

Reg : File generation time and empty file flow values

Lavanya Singaravelan <lavanya.singaravelan@tatacommunications.com>

Tue 07/01/2020 14:34

To: Sriram Ramanujam <sriram.ramanujam@tatacommunications.com>

1. On checking the inode information of the file, the file is getting renamed/moved exactly at the 10 th min.PI refer the below screenshot

```
lavanya@lavanya-VirtualBox:/var/log/nfcapd$ ls -l nfcapd.202001071300
-rw-r--r-- 1 root root 276 Jan  7 13:10 nfcapd.202001071300
lavanya@lavanya-VirtualBox:/var/log/nfcapd$ ls -l nfcapd.202001071310
-rw-r--r-- 1 root root 276 Jan  7 13:20 nfcapd.202001071310
lavanya@lavanya-VirtualBox:/var/log/nfcapd$ ls -l nfcapd.202001071250
-rw-r--r-- 1 root root 276 Jan  7 13:00 nfcapd.202001071250
lavanya@lavanya-VirtualBox:/var/log/nfcapd$ ls -l nfcapd.202001071240
-rw-r--r-- 1 root root 276 Jan  7 12:50 nfcapd.202001071240
```

2. If there is no flow in a file then the following information will be available in the file

```
lavanya@lavanya-VirtualBox:/var/log/nfcapd$ nfdump -r nfcapd.202001062150 -o raw
Summary: total flows: 0, total bytes: 0, total packets: 0, avg bps: 0, avg pps:
0, avg bpp: 0
Time window: 2020-01-06 21:50:00 - 2020-01-06 22:00:00
Total flows processed: 0, Blocks skipped: 0, Bytes read: 108
Sys: 0.001s flows/second: 0.0      Wall: 0.000s flows/second: 0.0
```

Thanks and Regards,
Lavanya Singaravelan