Linux Incident Response - getting the EXT4 file creation time

Taz Wake | Halkyn Consulting Ltd | Originally published 2023-10-28

EXT4 (released in 2006) **does** include a file creation timestamp, the only problem is that we can't always get access to it without examining disk images. That can significantly slow down incident response.

As an example, look at Ubuntu. This Linux distro has used EXT4 as the default file system since 2009. However, coreutils (which is the package that includes the stat command we generally use to find the creation time) only reported a Creation timestamp in version 8.31, released in March 2019.

Unfortunately, for various reasons, this means if your Ubuntu distro is older than jammy (22.04 LTS, released in 2022), you probably have Coreutils 8.30-3ubuntu2. So no creation time for you.

This is what it looks like when you check a file in live-response.

```
$ stat test.txt
  File: test.txt
  Size: 26              Blocks: 8          IO Block: 4096   regular file
Device: 801h/2049d      Inode: 3670765     Links: 1
Access: (0664/-rw-rw-r--)  Uid: ( 1000/sansforensics)   Gid: ( 1000/sansforensics)
Access: 2023-10-28 11:44:33.273640958 +0000
Modify: 2023-10-28 11:44:33.273640958 +0000
Change: 2023-10-28 11:44:33.273640958 +0000
 Birth: -
```

stat command output in Coreutils 8.30

However, all is not lost. The **debugfs** command can help, but it can be a bit complicated.

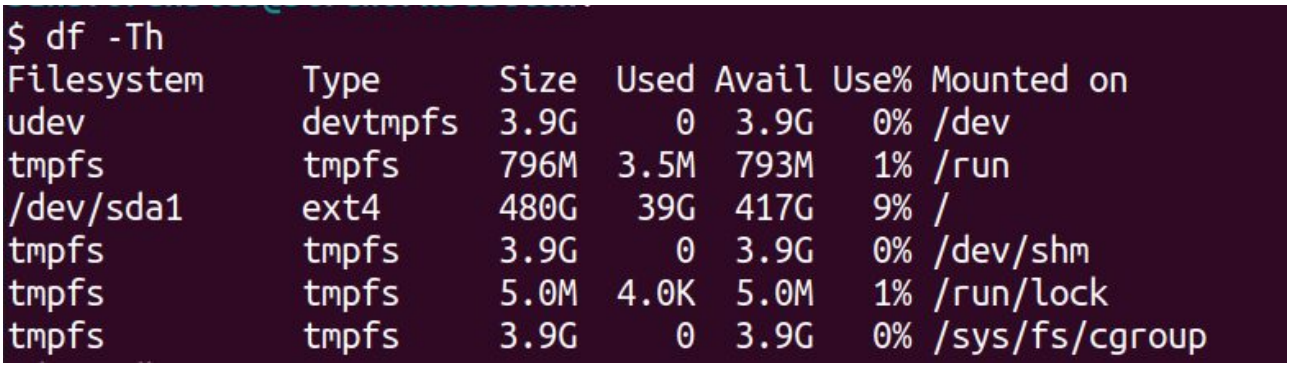
- First, you need to identify the **inode** number for the file. We can get the inode from the stat command output, or we can run:

In our example, the inode number is 3670765.

```
$ ls -i test.txt
3670765 test.txt
```

ls -i output

- Next, identify the mount point for the filesystem. There are a few ways to do this, the easiest might be to run the df -Th command but be aware some environments might be noisy, so grep can help.



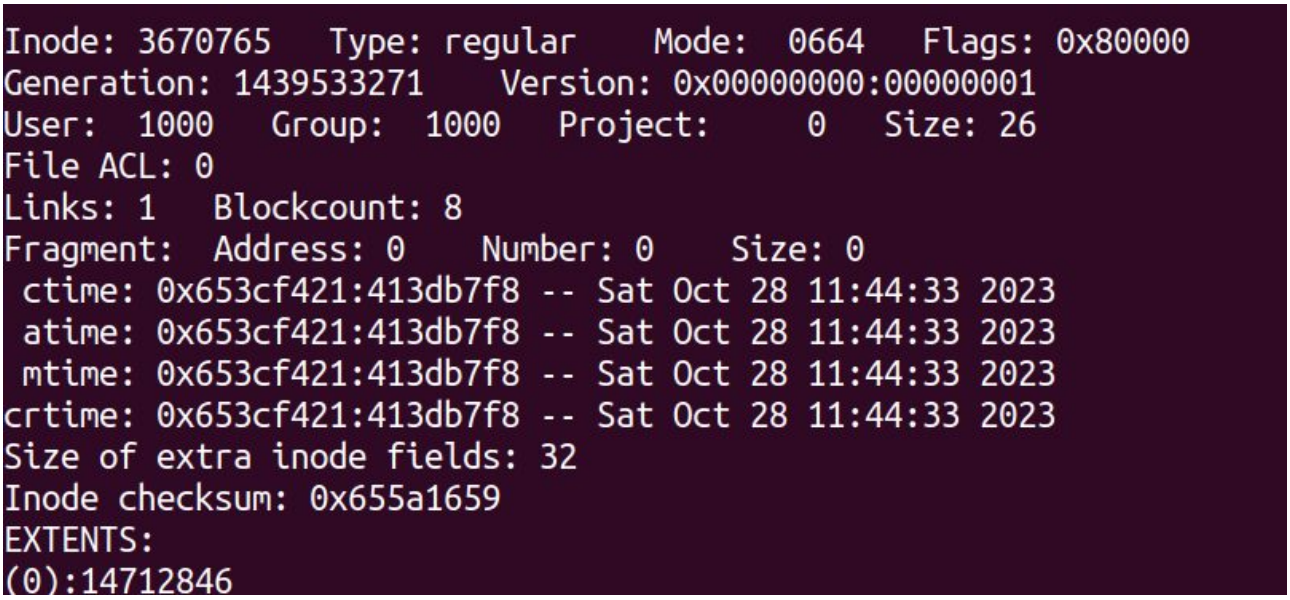
df -Th output

Looking at the data here, we can see that the / filesystem is mounted on /dev/sda1.

- Finally, you run the debugfs command (**as root**) with the -R argument to specify that you want it to run a command, and you give it the stat command, along with the inode number and mount point.

In our example, with inode 3670765 on /dev/sda1, the command would look like:

Now we can recover the creation timestamp



debugfs output showing creation timestamp

So, during live response on Linux platforms, add this to your tool kit and you will be able to get a creation timestamp even when the OS isn't new enough to realise it exists.

#Linux #Filesystems #Forensics #DFIR #IncidentResponse #Cybersecurity #Cyber

About Halkyn Consulting

Halkyn Consulting Ltd is a UK-based security and risk management consultancy providing 24/7 incident response, digital forensics, threat hunting, virtual security leadership (vCISO) and security compliance support to organisations worldwide. We deliver clear, practical, vendor-independent advice based on real-world threats — no hype, no upsell.

More free security resources are available at www.halkynconsulting.co.uk/security-resources.

Web: www.halkynconsulting.co.uk | **Email:** info@halkynconsulting.co.uk | **Tel:** +44 1244 940858