

MCSC2024

Investigation Series



U_SH3LL

ကျွန်တော် MCSC တုန်းက Disk Forensics တွေကိုပြန်ဖြေပြီးတော့ writeup ပြန်ရေးပေးထားပါတယ်
ဒီseries တခုလုံးကို Autopsy နဲ့ဖြေရင်တောင်ရပါတယ်ဒါပေမယ့်တခြားtoolတွေသုံးရတာလဲရှိပါတယ်

Disk Image Download link –

<https://drive.google.com/file/d/1PsAd7GHtWwCpMJ9b-EXrvklaNfxbj82/view?usp=sharing>

1. Investigation I (Profile) (25)

Our forensics team captured the disk image from the suspicious host. Can you help us with the initial investigation steps? First, you need to find the computer name and product name.

Flag Format - MCSC2024{Computer Name_Product Name}

ဒီဟာကတော့ computer name နဲ့ product name ကိုရှာရမှာပါ အရင်ဆုံး disk image ကို autopsy ပေါ်တင်လိုက်ပါတယ် ပြီးရင် ကျွန်တော်က tryhackme မှာ windows forensics လုပ်တုန်းက cheatsheet ဖိုင်လေးကိုသုံးလိုက်ပါတယ် ဒီမှာပါ



အဲဒီ location အတိုင်း autopsy မှာရှာကြည့်လိုက်တဲ့အခါ flag ကိုရပါတယ်

The screenshot shows the Autopsy interface. On the left is a file tree with folders like 'Speech', 'System', 'System32', etc. The main pane displays a table of files in the path '/img_Capture.E01/vol6/Windows/System32/config'. The file 'COMPONENTS.LOG1' is highlighted in red. The right pane shows the 'ComputerName' registry value.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
SECURITY.LOG2				2019-12-07 15:33:44 MMT	2024-08-23 10:23:35 MMT	2019-12-07 15:33:44 MMT	2019-12-07
SOFTWARE				2024-08-22 21:58:04 MMT	2024-08-23 10:23:35 MMT	2024-08-22 21:58:04 MMT	2019-12-07
SOFTWARE.LOG1				2019-12-07 15:33:44 MMT	2024-08-23 10:23:34 MMT	2019-12-07 15:33:44 MMT	2019-12-07
SOFTWARE.LOG2				2019-12-07 15:33:44 MMT	2024-08-23 10:23:33 MMT	2019-12-07 15:33:44 MMT	2019-12-07
SYSTEM				2024-08-22 21:58:04 MMT	2024-08-23 10:23:35 MMT	2024-08-22 21:58:04 MMT	2019-12-07
SYSTEM.LOG1				2019-12-07 15:33:44 MMT	2024-08-23 10:23:34 MMT	2019-12-07 15:33:44 MMT	2019-12-07
SYSTEM.LOG2				2019-12-07 15:33:44 MMT	2024-08-23 10:23:35 MMT	2019-12-07 15:33:44 MMT	2019-12-07
COMPONENTS.LOG1				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00

The right pane shows the 'ComputerName' registry value:

Name	Type	Value
(Default)	REG_SZ	mnmsrvc
ComputerName	REG_SZ	DESKTOP-KMMA

The screenshot shows the Autopsy interface. On the left is a file tree with folders like 'CurrentVersion', 'Accessibility', 'AdaptiveDisplayBrightness', etc. The main pane displays a table of registry values in the path '/img_Capture.E01/vol6/Windows/System32/config'. The 'CurrentVersion' registry value is highlighted.

Name	Type	Value
CompositionEditionID	REG_SZ	Enterprise
CurrentBuild	REG_SZ	19045
CurrentBuildNumber	REG_SZ	19045
CurrentMajorVersionNumber	REG_DWORD	0x0000000a (10)
CurrentMinorVersionNumber	REG_DWORD	0x00000000 (0)
CurrentType	REG_SZ	Multiprocessor Free
CurrentVersion	REG_SZ	6.3
EditionID	REG_SZ	Professional
EditionSubManufacturer	REG_SZ	(value not set)
EditionSubstring	REG_SZ	(value not set)
EditionSubVersion	REG_SZ	(value not set)
InstallationType	REG_SZ	Client
InstallDate	REG_DWORD	0x66c73598 (1724331416)
ProductName	REG_SZ	Windows 10 Pro
Releaseld	REG_SZ	2009
SoftwareType	REG_SZ	System
UBR	REG_DWORD	0x00000edb (3803)
PathName	REG_SZ	C:\Windows

flag -> MCSC2024{DESKTOP-KMMA,Widnows 10 Pro}

2 Investigation II (User Activity) (25)

You need to find out who the owner of this laptop is.

Do you know when the owner tried to log in with an incorrect password?

If another user attempted to log in with an incorrect password, identify the time.

