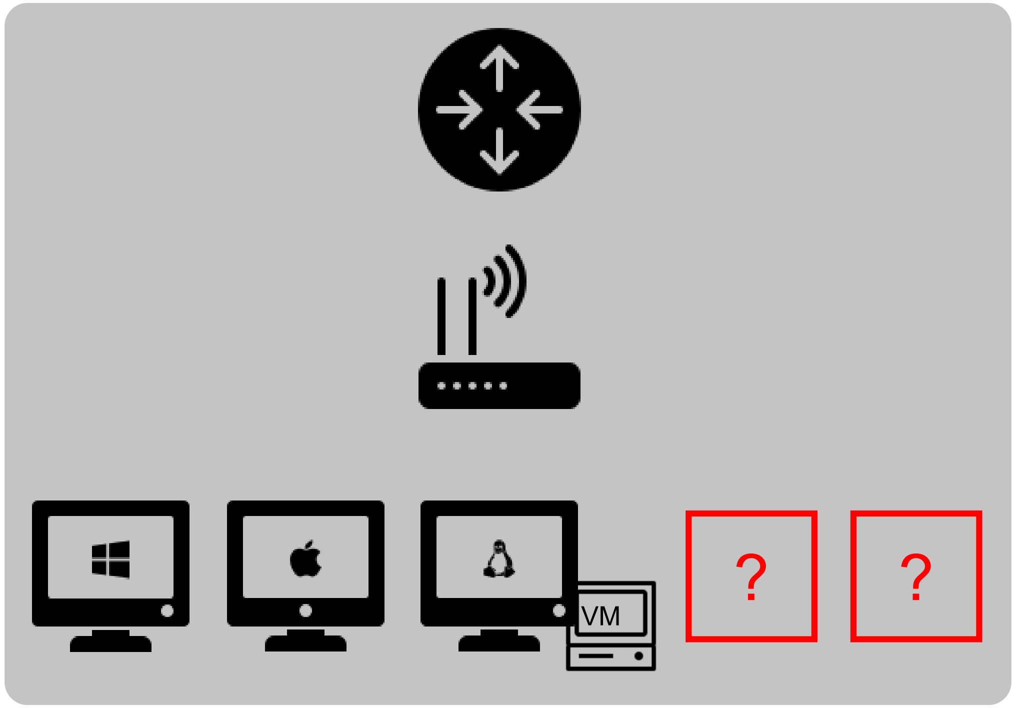
# The Generation and Use of TLS Fingerprints

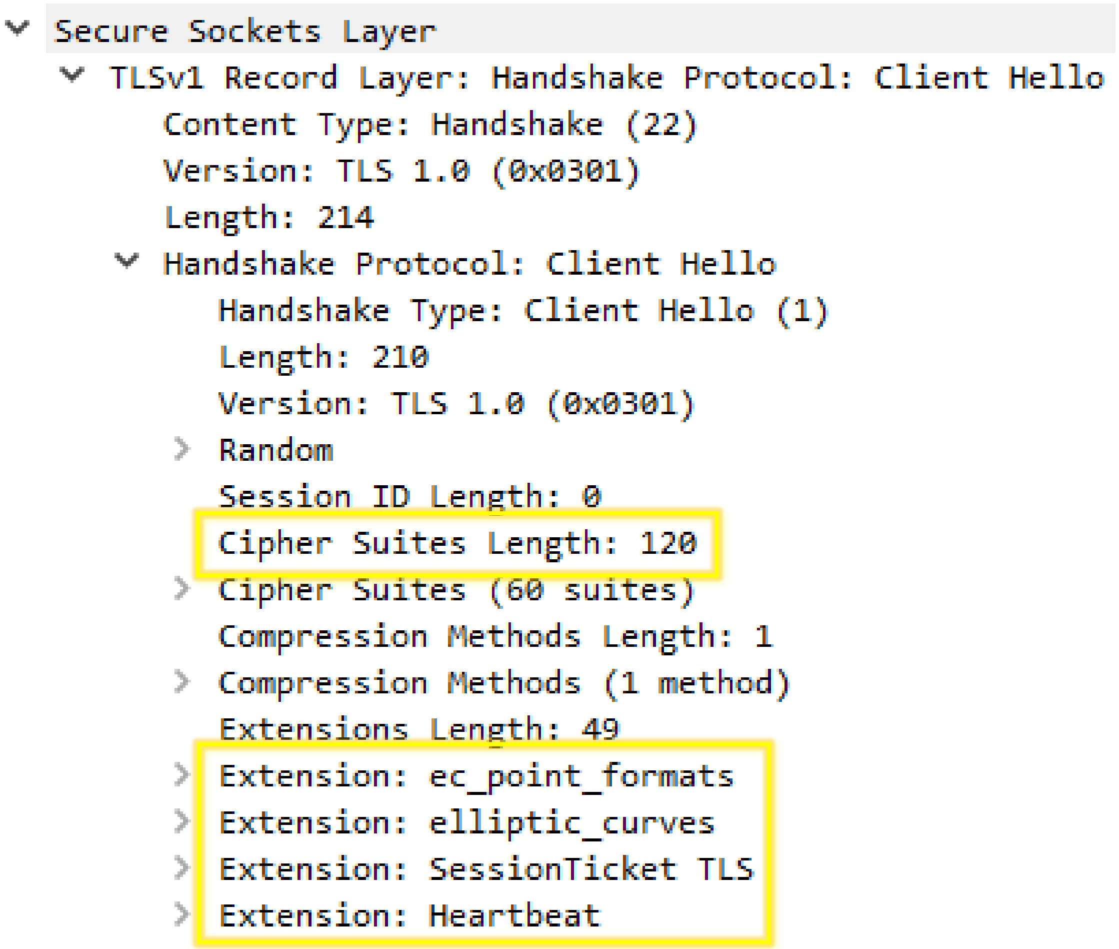
Blake Anderson, PhD; David McGrew, PhD; Keith Schomburg

Cisco

# Reducing the Visibility Gap



# TLS Fingerprinting Overview



```
Secure Sockets Layer
  TLSv1 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 214
    Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 210
      Version: TLS 1.0 (0x0301)
      Random
      Session ID Length: 0
      Cipher Suites Length: 120
      Cipher Suites (60 suites)
      Compression Methods Length: 1
      Compression Methods (1 method)
      Extensions Length: 49
      Extension: ec_point_formats
      Extension: elliptic_curves
      Extension: SessionTicket TLS
      Extension: Heartbeat
```

