Reaper,papc、evtx(gigasheet)

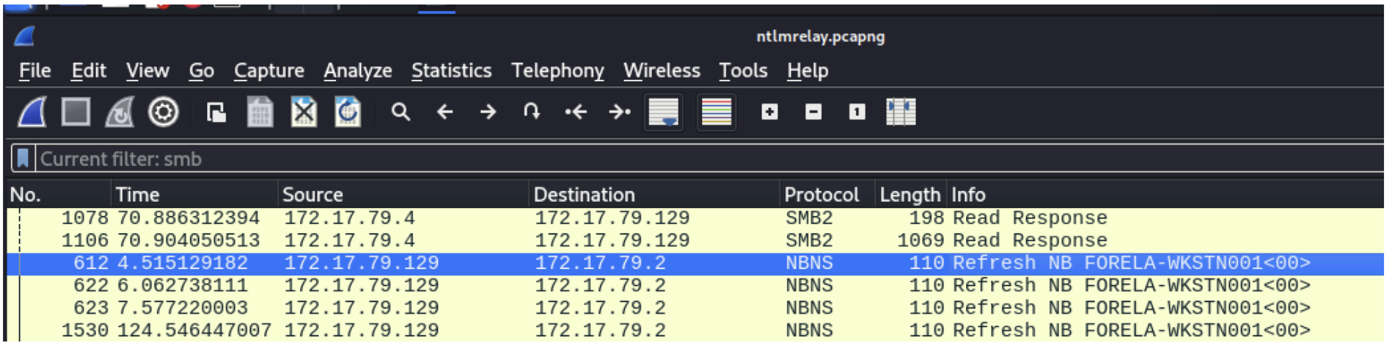
```
Sherlock Scenario
Our SIEM alerted us to a suspicious logon event which needs to be looked at
immediately . The alert details were that the IP Address and the Source
Workstation name were a mismatch .You are provided a network capture and
event logs from the surrounding time around the incident timeframe. Corelate
the given evidence and report back to your SOC Manager.
* * *
About Reaper
Reaper is a very easy Sherlock which covers NTLM relay attacks , comprised
of AD Forensics, MITM Attack detection & network forensics. In this sherlock
players will analyze network traffic and window event logs to find evidence
of NTLM relay attack which are common in active directory environments.
```

文件：ntlmrelay.pcapng、Security.evtx
使用工具：https://app.gigasheet.com/

慘了，他們的`evtx`好像有問題，時間點與封包完全差2個月...
使用先前的EvtxECmd＋Timeline Explorer也一樣...
能做就做吧...

Task 1

What is the IP Address for Forela-Wkstn001?



Current filter: smb

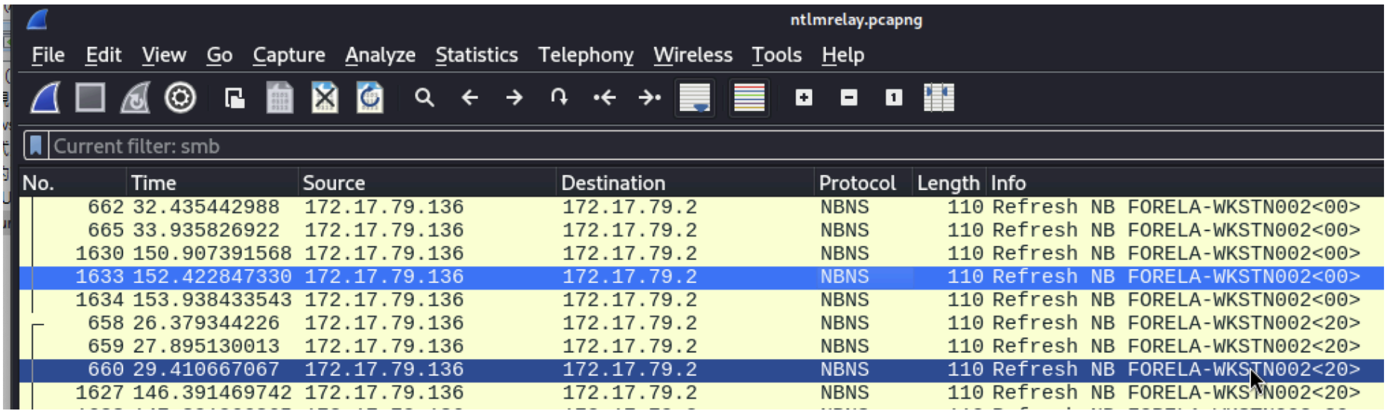
```
No.  Time           Source         Destination    Protocol Length Info
1078 70.886312394   172.17.79.4    172.17.79.129  SMB2      198 Read Response
1106 70.904050513   172.17.79.4    172.17.79.129  SMB2     1069 Read Response
 612 4.515129182    172.17.79.129  172.17.79.2    NBNS      110 Refresh NB FORELA-WKSTN001<00>
 622 6.062738111    172.17.79.129  172.17.79.2    NBNS      110 Refresh NB FORELA-WKSTN001<00>
 623 7.577220003    172.17.79.129  172.17.79.2    NBNS      110 Refresh NB FORELA-WKSTN001<00>
1530 124.546447007  172.17.79.129  172.17.79.2    NBNS      110 Refresh NB FORELA-WKSTN001<00>
```

