Security Professionals Network Inc.

実践講座：WiresharkによるKerberos通信の復号

2022.05.17

塩月誠人 <mshio@sec-pro.net>
合同会社セキュリティ・プロフェッショナルズ・ネットワーク

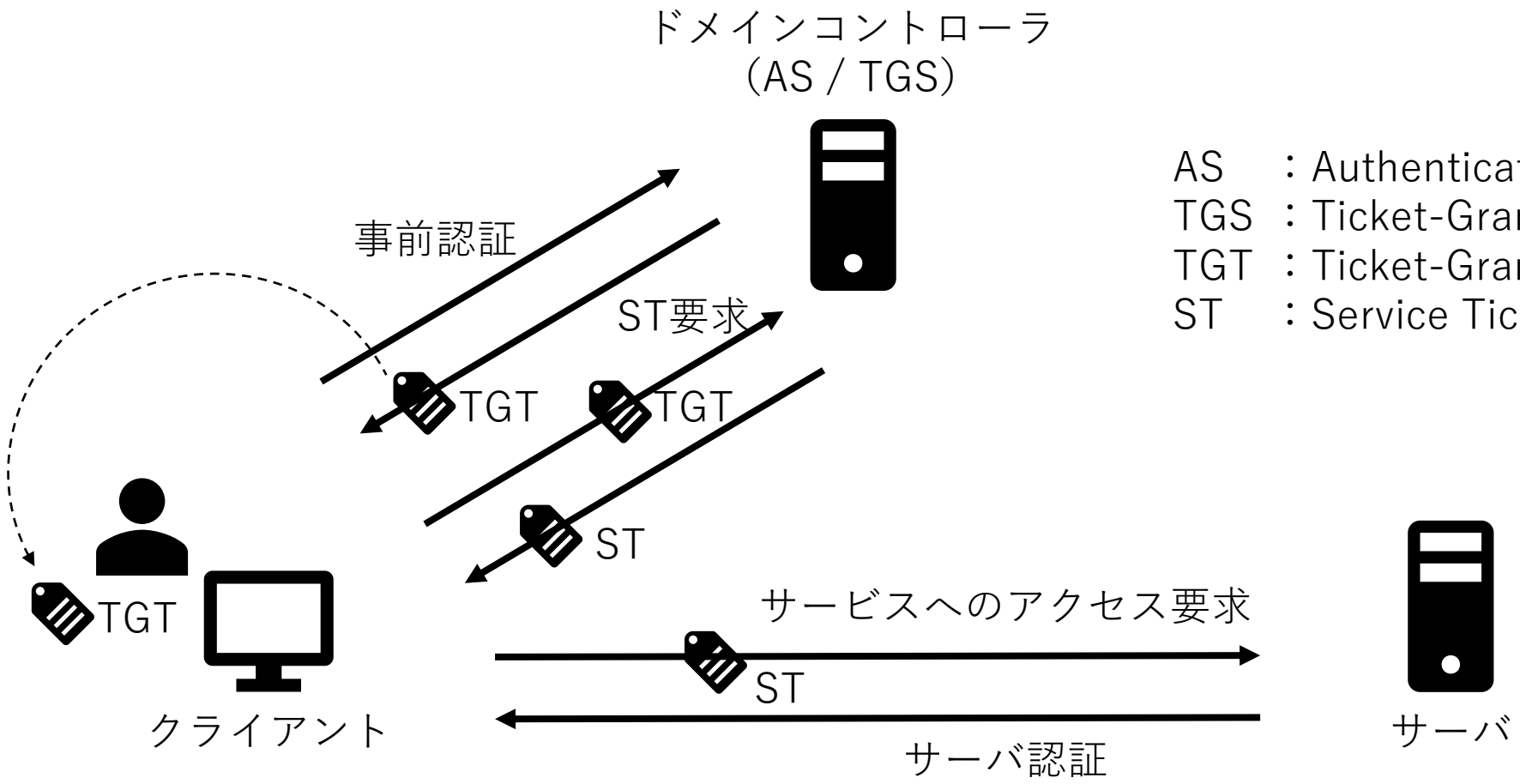
はじめに

WindowsのActive Directory環境下では主要な認証プロトコルとしてKerberosが用いられるため、認証に関するトラブルシューティングや攻撃手法の調査・解析を行う際にはKerberos認証のネットワーク通信を詳細に調べる必要があります。

一方でKerberos認証の通信データや互いにやり取りされるチケットは肝心な部分が各種の「鍵」で暗号化されており、Wiresharkでそのままパケットを表示させてもすべてを平文で見ることはできません。

本実践講座では基本的なKerberos認証の流れを説明するとともに、Active Directory環境下におけるKerberos認証の通信データをWireshark上で復号する手法について解説します。

Kerberos認証の概要

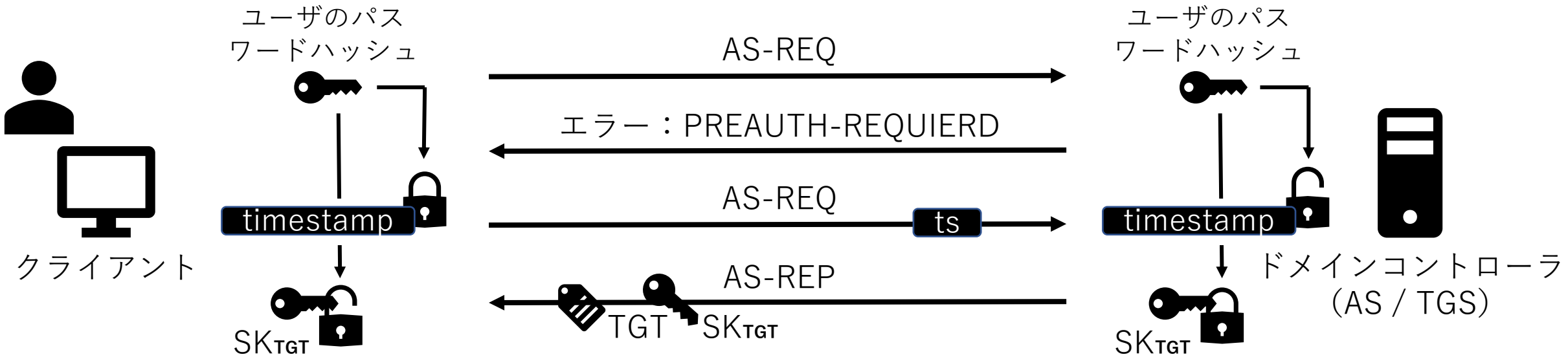


AS　：Authentication Service
TGS　：Ticket-Granting Service
TGT　：Ticket-Granting Ticket
ST　：Service Ticket

