The Return of the Yeti

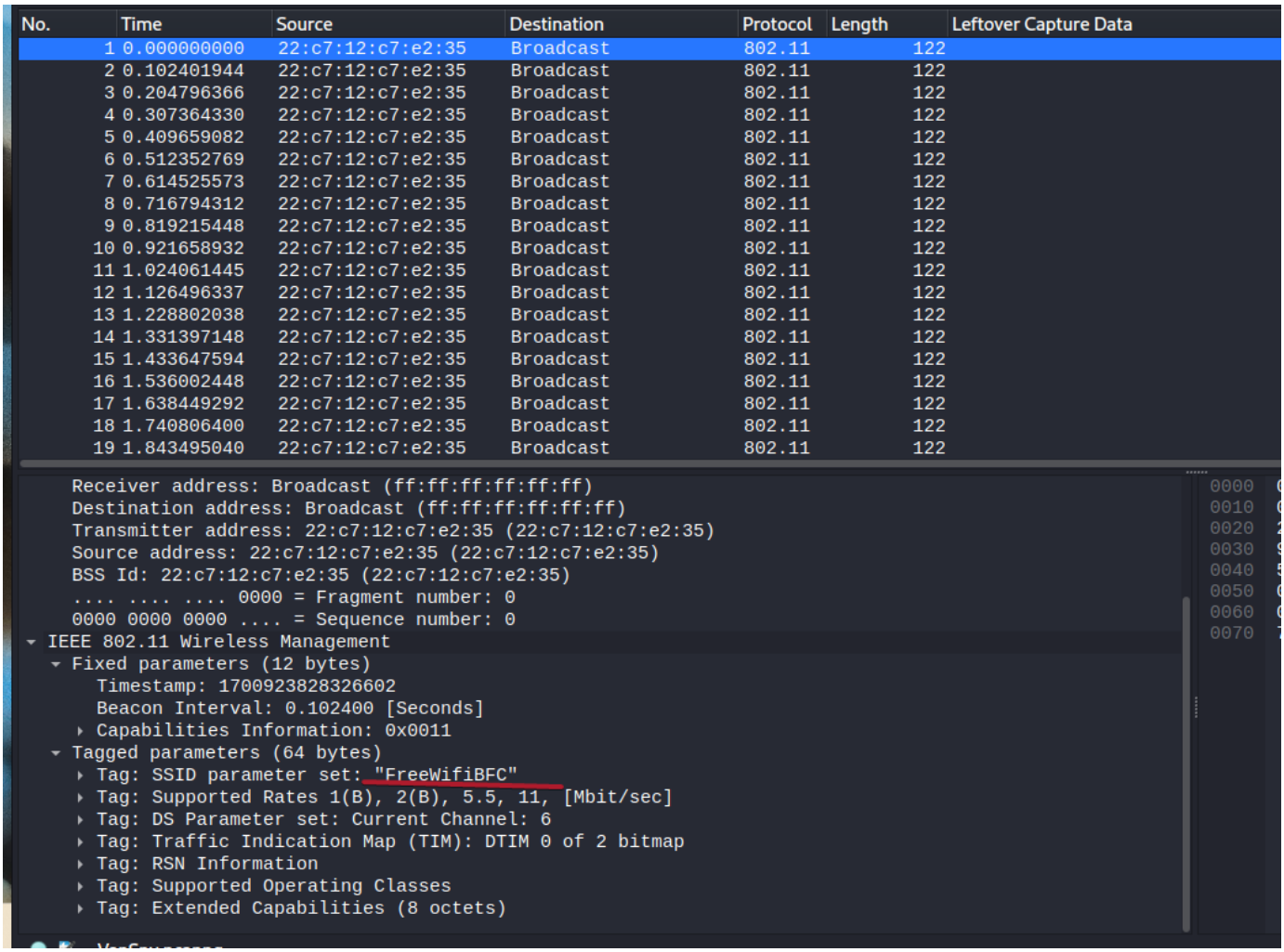
The Return of the Yeti

https://tryhackme.com/room/adv3nt0fdbopsjcap

WiFi hack

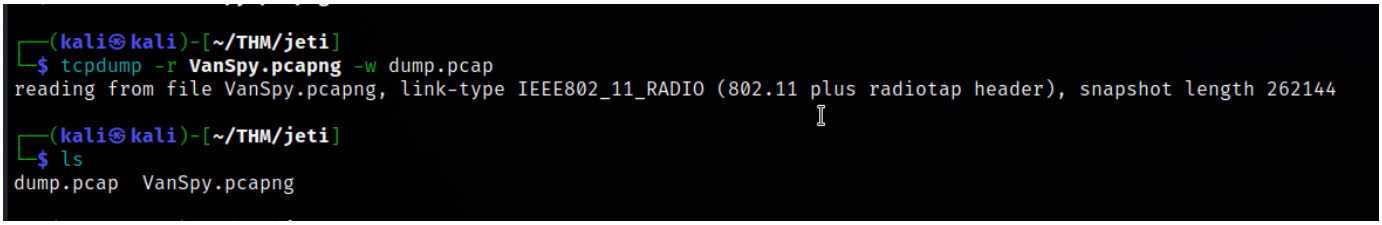
Download zip file, unzip and opend with wireshark

