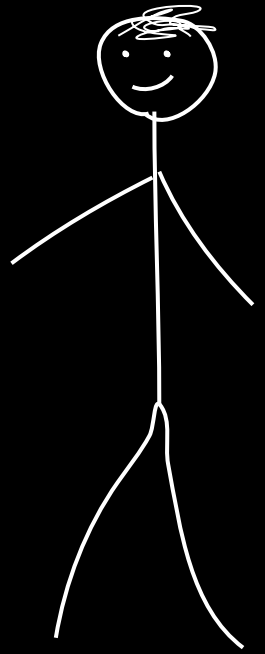
FOX10

John



Today I will show you…

What is JA4+?

How to use JA4+ to identify:

- Suspicious/Malicious connections through Res Proxies
- Bots
- AI Agents / MCP
- Exploit tools, Zero-Days
- DDoS tools
- Malware
- Devices and software on the network
- Malicious servers / C2s on the Internet
- Reverse Shells



JA4+ Network Fingerprinting

JA4+ Fingerprinting Suite

- JA4 - TLS Client Fingerprinting
- JA4Server - TLS Server Response Fingerprinting
- JA4HTTP - HTTP Client Fingerprinting
- JA4Latency - Light Distance/Latency Measuring Client
- JA4LatencyServer - Light Distance/Latency Measuring Server
- JA4X509 - X509 TLS Certificate Fingerprinting
- JA4SSH - SSH Traffic Fingerprinting
- JA4TCP - TCP OS/Device/Application Fingerprinting
- JA4TCPServer - TCP Server Response Fingerprinting
- JA4TCPScan - Active TCP Fingerprinting
- JA4DHCP - DHCP Fingerprinting
- JA4DHCPv6 - DHCPv6 Fingerprinting
- JA4Scan-TLS - Active TLS Server Fingerprint Scanner
- JA4Scan-QUIC - Active QUIC Server Fingerprint Scanner
- JA4NTP - NTP Fingerprinting
- JA4MCP - MCP Client Fingerprint
- JA4MCPServer - MCP Server Fingerprint
- JA4MCP.Behavior - MCP Behavior Fingerprint
- With more in development …

JA4+ Fingerprinting Suite

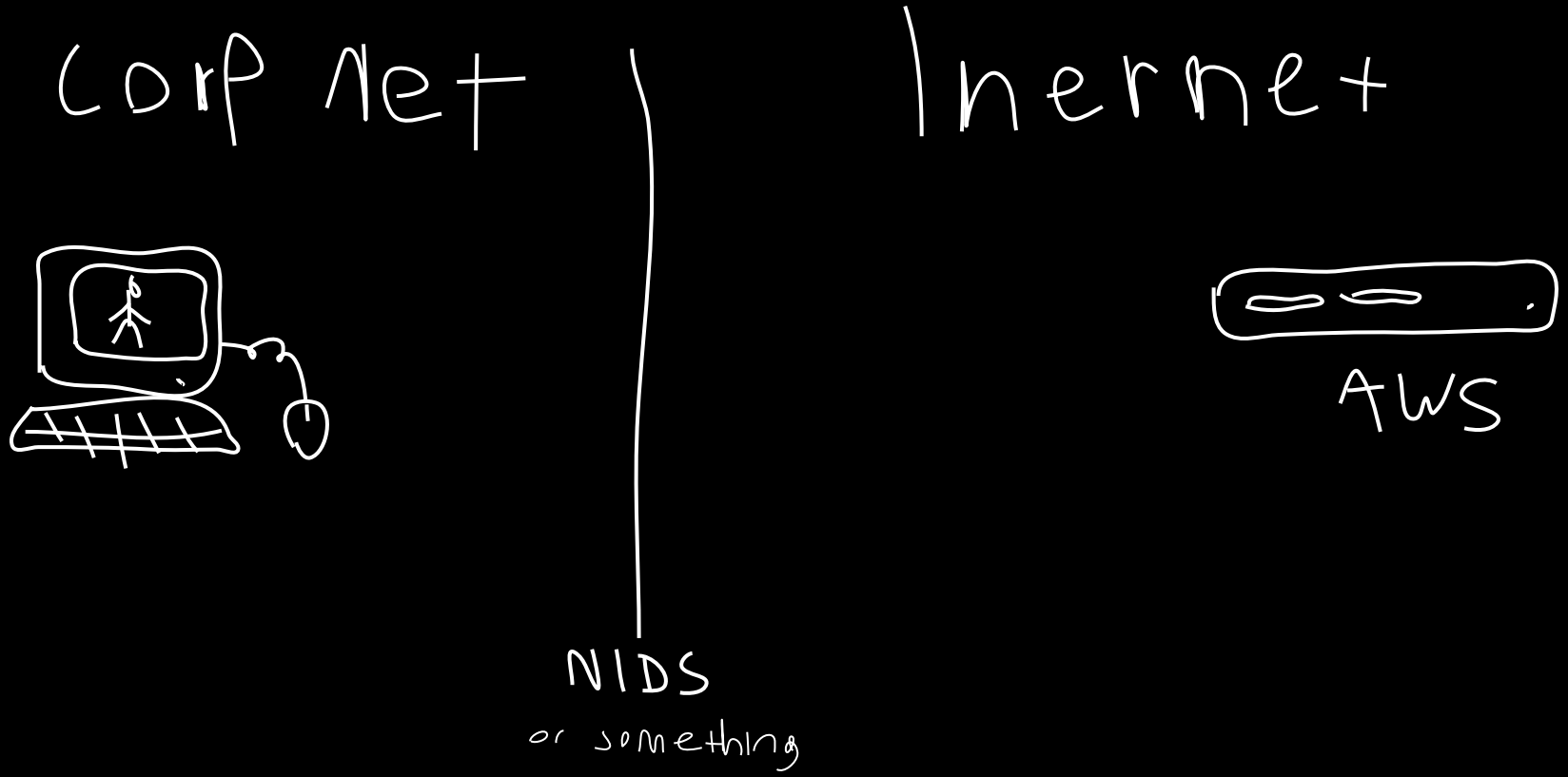
- JA4 - TLS Client Fingerprinting
- JA4S - TLS Server Response Fingerprinting
- JA4H - HTTP Client Fingerprinting
- JA4L - Light Distance/Latency Measuring Client
- JA4LS - Light Distance/Latency Measuring Server
- JA4X - X509 TLS Certificate Fingerprinting
- JA4SSH - SSH Traffic Fingerprinting
- JA4T - TCP OS/Device/Application Fingerprinting
- JA4TS - TCP Server Response Fingerprinting
- JA4TScan - Active TCP Fingerprinting
- JA4D - DHCP Fingerprinting
- JA4D6 - DHCPv6 Fingerprinting
- JA4Scan-TLS - Active TLS Server Fingerprint Scanner
- JA4Scan-QUIC - Active QUIC Server Fingerprint Scanner
- JA4N - NTP Fingerprinting
- JA4M - MCP Client Fingerprint
- JA4MS - MCP Server Fingerprint
- JA4MB - MCP Behavior Fingerprint
- With more in development …

Under Development…

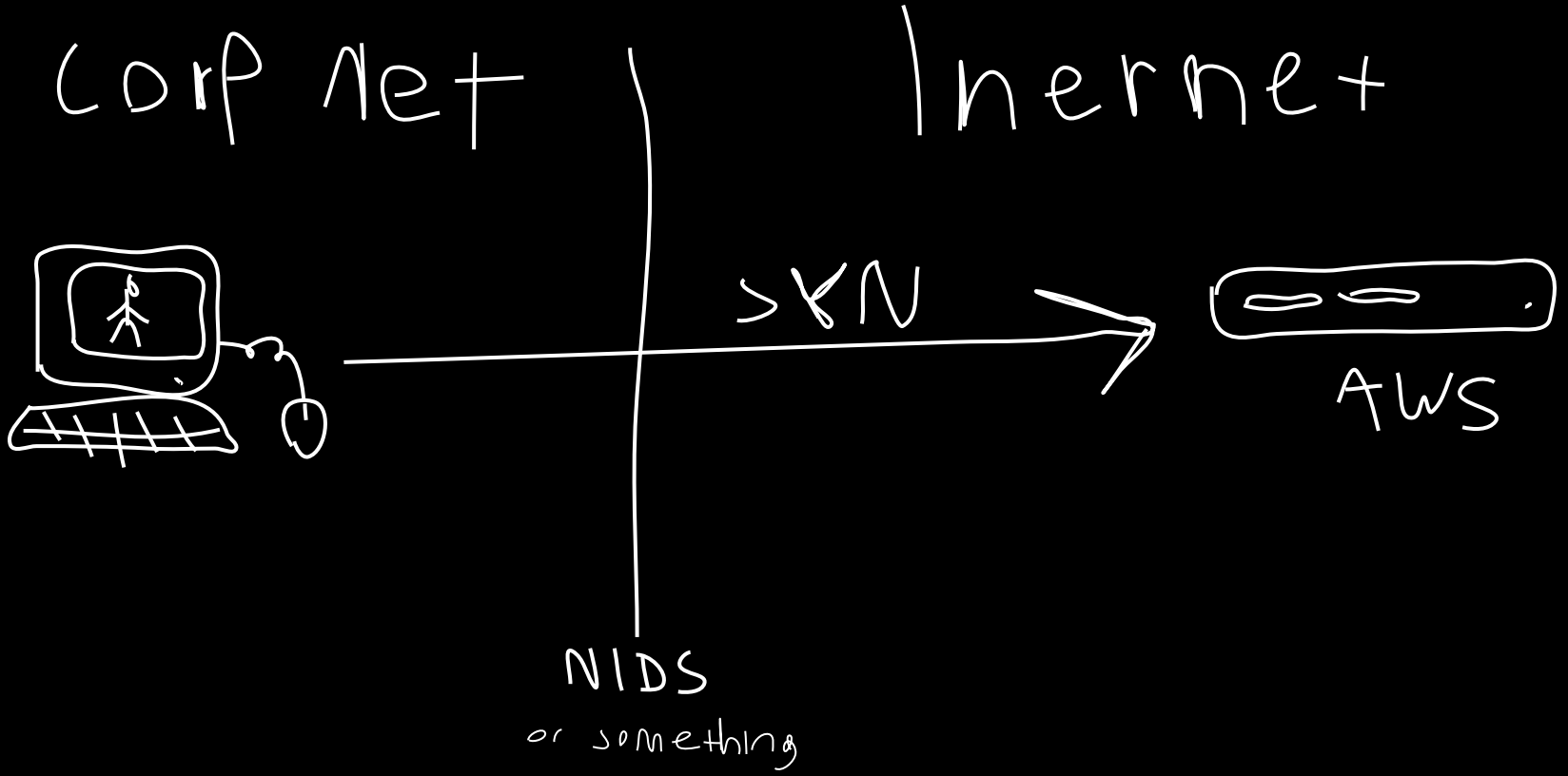
- JA4.Extension - Additional TLS Client Fingerprinting
- JA4T.Extension - Additional TCP Client Fingerprinting
- JA4H.Extension - Additional HTTP Client Fingerprinting
- JA4Scan-TCP - Active TCP Server Fingerprint Scanner
- JA4Scan-HTTP - Active HTTP Server Fingerprint Scanner
- JA4Scan-DTLS - Active DTLS Server Fingerprint Scanner
- JA4Scan-DOM - Active HTTP DOM Fingerprint Scanner
- JA4HTTPServer - HTTP Server Response Fingerprint
- JA4Email - Email Header Fingerprint
- JA4WiFi - Wireless Client Fingerprint
- JA4BGP - BGP Fingerprinting
- JA4IPv6 - IPv6 Fingerprinting
- JA4ARP - ARP Fingerprinting

