Extracting Personal Meeting ID(PMI) of a Zoom user account holder from a Forensic Disk Image?

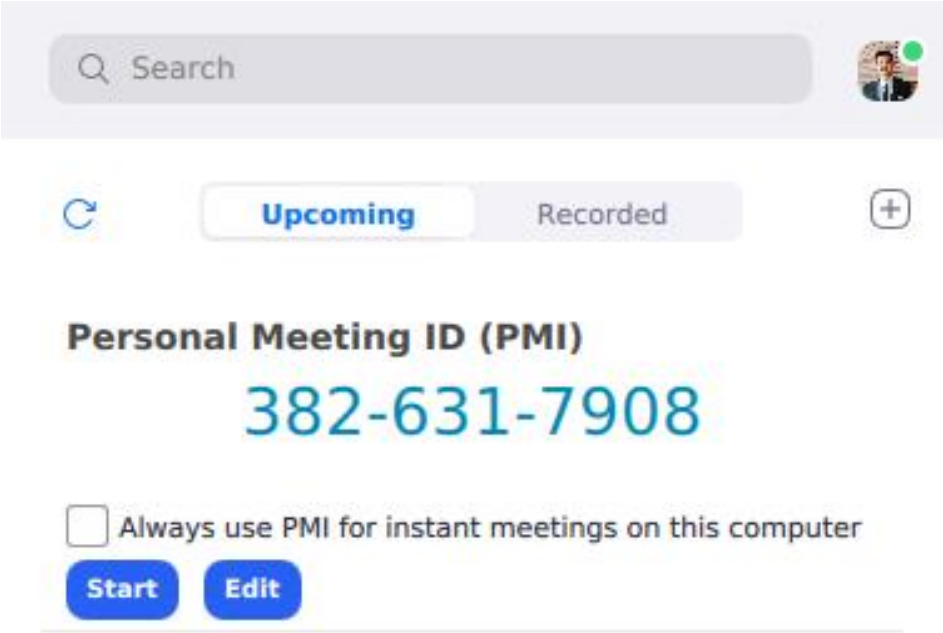
Daniel Addai

UNIVERSITY OF BALTIMORE
TOWSON UNIVERSITY

BJA

What is Zoom Personal Meeting ID(PMI)?

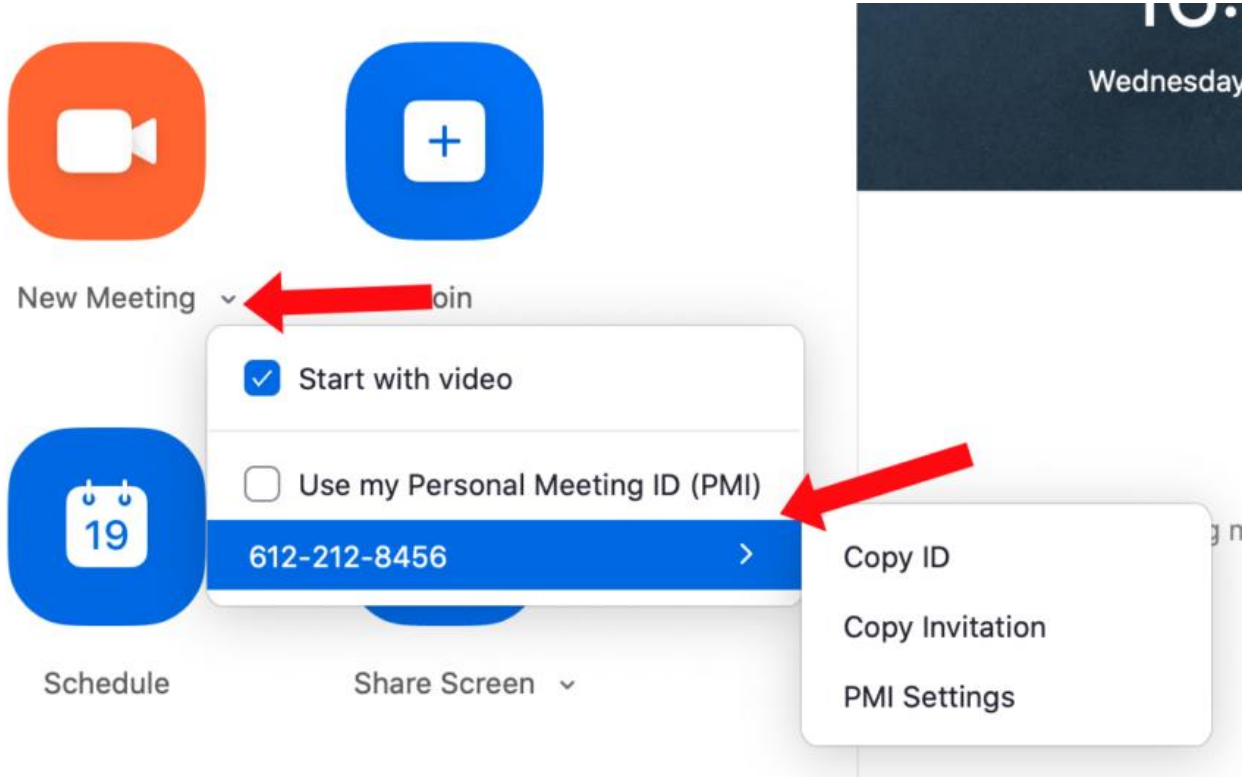
- A Personal Zoom Meeting ID is a unique identification number associated with an individual Zoom user. It serves as a static, personal virtual meeting room, allowing the user to host meetings using the same ID repeatedly.
- This feature provides a consistent and easily memorable meeting location for the user and is often used for regular or scheduled meetings.