The wi-fi network is in tagget paramtrs



Dump data

`tcpdump -r VanSpy.pcapng -w dump.pcap`



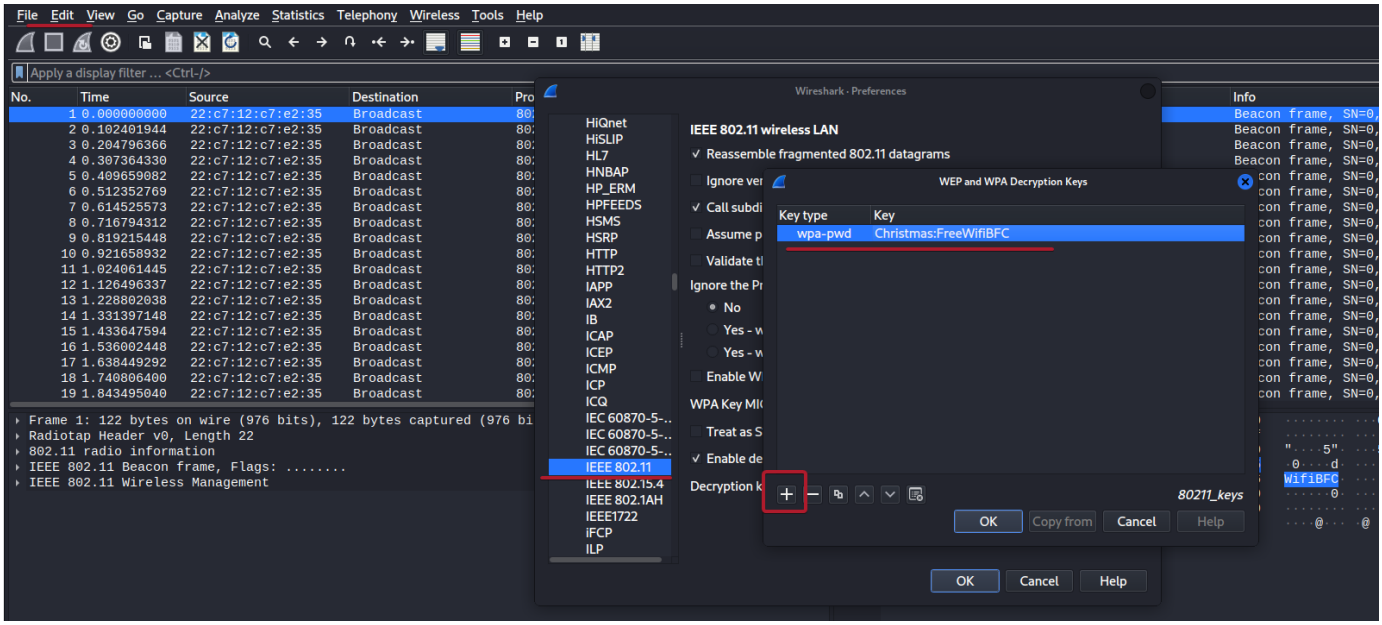
Crack password

`aircrack-ng -z dump.pcap -w /home/kali/Desktop/rockyou.txt`

```
                    Aircrack-ng 1.7

  [00:00:05] 31925/14344392 keys tested (6805.99 k/s)

  Time left: 35 minutes, 2 seconds                          0.22%

                     KEY FOUND! [ Christmas ]


  Master Key     : A8 3F 1D 1D 1D 1F 2D 06 8E D4 47 CE E9 FD 3A AA
                   B2 86 42 89 FA F8 49 93 D7 C1 A0 29 97 3D 44 9F

  Transient Key  : 77 1D BE 72 52 FD FF 30 4D 54 0A 82 D9 83 87 F1
                   10 AC 7B 70 B9 BF 9E D8 22 D8 C4 24 08 B5 BB EB
                   DD F2 C2 F4 2A 27 AA 24 81 FA 38 12 C3 42 F1 B3
                   12 0C E1 16 71 4F D1 90 1C 7B 0F AF CE 67 29 02

  EAPOL HMAC     : C1 0A 70 D9 65 94 5B 57 F2 98 8A E0 FC FD 2B 22


┌──(kali㉿kali)-[~/THM/jeti]
└─$
```

