Forensic Computing

Final Project (Case Study)

Tyler Abbott (300137187)

Case Description:

Our suspect in this case is an employee at a fortune 500 company that has been reported by an anonymous entity, reporting that they have "illegal" files installed on their machine. Our suspect works within the I.T. Department, and is a component of the "Help Desk" team. An OSINT report has been run on this individual to find that he/she goes by several aliases online, and owns several domain names. Many of these domains seem strange in nature, where experts are led to believe this person is possibly selling or distributing illegal photographs.

In the case, the suspect has had 1 business day to cover their tracks, as it took 24 hours to get a warrant from the local police department to obtain & secure the employee's workstation.

Before obtaining the device, we take notes and pictures of each action we take, and take careful notes of any notable markings, serial numbers, or irregularity. While the device is still running, we use our mobile equipment and make an image of the machine and determine the SHA-256 or MD5SUM of the image file. After successfully securing the device, we placed it in a signed & sealed bag so it can be brought into our laboratory for safekeeping or further investigation.

The rest of the investigation will be analyzing a bit-by-bit accurate copy of the employee's machine, and finding concrete evidence that coincides with the anonymous report.

Case Files:

https://phoenixnap.dl.sourceforge.net/project/dftt/Test%20Images/9_%20FAT%20Volume%20Label%20%231/9-fat-label.zip --output 9-fat-label.zip

Results & Findings:

Expected findings:

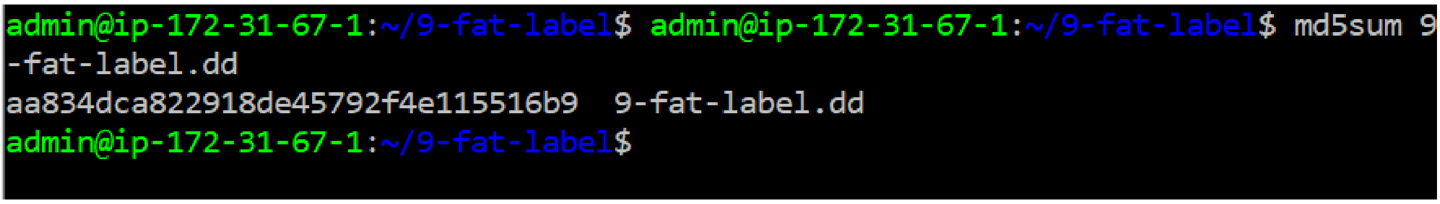
Our team expects to find incriminating evidence, or illegal activity from the materials retrieved from the employee's workstation.

Steps taken:

1. We will first need a workstation to work from, to analyse the image contents and perform operations on.
    a. Our first instincts were to use the provided UNIX server: learn.taliaq.com, however, this did not seem sustainable as we did not have "sudo" access to perform necessary actions. (sudo is required to mount drives, and required for installing The Sleuth KIt)
    b. Our second attempt was to spin-up a local server rack running ESXi 6.7, where multiple VMs can be run simultaneously. This proved to be difficult, as our experts forgot the 'root' password.
    c. Our last two resorts were to spin-up a local Raspberry Pi running Debian Ubuntu, or spin-up an AWS EC2 instance. The latter method was taken, as our team was concerned about the networking and computational ability of a Raspberry Pi device.

2. Once a workstation has been created, we need to install the necessary materials.
    a. curl https://phoenixnap.dl.sourceforge.net/project/dftt/Test%20Images/9_%20FAT%20Volume%20Label%20%231/9-fat-label.zip --output 9-fat-label.zip

