CrownJewel-2,evtx(gigasheet、EvtxECmd、Timeline Explorer),NTDS

```
Sherlock Scenario
Forela's Domain environment is pure chaos. Just got another alert from the Domain controller of NTDS.dit database being exfiltrated. Just one day prior you responded to an alert on the same domain controller where an attacker dumped NTDS.dit via vssadmin utility. However, you managed to delete the dumped files kick the attacker out of the DC, and restore a clean snapshot. Now they again managed to access DC with a domain admin account with their persistent access in the environment. This time they are abusing ntdsutil to dump the database. Help Forela in these chaotic times!!
* * *
About CrownJewel-2
In this very easy sherlock, you will learn how to detect NTDS.dit dumping which is one of the most critical Active directory attacks. You will get your hands on event logs to respond to an attack where the attacker utilized ntdsutil utility to dump the NTDS.dit database.
```

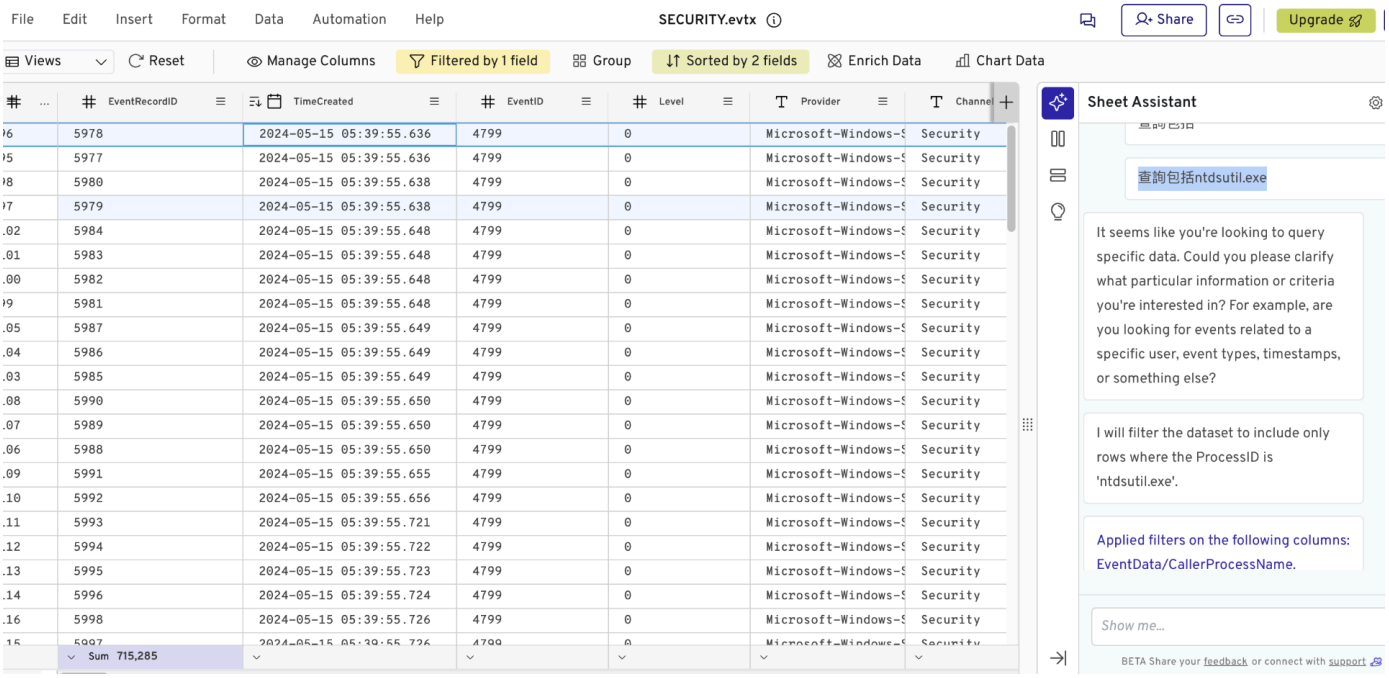
文件：SYSTEM.evtx、SECURITY.evtx、APPLICATION.evtx
使用工具：https://app.gigasheet.com/、EvtxECmd、Timeline Explorer

```
指令：
- EvtxECmd.exe   -f "C:\Users\TSO\Downloads\APPLICATION.evtx" --csv "C:\Users\TSO\Downloads\LOG" --csvf APPLICATION.csv
- EvtxECmd.exe   -f "C:\Users\TSO\Downloads\SECURITY.evtx" --csv "C:\Users\TSO\Downloads\LOG" --csvf SECURITY.csv
- EvtxECmd.exe   -f "C:\Users\TSO\Downloads\SYSTEM.evtx" --csv "C:\Users\TSO\Downloads\LOG" --csvf SYSTEM.csv
```

