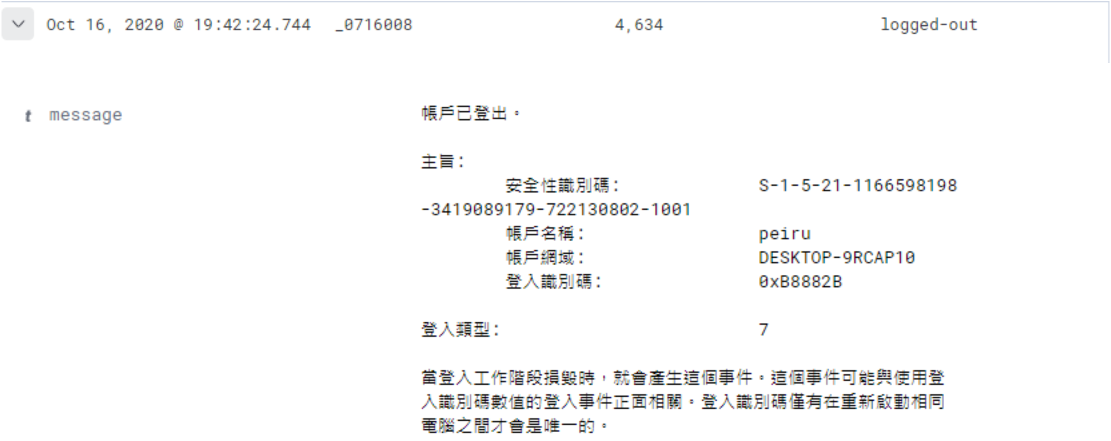
Network Security HW1

- Part A
  - Log Off (b)
    - Image

      Windows security log 4634: log off



```
Oct 16, 2020 @ 19:42:24.744   _0716008        4,634        logged-out

message     帳戶已登出。

            主旨:
                    安全性識別碼:          S-1-5-21-1166598198
            -3419089179-722130802-1001
                    帳戶名稱:              peiru
                    帳戶網域:              DESKTOP-9RCAP10
                    登入識別碼:            0xB8882B

            登入類型:                      7

            當登入工作階段損毀時，就會產生這個事件。這個事件可能與使用登
            入識別碼數值的登入事件正面相關。登入識別碼僅有在重新啟動相同
            電腦之間才會是唯一的。
```

✧Field chosen: event.action, message

✧Reason: It directly shows that I log out from windows 10

- Method

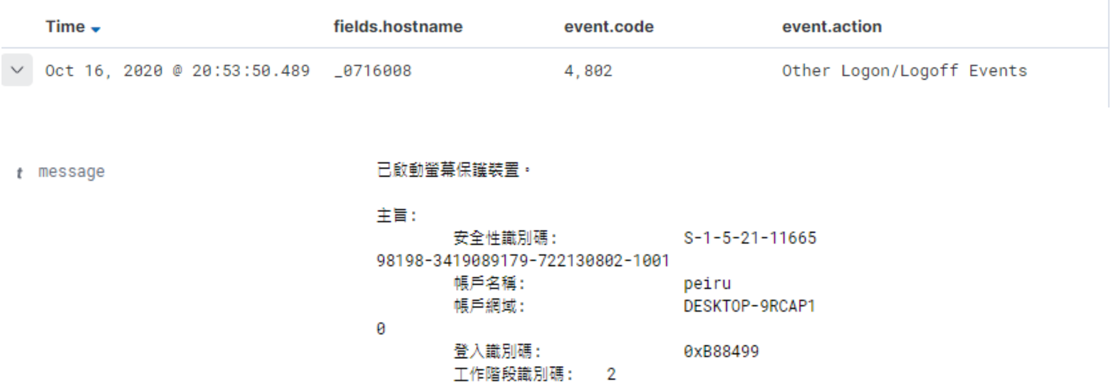
  ✧Lock my win10 (log out will cause the losing of current computer status)