AS Exchange（Authentication Service Exchange）

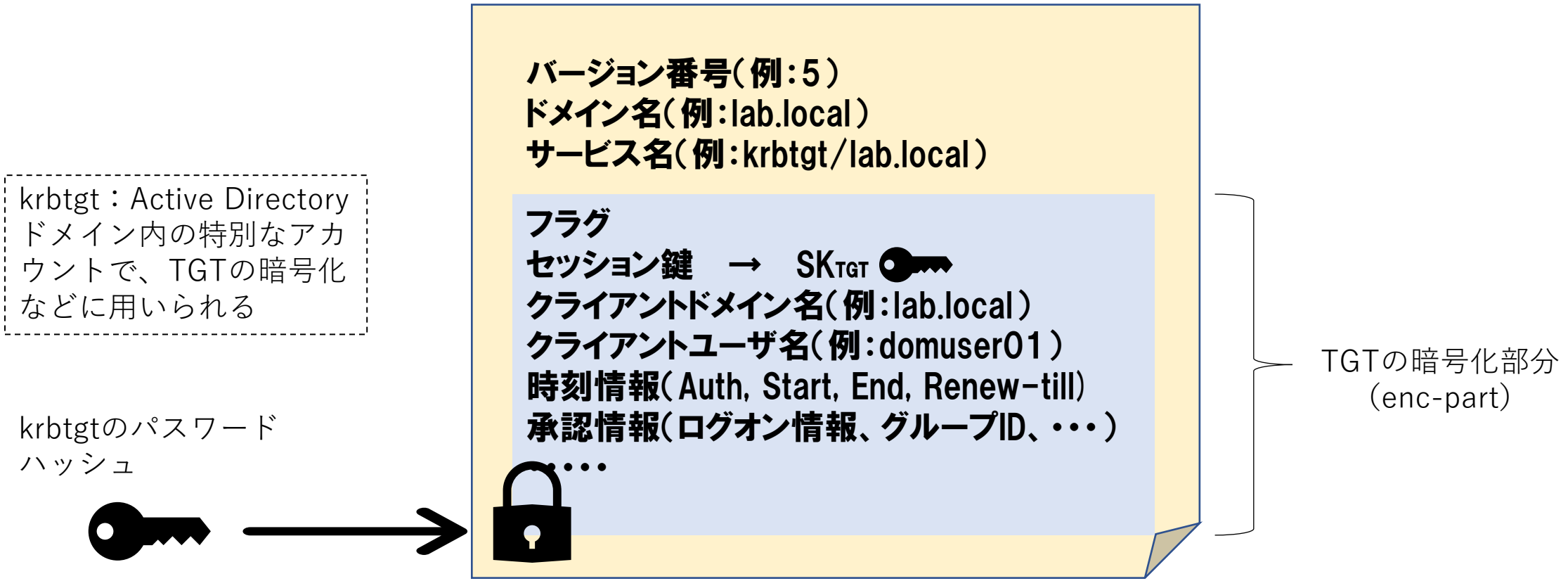
■ 事前認証 ～ TGTの取得

- AS-REQ（認証サービス要求）：クライアントのタイムスタンプをユーザのパスワードハッシュで暗号化して送ることによりクライアントを認証
- AS-REP（認証サービス応答）：認証を通過後、TGTおよびユーザのパスワードハッシュで暗号化したTGT用のセッション鍵（SK_{TGT}）をクライアントへ渡す



