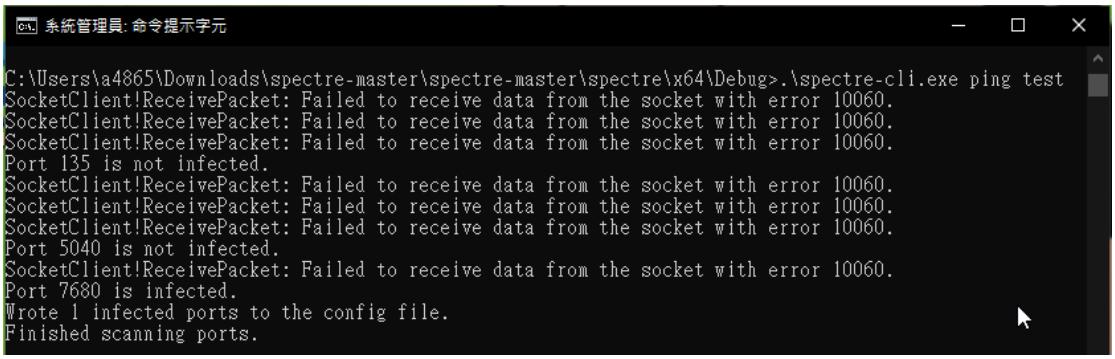
網安實務 Hw4

網工所碩一 309552005 吳偉誠

Question1