Task 1

When utilizing ntdsutil.exe to dump NTDS on disk, it simultaneously employs the Microsoft Shadow Copy Service. What is the most recent timestamp at which this service entered the running state, signifying the possible initiation of the NTDS dumping process?

查詢包括ntdsutil.exe



`2024-05-15 05:39:55`

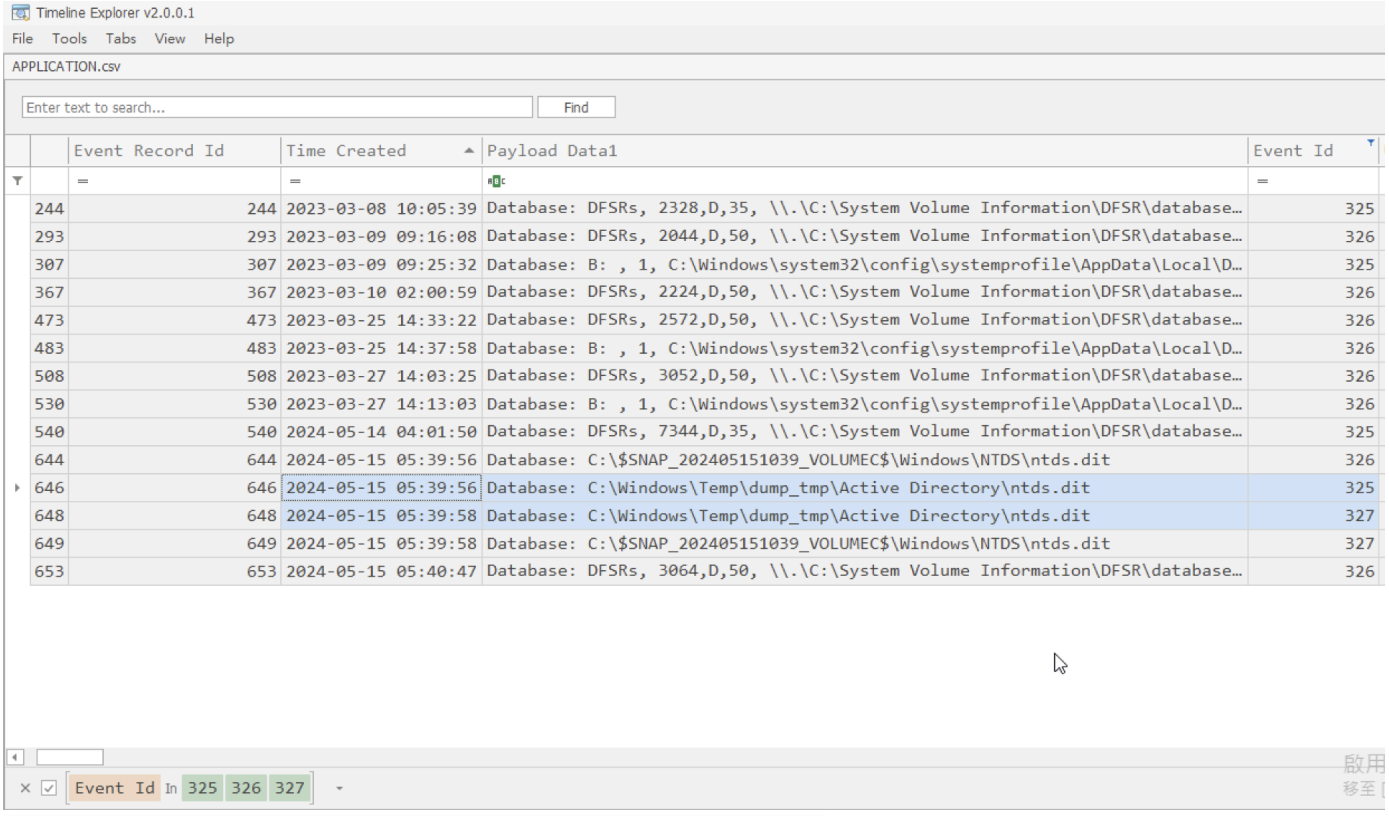
Task 2

Identify the full path of the dumped NTDS file.