How TLS works

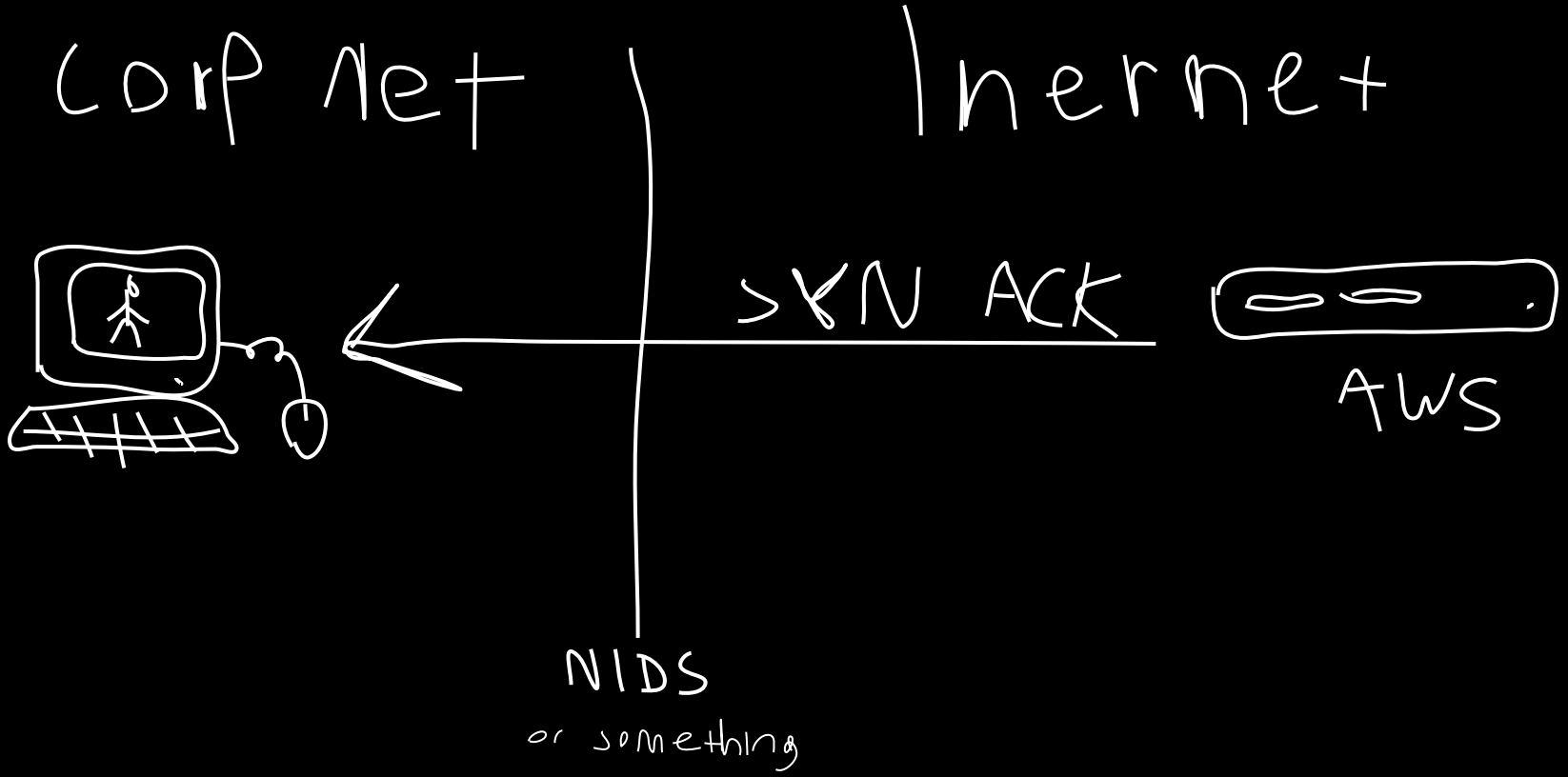
How TLS works



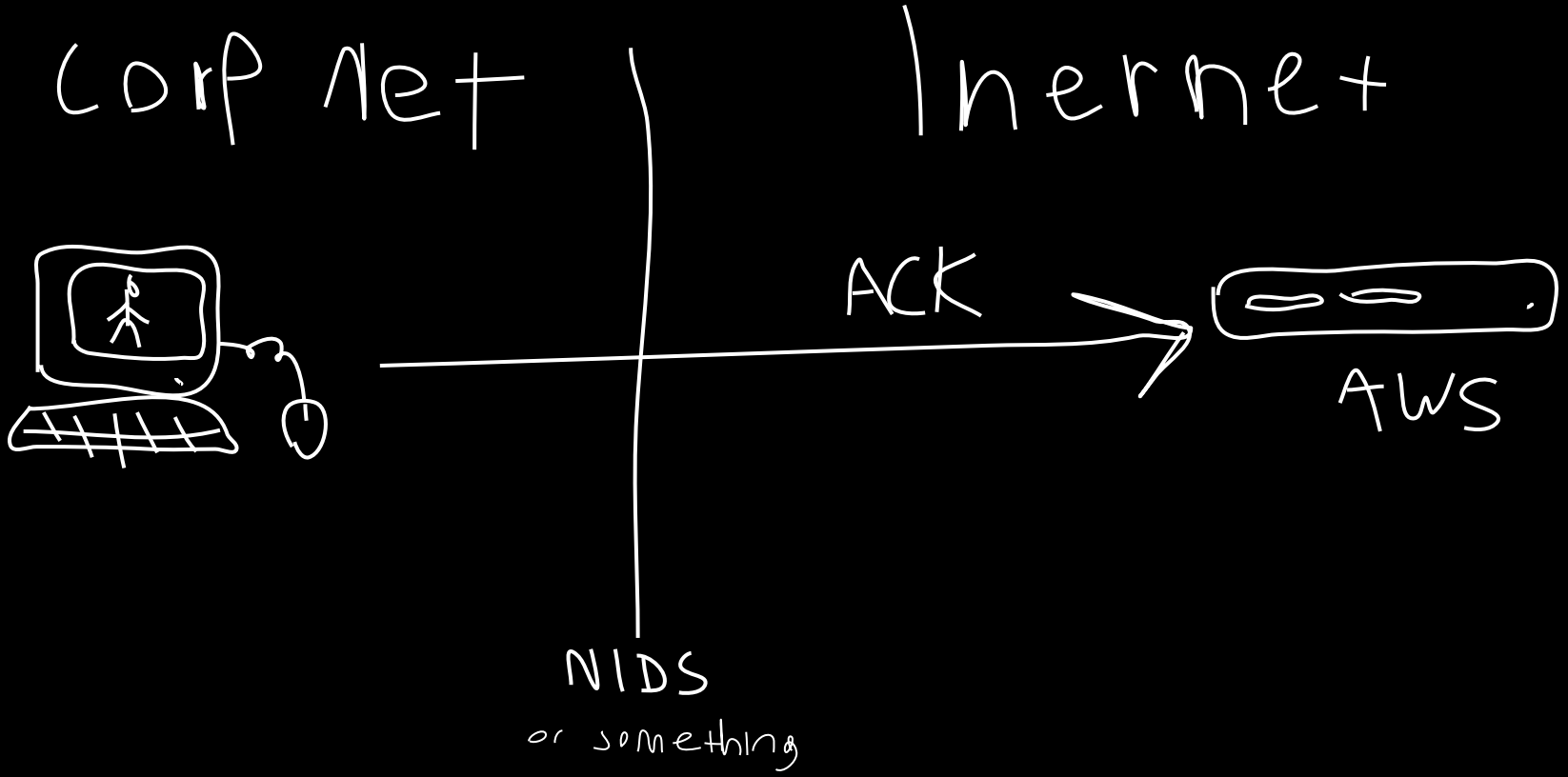
How TLS works



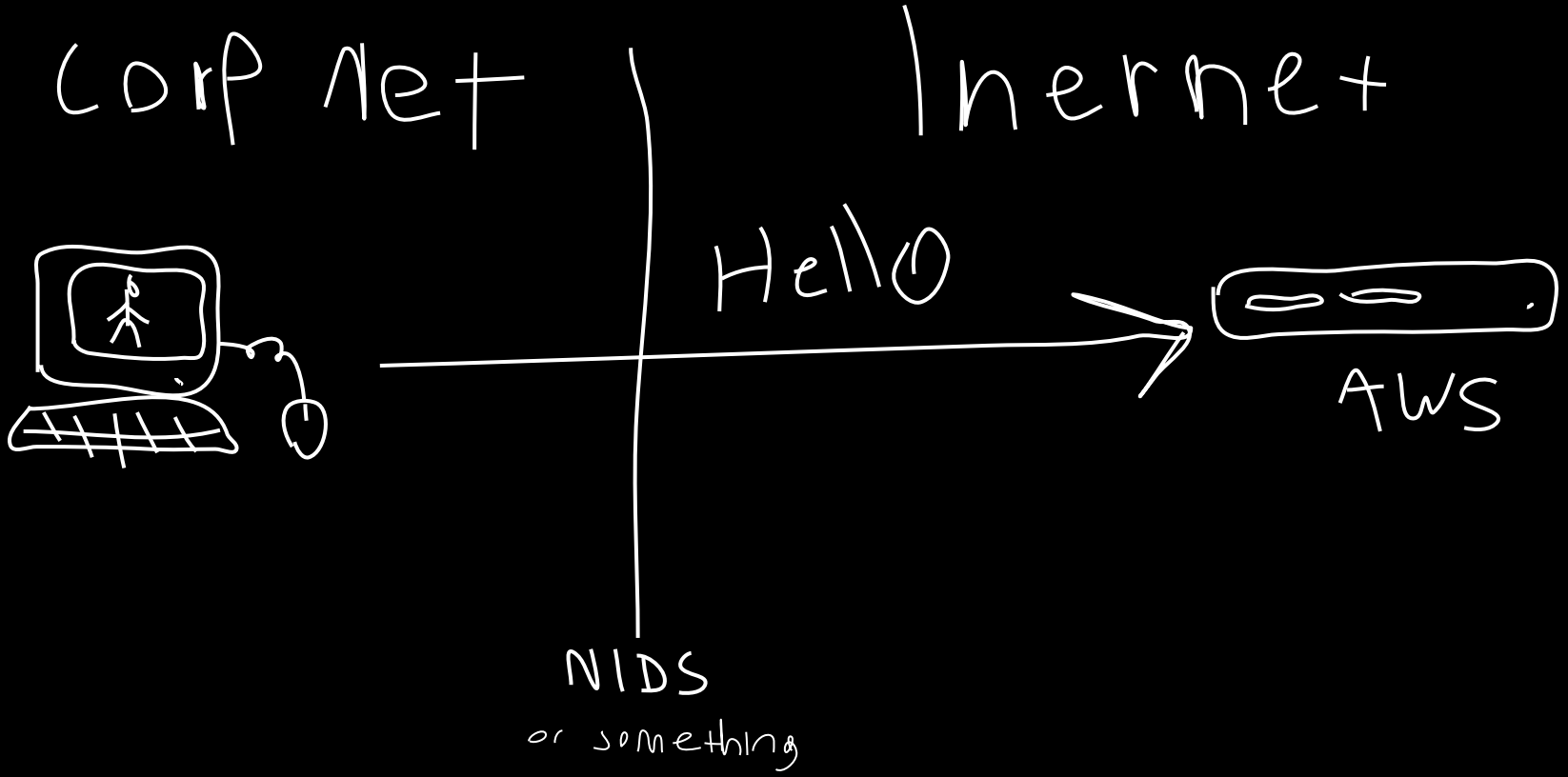
How TLS works



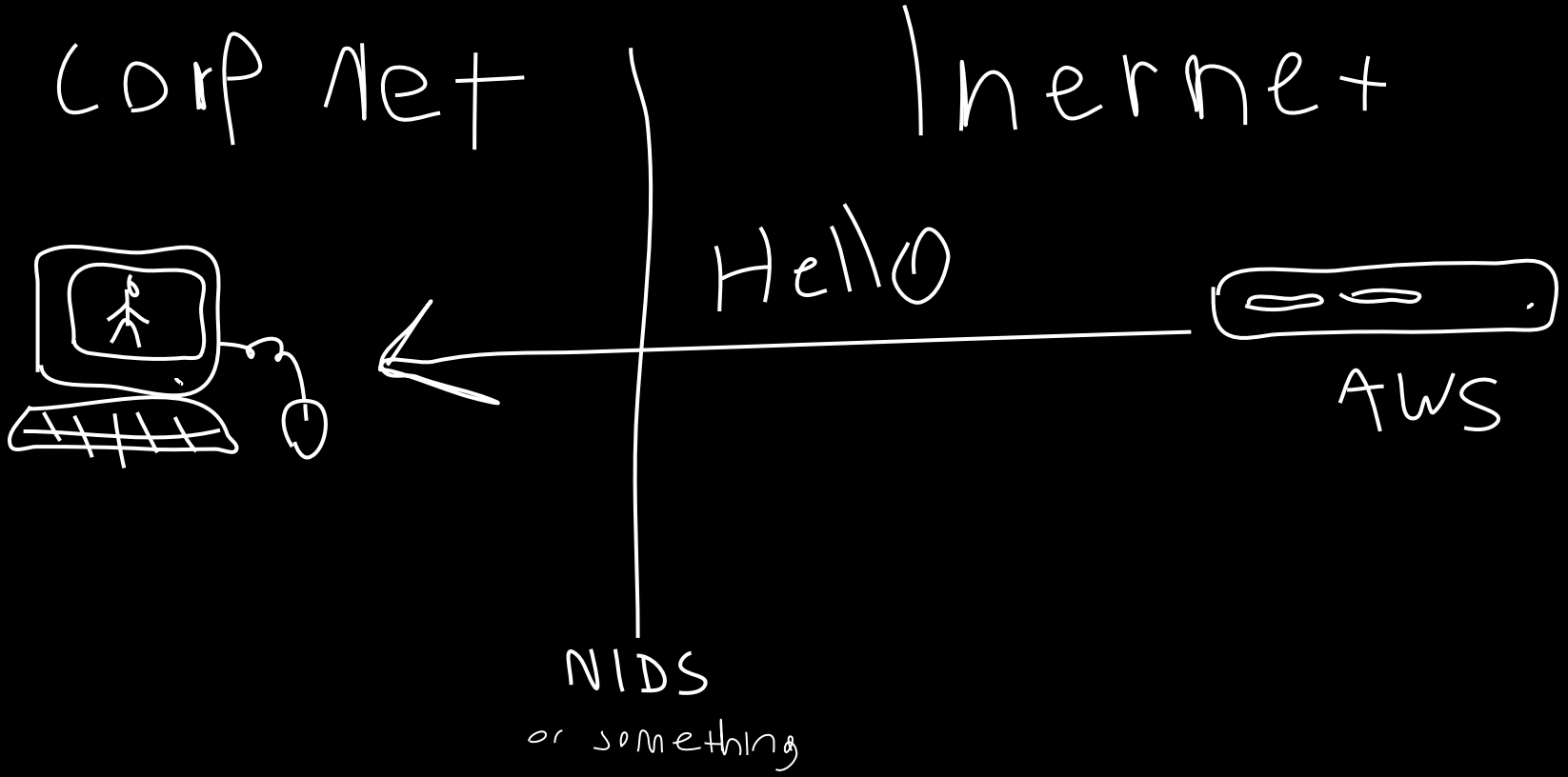
How TLS works



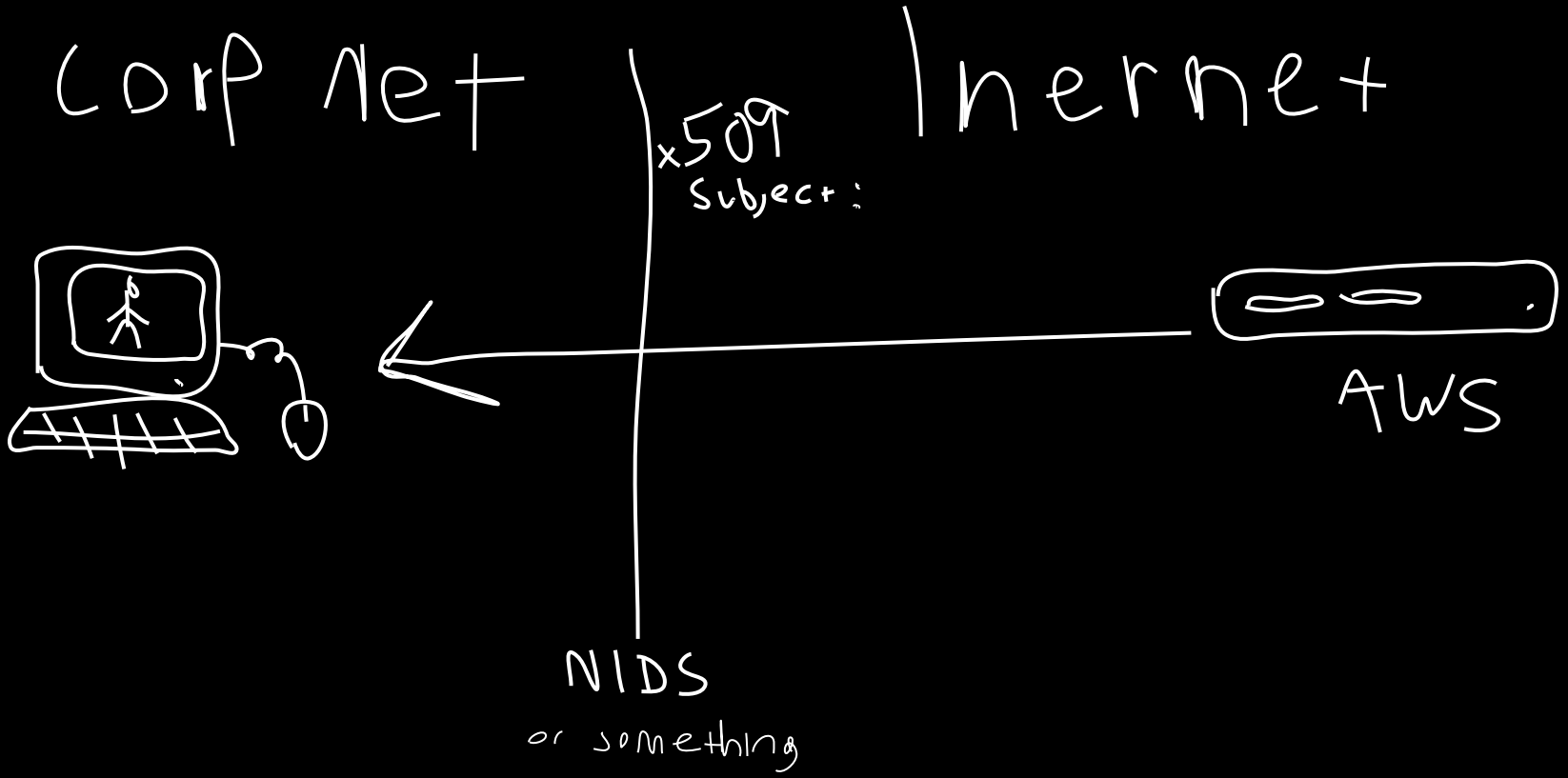
How TLS works



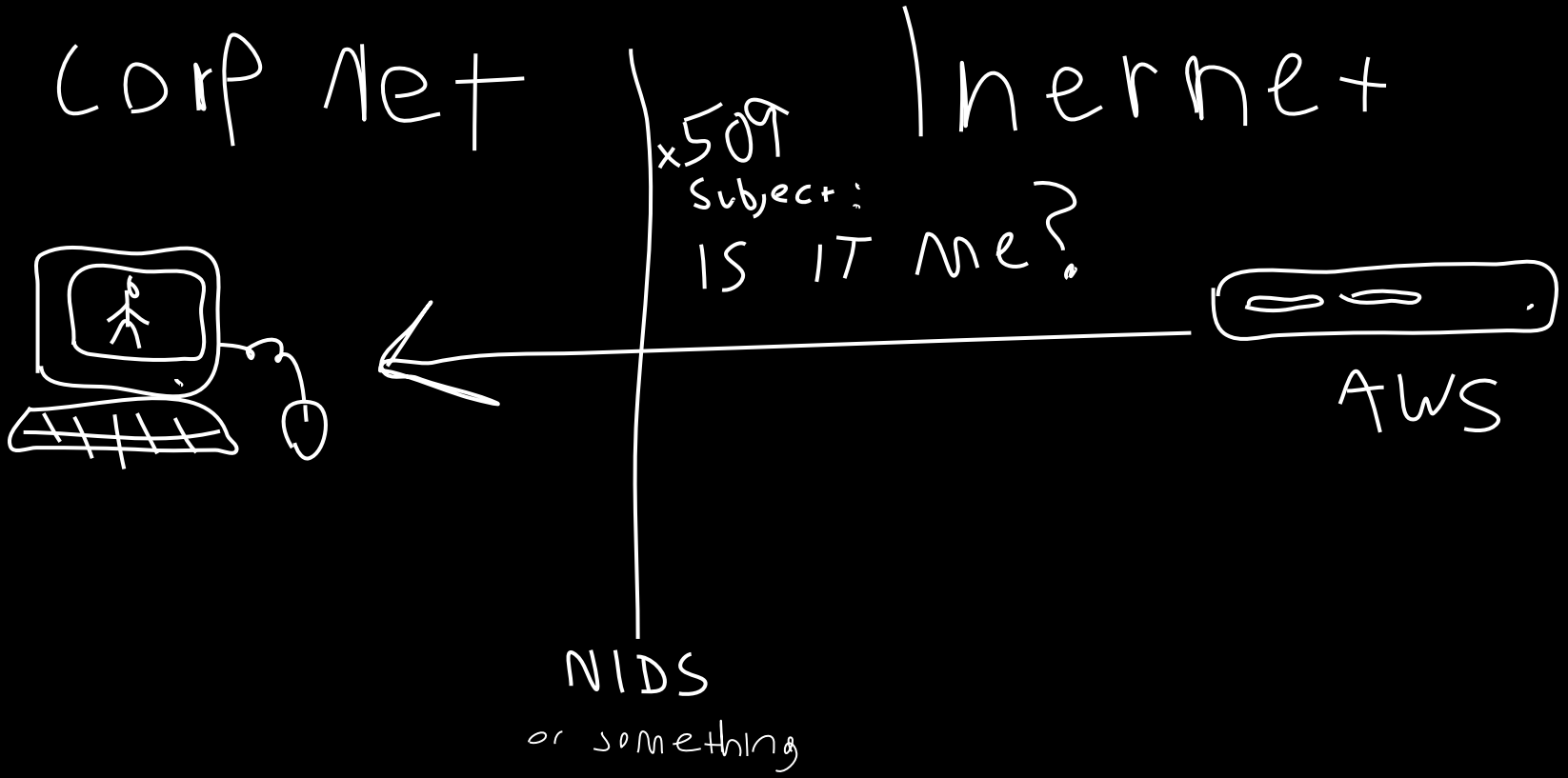
How TLS works



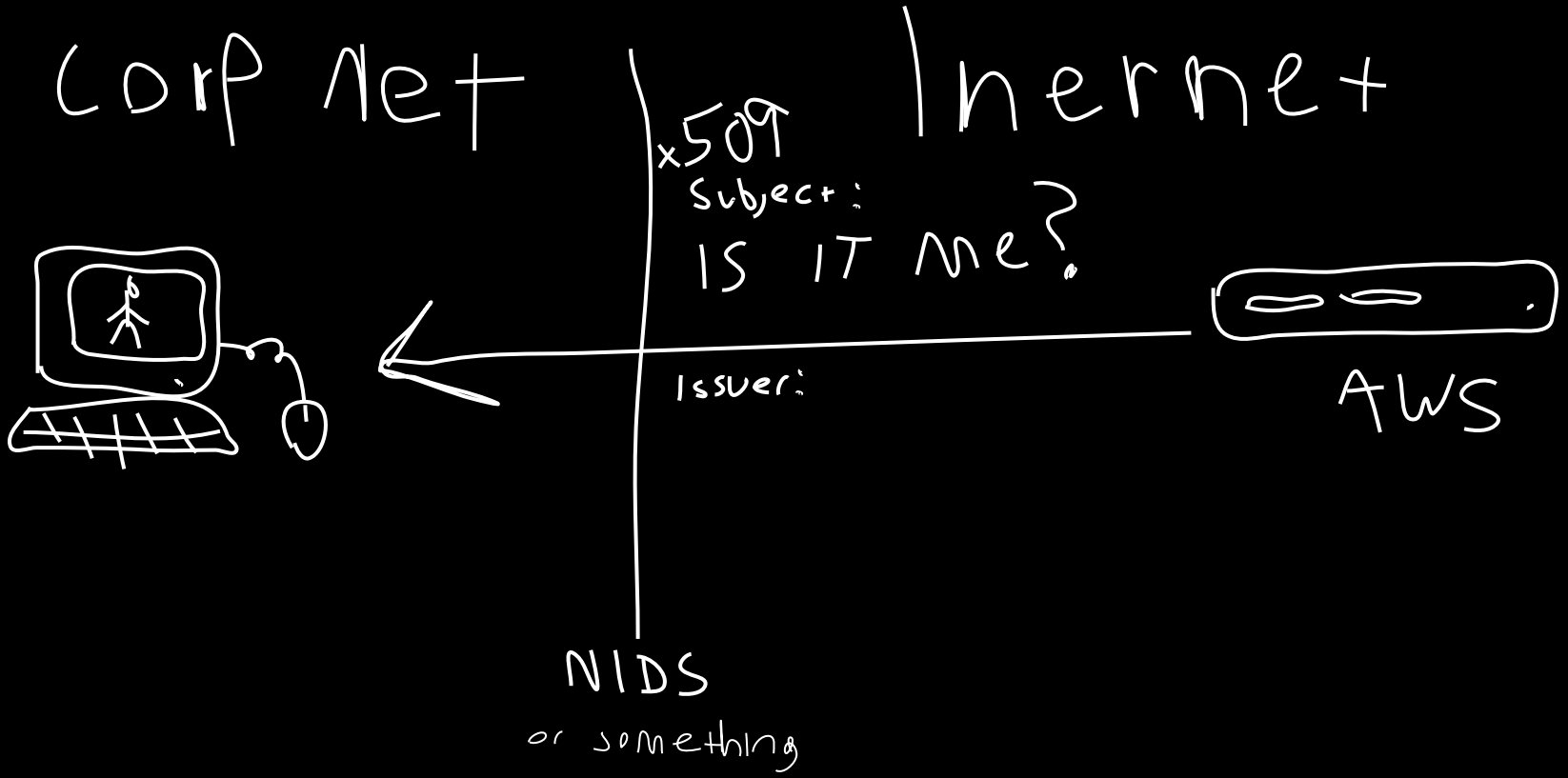
How TLS works



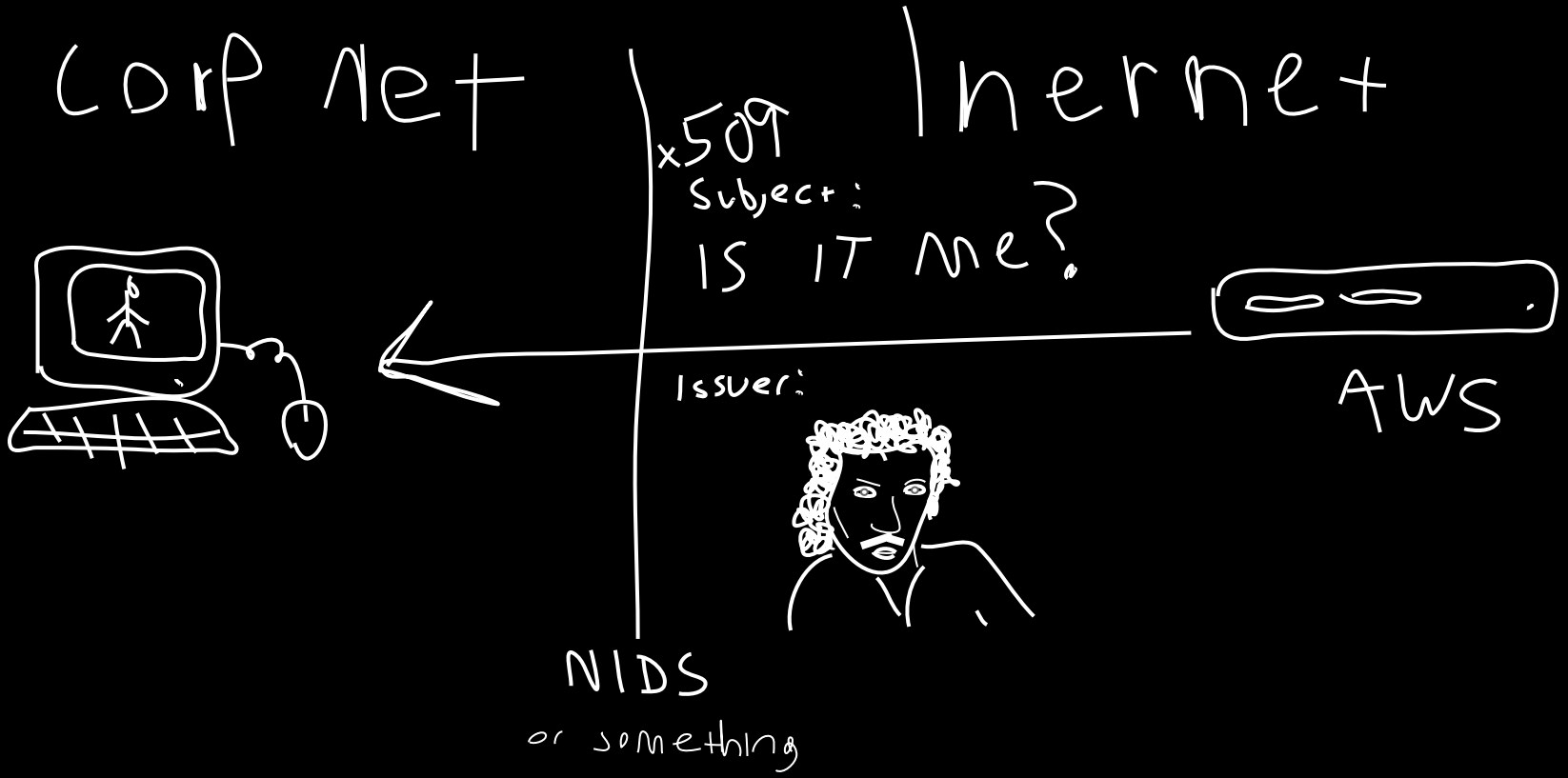
How TLS works



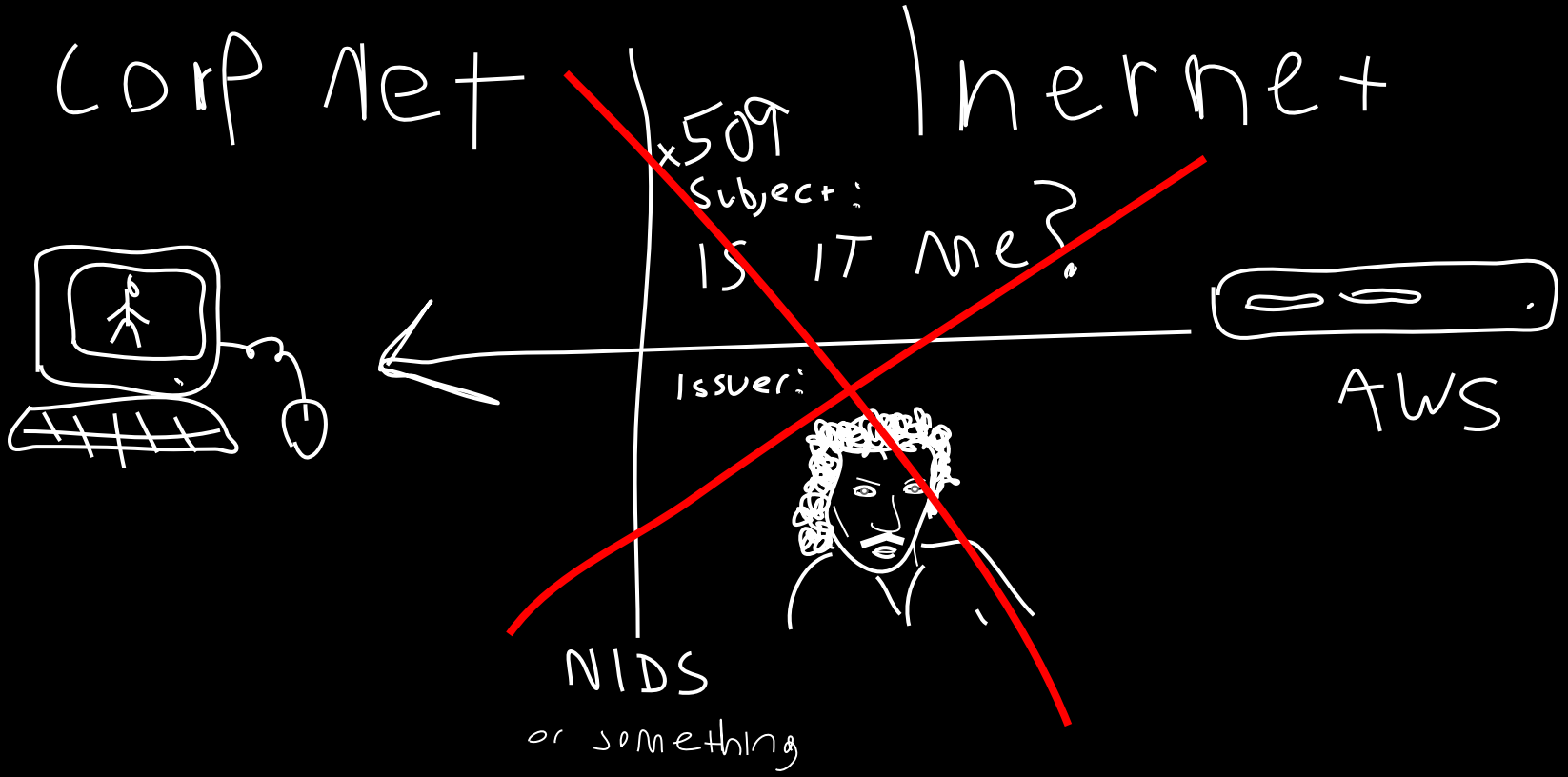
How TLS works



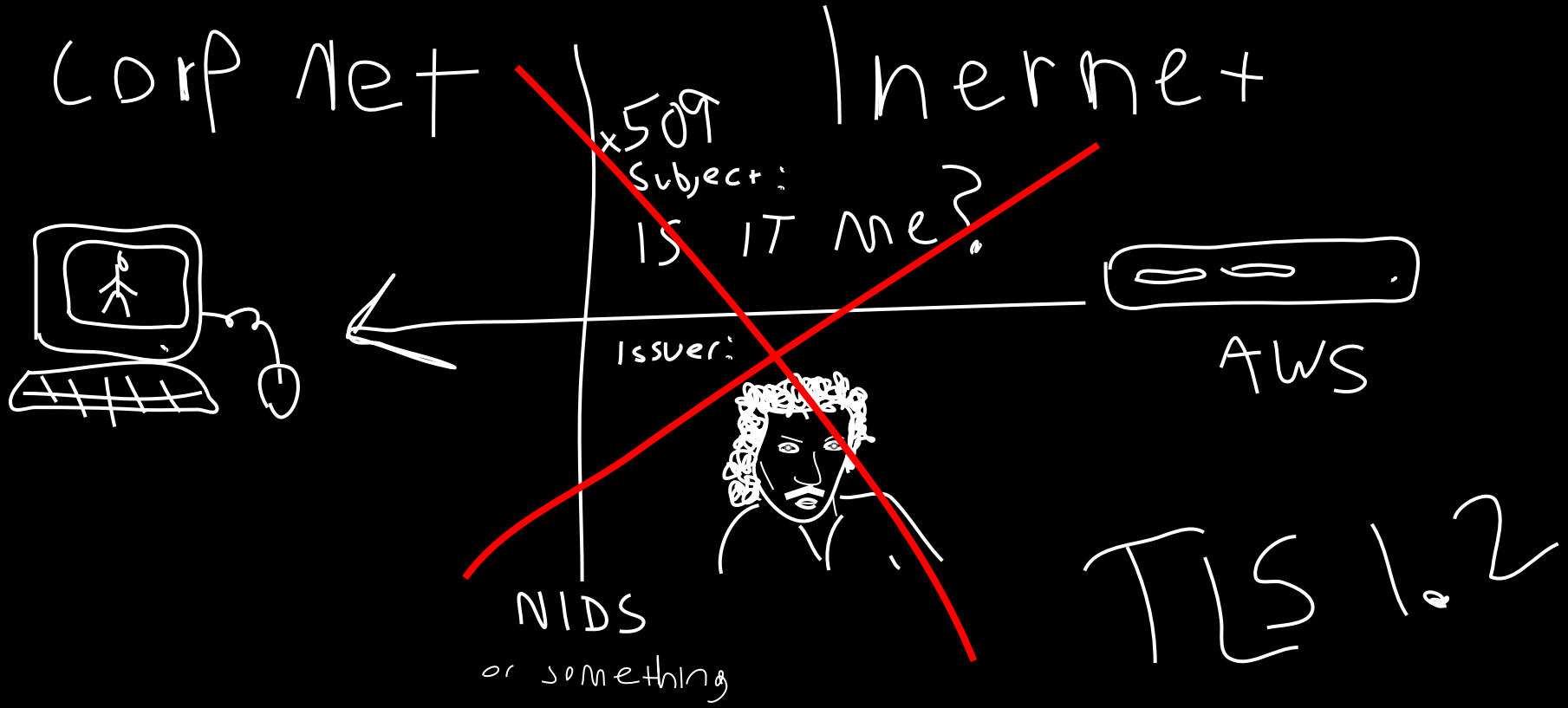
How TLS works



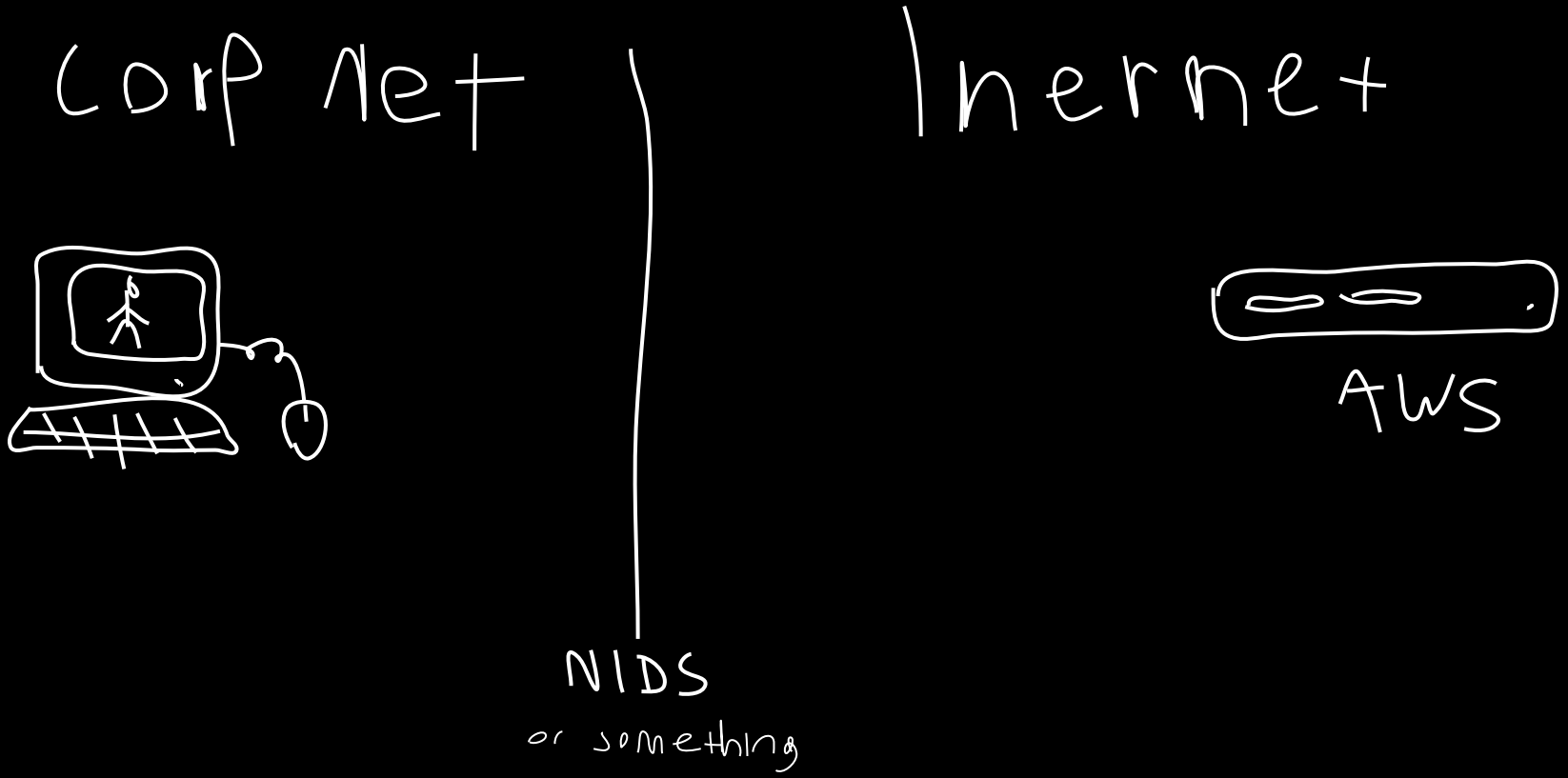
How TLS works



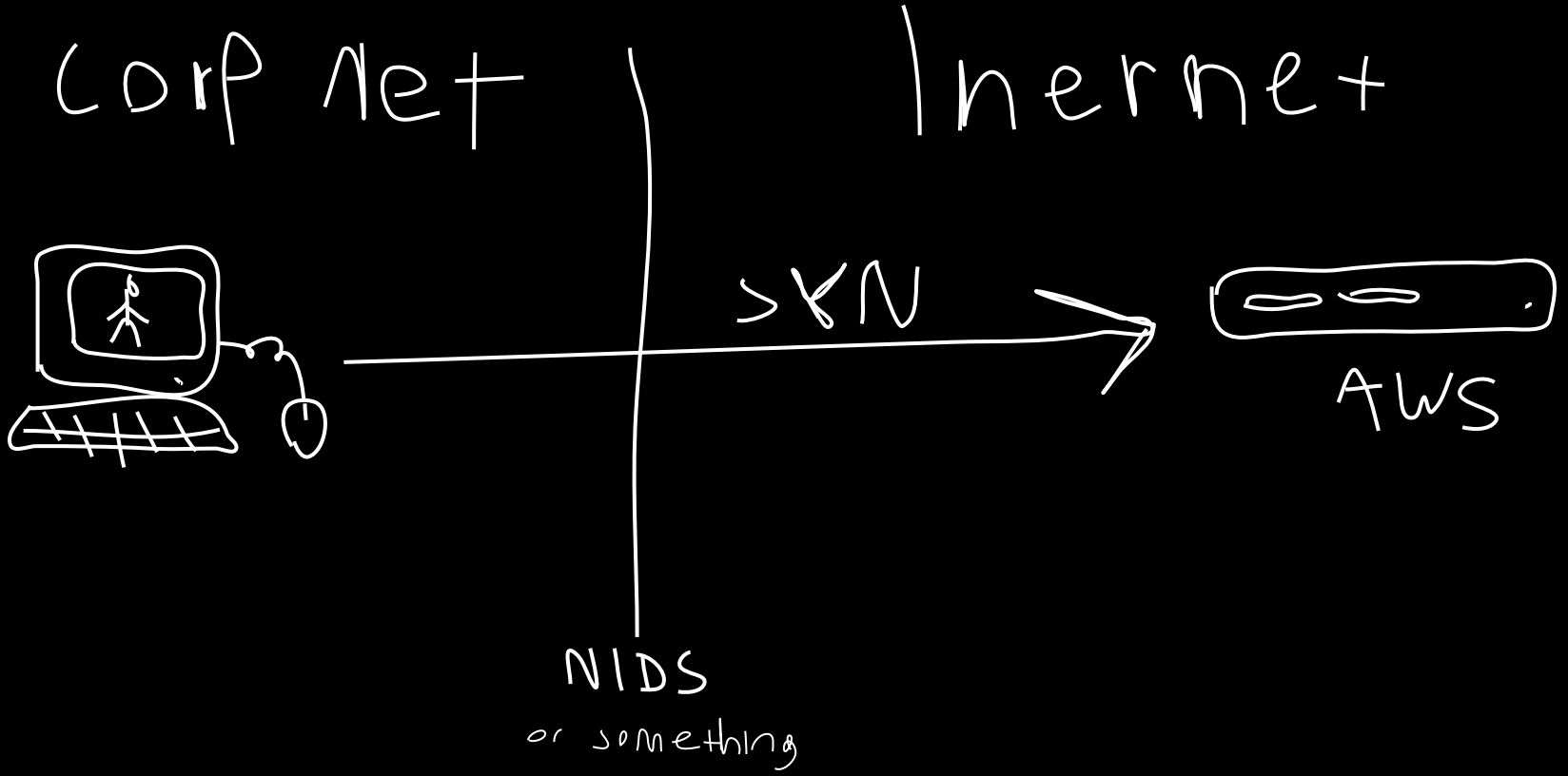
How TLS works



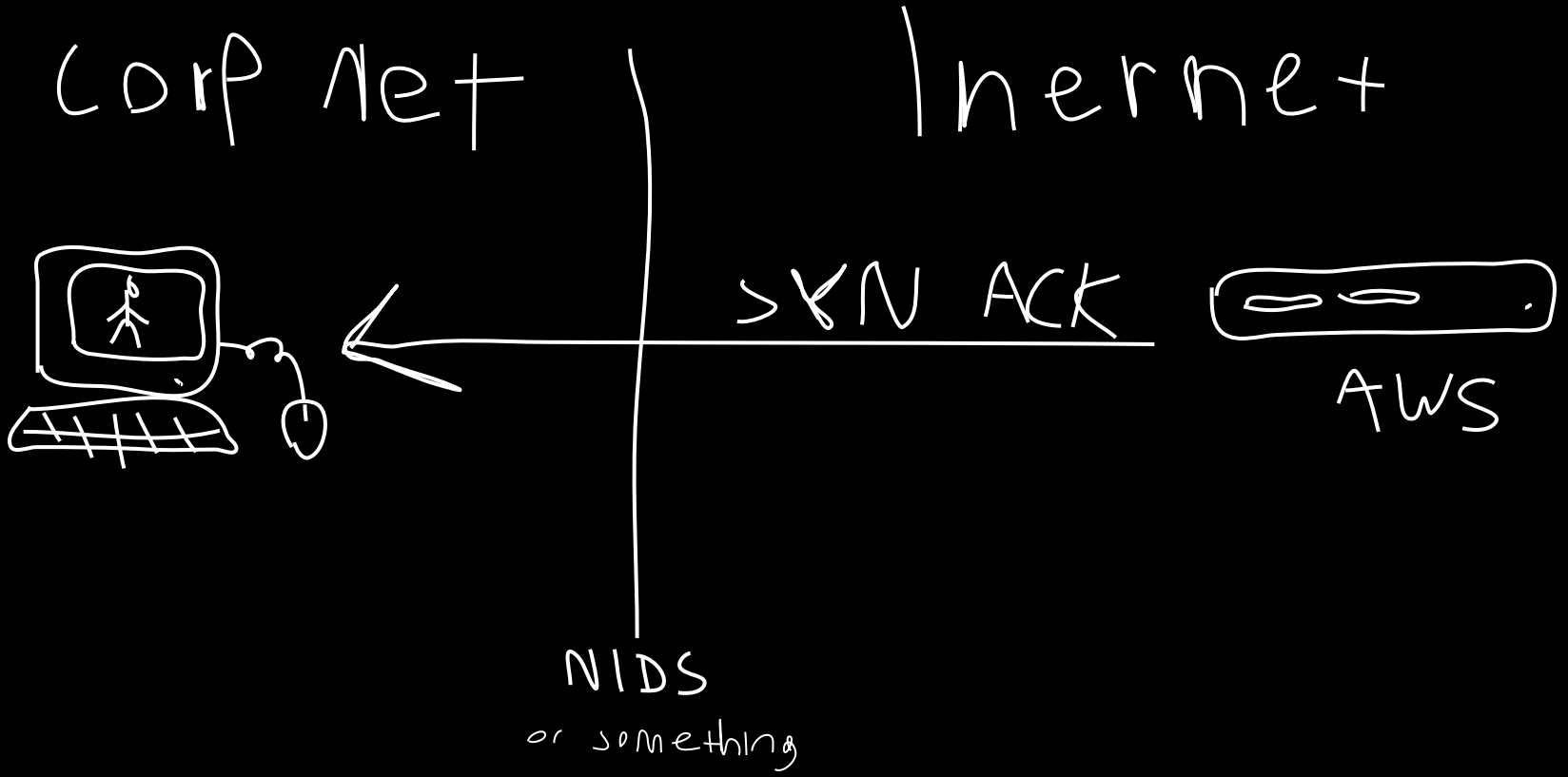
How TLS 1.3 works



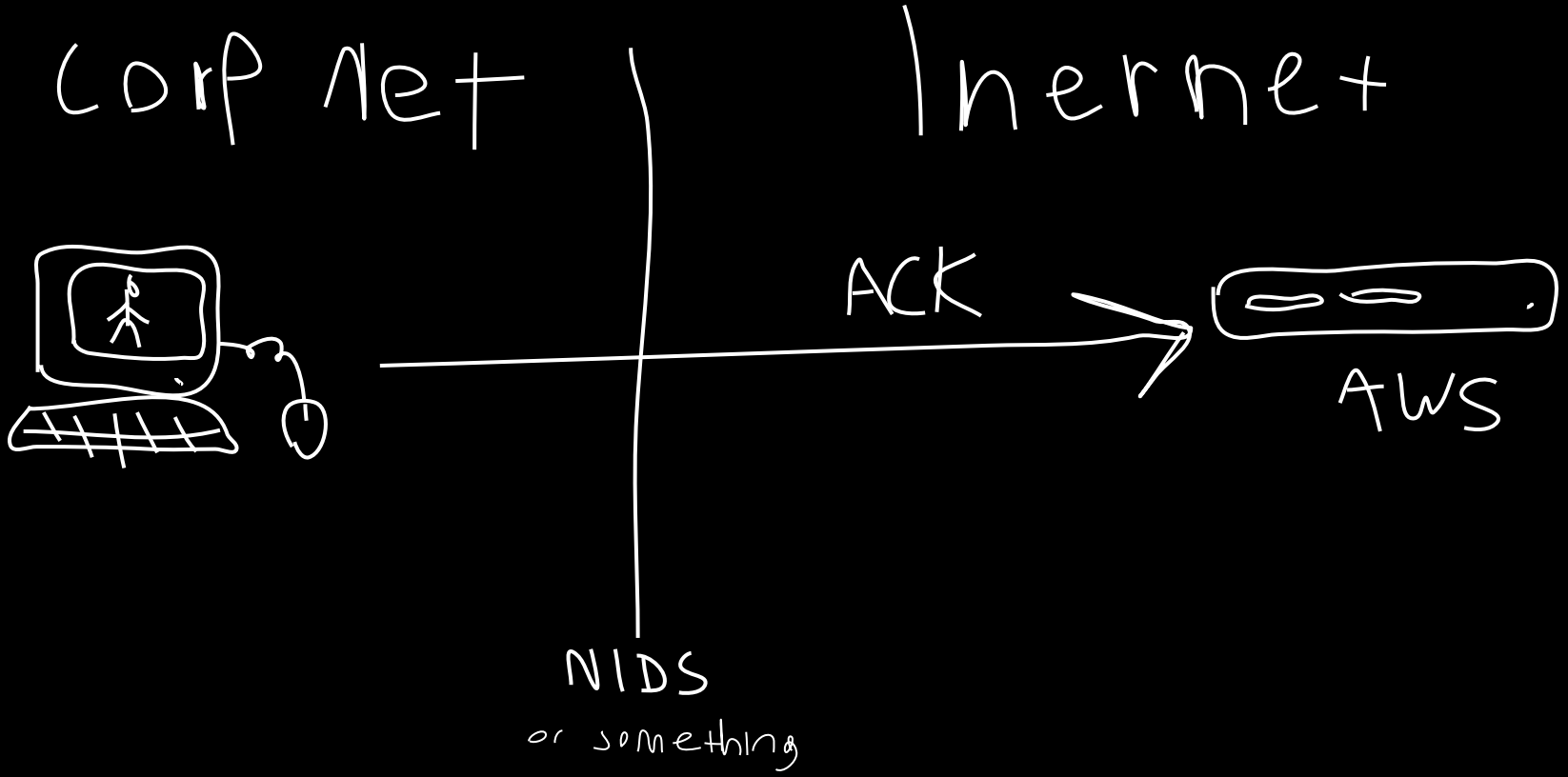
How TLS 1.3 works



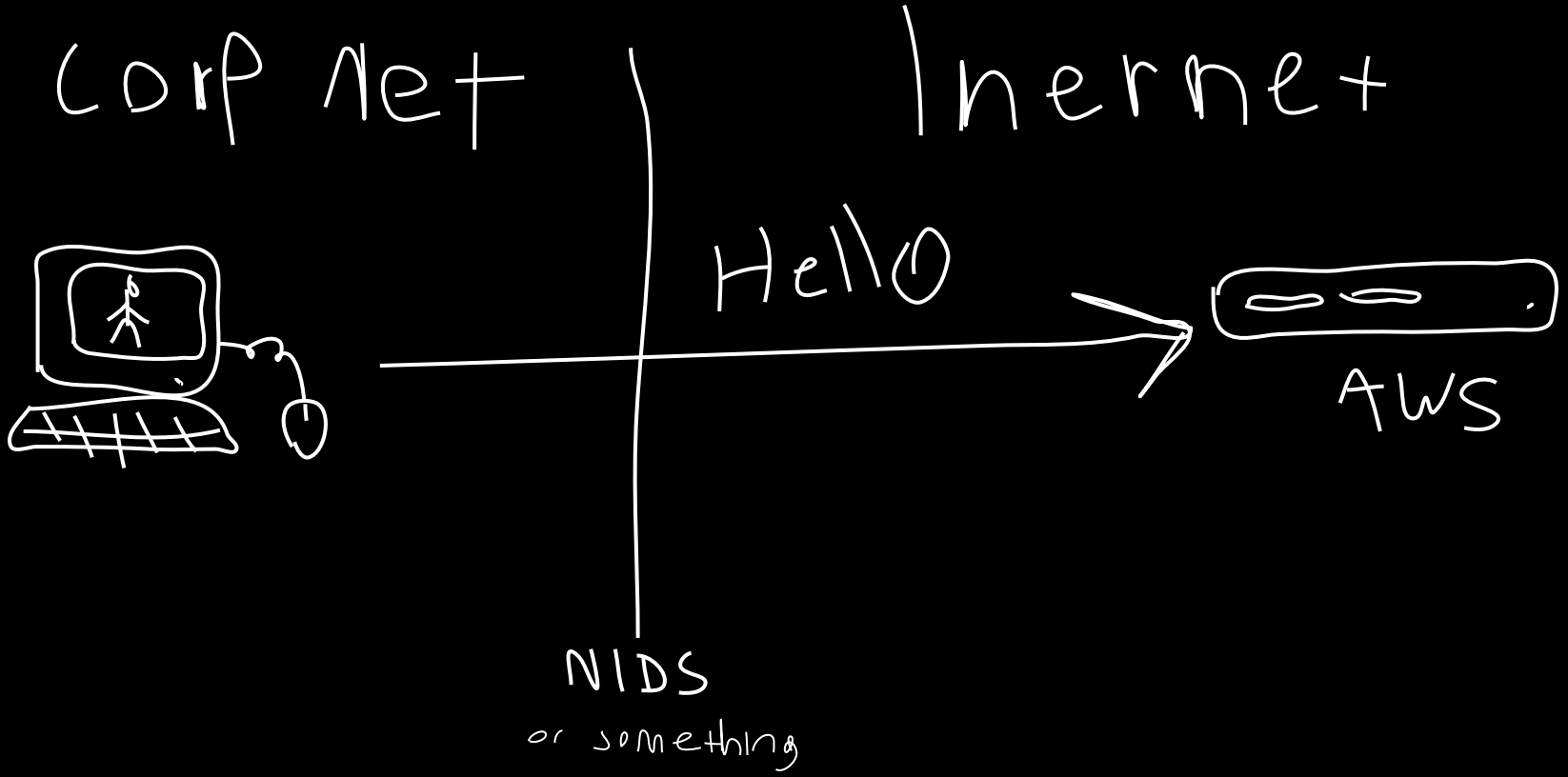
How TLS 1.3 works



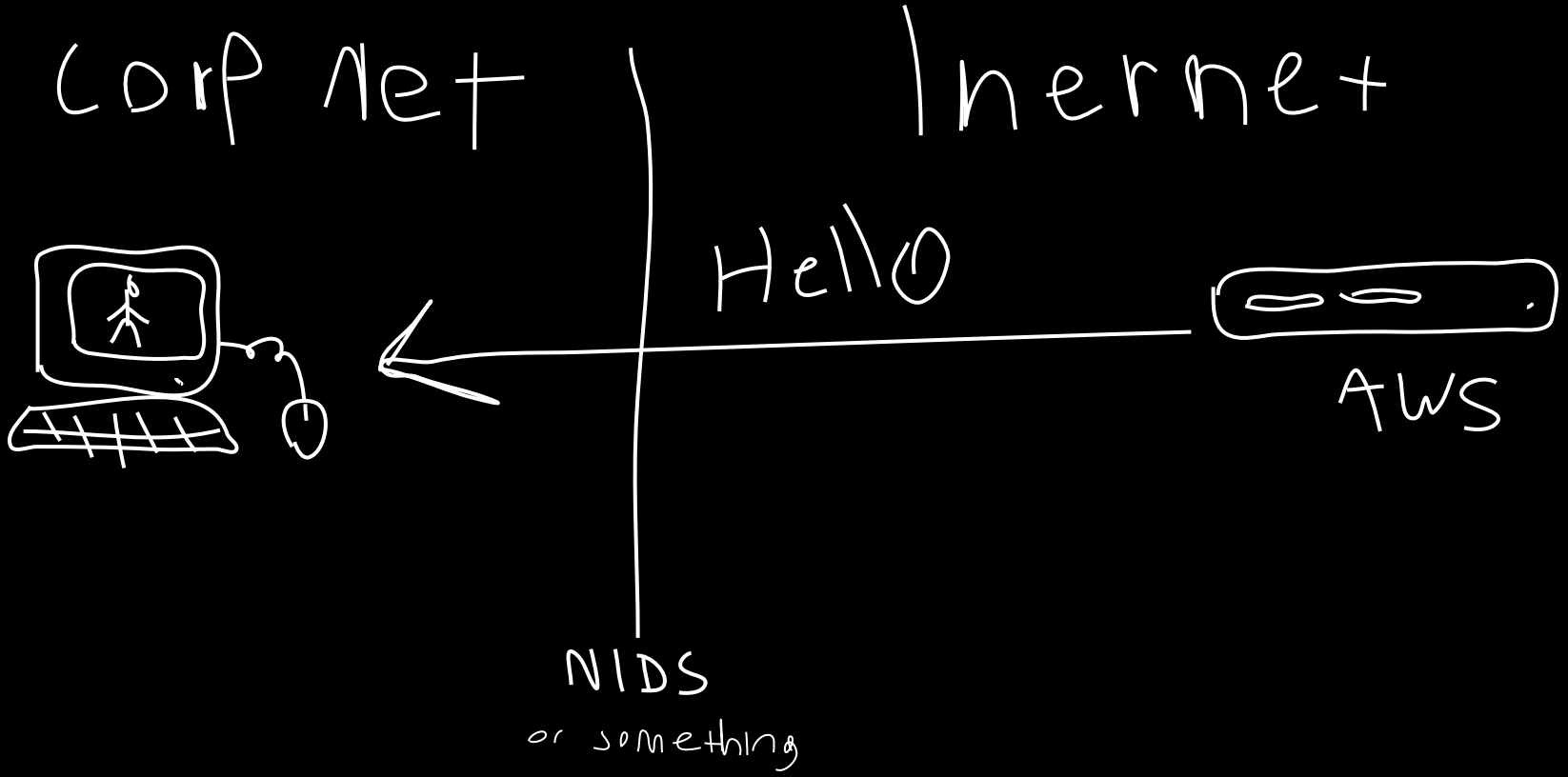
How TLS 1.3 works



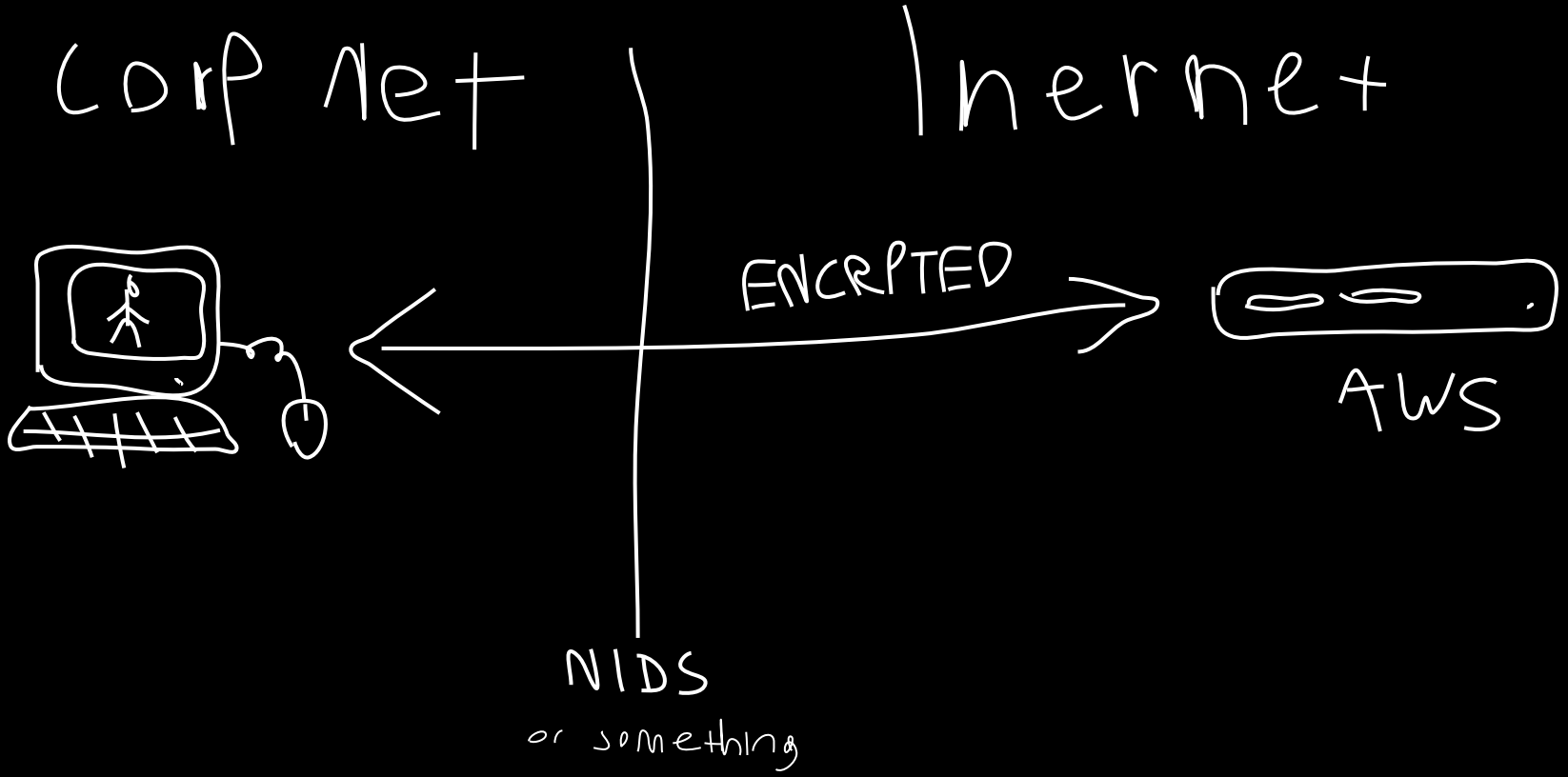
How TLS 1.3 works



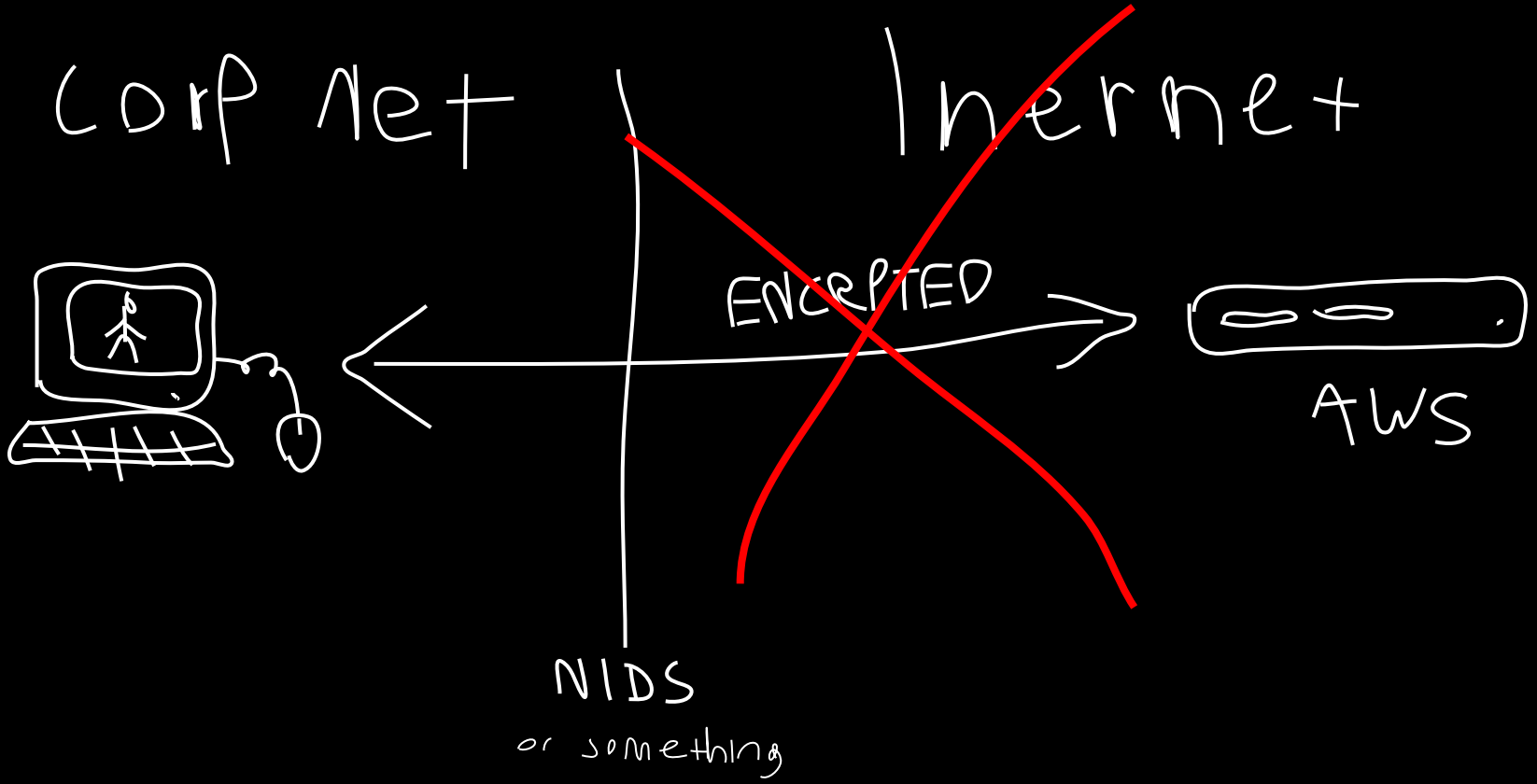
How TLS 1.3 works



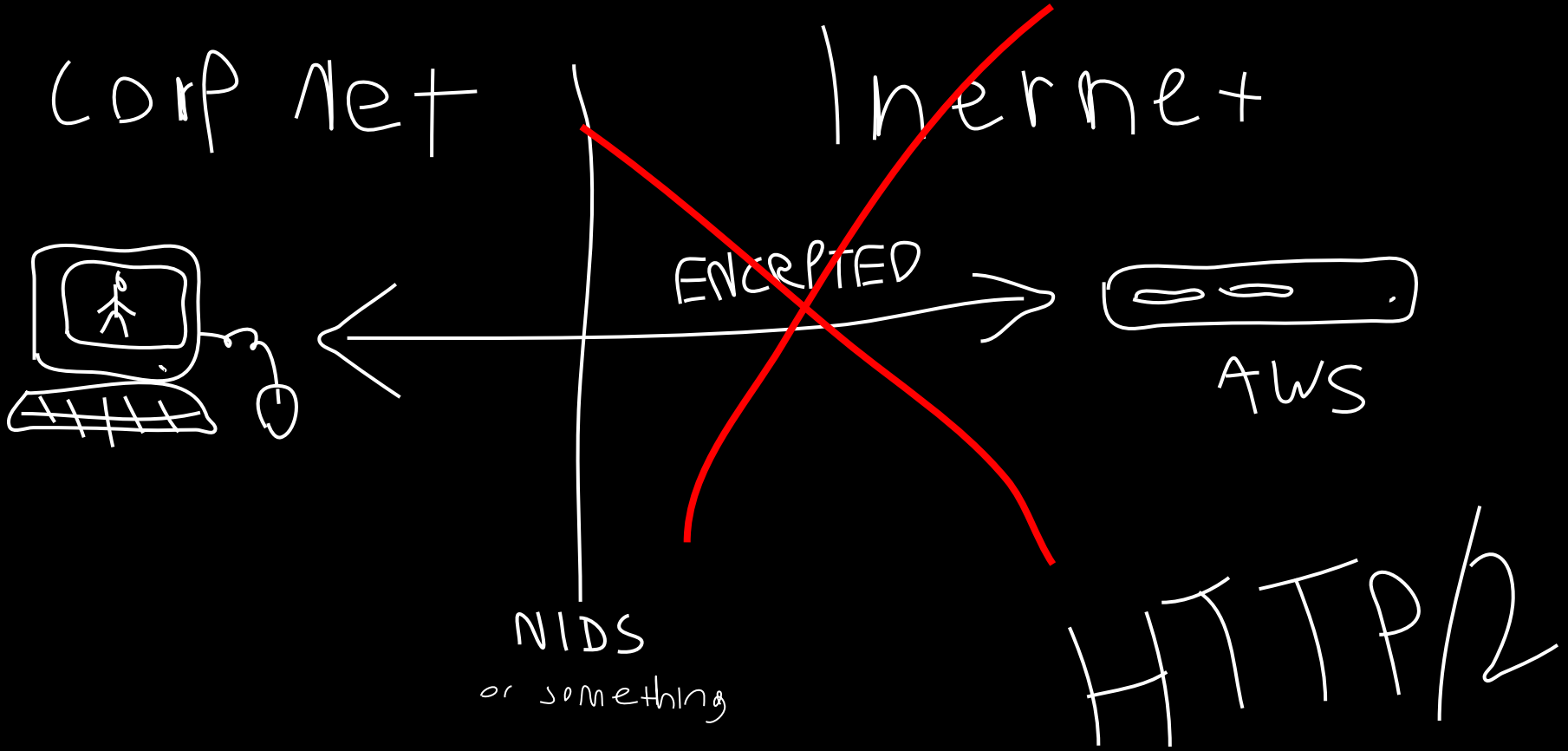
How TLS 1.3 works



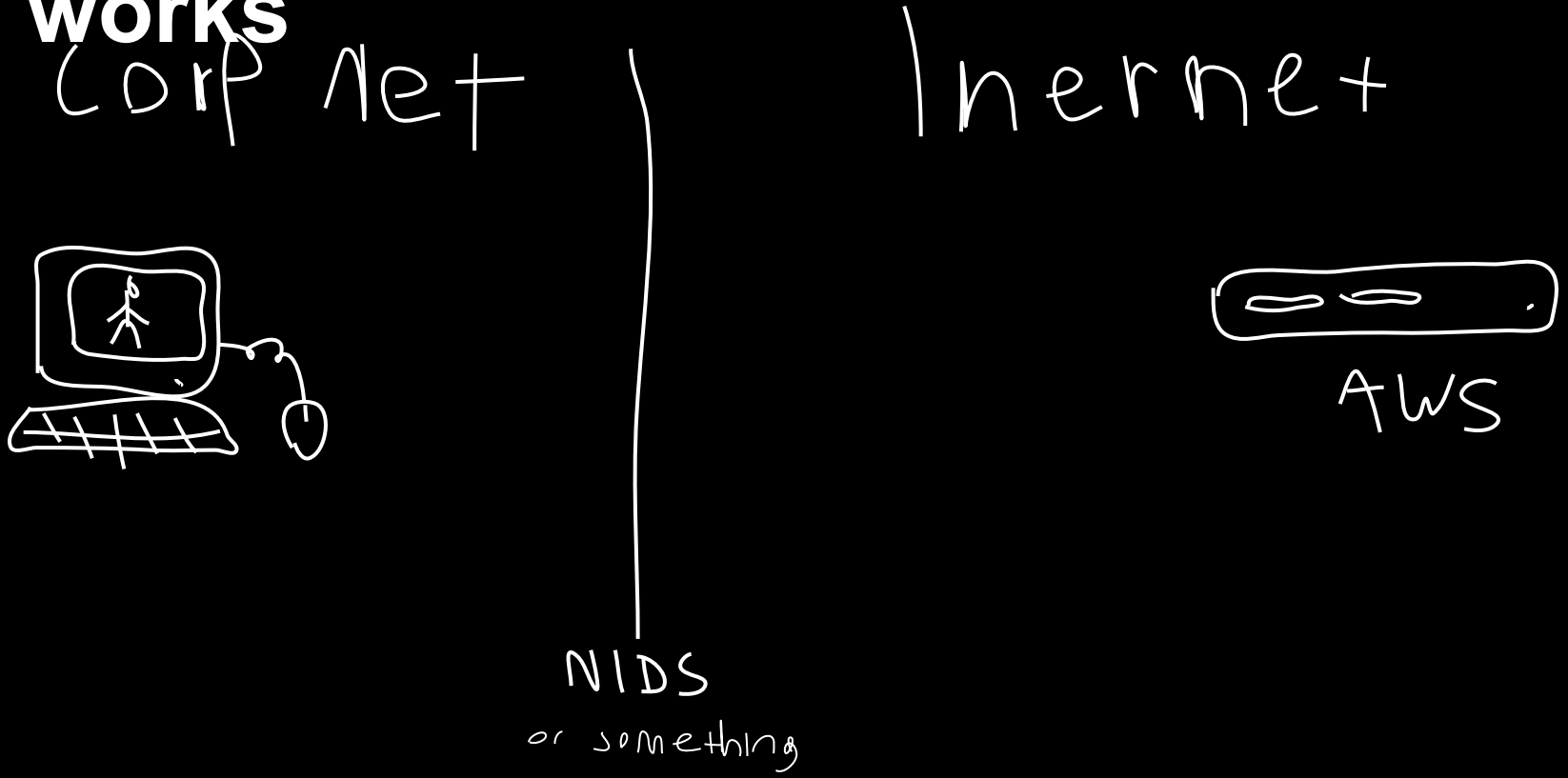
How TLS 1.3 works



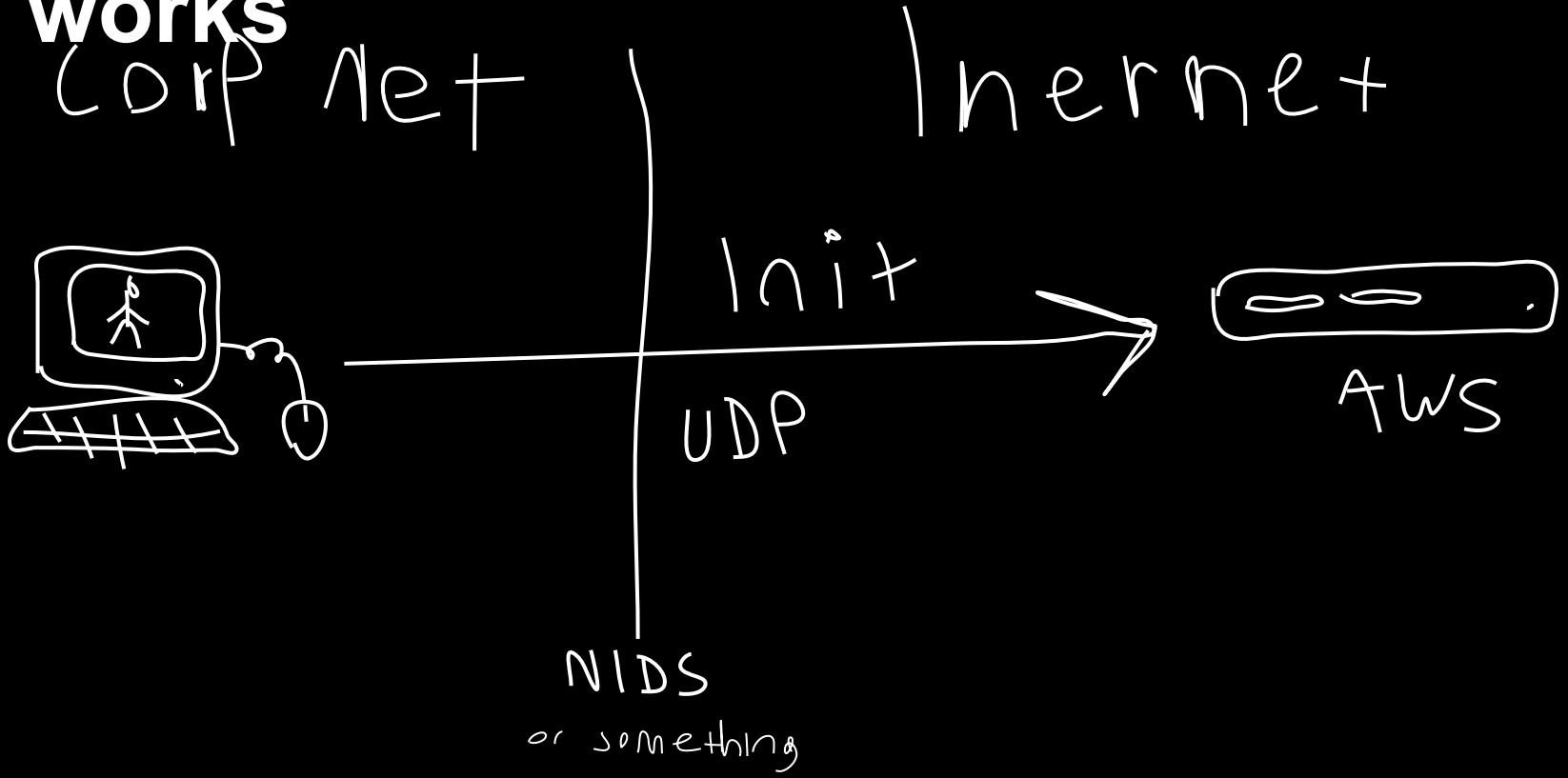
How TLS 1.3 works



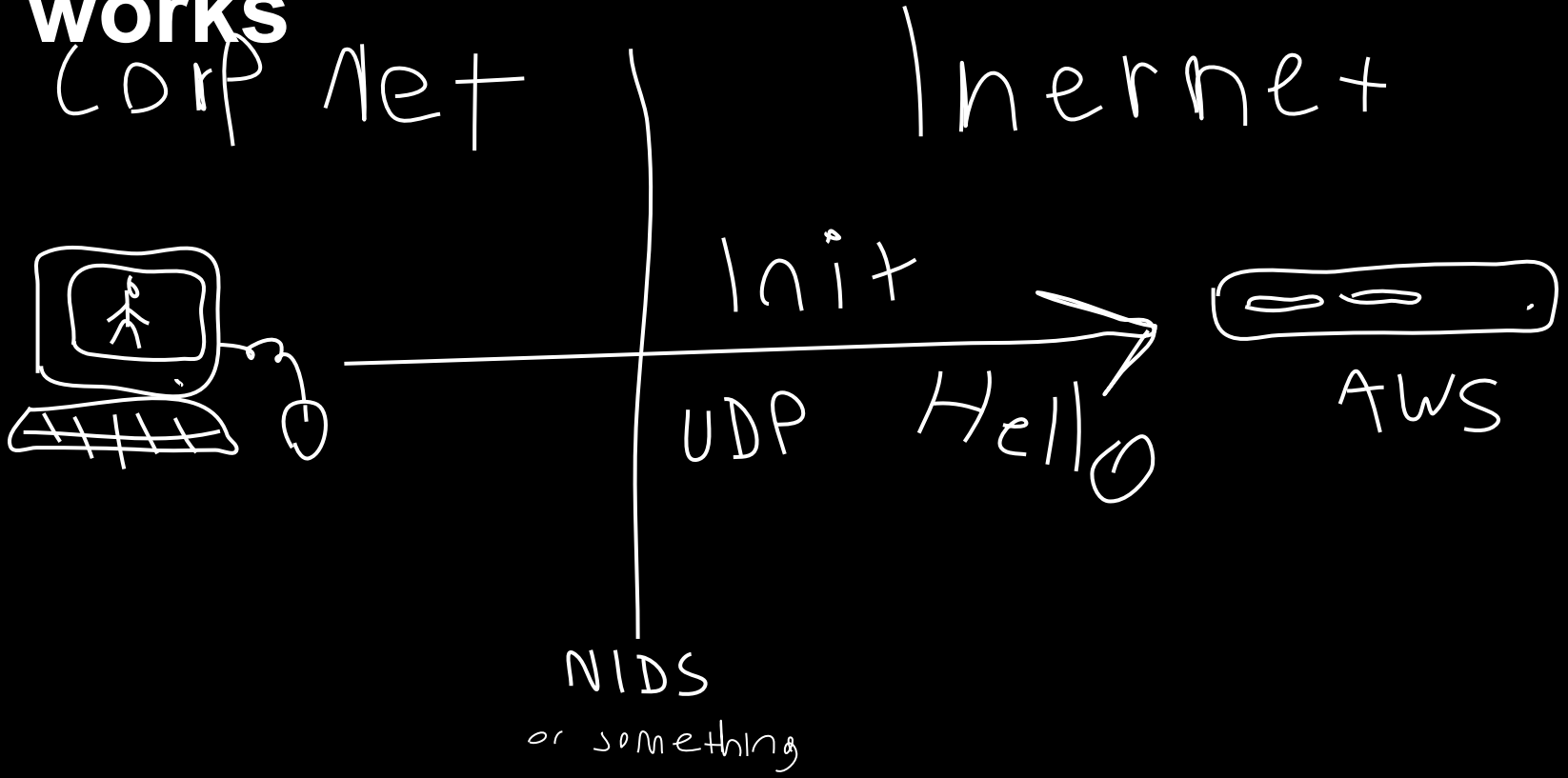
How HTTP/3 over QUIC with TLS 1.3 works



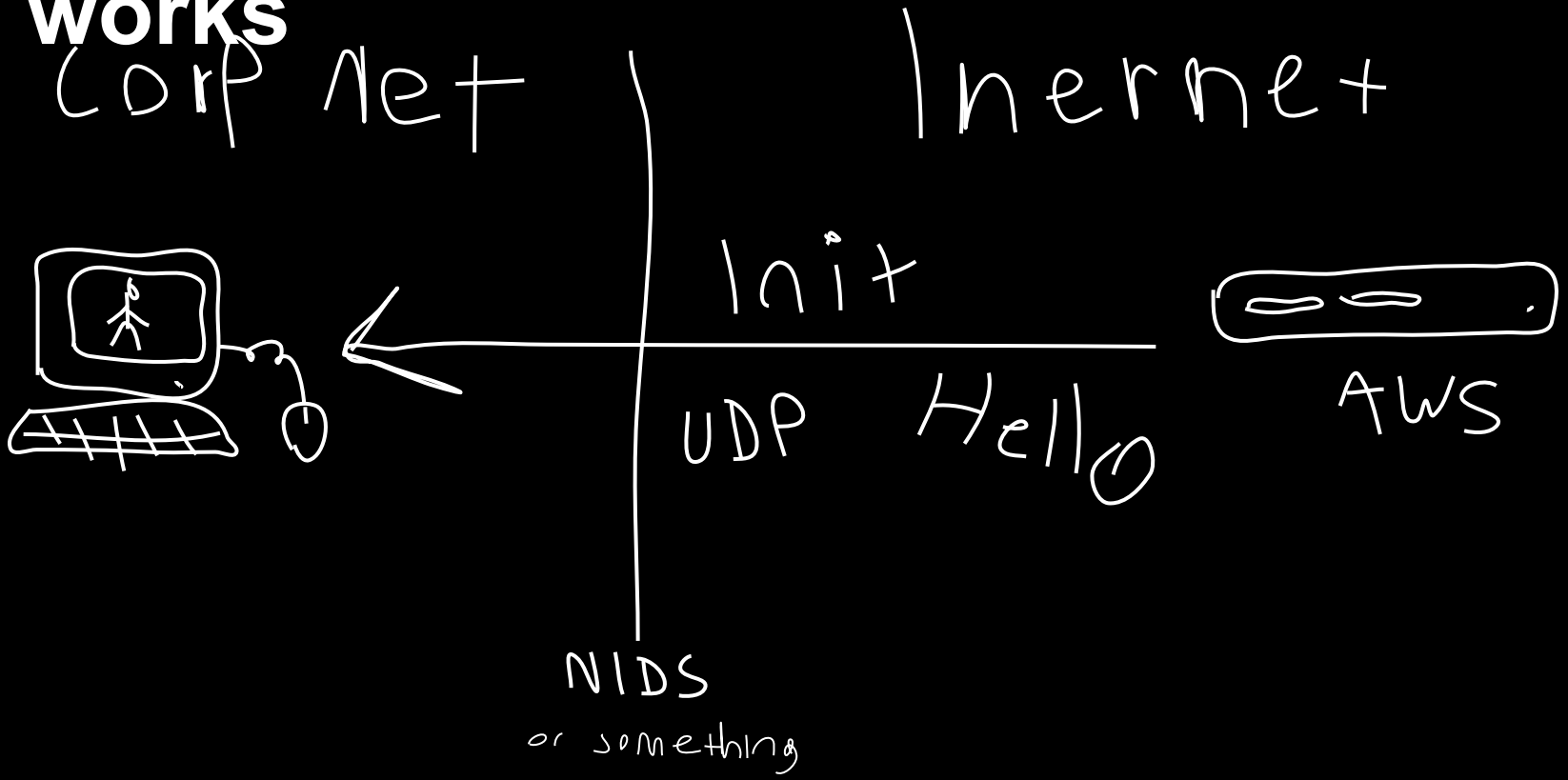
How HTTP/3 over QUIC with TLS 1.3 works



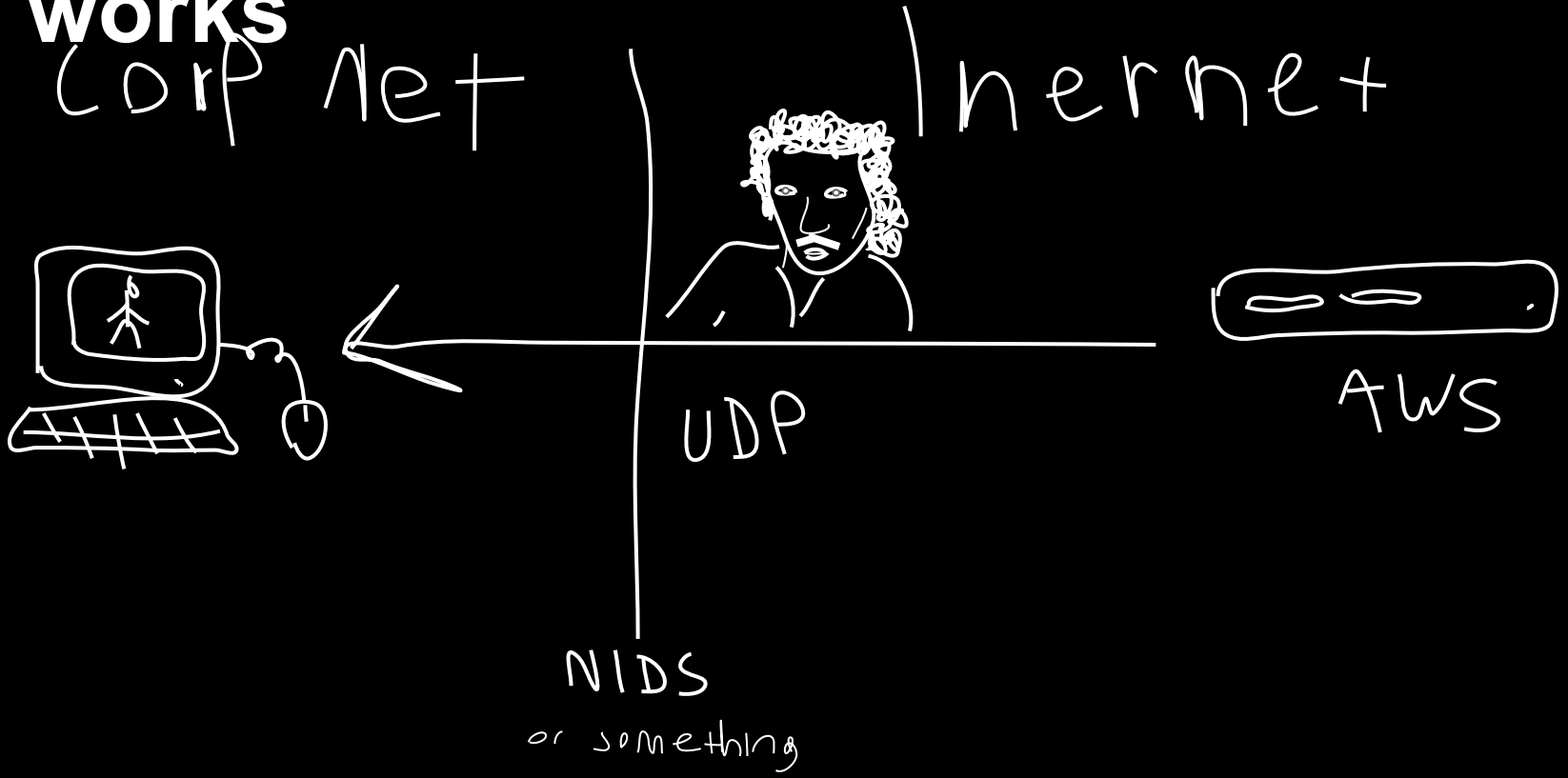
How HTTP/3 over QUIC with TLS 1.3 works



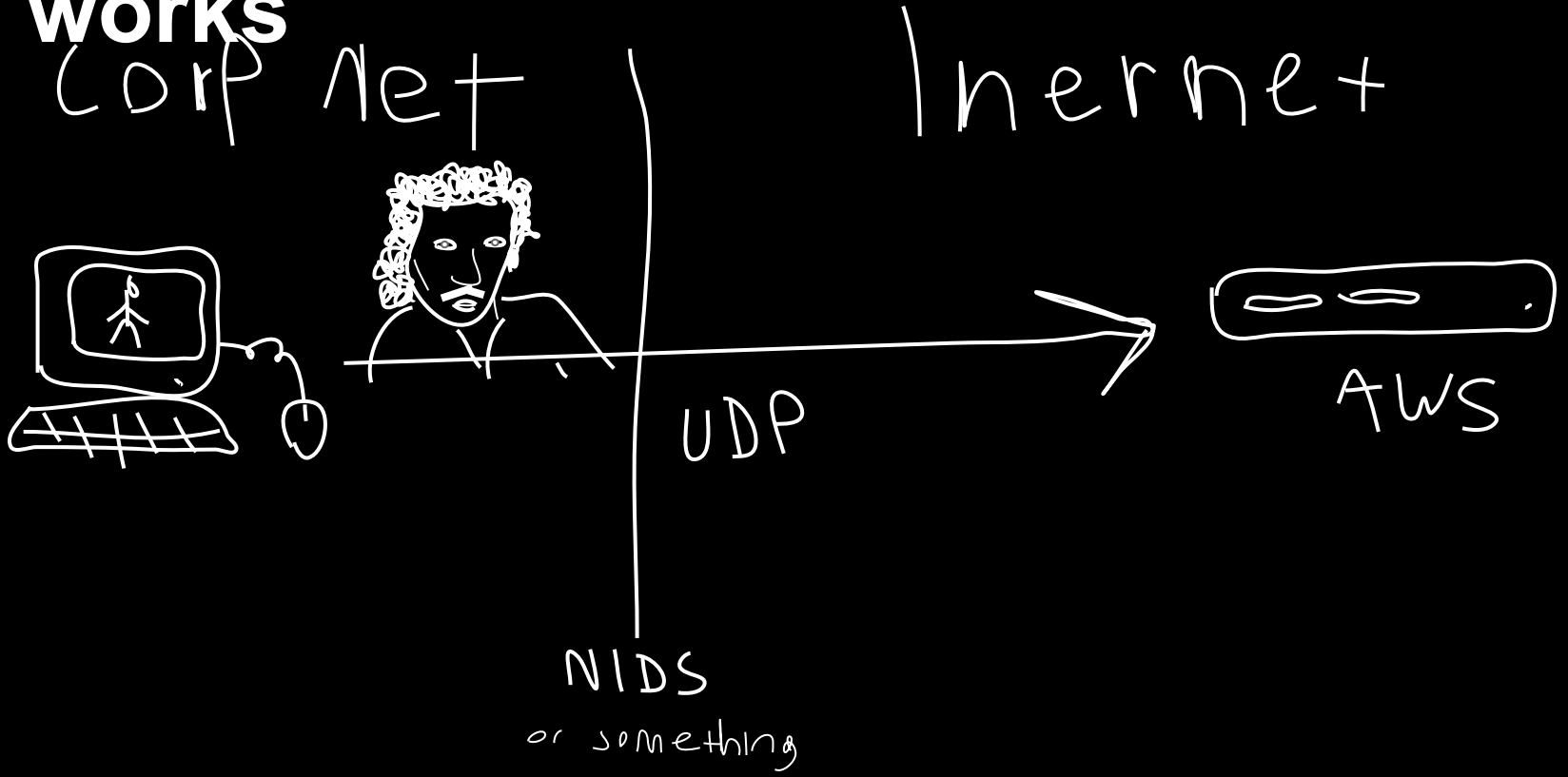
How HTTP/3 over QUIC with TLS 1.3 works



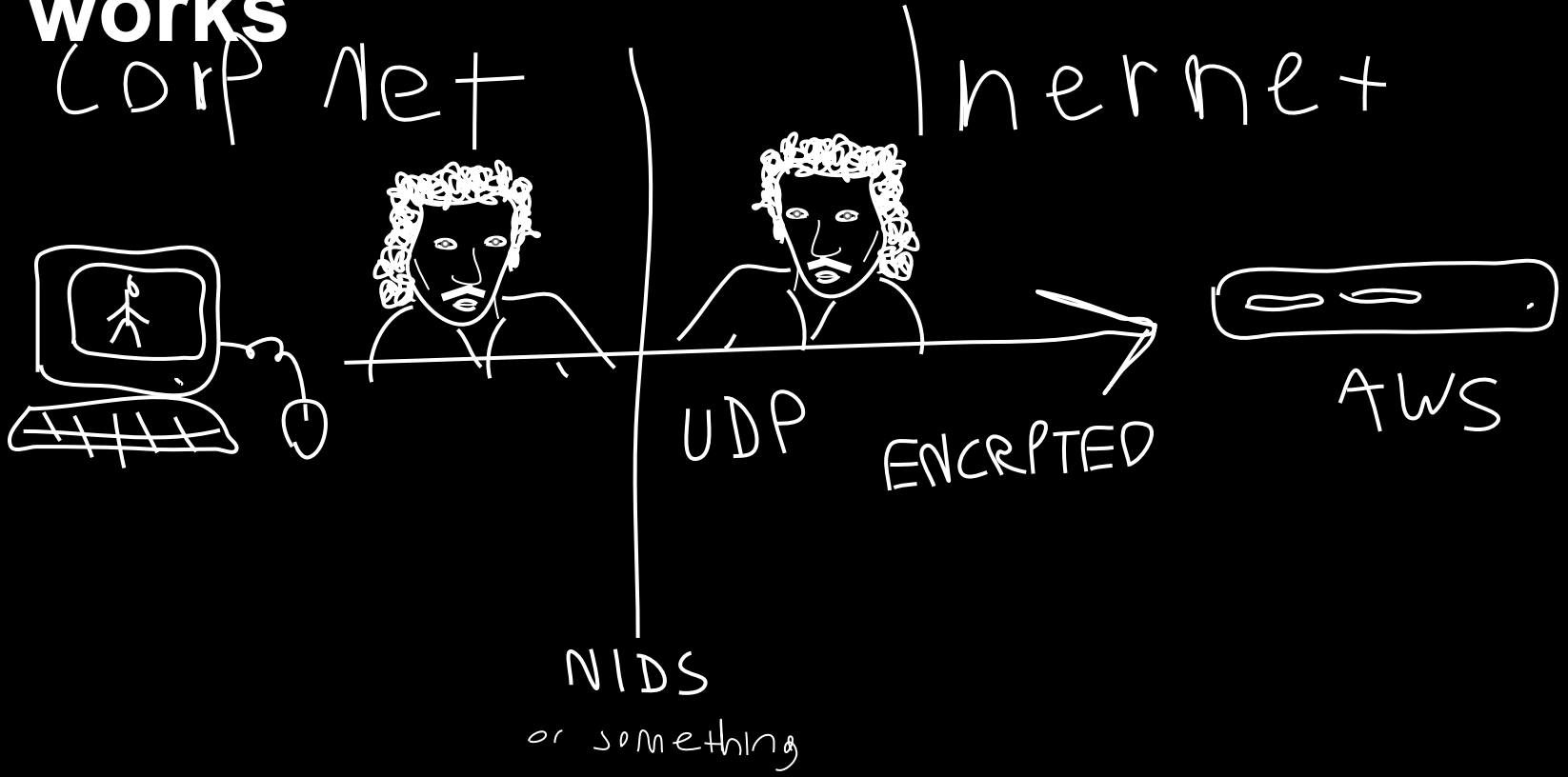
How HTTP/3 over QUIC with TLS 1.3 works



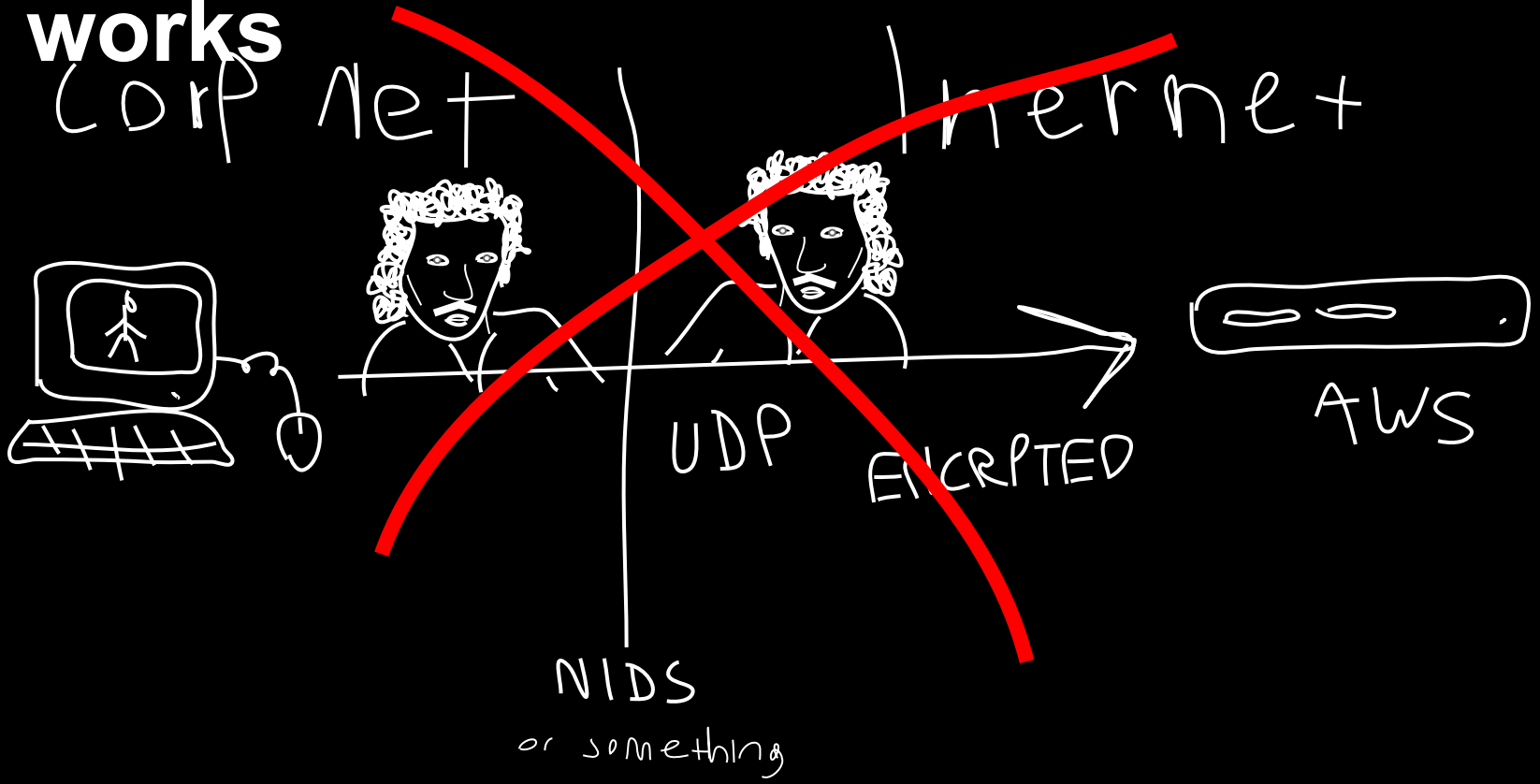
How HTTP/3 over QUIC with TLS 1.3 works



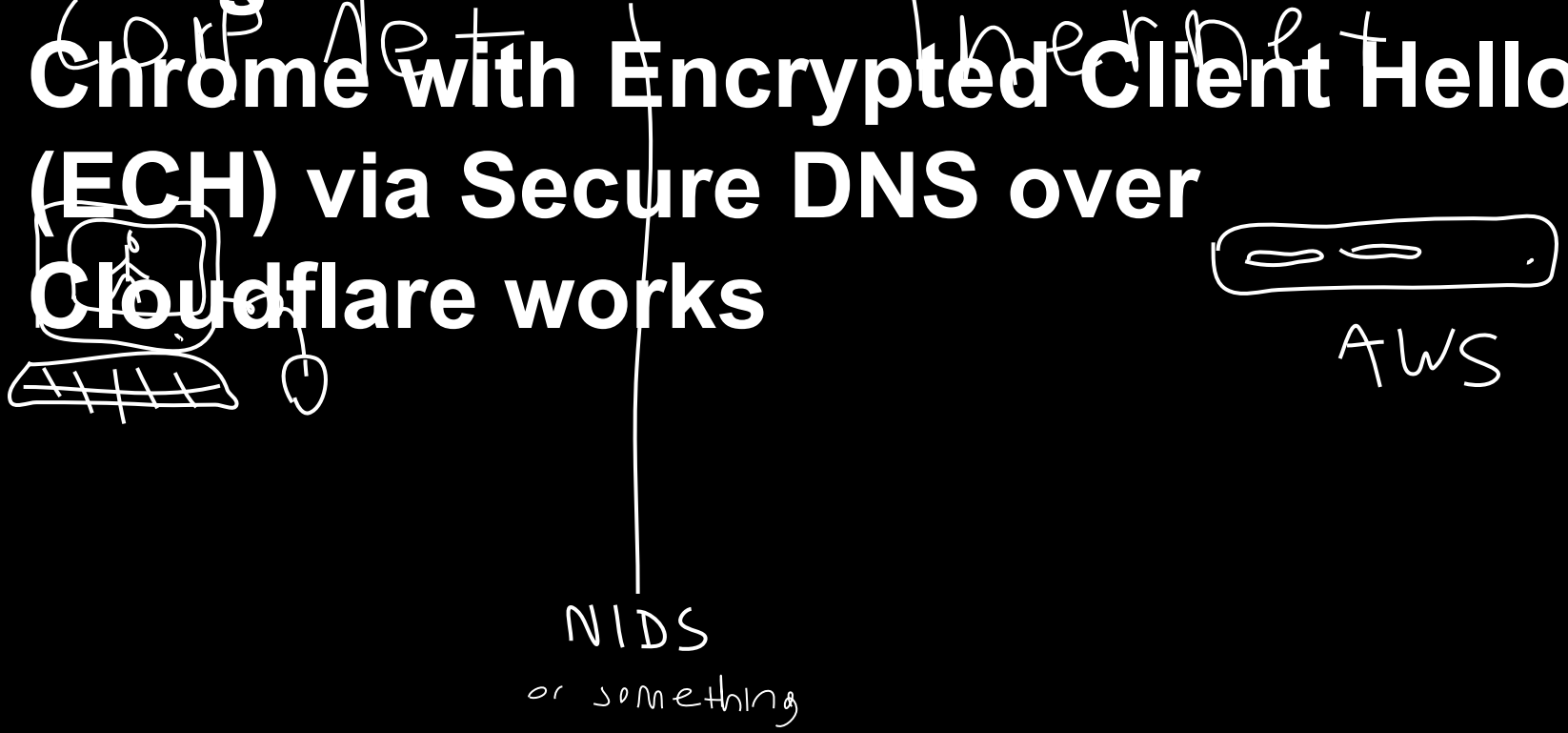
How HTTP/3 over QUIC with TLS 1.3 works



How HTTP/3 over QUIC with TLS 1.3 works

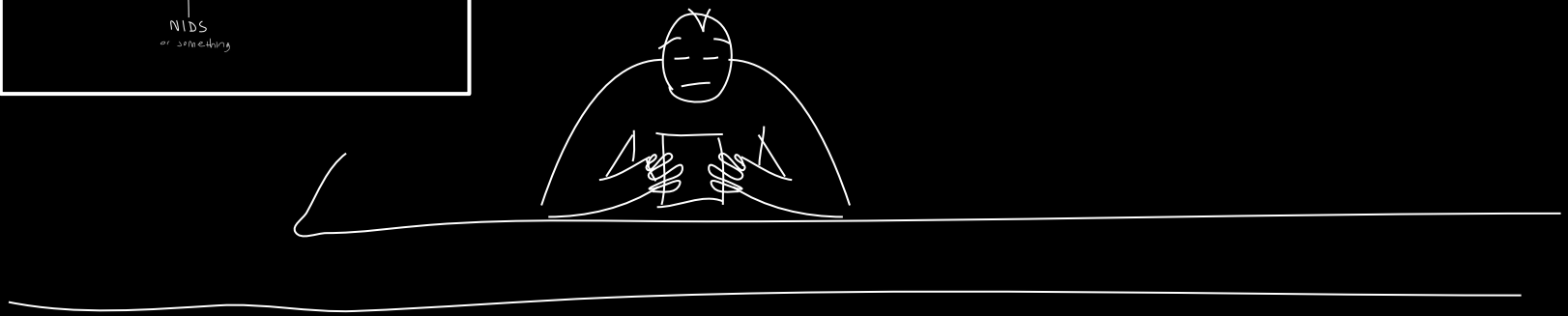


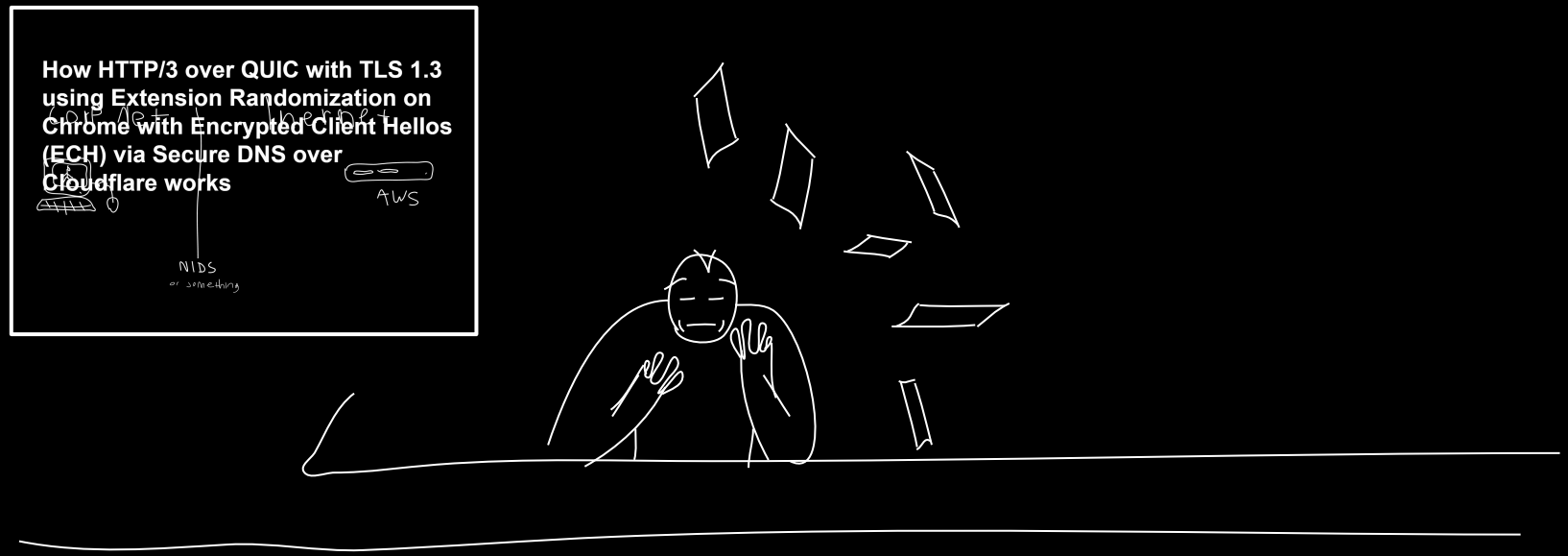
How HTTP/3 over QUIC with TLS 1.3 using Extension Randomization on Chrome with Encrypted Client Hellos (ECH) via Secure DNS over Cloudflare works



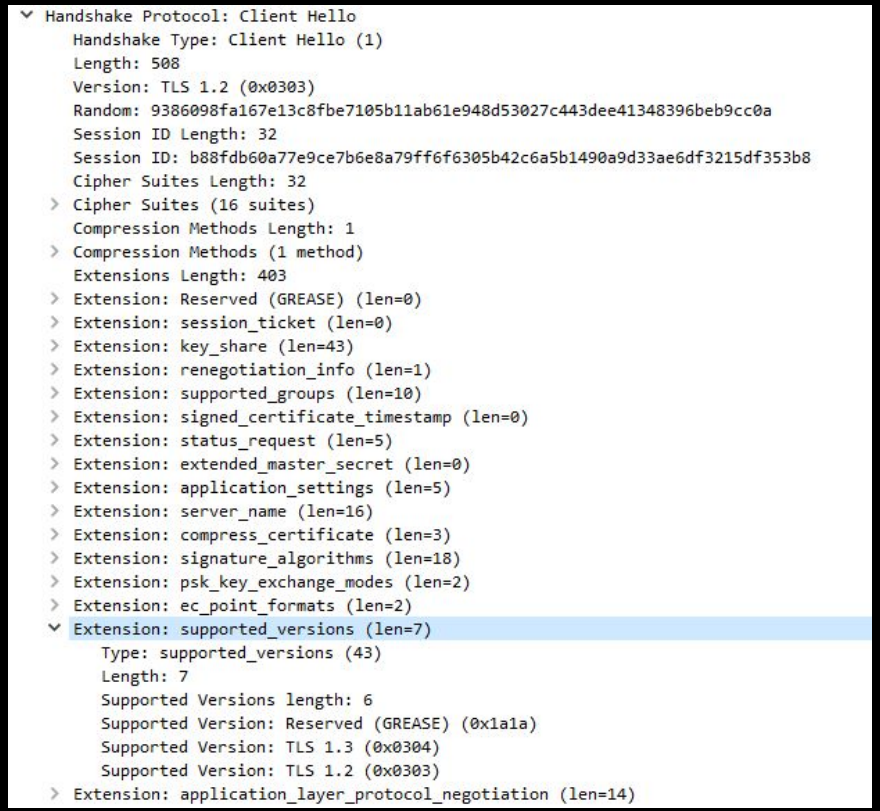
How HTTP/3 over QUIC with TLS 1.3 using Extension Randomization on Chrome with Encrypted Client Hellos (ECH) via Secure DNS over Cloudflare works



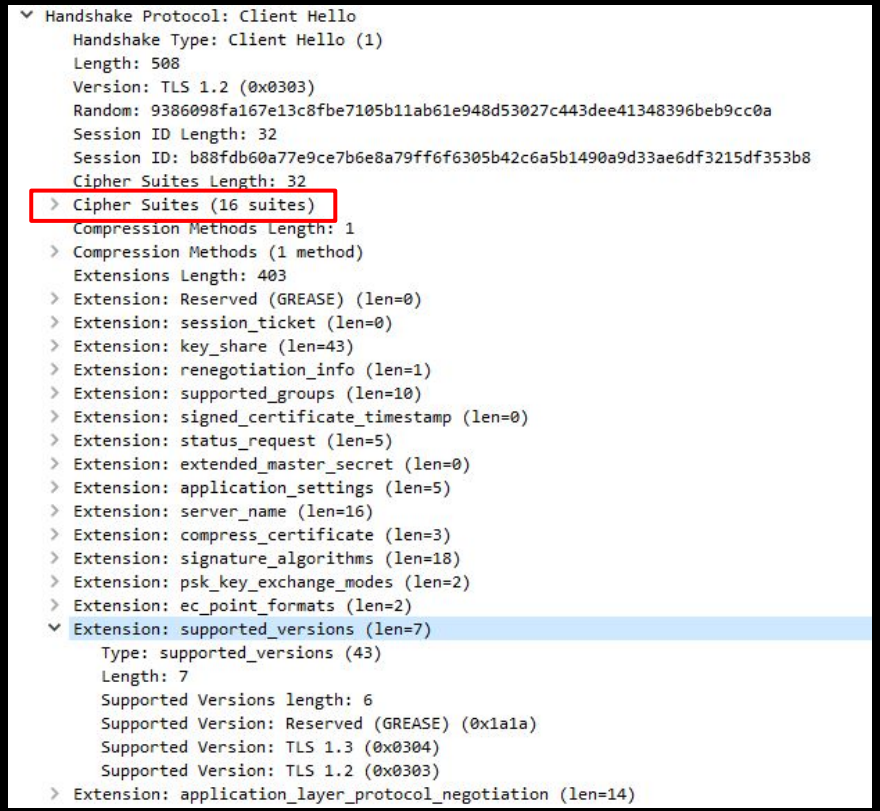



How HTTP/3 over QUIC with TLS 1.3 using Extension Randomization on Chrome with Encrypted Client Hellos (ECH) via Secure DNS over Cloudflare works
AWS
NIDS
or something

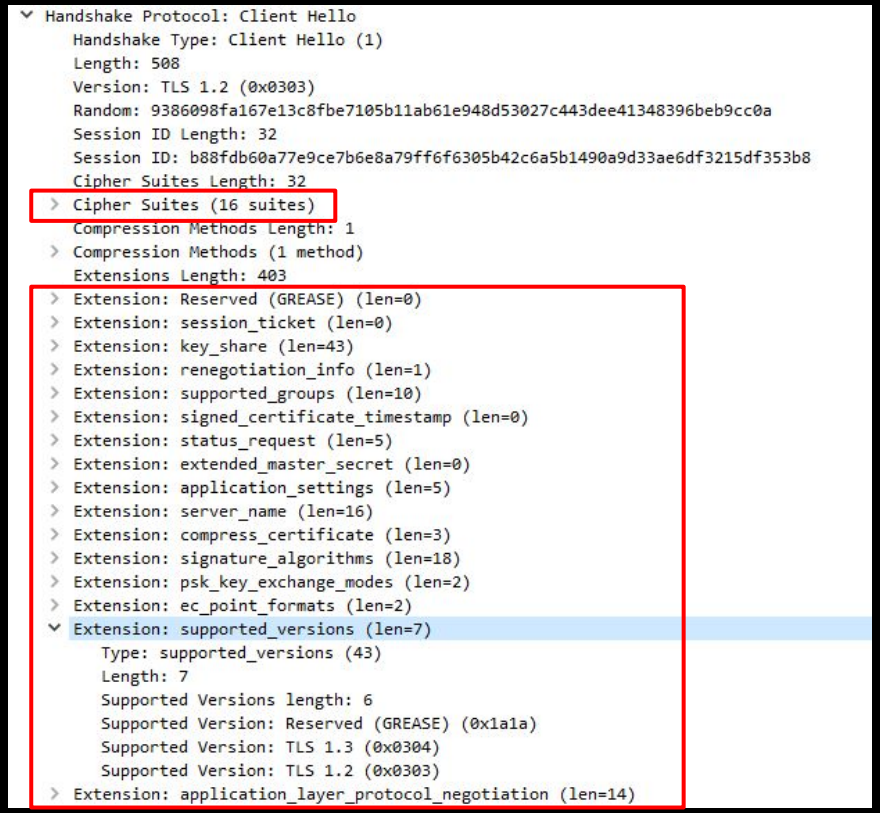
How TLS works (today)



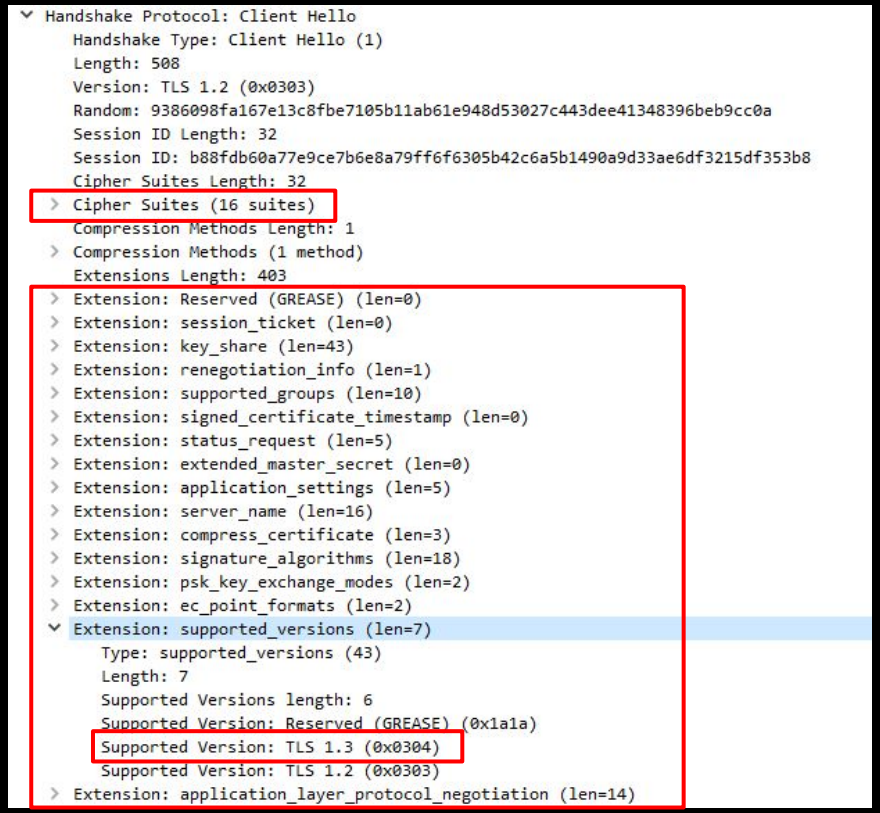
How TLS works (today)



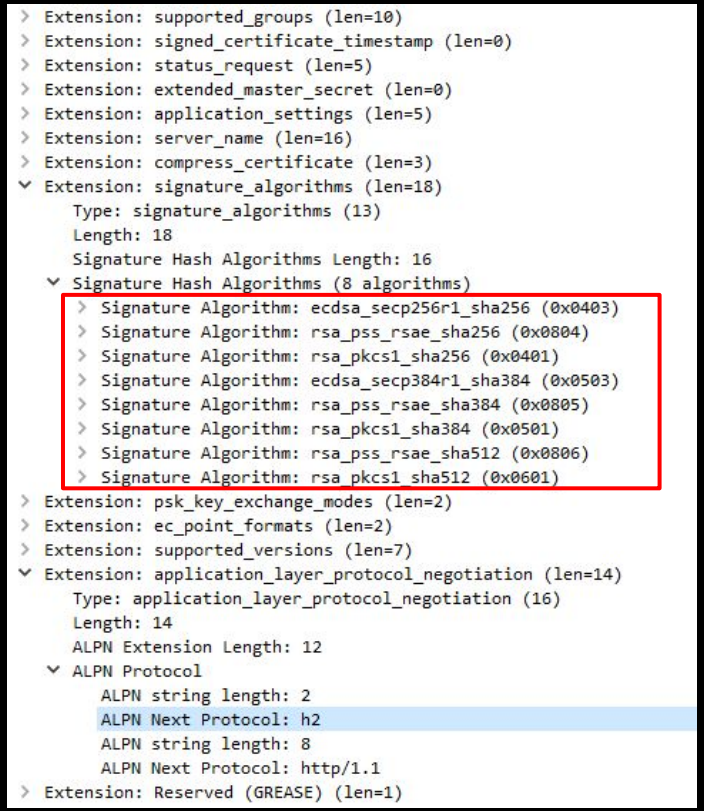
How TLS works (today)



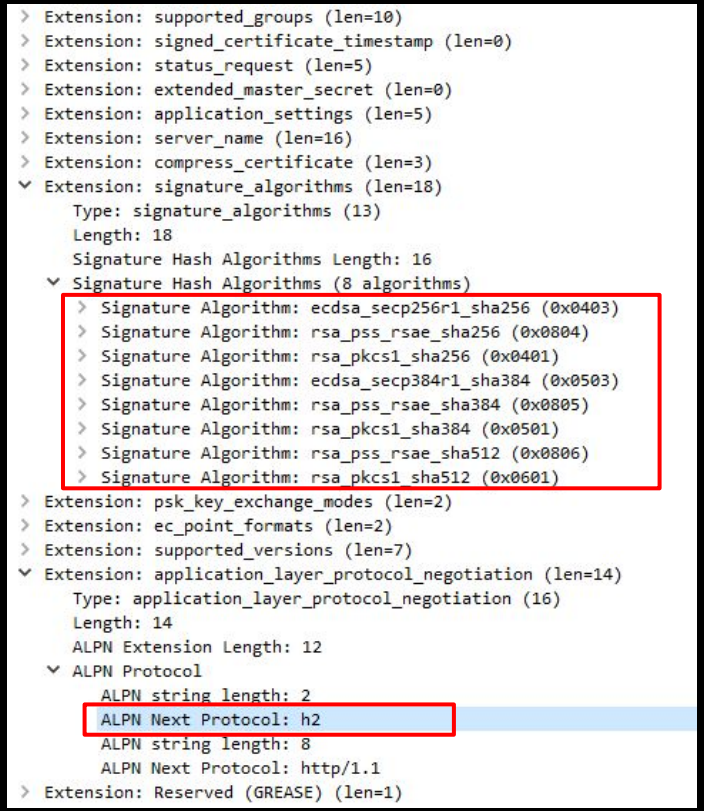
How TLS works (today)



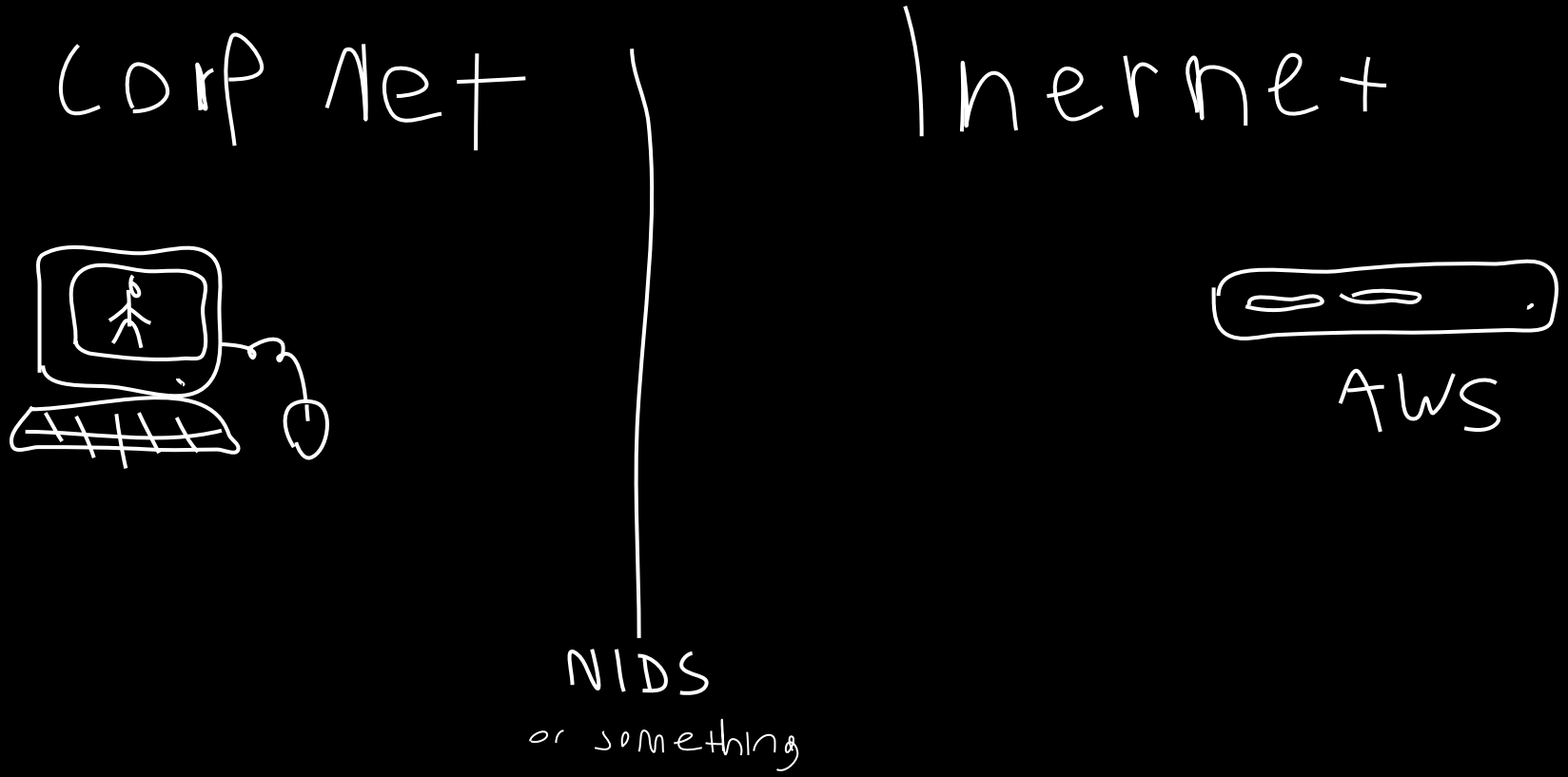
How TLS works (today)



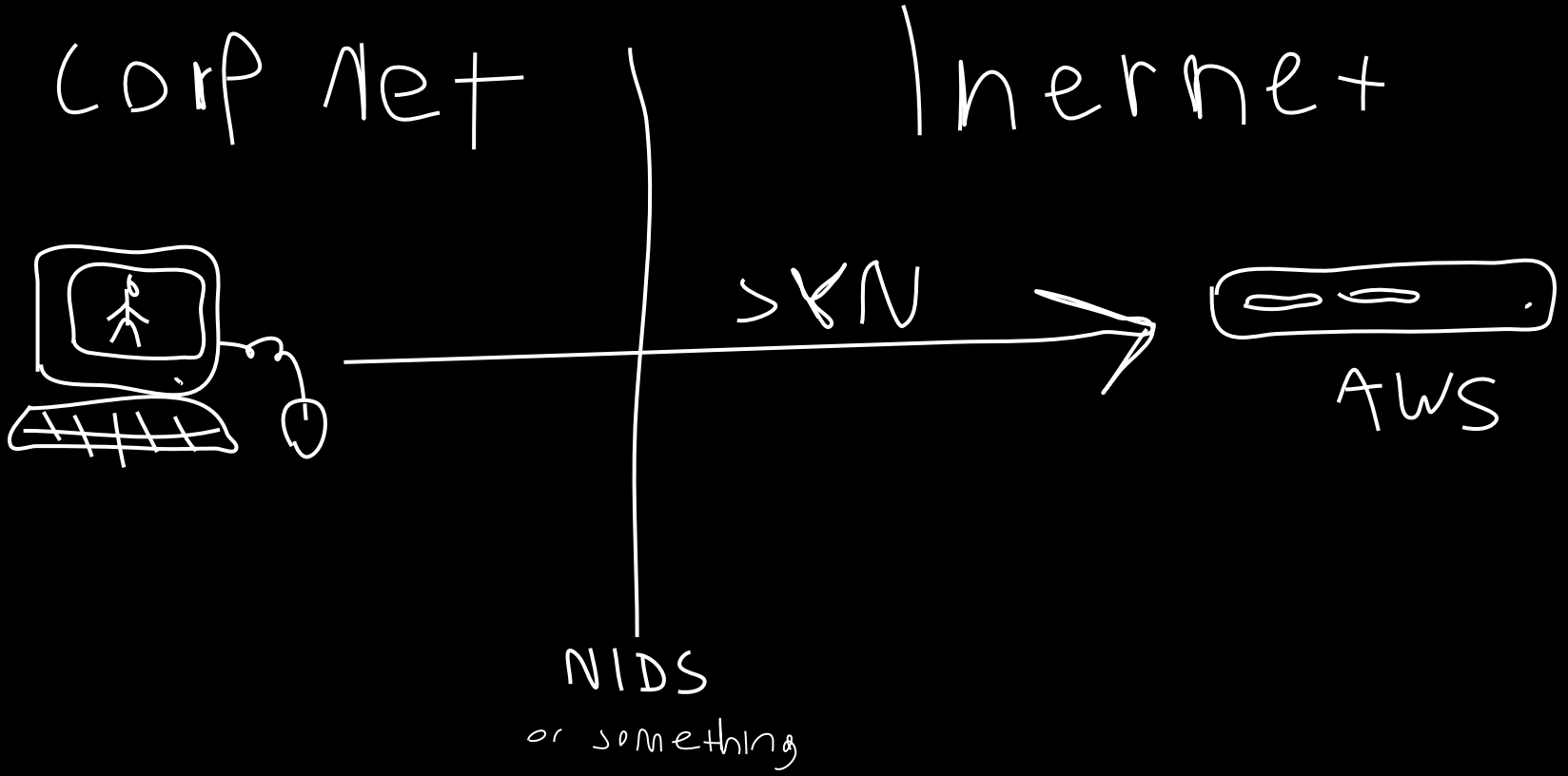
How TLS works (today)