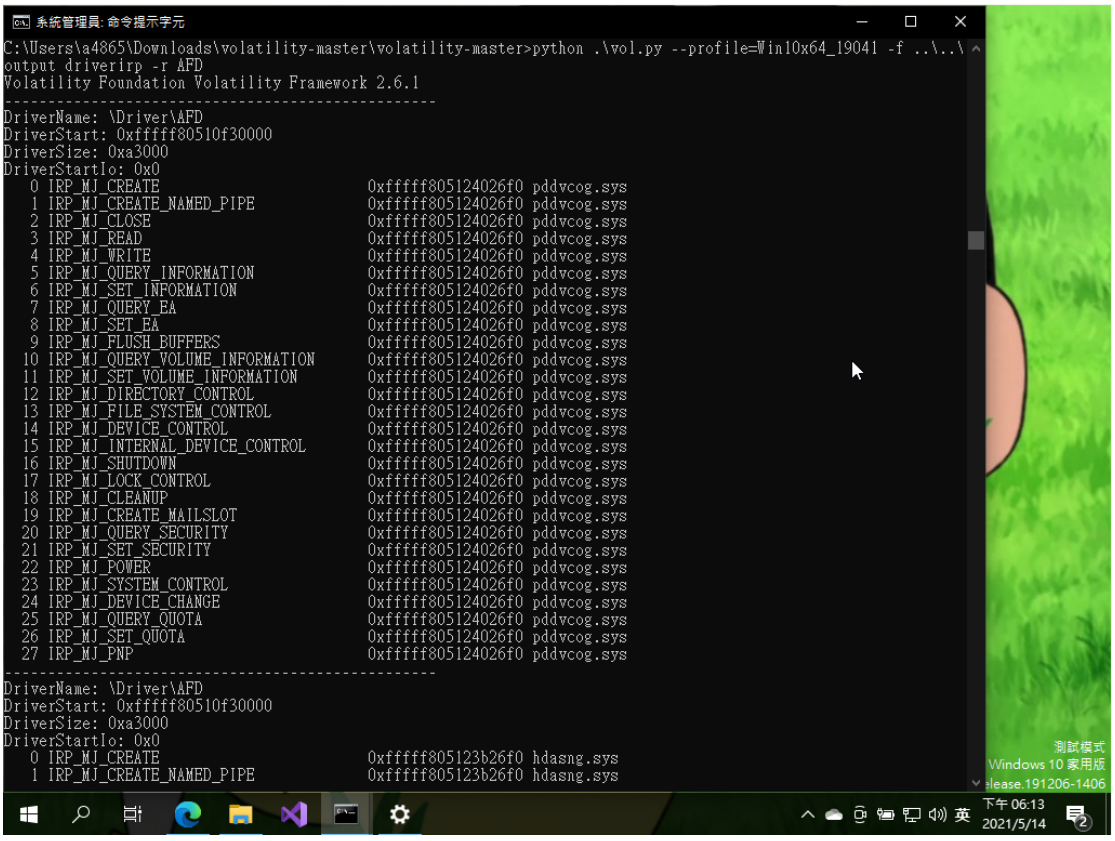


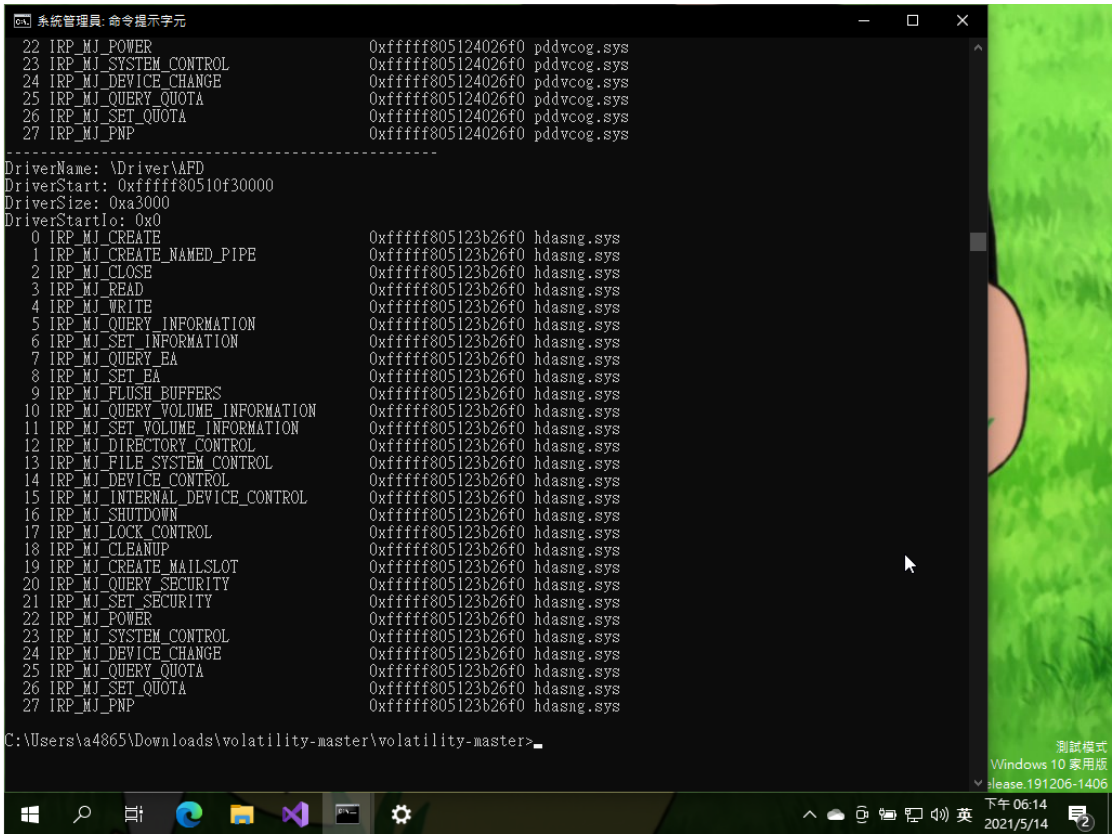
Question2

1)