`172.17.79.129`

Task 2

What is the IP Address for Forela-Wkstn002?

同上


ntlmrelay.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Current filter: smb

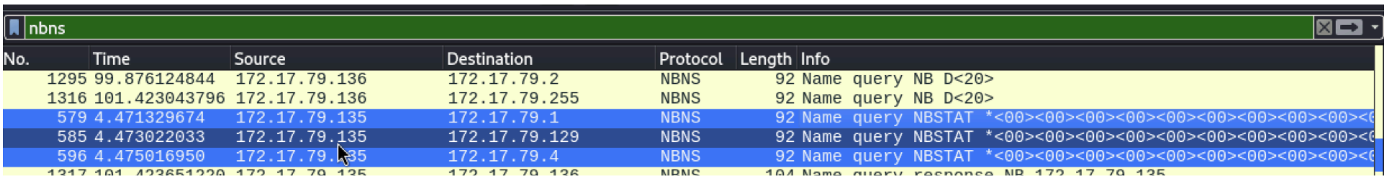
```
No.   Time          Source         Destination   Protocol Length Info
  662 32.435442988  172.17.79.136  172.17.79.2   NBNS        110 Refresh NB FORELA-WKSTN002<00>
  665 33.935826922  172.17.79.136  172.17.79.2   NBNS        110 Refresh NB FORELA-WKSTN002<00>
 1630 150.907391568 172.17.79.136  172.17.79.2   NBNS        110 Refresh NB FORELA-WKSTN002<00>
 1633 152.422847330 172.17.79.136  172.17.79.2   NBNS        110 Refresh NB FORELA-WKSTN002<00>
 1634 153.938433543 172.17.79.136  172.17.79.2   NBNS        110 Refresh NB FORELA-WKSTN002<00>
  658 26.379344226  172.17.79.136  172.17.79.2   NBNS        110 Refresh NB FORELA-WKSTN002<20>
  659 27.895130013  172.17.79.136  172.17.79.2   NBNS        110 Refresh NB FORELA-WKSTN002<20>
  660 29.410667067  172.17.79.136  172.17.79.2   NBNS        110 Refresh NB FORELA-WKSTN002<20>
 1627 146.391469742 172.17.79.136  172.17.79.2   NBNS        110 Refresh NB FORELA-WKSTN002<20>
```

`172.17.79.136`

Task 3

What is the username of the account whose hash was stolen by attacker?