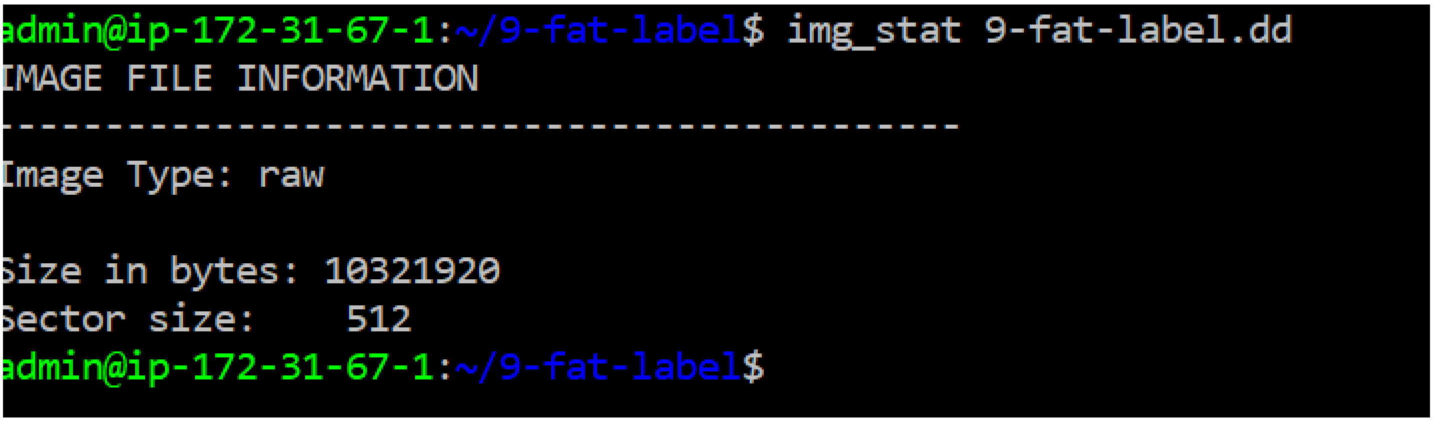
3. Once installed, we are required to unzip the materials, and save the files with appropriate naming conventions. We will need to run an 'MD5SUM' on the materials as proof the image has not been tampered with in transmission or during operation.



```
admin@ip-172-31-67-1:~/9-fat-label$ admin@ip-172-31-67-1:~/9-fat-label$ md5sum 9
-fat-label.dd
aa834dca822918de45792f4e115516b9  9-fat-label.dd
admin@ip-172-31-67-1:~/9-fat-label$
```

