Morris Worm Investigations

Overview

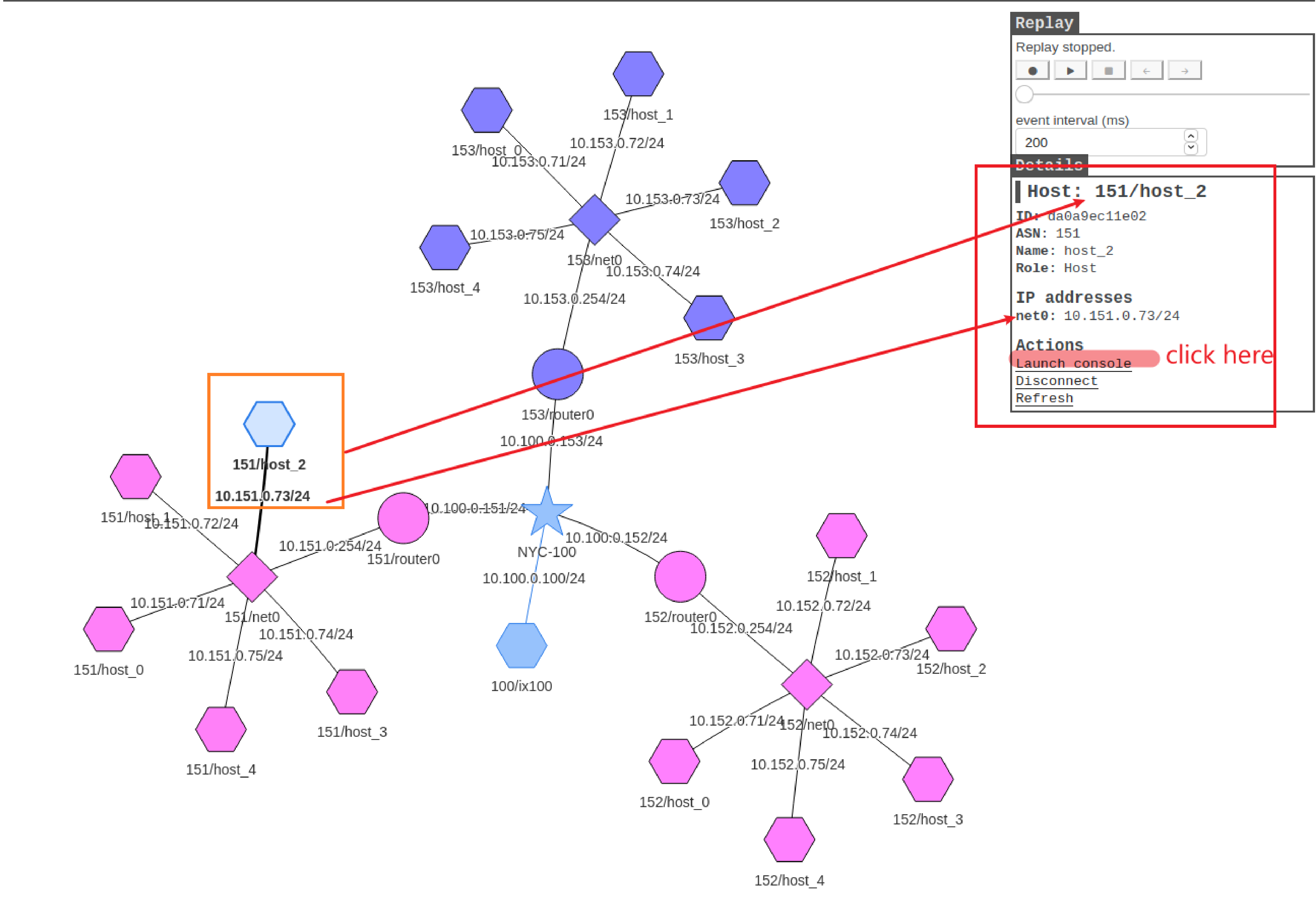
Analyze network ports used by worm

Analyze worm running processes

Create a timeline with file timestamps

Analyze network ports used by worm

SAJIN SHIVDAS



Replay

Replay stopped.

● ▶ ■ ← →

event interval (ms)