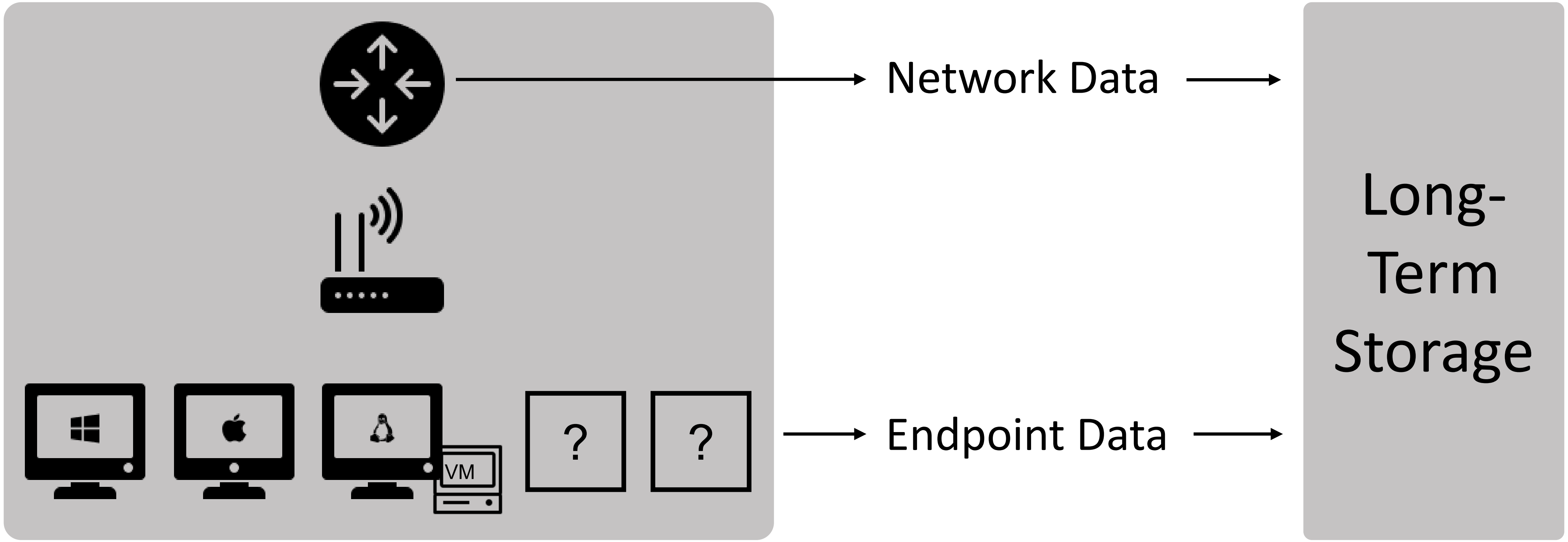
- TLS parameters offered in the ClientHello can provide library/process attribution [1-6]
- Applications
  - Network forensics
  - Malware detection [2]
  - Identifying obsolete/vulnerable software
  - OS fingerprinting [3]
- Advantages
  - No endpoint agent required
  - Completely passive

# Fingerprinting Goals

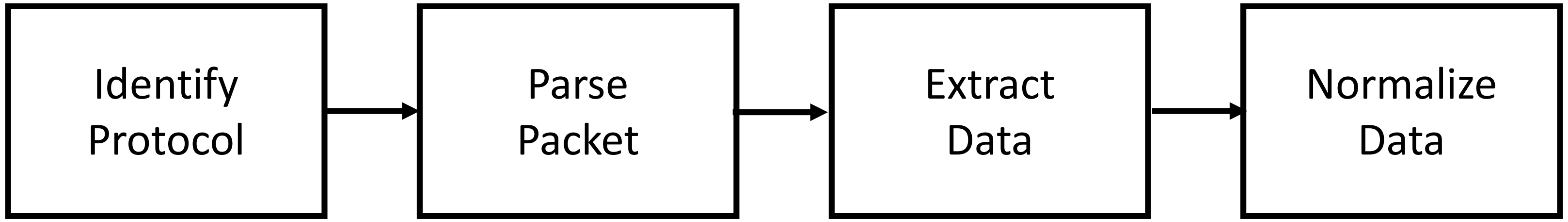
| | |
|---|---|
| Efficacy | • Maximize discerning power by including all informative data features |
| Flexibility | • Enable approximate matching where needed |
| Compatibility | • Accommodate missing data and new protocol features |
| Reversibility | • Fingerprint format is interpretable and forensically sound |
| Performance | • Fast and compact extraction and matching |

# Network and Endpoint Data Fusion

- Problem: Current fingerprint databases are slow to update and lack real-world, contextual data.
- Solution: Continuously and automatically fuse network and endpoint data.



# TLS Feature Extraction and Pre-Processing



- Cipher Suites
  - Generalize GREASE cipher suites: 0x0a0a,...,0xfafa -> GREASE
- Extensions
  - Generalize GREASE extension types/data
    - 0x0a0a,...,0xfafa -> GREASE
  - Remove session specific extension data
    - server_name, padding, session_ticket

# Comparison with Previous Work

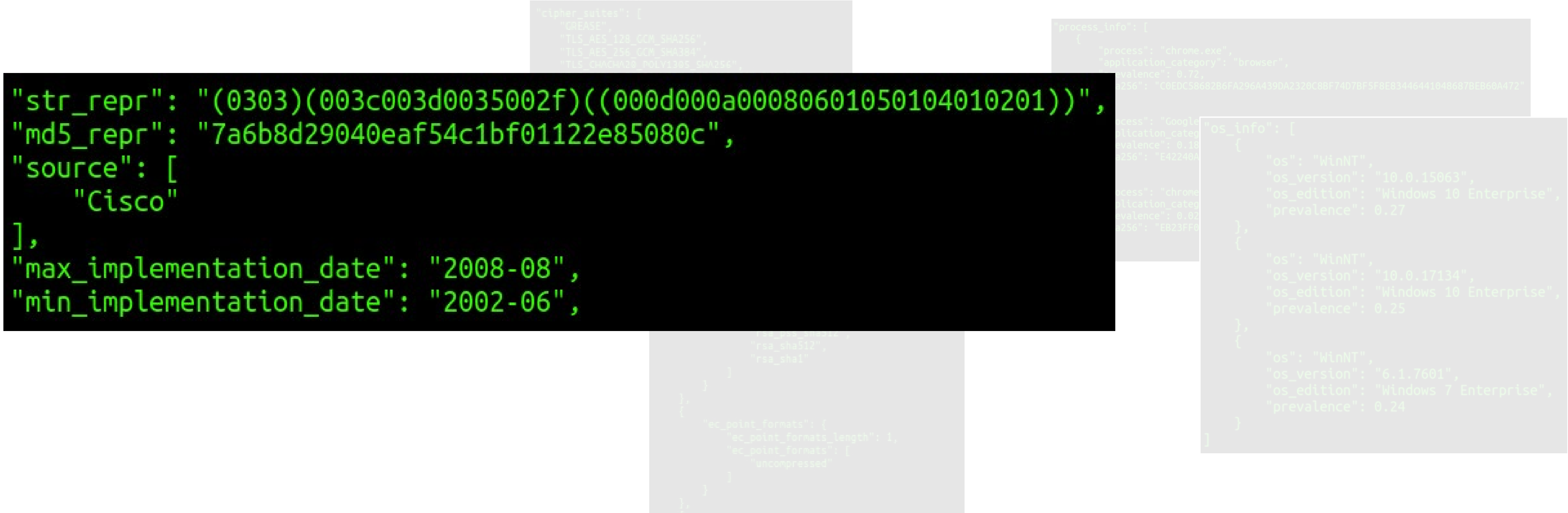
| | Database Size | Automatically Updated | GREASE Support | Static Extension Data |
|---|---|---|---|---|
| Our Work | ~1,500 | Yes | Yes | supported_groups<br>ec_point_formats<br>status_request<br>signature_algorithms<br>application_layer_protocol_negotiation<br>supported_versions<br>psk_key_exchange_modes |
| Kotzias et al. [4] | ~1,684 | No | Discards Locality | supported_groups<br>ec_point_formats |
| JA3 [5] | 158 | No | Discards All Data | supported_groups<br>ec_point_formats |
| FingerprinTLS [6] | 409 | No | No | supported_groups<br>ec_point_formats<br>signature_algorithms |

# TLS Fingerprint Database Schema

Metadata

TLS Information

Attribution



```
"str_repr": "(0303)(003c003d0035002f)((000d000a00080601050104010201))",
"md5_repr": "7a6b8d29040eaf54c1bf01122e85080c",
"source": [
    "Cisco"
],
"max_implementation_date": "2008-08",
"min_implementation_date": "2002-06",
```

```
"cipher_suites": [
    "GREASE",
    "TLS_AES_128_GCM_SHA256",
    "TLS_AES_256_GCM_SHA384",
    "TLS_CHACHA20_POLY1305_SHA256",
```

```
                "rsa_pss_sha512",
                "rsa_sha512",
                "rsa_sha1"
            ]
        }
    },
    {
        "ec_point_formats": {
            "ec_point_formats_length": 1,
            "ec_point_formats": [
                "uncompressed"
            ]
        }
    },
```

```
"process_info": [
    {
        "process": "chrome.exe",
        "application_category": "browser",
        "prevalence": 0.72,
        "sha256": "C0EDC58682B6FA296A439DA2320C8BF74D7BF5F8E8344644104868 7BEB60A472"
```

```
        ocess": "Google
        plication_categ
        evalence": 0.18
        a256": "E42240A

        ocess": "chrome
        plication_categ
        evalence": 0.02
        a256": "EB23FF0
```

