Charles Dulin

James Banfield

IA427 Digital Forensics

October 30th, 2024

A-427
Forensics Report
Internal Case
Tavon Jackon
Incident Status: In progress
Report written by:
TBD

Revision: 1
Read the requirements carefully to avoid overwork.
This is an individual assignment. Do not help each other in any way – no tips, no posting on Discord, Canvas, or anywhere else. This would be considered cheating.
Name:
Case Study 1 - Tavon Jackson works for Mr. Cookie (MRC) and has been a valued staff member in
the finance division for twelve years. About six months ago, Mr. Jones began acting erratically different from his usual persona. He was noticed to change his computer screen when anyone entered his office quickly. 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 Tavon would have a person to talk with if he chooses to do so. When HR reached out to Tavon and met him in his office, they found him irritable, agitated, and angry. When arriving, HR staff noticed Tavon 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 Tavon to turn over the flash drive and go home for the weekend (it was Friday at 2
pm). Tavon furnished the thumb drive and complained that MRC was invading his privacy, claiming that the thumb drive contained only pictures of buildings. Photographing unique architecture is a hobby for Mr. Jackson. The thumb drive was taken with no discussion. Tavon was so angry that he unplugged his machine on his way out. After Tavon left, HR put the thumb drive on the desk and sealed the room by contacting the IT security team, who arrived and removed Tavon's access from the pin code door. Security also removed all pins except HR, Security, and Kathy Stevens. Security then acquired images of the computer and flash drive and

moved all the original equipment to a highly secure, locked company area. 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 can be used with many different forensic analysis tools.

IA-427
Forensics Report
Internal Case
Tavon Jackon
Incident Status: In progress
Report written by:
TBD
Revision: 1

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. No use of removable storage devices is permitted.
3. 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.
4. All MRC electronic and computing resources are the property of MRC and may not be used for anything other than company work. MRC reserves the right to investigate the equipment as needed for any purpose.

1. Assignment: Formatting and Requirements
• There are two files to download from our class share:
o Tjackson_usb ~16GB
o TJackson_CPU ~25GB
• Follow the guidelines and expectations we have discussed for a full report
• The report should be thorough and professional.
• The report should be free of grammar, spelling, and other writing errors.
• Submit in PDF.
• Any image, discussion, or mention of anything related to a cookie supports the charge against Mr. Jackson.
• There are 14 artifacts in this case; every artifact is marked with an artifact number.
• No files have been deleted.

• Easter eggs - You are not required to locate and report on the EE.
• Easter egg information can be found on the Jackson computer. There are at least two places where you will find data. There are no files, but information related to the case can be found. They will not be marked as Easter eggs but will count to 3 extra credit points. If you pursue the extra credit, report on what you find using the formal full report format we have discussed and add the items at the end of your CPU analysis.
• Some images will have Exif info; ignore Exif analysis for this case (treat as jpeg).
• Your first six computer artifacts (based on your ordering of found artifact numbers) should have the full bullet report analysis and artifact image.
• The remaining artifacts should have the following analysis in addition to the artifact image:
o Name of file & deleted name if deleted
o Artifact number
o Work done to recover
o Notice of suspicious work
o Direction of evidence
2. Tool listing
3. Thumb drive analysis
4. Computer image analysis
5. Conclusion

Tools:

- Autopsy 4.21.0 is a version of the digital forensics platform autopsy, but comes with new features. It can be used to process images on removable USB devices and harddrives.
- Hexed.it is a web software that displays binary and hexadecimal data as a grid of cells. The data is also made up of editable hex codes.