Significance

- This information aids investigators in positively identifying the user, reconstructing timelines of Zoom-related events, and contributing valuable evidence for legal, compliance, or security purposes.
- Understanding of the user's Zoom interactions and facilitating a comprehensive investigation into specific virtual meetings and associated activities.

Starting your own zoom meeting with your Zoom Personal meeting ID as a host



Joining a zoom meeting using someone else's(Host) zoom meeting ID

Janyne Kizer is inviting you to a scheduled Zoom meeting.

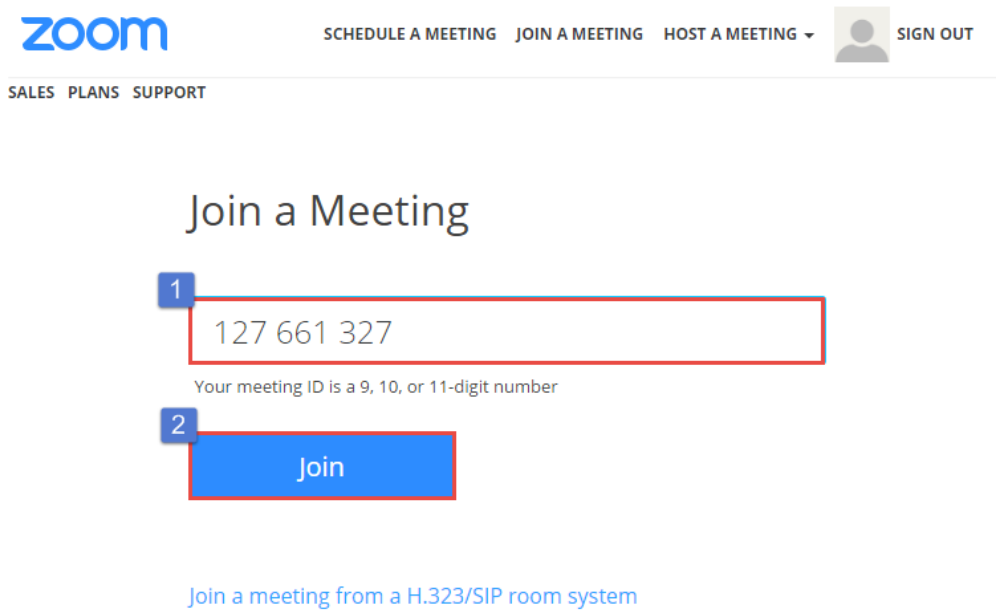
Topic: Jeff Test
Time: Mar 16, 2020 04:00 PM Eastern Time (US and Canada)

Join Zoom Meeting
https://ncsu.zoom.us/j/354136101

Meeting ID: 354 136 101

One tap mobile
+19292056099,,354136101# US (New York)
+13126266799,,354136101# US (Chicago)

Joining a zoom meeting using someone else's(Host) zoom meeting ID



Objectives/Goals

- Input : A windows disk image
- Output: Zoom Personal Meeting ID

Approach

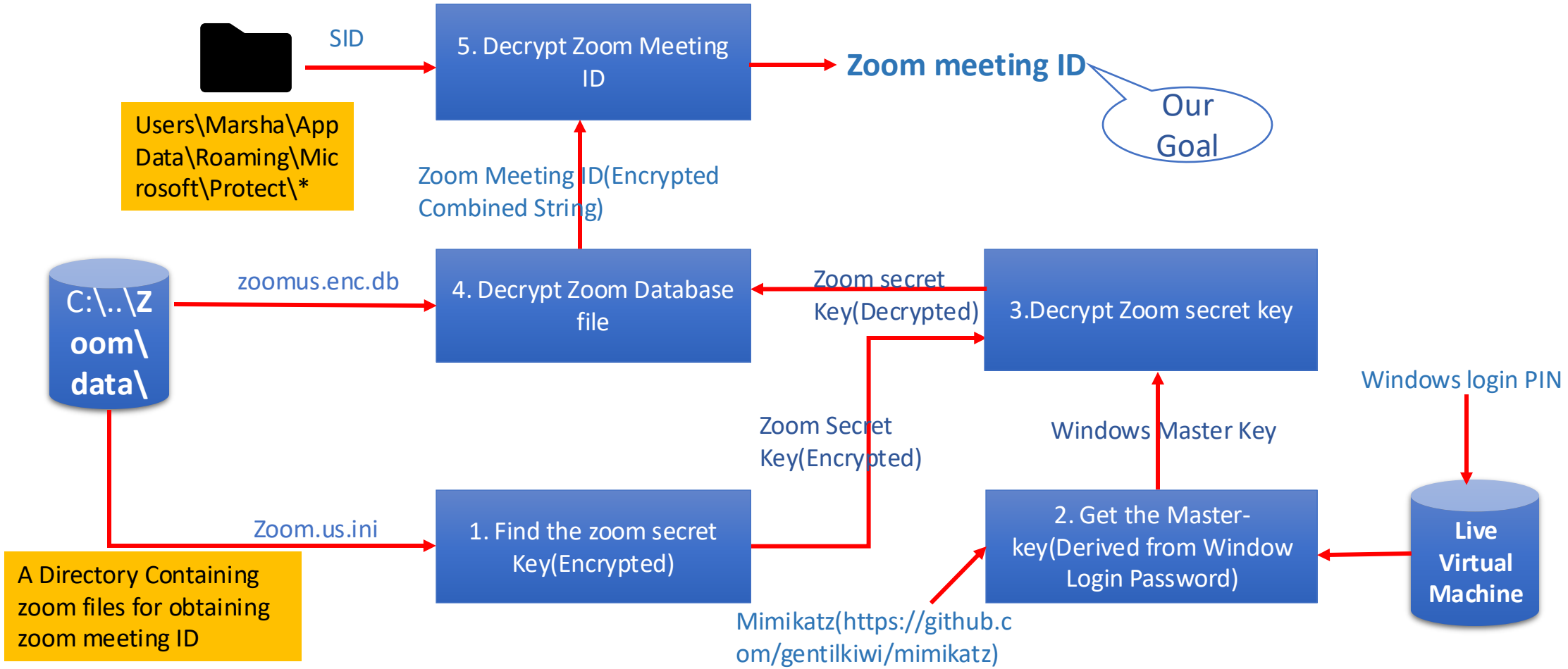
Prerequisites: 00_Cellebrite_Auto_Theft_And_Stealing.pptx