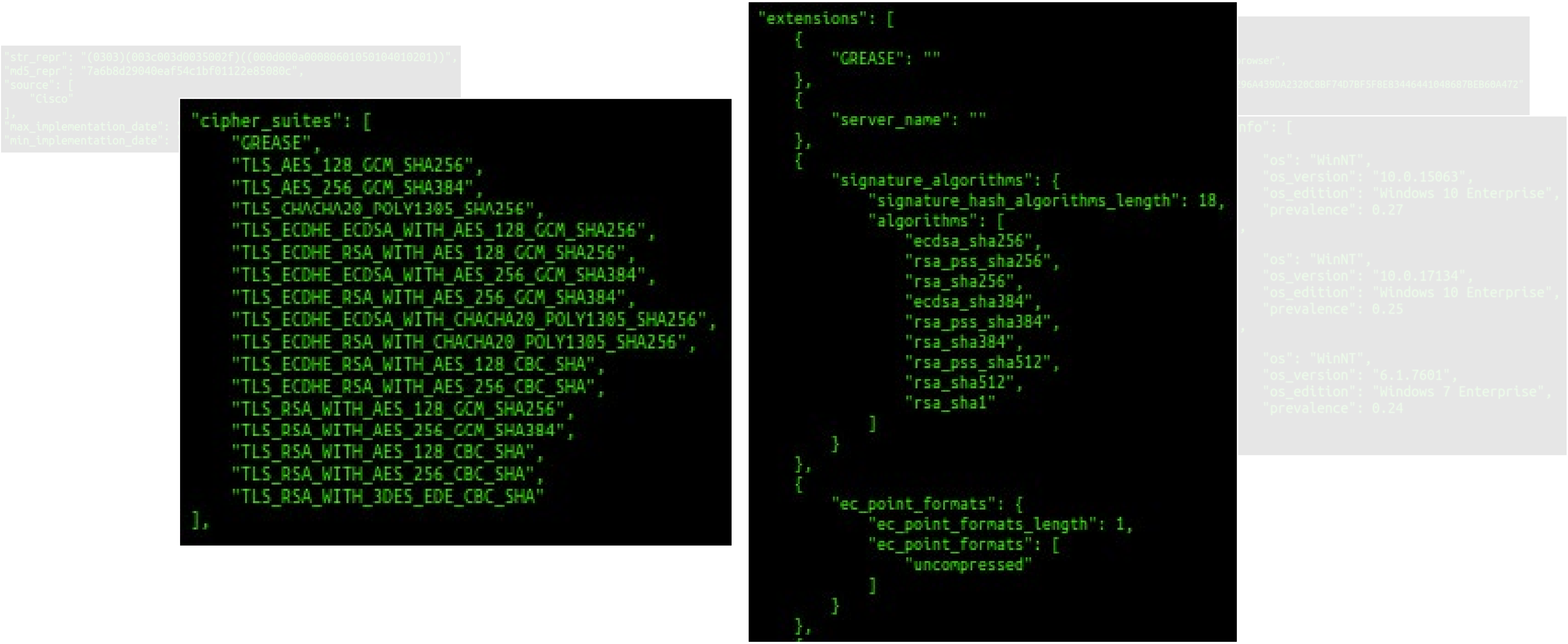
```
"os_info": [
    {
        "os": "WinNT",
        "os_version": "10.0.15063",
        "os_edition": "Windows 10 Enterprise",
        "prevalence": 0.27
    },
    {
        "os": "WinNT",
        "os_version": "10.0.17134",
        "os_edition": "Windows 10 Enterprise",
        "prevalence": 0.25
    },
    {
        "os": "WinNT",
        "os_version": "6.1.7601",
        "os_edition": "Windows 7 Enterprise",
        "prevalence": 0.24
    }
]
```

# TLS Fingerprint Database Schema

Metadata

TLS Information

Attribution



```
"str_repr": "(0303)(003c003d0035002f)((000d000a00080601050104010201))",
"md5_repr": "7a6b8d29040eaf54c1bf01122e85080c",
"source": [
    "Cisco"
],
"max_implementation_date":
"min_implementation_date":
```

```
"cipher_suites": [
    "GREASE",
    "TLS_AES_128_GCM_SHA256",
    "TLS_AES_256_GCM_SHA384",
    "TLS_CHACHA20_POLY1305_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256",
    "TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA",
    "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA",
    "TLS_RSA_WITH_AES_128_GCM_SHA256",
    "TLS_RSA_WITH_AES_256_GCM_SHA384",
    "TLS_RSA_WITH_AES_128_CBC_SHA",
    "TLS_RSA_WITH_AES_256_CBC_SHA",
    "TLS_RSA_WITH_3DES_EDE_CBC_SHA"
],
```

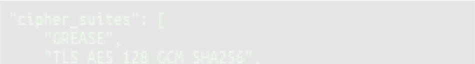
```
"extensions": [
    {
        "GREASE": ""
    },
    {
        "server_name": ""
    },
    {
        "signature_algorithms": {
            "signature_hash_algorithms_length": 18,
            "algorithms": [
                "ecdsa_sha256",
                "rsa_pss_sha256",
                "rsa_sha256",
                "ecdsa_sha384",
                "rsa_pss_sha384",
                "rsa_sha384",
                "rsa_pss_sha512",
                "rsa_sha512",
                "rsa_sha1"
            ]
        }
    },
    {
        "ec_point_formats": {
            "ec_point_formats_length": 1,
            "ec_point_formats": [
                "uncompressed"
            ]
        }
    },
```

```
browser",

296A439DA2320C8BF74D7BF5F8E83446441048687BEB60A472"
```

```
nfo": [

    "os": "WinNT",
    "os_version": "10.0.15063",
    "os_edition": "Windows 10 Enterprise",
    "prevalence": 0.27
,

    "os": "WinNT",
    "os_version": "10.0.17134",
    "os_edition": "Windows 10 Enterprise",
    "prevalence": 0.25
,

    "os": "WinNT",
    "os_version": "6.1.7601",
    "os_edition": "Windows 7 Enterprise",
    "prevalence": 0.24
```