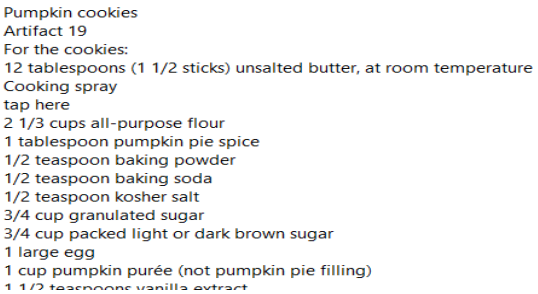
1. **File name:** GATE.jpg
2. **Artifact** 17
3. 203ecd203901b2bc1dff5e1591503fcb
4. GATE.jpg is a jpg file

5. File was stored on TJackson's computer: in the Desktop folder, recovered using autopsy.
6. File opened, there was no work done to recover. Standard bit-stream copy, extracted using autopsy.
7. Used Hexed.it and found a hidden file via steganography inside the GATE.jpg file.
8. The image is a hobby for Mr. Jackson. Taking and having pictures of unique architecture is Mr. Jacksons hobby. ALL electronic computing resources are property for MRC and should only be used for work purposes. Computer was also unplugged before investigation. MRC reserves the right to investigate as needed; that seemed to be a suppression of evidence tactic. Seems there was a file transferred into the GATE.jpg file.
9. **policy analysis** - Jackson is in breach of policy
   A. Policy 3: 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. Policy 4: All MRC electronic and computing resources are the property of MRC and may not be used for anything other than company work. MRC reserves the right to investigate the equipment as needed for any purpose.

1. **File Name:** No file name
2. **Artifact** 31
3. C0f9a83db6a9ea4d0f095e4b46e1c4fc
4. This file was a jpg file
5. File was stored inside of the GATE.jpg file. Recovered using hexed.it.
6. Used Hexed.it to recover the image. Searched file headers for jpegs and found a second header. Deleted the bytes before the second header, then exported the rest of the bytes after deletion.
7. This is a file of a cookie that was stored inside of a picture of unique architecture. Taking pictures of unique

architecture is a hobby for Mr. Jackson. Any pictures of cookies is supporting the charge against Mr. Jackson.

8. The image is of a specially designed cookie. Any image or discussion or anything related to cookies supports the evidence against Mr. Jackson. Mr. Jackson Could have been distributing images of cookies to outside sources. Transferred a jpg file of a cookie into a file of architecture, also claimed having photos of architecture was just a hobby of his. Having a picture of a cookie seems to not be for work purposes. This could have been a cookie designed by MRC.
9. **policy analysis** - Jackson is in breach of policy
    A. 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
    B. Policy 3: 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.


Pumpkin cookies
Artifact 19
For the cookies:
12 tablespoons (1 1/2 sticks) unsalted butter, at room temperature
Cooking spray
tap here
2 1/3 cups all-purpose flour
1 tablespoon pumpkin pie spice
1/2 teaspoon baking powder
1/2 teaspoon baking soda
1/2 teaspoon kosher salt
3/4 cup granulated sugar
3/4 cup packed light or dark brown sugar
1 large egg
1 cup pumpkin purée (not pumpkin pie filling)
1 1/2 teaspoons vanilla extract

1. **File Name:** pumpkin.xlsx
2. **Artifact** 19
3. b9ffbbd9876ebd90a681d04e1478f0f6
4. File was a xlsx file, but I couldn't open the file so I supplied a screenshot inside of the autopsy software.
5. File was stored on Jackson's computer: in the Documents folder, recovered using autopsy.
6. Used autopsy to search through Jackson's computer and looked through the documents. Found an xlsx file; Standard bit-stream file and extracted using autopsy.
7. File couldn't open. Tried changing the file extension and file header, but the file still couldn't open. When I uploaded the file into hexed.it it seemed as if bytes were missing/

replaced with different bytes, lots of 00 bytes in the editable hex codes. I could see the contents of the file inside the autopsy software, so I screenshotted that and supplied it for evidence.

8. This file is an instruction manual for making pumpkin cookies. Any type of evidence found relating to the discussion of cookies supports the evidence against Mr. Jackson. These instructions could have been distributed outside of the workplace. Don't know how or why he would have this file in his computer, it doesn't seem to be company work. File seems to be transferred to his computer. Mr. Jackson also unplugged the computer before investigation, believed to be an attempt on suppression of evidence. MRC reserves the right to investigate as needed
9. **policy analysis** - Jackson is in breach of policy
    A. 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
    B. Policy 3: 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.
    C. Policy 4: All MRC electronic and computing resources are the property of MRC and may not be used for anything other than company work. MRC reserves the right to investigate the equipment as needed for any purpose. 1. Assignment: Formatting and Requirements

artifact 73

The Best Snickerdoodle Cookie Recipe

★★★★★ 4.97 from 1122 votes

The Best Snickerdoodle Cookie Recipe. Soft and Chewy Snickerdoodle Cookies. The popular cinnamon-sugar soft and chewy sugar cookie recipe. A recipe that has been in the family for over 30 years!