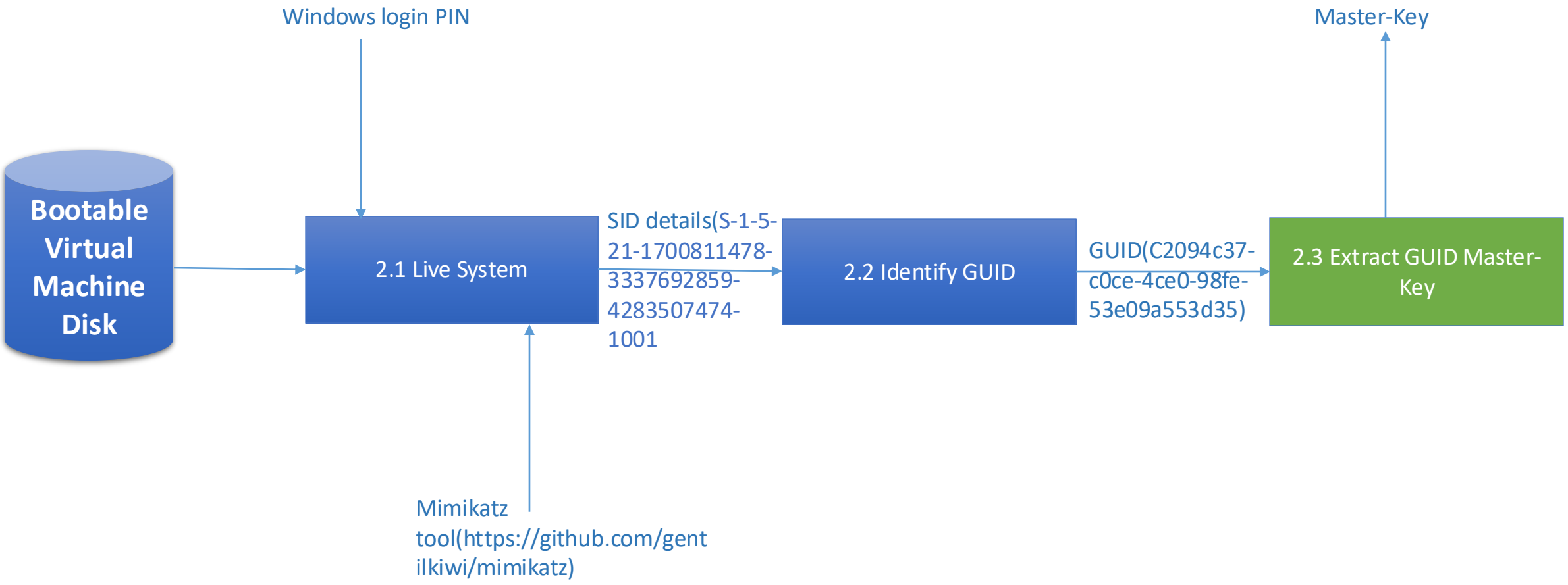
1. Follow the PPT to convert the E01 forensic image into a VM for this activity: Convert_Forensic Image_to_Virtual_Machine_Disk.pptx
2. Download Mimikatz from Github: https://github.com/gentilkiwi/mimikatz

Steps:

1. Find the Zoom secret Key.
2. Get the Windows User Master-key.
3. Decrypt Zoom secret Key.
4. Decrypt Zoom Database file.
5. Extract Combined String.
6. Decrypt Combined String to find Zoom Meeting ID.

