



**БЕЗОПАСНОСТЬ**  
информационных технологий  

---

**ФОРУМ - САНКТ-ПЕТЕРБУРГ**

Проблема автоматической  
классификации TLS-сессий с  
использованием цифровых отпечатков  
реализаций

Ишкуватов Сергей Маратович



## Классификация TLS-сессий по цифровым отпечаткам реализаций протоколов является важным инструментом мониторинга сетевой безопасности по следующим причинам:

1. Помогает выявить аномалии и необычную активность, которая может быть связана с атаками или нарушением безопасности в сети.
2. Обнаружение фактов использования уязвимого ПО.
3. Обнаружение фактов использования ПО запрещенного администратором сети.  
Обнаружение фактов использования средств анонимизации.
4. Обнаружение атак типа "Man-in-the-Middle".

## Классификация TLS-сессий возможна по:

- Конечные точки Extension ServerName (если используется)
- ServerName сертификата сервера
- Диапазоны IP-адресов сервера
- Цифровой отпечаток(ЦО) клиентской реализации TLS протокола (например JA3) + цифровой отпечаток TCP/IP

Используются в качестве признаков для блокировок РКН



```
Handshake Type: Client Hello (1)
Length: 508
Version: TLS 1.2 (0x0303)
Random: 1be3ee9fd5a4bb2f635dd8a25e0427ef9eb06286b4531dace32f59ab92a93033
Session ID Length: 32
Session ID: dbfe878dfb5e27f6ddcd27647dc7da2882df9ec1b8e5d27b7bae9a4c2f7d413c
Cipher Suites Length: 32
└─ Cipher Suites (16 suites)
  Cipher Suite: Reserved (GREASE) (0xcaca)
  Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
  Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
  Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
  Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
  Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
  Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
  Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
  Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xc03a)
  Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc03b)
  Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
  Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
  Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
  Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
  Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
  Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
Compression Methods Length: 1
└─ Compression Methods (1 method)
  Extensions Length: 403
└─ Extension: Reserved (GREASE) (len=0)
└─ Extension: server_name (len=11)
└─ Extension: extended_master_secret (len=0)
└─ Extension: renegotiation_info (len=1)
└─ Extension: supported_groups (len=10)
  Type: supported_groups (10)
  Length: 10
  Supported Groups List Length: 8
  └─ Supported Groups (4 groups)
    Supported Group: Reserved (GREASE) (0x1a1a)
    Supported Group: x25519 (0x001d)
    Supported Group: secp256r1 (0x0017)
    Supported Group: secp384r1 (0x0018)
└─ Extension: ec_point_formats (len=2)
└─ Extension: session_ticket (len=0)
└─ Extension: application_layer_protocol_negotiation (len=14)
└─ Extension: status_request (len=5)
└─ Extension: signature_algorithms (len=18)
└─ Extension: signed_certificate_timestamp (len=0)
└─ Extension: key_share (len=43)
└─ Extension: psk_key_exchange_modes (len=2)
└─ Extension: supported_versions (len=11)
└─ Extension: compress_certificate (len=3)
└─ Extension: Reserved (GREASE) (len=1)
└─ Extension: padding (len=214)
[JA3 Fullstring: 771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0]
[JA3: b32309a26951912be7dba376398abc3b]
```

## Что такое цифровой отпечаток реализации TLS

Под термином цифровой отпечаток реализации протокола TLS понимаются параметры, характеризующие именно эту конкретную реализацию протокола, конкретную версию библиотеки реализующий этот протокол (например Chromium, Android, .NET, Java) или группу возможных версий.



```
4 Internet Protocol Version 4
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▷ Differentiated Services Field: 0x60 (DSCP: CS3, ECN: Not-ECT)
  Total Length: 60
  Identification: 0xdb66 (56166)
  ▷ 010. .... = Flags: 0x2, Don't fragment
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 55
  Protocol: TCP (6)

1010 .... = Header Length: 40 bytes (10)
▷ Flags: 0x002 (SYN)
Window: 64240
[Calculated window size: 64240]
Urgent Pointer: 0
4 Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Oper
  ▷ TCP Option - Maximum segment size: 1460 bytes
  ▷ TCP Option - SACK permitted
  ▷ TCP Option - Timestamps
  ▷ TCP Option - No-Operation (NOP)
  ▷ TCP Option - Window scale: 7 (multiply by 128)
```

## Цифровой отпечаток TCP/IP

Под термином цифровой отпечаток TCP/IP понимаются параметры, определяемые ОС источника и маршрутом следования пакета.

## Наиболее популярные базы данных признаков

### Цифровые отпечатки TCP/IP:

- p0f – устарела;
- satori – обновляется, не учитывает связь MTU и TCP Maximum Segment Size;
- Nmap - только для ответов серверов, рассчитан на серию активных экспериментов.

### Цифровые отпечатки реализации TLS:

- JA3 – получила массовое распространение (Wireshark, Suricata, сервисы мониторинга ботнетов);
- Cisco Mercury – наиболее крупная открытая (~6000 записей), но больше не обновляется;
- Lee Brothers – устарела, обобщает классы реализаций.