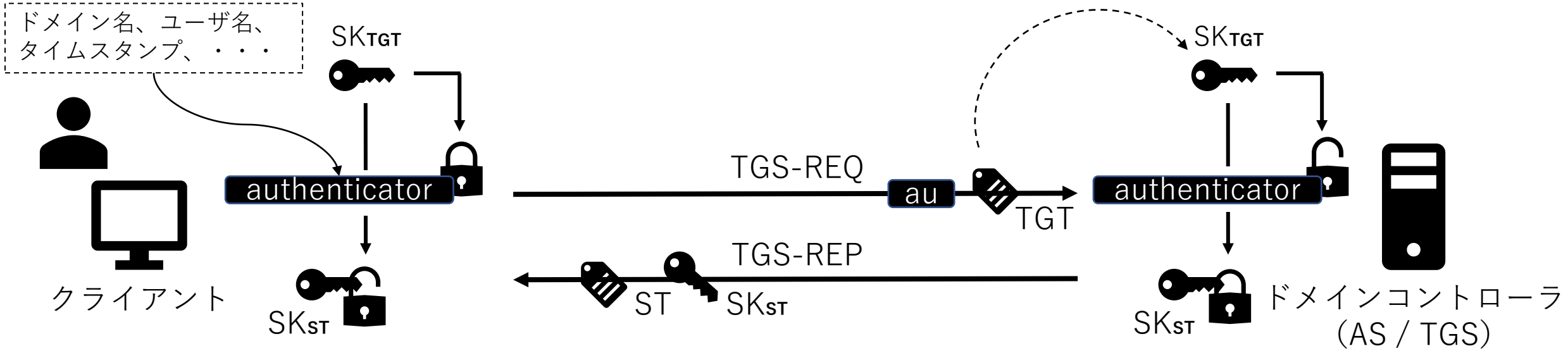
TGT

■ TGT（Ticket-Granting Ticket）の内容



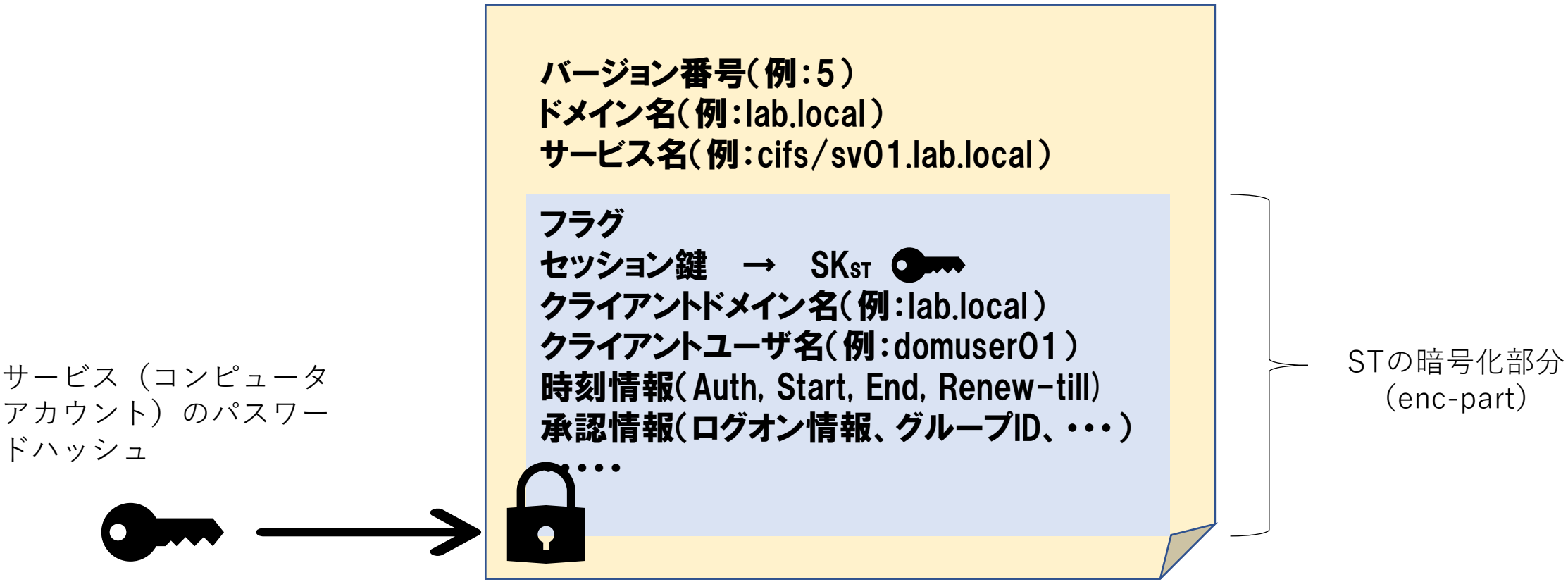
TGS Exchange（Ticket-Granting Service Exchange）

- STの要求 ～ STの取得
  - TGS-REQ（チケット交付サービス要求）：TGTおよびSK$_{TGT}$で暗号化した認証子（Authenticator）を送り、特定のサービスへアクセスするためのSTを要求
  - TGS-REP（チケット交付サービス応答）：認証子とTGTを検証後、STおよびSK$_{TGT}$で暗号化したST用のセッション鍵（SK$_{ST}$）をクライアントへ渡す



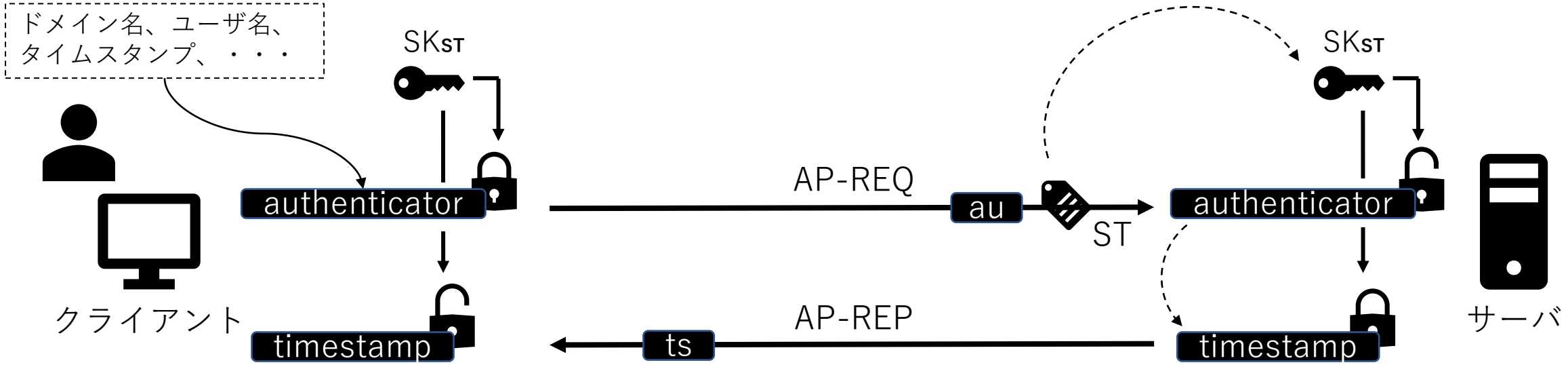
ST

■ ST（Service Ticket）の内容



CS Exchange（Client/Server Authentication Exchange）

- サービスへのアクセス要求 ～ サーバの認証
  - AP-REQ（アプリケーション要求）：STおよびSKSTで暗号化した認証子（Authenticator）を送り、サービスに対するアクセスを要求
  - AP-REP（アプリケーション応答）：認証子とSTを検証、相互認証（サーバの認証）の場合はクライアントのタイムスタンプを認証子から取り出しSKSTで暗号化して送り返す



通信の復号に必要な「鍵」

- ユーザのパスワードハッシュ
  - AS-REQのタイムスタンプ、AS-REPの暗号化部分（SK_{TGT}等）
- krbtgtのパスワードハッシュ
  - TGTの暗号化部分（SK_{TGT}、ユーザ名、時刻情報、承認情報等）
- サービス（コンピュータアカウント）のパスワードハッシュ
  - STの暗号化部分（SK_{ST}、ユーザ名、時刻情報、承認情報等）
- SK_{TGT}（AS-REPやTGTを復号することで入手）
  - TGS-REQの認証子、TGS-REPの暗号化部分（SK_{ST}等）
- SK_{ST}（TGS-REPやSTを復号することで入手）
  - AP-REQの認証子、AP-REPの暗号化部分（相互認証タイムスタンプ等）
- つまり三者（ユーザ、krbtgt、サービス）のパスワードハッシュがあればKerberos通信の復号が可能

