

1、因为镜像文件为 E01 (EWF) 所以需要用 ewfmount 命令把里面的数据取出来，需要安装 libewf 或者 ewf-tools

```
# jxkzs @ Finiox in ~ [16:07:02]
$ yaourt -Ss ewf
community/libewf 20140608-6 [installed]
  A library for support of the Expert Witness Compression Format (EWF)
```

2、挂载镜像

```
# jxkzs @ Finiox in ~ [16:09:57]
$ sudo mkdir /mnt/ewf

# jxkzs @ Finiox in ~ [16:10:05]
$ sudo ewfmount forensic/Zello-onlineshop\ webserver.e01 /mnt/ewf
ewfmount 20140608
```

3、可以看到挂载目录下有数据文件，因挂载是采用 ISO 9660 (CD images)，无权限对其进行修改，所以要将该文件 cp 出来进行二次挂载

```
# jxkzs @ Finiox in ~ [16:11:15]
$ sudo ls -al /mnt/ewf
total 4
drwxr-xr-x 2 root root          0 Jan  1  1970 .
drwxr-xr-x 4 root root    4096 Dec 11 16:10 ..
-r--r--r-- 1 root root 32212254720 Dec 11 16:11 ewf1

# jxkzs @ Finiox in ~ [16:11:49]
$ su
Password:
[root@Finiox jxkzs]# cd /mnt/ewf/
[root@Finiox ewf]# chmod ewf1 0755
chmod: invalid mode: 'ewf1'
Try 'chmod --help' for more information.
[root@Finiox ewf]# chmod 0755 ewf1
chmod: changing permissions of 'ewf1': Function not implemented
[root@Finiox ewf]# cd ..
[root@Finiox mnt]# ls -alh
total 12K
drwxr-xr-x  4 root root 4.0K Dec 11 16:10 .
drwxr-xr-x 17 root root 4.0K Dec  2 14:04 ..
drwxr-xr-x  2 root root   0 Jan  1  1970 ewf
drwxr-xr-x  5 root root 4.0K Dec 11 14:23 mount_v
[root@Finiox mnt]# cp
ewf/      mount_v/
[root@Finiox mnt]# cp ewf/ewf1 ./
[root@Finiox mnt]# exit
exit
```

4、安装 kpartx，利用其将文件系统自动挂载到/dev 目录上

```
# jxkzs @ Finiox in ~ [16:16:57]
$ yaourt -Ss kpartx
community/multipath-tools 0.8.5-1 [installed]
  Multipath tools for Linux (including kpartx)
aur/multipath-tools-git 2837.8a7e9b66-1 (33) (0.00)
  Tools to drive the Device Mapper multipathing driver (contains kpartx)
```

5、挂载 cp 出的数据

```
# jxkzs @ Finiox in ~ [16:17:44]
$ sudo kpartx -a /mnt/ewf1
[sudo] password for jxkzs:
```

6、挂载之后的数据在/dev/mapper 里，可以看到，此数据里有 1vm2

```
# jxkzs @ Finiox in ~ [16:18:23]
$ ls -al /dev/mapper
total 0
drwxr-xr-x  2 root root    140 Dec 11 16:17 .
drwxr-xr-x 21 root root   3720 Dec 11 16:17 ..
crw-----  1 root root 10, 236 Dec 11 16:17 control
lrwxrwxrwx  1 root root    7 Dec 11 16:17 loop0p1 -> ../dm-0
lrwxrwxrwx  1 root root    7 Dec 11 16:17 loop0p2 -> ../dm-1
lrwxrwxrwx  1 root root    7 Dec 11 16:17 loop0p3 -> ../dm-2
lrwxrwxrwx  1 root root    7 Dec 11 16:17 ubuntu--vg-ubuntu--lv -> ../dm-3
```

