EASTERN MICHIGAN UNIVERSITY

READ ALL INSTRUCTIONS TO AVOID MARKDOWN AND TO AVOID SCOPE CREEP

Copy image file from our shared drive.

The USB image is not compressed and can be read directly into your tool of choice (dd copy).

This assignment is not graded and will serve as practice.

Name: **Jesse Russell**

Assignment: Case Study 1 - Ben Fields, industrial espionage

Case description: Ben Fields works for Ray Beam and Associates (RBA), a defense contractor in DC that engineers and constructs military weapons for the United States. Ben has been a valued staff member in the design engineering division for twelve years. About six months ago, Mr. Fields 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 house that seems outside of his salary reach. His pass card has been used for authenticated building access multiple times and shows in recorded entries for odd hours and weekends. Ben's director, Patty McNulty, has reported this bizarre behavior to Human Resources so that Ben would have a person to talk with if he chooses to do so. When HR reached out to Ben and met in his office, they found him irritable, agitated, and angry.

Additionally, upon first arriving, HR staff noticed Ben removing a flash drive from his computer and placing it in his pocket. As removable storage devices are not allowed at RBA, the HR staff asked Ben to turn over the flash drive and go home for the weekend (Friday at 2 pm). Ben furnished the thumb drive and complained that RBA invaded his privacy, claiming that the thumb drive contained only family pictures. The thumb drive was taken with no discussion. Ben was so angry that he unplugged his machine on his way out. After Ben left, HR then put the thumb drive on the desk and sealed the room by contacting the IT security team, who arrived and removed Ben's access from the pin code door. Security also removed all pins except for HR, Security, and Patty McNulty. Security then acquired images from the computer, flash drive and then moved all the original equipment to a highly secure locked area.

The USB image has now been passed on to you, a dead box forensics expert within the security team. 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.

//note the midterm case will contain a computer image and USB images

Executive Summary – Ben Fields, an employee of RBA, is being investigated for a possible breach of company policy. It is suspected by HR that Ben may be involved in corporate espionage, but the goal of this internal investigation is based on a breach of corporate policy. Evidence has been handled in a secure and systematic process.

EASTERN MICHIGAN UNIVERSITY

Things to know for this case

1. Open note, Google, book (YOU MAY NOT HELP EACH OTHER)
2. ANY image containing weapons, or references to weapons, is evidence.
3. Although this case dips into federal crime and usually law enforcement would be contacted, RBA has asked you to investigate the data and file a preliminary report with HR.
4. For flat email, files provide any analysis concerning sender, times, DNS, etc., analyze any attachment if there is one. Reconstruct any attachment – you must include a brief synopsis of the conversion process. Write forensics comments based on what you found.
5. Any image of weaponry is considered evidence that data is being removed from company servers (policy 8)
6. Review the images as we have in class and answer the outlined questions below.
7. All Hashes should be MD5

EASTERN MICHIGAN UNIVERSITY

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 RBA and should not be distributed outside of the company. Examples – Patents, formulas, trade secrets, customer lists, unpublished financial information
2. Employees may not transfer sensitive data belonging to RBA to other devices or accounts. When the 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 data recipients are properly authorized people or organizations and have adequate security policies.
7. Report scams, privacy breaches, and hacking attempts.
8. RBA proprietary information stored on electronic and computing devices, whether owned or leased by RBA, the employee, or a third party, remains the sole property of RBA and can not be transferred or removed without written approval.
9. All RBA electronic and computing resources are the property of RBA and are not to be used for anything outside of company work. RBA reserves the right to investigate the equipment as needed for any purpose.
10. BYOD - any personal electronic device attached to RBA IT solutions (IE corporate WIFI, LAN, etc.) are subject to all RBA policy.
11. RBA email systems are for the sole purpose of RBA business.