Keytabファイルと「鍵」のタイプ

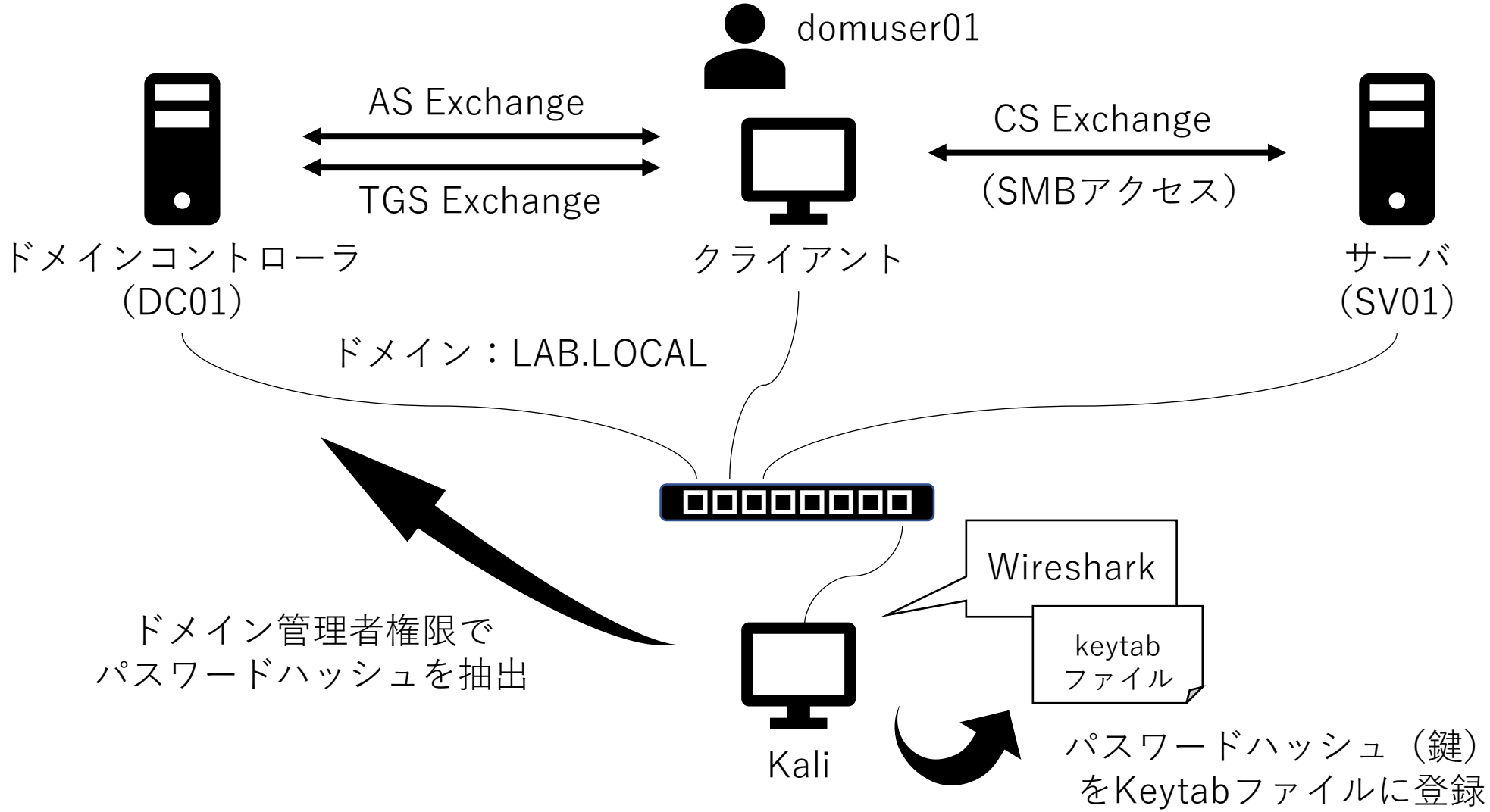
- Keytabファイルとは・・・
  - Windows以外のKerberos環境で使用される、アカウント認証情報（パスワードハッシュ）が入ったファイル
  - UNIX/Linux上のKerberosアプリケーションなどはKeytabファイルを使用して認証
  - WiresharkもKeytabファイルの情報を利用してKerberos通信の復号を行う

- 主要な「鍵」のタイプ（暗号のタイプ）
  - AES256-CTS-HMAC-SHA1-96 (18) ← 通常はこれが使用
  - AES128-CTS-HMAC-SHA1-96 (17)
  - RC4-HMAC (23)
  - 使われる暗号のタイプは設定やネゴシエーションにより決定
  - 暗号のタイプごとに異なるパスワードハッシュが使用
  - アカウントそれぞれについて、使用されている暗号のタイプごとにKeytabファイルへパスワードハッシュを登録

鍵の収集とKeytabファイルの作成

- 基本的な考え方
  - ADからアカウントのパスワードハッシュを抜き出してKeytabファイルへ登録
  - 当然のことながらパスワードハッシュを抜き出すためにはドメイン管理者権限が必要
- 注意点
  - ここでの「鍵」とは、すなわちパスワードハッシュなので、実運用環境のアカウントを処理する際にはそれらが漏えいしないよう取り扱いに注意すること
  - パスワードハッシュを登録するKeytabファイルについても、その内容は暗号化されていないため、Keytabファイル自体の安全性を十分に確保すること
- 実習環境
  - Wireshark実行環境：Kali Linux 2021.2、Wireshark Version 3.4.4
  - ドメインコントローラ：DC01.LAB.LOCAL（Windows Server 2019）
  - クライアントユーザアカウント：domuser01
  - サービス（コンピュータ）アカウント：SV01$（コンピュータ名：SV01）
  - ドメイン管理者アカウント／パスワード：domadmin / Domad00