Christmas

Back to wireshark and add key



Filter to tcp and here a lot of packets, some looks like RDP but they encrypted. Last tcp packets have normal plaitext, and it is malicious job history)) Someone used mimikatz!!!

```
  .#####.   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(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # token::elevate
Token Id  : 0
User name :
SID name  : NT AUTHORITY\SYSTEM

496      {0;000003e7} 1 D 16529            NT AUTHORITY\SYSTEM       S-1-5-18 (04g,21p)        Primary
 -> Impersonated !
 * Process Token : {0;0002bbfa} 2 D 25564822         INTERN-PC\Administrator    S-1-5-21-1966530601-3185510712-10604624-500 (14g,24p)        Primary
 * Thread Token  : {0;000003e7} 1 D 25609341         NT AUTHORITY\SYSTEM        S-1-5-18 (04g,21p)        Impersonation (Delegation)

mimikatz(commandline) # crypto::capi
Local CryptoAPI RSA CSP patched
Local CryptoAPI DSS CSP patched

mimikatz(commandline) # crypto::certificates /systemstore:LOCAL_MACHINE /store:"Remote Desktop" /export
 * System Store  : 'LOCAL_MACHINE' (0x00020000)
 * Store         : 'Remote Desktop'

 0. INTERN-PC
    Subject  : CN=INTERN-PC
    Issuer   : CN=INTERN-PC
    Serial   : ffb1d93a1df0324cadd5e13f3f9f1b51
    Algorithm: 1.2.840.113549.1.1.1 (RSA)
    Validity : 11/22/2023 9:18:19 PM -> 5/23/2024 9:18:19 PM
    Hash SHA1: a0168513fd57577ecc0204f01441a3bd5401ada7
         Key Container  : TSSecKeySet1
```