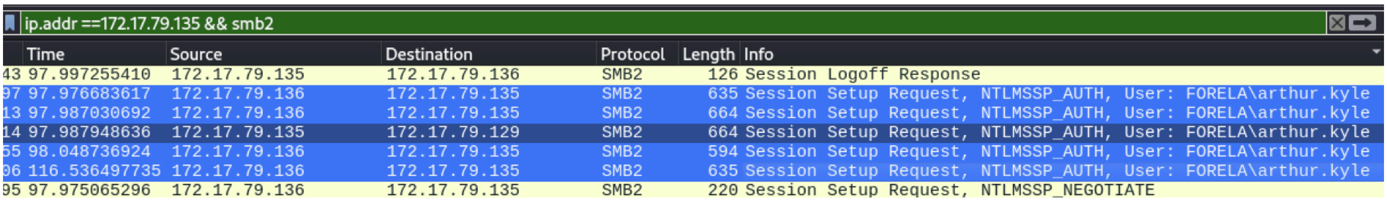
看到尾數135有做請求



nbns

```
No.   Time          Source         Destination     Protocol Length Info
 1295 99.876124844  172.17.79.136  172.17.79.2     NBNS         92 Name query NB D<20>
 1316 101.423043796 172.17.79.136  172.17.79.255   NBNS         92 Name query NB D<20>
  579 4.471329674   172.17.79.135  172.17.79.1     NBNS         92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><0
  585 4.473022033   172.17.79.135  172.17.79.129   NBNS         92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><0
  596 4.475016950   172.17.79.135  172.17.79.4     NBNS         92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><0
 1317 101.423651220 172.17.79.135  172.17.79.136   NBNS        104 Name query response NB 172.17.79.135
```

filter：`ip.addr ==172.17.79.135 && smb2`



ip.addr ==172.17.79.135 && smb2

```
   Time          Source         Destination    Protocol Length Info
43 97.997255410  172.17.79.135  172.17.79.136  SMB2        126 Session Logoff Response
97 97.976683617  172.17.79.136  172.17.79.135  SMB2        635 Session Setup Request, NTLMSSP_AUTH, User: FORELA\arthur.kyle
13 97.987030692  172.17.79.136  172.17.79.135  SMB2        664 Session Setup Request, NTLMSSP_AUTH, User: FORELA\arthur.kyle
14 97.987948636  172.17.79.135  172.17.79.129  SMB2        664 Session Setup Request, NTLMSSP_AUTH, User: FORELA\arthur.kyle
55 98.048736924  172.17.79.136  172.17.79.135  SMB2        594 Session Setup Request, NTLMSSP_AUTH, User: FORELA\arthur.kyle
06 116.536497735 172.17.79.136  172.17.79.135  SMB2        635 Session Setup Request, NTLMSSP_AUTH, User: FORELA\arthur.kyle
95 97.975065296  172.17.79.136  172.17.79.135  SMB2        220 Session Setup Request, NTLMSSP_NEGOTIATE
```

`arthur.kyle`

Task 4

What is the IP Address of Unknown Device used by the attacker to intercept credentials?

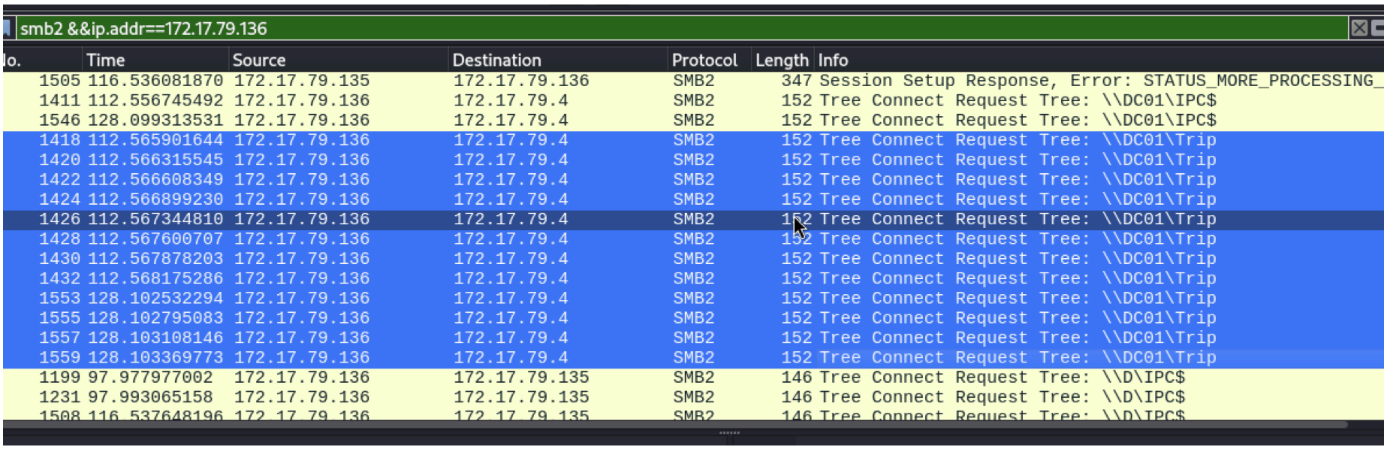
同上

`172.17.79.135`

Task 5

What was the fileshare navigated by the victim user account?