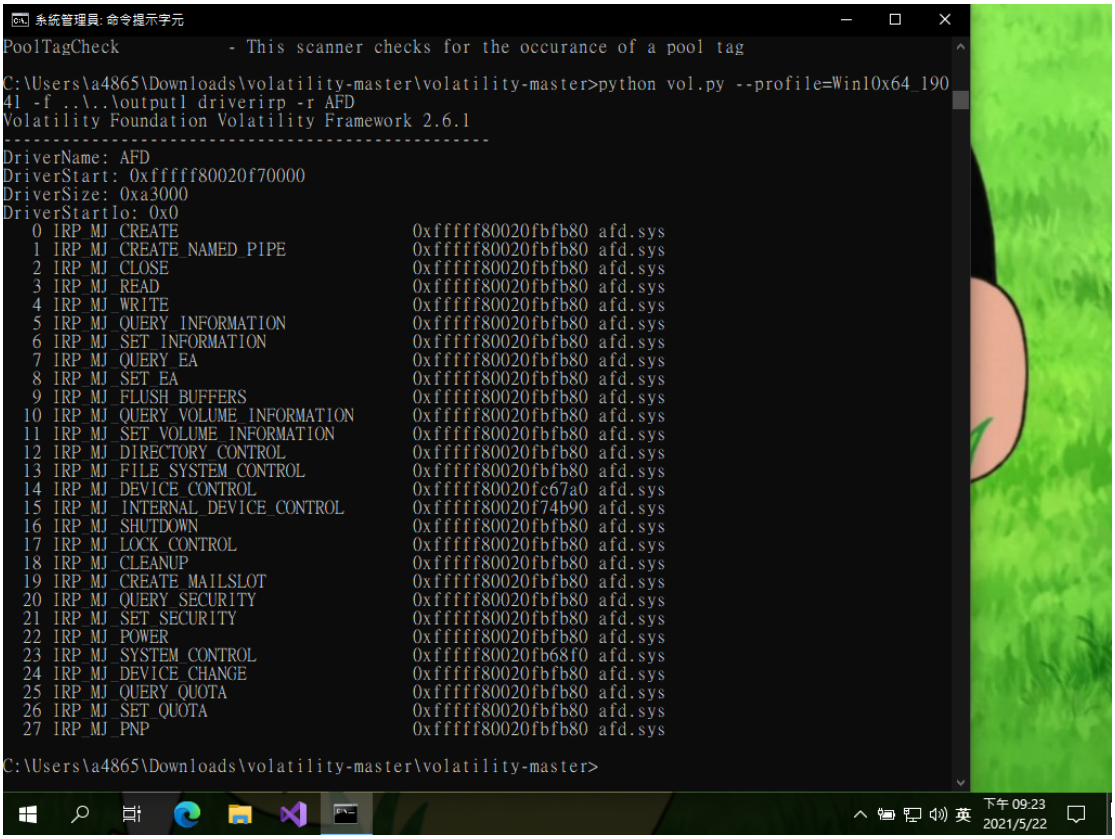
Interrupt Request Packets (IRPs) are essentially just an instruction for the driver. These packets allow the driver to act on the specific major function by providing the relevant information required by the function.

2)




系統管理員: 命令提示字元
22 IRP_MJ_POWER 0xfffff805124026f0 pddvcog.sys
23 IRP_MJ_SYSTEM_CONTROL 0xfffff805124026f0 pddvcog.sys
24 IRP_MJ_DEVICE_CHANGE 0xfffff805124026f0 pddvcog.sys
25 IRP_MJ_QUERY_QUOTA 0xfffff805124026f0 pddvcog.sys
26 IRP_MJ_SET_QUOTA 0xfffff805124026f0 pddvcog.sys
27 IRP_MJ_PNP 0xfffff805124026f0 pddvcog.sys
DriverName: \Driver\AFD
DriverStart: 0xfffff80510f30000
DriverSize: 0xa3000
DriverStartIo: 0x0
0 IRP_MJ_CREATE 0xfffff805123b26f0 hdasng.sys
1 IRP_MJ_CREATE_NAMED_PIPE 0xfffff805123b26f0 hdasng.sys
2 IRP_MJ_CLOSE 0xfffff805123b26f0 hdasng.sys
3 IRP_MJ_READ 0xfffff805123b26f0 hdasng.sys
4 IRP_MJ_WRITE 0xfffff805123b26f0 hdasng.sys
5 IRP_MJ_QUERY_INFORMATION 0xfffff805123b26f0 hdasng.sys
6 IRP_MJ_SET_INFORMATION 0xfffff805123b26f0 hdasng.sys
7 IRP_MJ_QUERY_EA 0xfffff805123b26f0 hdasng.sys
8 IRP_MJ_SET_EA 0xfffff805123b26f0 hdasng.sys
9 IRP_MJ_FLUSH_BUFFERS 0xfffff805123b26f0 hdasng.sys
10 IRP_MJ_QUERY_VOLUME_INFORMATION 0xfffff805123b26f0 hdasng.sys
11 IRP_MJ_SET_VOLUME_INFORMATION 0xfffff805123b26f0 hdasng.sys
12 IRP_MJ_DIRECTORY_CONTROL 0xfffff805123b26f0 hdasng.sys
13 IRP_MJ_FILE_SYSTEM_CONTROL 0xfffff805123b26f0 hdasng.sys
14 IRP_MJ_DEVICE_CONTROL 0xfffff805123b26f0 hdasng.sys
15 IRP_MJ_INTERNAL_DEVICE_CONTROL 0xfffff805123b26f0 hdasng.sys
16 IRP_MJ_SHUTDOWN 0xfffff805123b26f0 hdasng.sys
17 IRP_MJ_LOCK_CONTROL 0xfffff805123b26f0 hdasng.sys
18 IRP_MJ_CLEANUP 0xfffff805123b26f0 hdasng.sys
19 IRP_MJ_CREATE_MAILSLOT 0xfffff805123b26f0 hdasng.sys
20 IRP_MJ_QUERY_SECURITY 0xfffff805123b26f0 hdasng.sys
21 IRP_MJ_SET_SECURITY 0xfffff805123b26f0 hdasng.sys
22 IRP_MJ_POWER 0xfffff805123b26f0 hdasng.sys
23 IRP_MJ_SYSTEM_CONTROL 0xfffff805123b26f0 hdasng.sys
24 IRP_MJ_DEVICE_CHANGE 0xfffff805123b26f0 hdasng.sys
25 IRP_MJ_QUERY_QUOTA 0xfffff805123b26f0 hdasng.sys
26 IRP_MJ_SET_QUOTA 0xfffff805123b26f0 hdasng.sys
27 IRP_MJ_PNP 0xfffff805123b26f0 hdasng.sys
C:\Users\a4865\Downloads\volatility-master\volatility-master>
測試模式
Windows 10 家用版
下午 06:14
2021/5/14

