

DJI Mavic Air Investigations

Mavic microSD card Expert Witness/Encase format

Obtain the microSD image

Download microSD card image

```
kali@kali: ~/Marvic_air 109x36
(kali@kali)-[~/Marvic_air]
└─$ wget https://www.dropbox.com/s/3srna99g65poavo/DF048.E01
--2021-05-08 09:50:29-- https://www.dropbox.com/s/3srna99g65poavo/DF048.E01
Resolving www.dropbox.com (www.dropbox.com)... 162.125.6.18, 2620:100:601c:18::a27d:612
Connecting to www.dropbox.com (www.dropbox.com)|162.125.6.18|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: /s/raw/3srna99g65poavo/DF048.E01 [following]
--2021-05-08 09:50:29-- https://www.dropbox.com/s/raw/3srna99g65poavo/DF048.E01
Reusing existing connection to www.dropbox.com:443.
```

Verify hash code

```
(kali@kali)-[~/Marvic_air]
└─$ md5sum DF048.E01
d1651cfacd5b1827e337ad0a826002ae DF048.E01
```

Find the format of Mavic microSD

```
kali@kali: ~/Marvic_air 93x26  
  
(kali@kali)-[~/Marvic_air]  
└─$ file DF048.E01  
DF048.E01: EWF/Expert Witness/EnCase image file format ←  
  
(kali@kali)-[~/Marvic_air]  
└─$ sudo apt-get install ewf-tools  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
ewf-tools is already the newest version (20140807-2+b2).  
The following packages were automatically installed and are no longer required:  
  libpython3.8 libpython3.8-dev libqt5opengl5 libxml-dom-perl libxml-perl  
  libxml-regexp-perl python3.8-dev  
Use 'sudo apt autoremove' to remove them.  
0 upgraded, 0 newly installed, 0 to remove and 1112 not upgraded.
```

Show image
information

```
(kali@kali)-[~/Marvic_air]
└─$ ewfinfo DF048.E01
ewfinfo 20140807

Acquiry information
Case number:           DF048
Description:           untitled
Examiner name:
Evidence number:       DJI Mavic Air
Notes:
Acquisition date:     Thu Jun 28 15:59:48 2018
System date:           Thu Jun 28 15:59:48 2018
Operating system used: Win 201x
Software version used: ADI3.4.0.1
Password:              N/A

EWF information
File format:           FTK Imager
Sectors per chunk:     64
Compression method:    deflate
Compression level:     no compression

Media information
Media type:            fixed disk
Is physical:           yes
Bytes per sector:      512
Number of sectors:     16777216
Media size:            8.0 GiB (8589934592 bytes)

Digest hash information
MD5:                   7285a252d6c4582e120e06f3c13861ff
SHA1:                  8bb139ec8196e238d17e729ce9cfe585adfc616e
```

Verify image hash

```
kali@kali: ~/Marvic_air
(kali@kali)~[~/Marvic_air]
$ ewfverify DF048.E01
ewfverify 20140807

Verify started at: May 08, 2021 15:51:18
This could take a while.

Status: at 13%.
verified 1.0 GiB (1129742336 bytes) of total 8.0 GiB (8589934592 bytes).
completion in 26 second(s) with 273 MiB/s (286331153 bytes/second).

Status: at 29%.
verified 2.3 GiB (2504163328 bytes) of total 8.0 GiB (8589934592 bytes).
completion in 19 second(s) with 303 MiB/s (318145725 bytes/second).

Status: at 44%.
verified 3.6 GiB (3858759680 bytes) of total 8.0 GiB (8589934592 bytes).
completion in 15 second(s) with 303 MiB/s (318145725 bytes/second).

Status: at 60%.
verified 4.8 GiB (5192220672 bytes) of total 8.0 GiB (8589934592 bytes).
completion in 10 second(s) with 315 MiB/s (330382099 bytes/second).

Status: at 75%.
verified 6.0 GiB (6509854720 bytes) of total 8.0 GiB (8589934592 bytes).
completion in 6 second(s) with 315 MiB/s (330382099 bytes/second).

Status: at 90%.
verified 7.2 GiB (7815626752 bytes) of total 8.0 GiB (8589934592 bytes).
completion in 2 second(s) with 315 MiB/s (330382099 bytes/second).

Verify completed at: May 08, 2021 15:51:44

Read: 8.0 GiB (8589934592 bytes) in 26 second(s) with 315 MiB/s (330382099 bytes/second).

MD5 hash stored in file: 7285a252d6c4582e120e06f3c13861ff
MD5 hash calculated over data: 7285a252d6c4582e120e06f3c13861ff

Additional hash values:
SHA1: 8bb139ec8196e238d17e729ce9cfe585adfc616e

ewfverify: SUCCESS
```