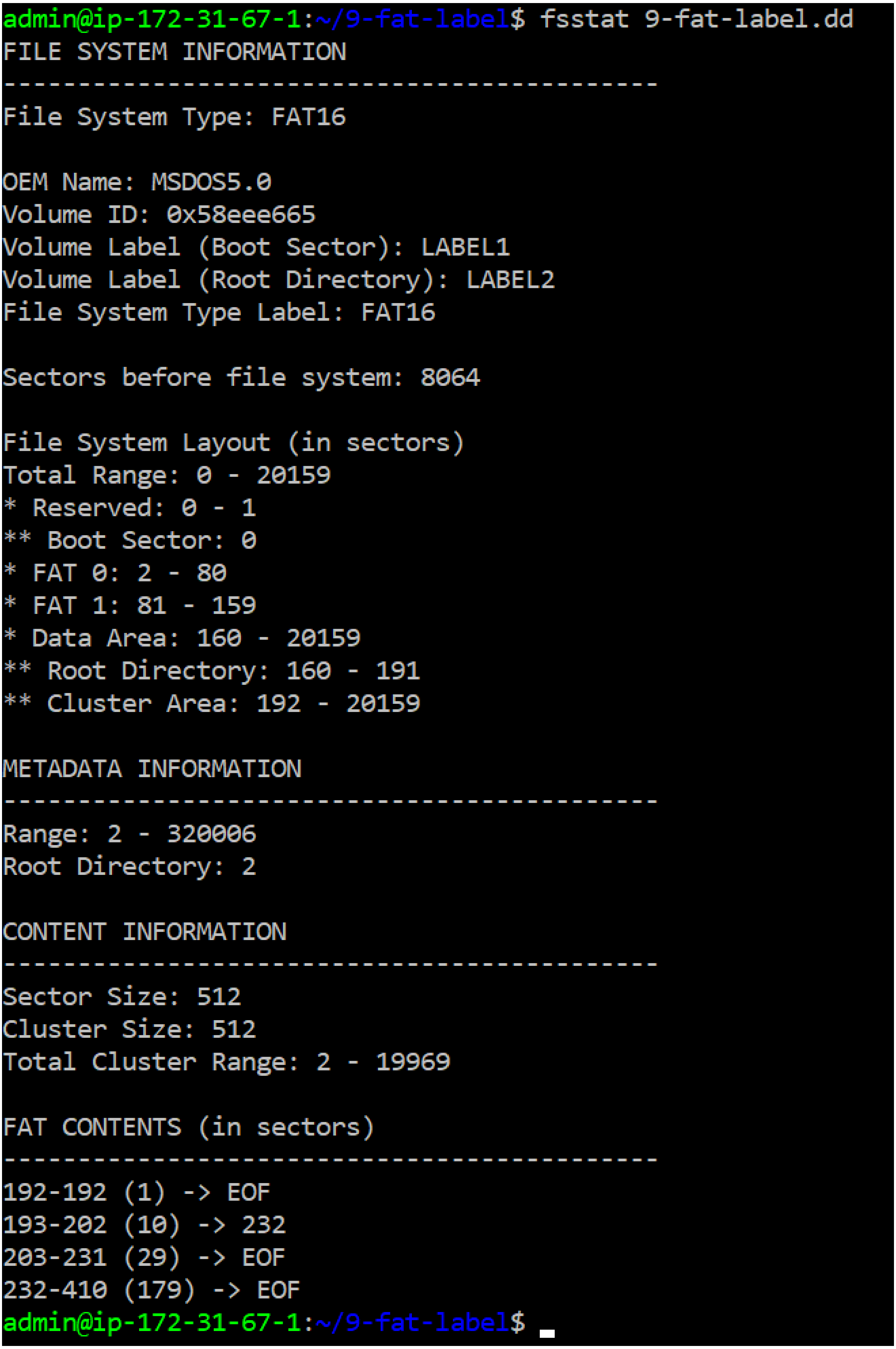
This MD5 hash is equivalent to our original copy, so we can ensure that no data was tampered during transmission: [FAT Volume Label Test #1 (sourceforge.net)]

4. Since this image is more-or-less a black box to us, we will need to do some reconnaissance on it.



```
admin@ip-172-31-67-1:~/9-fat-label$ img_stat 9-fat-label.dd
IMAGE FILE INFORMATION
--------------------------------------------
Image Type: raw

Size in bytes: 10321920
Sector size:    512
admin@ip-172-31-67-1:~/9-fat-label$
```