鍵の収集とKeytabファイルの作成



鍵の収集とKeytabファイルの作成

■ パスワードハッシュを一つずつ手作業で登録する方法

```
# impacket-secretsdump  -just-dc-user  krbtgt  domadmin:Domad00@dc01.lab.local
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:69265d5ce063a52dc56afbecf64e5f6c:::
[*] Kerberos keys grabbed
krbtgt:aes256-cts-hmac-sha1-96:a10ed2949c545560cf756e200156fbfcbef6535626374535 92ecd39969a2fefa
krbtgt:aes128-cts-hmac-sha1-96:58b150959aeedfabdb8cc9b30341f234
krbtgt:des-cbc-md5:dfabdcbaae155e89
[*] Cleaning up...
```

対象アカウントの指定

ドメイン管理者のユーザ名：パスワード@ドメインコントローラ

rc4-hmac（NTLMハッシュ）

aes256-cts-hmac-sha1-96

aes128-cts-hmac-sha1-96

→ impacket-secretsdump（Impacketのsecretsdump.py）を使用して、ドメインコントローラ（dc01.lab.local）からアカウントkrbtgt、domuser01、およびsv01$のパスワードハッシュを収集

鍵の収集とKeytabファイルの作成

```
# ktutil
ktutil:  addent -key -p krbtgt@LAB.LOCAL -k 1 -e aes256-cts-hmac-sha1-96
Key for krbtgt@LAB.LOCAL (hex): a10ed2949c545560cf756e200156fbfcbef6535626374535 92ecd39969a2fefa
ktutil:  addent -key -p domuser01@LAB.LOCAL -k 1 -e aes256-cts-hmac-sha1-96
Key for domuser01@LAB.LOCAL (hex): 9075c245278da5da9ff0b1ef57952695143ef01ea59630d5bb1ec2901e8ca2a4
ktutil:  addent -key -p SV01$@LAB.LOCAL -k 1 -e aes256-cts-hmac-sha1-96
Key for SV01$@LAB.LOCAL (hex): 9da7d1a747cc9107db9bcf6cb11e8d28072c085d0c7aa0b17e2c2307b64eafc9
ktutil:  wkt LAB.LOCAL.keytab
ktutil:  quit
```

→ ktutilコマンドを使用してアカウントkrbtgt、domuser01、およびsv01$のAES256-CTS-HMAC-SHA1-96タイプのパスワードハッシュをkeytabファイル「LAB.LOCAL.keytab」に保存

addentのオプション：

- -key ・・・ 16進数の鍵（パスワードハッシュ）を直接入力する場合に指定
- -password ・・・ 平文パスワードを入力してパスワードハッシュに変換する場合に指定
- -p プリンシパル ・・・ アカウントの指定
- -k 鍵のバージョン番号 ・・・ Wiresharkを使う上では何番でも良い
- -e 暗号のタイプ ・・・ aes256-cts-hmac-sha1-96, aes128-cts-hmac-sha1-96, rc4-hmac等

鍵の収集とKeytabファイルの作成

```
# klist -e -K -k LAB.LOCAL.keytab
Keytab name: FILE:LAB.LOCAL.keytab
KVNO Principal
---- --------------------------------------------------------------------------
   1 krbtgt@LAB.LOCAL (aes256-cts-hmac-sha1-96)  (0xa10ed2949c545560cf756e200156fbfcbef653562637
453592ecd39969a2fefa)
   1 domuser01@LAB.LOCAL (aes256-cts-hmac-sha1-96)  (0x9075c245278da5da9ff0b1ef57952695143ef01ea
59630d5bb1ec2901e8ca2a4)
   1 SV01$@LAB.LOCAL (aes256-cts-hmac-sha1-96)  (0x9da7d1a747cc9107db9bcf6cb11e8d28072c085d0c7aa
0b17e2c2307b64eafc9)
```

→ klistコマンドを使用してkeytabファイル「LAB.LOCAL.keytab」の内容を表示し、正しく登録されたことを確認

klistのオプション：

-e ・・・ 暗号のタイプを表示

-K ・・・ 16進数の鍵（パスワードハッシュ）を表示

-k keytabファイル ・・・ keytabファイルの指定

鍵の収集とKeytabファイルの作成

■ 全アカウントのパスワードハッシュをまとめて一気に登録する方法

```
# samba-tool drs clone-dc-database --include-secrets --targetdir=/tmp/work --server=dc01.lab.l
ocal --username=domadmin --password=Domad00 lab.local
```

→ samba-toolを使用してLAB.LOCALドメインの情報を/tmp/work以下にまるごとコピー

```
# samba-tool domain exportkeytab --configfile=/tmp/work/etc/smb.conf LAB.LOCAL.keytab
```