Prep Time	Cook Time	Total Time
15 mins	10 mins	25 mins

Course: Dessert Cuisine: American Keyword: snickerdoodle cookies Servings: 24

Equipment

- kitchenaid mixer
- baking sheet
- parchment paper baking sheets
- measuring cups and spoons
- spatula set
- turner
- cookie scoop

Ingredients

- 1 cup Unsalted Butter (softened)
- 1 1/2 cups Sugar
- 2 large Eggs
- 2 teaspoons Vanilla
- 2 3/4 cup Flour
- 1 1/2 teaspoon Cream of Tartar (for less tang, use 1 teaspoon)
- 1/2 teaspoon Baking Soda
- 3/4 teaspoon Salt

1. **File Name:** snickerdoodle.pdf
2. **Artifact 73**
3. 633cbe83178a731b124bb4be27ff5333
4. File is a pdf file
5. File was located on Jackson's computer: in the documents folder, recovered using autopsy.
6. Standard bit stream copy, extracted using autopsy. No problems when opening the file.

7. This pdf file is a cookie recipe, anything related to cookies in discussion or images supports the evidence against Mr. Jackson. Also there was a file stored inside of snickerdoodle.pdf via steganography.
8. Any image or discussion related to cookies supports the claims/ evidence against Mr. Jackson. These instructions could have been distributed outside of the workplace. This file doesn't seem to align with his line of work, or used for work purposes. File seems to be transferred to his computer. There was also a file hidden inside of snickerdoodle.pdf. Mr. Jackson also unplugged the computer before investigation, believed to be an attempt on suppression of evidence. MRC reserves the right to investigate as needed.
9. **policy analysis** - Jackson is in breach of policy
    A. 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
    B. Policy 3: 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.
    C. Policy 4: All MRC electronic and computing resources are the property of MRC and may not be used for anything other than company work. MRC reserves the right to investigate the equipment as needed for any purpose.

1. **File Name:** No name of file
2. **Artifact** 3
3. 83536086166ac07aaae92cddd986e6e9
4. File is a jpg file
5. File was stored inside of the snickerdoodle.pdf file. Recovered using autopsy.
6. Used hexed.it to recover. Searched for file headers in snickerdoodl.pdf for jpegs, even though snickerdoodle.pdf is a df file, and found a jpg header. Deleted the bytes before the header, then exported the rest of the bytes after deletion.

7. Any image relating to a cookie is evidence supporting the claims against Mr. Jackson. This was a file hidden inside of another file that was related to a cookie recipe. This could have been the finished product of the cookie recipe.
8. Anything related to cookie is supporting evidence against Mr. Jackson. This file was also transferred into another file, which was a pdf file of a snickerdoodle cookie recipe. This file doesn't seem to be used for company work purposes.
9. **policy analysis** - Jackson is in breach of policy
    A. 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
    B. Policy 3: 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.

1. **File Name:** SPACE.jpg
2. **Artifact** 44
3. b5c8a5111db6638fc83fd1320e4f3216
4. File is a jpg file
5. File was located on Jackson's computer: in the pictures folder. Recovered using autopsy.
6. Standard bitstream copy. Extracted using autopsy.
7. Hidden file inside of SPACE.jpg file, found this information by using hexed,it. File opened with no problems.
8. Used hexed.it and found there was a hidden zip file inside of this jpg picture named SPACE.jpg. Company electronics should be used for work purposes only. Taking and having pictures of architecture is a hobby for Mr. Jackson, this picture is not for work purposes. Mr. Jackson also unplugged the computer before investigation, believed to be an attempt on suppression of evidence. MRC reserves the right to investigate as needed.
9. **policy analysis** - Jackson is in breach of policy