200

Details

Host: 151/host_2

ID: da0a9ec11e02
ASN: 151
Name: host_2
Role: Host

IP addresses

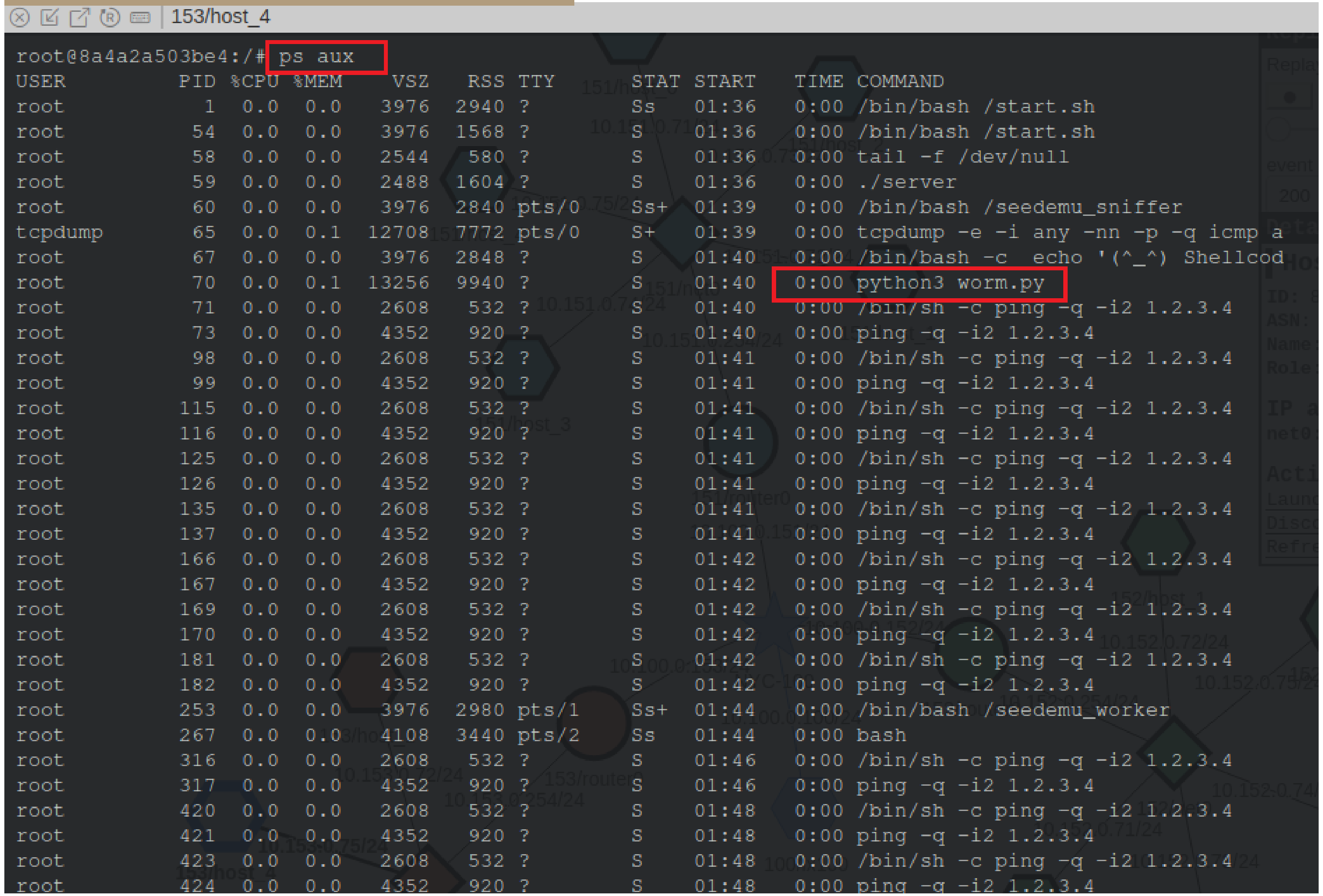
net0: 10.151.0.73/24

Actions

Launch console
Disconnect
Refresh

click here

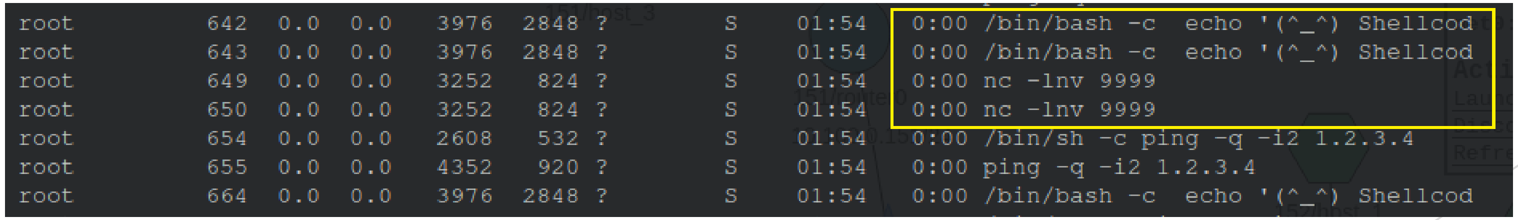
Check processes



153/host_4

```
root@8a4a2a503be4:/# ps aux
USER          PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root            1  0.0  0.0   3976  2940 ?        Ss   01:36   0:00 /bin/bash /start.sh
root           54  0.0  0.0   3976  1568 ?        S    01:36   0:00 /bin/bash /start.sh
root           58  0.0  0.0   2544   580 ?        S    01:36   0:00 tail -f /dev/null
root           59  0.0  0.0   2488  1604 ?        S    01:36   0:00 ./server
root           60  0.0  0.0   3976  2840 pts/0    Ss+  01:39   0:00 /bin/bash /seedemu_sniffer
tcpdump        65  0.0  0.1  12708  7772 pts/0    S+   01:39   0:00 tcpdump -e -i any -nn -p -q icmp a
root           67  0.0  0.0   3976  2848 ?        S    01:40   0:00 /bin/bash -c  echo '(^_^) Shellcod
root           70  0.0  0.1  13256  9940 ?        S    01:40   0:00 python3 worm.py
root           71  0.0  0.0   2608   532 ?        S    01:40   0:00 /bin/sh -c ping -q -i2 1.2.3.4
root           73  0.0  0.0   4352   920 ?        S    01:40   0:00 ping -q -i2 1.2.3.4
root           98  0.0  0.0   2608   532 ?        S    01:41   0:00 /bin/sh -c ping -q -i2 1.2.3.4
root           99  0.0  0.0   4352   920 ?        S    01:41   0:00 ping -q -i2 1.2.3.4
root          115  0.0  0.0   2608   532 ?        S    01:41   0:00 /bin/sh -c ping -q -i2 1.2.3.4
root          116  0.0  0.0   4352   920 ?        S    01:41   0:00 ping -q -i2 1.2.3.4
root          125  0.0  0.0   2608   532 ?        S    01:41   0:00 /bin/sh -c ping -q -i2 1.2.3.4
root          126  0.0  0.0   4352   920 ?        S    01:41   0:00 ping -q -i2 1.2.3.4
root          135  0.0  0.0   2608   532 ?        S    01:41   0:00 /bin/sh -c ping -q -i2 1.2.3.4
root          137  0.0  0.0   4352   920 ?        S    01:41   0:00 ping -q -i2 1.2.3.4
root          166  0.0  0.0   2608   532 ?        S    01:42   0:00 /bin/sh -c ping -q -i2 1.2.3.4
root          167  0.0  0.0   4352   920 ?        S    01:42   0:00 ping -q -i2 1.2.3.4
root          169  0.0  0.0   2608   532 ?        S    01:42   0:00 /bin/sh -c ping -q -i2 1.2.3.4
root          170  0.0  0.0   4352   920 ?        S    01:42   0:00 ping -q -i2 1.2.3.4
root          181  0.0  0.0   2608   532 ?        S    01:42   0:00 /bin/sh -c ping -q -i2 1.2.3.4
root          182  0.0  0.0   4352   920 ?        S    01:42   0:00 ping -q -i2 1.2.3.4
root          253  0.0  0.0   3976  2980 pts/1    Ss+  01:44   0:00 /bin/bash /seedemu_worker
root          267  0.0  0.0   4108  3440 pts/2    Ss   01:44   0:00 bash
root          316  0.0  0.0   2608   532 ?        S    01:46   0:00 /bin/sh -c ping -q -i2 1.2.3.4
root          317  0.0  0.0   4352   920 ?        S    01:46   0:00 ping -q -i2 1.2.3.4
root          420  0.0  0.0   2608   532 ?        S    01:48   0:00 /bin/sh -c ping -q -i2 1.2.3.4
root          421  0.0  0.0   4352   920 ?        S    01:48   0:00 ping -q -i2 1.2.3.4
root          423  0.0  0.0   2608   532 ?        S    01:48   0:00 /bin/sh -c ping -q -i2 1.2.3.4
root          424  0.0  0.0   4352   920 ?        S    01:48   0:00 ping -q -i2 1.2.3.4
```