也可以利用 fdisk 查看新的设备文件

```
Disk /dev/nvme0n1: 476.94 GiB, 512110190592 bytes, 1000215216 sectors
Disk model: WDC PC SN730 SDBPNTY-512G-1027
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: gpt
Disk identifier: FD16259A-55D1-4126-A267-66686BB15D1

Device            Start      End  Sectors  Size Type
/dev/nvme0n1p1     2048     4196351  4194304    2G EFI System
/dev/nvme0n1p2    4196352  991954943  987758592  471G Linux filesystem
/dev/nvme0n1p3   991954944 1000215182   8260239    3.9G Linux swap

Disk /dev/loop0: 30 GiB, 32212254720 bytes, 62914560 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: gpt
Disk identifier: F486220C-C09E-4E01-8993-63A05C980756

Device            Start      End  Sectors  Size Type
/dev/loop0p1       2048     4095    2048    1M BIOS boot
/dev/loop0p2       4096  2101247  2097152    1G Linux filesystem
/dev/loop0p3    2101248 62912511 60811264   29G Linux filesystem

Disk /dev/mapper/ubuntu--vg-ubuntu--lv: 20 GiB, 21474836480 bytes, 41943040 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

8、显示该镜像一共有三个分区，因第一个分区是 BIOS，所以直接挂载分区 2，3 即可：

```
# jxkzs @ Finiox in ~ [16:19:36] C:1
$ sudo mount /dev/mapper/loop0p2 /mnt/mount_v/2
```


挂载分区 2 后查看该分区数据，发现该分区挂载点为/boot 用作启动该系统

```
# jxkzs @ Finiox in ~ [16:20:06]
$ ls -al /mnt/mount_v/2
total 302212
drwxr-xr-x 4 root root      4096 Sep 29 13:24 .
drwxr-xr-x 5 root root      4096 Dec 11 14:23 ..
-rw-r--r-- 1 root root    237769 Aug 26 21:15 config-5.4.0-45-generic
-rw-r--r-- 1 root root    237769 Sep  5 03:08 config-5.4.0-47-generic
-rw-r--r-- 1 root root    237769 Sep 10 18:12 config-5.4.0-48-generic
drwxr-xr-x 4 root root      4096 Sep 29 13:24 grub
lrwxrwxrwx 1 root root       27 Sep 29 13:24 initrd.img -> initrd.img-5.4.0-48-generic
-rw-r--r-- 1 root root  86289660 Sep  3 10:53 initrd.img-5.4.0-45-generic
-rw-r--r-- 1 root root  86294161 Sep 29 13:23 initrd.img-5.4.0-47-generic
-rw-r--r-- 1 root root  86301057 Sep 29 13:24 initrd.img-5.4.0-48-generic
lrwxrwxrwx 1 root root       27 Sep 29 13:24 initrd.img.old -> initrd.img-5.4.0-47-generic
drwx----- 2 root root    16384 Sep  3 10:22 lost+found
-rw-r--r-- 1 root root   182704 Aug 18 18:46 memtest86+.bin
-rw-r--r-- 1 root root   184380 Aug 18 18:46 memtest86+.elf
-rw-r--r-- 1 root root   184884 Aug 18 18:46 memtest86+_multiboot.bin
-rw----- 1 root root   4740251 Aug 26 21:15 System.map-5.4.0-45-generic
-rw----- 1 root root   4740251 Sep  5 03:08 System.map-5.4.0-47-generic
-rw----- 1 root root   4743112 Sep 10 18:12 System.map-5.4.0-48-generic
lrwxrwxrwx 1 root root       24 Sep 29 13:24 vmlinuz -> vmlinuz-5.4.0-48-generic
-rw----- 1 root root  11670272 Aug 26 21:19 vmlinuz-5.4.0-45-generic
-rw----- 1 root root  11670272 Sep  5 03:18 vmlinuz-5.4.0-47-generic
-rw----- 1 root root  11678464 Sep 10 18:36 vmlinuz-5.4.0-48-generic
lrwxrwxrwx 1 root root       24 Sep 29 13:24 vmlinuz.old -> vmlinuz-5.4.0-47-generic
```

9、因第三个分区是 1vm，所以直接搜索就可以找到 1vm 信息

```
# jxkzs @ Finiox in ~ [16:20:31]
$ sudo lvscan
ACTIVE                               '/dev/ubuntu-vg/ubuntu-lv' [20.00 GiB] inherit
```

进一步查看可以看到 lv 及 vg 的信息和该设备的 UUID

```
# jxkzs @ Finiox in ~ [16:20:31]
$ sudo lvscan
ACTIVE                               '/dev/ubuntu-vg/ubuntu-lv' [20.00 GiB] inherit

