**Dridex Traffic Analysis**

**Introduction:** Dridex is a long-running banking trojan that first appeared around 2011, primarily spread through malicious email attachments and macros. It is significant because it evolved from simple credential theft into a modular malware platform capable of delivering ransomware and other payloads, often used by organized cybercriminal groups. Understanding its network traffic, especially encrypted C2 communications, helps defenders develop detection strategies that remain effective even when attackers attempt to hide behind TLS encryption.

**Objective:** Analyze actual Dridex traffic from Palo Alto Unit42 PCAP dataset.

**Tools used:** Wireshark, Suricata,MITRE ATT&CK framework.

**Focus areas**:

* Identify malicious TLS/SSL traffic patterns.
* Examine suspicious certificates and handshake behavior.
* Write detection rules that do not rely on payload decryption.
* Map observations to adversary TTPs.

**Dataset:** Palo Alto Unit42 Dridex PCAPs (https://github.com/pan-unit42/wireshark-tutorial-Dridex-traffic)

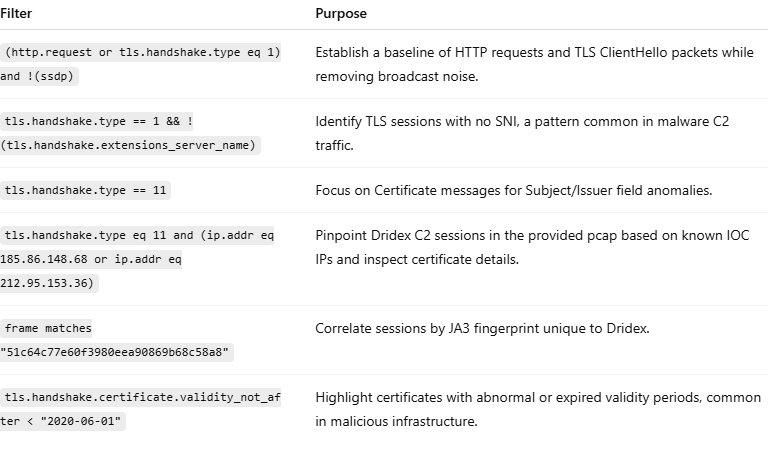
**Methodology:**

**Wireshark Setup:**

* Built initial customized layout for enhanced HTTP traffic analysis then further tuned it for TLS analysis, adding columns for metadata such as Sever Name Indication (SNI), JA3 fingerprints, and TLS version. (Certificate details such as Subject CN and Issuer were inspected manually as opposed to adding these fields to the configuration, since my build does not expose per-RDN fields as clean column options.)

**Filtering strategy:**

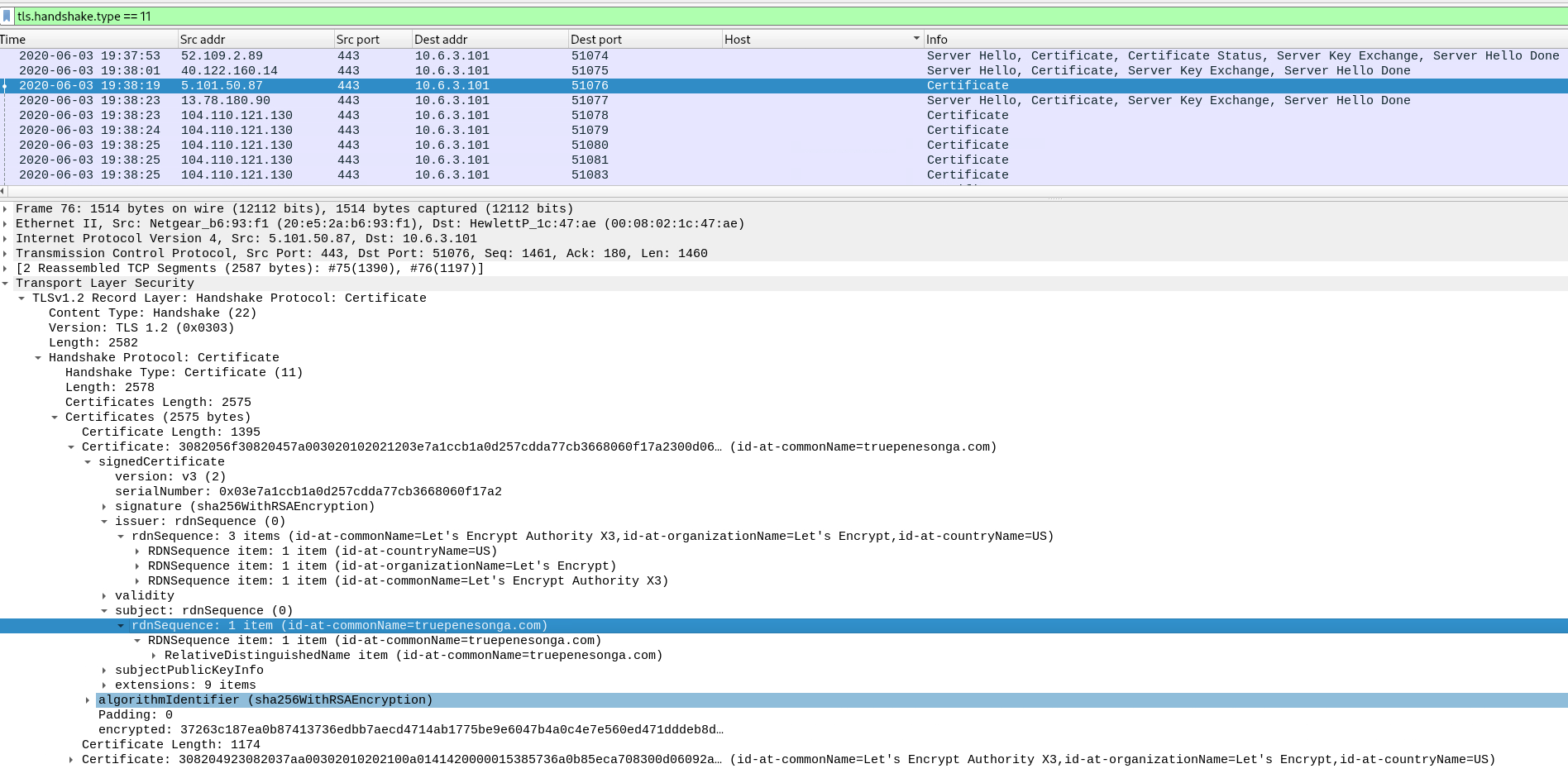
* To isolate Dridex infection and post-infection C2 traffic, I built progressive display filters that targeted TLS handshake anomalies, certificate metadata, and JA3 fingerprints. Rather than simply pivoting on IPs, the focus was on protocol behaviors more indicative of malicious activity. *See* ***Table 1***.