worm.py process

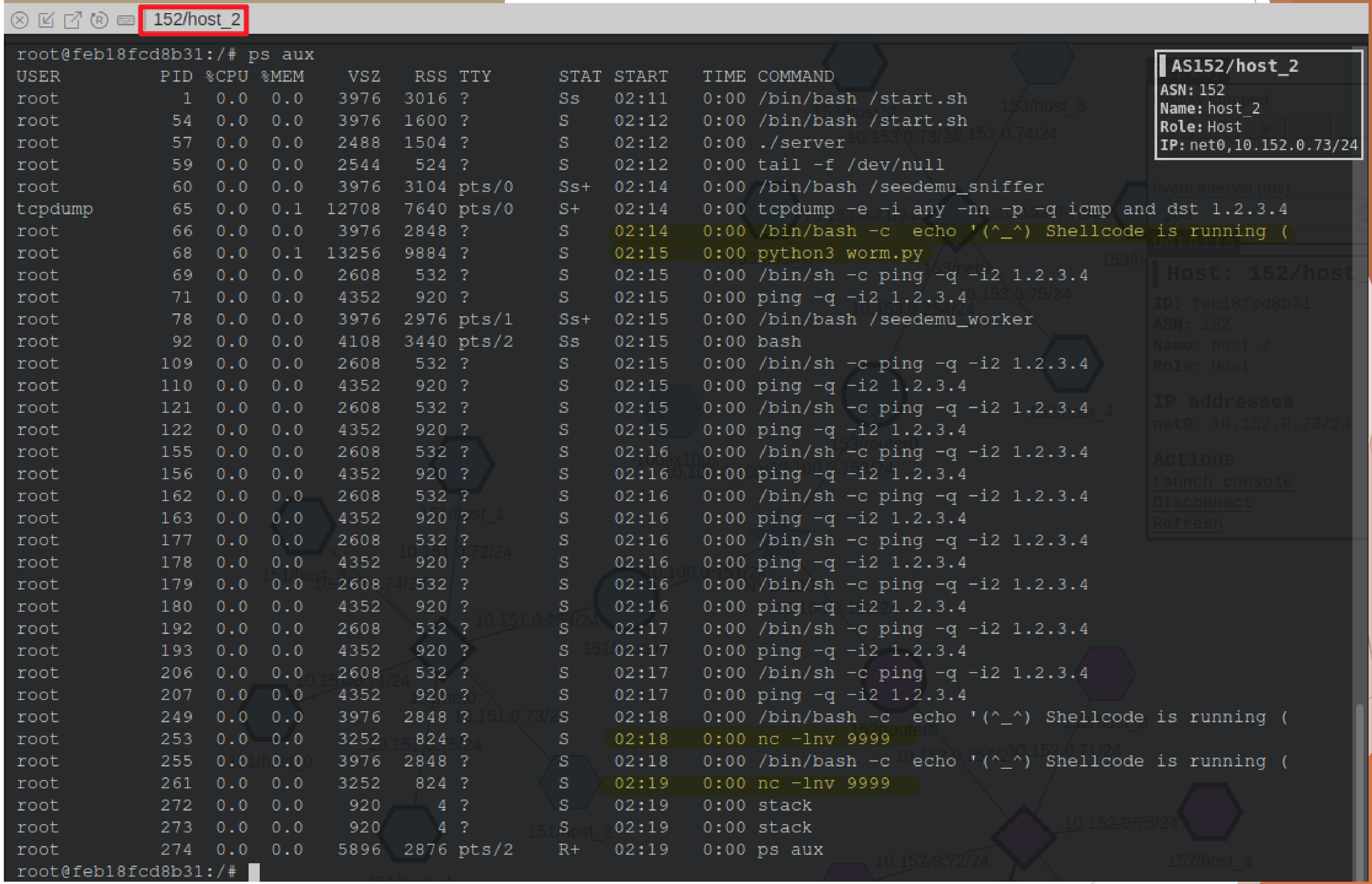


```
root          642  0.0  0.0   3976  2848 ?        S    01:54   0:00 /bin/bash -c  echo '(^_^) Shellcod
root          643  0.0  0.0   3976  2848 ?        S    01:54   0:00 /bin/bash -c  echo '(^_^) Shellcod
root          649  0.0  0.0   3252   824 ?        S    01:54   0:00 nc -lnv 9999
root          650  0.0  0.0   3252   824 ?        S    01:54   0:00 nc -lnv 9999
root          654  0.0  0.0   2608   532 ?        S    01:54   0:00 /bin/sh -c ping -q -i2 1.2.3.4
root          655  0.0  0.0   4352   920 ?        S    01:54   0:00 ping -q -i2 1.2.3.4
root          664  0.0  0.0   3976  2848 ?        S    01:54   0:00 /bin/bash -c  echo '(^_^) Shellcod
```

listening to port 9999

SAJIN SHIVDAS

Another machine

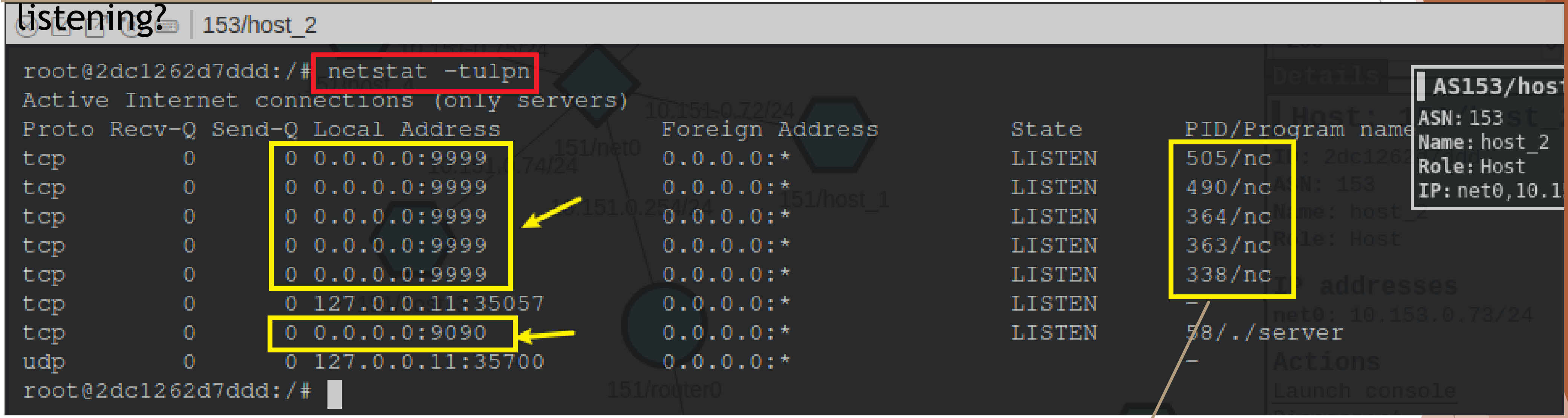


```
root@feb18fcd8b31:/# ps aux
USER             PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root               1  0.0  0.0   3976  3016 ?        Ss   02:11   0:00 /bin/bash /start.sh
root              54  0.0  0.0   3976  1600 ?        S    02:12   0:00 /bin/bash /start.sh
root              57  0.0  0.0   2488  1504 ?        S    02:12   0:00 ./server
root              59  0.0  0.0   2544   524 ?        S    02:12   0:00 tail -f /dev/null
root              60  0.0  0.0   3976  3104 pts/0    Ss+  02:14   0:00 /bin/bash /seedemu_sniffer
tcpdump           65  0.0  0.1  12708  7640 pts/0    S+   02:14   0:00 tcpdump -e -i any -nn -p -q icmp and dst 1.2.3.4
root              66  0.0  0.0   3976  2848 ?        S    02:14   0:00 /bin/bash -c  echo '(^_^) Shellcode is running (
root              68  0.0  0.1  13256  9884 ?        S    02:15   0:00 python3 worm.py
root              69  0.0  0.0   2608   532 ?        S    02:15   0:00 /bin/sh -c ping -q -i2 1.2.3.4
root              71  0.0  0.0   4352   920 ?        S    02:15   0:00 ping -q -i2 1.2.3.4
root              78  0.0  0.0   3976  2976 pts/1    Ss+  02:15   0:00 /bin/bash /seedemu_worker
root              92  0.0  0.0   4108  3440 pts/2    Ss   02:15   0:00 bash
root             109  0.0  0.0   2608   532 ?        S    02:15   0:00 /bin/sh -c ping -q -i2 1.2.3.4
root             110  0.0  0.0   4352   920 ?        S    02:15   0:00 ping -q -i2 1.2.3.4
root             121  0.0  0.0   2608   532 ?        S    02:15   0:00 /bin/sh -c ping -q -i2 1.2.3.4
root             122  0.0  0.0   4352   920 ?        S    02:15   0:00 ping -q -i2 1.2.3.4
root             155  0.0  0.0   2608   532 ?        S    02:16   0:00 /bin/sh -c ping -q -i2 1.2.3.4
root             156  0.0  0.0   4352   920 ?        S    02:16   0:00 ping -q -i2 1.2.3.4
root             162  0.0  0.0   2608   532 ?        S    02:16   0:00 /bin/sh -c ping -q -i2 1.2.3.4
root             163  0.0  0.0   4352   920 ?        S    02:16   0:00 ping -q -i2 1.2.3.4
root             177  0.0  0.0   2608   532 ?        S    02:16   0:00 /bin/sh -c ping -q -i2 1.2.3.4
root             178  0.0  0.0   4352   920 ?        S    02:16   0:00 ping -q -i2 1.2.3.4
root             179  0.0  0.0   2608   532 ?        S    02:16   0:00 /bin/sh -c ping -q -i2 1.2.3.4
root             180  0.0  0.0   4352   920 ?        S    02:16   0:00 ping -q -i2 1.2.3.4
root             192  0.0  0.0   2608   532 ?        S    02:17   0:00 /bin/sh -c ping -q -i2 1.2.3.4
root             193  0.0  0.0   4352   920 ?        S    02:17   0:00 ping -q -i2 1.2.3.4
root             206  0.0  0.0   2608   532 ?        S    02:17   0:00 /bin/sh -c ping -q -i2 1.2.3.4
root             207  0.0  0.0   4352   920 ?        S    02:17   0:00 ping -q -i2 1.2.3.4
root             249  0.0  0.0   3976  2848 ?        S    02:18   0:00 /bin/bash -c  echo '(^_^) Shellcode is running (
root             253  0.0  0.0   3252   824 ?        S    02:18   0:00 nc -lnv 9999
root             255  0.0  0.0   3976  2848 ?        S    02:18   0:00 /bin/bash -c  echo '(^_^) Shellcode is running (
root             261  0.0  0.0   3252   824 ?        S    02:19   0:00 nc -lnv 9999
root             272  0.0  0.0    920     4 ?        S    02:19   0:00 stack
root             273  0.0  0.0    920     4 ?        S    02:19   0:00 stack
root             274  0.0  0.0   5896  2876 pts/2    R+   02:19   0:00 ps aux
root@feb18fcd8b31:/#
```