In the end is something like id_rsa , but .pfx extension and base64 encoded

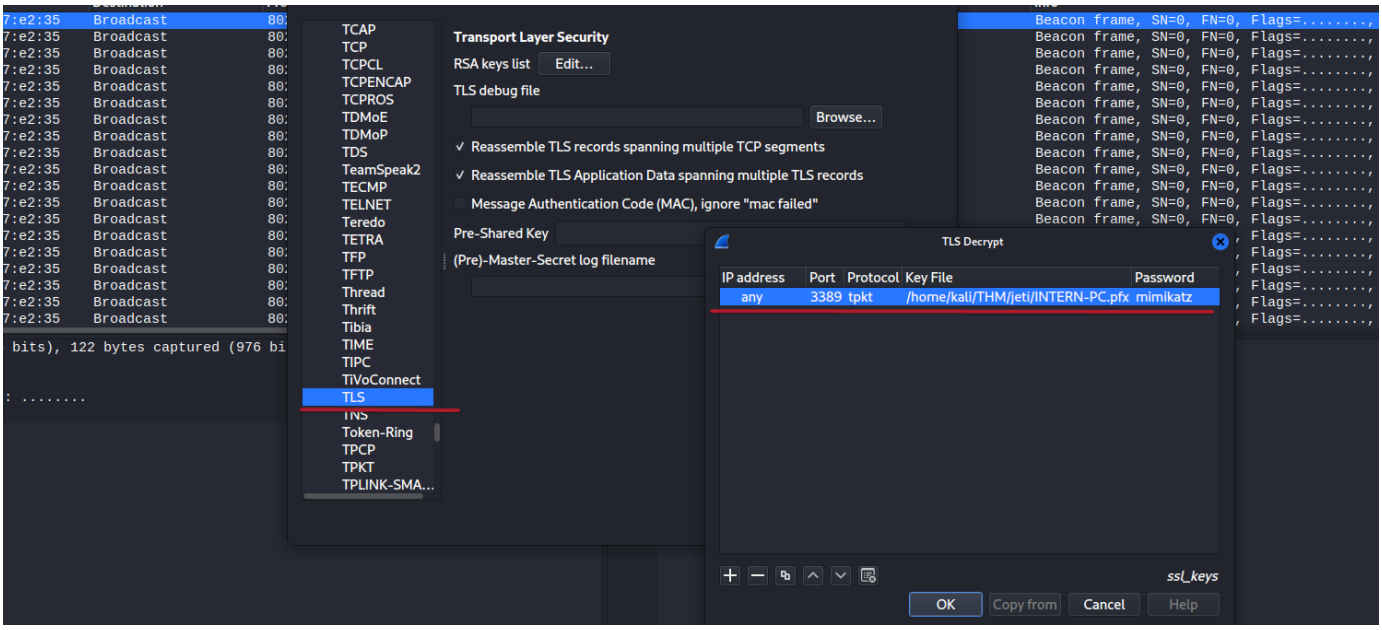
```
PS C:\Users\Administrator> [Convert]::ToBase64String([IO.File]::ReadAllBytes("/users/administrator/LOCAL_MACHINE_Remote Desktop_0_INTERN-PC.pfx"))
MIIJuQIBAzCCCXUGCSqGSIb3DQEHAaCCCWYEgglmMIIJXjCCBecGCSqGSIb3DQEHAaCCBdgEggXUMIIF0DCCBcwGCyqGSIb3DQEMCgECoIIE/
jCCBPowHAYKKoZIhvcNAQwBAzAOBAiAw9dZ0qgvUQICB9AEggTYbMKna0YqJ1eN3FGKKUtsoCZAJ8KzbSKMBc86sCZdUBLsTq8Z4sWnFgQitLtXIrDnioaC9N6akgG8x8uLLUndmTreNAfQRcLiALGJoKf79rgQ6I4Bh6FzphNjuwCLzaqNiknSBWqJRZ7N+/
G76H9jLWqNIfxrMdtAL9dLfbj8Zb7n8rwUIb5Wd3hrzowk9trlPnShkuzyyvASFIONLc1r/K2c8c6LqpucsdDb8A7LqM8uNd3P8sE8RW+/
qDs92mOW6iR1jEEGAOGlkIKbdLFBXdR6XraK8iDHygxcHKbM02/3Nh5BOm3C0JTKTlT32Yhxr9fR6ZMdvDOIs+Hv0bj2CWXwGFD8yderiRn67cEvhGvbPqqsncqfk+6LpmjwFOGo8xwmhNN15vS/
JtooJ0EWAevjEJmbRsoiJPVFa4wqsEZkGeUMwElL3xT1Nf06J57n4ptiH9syCoyVCQoJU9QgDiIEMKBKq6oD6BJFrW34io7Z+f2ihS9HzWZxP3keYvilPvetaYn5mMhWdrIUlT8ZoAn+4XaYXOH0IgThmxwKYacENbX/y/
QGTwNU9UMxI0nGTTSFWjafi6CkREmSw2IExwlAYD9Unswj93cOHRvZdSsxcyD22Qw51t62Leb00hrGJILDMIwXqiFZAtp4rq/M/
J8pcwgS5oj0YT8TSEkNPSwFdTew+AcDmzD7rP6GVvexgxTd37WdrQBCMK3e1ekEDM1FhcE0HtpuT5c9y2IOtsgkSCiI6nX+OE0lgf9onpAP2PCnJv8CJf7Jl5vdTskRG71sOa/
ZRIx2QNcbpe5fmmfpxiNatky+BtFpcqEoUCXZXXIPav0B1umhQ7JDWSkGaJpCHYmCgvtqETJMNIt6K5/WXhYcP2/viB1n/JFwFyZes5E6rxc7XtRDc/
J2n7HduYRv2iSlNxkGKFkiTDyeKCextO5l74ZFvNepaFtTZGl4OJgYPYTrDATYK3BJosVQuNhPO5ojwdkfhyQz2HEzAfWUcoQemdeNuC30JeCMTrgZ5fg/Hn529BCObGCotkR9FfCLSDnJJv/R9VOaB+RMtb5B7ngPGSsCr9MEZa0kXAzZdDF9/
eebYYtOwsj6qLrxcgxgX69kVYtdJQYSP8Nzof8ybdn2bSI58E44OQkODUPk/
ZY2K7AVO6Mresb08+2l9vA0Pkgc1+Q4PXil28hxGR5QrHjPruafppzzwixBwaXDYdiuDPv0aK2Nsqx38ditTpBjgjtVzVnMPlgp3eGOEJ9346fHMmjxRkrnYMBq2baw9rdwARKCbz+Rq4j4FFkg5rIb+Xu2LVHJrr8tcUSrN5zcBp6A7MZ30tP4kGuhy0wHjWGGOxEUO3VNKjnw
