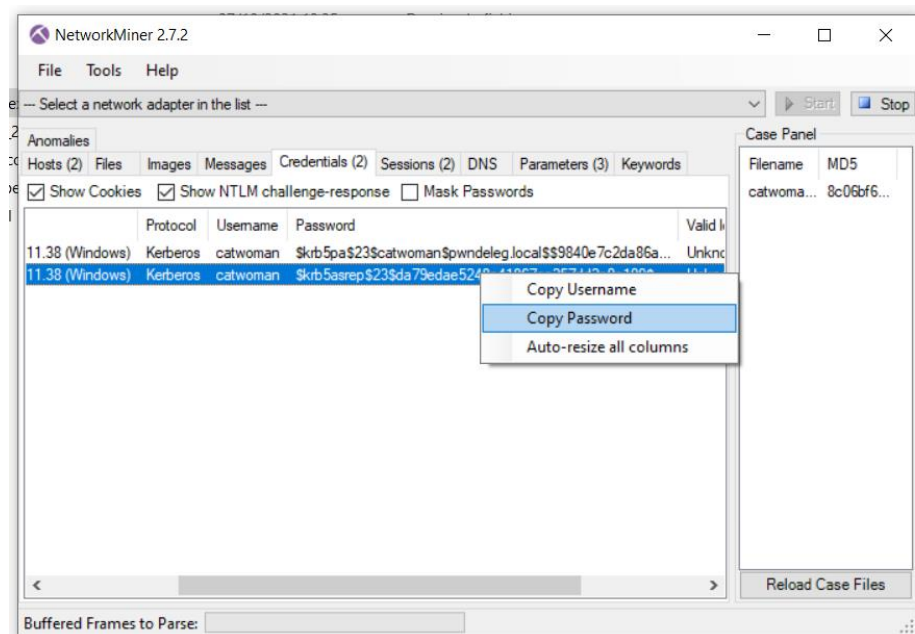


Challenge 1 : Le ticket de Catwoman

On a un fichier de capture pcap dans lequel on a une authentification kerberos :

172.20.103.6	172.20.111.38	TCP	66 50339 → 88 [SYN, Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SA
172.20.111.38	172.20.103.6	TCP	66 88 → 50339 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=146
172.20.103.6	172.20.111.38	TCP	54 50339 → 88 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
172.20.103.6	172.20.111.38	TCP	58 50339 → 88 [PSH, ACK] Seq=1 Ack=1 Win=2102272 Len=4 [TCP
172.20.111.38	172.20.103.6	TCP	54 88 → 50339 [ACK] Seq=1 Ack=5 Win=2102272 Len=0
172.20.103.6	172.20.111.38	KRBS	285 AS-REQ
172.20.111.38	172.20.103.6	KRBS	1452 AS-REP
172.20.103.6	172.20.111.38	TCP	54 50339 → 88 [FIN, ACK] Seq=236 Ack=1399 Win=2100992 Len=0
172.20.111.38	172.20.103.6	TCP	54 88 → 50339 [ACK] Seq=1399 Ack=237 Win=2102016 Len=0
172.20.111.38	172.20.103.6	TCP	54 88 → 50339 [RST, ACK] Seq=1399 Ack=237 Win=0 Len=0
172.20.103.6	172.20.111.38	SMB2	126 Tree Disconnect Request
172.20.111.38	172.20.103.6	SMB2	126 Tree Disconnect Response
172.20.103.6	172.20.111.38	SMB2	126 Session Logoff Request
172.20.111.38	172.20.103.6	SMB2	126 Session Logoff Response
172.20.103.6	172.20.111.38	TCP	54 50337 → 445 [RST, ACK] Seq=145 Ack=145 Win=0 Len=0

On peut extraire le jeton TGT avec l'utilitaire Windows NetworkMiner :



Ensuite on lance un bruteforce pour retrouver le mot de passe de Catwoman :

```
> john passwd --format=krb5tgs --wordlist=/root/rockyou.txt
Using default input encoding: UTF-8
No password hashes loaded (see FAQ)
> john passwd --wordlist=/root/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
ilovebatman (?)
1g 0:00:00:00 DONE (2022-03-22 15:41) 1.492g/s 968979p/s 968979c/s 968979
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```