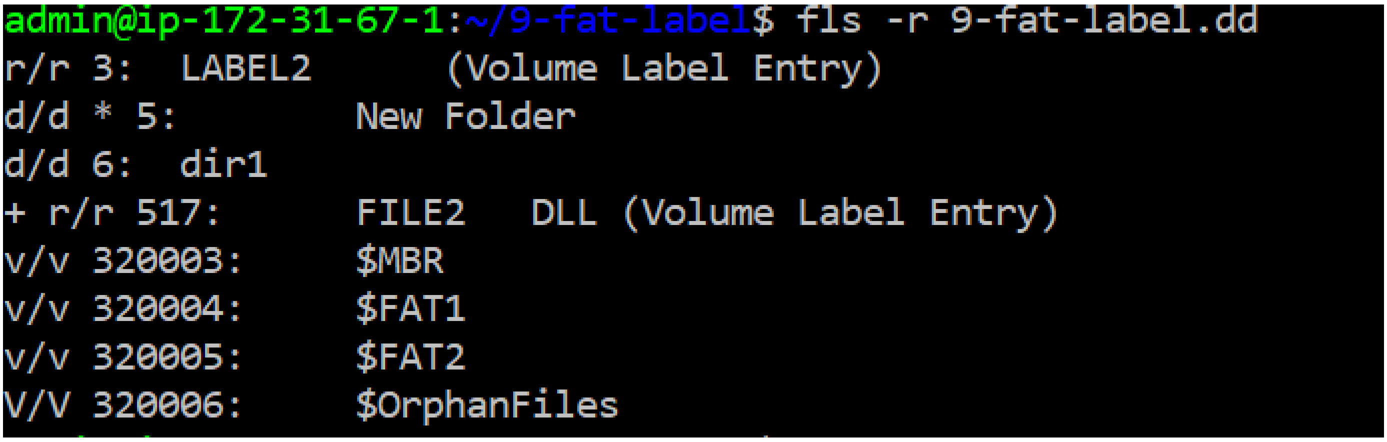
This image proves that this is a RAW image, and we can see the sector size and total size is around 1.29 MB.



```
admin@ip-172-31-67-1:~/9-fat-label$ fsstat 9-fat-label.dd
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: FAT16

OEM Name: MSDOS5.0
Volume ID: 0x58eee665
Volume Label (Boot Sector): LABEL1
Volume Label (Root Directory): LABEL2
File System Type Label: FAT16

Sectors before file system: 8064

File System Layout (in sectors)
Total Range: 0 - 20159
* Reserved: 0 - 1
** Boot Sector: 0
* FAT 0: 2 - 80
* FAT 1: 81 - 159
* Data Area: 160 - 20159
** Root Directory: 160 - 191
** Cluster Area: 192 - 20159

METADATA INFORMATION
--------------------------------------------
Range: 2 - 320006
Root Directory: 2

CONTENT INFORMATION
--------------------------------------------
Sector Size: 512
Cluster Size: 512
Total Cluster Range: 2 - 19969

FAT CONTENTS (in sectors)
--------------------------------------------
192-192 (1) -> EOF
193-202 (10) -> 232
203-231 (29) -> EOF
232-410 (179) -> EOF
admin@ip-172-31-67-1:~/9-fat-label$ 
```

This command further expands on our reconnaissance, and we can see the File System type is FAT16, and there are 8064 sectors before the file system. This information may prove to be useful later.

5. Once reconnaissance is complete, we may start investigating the contents of the image.

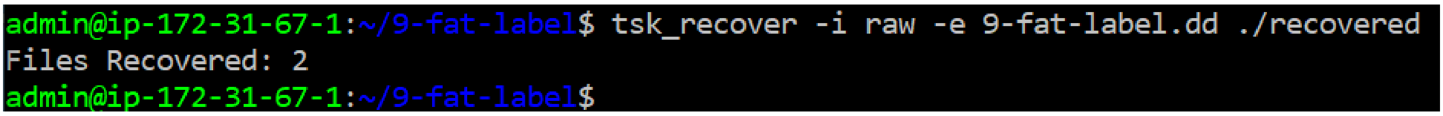


```
admin@ip-172-31-67-1:~/9-fat-label$ fls -r 9-fat-label.dd
r/r 3:  LABEL2      (Volume Label Entry)
d/d * 5:        New Folder
d/d 6:  dir1
+ r/r 517:      FILE2   DLL (Volume Label Entry)
v/v 320003:     $MBR
v/v 320004:     $FAT1
v/v 320005:     $FAT2
V/V 320006:     $OrphanFiles
```

Running the ‘fls’ command, we can see all files and directories on an image. We can manipulate the results by adding different options, such as ‘-r’ for recursive. Option ‘-d’ can be used for deleted entries only.

Once we have identified there are some deleted items, it is good to recover these early on, as the suspect is likely to try and cover their tracks by ‘deleting’ the evidence.

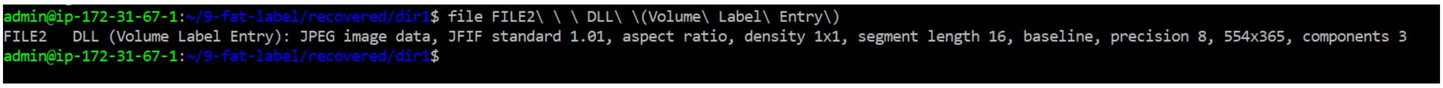
We can use command ‘tsk_recover’:



```
admin@ip-172-31-67-1:~/9-fat-label$ tsk_recover -i raw -e 9-fat-label.dd ./recovered
Files Recovered: 2
admin@ip-172-31-67-1:~/9-fat-label$
```

This is where I discovered a deleted directory and deleted file.