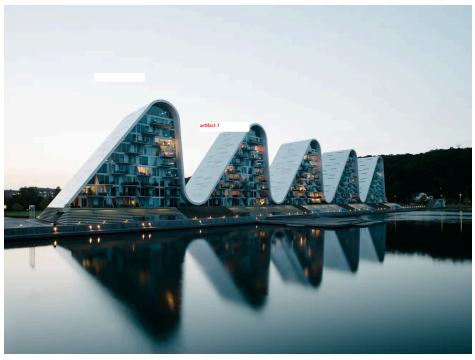
A. Policy 4: All MRC electronic and computing resources are the property of MRC and may not be used for anything other than company work. MRC reserves the right to investigate the equipment as needed for any purpose.

1. **File Name:** christmas.jpg
2. **Artifact** 56
3. 65d3cd5a4417f6d73d6b062d6f8b0405
4. File type is a jpg file type
5. File was located inside of a zip folder, which was hidden inside of a jpg file. Recovered using hexed.it.
6. Uploaded SPACE.jpg file into hexed.it. Looked for the end of a jpg file, searching for FF D9. Found the end of the jpg, and the start of a new file. I then exported the bytes of the file ending in FF D9. I then Changed file extension of the new file from jpg to zip. Then the christmas.jpg file was one of the files located in the zip folder.
7. Any image relating to cookies is supporting evidence against Mr. Jakson. The image was hidden inside of a zip file, which the zip file was hidden inside of a jpg file.
8. Any image or discussion relating to cookies is supporting evidence against Mr. Jackson. Pictures of cookies could be confidential. This picture of cookies was transferred into another file, which seemed to be an attempt to hide the picture inside of another file. The computer was unplugged before investigation, which seemed to be an attempt to suppress or delete evidence.
9. **policy analysis** - Jackson was in breach of policy
    A. 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

B. Policy 3: 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.

1. **File Name:** cookies.jpg
2. **Artifact** 4
3. 5cf1ea1624cb765eba7f3b16444a65d5
4. File is a jpg file
5. File was located inside of a zip folder, which was hidden inside of a jpg file. Recovered using hexed.it.
6. Uploaded SPACE.jpg file into hexed.it. Looked for the end of a jpg file, searching for FF D9. Found the end of the jpg, and the start of a new file. I then exported the rest of the new file. Changed file extension of the new file from jpg to zip. Then the cookies.jpg file was one of the files located in the zip folder.
7. Any image relating to cookies is supporting evidence against Mr. Jakson. The image was hidden inside of a zip file, which the zip file was hidden inside of a jpg file.
8. Any image or discussion relating to cookies is supporting evidence against Mr. Jackson. Pictures of cookies could be confidential. This picture of cookies was transferred into another file, which seemed to be an attempt to hide the picture inside of another file.
   policy analysis - Jackson was in breach of policy
   A. 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
   B. 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.

1. **File Name:** tokyo.jpg
2. **Artifact** 63
3. c2c03e98ae8cf6f657ece16ca4022c75
4. File is a jpg file
5. File was located on Jackson's computer: in the downloads folder.
6. Standard bitstream copy. Extracted using autopsy.
7. Pictures of architecture is a hobby of Mr. Jackson, architectural pictures should still not be on company computers. Attempts of hiding files were used before with Jackson's hobby, taking pictures of unique architecture. There was no sign of hidden files inside of tokyo.jpg. The file opened with no problems.
8. The picture is of architecture, which is a hobby of Mr. jackson. Attempts of hiding files were used before with Jackson. File seems to be transferred onto the company computer, company computers should be for work purposes only.
9. **policy analysis** - Jackson is in breach of contract
    A. Policy 3: 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. Policy 4: All MRC electronic and computing resources are the property of MRC and may not be used for anything other than company work. MRC reserves the right to investigate the equipment as needed for any purpose.