VEAtPF14kG3VH5cReQaKK8l6Dsm13yJXQRlXE73Q/l77jSbfleSHqT/MlU6QLvscuQHLzamcLUr7Sr0B6szZ0qdCnvvGHSxTF0k+N+H0u7vThegaGuADTY9VANSCoZOULu+2+Ildk+AEKiw05LkWkrcSXeXb3XsIIiXNKNT22h5/
g4Sh7Ym8htxkIBtFqRPcVUb6299tWwEXBVXW4ELZhrh6IUUvEEgREu5q9L99ptmcf5ol/
io5tKmaWfJP3EG0J9H9ZxdSjpAKytJGrwYPfcVI5TGBujANBgkrBgEEAYI3EQIxADATBgkqhkiG9w0BCRQxGh4YAFQAUwBTAGUAYwBLAGUAeQBTAGUAdAAxMGsGCSsGAQQBgjcRATFeHlwATQBpAGMAcgBvAHMAbwBmAHQAIABFAG4AaABhAG4AYwBlAGQAIABDAHIAeQBwAHQAbwBnAHIAYQBwAGgAaQBjACAAUAByAG8AdgBpAG4AZQByACAAdgAxAC4AMDCCA28GCSqGSIb3DQEHBqCCA2AwggNcAgEAMIIDVQYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQMwDgQIZR5vgi1/9TwCAgfQgIIDKMAMzHPfMLau7IZawMhOd06
AcO2SXQFsZ3kyPLQGrFWcsxEiUDDmcjQ5rZRySOaRyz5PzyIFCUCHcKp5cmlYJTdH4fSlfaHyC9TKJrdEuT2Pn8pq9C/snjuE23LU70c2U+NSQhqAulUcA64eTDyPo74Z2OdRk5jIQ0Y0hYE/F+DSDbn3J2tkfklSyufJloBQAr5p1eZO/
lj5OdZmzCHGP9bsInKX3cuD5ybz1KMNPQd/oHuMFH/DB79ZaMooerFh22QUtry3ZEgMcj+CE0H3B67qTX5NyHVDzZRoxYrjTox5cOfDjroZx/LfeSbei+BC7gBFK2lDOTp4NXevCOsRJ/8OjpyizGIUAhIKYUZSugAgw8r387QimWImKYrWeLj0rqYl0S/
+G+HErQm38Vq6KtgGc9jmoMbHDXyk2PK9IV1GorSJ+dn3LDTrzrBpms+fkNjxHh6ke/4UQii6tPKEWnzNysx+hwMROL5QO5jZp659HBloTmo3sMP+houFQ2PF15Wd4Nr/ujoDTSVUKBoP0q+3U1tJQ2jYTRZvu4YC2A8RWYSI4vDq//
i2lykZHQ6IXU8OjYpgsuwupXpdzqgt4jBBpAn+qWO747xw8+8S/hyqYgAMCpZO1h2nolUsKmc/ejIB2VHT4+DyQi2vLzSlkiBdYTOxx3Z/
IbeBiSaYEBxQbs+KAM4jLSFNgllHcD8UeJMQJFZyWYeG4CuRMbS4+D5QH6nF+xI2NZrqlIJpI8BXR5guh2fxYwc8Pw2W1ytmH8k27G/Zj5yLQpwjv+zTm1TSoLYtzlnfY8WpKXmtCOyECrCE875BwYOBJYBLUyQ3vYh7P+T3rE08l2Yjaci/
naEztdE0HBSs1NhRH9jQ4Uv4iIlq/2Z9lYRRydI4FcAwt/7rIjen/eA1YcswOTmXlwa4PruuPgcVgxuSLS0bWW5fPme8pmVg2fXjtU3ZEZPFC4FliYUmtyNkMFkV5v4vIsMMCpkzF0gmsZXQ/BIh539OawUFGeInJE0Bjqoe05LXuumF3PqX+TKQG/2s/
8YDmLVnrT2RNPFWzDuQmM1buiB/QCvwll4XkbEwOzAfMAcGBSsOAwIaBBR6ftNHys88ZCYwfdP8LaxQr5XftwQUtb3ikBVC1OJKqXdooS6Y7phEqcYCAgfQ
PS C:\Users\Administrator> exit
```

