What can you find from SAM?

- SAM (Security Account Manager)
  - Contains user account information for users and groups on the system
  - Also contains logon passwords
- Use of SAM
  - Resolve user to SID
  - Find out who is the last one logged in

SID - Security Identifiers

- Unique alphanumeric character strings of variable length assigned to each user.
- Windows then grants or denies access and privileges to resources based on Access Control Lists (ACL), which use SIDs to uniquely identify users and/or their group memberships.
- SAM contains hashed passwords and usernames for authentication.

SID (Contd.)

SIDs in a typical multiuser system:

- HKU\.DEFAULT
- HKU\S-1-5-18
- HKU\S-1-5-19
- HKU\S-1-5-20

System Accounts

- HKU\S-1-5-21-1116317227-3122546243-4014252641-1000
- HKU\S-1-5-21-1116317227-3122546243-4014252641-1002

Individual User Accounts

"S" identifies the string as SID.

"1" SID specification version.

"5" is the identifier authority value.

"21-1116317227-3122546273-4014252621" identifier for unique individual user accounts.

"1000" or "1002" is the **Relative ID (RID).**

Identifying Last Logon using RID

- Windows stores the last logon time for a user at : SAM\Domains\Account\Users\%RID%\F

  (%RID% is the relative ID (RID) of the user.)

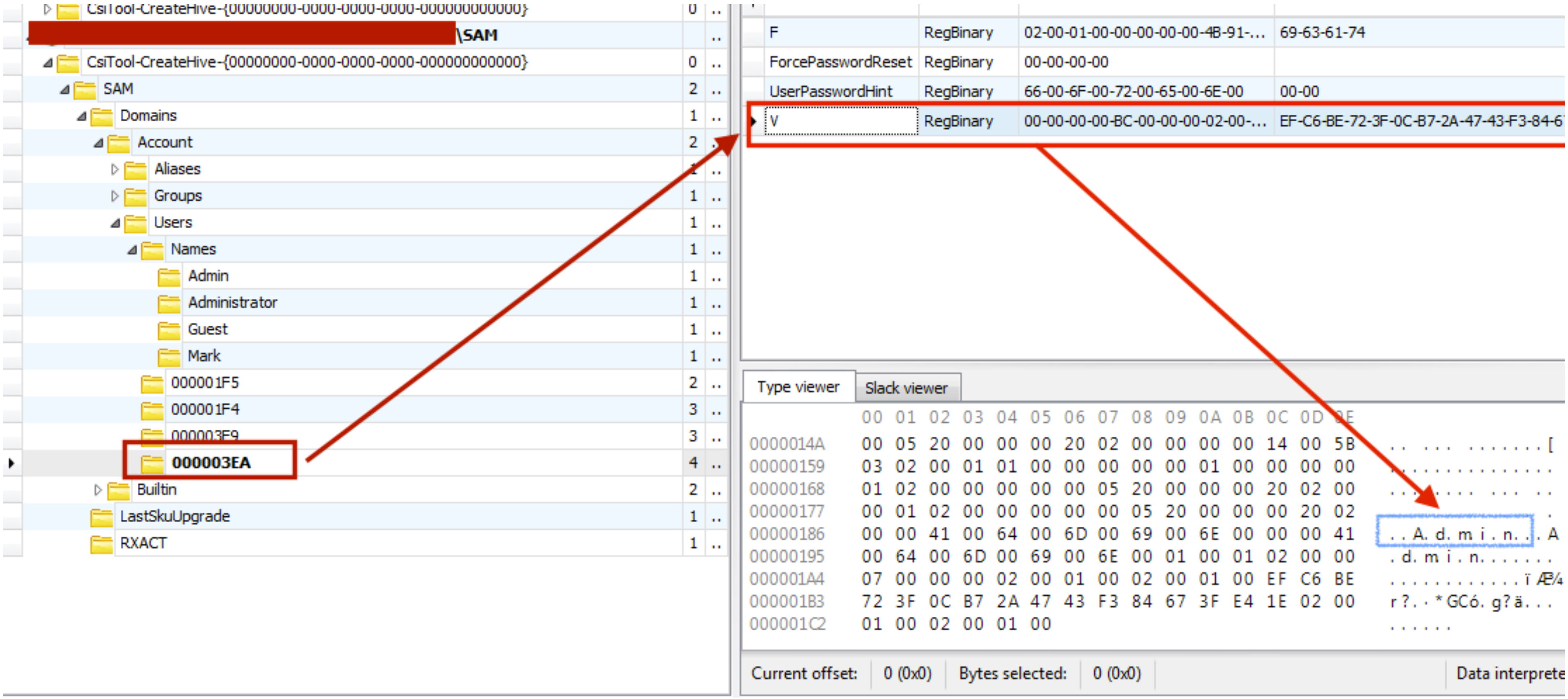
- There are multiple ways to find the SID-Username mapping.