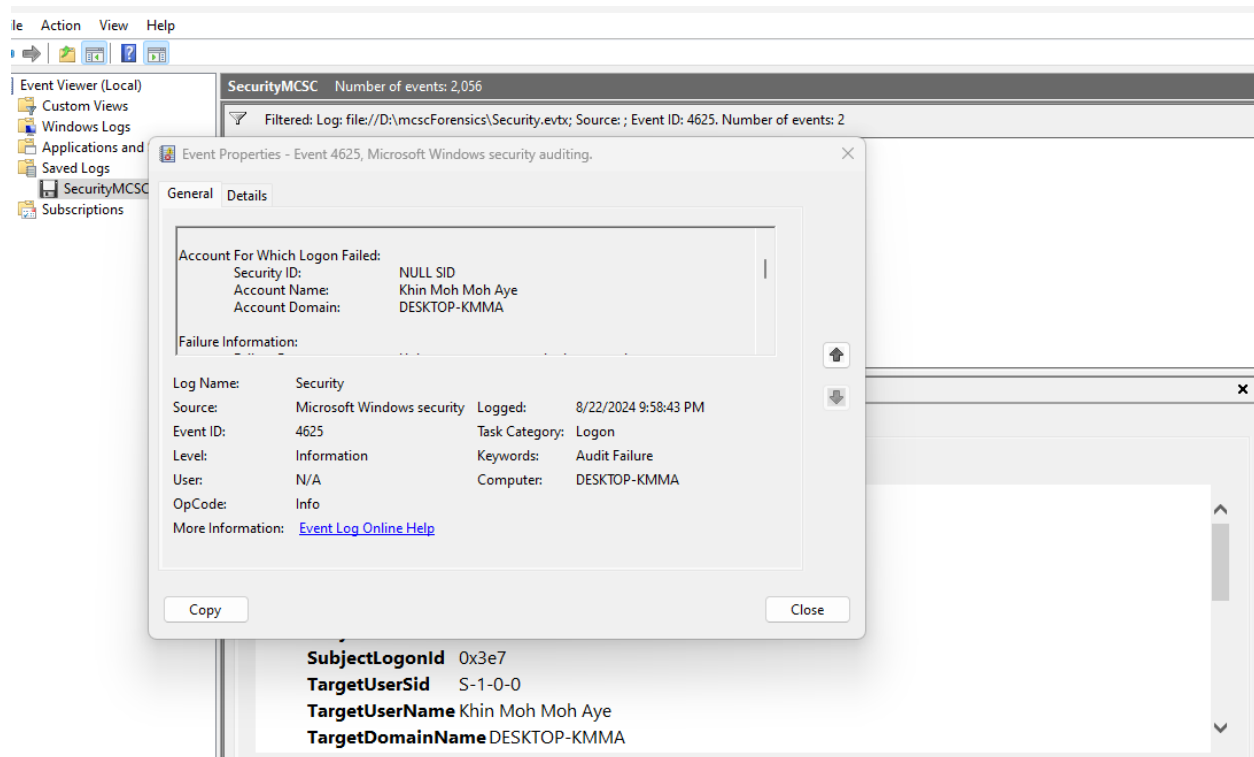
(Timezone is based on machine timezone)

Flag Format - MCSC2024{Mg Mg_2020-01-30 23:25:10_Ko Ko_2021-01-30 23:25:11}

ဒီမှာတော့ login failed ဖြစ်တဲ့ username နဲ့အချိန်ကိုမေးထားပါတယ် အဲ့တော့ ကျွန်တော် chatgpt ကိုမေးလိုက်ပါတယ် သူကဒီ path ထဲက security event file ကိုကြည့်ခိုင်းပါတယ်

C:\Windows\System32\winevt\Logs

အဲ့တော့ အဲ့နေရာကိုသွားပြီး Security.evtx ဖိုင်ကို extract လုပ်လိုက်ပါတယ် ပြီးရင် ကျွန်တော့်စက်ထဲက event viewer ကိုဖွင့်ပြီး import လုပ်လိုက်ပါတယ် ပြီးတဲ့အခါ login fail ဖြစ်တဲ့ event id 4625 ကို filter လုပ်ကြည့်တဲ့အခါမှာ event နှစ်ခုကိုတွေ့ရပါတယ်



flag ->

MCSC2024{Khin Moh Moh Aye_2024-08-22 15:28:43_BayLuWa_2024-08-22 15:37:56}

|

MCSC2024{BayLuWa_2024-08-22 15:37:56_Khin Moh Moh Aye_2024-08-22 15:28:43}

Event နှစ်ခုဖြစ်တဲ့အတွက် ဘယ်တခုက ရှေ့လဲနောက်လဲသေချာမသိပါဘူး

3 Investigation III (Network) (25)

Please find the device's IP address and gateway IP address.