Mount an Expert Witness Compression Format (EWF) image file

```
kali@kali: ~/Marvic
(kali@kali)-[~/Marvic_air]
└─$ mkdir ext_sd

(kali@kali)-[~/Marvic_air]
└─$ ewfmount DF048.E01 ext_sd
ewfmount 20140807

(kali@kali)-[~/Marvic_air]
└─$ ls ext_sd
ewf1
```

usage: **ewfmount** *image* *mount_point*

- *image*: an Expert Witness Compression Format (EWF) image file
- *mount_point*: the directory to serve as mount point

```
(kali@kali)-[~/Marvic_air]
└─$ ls -l ext_sd
total 0
-r--r--r-- 1 root root 8589934592 May  8 11:51 ewf1 ←
```

Note: the permission and owner have been changed

```
kali@kali: ~/Marvic_air 93x45
(kali@kali)-[~/Marvic_air]
└─$ ls -l
total 17015044
drwxr-xr-x 4 kali kali      4096 Oct 11  2018 Android_Logical
-rw-r--r-- 1 kali kali  415154789 May  3 10:45 Android_Logical.zip
-rw-r--r-- 1 kali kali  8418291569 May  8 10:17 DF048.E01
-rw-r--r-- 1 kali kali  8589934592 May  7 16:30 df048_internal_microSD.001
dr-xr-xr-x 2 root root          0 May  8 16:10 ext_sd
drwxr-xr-x 2 kali kali      4096 May  8 11:27 ext_sd_mountpoint
```

Show all files

```
(kali@kali)-[~/Marvic_air]
└─$ fls -r ext_sd/ewf1
d/d 3:  LOST.DIR
d/d 4:  DCIM
+ d/d 3077:  100MEDIA
++ r/r 1357829: DJI_0001.MP4
++ r/r 1357830: DJI_0002.MP4
++ r/r 1357831: DJI_0003.MP4
++ r/r 1357832: DJI_0004.MP4
++ r/r 1357833: DJI_0005.MP4
++ r/r * 1357836:  .DJI_0005.MP4.trinf
++ r/r * 1357839:  .DJI_0005.MP4.avc1
d/d 5:  MISC
+ d/d 4101:  THM
++ d/d 5125:  100
+++ r/r 1358853:  DJI_0001.THM
+++ r/r 1358854:  DJI_0002.THM
+++ r/r 1358855:  DJI_0003.THM
+++ r/r 1358856:  DJI_0004.THM
+++ r/r 1358857:  DJI_0005.THM
+ d/d 4102:  GIS
++ r/r 6150:  dji.gis
+ d/d 4103:  IDX
++ r/r * 1356807:  .VR_dji_A2UMXs
++ r/r * 1356810:  .VR_dji_kzIxFO
d/d 8:  System Volume Information
+ r/r 208425991:  IndexerVolumeGuid
+ r/r 208425994:  WPSettings.dat
d/d 10:  .fseventsd
+ r/r 1031:  fseventsd-uuid
v/v 268368899:  $MBR
v/v 268368900:  $FAT1
v/v 268368901:  $FAT2
V/V 268368902:  $OrphanFiles
```


Where was the first video taken?