How to obtain Zoom Personal Meeting ID(PMI) from a Forensic Image




Windows login PIN
Master-Key
Bootable Virtual Machine Disk
2.1 Live System
SID details(S-1-5-21-1700811478-3337692859-4283507474-1001
2.2 Identify GUID
GUID(C2094c37-c0ce-4ce0-98fe-53e09a553d35)
2.3 Extract GUID Master-Key
Mimikatz tool(https://github.com/gentilkiwi/mimikatz)

Step 1: Find the secret Key

Show the decryption Key

```
┌──(root💀kali)-[/media/…/AppData/Roaming/Zoom/data]
└─# cat Zoom.us.ini
[ZoomChat]
win_osencrypt_key=ZWOSKEYAQAAANCMnd8BFdERjHoAwE/Cl+sBAAAAN0wJws7A4EyY/lPgml
gAAAAAIAACAAAACfbLWwMYxJQedFumm5qQeAUg7MAuCHhd89pMkUwuEp1TAAAAC3oDDqmxxb7us
ji3TNUFFd14/5NQbHwre9nmMSM6wg1+BNU2Xj5KFcjtJWWBLD+bU3qF+rDScw==
```

Purge these Characters from the decryption key, save and copy to local System Document

```
┌──(root💀kali)-[/media/…/AppData/Roaming/Zoom/data]
└─# cat Zoom.us.ini
[ZoomChat]
win_osencrypt_key=ZWOSKEYAQAAANCMnd8BFdERjHoAwE/Cl+sBAAAAN0wJws7A4EyY/lPgml
gAAAAAIAACAAAACfbLWwMYxJQedFumm5qQeAUg7MAuCHhd89pMkUwuEp1TAAAAC3oDDqmxxb7us
ji3TNUFFd14/5NQbHwre9nmMSM6wg1+BNU2Xj5KFcjtJWWBLD+bU3qF+rDScw==
```

Store the trimmed Decryption key into zoom.txt file

```
┌──(root💀kali)-[/home/kali/Documents]
└─# cat Zoom.us.ini > /home/kali/Documents/zoom.txt
```

Show the trimmed decryption key

```
┌──(root💀kali)-[/home/kali/Documents]
└─# cat zoom.txt
AQAAANCMnd8BFdERjHoAwE/Cl+sBAAAAN0wJws7A4EyY/lPgmlU9NQAAAAACAAAAAAAQZgAAAAEAACAAAABpDI8XS07wR6GQwv5N2VBlNGB1DQwTcFjpScQwmF
iNvgAAAAAOgAAAAAIAACAAAACfbLWwMYxJQedFumm5qQeAUg7MAuCHhd89pMkUwuEp1TAAAAC3oDDqmxxb7usbEQdURdXvuSWx3tSmBn0BZfdOYd1iFZmXu/EX
Joh09/37z2YM5iJAAAAA9VIw30eaBS4olqrMlQvzDrV5rji3TNUFFd14/5NQbHwre9nmMSM6wg1+BNU2Xj5KFcjtJWWBLD+bU3qF+rDScw==
```

Decode the decryption key from base64 And Show the decoded Key

```
(base) ┌──(root💀kali)-[/home/kali/Documents]
└─# base64 -d -i zoom.txt > decoded.bat

(base) ┌──(root💀kali)-[/home/kali/Documents]
└─# cat decoded.bat
Ḱ◆◆◆◆z◆O◆7L      ◆◆◆◆L◆◆S◆◆U=5f i
                                  ◆KN◆G◆◆◆◆M◆Pe4`u
pX◆I◆0◆X◆◆◆ ◆l◆◆1◆IA◆E◆i◆◆◆R◆◆◆◆◆=◆◆◆◆)◆0◆◆0◆[◆◆E◆◆%◆◆h}e◆Na◆b◆◆◆◆&◆t◆◆◆◆f

~◆6^>J◆◆%e◆,?◆Sz◆◆◆◆s
```

Step 2: Get the Windows Master-key

Show the Master-Key is stored in Security Identifier(SID) of the User's Account

```
root@kali: /media/kali/Windows/Users/marsh/

(base) ┌──(root💀kali)-[/media/…/AppData/Roaming/Microsoft/Protect]
└─# ll
total 5
-rwxrwxrwx 1 kali kali   24 Mar 23  2021 CREDHIST
drwxrwxrwx 1 kali kali 4096 Jul 24  2021 S-1-5-21-1700811478-3337692859-4283507474-1001
```

Show the Master-key is encrypted

```
-rwxrwxrwx 2 kali kali 468 Jul 29  2021 26c81da6-3c22-4610-a503-e7e60a79776c
-rwxrwxrwx 2 kali kali 468 Jul 29  2021 c2094c37-c0ce-4ce0-98fe-53e09a553d35
-rwxrwxrwx 2 kali kali  24 Jul 24  2021 Preferred

(base) ┌──(root💀kali)-[/media/…/Roaming/Microsoft/Protect/S-1 78-
└─# cat c2094c37-c0ce-4ce0-98fe-53e09a553d35
c2094c37-c0ce-4ce0-98fe-53e09a553d35◆◆
jV[\◆◆◆◆◆&A\◆◆f◆◆v◆◆◆B◆,◆p◆◆◆
◆n◆л◆◆◆◆◆@◆
(base) ┌──(root💀kali)-[/media/…/Roaming/Micros -5-21-1700811478-
```