## Недостатки существующих представлений

- в качестве информативных признаков используют только данные начального TLS-рукопожатия, но не описывают закономерности и типичные сценарии приёма/передачи;
- учитываются только четкие совпадения признаков;
- реализация TLS веб-браузера Chromium начиная с недавнего времени случайным образом перемешивает список Extensions, в результате чего ЦО одной из последних версий даёт факториал 14 возможных вариаций записи для одной реализации.

## Решение проблемы учета только четких совпадений признаков



$$\bullet \text{lev}(a, b) = \begin{cases} |a|, \text{ если } |b| = 0 \\ |b|, \text{ если } |a| = 0 \\ \text{lev}(\text{tail}(a), \text{tail}(b)), \text{ если } a[0] = b[0] \\ 1 + \min \begin{cases} \text{lev}(\text{tail}(a), b) \\ \text{lev}(a, \text{tail}(b)) \\ \text{lev}(\text{tail}(a), \text{tail}(b)) \end{cases}, \text{ в остальных случаях} \end{cases}$$

$$\text{distance}(a, b) = \sum_{i=0}^n s_i \Delta_i(a, b)$$

$n$  – количество возможных параметров ЦО, по которому производится сравнение;  
 $\Delta_i(a, b)$  – количественное значение отличия  $i$ -го параметра отпечатков  $a$  и  $b$ ;  
 $s_i$  – информативность  $i$ -го параметра.



# Расстояния Левенштейна для оценки близости цифровых отпечатков ЈАЗ



Искомый ЦО

Найденные ЦО соседи

Суммарное расстояние до искомого

| Finger  | ΔVer | ΔCS | ΔExt | ΔSuppGro | ΔPtF | ΣΔ       |
|---|------|-----|------|----------|------|----------|
| <b>771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-129-65413-156-157-47-53-10,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0</b> |      |     |      |          |      | <b>0</b> |
| 771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-129-65413-156-157-47-53-10,0-23-65281-10-11-35-16-5-13-18-51-45-43-27,29-23-24,0           | 0    | 0   | 1    | 0        | 0    | 1        |
| 771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-129-65413-156-157-47-53-10,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21-41,29-23-24,0     | 0    | 0   | 1    | 0        | 0    | 1        |
| 771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-129-65413-156-157-47-53-10,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-41,29-23-24,0        | 0    | 0   | 1    | 0        | 0    | 1        |
| 771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-129-65413-156-157-47-53-10,0-23-65281-10-11-35-5-13-18-51-45-43-27-21,29-23-24,0           | 0    | 0   | 2    | 0        | 0    | 2        |
| 771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-129-65413-156-157-47-53-10,0-23-65281-10-11-35-5-13-18-51-45-43-27-21-41,29-23-24,0        | 0    | 0   | 2    | 0        | 0    | 2        |
| 771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,,,  | 0    | 2   | 0    | 0        | 0    | 2        |
| 771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0                  | 0    | 2   | 0    | 0        | 0    | 2        |
| 771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0                     | 0    | 3   | 0    | 0        | 0    | 3        |
| 771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,0-23-65281-10-11-35-16-5-13-18-30032-51-45-43-27-21,29-23-24,0            | 0    | 2   | 1    | 0        | 0    | 3        |
| 771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,0-23-65281-10-11-35-16-5-13-18-51-45-43-21,29-23-24,0                     | 0    | 2   | 1    | 0        | 0    | 3        |
| 771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-17513-21,29-23-24,0            | 0    | 2   | 1    | 0        | 0    | 3        |
| 771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-21-41,29-23-24,0               | 0    | 2   | 1    | 0        | 0    | 3        |
| 771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-219,29-23-24,0                 | 0    | 2   | 1    | 0        | 0    | 3        |
| 771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-22,29-23-24,0                  | 0    | 2   | 1    | 0        | 0    | 3        |
| 771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-41,29-23-24,0                  | 0    | 2   | 1    | 0        | 0    | 3        |
| 771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-44510,29-23-24,0               | 0    | 2   | 1    | 0        | 0    | 3        |
| 771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-54538-21,29-23-24,0            | 0    | 2   | 1    | 0        | 0    | 3        |
| 771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,0-23-65281-10-11-35-5-13-18-51-45-43-27-21,29-23-24,0                     | 0    | 2   | 1    | 0        | 0    | 3        |
| 771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,23-65281-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0                    | 0    | 2   | 1    | 0        | 0    | 3        |
| 771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,0-23-65281-10-11-35-16-5-13-18-30032-51-45-43-27,29-23-24,0               | 0    | 2   | 2    | 0        | 0    | 4        |
| 771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,0-23-65281-10-11-35-16-5-13-18-30032-51-45-43-27-41,29-23-24,0            | 0    | 2   | 2    | 0        | 0    | 4        |
| 771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,0-23-65281-10-11-35-16-5-13-18-51-45-42-43-27-41,29-23-24,0               | 0    | 2   | 2    | 0        | 0    | 4        |
| 771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,0-23-65281-10-11-35-16-5-13-18-51-45-43-27,29-23-24,0                     | 0    | 2   | 2    | 0        | 0    | 4        |
| 771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-10833,29-23-24,0               | 0    | 2   | 2    | 0        | 0    | 4        |
| 771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-54538-21-41,29-23-24,0         | 0    | 2   | 2    | 0        | 0    | 4        |
| 771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,0-23-65281-10-11-35-16-5-13-18-51-45-43-27-54538-41,29-23-24,0            | 0    | 2   | 2    | 0        | 0    | 4        |
| 771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,0-23-65281-10-11-35-16-5-13-18-51-45-43-41,29-23-24,0                     | 0    | 2   | 2    | 0        | 0    | 4        |
| 771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,0-23-65281-10-11-35-5-13-18-30032-51-45-43-27-21,29-23-24,0               | 0    | 2   | 2    | 0        | 0    | 4        |
| 771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,0-23-65281-10-11-35-5-13-18-51-45-43-27,29-23-24,0                        | 0    | 2   | 2    | 0        | 0    | 4        |
| 771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53-10,0-23-65281-10-11-35-5-13-18-51-45-43-27-21-41,29-23-24,0                  | 0    | 2   | 2    | 0        | 0    | 4        |