# jxkzs @ Finiox in ~ [16:20:41]
$ sudo lvsdisplay
--- Logical volume ---
LV Path                /dev/ubuntu-vg/ubuntu-lv
LV Name                 ubuntu-lv
VG Name                 ubuntu-vg
LV UUID                 5ySSX8-J532-BFQ6-aKuC-4sdg-x2IW-53XXXf
LV Write Access         read/write
LV Creation host, time ubuntu-server, 2020-09-03 10:22:59 +0800
LV Status                available
# open                  0
LV Size                 20.00 GiB
Current LE              5120
Segments                1
Allocation               inherit
Read ahead sectors      auto
- currently set to     256
Block device            254:3
```

10、将该分区挂载起来

```
# jxkzs @ Finiox in ~ [16:21:53] C:32
$ sudo mount /dev/ubuntu-vg/ubuntu-lv /mnt/mount_v/3
```

查看该分区数据判断挂载点为/

```
# jxkzs @ Finiox in ~ [16:21:58]
$ ls -al /mnt/mount_v/3
total 2097256
drwxr-xr-x 20 root root      4096 Sep  3 10:24 .
drwxr-xr-x  5 root root      4096 Dec 11 14:23 ..
lrwxrwxrwx  1 root root         7 Aug  1 00:28 bin -> usr/bin
drwxr-xr-x  2 root root      4096 Sep  3 10:23 boot
drwxr-xr-x  2 root root      4096 Sep  3 10:23 cdrom
drwxr-xr-x  5 root root      4096 Aug  1 00:29 dev
drwxr-xr-x 146 root root    12288 Sep 29 13:25 etc
drwxr-xr-x  3 root root      4096 Sep  3 10:29 home
lrwxrwxrwx  1 root root         7 Aug  1 00:28 lib -> usr/lib
lrwxrwxrwx  1 root root         9 Aug  1 00:28 lib32 -> usr/lib32
lrwxrwxrwx  1 root root         9 Aug  1 00:28 lib64 -> usr/lib64
lrwxrwxrwx  1 root root        10 Aug  1 00:28 libx32 -> usr/libx32
drwx----- 2 root root    16384 Sep  3 10:22 lost+found
drwxr-xr-x  3 root root      4096 Sep  3 10:55 media
drwxr-xr-x  2 root root      4096 Aug  1 00:28 mnt
drwxr-xr-x  2 root root      4096 Aug  1 00:28 opt
drwxr-xr-x  2 root root      4096 Apr 15 2020 proc
drwx----- 6 root root      4096 Sep  7 11:37 root
drwxr-xr-x 11 root root      4096 Aug  1 00:29 run
lrwxrwxrwx  1 root root         8 Aug  1 00:28 sbin -> usr/sbin
drwxr-xr-x  6 root root      4096 Sep  3 10:29 snap
drwxr-xr-x  2 root root      4096 Aug  1 00:28 srv
-rw-----  1 root root 2147483648 Sep  3 10:24 swap.img
drwxr-xr-x  2 root root      4096 Apr 15 2020 sys
drwxrwxrwt 22 root root      4096 Sep 29 16:39 tmp
drwxr-xr-x 14 root root      4096 Aug  1 00:29 usr
drwxr-xr-x 15 root root      4096 Sep  3 16:14 var
```

11、用 chroot 命令将该挂载点设为根目录 (/), 并以 root 用户启动。
因分区 2 为 /boot, 对于取证来讲没有影响, 所以以 root 用户启动的时候没有将此分区的信息一起加进去, 如需加入此信息需要把分区而卸载后再从新挂载到分区 3 挂载点的 /boot 目录

```
# jxkzs @ Finiox in ~ [16:26:47]
$ sudo chroot /mnt/mount_v/3
```

这样就相当于把此系统仿真起来了, 就可以继续操作了

```
$ sudo chroot /mnt/mount_v/3
root@Finiox:/# ls -al /var/www/
total 20
drwxr-xr-x  5 root      root      4096 Sep  3 16:59 .
drwxr-xr-x 15 root      root      4096 Sep  3 16:14 ..
drwxr-xr-x  3 root      root      4096 Sep  3 16:59 html
drwxr-xr-x  5 root      root      4096 Sep  3 16:59 htmlwordpress
drwxr-xr-x  5 www-data  www-data  4096 Sep  3 16:52 wordpress
root@Finiox:/#

root@Finiox:/# uname -a
Linux Finiox 5.9.13-arch1-1 #1 SMP PREEMPT Tue, 08 Dec 2020 12:09:55 +0000 x86_64 x86_64 x86_64 GNU/Linux
```