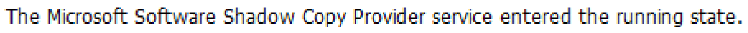
CrownJewel-2 Challenge

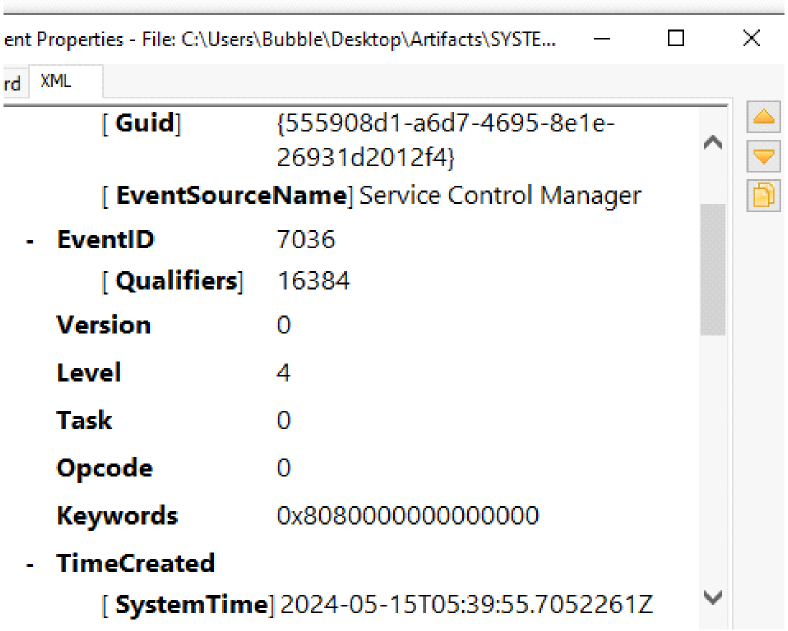
Sherlock Scenario
Forela's Domain environment is pure chaos. Just got another alert from the Domain controller of NTDS.dit database being exfiltrated. Just one day prior you responded to an alert on the same domain controller where an attacker dumped NTDS.dit via vssadmin utility. However, you managed 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!!

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?

I searched in System logs for Event ID 7036 which shows service state changed and analyzed the logs until I found the "Microsoft Software Shadow Copy" like in the question in the task



The Microsoft Software Shadow Copy Provider service entered the running state.



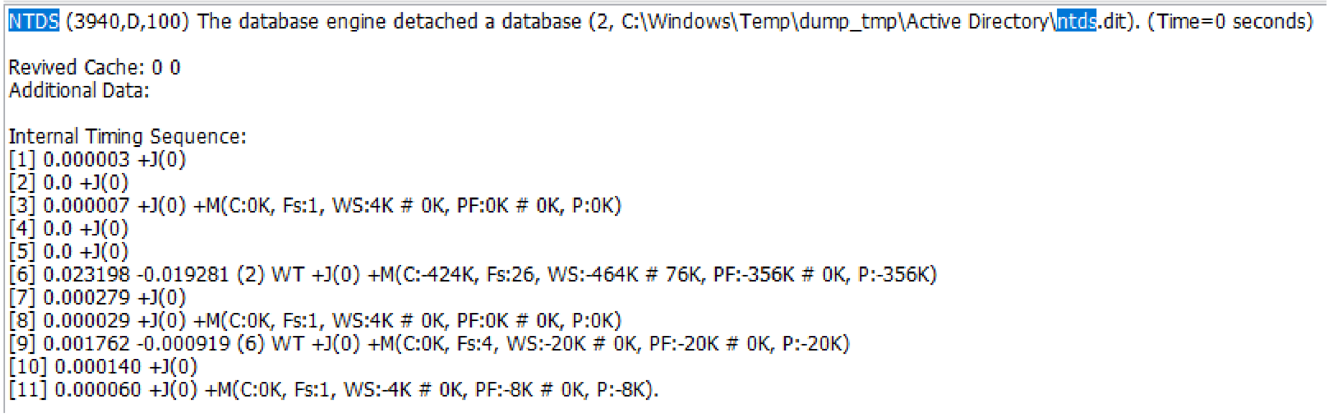
ent Properties - File: C:\Users\Bubble\Desktop\Artifacts\SYSTE...

```
        [ Guid]            {555908d1-a6d7-4695-8e1e-
                           26931d2012f4}
        [ EventSourceName] Service Control Manager
 -  EventID                7036
        [ Qualifiers]      16384
    Version                0
    Level                  4
    Task                   0
    Opcode                 0
    Keywords               0x8080000000000000
 -  TimeCreated
        [ SystemTime] 2024-05-15T05:39:55.7052261Z
```