- In SAM hive, it can be determined by examining the V value for each RID at SAM\Domains\Account\Users key.

- The following two screenshot will show:
  - Finding Usernames from RID (V-values)
  - Determining last logon time for the RID. (F-values)

Finding Username from RID

- Select RIDs under SAM\Domains\Account\Users
- Select V entry and scroll the hex values till the end.



```
▷ CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}   0
  [redacted]\SAM
◢ CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}   0
  ◢ SAM                                                       2
    ◢ Domains                                                 1
      ◢ Account                                               2
        ▷ Aliases                                             1
        ▷ Groups                                              1
        ◢ Users                                               1
          ◢ Names                                             1
              Admin                                           1
              Administrator                                   1
              Guest                                           1
              Mark                                            1
            000001F5                                          2
            000001F4                                          3
            000003E9                                          3
            000003EA                                          4
      ▷ Builtin                                               2
    LastSkuUpgrade                                            1
    RXACT                                                     1
```

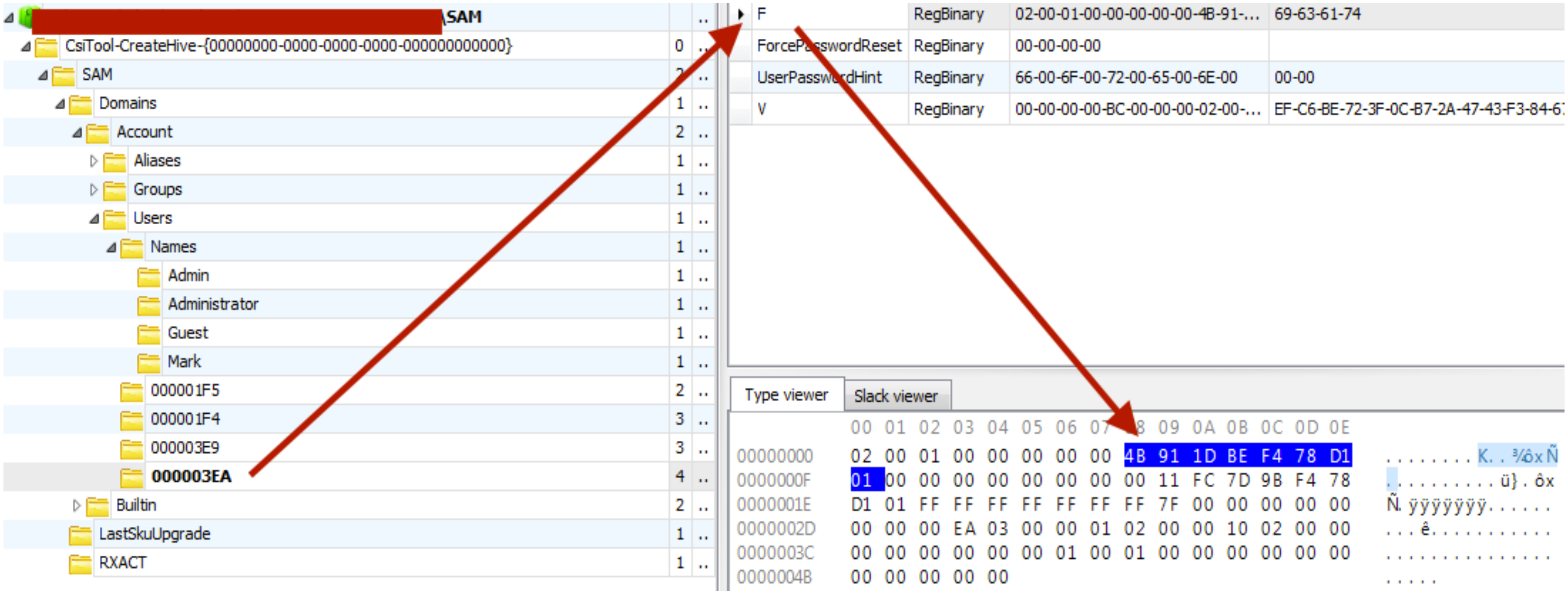
F	RegBinary	02-00-01-00-00-00-00-00-4B-91-...	69-63-61-74
ForcePasswordReset	RegBinary	00-00-00-00	
UserPasswordHint	RegBinary	66-00-6F-00-72-00-65-00-6E-00	00-00
V	RegBinary	00-00-00-00-BC-00-00-00-02-00-...	EF-C6-BE-72-3F-0C-B7-2A-47-43-F3-84-6

```
          00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E
0000014A  00 05 20 00 00 00 20 02 00 00 00 00 14 00 5B   ..  ...  .......[
00000159  03 02 00 01 01 00 00 00 00 00 01 00 00 00 00   ...............
00000168  01 02 00 00 00 00 00 05 20 00 00 00 20 02 00   ........ ... ..
00000177  00 01 02 00 00 00 00 00 05 20 00 00 00 20 02          .
00000186  00 00 41 00 64 00 6D 00 69 00 6E 00 00 00 41   ..A.d.m.i.n...A
00000195  00 64 00 6D 00 69 00 6E 00 01 00 01 02 00 00   .d.m.i.n.......
000001A4  07 00 00 00 02 00 01 00 02 00 01 00 EF C6 BE   ............ïÆ¾
000001B3  72 3F 0C B7 2A 47 43 F3 84 67 3F E4 1E 02 00   r?.·*GCó.g?ä...
000001C2  01 00 02 00 01 00                              ......
```