AS152/host_2
ASN: 152
Name: host_2
Role: Host
IP: net0,10.152.0.73/24

Analyze worm running processes

What ports are listening?



153/host_2

```
root@2dc1262d7ddd:/# netstat -tulpn
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:9999            0.0.0.0:*               LISTEN      505/nc
tcp        0      0 0.0.0.0:9999            0.0.0.0:*               LISTEN      490/nc
tcp        0      0 0.0.0.0:9999            0.0.0.0:*               LISTEN      364/nc
tcp        0      0 0.0.0.0:9999            0.0.0.0:*               LISTEN      363/nc
tcp        0      0 0.0.0.0:9999            0.0.0.0:*               LISTEN      338/nc
tcp        0      0 127.0.0.11:35057        0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:9090            0.0.0.0:*               LISTEN      58/./server
udp        0      0 127.0.0.11:35700        0.0.0.0:*                           -
root@2dc1262d7ddd:/#
```

AS153/host
ASN: 153
Name: host_2
Role: Host
IP: net0,10.1

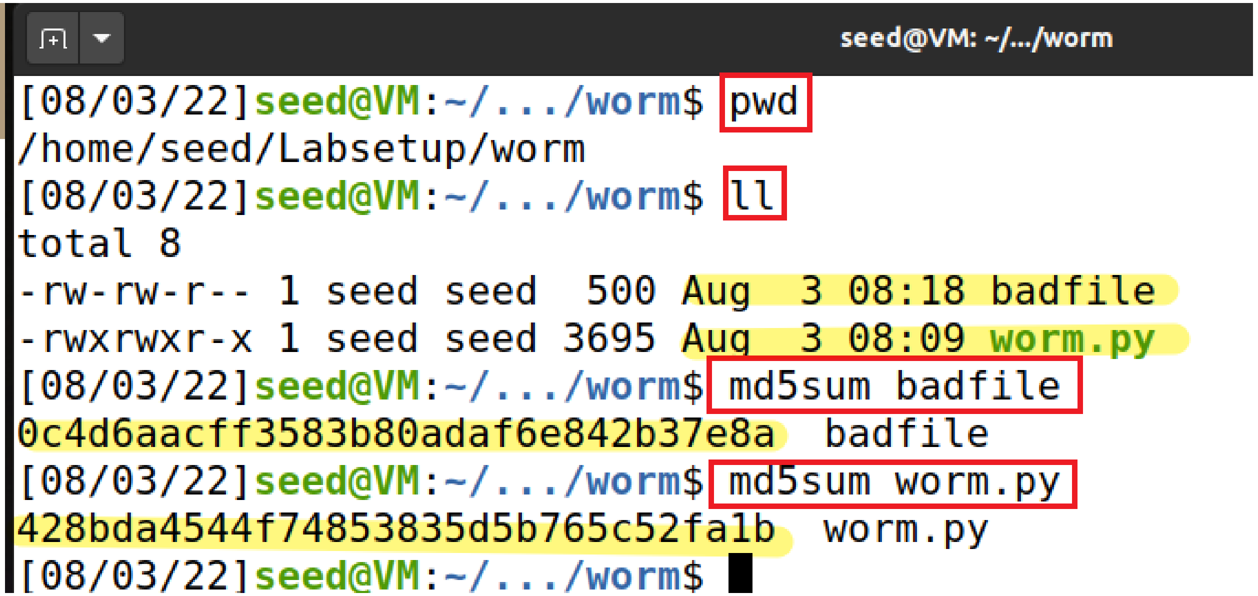
nc command

- listen to port 9999

Create a timeline with file timestamps

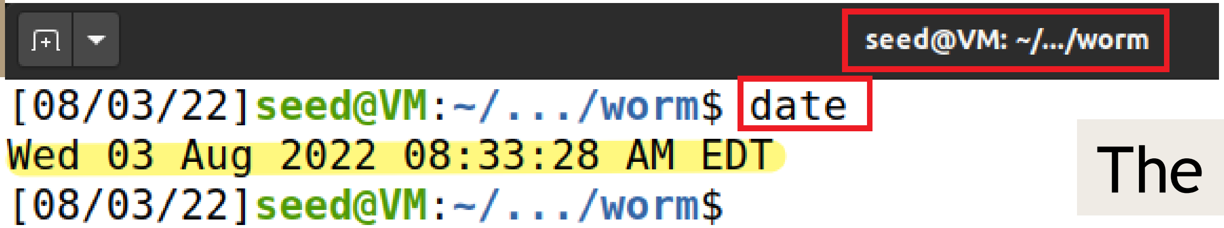
SAJIN SHIVDAS

Check attack files hash code



```
[08/03/22]seed@VM:~/.../worm$ pwd
/home/seed/Labsetup/worm
[08/03/22]seed@VM:~/.../worm$ ll
total 8
-rw-rw-r-- 1 seed seed  500 Aug  3 08:18 badfile
-rwxrwxr-x 1 seed seed 3695 Aug  3 08:09 worm.py
[08/03/22]seed@VM:~/.../worm$ md5sum badfile
0c4d6aacff3583b80adaf6e842b37e8a  badfile
[08/03/22]seed@VM:~/.../worm$ md5sum worm.py
428bda4544f74853835d5b765c52fa1b  worm.py
[08/03/22]seed@VM:~/.../worm$ 
```