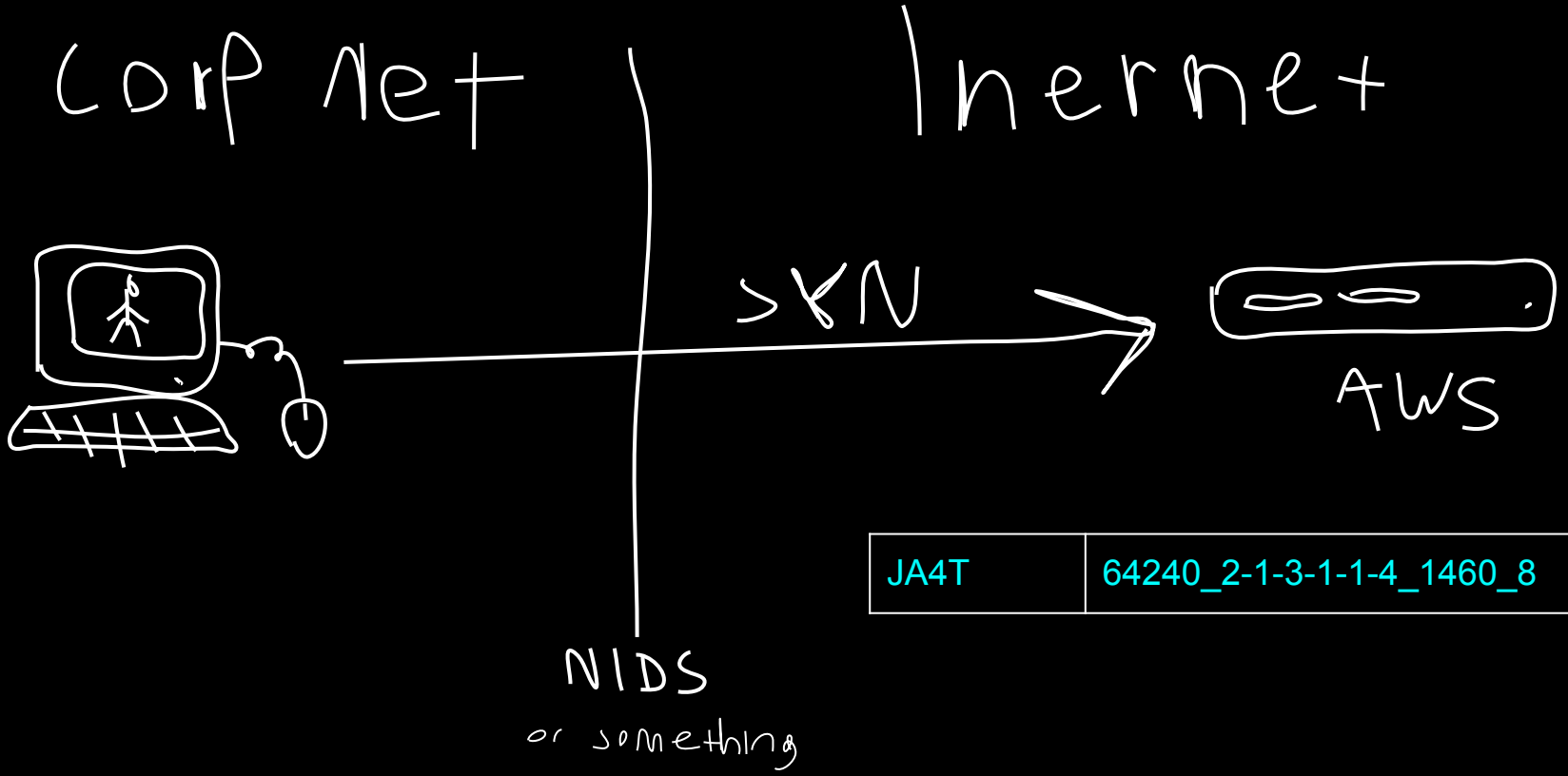
How TLS works



How TLS works

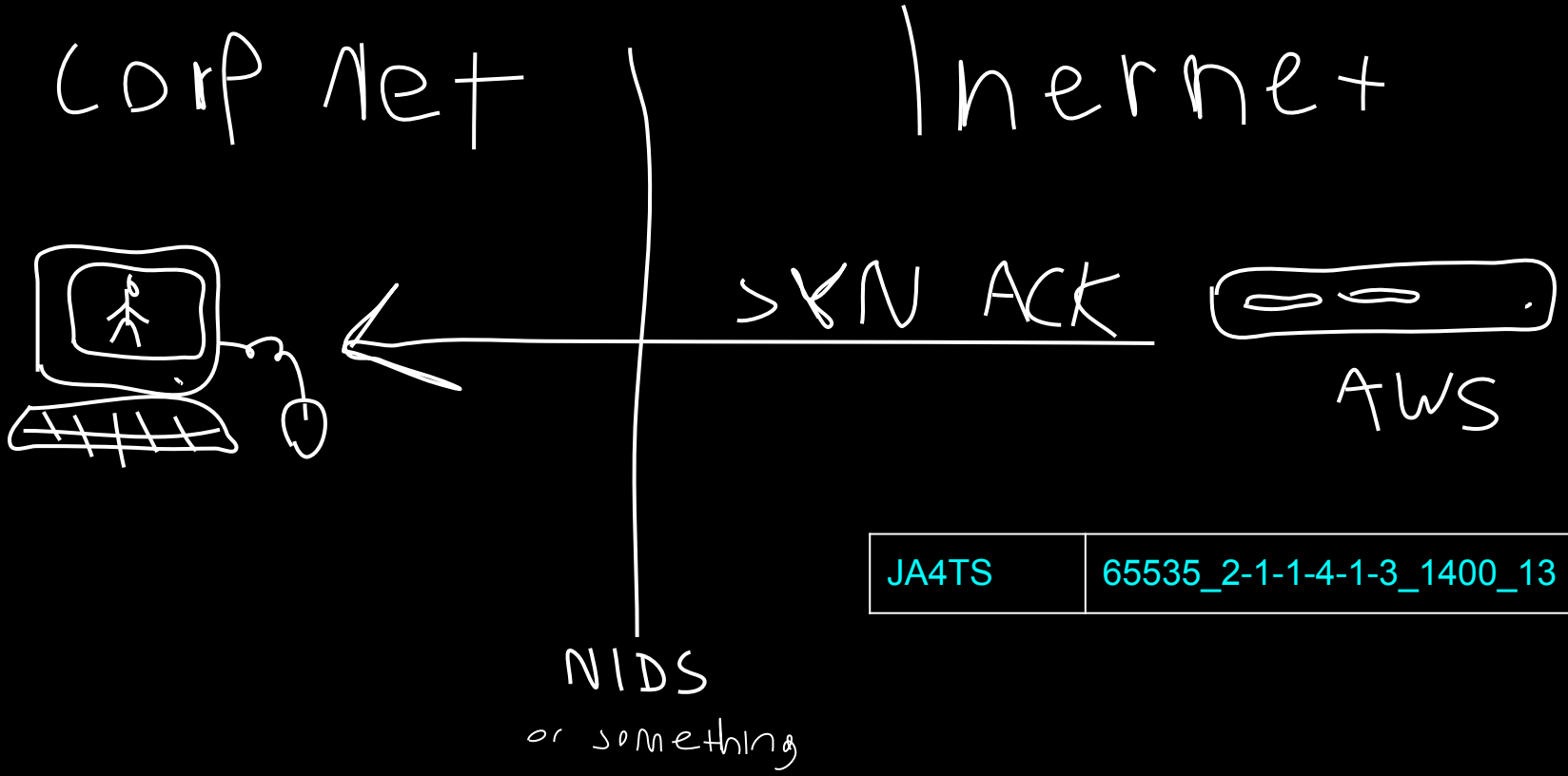


How TLS works



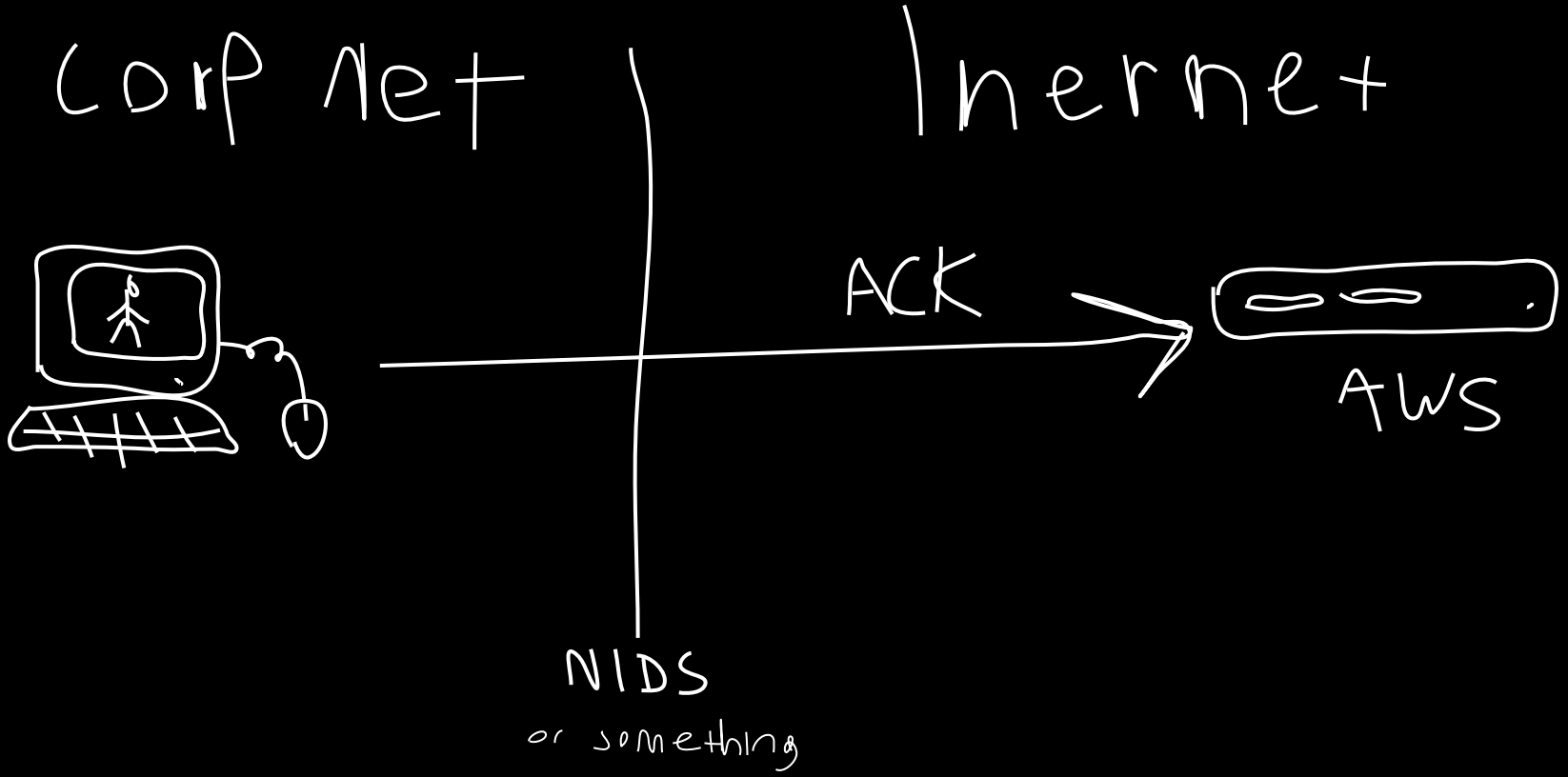
JA4T	64240_2-1-3-1-1-4_1460_8

How TLS works

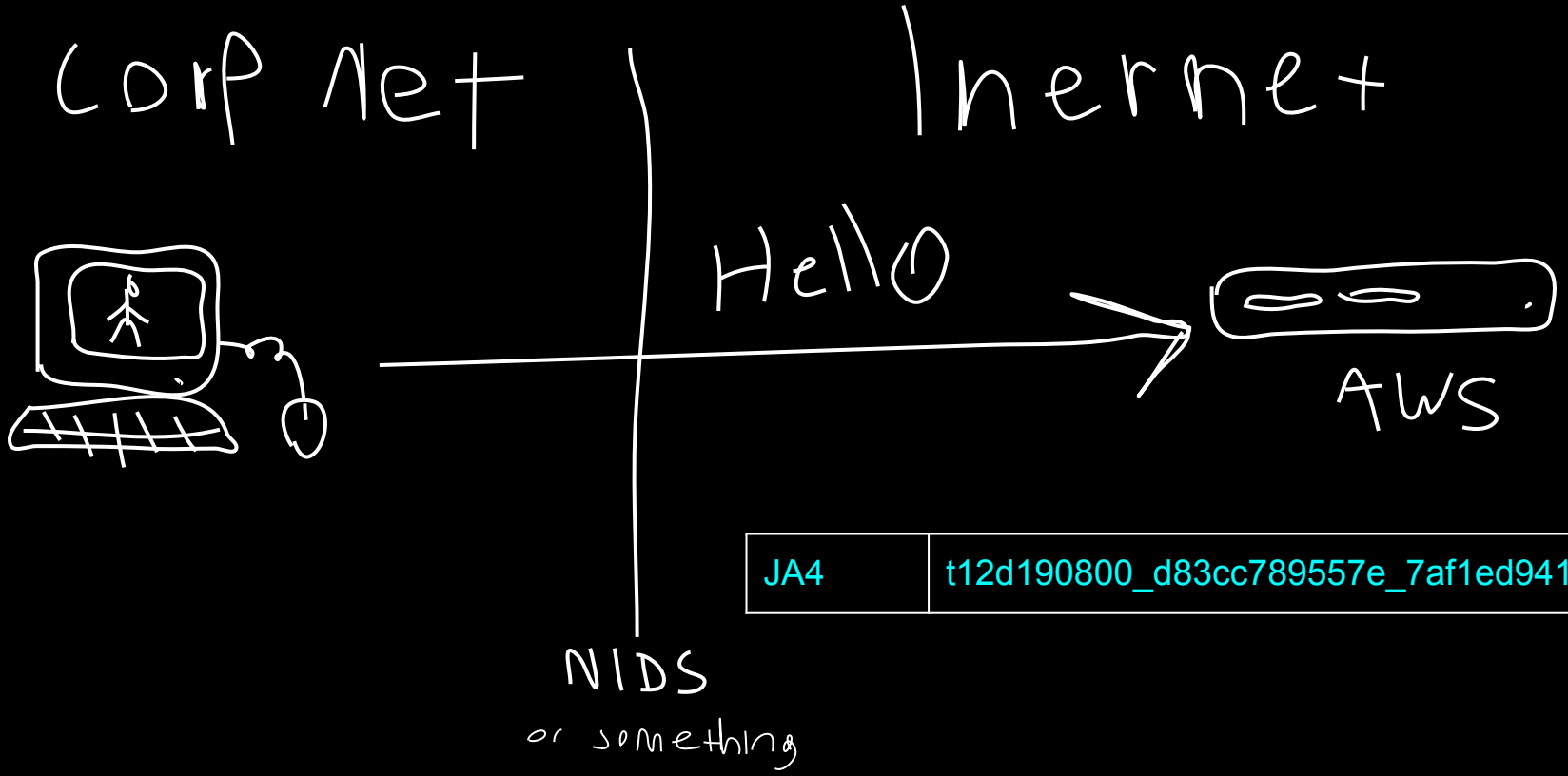


JA4TS	65535_2-1-1-4-1-3_1400_13

How TLS works

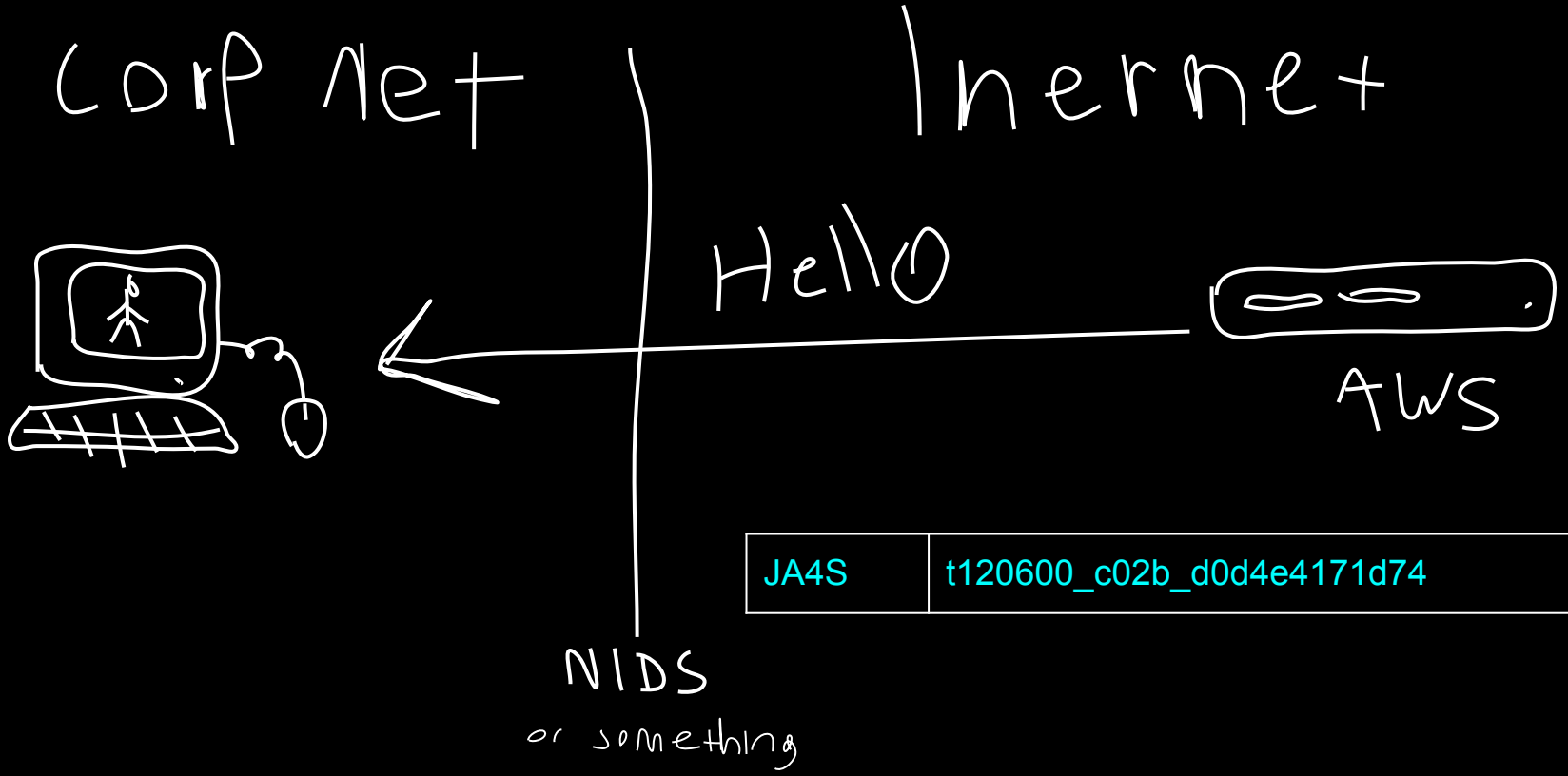


How TLS works



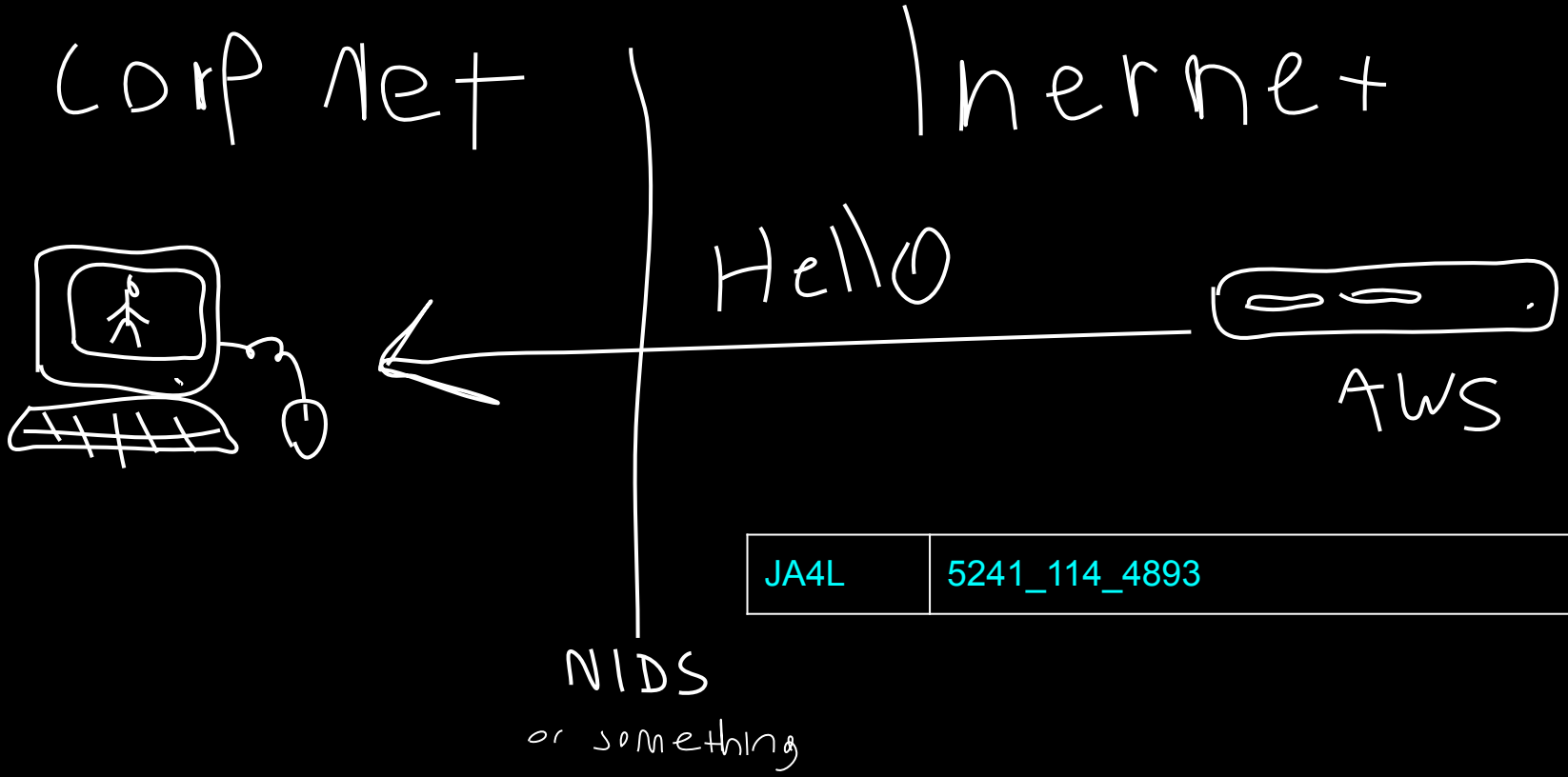
JA4	t12d190800_d83cc789557e_7af1ed941c26

How TLS works



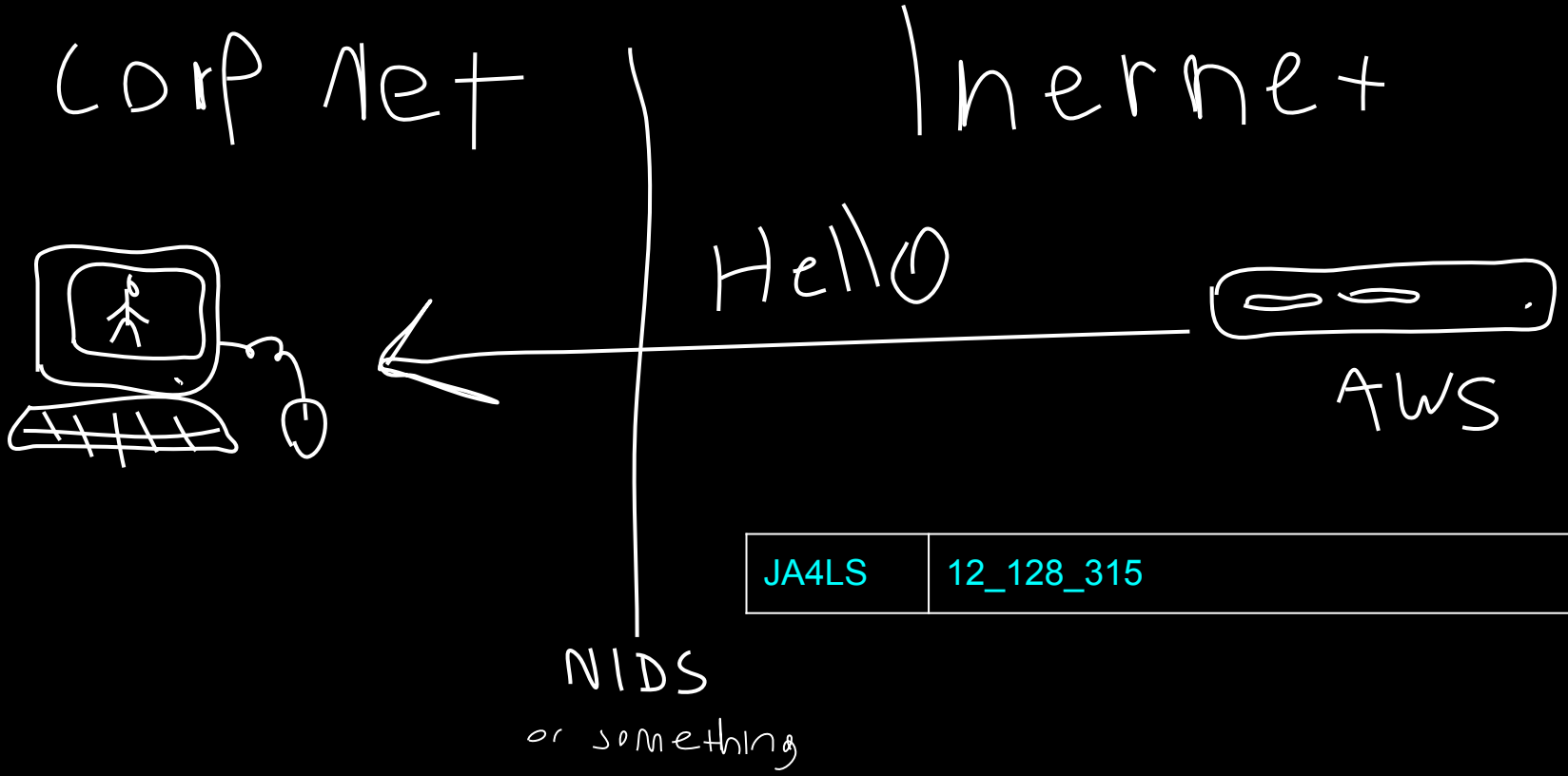
JA4S	t120600_c02b_d0d4e4171d74

How TLS works



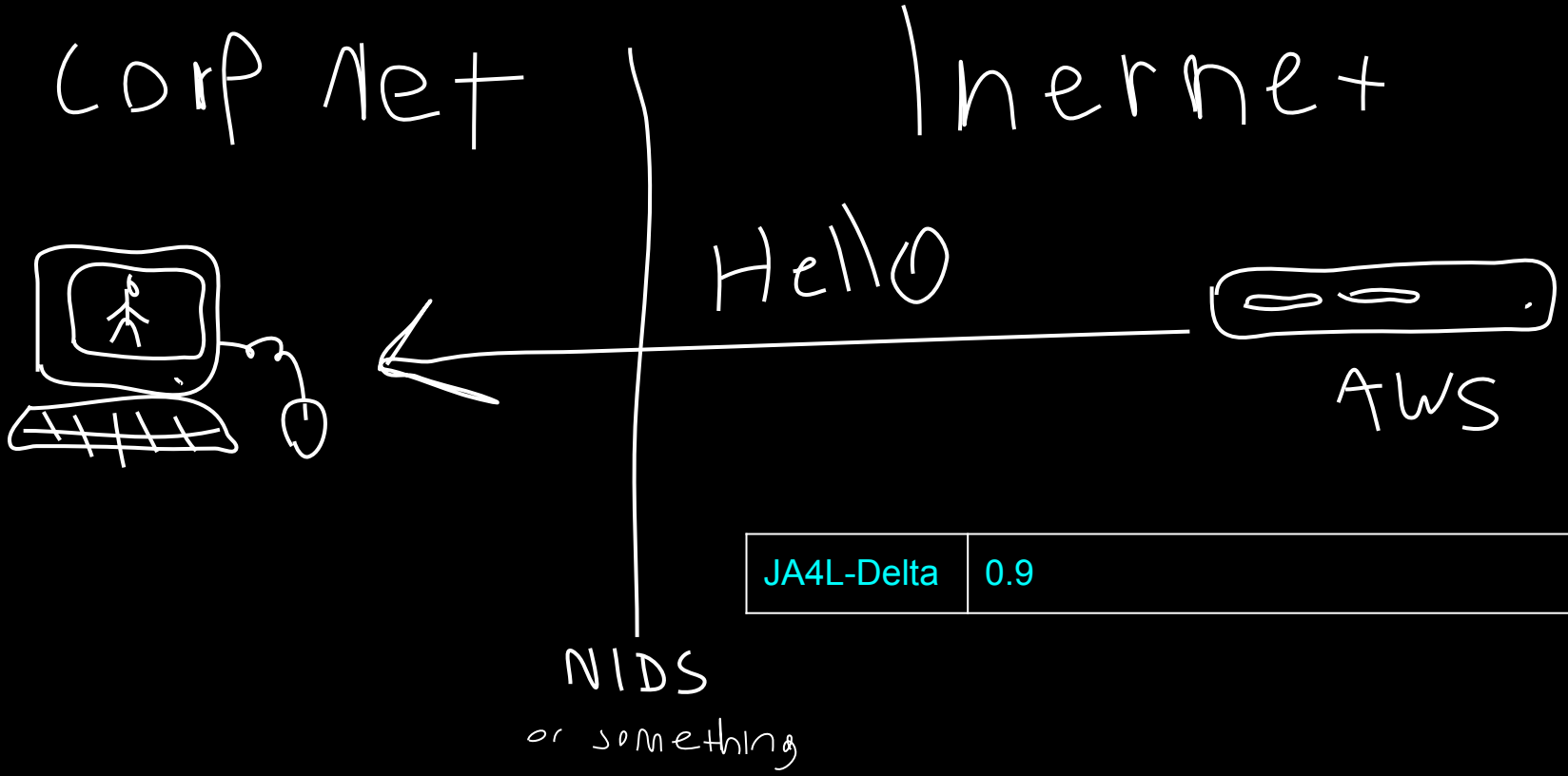
JA4L	5241_114_4893

How TLS works



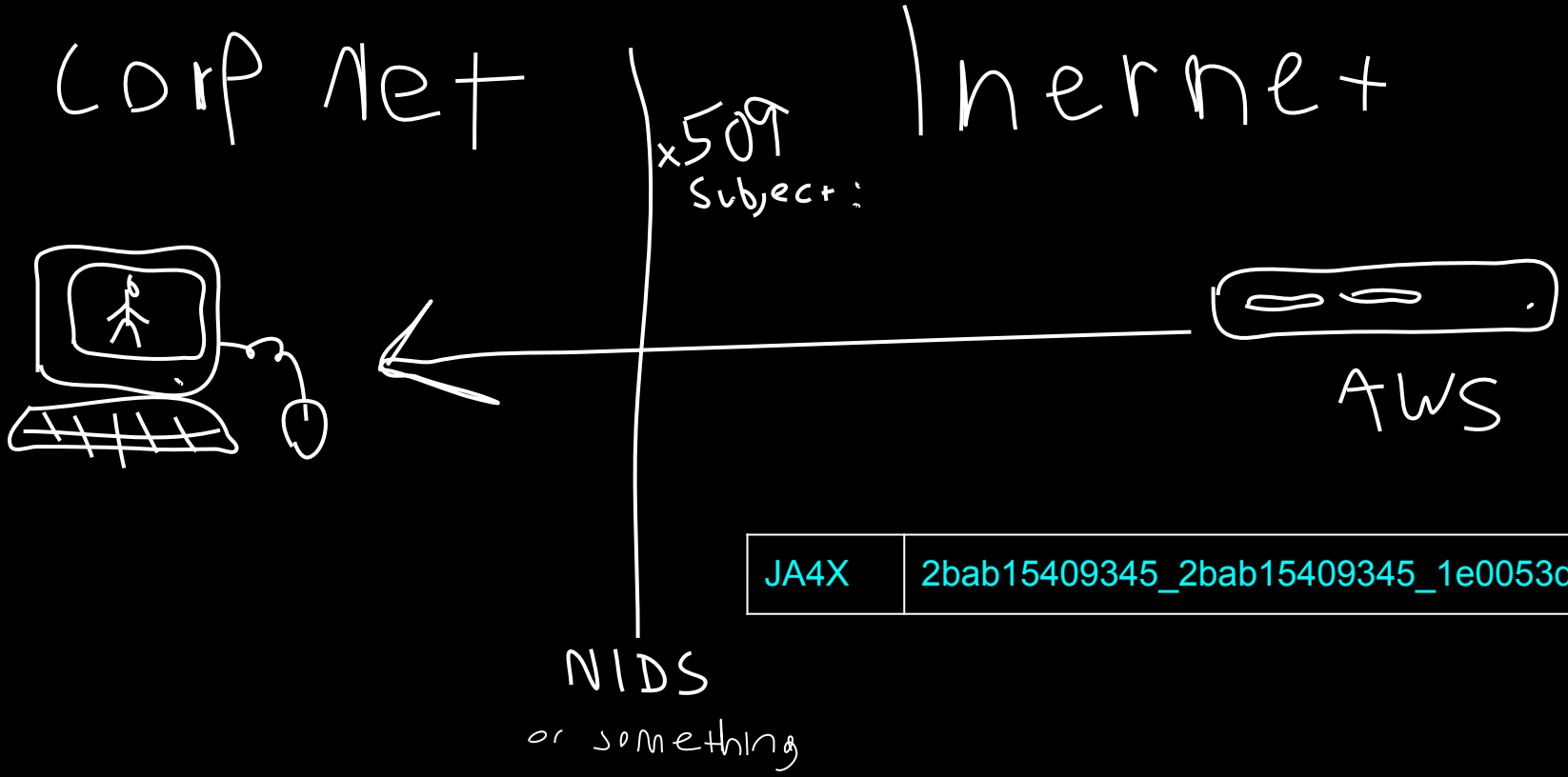
JA4LS	12_128_315

How TLS works



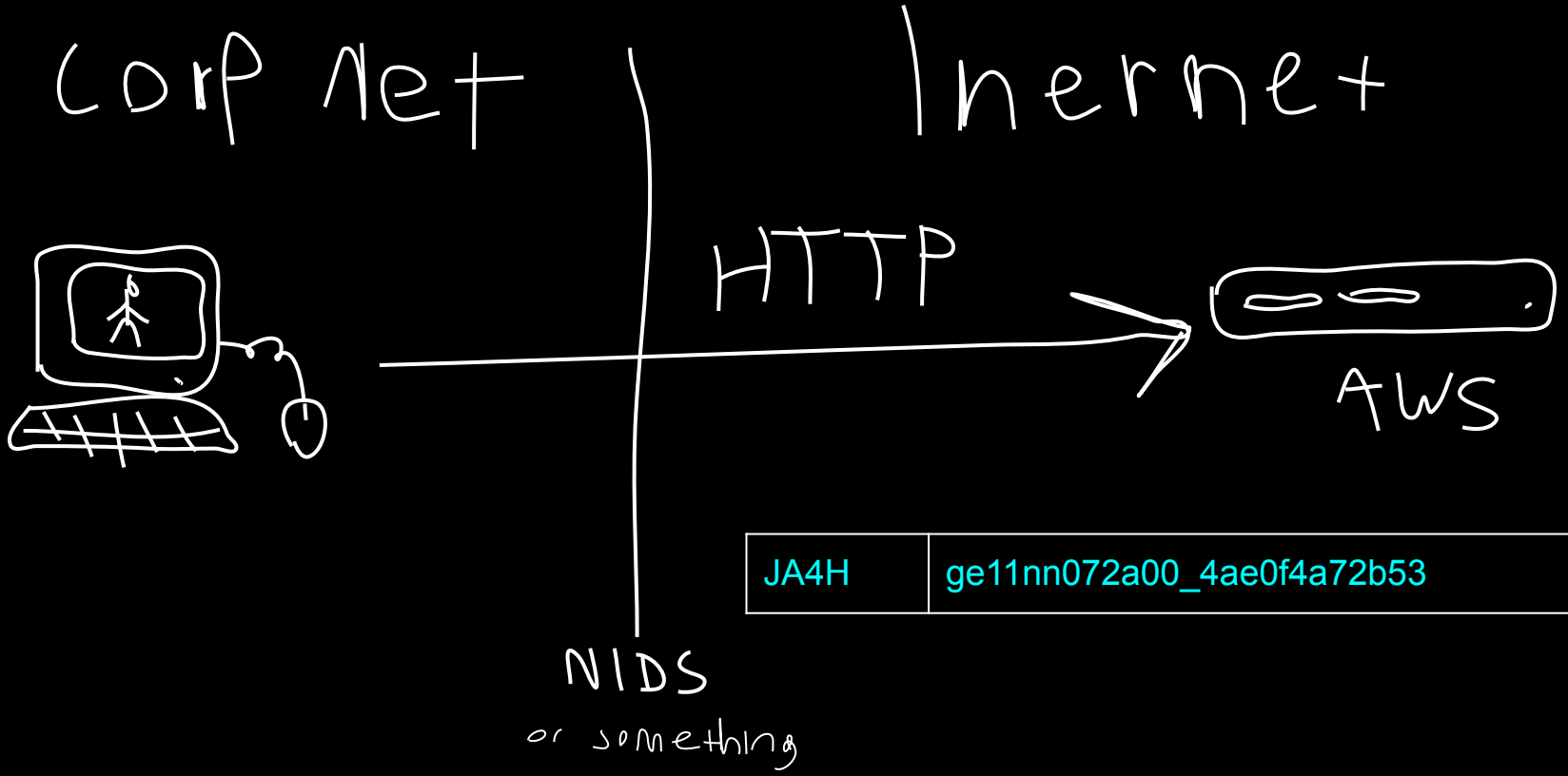
JA4L-Delta	0.9

How TLS works



JA4X	2bab15409345_2bab15409345_1e0053d9ccd0

How TLS works



JA4H	ge11nn072a00_4ae0f4a72b53

Identify traffic from Proxies

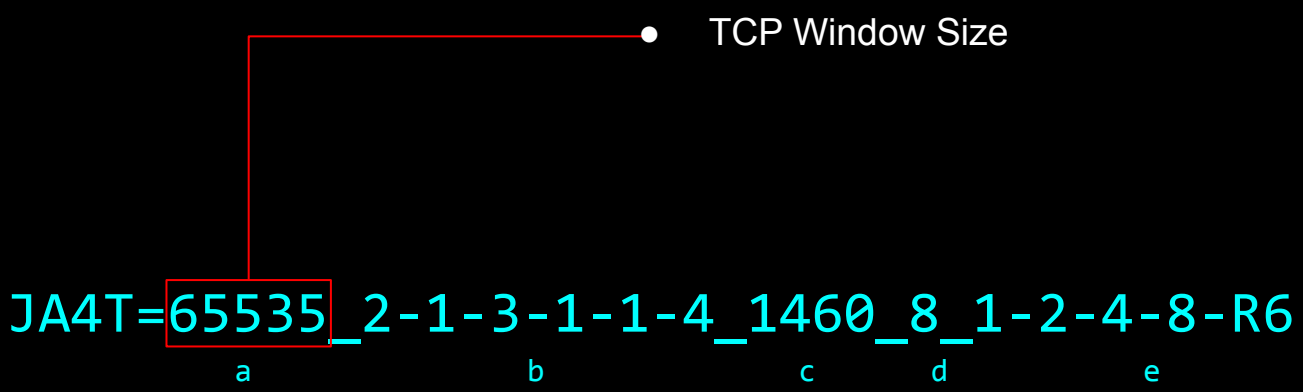
Utilizing:

JA4TCP + JA4Latency

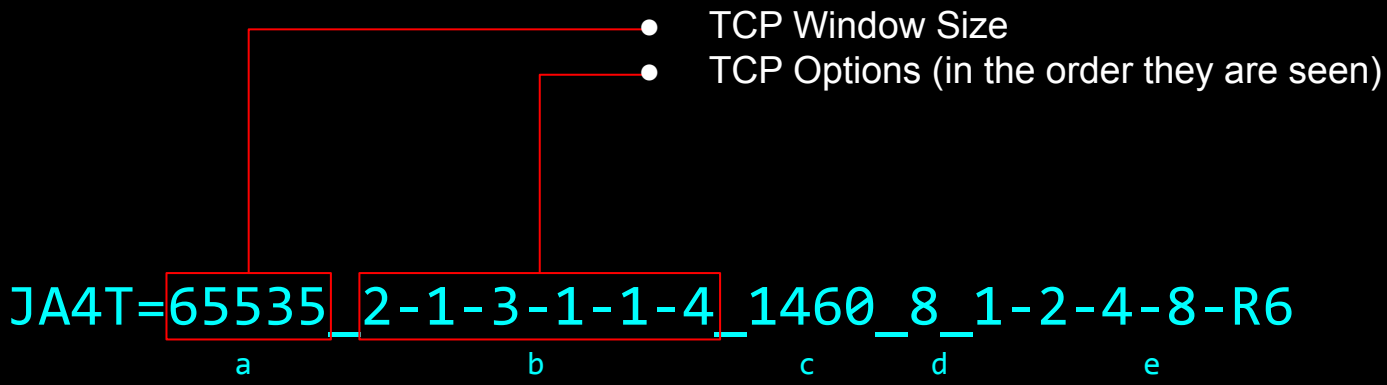
JA4T/S/Scan: TCP Fingerprint

```
JA4T=65535_2-1-3-1-1-4_1460_8_1-2-4-8-R6
     a           b          c    d      e
```

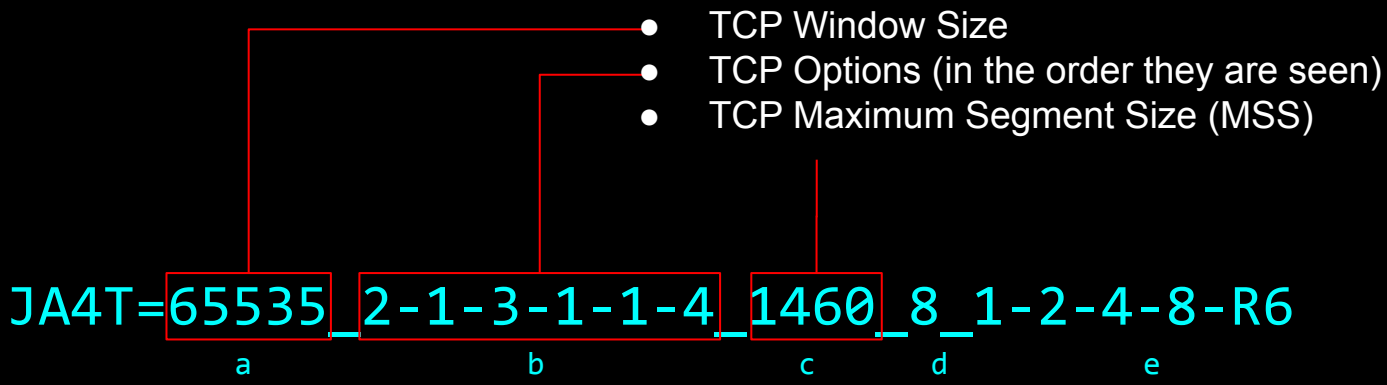
JA4T/S/Scan: TCP Fingerprint



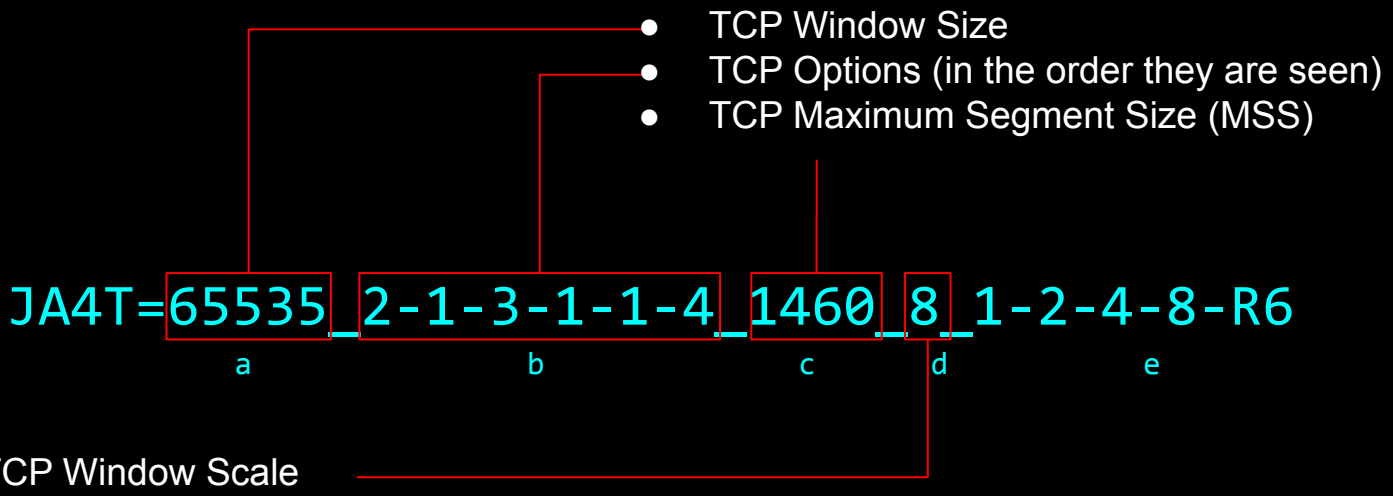
JA4T/S/Scan: TCP Fingerprint



JA4T/S/Scan: TCP Fingerprint

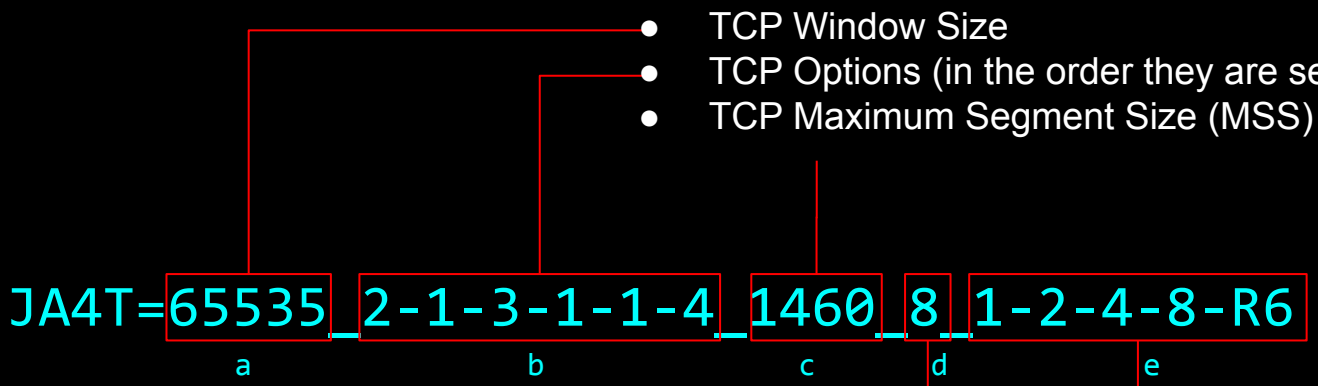


JA4T/S/Scan: TCP Fingerprint



FoxIO License 1.1

JA4T/S/Scan: TCP Fingerprint



JA4T - TCP OS/Device Fingerprinting

JA4T - TCP Client Fingerprint Examples	
OS / Device	**JA4T**
Windows 11	65535_2-1-3-1-1-4_1460_8
Windows 10	64240_2-1-3-1-1-4_1460_8
Ubuntu 22.04 on Win11 WSL	64240_2-4-8-1-3_1460_7
AWS Windows Server 2022	62727_2-1-3-1-1-4_1460_8
AWS Unix	62727_2-4-8-1-3_1460_7
AWS Unix (internal)	62727_2-4-8-1-3_8961_7
Android 12	42600_2-4-8-1-3_1460_12
Android 13	65535_2-4-8-1-3_1460_9
OSX/iOS (all versions)	65535_2-1-3-1-1-8-4-0-0_1460_6

JA4T - TCP OS/Device Fingerprinting

JA4T - TCP Client Fingerprint Examples	
OS / Device	**JA4T**
Windows 11	65535_2-1-3-1-1-4_1460_8
Windows 10	64240_2-1-3-1-1-4_1460_8
Ubuntu 22.04 on Win11 WSL	64240_2-4-8-1-3_1460_7
AWS Windows Server 2022	62727_2-1-3-1-1-4_1460_8
AWS Unix	62727_2-4-8-1-3_1460_7
AWS Unix (internal)	62727_2-4-8-1-3_8961_7
Android 12	42600_2-4-8-1-3_1460_12
Android 13	65535_2-4-8-1-3_1460_9
OSX/iOS (all versions)	65535_2-1-3-1-1-8-4-0-0_1460_6

VPN Detection

Maximum Transmission Unit (MTU) over Ethernet - 1500 Bytes			
IPv4 - 20B	1480 Bytes Remaining		
IPv4 - 20B	TCP - 20B	1460 Bytes (The most common MSS value)	
IPv4 - 20B	TCP - 20B	Wireguard VPN - 80B	1380 Bytes (The MSS of a device going through a VPN)

VPN Detection

OS / Device	VPN / Proxy	JA4T
Windows 11	None	64240_2-1-3-1-1-4_1460_8
Windows 11	OpenVPN	64240_2-1-3-1-1-4_1326_8
Windows 11	Wireguard VPN	64860_2-1-3-1-1-4_1380_8
iPhone	None	65535_2-1-3-1-1-8-4-0-0_1460_6
iPhone	OpenVPN	65535_2-1-3-1-1-8-4-0-0_1326_6
iPhone	iCloud Relay	64240_2-4-8-1-3_1380_13

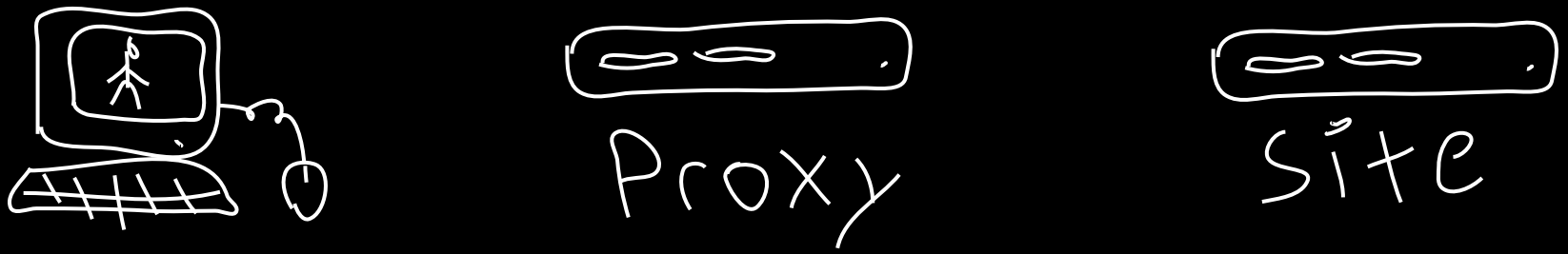
VPN Detection

Windows 10	Chrome 133 DNT	Wireguard VPN - MTU Large	Local	t13d1517h2_8daaf6152771_b6f405a00624	64860_2-1-3-1-1-4_1380_8
Windows 10	Chrome 133 DNT	Wireguard VPN - MTU Auto	Local	t13d1517h2_8daaf6152771_b6f405a00624	64578_2-1-3-1-1-4_1374_8
Windows 10	Chrome 133 DNT	Wireguard VPN - MTU Small	Local	t13d1517h2_8daaf6152771_b6f405a00624	65340_2-1-3-1-1-4_1210_8
Windows 10	Chrome 133 DNT	OpenVPN - UDP - MTU Small	Local	t13d1517h2_8daaf6152771_b6f405a00624	65340_2-1-3-1-1-4_1210_8
Windows 10	Chrome 133 DNT	OpenVPN - TCP - MTU Small	Local	t13d1517h2_8daaf6152771_b6f405a00624	65340_2-1-3-1-1-4_1210_8
Windows 10	Chrome 133 DNT	OpenVPN - UDP - MTU Auto	Local	t13d1517h2_8daaf6152771_b6f405a00624	64446_2-1-3-1-1-4_1286_8
Windows 10	Chrome 133 DNT	OpenVPN - TCP - MTU Auto	Local	t13d1517h2_8daaf6152771_b6f405a00624	64240_2-1-3-1-1-4_1284_8
Windows 10	Chrome 133 DNT	OpenVPN - TCP - MTU Large	Local	t13d1517h2_8daaf6152771_b6f405a00624	65142_2-1-3-1-1-4_1284_8
Windows 10	Chrome 133 DNT	OpenVPN - UDP - MTU Large	Local	t13d1517h2_8daaf6152771_b6f405a00624	64768_2-1-3-1-1-4_1286_8

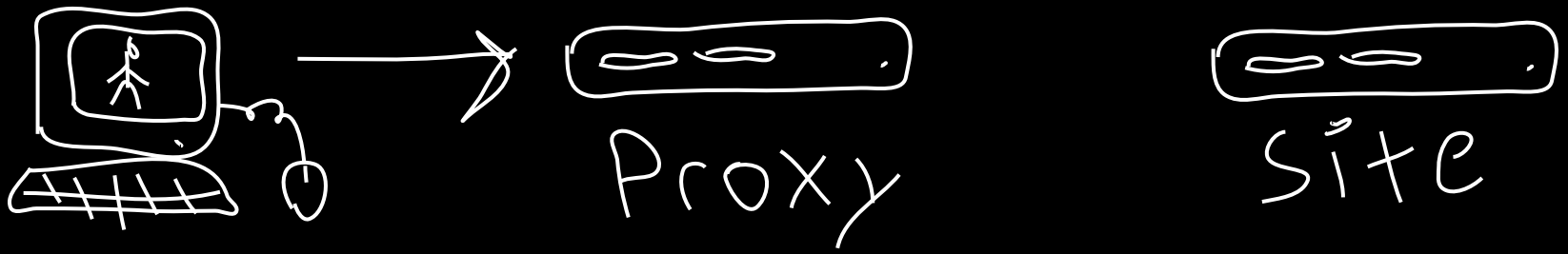
VPN Detection

OS / Device	VPN / Proxy	JA4T
Windows 11	None	64240_2-1-3-1-1-4_1460_8
Windows 11	OpenVPN	64240_2-1-3-1-1-4_1326_8
Windows 11	Wireguard VPN	64860_2-1-3-1-1-4_1380_8
iPhone	None	65535_2-1-3-1-1-8-4-0-0_1460_6
iPhone	OpenVPN	65535_2-1-3-1-1-8-4-0-0_1326_6
iPhone	iCloud Relay	64240_2-4-8-1-3_1380_13

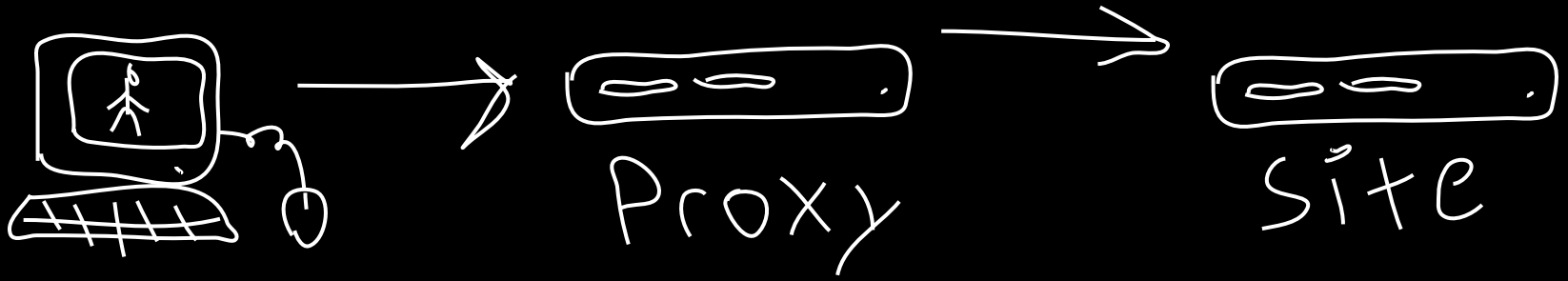
How Proxies Work - TCP



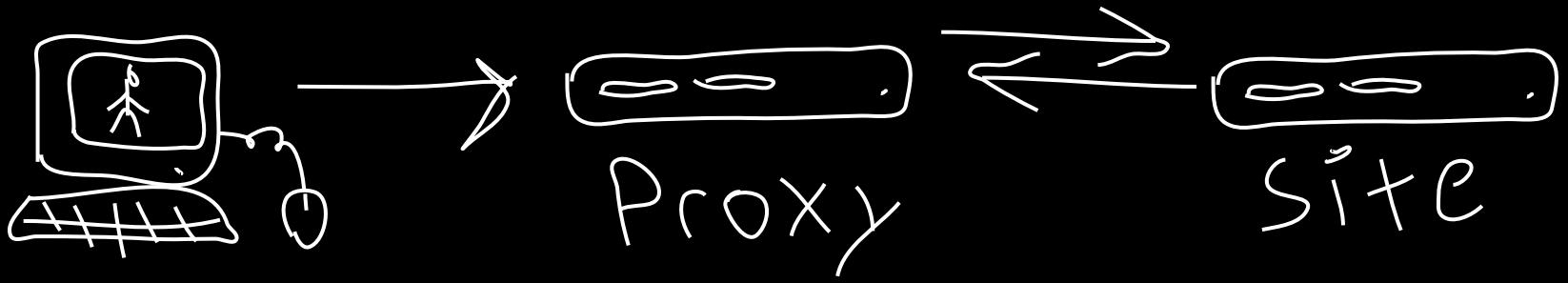
How Proxies Work - TCP



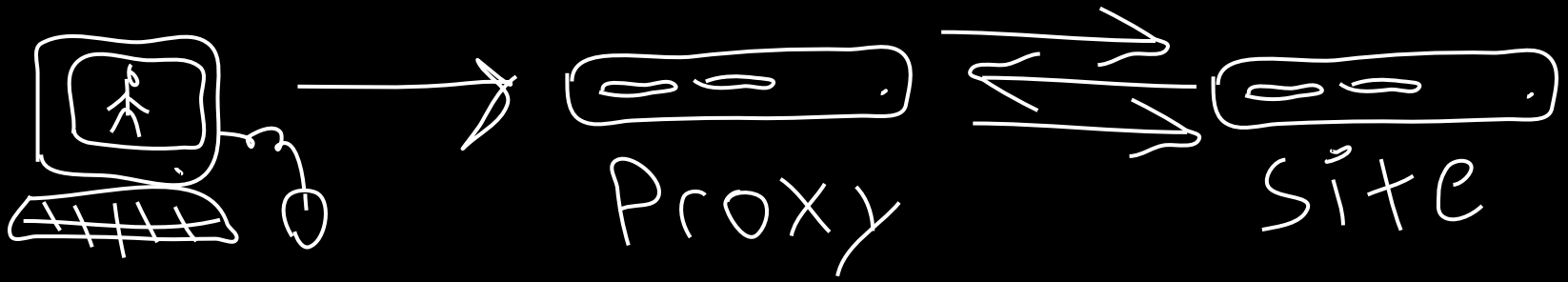
How Proxies Work - TCP



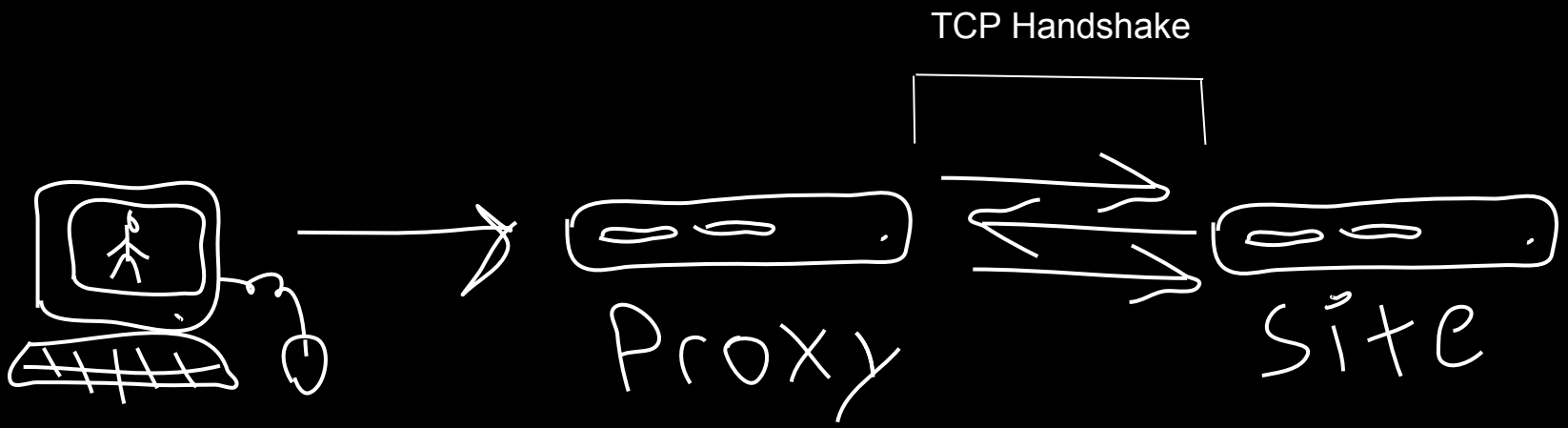
How Proxies Work - TCP



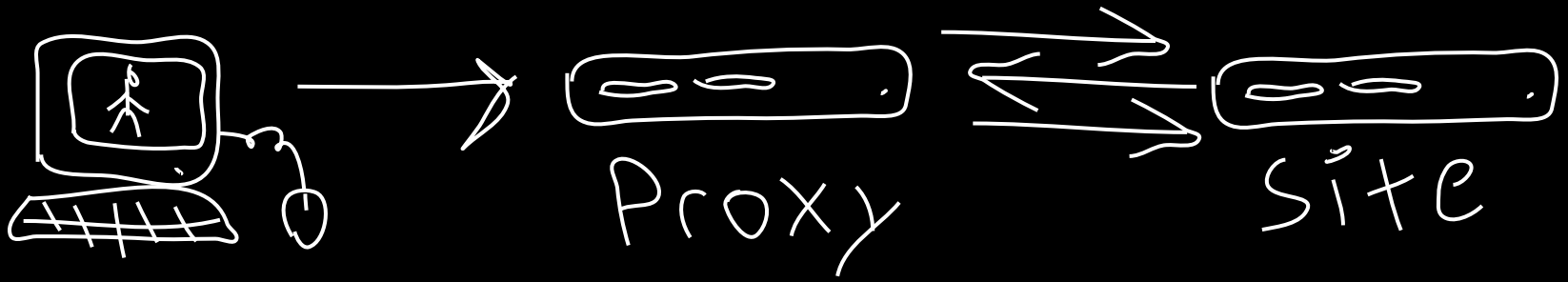
How Proxies Work - TCP



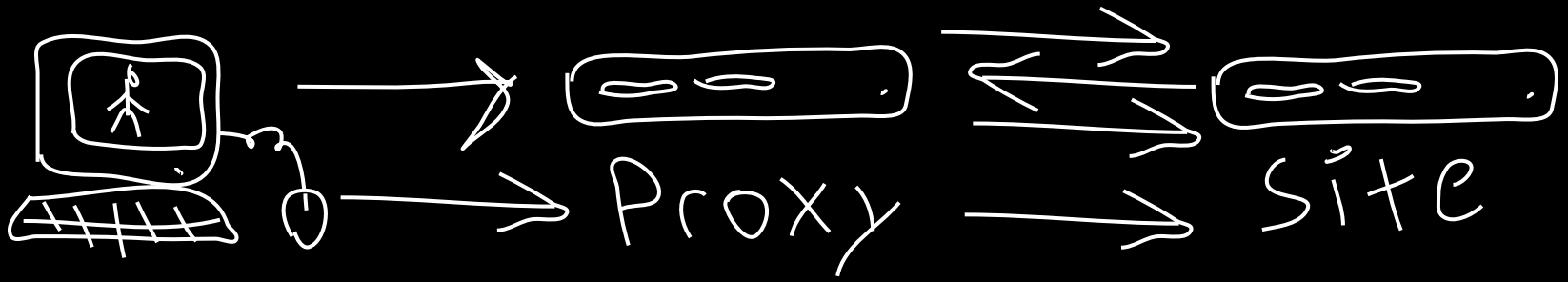
How Proxies Work - TCP



How Proxies Work - TCP



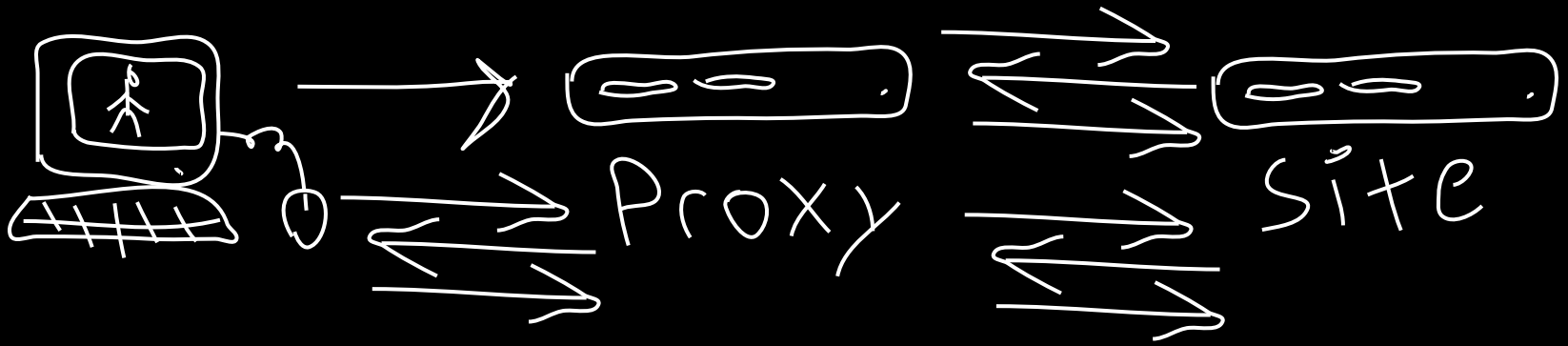
How Proxies Work - TCP



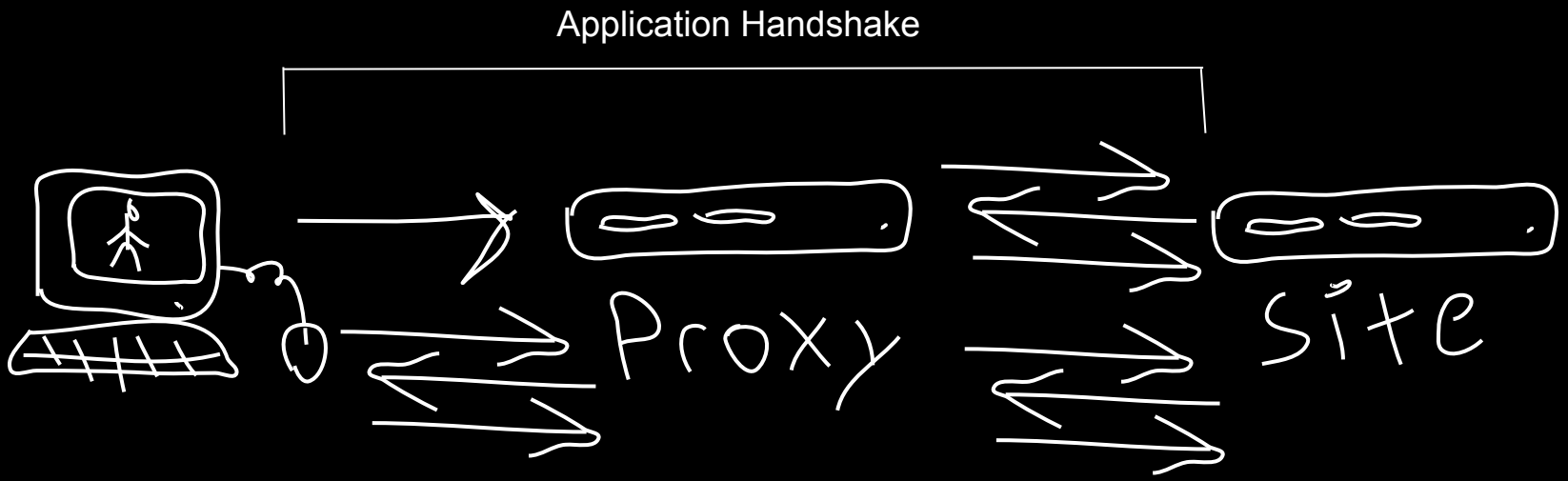
How Proxies Work - TCP



How Proxies Work - TCP



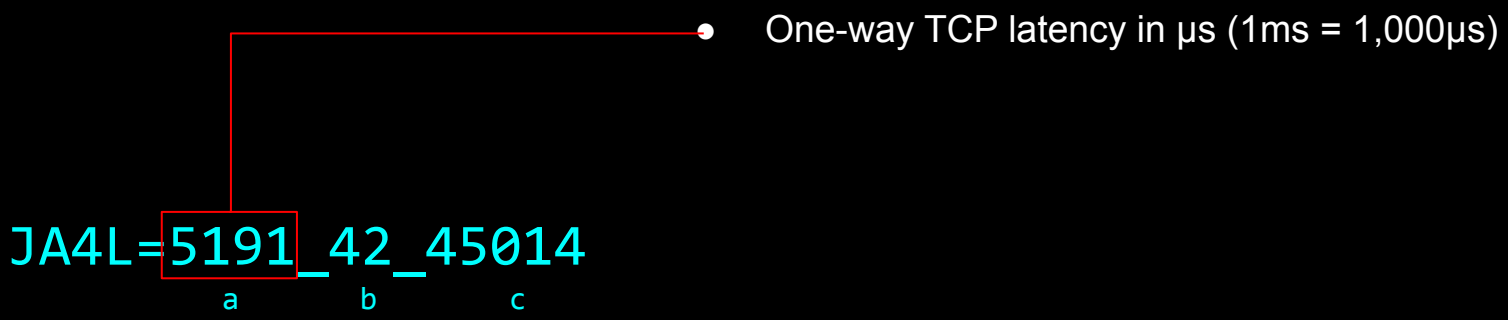
How Proxies Work - TCP



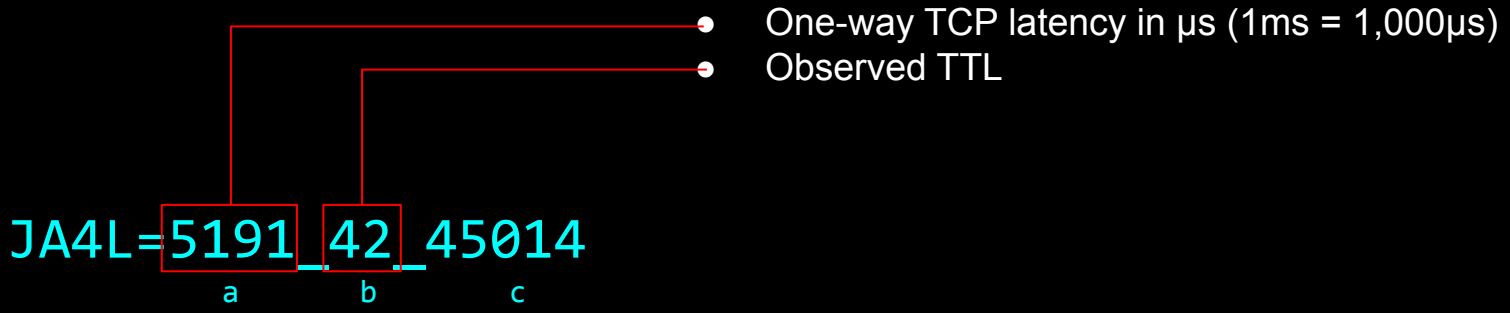
JA4L: Light Distance/Location Fingerprint

```
JA4L=5191_42_45014
     a    b     c
```

