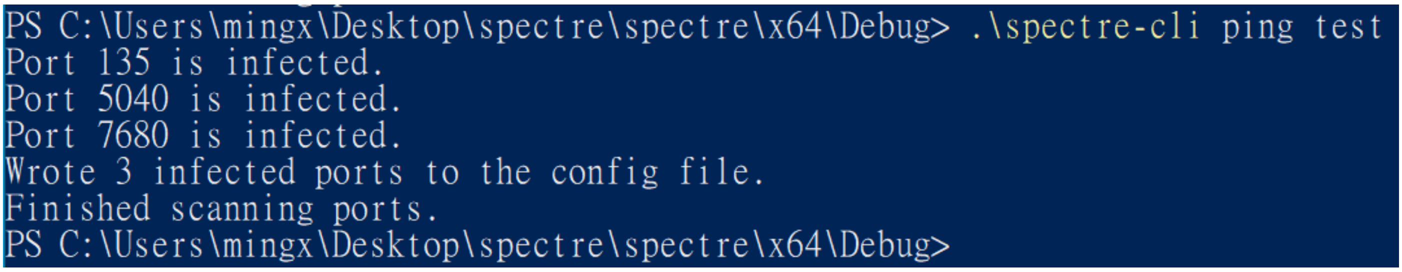
HW4. Memory Foresics

L091025 清大資工所 熊詩旻

Task1. Installing rootkit

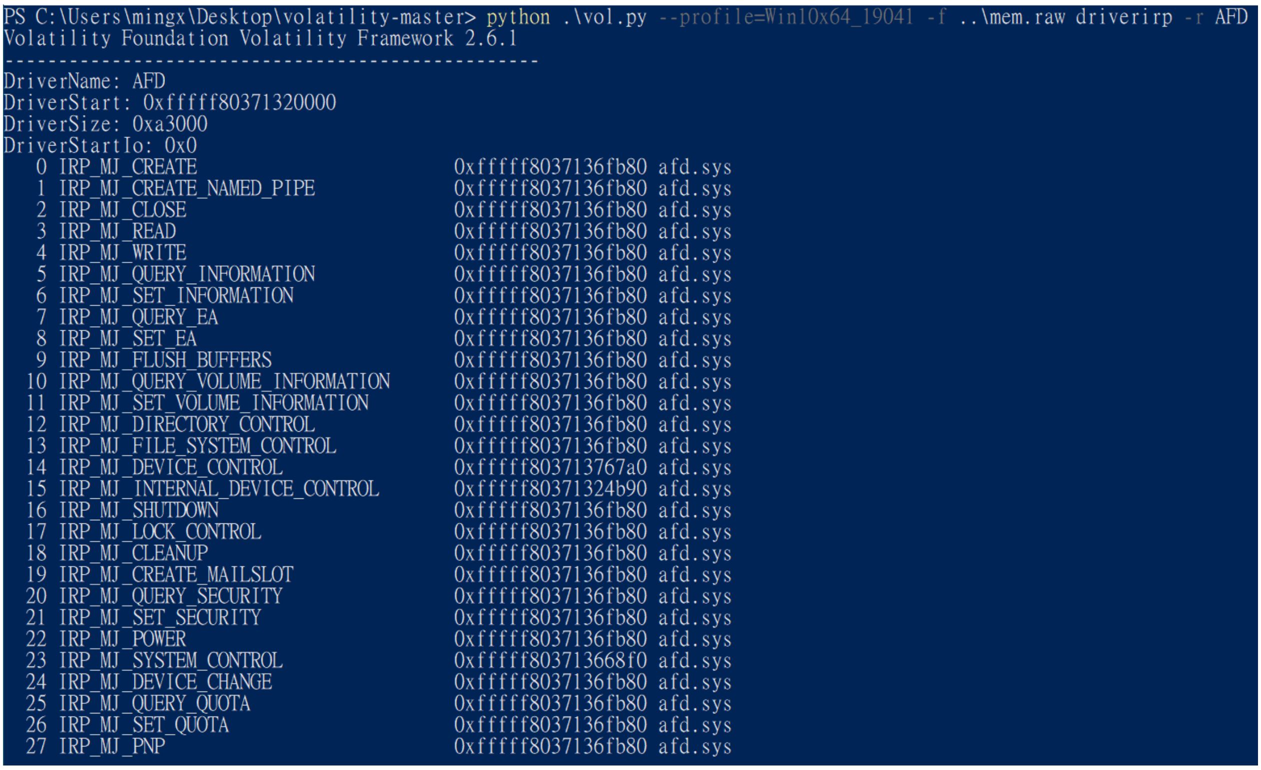


```
PS C:\Users\mingx\Desktop\spectre\spectre\x64\Debug> .\spectre-cli ping test
Port 135 is infected.