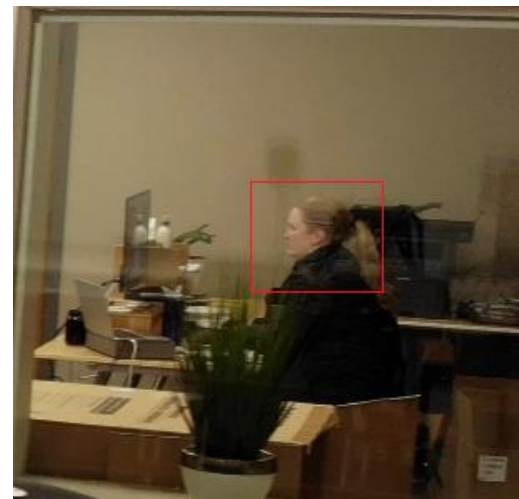
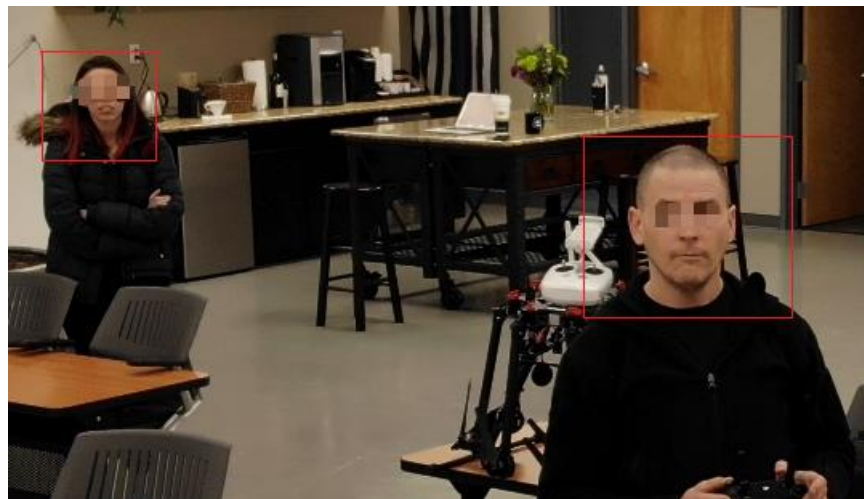
```
Kali@Kali: ~  
  
(kali@kali)-[~/Marvic_air]  
└─$ istat -i raw ext_sd/ewf1 1357829 | head  
Directory Entry: 1357829  
Allocated  
File Attributes: File, Archive  
Size: 785356701  
Name: DJI_0001.MP4  
  
Directory Entry Times:  
Written:      2018-02-02 17:31:20 (EST)  
Accessed:     2018-06-21 00:00:00 (EDT)  
Created:      2018-02-02 17:31:20 (EST)
```

How to play the video?

```
kali@kali: ~/Marvic_air 94x37  
  
(kali@kali)-[~/Marvic_air]  
└─$ icat ext_sd/ewf1 1357829 > DJI_0001.MP4  
  
(kali@kali)-[~/Marvic_air]  
└─$ vlc DJI_0001.MP4  
VLC media player 3.0.12 Vetinari (revision 3.0.12-1-0-gd147bb5e7e)  
[0000555dba4745b0] main libvlc: Running vlc with the default interface. Use 'cvl
```

```
(kali@kali)-[~/Marvic_air]  
└─$ md5sum DJI_0001.MP4  
a582c24d5a4bced66004e4609481a01e DJI_0001.MP4 ←
```

How many people were shown on the first video?



DJI_0001.MP4

three

Is this video same as the video in internal microSD card?

recall the hashes/timestamps of videos in internal microSD card

```
kali@kali: ~/Marvic_air 94x37

(kali@kali)-[~/Marvic_air]
└─$ md5sum /media/kali/2019-1B01/DCIM/100MEDIA/*.MP4
a582c24d5a4bced66004e4609481a01e  /media/kali/2019-1B01/DCIM/100MEDIA/DJI_0001.MP4
3b30c6a1028ac8b5f69ffbd3bd2ca04a  /media/kali/2019-1B01/DCIM/100MEDIA/DJI_0002.MP4
4bb7099743e3545a441c3f3ff5e156e7  /media/kali/2019-1B01/DCIM/100MEDIA/DJI_0003.MP4
5e329546924320e8cb20d2afb158538b  /media/kali/2019-1B01/DCIM/100MEDIA/DJI_0004.MP4
7b36420bee81a6ab403b521047d67f37  /media/kali/2019-1B01/DCIM/100MEDIA/DJI_0005.MP4

(kali@kali)-[~/Marvic_air]
└─$ stat /media/kali/2019-1B01/DCIM/100MEDIA/DJI_0001.MP4
File: /media/kali/2019-1B01/DCIM/100MEDIA/DJI_0001.MP4
  Size: 785356701      Blocks: 1533952      IO Block: 32768   regular file
Device: 700h/1792d   Inode: 265           Links: 1
Access: (0644/-rw-r--r--)  Uid: ( 1000/      kali)   Gid: ( 1000/      kali)
Access: 2018-06-20 20:00:00.000000000 -0400
Modify: 2018-02-02 12:31:20.000000000 -0500
Change: 2018-02-02 12:31:21.000000000 -0500
 Birth: -
```

same

Verify the serial number of the image

```
kali@kali: ~/Marvic_air 94x37
(kali@kali)-[~/Marvic_air]
└─$ file ext_sd/ewf1
ext_sd/ewf1: DOS/MBR boot sector, code offset 0x58+2, OEM-ID "android ", sectors/cluster 64, reserved sectors 64, sectors/track 16, heads 4, sectors 16777216 (volumes > 32 MB), FAT (32 bit), sectors/FAT 2048, reserved 0x1, serial number 0x20191b01, unlabeled
```

It turns out the microSD card is the same as internal microSD card