Answer: 2024-05-15 05:39:55

Task 2:
Identify the full path of the dumped NTDS file.

I searched for NTDS in the Application logs and found unusual path

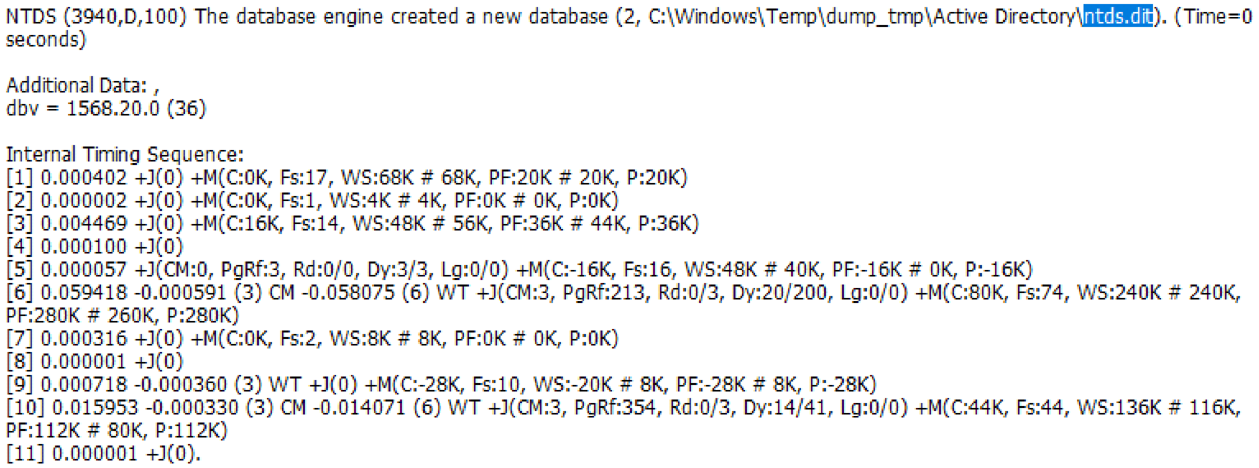


```
NTDS (3940,D,100) The database engine detached a database (2, C:\Windows\Temp\dump_tmp\Active Directory\ntds.dit). (Time=0 seconds)

Revived Cache: 0 0
Additional Data:

Internal Timing Sequence:
[1] 0.000003 +J(0)
[2] 0.0 +J(0)
[3] 0.000007 +J(0) +M(C:0K, Fs:1, WS:4K # 0K, PF:0K # 0K, P:0K)
[4] 0.0 +J(0)
[5] 0.0 +J(0)
[6] 0.023198 -0.019281 (2) WT +J(0) +M(C:-424K, Fs:26, WS:-464K # 76K, PF:-356K # 0K, P:-356K)
[7] 0.000279 +J(0)
[8] 0.000029 +J(0) +M(C:0K, Fs:1, WS:4K # 0K, PF:0K # 0K, P:0K)
[9] 0.001762 -0.000919 (6) WT +J(0) +M(C:0K, Fs:4, WS:-20K # 0K, PF:-20K # 0K, P:-20K)
[10] 0.000140 +J(0)
[11] 0.000060 +J(0) +M(C:0K, Fs:1, WS:-4K # 0K, PF:-8K # 0K, P:-8K).
```