Flag Format - MCSC2024{1.1.1.3_1.1.1.1}

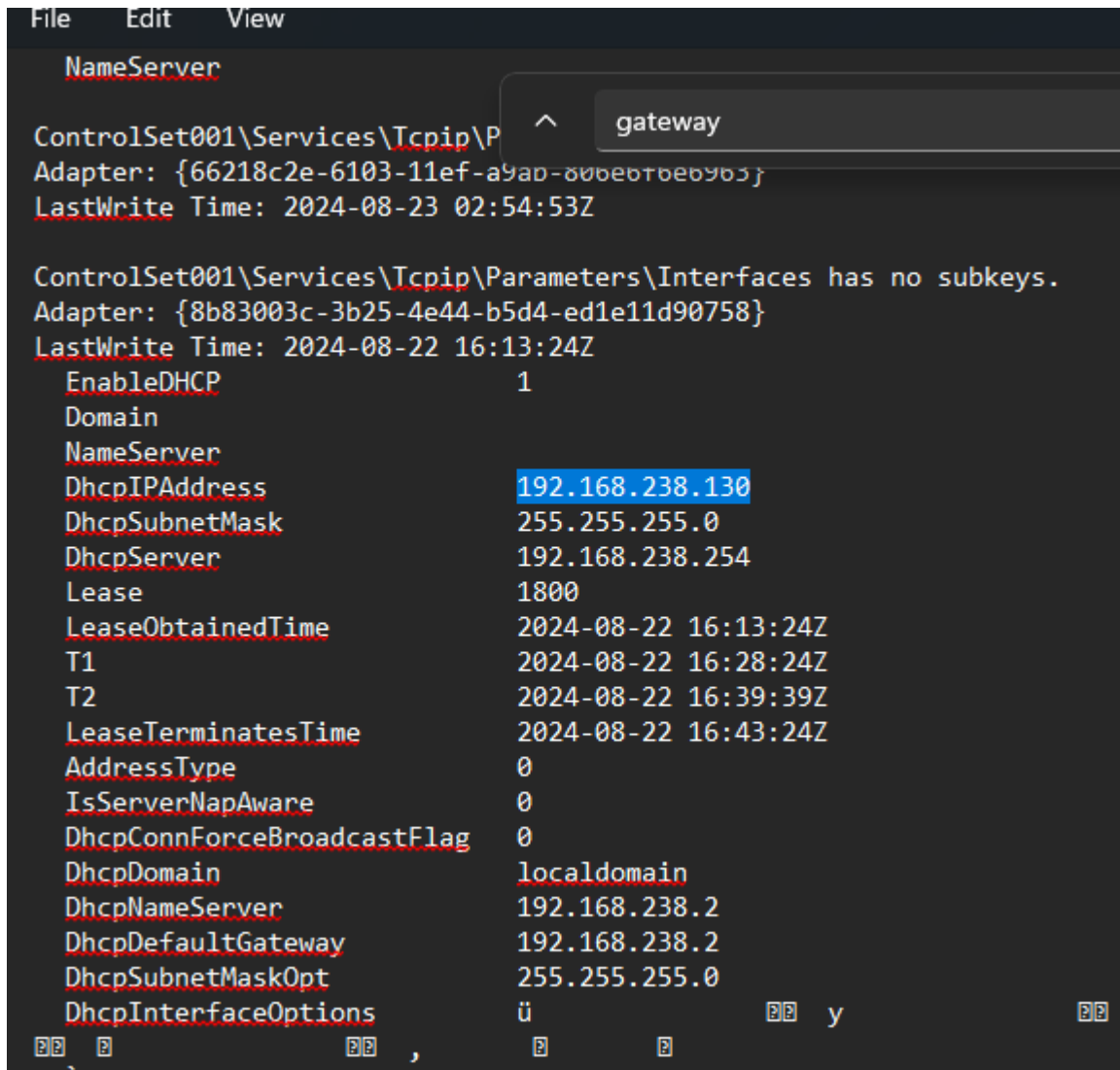
ဒီတခုအတွက်လဲ tryhackme cheatsheetကိုသုံးခဲ့ပါတယ်

Network Interfaces and Past Networks:
SYSTEM\CurrentControlSet\Services\Tcpip
\Parameters\Interfaces