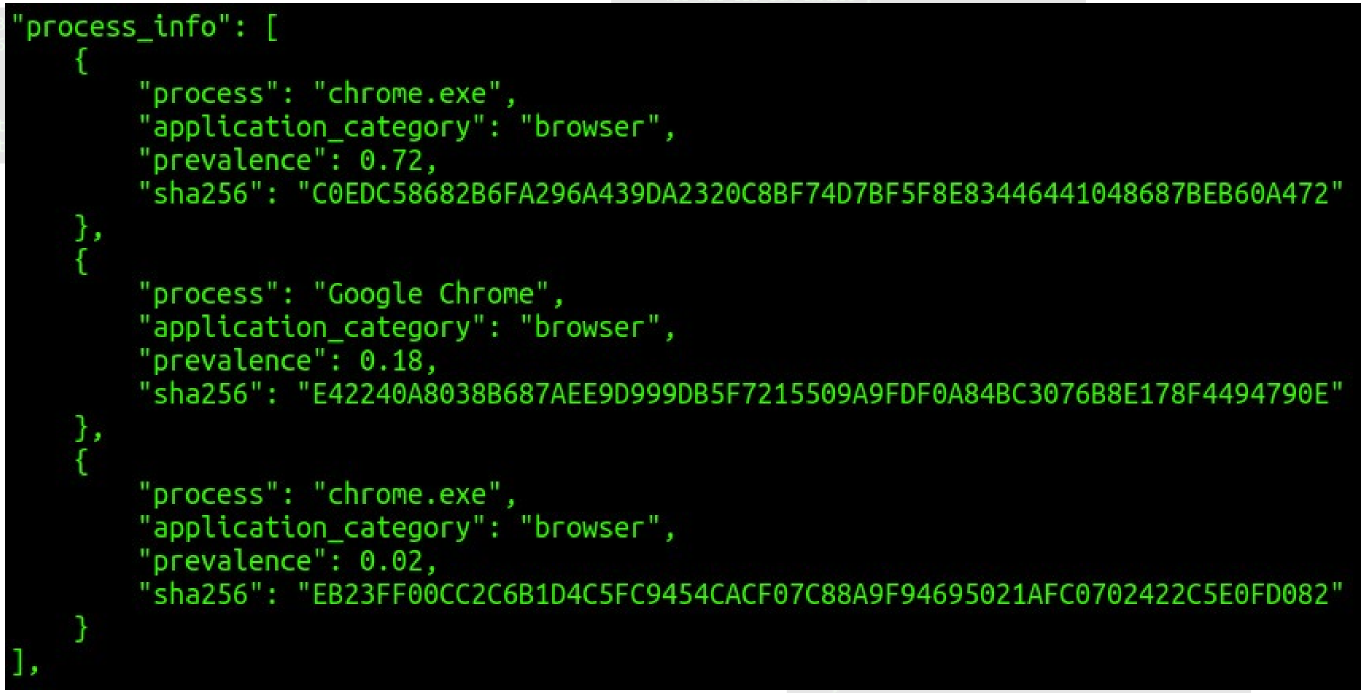
# TLS Fingerprint Database Schema

Metadata TLS Information **Attribution**

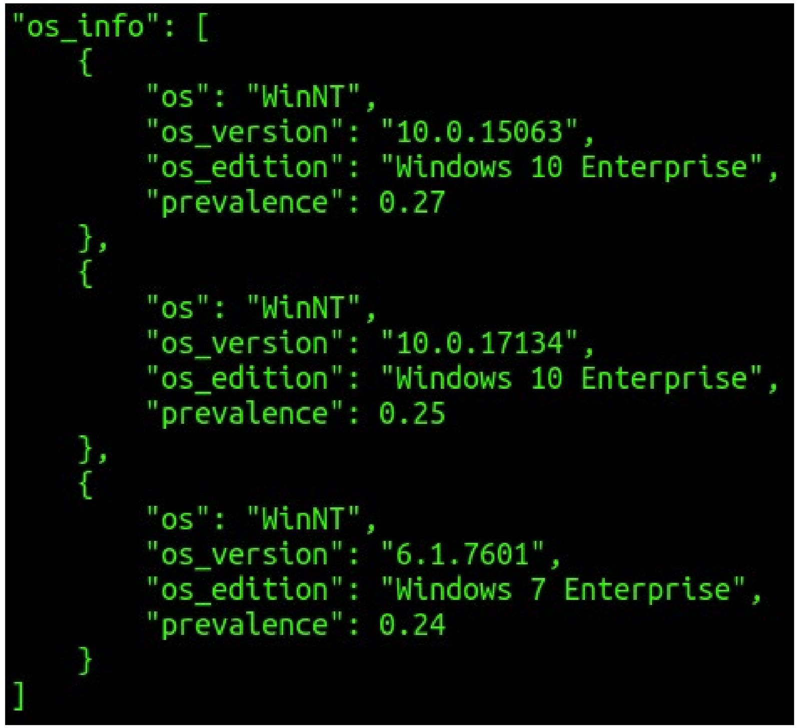


```
"cipher_suites": [
    "GREASE",
    "TLS_AES_128_GCM_SHA256",
```

```
"str_repr": "(03
"md5_repr": "7a6
"source": [
    "Cisco"
],
"max_implementat
"min_implementat
```



```
"process_info": [
    {
        "process": "chrome.exe",
        "application_category": "browser",
        "prevalence": 0.72,
        "sha256": "C0EDC58682B6FA296A439DA2320C8BF74D7BF5F8E83446441048687BEB60A472"
    },
    {
        "process": "Google Chrome",
        "application_category": "browser",
        "prevalence": 0.18,
        "sha256": "E42240A8038B687AEE9D999DB5F7215509A9FDF0A84BC3076B8E178F4494790E"
    },
    {
        "process": "chrome.exe",
        "application_category": "browser",
        "prevalence": 0.02,
        "sha256": "EB23FF00CC2C6B1D4C5FC9454CACF07C88A9F94695021AFC0702422C5E0FD082"
    }
],
```

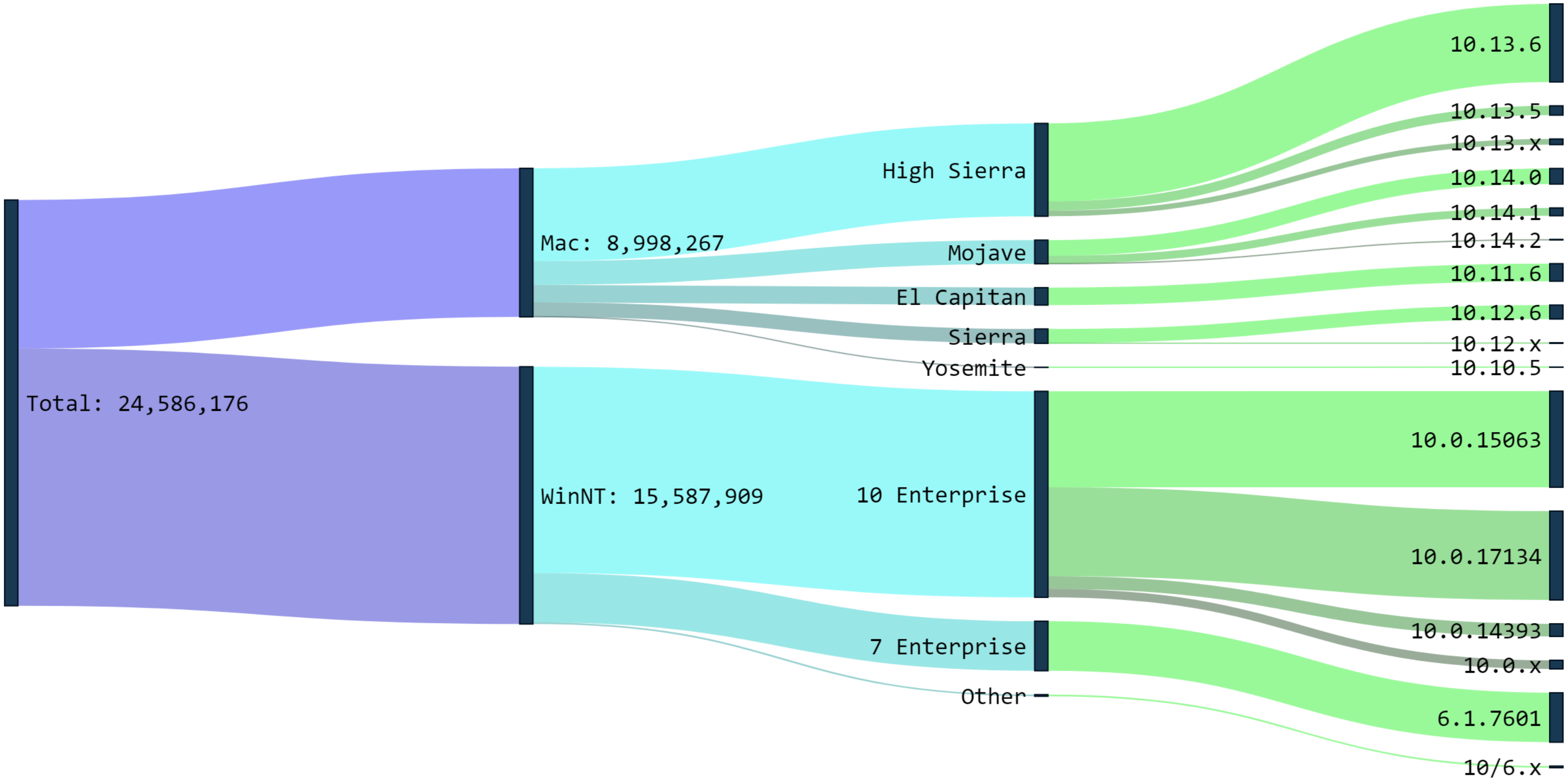


```
"os_info": [
    {
        "os": "WinNT",
        "os_version": "10.0.15063",
        "os_edition": "Windows 10 Enterprise",
        "prevalence": 0.27
    },
    {
        "os": "WinNT",
        "os_version": "10.0.17134",
        "os_edition": "Windows 10 Enterprise",
        "prevalence": 0.25
    },
    {
        "os": "WinNT",
        "os_version": "6.1.7601",
        "os_edition": "Windows 7 Enterprise",
        "prevalence": 0.24
    }
]
```

