# SIBINTEK CTF 2025

## Задания

09.11.2025

**Название:** Высокочастотный анализ

**Категория:** Joy

**Очки:** динамическое начисление

**Описание:** Внучка генерального директора ДНК с младенчества слушала разговоры старших про нефть, нефтепродукты и всё такое прочее. Девочка в школе очень хорошо учится, собирается поступать в "Керосинку", умничка просто, хотя она и проказница.

Когда она узнала, что дедушка, наконец-то, согласился пересесть со своей раритетной "Волги" на нормальный, современный седан представительского класса - она прислала ему сообщение: "Дедуля, не забудь добавить вот это" - и приложила картинку.

**Формат флага:** Sibintek{слово-слово-слово_слово}
**Флаг:** Sibintek{метил-трет-бутиловый_эфир}

01

**Анализ изображения.**
Открываем файл Pic.jpg. На изображении видна последовательность эмодзи с математическими символами.

На картинке представлены следующие символы:

- ⭐ (звезда)
- 💙 (синее сердце)
- 💭 (облачко мысли)
- ➕ (плюс)
- ➖ (минус)
- ➡️ (стрелка вправо)
- 🟰 (знак равно)

02

**Определение контекста задачи.**
Из описания задания мы знаем несколько важных деталей:

1. Внучка готовится поступать в **"Керосинку"** - это разговорное название Российского государственного университета нефти и газа имени И.М. Губкина (РГУ нефти и газа). Это означает, что девочка хорошо разбирается в химии.
2. Упоминается переход дедушки **с раритетной "Волги" на современный седан**. Старые отечественные автомобили, такие как "Волга", обычно заправляются бензином АИ-92, а современные иномарки требуют бензин АИ-95 или АИ-98.
3. Формат флага: **слово-слово-слово_слово** - подсказывает, что ответ будет состоять из нескольких слов.

Эти подсказки указывают на то, что задача связана с химией нефтепродуктов и повышением октанового числа бензина.

# 03

**Расшифровка эмодзи как химических элементов.**

Поскольку задача связана с химией, логично предположить, что эмодзи представляют собой химические элементы:

- ⭐ (звезда) = **C** (углерод, Carbon)
- ❤️ (сердце) = **H** (водород, Hydrogen)
- ☁️ (облако) = **O** (кислород, Oxygen)

Эти три элемента (C, H, O) являются основными компонентами органических соединений, в том числе углеводородов и нефтепродуктов.

# 04

**Составление химического уравнения.**
Теперь расшифруем каждую строку изображения, переводя эмодзи в химические формулы:

**Строка 1:** ⭐❤️❤️❤️☁️❤️ **+**
Расшифровка: **$CH_3OH$ +** (метанол)

**Строка 2:** ⭐❤️❤️❤️⭐❤️❤️❤️⭐❤️❤️❤️⭐ **—**
Расшифровка: **$CH_3)_3C–H$** (изобутан или 2-метилпропан)**

**Строка 3:** ⭐❤️❤️ **→**
**Расшифровка: $CH_2$** = (промежуточный продукт реакции)

**Строка 4:** ⭐❤️❤️❤️⭐❤️❤️❤️⭐❤️❤️❤️⭐**—**☁️**—**⭐❤️❤️❤️
Расшифровка: **$(CH_3)_3C–O–CH_3$** (продукт реакции)

Полное химическое уравнение:

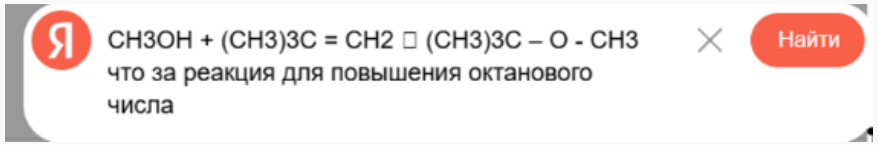
$$CH_3OH + (CH_3)_3C–H \rightarrow CH_2 + (CH_3)_3C–O–CH_3$$

Однако правильнее записать его так:

$$CH_3OH + (CH_3)_3C^+ \rightarrow (CH_3)_3C–O–CH_3 + H^+$$

## 05

**Определение химического соединения.**
Итоговая формула $(CH_3)_3C–O–CH_3$ представляет собой эфир. Вводим эту формулу в поисковую систему вместе с контекстом "повышение октанового числа бензина":




Поисковые результаты показывают, что это соединение называется **метил-трет-бутиловый эфир (МТБЭ).**

**Метил-трет-бутиловый эфир (МТБЭ)** - это высокооктановая кислородсодержащая добавка к автомобильным бензинам. МТБЭ используется для повышения октанового числа бензина, что как раз соответствует контексту задачи - переход с 92-го на 95-й бензин.

## 06

**Формирование флага.**
Название вещества "метил-трет-бутиловый эфир" идеально соответствует формату флага:

- **слово-слово-слово_слово**
- метил-трет-бутиловый_эфир

## 07

**Применение в реальной жизни.**

В данном задании использовалась техника **визуального кодирования** с помощью эмодзи для представления химической информации. Эта техника демонстрирует несколько важных принципов информационной безопасности и криптографии:

В данном случае использовалось визуальное кодирование через эмодзи, которое на первый взгляд выглядит как обычный набор символов, но на самом деле содержит зашифрованное химическое уравнение.