သူပြောတဲ့ path အတိုင်း autopsy မှာလဲကြည့်လို့ရပါတယ် ကျွန်တော်က

C:\Windows\System32\config\SYSTEM registry hive ကိုdump လိုက်ပါတယ် ပြီးတဲ့အခါ

RegRipper tool ကိုသုံးပြီး data တွေယူလိုက်ပါတယ်အဲ့ထဲကမှ Ip and Gateway ကို filter
လုပ်လိုက်ရင် flag ရပါပြီ



```
File Edit View
NameServer
ControlSet001\Services\Tcpip\Parameters\Interfaces\{66218c2e-6103-11ef-a9ad-80bbeb7beb9b5}
Adapter: {66218c2e-6103-11ef-a9ad-80bbeb7beb9b5}
LastWrite Time: 2024-08-23 02:54:53Z

ControlSet001\Services\Tcpip\Parameters\Interfaces\{8b83003c-3b25-4e44-b5d4-ed1e11d90758}
Adapter: {8b83003c-3b25-4e44-b5d4-ed1e11d90758}
LastWrite Time: 2024-08-22 16:13:24Z
  EnableDHCP 1
  Domain
  NameServer
  DhcpIPAddress 192.168.238.130
  DhcpSubnetMask 255.255.255.0
  DhcpServer 192.168.238.254
  Lease 1800
  LeaseObtainedTime 2024-08-22 16:13:24Z
  T1 2024-08-22 16:28:24Z
  T2 2024-08-22 16:39:39Z
  LeaseTerminatesTime 2024-08-22 16:43:24Z
  AddressType 0
  IsServerNapAware 0
  DhcpConnForceBroadcastFlag 0
  DhcpDomain localdomain
  DhcpNameServer 192.168.238.2
  DhcpDefaultGateway 192.168.238.2
  DhcpSubnetMaskOpt 255.255.255.0
  DhcpInterfaceOptions ü y
```

flag -> MCSC2024{192.168.238.130_192.168.238.2}

4 Investigation IV (Music) (25)

We think the owner likes to listen to music. Can you find the name of the last Myanmar song and the last English song she listened to?

Flag Format - MCSC2024{The last myanmar song_The last english song}

ဒီတခုအတွက်တော့ ကျွန်တော် autopsy မှာ Web History ဆိုပြီးသက်သက်ပြပေးတဲ့ နေရာရှိပါတယ် အဲမှာ user က သူနားထောင်ချင်တဲ့သီချင်းတွေကို youtube မှာ search လုပ်ထားတာကိုတွေ့မိပါတယ် သီချင်းတွေကလဲများပါတယ် ဒါမယ့် သူက last song ဆိုတော့ အချိန်နဲ့တွဲကြည့်လိုက်တဲ့အခါ song နှစ်ခုတွေ့ပါတယ်

History		0	https://www.youtube.com/watch?v=wKn7fhFW3Ms	2024-08-22 21:04:51 MMT	https://
History		0	https://www.youtube.com/	2024-08-22 21:05:16 MMT	https://
History		0	https://www.youtube.com/results?search_query=top...	2024-08-22 21:05:54 MMT	https://
History		0	https://www.youtube.com/watch?v=JMWQXWQdQMg	2024-08-22 21:05:58 MMT	https://
History		0	https://www.youtube.com/watch?v=5ykFSOdqSC4	2024-08-22 21:06:25 MMT	https://
History		0	https://www.youtube.com/watch?v=lnWse7McFsk	2024-08-22 21:06:57 MMT	https://

Hex	Text	Application	Source File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other O
Result: 145 of 205 Result < >									
Visit Details									
Title:	Cuddle - Yung Hugo Feat. GRACEe [Lyrics] - YouTube								
Username:	Default								
Date Accessed:	2024-08-22 21:04:51 MMT								
Domain:	youtube.com								
URI:	https://www.youtube.com/watch?v=wKn7fhFW3Ms								

Source Name	S	C	O	URL	Date Accessed	Referrer URL
History			0	https://www.youtube.com/	2024-08-22 21:05:54 MMT	https://www.youtube.com/
History			0	https://www.youtube.com/results?search_query=top...	2024-08-22 21:05:54 MMT	https://www.youtube.com/results?search...
History			0	https://www.youtube.com/watch?v=JMWQXWQdQMg	2024-08-22 21:05:58 MMT	https://www.youtube.com/watch?v=JMW...
History			0	https://www.youtube.com/watch?v=5ykFSOdqSC4	2024-08-22 21:06:25 MMT	https://www.youtube.com/watch?v=5yk...
History			0	https://www.youtube.com/watch?v=lnWse7McFsk	2024-08-22 21:06:57 MMT	https://www.youtube.com/watch?v=lnW...
History			0	https://www.youtube.com/results?search_query=thee	2024-08-22 21:08:08 MMT	https://www.youtube.com/results?search...
History			0	https://www.youtube.com/watch?v=OdxSbc0ap-s	2024-08-22 21:08:23 MMT	https://www.youtube.com/watch?v=Odx...
History			0	https://www.youtube.com/results?search_query=whit...	2024-08-22 21:10:55 MMT	https://www.youtube.com/results?search...

Hex	Text	Application	Source File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
-----	------	-------------	----------------------	------------	----------------	------------------	---------	-------------	-------------------

Result: 152 of 205	Result	←	→
--------------------	--------	---	---

Visit Details	
Title:	Megan Thee Stallion - Mamushi (feat. Yuki Chiba) [Official Video] - YouTube
Username:	Default
Date Accessed:	2024-08-22 21:08:23 MMT
Domain:	youtube.com
URL:	https://www.youtube.com/watch?v=OdxSbc0ap-s
Referrer URL:	https://www.youtube.com/watch?v=OdxSbc0ap-s
Program Name:	Microsoft Edge
Source	
Host:	Capture.E01_1 Host

ဒီနေရာမှာ Megan Thee Stallion ကို ကျွန်တော်က သိချင်းနာမည်ပဲမှတ်တာ youtubeမှာရှာကြည့်မှ Mamushi က သိချင်းနာမည်ဖြစ်တယ် :3

Flag -> MCSC2024{Cuddle_Mamushi}

5 Investigation V (Background) (25)

You have to find the current Desktop Background Photo.