EASTERN MICHIGAN UNIVERSITY

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 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 are required as evidence
   - Submit in PDF

2. Target System & Devices
   - 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.

3. Initial evidence processed

(EVIDENCE MUST BE IN ALPHABETICAL ORDER AND ANALYZED IN SAME ORDER BELOW)

Item to analyze	Assigned to	Status / Completion date
Family1.jpg	Jesse Russell	Completed on 3/1/2021
Family2.jpg	Jesse Russell	Completed on 3/1/2021
Family3.pdf	Jesse Russell	Completed on 3/1/2021
Family 4.jpg	Jesse Russell	Completed on 3/1/2021
Family5.jpg	Jesse Russell	Completed on 3/1/2021
Grocery list.xls	Jesse Russell	Completed on 3/1/2021
Hey!.eml	Jesse Russell	Completed on 3/1/2021

4. Tool listing

ProDiscover, Version 8.2.0.2

This is a program used for capturing images of suspect machines and analyzing them. See: www.techpathways.com/ProDiscoverDFT.htm

Hexed.it

Hexed.it is an online browser based hex editor. It is used to analyze the hexes of files and fix any broken headers. See: www.hexed.it

WinRAR

WinRAR is a free utility used to decompress .zip files, and serves as a tool to view the contents of files without decompressing them.

WinMD5Free 1.20

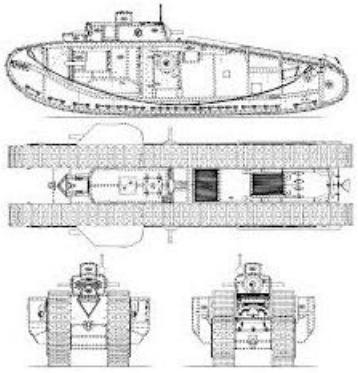
WinMD5Free is a utililty that allows an investivator to verify the integrity of files.

Thumb drive (7 files, nothing deleted -- Ben did not have time).
Every file, including discovery files, should follow the process of listing filename, hash, and comment unless noted)

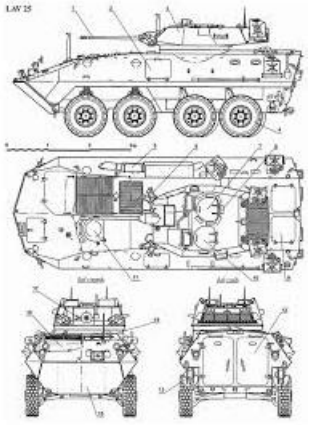
List your evidence in alphabetic order, like your list above.

1. Family1.jpg
    a. Hash: b4167af2329f8b650a38111070121440
    b. Image: 
    c. Comment: This image appears to be an innocent picture of a family, but steganography was used to alter the file.
        i. Family1HIDDEN.jpg
            1. Hash: d9073bb026c693ec6ae4318ea2ea845d
            2. Image: 
            3. Comment: Reversing the steganography of Family1.jpg yielded this image of a weapon developed by RBA. This is a violation of company policy.

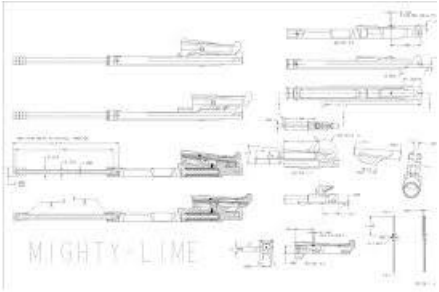
2. Family2.jpg
    a. Hash: 32dd66040ac9f2bc9543d105c6270aef
    b. Image: 
    c. Comment: This image appears to be an innocent picture of a family, and no evidence of steganography was found.

3. Family3.jpg
    a. Hash: 0f497d8c8fac23ea752cfc590d51b50c
    b. Image: 
    c. Comment: This file had it's header and file extension changed to hide the fact that it was a .jpg file. This image was found by correcting the header and changing the file extension to .jpg. This appears to be blueprints of an RBA weapon, a clear violation of company policy.

