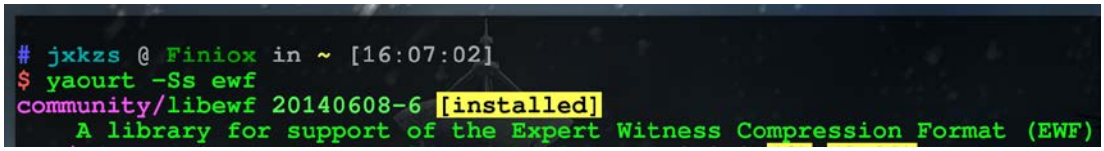
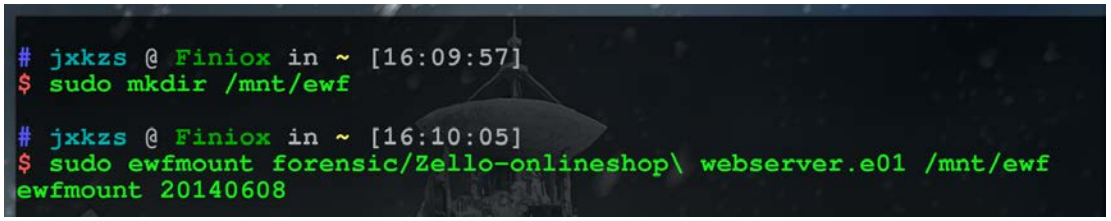
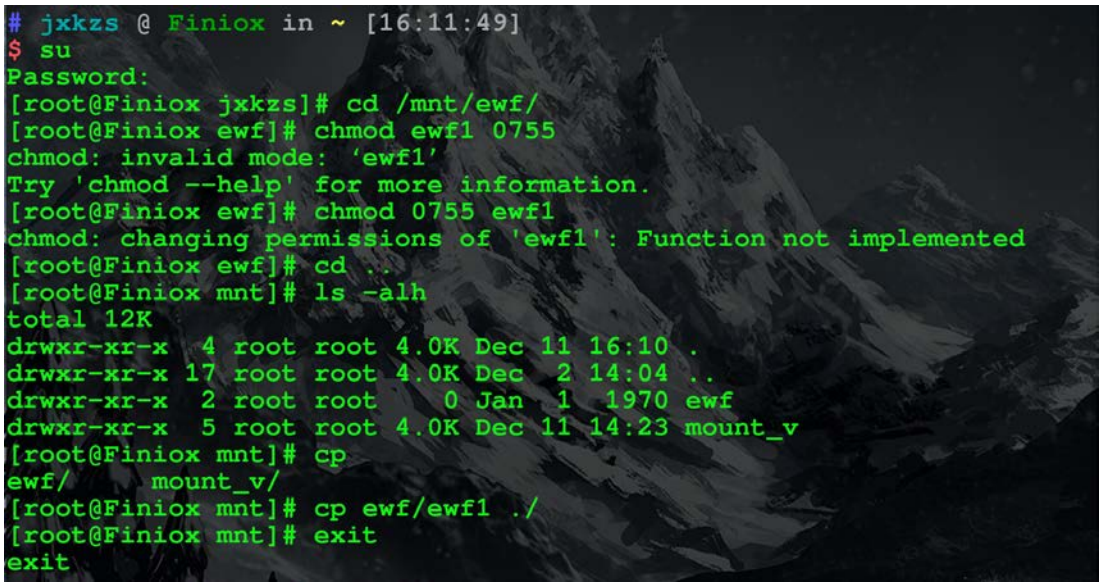
1、因为镜像文件为 E01（EWF）所以需要用 ewfmount 命令把里面的数据取出来，需要安装 libewf 或者 ewf-tools



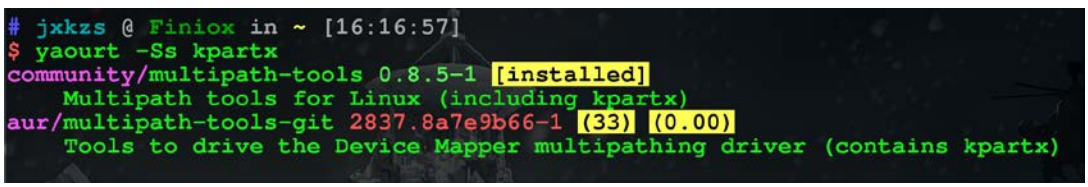

2、挂载镜像




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


4、安装 kpartx，利用其将文件系统自动挂载到/dev 目录上



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 lvm2

```
# 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
```