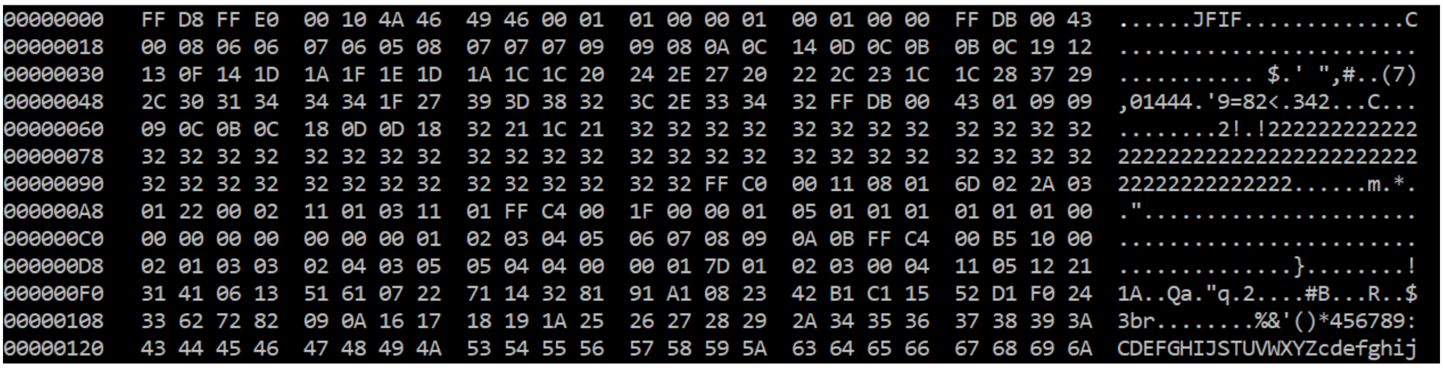
Investigating the file further:



```
admin@ip-172-31-67-1:~/9-fat-label/recovered/dir1$ file FILE2\ \ \ DLL\ \(Volume\ Label\ Entry\)
FILE2   DLL (Volume Label Entry): JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 554x365, components 3
admin@ip-172-31-67-1:~/9-fat-label/recovered/dir1$
```

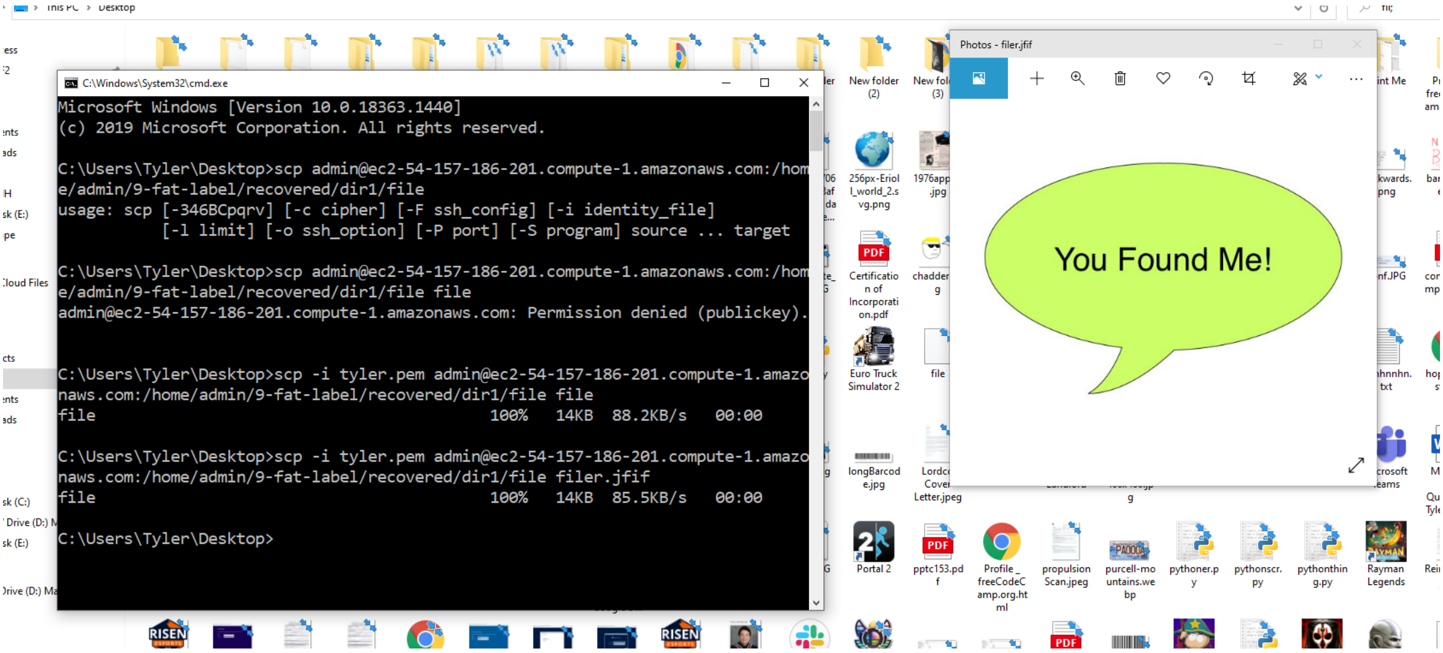
This is where we can see the this deleted file is a JPEG image.