**Table 1**: Wireshark display filters applied during analysis.

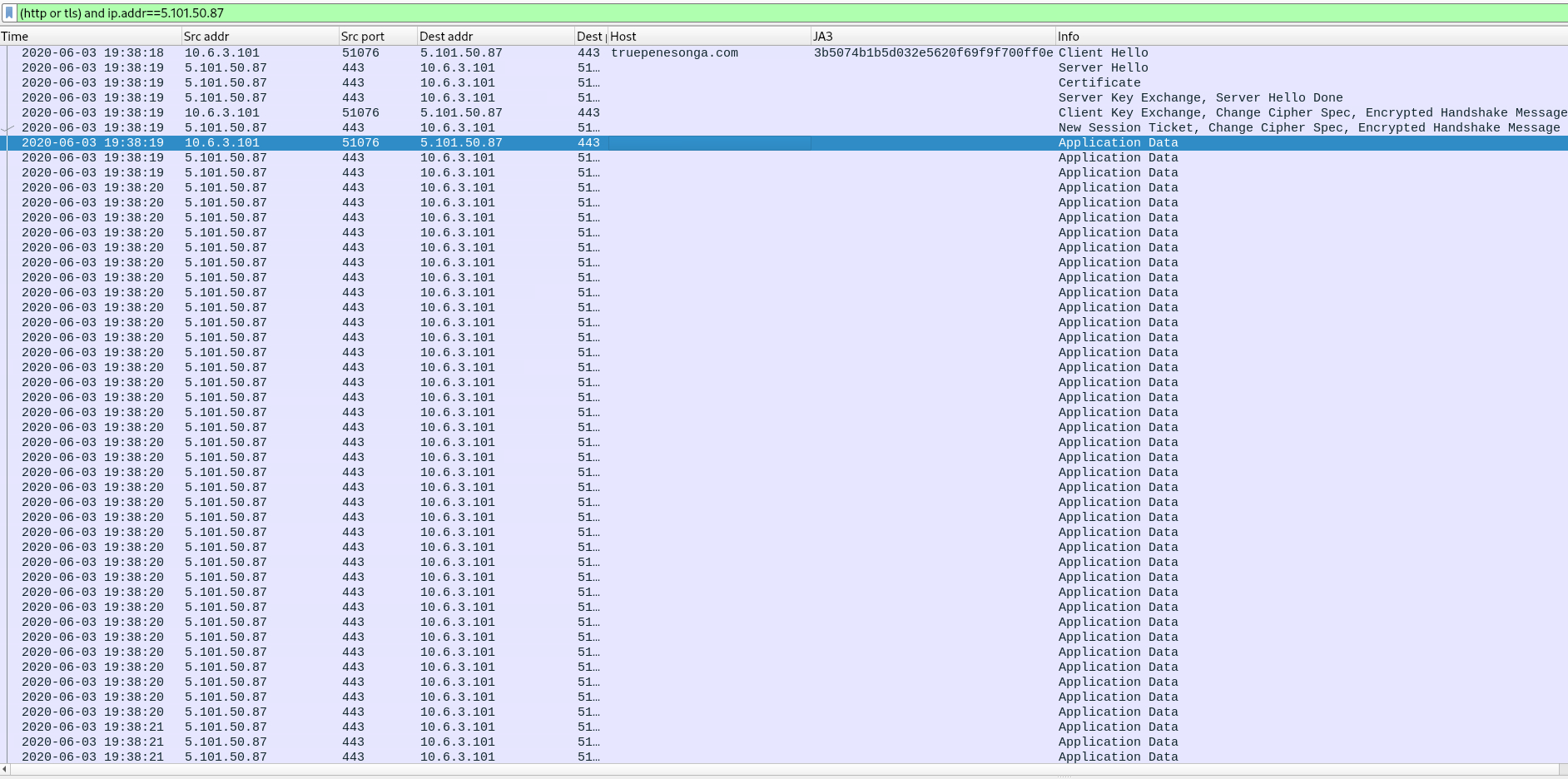
**Timeline and Flow of Infection:**

**Initial Contact/Loader Download**

* Client reaches truepenesonga[.]com
* Let’s Encrypt CA is not malicious on its own, but domain is known malicious.
* The post-handshake bulk TLS application data is consistent with a staged payload download (Dridex loader); when correlated with the malicious domain and JA3 fingerprint, this exchange marks the start of the infection chain.



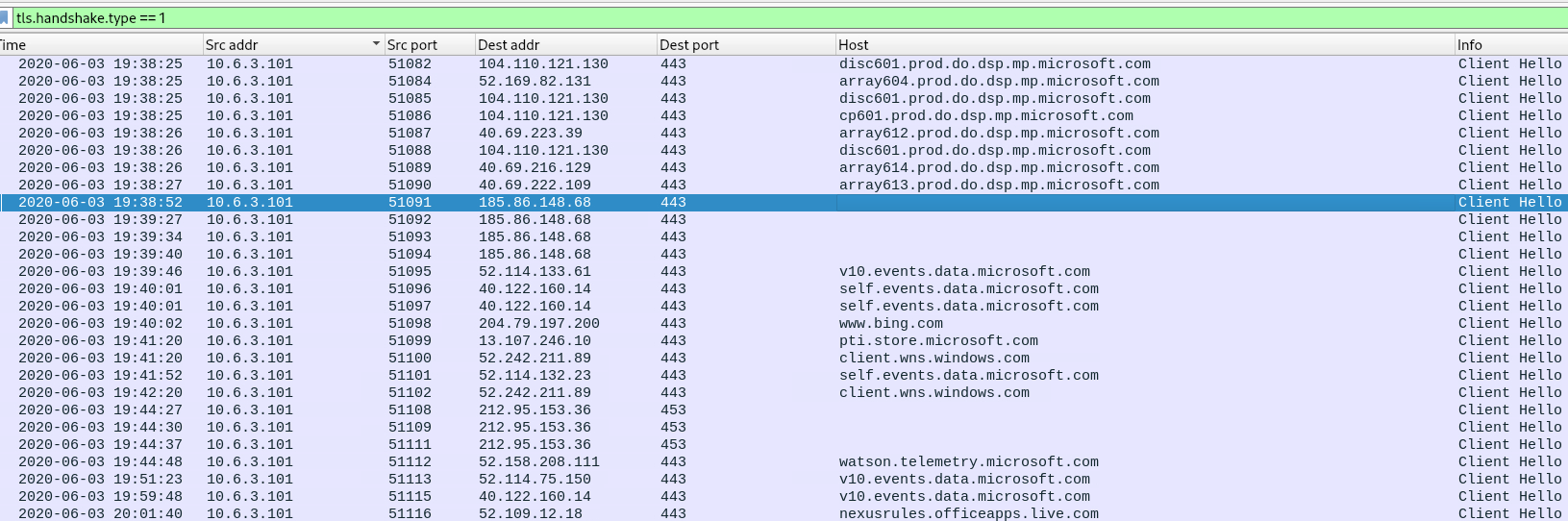
**Figure 1**: TLS handshake to truepenesonga[.]com showing certificate chain issued by Let’s Encrypt Authority X3. The presence of a legitimate CA does not imply trust — this domain is confirmed malicious and served as the Dridex loader distribution host.