Port 5040 is infected.
Port 7680 is infected.
Wrote 3 infected ports to the config file.
Finished scanning ports.
PS C:\Users\mingx\Desktop\spectre\spectre\x64\Debug>
```

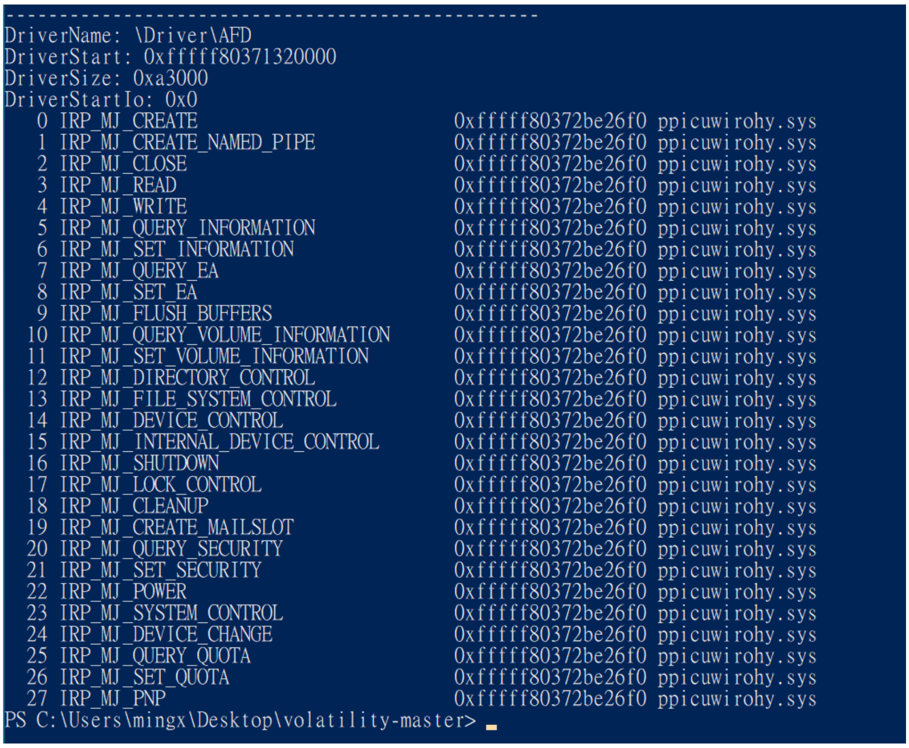
Task2

1) Simply Explain "IRP Major Function".
   IRP means I/O request packet, IRP Major Function tells the driver what operation it or the underlying device driver should carry out to satisfy the I/O request.

2) Generate a memory dump in test mode. Use Volatility to show the MajorFunction array of AFD. Take a screenshot of your result.