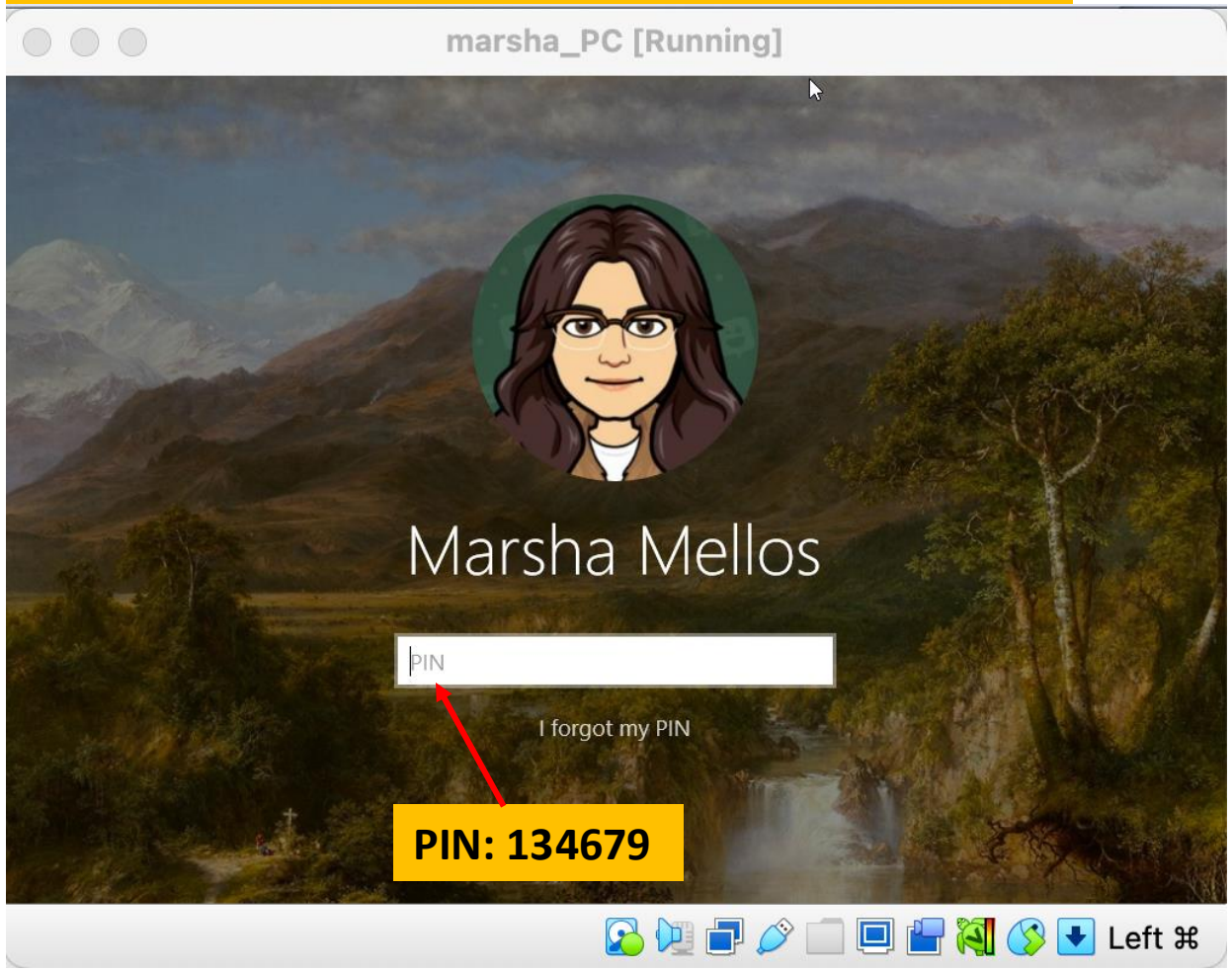
Global Unique Identifier(GUID) of interest