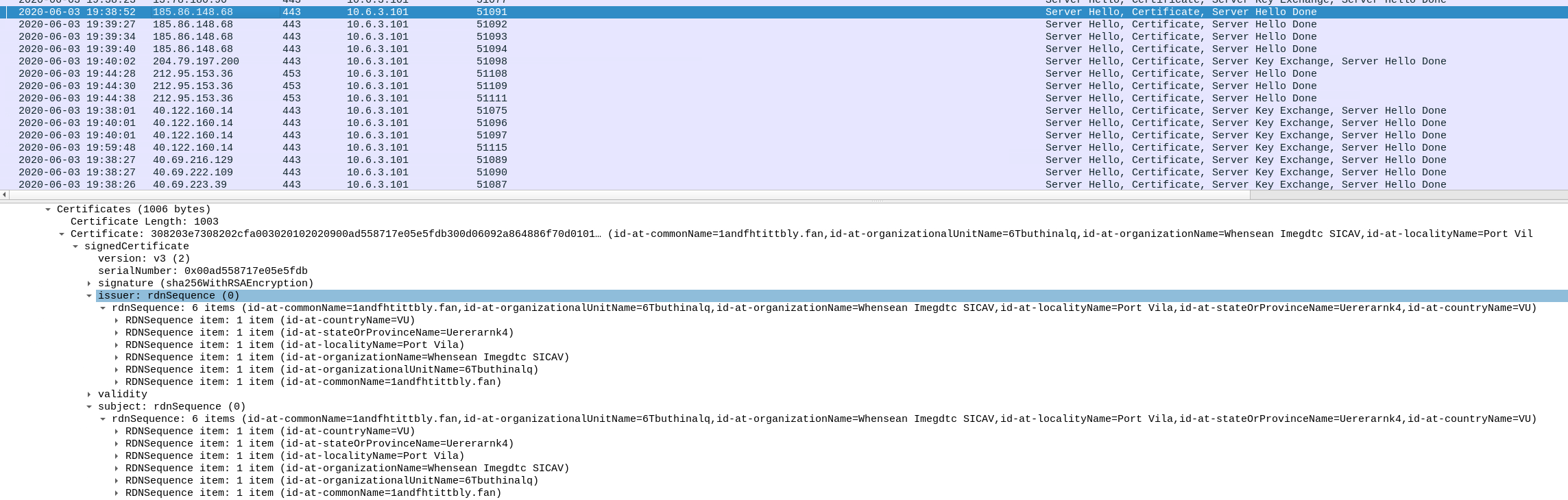
**Figure 2**: Encrypted TLS Application Data exchange between the victim host and truepenesonga[.]com immediately following the handshake. This traffic likely represents the download of the Dridex loader payload from the malicious domain over HTTPS, concealed within legitimate-appearing encrypted communication.

**Post-Infection Command-and Control (C2) Activity**

* Following execution of the loader, the infected host initiates new TLS sessions to two raw IP addresses (185.86.148[.]68, 212.95.153[.]36) with no associated domain names.
* These sessions exhibit a distinct JA3 fingerprint (51c64c77e60f3980eea90869b68c58a8) compared to the loader’s (3b5074b1b5d032e5620f69f9f700ff0e), indicating a process transition—likely from the downloader to the Dridex payload—and the use of a different TLS stack.