  ✧Log in the computer

  ✧The log appears on kibana

- Screensaver Invoke (c)
  - Image

    Windows Security log 4802: screensaver invoked



```
Time                           fields.hostname   event.code   event.action
Oct 16, 2020 @ 20:53:50.489    _0716008          4,802        Other Logon/Logoff Events

message     已啟動螢幕保護裝置。

            主旨:
                    安全性識別碼:          S-1-5-21-11665
            98198-3419089179-722130802-1001
                    帳戶名稱:              peiru
                    帳戶網域:              DESKTOP-9RCAP1
            0
                    登入識別碼:            0xB88499
                    工作階段識別碼:    2
```

✧Field chosen: message

✧Reason: It shows that I invoke the screensaver

- Method

  ✧Open gpedit.msc

✧Allow auditing succeed/failure of logon event

✧Since triggering the screensaver belongs to ‘other logon/logoff event’, it is not in the default setting of logon event. Thus, we need to allow it in ‘Advance auditing policy’

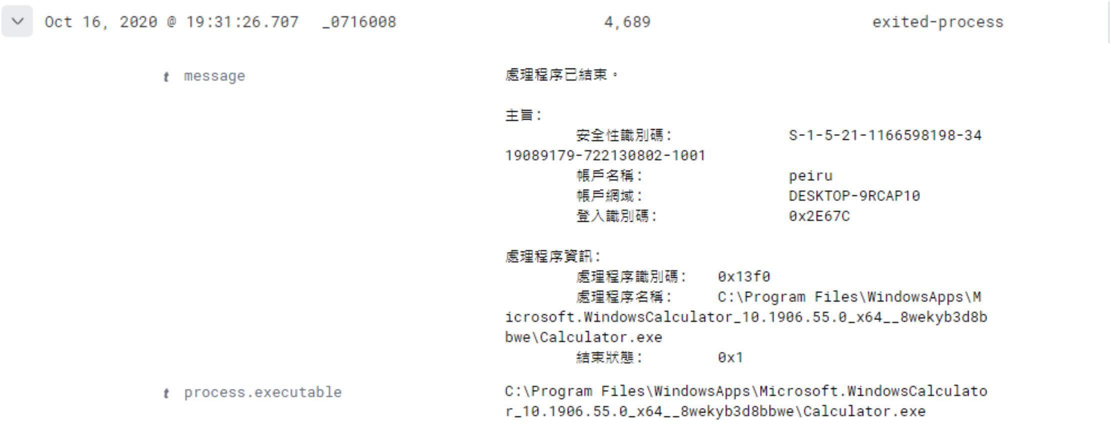
✧Idle my computer to invoke screensaver

✧The log finally appears on kibana

■ Close calculator.exe (f)

◆ Image

Windows security log 4689: process terminate



```
Oct 16, 2020 @ 19:31:26.707   _0716008                4,689                 exited-process

        t  message                  處理程序已結束。

                                    主旨:
                                            安全性識別碼:           S-1-5-21-1166598198-34
                                    19089179-722130802-1001
                                            帳戶名稱:               peiru
                                            帳戶網域:               DESKTOP-9RCAP10
                                            登入識別碼:             0x2E67C

                                    處理程序資訊:
                                            處理程序識別碼:    0x13f0
                                            處理程序名稱:      C:\Program Files\WindowsApps\M
                                    icrosoft.WindowsCalculator_10.1906.55.0_x64__8wekyb3d8b
                                    bwe\Calculator.exe
                                            結束狀態:          0x1
        t  process.executable       C:\Program Files\WindowsApps\Microsoft.WindowsCalculato
                                    r_10.1906.55.0_x64__8wekyb3d8bbwe\Calculator.exe
```

✧Field chosen: event.action, message, process.executable

✧Reason: It shows that I terminate a process (event.action), and the process is indeed calculator.exe (message, process.executable)