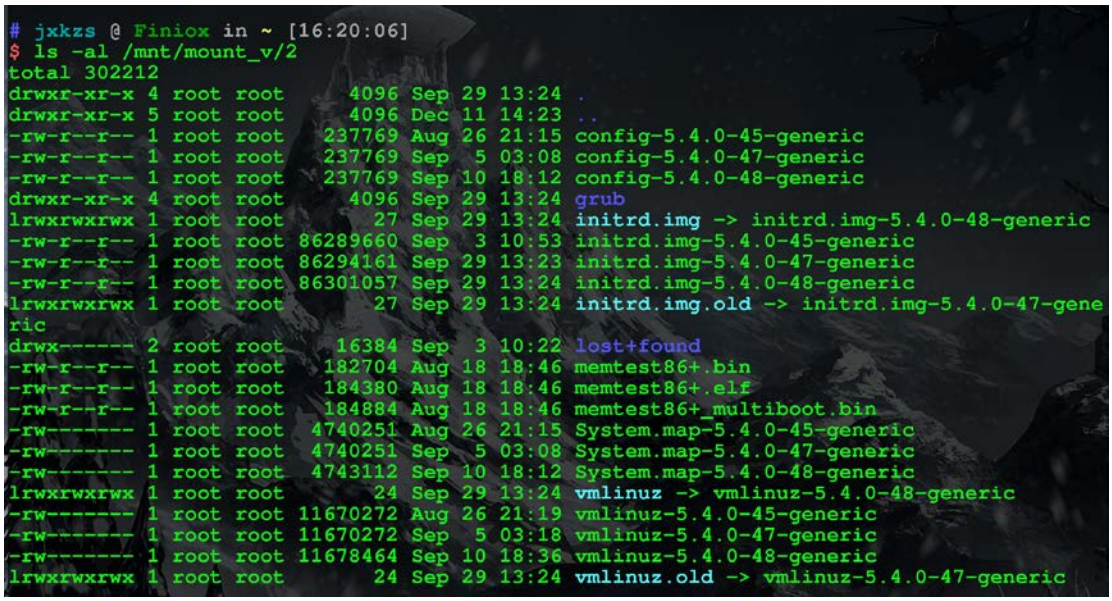
也可以利用 fdisk 查看新的设备文件

```
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-A267-66686BBB15D1

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：

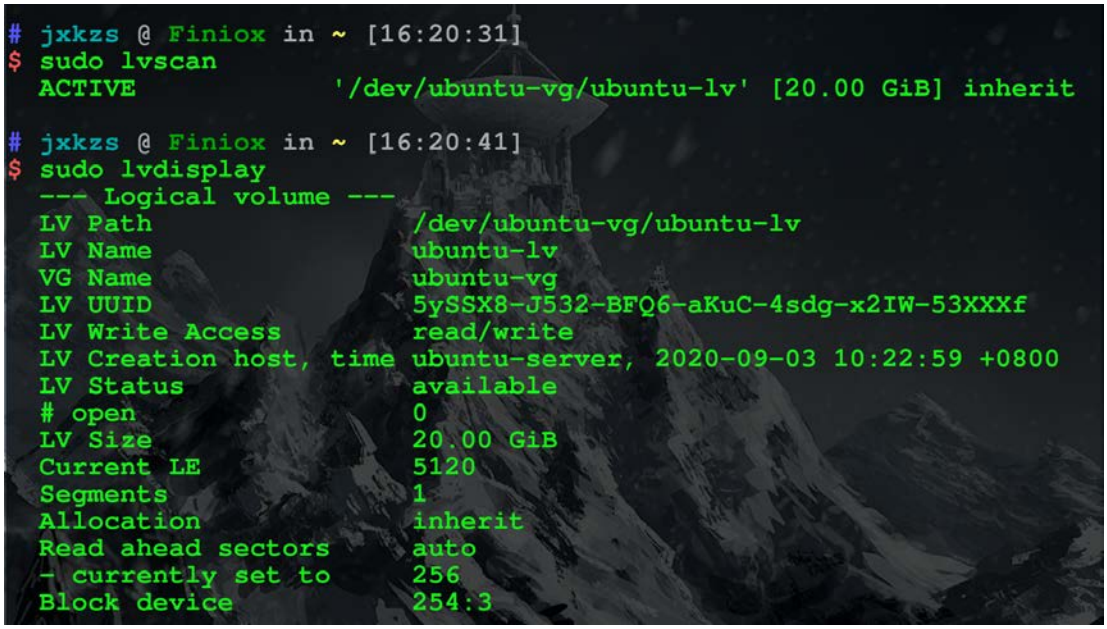
```
# jxkzs @ Finiox in ~ [16:19:36] C:1
$ sudo mount  /dev/mapper/loop0p2 /mnt/mount_v/2
```

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

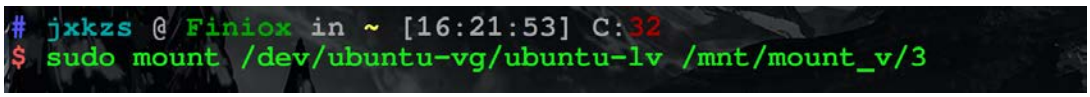



9、因第三个分区是 lvm，所以直接搜索就可以找到 lvm 信息


进一步查看可以看到 lv 及 vg 的信息和该设备的 UUID




10、将该分区挂载起来



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-x---  5 root     root     4096 Sep  3 16:59 htmlwordpress
drwxr-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_6
4 x86_64 GNU/Linux
```