* The presented X.509 certificates contain randomized alphanumeric subject and issuer fields and lack Subject Alternative Name (SAN) entries, consistent with auto-generated or self-signed certificates frequently observed in malware C2 infrastructure.
* Although the encrypted payload prevents direct validation of the exchanged content, the timing, JA3 shift, and anomalous TLS characteristics strongly suggest these sessions represent Dridex post-compromise C2 or stage-retrieval activity.



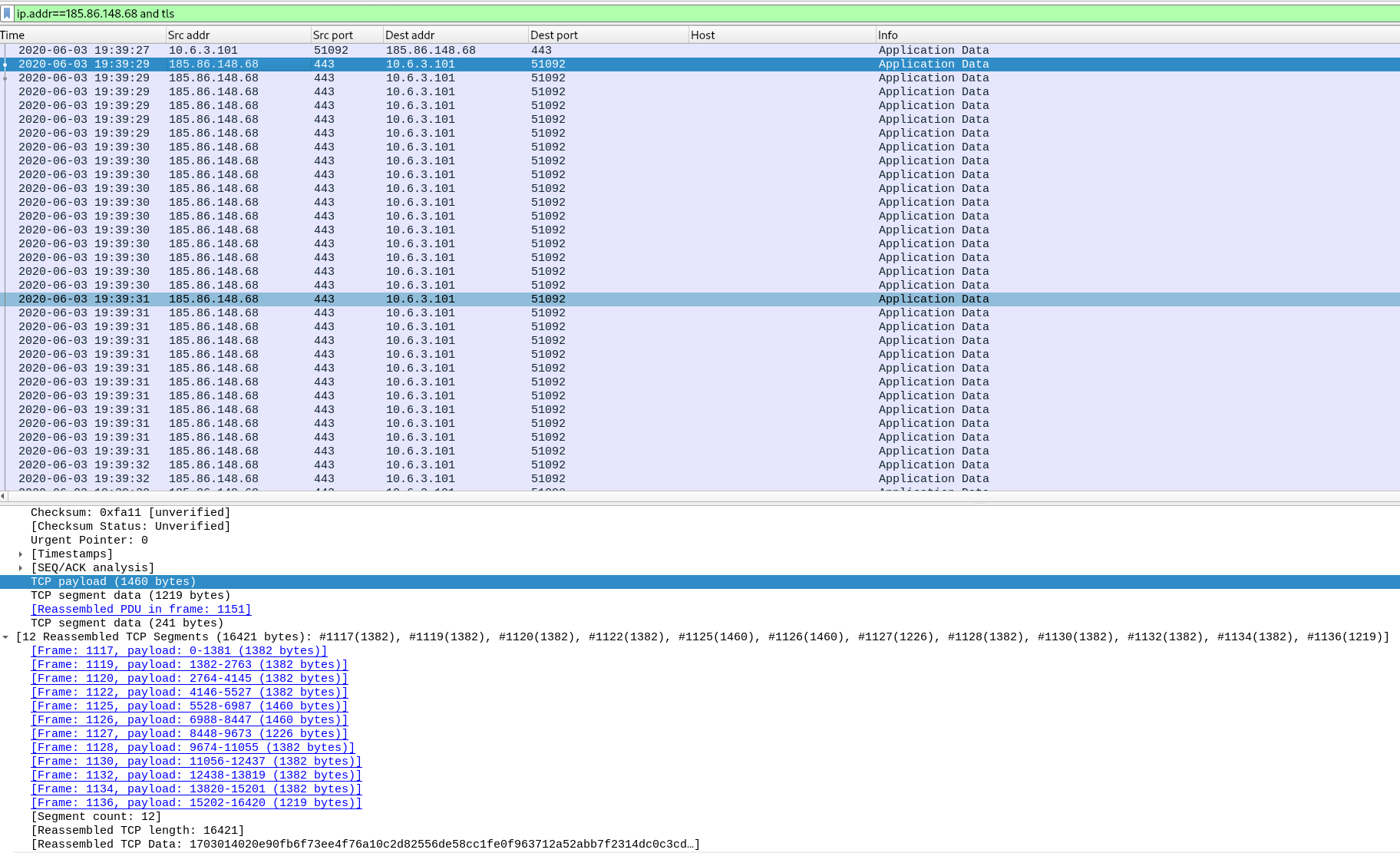
**Figure 3**: Overview of TLS ClientHello packets observed immediately after the loader stage. The host begins new TLS sessions to raw IP addresses (185.86.148[.]68, 212.95.153[.]36) alongside normal Microsoft telemetry traffic. These bare-IP handshakes mark the pivot from the benign loader phase toward the suspected Dridex C2 communication, examined in subsequent figures that highlight the absence of SNI and certificate irregularities.