filter：`smb2 &&ip.addr==172.17.79.136`

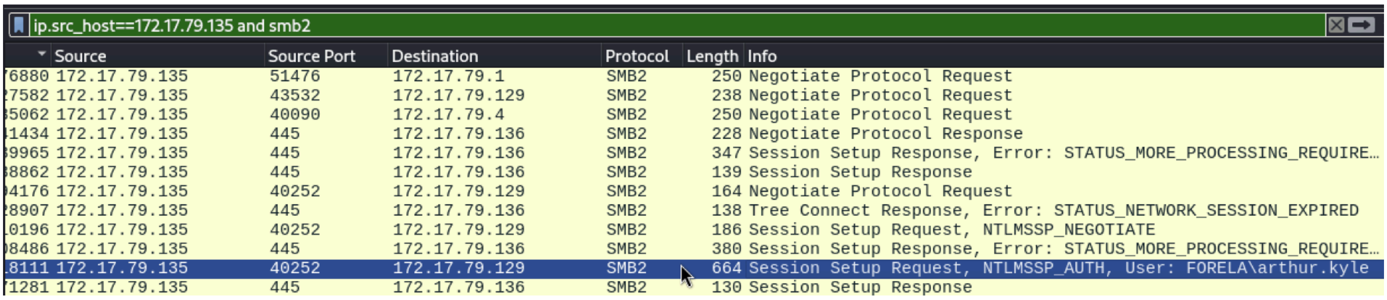


```
smb2 &&ip.addr==172.17.79.136
lo.   Time          Source          Destination     Protocol Length Info
 1505 116.536081870 172.17.79.135   172.17.79.136   SMB2      347 Session Setup Response, Error: STATUS_MORE_PROCESSING_
 1411 112.556745492 172.17.79.136   172.17.79.4     SMB2      152 Tree Connect Request Tree: \\DC01\IPC$
 1546 128.099313531 172.17.79.136   172.17.79.4     SMB2      152 Tree Connect Request Tree: \\DC01\IPC$
 1418 112.565901644 172.17.79.136   172.17.79.4     SMB2      152 Tree Connect Request Tree: \\DC01\Trip
 1420 112.566315545 172.17.79.136   172.17.79.4     SMB2      152 Tree Connect Request Tree: \\DC01\Trip
 1422 112.566608349 172.17.79.136   172.17.79.4     SMB2      152 Tree Connect Request Tree: \\DC01\Trip
 1424 112.566899230 172.17.79.136   172.17.79.4     SMB2      152 Tree Connect Request Tree: \\DC01\Trip
 1426 112.567344810 172.17.79.136   172.17.79.4     SMB2      152 Tree Connect Request Tree: \\DC01\Trip
 1428 112.567600707 172.17.79.136   172.17.79.4     SMB2      152 Tree Connect Request Tree: \\DC01\Trip
 1430 112.567878203 172.17.79.136   172.17.79.4     SMB2      152 Tree Connect Request Tree: \\DC01\Trip
 1432 112.568175286 172.17.79.136   172.17.79.4     SMB2      152 Tree Connect Request Tree: \\DC01\Trip
 1553 128.102532294 172.17.79.136   172.17.79.4     SMB2      152 Tree Connect Request Tree: \\DC01\Trip
 1555 128.102795083 172.17.79.136   172.17.79.4     SMB2      152 Tree Connect Request Tree: \\DC01\Trip
 1557 128.103108146 172.17.79.136   172.17.79.4     SMB2      152 Tree Connect Request Tree: \\DC01\Trip
 1559 128.103369773 172.17.79.136   172.17.79.4     SMB2      152 Tree Connect Request Tree: \\DC01\Trip
 1199 97.977977002  172.17.79.136   172.17.79.135   SMB2      146 Tree Connect Request Tree: \\D\IPC$
 1231 97.993065158  172.17.79.136   172.17.79.135   SMB2      146 Tree Connect Request Tree: \\D\IPC$
 1508 116.537648196 172.17.79.136   172.17.79.135   SMB2      146 Tree Connect Request Tree: \\D\IPC$
```

`\\DC01\Trip`

Task 6

What is the source port used to logon to target workstation using the compromised account?