◆ Method

✧Open gpedit.msc

✧Allow auditing succeed/failure of process tracking

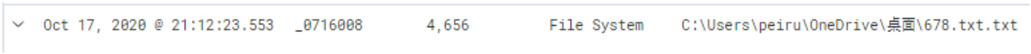
✧Open then close calculator.exe

✧The log appears on kibana

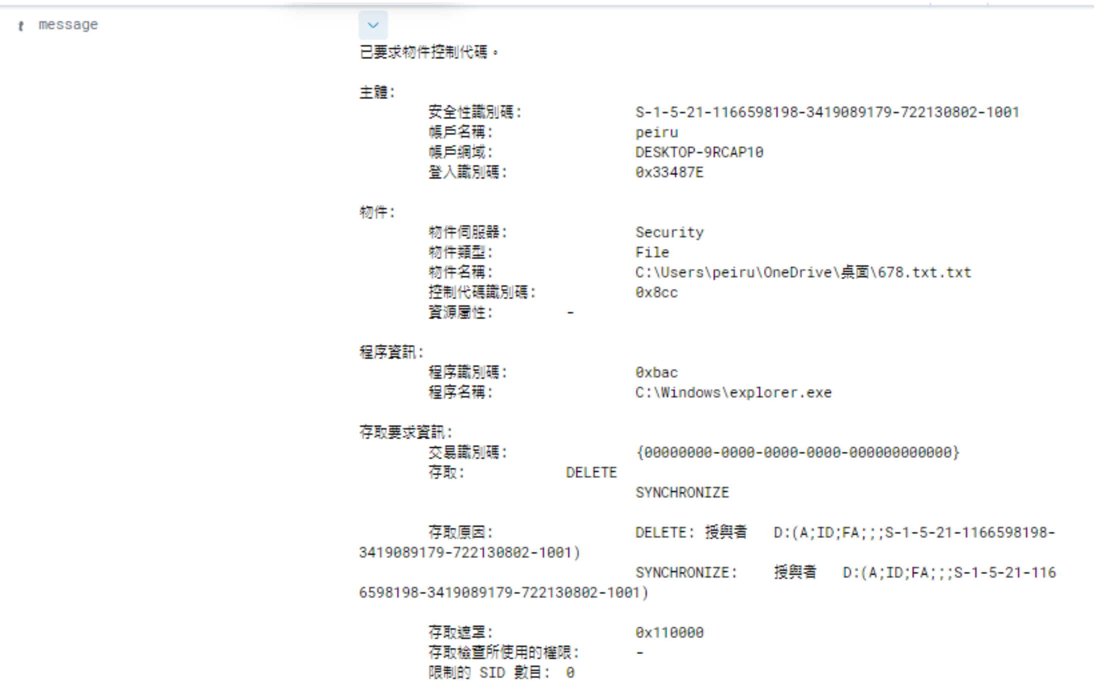
■ Change file name (h)