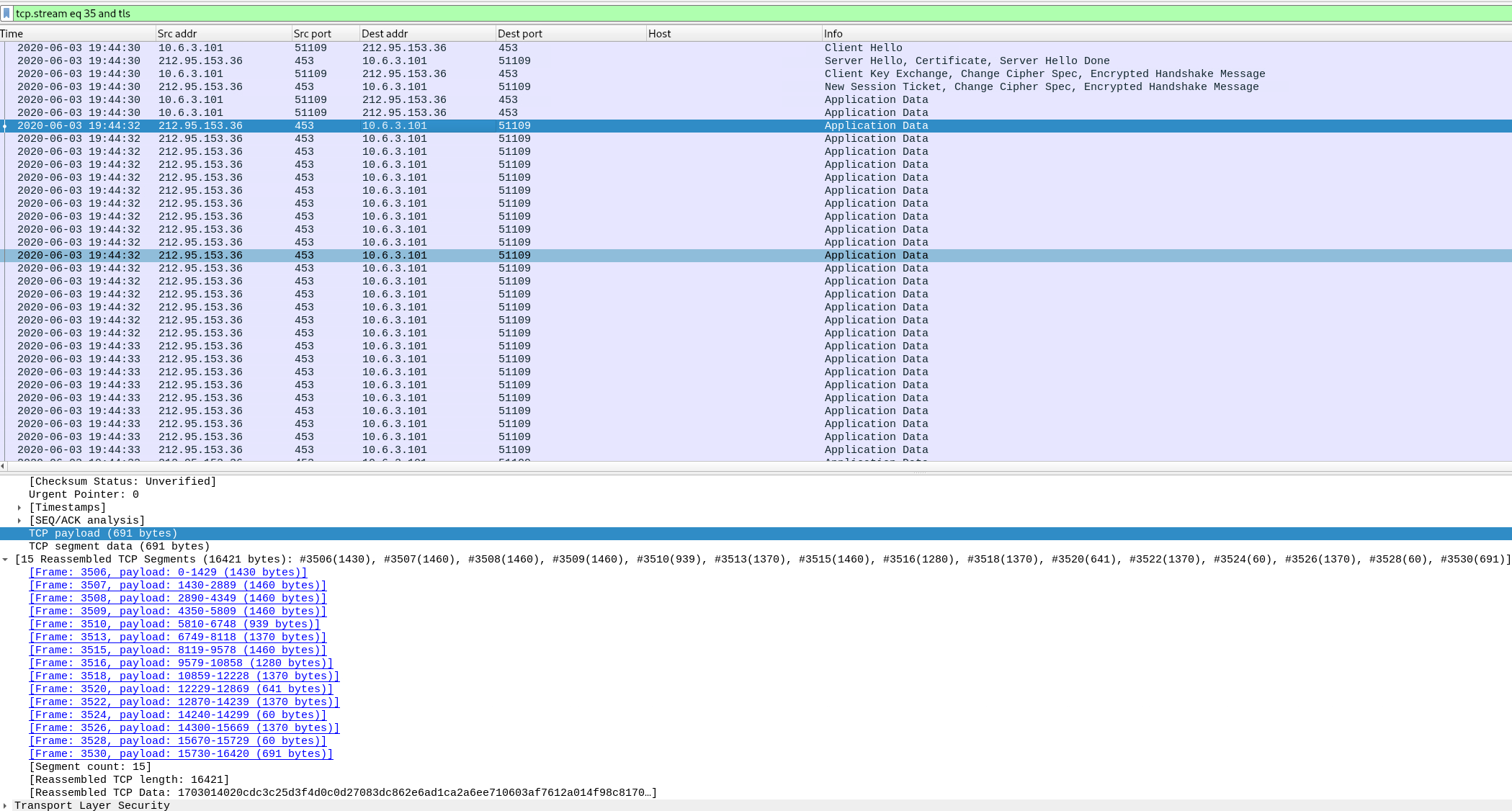
**Figure 4**: TLS ServerHello and Certificate exchange for the C2 IP (185.86.148[.]68). The session contains no Server Name Indication (SNI) value and presents an X.509 certificate with no Subject Alternative Name (SAN) and randomized issuer/subject fields (e.g., “landfhtbtly.fan,” “GTbuthinlq”). These anomalies—combined with direct IP communication and the timing of the session—are strong indicators of auto-generated or self-signed certificates commonly used in Dridex C2 infrastructure. Similar characteristics were observed for the second C2 IP (212.95.153[.]36).