Check time zone

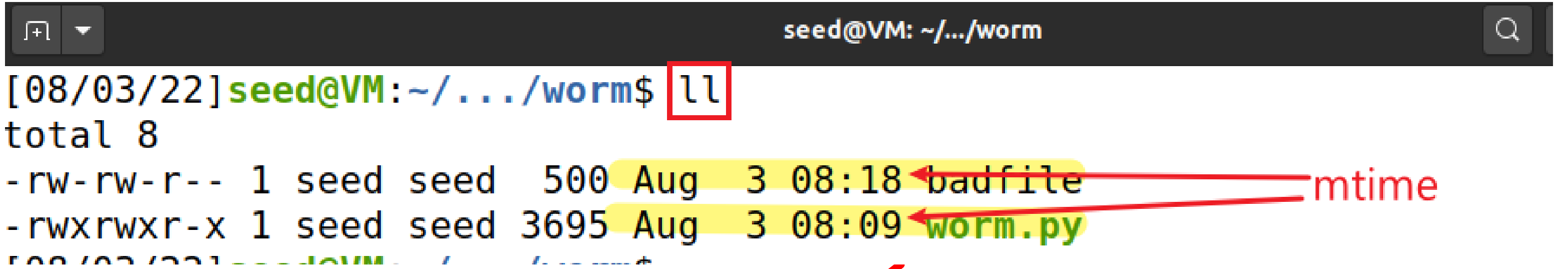


```
[08/03/22]seed@VM:~/.../worm$ date
Wed 03 Aug 2022 08:33:28 AM EDT
[08/03/22]seed@VM:~/.../worm$
```

The investigation date/EDT

SAJIN SHIVDAS

Check time stamps



```
seed@VM: ~/.../worm
[08/03/22]seed@VM:~/.../worm$ ll
total 8
-rw-rw-r-- 1 seed seed  500 Aug  3 08:18 badfile
-rwxrwxr-x 1 seed seed 3695 Aug  3 08:09 worm.py
[08/03/22]seed@VM:~/.../worm$
```

mtime

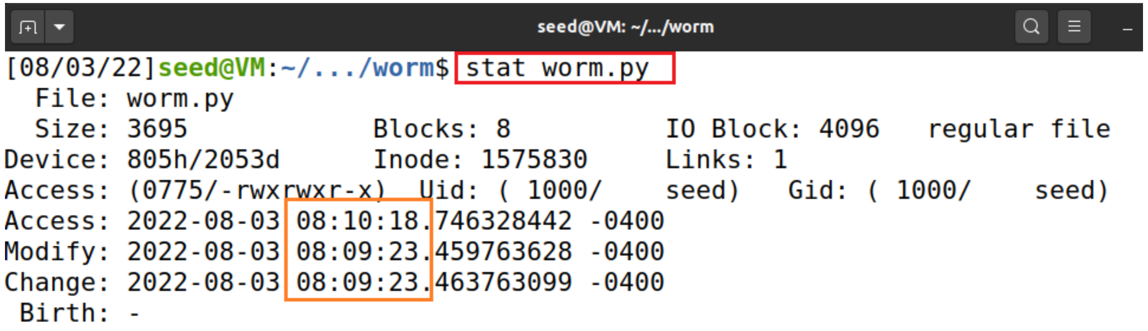
Changes C

	File Contents are Modified	Metadata is Modified	File Accessed	Command to Use
mtime	C			**ls -l** or **stat**
ctime		C		**ls -cl** or **stat**
atime			C	**ls -ul** or **stat**

Note that changes of **mtime** may change **ctime** and **atime** as well.

Check time stamps of worm.py

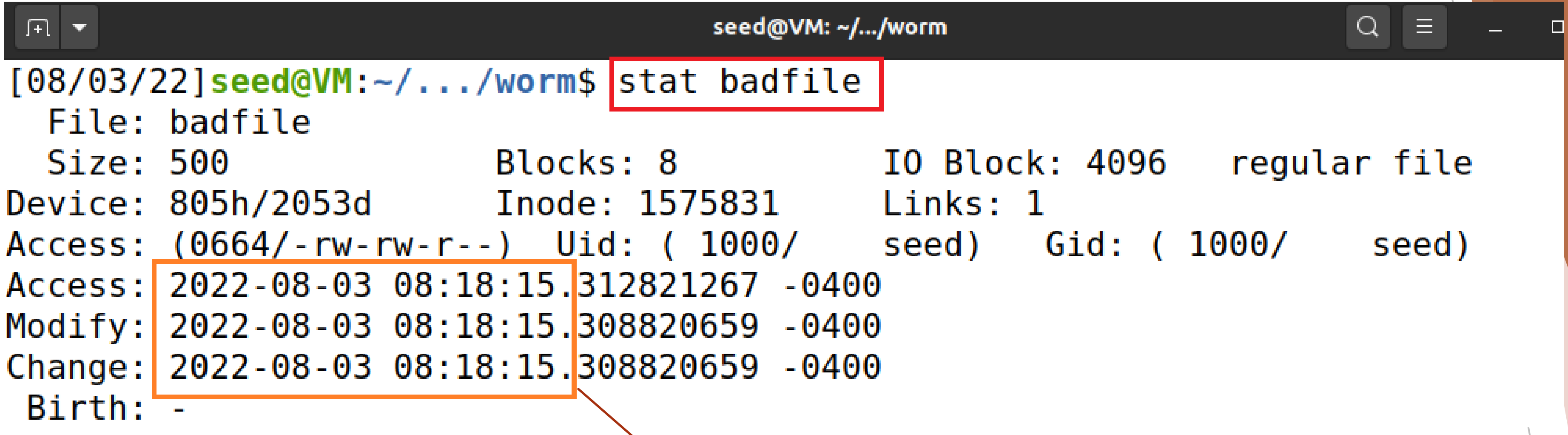
- worm.py
- A user changed content on 2022-8-3 08:09:23
- Accessed on 55 second later (e.g., read file)



```
[08/03/22]seed@VM:~/.../worm$ stat worm.py
  File: worm.py
  Size: 3695            Blocks: 8          IO Block: 4096   regular file
Device: 805h/2053d      Inode: 1575830     Links: 1
Access: (0775/-rwxrwxr-x)  Uid: ( 1000/    seed)   Gid: ( 1000/    seed)
Access: 2022-08-03 08:10:18.746328442 -0400
Modify: 2022-08-03 08:09:23.459763628 -0400
Change: 2022-08-03 08:09:23.463763099 -0400
 Birth: -
```