3)


系統管理員: 命令提示字元
PoolTagCheck - This scanner checks for the occurance of a pool tag
C:\Users\a4865\Downloads\volatility-master\volatility-master>python vol.py --profile=Win10x64_190
41 -f ..\..\output1 driverirp -r AFD
Volatility Foundation Volatility Framework 2.6.1
DriverName: AFD
DriverStart: 0xfffff80020f70000
DriverSize: 0xa3000
DriverStartIo: 0x0
0 IRP_MJ_CREATE 0xfffff80020fbfb80 afd.sys
1 IRP_MJ_CREATE_NAMED_PIPE 0xfffff80020fbfb80 afd.sys
2 IRP_MJ_CLOSE 0xfffff80020fbfb80 afd.sys
3 IRP_MJ_READ 0xfffff80020fbfb80 afd.sys
4 IRP_MJ_WRITE 0xfffff80020fbfb80 afd.sys
5 IRP_MJ_QUERY_INFORMATION 0xfffff80020fbfb80 afd.sys
6 IRP_MJ_SET_INFORMATION 0xfffff80020fbfb80 afd.sys
7 IRP_MJ_QUERY_EA 0xfffff80020fbfb80 afd.sys
8 IRP_MJ_SET_EA 0xfffff80020fbfb80 afd.sys
9 IRP_MJ_FLUSH_BUFFERS 0xfffff80020fbfb80 afd.sys
10 IRP_MJ_QUERY_VOLUME_INFORMATION 0xfffff80020fbfb80 afd.sys
11 IRP_MJ_SET_VOLUME_INFORMATION 0xfffff80020fbfb80 afd.sys
12 IRP_MJ_DIRECTORY_CONTROL 0xfffff80020fbfb80 afd.sys
13 IRP_MJ_FILE_SYSTEM_CONTROL 0xfffff80020fbfb80 afd.sys
14 IRP_MJ_DEVICE_CONTROL 0xfffff80020fc67a0 afd.sys
15 IRP_MJ_INTERNAL_DEVICE_CONTROL 0xfffff80020f74b90 afd.sys
16 IRP_MJ_SHUTDOWN 0xfffff80020fbfb80 afd.sys
17 IRP_MJ_LOCK_CONTROL 0xfffff80020fbfb80 afd.sys
18 IRP_MJ_CLEANUP 0xfffff80020fbfb80 afd.sys
19 IRP_MJ_CREATE_MAILSLOT 0xfffff80020fbfb80 afd.sys
20 IRP_MJ_QUERY_SECURITY 0xfffff80020fbfb80 afd.sys
21 IRP_MJ_SET_SECURITY 0xfffff80020fbfb80 afd.sys
22 IRP_MJ_POWER 0xfffff80020fbfb80 afd.sys
23 IRP_MJ_SYSTEM_CONTROL 0xfffff80020fb68f0 afd.sys
24 IRP_MJ_DEVICE_CHANGE 0xfffff80020fbfb80 afd.sys
25 IRP_MJ_QUERY_QUOTA 0xfffff80020fbfb80 afd.sys
26 IRP_MJ_SET_QUOTA 0xfffff80020fbfb80 afd.sys
27 IRP_MJ_PNP 0xfffff80020fbfb80 afd.sys
C:\Users\a4865\Downloads\volatility-master\volatility-master>
下午 09:23
2021/5/22