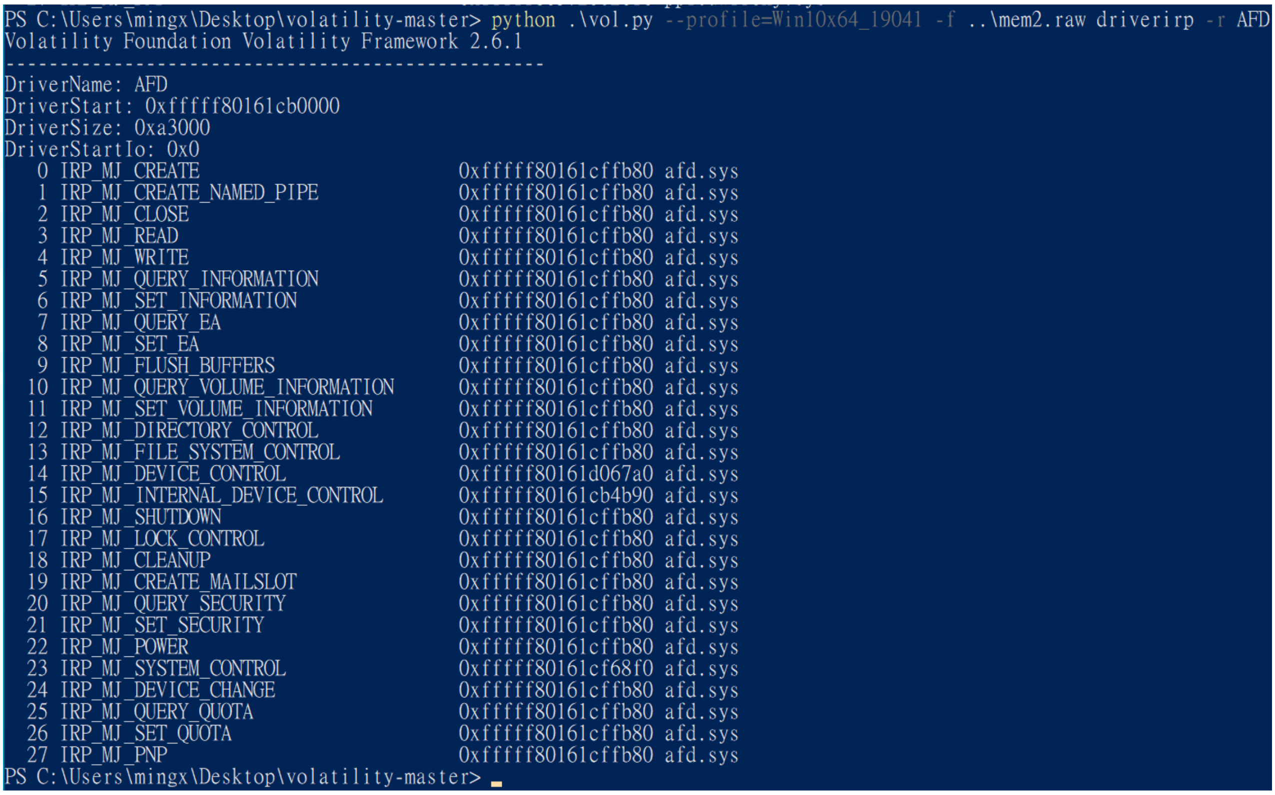


```
PS C:\Users\mingx\Desktop\volatility-master> python .\vol.py --profile=Win10x64_19041 -f ..\mem.raw driverirp -r AFD
Volatility Foundation Volatility Framework 2.6.1
--------------------------------------------------
DriverName: AFD
DriverStart: 0xfffff80371320000
DriverSize: 0xa3000
DriverStartIo: 0x0
   0 IRP_MJ_CREATE                      0xfffff8037136fb80 afd.sys
   1 IRP_MJ_CREATE_NAMED_PIPE           0xfffff8037136fb80 afd.sys
   2 IRP_MJ_CLOSE                       0xfffff8037136fb80 afd.sys
   3 IRP_MJ_READ                        0xfffff8037136fb80 afd.sys
   4 IRP_MJ_WRITE                       0xfffff8037136fb80 afd.sys
   5 IRP_MJ_QUERY_INFORMATION           0xfffff8037136fb80 afd.sys
   6 IRP_MJ_SET_INFORMATION             0xfffff8037136fb80 afd.sys
   7 IRP_MJ_QUERY_EA                    0xfffff8037136fb80 afd.sys
   8 IRP_MJ_SET_EA                      0xfffff8037136fb80 afd.sys
   9 IRP_MJ_FLUSH_BUFFERS               0xfffff8037136fb80 afd.sys
  10 IRP_MJ_QUERY_VOLUME_INFORMATION    0xfffff8037136fb80 afd.sys
  11 IRP_MJ_SET_VOLUME_INFORMATION      0xfffff8037136fb80 afd.sys
  12 IRP_MJ_DIRECTORY_CONTROL           0xfffff8037136fb80 afd.sys
  13 IRP_MJ_FILE_SYSTEM_CONTROL         0xfffff8037136fb80 afd.sys
  14 IRP_MJ_DEVICE_CONTROL              0xfffff803713767a0 afd.sys
  15 IRP_MJ_INTERNAL_DEVICE_CONTROL     0xfffff80371324b90 afd.sys
  16 IRP_MJ_SHUTDOWN                    0xfffff8037136fb80 afd.sys
  17 IRP_MJ_LOCK_CONTROL                0xfffff8037136fb80 afd.sys
  18 IRP_MJ_CLEANUP                     0xfffff8037136fb80 afd.sys
  19 IRP_MJ_CREATE_MAILSLOT             0xfffff8037136fb80 afd.sys
  20 IRP_MJ_QUERY_SECURITY              0xfffff8037136fb80 afd.sys
  21 IRP_MJ_SET_SECURITY                0xfffff8037136fb80 afd.sys
  22 IRP_MJ_POWER                       0xfffff8037136fb80 afd.sys
  23 IRP_MJ_SYSTEM_CONTROL              0xfffff803713668f0 afd.sys
  24 IRP_MJ_DEVICE_CHANGE               0xfffff8037136fb80 afd.sys
  25 IRP_MJ_QUERY_QUOTA                 0xfffff8037136fb80 afd.sys
  26 IRP_MJ_SET_QUOTA                   0xfffff8037136fb80 afd.sys
  27 IRP_MJ_PNP                         0xfffff8037136fb80 afd.sys
```



```
--------------------------------------------------
DriverName: \Driver\AFD
DriverStart: 0xfffff80371320000
DriverSize: 0xa3000
DriverStartIo: 0x0