Current offset: 0 (0x0) | Bytes selected: 0 (0x0) | Data interprete

Determining Last logon

- Select the F value for RID.
- Bytes 9-16 are Last logon time in FILETIME format for the associated user.
- Convert the FILETIME to Date & Time. (Use Dcode).



[redacted]\SAM		..
CsiTool-CreateHive-{00000000-0000-0000-0000-000000000000}	0	..
SAM	2	..
Domains	1	..
Account	2	..
Aliases	1	..
Groups	1	..
Users	1	..
Names	1	..
Admin	1	..
Administrator	1	..
Guest	1	..
Mark	1	..
000001F5	2	..
000001F4	3	..
000003E9	3	..
000003EA	4	..
Builtin	2	..
LastSkuUpgrade	1	..
RXACT	1	..

F	RegBinary	02-00-01-00-00-00-00-00-4B-91-...	69-63-61-74
ForcePasswordReset	RegBinary	00-00-00-00	
UserPasswordHint	RegBinary	66-00-6F-00-72-00-65-00-6E-00	00-00
V	RegBinary	00-00-00-00-BC-00-00-00-02-00-...	EF-C6-BE-72-3F-0C-B7-2A-47-43-F3-84-67

```
          00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E
00000000  02 00 01 00 00 00 00 00 4B 91 1D BE F4 78 D1   ........K..¾ôxÑ
0000000F  01 00 00 00 00 00 00 00 00 11 FC 7D 9B F4 78   ..........ü}.ôx
0000001E  D1 01 FF FF FF FF FF FF FF 7F 00 00 00 00 00   Ñ.ÿÿÿÿÿÿÿ......
0000002D  00 00 00 EA 03 00 00 01 02 00 00 10 02 00 00   ...ê...........
0000003C  00 00 00 00 00 00 01 00 01 00 00 00 00 00 00   ...............
0000004B  00 00 00 00 00                                 .....
```