◆ Image

✧ Windows security log 4656: A handle to an object was requested



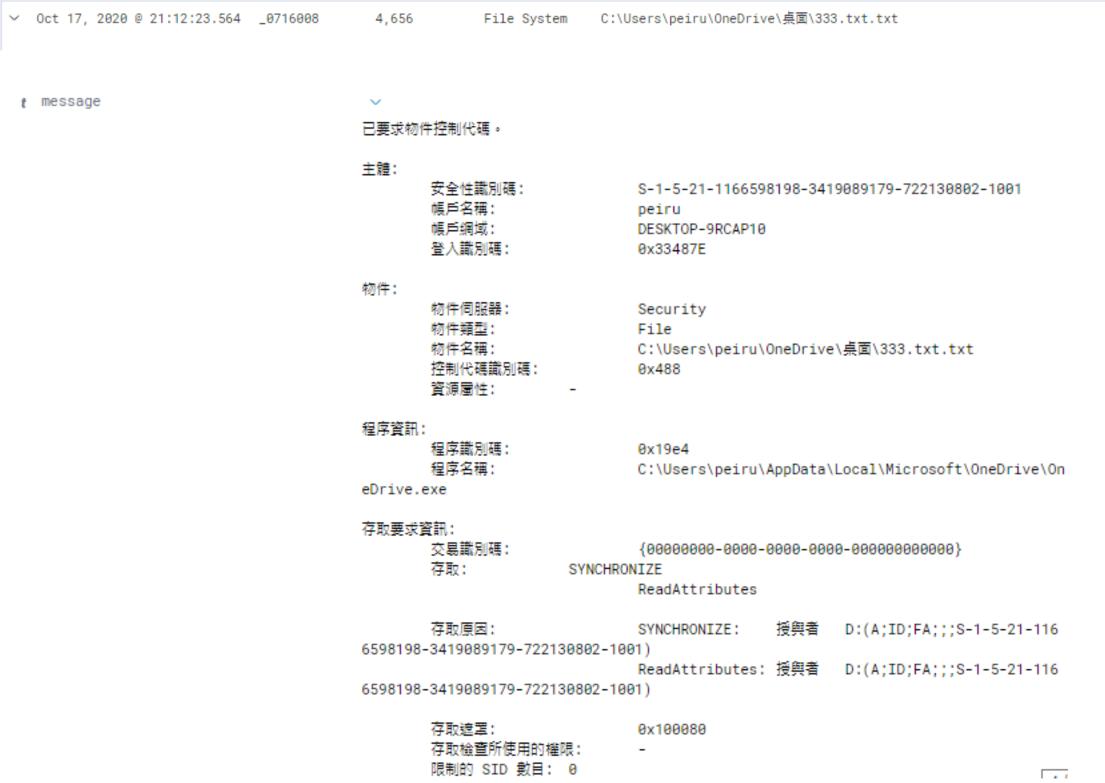
```
Oct 17, 2020 @ 21:12:23.553   _0716008      4,656        File System     C:\Users\peiru\OneDrive\桌面\678.txt.txt
```



```
t  message
                        已要求物件控制代碼。

                        主體:
                                安全性識別碼:           S-1-5-21-1166598198-3419089179-722130802-1001
                                帳戶名稱:               peiru
                                帳戶網域:               DESKTOP-9RCAP10
                                登入識別碼:             0x33487E

                        物件:
                                物件伺服器:             Security
                                物件類型:               File
                                物件名稱:               C:\Users\peiru\OneDrive\桌面\678.txt.txt
                                控制代碼識別碼:         0x8cc
                                資源屬性:       -

                        程序資訊:
                                程序識別碼:             0xbac
                                程序名稱:               C:\Windows\explorer.exe

                        存取要求資訊:
                                交易識別碼:             {00000000-0000-0000-0000-000000000000}
                                存取:           DELETE
                                                        SYNCHRONIZE

                                存取原因:               DELETE: 授與者   D:(A;ID;FA;;;S-1-5-21-1166598198-
                        3419089179-722130802-1001)
                                                        SYNCHRONIZE:    授與者   D:(A;ID;FA;;;S-1-5-21-116
                        6598198-3419089179-722130802-1001)

                                存取遮罩:               0x110000
                                存取檢查所使用的權限:   -
                                限制的 SID 數目:  0
```

*It shows that file 678.txt.txt has been changed (存取原因:delete)

*HandleID of 678.txt.txt is 0x8cc

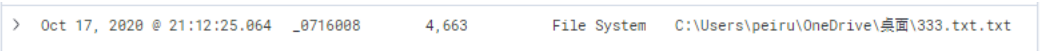


```
﹀  Oct 17, 2020 @ 21:12:23.564   _0716008        4,656        File System    C:\Users\peiru\OneDrive\桌面\333.txt.txt


t  message
                        已要求物件控制代碼。

                        主體:
                                安全性識別碼:           S-1-5-21-1166598198-3419089179-722130802-1001
                                帳戶名稱:               peiru
                                帳戶網域:               DESKTOP-9RCAP10
                                登入識別碼:             0x33487E

                        物件:
                                物件伺服器:             Security
                                物件類型:               File
                                物件名稱:               C:\Users\peiru\OneDrive\桌面\333.txt.txt
                                控制代碼識別碼:         0x488
                                資源屬性:       -

                        程序資訊:
                                程序識別碼:             0x19e4
                                程序名稱:               C:\Users\peiru\AppData\Local\Microsoft\OneDrive\On
                        eDrive.exe

                        存取要求資訊:
                                交易識別碼:             {00000000-0000-0000-0000-000000000000}
                                存取:           SYNCHRONIZE
                                                        ReadAttributes

                                存取原因:               SYNCHRONIZE:    授與者   D:(A;ID;FA;;;S-1-5-21-116
                        6598198-3419089179-722130802-1001)
                                                        ReadAttributes: 授與者   D:(A;ID;FA;;;S-1-5-21-116
                        6598198-3419089179-722130802-1001)

                                存取遮罩:               0x100080
                                存取檢查所使用的權限:   -
                                限制的 SID 數目:  0
```