   0 IRP_MJ_CREATE                          0xfffff80372be26f0 ppicuwirohy.sys
   1 IRP_MJ_CREATE_NAMED_PIPE               0xfffff80372be26f0 ppicuwirohy.sys
   2 IRP_MJ_CLOSE                           0xfffff80372be26f0 ppicuwirohy.sys
   3 IRP_MJ_READ                            0xfffff80372be26f0 ppicuwirohy.sys
   4 IRP_MJ_WRITE                           0xfffff80372be26f0 ppicuwirohy.sys
   5 IRP_MJ_QUERY_INFORMATION               0xfffff80372be26f0 ppicuwirohy.sys
   6 IRP_MJ_SET_INFORMATION                 0xfffff80372be26f0 ppicuwirohy.sys
   7 IRP_MJ_QUERY_EA                        0xfffff80372be26f0 ppicuwirohy.sys
   8 IRP_MJ_SET_EA                          0xfffff80372be26f0 ppicuwirohy.sys
   9 IRP_MJ_FLUSH_BUFFERS                   0xfffff80372be26f0 ppicuwirohy.sys
  10 IRP_MJ_QUERY_VOLUME_INFORMATION        0xfffff80372be26f0 ppicuwirohy.sys
  11 IRP_MJ_SET_VOLUME_INFORMATION          0xfffff80372be26f0 ppicuwirohy.sys
  12 IRP_MJ_DIRECTORY_CONTROL               0xfffff80372be26f0 ppicuwirohy.sys
  13 IRP_MJ_FILE_SYSTEM_CONTROL             0xfffff80372be26f0 ppicuwirohy.sys
  14 IRP_MJ_DEVICE_CONTROL                  0xfffff80372be26f0 ppicuwirohy.sys
  15 IRP_MJ_INTERNAL_DEVICE_CONTROL         0xfffff80372be26f0 ppicuwirohy.sys
  16 IRP_MJ_SHUTDOWN                        0xfffff80372be26f0 ppicuwirohy.sys
  17 IRP_MJ_LOCK_CONTROL                    0xfffff80372be26f0 ppicuwirohy.sys
  18 IRP_MJ_CLEANUP                         0xfffff80372be26f0 ppicuwirohy.sys
  19 IRP_MJ_CREATE_MAILSLOT                 0xfffff80372be26f0 ppicuwirohy.sys
  20 IRP_MJ_QUERY_SECURITY                  0xfffff80372be26f0 ppicuwirohy.sys
  21 IRP_MJ_SET_SECURITY                    0xfffff80372be26f0 ppicuwirohy.sys
  22 IRP_MJ_POWER                           0xfffff80372be26f0 ppicuwirohy.sys
  23 IRP_MJ_SYSTEM_CONTROL                  0xfffff80372be26f0 ppicuwirohy.sys
  24 IRP_MJ_DEVICE_CHANGE                   0xfffff80372be26f0 ppicuwirohy.sys
  25 IRP_MJ_QUERY_QUOTA                     0xfffff80372be26f0 ppicuwirohy.sys
  26 IRP_MJ_SET_QUOTA                       0xfffff80372be26f0 ppicuwirohy.sys
  27 IRP_MJ_PNP                             0xfffff80372be26f0 ppicuwirohy.sys
PS C:\Users\mingx\Desktop\volatility-master>
```

3) Disable test mode and generate another image. Use Volatility to show the MajorFunction array of AFD. Take a screenshot of your result.