save output in file, I create same name **INTERN-PC.pfx**

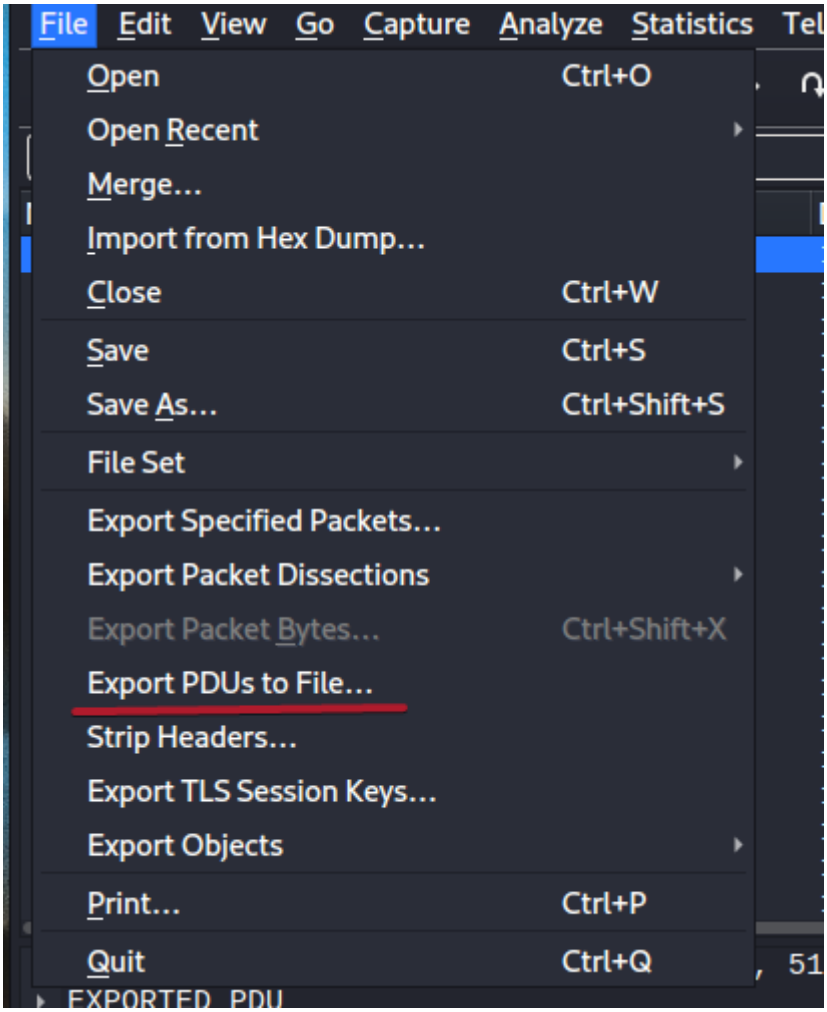
I can add this to TLS protocol. The password of this command:

cmd /c mimikatz.exe privilege::debug token::elevate crypto::capi "crypto::certificates /systemstore:LOCAL_MACHINE /store:`"Remote Desktop`" /export" exit

should be **mimikatz**



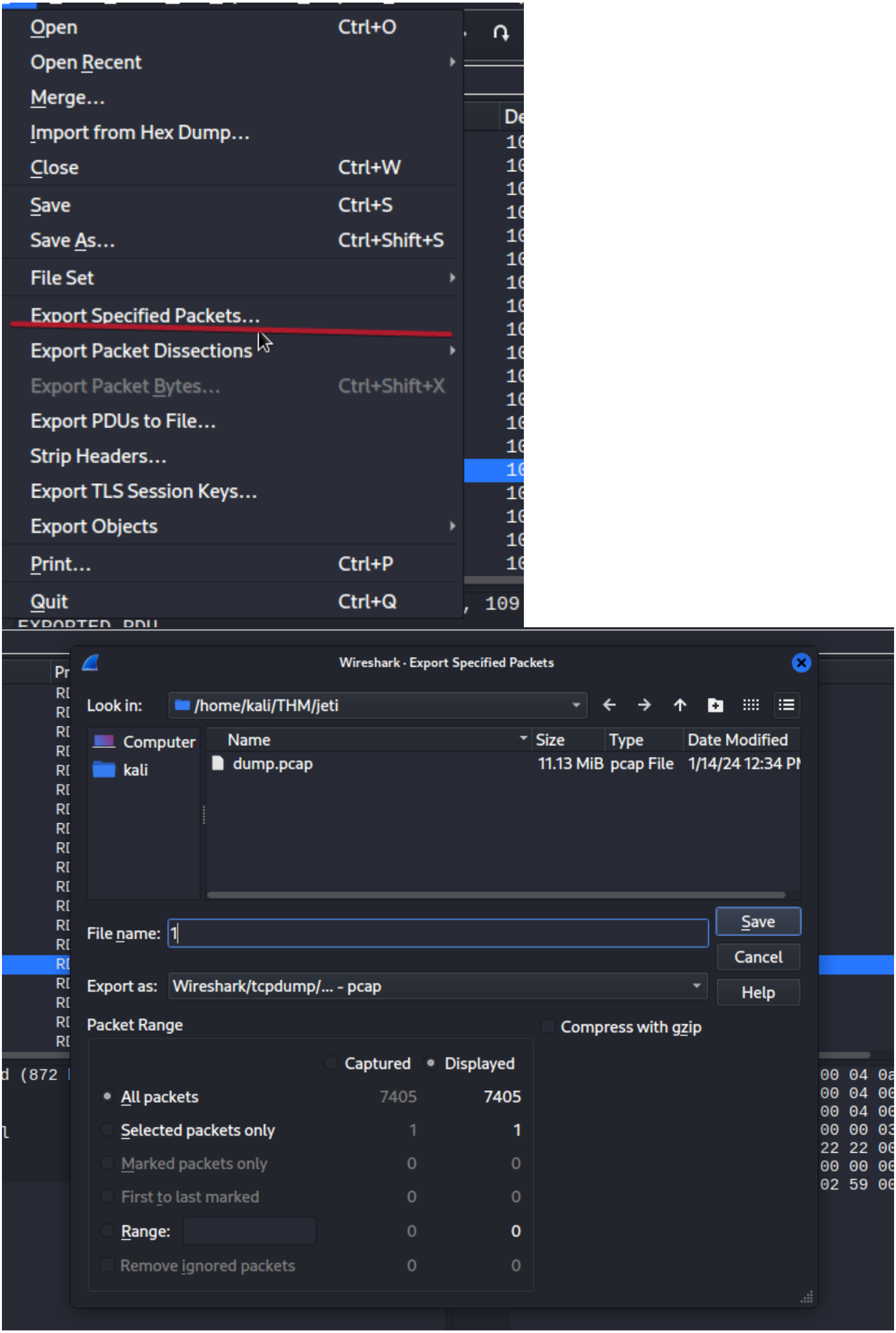
Ok file changed, enumerate I export PDUs