參考：https://docs.velociraptor.app/exchange/artifacts/pages/ntdsutil/

event id ： `325、327`

但完全找不到event id...，我改用桌面版就正常了



`C:\Windows\Temp\dump_tmp\Active Directory\ntds.dit`

Task 3

When was the database dump created on the disk?

同上event id：325
`2024-05-15 05:39:56`

Task 4

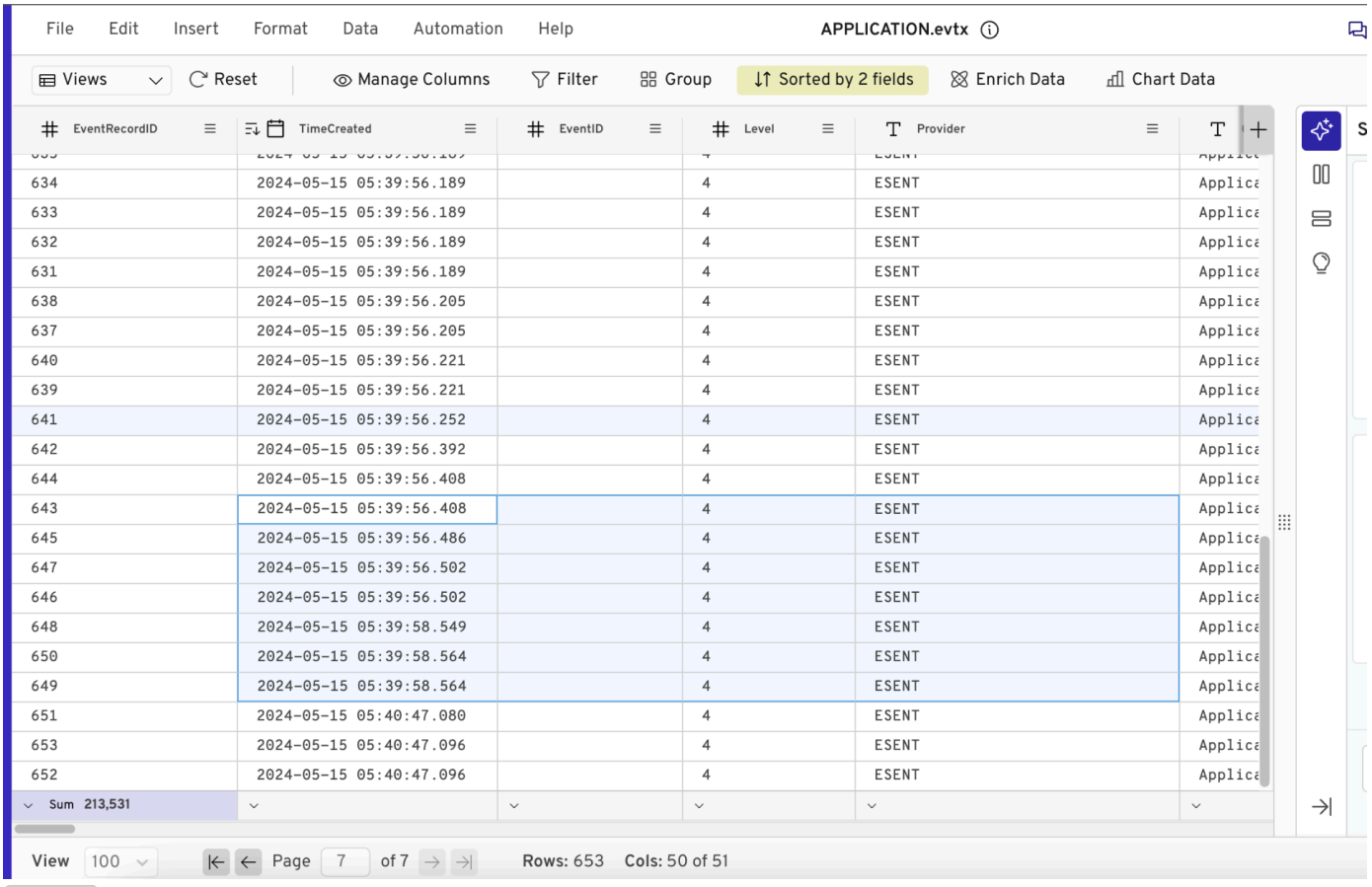
When was the newly dumped database considered complete and ready for use?