Quickly analyzing the hexdump we can confirm this to be legitimate:



```
00000000   FF D8 FF E0  00 10 4A 46  49 46 00 01  01 00 00 01  00 01 00 00  FF DB 00 43  ......JFIF.............C
00000018   00 08 06 06  07 06 05 08  07 07 07 09  09 08 0A 0C  14 0D 0C 0B  0B 0C 19 12  ........................
00000030   13 0F 14 1D  1A 1F 1E 1D  1A 1C 1C 20  24 2E 27 20  22 2C 23 1C  1C 28 37 29  ........... $.' ",#..(7)
00000048   2C 30 31 34  34 34 1F 27  39 3D 38 32  3C 2E 33 34  32 FF DB 00  43 01 09 09  ,01444.'9=82<.342...C...
00000060   09 0C 0B 0C  18 0D 0D 18  32 21 1C 21  32 32 32 32  32 32 32 32  32 32 32 32  ........2!.!222222222222
00000078   32 32 32 32  32 32 32 32  32 32 32 32  32 32 32 32  32 32 32 32  32 32 32 32  222222222222222222222222
00000090   32 32 32 32  32 32 32 32  32 32 32 32  32 32 FF C0  00 11 08 01  6D 02 2A 03  22222222222222......m.*.
000000A8   01 22 00 02  11 01 03 11  01 FF C4 00  1F 00 00 01  05 01 01 01  01 01 01 00  ."......................
000000C0   00 00 00 00  00 00 00 01  02 03 04 05  06 07 08 09  0A 0B FF C4  00 B5 10 00  ........................
000000D8   02 01 03 03  02 04 03 05  05 04 04 00  00 01 7D 01  02 03 00 04  11 05 12 21  ..............}........!
000000F0   31 41 06 13  51 61 07 22  71 14 32 81  91 A1 08 23  42 B1 C1 15  52 D1 F0 24  1A..Qa."q.2....#B...R..$
00000108   33 62 72 82  09 0A 16 17  18 19 1A 25  26 27 28 29  2A 34 35 36  37 38 39 3A  3br........%&'()*456789:
00000120   43 44 45 46  47 48 49 4A  53 54 55 56  57 58 59 5A  63 64 65 66  67 68 69 6A  CDEFGHIJSTUVWXYZcdefghij
```