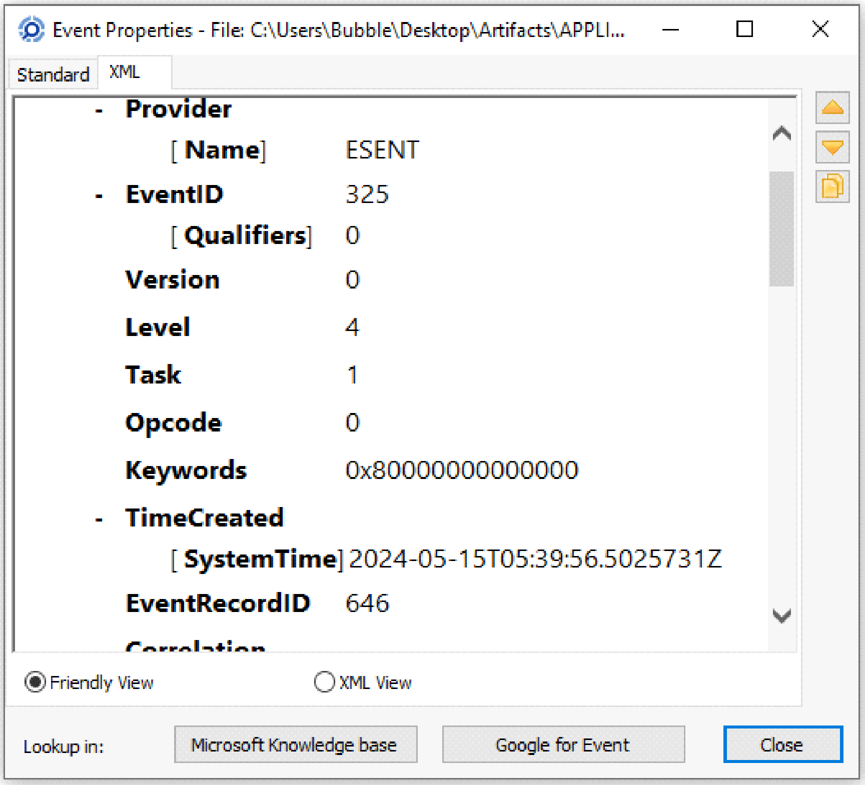
Answer: C:\Windows\Temp\dump_tmp\Active Directory\ntds.dit

Task 3:
When was the database dump created on the disk?

I searched for ntds.dit in Application logs and noticed the description is "The database engine created a new database" with the path from task 2



```
NTDS (3940,D,100) The database engine created a new database (2, C:\Windows\Temp\dump_tmp\Active Directory\ntds.dit). (Time=0
seconds)

Additional Data: ,
dbv = 1568.20.0 (36)

Internal Timing Sequence:
[1] 0.000402 +J(0) +M(C:0K, Fs:17, WS:68K # 68K, PF:20K # 20K, P:20K)
[2] 0.000002 +J(0) +M(C:0K, Fs:1, WS:4K # 4K, PF:0K # 0K, P:0K)
[3] 0.004469 +J(0) +M(C:16K, Fs:14, WS:48K # 56K, PF:36K # 44K, P:36K)
[4] 0.000100 +J(0)
[5] 0.000057 +J(CM:0, PgRf:3, Rd:0/0, Dy:3/3, Lg:0/0) +M(C:-16K, Fs:16, WS:48K # 40K, PF:-16K # 0K, P:-16K)
[6] 0.059418 -0.000591 (3) CM -0.058075 (6) WT +J(CM:3, PgRf:213, Rd:0/3, Dy:20/200, Lg:0/0) +M(C:80K, Fs:74, WS:240K # 240K,
PF:280K # 260K, P:280K)
[7] 0.000316 +J(0) +M(C:0K, Fs:2, WS:8K # 8K, PF:0K # 0K, P:0K)
[8] 0.000001 +J(0)
[9] 0.000718 -0.000360 (3) WT +J(0) +M(C:-28K, Fs:10, WS:-20K # 8K, PF:-28K # 8K, P:-28K)
[10] 0.015953 -0.000330 (3) CM -0.014071 (6) WT +J(CM:3, PgRf:354, Rd:0/3, Dy:14/41, Lg:0/0) +M(C:44K, Fs:44, WS:136K # 116K,
PF:112K # 80K, P:112K)
[11] 0.000001 +J(0).
```