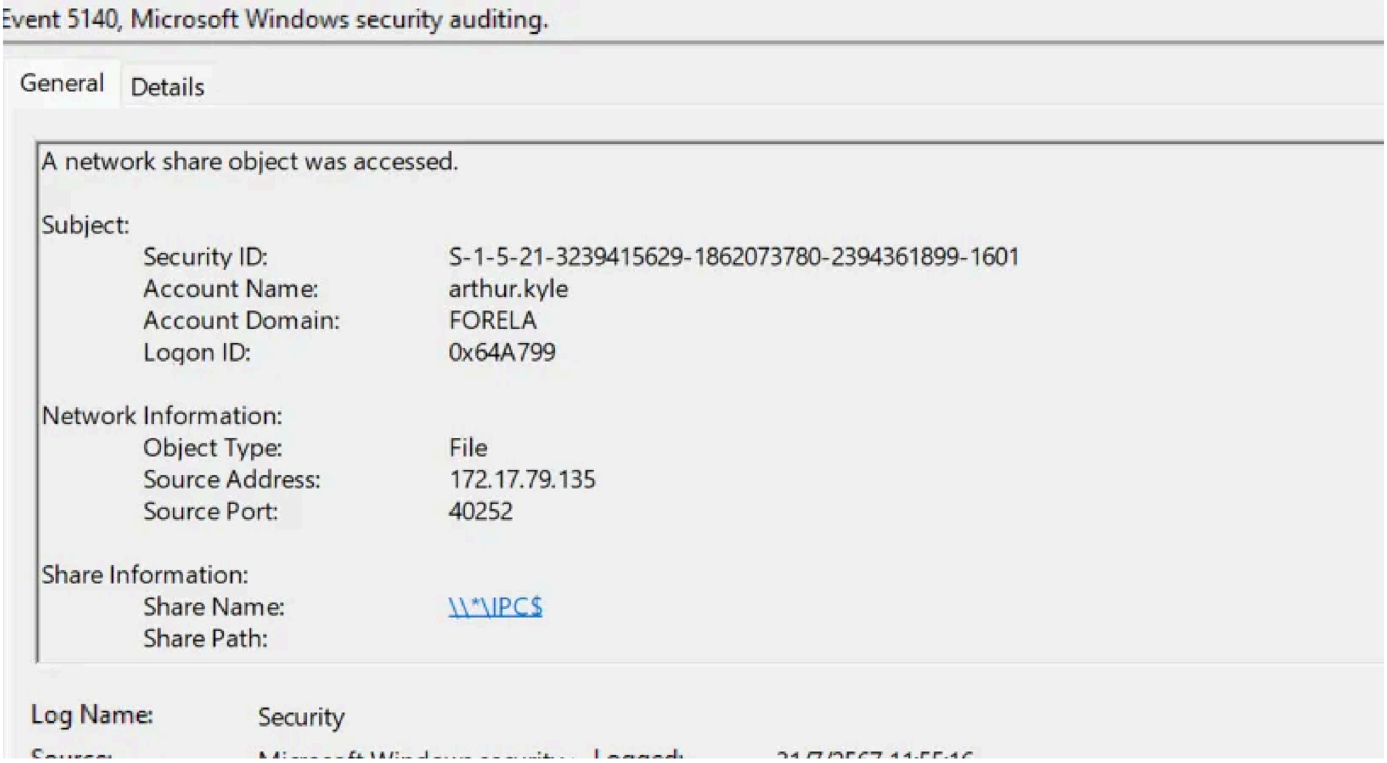
```
ip.src_host==172.17.79.135 and smb2
      Source          Source Port Destination     Protocol Length Info
6880 172.17.79.135   51476       172.17.79.1     SMB2      250 Negotiate Protocol Request
7582 172.17.79.135   43532       172.17.79.129   SMB2      238 Negotiate Protocol Request
5062 172.17.79.135   40090       172.17.79.4     SMB2      250 Negotiate Protocol Request
1434 172.17.79.135   445         172.17.79.136   SMB2      228 Negotiate Protocol Response
9965 172.17.79.135   445         172.17.79.136   SMB2      347 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRE…
8862 172.17.79.135   445         172.17.79.136   SMB2      139 Session Setup Response
4176 172.17.79.135   40252       172.17.79.129   SMB2      164 Negotiate Protocol Request
8907 172.17.79.135   445         172.17.79.136   SMB2      138 Tree Connect Response, Error: STATUS_NETWORK_SESSION_EXPIRED
0196 172.17.79.135   40252       172.17.79.129   SMB2      186 Session Setup Request, NTLMSSP_NEGOTIATE
8486 172.17.79.135   445         172.17.79.136   SMB2      380 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRE…
8111 172.17.79.135   40252       172.17.79.129   SMB2      664 Session Setup Request, NTLMSSP_AUTH, User: FORELA\arthur.kyle
1281 172.17.79.135   445         172.17.79.136   SMB2      130 Session Setup Response
```

`40252`

從這之後封包找不到，只能看別人做的。。。

Task 7

What is the Logon ID for the malicious session?



