 Lb
\$1.78 for 1 item -
expires in a
month

iii. Snickerdoodle.pdf

1. This file was found hidden inside family.jpg using reverse steganography. It looks to be a PDF of a cookie recipe.
2. Hash: 8c595513172ec2e122e2e3c935dae8ad
3. Image:



Walmart 

Walmart
2515 Ellsworth Rd
YPSILANTI, MI 48197
Sponsored

Mrs. Sigg's Snickerdoodles

★★★★★

Prep 20 m	Cook 10 m	Ready In 1 h
--------------	--------------	-----------------

Recipe By: Beth Sigworth

"These wonderful cinnamon-sugar cookies became very popular with my friends at church. My pastor loves them! You will too! Crispy edges, and chewy centers; these cookies are a crowd pleaser for sure!"

Ingredients

1/2 cup butter, softened 1/2 cup shortening 1 1/2 cups white sugar 2 eggs 2 teaspoons vanilla extract 2 3/4 cups all-purpose flour	2 teaspoons cream of tartar 1 teaspoon baking soda 1/4 teaspoon salt 2 tablespoons white sugar 2 teaspoons ground cinnamon
---	--

Directions

- 1 Preheat oven to 400 degrees F (200 degrees C).
- 2 Cream together butter, shortening, 1 1/2 cups sugar, the eggs and the vanilla. Blend in the flour, cream of tartar, soda and salt. Shape dough by rounded spoonfuls into balls.
- 3 Mix the 2 tablespoons sugar and the cinnamon. Roll balls of dough in mixture. Place 2 inches apart on ungreased baking sheets.
- 4 Bake 8 to 10 minutes, or until set but not too hard. Remove immediately from baking sheets.

ALL RIGHTS RESERVED © 2019 Allrecipes.com
Printed From Allrecipes.com 3/4/2019

Pete and Gerry's –
Organic Eggs
Organic Cage
Free Large Grade
AA Eggs 12 Ct
\$4.74 for 1 item -
expires in 5 days

McCormick
Pure Vanilla
Extract 2 Fl Oz
\$6.83 for 1 item -
expires in 5 days

C&H Pure Cane
Granulated
Sugar 4 Lb
\$1.78 for 1 item -
expires in a
month

4. Family3.jpg

- a. Found on flash drive seized from Bob. This appears to be a picture of a family. The does not seem to be evidence of steganography in this file.
- b. Hash: b12cde61e302de417ba110b1349b660d



- c. Image:

5. Family4.jpg

- Found on flash drive seized from Bob. This appears to be a picture of a family. The does not seem to be evidence of steganography in this file.
- Hash: e05e2f86b9fe2851624bbe328cb9ee09



c. Image:

6. Customer Reference List Template.xlsx

- Found in recycle bin of Bob's computer. This is an excel file detailing new MRC clients. There does not appear to be anything suspicious about this file, but since this is confidential information, this should be stored in a more secure location than the recycle bin or deleted entirely.
- Hash: fa2a448561b61de2a1f5e80b4115e830
- Image:

MR. Cookie new client contacts for March 2019						
Customer Name	Job Address	City	Phone #	Last purchase amount	Resell Company	Mark up
Reimer, Dick	3519 Pine Forest Drive	Green Bay	606-0365	\$ 300,000.00	Cookie Factory	56%
Callahan, Mark	218 Nob Hill Lane	De Pere	362-3825	\$ 25,000.00	Mark's Sweets	48%
Baranczyk, Kay	2916 Copper Mountain Court	Green Bay	373-4849	\$ 978,000.00	Cookie Bar	36%
Trupke, Tim	1811 Grace Street	De Pere	676-2184	\$ 11,000.00	Bayside Cookies	53%
Gustafson, Bob	3209 Ferndale Acres Drive	Hobart	498-2424	\$ 3,500.00	TBC - trial case	44%
VanDenHoven, Bob	1228 O'Keefe Court	De Pere	609-0491	\$ 3,200,000.00	Mrs. Weeds	29%
CONFIDENTIAL						

7. Family Picture.eml

- Found in recycle bin of Bob's computer
- Email Content:

I do have the picture it's attached!! Hope it's enough to fill you up for a while!
Bob
- Hash: 8e35c98c1f1753b40e893cb7a9b26418
- Email Data:
 - Sender: keptasecret427@yahoo.com
 - Domain: www.yahoo.com
 - Sent date: Mon, 4 Mar 2019 17:50:25
 - Receiver: keepasecret427@gmail.com
 - Domain: www.gmail.com
 - Received date: Mon, 4 Mar 2019 09:50:29
 - SMTP Sever: 66.163.184.147

e. Attached File – Base64 encoded

i. Email Attachment.jpg

1. This appears to be an innocent picture of a family, but steganography was used to hide a zip file inside the attachment.
See below
2. Hash: ffb79dbe4f9ed5ba7f45b3730aed6113
3. Image:



a. Cookie1.jpg

- i. This image was found inside the zip folder hidden in the email attachment.
- ii. Hash: aaa1e2b1c02ed0653a8729fb1a5f33a8
- iii. Image:



- b. Cookie 2.jpg
 - i. This image was found inside the zip folder hidden in the email attachment. It had its header and extension changed to make it look like a PDF. Correcting the header and extension resulted in finding cookie 2.jpg.
 - ii. Hash: 0a1dd806e8a6880e6014e5f5773e0f19
 - iii. Image:




- 8. IMG-1189.JPG
 - a. Found on USB2. This is an image of cookies.
 - b. Hash: 40005b165d57421f461f348cd298f6fd



- c. Image:

9. To do.txt

- a. Found in recycle bin of Bob's computer. This appears to be a reminder to Bob to call a person who works for a competitor to MRC, setting up a transfer of some kind.
- b. Hash: c5e15b4c00bc0f1693a3442575c15506
- c. Image:

 R331FX9.txt - Notepad

File Edit Format View Help

Call Terry at Competitive Cookies and set up next transfer



Final analysis:

a. What MRC policy was broken?

Policy Number	Policy
1	Confidential paper documents and electronic files are the sole property of MRC and should not be distributed outside of the company. Examples – Patents, formulas, trade secrets, customer lists, unpublished financial information
2	Avoid transferring sensitive data (e.g. customer information, employee records, confidential) to other devices or accounts. When mass transfer of such data is needed, we request employees to ask our [Security Specialists] for help.
4	No use of removable storage devices is permitted.
6	Ensure that the recipients of the data are properly authorized people or organizations and have adequate security policies.
8	MRC proprietary information stored on electronic and computing devices whether owned or leased by MRC, the employee or a third party, remains the sole property of MRC and can not be transferred or removed without written approval.

b. Final conclusion

In my professional opinion, it is clear that Bob Jones broke multiple company policies, and may be selling company secrets to competitors of MRC. For instance, Bob had multiple recipes and pictures of cookies hidden inside seemingly innocent pictures of his family, using steganography. The fact that these files were hidden hints to the conclusion that Bob had a reason to hide these files, and implies he is selling those to other companies. An email was sent from Bob's computer that contained a picture of his family, but steganography was used to hide more pictures of cookies. The email is signed from Bob, but the .eml file shows it was sent from James Banfield. This may be an alias of Bob's, or a real other person. This piece of evidence may require further investigation.