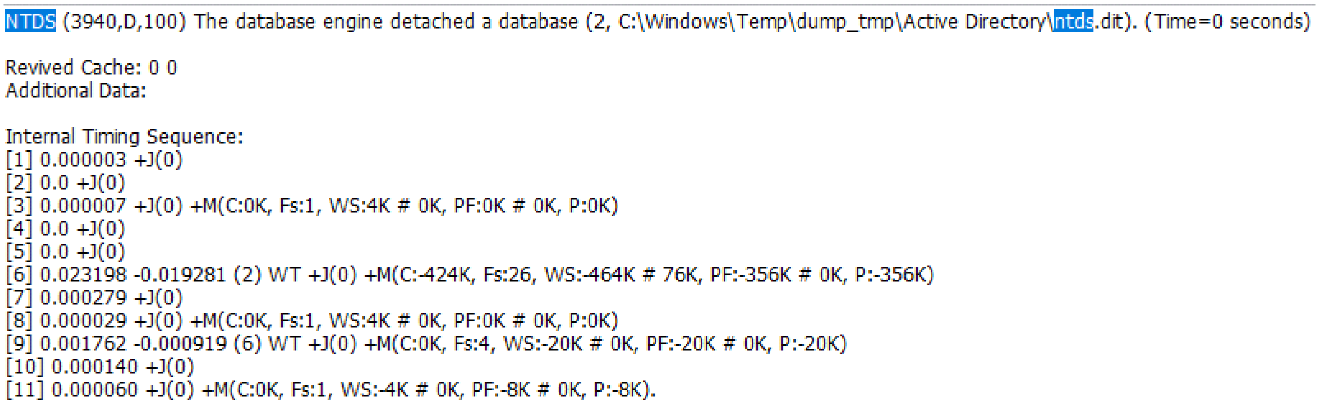

Event Properties - File: C:\Users\Bubble\Desktop\Artifacts\APPLI...
Standard
XML

```
- Provider
    [ Name]        ESENT
- EventID          325
    [ Qualifiers]  0
  Version          0
  Level            4
  Task             1
  Opcode           0
  Keywords         0x80000000000000
- TimeCreated
    [ SystemTime]  2024-05-15T05:39:56.5025731Z
  EventRecordID    646
  Correlation
```

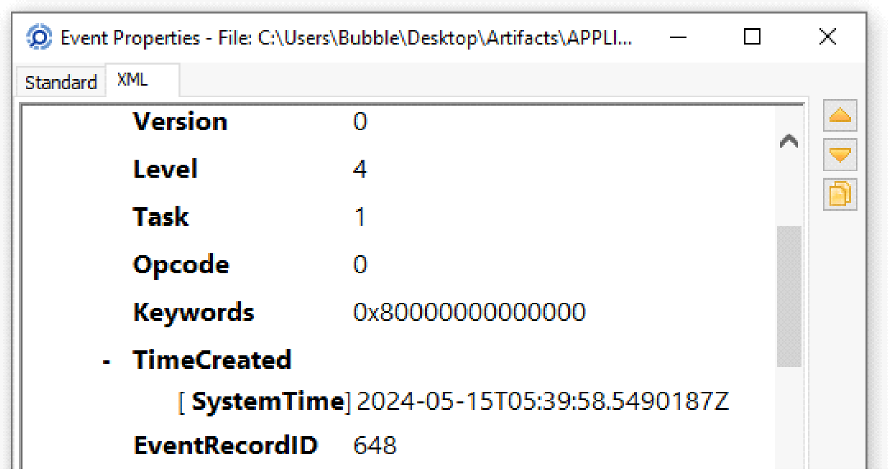
Answer: 2024-05-15 05:39:56

Task 4:
When was the newly dumped database considered complete and ready for use?