If you find it, you will get the flag.

Flag Format - MCSC2024{flag}

ဒီအပုဒ်ဖြေဖို့လဲ chatgpt ကိုသုံးခဲ့ပါတယ် ဒါမယ့်နည်းနည်းကြာသွားတယ် possible paths တွေများလို့

C:\Users\Khin Moh Moh

Aye\AppData\Roaming\Microsoft\Windows\Themes\TranscodedWallpaper

Flag picture ကဒီ path မှာရှိတာပါ အုတိုင်းသွားကြည့်တဲ့အခါ နိုင်လှပုံနဲ့ flag ကိုရရှိပါတယ် :3

Listing

/img_Capture.E01/vol_vol6/Users/Khin Moh Moh Aye/AppData/Roaming/Microsoft/Windows/Themes

5 Res

Table Thumbnail Summary


Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
[current folder]				2024-08-22 20:21:32 MMT	2024-08-22 20:21:32 MMT	2024-08-22 21:50:34 MMT	2024-08-22 19:42:29 MMT	704
[parent folder]				2024-08-22 19:42:29 MMT	2024-08-22 19:42:29 MMT	2024-08-22 21:51:26 MMT	2024-08-22 19:41:52 MMT	56
CachedFiles				2024-08-22 22:35:34 MMT	2024-08-22 22:35:34 MMT	2024-08-22 22:36:49 MMT	2024-08-22 22:35:34 MMT	304
slideshow.ini				2024-08-22 20:21:27 MMT	2024-08-22 20:21:27 MMT	2024-08-22 20:21:27 MMT	2024-08-22 20:21:27 MMT	0
TranscodedWallpaper			0	2024-08-22 20:21:27 MMT	2024-08-22 20:21:27 MMT	2024-08-22 22:35:33 MMT	2024-08-22 19:42:29 MMT	88589

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

0° 100% Reset

Tags Mer



Flag -> MCSC2024{y0u_f0uNd_h3R_l0v3R}

တခြား possible paths တွေရှိပါသေးတယ် ကိုယ့်ကိုဖြေရင်းနဲ့မှ ရှာကြည့်ကြပေါ့

6 Investigation VI (Confidential) (25)

Do you know the childhood nickname of Khin Moh Moh Aye and her pet's first name?

Flag Format - MCSC2024{Phyu Phyu_Ag Net}

ဒီအပိုဒ်က ကျွန်တော် ရှေ့ကအပိုဒ်ဖြေနေရင်းနဲ့ရပြီးသားပါ ရှာကြံရင်းနဲ့ တွေ့လိုက်တာ

Name	S	C	O	Modified Time
NTUSER.DAT			0	2024-08-22 21:58:01 MMT
ntuser.dat.LOG1			0	2024-08-22 19:41:52 MMT
ntuser.dat.LOG2			0	2024-08-22 19:41:52 MMT
NTUSER.DAT{53b39e88-18c4-11ea-a811-000d3aa46f}			0	2024-08-22 19:42:22 MMT
NTUSER.DAT{53b39e88-18c4-11ea-a811-000d3aa46f}			0	2024-08-22 19:41:52 MMT
NTUSER.DAT{53b39e88-18c4-11ea-a811-000d3aa46f}			0	2024-08-22 19:41:52 MMT
ntuser.ini			0	2024-08-22 19:41:52 MMT

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations
Capture.E01_1 Host Details								
Last Login:		2024-08-22 22:35:32 MMT						
Login Count:		6						
Security Question 1:		What was your first pet's name?						
Security Answer 1:		Ba Sai						
Security Question 2:		What was your childhood nickname?						
Security Answer 2:		Pan Nu Thway						
Security Question 2:		What's the name of the first school you attended?						
Security Answer 3:		Dagon 1						
Password Fail Date:		2024-08-22 21:58:43 MMT						
Password Settings:		Password does not expire, Password not required						
Flag:		Normal user account						
Home Directory:		C:/Users/Khin Moh Moh Aye						

Analyzing files from

ကျွန်တော်ထင်တာတော့ disk image စ importတည်းက moduleတချို့runထားပြီးသားမို့ ပေါ်တာနေမယ် Capture.E01 ကိုနှိပ်လိုက်ပြီး အောက်နားက OS Account ဆိုတဲ့ tab မှာflag ကိုတွေ့တာပါ

Flag -> MCSC2024{Pan Nu Thway_Ba Sai}

7 Investigation VII (Private Information) (100)

Do you know the email and password of the device owner?