```
PS C:\Users\mingx\Desktop\volatility-master> python .\vol.py --profile=Win10x64_19041 -f ..\mem2.raw driverirp -r AFD
Volatility Foundation Volatility Framework 2.6.1
--------------------------------------------------
DriverName: AFD
DriverStart: 0xfffff80161cb0000
DriverSize: 0xa3000
DriverStartIo: 0x0
   0 IRP_MJ_CREATE                          0xfffff80161cffb80 afd.sys
   1 IRP_MJ_CREATE_NAMED_PIPE               0xfffff80161cffb80 afd.sys
   2 IRP_MJ_CLOSE                           0xfffff80161cffb80 afd.sys
   3 IRP_MJ_READ                            0xfffff80161cffb80 afd.sys
   4 IRP_MJ_WRITE                           0xfffff80161cffb80 afd.sys
   5 IRP_MJ_QUERY_INFORMATION               0xfffff80161cffb80 afd.sys
   6 IRP_MJ_SET_INFORMATION                 0xfffff80161cffb80 afd.sys
   7 IRP_MJ_QUERY_EA                        0xfffff80161cffb80 afd.sys
   8 IRP_MJ_SET_EA                          0xfffff80161cffb80 afd.sys
   9 IRP_MJ_FLUSH_BUFFERS                   0xfffff80161cffb80 afd.sys
  10 IRP_MJ_QUERY_VOLUME_INFORMATION        0xfffff80161cffb80 afd.sys
  11 IRP_MJ_SET_VOLUME_INFORMATION          0xfffff80161cffb80 afd.sys
  12 IRP_MJ_DIRECTORY_CONTROL               0xfffff80161cffb80 afd.sys
  13 IRP_MJ_FILE_SYSTEM_CONTROL             0xfffff80161cffb80 afd.sys
  14 IRP_MJ_DEVICE_CONTROL                  0xfffff80161d067a0 afd.sys
  15 IRP_MJ_INTERNAL_DEVICE_CONTROL         0xfffff80161cb4b90 afd.sys
  16 IRP_MJ_SHUTDOWN                        0xfffff80161cffb80 afd.sys
  17 IRP_MJ_LOCK_CONTROL                    0xfffff80161cffb80 afd.sys
  18 IRP_MJ_CLEANUP                         0xfffff80161cffb80 afd.sys
  19 IRP_MJ_CREATE_MAILSLOT                 0xfffff80161cffb80 afd.sys
  20 IRP_MJ_QUERY_SECURITY                  0xfffff80161cffb80 afd.sys
  21 IRP_MJ_SET_SECURITY                    0xfffff80161cffb80 afd.sys
  22 IRP_MJ_POWER                           0xfffff80161cffb80 afd.sys
  23 IRP_MJ_SYSTEM_CONTROL                  0xfffff80161cf68f0 afd.sys
  24 IRP_MJ_DEVICE_CHANGE                   0xfffff80161cffb80 afd.sys
  25 IRP_MJ_QUERY_QUOTA                     0xfffff80161cffb80 afd.sys
  26 IRP_MJ_SET_QUOTA                       0xfffff80161cffb80 afd.sys
  27 IRP_MJ_PNP                             0xfffff80161cffb80 afd.sys
PS C:\Users\mingx\Desktop\volatility-master>
```