4. Family4.jpg
    a. Hash: 53d9e7bf954acde26667e09423ce47de
    b. Image: 
    c. Comment: This appears to be an innocent family picture, but if the hex of the file is analyzed, it contains two additional images of weapons developed by RBA.
        i. Family4HIDDEN1.jpg
            1. Hash: b737a8689e6025540c73ebcb727a65ed
            2. Image: 
            3. Comment: This is an image of a weapon being developed by RBA, which makes this a clear violation of company policy. This was found by reversing the steganography process of family4.jpg.

ii. Family4HIDDEN2.jpg
    1. Hash: c712defad28bd355bd62b563170e636f
    2. Image: 
    3. Comment: This is a blueprint of a weapon being developed by RBA, which is a clear violation of company policy. This was found by reversing the steganography process of family4.jpg.

5. Family5.jpg
    a. Hash: d7a668e19f145442412e48261600a288
    b. Image: 
    c. Comment: This appears to be an innocent picture of family, but steganography was used to hide a .zip file containing additional images of weapons developed by RBA.
        i. Weapon3.jpg
            1. Hash: bd3e9b8bf424caac12e7acb3dd638798
            2. Image: 
            3. Comment: This is an image of a weapon developed by RBA, which is a clear violation of company policy.

ii. Weapon4.jpg
    1. Hash: 23f88e00aed4e846dfc68c175005c2b7
    2. Image: 
    3. Comment: This is an image of a weapon developed by RBA, which is a clear violation of company policy.
iii. Weapon7.jpg
    1. Hash: 0f3162a8b39294fe350cd90653de57fa
    2. Image: 

    3. Comment: This is an blueprint of a weapon developed by RBA, which is a clear violation of company policy.

6. Hey!.eml
    a. Email Content

```
How are you?Family is good here, busy with work - ya know saving the world =
one tank at=C2=A0a time.
Give me a call when you can,Ima
```

    b. Email Data
        i. Sender: ima_spy@yahoo.com
            1. Domain: Yahoo
            2. Sent date: 3/3/20 11:52
        ii. Receiver: caseystudy2@gmail.com
            1. Domain: Google.vom
            2. Received date: 3/3/20 11:56

c. Attached File – Base64 encoded

i. Image: 

ii. Comment: This attachment is of a weapon developed by RBA, therefore it is a clear violation of company policy.

7. Grocery list.xlsx

a. Hash: 50c145a4b335b301c3240bc248721f29

b. Sheet 1 Image:

Grocery list
Apples
Turkey
Ham
Eggs
Butter Milk

c. Comment: This is Sheet 1 of the excel worksheet. It appears to be an innocent grocery list, but if Sheet 2 is looked at, there is some suspicious information.

d. Sheet 2 Image:

account	delivery	product	$ due at date
1	sold	SAMissle N2500	paid
2	3/12/20	xr7-vx	$375,000.00
3	6/19/20	CAT4000	$188,000.00
4	11/15/20	FTR-8500	$2,500,000.00

e. Comment: This appears to be a file detailing sales of RBA products. This may require additional investigation to find out if this is related to his job at RBA.

Final analysis:

a. What RBA policy was broken (copy and paste from above)?

Policy Number	Policy
1	Confidential paper documents and electronic files are the sole property of RBA and should not be distributed outside of the company. Examples – Patents, formulas, trade secrets, customer lists, unpublished financial information
2	Employees may not transfer sensitive data belonging to RBA to other devices or accounts. When the 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.
8	RBA proprietary information stored on electronic and computing devices, whether owned or leased by RBA, the employee, or a third party, remains the sole property of RBA and can not be transferred or removed without written approval.

Conclusion

As listed in the section above and in the evidence laid out in this report, Ben Fields clearly violated company policies on multiple occasions. Ben fields downloaded multiple protected company files to his USB drive, of which neither actions are permitted. He also distributed some of this material to an outside party, which is also a violation. Some pieces of evidence may require further investigation, such as the excel spread sheet, to determine their value in this case.