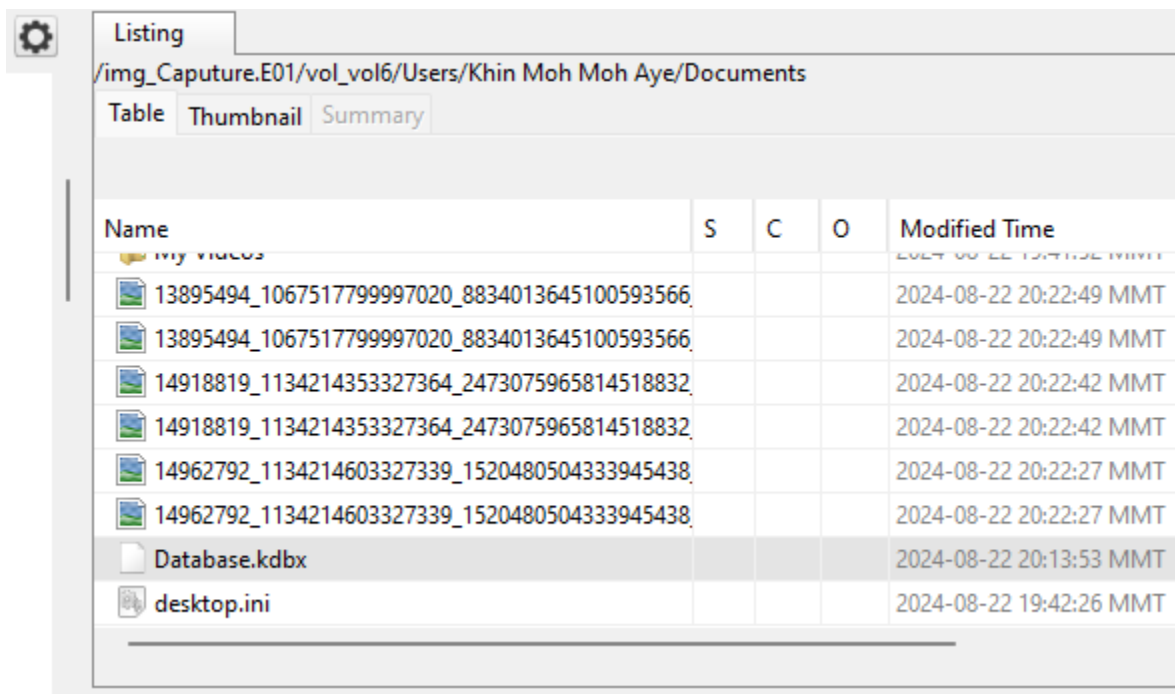
Flag Format - MCSC2024{mama@gmail.com_password}

ဒီအပုဒ်ကတော့ အခက်ဆုံးမို့ 100 ပေးထားတာလားမသိဘူး ကျွန်တော့်အတွက်ကတော့လွယ်တယ် :3

ကျွန်တော် ဟိုကြည့်ဒီကြည့်ရင်းနဲ့ keepass programကို installထားတာ sus ဖြစ်မိပါတယ်

အဲ့တော့ရှေ့ပိုင်းတွေမှာ ကျွန်တော် analysis လုပ်ရင်းနဲ့

Documents folder ထဲမှာ Database.kdbx ဆိုတဲ့ဖိုင်တခုတွေ့ပါတယ်



Listing				
/img_Capture.E01/vol_vol6/Users/Khin Moh Moh Aye/Documents				
Table	Thumbnail	Summary		
Name	S	C	O	Modified Time
my videos				2024-08-22 13:41:52 MMT
13895494_1067517799997020_8834013645100593566				2024-08-22 20:22:49 MMT
13895494_1067517799997020_8834013645100593566				2024-08-22 20:22:49 MMT
14918819_1134214353327364_2473075965814518832				2024-08-22 20:22:42 MMT
14918819_1134214353327364_2473075965814518832				2024-08-22 20:22:42 MMT
14962792_1134214603327339_1520480504333945438				2024-08-22 20:22:27 MMT
14962792_1134214603327339_1520480504333945438				2024-08-22 20:22:27 MMT
Database.kdbx				2024-08-22 20:13:53 MMT
desktop.ini				2024-08-22 19:42:26 MMT

kdbx ဆိုတာ keepass db file ပါ အချိန်မှာ Challenge creatorနဲ့စကားပြောမိရင်းသူက keepass ကို bruteforce လုပ်ရမယ်လို့ပြောတော့(ဟင့်မတောင်းပါဘူး သူ့ဘာသာပေးသွားတာ:3) ကျွန်တော် keepass2john နဲ့ kdbx ကို crackable format ပြောင်းကြည့်တယ် ဒါပေမယ့်အဆင်မပြေဘူးဗျ version မကိုက်နေတာ အဲ့တာနဲ့ keepass bruteforce tool လိုက်ရှာကြည့်ရင်း ဒီtoolကိုတွေ့ပါတယ်