# Решение проблемы перемешивания параметров реализациями Google

Для всех реализаций, содержащих значения GREASE(Generate Random Extensions And Sustain Extensibility), перед хешированием сортировать список Extensions. Это позволит сохранить совместимость новых записей со всеми старыми записями, практически не увеличивая риски возникновения коллизий и позволит описать все возможные комбинации.

```
771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-45-51-17513-43-16-11-13-18-65281-23-35-27-10-5-21,29-23-24,0
771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-5-10-11-18-65281-45-51-23-17513-43-27-35-13-16-21,29-23-24,0
771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-5-17513-43-10-11-27-45-65281-13-51-23-18-16-35-21,29-23-24,0
771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-5-45-43-18-27-23-65281-35-13-16-17513-11-10-51-21,29-23-24,0
771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-5-65281-16-35-10-18-27-45-13-51-23-43-11-17513-21,29-23-24,0
771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-51-45-10-11-43-16-17513-13-23-65281-27-18-5-35-41,29-23-24,0
771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,10-13-65281-17513-35-0-43-16-5-23-11-27-18-51-45-21,29-23-24,0
771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,10-17513-5-13-18-23-11-27-51-43-16-45-65281-0-35-21,29-23-24,0
771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,10-18-5-45-16-0-13-23-17513-43-65281-11-35-27-51-21,29-23-24,0
771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,10-35-0-23-5-43-13-65281-11-45-16-27-17513-18-51-21,29-23-24,0
771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,10-45-18-13-5-16-51-0-27-65281-17513-43-35-11-23-21,29-23-24,0
771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,10-45-65281-0-16-18-43-35-5-13-51-23-27-11-17513-21,29-23-24,0
771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,10-51-17513-0-5-43-11-27-16-18-35-23-13-65281-45-21,29-23-24,0
771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,11-10-17513-51-65281-35-0-18-45-13-23-16-43-5-27-21,29-23-24,0
Handshake Protocol: Client Hello
  Handshake Type: Client Hello (1)
  Length: 508
  Version: TLS 1.2 (0x0303)
  Random: 04744cd923231bbe9b22fbdafadc8e87bd445efdc32554ae4b84deb4445682
  Session ID Length: 32
  Session ID: 81302fe30a746e0e5a1656435ceb5e9312f2b33186da511d0b4a85df398d8e40
  Cipher Suites Length: 32
  Cipher Suites (16 suites)
  Compression Methods Length: 1
  Compression Methods (1 method)
  Extensions Length: 403
  > Extension: Reserved (GREASE) (len=0)
  > Extension: server_name (len=21)
  > Extension: psk_key_exchange_modes (len=2)
  > Extension: key_share (len=43)
  > Extension: application_settings (len=5)
  > Extension: supported_versions (len=7)
  > Extension: application_layer_protocol_negotiation (len=14)
  > Extension: ec_point_formats (len=2)
  > Extension: signature_algorithms (len=18)
  > Extension: signed_certificate_timestamp (len=0)
  > Extension: renegotiation_info (len=1)
  > Extension: extended_master_secret (len=0)
  > Extension: session_ticket (len=0)
  > Extension: compress_certificate (len=3)
  > Extension: supported_groups (len=10)
  > Extension: status_request (len=5)
  > Extension: Reserved (GREASE) (len=1)
  > Extension: padding (len=199)
[JA3 Fullstring: 771,4865-4866-4867-49195-49199-49196-49200-52393-52392-49171-49172-156-157-47-53,0-45-51-17513-43-16-11-13-18-65281-23-35-27-10-5-21,29-23-24,0]
```



# Спасибо

Контактные данные



Ишкуватов Сергей Маратович



sysroot0@gmail.com



+79062511672