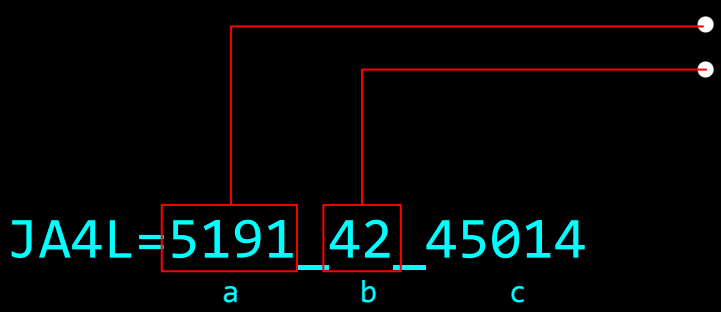
JA4L: Light Distance/Location Fingerprint



JA4L: Light Distance/Location Fingerprint



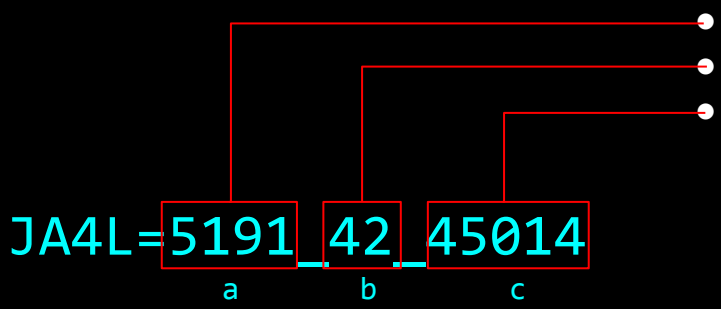
JA4L: Light Distance/Location Fingerprint



- One-way TCP latency in µs (1ms = 1,000µs)
- Observed TTL

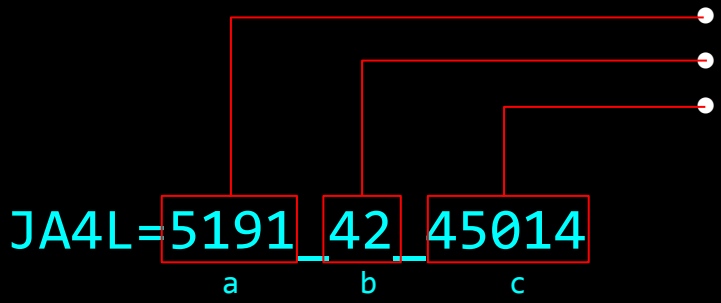
- Initial TTL 64 - Mac, Linux, Phones, IoT
- Initial TTL 128 - Windows
- Initial TTL 255 - Cisco, F5, Networking Devices
- Estimated Hop Count = Estimated Initial TTL - Observed TTL

JA4L: Light Distance/Location Fingerprint



- One-way TCP latency in µs (1ms = 1,000µs)
- Observed TTL
- One-way application handshake latency

JA4L: Light Distance/Location Fingerprint



- One-way TCP latency in µs (1ms = 1,000µs)
- Observed TTL
- One-way application handshake latency

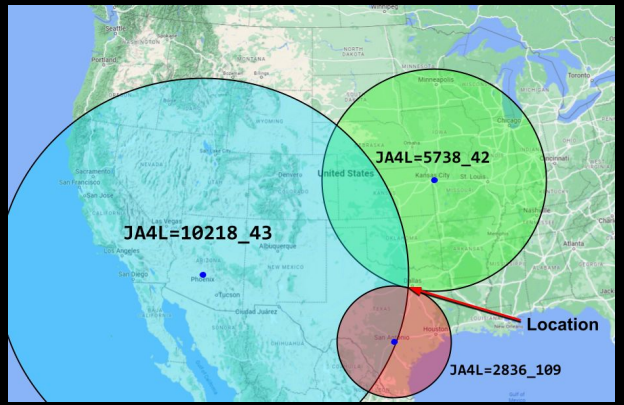
Physical distance between client and server can be measured using this formula (still in testing):
D = jc/p

j = JA4L_a
c = Speed of light per µs in fiber (0.128 miles/µs or 0.206km/µs)
p = Propagation delay factor

JA4L-C = 2449_42

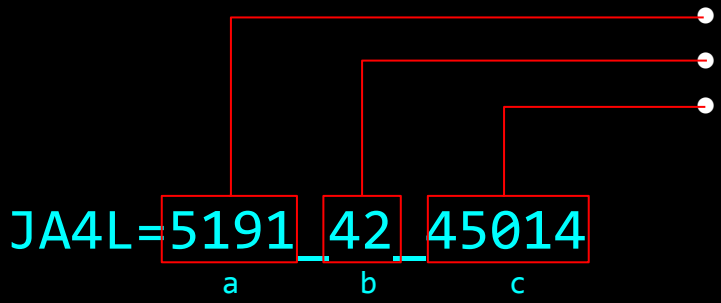
2449x0.128/1.6=195
The client is within 195 miles of the server having traversed 22 hops.
(actual distance was 194 miles)

Hop Count	Propagation Delay Factor
<=21	1.5
22	1.6
23	1.7
24	1.8
25	1.9
>=26	2.0



Patent Pending
FoxIO License 1.1

JA4L: Light Distance/Location Fingerprint



- One-way TCP latency in µs (1ms = 1,000µs)
- Observed TTL
- One-way application handshake latency

JA4L-Delta = JA4L_c / JA4L_a
(this is simplified, actual calculation requires tuning)

Most direct connections JA4L-Delta <= 1
Most proxied connections JA4L-Delta >= 2

Direct Connection

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36

Direct Connection

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36

Direct Connection

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36

JA4T: 65535_2-1-3-1-1-4_1460_8

Direct Connection

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36

JA4T: 65535_2-1-3-1-1-4_1460_8

OS / Device	**JA4T**
Windows 11	65535_2-1-3-1-1-4_1460_8

Direct Connection

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36

JA4T: 65535_2-1-3-1-1-4_1460_8

JA4L: 5241_114_4893

Direct Connection

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36

JA4T: 65535_2-1-3-1-1-4_1460_8

JA4L: 5241_114_4893

JA4L-Delta: 0.9

Proxy Detection

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36

Proxy Detection

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36

JA4T: 65535_2-4-8-1-3_1460_4

Proxy Detection

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36

JA4T: 65535_2-4-8-1-3_1460_4

OS / Device	**JA4T**
Windows 11	65535_2-1-3-1-1-4_1460_8
Android TV	65535_2-4-8-1-3_1460_4

Proxy Detection

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36

JA4T: 65535_2-4-8-1-3_1460_4

JA4L: 3242_45_15023

Proxy Detection

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36

JA4T: 65535_2-4-8-1-3_1460_4

JA4L: 3242_45_15023

JA4L-Delta: 4.6

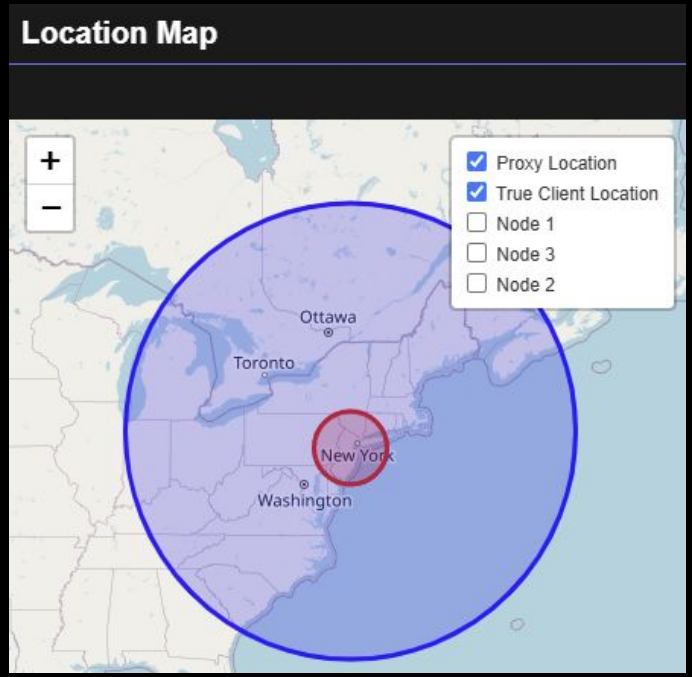
Proxy Detection

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36

JA4T: 65535_2-4-8-1-3_1460_4

JA4L: 3242_45_15023

JA4L-Delta: 4.6



Proxy Detection

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36

JA4T: 65535_2-4-8-1-3_1460_8

Proxy Detection

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36

JA4T: 65535_2-4-8-1-3_1460_8

OS / Device	**JA4T**
Windows 11	65535_2-1-3-1-1-4_1460_8
Ubuntu 22.04	65535_2-4-8-1-3_1460_8

Proxy Detection

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36

JA4T: 65535_2-4-8-1-3_1460_8

JA4L: 3242_45_15023

JA4L-Delta: 4.6

Proxy Detection

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36

JA4T: 65535_2-4-8-1-3_1460_8

JA4L: 3242_45_15023

JA4L-Delta: 4.6

IP: 190.97.231.245

IP-Enrichment: ZScaler

Proxy Detection

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36

JA4T: 65535_2-4-8-1-3_1460_8

JA4L: 3242_45_15023

JA4L-Delta: 4.6

IP: 190.97.231.245

IP-Enrichment: Residential Proxy PROXYJET

Residential Proxies

- Attacks, fraud, bots, scrapping, and other threats
  - Threat actors have moved almost entirely to using residential proxies
- No legitimate, normal users
  - They use commercial VPNs
  - Some, like NordVPN, attempted it but turned it off
- All of the non-legitimate traffic has moved into a single bucket
  - Initial detection starts here

Detecting Residential Proxies

- IP-based detection is meaningless
  - Real users
  - Individual session detection required
- Client-side JavaScript
  - This works - for websites with web clients
  - Does not work for API’s and applications
- Solution: Detect all residential proxied sessions at the protocol level

Identify Inbound bots, AI, hacking tools, zero day attacks, scrapers

Utilizing:

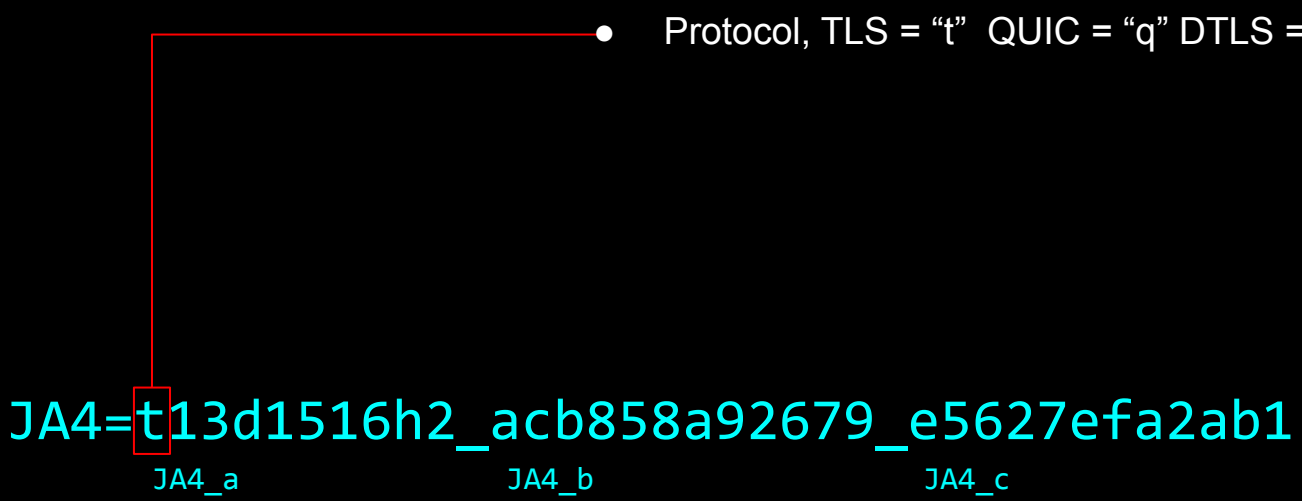
JA4 + JA4H

JA4: TLS Client Fingerprint

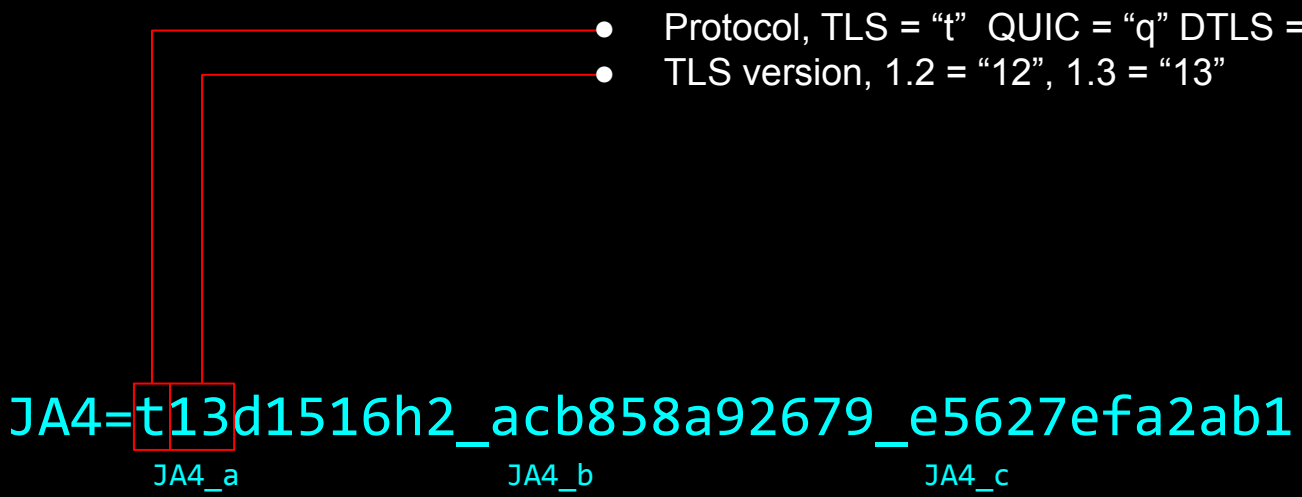
JA4=t13d1516h2_acb858a92679_e5627efa2ab1

JA4_a JA4_b JA4_c

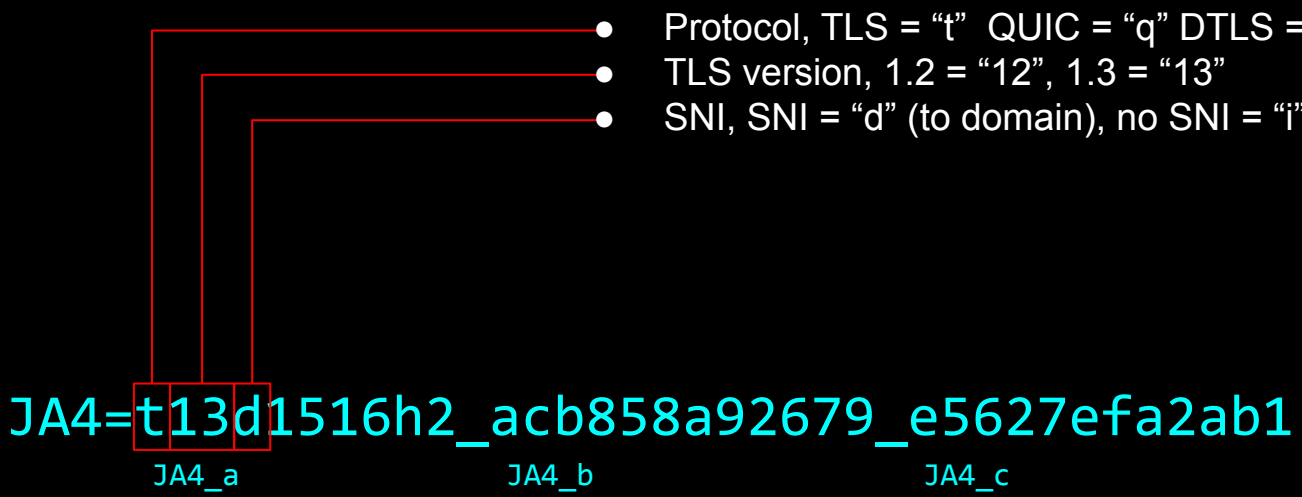
JA4: TLS Client Fingerprint



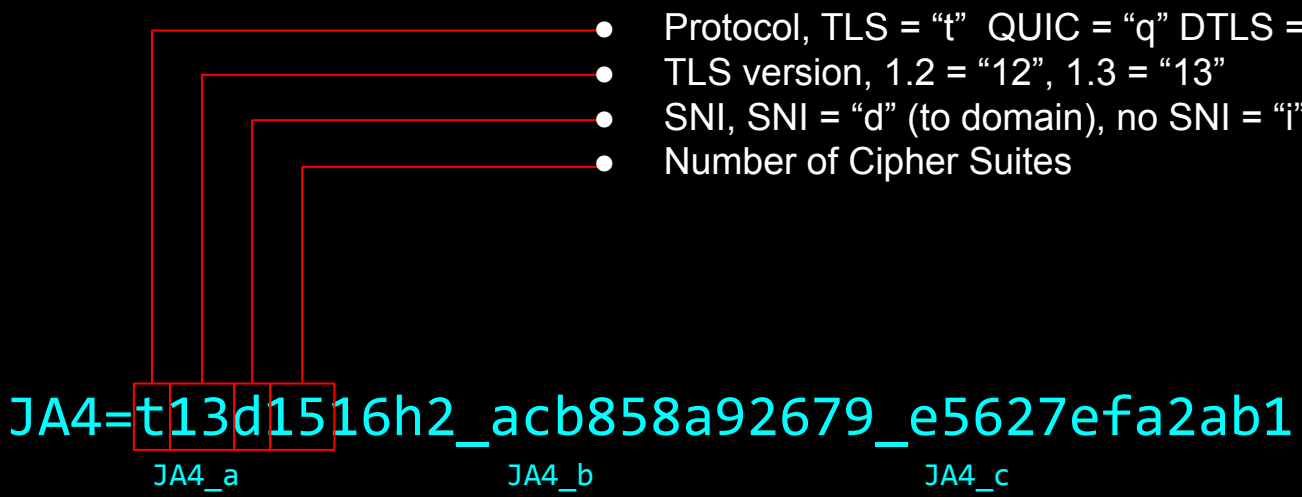
JA4: TLS Client Fingerprint



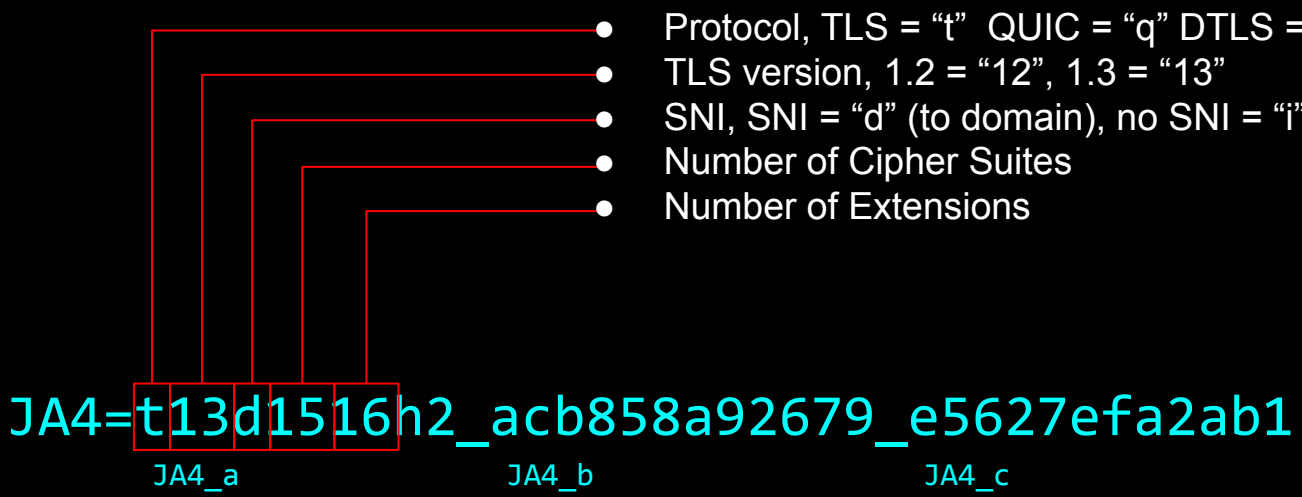
JA4: TLS Client Fingerprint



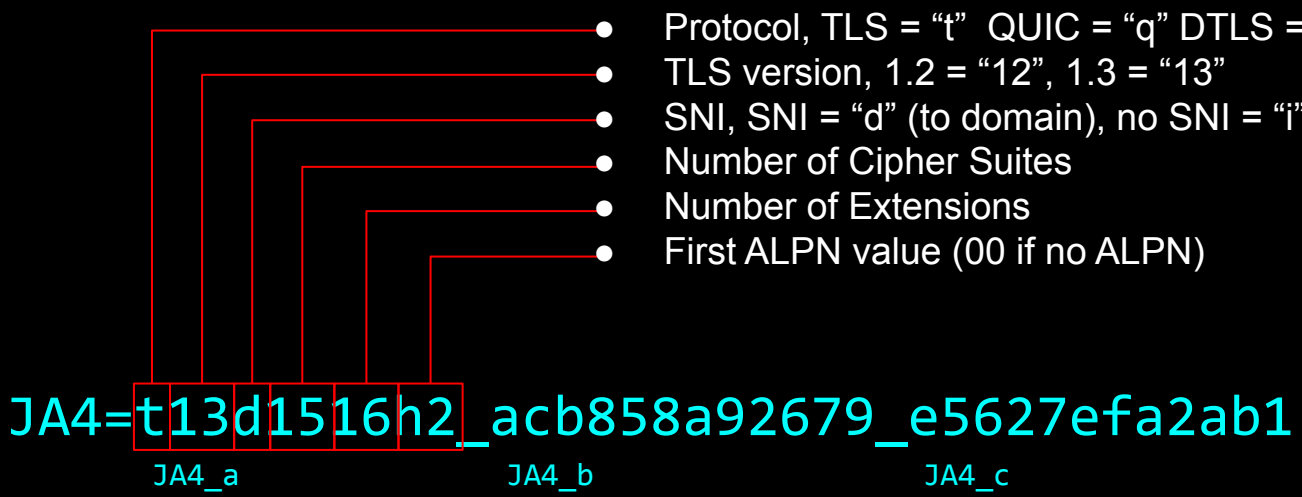
JA4: TLS Client Fingerprint



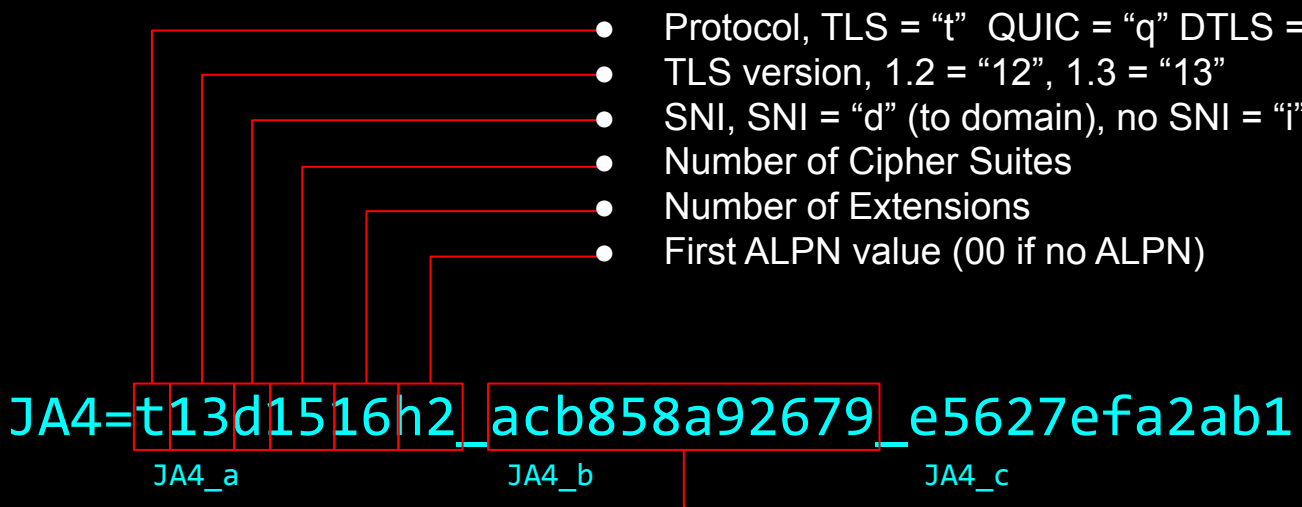
JA4: TLS Client Fingerprint



JA4: TLS Client Fingerprint

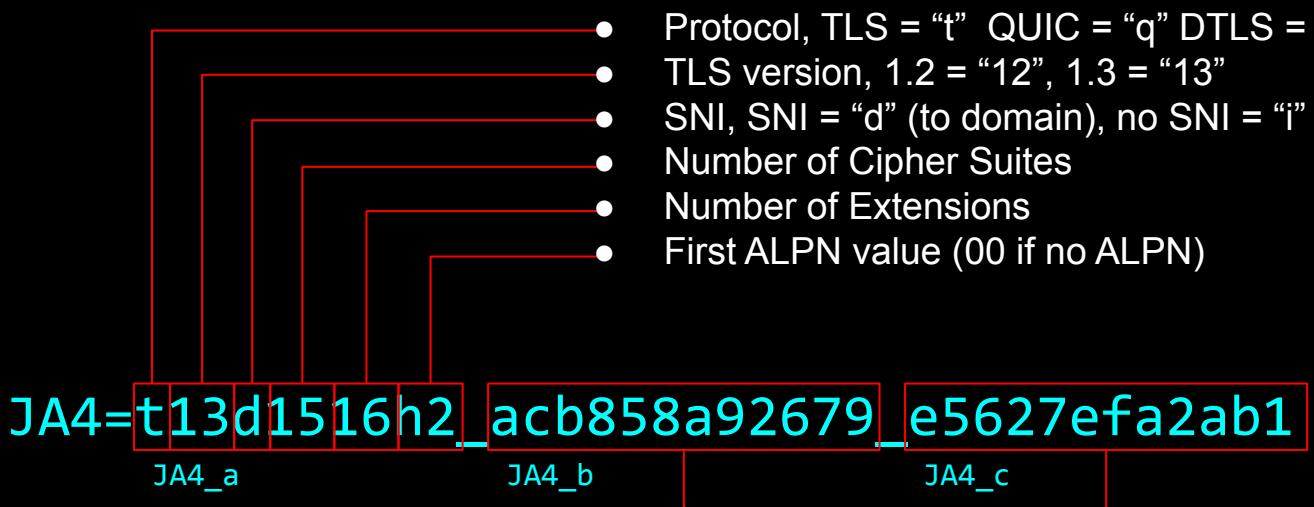


JA4: TLS Client Fingerprint



- Truncated SHA256 hash of the Cipher Suites, sorted

JA4: TLS Client Fingerprint



- Truncated SHA256 hash of the Cipher Suites, sorted
- Truncated SHA256 hash of the Extensions, sorted
  + Signature Algorithms, in the order they appear

AI Detection

User-Agent: Mozilla/5.0 AppleWebKit/537.36 (KHTML, like Gecko); compatible; ChatGPT-User/1.0; +https://openai.com/bot

JA4: t13d1712h2_5b57614c22b0_ef7df7f74e48

AI Detection

User-Agent: Mozilla/5.0 AppleWebKit/537.36 (KHTML, like Gecko); compatible; ChatGPT-User/1.0; +https://openai.com/bot

JA4: t13d1712h2_5b57614c22b0_ef7df7f74e48

AI Detection

User-Agent: Mozilla/5.0 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0; compatible; OAI-SearchBot/1.0; +https://openai.com/searchbot

JA4: t13d1712h2_5b57614c22b0_ef7df7f74e48

AI Detection

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36; compatible; OAI-SearchBot/1.0; +https://openai.com/searchbot

JA4: t13d1712h2_5b57614c22b0_ef7df7f74e48

AI Detection

User-Agent: Mozilla/5.0 AppleWebKit/537.36 (KHTML, like Gecko); compatible

JA4: t13d1712h2_5b57614c22b0_ef7df7f74e48

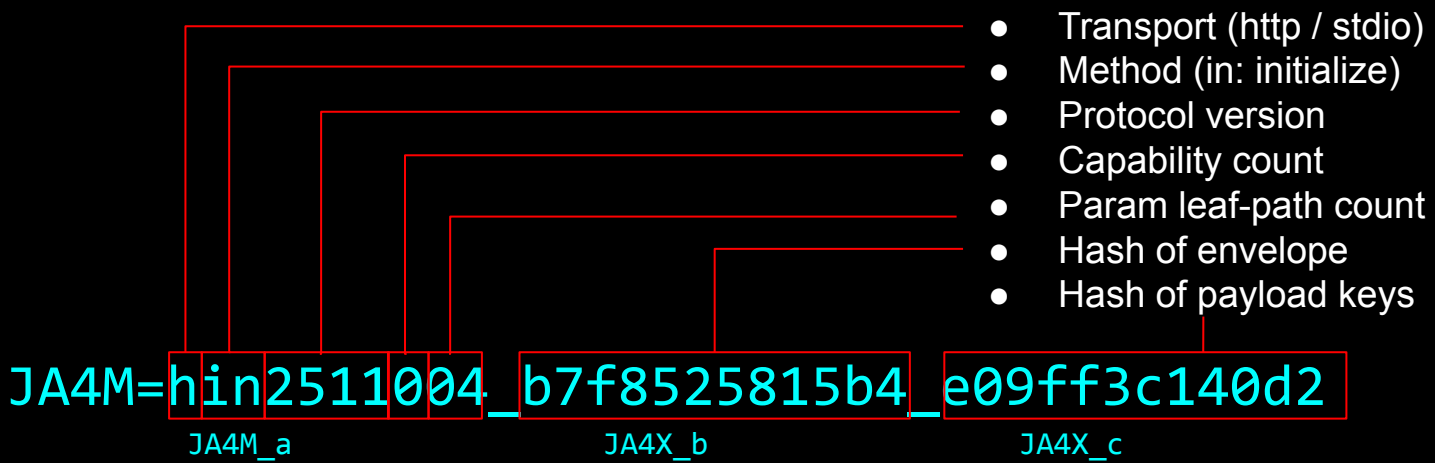
2025

Website / tool	UA	JA4T	JA4L	JA4	JA4H	IP	Anomaly
chat.chatgpt.com	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36	65535_2-4-8-1-3_1360_13	32839_56_36798	t13d2812h2_a01be8c064b6_ef4b9b248d72	ge20nn16enus_da9415befcf1_0000000000000_000000000000	2a09:bac5:1dac:1250::1d3:7c // AS13335 - Cloudflare, Inc.	Proxied + VPN
firecrawl.dev	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36	64240_2-4-8-1-3_1460_7	3468_50_4649	t13d1516h2_8daaf6152771_d8a2da3f94cd	ge20nn13enus_0e897bb088aa_000000000000_000000000000	195.64.119.122 // AS22773 - Cox Communications Inc. - Residential	Residential Proxied
firecrawl.dev	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36	64240_2-4-8-1-3_1460_7	3446_50_9894	t13d1516h2_8daaf6152771_d8a2da3f94cd	ge20nn13enus_0e897bb088aa_000000000000_000000000000	216.247.234.11 // AS22773 - Cox Communications Inc. - Residential	Residential Proxied
scrapegraph.ai	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36	65535_2-4-8-1-3_1440_6	44757_51_268208	t13d1812h1_85036bcba153_d41ae481755e	ge11nn08enus_1c3593bad54e_000000000000_000000000000	2603:8001:4c01:a08e:495c:801e:79cb:cbeb // AS20001 - Charter Communications Inc - Residential	Residential Proxied
scrapegraph.ai	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36	65535_2-4-8-1-3_1460_10	32137_47_114697	t13d1516h2_8daaf6152771_d8a2da3f94cd	ge20nn13enus_0c2c1d640f3e_000000000000_000000000000	208.70.11.66 // AS43641 - SOLLUTIUM EU Sp z.o.o. - Hosting	Residential Proxied
kimi.com	Mozilla/5.0 (X11; Ubuntu; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.5414.145 Safari/537.36	59220_2-4-8-1-3_1460_7	120798_52_157117	t13d1516h2_8daaf6152771_02713d6af862	ge20nn090000_3fc2d4f2629d_0000000000000_000000000000	47.79.250.133 // AS45102 - Alibaba (US) Technology Co., Ltd. - Hosting	Browser spoofing
kimi.com	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36 SLBrowser/9.0.5.9101 SLBChan/111 SLBVPV/64-bit	64240_2-4-8-1-3_1360_7	115307_46_157771	t13d1516h2_8daaf6152771_02713d6af862	ge20nn14zhcn_c2507efc711e_0000000000000_000000000000	148.253.49.54 // AS54994 - Meteverse Limited. - Hosting	Proxied + VPN
grok.com	Mozilla/5.0 (iPhone; CPU iPhone OS 18_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.0 Mobile/15E148 Safari/604.1	64240_2-4-8-1-3_1460_7	3440_51_12098	t13d2013h2_a09f3c656075_93f65c6c1207	ge20nn08enus_1945e0741196_000000000000_000000000000	185.230.122.165 // AS7029 - Windstream Communications LLC - Residential	Residential Proxied
grok.com	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0 Safari/537.36	64240_2-4-8-1-3_1460_7	8592_50_15757	t13d1515h2_8daaf6152771_cc38aef784ae	ge20nn13enus_0c2c1d640f3e_000000000000_000000000000	159.148.62.218 // AS210906 - UAB "Bite Lietuva" - Residential	Residential Proxied
grok.com	Mozilla/5.0 (iPhone; CPU iPhone OS 18_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.0 Mobile/15E148 Safari/604.1	64240_2-4-8-1-3_1460_7	17904_48_39793	t13d2013h2_a09f3c656075_93f65c6c1207	ge20nn08enus_1945e0741196_000000000000_000000000000	92.71.125.254 // AS212238 - Datacamp Limited - Residential	Residential Proxied
grok.com	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0 Safari/537.36	65535_2-1-3-4-8_1460_12	11584_46_88058	t13d1515h2_8daaf6152771_cc38aef784ae	ge20nn13enus_0c2c1d640f3e_000000000000_000000000000	208.190.13.92 // AS7018 - AT&T Enterprises, LLC - Residential	Residential Proxied
grok.com	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0 Safari/537.36	65535_2-4-8-1-3_1460_8	8901_51_19563	t13d1515h2_8daaf6152771_cc38aef784ae	ge20nn13enus_0c2c1d640f3e_000000000000_000000000000	73.165.83.138 // AS7922 - Comcast Cable Communications, LLC -Residential	Residential Proxied

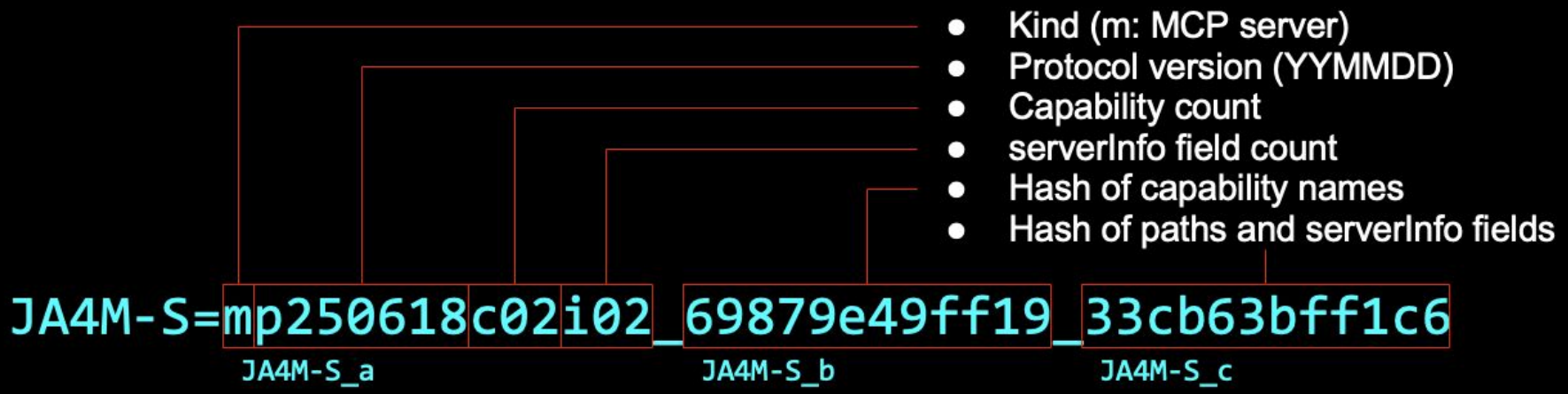
FOXIO

Client (version)	JA4	JA4H	Declared User-Agent	Bucket
Claude Code 2.1.312	t13d1713h1_5b57614c22b0_7f527383e249	po11nn090000_095b1aa3232e	claude-code/2.1.312 (sdk-cli)	A
Codex CLI 0.165.0	t13d1011h2_61a7ad8aa9b6_0d308c48d2a3	po20nn040000_8b845447523e	codex-mcp-client/0.165.0	B
OpenCode 1.19.5	t13d1713h1_5b57614c22b0_7f527383e249	po11nn070000_3b40135eb3e6	opencode/1.19.5	C
OpenClaw 2026.10.9	t13d5212h1_b262b3658495_8e6e362c5eac	po11nn09enus_a70274d887ee	undici	D
Hermes Agent 0.22.5	t13d1712h1_ab0a1bf427ad_8e6e362c5eac	he11nn050000_e161b8ad0830	python-httpx2/2.12.0	E
Kimi Code 2.4.1	t13d5212h1_b262b3658495_8e6e362c5eac	po11nn09enus_8537c0154ff6	node	F
Gemini CLI 0.66.0	t13d5212h1_b262b3658495_8e6e362c5eac	po11nn09enus_8537c0154ff6	node	F
Cline 3.0.74	t13d1713h1_5b57614c22b0_6a3d802a7139	po11nn070000_3b40135eb3e6	Bun/1.4.2	G
pi 1.4.0	t13d5212h1_b262b3658495_8e6e362c5eac	po11nn09enus_a70274d887ee	undici	D
DeepSeek Harness 0.2.1-rc.3	t13d5212h1_b262b3658495_8e6e362c5eac	po11nn11enus_dab96355d7f4	node	H
ARTEX v0.4.0-4-g7f8c7cb	t13d1312h2_f57a46bbacb6_ab7e3b40a677	po20nn060000_00558244f8fb	Go-http-client/2.0	I
TypeScript SDK 1.32.2	t13d5212h1_b262b3658495_8e6e362c5eac	po11nn09enus_8537c0154ff6	node	F
Python SDK 1.30.0	t13d1713h1_ab0a1bf427ad_ecd0401ec68b	po11nn070000_87ff41af6287	python-httpx/0.28.1	J
Go SDK 1.6.1	t13d131100_f57a46bbacb6_ab7e3b40a677	po11nn060000_ed383ed8462e	Go-http-client/1.1	K
C# SDK 1.4.1	t13d121100_a538d02d76d5_f6eeaf393d2e	po11nn040000_7c0b1ea88ba6	absent	L
Java SDK 0.14.1	t13d311200_1d947a95fc68_7e1102d2036b	po11nn070000_250377d58c28	Java-http-client/21.0.13	M
Rust SDK (rmcp) 0.16.0	t13d1011h1_61a7ad8aa9b6_0d308c48d2a3	po11nn040000_37e0f4d4b668	absent	N

JA4M

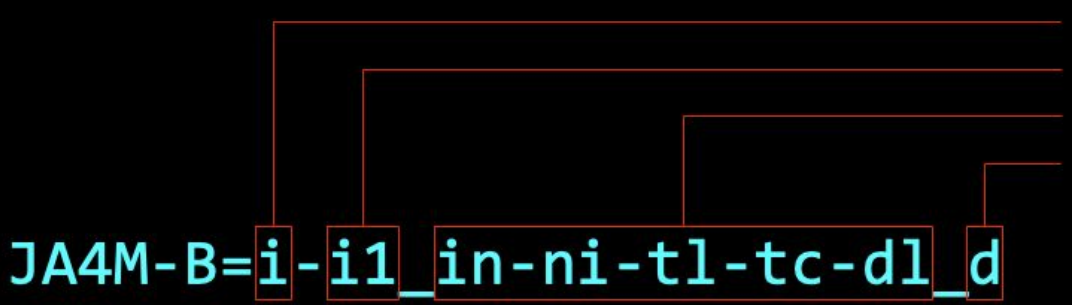

Transport (http / stdio)
Method (in: initialize)
Protocol version
Capability count
Param leaf-path count
Hash of envelope
Hash of payload keys
JA4M=hin2511004_b7f8525815b4_e09ff3c140d2
JA4M_a
JA4X_b
JA4X_c

JA4MS


Kind (m: MCP server)
Protocol version (YYMMDD)
Capability count
serverInfo field count
Hash of capability names
Hash of paths and serverInfo fields
JA4M-S=mp250618c02i02_69879e49ff19_33cb63bff1c6
JA4M-S_a
JA4M-S_b
JA4M-S_c

FOXIO

JA4MB



- Opening move (i: initialize)
- Id scheme (i1: integers from 1)
- Flow: every method, in order
- Teardown (d: DELETE)

FOXIO

Stateful vs stateless MCP

Client	Mode	First request JA4M-C	tools/list JA4M-C	JA4M-B
Python mcp 2.3.0	stateful (2025-11-25)	hin2511004_12f16ae4b4b4_e09ff3c140d2	htl0000000_5d04335a4a9f_000000000000	i-i1_in-ni-gt-tl-tc-dl_d
Python mcp 2.3.0	stateless, probes first	hsd2607004_12f16ae4b4b4_917940d39a27	htl2607004_12f16ae4b4b4_917940d39a27	d-i1_sd-tl-tc_n
Python mcp 2.3.0	stateless, no probe	htl2607004_12f16ae4b4b4_917940d39a27	htl2607004_12f16ae4b4b4_917940d39a27	s-i1_tl-tc_n
TS client 2.3.1	stateful (2025-11-25)	hin2511004_b7f8525815b4_e09ff3c140d2	htl0000000_c71d7e181fba_000000000000	i-i0_in-ni-gt-tl-tc_n
TS client 2.3.1	stateless, probes first	hsd2607004_12f16ae4b4b4_917940d39a27	htl2607004_5cff010dc9e8_917940d39a27	d-sX_sd-tl-tc_n
Go go-sdk 1.8.0	stateful (2025-11-25)	hin2511104_12f16ae4b4b4_1b92a8085db9	htl0000000_5d04335a4a9f_000000000000	i-i1_in-gt-ni-tl-tc-dl_d
Go go-sdk 1.8.0	stateless, probes first	hsd2607104_12f16ae4b4b4_37c49ff40b8f	htl2607104_12f16ae4b4b4_37c49ff40b8f	d-i1_sd-tl-tc_n
Claude Code 2.1.312	stateless, probes first	hsd2607209_12f16ae4b4b4_6e5b0758e07d	htl2607209_5cff010dc9e8_6e5b0758e07d	d-sX_sd-sl-tl-sd-sl_n

FOXIO

AI agents: MCP library and JA4M

Agent	MCP library (from source)	JA4M	JA4MB
Claude Code 2.1.312	TS official (bundled)	hsd2607209_12f16ae4b4b4_6e5b0758e07d	d-sX_sd-in-ni-gt-tl-sd-in-ni-gt-tl-tc_n
Codex CLI 0.165.0	Rust rmcp (bundled)	hin2506106_12f16ae4b4b4_680ecf23efc8	i-i0_in-ni-gt-tl-dl_d
OpenCode 1.19.5	TS official (bundled)	hin2511104_b7f8525815b4_929a57a0d43e	i-i0_in-ni-gt-tl-tc-nc_n
OpenClaw 2026.10.9	TS official 1.32.0	hin2511004_b7f8525815b4_e09ff3c140d2	i-i0_in-ni-gt-tl-dl_d
Hermes Agent 0.22.5	Python mcp 2.3.0	hin2511206_12f16ae4b4b4_02a506e749b5	h-i1_hd-gt-in-gt-ni-tl-dl-hd-gt-in-gt-ni-tl-dl_d
Kimi Code 2.4.1	TS official (bundled, 2025-11-25 generation)	hin2511004_b7f8525815b4_e09ff3c140d2	i-i0_in-in-ni-ni-gt-tl-gt-tl-tc-nc_n
Gemini CLI 0.66.0	TS official 1.27.1 (bundled)	hin2506104_b7f8525815b4_ed3e6dfece11	i-i0_in-ni-gt-tl_n
Cline 3.0.74	TS official 1.32.2	hin2511004_b7f8525815b4_e09ff3c140d2	i-i0_in-ni-gt-tl_n
pi 1.4.0	pi-mcp 1.4.0 (own client, no SDK)	hin2511104_12f16ae4b4b4_929a57a0d43e	i-i1_in-ni-gt-tl-dl-in-ni-gt-tl-tc-dl_d
DeepSeek Harness 0.2.1-rc.3	TS v2 client 2.2.0	hsd2607004_12f16ae4b4b4_917940d39a27	d-sX_sd-in-ni-gt-tl-tc_n
ARTEX v0.4.0-4-g7f8c7cb	Go ARTEX mcphttp @7f8c7cb (no SDK)	hin2506004_12f16ae4b4b4_447ecc75d11f	i-i1_in-ni-tl-tc-dl_d

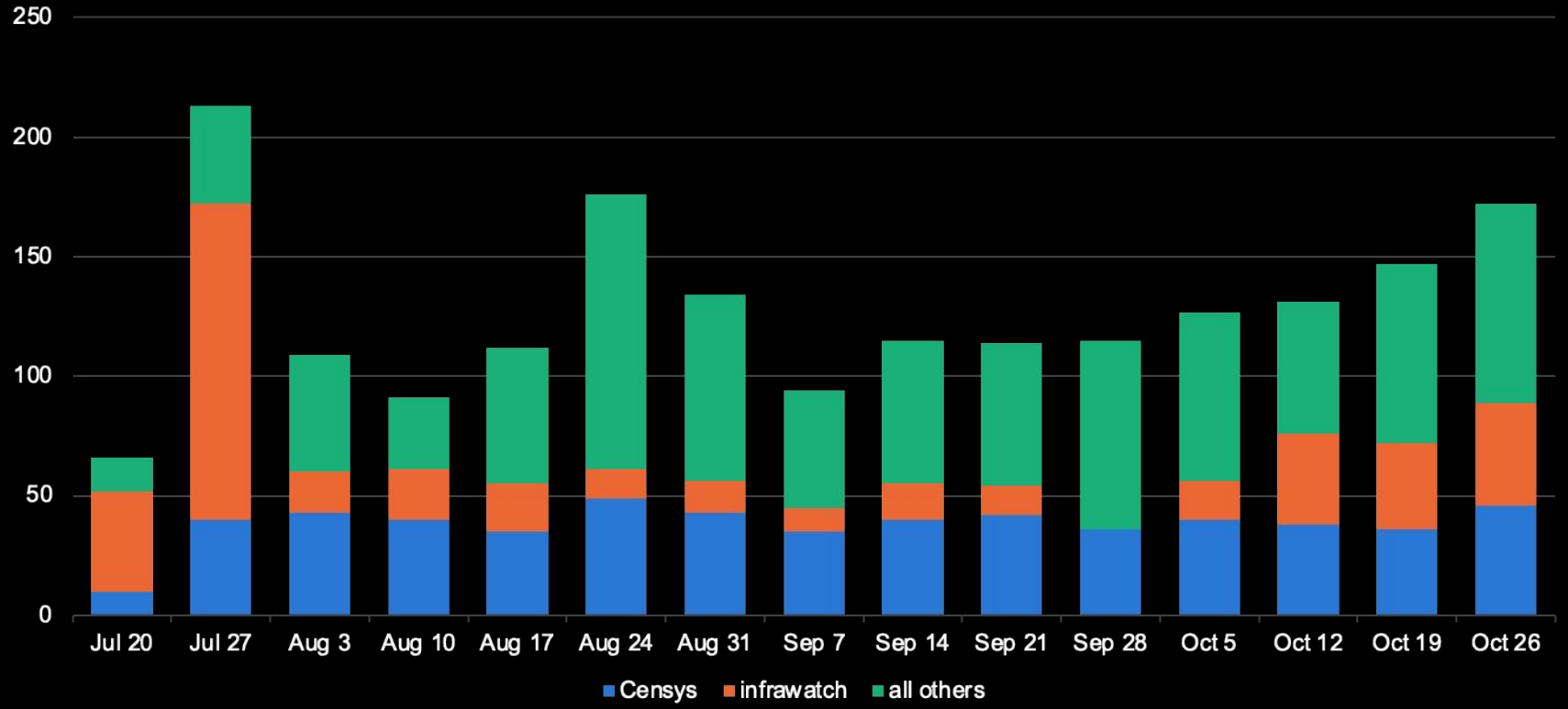
FOXIO

Official SDKs

SDK	Envelope order (b)	Ids	JA4M	JA4M
TS official 1.32.2	method,params,jsonrpc,id	i0	hin2511004_b7f8525815b4_e09ff3c140d2	i-i0_in-ni-gt-tl_n
Python mcp 1.30.0	method,params,jsonrpc,id	i0	hin2511004_b7f8525815b4_e09ff3c140d2	i-i0_in-gt-ni-tl-dl_d
Go go-sdk 1.6.1	jsonrpc,id,method,params	i1	hin2511104_12f16ae4b4b4_1b92a8085db9	i-i1_in-gt-ni-tl-dl_d
.NET official 1.4.1	method,params,id,jsonrpc	i1	hin2511004_cc8229be3b76_e09ff3c140d2	i-i1_in-gt-ni-tl-dl_d
Java official 0.14.1	jsonrpc,method,id,params	u8	hin2506004_b79ad83d5495_e09ff3c140d2	i-u8_in-gt-ni-tl-dl_d
Rust rmcp 0.16.0	jsonrpc,id,method,params	i0	hin2503004_12f16ae4b4b4_447ecc75d11f	i-i0_in-ni-gt-tl-dl_d

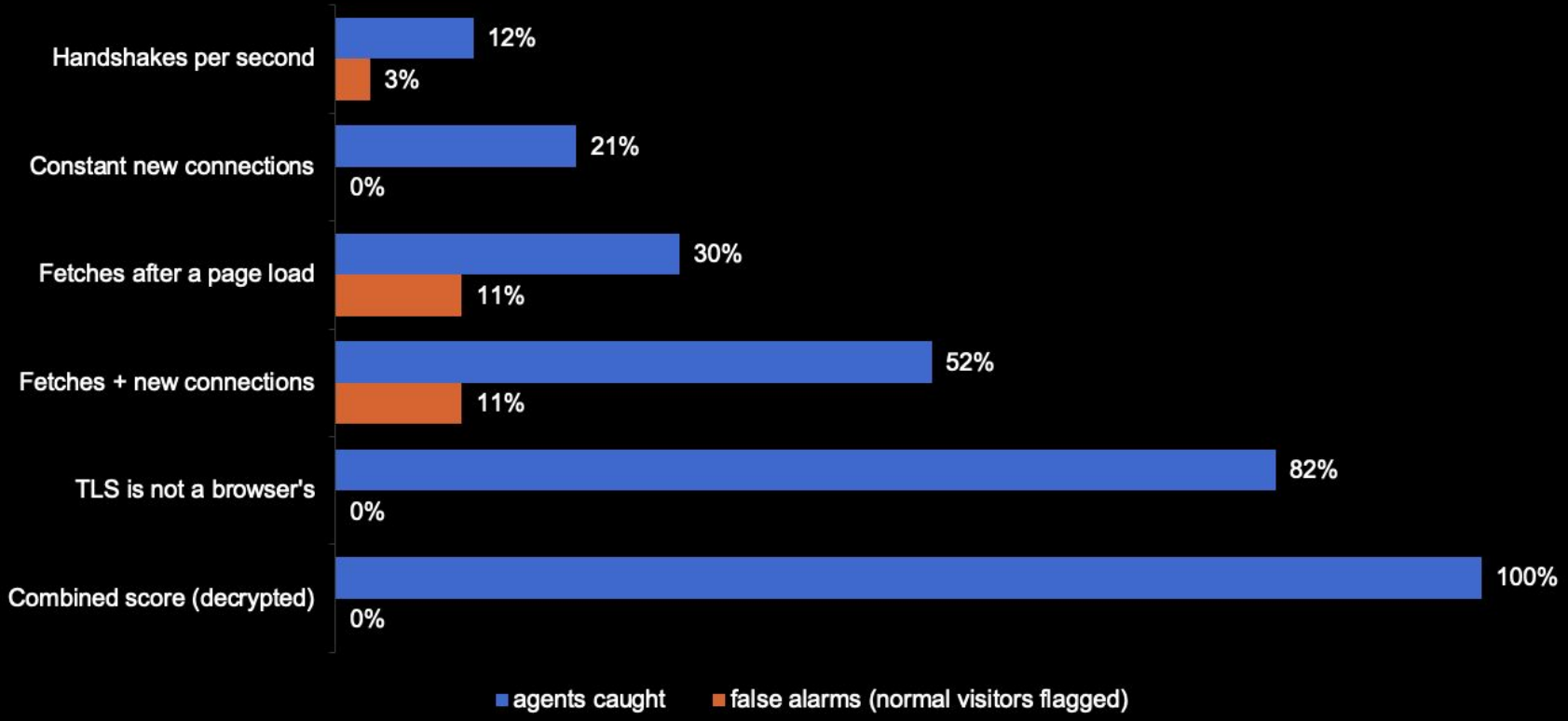
FOXIO

MCP sessions per week, by declared scanner



FOXIO

Incoming traffic



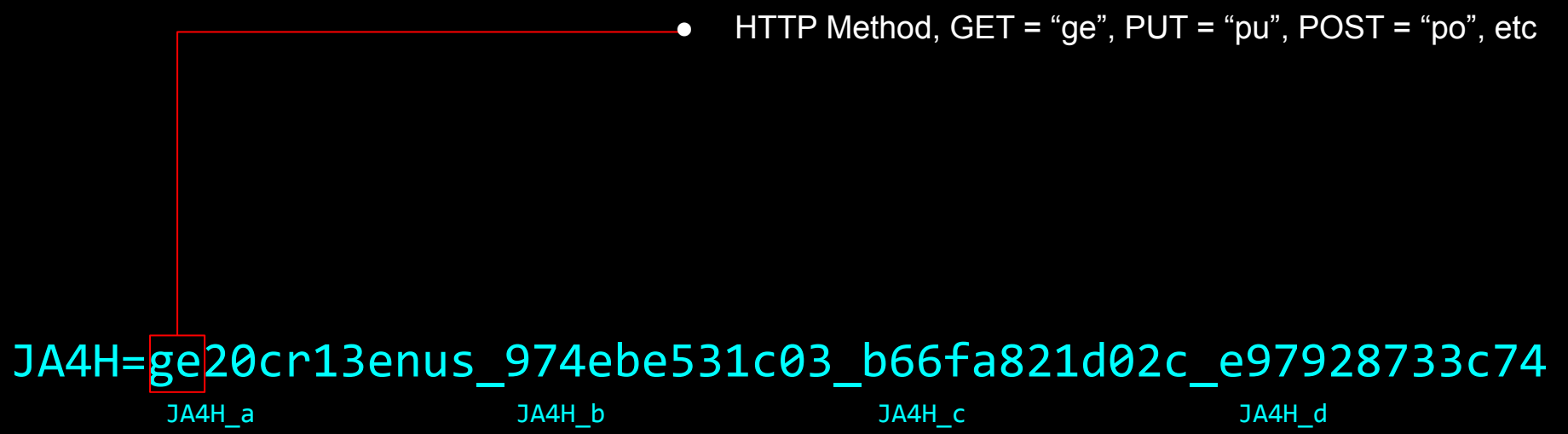
Exploit Tool Detection

JA4H: HTTP Client Fingerprint

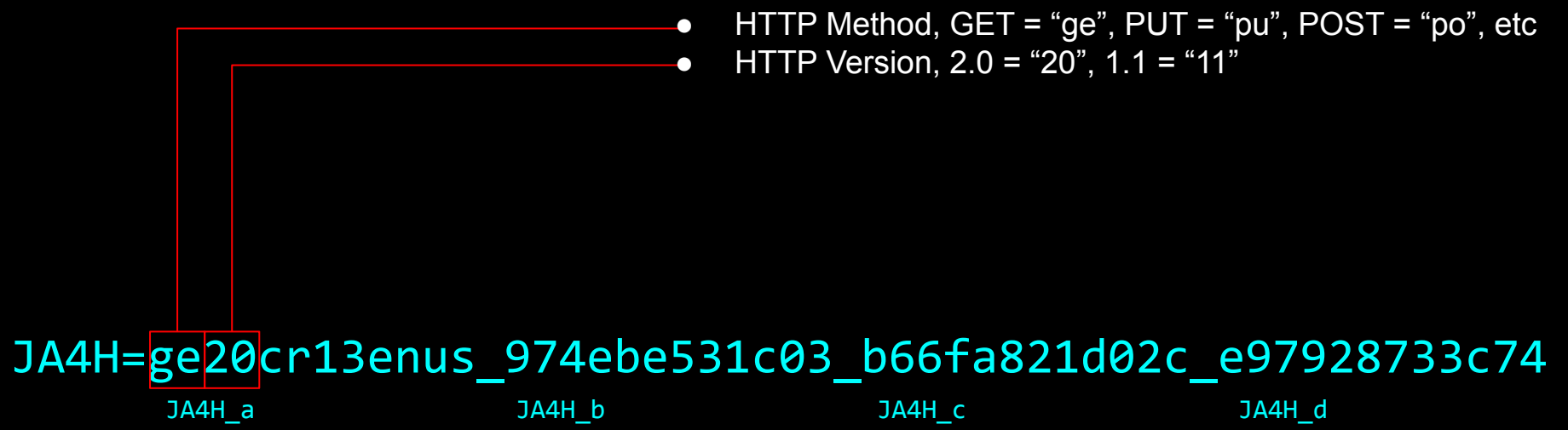
JA4H=ge20cr13enus_974ebe531c03_b66fa821d02c_e97928733c74

JA4H_a JA4H_b JA4H_c JA4H_d

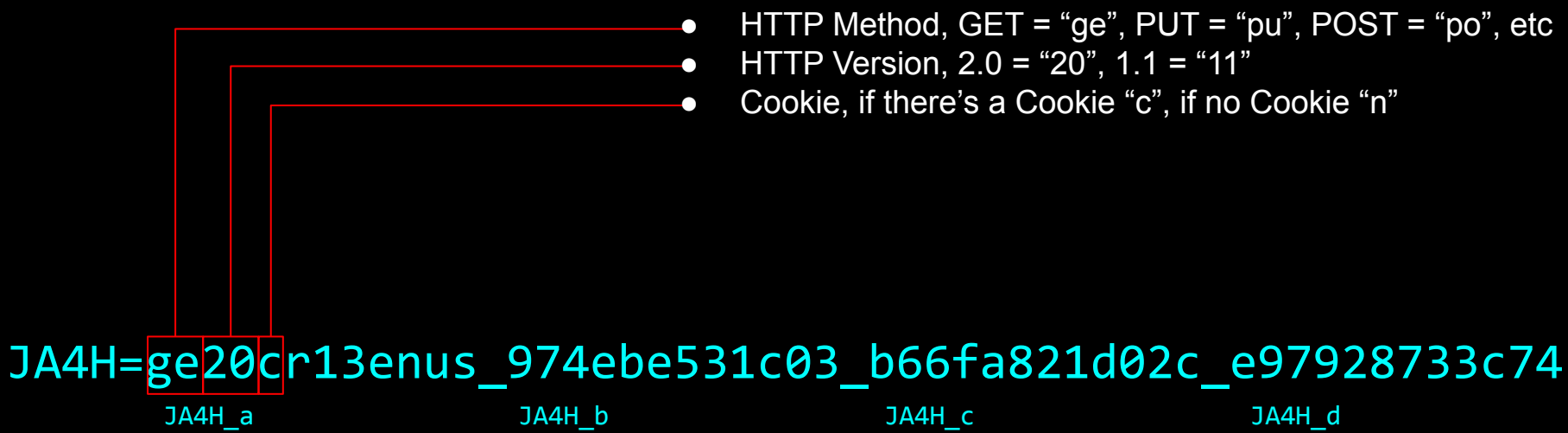
JA4H: HTTP Client Fingerprint



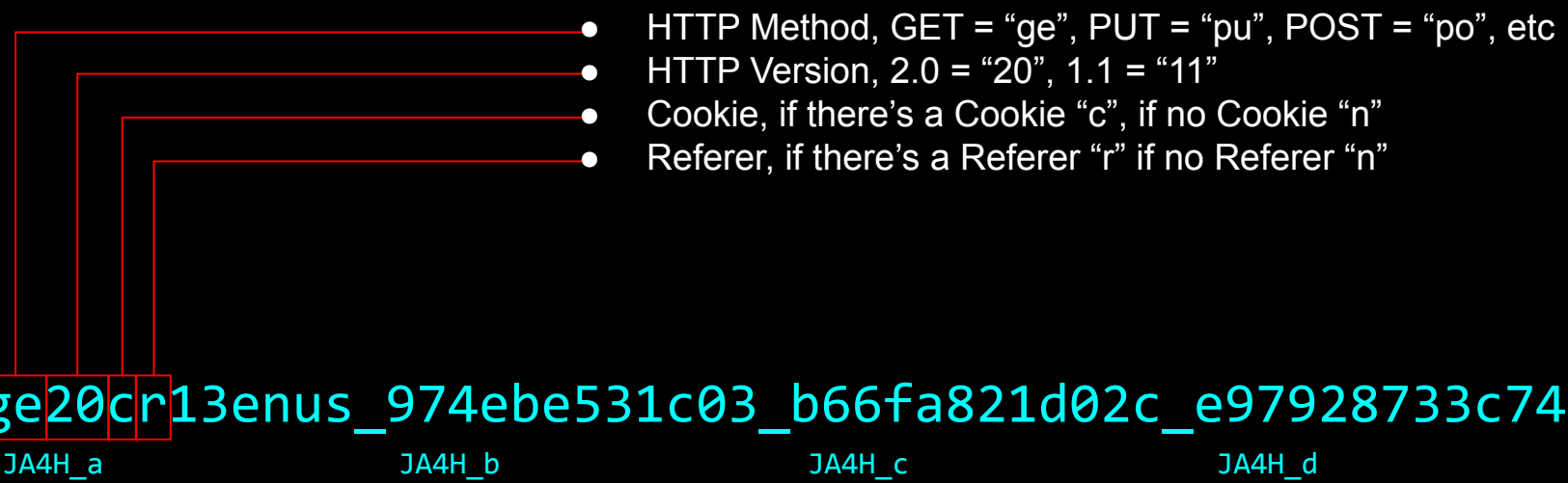
JA4H: HTTP Client Fingerprint



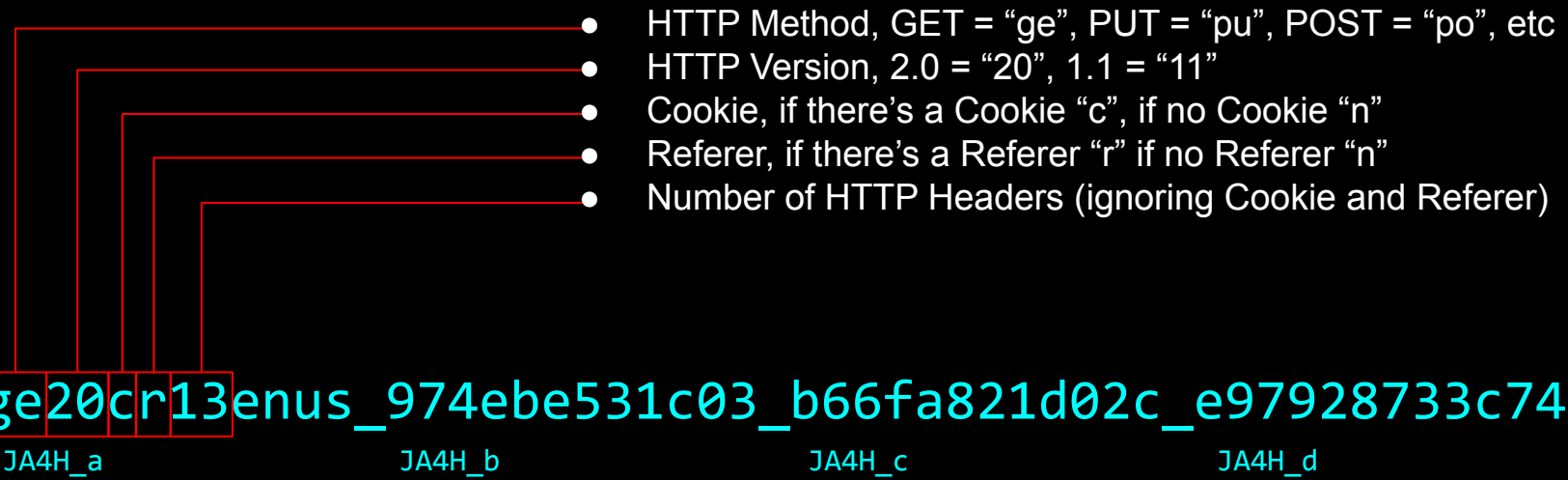
JA4H: HTTP Client Fingerprint



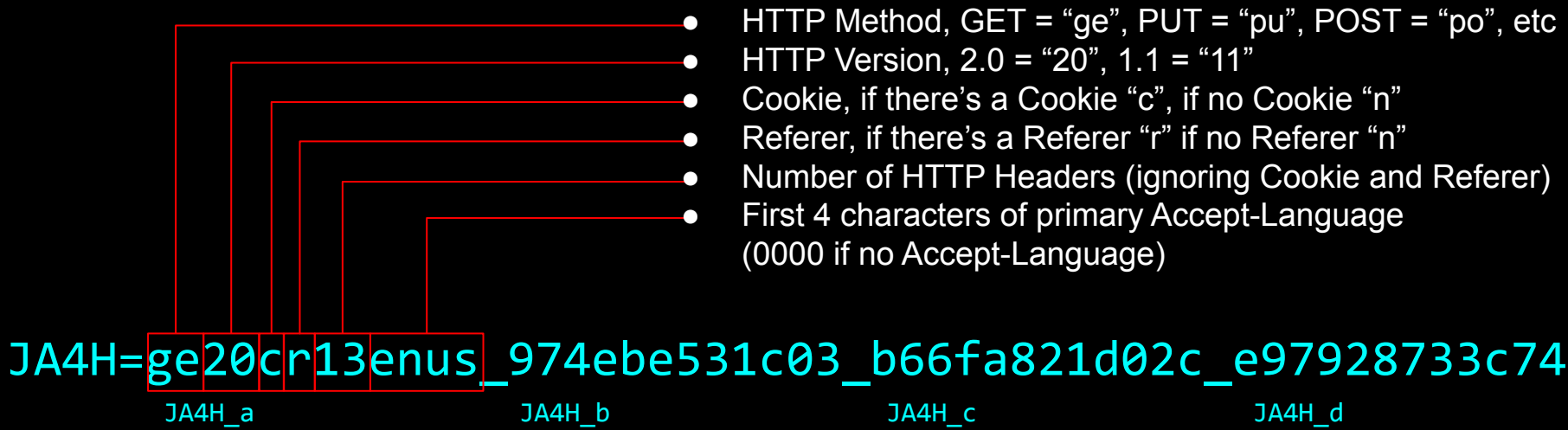
JA4H: HTTP Client Fingerprint



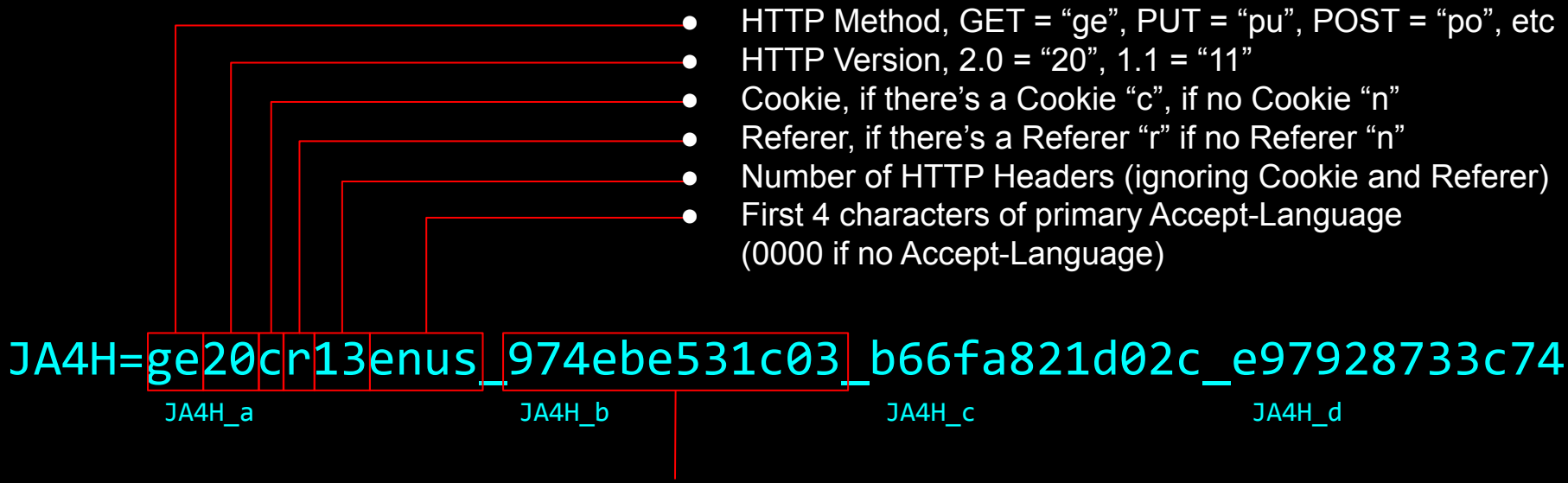
JA4H: HTTP Client Fingerprint



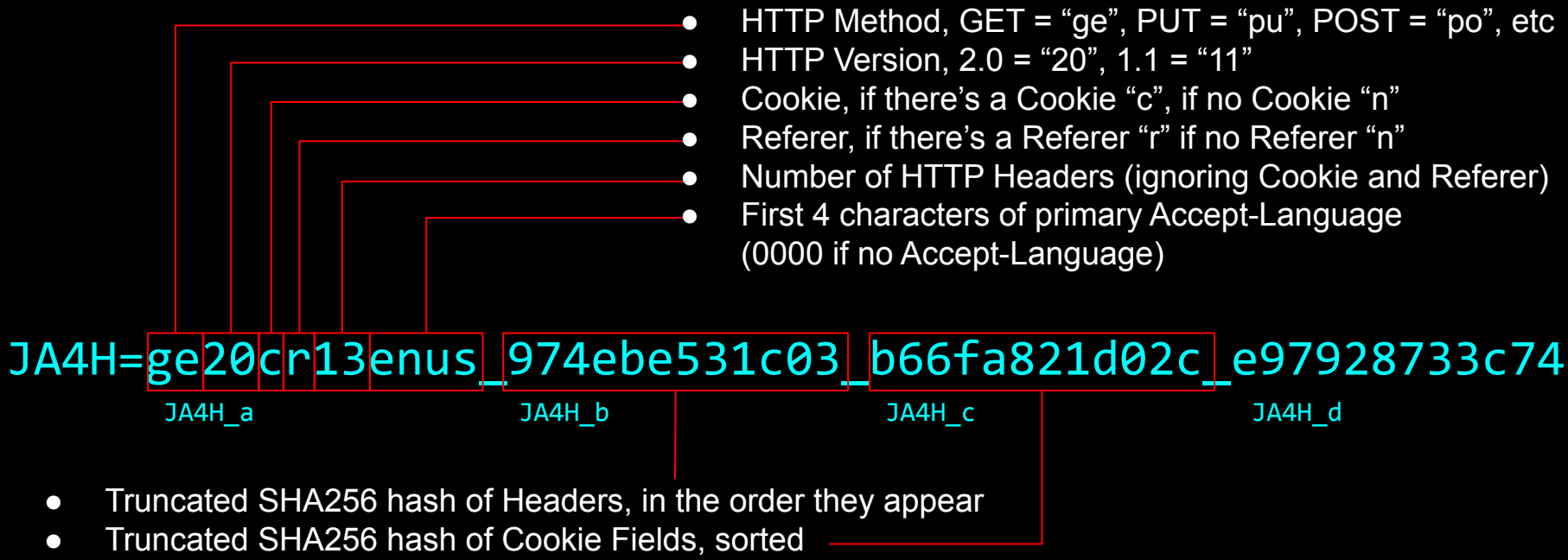
JA4H: HTTP Client Fingerprint



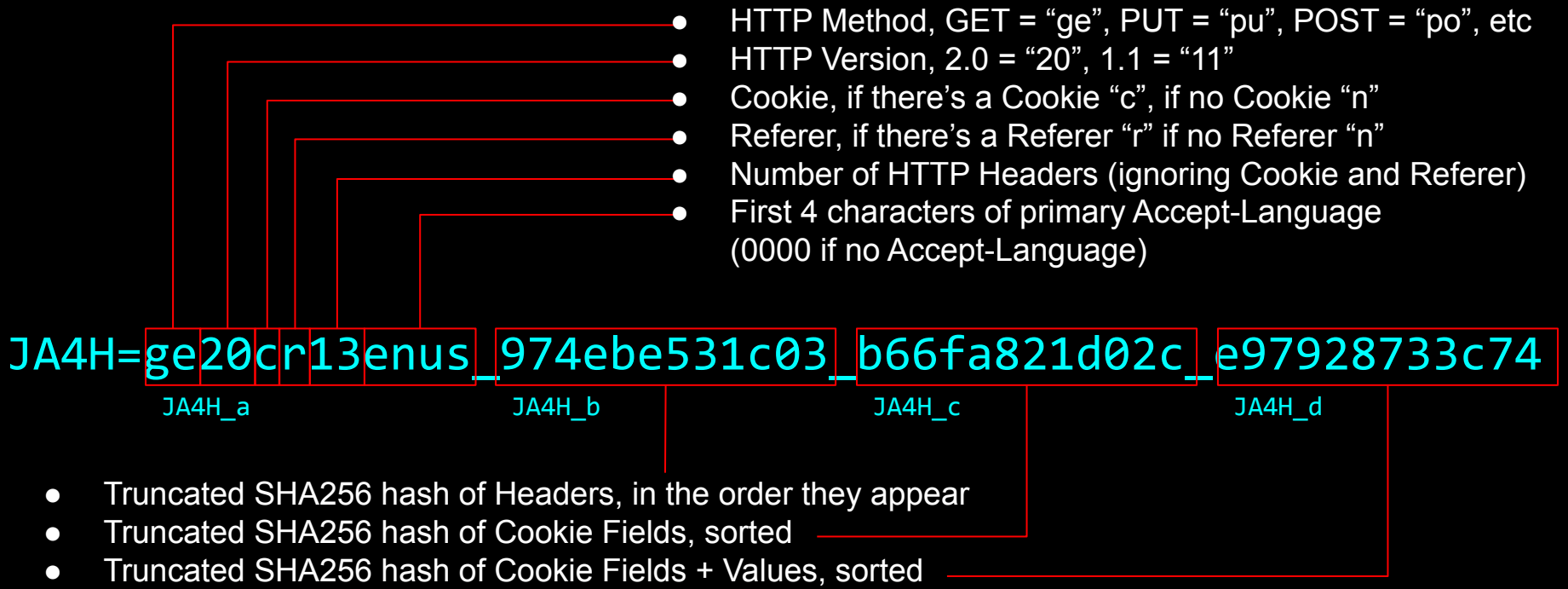
JA4H: HTTP Client Fingerprint



JA4H: HTTP Client Fingerprint



JA4H: HTTP Client Fingerprint



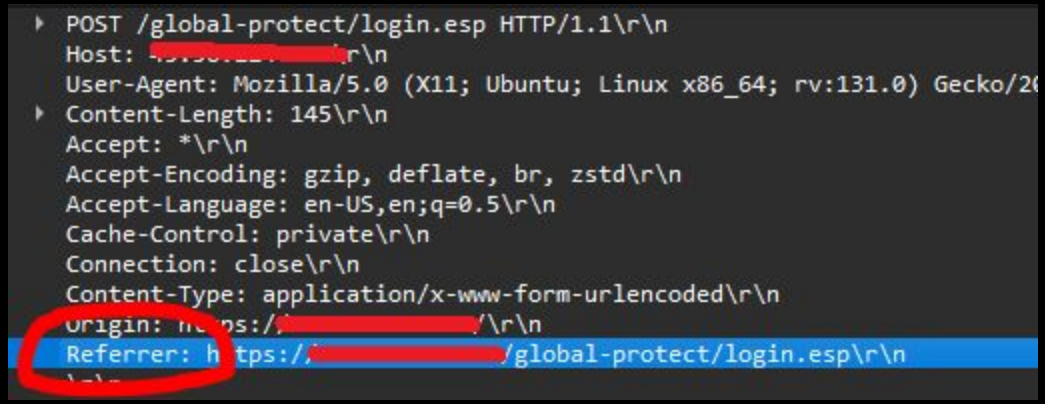
JA4H: HTTP Client Fingerprint

Application	Application Fingerprint		Website Cookie Fingerprint	User Cookie Fingerprint
	JA4H_a	JA4H_b	JA4H_c	JA4H_d
Chrome	ge20cr13enus	974ebe531c03	b66fa821d02c (cnn.com)	e97928733c74 (me)
	JA4H = ge20cr13enus_974ebe531c03_b66fa821d02c_e97928733c74			
IcedID Malware Dropper	ge11cn020000	9ed1ff1f7b03	cd8dafe26982	a51681cc67b
	JA4H_abc = ge11cn020000_9ed1ff1f7b03_cd8dafe26982			
Cobalt Strike	ge11cn060000	4e59edc1297a	4da5efaf0cbd	77ba3814cca4
	JA4H_ab = ge11cn060000_4e59edc1297a			
Lumma Malware	po11nn050000	d253db9d024b	000000000000	000000000000
	JA4H_ab = po11nn050000_d253db9d024b			
Tesla Browser	po11nr12enus	d60c2691a131	000000000000	000000000000
	JA4H_ab = po11nr12enus_d60c2691a131			