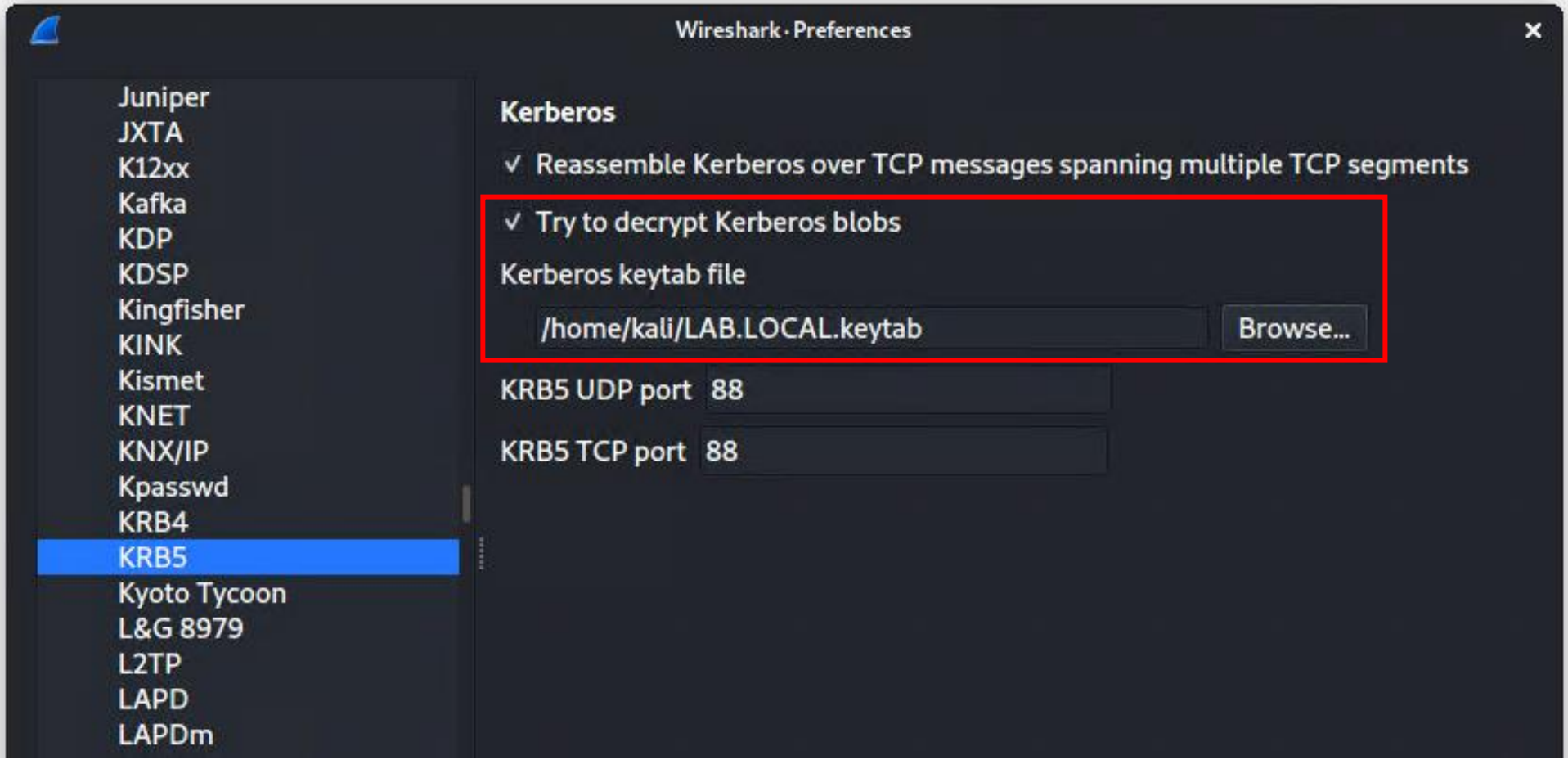
→ コピーしたドメイン情報から全アカウントのパスワードハッシュを抜き出して、keytabファイル「LAB.LOCAL.keytab」に保存

```
# klist -e -K -k LAB.LOCAL.keytab
```

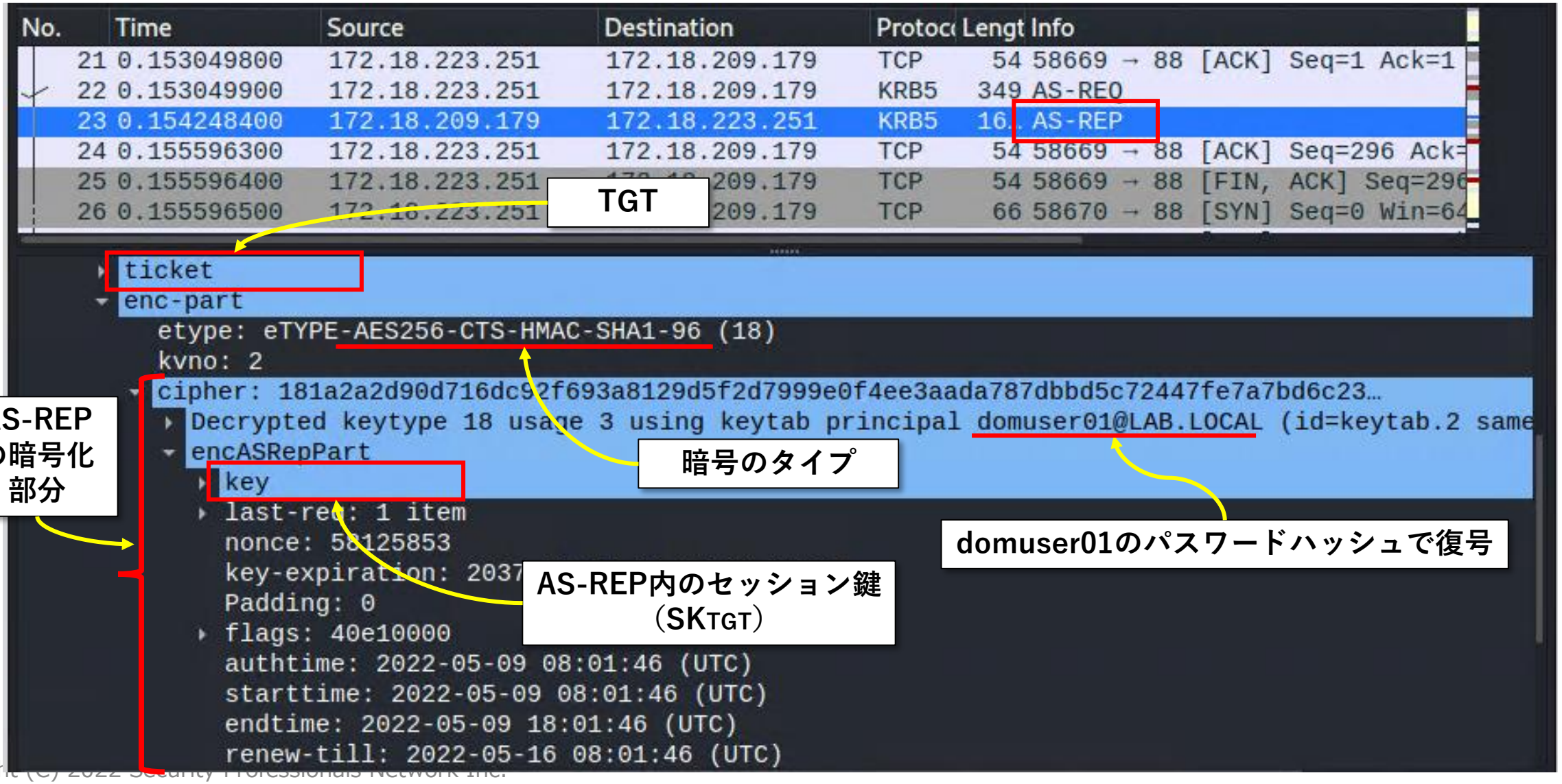
→ klistコマンドを使用してkeytabファイル「LAB.LOCAL.keytab」の内容を表示し、正しく登録されたことを確認