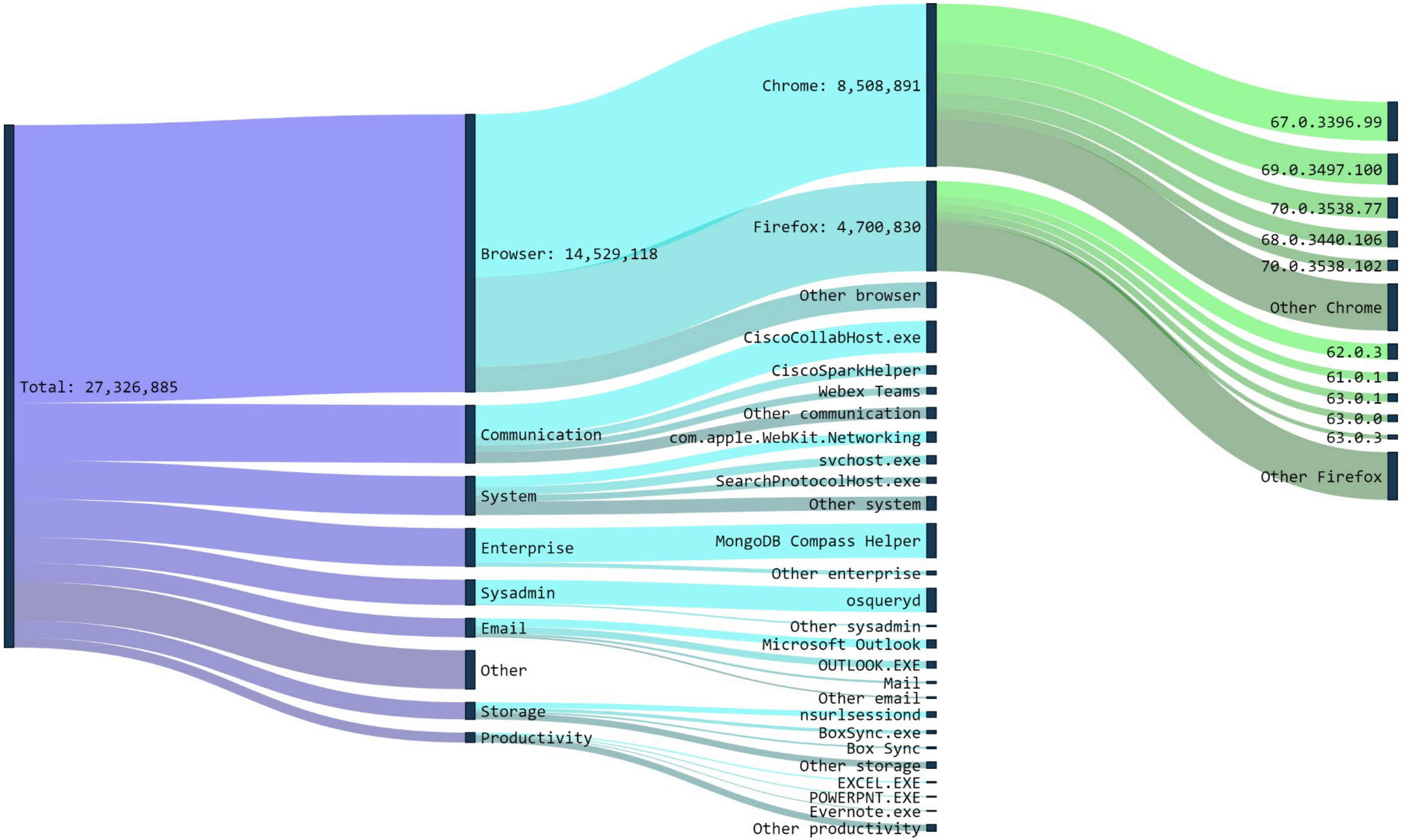
# General Stats

- Generated from 30M+ real-world TLS sessions
- 1,567 fingerprints
  - 454 unique cipher suite vectors
  - 1,092 unique cipher suite + extension type vectors
- 12,644 unique process hashes
  - 2,411 unique process names