Exploit Tool Detection

Application	Application Fingerprint		Website Cookie Fingerprint	User Cookie Fingerprint
	JA4H_a	JA4H_b	JA4H_c	JA4H_d
Sharepoint ITW Exploit 1	po11nr060000	4ea4093e6290	000000000000	000000000000
	JA4H = po11nr060000_4ea4093e6290_000000000000_000000000000			
Sharepoint / General Exploit	po11nr070000	fbfc4db16e6f	000000000000	000000000000
	JA4H = po11nr070000_fbfc4db16e6f_000000000000_000000000000			
Sharepoint ITW Exploit 3	po11nr050000	a9e6c43a0296	000000000000	000000000000
	JA4H = po11nr050000_a9e6c43a0296_000000000000_000000000000			
Exploit SOHO Routers 1	ge11cr06enus	cc6ec9a91856	f381814948c2	2b5d474829c7
	JA4H = ge11cr06enus_cc6ec9a91856_f381814948c2_2b5d474829c7			
Exploit SOHO Routers 2	ge11cr08enus	9ad22a44e1f2	f381814948c2	2b5d474829c7
	JA4H = ge11cr08enus_9ad22a44e1f2_f381814948c2_2b5d474829c7			

Exploit Tool Detection



Bot Detection

Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)

JA4T: 28400_2-1-1-4-1-3_1420_7

JA4L: 23567_48_135958

JA4L-Delta: 5.7

JA4: t12d2408h2_d83cc789557e_7af1ed941c26

JA4H: ge11nr05zhcn_57b25be6c550_000000000000_000000000000

Evilginx Detection

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/146.0.0.0 Safari/537.36

JA4T: 65535_2-4-8-1-3_1460_8

JA4L: 3242_45_3150

JA4L-Delta: 1

Evilginx Detection

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/146.0.0.0 Safari/537.36

JA4T: 65535_2-4-8-1-3_1460_8

JA4L: 3242_45_3150

JA4L-Delta: 1

JA4: t13d141000_cbb2034c60b8_e7c285222651

Evilginx Detection

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/146.0.0.0 Safari/537.36

JA4T: 65535_2-4-8-1-3_1460_8

JA4L: 3242_45_3150

JA4L-Delta: 1

JA4: t13d141000_cbb2034c60b8_e7c285222651

Evilginx Detection

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/146.0.0.0 Safari/537.36

JA4T: 65535_2-4-8-1-3_1460_8

JA4L: 3242_45_3150

JA4L-Delta: 1

JA4: t13d141000_cbb2034c60b8_e7c285222651

Client	JA4
Chrome 146	t13d1516h2_8daaf6152771_d8a2da3f94cd
GoLang	t13d141000_cbb2034c60b8_e7c285222651

Evilginx Pro Detection

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/146.0.0.0 Safari/537.36

JA4T: 65535_2-4-8-1-3_1460_8

JA4L: 3242_45_3150

JA4L-Delta: 1

JA4: t13d1516h2_8daaf6152771_d8a2da3f94cd

Client	JA4
Chrome 146	t13d1516h2_8daaf6152771_d8a2da3f94cd
GoLang	t13d141000_cbb2034c60b8_e7c285222651

Evilginx Pro Detection

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/146.0.0.0 Safari/537.36

JA4T: 65535_2-4-8-1-3_1460_8

JA4L: 3242_45_3150

JA4L-Delta: 1

JA4: t13d1516h2_8daaf6152771_d8a2da3f94cd

JA4H: po11cr16enus_027ad1d778b0_2c99c2a1aa3f_a2498229bd76

Evilginx Pro Detection

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/146.0.0.0 Safari/537.36

JA4T: 65535_2-4-8-1-3_1460_8

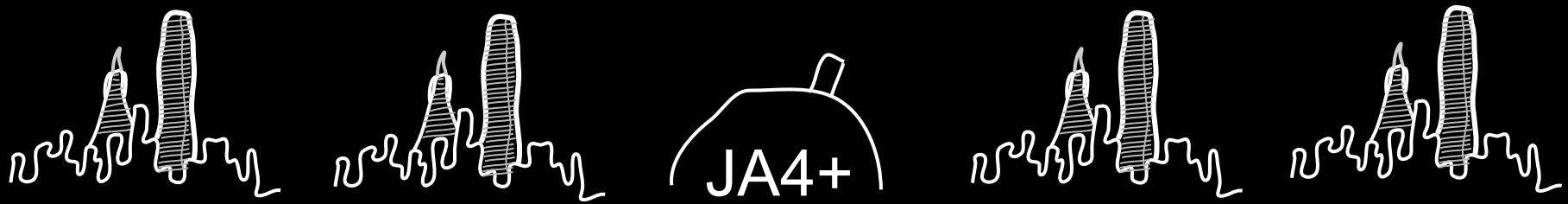
JA4L: 3242_45_3150

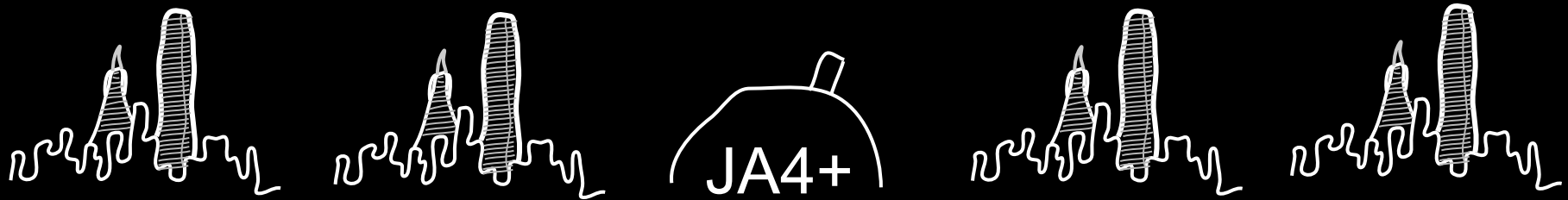
JA4L-Delta: 1

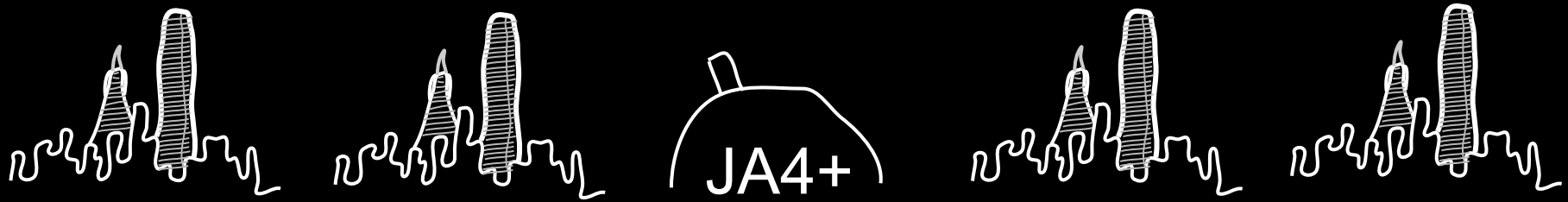
JA4: t13d1516h2_8daaf6152771_d8a2da3f94cd

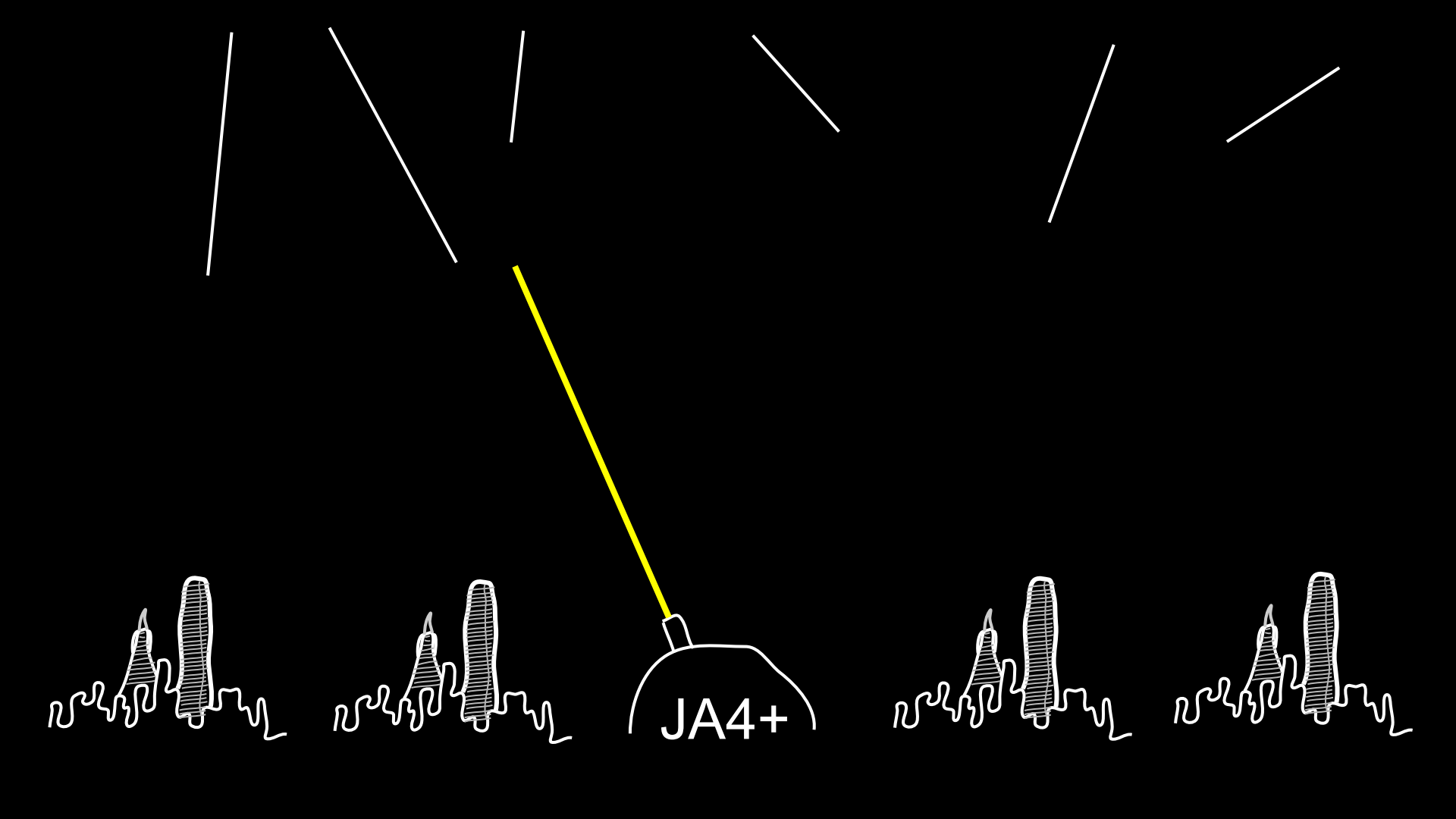
JA4H: po11cr16enus_027ad1d778b0_2c99c2a1aa3f_a2498229bd76

Client	JA4H
Chrome 146	po20cr15enus_604dc888f32f_b141f7cb72ca_0d76301874ba
Evilginx	po11cr16enus_027ad1d778b0_2c99c2a1aa3f_a2498229bd76

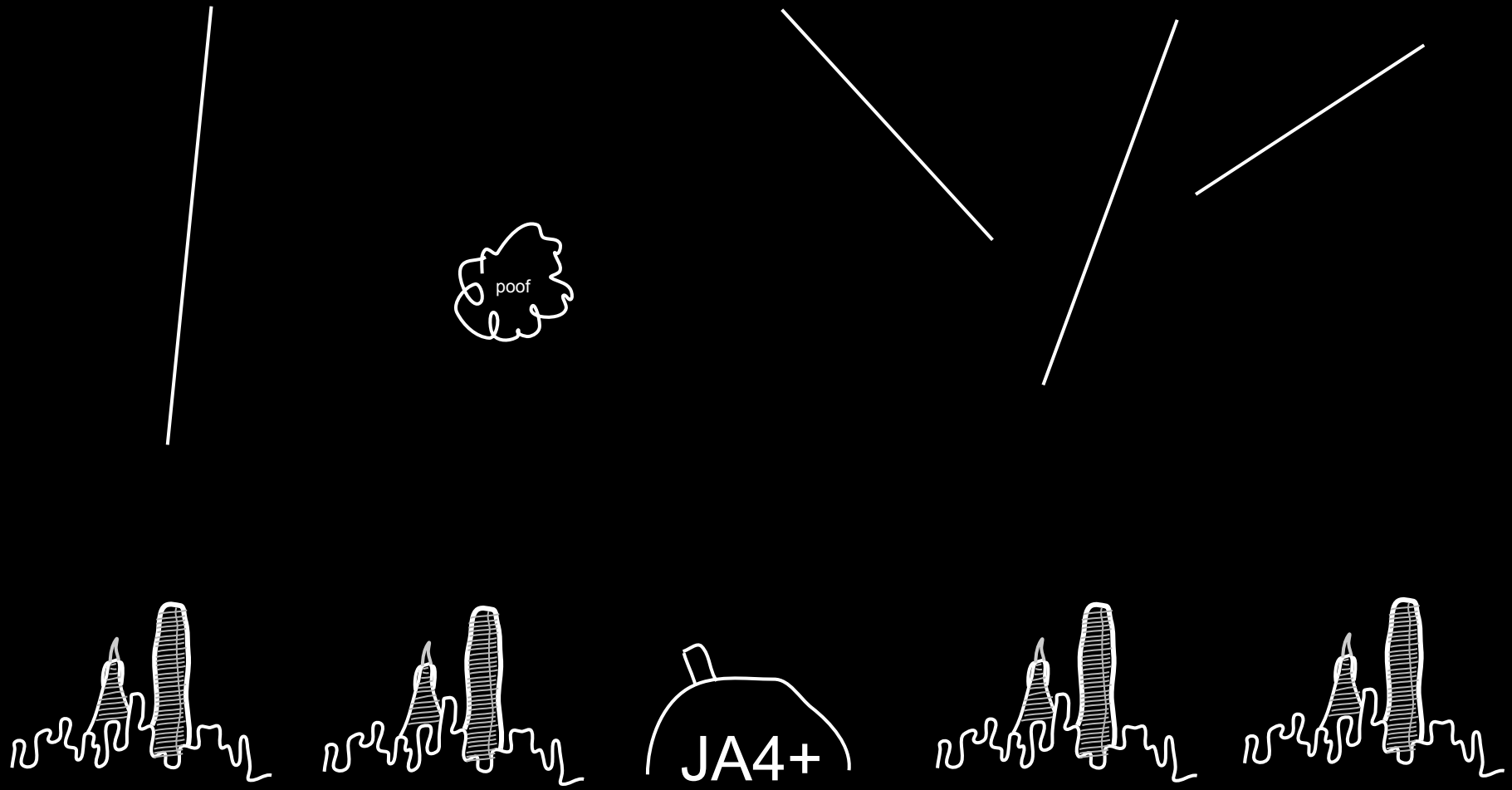

JA4+

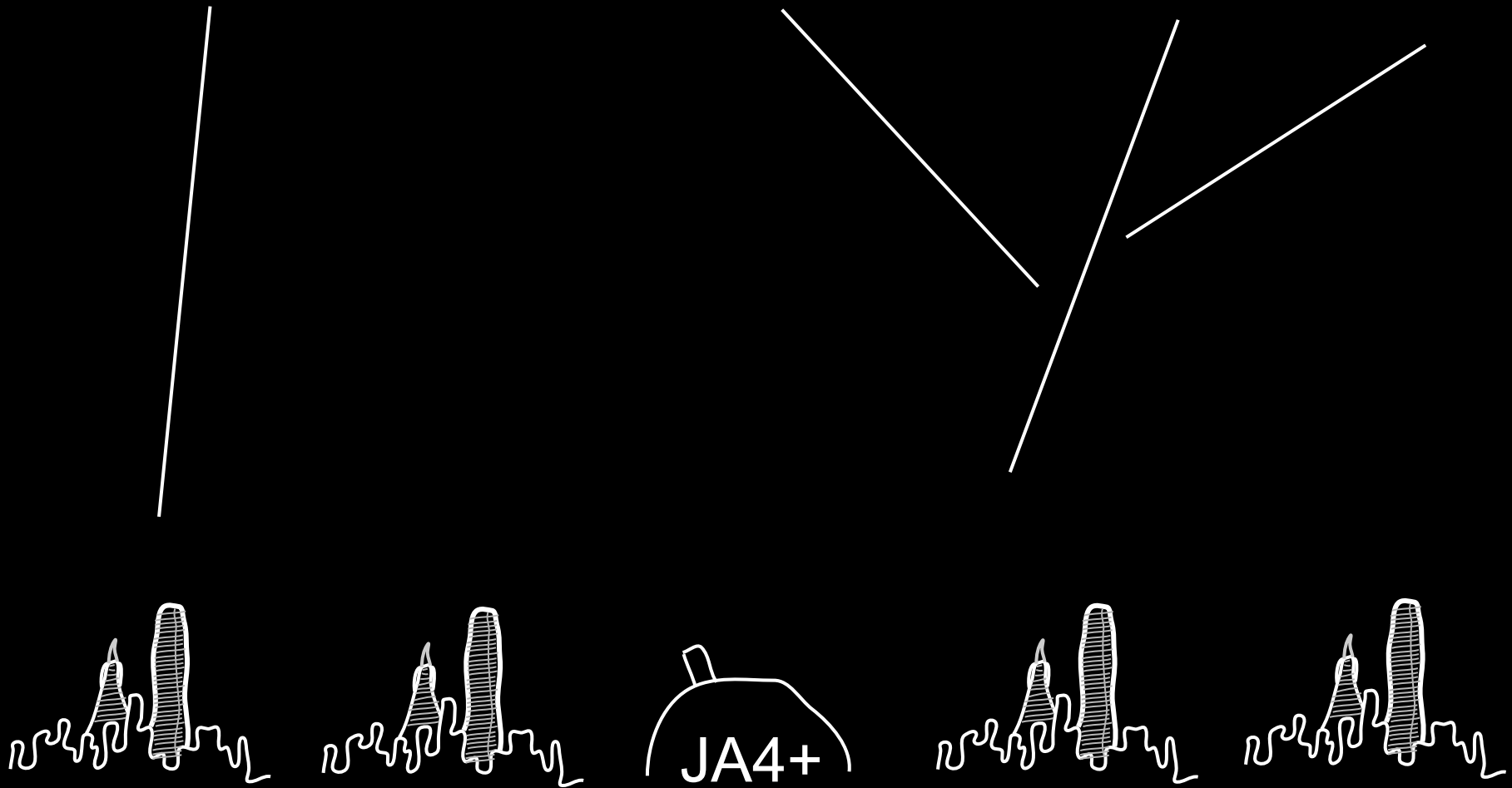

JA4+


JA4+


JA4+


poof
JA4+


poof
JA4+


JA4+

Identify malware, RMMs, C2 Infra

Utilizing:

JA4 + JA4S + JA4TS + JA4X + JA4H

Lumma Stealer

JA4 = t12d190800_d83cc789557e_7af1ed941c26 (WinINet)
JA4S = t120600_c02b_d0d4e4171d74 (Cloudflare response)
JA4TS = 65535_2-1-1-4-1-3_1400_13 (Cloudflare TCP Response to Windows)

Lumma Stealer

JA4 = t12d190800_d83cc789557e_7af1ed941c26 AND
JA4S = t120600_c02b_d0d4e4171d74 AND
JA4TS = 65535_2-1-1-4-1-3_1400_13 AND
New Domain

Malware Detection with JA4H

Application	Application Fingerprint		Website Cookie Fingerprint	User Cookie Fingerprint
	JA4H_a	JA4H_b	JA4H_c	JA4H_d
Rusty Stealer	po11nn050000	ac9aaa8a3e9d	000000000000	000000000000
	JA4H_ab = po11nn050000_ac9aaa8a3e9d			
Rhadamanthys Malware	ge11nn072a00	4ae0f4a72b53	000000000000	000000000000
	JA4H_ab = ge11nn072a00_4ae0f4a72b53			
Atera RRM	ge11nn040000	3f76751f2ae6	000000000000	000000000000
	JA4H_ab = ge11nn040000_3f76751f2ae6			
NetSupport RAT	po11nn050000	dee2ecda03a6	000000000000	000000000000
	JA4H_ab = po11nn050000_dee2ecda03a6			
Sliver Malware	po11nn060000	eeacb637adbb	000000000000	000000000000
	JA4H_ab = po11nn060000_eeacb637adbb			

Rhadamanthys

Sample 1:
JA4 = t12d030600_66e10a142862_9b994c9d23f8
JA4S = t120200_009c_344b4dce5a52
JA4X = 2bab15409345_2bab15409345_1e0053d9ccd0

Rhadamanthys

Sample 1:
JA4 = t12d030600_66e10a142862_9b994c9d23f8
JA4S = t120200_009c_344b4dce5a52
JA4X = 2bab15409345_2bab15409345_1e0053d9ccd0

Sample 2:
JA4 = t12d400700_9719658096a2_7b0ba9b4cf08
JA4S = t120200_cca8_344b4dce5a52
JA4X = 2bab15409345_2bab15409345_1e0053d9ccd0

Rhadamanthys

Sample 1:
JA4 = t12d030600_66e10a142862_9b994c9d23f8
JA4S = t120200_009c_344b4dce5a52
JA4X = 2bab15409345_2bab15409345_1e0053d9ccd0

Sample 2:
JA4 = t12d400700_9719658096a2_7b0ba9b4cf08
JA4S = t120200_cca8_344b4dce5a52
JA4X = 2bab15409345_2bab15409345_1e0053d9ccd0

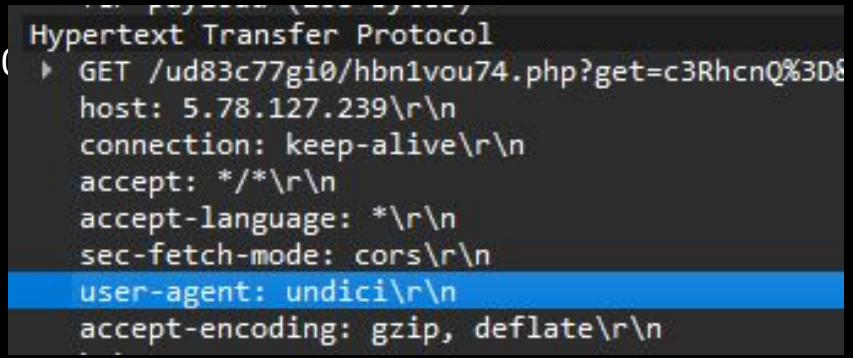
JA4H = ge11nn072a00_4ae0f4a72b53_000000000000_000000000000

Rhadamanthys

Sample 1:
JA4 = t12d030600_66e10a142862_9b994c9d23f8
JA4S = t120200_009c_344b4dce5a52
JA4X = 2bab15409345_2bab15409345_1e0053d9ccd0

Sample 2:
JA4 = t12d400700_9719658096a2_7b0ba9b4cf08
JA4S = t120200_cca8_344b4dce5a52
JA4X = 2bab15409345_2bab15409345_1e0053d9ccd0

JA4H = ge11nn072a00_4ae0f4a72b53_000000000000_00(



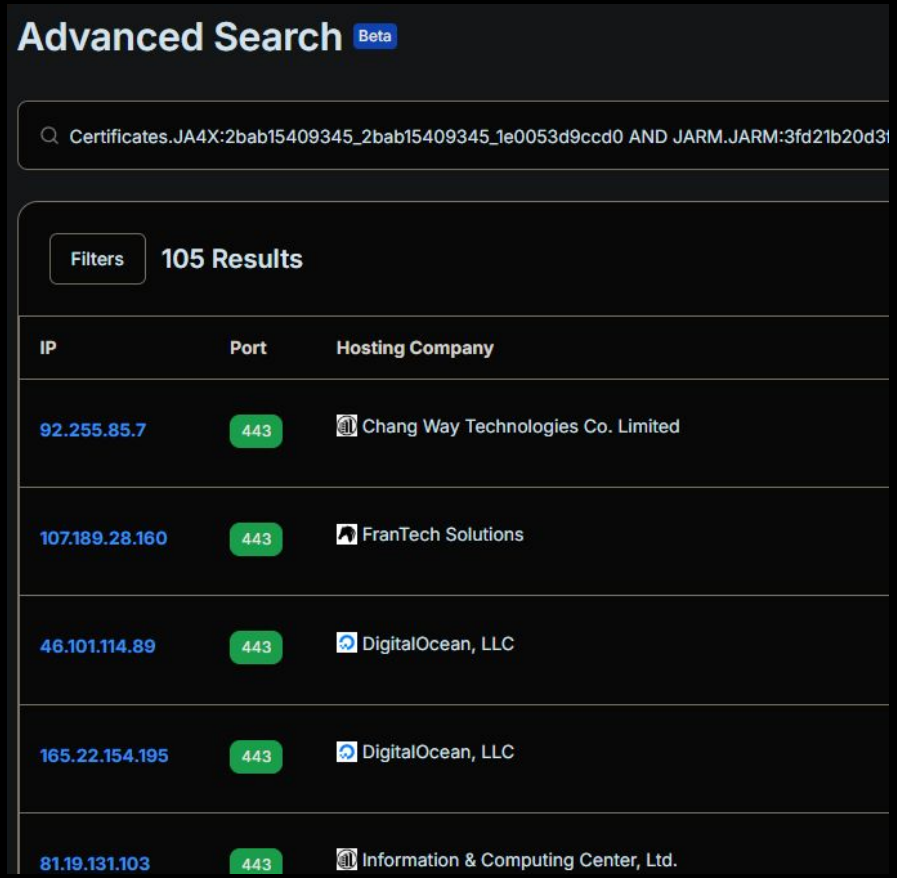
Summary - 20/719 Files	Detections	First seen	Last seen	Submitters
08e2a5b0873457d816ec48b7ad36bcbdf85cdf207e8adf3a2193ee275508d7e6 C:\Users\user\AppData\Local\Temp\cmd.bat bat long-sleeps checks-user-input service-scan persistence checks-cpu-name detect-debug-environment cve-2016-2569 exploit	0 / 59	2025-02-26 18:39:12	2025-02-26 18:39:12	1
39d789a5bfd6f2d2db52226b3f77f88ebb6d92d0baae6561c3b27f315b17738d stage3.bat powershell calls-wmi detect-debug-environment long-sleeps persistence checks-cpu-name checks-disk-space checks-bios	0 / 62	2025-03-05 04:36:26	2025-03-05 04:36:26	1
40bf4e833622eb7d4f0749a6593520630435a38d08dd3fb71ddc578a05ad3c62 No meaningful names powershell url-pattern calls-wmi persistence detect-debug-environment long-sleeps service-scan checks-user-input self-delete ...	0 / 63	2025-03-17 22:40:15	2025-03-17 22:40:15	1
48c3b19d977f0bd7ec81ddfa530536086d5acf79a323e1ac0c189cc5b3222ef0 dump.txt powershell calls-wmi detect-debug-environment long-sleeps checks-cpu-name	0 / 63	2025-04-01 21:37:36	2025-04-01 21:37:36	1
7e071f43bbe95f9a86c86fb35e251da17ce51c6271bf8a327d0948e931493150 command.cmd text	0 / 62	2025-03-09 21:50:59	2025-03-09 21:50:59	1
826108c37b072ed4ef1f909b5aca6a96fc80b6d67ab7845f54db51949538778d $PLUGINSDIR/app-64.7z 7zip contains-pe checks-user-input detect-debug-environment long-sleeps	0 / 61	2025-02-20 23:26:05	2025-02-20 23:26:05	1
a04c635dead3effab39362f70773d2abbf6c6eee2081b87d5849508aa53cc667 fjlsjiaubyvcrs.ps1 powershell calls-wmi detect-debug-environment long-sleeps checks-cpu-name	0 / 62	2025-04-04 20:44:47	2025-04-07 04:49:50	4
ac423d88f830c0f7b79c6811f60288567944652e8dd67474eac6c39e63b0262c payload_1.ps1 powershell url-pattern exe-pattern persistence checks-user-input long-sleeps checks-cpu-name detect-debug-environment	0 / 59	2025-02-23 00:51:16	2025-02-23 00:51:16	1
ba7e385d5d6f429178b281d701b03a2b7039b541806754c6ffcc918d2cb4da84 payload_1.ps1 powershell url-pattern detect-debug-environment long-sleeps	0 / 62	2025-03-31 20:05:56	2025-03-31 20:05:56	1

Rhadamanthys

JA4X = 2bab15409345_2bab15409345_1e0053d9ccd0

AND

JARM = 3fd21b20d3fd3fd21c43d21b21b43d1ec49a4b64df0a9e9f328abd60285841



Patent Pending
FoxIO License 1.1

JA4D: DHCP Fingerprint

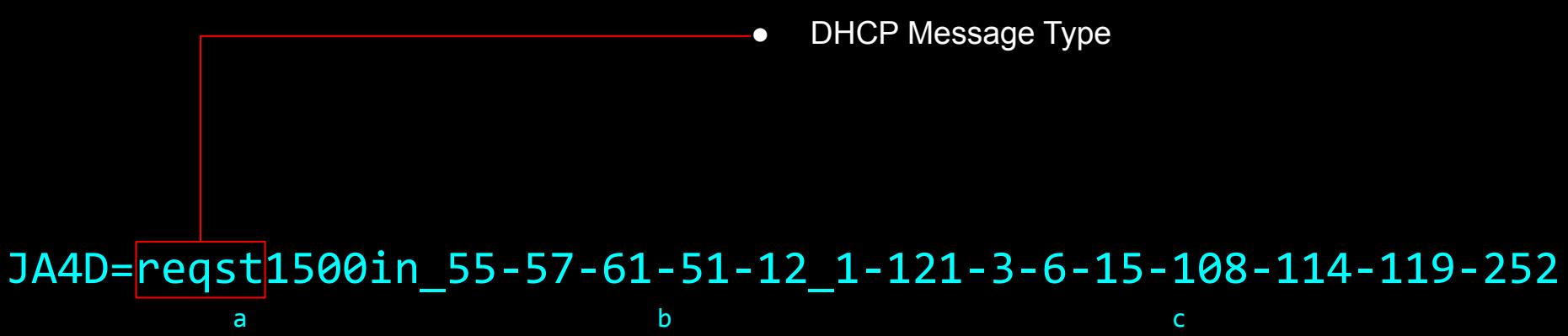
(iPhone Example)

```
JA4D=reqst1500in_55-57-61-51-12_1-121-3-6-15-108-114-119-252
          a                    b                        c
```

Patent Pending
FoxIO License 1.1

JA4D: DHCP Fingerprint

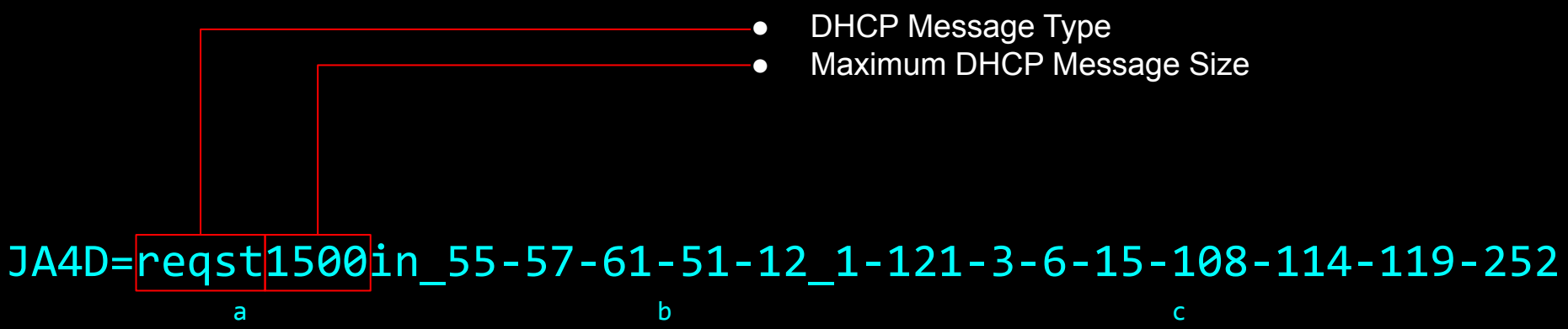
(iPhone Example)



Patent Pending
FoxIO License 1.1

JA4D: DHCP Fingerprint

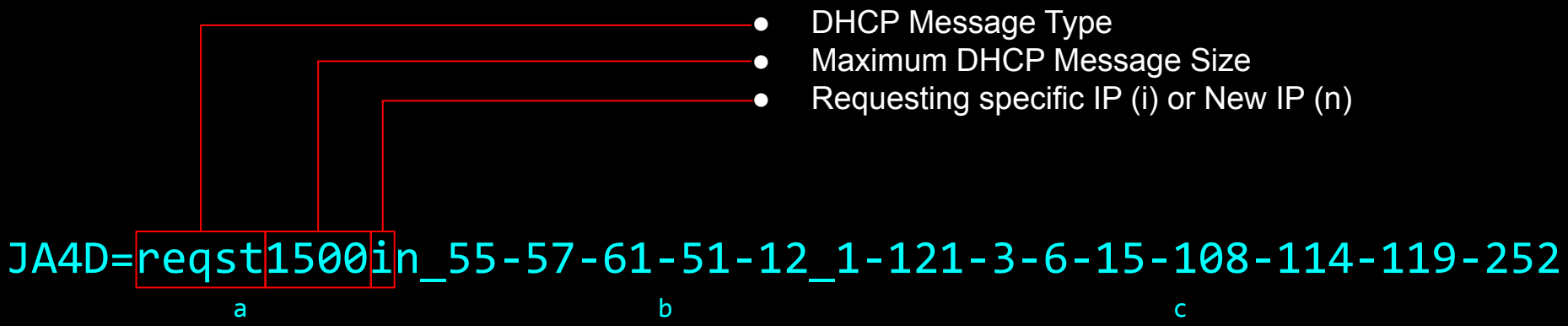
(iPhone Example)



Patent Pending
FoxIO License 1.1

JA4D: DHCP Fingerprint

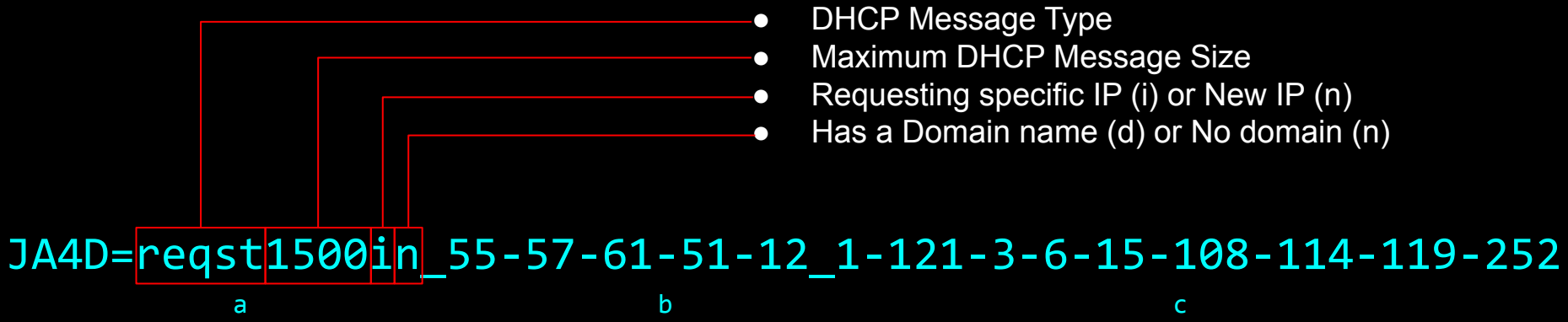
(iPhone Example)



Patent Pending
FoxIO License 1.1

JA4D: DHCP Fingerprint

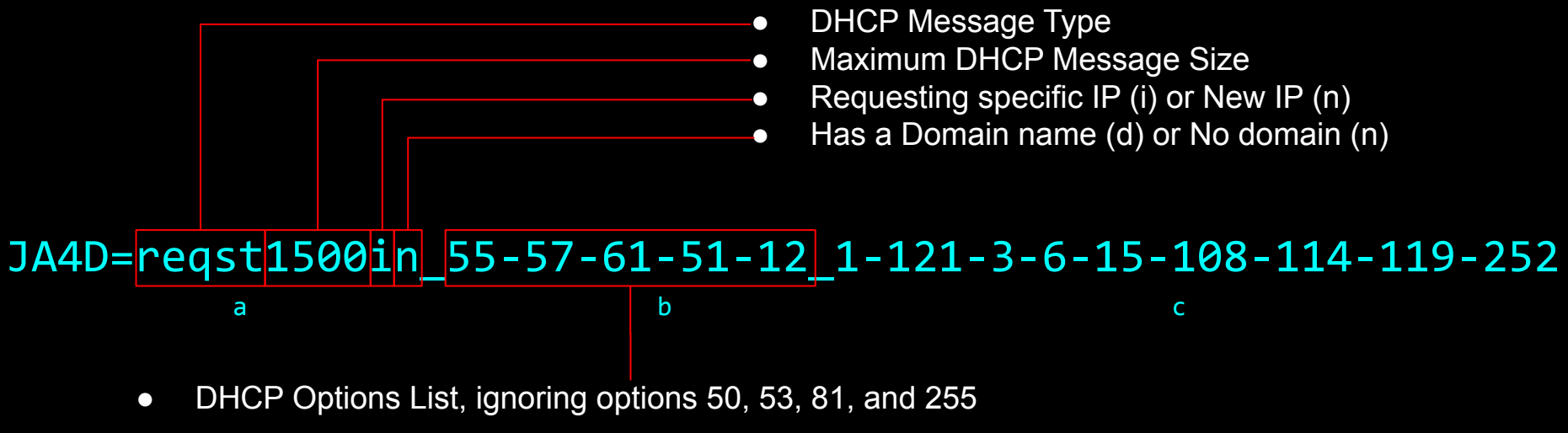
(iPhone Example)



Patent Pending
FoxIO License 1.1

JA4D: DHCP Fingerprint

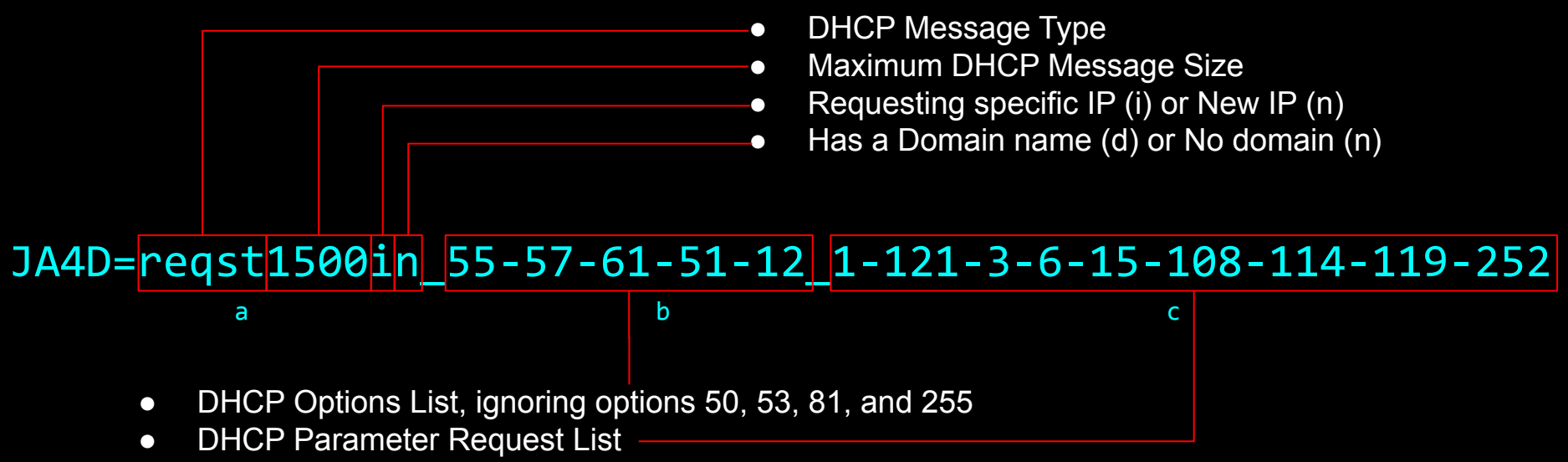
(iPhone Example)



Patent Pending
FoxIO License 1.1

JA4D: DHCP Fingerprint

(iPhone Example)



Patent Pending
FoxIO License 1.1

JA4D6: DHCPv6 Fingerprint

(Windows 11 Example)

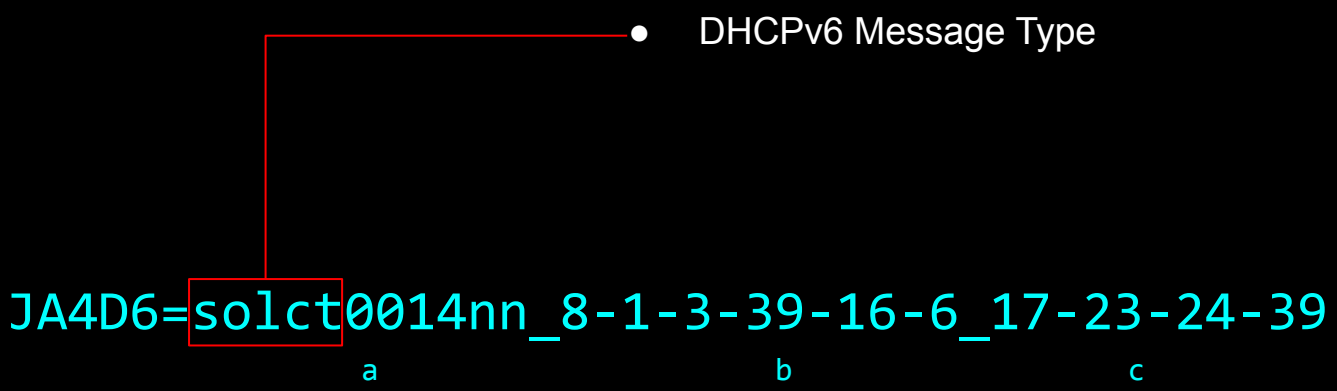
JA4D6=solct0014nn_8-1-3-39-16-6_17-23-24-39

a b c

Patent Pending
FoxIO License 1.1

JA4D6: DHCPv6 Fingerprint

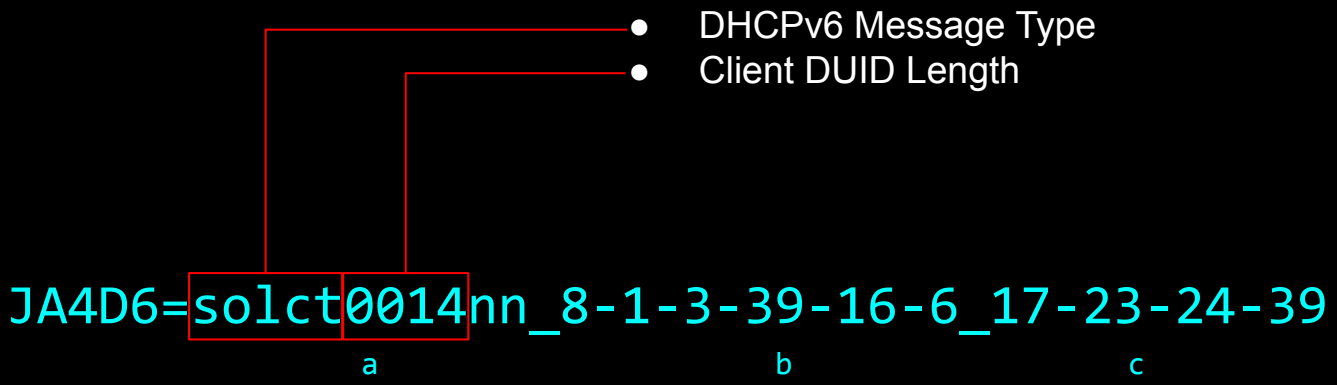
(Windows 11 Example)



Patent Pending
FoxIO License 1.1

JA4D6: DHCPv6 Fingerprint

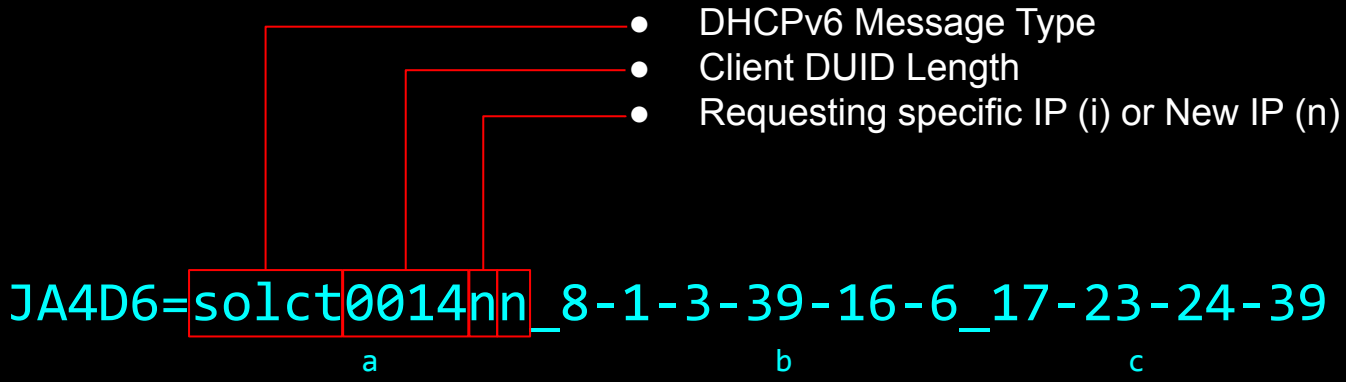
(Windows 11 Example)



Patent Pending
FoxIO License 1.1

JA4D6: DHCPv6 Fingerprint

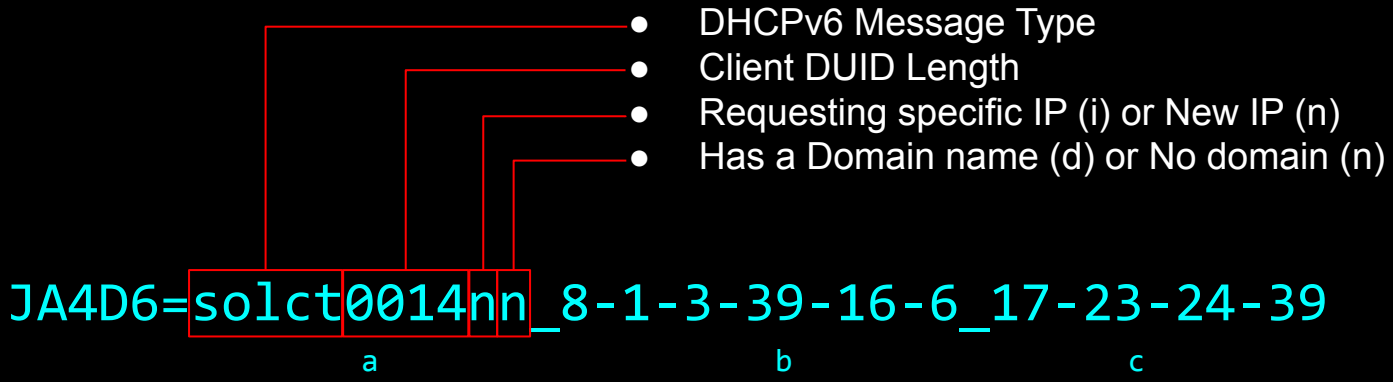
(Windows 11 Example)



Patent Pending
FoxIO License 1.1

JA4D6: DHCPv6 Fingerprint

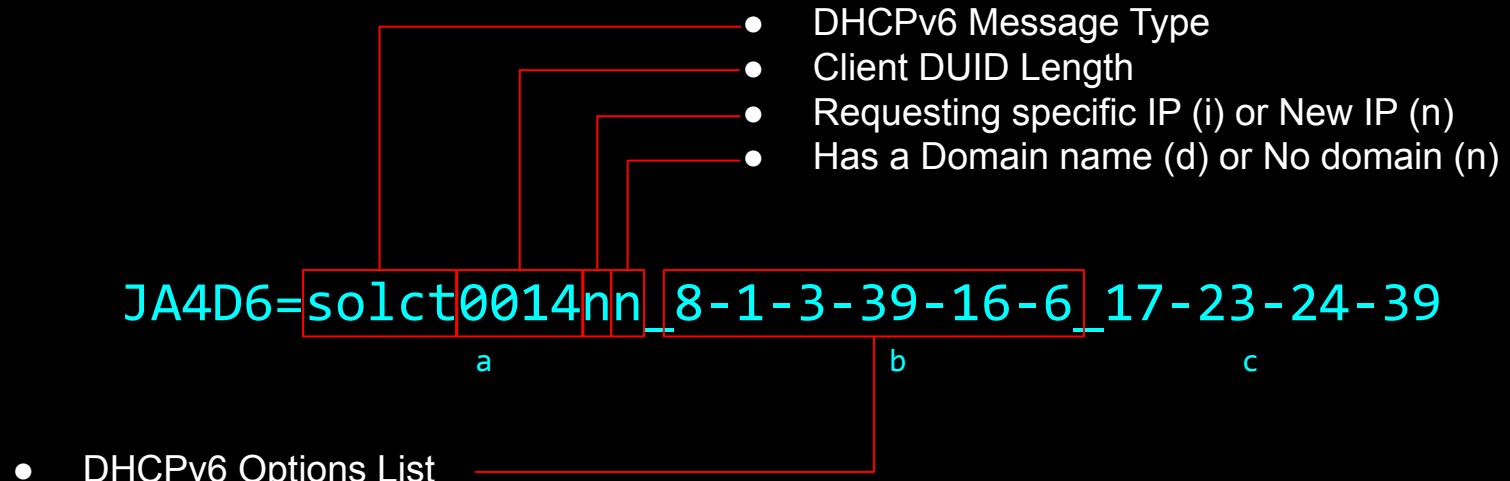
(Windows 11 Example)



Patent Pending
FoxIO License 1.1

JA4D6: DHCPv6 Fingerprint

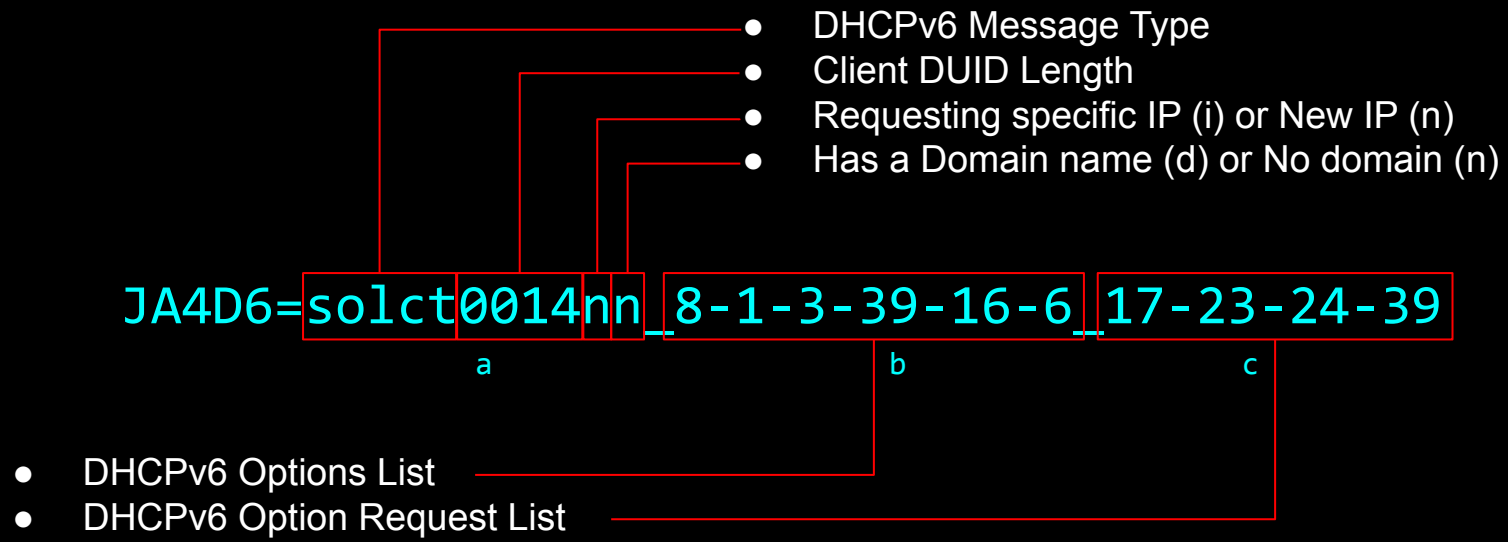
(Windows 11 Example)



Patent Pending
FoxIO License 1.1

JA4D6: DHCPv6 Fingerprint

(Windows 11 Example)



JA4+ Fingerprints	Operating System	Device
ja4d == disco1500nn_61-57-60-12-55_1-3-6-15-26-28-51-58-59-43-114-108	Android 16	Samsung Phone
ja4d == reqst1500in_61-57-60-12-55_1-3-6-15-26-28-51-58-59-43-114-108	Android 16	Samsung Phone
ja4d == disco0000nn_61-12-60-55_1-3-6-15-31-33-43-44-46-47-119-121-249-252	Windows 10/11	Desktop/Laptop
ja4d == reqst0000id_61-12-60-55_1-3-6-15-31-33-43-44-46-47-119-121-249-252	Windows 10/11	Desktop/Laptop
ja4d6 == solct0014nn_8-1-3-39-16-6_17-23-24-39	Windows 10/11	Desktop/Laptop
ja4d6 == reqst0014nn_8-1-2-3-5-39-16-6_17-23-24-39	Windows 10/11	Desktop/Laptop
ja4d == reqst0576nn_57-55-12-60-61_1-3-6-12-15-28-42	Embedded Linux 1.34	Ubiquiti Cameras
ja4d == reqst0576nn_57-55-60-12_1-3-6-15-28-42-121	Embedded Linux 1.30	Phillips Hue Bridge
ja4d == reqst0576nn_61-57-55-60-12_1-3-6-12-15-28-42-43	Ubiquiti	Ubiquiti Hardware
ja4d == disco1500nn_57-55-60-61-12_1-2-3-6-69	EMLAB	LIFX Smart Bulbs
ja4d == disco0576nn_57-55-61-12_1-3-26-252-42-15-6-12	Android TV	LG WebOS TV
ja4d == disco0576nn_57-55-61-12_1-3-26-252-43-42-6-12	Android TV	Samsung TV
ja4d == reqst0000nn_61-12-55_1-3-6-12-15-28	Epson	Epson Printer

JA4SSH: SSH Traffic Fingerprint

(fingerprints SSH sessions)

JA4SSH: SSH Traffic Fingerprint

(fingerprints SSH sessions)

192.168.1.169	44.212.59.210	SSHv2	u	36 Client:
44.212.59.210	192.168.1.169	SSHv2		36 Server:
192.168.1.169	44.212.59.210	TCP		0 64339 → 22 [ACK]
192.168.1.169	44.212.59.210	SSHv2	n	36 Client:
44.212.59.210	192.168.1.169	SSHv2		36 Server:
192.168.1.169	44.212.59.210	TCP		0 64339 → 22 [ACK]
192.168.1.169	44.212.59.210	SSHv2	a	36 Client:
44.212.59.210	192.168.1.169	SSHv2		36 Server:
192.168.1.169	44.212.59.210	TCP		0 64339 → 22 [ACK]
192.168.1.169	44.212.59.210	SSHv2	m	36 Client:
44.212.59.210	192.168.1.169	SSHv2		36 Server:
192.168.1.169	44.212.59.210	TCP		0 64339 → 22 [ACK]
192.168.1.169	44.212.59.210	SSHv2	e	36 Client:
44.212.59.210	192.168.1.169	SSHv2		36 Server:
192.168.1.169	44.212.59.210	TCP		0 64339 → 22 [ACK]
192.168.1.169	44.212.59.210	SSHv2		36 Client:
44.212.59.210	192.168.1.169	SSHv2		36 Server:
192.168.1.169	44.212.59.210	TCP		0 64339 → 22 [ACK]
192.168.1.169	44.212.59.210	SSHv2	-	36 Client:
44.212.59.210	192.168.1.169	SSHv2		36 Server:
192.168.1.169	44.212.59.210	TCP		0 64339 → 22 [ACK]
192.168.1.169	44.212.59.210	SSHv2	a	36 Client:
44.212.59.210	192.168.1.169	SSHv2		36 Server:
192.168.1.169	44.212.59.210	TCP		0 64339 → 22 [ACK]
192.168.1.169	44.212.59.210	SSHv2	⏎	36 Client:
44.212.59.210	192.168.1.169	SSHv2		52 Server:
44.212.59.210	192.168.1.169	SSHv2		68 Server:
192.168.1.169	44.212.59.210	TCP		0 64339 → 22 [ACK]

JA4SSH: SSH Traffic Fingerprint

(fingerprints SSH sessions)

```
44.212.59.210   192.168.1.197  SSHv2      76 Server:
192.168.1.197   44.212.59.210  SSHv2      76 Client:
44.212.59.210   192.168.1.197  TCP         0 22 → 46396 [ACK]
44.212.59.210   192.168.1.197  SSHv2      76 Server:
192.168.1.197   44.212.59.210  SSHv2      76 Client:
44.212.59.210   192.168.1.197  TCP         0 22 → 46396 [ACK]
44.212.59.210   192.168.1.197  SSHv2      76 Server:
192.168.1.197   44.212.59.210  SSHv2      76 Client:
44.212.59.210   192.168.1.197  TCP         0 22 → 46396 [ACK]
44.212.59.210   192.168.1.197  SSHv2      76 Server:
192.168.1.197   44.212.59.210  SSHv2      76 Client:
44.212.59.210   192.168.1.197  TCP         0 22 → 46396 [ACK]
44.212.59.210   192.168.1.197  SSHv2      76 Server:
192.168.1.197   44.212.59.210  SSHv2      76 Client:
44.212.59.210   192.168.1.197  TCP         0 22 → 46396 [ACK]
44.212.59.210   192.168.1.197  SSHv2      76 Server:
192.168.1.197   44.212.59.210  SSHv2      76 Client:
44.212.59.210   192.168.1.197  TCP         0 22 → 46396 [ACK]
44.212.59.210   192.168.1.197  SSHv2      76 Server:
192.168.1.197   44.212.59.210  SSHv2      76 Client:
44.212.59.210   192.168.1.197  TCP         0 22 → 46396 [ACK]
44.212.59.210   192.168.1.197  SSHv2      76 Server:
192.168.1.197   44.212.59.210  SSHv2      76 Client:
44.212.59.210   192.168.1.197  TCP         0 22 → 46396 [ACK]
44.212.59.210   192.168.1.197  SSHv2      76 Server:
192.168.1.197   44.212.59.210  SSHv2      76 Client:
44.212.59.210   192.168.1.197  TCP         0 22 → 46396 [ACK]
192.168.1.197   44.212.59.210  SSHv2     412 Client:
192.168.1.197   44.212.59.210  SSHv2     124 Client:
44.212.59.210   192.168.1.197  TCP         0 22 → 46396 [ACK]
```

JA4SSH: SSH Traffic Fingerprint

(fingerprints SSH sessions)

192.168.1.169	44.212.59.210	SSHv2	36	Client:
44.212.59.210	192.168.1.169	SSHv2	36	Server:
192.168.1.169	44.212.59.210	TCP	0	64339 → 22 [ACK]
192.168.1.169	44.212.59.210	SSHv2	36	Client:
44.212.59.210	192.168.1.169	SSHv2	36	Server:
192.168.1.169	44.212.59.210	TCP	0	64339 → 22 [ACK]
192.168.1.169	44.212.59.210	SSHv2	36	Client:
44.212.59.210	192.168.1.169	SSHv2	36	Server:
192.168.1.169	44.212.59.210	TCP	0	64339 → 22 [ACK]
192.168.1.169	44.212.59.210	SSHv2	36	Client:
44.212.59.210	192.168.1.169	SSHv2	36	Server:
192.168.1.169	44.212.59.210	TCP	0	64339 → 22 [ACK]
192.168.1.169	44.212.59.210	SSHv2	36	Client:
44.212.59.210	192.168.1.169	SSHv2	36	Server:
192.168.1.169	44.212.59.210	TCP	0	64339 → 22 [ACK]
192.168.1.169	44.212.59.210	SSHv2	36	Client:
44.212.59.210	192.168.1.169	SSHv2	36	Server:
192.168.1.169	44.212.59.210	TCP	0	64339 → 22 [ACK]
192.168.1.169	44.212.59.210	SSHv2	36	Client:
44.212.59.210	192.168.1.169	SSHv2	36	Server:
192.168.1.169	44.212.59.210	TCP	0	64339 → 22 [ACK]
192.168.1.169	44.212.59.210	SSHv2	36	Client:
44.212.59.210	192.168.1.169	SSHv2	36	Server:
192.168.1.169	44.212.59.210	TCP	0	64339 → 22 [ACK]
192.168.1.169	44.212.59.210	SSHv2	36	Client:
44.212.59.210	192.168.1.169	SSHv2	52	Server:
44.212.59.210	192.168.1.169	SSHv2	68	Server:
192.168.1.169	44.212.59.210	TCP	0	64339 → 22 [ACK]

44.212.59.210	192.168.1.197	SSHv2	76	Server:
192.168.1.197	44.212.59.210	SSHv2	76	Client:
44.212.59.210	192.168.1.197	TCP	0	22 → 46396 [ACK]
44.212.59.210	192.168.1.197	SSHv2	76	Server:
192.168.1.197	44.212.59.210	SSHv2	76	Client:
44.212.59.210	192.168.1.197	TCP	0	22 → 46396 [ACK]
44.212.59.210	192.168.1.197	SSHv2	76	Server:
192.168.1.197	44.212.59.210	SSHv2	76	Client:
44.212.59.210	192.168.1.197	TCP	0	22 → 46396 [ACK]
44.212.59.210	192.168.1.197	SSHv2	76	Server:
192.168.1.197	44.212.59.210	SSHv2	76	Client:
44.212.59.210	192.168.1.197	TCP	0	22 → 46396 [ACK]
44.212.59.210	192.168.1.197	SSHv2	76	Server:
192.168.1.197	44.212.59.210	SSHv2	76	Client:
44.212.59.210	192.168.1.197	TCP	0	22 → 46396 [ACK]
44.212.59.210	192.168.1.197	SSHv2	76	Server:
192.168.1.197	44.212.59.210	SSHv2	76	Client:
44.212.59.210	192.168.1.197	TCP	0	22 → 46396 [ACK]
44.212.59.210	192.168.1.197	SSHv2	76	Server:
192.168.1.197	44.212.59.210	SSHv2	76	Client:
44.212.59.210	192.168.1.197	TCP	0	22 → 46396 [ACK]
44.212.59.210	192.168.1.197	SSHv2	76	Server:
192.168.1.197	44.212.59.210	SSHv2	76	Client:
44.212.59.210	192.168.1.197	TCP	0	22 → 46396 [ACK]
44.212.59.210	192.168.1.197	SSHv2	76	Server:
192.168.1.197	44.212.59.210	SSHv2	76	Client:
44.212.59.210	192.168.1.197	TCP	0	22 → 46396 [ACK]
192.168.1.197	44.212.59.210	SSHv2	412	Client:
192.168.1.197	44.212.59.210	SSHv2	124	Client:
44.212.59.210	192.168.1.197	TCP	0	22 → 46396 [ACK]