Same log from task 2



```
NTDS (3940,D,100) The database engine detached a database (2, C:\Windows\Temp\dump_tmp\Active Directory\ntds.dit). (Time=0 seconds)

Revived Cache: 0 0
Additional Data:

Internal Timing Sequence:
[1] 0.000003 +J(0)
[2] 0.0 +J(0)
[3] 0.000007 +J(0) +M(C:0K, Fs:1, WS:4K # 0K, PF:0K # 0K, P:0K)
[4] 0.0 +J(0)
[5] 0.0 +J(0)
[6] 0.023198 -0.019281 (2) WT +J(0) +M(C:-424K, Fs:26, WS:-464K # 76K, PF:-356K # 0K, P:-356K)
[7] 0.000279 +J(0)
[8] 0.000029 +J(0) +M(C:0K, Fs:1, WS:4K # 0K, PF:0K # 0K, P:0K)
[9] 0.001762 -0.000919 (6) WT +J(0) +M(C:0K, Fs:4, WS:-20K # 0K, PF:-20K # 0K, P:-20K)
[10] 0.000140 +J(0)
[11] 0.000060 +J(0) +M(C:0K, Fs:1, WS:-4K # 0K, PF:-8K # 0K, P:-8K).
```



Event Properties - File: C:\Users\Bubble\Desktop\Artifacts\APPLI...
Standard
XML

Version 0

Level 4

Task 1

Opcode 0

Keywords 0x80000000000000

- **TimeCreated**

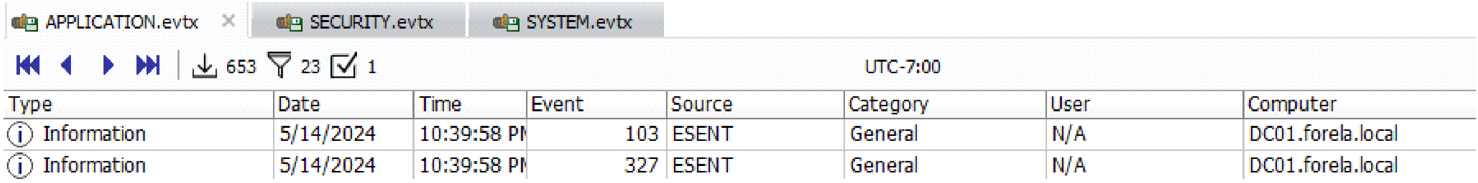
  [**SystemTime**] 2024-05-15T05:39:58.5490187Z

EventRecordID 648

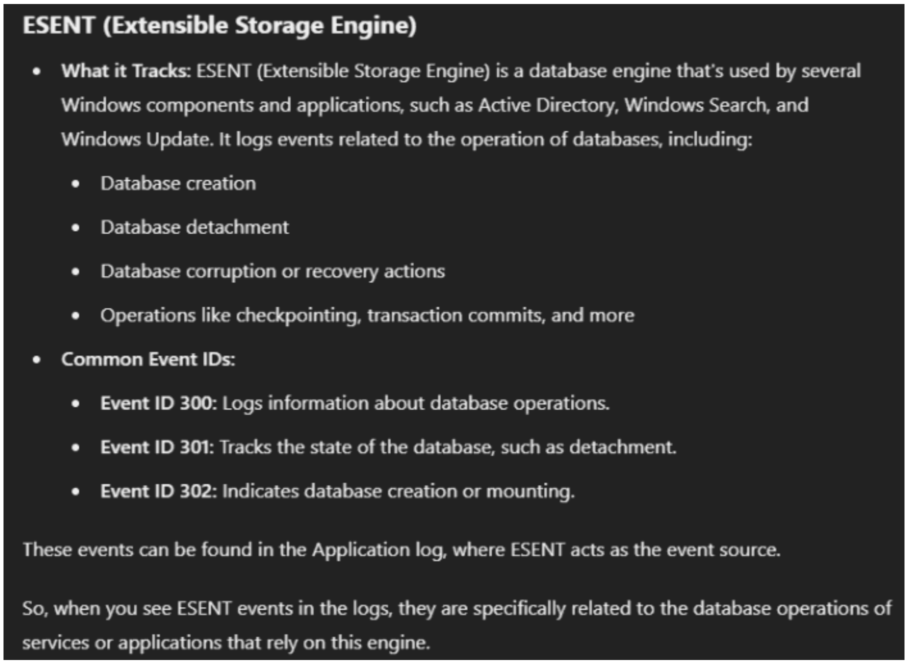
Answer: 2024-05-15 05:39:58

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?