1. **FIle Name: wave.jpg**
2. **Artifact** 7
3. 1a25641db4ce561209965845f8008bfe
4. File type is a jpg file
5. File was stored on Jackson's computer: in the pictures folder. Recovered using autopsy.
6. Standard bitstream copy. Extracted using autopsy.
7. Uploaded file into hexed.it. File seemed to be a png file, so I switched the file header to png. The file still opened with no problems.
8. Taking pictures of unique architecture is a hobby of Mr. Jackson's. MRC computers should be used for work purposes only. This picture seemed to be transferred onto Mr. Jackson's computer. Computer aws also unplugged before investigation, which seemed to be an attempt of suppressing or deletion of evidence. MRC reserves the right to investigate as needed
9. **policy analysis** - Jackson is in breach of policy
    A. Policy 3: 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. Policy 4: All MRC electronic and computing resources are the property of MRC and may not be used for anything other than company work. MRC reserves the right to investigate the equipment as needed for any purpose.

1. **File Name:** EMPIRE.jpg
2. **Artifact** 23
3. Standard bitstream copy. Extracted using autopsy.
4. Taking/ having pictures of unique architecture is a hobby for Mr. jackson. Having pictures of Architecture on company computers is still against company policy.

Attempts of hiding files were used before with Jackson's hobby, taking pictures of unique architecture. There was no sign of hidden files inside of tokyo.jpg. The file opened with no problems.

5. The image is of architecture and is a hobby of Mr. Jackson's, but architectural pictures Should still not be on a USb plugged into a work computer.
   Company computers are for work use only. No use of removable storage devices is permitted.

1. **File Name:** 432park.jpg
2. **Artifact** 45
3. Standard bitstream copy, extracted using autopsy.
4. Pictures of architecture is a hobby of Mr. Jackson, architectural pictures should still not be on personal USB, with the USB being used on company computers. Attempts of hiding files were used before with Jackson's hobby, taking pictures of unique architecture. There was no sign of hidden files inside of 432park.jpg. The file did not open with no problems. I had to switch the header of the file in hexed.it. Then the file opened.
5. The picture is of architecture, which is a hobby of Mr. jackson. Attempts of hiding files were used before with Jackson. No pictures of unique architecture should be on a personal USB plugged into a company computer. No use of removable storage devices is permitted. Header in the file needed to be changed for it to open, this means that the header of the file was changed so the file can't open.

1. **File Name:** Guggenheim.jpg
2. **Artifact:** 21
3. Standard bitstream copy, extracted using autopsy.

4. Pictures of architecture is a hobby of Mr. Jackson, architectural pictures should still not be on personal USB, with the USB being used on company computers. Attempts of hiding files were used before with Jackson's hobby, taking pictures of unique architecture. There was no sign of hidden files inside of guggenheimk.jpg. The file did not open with no problems. I had to switch the header of the file in hexed.it. Then the file opened.
5. The picture is of architecture, which is a hobby of Mr. jackson. Attempts of hiding files were used before with Jackson. No pictures of unique architecture should be on a personal USB plugged into a company computer. No use of removable storage devices is permitted. Header in the file needed to be changed for it to open, this means that the header of the file was changed so the file can't open.
6.

Conclusion:

In my expert opinion I believe mr. Jackson has stolen and distributed sensitive information about MRC. I believe he has stolen pictures and recipes of different cookies and has sold them to competitor companies.

Policy Breach:

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. No use of removable storage devices is permitted.
3. 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.
4. All MRC electronic and computing resources are the property of MRC and may not be used for anything other than company work. MRC reserves the right to investigate the equipment as needed for any purpose.

Instances of stolen sensitive information:

1. Mr. Jackson had a snickerdoodle cookie recipe & a pumpkin cookie recipe inside of the snickerdoodle.pdf file & pumpkin.xlsx file.

Instances of pictures of MRC finished cookies

1. Mr. Jackson had pictures of cookies stored and hidden inside of architectural pictures. Mr. Jackson claimed he takes pictures of unique architecture as a hobby, that seems to be a lie. He also had pictures of cookies inside of cookie recipe files.

The investigation has discovered and distributed artifact evidence supporting the evidence against Mr. jackson. Also Mr. Jackson breached MRC policy by unplugging his computer before investigation and using a removable USB drive.