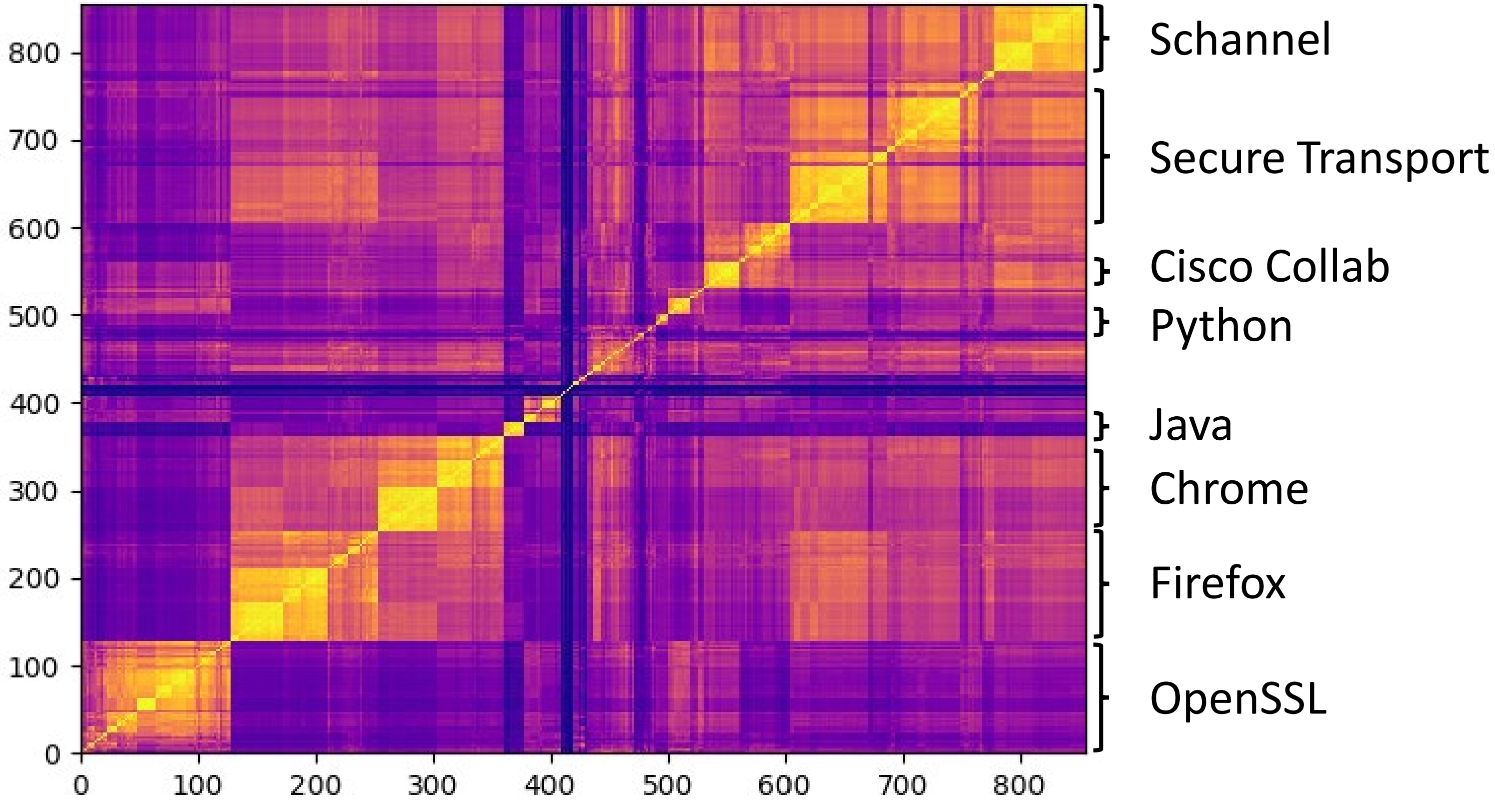
# Operating System Representation



# Application Representation



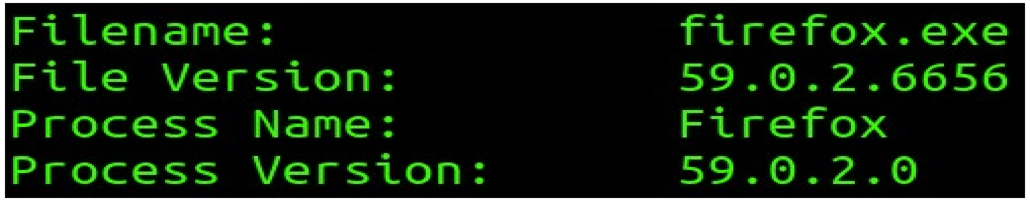
# Similarity Matrix



# Approximate TLS Fingerprinting

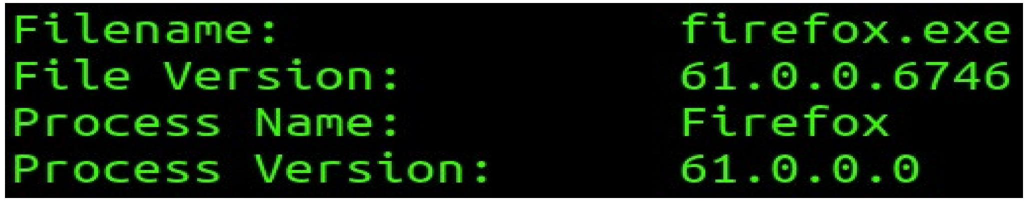
- String alignment over TLS features

True Label



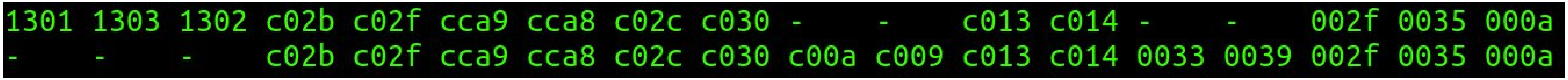
```
Filename:                     firefox.exe
File Version:                 59.0.2.6656
Process Name:                 Firefox
Process Version:              59.0.2.0
```

Inferred Label



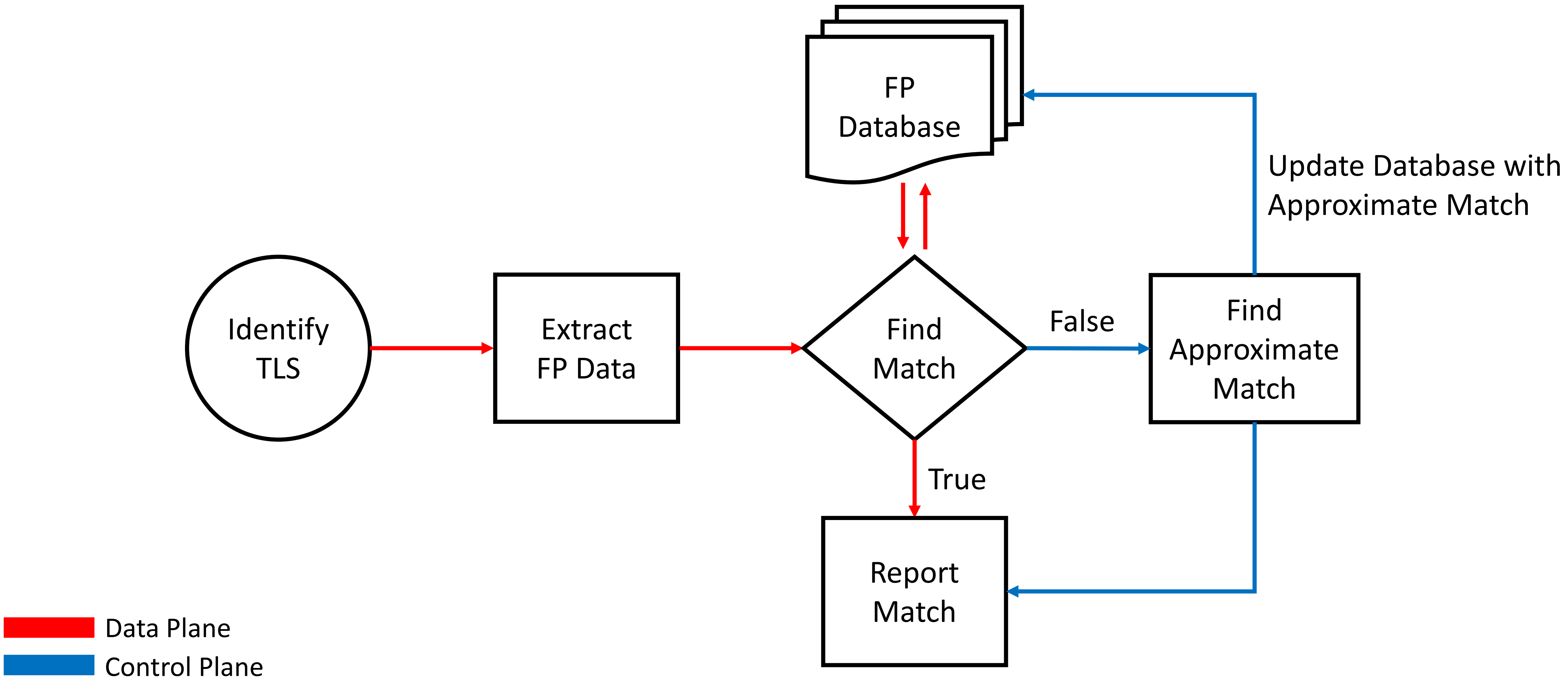
```
Filename:                     firefox.exe
File Version:                 61.0.0.6746
Process Name:                 Firefox
Process Version:              61.0.0.0
```