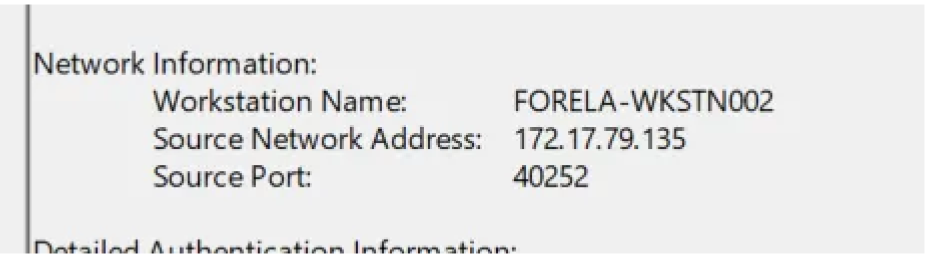
```
Event 5140, Microsoft Windows security auditing.
```

```
A network share object was accessed.

Subject:
        Security ID:            S-1-5-21-3239415629-1862073780-2394361899-1601
        Account Name:           arthur.kyle
        Account Domain:         FORELA
        Logon ID:               0x64A799

Network Information:
        Object Type:            File
        Source Address:         172.17.79.135
        Source Port:            40252

Share Information:
        Share Name:             \\*\IPC$
        Share Path:

Log Name:       Security
```

`0x64A799`

Task 8

The detection was based on the mismatch of hostname and the assigned IP Address.What is the workstation name and the source IP Address from which the malicious logon occur?

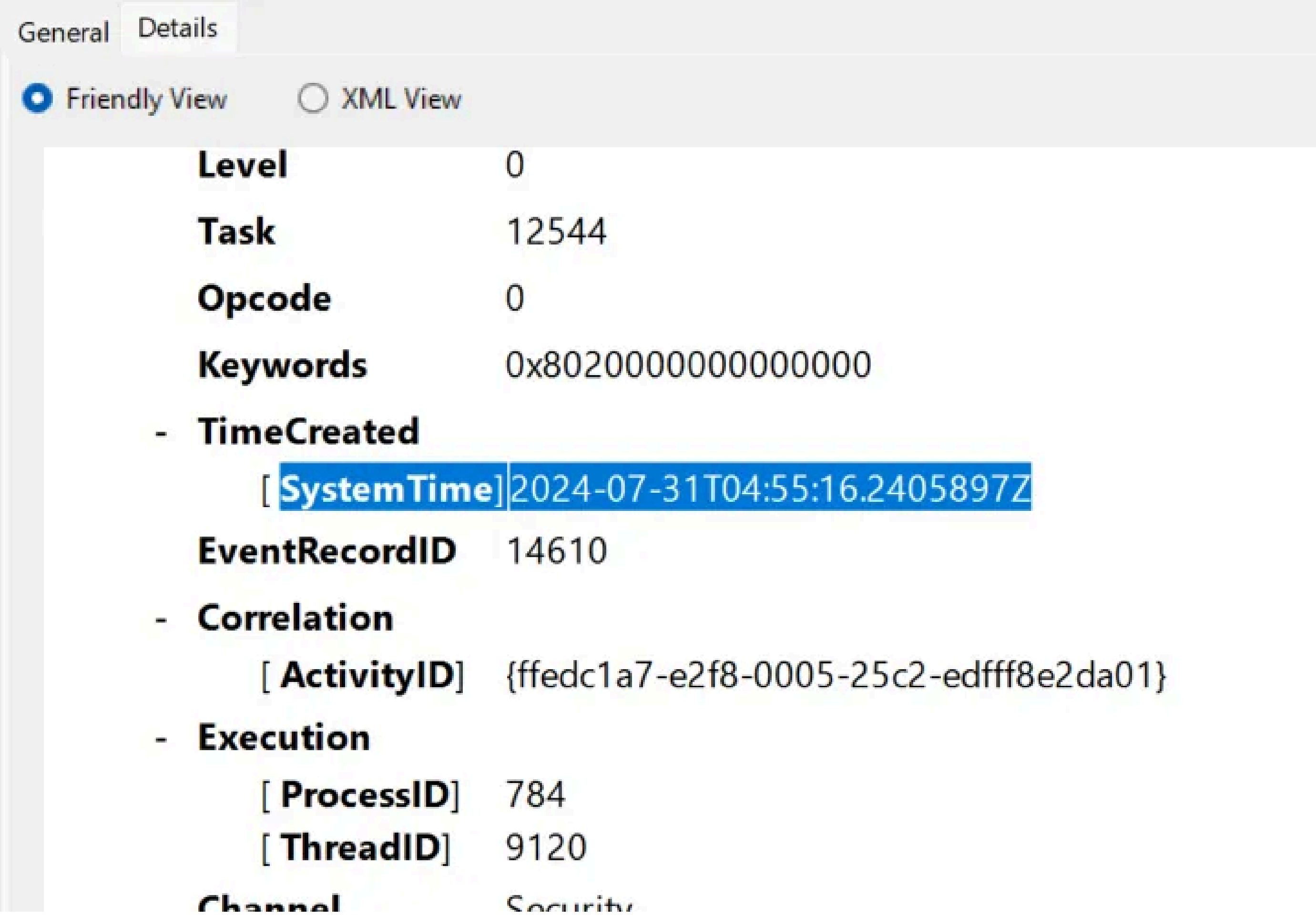


```
Network Information:
        Workstation Name:          FORELA-WKSTN002
        Source Network Address:    172.17.79.135
        Source Port:               40252

Detailed Authentication Information:
```