Now I asking in discord how to find data! The very good variant is to use this tool:

https://github.com/GoSecure/pyrdp

But before I need to export daa from 7 layer


Open Ctrl+O
Open Recent
Merge...
Import from Hex Dump...
Close Ctrl+W
Save Ctrl+S
Save As... Ctrl+Shift+S
File Set
Export Specified Packets...
Export Packet Dissections
Export Packet Bytes... Ctrl+Shift+X
Export PDUs to File...
Strip Headers...
Export TLS Session Keys...
Export Objects
Print... Ctrl+P
Quit Ctrl+Q
Wireshark · Export Specified Packets
Look in: /home/kali/THM/jeti
Computer
kali
Name Size Type Date Modified
dump.pcap 11.13 MiB pcap File 1/14/24 12:34 PM
File name: 1
Save
Cancel
Help
Export as: Wireshark/tcpdump/... - pcap
Packet Range
Compress with gzip
Captured Displayed
All packets 7405 7405
Selected packets only 1 1
Marked packets only 0 0
First to last marked 0 0
Range: 0 0
Remove ignored packets 0 0

Download tool

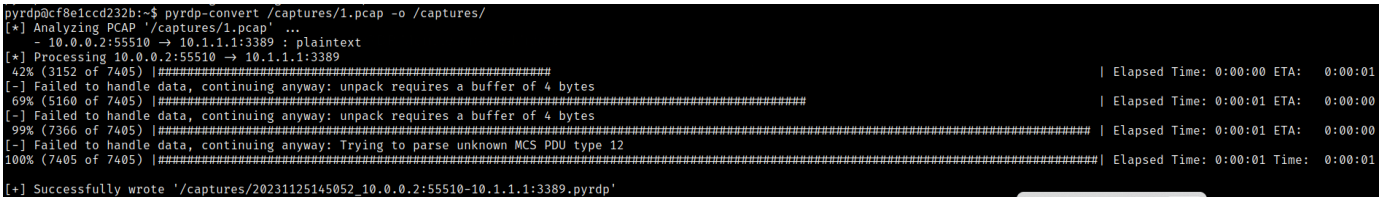
```
docker pull gosecure/pyrdp:latest
```

run in docker

```
sudo docker run -it -v /home/kali/THM/jeti/:/captures gosecure/pyrdp:latest
```

I a inside conteiner with this tool!!!

```
pyrdp-convert /captures/1.pcap -o /captures/
```