Alignment

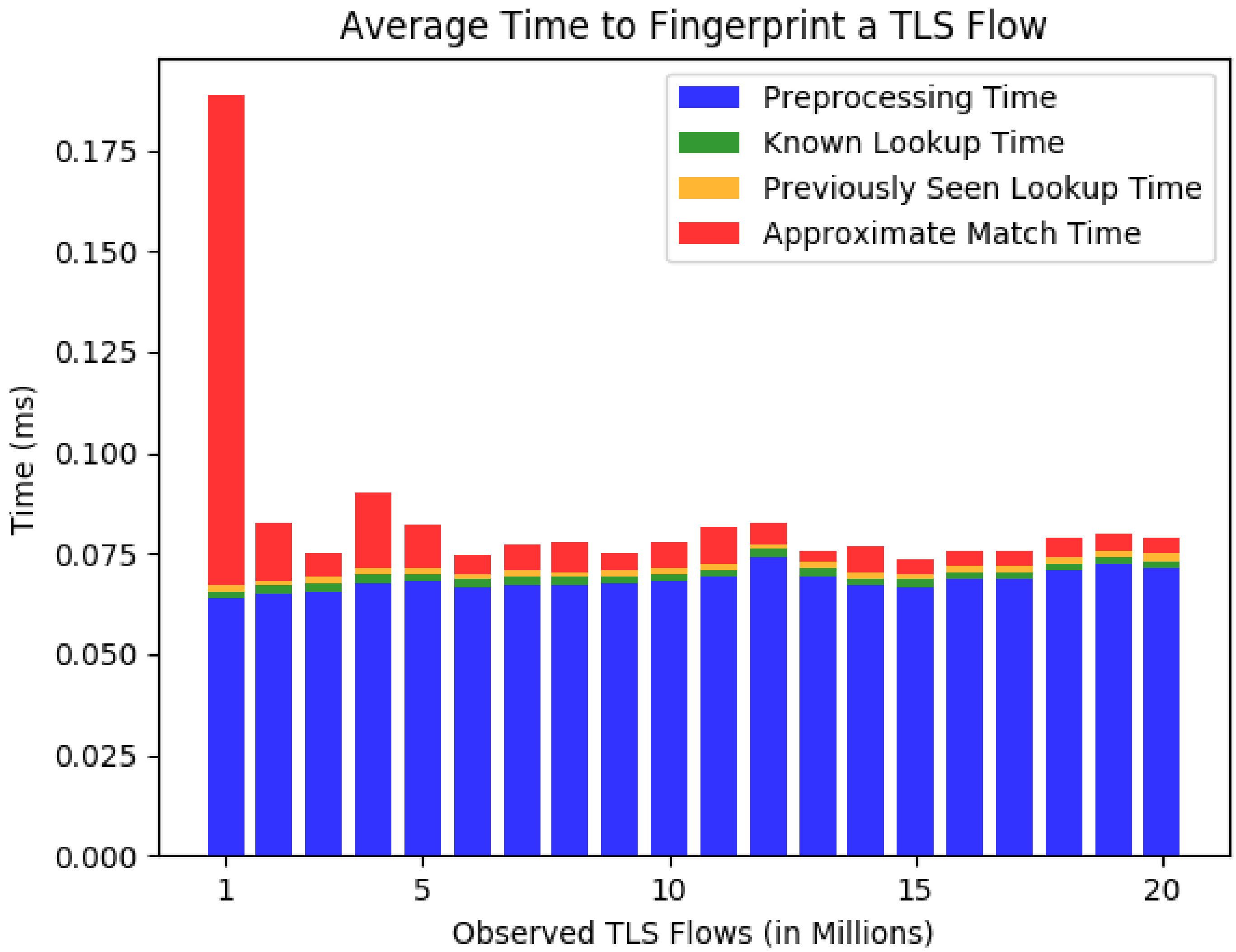


```
1301 1303 1302 c02b c02f cca9 cca8 c02c c030 -    -    c013 c014 -    -    002f 0035 000a
-    -    -    c02b c02f cca9 cca8 c02c c030 c00a c009 c013 c014 0033 0039 002f 0035 000a
```