WiresharkのKRB5プロパティ設定

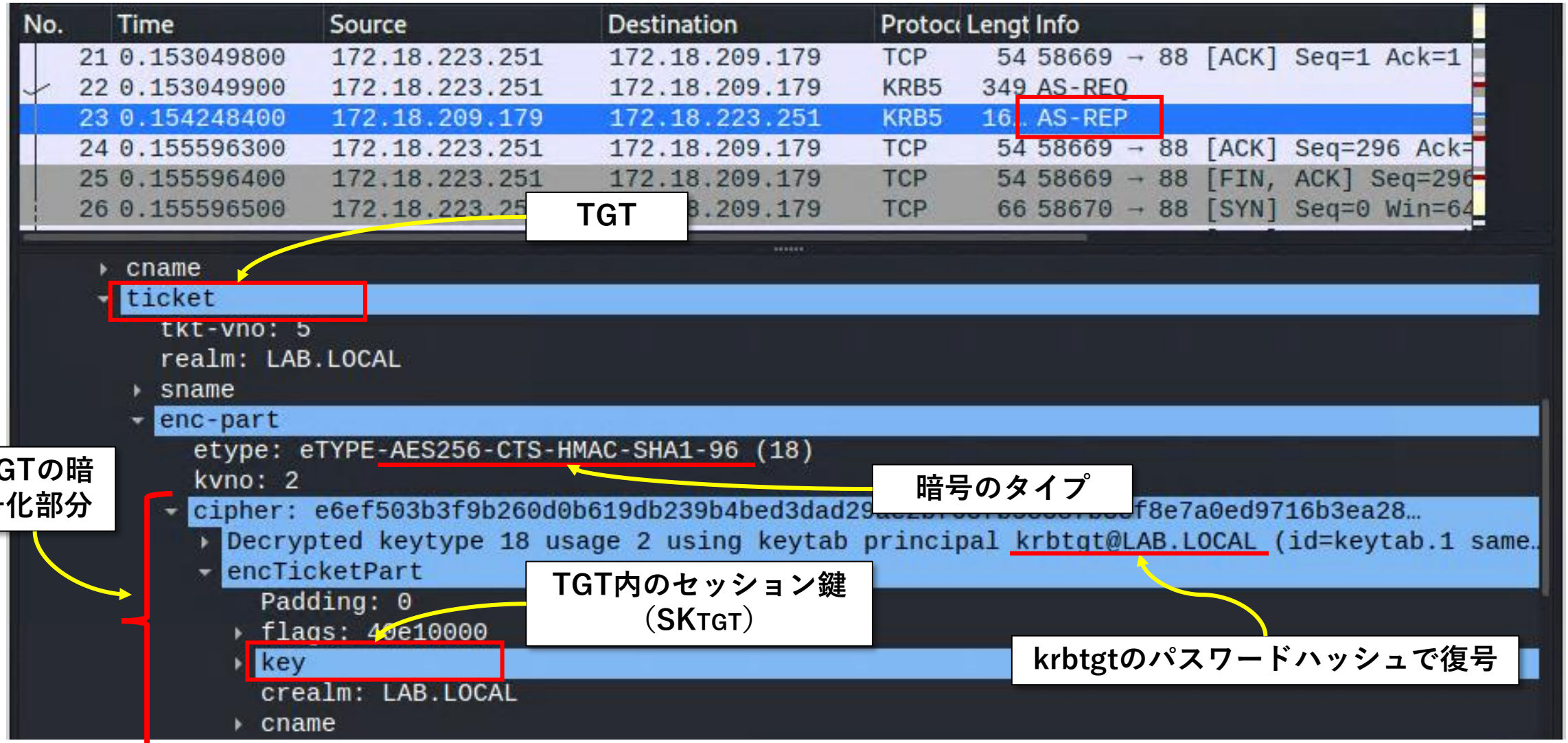
- Wiresharkを起動、Edit / Preferences / Protocols / KRB5 で以下を設定