Show the Master-key is encrypted

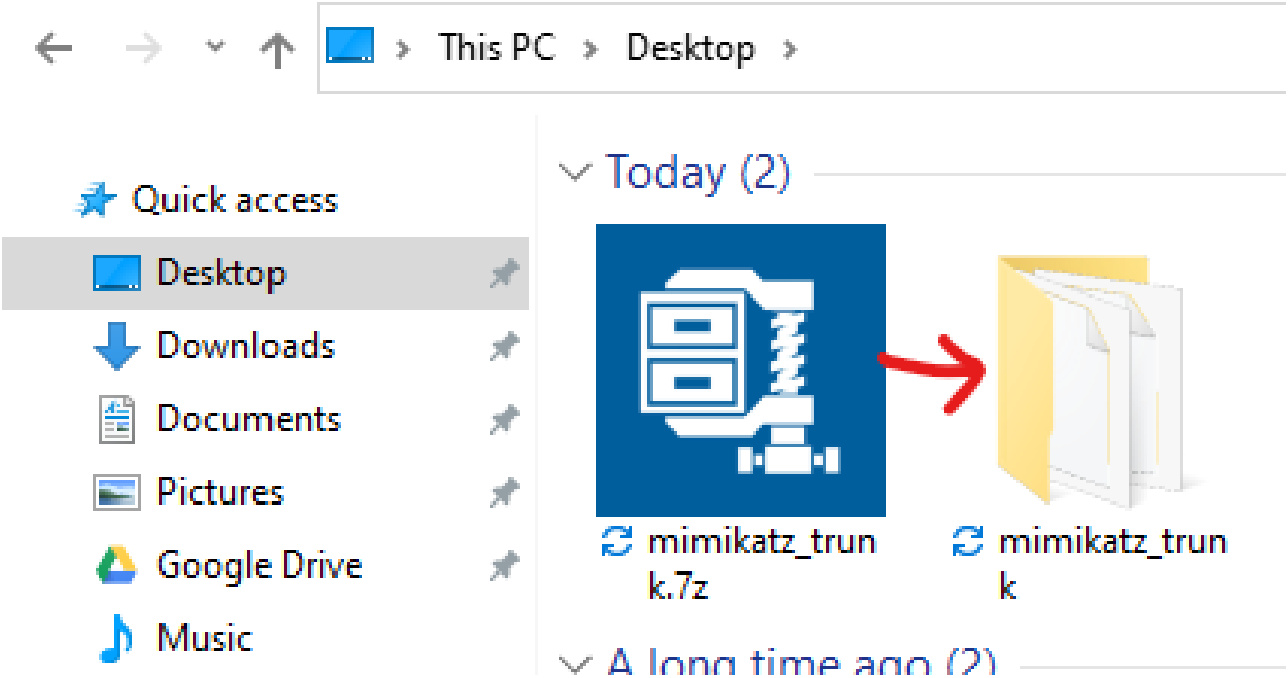
Prerequisite:

1. Follow the PPT to convert the E01 forensic image into a VM for this activity: [Convert_Forensic Image_to_Virtual_Machine_Disk.pptx]
2. Download Mimikatz from Github: https://github.com/gentilkiwi/mimikatz

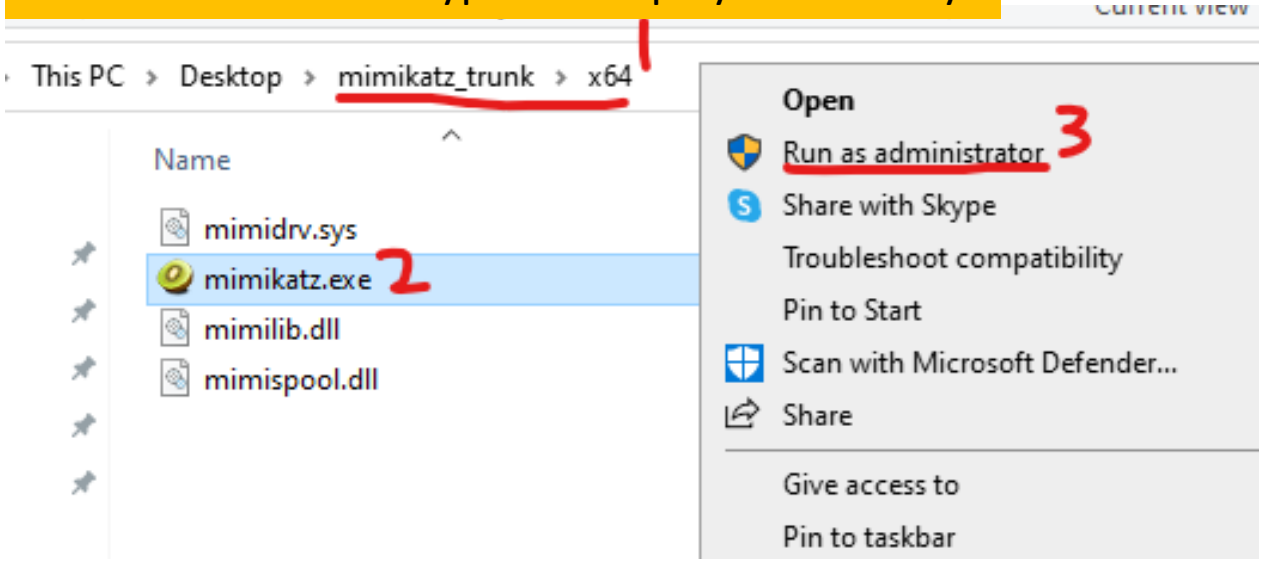
Boot the New Virtual Machine Windows system



Use Mimikatz to decrypt and display Master-key



Use Mimikatz to decrypt and display Master-key



Use Mimikatz to decrypt and display Master-key

```
  .#####.   mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::dpapi

Authentication Id : 0 ; 421231 (00000000:00066d6f)
Session           : Interactive from 1
User Name         : marsh
Domain            : LAPTOP-9I2MMKOU
Logon Server      : (null)
Logon Time        : 2/13/2024 18:54:06
SID               : S-1-5-21-1700811478-3337692859-4283507474-1001
```