В реальной жизни подобные методы могут применяться:
- Для передачи конфиденциальной информации в открытых каналах связи
- В социальных сетях для скрытой коммуникации
- Для обхода систем автоматического мониторинга текстовых сообщений

**Название:** Операция «Чёрное золото»

**Категория:** AD DC

**Очки:** динамическое начисление

**Описание:** Служба информационной безопасности АО «Дудинская Нефтяная Компания» зафиксировала аномальную активность в корпоративной доменной сети. Системы мониторинга показали необъяснимый доступ к критически важному серверу, содержащему проекты по разведке новых месторождений.

Подозрения пали на использование сложной атаки, скомпрометировавшей саму инфраструктуру домена. Для расследования инцидента был снят дамп памяти с рабочей станции инженера-геолога Ивана Петрова, с которой, предположительно, и была инициирована атака.

```
Sibintek{GoldenTicket_User:[Username]_Domain:[Domain]_SID:[DomainSID]_KRBTGT_NTLM:[First8CharsOfAdminKRBTGTHash]_Admin:[AdminUser]@[Domain]:[AdminPassword]}.
```

**Флаг:** Sibintek{GoldenTicket_User:FalseAdmin_Domain:dnk.local_SID:S-1-5-21-4283513613-2830627660-261587487_KRBTGT_NTLM:7cac020f_Admin:admin.dna@dnk.local:DNK_Admin123!}

01

**Подготовка инструментов.**
Для анализа дампа памяти нам понадобится инструмент pypykatz, который специализируется на извлечении учетных данных из дампов Windows.

Установка pypykatz:

```
pip install pypykatz
```

02

**Анализ дампа памяти.**
Запускаем анализ дампа с помощью pypykatz, указав модуль LSA для извлечения Kerberos тикетов:

```
pypykatz lsa minidump ctf_final.dmp
```

03

**Поиск артефактов Golden Ticket.**

В выводе pypykatz ищем сессии аутентификации, содержащие аномальные Kerberos тикеты. Обращаем внимание на следующие признаки Golden Ticket:

- Наличие пользователя с нестандартным именем (не существующего в домене)
- Доменное имя, соответствующее атакованному домену
- Отсутствие пароля для Kerberos учетных данных (тикет сгенерирован искусственно)

В выводе находим несколько сессий аутентификации. Особое внимание уделяем сессии пользователя Ivan.Petrov:

```
== LogonSession ==
authentication_id 414071 (65177)
session_id 1
username Ivan.Petrov
domainname dnk
logon_server DC-1
logon_time 2025-10-29T23:13:00.021735+00:00
sid S-1-5-21-4283513613-2830627660-261587487-1103
luid 414071
    == Kerberos ==
            Username: FalseAdmin
            Domain: dnk.local
```

Из самого яркого - отсутствуют пароли для Kerberos. Для примера, у пользователя admin.dna данное поле выглядит вот так:

```
== Kerberos ==
                Username: admin.dna
                Domain: DNK.LOCAL
                Password: DNK_Admin123!
                password
(hex)44004e004b005f00410064006d0069006e00310032003300210000000000000
                AES128 Key: 7cac020f26d60517995453bf758e1485
                AES256 Key:
6eaecd16049459e30a788c910754e579ca2fc12e3165a3ccd314d6eef6c59b94
```

## 02

**Извлечение параметров Golden Ticket.**
Из найденной сессии извлекаем следующие параметры:

- Username: `FalseAdmin` - фальшивый пользователь, созданный для Golden Ticket
- Domain: `dnk.local` - целевой домен атаки
- Domain SID: `S-1-5-21-4283513613-2830627660-261587487` - идентификатор безопасности домена (извлекается из SID пользователя, убирая RID `1103`, либо любой другой учетки)

## 03

**Извлечение NTLM хэша администратора.**
В сессии администратора находим NTLM хэш:

```
== MSV ==
    Username: admin.dna
    Domain: dnk
    LM: NA
    NT: 7cac020f26d60517995453bf758e1485
```

Для флага используем первые 8 символов NTLM хэша: `7cac020f`

## 04

**Поиск учетных данных администратора.**
В других сессиях аутентификации находим учетные данные администратора домена:

```
== LogonSession ==
authentication_id 2624505 (280bf9)
session_id 1
username admin.dna
domainname dnk
logon_server DC-1
logon_time 2025-10-29T23:47:36.722303+00:00
sid S-1-5-21-4283513613-2830627660-261587487-1104
luid 2624505
```

```
== Kerberos ==
        Username: admin.dna
        Domain: DNK.LOCAL
        Password: DNK_Admin123!
```

# 05

**Формирование флага.**
Собираем все найденные параметры в соответствии с маской флага:

```
Sibintek{GoldenTicket_User:[Username]_Domain:[Domain]_SID:[DomainSID]_KRBTGT_NTLM:[First8CharsOfKRBTGTHash]_Admin:[AdminUser]@[Domain]:[AdminPassword]}
```

```
Sibintek{GoldenTicket_User:FalseAdmin_Domain:dnk.local_SID:S-1-5-21-4283513613-2830627660-261587487_KRBTGT_NTLM:7cac020f_Admin:admin.dna@dnk.local:DNK_Admin123!}
```

# 06

**Применение в реальной жизни.**

Атака Golden Ticket представляет собой серьезную угрозу для корпоративных сред Active Directory. В реальной жизни эта атака выполняется следующим образом:

1. Компрометация контроллера домена: злоумышленник получает доступ к контроллеру домена через различные векторы атаки.
2. Кража хэша KRBTGT: с помощью инструментов вроде Mimikatz выполняется дамп хэша учетной записи KRBTGT.
3. Генерация тикета: используя украденный хэш, создается тикет Kerberos с произвольными параметрами.
4. Неограниченный доступ: сгенерированный тикет предоставляет доступ к любым ресурсам домена.