SAJIN SHIVDAS

Check time stamps of **badfile**



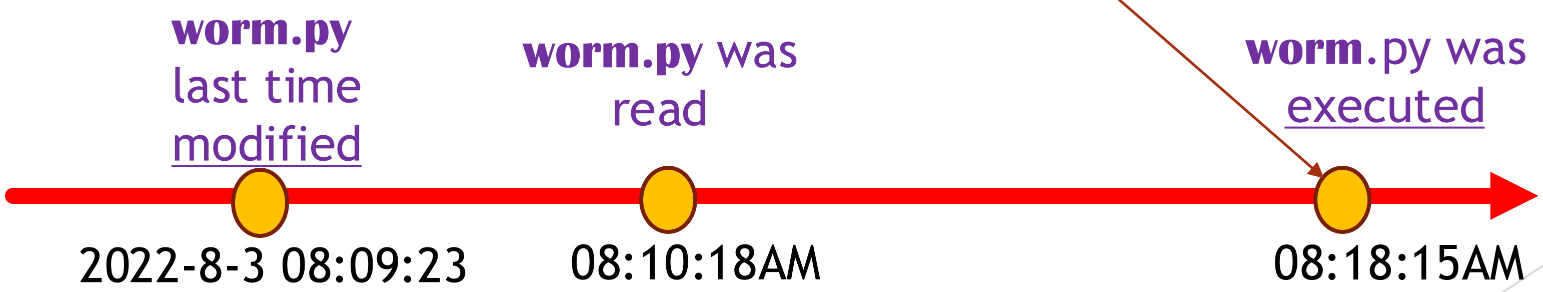
seed@VM: ~/.../worm

```
[08/03/22]seed@VM:~/.../worm$ stat badfile
  File: badfile
  Size: 500             Blocks: 8          IO Block: 4096   regular file
Device: 805h/2053d      Inode: 1575831     Links: 1
Access: (0664/-rw-rw-r--)  Uid: ( 1000/    seed)   Gid: ( 1000/    seed)
Access: 2022-08-03 08:18:15.312821267 -0400
Modify: 2022-08-03 08:18:15.308820659 -0400
Change: 2022-08-03 08:18:15.308820659 -0400
 Birth: -
```