**Behavioral Indicators and Traffic Characteristics**

* Bulk Transfer Behavior
  + TLS Application Data bursts (~16 KB) segmented across ~40 packets within 3 seconds suggest a large stage or payload download rather than interactive beaconing.
  + A second burst from 212.95.153[.]36 follows immediately, likely retrieving a secondary module.



**Figure 5:** TLS Application Data burst from 185.86.148.68.



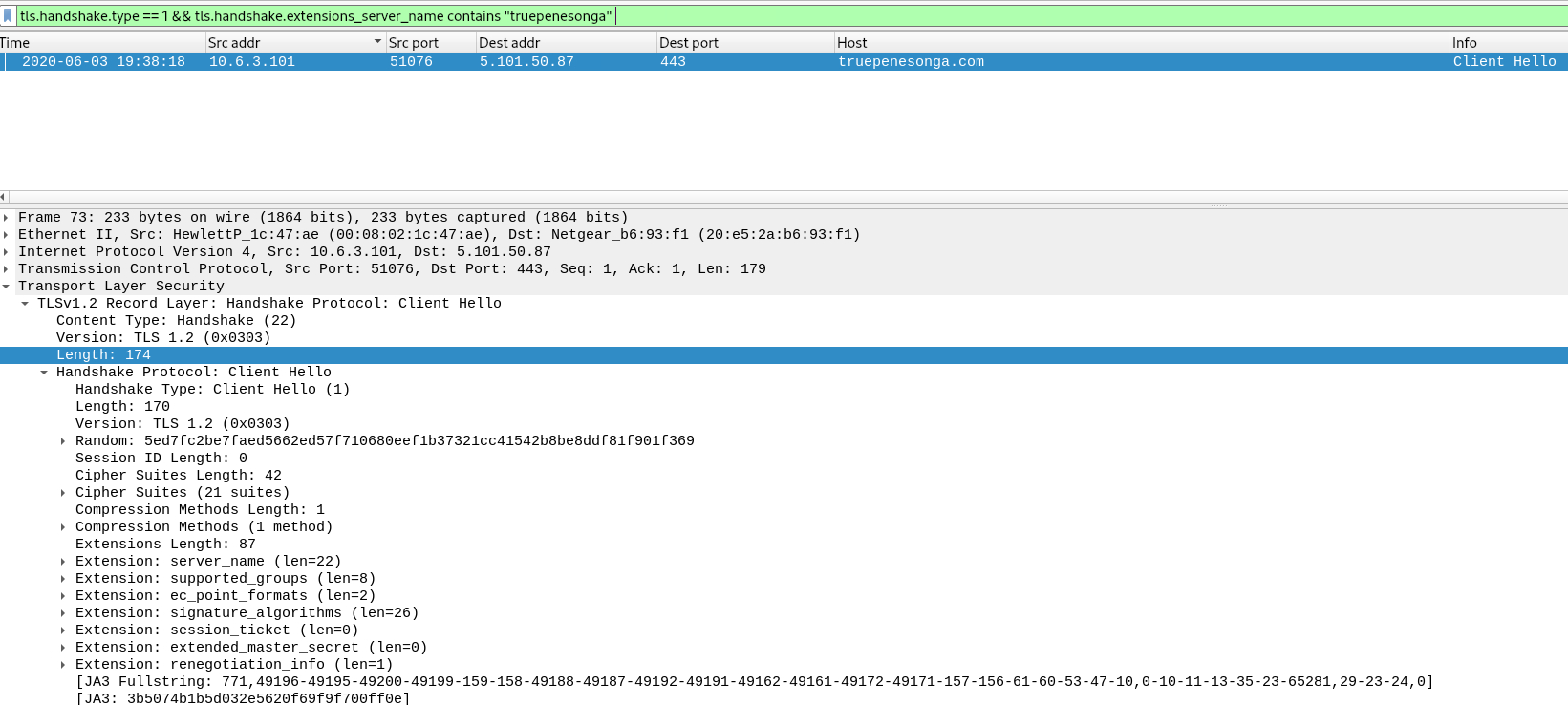
**Figure 6:** Subsequent burst from 212.95.153.36.