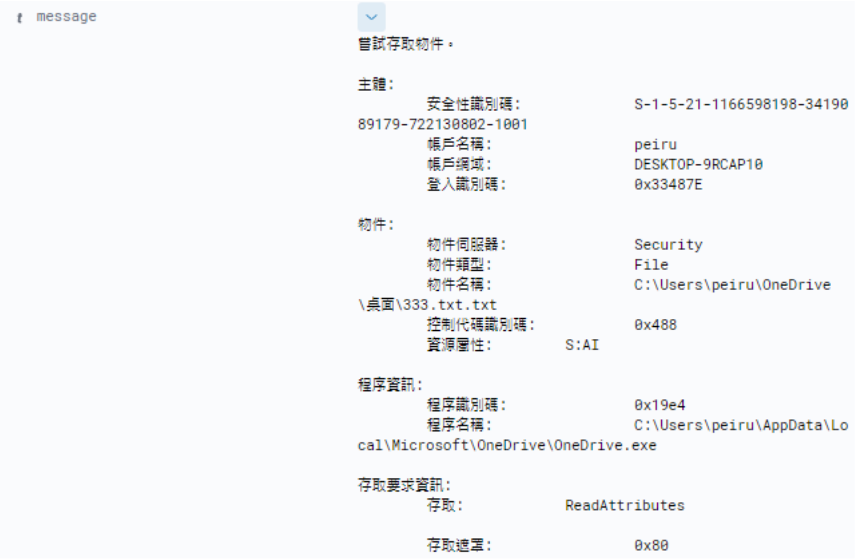
*It shows that file 333.txt.txt has been synchronized with 678.txt.txt

*HandleID of 333.txt.txt is 0x488

✧ Windows security log 4663: An attempt was made to access an object

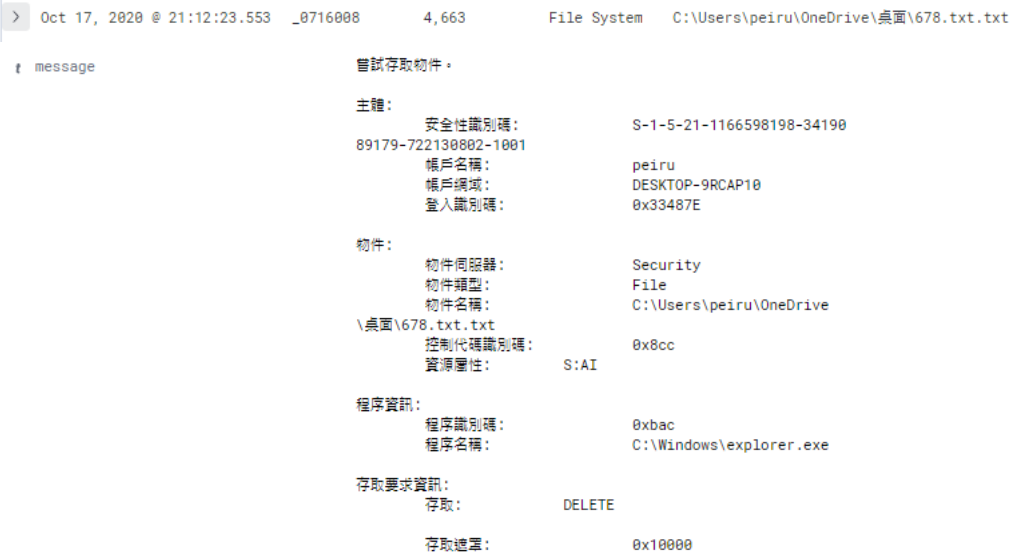


```
>  Oct 17, 2020 @ 21:12:25.064   _0716008        4,663        File System    C:\Users\peiru\OneDrive\桌面\333.txt.txt
```



```
t message          嘗試存取物件。

                   主體:
                           安全性識別碼:              S-1-5-21-1166598198-34190
                   89179-722130802-1001
                           帳戶名稱:                  peiru
                           帳戶網域:                  DESKTOP-9RCAP10
                           登入識別碼:                0x33487E

                   物件:
                           物件伺服器:                Security
                           物件類型:                  File
                           物件名稱:                  C:\Users\peiru\OneDrive
                   \桌面\333.txt.txt
                           控制代碼識別碼:            0x488
                           資源屬性:          S:AI

                   程序資訊:
                           程序識別碼:                0x19e4
                           程序名稱:                  C:\Users\peiru\AppData\Lo
                   cal\Microsoft\OneDrive\OneDrive.exe

                   存取要求資訊:
                           存取:              ReadAttributes

                           存取遮罩:                  0x80
```