`FORELA-WKSTN002, 172.17.79.135`

Task 9

At what UTC time did the the malicious logon happen?



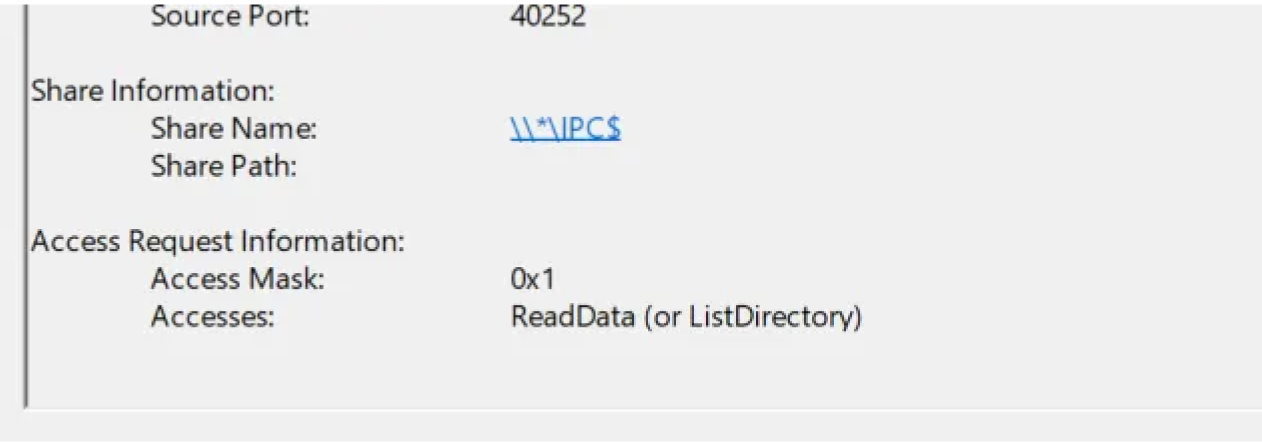
● Friendly View ○ XML View

```
        Level            0
        Task             12544
        Opcode           0
        Keywords         0x8020000000000000
      - TimeCreated
            [ SystemTime] 2024-07-31T04:55:16.2405897Z
        EventRecordID    14610
      - Correlation
            [ ActivityID] {ffedc1a7-e2f8-0005-25c2-edfff8e2da01}
      - Execution
            [ ProcessID]  784
            [ ThreadID]   9120
        Channel          Security
```

`2024-07-31 04:55:16`

Task 10

What is the share Name accessed as part of the authentication process by the malicious tool used by the attacker?



```
        Source Port:            40252

Share Information:
        Share Name:             \\*\IPC$
        Share Path:

Access Request Information:
        Access Mask:            0x1
        Accesses:               ReadData (or ListDirectory)
```

`\\*\IPC$`