同上Task2 event id：327
`2024-05-15 05:39:58`

Task 5

Event logs use event sources to track events coming from different sources. Which event source provides database status data like creation and detachment?

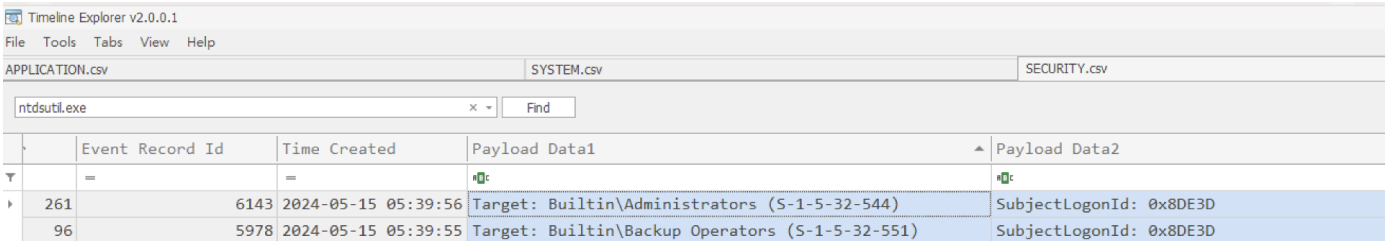
我記得web有出現過



`ESENT`

Task 6

When ntdsutil.exe is used to dump the database, it enumerates certain user groups to validate the privileges of the account being used. Which two groups are enumerated by the ntdsutil.exe process? Give the groups in alphabetical order joined by comma space.

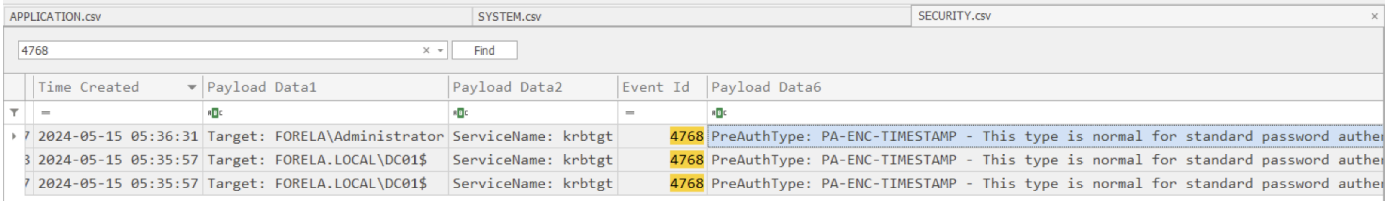


`Administrators, Backup Operators`

Task 7

Now you are tasked to find the Login Time for the malicious Session. Using the Logon ID, find the Time when the user logon session started.

event id：4768



`2024-05-15 05:36:31`