<https://github.com/r3nt0n/keepass4brute>

ဒီကောင်ကိုပြောင်းသုံးကြည့်တော့ အဆင်ပြေသွားပါတယ် wordlist ကတော့ the greatest rockyou
ပဲပေါ့ password ကလဲ rockyou ဆိုပြီးတွေ့ပါတယ် အဲ့တာနဲ့ keepass programကိုဒေါင်းပြီး ခုနက
kdbx ဖိုင်ကိုဖွင့်ကြည့်တဲ့အခါ email and password ရရှိပါတယ်

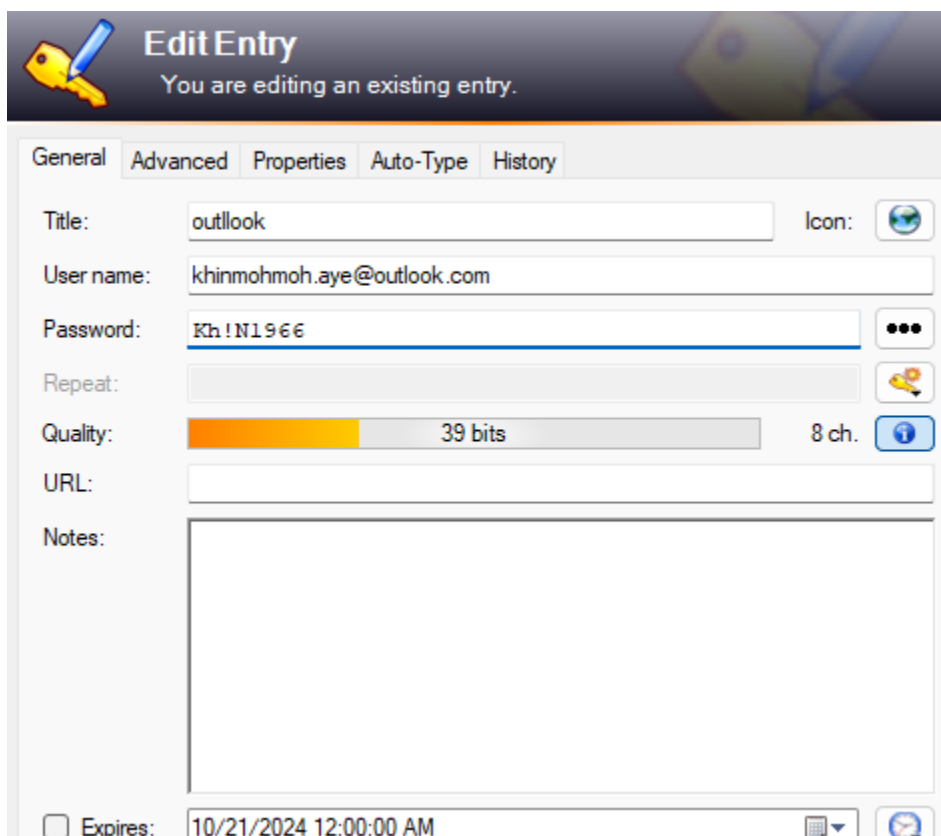
```
(kali㉿kali)-[~/Desktop/keepass4brute]
$ ./keepass4brute.sh ../Database.kdbx /usr/share/wordlists/rockyou.txt
keepass4brute 1.3 by r3nt0n
https://github.com/r3nt0n/keepass4brute

[+] Words tested: 8/14344392 - Attempts per minute: 240 - Estimated time remaining: 10m24s
[+] Current attempt: rockyou

[*] Password found: rockyou

(kali㉿kali)-[~/Desktop/keepass4brute]
$

(kali㉿kali)-[~/Desktop/keepass4brute]
$
```



P.S creator ပြောတာက kbdx password ကအဲ့ထဲမှာပဲရှိတယ် bruteforce
တိုက်လဲရတယ်လို့ပြောပါတယ် ကျွန်တော်က ရှာရင်ကြာနေမှာစိုးလို့ bruteforce ပဲရွေးလိုက်ပါတယ်
တကယ်လို့ လိုက်ဖြေကြည့်ရင် rockyou ဆိုတဲ့ password တွေရင်ကျွန်တော့်ကိုလာပြောပြပါအုံး

Flag -> MCSC2024{khinmohmoh.aye@outlook.com_Kh!N1966}

8 Investigation VIII (Bonus) (50)

After getting the email password, find the user's password and discord username.

Password is almost same as email password. (eg. password - m1N7hU >> M!nThU)

Flag Format - MCSC2024{userpassword_discordusername}

ဒီအပုဒ်ကနည်းနည်းတော့စားပေမယ့် မိုက်ပါတယ် ရှေ့မှာ email passwordရခဲ့ပြီဆိုတော့ window
user password ကိုထပ်ရှာခိုင်းပါတယ် အဲဒါမှာ almost same ဆိုပြီး format
နည်းနည်းလေးကွာတာကိုပြထားပါတယ်

m1N7hU >> M!nThU

! -> 1 , capital letter -> small letter စသဖြင့်ပေါ့

အဲ့တော့ ကျွန်တော် chatgpt သုံးပြီး possible wordlist ထုတ်လိုက်ပါတယ်

32 လုံးလားမသိထွက်လာတယ် အိုကေ password list တော့ရပြီ bruteforce တိုက်ဖို့ hash
လိုပါတယ် အဲ့တော့ mimikatz ကိုသုံးပြီး SAM ထဲကနေ NTLM hash ကိုထုတ်လိုက်ပါတယ်

```
zerologon
postzerologon

mimikatz # lsadump::sam /system:D:\mcscForensics\SYSTEM /sam:D:\mcscForensics\SAM
Domain : DESKTOP-KMMA
```