There is a column named "Source"



Type	Date	Time	Event	Source	Category	User	Computer
Information	5/14/2024	10:39:58 PI	103	ESENT	General	N/A	DC01.forela.local
Information	5/14/2024	10:39:58 PI	327	ESENT	General	N/A	DC01.forela.local



ESENT (Extensible Storage Engine)

- **What it Tracks:** ESENT (Extensible Storage Engine) is a database engine that's used by several Windows components and applications, such as Active Directory, Windows Search, and Windows Update. It logs events related to the operation of databases, including:
  - Database creation
  - Database detachment
  - Database corruption or recovery actions
  - Operations like checkpointing, transaction commits, and more
- **Common Event IDs:**
  - **Event ID 300:** Logs information about database operations.
  - **Event ID 301:** Tracks the state of the database, such as detachment.
  - **Event ID 302:** Indicates database creation or mounting.

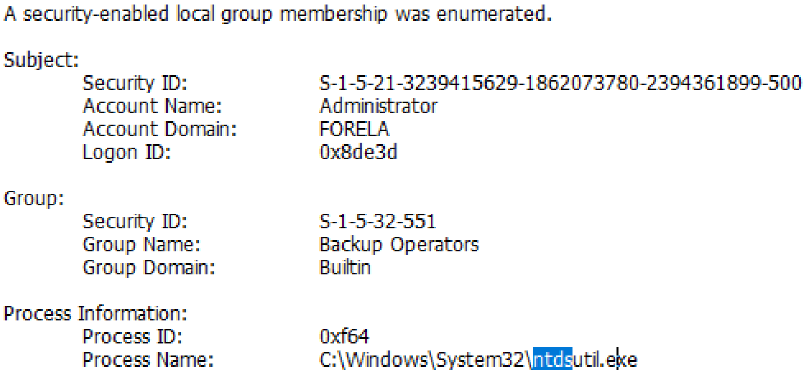
These events can be found in the Application log, where ESENT acts as the event source.

So, when you see ESENT events in the logs, they are specifically related to the database operations of services or applications that rely on this engine.

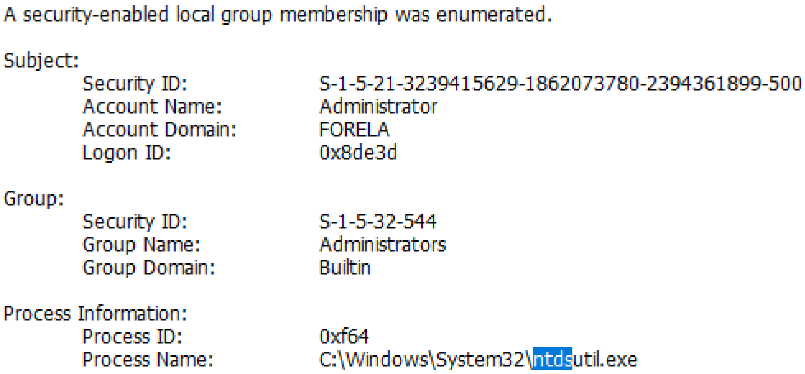
Answer: ESENT

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? Also, find the Logon ID so we can easily track the malicious session in our hunt.

I searched for NTDS in Security logs and found the Group name and Logon ID



```
A security-enabled local group membership was enumerated.

Subject:
        Security ID:            S-1-5-21-3239415629-1862073780-2394361899-500
        Account Name:           Administrator
        Account Domain:         FORELA
        Logon ID:               0x8de3d

Group:
        Security ID:            S-1-5-32-551
        Group Name:             Backup Operators
        Group Domain:           Builtin

Process Information:
        Process ID:             0xf64
        Process Name:           C:\Windows\System32\ntdsutil.exe
```