FOXIO

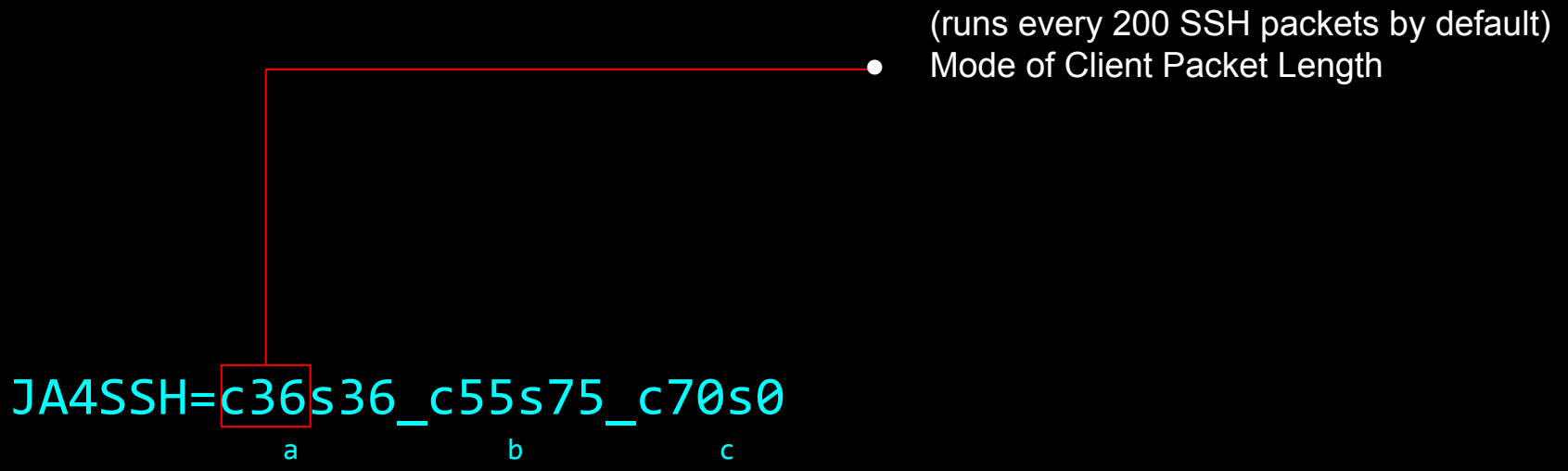
JA4SSH: SSH Traffic Fingerprint

(fingerprints SSH sessions)

```
JA4SSH=c36s36_c55s75_c70s0
       a        b        c
```

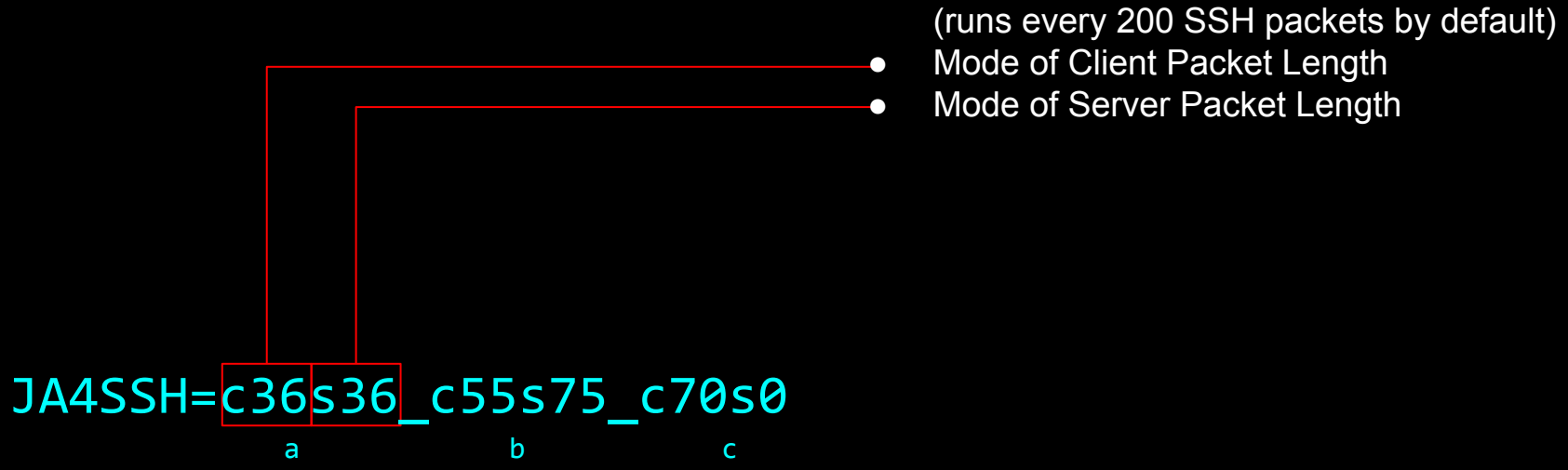
JA4SSH: SSH Traffic Fingerprint

(fingerprints SSH sessions)



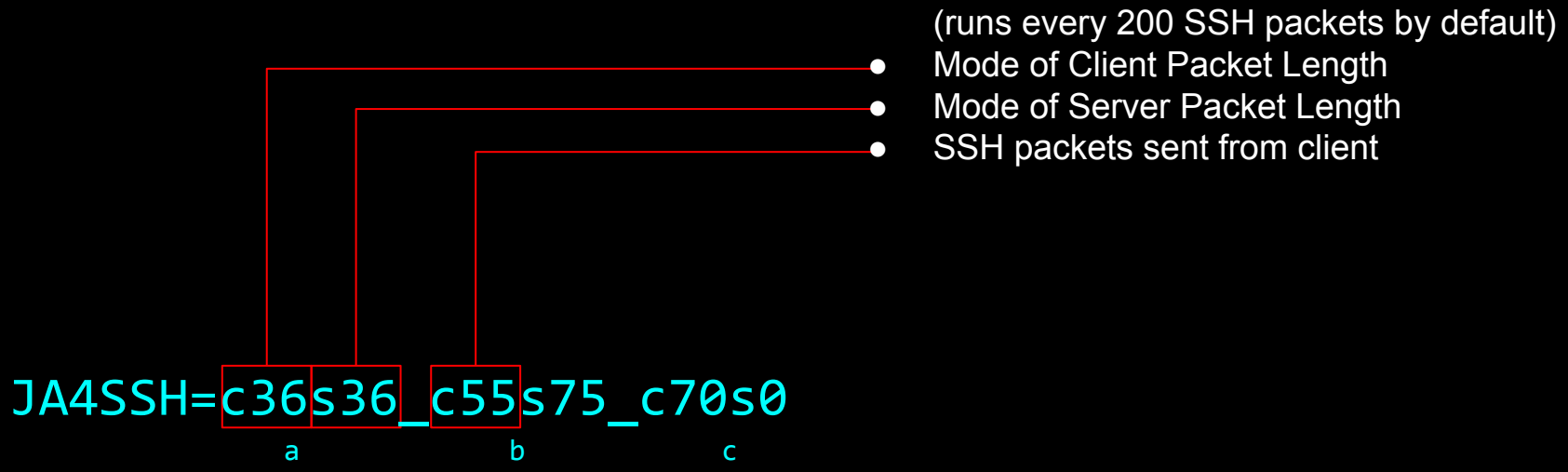
JA4SSH: SSH Traffic Fingerprint

(fingerprints SSH sessions)



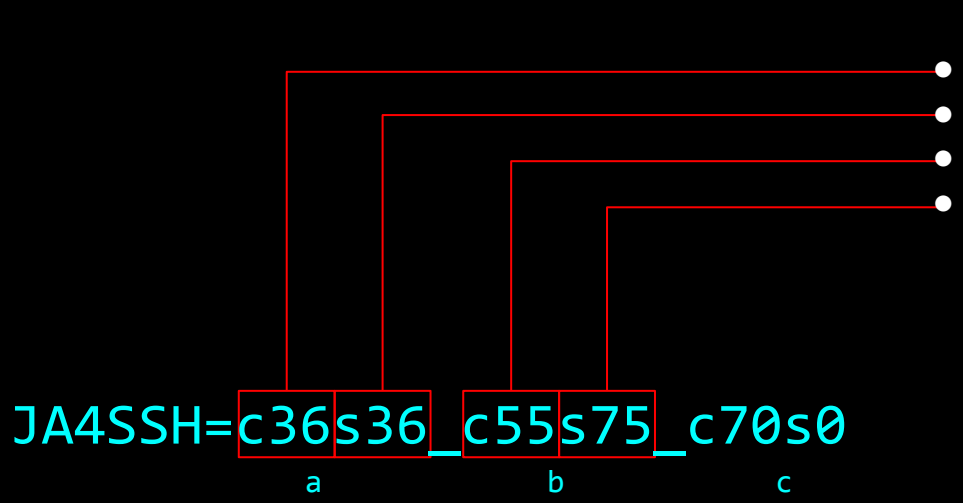
JA4SSH: SSH Traffic Fingerprint

(fingerprints SSH sessions)



JA4SSH: SSH Traffic Fingerprint

(fingerprints SSH sessions)

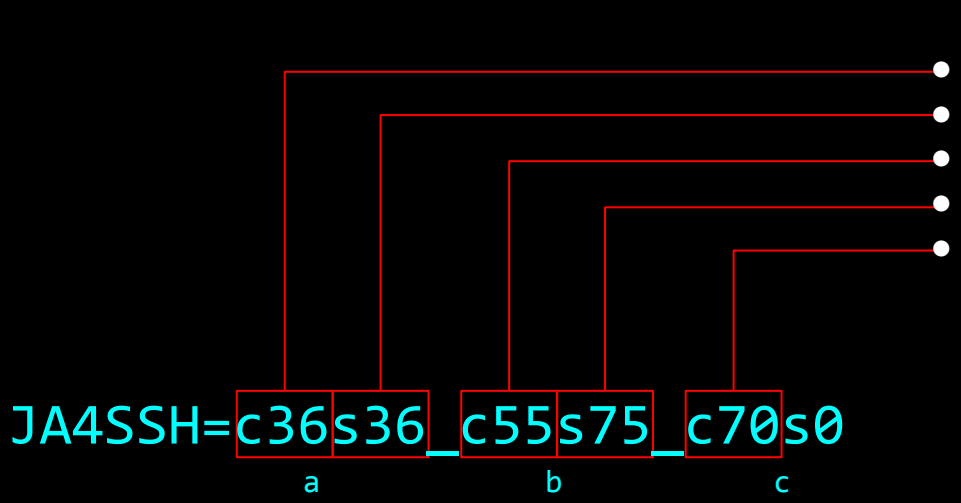


(runs every 200 SSH packets by default)

- Mode of Client Packet Length
- Mode of Server Packet Length
- SSH packets sent from client
- SSH packets sent from server

JA4SSH: SSH Traffic Fingerprint

(fingerprints SSH sessions)

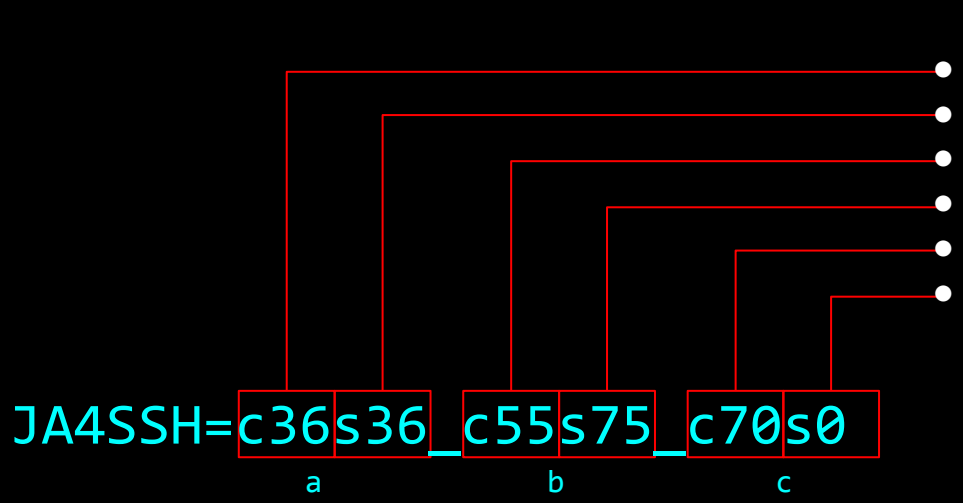


(runs every 200 SSH packets by default)

- Mode of Client Packet Length
- Mode of Server Packet Length
- SSH packets sent from client
- SSH packets sent from server
- Bare ACKs sent from client

JA4SSH: SSH Traffic Fingerprint

(fingerprints SSH sessions)

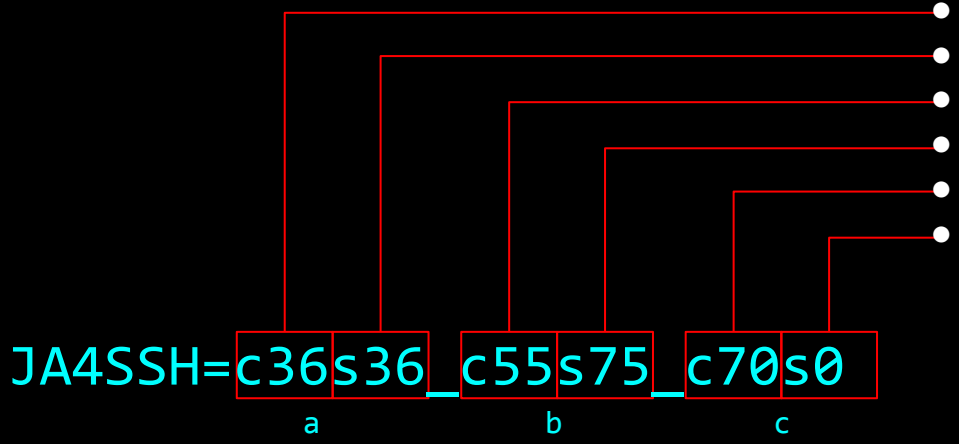


(runs every 200 SSH packets by default)

- Mode of Client Packet Length
- Mode of Server Packet Length
- SSH packets sent from client
- SSH packets sent from server
- Bare ACKs sent from client
- Bare ACKs sent from server

JA4SSH: SSH Traffic Fingerprint

(fingerprints SSH sessions)



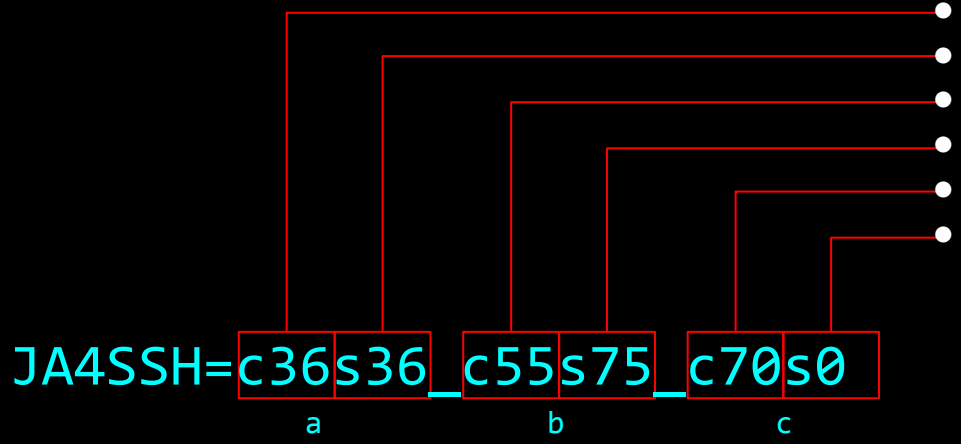
(runs every 200 SSH packets by default)

- Mode of Client Packet Length
- Mode of Server Packet Length
- SSH packets sent from client
- SSH packets sent from server
- Bare ACKs sent from client
- Bare ACKs sent from server

Bare ACKs are sent from the initiating side (eg. side doing the typing)

JA4SSH: SSH Traffic Fingerprint

(fingerprints SSH sessions)



(runs every 200 SSH packets by default)

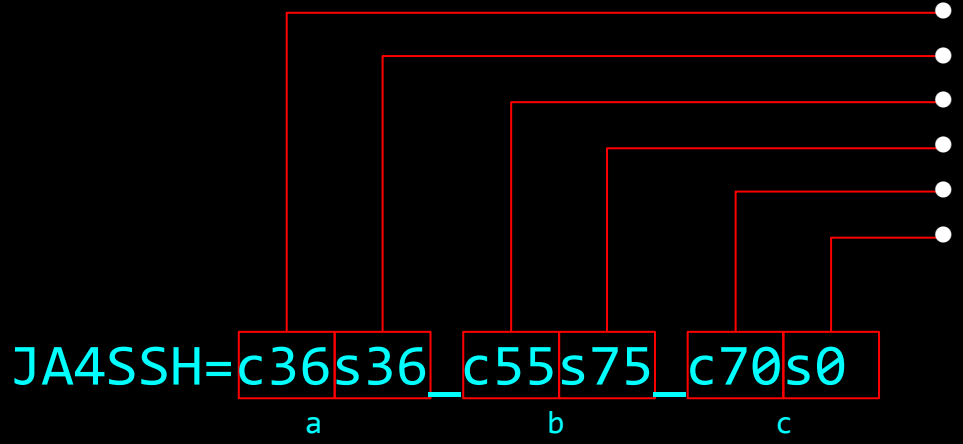
- Mode of Client Packet Length
- Mode of Server Packet Length
- SSH packets sent from client
- SSH packets sent from server
- Bare ACKs sent from client
- Bare ACKs sent from server

Bare ACKs are sent from the initiating side (eg. side doing the typing)

- `Interactive SSH Session = c36s36_c51s80_c69s0`
  - Padded to 36 (minimum length over chacha20-poly1305), all ACKs from client

JA4SSH: SSH Traffic Fingerprint

(fingerprints SSH sessions)



(runs every 200 SSH packets by default)

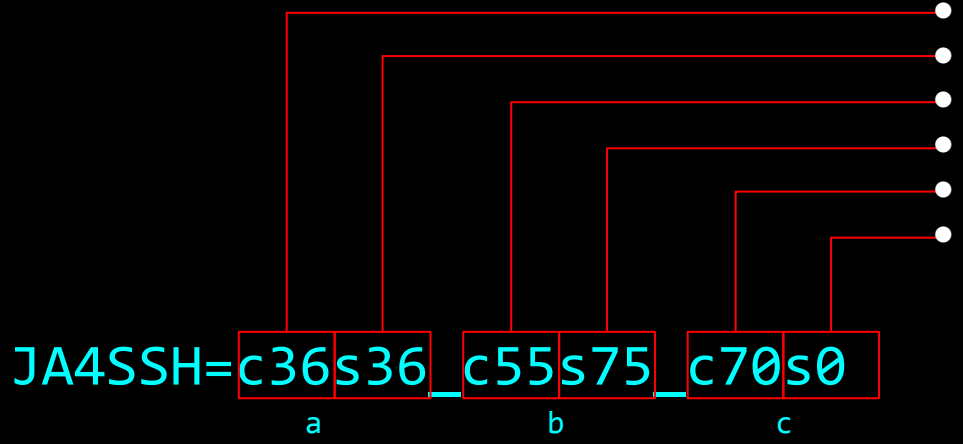
- Mode of Client Packet Length
- Mode of Server Packet Length
- SSH packets sent from client
- SSH packets sent from server
- Bare ACKs sent from client
- Bare ACKs sent from server

Bare ACKs are sent from the initiating side (eg. side doing the typing)

- `Interactive SSH Session = c36s36_c51s80_c69s0`
  - Padded to 36 (minimum length over chacha20-poly1305), all ACKs from client
- `Reverse SSH Session = c76s76_c71s59_c0s70`
  - Double Padded to 76, all ACKs from server

JA4SSH: SSH Traffic Fingerprint

(fingerprints SSH sessions)



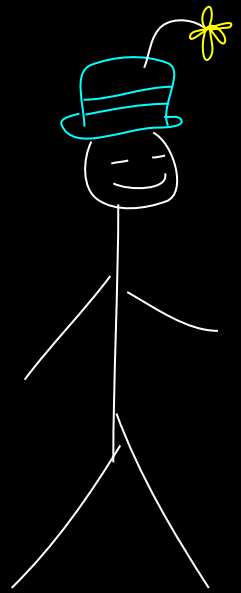
(runs every 200 SSH packets by default)

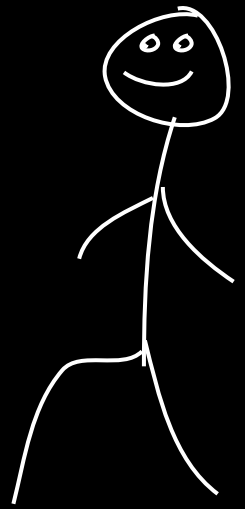
- Mode of Client Packet Length
- Mode of Server Packet Length
- SSH packets sent from client
- SSH packets sent from server
- Bare ACKs sent from client
- Bare ACKs sent from server

Bare ACKs are sent from the initiating side (eg. side doing the typing)

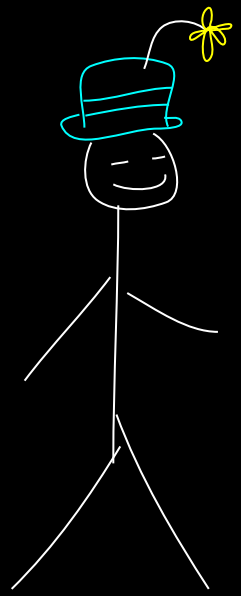
- `Interactive SSH Session` = `c36s36_c51s80_c69s0`
  - Padded to 36 (minimum length over chacha20-poly1305), all ACKs from client
- `Reverse SSH Session` = `c76s76_c71s59_c0s70`
  - Double Padded to 76, all ACKs from server
- `WinSCP File Transfer to Client` = `c0s1460_c0s179_c21s0`
  - Max window from server 1460, all ACKs from client

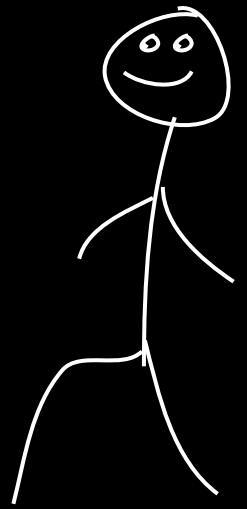
New Problem

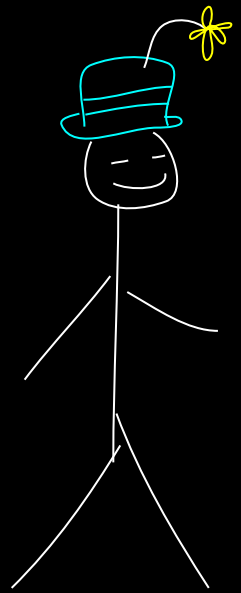




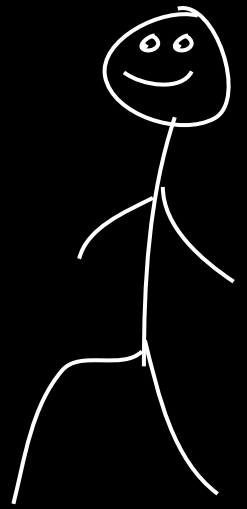
Hello!

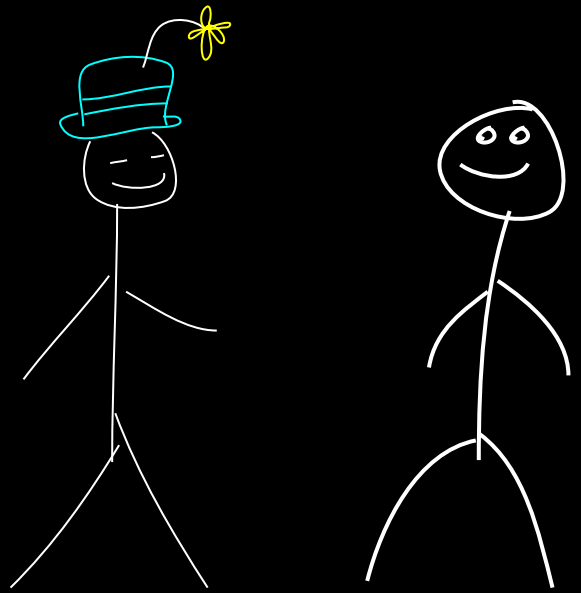




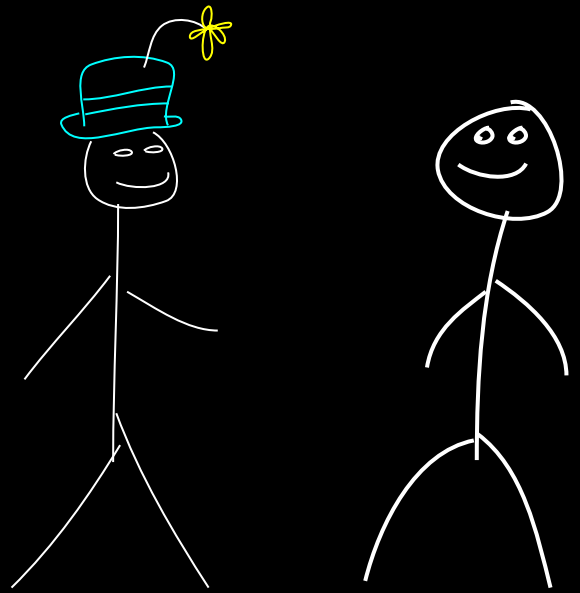


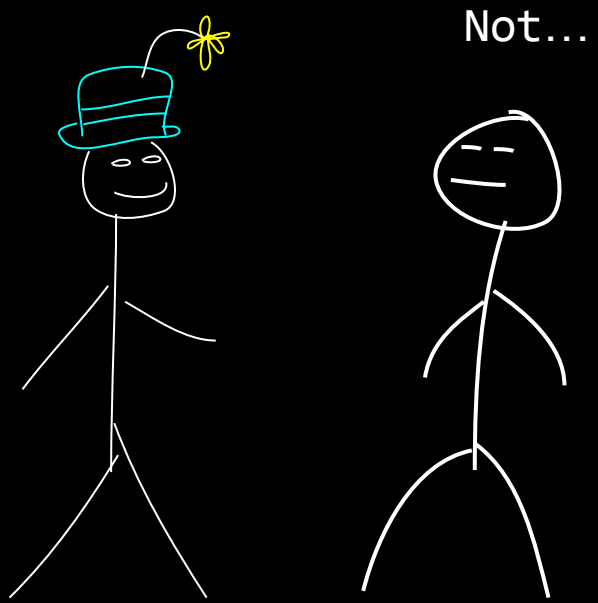
Hello!

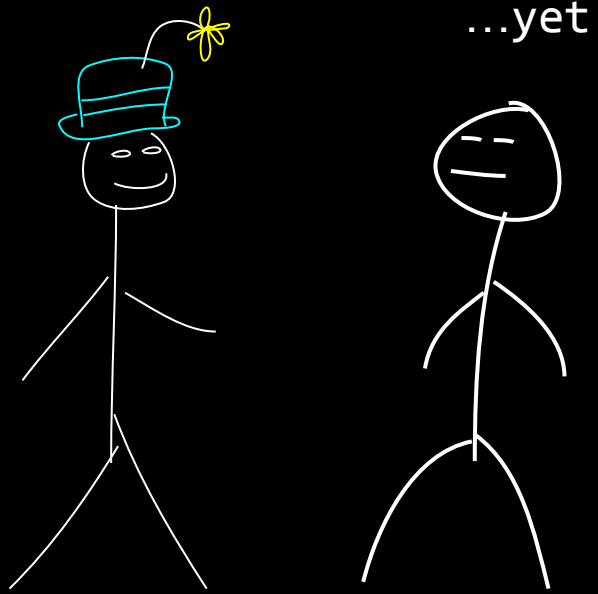




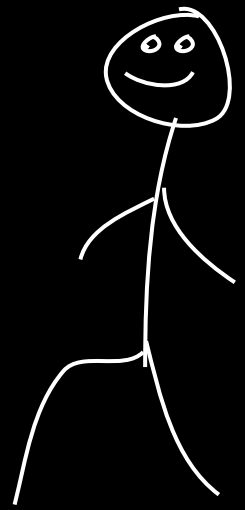
Can you tell how many devices are behind a NAT’d IP, like a hotspot, just by looking at network traffic?

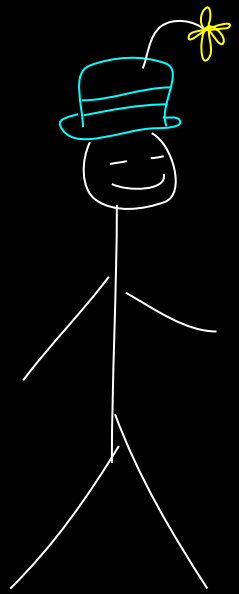



Not...

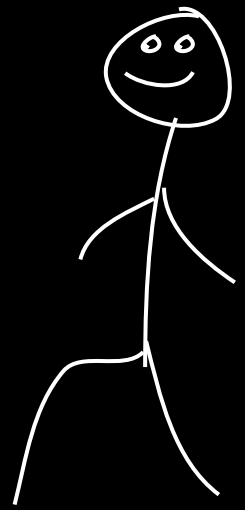

...yet

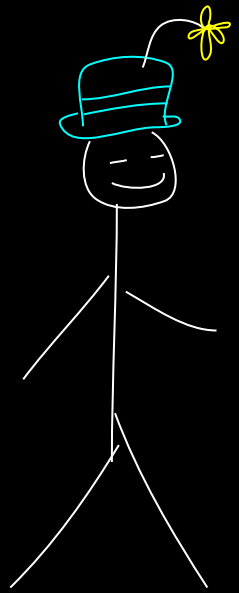
Good-by!



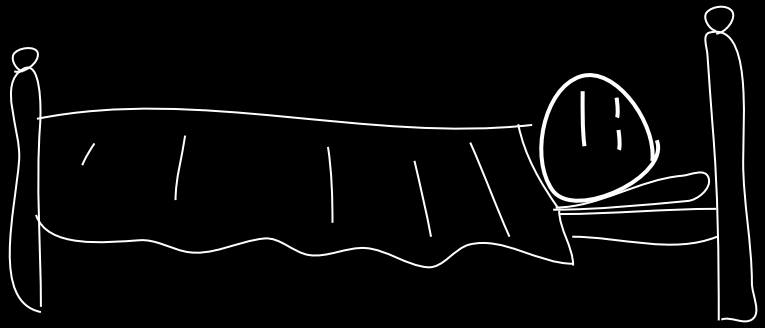


Good-by!

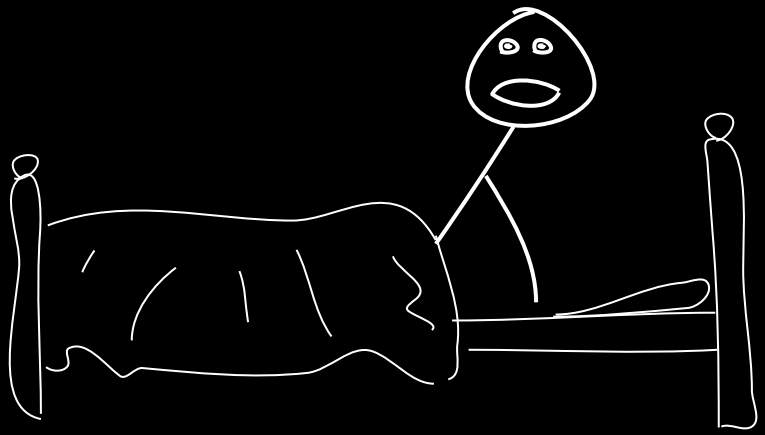




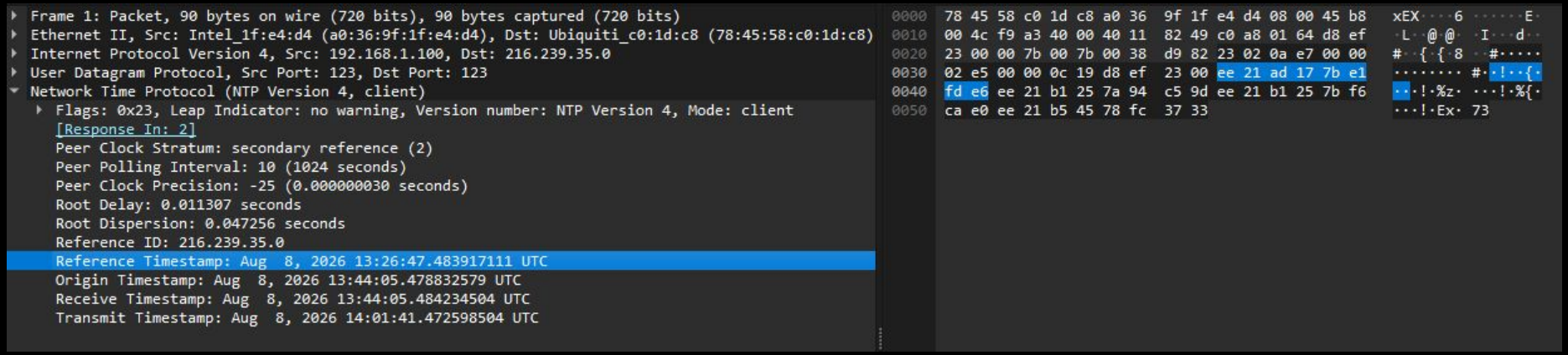
One month later…



NTP



NTP

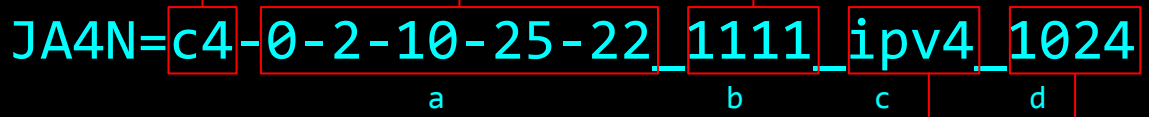

Frame 1: Packet, 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
Ethernet II, Src: Intel_1f:e4:d4 (a0:36:9f:1f:e4:d4), Dst: Ubiquiti_c0:1d:c8 (78:45:58:c0:1d:c8)
Internet Protocol Version 4, Src: 192.168.1.100, Dst: 216.239.35.0
User Datagram Protocol, Src Port: 123, Dst Port: 123
Network Time Protocol (NTP Version 4, client)
Flags: 0x23, Leap Indicator: no warning, Version number: NTP Version 4, Mode: client
[Response In: 2]
Peer Clock Stratum: secondary reference (2)
Peer Polling Interval: 10 (1024 seconds)
Peer Clock Precision: -25 (0.000000030 seconds)
Root Delay: 0.011307 seconds
Root Dispersion: 0.047256 seconds
Reference ID: 216.239.35.0
Reference Timestamp: Aug 8, 2026 13:26:47.483917111 UTC
Origin Timestamp: Aug 8, 2026 13:44:05.478832579 UTC
Receive Timestamp: Aug 8, 2026 13:44:05.484234504 UTC
Transmit Timestamp: Aug 8, 2026 14:01:41.472598504 UTC
0000 78 45 58 c0 1d c8 a0 36 9f 1f e4 d4 08 00 45 b8
0010 00 4c f9 a3 40 00 40 11 82 49 c0 a8 01 64 d8 ef
0020 23 00 00 7b 00 7b 00 38 d9 82 23 02 0a e7 00 00
0030 02 e5 00 00 0c 19 d8 ef 23 00 ee 21 ad 17 7b e1
0040 fd e6 ee 21 b1 25 7a 94 c5 9d ee 21 b1 25 7b f6
0050 ca e0 ee 21 b5 45 78 fc 37 33

FoxIO License 1.1

JA4N: NTP Fingerprint

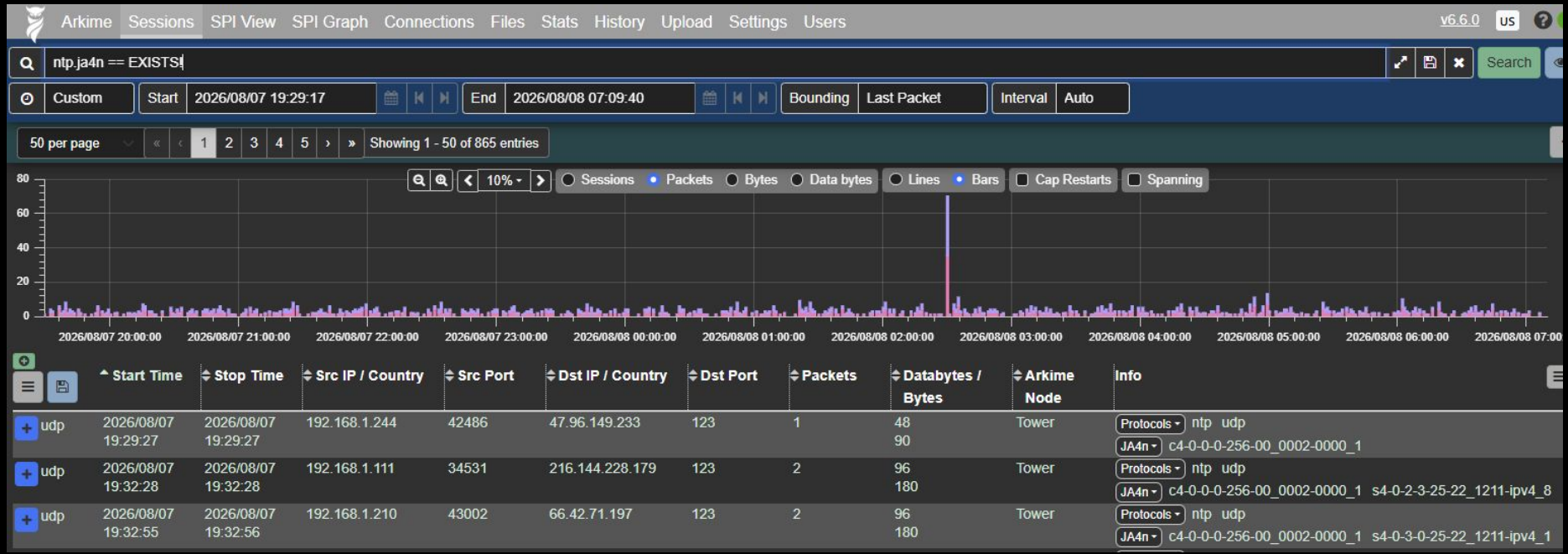
(not final)

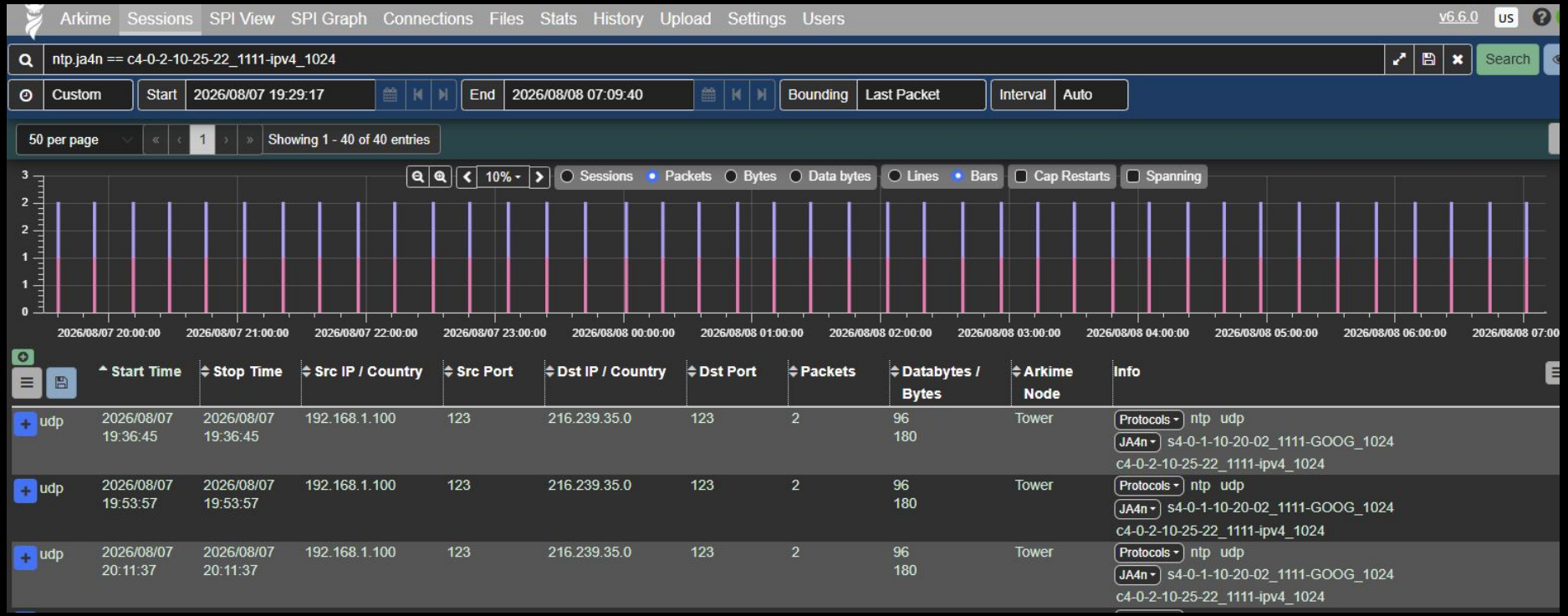
- Mode + Version
- Peering and Root Details
- Timestamps (0=0, 1=real time, 2=random time)



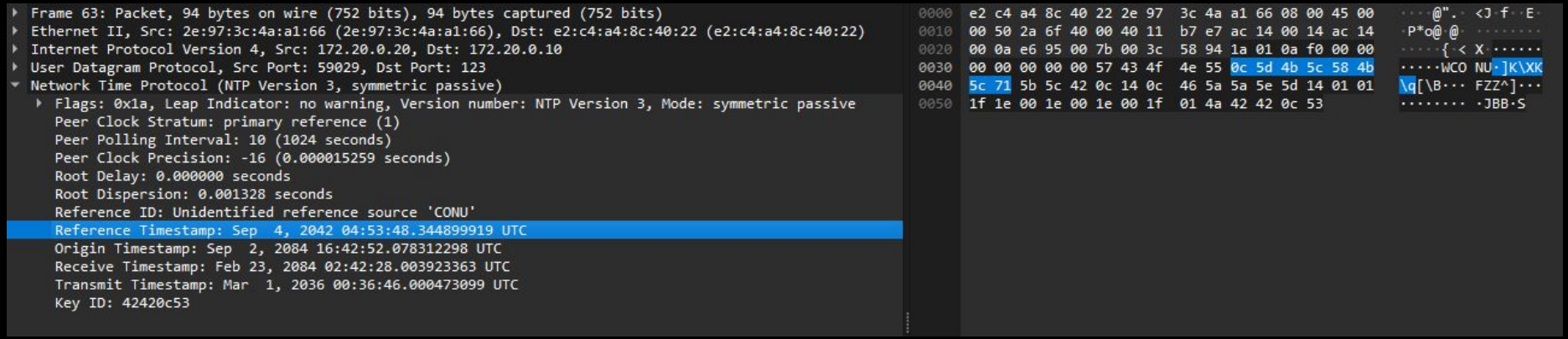
- Reference ID
- Polling Interval in seconds

Example JA4N Fingerprints	
OS / Device	**JA4N**
UnRAID (Slack)	c4-0-2-10-25-22_1111_ipv4_1024
Windows 11	c3-3-0-17-23-01_1001_0000_131072
Ubiquiti	c4-0-0-0-256-00_0002_0000_1
Tesla	c4-0-0-10-224-00_0002_0000_1024
Thermostat	c4-3-0-12-256-00_0001_0000_4096
Android	c3-0-0-0-256-00_0001_0000_1
AV Receiver	c4-3-0-3-6-11_0001_0000_8


Arkime
Sessions
SPI View
SPI Graph
Connections
Files
Stats
History
Upload
Settings
Users
v6.6.0
US
ntp.ja4n == EXISTS!
Search
Custom
Start
2026/08/07 19:29:17
End
2026/08/08 07:09:40
Bounding
Last Packet
Interval
Auto
50 per page
1
2
3
4
5
Showing 1 - 50 of 865 entries
10%
Sessions
Packets
Bytes
Data bytes
Lines
Bars
Cap Restarts
Spanning
80
60
40
20
0
2026/08/07 20:00:00
2026/08/07 21:00:00
2026/08/07 22:00:00
2026/08/07 23:00:00
2026/08/08 00:00:00
2026/08/08 01:00:00
2026/08/08 02:00:00
2026/08/08 03:00:00
2026/08/08 04:00:00
2026/08/08 05:00:00
2026/08/08 06:00:00
2026/08/08 07:00
Start Time
Stop Time
Src IP / Country
Src Port
Dst IP / Country
Dst Port
Packets
Databytes / Bytes
Arkime Node
Info
udp
2026/08/07 19:29:27
2026/08/07 19:29:27
192.168.1.244
42486
47.96.149.233
123
1
48
90
Tower
Protocols
ntp
udp
JA4n
c4-0-0-0-256-00_0002-0000_1
udp
2026/08/07 19:32:28
2026/08/07 19:32:28
192.168.1.111
34531
216.144.228.179
123
2
96
180
Tower
Protocols
ntp
udp
JA4n
c4-0-0-0-256-00_0002-0000_1
s4-0-2-3-25-22_1211-ipv4_8
udp
2026/08/07 19:32:55
2026/08/07 19:32:56
192.168.1.210
43002
66.42.71.197
123
2
96
180
Tower
Protocols
ntp
udp
JA4n
c4-0-0-0-256-00_0002-0000_1
s4-0-3-0-25-22_1211-ipv4_1


Arkime
Sessions
SPI View
SPI Graph
Connections
Files
Stats
History
Upload
Settings
Users
v6.6.0
US
ntp.ja4n == c4-0-2-10-25-22_1111-ipv4_1024
Search
Custom
Start
2026/08/07 19:29:17
End
2026/08/08 07:09:40
Bounding
Last Packet
Interval
Auto
50 per page
1
Showing 1 - 40 of 40 entries
10%
Sessions
Packets
Bytes
Data bytes
Lines
Bars
Cap Restarts
Spanning
3
2
2
1
1
0
2026/08/07 20:00:00
2026/08/07 21:00:00
2026/08/07 22:00:00
2026/08/07 23:00:00
2026/08/08 00:00:00
2026/08/08 01:00:00
2026/08/08 02:00:00
2026/08/08 03:00:00
2026/08/08 04:00:00
2026/08/08 05:00:00
2026/08/08 06:00:00
2026/08/08 07:00
Start Time
Stop Time
Src IP / Country
Src Port
Dst IP / Country
Dst Port
Packets
Databytes / Bytes
Arkime Node
Info
udp
2026/08/07 19:36:45
2026/08/07 19:36:45
192.168.1.100
123
216.239.35.0
123
2
96
180
Tower
Protocols
ntp
udp
JA4n
s4-0-1-10-20-02_1111-GOOG_1024
c4-0-2-10-25-22_1111-ipv4_1024
udp
2026/08/07 19:53:57
2026/08/07 19:53:57
192.168.1.100
123
216.239.35.0
123
2
96
180
Tower
Protocols
ntp
udp
JA4n
s4-0-1-10-20-02_1111-GOOG_1024
c4-0-2-10-25-22_1111-ipv4_1024
udp
2026/08/07 20:11:37
2026/08/07 20:11:37
192.168.1.100
123
216.239.35.0
123
2
96
180
Tower
Protocols
ntp
udp
JA4n
s4-0-1-10-20-02_1111-GOOG_1024
c4-0-2-10-25-22_1111-ipv4_1024

Covert Exfil



Covert Exfil

JA4N = c4-3-0-12-256-00_0001_0000_4096



Example JA4N Fingerprints	
OS / Device	**JA4N**
UnRAID (Slack)	c4-0-2-10-25-22_1111_ipv4_1024
Windows 11	c3-3-0-17-23-01_1001_0000_131072
Ubiquiti	c4-0-0-0-256-00_0002_0000_1
Tesla	c4-0-0-10-224-00_0002_0000_1024
Thermostat	c4-3-0-12-256-00_0001_0000_4096
Android	c3-0-0-0-256-00_0001_0000_1
AV Receiver	c4-3-0-3-6-11_0001_0000_8

Covert Exfil

JA4N = c4-3-0-12-256-00_0001_0000_4096

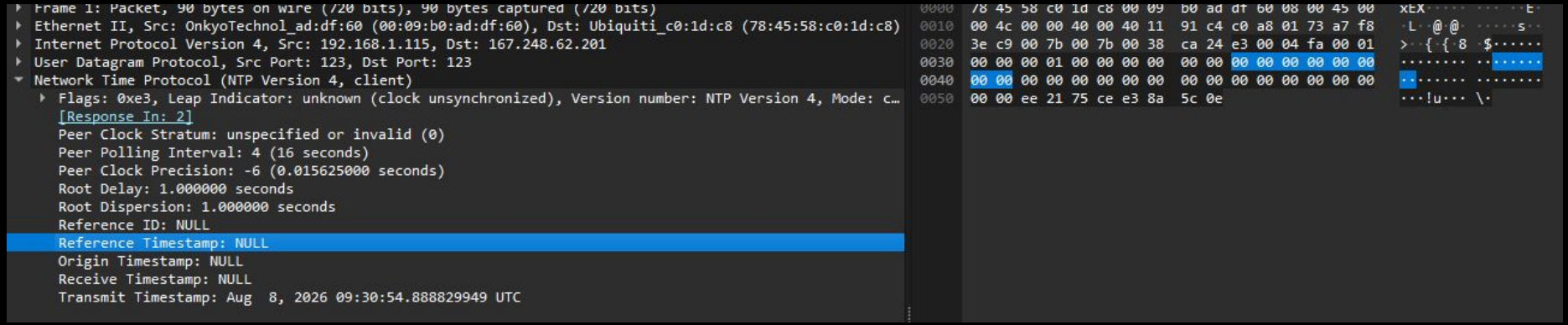


Covert Exfil

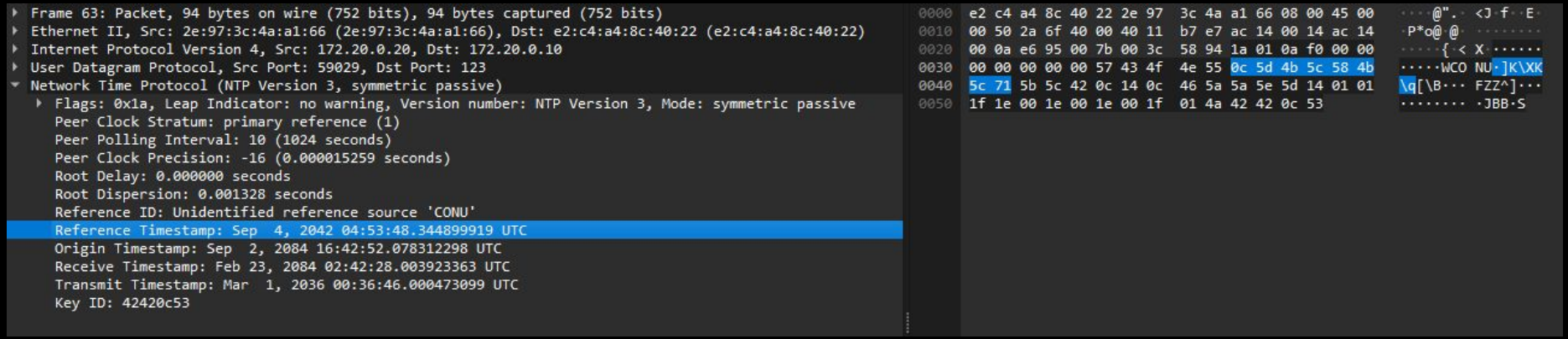
JA4N = c4-3-0-12-256-00_2222_ipv4_4096



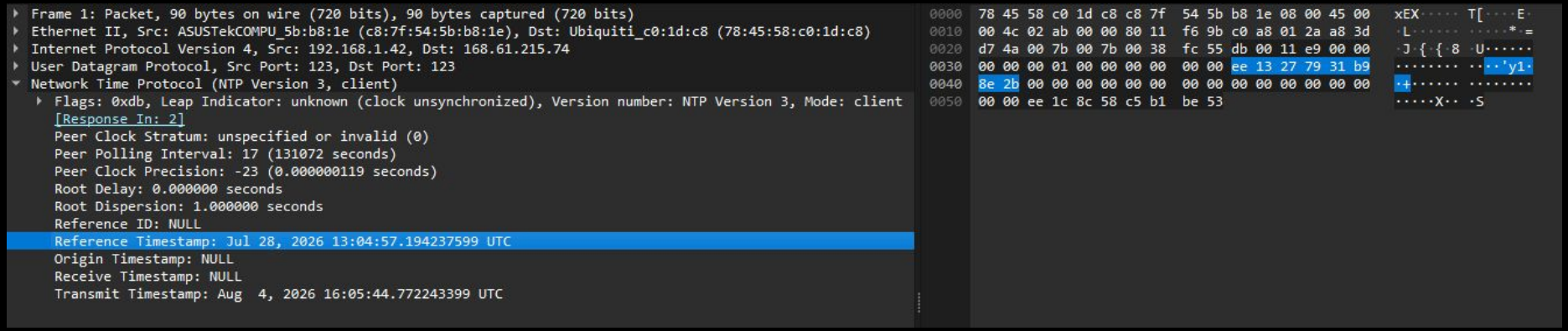
Covert Exfil



Covert Exfil



Tracking Systems



JA4X: X509 Fingerprint

(fingerprints how a cert is created)

CREDIT: W

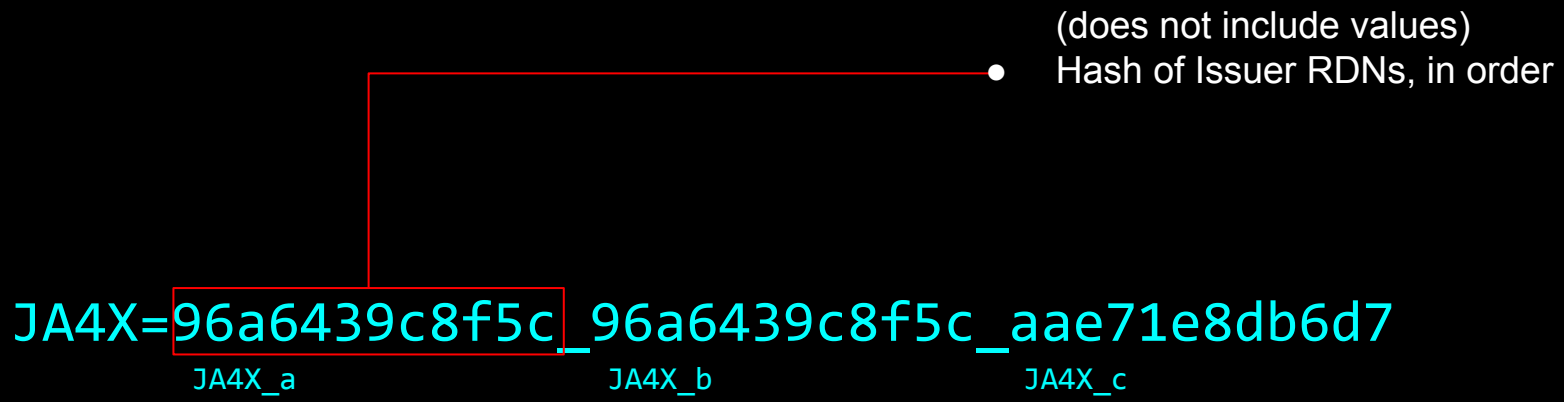
JA4X=96a6439c8f5c_96a6439c8f5c_aae71e8db6d7

JA4X_a JA4X_b JA4X_c

JA4X: X509 Fingerprint

(fingerprints how a cert is created)

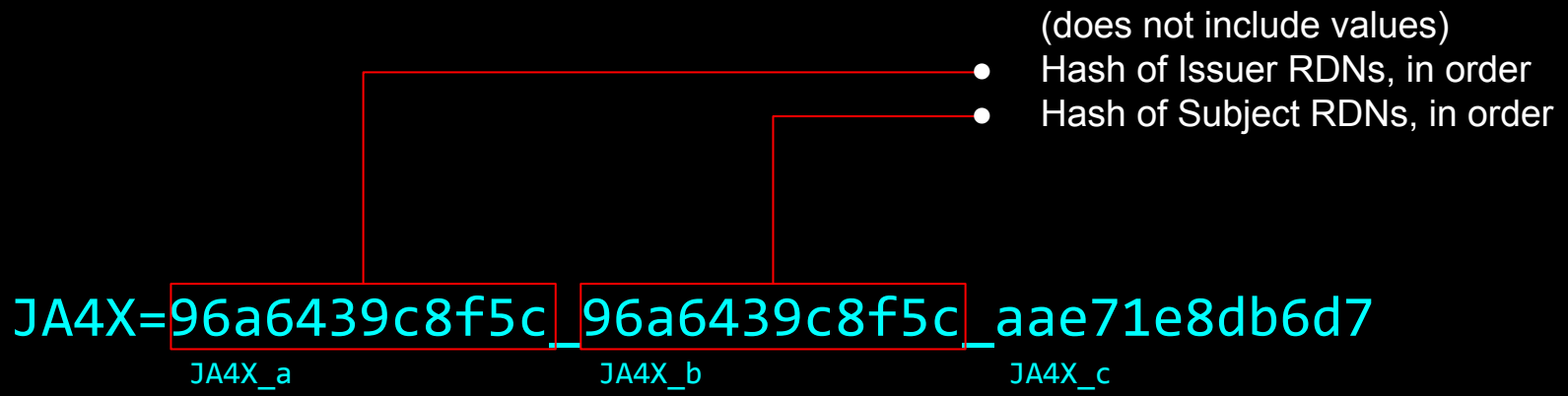
CREDIT: W



JA4X: X509 Fingerprint

(fingerprints how a cert is created)

CREDIT: W



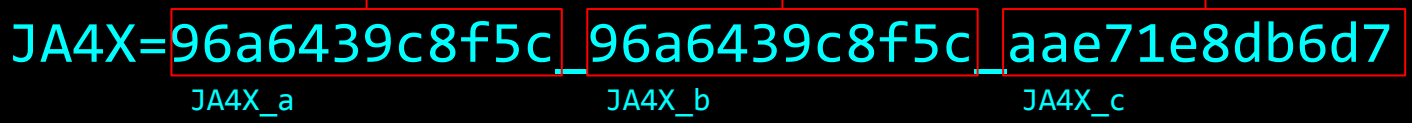
JA4X: X509 Fingerprint

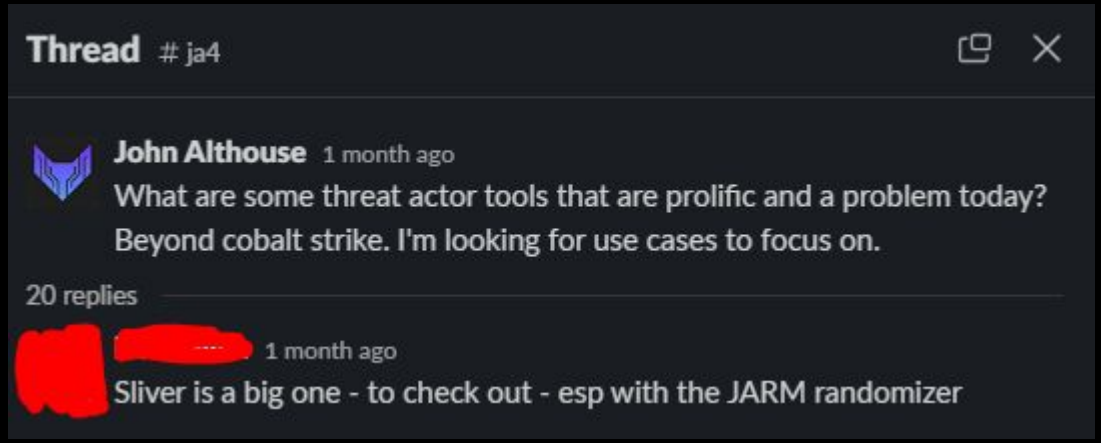
(fingerprints how a cert is created)

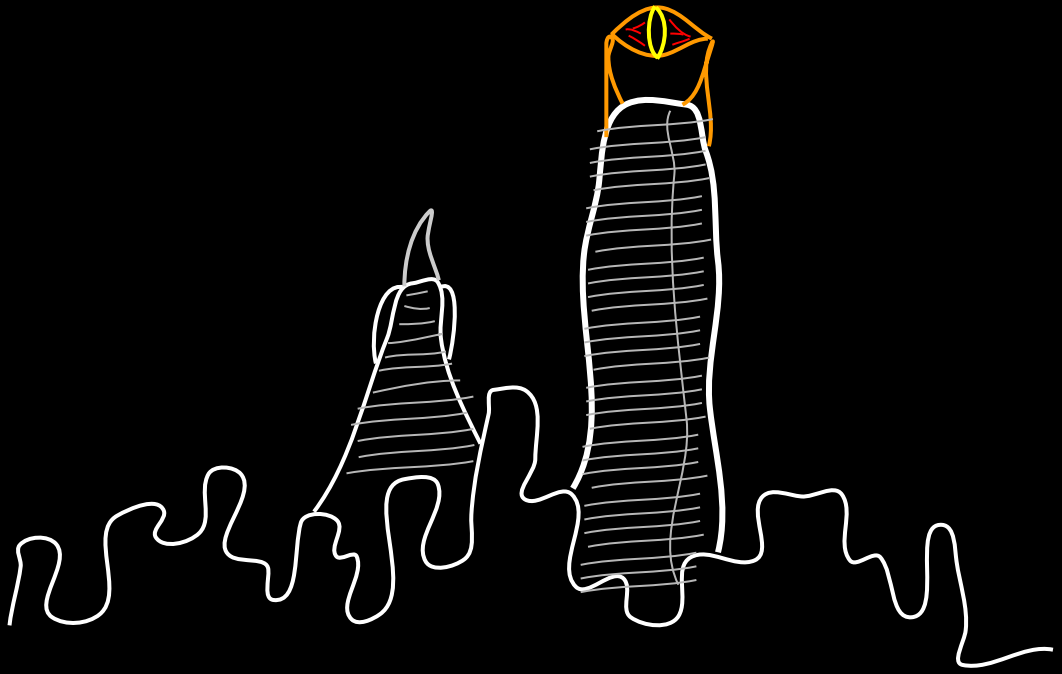
CREDIT: W

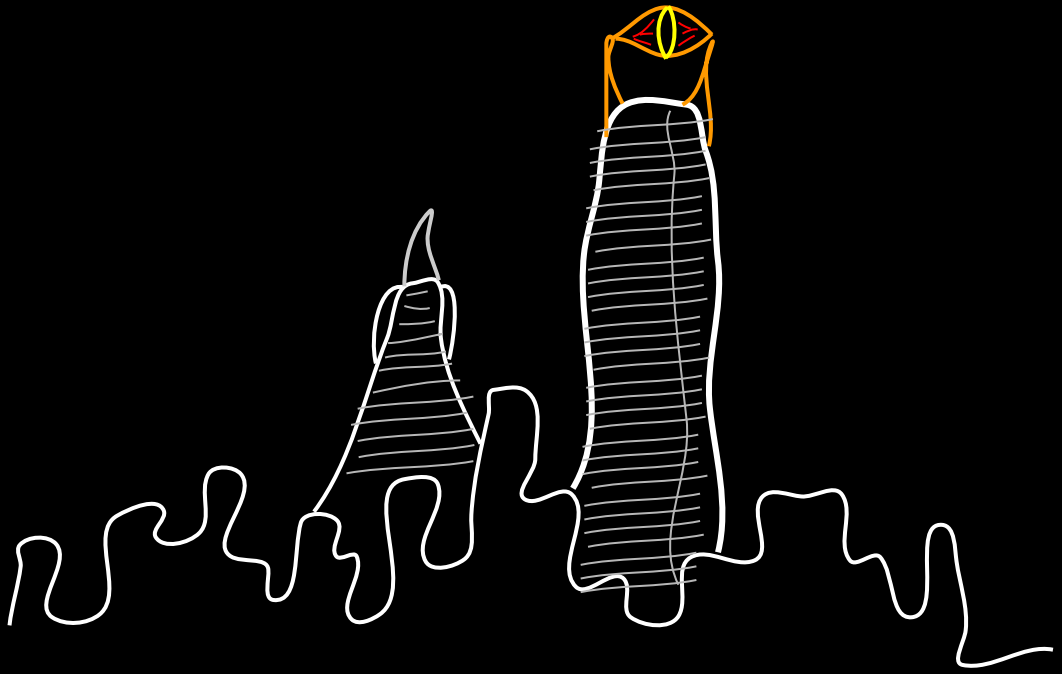
(does not include values)

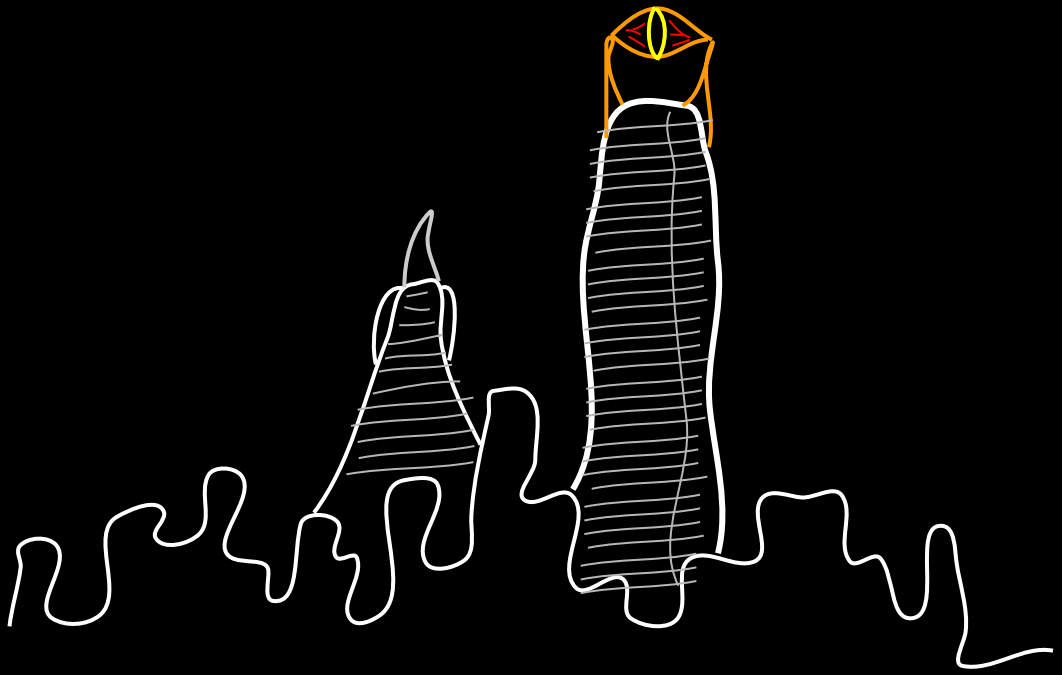
- Hash of Issuer RDNs, in order
- Hash of Subject RDNs, in order
- Hash of Extensions, in order



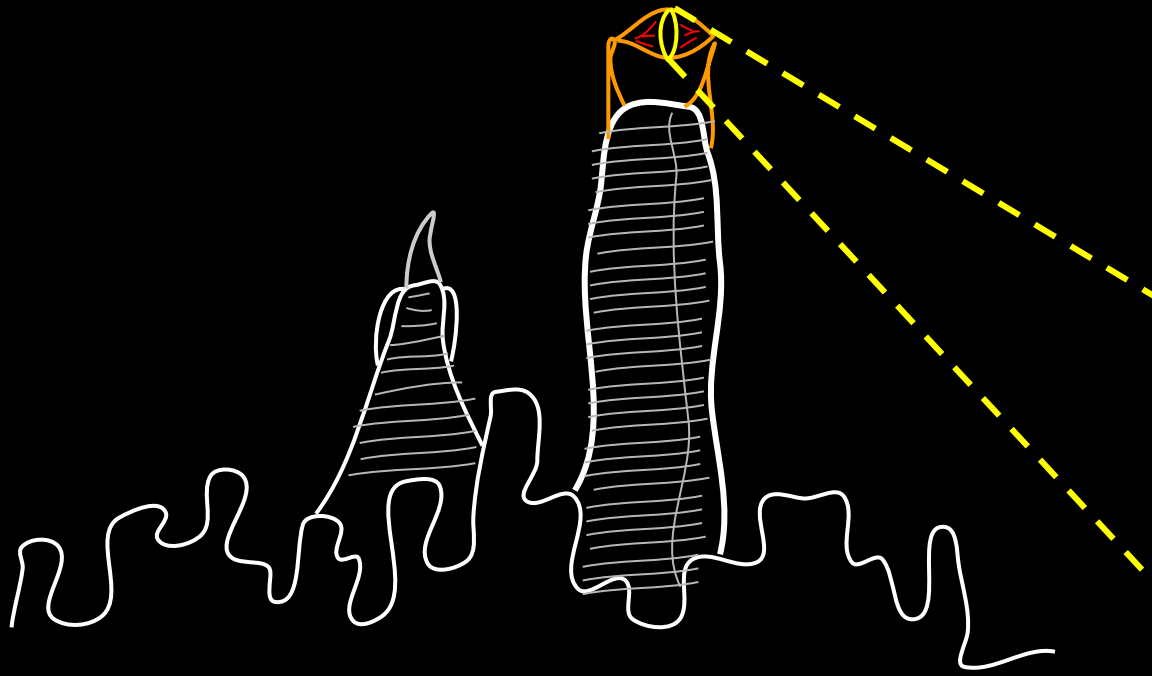

Thread # ja4
John Althouse 1 month ago
What are some threat actor tools that are prolific and a problem today? Beyond cobalt strike. I'm looking for use cases to focus on.
20 replies
[redacted] 1 month ago
Sliver is a big one - to check out - esp with the JARM randomizer