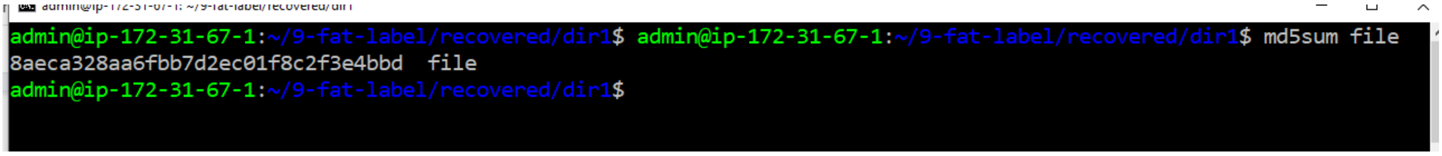
Since this AWS machine has no GUI, I will have to copy this to my own personal device to investigate the JPEG, and visually confirm what it is:



```
Microsoft Windows [Version 10.0.18363.1440]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Tyler\Desktop>scp admin@ec2-54-157-186-201.compute-1.amazonaws.com:/hom
e/admin/9-fat-label/recovered/dir1/file
usage: scp [-346BCpqrv] [-c cipher] [-F ssh_config] [-i identity_file]
           [-l limit] [-o ssh_option] [-P port] [-S program] source ... target

C:\Users\Tyler\Desktop>scp admin@ec2-54-157-186-201.compute-1.amazonaws.com:/hom
e/admin/9-fat-label/recovered/dir1/file file
admin@ec2-54-157-186-201.compute-1.amazonaws.com: Permission denied (publickey).


C:\Users\Tyler\Desktop>scp -i tyler.pem admin@ec2-54-157-186-201.compute-1.amazo
naws.com:/home/admin/9-fat-label/recovered/dir1/file file
file                                          100%   14KB  88.2KB/s   00:00

C:\Users\Tyler\Desktop>scp -i tyler.pem admin@ec2-54-157-186-201.compute-1.amazo
naws.com:/home/admin/9-fat-label/recovered/dir1/file filer.jfif
file                                          100%   14KB  85.5KB/s   00:00

C:\Users\Tyler\Desktop>
```

The found file is incriminating evidence, and we now need to prove that this file exists on the employee's machine.

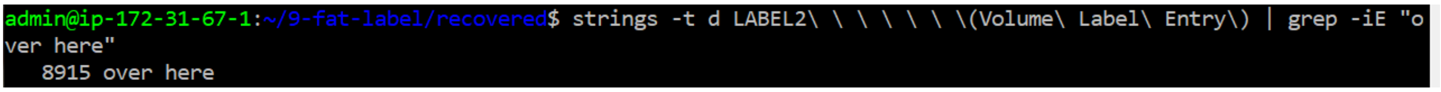
We can take an MD5SUM of the target file:



```
admin@ip-172-31-67-1:~/9-fat-label/recovered/dir1$ admin@ip-172-31-67-1:~/9-fat-label/recovered/dir1$ md5sum file
8aeca328aa6fbb7d2ec01f8c2f3e4bbd  file
admin@ip-172-31-67-1:~/9-fat-label/recovered/dir1$
```

Lastly, before completing the formal report to be presented to the courts, we have gotten a "head's up" from the anonymous contact, that the phrase "over here!" may be useful for our investigation.

We can run this string against the image contents:



```
admin@ip-172-31-67-1:~/9-fat-label/recovered$ strings -t d LABEL2\ \ \ \ \ \(Volume\ Label\ Entry\) | grep -iE "o
ver here"
   8915 over here
```

6. Our team has found incriminating evidence and activity. Our last step is to finalize our formal report with irrefutable proof that the target suspect has illegal media on their device. We will bring this evidence to the local police department and court system, where we will present the results in a professional manner.

Sources:

FAT Volume Label Test #1 (sourceforge.net)

https://www.youtube.com/watch?v=R-IE2j04Chc

https://www.youtube.com/watch?v=Id9RW3pxAKg

https://www.howtoinstall.me/ubuntu/18-04/sleuthkit/

http://blog.hakzone.info/posts-and-articles/linux/disk-analysis-with-fdisk-mmls-fsstat-and-fls/

https://unix.stackexchange.com/questions/577050/bash-fdisk-command-not-found

https://www.forensicfocus.com/forums/general/mmls-fsstat-fls-cannot-determine-partition-type-of-dd/