**JA3 Fingerprint Analysis**

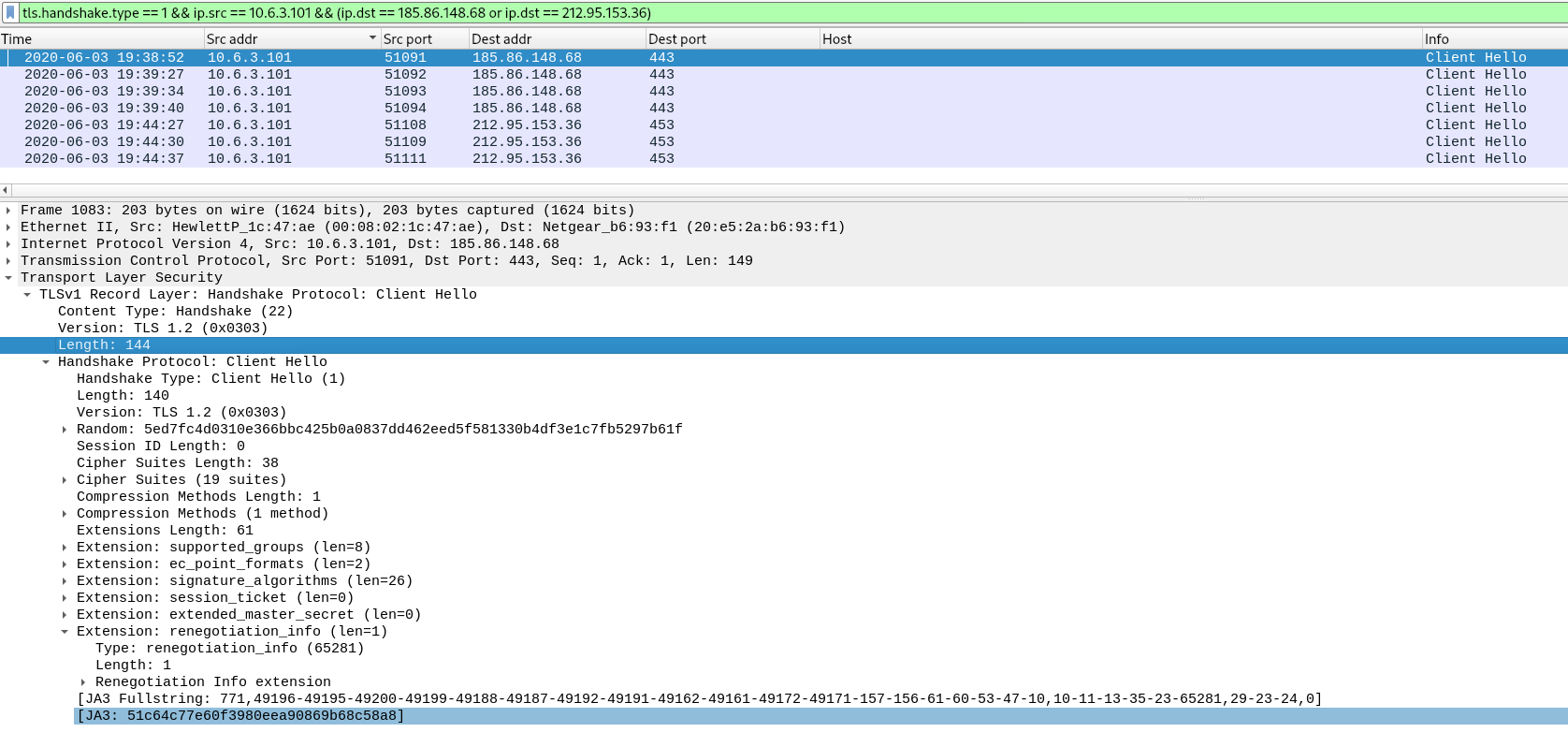
During analysis of the Dridex infection traffic, TLS ClientHello messages were inspected to extract JA3 fingerprints—hashes derived from TLS parameters (cipher suites, extensions, elliptic curves, etc.) that uniquely characterize a client’s TLS implementation.

While JA3 values are not inherently malicious, they provide consistent identifiers for TLS stacks often reused by specific malware families.