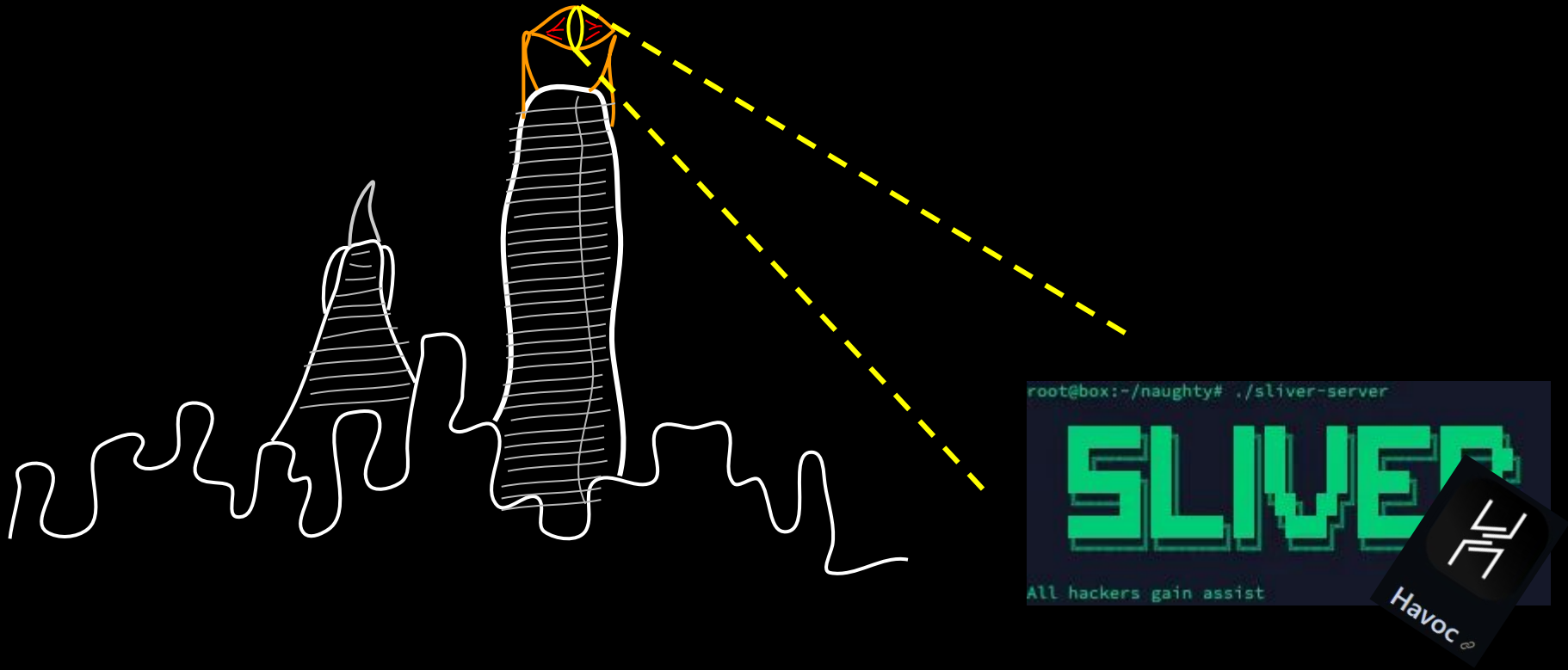





root@box:~/naughty# ./sliver-server
SLIVER
All hackers gain assist




root@box:~/naughty# ./sliver-server
SLIVER
All hackers gain assist


root@box:-/naughty# ./sliver-server
SLIVER
All hackers gain assist
Havoc

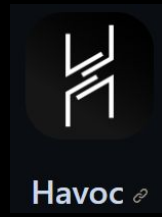
FOXIO

Sliver C2

```go
func randomSubject(commonName string) *pkix.Name {
	country, province, locale, street := randomProvinceLocalityStreetAddress()
	return &pkix.Name{
		Organization:  randomOrganization(),
		Country:       country,
		Province:      province,
		Locality:      locale,
		StreetAddress: street,
		PostalCode:    randomPostalCode(country),
		CommonName:    commonName,
	}
```

```go
func randomOrganization() []string {
	adjective, _ := codenames.RandomAdjective()
	noun, _ := codenames.RandomNoun()
	suffix := orgSuffixes[insecureRand.Intn(len(orgSuffixes))]

	var orgName string
	switch insecureRand.Intn(8) {
	case 0:
		orgName = strings.TrimSpace(fmt.Sprintf("%s %s, %s", adjective, noun, suffix))
	case 1:
		orgName = strings.TrimSpace(strings.ToLower(fmt.Sprintf("%s %s, %s", adjective, noun, suffix)))
	case 2:
		orgName = strings.TrimSpace(fmt.Sprintf("%s, %s", noun, suffix))
	case 3:
		orgName = strings.TrimSpace(strings.Title(fmt.Sprintf("%s %s, %s", adjective, noun, suffix)))
	case 4:
		orgName = strings.TrimSpace(strings.Title(fmt.Sprintf("%s %s", adjective, noun)))
	case 5:
		orgName = strings.TrimSpace(strings.ToLower(fmt.Sprintf("%s %s", adjective, noun)))
	case 6:
		orgName = strings.TrimSpace(strings.Title(fmt.Sprintf("%s", noun)))
	case 7:
		noun2, _ := codenames.RandomNoun()
		orgName = strings.TrimSpace(strings.ToLower(fmt.Sprintf("%s-%s", noun, noun2)))
	default:
		orgName = ""
```



Sliver (and Havoc) C2

ip		subjectOrganizationName	sha256	ja4x
99.79.189.27	443	mild fanlight	c6d50f752002cb2be8500db23ebd8fdf4b5ec631813d0a667e47c35e4107cda9	000000000000_4f24da86fad6_bf0f0589fc03
93.115.16.227	443	Blue Eel, Plc	ab6eb7b34ab1d9f7b522f3819d21211806686d42b04ff3acec8f91bee4f7e8f2	000000000000_7c32fa18c13e_bf0f0589fc03
93.115.16.227	443	Long	32d894ef187fb05cbbbdc4a81d8c44f38dfdd8ce96a333ff4ddb7d9bddfacf8f	000000000000_7c32fa18c13e_bf0f0589fc03
91.219.150.158	443	puny civilisation, corporation	5f5069810a65f72f532eb335105465684b5b0535bdf7c91c42072752f856427d	000000000000_7c32fa18c13e_bf0f0589fc03
91.219.148.57	443	Flexible Wrecker	7a71c5c87ea8b51efc3e32a5b191ec8dd5e998b1dad49680d94da0d9c7d03929	000000000000_7c32fa18c13e_bf0f0589fc03
91.219.148.57	443	ambitious sled, incorporated	1ac00bd2447932acecc8a484fec9b2b3b31d7d6da0472db1694d8eb57c598b98	000000000000_7c32fa18c13e_bf0f0589fc03
91.199.147.205	443	implicit timber, llc.	1c17a2e22ea29918d114a7ab8e9c842ec1cd178ffa37d6e3eda73fed34f22688	000000000000_7c32fa18c13e_bf0f0589fc03
89.147.110.79	443	kid, company	6940b9e6d727076306187ceedcc8178ab763e32a7bc4d1863dd052a99383931f	000000000000_7c32fa18c13e_bf0f0589fc03
88.119.170.136	443	horrible bifocals, ltd.	4b04321f07bb3d3b02959ed16228bba28f5645a7d577bfa740453df2a05adede	000000000000_7c32fa18c13e_bf0f0589fc03
81.200.149.183	443	cocoa, corp.	c187759d534a98d636c4417a0ec50c6a99aef586ba58638b7beddf36f1ca2d90	000000000000_7c32fa18c13e_bf0f0589fc03
8.210.232.186	443	Marvellous Hammer	fac43170fa414488f1a7676c764976ba7c1812616cbcdde9eaa8c595e7583250	000000000000_7c32fa18c13e_bf0f0589fc03
72.142.102.168	443	bizarre riverbed, plc.	03be6a8ec0af06496c42bba2b1a0dfd849d42ea6f9cd3401c5e4800220632ce7	000000000000_7c32fa18c13e_bf0f0589fc03
68.183.30.174	443	Trial	82b2f44f38a139eb9d285c38d0375a75b34253f4c420b4f9a1f5f555fda92522	000000000000_7c32fa18c13e_bf0f0589fc03
64.31.55.85	443	dutch line	2fe84780f825ee9012bd7ed01a731511bdc07c3cfc47fb86e041ac5e7ecae242	000000000000_7c32fa18c13e_bf0f0589fc03
64.227.17.174	443	Straightforward Nursery	9c29397f48d9cc4e090af48417618ee32ab74077651994a1203053b555592ea1	000000000000_7c32fa18c13e_bf0f0589fc03
64.225.109.152	8888	hot professional, plc	9af338cdf862047a3d9b89f8fc175485549e60cf2f39547ed1165fa509778d5a	000000000000_7c32fa18c13e_bf0f0589fc03
64.225.109.152	8443	delightful marketing, inc	836c2eda0476a97e85ec50ff19d9d530940faa48940b1576d6a2c95c4c28d00e	000000000000_7c32fa18c13e_bf0f0589fc03

Sliver (and Havoc) C2

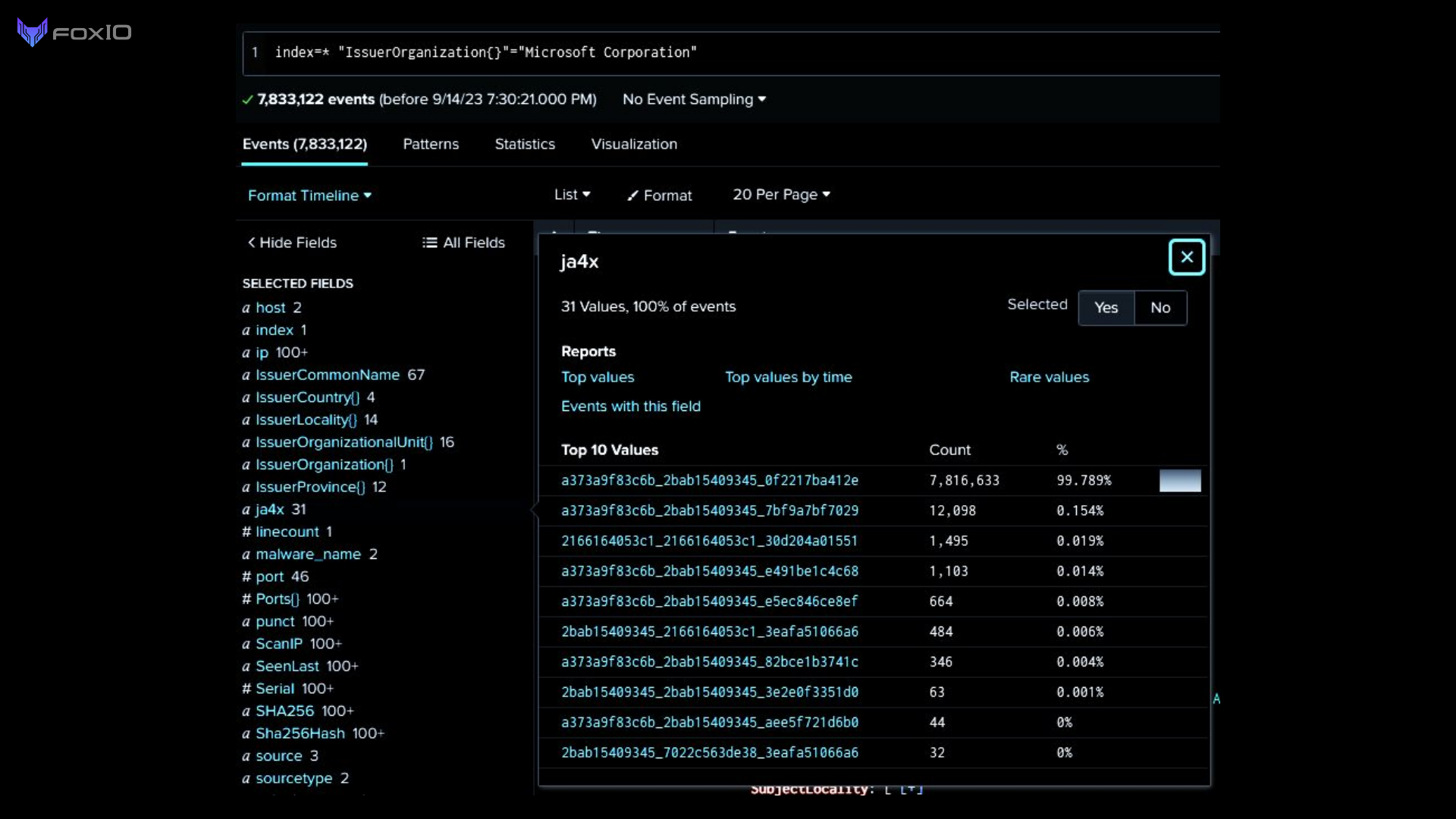
JA4X=000000000000_7c32fa18c13e_bf0f0589fc03
JA4X=000000000000_4f24da86fad6_bf0f0589fc03

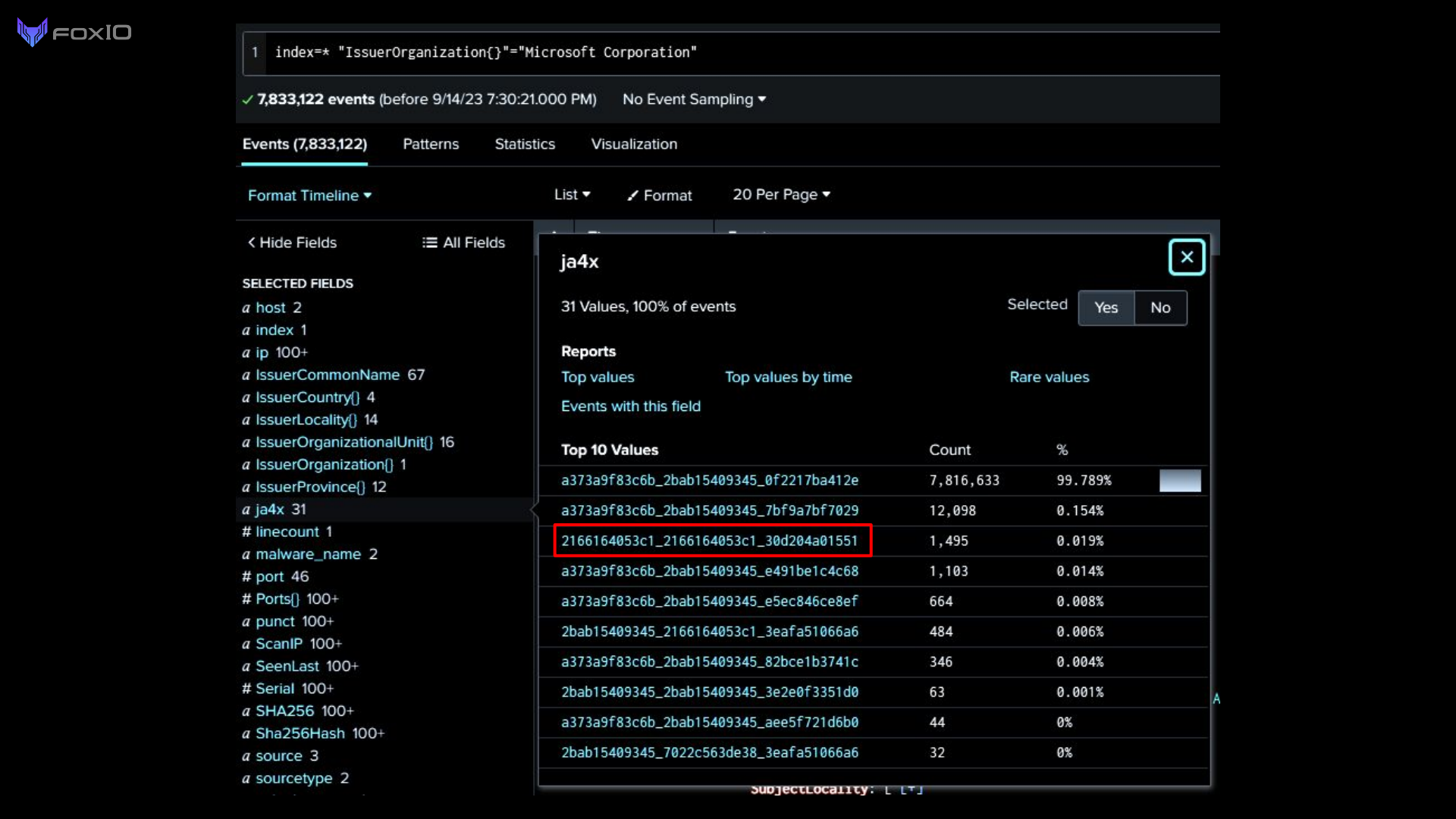
ip		subjectOrganizationName	sha256	ja4x
99.79.189.27	443	mild fanlight	c6d50f752002cb2be8500db23ebd8fdf4b5ec631813d0a667e47c35e4107cda9	000000000000_4f24da86fad6_bf0f0589fc03
93.115.16.227	443	Blue Eel, Plc	ab6eb7b34ab1d9f7b522f3819d21211806686d42b04ff3acec8f91bee4f7e8f2	000000000000_7c32fa18c13e_bf0f0589fc03
93.115.16.227	443	Long	32d894ef187fb05cbbbdc4a81d8c44f38dfdd8ce96a333ff4ddb7d9bddfacf8f	000000000000_7c32fa18c13e_bf0f0589fc03
91.219.150.158	443	puny civilisation, corporation	5f5069810a65f72f532eb335105465684b5b0535bdf7c91c42072752f856427d	000000000000_7c32fa18c13e_bf0f0589fc03
91.219.148.57	443	Flexible Wrecker	7a71c5c87ea8b51efc3e32a5b191ec8dd5e998b1dad49680d94da0d9c7d03929	000000000000_7c32fa18c13e_bf0f0589fc03
91.219.148.57	443	ambitious sled, incorporated	1ac00bd2447932acecc8a484fec9b2b3b31d7d6da0472db1694d8eb57c598b98	000000000000_7c32fa18c13e_bf0f0589fc03
91.199.147.205	443	implicit timber, llc.	1c17a2e22ea29918d114a7ab8e9c842ec1cd178ffa37d6e3eda73fed34f22688	000000000000_7c32fa18c13e_bf0f0589fc03
89.147.110.79	443	kid, company	6940b9e6d727076306187ceedcc8178ab763e32a7bc4d1863dd052a99383931f	000000000000_7c32fa18c13e_bf0f0589fc03
88.119.170.136	443	horrible bifocals, ltd.	4b04321f07bb3d3b02959ed16228bba28f5645a7d577bfa740453df2a05adede	000000000000_7c32fa18c13e_bf0f0589fc03
81.200.149.183	443	cocoa, corp.	c187759d534a98d636c4417a0ec50c6a99aef586ba58638b7beddf36f1ca2d90	000000000000_7c32fa18c13e_bf0f0589fc03
8.210.232.186	443	Marvellous Hammer	fac43170fa414488f1a7676c764976ba7c1812616cbcdde9eaa8c595e7583250	000000000000_7c32fa18c13e_bf0f0589fc03
72.142.102.168	443	bizarre riverbed, plc.	03be6a8ec0af06496c42bba2b1a0dfd849d42ea6f9cd3401c5e4800220632ce7	000000000000_7c32fa18c13e_bf0f0589fc03
68.183.30.174	443	Trial	82b2f44f38a139eb9d285c38d0375a75b34253f4c420b4f9a1f5f555fda92522	000000000000_7c32fa18c13e_bf0f0589fc03
64.31.55.85	443	dutch line	2fe84780f825ee9012bd7ed01a731511bdc07c3cfc47fb86e041ac5e7ecae242	000000000000_7c32fa18c13e_bf0f0589fc03
64.227.17.174	443	Straightforward Nursery	9c29397f48d9cc4e090af48417618ee32ab74077651994a1203053b555592ea1	000000000000_7c32fa18c13e_bf0f0589fc03
64.225.109.152	8888	hot professional, plc	9af338cdf862047a3d9b89f8fc175485549e60cf2f39547ed1165fa509778d5a	000000000000_7c32fa18c13e_bf0f0589fc03
64.225.109.152	8443	delightful marketing, inc	836c2eda0476a97e85ec50ff19d9d530940faa48940b1576d6a2c95c4c28d00e	000000000000_7c32fa18c13e_bf0f0589fc03

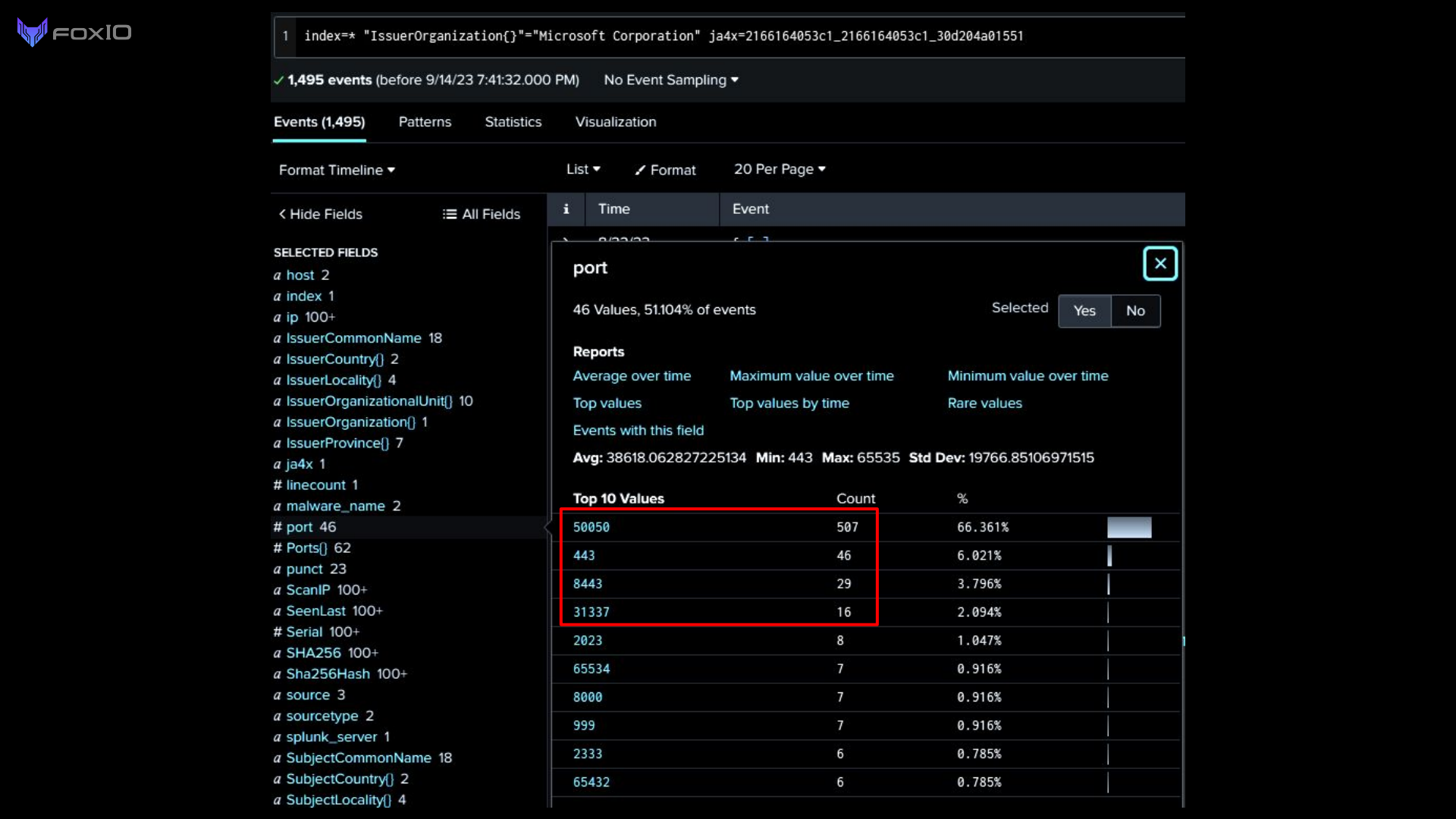
Sliver (and Havoc) C2

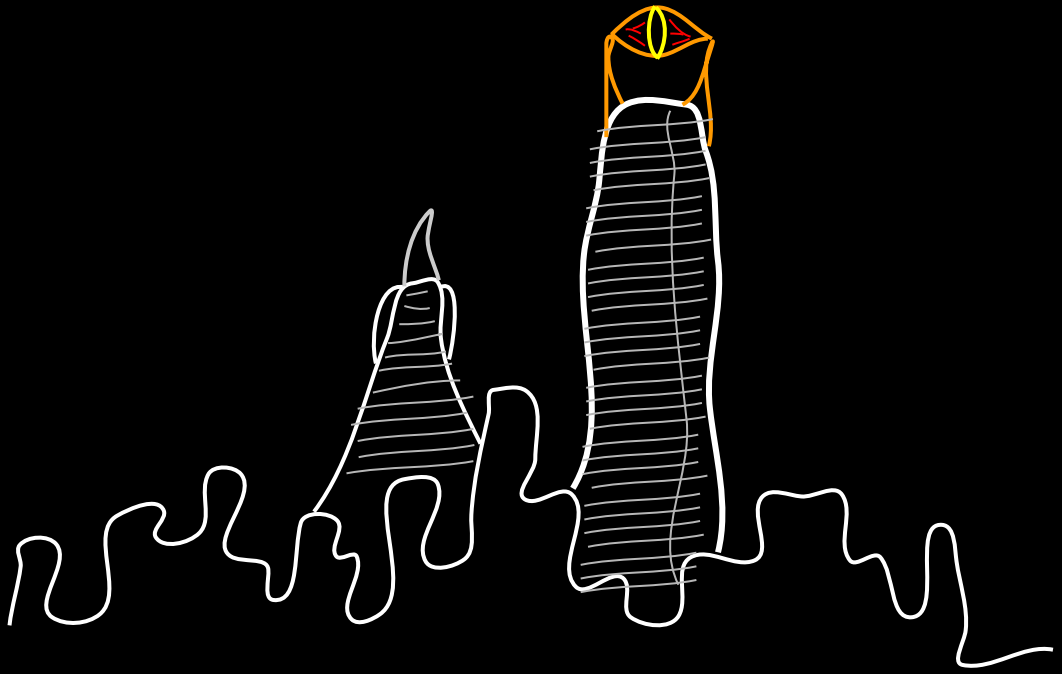
JA4X=000000000000_7c32fa18c13e_bf0f0589fc03
JA4X=000000000000_4f24da86fad6_bf0f0589fc03

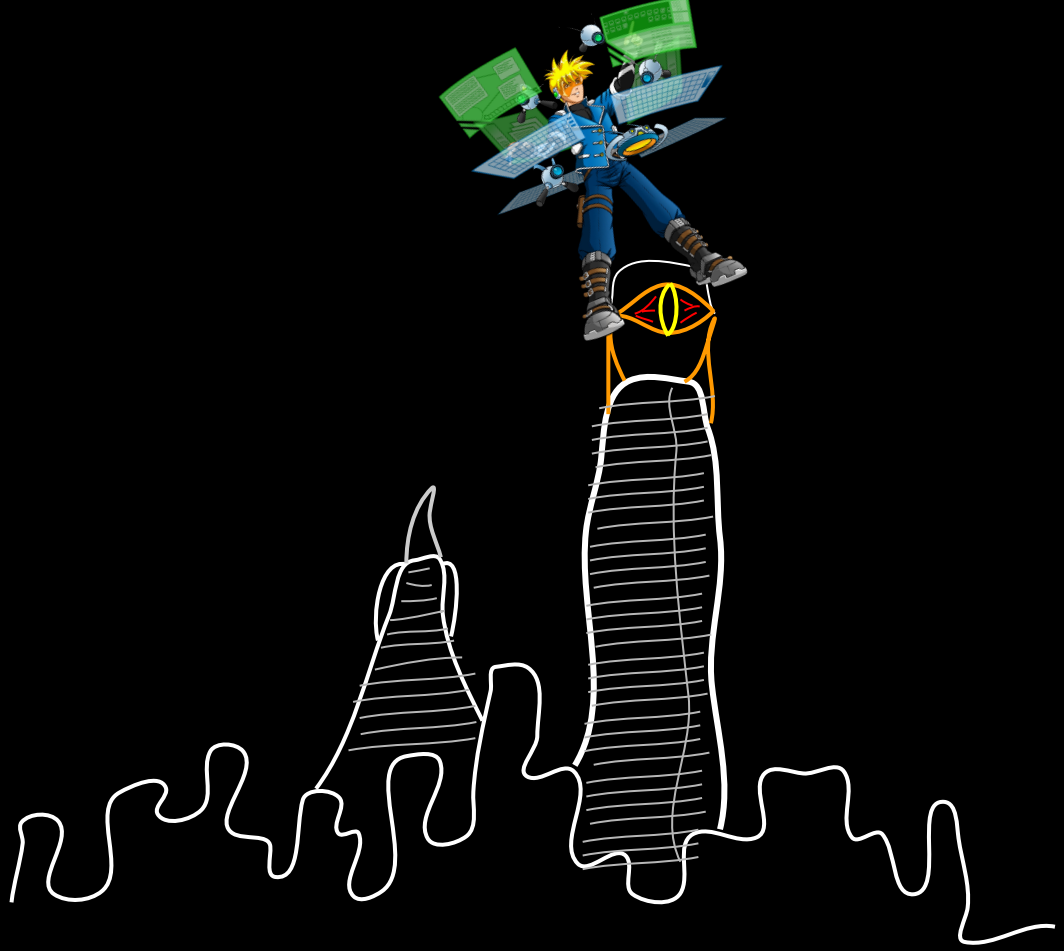
Sliver C2 List Identified from JA4X Internet Scan Sept. 9th 2023 (this is not a full list, just a small excerpt for example purposes)	
IP Address	**Domain**
81.200.149.183	1293195-ci21745.tw1.ru
99.79.189.27	mobile-atrf.com
64.225.109.152	staging.cupid.blunun.com
46.148.26.88	microsoft.com.updatenetworksinfo.com
45.32.120.18	hlakgabiugalibafnafadsfapian.micsoft.org
35.89.230.67	remote.install-update.zip, apex.ca-utilities.com
34.29.188.70	fareharbor.praetorian-assessment.xyz
188.127.231.180	deniszeleniy.ru
185.34.52.140	prefetch.lnrgov.info
185.25.51.144	mirror-server-ubuntu.com
18.168.121.23	walbridgefinancial.com
176.123.1.144	mol.stoerte.net
93.115.16.227	off-tube.lol
172.96.137.224	americajobmail.site
118.195.148.41	[no domain]
118.195.214.195	[no domain]
118.195.128.2	[no domain]
172.176.103.110	llama.punchcyber.com
167.172.228.48	hide.monster
167.114.115.246	aenabasil.com.br

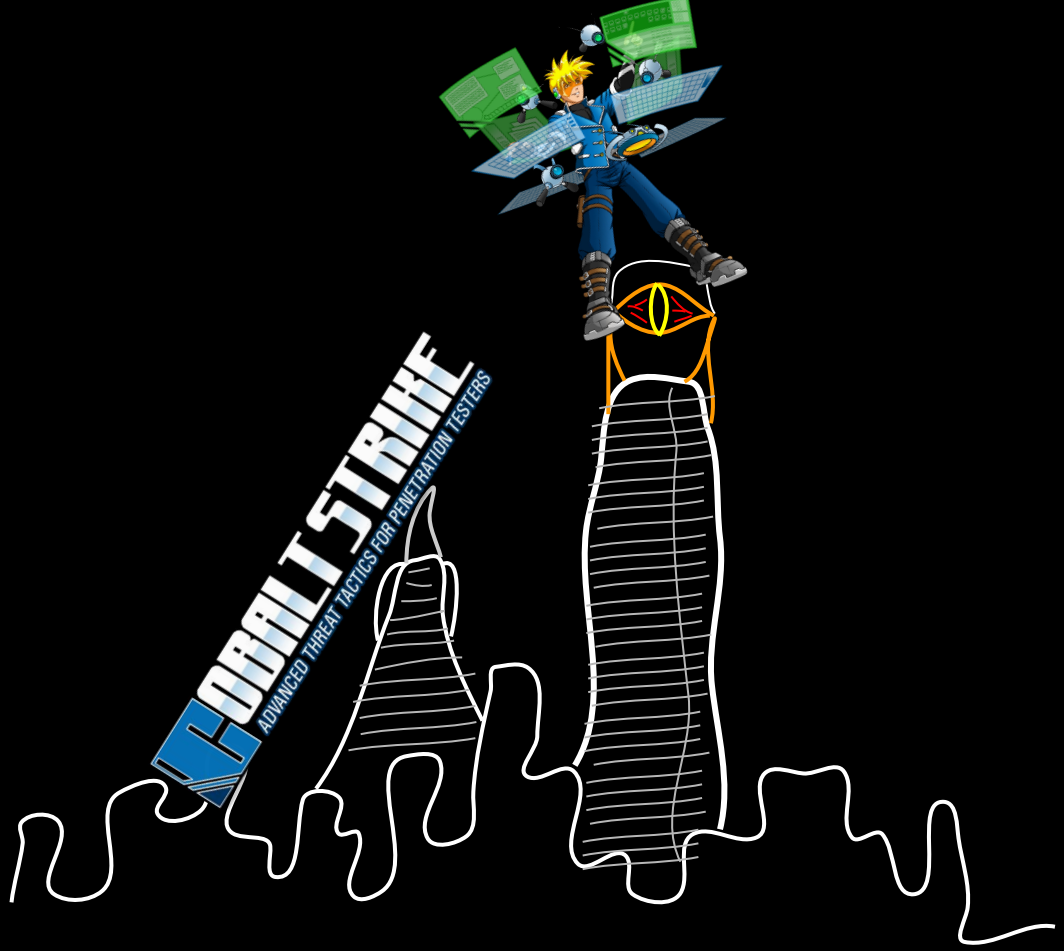

1 index=* "IssuerOrganization{}"="Microsoft Corporation"
✓ 7,833,122 events (before 9/14/23 7:30:21.000 PM) No Event Sampling
Events (7,833,122) Patterns Statistics Visualization
Format Timeline List Format 20 Per Page
Hide Fields All Fields
SELECTED FIELDS
a host 2
a index 1
a ip 100+
a IssuerCommonName 67
a IssuerCountry{} 4
a IssuerLocality{} 14
a IssuerOrganizationalUnit{} 16
a IssuerOrganization{} 1
a IssuerProvince{} 12
a ja4x 31
linecount 1
a malware_name 2
port 46
Ports{} 100+
a punct 100+
a ScanIP 100+
a SeenLast 100+
Serial 100+
a SHA256 100+
a Sha256Hash 100+
a source 3
a sourcetype 2
ja4x
31 Values, 100% of events
Selected Yes No
Reports
Top values Top values by time Rare values
Events with this field
Top 10 Values Count %
a373a9f83c6b_2bab15409345_0f2217ba412e 7,816,633 99.789%
a373a9f83c6b_2bab15409345_7bf9a7bf7029 12,098 0.154%
2166164053c1_2166164053c1_30d204a01551 1,495 0.019%
a373a9f83c6b_2bab15409345_e491be1c4c68 1,103 0.014%
a373a9f83c6b_2bab15409345_e5ec846ce8ef 664 0.008%
2bab15409345_2166164053c1_3eafa51066a6 484 0.006%
a373a9f83c6b_2bab15409345_82bce1b3741c 346 0.004%
2bab15409345_2bab15409345_3e2e0f3351d0 63 0.001%
a373a9f83c6b_2bab15409345_aee5f721d6b0 44 0%
2bab15409345_7022c563de38_3eafa51066a6 32 0%


FOXIO
1 index=* "IssuerOrganization{}"="Microsoft Corporation"
✓ 7,833,122 events (before 9/14/23 7:30:21.000 PM) No Event Sampling
Events (7,833,122) Patterns Statistics Visualization
Format Timeline List Format 20 Per Page
Hide Fields All Fields
SELECTED FIELDS
a host 2
a index 1
a ip 100+
a IssuerCommonName 67
a IssuerCountry{} 4
a IssuerLocality{} 14
a IssuerOrganizationalUnit{} 16
a IssuerOrganization{} 1
a IssuerProvince{} 12
a ja4x 31
linecount 1
a malware_name 2
port 46
Ports{} 100+
a punct 100+
a ScanIP 100+
a SeenLast 100+
Serial 100+
a SHA256 100+
a Sha256Hash 100+
a source 3
a sourcetype 2
ja4x
31 Values, 100% of events
Selected Yes No
Reports
Top values Top values by time Rare values
Events with this field
Top 10 Values Count %
a373a9f83c6b_2bab15409345_0f2217ba412e 7,816,633 99.789%
a373a9f83c6b_2bab15409345_7bf9a7bf7029 12,098 0.154%
2166164053c1_2166164053c1_30d204a01551 1,495 0.019%
a373a9f83c6b_2bab15409345_e491be1c4c68 1,103 0.014%
a373a9f83c6b_2bab15409345_e5ec846ce8ef 664 0.008%
2bab15409345_2166164053c1_3eafa51066a6 484 0.006%
a373a9f83c6b_2bab15409345_82bce1b3741c 346 0.004%
2bab15409345_2bab15409345_3e2e0f3351d0 63 0.001%
a373a9f83c6b_2bab15409345_aee5f721d6b0 44 0%
2bab15409345_7022c563de38_3eafa51066a6 32 0%
SubjectLocality: [[+]


1 index=* "IssuerOrganization{}"="Microsoft Corporation" ja4x=2166164053c1_2166164053c1_30d204a01551
1,495 events (before 9/14/23 7:41:32.000 PM) No Event Sampling
Events (1,495) Patterns Statistics Visualization
Format Timeline List Format 20 Per Page
Hide Fields All Fields
SELECTED FIELDS
a host 2
a index 1
a ip 100+
a IssuerCommonName 18
a IssuerCountry{} 2
a IssuerLocality{} 4
a IssuerOrganizationalUnit{} 10
a IssuerOrganization{} 1
a IssuerProvince{} 7
a ja4x 1
linecount 1
a malware_name 2
port 46
Ports{} 62
a punct 23
a ScanIP 100+
a SeenLast 100+
Serial 100+
a SHA256 100+
a Sha256Hash 100+
a source 3
a sourcetype 2
a splunk_server 1
a SubjectCommonName 18
a SubjectCountry{} 2
a SubjectLocality{} 4
i Time Event
port
46 Values, 51.104% of events
Selected Yes No
Reports
Average over time Maximum value over time Minimum value over time
Top values Top values by time Rare values
Events with this field
Avg: 38618.062827225134 Min: 443 Max: 65535 Std Dev: 19766.85106971515
Top 10 Values Count %
50050 507 66.361%
443 46 6.021%
8443 29 3.796%
31337 16 2.094%
2023 8 1.047%
65534 7 0.916%
8000 7 0.916%
999 7 0.916%
2333 6 0.785%
65432 6 0.785%






COBALT STRIKE
ADVANCED THREAT TACTICS FOR PENETRATION TESTERS



THREAT RESEARCH

Chinese Threat Actor Used Modified Cobalt Strike Variant to Attack Taiwanese Critical Infrastructure

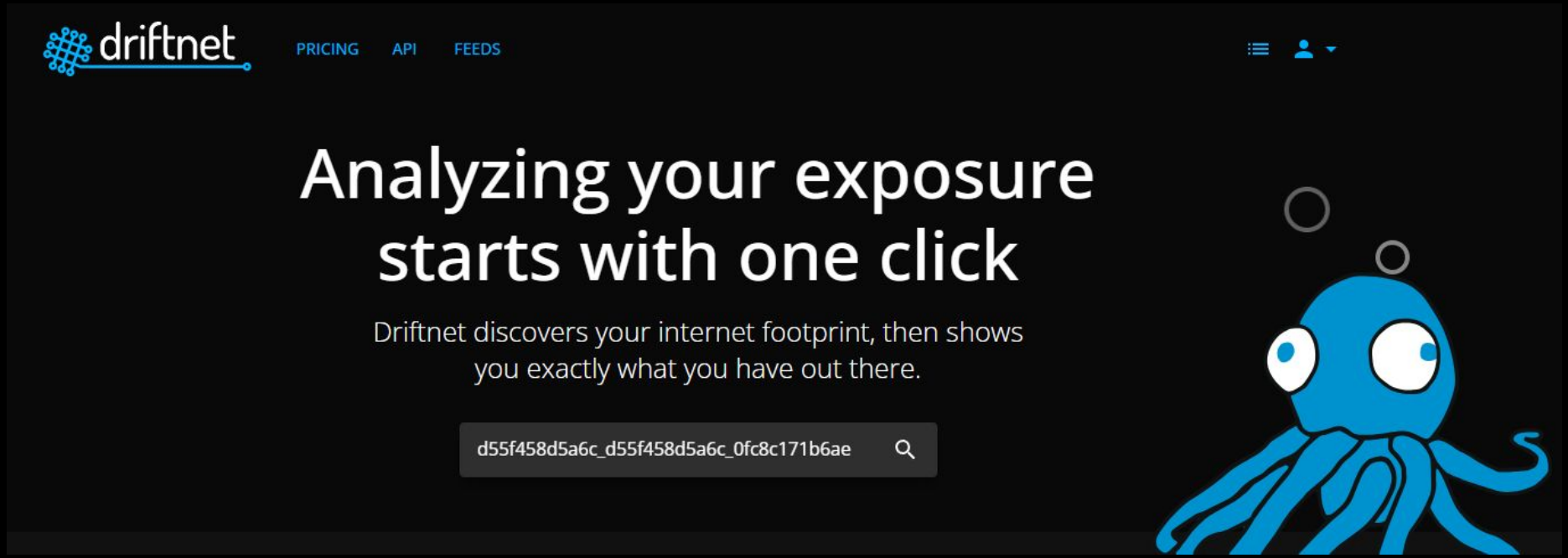
EclecticIQ researchers identified a malicious web server very likely operated by a Chinese threat actor used to target Taiwanese government entities, including critical infrastructure.

Arda Büyükkaya – June 2, 2023

FOXIO

SoftEther VPN

JA4X=d55f458d5a6c_d55f458d5a6c_0fc8c171b6ae



SoftEther VPN

JA4X=d55f458d5a6c_d55f458d5a6c_0fc8c171b6ae

Date (UTC)	IP	Port	Hosting Entity	Signature	Search Term	TLS	Service
2023-10-23	8.210.193.124	tcp/5555	Alibaba (US) Technology Co., Ltd.	—	d55f458d5a6c_d55f458d5a6c_0fc8c	Self-Signed	http
2023-10-23	43.134.78.141	tcp/443	Tencent Building, Kejizhongyi Avenu	—	d55f458d5a6c_d55f458d5a6c_0fc8c	Self-Signed	http
2023-10-23	174.128.250.222	tcp/992	SHARKTECH	SoftEther VPN httpd	d55f458d5a6c_d55f458d5a6c_0fc8c	Self-Signed	http
2023-10-23	82.65.129.251	tcp/5555	Proxad / Free SAS	—	d55f458d5a6c_d55f458d5a6c_0fc8c	Self-Signed	http
2023-10-23	202.29.177.250	tcp/443	Office of the basic education comm	—	d55f458d5a6c_d55f458d5a6c_0fc8c	Self-Signed	http
2023-10-23	222.133.35.38	tcp/5555	CHINA UNICOM China169 Backbon	—	d55f458d5a6c_d55f458d5a6c_0fc8c	Self-Signed	http
2023-10-23	204.188.219.239	tcp/5555	SHARKTECH INC	SoftEther VPN httpd	d55f458d5a6c_d55f458d5a6c_0fc8c	Self-Signed	http
2023-10-23	109.195.227.177	tcp/1723	JSC "ER-Telecom Holding" Rostov-na	SoftEther VPN httpd	d55f458d5a6c_d55f458d5a6c_0fc8c	Self-Signed	http
2023-10-23	95.154.199.38	tcp/992	IPSERVER WORLD LTD	SoftEther VPN httpd	d55f458d5a6c_d55f458d5a6c_0fc8c	Self-Signed	http
2023-10-23	174.128.247.153	tcp/443	SHARKTECH	SoftEther VPN httpd	d55f458d5a6c_d55f458d5a6c_0fc8c	Self-Signed	http
2023-10-23	193.77.158.253	tcp/5555	SiOL d.o.o. (Slovenia Online)	—	d55f458d5a6c_d55f458d5a6c_0fc8c	Self-Signed	http
2023-10-23	43.154.126.191	tcp/443	Tencent Building, Kejizhongyi Avenu	—	d55f458d5a6c_d55f458d5a6c_0fc8c	Self-Signed	http
2023-10-23	43.134.26.119	tcp/443	Tencent Building, Kejizhongyi Avenu	—	d55f458d5a6c_d55f458d5a6c_0fc8c	Self-Signed	http
2023-10-23	2.136.131.22	tcp/5555	Telefonica_de_Espana	SoftEther VPN httpd	d55f458d5a6c_d55f458d5a6c_0fc8c	Self-Signed	http
2023-10-23	110.50.97.138	tcp/5555	GreenNet Co.,Ltd.	—	d55f458d5a6c_d55f458d5a6c_0fc8c	Self-Signed	http
2023-10-23	101.32.102.74	tcp/888	Tencent Building, Kejizhongyi Avenu	—	d55f458d5a6c_d55f458d5a6c_0fc8c	Self-Signed	http
2023-10-23	8.212.20.14	tcp/443	Alibaba (US) Technology Co., Ltd.	—	d55f458d5a6c_d55f458d5a6c_0fc8c	Self-Signed	http
2023-10-23	152.32.202.89	tcp/443	UCLOUD INFORMATION TECHNOLC	—	d55f458d5a6c_d55f458d5a6c_0fc8c	Self-Signed	http
2023-10-23	109.167.10.226	tcp/5555	Airenetworks	—	d55f458d5a6c_d55f458d5a6c_0fc8c	Self-Signed	http
2023-10-23	118.121.202.186	tcp/5555	CHINANET SiChuan Telecom Interne	—	d55f458d5a6c_d55f458d5a6c_0fc8c	Self-Signed	http
2023-10-23	61.141.202.37	tcp/992	No.31,Jin-rong Street	SoftEther VPN httpd	d55f458d5a6c_d55f458d5a6c_0fc8c	Self-Signed	http
2023-10-23	220.163.124.244	tcp/1194	Internet-Bar in CHINANET YunNan p	—	d55f458d5a6c_d55f458d5a6c_0fc8c	Self-Signed	http
2023-10-23	178.254.35.159	tcp/443	1Blu 178.254.32.0/22	—	d55f458d5a6c_d55f458d5a6c_0fc8c	Self-Signed	http
2023-10-23	76.183.113.219	tcp/443	TWC-11427-TEXAS	—	d55f458d5a6c_d55f458d5a6c_0fc8c	Self-Signed	http
2023-10-23	115.126.43.14	tcp/5555	Forewin Telecom Group Limited, ISI	—	d55f458d5a6c_d55f458d5a6c_0fc8c	Self-Signed	http

Metasploit

JA4X=2bab15409345_2bab15409345_75f1b0fafedd

Date (UTC)	IP	Port	Hosting Entity	Signature	Search Term	Banner	TLS
2023-10-23	54.254.91.191	tcp/3790	AMAZON-02	nginx without version info	2bab15409345_2bab15409345_75f1b0fafedd	nginx	Self-Signed
2023-10-23	1.15.186.229	tcp/3790	Shenzhen Tencent Comp	nginx without version info	2bab15409345_2bab15409345_75f1b0fafedd	nginx	Self-Signed
2023-10-23	103.6.238.33	tcp/3790	CX2 Computer Exchange	nginx without version info	2bab15409345_2bab15409345_75f1b0fafedd	nginx	Self-Signed
2023-10-23	154.215.23.173	tcp/3790	HK Qianlong Technology	Metasploit Pro (and Commu	2bab15409345_2bab15409345_75f1b0fafedd	nginx	Self-Signed
2023-10-23	149.202.167.171	tcp/3790	OVH Technical Contact	nginx without version info	2bab15409345_2bab15409345_75f1b0fafedd	nginx	Self-Signed
2023-10-23	103.113.71.74	tcp/3790	Stark Industries Solutions	nginx without version info	2bab15409345_2bab15409345_75f1b0fafedd	nginx	Self-Signed
2023-10-23	154.215.19.186	tcp/3790	HK Qianlong Technology	Metasploit Pro (and Commu	2bab15409345_2bab15409345_75f1b0fafedd	nginx	Self-Signed
2023-10-23	107.174.69.212	tcp/6553	CC-107-174-69-0-24	Metasploit Pro (and Commu	2bab15409345_2bab15409345_75f1b0fafedd	nginx	Self-Signed
2023-10-23	154.215.23.163	tcp/3790	HK Qianlong Technology	nginx without version info	2bab15409345_2bab15409345_75f1b0fafedd	nginx	Self-Signed
2023-10-23	139.196.124.207	tcp/6667	Hangzhou Alibaba Advert	nginx without version info	2bab15409345_2bab15409345_75f1b0fafedd	nginx	Self-Signed
2023-10-23	45.159.248.56	tcp/3790	Stark Industries Solutions	nginx without version info	2bab15409345_2bab15409345_75f1b0fafedd	nginx	Self-Signed
2023-10-23	207.180.201.51	tcp/3790	CONTABO	nginx without version info	2bab15409345_2bab15409345_75f1b0fafedd	nginx	Self-Signed
2023-10-23	178.236.246.115	tcp/3790	Aeza Network	nginx without version info	2bab15409345_2bab15409345_75f1b0fafedd	nginx	Self-Signed
2023-10-23	154.215.22.166	tcp/3790	HK Qianlong Technology	Metasploit Pro (and Commu	2bab15409345_2bab15409345_75f1b0fafedd	nginx	Self-Signed
2023-10-23	154.215.19.164	tcp/3790	HK Qianlong Technology	Metasploit Pro (and Commu	2bab15409345_2bab15409345_75f1b0fafedd	nginx	Self-Signed
2023-10-23	154.215.21.185	tcp/3790	HK Qianlong Technology	nginx without version info	2bab15409345_2bab15409345_75f1b0fafedd	nginx	Self-Signed
2023-10-23	45.63.86.203	tcp/3790	NET-45-63-86-0-23	nginx without version info	2bab15409345_2bab15409345_75f1b0fafedd	nginx	Self-Signed
2023-10-23	209.97.188.38	tcp/3790	DIGITALOCEAN-ASN	nginx without version info	2bab15409345_2bab15409345_75f1b0fafedd	nginx	Self-Signed
2023-10-23	154.215.18.166	tcp/3790	HK Qianlong Technology	Metasploit Pro (and Commu	2bab15409345_2bab15409345_75f1b0fafedd	nginx	Self-Signed
2023-10-23	182.161.69.154	tcp/3790	POWER LINE DATACENTE	nginx without version info	2bab15409345_2bab15409345_75f1b0fafedd	nginx	Self-Signed
2023-10-23	154.215.23.168	tcp/3790	HK Qianlong Technology	Metasploit Pro (and Commu	2bab15409345_2bab15409345_75f1b0fafedd	nginx	Self-Signed
2023-10-23	144.91.80.191	tcp/3790	CONTABO	nginx without version info	2bab15409345_2bab15409345_75f1b0fafedd	nginx	Self-Signed
2023-10-23	41.76.134.133	tcp/3790	Customer Allocation	nginx without version info	2bab15409345_2bab15409345_75f1b0fafedd	nginx	Self-Signed
2023-10-23	5.196.213.98	tcp/3790	OVH Static IP	nginx without version info	2bab15409345_2bab15409345_75f1b0fafedd	nginx	Self-Signed
2023-10-23	154.215.20.172	tcp/3790	HK Qianlong Technology	Metasploit Pro (and Commu	2bab15409345_2bab15409345_75f1b0fafedd	nginx	Self-Signed

Qakbot

JA4X=2bab15409345_af684594efb4_000000000000

Date (...	IP	Port	Hosting Entity	Signature	Search Term	Service	Banner
2023-10-23	189.140.66.63	tcp/443	Gestión de direccionamiento l	—	2bab15409345_af684594efb4_		
2023-10-23	47.18.213.41	tcp/443	OOL-CPE-HCVLNY-47-18-208-0	nginx with version info and/or	2bab15409345_af684594efb4_	http	nginx/1.9.12
2023-10-23	64.121.161.102	tcp/443	RCN Corporation	nginx with version info and/or	2bab15409345_af684594efb4_	http	nginx/1.9.12
2023-10-23	125.209.114.181	tcp/443	Multinet Pakistan Pvt. Ltd.	—	2bab15409345_af684594efb4_		
2023-10-23	23.93.65.180	tcp/443	Sonic.net, Inc.	—	2bab15409345_af684594efb4_		
2023-10-23	173.88.135.179	tcp/443	TWC-10796-MIDWEST	nginx with version info and/or	2bab15409345_af684594efb4_	http	nginx/1.9.12
2023-10-23	72.132.174.169	tcp/443	TWC-20001-PACWEST	nginx with version info and/or	2bab15409345_af684594efb4_	http	nginx/1.9.12
2023-10-23	186.182.15.91	tcp/443	Techtel LMDS Comunicaciones	—	2bab15409345_af684594efb4_		
2023-10-23	69.133.162.35	tcp/443	TWC-11426-CAROLINAS	nginx with version info and/or	2bab15409345_af684594efb4_	http	nginx/1.9.12
2023-10-23	184.16.79.167	tcp/443	FiberOptic-D Frontier Commur	nginx with version info and/or	2bab15409345_af684594efb4_	http	nginx/1.9.12
2023-10-23	172.115.17.50	tcp/443	TWC-20001-PACWEST	—	2bab15409345_af684594efb4_		
2023-10-22	74.12.146.78	tcp/2222	DSL-74-12-146-0-1600107141	—	2bab15409345_af684594efb4_		
2023-10-22	197.204.136.50	tcp/443	AS de ALGERIE TELECOM	—	2bab15409345_af684594efb4_		
2023-10-22	2.50.53.174	tcp/443	Emirates Internet	—	2bab15409345_af684594efb4_		
2023-10-22	97.93.211.58	tcp/443	CHARTER-20115	—	2bab15409345_af684594efb4_		
2023-10-22	77.86.98.236	tcp/443	Statics	nginx with version info and/or	2bab15409345_af684594efb4_	http	nginx/1.9.12
2023-10-22	188.26.232.198	tcp/443	RCS & RDS Residential	—	2bab15409345_af684594efb4_		
2023-10-22	77.124.172.23	tcp/443	PARTNER-AS	—	2bab15409345_af684594efb4_		
2023-10-22	47.181.12.202	tcp/443	FTR3 FiberOptic-S Chino Hills (	nginx with version info and/or	2bab15409345_af684594efb4_	http	nginx/1.9.12
2023-10-22	70.174.49.244	tcp/443	ASN-CXA-ALL-CCI-22773-RDC	nginx with version info and/or	2bab15409345_af684594efb4_	http	nginx/1.9.12
2023-10-22	96.246.147.170	tcp/443	UUNET	nginx with version info and/or	2bab15409345_af684594efb4_	http	nginx/1.9.12
2023-10-22	24.45.153.245	tcp/443	OOL-CPE-CORMNY-24-45-144-	nginx with version info and/or	2bab15409345_af684594efb4_	http	nginx/1.9.12
2023-10-22	78.92.133.215	tcp/443	Magyar Telekom customers us	nginx with version info and/or	2bab15409345_af684594efb4_	http	nginx/1.9.12
2023-10-22	66.113.28.4	tcp/443	StratusIQ	—	2bab15409345_af684594efb4_		
2023-10-22	64.46.22.26	tcp/443	Novus Entertainment Inc.	—	2bab15409345_af684594efb4_		

Pikabot

JA4X=1a59268f55e5_1a59268f55e5_795797892f9c (NOT “Aegir”)

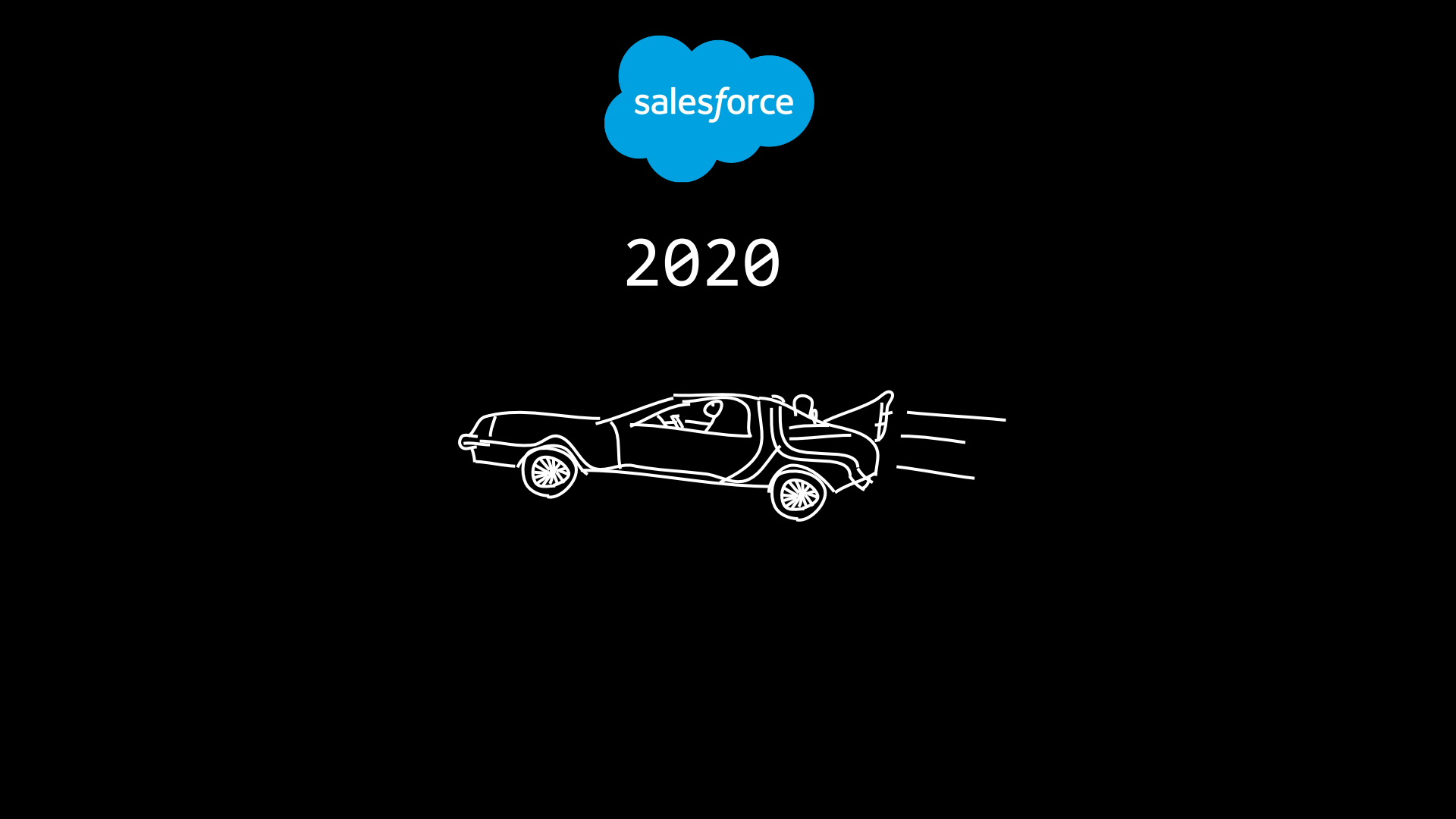


FOXIO

Pikabot

JA4X=1a59268f55e5_1a59268f55e5_795797892f9c (NOT “Aegir”)

IP	Ports	Sha256 Hash	SeenFirst	SeenLast
88.214.27.74	443	20FB3D6253E7A7B50FAB3168EFF282B854556F68ABAD92F92AD0A80FA6D533DE	2023-10-09 01:16:40	2023-10-17 01:30:14
78.128.112.208	443	C5EDA0F709BC00E9057B6C31DD6CE48DDB180D9E0EFBC68FD88D812E0D9735E7	2023-10-18 01:27:15	2023-10-18 01:27:15
91.215.85.197	443	CE220DED334B3EF085C297B19DD14C314C1CBA78865BB6D1C5C6A302A2F70636	2023-10-19 01:45:38	2023-10-19 01:45:38
109.107.182.11	443	E1E80116DD3E52BA830B9B8A3213A39ABACADF0C5395ABB2687E16864360443E	2023-10-20 02:00:37	2023-10-20 02:00:37
109.107.182.13	443	3D5F0C19D7677AACBEC93406711FD84AC8A5DE82FBF630E1E614799E27EE1BA9	2023-10-19 01:20:12	2023-10-19 01:20:12
80.79.78.221	5101	4A148766AAD489ED7262FC790C86C8D61FCD87675EBAB334B435171447DE4585	2022-08-29 06:43:07	2023-10-17 12:41:16
109.107.182.11	443	8EABFB51730E881A5BFDB42BEC50B77E49DFC3D80D4BB5C30D91170E72794B08	2023-10-19 00:34:01	2023-10-19 00:34:01
91.215.85.154	443	027B4CCB9BF99ADF6AFF55C22466000CD18DECAF274580E0405F427C14BCD9D6	2023-10-20 01:37:30	2023-10-20 01:37:30
193.232.104.221	5101	4A148766AAD489ED7262FC790C86C8D61FCD87675EBAB334B435171447DE4585	2022-09-09 23:29:49	2023-10-17 13:12:47
109.107.182.16	443	5753F1BD202768B7BD4CD77A90BB4D7CA0C5ADA7CA2104F0FC369A216F236AFE	2023-10-19 00:36:10	2023-10-19 00:36:10
132.148.79.222	2222	391F4A533EB7A9BD66F6250872544093338 51DFB02DDEF4D36E95A3AC6FF2564	2023-05-15 09:04:05	2023-10-23 04:32:59
109.107.182.10	443	210361369EA9332072A4EE428BF232C7127F938288169CB47D2F2833F225B1EE	2023-10-20 01:16:58	2023-10-20 01:16:58
109.107.182.12	443	CEC45CD82077DF0C1A5A7FE2C2A226203143BA1443554416BC289996414392F6	2023-10-19 00:59:40	2023-10-19 00:59:40
109.107.182.13	443	BCEFEEFCC6CEFE1EAD0E4ADF144F868ED931DFA6B5416C6C3A444EE30692DECA	2023-10-20 02:01:41	2023-10-20 02:01:41
109.107.182.14	443	CC98C6A8B6D77E70F0030BB8F0EAC973A9553B7C0F8D0B818E7159A67AE88ACA	2023-10-20 03:08:39	2023-10-20 03:08:39


salesforce
2020

JARM

Created By:

John Althouse
Andrew Smart
RJ Nunnally
Mike Brady

* Caleb Yu

Example Output

Domain	JARM
salesforce.com	2ad2ad0002ad2ad00042d42d00000069d641f34fe76acdc05c40262f8815e5
force.com	2ad2ad0002ad2ad00042d42d00000069d641f34fe76acdc05c40262f8815e5
google.com	27d40d40d29d40d1dc42d43d00041d4689ee210389f4f6b4b5b1b93f92252d
youtube.com	27d40d40d29d40d1dc42d43d00041d4689ee210389f4f6b4b5b1b93f92252d
gmail.com	27d40d40d29d40d1dc42d43d00041d4689ee210389f4f6b4b5b1b93f92252d
facebook.com	27d27d27d29d27d1dc41d43d00041d741011a7be03d7498e0df05581db08a9
instagram.com	27d27d27d29d27d1dc41d43d00041d741011a7be03d7498e0df05581db08a9
oculus.com	29d29d20d29d29d21c41d43d00041d741011a7be03d7498e0df05581db08a9

Shodan @shodanhq · Nov 17, 2020

We've added JARM fingerprinting and with it introduce a new "ssl.jarm" property/ filter/ facet. Here's a breakdown of the current values for JARM fingerprints in Shodan: beta.shodan.io/search/facet?q... (h/t @4A4133 and @SalesforceEng)

57 132

RISKIQ

EXTERNAL THREAT MANAGEMENT , ANALYST

RiskIQ's New JARM Feature Supercharges Incident Response

JANUARY 02, 2021 | BY TEAM RISKIQ

There will be many more breaches like the one of SolarWinds.

Moving into 2021 and beyond, the ability to view your organization from the
these internet-scale attacks by advanced APTs. FireEye and other security e

JARM in Censys Search 2.0

Updated · 2 years ago

Censys

BinaryEdge API Documentation

JARM

The JARM module attempts to actively fingerprint an SSL/T
responses that can be used to quickly identify default applic

JARM

```
curl -v -L https://api.binaryedge.io/v1/tasks -d '
```

paloalto NETWORKS

Follow 101 Followers · Cortex ML/AI Team PAN-OS About

CORTEX XSOAR BY PALO ALTO NETWORKS

- Index
- Integrations
  - abuse.ch SSL Blacklist Feed
  - AbuseIPDB
  - Acalvio ShadowPlex
  - Accessdata
  - Active Directory Authentication
  - Active Directory Query v2

JARM

Active TLS fingerprinting using JARM

Configure JARM on Cortex XSOAR

1. Navigate to **Settings** > **Integrations** > **Servers & Services**.

Jarm

In Palo Alto Networks Developer Blog. More on Medium.

Andrew Scott · Jan 29

Fingerprinting SSL Servers using JARM and Python

Introducing pyJARM, the simple way to use JARM with Python

VT

HD Moore
@hdmoore

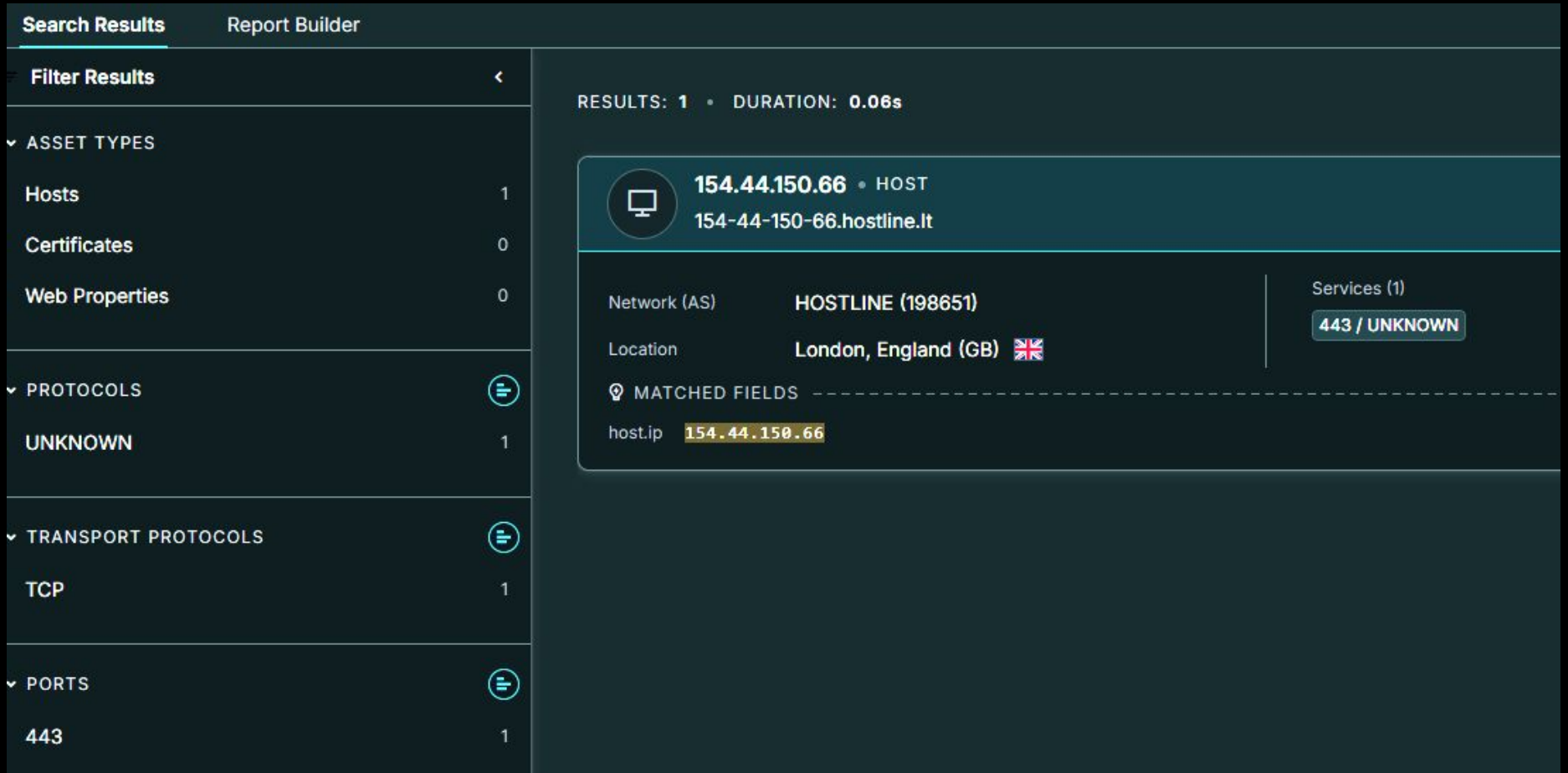
Want to play with JARM active TLS fingerprinting in Go? Check out jarm-go: github.com/RumbleDiscover... (cc @4A4133)

```
Developer@DESKTOP-KHI4610 MSYS ~/go
$ go get github.com/RumbleDiscovery/jarm-go/cmd/jarmscan

Developer@DESKTOP-KHI4610 MSYS ~/go
$ jarmscan www.salesforce.com
JARM: 2ad2ad0002ad2ad00042d42d00000069d641f34fe76acdc05c40262f8815e5
```

DPRK C2 – 154.44.150.66

DPRK C2 – 154.44.150.66



Details

timestamp		2026-05-03T03:08:02Z
ip		154.44.150.66
port-tcp		443
entity		Hostline
asn		AS198651 HOSTLINE, UAB
geo-area		LONDON; England
geo-country		GB
server-banner		
tls-alert	tls	internal error

jarm-fuzzyhash;=00000000000000000000000000000000000000000000000000000000000000

help

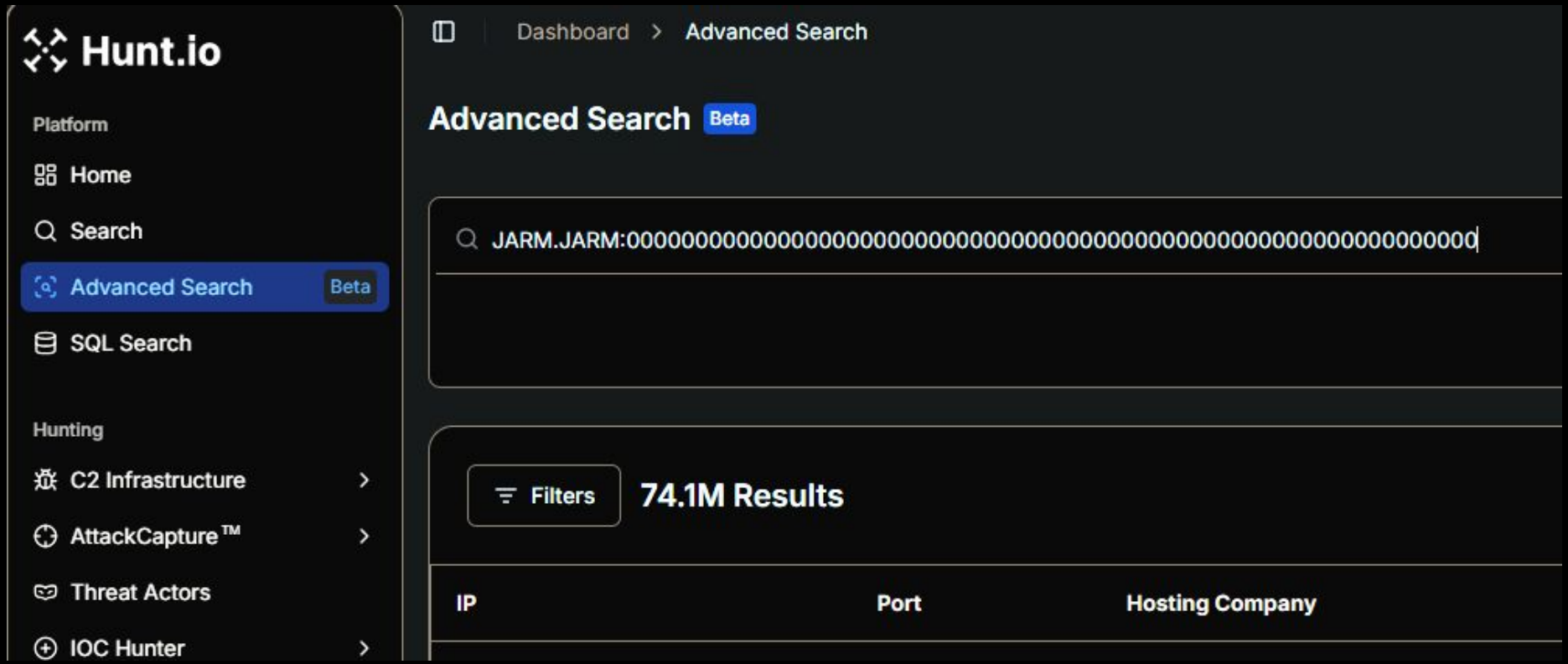
SUMMARY | INTERNET-WIDE SCANS | REGISTRATIONS | DNS | CERTIFICATE TRANSPARENCY | FINGERPRINTS

Most recent results only

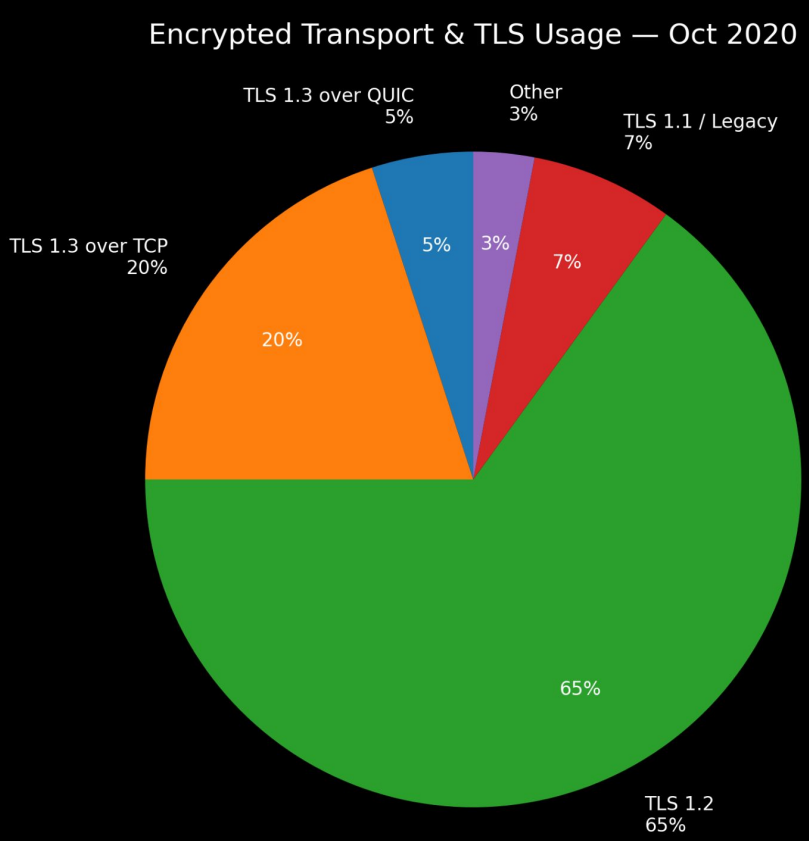
JARM / 15.6M results

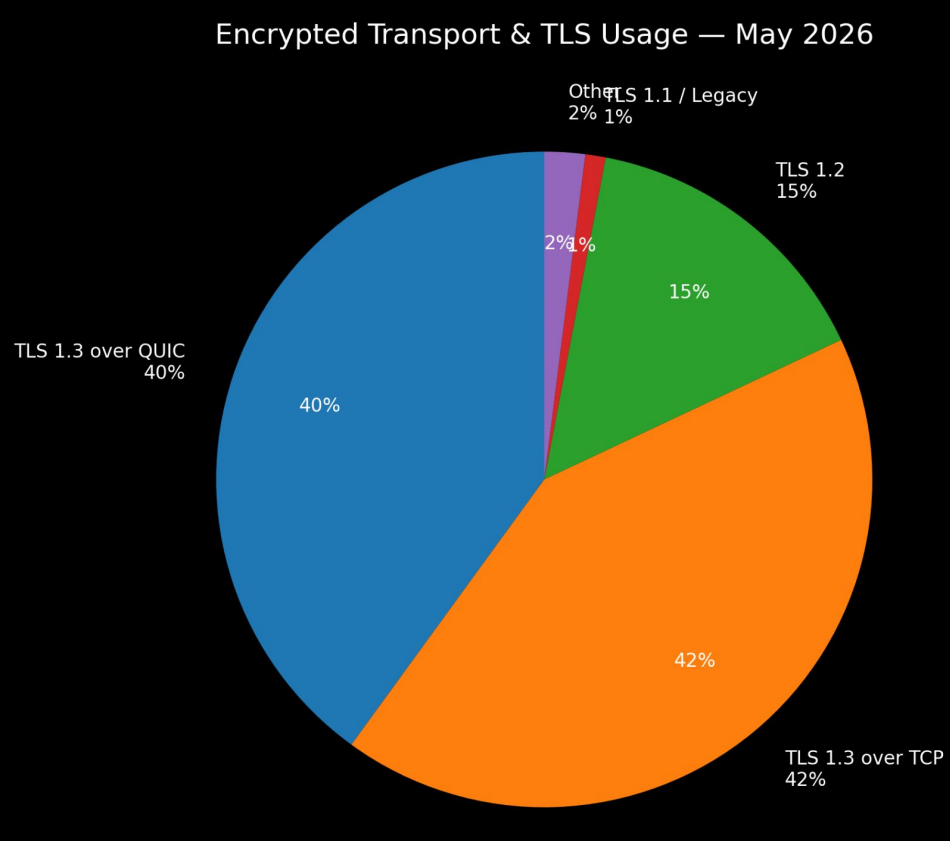
Query timed out; results may be incomplete. Consider reducing the time period for this search.