ဒါကတော့ mimikatz ထဲမှာသုံးတဲ့ command ပါ

lsadump::sam /system:YourSYSTEMhive /sam:YourSAMhive

SYSTEM နဲ့ SAM ကတော့ C:\\Windows\\System32\\config ထဲမှာရှိပါတယ်
ကျွန်တော်ကအစတည်းက autopsy ကနေ extract လုပ်ထားပြီးသားပါ

```
* Packages *
  NTLM-Strong-NTOWF

* Primary:Kerberos *
  Default Salt : WDAGUtilityAccount
  Credentials
    des_cbc_md5      : 4fea8a10df585d61

RID : 000003e9 (1001)
User : Khin Moh Moh Aye
Hash NTLM: 1f0c3715e39684c6fd81a9d3244f7111

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
  Random Value : cc224fc3f664d9dd1804a37eadea14dc

* Primary:Kerberos-Newer-Keys *
  Default Salt : DESKTOP-47HHGHMKhin Moh Moh Aye
  Default Iterations : 4096
  Credentials
    aes256_hmac      (4096) : 1ac889775a4ba89843b225a422922ddd30a9b200b7737c1b9e7dfc06
    aes128_hmac      (4096) : 24713b9382306955ec9a8574794e01f1
    des_cbc_md5      (4096) : 20da2557e34532d9
  OldCredentials
    aes256_hmac      (4096) : 1ac889775a4ba89843b225a422922ddd30a9b200b7737c1b9e7dfc06
    aes128_hmac      (4096) : 24713b9382306955ec9a8574794e01f1
    des_cbc_md5      (4096) : 20da2557e34532d9

* Packages *
  NTLM-Strong-NTOWF

* Primary:Kerberos *
```

NTLM hash ကို file ထဲသိမ်းပြီး john နဲ့ ခုနက wordlist ကိုသုံးပြီး crack လိုက်တဲ့အခါ user's
password ကိုရပါတယ်

```
$ nano khin.txt

(kali㉿kali)-[~/Desktop]
$ john --format=NT hash.txt -w=khin.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 128/128 SSE2 4x3])
Warning: no OpenMP support for this hash type, consider
Press 'q' or Ctrl-C to abort, almost any other key for s
kH1n1966      (?)
1g 0:00:00:00 DONE (2024-10-20 21:13) 11.11g/s 355.5p/s
Use the "--show --format=NT" options to display all of t
Session completed.

(kali㉿kali)-[~/Desktop]
$
```

Ok user password တော့ရပြီ discord username ရှာဖို့ကျန်ပါသေးတယ် ဒီဟာကလွယ်ပါတယ်

C:\\Users\\Khin Moh Moh Aye\\AppData\\Roaming\\discord

ထဲမှာ usercachedata.json ရှိပါတယ် အဲ့ဒါမှာ Ctrl+f နဲ့ username ရှာကြည့်တဲ့အခါ

flagရပါတယ် ပုံမှန် dc username က # sign ပါတာဆိုတော့ မသေချာလို့

နောက်တဖိုင်မှာထပ်ရှာကြည့်တော့လဲ ဒီအဖြေပဲရပါတယ် ဘယ်ဖိုင်လဲမမှတ်မိတော့လို့

ပဲထည့်ပေးလိုက်ပါတယ်

```
DataCache.json X
cscForensics > user\\data\\cache\\json > MultiAccountStore

> username Aa ab_* 1 of 2

{"GameDisplayModeStorage":{"games":{}}, "RTCRegionStore":{"_state":{"preferredRegions":["singapore","hongkong","india","dubai"], "lastGeoRankedOrder":["singapore","hongkong","india","japan","dubai"], "lastTestTimestamp":1724333638109}, "_version":1}, "email_cache":"khinmohmoh.aye@outlook.com", "MultiAccountStore":{"_state":{"users":[{"id":"12761686419", "avatar":null, "username":"khinmoh1966_73524", "discriminator":"0", "tokenStatus":2, "pushSyncToken":null}], "canUseMultiAccountMobile":false}, "_version":1}, "SelectivelySyncedUserSettingsStore":{"_state":{}, "_version":2}, "SelectedGuildStore":{"_state":{"selectedGuildTimestampMillis":{}, "selectedGuildId":null, "lastSelectedGuildId":null}, "_v", "DefaultProfileStore":{"_state":{"lastVisitedPath":null}, "_version":1}, "ApplicationEngage":{"_state":{"pendingTraces":{
```