badfile

- created on 2022-08-03 08:18:15

because **badfile** was created



worm.py last time modified

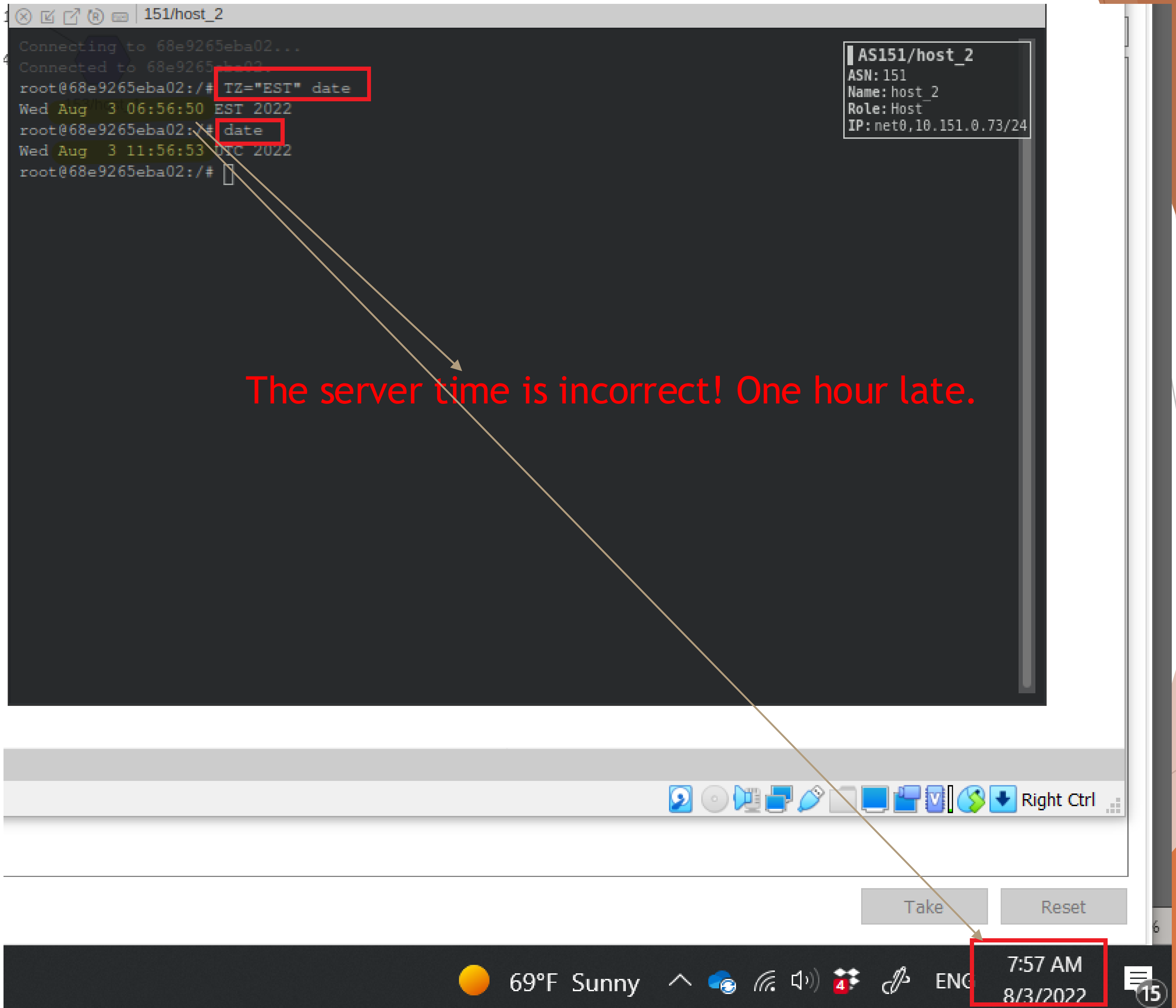
2022-8-3 08:09:23

worm.py was read

08:10:18AM

worm.py was executed

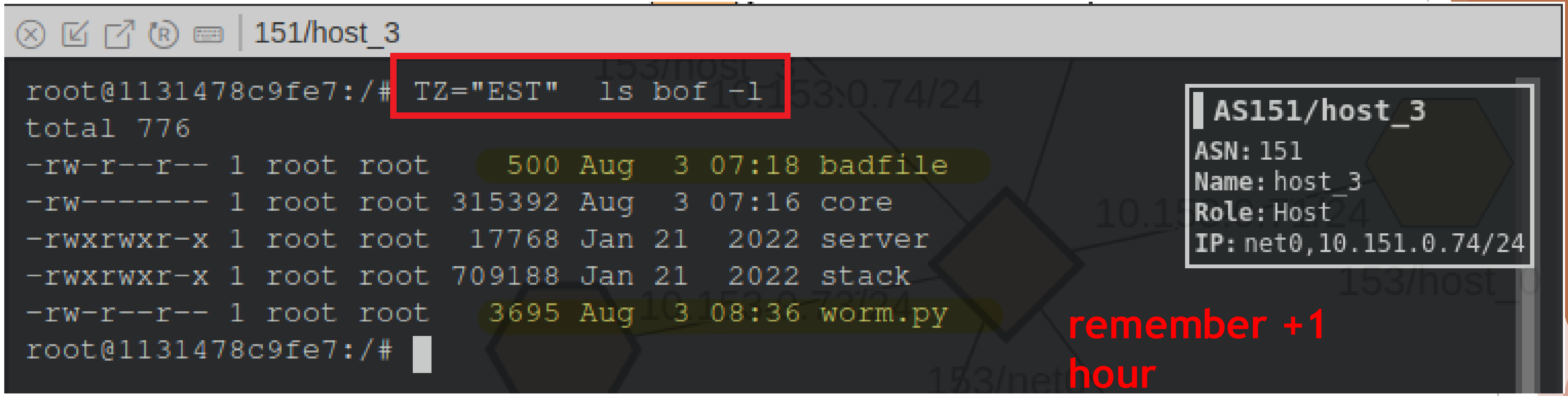
08:18:15AM



```
Connecting to 68e9265eba02...
Connected to 68e9265eba02.
root@68e9265eba02:/# TZ="EST" date
Wed Aug  3 06:56:50 EST 2022
root@68e9265eba02:/# date
Wed Aug  3 11:56:53 UTC 2022
root@68e9265eba02:/#
```

```
AS151/host_2
ASN: 151
Name: host_2
Role: Host
IP: net0,10.151.0.73/24
```

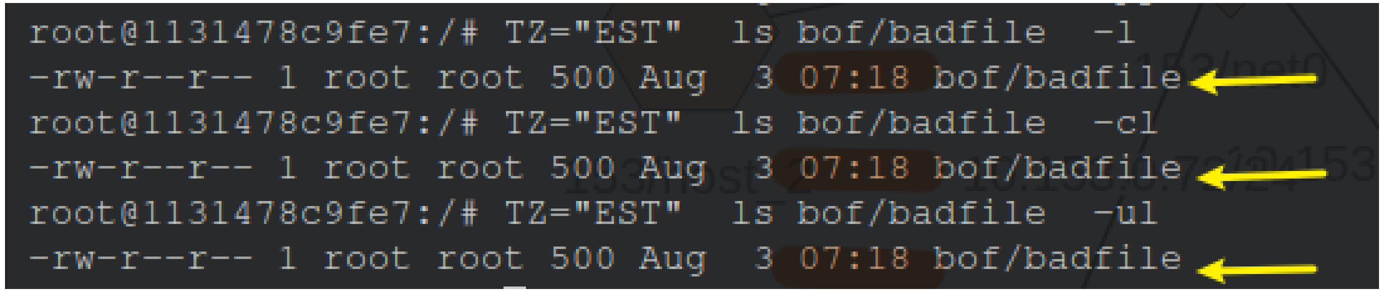
The server time is incorrect! One hour late.



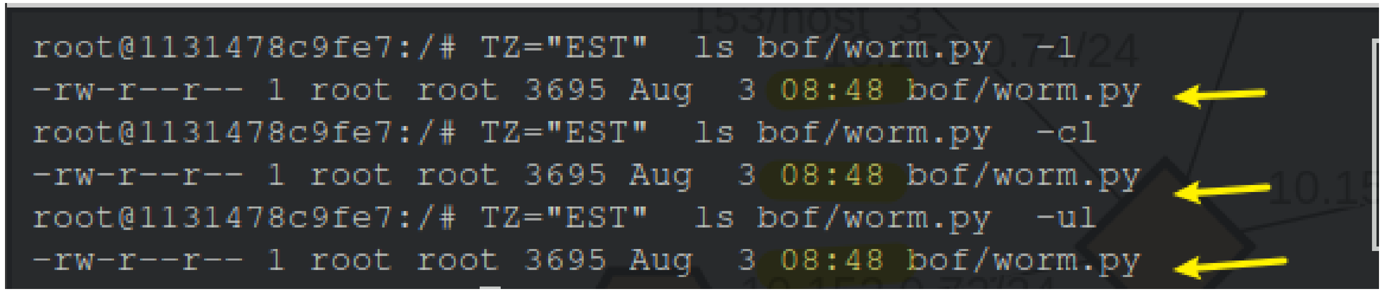
```
root@1131478c9fe7:/# TZ="EST"  ls bof -l
total 776
-rw-r--r-- 1 root root    500 Aug  3 07:18 badfile
-rw------- 1 root root 315392 Aug  3 07:16 core
-rwxrwxr-x 1 root root  17768 Jan 21  2022 server
-rwxrwxr-x 1 root root 709188 Jan 21  2022 stack
-rw-r--r-- 1 root root   3695 Aug  3 08:36 worm.py
root@1131478c9fe7:/#
```

AS151/host_3
ASN: 151
Name: host_3
Role: Host
IP: net0,10.151.0.74/24

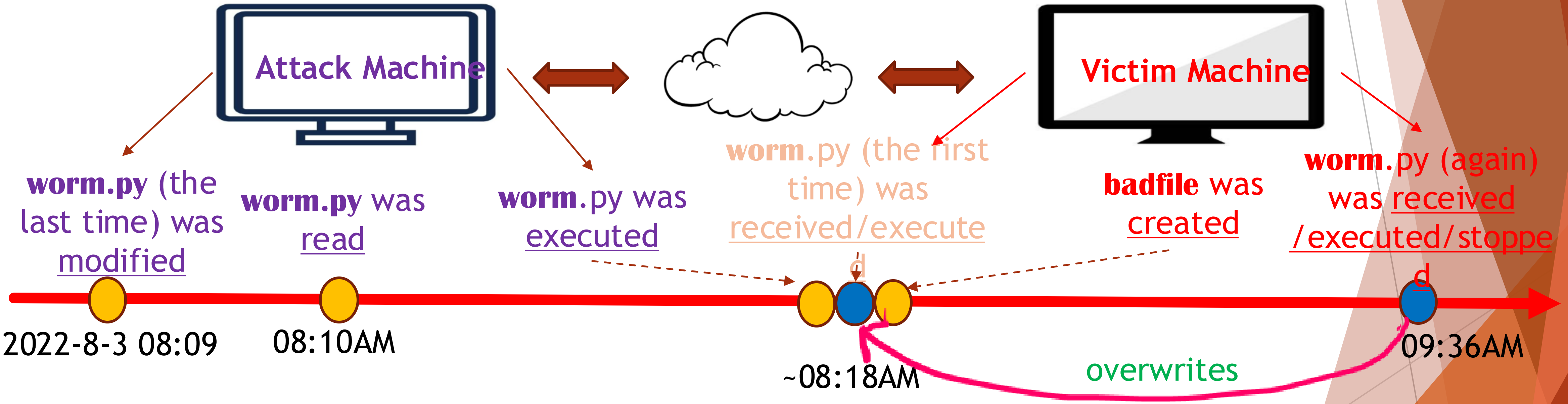
remember +1 hour



```
root@1131478c9fe7:/# TZ="EST"  ls bof/badfile  -l
-rw-r--r-- 1 root root 500 Aug  3 07:18 bof/badfile
root@1131478c9fe7:/# TZ="EST"  ls bof/badfile  -cl
-rw-r--r-- 1 root root 500 Aug  3 07:18 bof/badfile
root@1131478c9fe7:/# TZ="EST"  ls bof/badfile  -ul
-rw-r--r-- 1 root root 500 Aug  3 07:18 bof/badfile
```



```
root@1131478c9fe7:/# TZ="EST"  ls bof/worm.py  -l
-rw-r--r-- 1 root root 3695 Aug  3 08:48 bof/worm.py
root@1131478c9fe7:/# TZ="EST"  ls bof/worm.py  -cl
-rw-r--r-- 1 root root 3695 Aug  3 08:48 bof/worm.py
root@1131478c9fe7:/# TZ="EST"  ls bof/worm.py  -ul
-rw-r--r-- 1 root root 3695 Aug  3 08:48 bof/worm.py
```