Timestamp (UTC)	IP	Port	Entity	ASN
2026-05-05 08:30:00	148.230.121.26	443	Hostinger	AS47583 Hostinger International Limited
2026-05-05 08:30:00	188.114.99.212	2096	Cloudflare	AS13335 Cloudflare, Inc.
2026-05-05 08:30:00	223.123.150.149	443	China Mobile Hong Kong	AS137872 China Mobile Hong Kong Compa
2026-05-05 08:30:00	2a01:4f8:1c1a:208	5061	Hetzner	AS24940 Hetzner Online GmbH


Hunt.io
Platform
Home
Search
Advanced Search
Beta
SQL Search
Hunting
C2 Infrastructure
AttackCapture™
Threat Actors
IOC Hunter
Dashboard
Advanced Search
Advanced Search
Beta
JARM.JARM:00000000000000000000000000000000000000000000000000000000000000
Filters
74.1M Results
IP
Port
Hosting Company

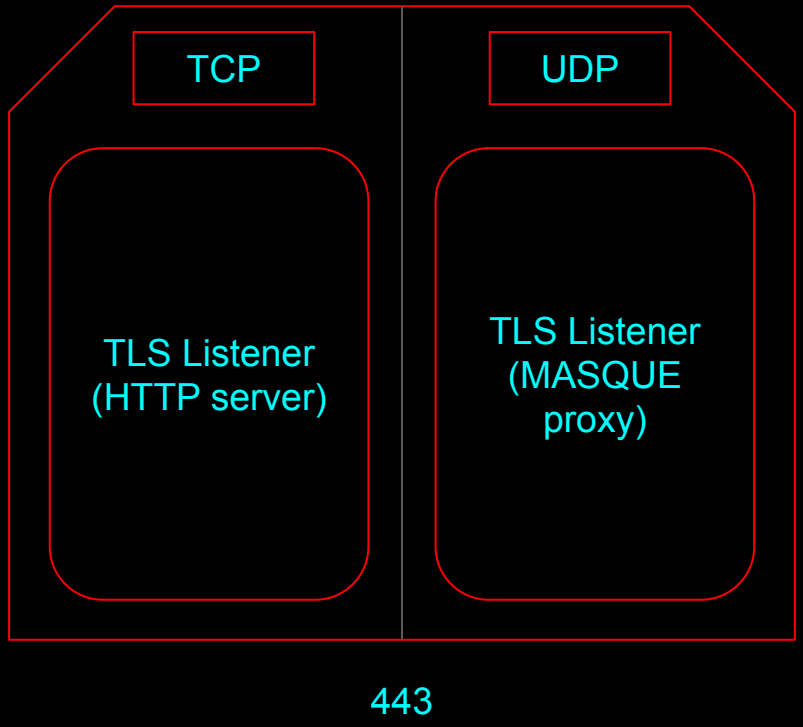
Why is JARM no longer working?





It’s time to create JA4Scan

Dual-stack deployments



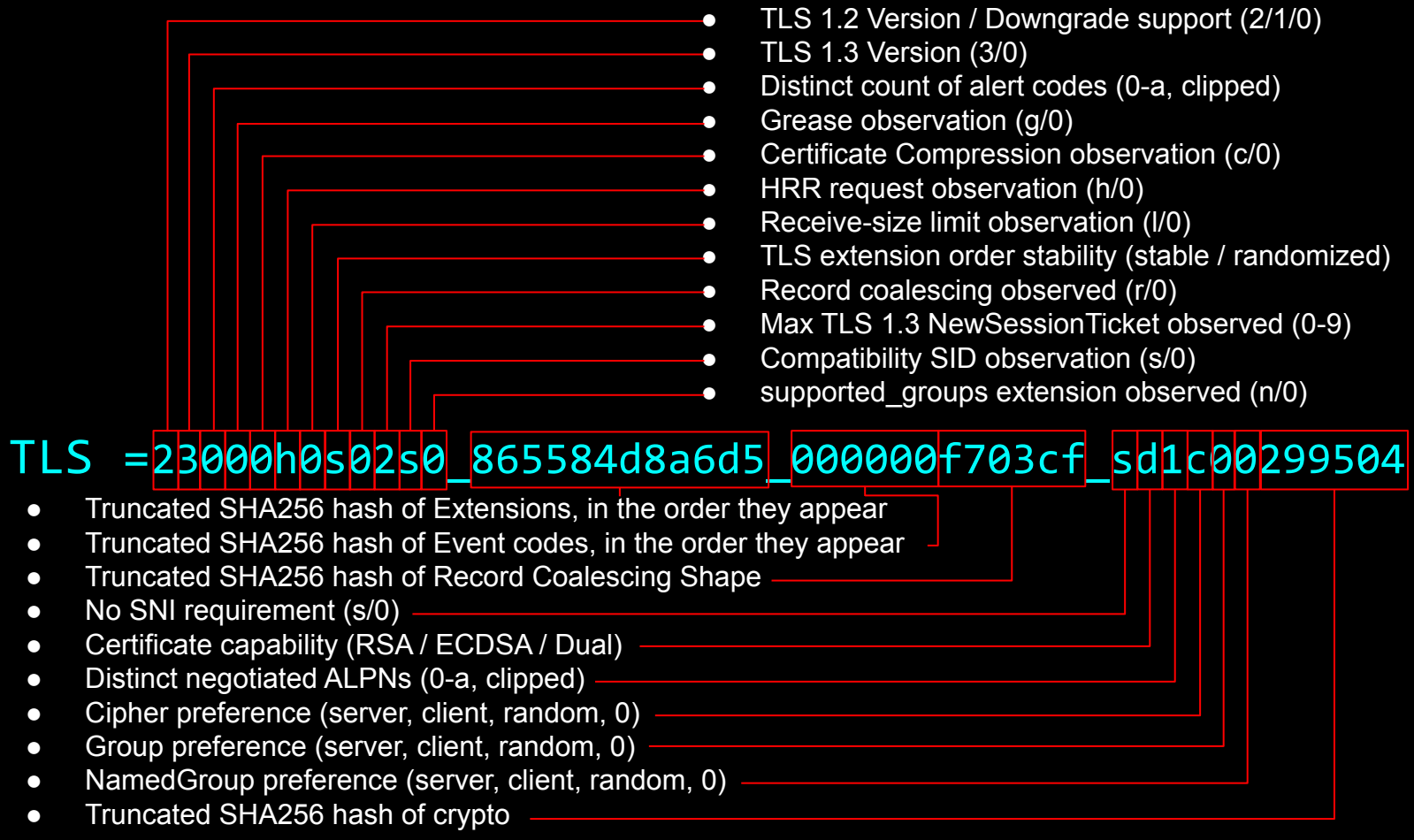
Probes

TCP	1. No SNI 2. TLS 1.3 baseline 3. Force HRR 4. ECDSA-only 5. RSA-only 6. TLS 1.3 parser-stress	7. TLS 1.2 baseline 8. TLS 1.2 minimal 9. Chacha cipher first 10. AES cipher first 11. TLS 1.2 parser-stress
QUIC	1. No SNI 2. Baseline 3. Force HRR 4. ECDSA-only 5. RSA-only 6. Minimal	

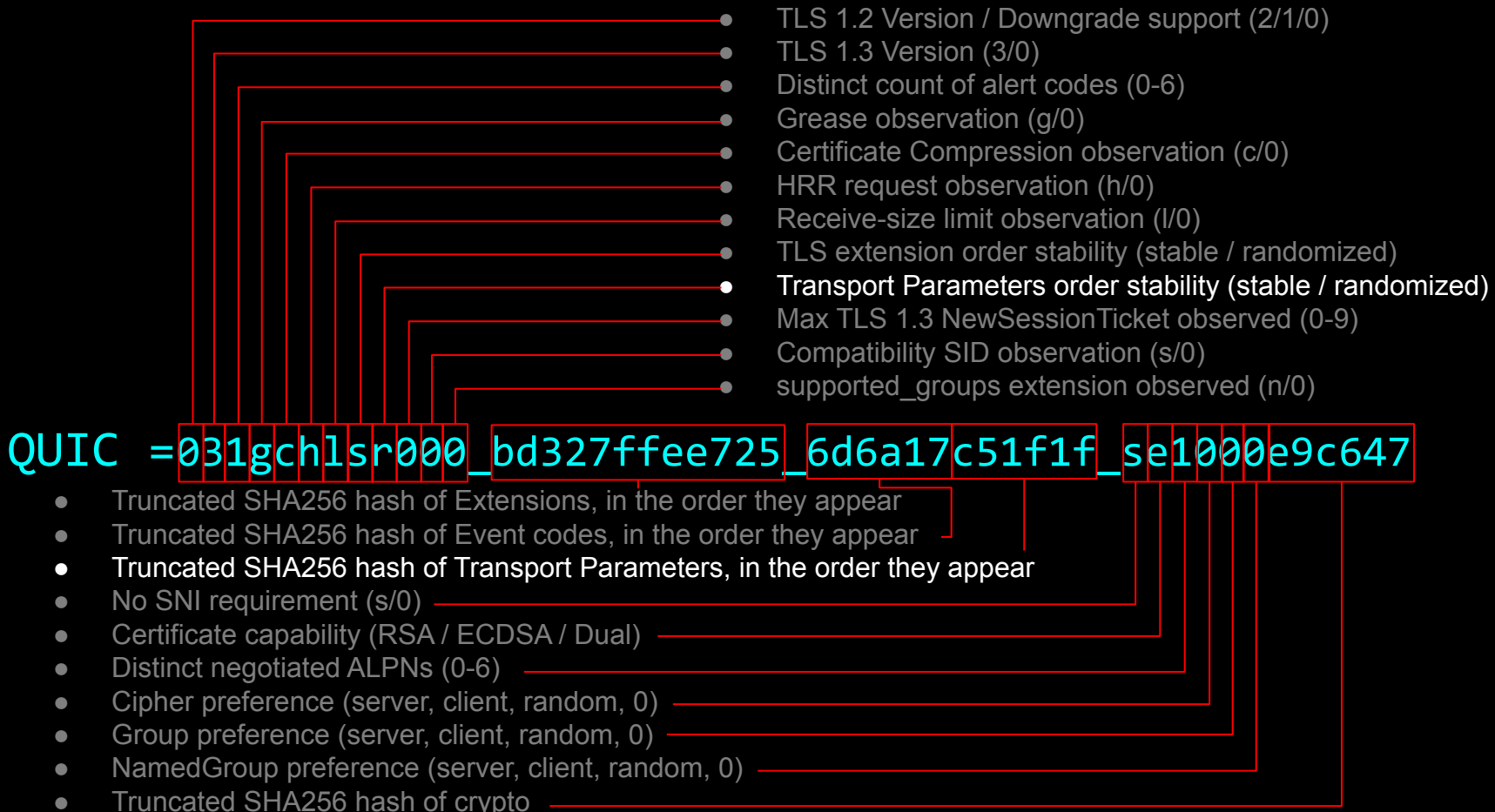
Session Tickets

	Lifetime	Nonce signal	# tickets
Golang stdlib	7d	-	1
OpenSSL 3 / 1	2h	8 - counter	2
BoringSSL	2d	1 - counter	2
JDK	24h	1 - counter from 1	1
rustls (less)	12h	32 - random	2
s2n-tls	15h	2 - counter	1
picotls	app-set	-	1

JA4Scan-TLS Fingerprint



JA4Scan-QUIC Fingerprint



Translating to known libraries

httpd w/ LibreSSL eg. openbsd.org

```
[tcp] 23100h0r00s0_30ed81094e50_72ae3ede9eb2_sr0sscc9217d
  > tls=libressl          quic=none                  [high]
```

NGINX w/ LibreSSL eg. suckless.org

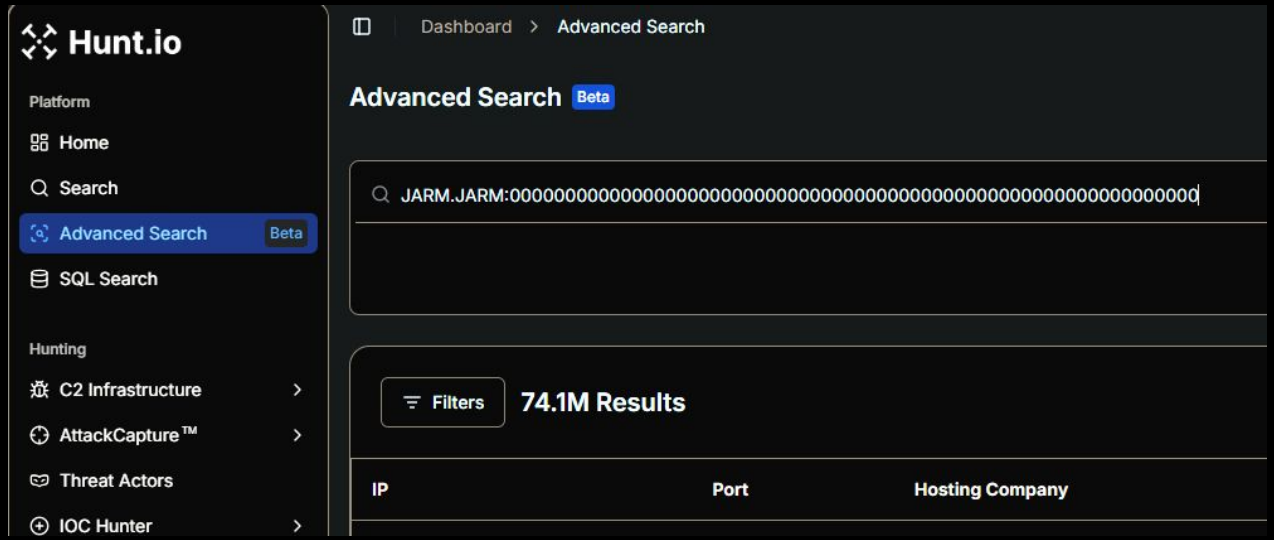
```
[tcp] 23100h0r00s0_3dafc7d50665_72ae3ede9eb2_sr1sscc9217d
  > tls=libressl          quic=none                  [high]
```

Pingora w/ BoringSSL and Quiche eg. cloudflare.com

```
[quic] 0300chlss200_8960528bd01f_000000b36f05_sd1000e9c647
  > tls=boringssl         quic=quiche-cloudflare     [high]
```

Caddy w/ crypto/tls and quic-go eg. caddyserver.com

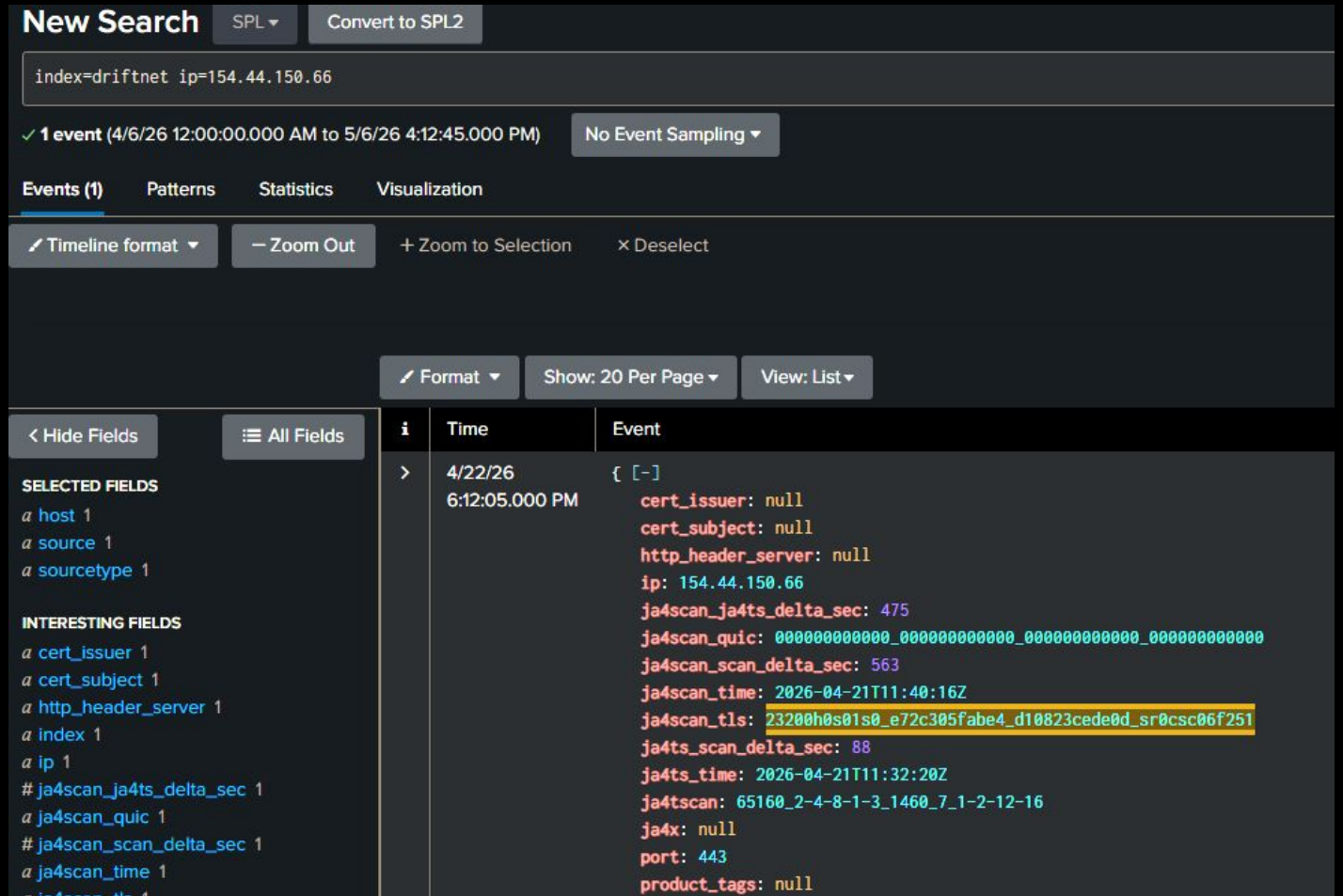
```
[quic] 032g0hlss000_52347523195b_d10823008abe_0e10s05444e9
  > tls=go-tls            quic=quic-go               [high]
```



After scanning the internet, the millions of IPs that did not respond to JARM *did* respond to JA4Scan

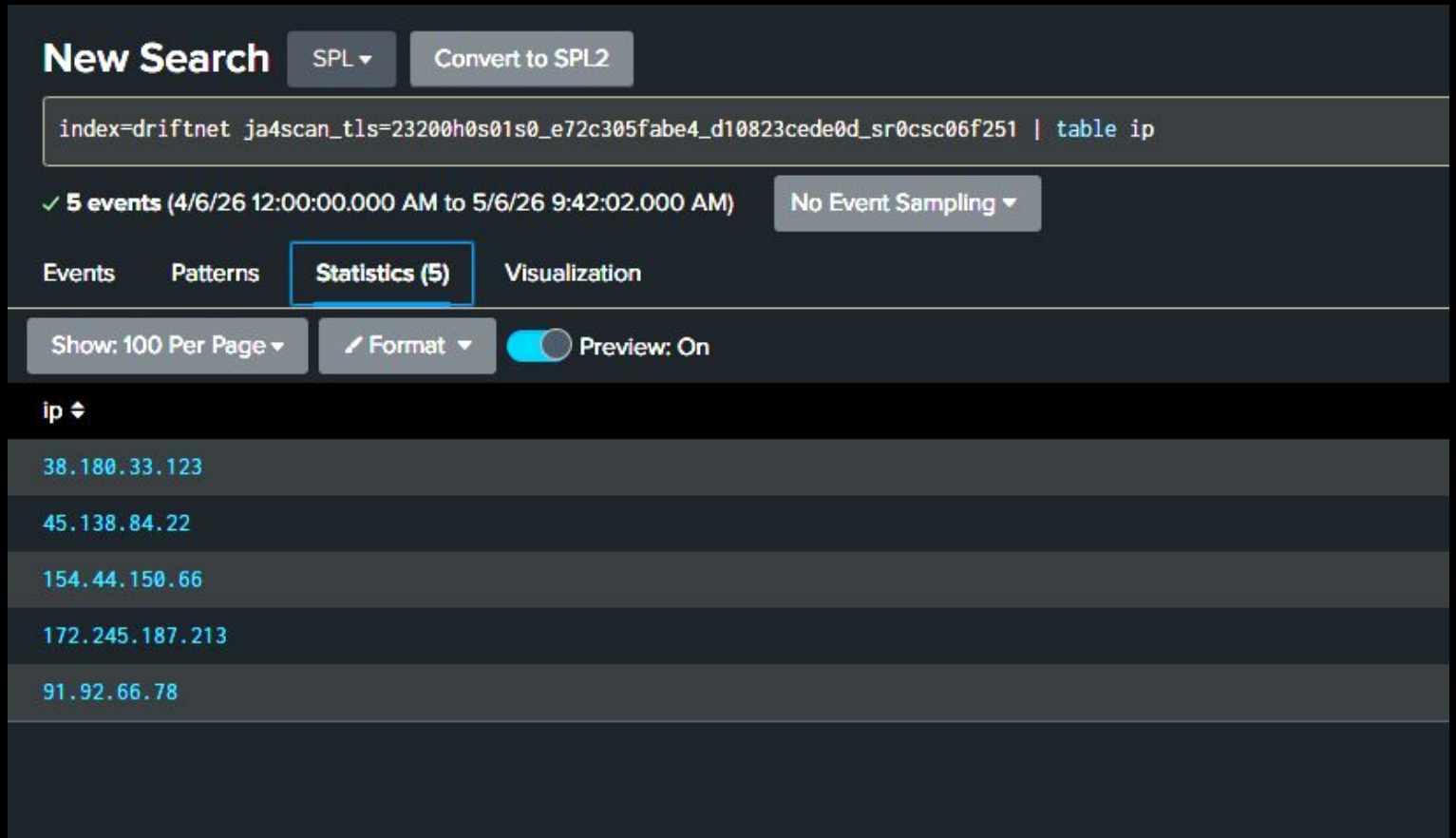
DPRK C2 IP = 154.44.150.66

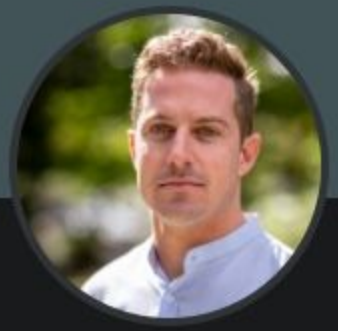
DPRK C2 IP = 154.44.150.66



DPRK C2 IP = 154.44.150.66
JA4Scan-TLS = 23200h0s01s0_e72c305fabe4_d10823cede0d_sr0csc06f251

DPRK C2 IP = 154.44.150.66
JA4Scan-TLS = 23200h0s01s0_e72c305fabe4_d10823cede0d_sr0csc06f251





Greg Lesnewich · 2nd

Threat Research at Proofpoint

United States · Contact info

500+ connections

Proofpoint

hgmydr.wiki - 77.73.39.115
zxzaq.com - 65.38.121.27
upgybj.store - 185.82.126.4

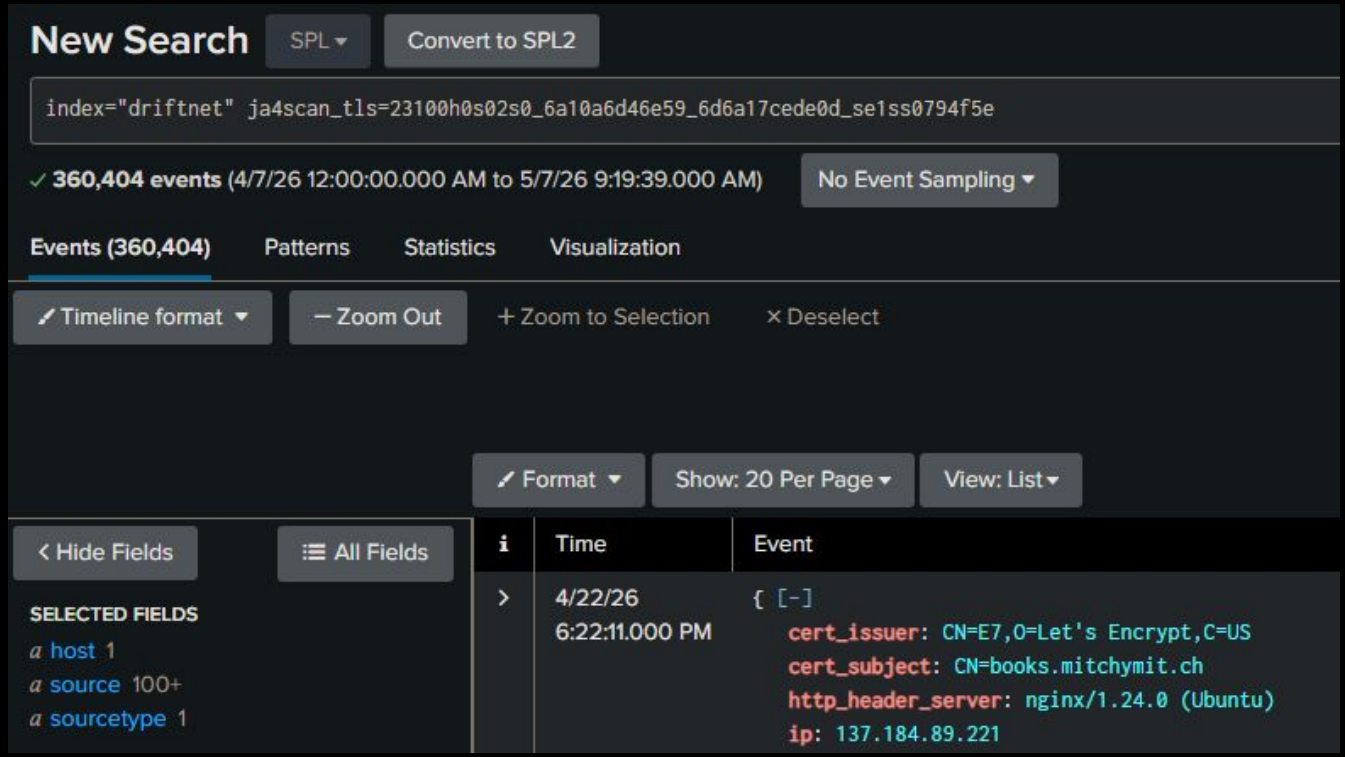
hgmydr.wiki - 77.73.39.115
zxzaq.com - 65.38.121.27
upgybj.store - 185.82.126.4


```
cert_issuer: CN=E8,O=Let's Encrypt,C=US
cert_subject: CN=zxzaq.com
http_header_server: nginx
ip: 65.38.121.27
ja4scan_ja4ts_delta_sec: -5473
ja4scan_quic: 000000000000_000000000000_000000000000_000000000000
ja4scan_scan_delta_sec: 568
ja4scan_time: 2026-04-20T04:14:14Z
ja4scan_tls: 23100h0s02s0_6a10a6d46e59_6d6a17cede0d_se1ss0794f5e
ja4ts_scan_delta_sec: 6041
ja4ts_time: 2026-04-20T05:45:27Z
ja4tscan: 43440_2-4-8-1-3_1360_8_1-2-4-8-16
ja4x: a373a9f83c6b_7022c563de38_2e3757343cb0
port: 443
product_tags: [ [+]
]
protocol: tcp
scan_time: 2026-04-20T04:04:46Z
```

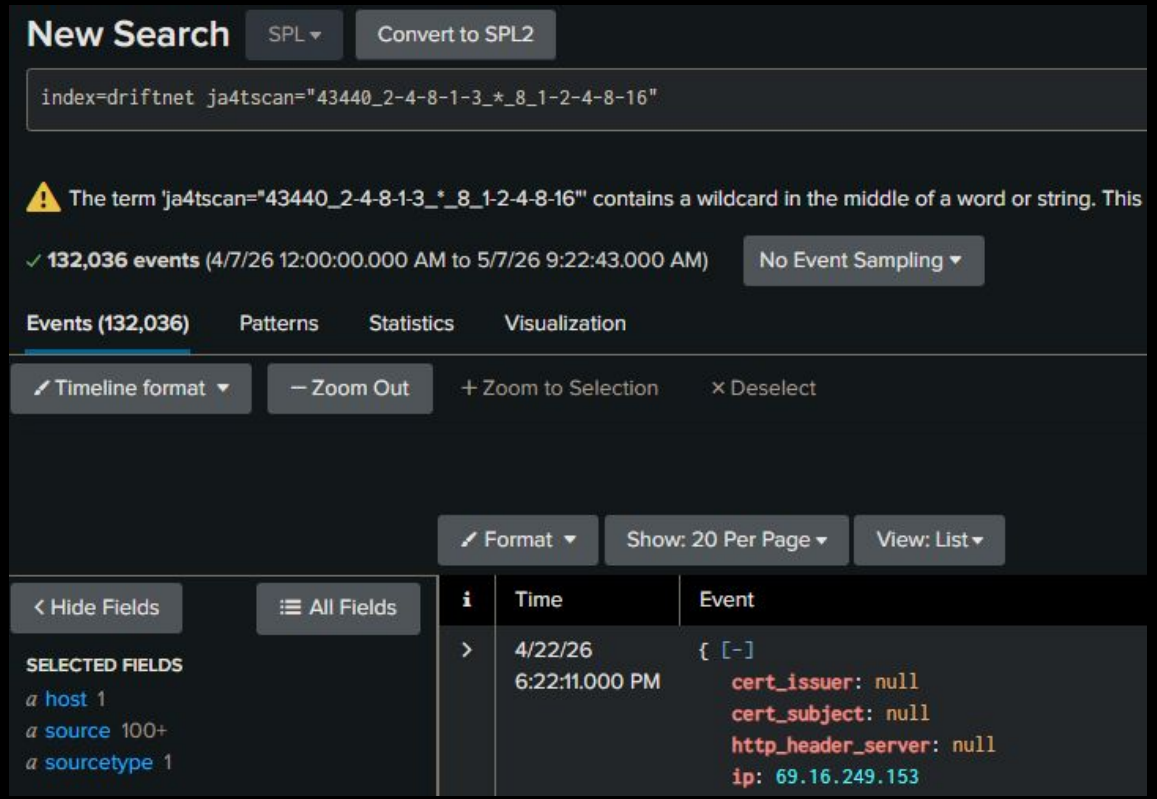
hgmydr.wiki - 77.73.39.115
zxzaq.com - 65.38.121.27
upgybj.store - 185.82.126.4


```
cert_issuer: CN=E7,O=Let's Encrypt,C=US
cert_subject: CN=hgmydr.wiki
http_header_server: nginx
ip: 77.73.39.115
ja4scan_ja4ts_delta_sec: 40388
ja4scan_quic: 000000000000_000000000000_000000000000_000000000000
ja4scan_scan_delta_sec: 568
ja4scan_time: 2026-04-20T11:12:47Z
ja4scan_tls: 23100h0s02s0_6a10a6d46e59_6d6a17cede0d_se1ss0794f5e
ja4ts_scan_delta_sec: -39820
ja4ts_time: 2026-04-19T23:59:39Z
ja4tscan: 43440_2-4-8-1-3_1460_8_1-2-4-8-16
ja4x: a373a9f83c6b_7022c563de38_2e3757343cb0
port: 443
product_tags: [ [+]
]
protocol: tcp
scan_time: 2026-04-20T11:03:19Z
```

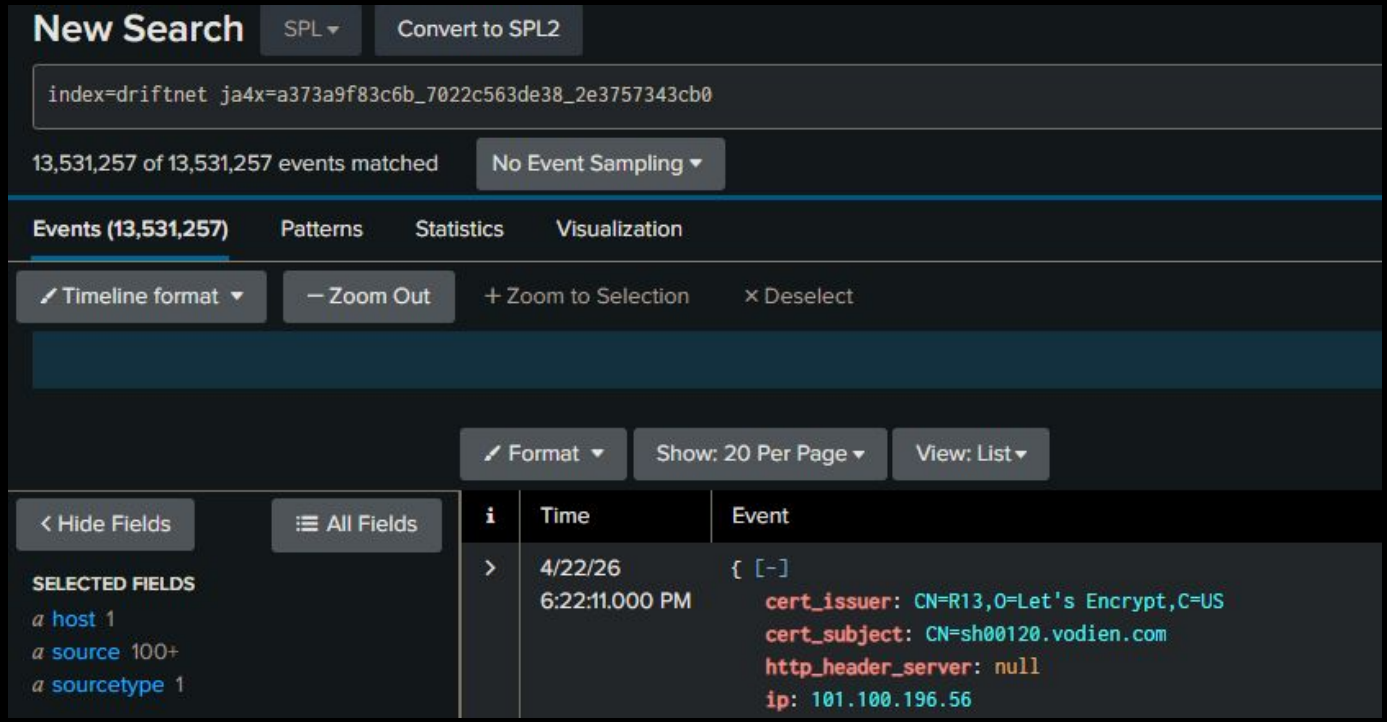
hgmydr.wiki - 77.73.39.115
zxzaq.com - 65.38.121.27
upgybj.store - 185.82.126.4



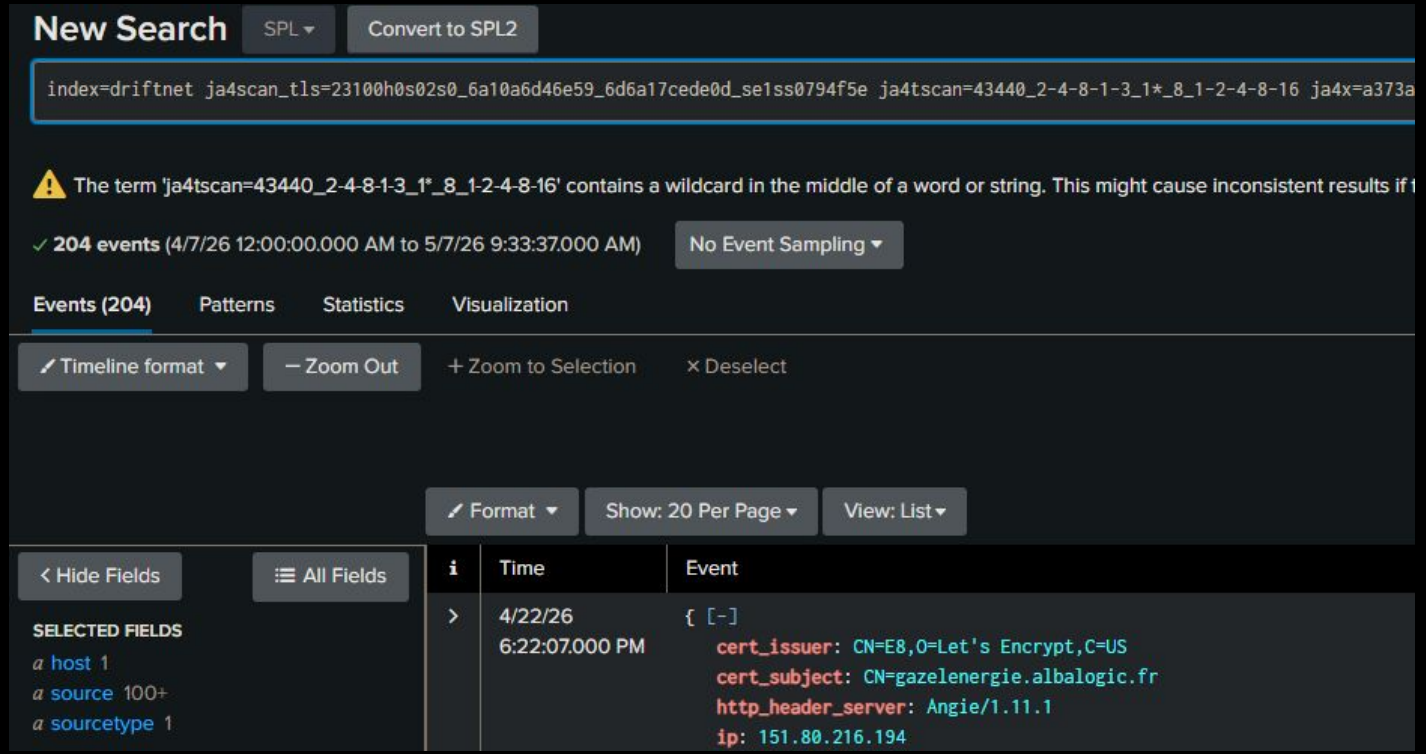
hgmydr.wiki - 77.73.39.115
zxzaq.com - 65.38.121.27
upgybj.store - 185.82.126.4



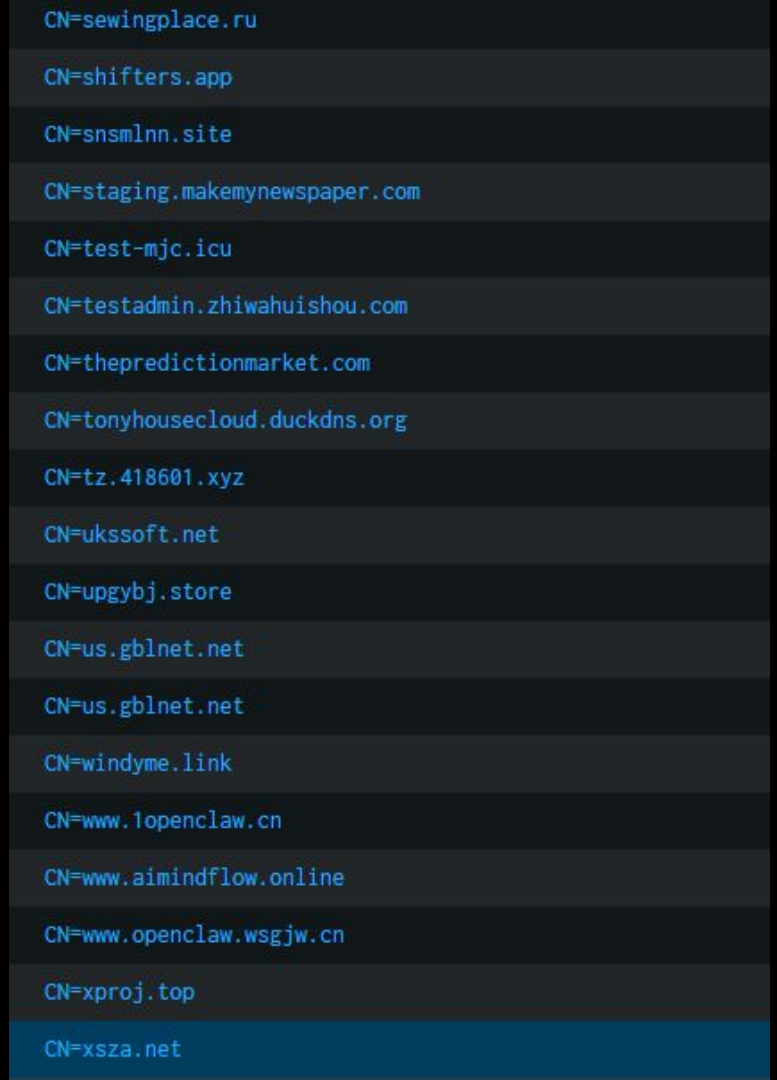
hgmydr.wiki - 77.73.39.115
zxzaq.com - 65.38.121.27
upgybj.store - 185.82.126.4



hgmydr.wiki - 77.73.39.115
zxzaq.com - 65.38.121.27
upgybj.store - 185.82.126.4



hgmydr.wiki - 77.73.39.115
zxzaq.com - 65.38.121.27
upgybj.store - 185.82.126.4



hgmydr.wiki - 77.73.39.115
zxzaq.com - 65.38.121.27
upgybj.store - 185.82.126.4



hgmydr.wiki - 77.73.39.115
zxzaq.com - 65.38.121.27
upgybj.store - 185.82.126.4

New UNK_HeatSink C2:
xsza.net - 185.51.134.30





Christy Quinn · 1st

Cyber analysis and investigations

London Area, United Kingdom · Contact info

National Gas

Issued To

Common Name (CN)	ssavpn.ssa.gov
Organization (O)	Social Security Administration
Organization Unit (OU)	-

Issued By

Common Name (CN)	DigiCert Global G2 TLS RSA SHA256 2020 CA1
Organization (O)	DigiCert Inc
Organization Unit (OU)	-

Validity Period

Issued On	2024-07-08 00:00:00
Expires On	2025-07-07 23:59:59

Fingerprints

SHA-256 Fingerprint	8479853E4217FC69F7534AF083576265F18BDADD25CE116194B8D3AE8D11E14B
SHA-1 Fingerprint	19A58F69078D25E01594FA6B812729D5089775FC

JA4X

JA4X	a373a9f83c6b_2bab15409345_8af5bbe4d352
JA4XIssuer	a373a9f83c6b
JA4XSubject	2bab15409345
JA4XExt	8af5bbe4d352

Fake DigiCert Issued Cert

Issued To

Common Name (CN)	ssavpn.ssa.gov
Organization (O)	Social Security Administration
Organization Unit (OU)	-

Issued By

Common Name (CN)	DigiCert Global G2 TLS RSA SHA256 2020 CA1
Organization (O)	DigiCert Inc
Organization Unit (OU)	-

Validity Period

Issued On	2024-07-08 00:00:00
Expires On	2025-07-07 23:59:59

Fingerprints

SHA-256 Fingerprint	8479853E4217FC69F7534AF083576265F18BDADD25CE116194B8D3AE8D11E14B
SHA-1 Fingerprint	19A58F69078D25E01594FA6B812729D5089775FC

JA4X

JA4X	a373a9f83c6b_2bab15409345_8af5bbe4d352
JA4XIssuer	a373a9f83c6b
JA4XSubject	2bab15409345
JA4XExt	8af5bbe4d352

Real Cert

Issued To

Common Name (CN)	ssavpn.ssa.gov
Organization (O)	Social Security Administration
Organization Unit (OU)	-

Issued By

Common Name (CN)	DigiCert Global G2 TLS RSA SHA256 2020 CA1
Organization (O)	DigiCert Inc
Organization Unit (OU)	-

Validity Period

Issued On	2024-07-08 00:00:00
Expires On	2025-07-07 23:59:59

Fingerprints

SHA-256 Fingerprint	7BCF5AC8AD73E29D173F8B5E4B2AEB2DDF9562D0CB48E109A22FC6289CE5FEA0
SHA-1 Fingerprint	6A2CA5469D26759D27987DF4424B791119A47844

JA4X

JA4X	a373a9f83c6b_2bab15409345_2cdf432ec278
JA4XIssuer	a373a9f83c6b
JA4XSubject	2bab15409345
JA4XExt	2cdf432ec278

23.137.253.132

23.137.253.132

JA4Scan-TLS = 23000h0s02sn_e655dcb7f4a0_1b98decede0d_sr3sssbe8207

23.137.253.132

JA4Scan-TLS = 23000h0s02sn_e655dcb7f4a0_1b98decede0d_sr3sssbe8207

90% cert_issuer="CN=mitmproxy,O=mitmproxy"

23.137.253.132

JA4Scan-TLS = 23000h0s02sn_e655dcb7f4a0_1b98decede0d_sr3sssbe8207

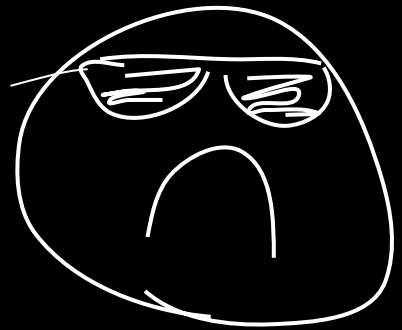
90% cert_issuer="CN=mitmproxy,O=mitmproxy"

ja4x-hash	cert	a373a9f83c6b_2bab15409345_8af5bbe4d352
server-banner	nmap	HTTP/1.1 400 Bad Request\x0d\x0aServer: mitmproxy 11.0.2\x0d\x0aConnection: close\x0d\x0aContent-Type: text/html\x0d\x0acontent-length: 173\x0d\x0a\x0d\x0a<html>\x0a<head>\x0a <title>400 Bad Request</title>\x0a</head>\x0a<body>\x0a 400 Bad Request \x0a HTTP request has no host header, destination unknown. \x0a</body>\x0a</html>

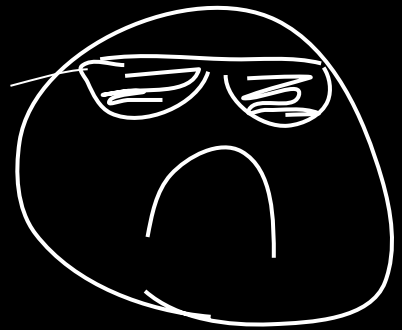
Pivot to find more of these!

ja4scan-tls=23000h0s02sn_e655dcb7f4a0_1b98decede0d_sr3sssbe8207 (mitmproxy)
AND
cert_issuer!="CN=mitmproxy,O=mitmproxy"
AND
cert_subject=*vpn*

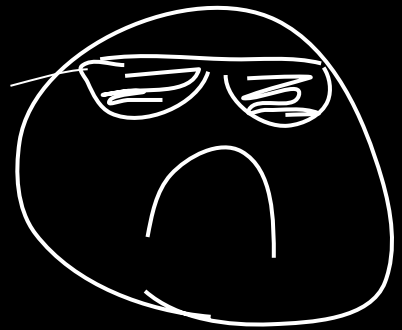
Malicious IP	Target Domain	Target Org	Target System
23.137.253.132	ssavpn.ssa.gov	U.S. Social Security Administration (Holds Social Security numbers, job and earnings history, addresses, disability records, and family relationships)	Cisco ASA



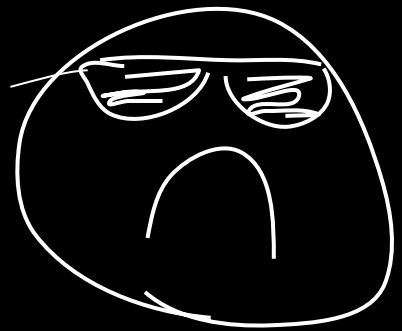
Malicious IP	Target Domain	Target Org	Target System
23.137.253.132	ssavpn.ssa.gov	U.S. Social Security Administration (Holds Social Security numbers, job and earnings history, addresses, disability records, and family relationships)	Cisco ASA
66.92.20.231	oktavpn.usip.org	U.S. Institute for Peace (Diplomatic strategy, conflict-resolution efforts, foreign policy networks, ally communications, and sensitive peacebuilding initiatives)	Cisco ASA



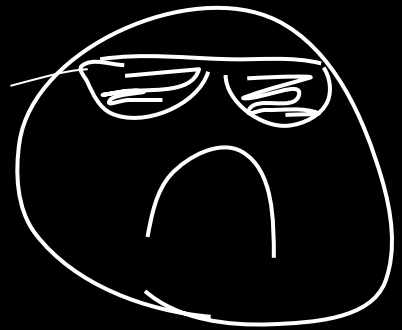
Malicious IP	Target Domain	Target Org	Target System
23.137.253.132	ssavpn.ssa.gov	U.S. Social Security Administration (Holds Social Security numbers, job and earnings history, addresses, disability records, and family relationships)	Cisco ASA
66.92.20.231	oktavpn.usip.org	U.S. Institute for Peace (Diplomatic strategy, conflict-resolution efforts, foreign policy networks, ally communications, and sensitive peacebuilding initiatives)	Cisco ASA
38.143.109.201	vpn.csis.org	U.S. Center for Strategic and International Studies (National security policy, geopolitical research, government and defense contacts, and global strategic forecasting)	Cisco ASA



Malicious IP	Target Domain	Target Org	Target System
23.137.253.132	ssavpn.ssa.gov	U.S. Social Security Administration (Holds Social Security numbers, job and earnings history, addresses, disability records, and family relationships)	Cisco ASA
66.92.20.231	oktavpn.usip.org	U.S. Institute for Peace (Diplomatic strategy, conflict-resolution efforts, foreign policy networks, ally communications, and sensitive peacebuilding initiatives)	Cisco ASA
38.143.109.201	vpn.csis.org	U.S. Center for Strategic and International Studies (National security policy, geopolitical research, government and defense contacts, and global strategic forecasting)	Cisco ASA
154.44.0.165	cloud-wfhvpn.tsmc.com	Taiwan Semiconductor - TSMC (Advanced semiconductor manufacturing processes, chip designs, technology supply chains, and chip production capabilities)	Cisco ASA



Malicious IP	Target Domain	Target Org	Target System
23.137.253.132	ssavpn.ssa.gov	U.S. Social Security Administration (Holds Social Security numbers, job and earnings history, addresses, disability records, and family relationships)	Cisco ASA
66.92.20.231	oktavpn.usip.org	U.S. Institute for Peace (Diplomatic strategy, conflict-resolution efforts, foreign policy networks, ally communications, and sensitive peacebuilding initiatives)	Cisco ASA
38.143.109.201	vpn.csis.org	U.S. Center for Strategic and International Studies (National security policy, geopolitical research, government and defense contacts, and global strategic forecasting)	Cisco ASA
154.44.0.165	cloud-wfhvpn.tsmc.com	Taiwan Semiconductor - TSMC (Advanced semiconductor manufacturing processes, chip designs, technology supply chains, and chip production capabilities)	Cisco ASA
154.49.127.17	vpn-y12nongfe.cns.doe.gov	U.S. Department of Energy - Y-12 National Security Complex (U.S. Nuclear weapons stockpile management, uranium processing operations, nuclear weapons technologies and security)	Cisco ASA



Malicious IP	Target Domain	Target Org	Target System
23.137.253.132	ssavpn.ssa.gov	U.S. Social Security Administration (Holds Social Security numbers, job and earnings history, addresses, disability records, and family relationships)	Cisco ASA
66.92.20.231	oktavpn.usip.org	U.S. Institute for Peace (Diplomatic strategy, conflict-resolution efforts, foreign policy networks, ally communications, and sensitive peacebuilding initiatives)	Cisco ASA
38.143.109.201	vpn.csis.org	U.S. Center for Strategic and International Studies (National security policy, geopolitical research, government and defense contacts, and global strategic forecasting)	Cisco ASA
154.44.0.165	cloud-wfhvpn.tsmc.com	Taiwan Semiconductor - TSMC (Advanced semiconductor manufacturing processes, chip designs, technology supply chains, and chip production capabilities)	Cisco ASA
154.49.127.17	vpn-y12nongfe.cns.doe.gov	U.S. Department of Energy - Y-12 National Security Complex (U.S. Nuclear weapons stockpile management, uranium processing operations, nuclear weapons technologies and security)	Cisco ASA



Malicious IP	Target Domain	Target Org	Target System
23.137.253.132	ssavpn.ssa.gov	U.S. Social Security Administration (Holds Social Security numbers, job and earnings history, addresses, disability records, and family relationships)	Cisco ASA
66.92.20.231	oktavpn.usip.org	U.S. Institute for Peace (Diplomatic strategy, conflict-resolution efforts, foreign policy networks, ally communications, and sensitive peacebuilding initiatives)	Cisco ASA
38.143.109.201	vpn.csis.org	U.S. Center for Strategic and International Studies (National security policy, geopolitical research, government and defense contacts, and global strategic forecasting)	Cisco ASA
154.44.0.165	cloud-wfhvpn.tsmc.com	Taiwan Semiconductor - TSMC (Advanced semiconductor manufacturing processes, chip designs, technology supply chains, and chip production capabilities)	Cisco ASA
154.49.127.17	vpn-y12nongfe.cns.doe.gov	U.S. Department of Energy - Y-12 National Security Complex (U.S. Nuclear weapons stockpile management, uranium processing operations, nuclear weapons technologies and security)	Cisco ASA



Malicious IP	Target Domain	Target Org	Target System
23.137.253.132	ssavpn.ssa.gov	U.S. Social Security Administration (Holds Social Security numbers, job and earnings history, addresses, disability records, and family relationships)	Cisco ASA
66.92.20.231	oktavpn.usip.org	U.S. Institute for Peace (Diplomatic strategy, conflict-resolution efforts, foreign policy networks, ally communications, and sensitive peacebuilding initiatives)	Cisco ASA
38.143.109.201	vpn.csis.org	U.S. Center for Strategic and International Studies (National security policy, geopolitical research, government and defense contacts, and global strategic forecasting)	Cisco ASA
154.44.0.165	cloud-wfhvpn.tsmc.com	Taiwan Semiconductor - TSMC (Advanced semiconductor manufacturing processes, chip designs, technology supply chains, and chip production capabilities)	Cisco ASA
154.49.127.17	vpn-y12nongfe.cns.doe.gov	U.S. Department of Energy - Y-12 National Security Complex (U.S. Nuclear weapons stockpile management, uranium processing operations, nuclear weapons technologies and security)	Cisco ASA



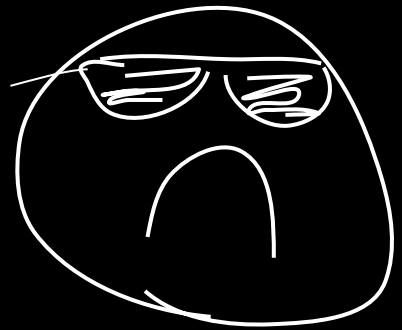
Malicious IP	Target Domain	Target Org	Target System
23.137.253.132	ssavpn.ssa.gov	U.S. Social Security Administration (Holds Social Security numbers, job and earnings history, addresses, disability records, and family relationships)	Cisco ASA
66.92.20.231	oktavpn.usip.org	U.S. Institute for Peace (Diplomatic strategy, conflict-resolution efforts, foreign policy networks, ally communications, and sensitive peacebuilding initiatives)	Cisco ASA
38.143.109.201	vpn.csis.org	U.S. Center for Strategic and International Studies (National security policy, geopolitical research, government and defense contacts, and global strategic forecasting)	Cisco ASA
154.44.0.165	cloud-wfhvpn.tsmc.com	Taiwan Semiconductor - TSMC (Advanced semiconductor manufacturing processes, chip designs, technology supply chains, and chip production capabilities)	Cisco ASA
154.49.127.17	vpn-y12nongfe.cns.doe.gov	U.S. Department of Energy - Y-12 National Security Complex (U.S. Nuclear weapons stockpile management, uranium processing operations, nuclear weapons technologies and security)	Cisco ASA



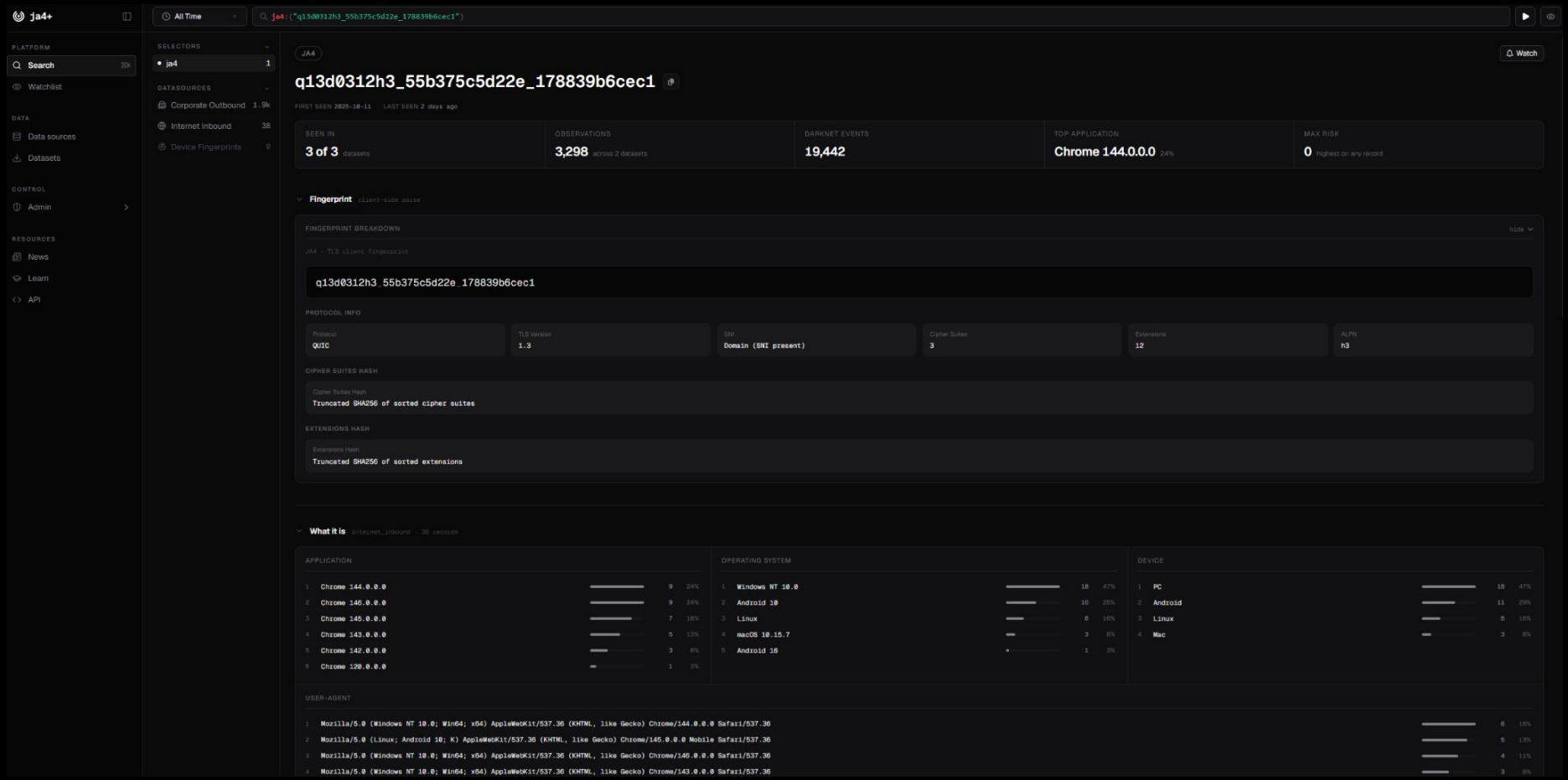
Malicious IP	Target Domain	Target Org	Target System
23.137.253.132	ssavpn.ssa.gov	U.S. Social Security Administration (Holds Social Security numbers, job and earnings history, addresses, disability records, and family relationships)	Cisco ASA
66.92.20.231	oktavpn.usip.org	U.S. Institute for Peace (Diplomatic strategy, conflict-resolution efforts, foreign policy networks, ally communications, and sensitive peacebuilding initiatives)	Cisco ASA
38.143.109.201	vpn.csis.org	U.S. Center for Strategic and International Studies (National security policy, geopolitical research, government and defense contacts, and global strategic forecasting)	Cisco ASA
154.44.0.165	cloud-wfhvpn.tsmc.com	Taiwan Semiconductor - TSMC (Advanced semiconductor manufacturing processes, chip designs, technology supply chains, and chip production capabilities)	Cisco ASA
154.49.127.17	vpn-y12nongfe.cns.doe.gov	U.S. Department of Energy - Y-12 National Security Complex (U.S. Nuclear weapons stockpile management, uranium processing operations, nuclear weapons technologies and security)	Cisco ASA



Malicious IP	Target Domain	Target Org	Target System
23.137.253.132	ssavpn.ssa.gov	U.S. Social Security Administration (Holds Social Security numbers, job and earnings history, addresses, disability records, and family relationships)	Cisco ASA
66.92.20.231	oktavpn.usip.org	U.S. Institute for Peace (Diplomatic strategy, conflict-resolution efforts, foreign policy networks, ally communications, and sensitive peacebuilding initiatives)	Cisco ASA
38.143.109.201	vpn.csis.org	U.S. Center for Strategic and International Studies (National security policy, geopolitical research, government and defense contacts, and global strategic forecasting)	Cisco ASA
154.44.0.165	cloud-wfhvpn.tsmc.com	Taiwan Semiconductor - TSMC (Advanced semiconductor manufacturing processes, chip designs, technology supply chains, and chip production capabilities)	Cisco ASA
154.49.127.17	vpn-y12nongfe.cns.doe.gov	U.S. Department of Energy - Y-12 National Security Complex (U.S. Nuclear weapons stockpile management, uranium processing operations, nuclear weapons technologies and security)	Cisco ASA



There was no malware
There was no Zero-Day
There were only packets


ja4+
All Time
ja4:("q13d0312h3_55b375c5d22e_178839b6cec1")
PLATFORM
Search
Watchlist
DATA
Data sources
Datasets
CONTROL
Admin
RESOURCES
News
Learn
API
SELECTORS
ja4 1
DATASOURCES
Corporate Outbound 1.9k
Internet Inbound 38
Device Fingerprints 0
JA4
Watch
q13d0312h3_55b375c5d22e_178839b6cec1
FIRST SEEN 2025-10-11 LAST SEEN 2 days ago
SEEN IN
3 of 3 datasets
OBSERVATIONS
3,298 across 2 datasets
DARKNET EVENTS
19,442
TOP APPLICATION
Chrome 144.0.0.0 24%
MAX RISK
0 highest on any record
Fingerprint client-side source
FINGERPRINT BREAKDOWN
hide
JA4 · TLS client fingerprint
q13d0312h3_55b375c5d22e_178839b6cec1
PROTOCOL INFO
Protocol
QUIC
TLS Version
1.3
SNI
Domain (SNI present)
Cipher Suites
3
Extensions
12
ALPN
h3
CIPHER SUITES HASH
Cipher Suites Hash
Truncated SHA256 of sorted cipher suites
EXTENSIONS HASH
Extensions Hash
Truncated SHA256 of sorted extensions
What it is internet_inbound · 38 records
APPLICATION
1 Chrome 144.0.0.0 9 24%
2 Chrome 146.0.0.0 9 24%
3 Chrome 145.0.0.0 7 18%
4 Chrome 143.0.0.0 5 13%
5 Chrome 142.0.0.0 3 8%
6 Chrome 120.0.0.0 1 3%
OPERATING SYSTEM
1 Windows NT 10.0 18 47%
2 Android 10 10 26%
3 Linux 6 16%
4 macOS 10.15.7 3 8%
5 Android 16 1 3%
DEVICE
1 PC 18 47%
2 Android 11 29%
3 Linux 6 16%
4 Mac 3 8%
USER-AGENT
1 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36 6 16%
2 Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Mobile Safari/537.36 5 13%
3 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/146.0.0.0 Safari/537.36 4 11%
4 Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36 3 8%

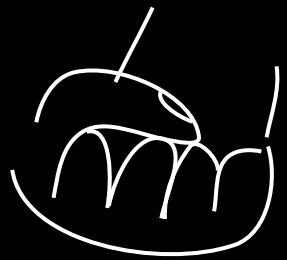
JA4+ Enabled SW & HW Firewall / WAF / NDR

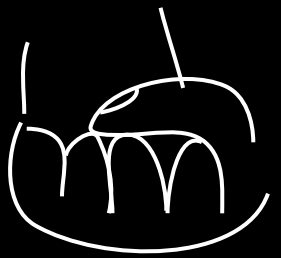
Feature	Proxy	Agent
eBPF/XDP Packet Filtering	✅	✅
Access Rules (4M IPv4 / 1M IPv6 CIDRs)	✅	✅
CIDR Coalescing	✅	✅
JA4T · JA4TS · JA4L · JA4LS (TCP/IP fingerprints)	✅	✅
IDS / Intrusion Detection	✅	✅
Threat Intelligence & GeoIP	✅	✅
BPF Stats & TCP Fingerprinting	✅	✅
Event Sending (Fingerprint + IDS)	✅	✅
Terminal TUI (ratatui)	✅	✅
File / Syslog / ETW Logging	✅	✅
Windows Service (SCM)	✅	✅
HTTP/HTTPS Reverse Proxy	✅	❌
TLS & ACME Certificates	✅	❌
JA4 · JA4H · JA4S · JA4X (application fingerprints)	✅	❌
WAF (Wirefilter expressions)	✅	❌
Rate Limiting	✅	❌
CAPTCHA Protection	✅	❌
Content Scanning (ClamAV)	✅	❌
Windows Support	⚠️ Agent features only	✅





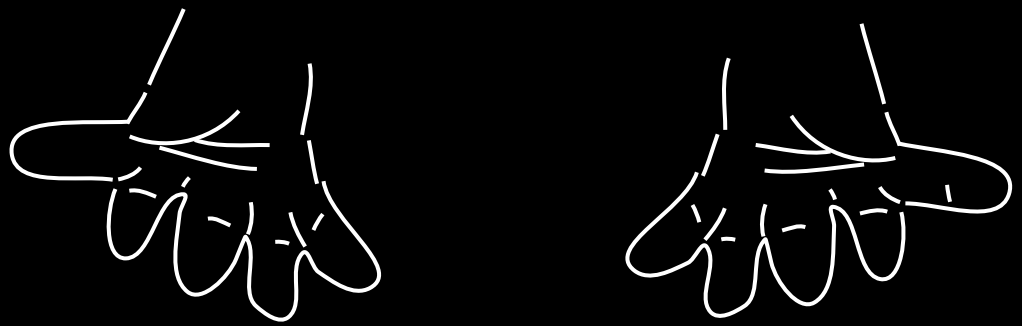
GIVE IT TO ME NOW







GIVE IT TO ME NOW



JA4+

foxio.io

ja4db.foxio.io

github.com/foxio-llc/ja4

github.com/foxio-llc/ja4tscan

github.com/foxio-llc/ja4scan-tls

https://github.com/foxio-llc/ja4-go

License

- JA4+ is open source, free, licensed under the FoxIO License
  - Monetization requires OEM License
  - OEM License is free for nonprofits, small businesses and startups
  - All methods are patented or patent-pending


censys
paloalto NETWORKS
VECTRA
WIRESHARK
ExtraHop
CLOUDFLARE
zeek
Vercel
nzyme
Arkime
fastly
f5
Security Onion
ENEA
Hunt.io
eSENTIRE
amazon cloudfront
Google Cloud
MISP Threat Sharing
GREY NOISE
Akamai
NGINX
TEAM CYMRU
SURICATA



foxio.io

Session Feedback

John Althouse
john@foxio.io

@4A4133

in/johnalthouse