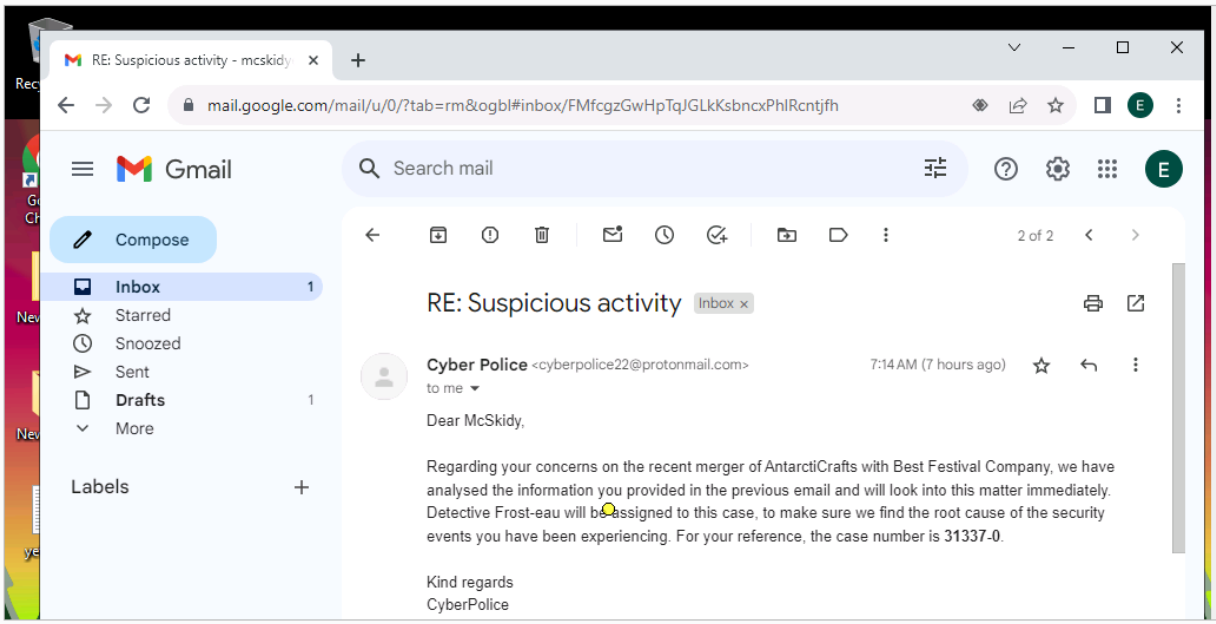
To run a video I used this command

```
sudo docker run -e DISPLAY=$DISPLAY -e QT_X11_NO_MITSHM=1 --net=host -v
/home/kali/THM/jeti/:/captures gosecure/pyrdp:latest pyrdp-player
/captures/20231125145052_10.0.0.2:55510-10.1.1.1:3389.pyrdp
```

Here is information about police number and yetikey

Speed: 1x Scale to window

Pause



<Shift pressed>
<Return released>
<Return pressed>
<Meta pressed>
<Meta pressed>
<Control released>CC
<Control pressed>

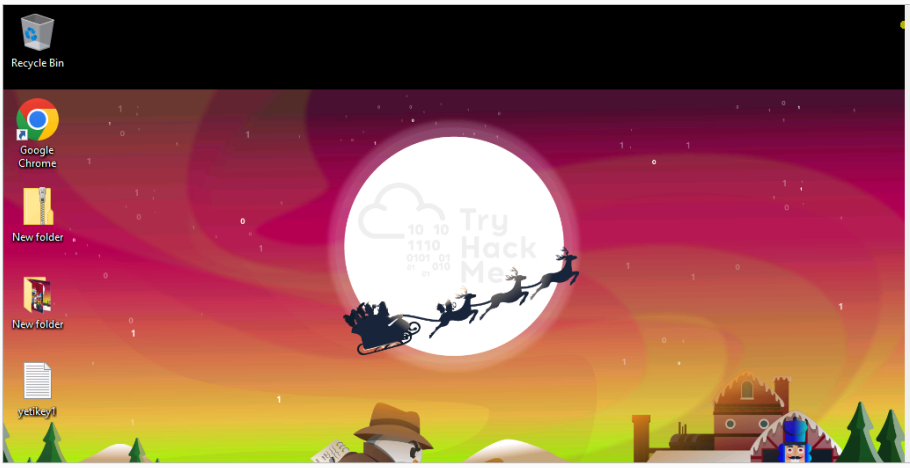
CLIPBOARD DATA: https://mail.google.com/mail/u/0/?tab=rm&ogbl#inbox

Live connections Replays

/captures/20231125145052_10.0.0.2:55510-10.1.1.1:3389.pyrdp

Speed: 1x Scale to window

Pause



<Op pressed>
<Return released>
<Return pressed>

CLIPBOARD DATA: 1-1f9548f131522e85ea30e801dfd9b1a4e526003f9e83301faad85e6154ef2834