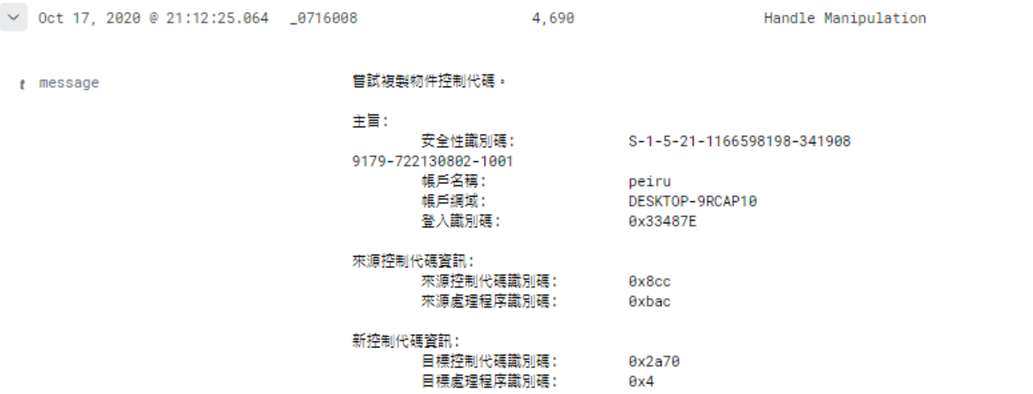
*HandleID of 333.txt.txt is 0x488



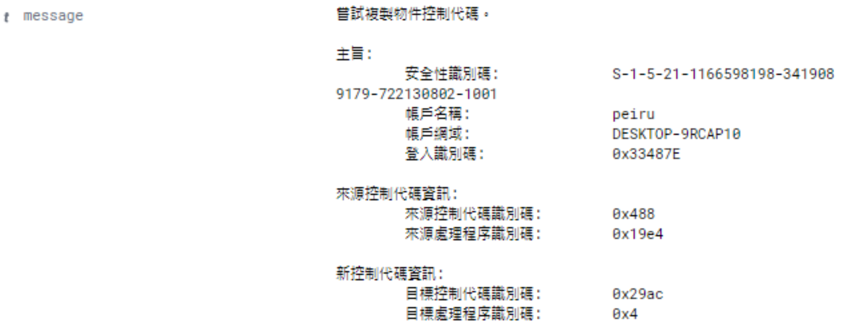
```
>  Oct 17, 2020 @ 21:12:23.553   _0716008      4,663      File System    C:\Users\peiru\OneDrive\桌面\678.txt.txt

t message          嘗試存取物件。

                   主體:
                           安全性識別碼:              S-1-5-21-1166598198-34190
                   89179-722130802-1001
                           帳戶名稱:                  peiru
                           帳戶網域:                  DESKTOP-9RCAP10
                           登入識別碼:                0x33487E

                   物件:
                           物件伺服器:                Security
                           物件類型:                  File
                           物件名稱:                  C:\Users\peiru\OneDrive
                   \桌面\678.txt.txt
                           控制代碼識別碼:            0x8cc
                           資源屬性:          S:AI

                   程序資訊:
                           程序識別碼:                0xbac
                           程序名稱:                  C:\Windows\explorer.exe

                   存取要求資訊:
                           存取:              DELETE

                           存取遮罩:                  0x10000
```

*HandleID of 678.txt.txt is 0x8cc

✧ Windows security log 4690: An attempt was made to duplicate a handle to an object