Type the following commands

Use Mimikatz to decrypt and display Master-key the SID of the User's account

```
Authentication Id : 0 ; 421231 (00000000:00066d6f)
Session           : Interactive from
User Name         : marsh
Domain            : LAPTOP-9I2MMKOU
Logon Server      : (null)
Logon Time        : 2/13/2024 18:54:06
SID               : S-1-5-21-1700811478-3337692859-4283507474-1001
        [00000000]
        * GUID      :  {26c81da6-3c22-4610-a503-e7e60a79776c}
        * Time      :  2/13/2024 19:31:32
        * MasterKey :  1dbb9661f3e869cdf903cfbae46b59bfe22817024a
38fab0a6de7a010e2ad150d2dbed6615
        * sha1(key) :  11d5a9d469fc58a378d51dde84b9a9ad0b4ad517
        [00000001]
```

Marsha's Security Identifier(SID)

Show the Master-key

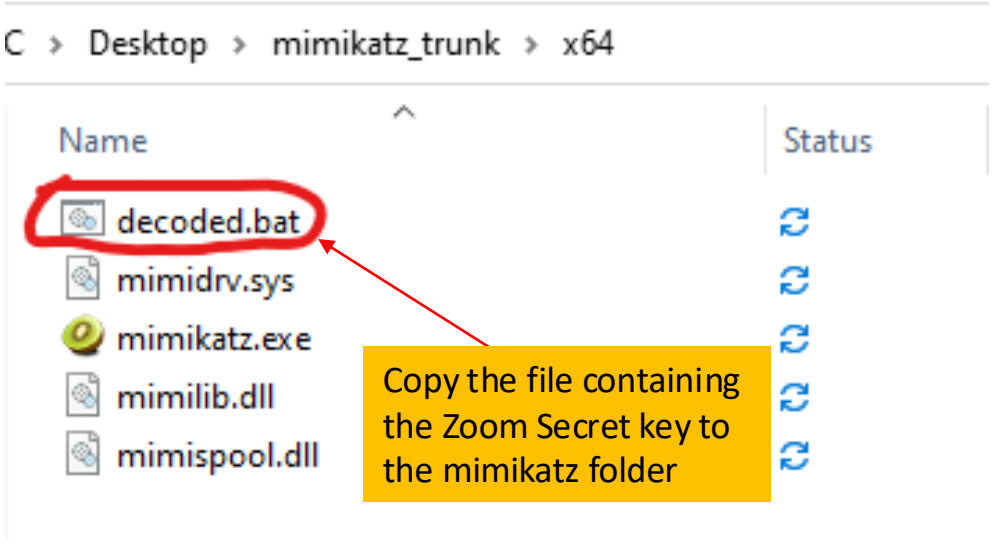
```
38fab0a6de7a010e2ad150d2dbed6615
         * sha1(key) :  11d5a9d469fc58a378d51dde84b9a9ad0b4ad517
         [00000001]
         * GUID      :  {6c0e5a72-9907-47ab-a702-b
         * Time      :  2/13/2024 19:31:32
         * MasterKey :  37adb675aa384140af98326b9ac24160dc8f6029                    3adb4fc
282fba67d5e54f556a68cd1c66da67e9
         * sha1(key) :  67f7835c52d5c594e0ad8c23baaae84c9c6fa989
         [00000002]
         * GUID      :  {c2094c37-c0ce-4ce0-98fe-53e09a553d35}
         * Time      :  2/13/2024 19:31:32
         * MasterKey :  9ea76e10f983a9e73a0eb742b581e3a77d9d82f8bec430649a98b926d09d2c5c9ee
a07e7fd1f45d46ad7f7d97a7f03c5c14
         * sha1(key) :  b579c41cea76baa853c5a8195b3c908ef9fe9ec6
```

GUID of interest

Decrypted Master-Key

Step 3: Decrypt zoom secret key

Use Mimikatz to decrypt the zoom secret Key



Copy the file containing the Zoom Secret key to the mimikatz folder

Use Mimikatz to decrypt the zoom secret Key

```
mimikatz # dpapi::blob /in:"decoded.bat" /unprotect /masterkey:9ea76e10f983a9e73a0eb742b581e3a77d9d82f8bec430649a98b926d
09d2c5c9ee181996e560ba6f48b85aea06bb9f6a07e7fd1f45d46ad7f7d97a7f03c5c14
**BLOB**
  dwVersion          : 00000001 - 1
  guidProvider       : {df9d8cd0-1501-11d1-8c7a-
  dwMasterKeyVersion : 00000001 - 1
  guidMasterKey      : {c2094c37-c0ce-4ce0-98fe-
  dwFlags            : 00000000 - 0 ()
  dwDescriptionLen   : 00000002 - 2
  szDescription      :
  algCrypt           : 00006610 - 26128 (CALG_AES_256)
  dwAlgCryptLen      : 00000100 - 256
  dwSaltLen          : 00000020 - 32
```

Command to decrypt the encrypted Secret Key

Use Mimikatz to decrypt the zoom secret Key

```
  pbHmackKey          :
  algHash             : 0000800e - 32782 (CALG_SHA_512)
  dwAlgHashLen        : 00000200 - 512
  dwHmac2KeyLen       : 00000020 - 32
  pbHmack2Key         : 9f6cb5b0318c4941e745ba69b9a90780520ecc02e08785df3da4c914
  dwDataLen           : 00000030 - 48
  pbData              : b7a030ea9b1c5beeeb1b11075445d5efb925b1ded4a6067d0165f74e
  dwSignLen           : 00000040 - 64
  pbSign              : f55230df479a052e289                    b74cd50515dd78ff
b537a85fab0d273

 * using CryptUnprotectData API
 * masterkey     : 9ea76e10f983a9e73a0eb742b581e3a77d9d82f8bec430649a98b926d09d
57a7f03c5c14
description :
data: 2b 4a 44 6b 69 59 51 52 64 59 41 62 44 35 32 74 67 50 51 57 4a 66 49 72 4
d
```