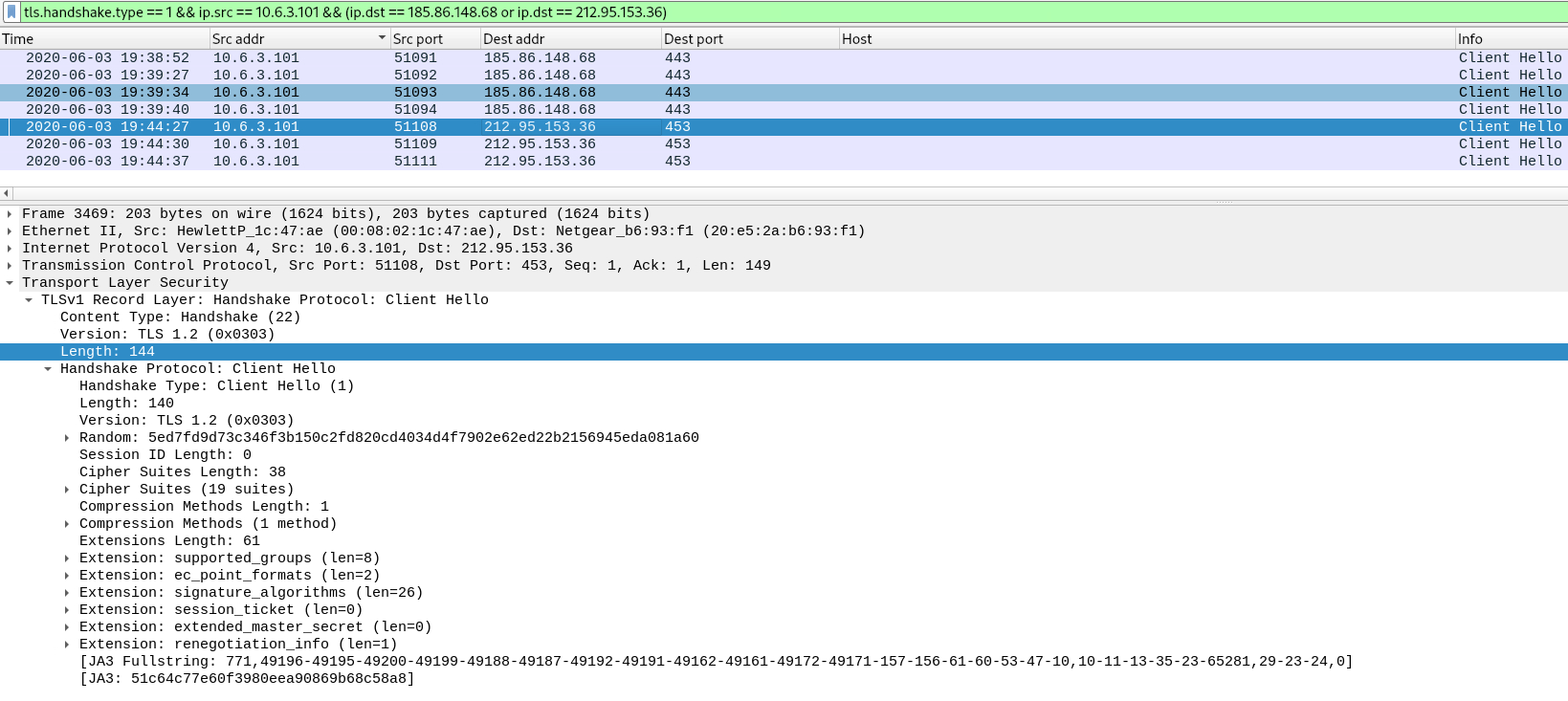
* **Observed Values:**
  + **3b5074b1b5d032e5620f69f9f700ff0e** – Observed in TLS connections to truepenesonga[.]com. According to open-source threat intelligence, including entries on AlienVault OTX and Netresec’s malware TLS research, this JA3 has previously been linked to Dridex downloaders and similar malware families
  + **51c64c77e60f3980eea90869b68c58a8** – Observed consistently in subsequent TLS sessions to the C2 IPs 185.86.148[.]68 and 212.95.153[.]36.
    - These sessions contained no Server Name Indication (SNI) and used bare IP addresses, consistent with malware-internal TLS communications.
    - The fingerprint remained identical across both C2 endpoints, suggesting reuse of the same embedded TLS library by the Dridex payload.
* **Interpretation:**
  + The host initially contacted truepenesonga[.]com using JA3 3b5074b1b5d032e5620f69f9f700ff0e (Figure 5). Immediately afterward, it initiated bare-IP TLS sessions to 185.86.148[.]68 and 212.95.153[.]36 using JA3 51c64c77e60f3980eea90869b68c58a8 (Figures 6–7).
  + The consistent reuse of the second JA3 across multiple C2 IPs reinforces attribution, as legitimate applications rarely change TLS stacks mid-session sequence.



**Figure 7:** ClientHello to truepenesonga[.]com showing JA3 3b5074b1b5d032e5620f69f9f700ff0e.



**Figure 8:** ClientHello to 185.86.148[.]68 showing JA3 51c64c77e60f3980eea90869b68c58a8 and no SNI.



**Figure 9:** ClientHello to 212.95.153[.]36 showing identical JA3 51c64c77e60f3980eea90869b68c58a8 and no SNI.

**Detection Opportunities**