Attack Machine

Victim Machine

worm.py (the last time) was modified

2022-8-3 08:09

worm.py was read

08:10AM

worm.py was executed

worm.py (the first time) was received/executed

~08:18AM

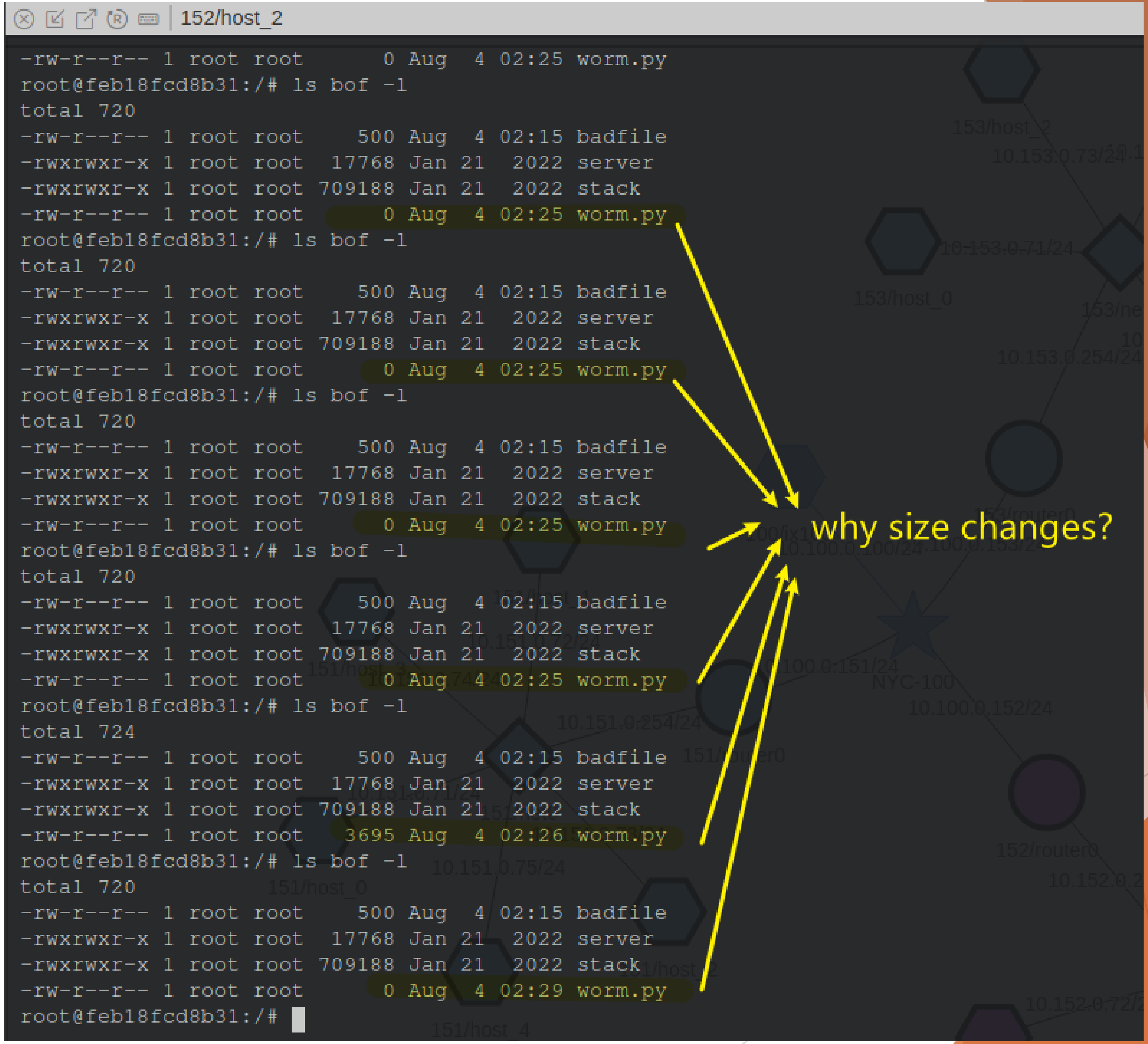
badfile was created

worm.py (again) was received/executed/stopped

09:36AM

overwrites

Question



```
-rw-r--r-- 1 root root      0 Aug  4 02:25 worm.py
root@feb18fcd8b31:/# ls bof -l
total 720
-rw-r--r-- 1 root root    500 Aug  4 02:15 badfile
-rwxrwxr-x 1 root root  17768 Jan 21  2022 server
-rwxrwxr-x 1 root root 709188 Jan 21  2022 stack
-rw-r--r-- 1 root root      0 Aug  4 02:25 worm.py
root@feb18fcd8b31:/# ls bof -l
total 720
-rw-r--r-- 1 root root    500 Aug  4 02:15 badfile
-rwxrwxr-x 1 root root  17768 Jan 21  2022 server
-rwxrwxr-x 1 root root 709188 Jan 21  2022 stack
-rw-r--r-- 1 root root      0 Aug  4 02:25 worm.py
root@feb18fcd8b31:/# ls bof -l
total 720
-rw-r--r-- 1 root root    500 Aug  4 02:15 badfile
-rwxrwxr-x 1 root root  17768 Jan 21  2022 server
-rwxrwxr-x 1 root root 709188 Jan 21  2022 stack
-rw-r--r-- 1 root root      0 Aug  4 02:25 worm.py
root@feb18fcd8b31:/# ls bof -l
total 720
-rw-r--r-- 1 root root    500 Aug  4 02:15 badfile
-rwxrwxr-x 1 root root  17768 Jan 21  2022 server
-rwxrwxr-x 1 root root 709188 Jan 21  2022 stack
-rw-r--r-- 1 root root      0 Aug  4 02:25 worm.py
root@feb18fcd8b31:/# ls bof -l
total 724
-rw-r--r-- 1 root root    500 Aug  4 02:15 badfile
-rwxrwxr-x 1 root root  17768 Jan 21  2022 server
-rwxrwxr-x 1 root root 709188 Jan 21  2022 stack
-rw-r--r-- 1 root root   3695 Aug  4 02:26 worm.py
root@feb18fcd8b31:/# ls bof -l
total 720
-rw-r--r-- 1 root root    500 Aug  4 02:15 badfile
-rwxrwxr-x 1 root root  17768 Jan 21  2022 server
-rwxrwxr-x 1 root root 709188 Jan 21  2022 stack
-rw-r--r-- 1 root root      0 Aug  4 02:29 worm.py
root@feb18fcd8b31:/#
```

why size changes?

SAJIN SHIVDAS