Decrypted Secret Key in Hex

Show the Decrypted Zoom Secret Key

```
0000000  2B 4A 44 6B 69 59 51 52 64 59 41 62 44 35 32 74   +JDkiYQRdYAbD52t
0000010  67 50 51 57 4A 66 49 72 43 79 58 44 4B 31 45 65   gPQWJfIrCyXDK1Ee
0000020  4C 61 4E 59 57 79 45 6A 75 58 6F 3D 00 00 00 00   LaNYWyEjuXo=....
```

Step 4: Decrypt Zoom Database file

Decrypt the Encrypted “Zoomus.enc.db” file to access the Database

```
┌──(root💀kali)-[/home/kali/Documents/sqlcipher]
└─# sqlcipher /home/kali/Documents/zoomus.enc.db
SQLite version 3.42.0 2023-05-16 12:36:15 (SQLCipher 4.5.5 community)
Enter ".help" for usage hints.
sqlite> PRAGMA key = '+JDkiYQRdYAbD52tqPQWJfIrCyXDKiEeLaNYWyEjuXo=';
ok
sqlite> PRAGMA kdf_iter = '4000';
sqlite> PRAGMA cipher_page_size= 1024;
sqlite>
```

Step 5: Extract Combined String

Extract combined string from the zoom_kv table

```
sqlite> SELECT * FROM zoom_kv;
```

Show the Base64 encoded and encrypted combined String

```
com.zoom.client.saved.meetingid.HhhhhN0kzycTgmq9cNya-K-tfAO-X-vn7CSTHCH7i-Y-.enc|gbfE5IKzmC1pUyRavQCa/oAz4yMQH9jWHftjfLlHM
4RBfJeyFzOkXrmnZWXK+qPr8wxt7Y5sN1tviV2791Nn/IkRflbt6trFmC4fLrvT1KipEqkGGgtGo1T5q2hVJYxo1zuVEBpVHyQRpqYT62wvSA==|ZoomChat
```

Step 6: Decrypt Combined String to find Zoom Meeting ID

Get secret key and Initial value pair to Decrypt String using Python script.

```
import hashlib

sid = b"S-1-5-21-1700811478-3337692859-4283507474-1001"

# Calculate the SHA-256 hash for the SID
key = hashlib.sha256(sid).digest()

# Hash the key itself
iv = hashlib.sha256(key).digest()

# Extract the first 16 bytes (128 bits) for the initialization vector (IV)
iv = iv[:16]

# Print the key and IV in hexadecimal format
print("Key:", " ".join(format(n, '02x') for n in key))
print("IV:", " ".join(format(n, '02x') for n in iv))
```

SID is the SID is of the User Marsha

1. Key: To find the Key for the AES Decryption, you calculate the SHA-256 hash of the SID
2. Initialization Vector(IV): First 16 bytes of the SHA256 of the resulting “Key”

Decode and Decrypt Combined string using Python script

```
/Users/newuser/PycharmProjects/pythonProject1/venv/bin/python /Users/newuser/Documents/CFYI/RA/reviewe
Key: 51 7d a8 c5 3c 8e e3 88 df c4 57 d0 5f c4 39 12 a8 a9 d7 5f 66 5f ed e3 50 85 60 c5 9d ad c1 12
IV: 78 33 4c 44 bd cd a4 e0 12 4b 04 30 c2 a6 27 d4
```

Decode and Decrypt Combined string using Python script

```python
# Input data
ciphertext_base64 = "gbfE5IKzmC1pUyRavQCa/oAz4yMQH9jWHftjfLlHM4RBfJeyFzC
key_hex = "517DA8C53C8EE388DFC457D05FC43912A8A9D75F665FEDE3508560C59DADC
iv_hex = "78334c44bdcda4e0124b0430c2a627d4"

# Decode the base64 encoded ciphertext
ciphertext = base64.b64decode(ciphertext_base64)

# Convert hexadecimal strings to bytes
key = bytes.fromhex(key_hex)
iv = bytes.fromhex(iv_hex)

# Create an AES cipher object
cipher = AES.new(key, AES.MODE_CBC, iv)

# Decrypt the ciphertext and remove padding
plaintext = unpad(cipher.decrypt(ciphertext), AES.block_size)

# Convert the plaintext to a string
plaintext_str = plaintext.decode('utf-8')

# Print the decrypted plaintext
print("Decrypted Text:", plaintext_str)
```

Encoded and encrypted Combined String

Decode Combined String

Decrypt Combined String

Zoom Personal Meeting ID

```
/Users/newuser/PycharmProjects/pythonProject1/venv/bin/python /Users/newuser/Documents/CFYI/RA/reviewed/AESsid.py
Decrypted Text: 956621847|Life has No Ctrl+Alt+Del - the Passcode is "4n6";81714328207|Marsha Mellos' Zoom Meeting;10000
```