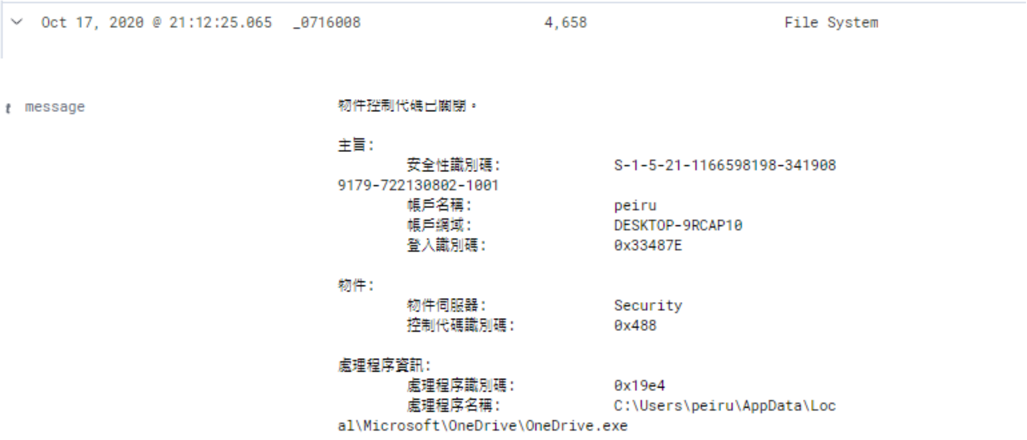
```
v  Oct 17, 2020 @ 21:12:25.064   _0716008            4,690                  Handle Manipulation

t message          嘗試複製物件控制代碼。

                   主旨:
                           安全性識別碼:              S-1-5-21-1166598198-341908
                   9179-722130802-1001
                           帳戶名稱:                  peiru
                           帳戶網域:                  DESKTOP-9RCAP10
                           登入識別碼:                0x33487E

                   來源控制代碼資訊:
                           來源控制代碼識別碼:        0x8cc
                           來源處理程序識別碼:        0xbac

                   新控制代碼資訊:
                           目標控制代碼識別碼:        0x2a70
                           目標處理程序識別碼:        0x4
```



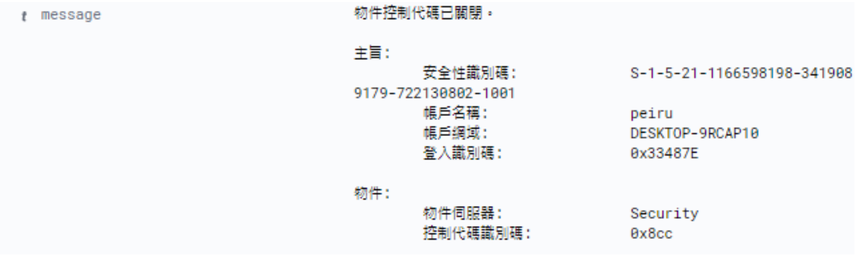
```
t message                    嘗試複製物件控制代碼。

                             主旨:
                                     安全性識別碼:          S-1-5-21-1166598198-341908
                             9179-722130802-1001
                                     帳戶名稱:              peiru
                                     帳戶網域:              DESKTOP-9RCAP10
                                     登入識別碼:            0x33487E

                             來源控制代碼資訊:
                                     來源控制代碼識別碼:    0x488
                                     來源處理程序識別碼:    0x19e4

                             新控制代碼資訊:
                                     目標控制代碼識別碼:    0x29ac
                                     目標處理程序識別碼:    0x4
```

*It shows that the file tries to handle the manipulation from 678.txt.txt to 333.txt.txt

✧Windows security log 4658: The handle to an object was closed



```
⌄ Oct 17, 2020 @ 21:12:25.065  _0716008              4,658                  File System

t message                    物件控制代碼已關閉。

                             主旨:
                                     安全性識別碼:          S-1-5-21-1166598198-341908
                             9179-722130802-1001
                                     帳戶名稱:              peiru
                                     帳戶網域:              DESKTOP-9RCAP10
                                     登入識別碼:            0x33487E

                             物件:
                                     物件伺服器:            Security
                                     控制代碼識別碼:        0x488

                             處理程序資訊:
                                     處理程序識別碼:        0x19e4
                                     處理程序名稱:          C:\Users\peiru\AppData\Loc
                             al\Microsoft\OneDrive\OneDrive.exe
```



```
t message                    物件控制代碼已關閉。

                             主旨:
                                     安全性識別碼:          S-1-5-21-1166598198-341908
                             9179-722130802-1001
                                     帳戶名稱:              peiru
                                     帳戶網域:              DESKTOP-9RCAP10
                                     登入識別碼:            0x33487E

                             物件:
                                     物件伺服器:            Security
                                     控制代碼識別碼:        0x8cc
```