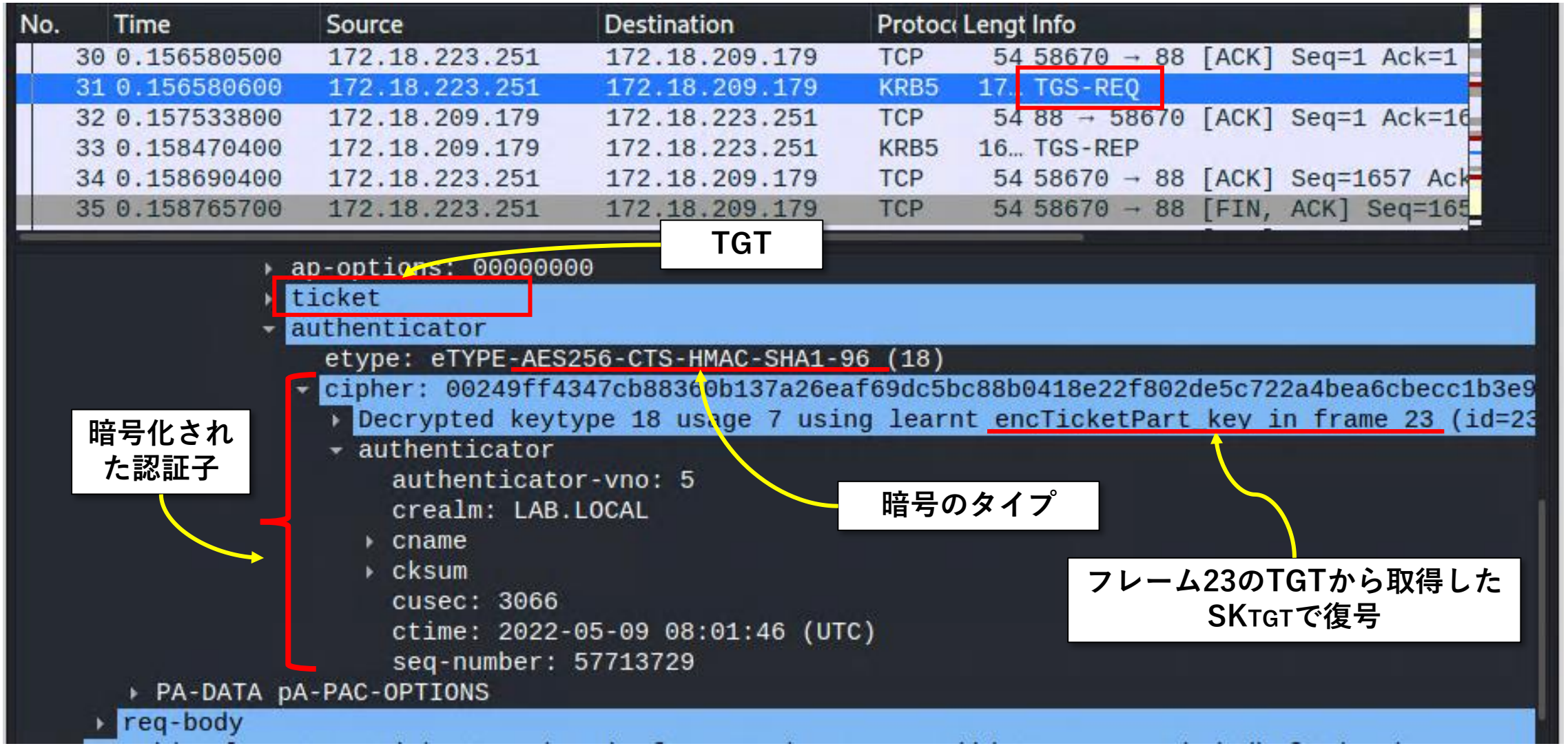
Kerberos通信の復号（AS-REP）



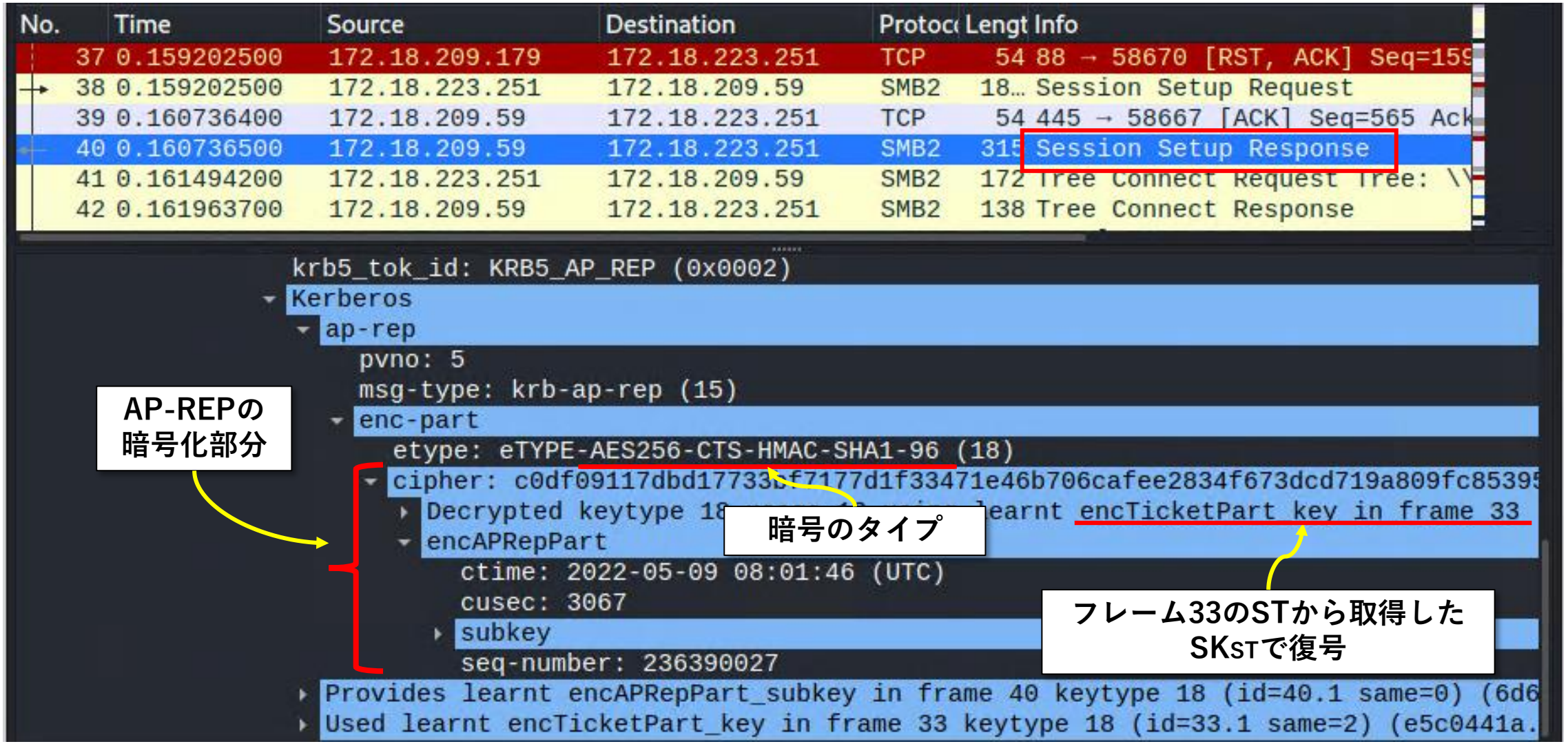
Kerberos通信の復号（AS-REP）



Kerberos通信の復号（TGS-REQ）



Kerberos通信の復号（AP-REP）



参考URL

- RFC 4120 - The Kerberos Network Authentication Service (V5)
  https://www.ietf.org/rfc/rfc4120.txt
- [MS-KILE]: Kerberos Protocol Extensions
  https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-kile/2a32282e-dd48-4ad9-a542-609804b02cc9
- All you need to know about Keytab files
  https://docs.microsoft.com/ja-jp/archive/blogs/pie/all-you-need-to-know-about-keytab-files
- Keytab Extraction
  https://wiki.samba.org/index.php/Keytab_Extraction
- Kerberos - Wireshark Wiki
  https://wiki.wireshark.org/Kerberos.md