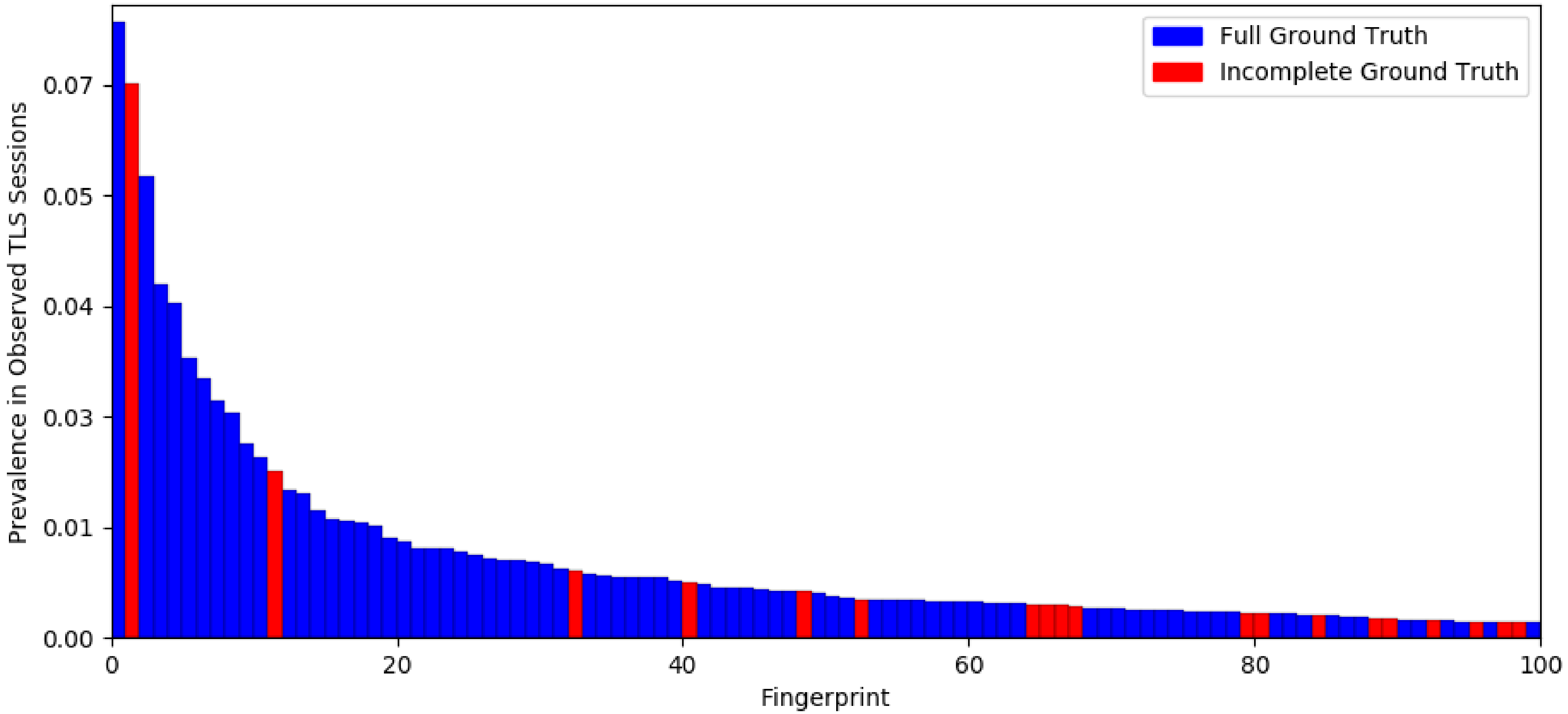
# Fingerprint Matching Overview



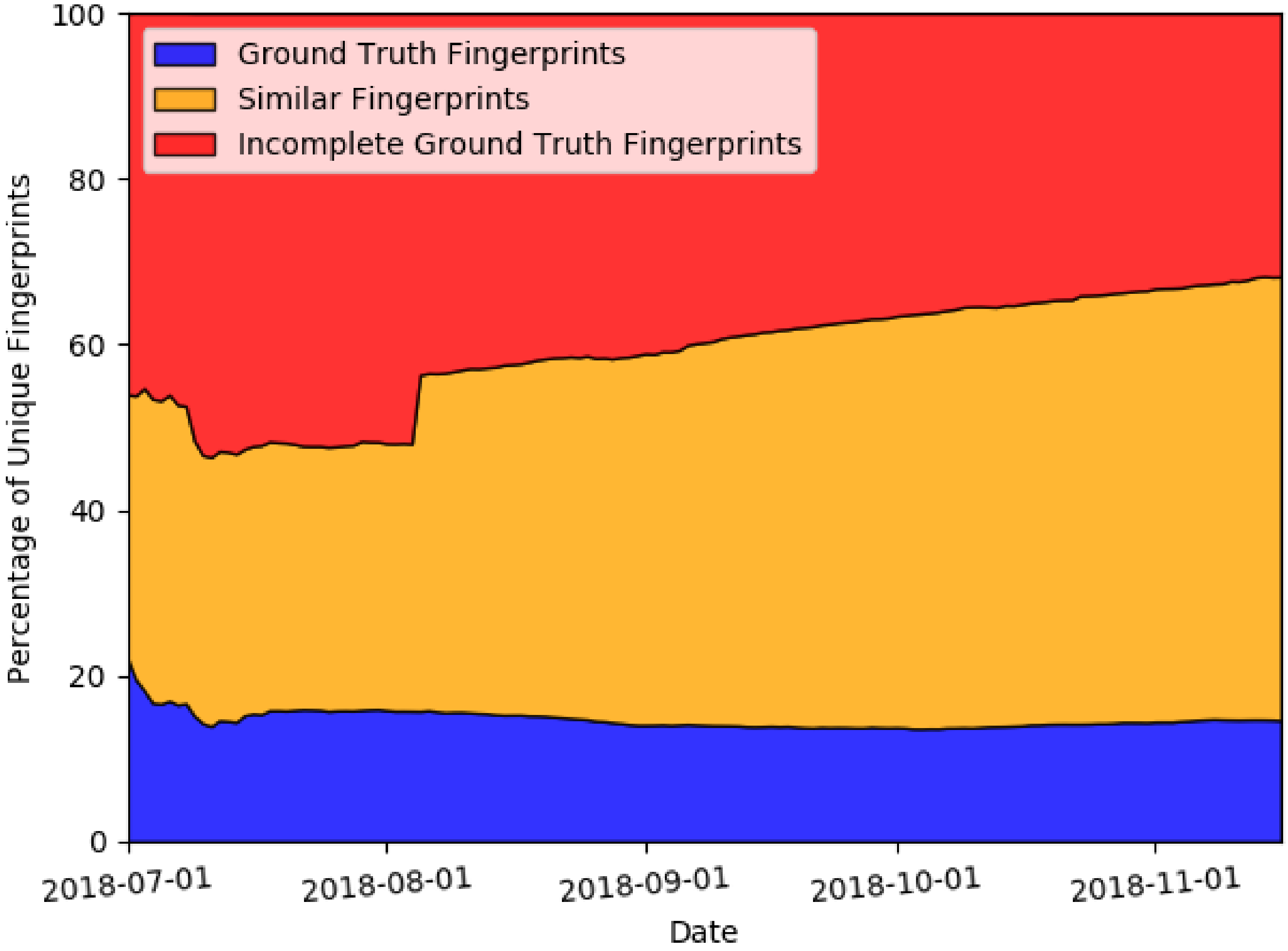
# Performance (Unoptimized Python)



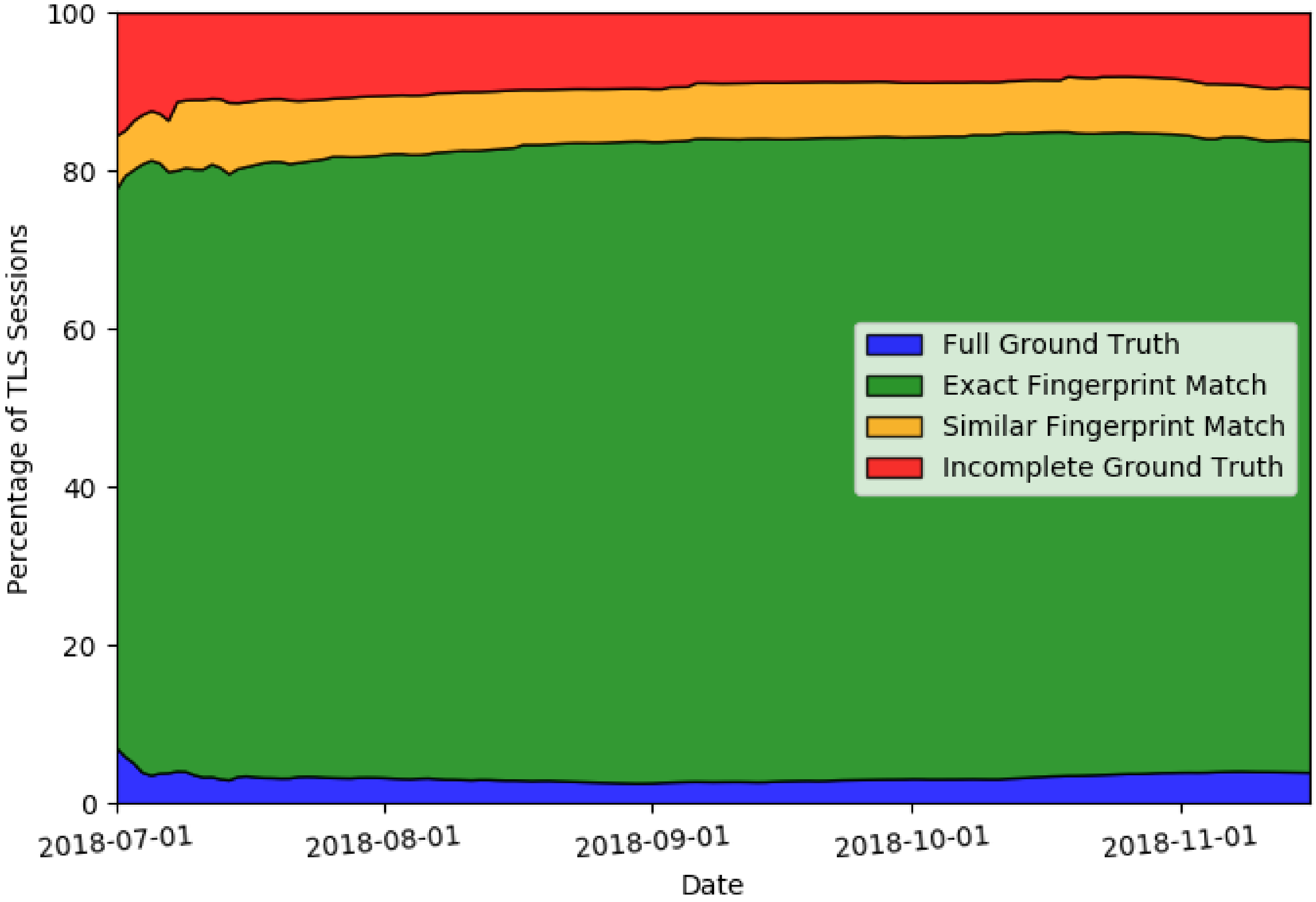
# Fingerprint Prevalence



# TLS Fingerprint Visibility



# TLS Session Visibility



# Implementation

- Fingerprint database and relevant code has been open-sourced:
  - https://github.com/cisco/joy
- Joy
  - Packet parsing and fingerprint extraction
- Python Scripts
  - Exact and approximate matching
  - Generation of custom fingerprint database from Joy output

# Next Steps

- More data!
  - iOS, Android, and Linux
- Incorporate other fingerprint databases
- Time window analysis

# References

[1] https://github.com/cisco/joy

[2] Blake Anderson, Subharthi Paul, David McGrew; Deciphering Malware's Use of TLS (without Decryption); arxiv, 2016; Journal of Computer Virology and Hacking Techniques, 2017.

[3] Blake Anderson, David McGrew; OS Fingerprinting: New Techniques and a Study of Information Gain and Obfuscation; IEEE CNS 2017, https://arxiv.org/abs/1706.08003

[4] Platon Kotzias, Abbas Razaghpanah, Johanna Amann, Kenneth G. Paterson, Narseo Vallina-Rodriguez, Juan Caballero; Coming of Age: A Longitudinal Study of TLS Deployment; IMC, 2018

[5] John B. Althouse, Jeff Atkinson, Josh Atkins; JA3 – A Method for Profiling SSL/TLS Clients

[6] Lee Brotherston; FingerprinTLS

# Thank You