✧Log order: 4656->4663->4690->4658

✧Field chosen: message, winlog.event_data.ObjectName

✧Reason: The ObjectName field indicates which object(file) I access, and the message shows what operation I have done on the object(file)

◆ Method

✧Open gpedit.msc

✧Allow auditing succeed/failure of object access

✧Create a file 678.txt.txt

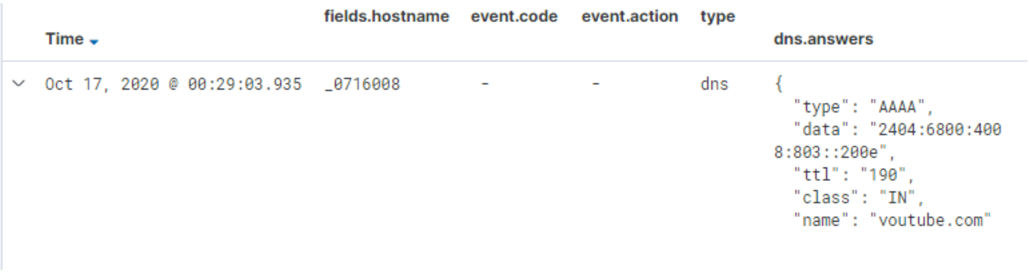
✧Allow auditing all the changes on the file 678.txt.txt

✧Change the file name from 678.txt.txt to 333.txt.txt

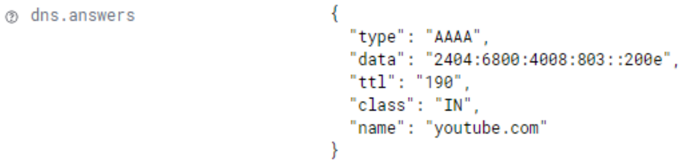
✧The log appears on kibana

- DNS query (i)
  - Image

    Packetbeat: no event code



```
                                  fields.hostname  event.code  event.action  type
  Time ▾                                                                           dns.answers
﹀ Oct 17, 2020 @ 00:29:03.935   _0716008              -            -          dns     {
                                                                                   "type": "AAAA",
                                                                                   "data": "2404:6800:400
                                                                                 8:803::200e",
                                                                                   "ttl": "190",
                                                                                   "class": "IN",
                                                                                   "name": "youtube.com"
```



```
⑦ dns.answers                       {
                                      "type": "AAAA",
                                      "data": "2404:6800:4008:803::200e",
                                      "ttl": "190",
                                      "class": "IN",
                                      "name": "youtube.com"
                                    }
```

✧Fields chosen: type, dns.answer

✧Reason: It shows that I use the command dnslookup(type) to visit youtube.com(dns.answer)

  - Method

✧Type ‘nslookup youtube.com’ on cmd

✧Go to kibana and search ‘youtube.com’

✧The log appears

- Part B

I began to write this homework two weeks before the deadline, however, I spent about one week trying to fix my hardware problems. At first, I wrote my homework on my laptop but the RAM of my laptop is 8G. It’s insufficient to support two VM machines and my local host. Thus, my laptop will shutdown automatically while I’m doing my homework. To solve this problem, I borrow a laptop from my mother and add more RAM to the laptop. Since the laptop hasn’t been used for a long time, the hard disk of the laptop has some problem. So, I spent another two days trying to fix the problem.

After I solved my hardware problems, I faced other problems. The amount of log appears on my computer is very small. It seems that I have to shutdown the docker completely to let more logs appear.

I found the log “log-off” as long as I connected to kibana successfully. However, I found out that finding other logs are more challenging. It’s necessary to change gpedit.msc file to see the log on the event viewer. The problem I encounter is that the version of my windows10 VM is home, gpedit.msc file is not in my windows/system32 folder. I tried to run gpedit.dll to acquire gpedit.msc but in vain. So, I create a new windows10 VM with version pro. And I eventually saw the gpedit.msc file!