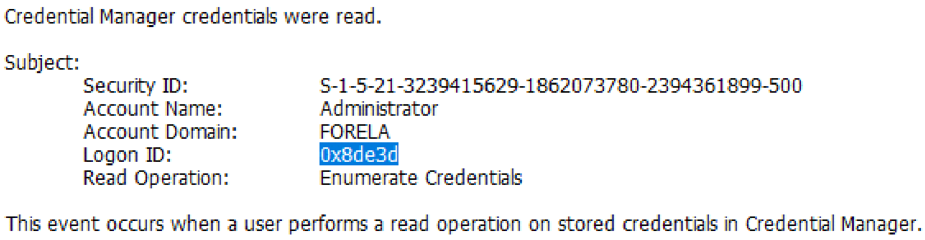


```
A security-enabled local group membership was enumerated.

Subject:
        Security ID:            S-1-5-21-3239415629-1862073780-2394361899-500
        Account Name:           Administrator
        Account Domain:         FORELA
        Logon ID:               0x8de3d

Group:
        Security ID:            S-1-5-32-544
        Group Name:             Administrators
        Group Domain:           Builtin

Process Information:
        Process ID:             0xf64
        Process Name:           C:\Windows\System32\ntdsutil.exe
```

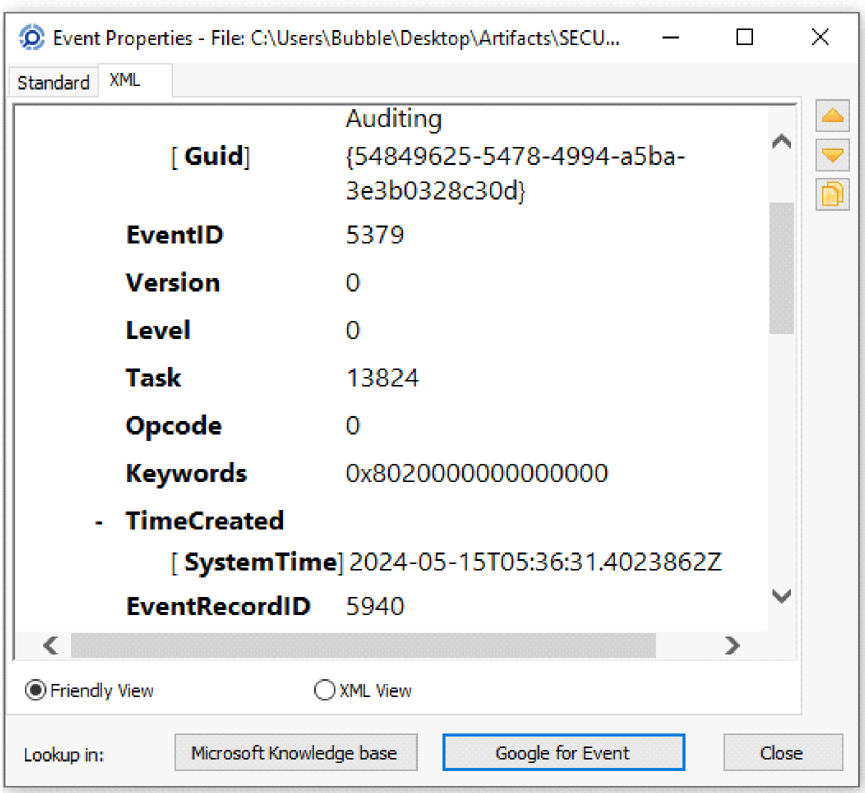
Answer: Administrators, Backup Operators, 0x8DE3D

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.

I searched for Logon ID "0x8de3d" in Security logs and noticed a log which said "credentials were read"



```
Credential Manager credentials were read.

Subject:
	Security ID:		S-1-5-21-3239415629-1862073780-2394361899-500
	Account Name:		Administrator
	Account Domain:		FORELA
	Logon ID:		0x8de3d
	Read Operation:		Enumerate Credentials

This event occurs when a user performs a read operation on stored credentials in Credential Manager.
```



Event Properties - File: C:\Users\Bubble\Desktop\Artifacts\SECU...

```
                  Auditing
      [ Guid]     {54849625-5478-4994-a5ba-
                  3e3b0328c30d}
    EventID       5379
    Version       0
    Level         0
    Task          13824
    Opcode        0
    Keywords      0x8020000000000000
  - TimeCreated
      [ SystemTime] 2024-05-15T05:36:31.4023862Z
    EventRecordID 5940
```

● Friendly View ○ XML View

2024-05-15 05:36:31