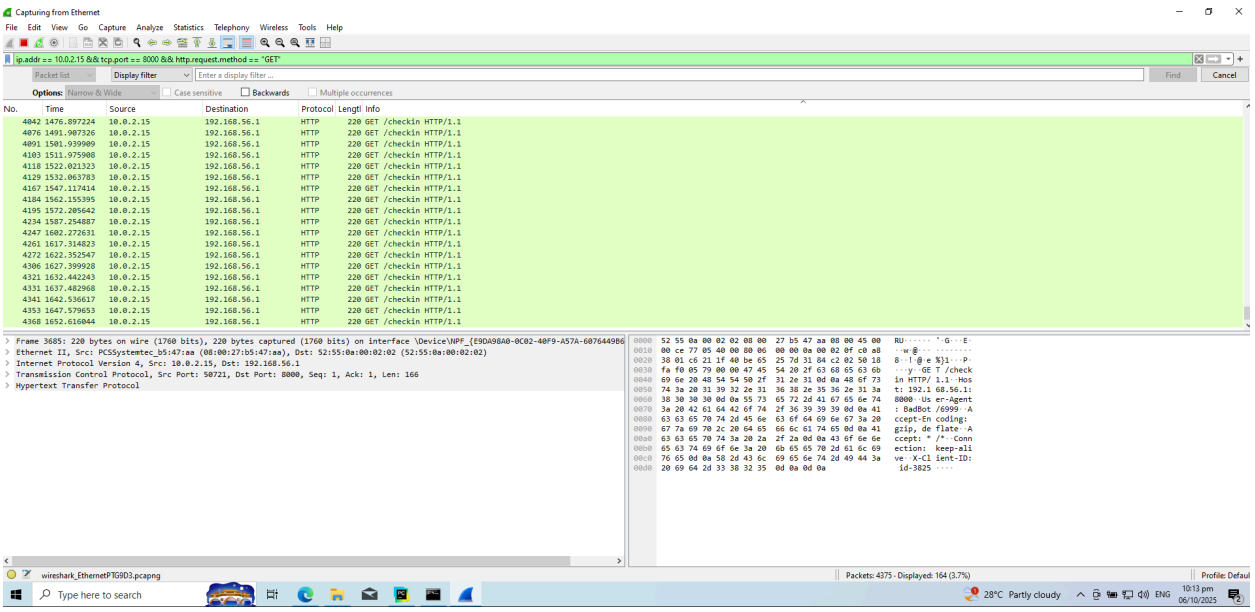
(note: Please read the README.md before opening this)
Some Pictures may be blurry this is intentional because I don't want to put sensitive raw information online, Raw files are available upon request including the PCAP

WireShark Network Traffic Analysis
By CrawfordFan223

This is my First Ever project uploaded on GitHub, I am a Third Year BSIT Student specializing in Cybersecurity! Enjoy!

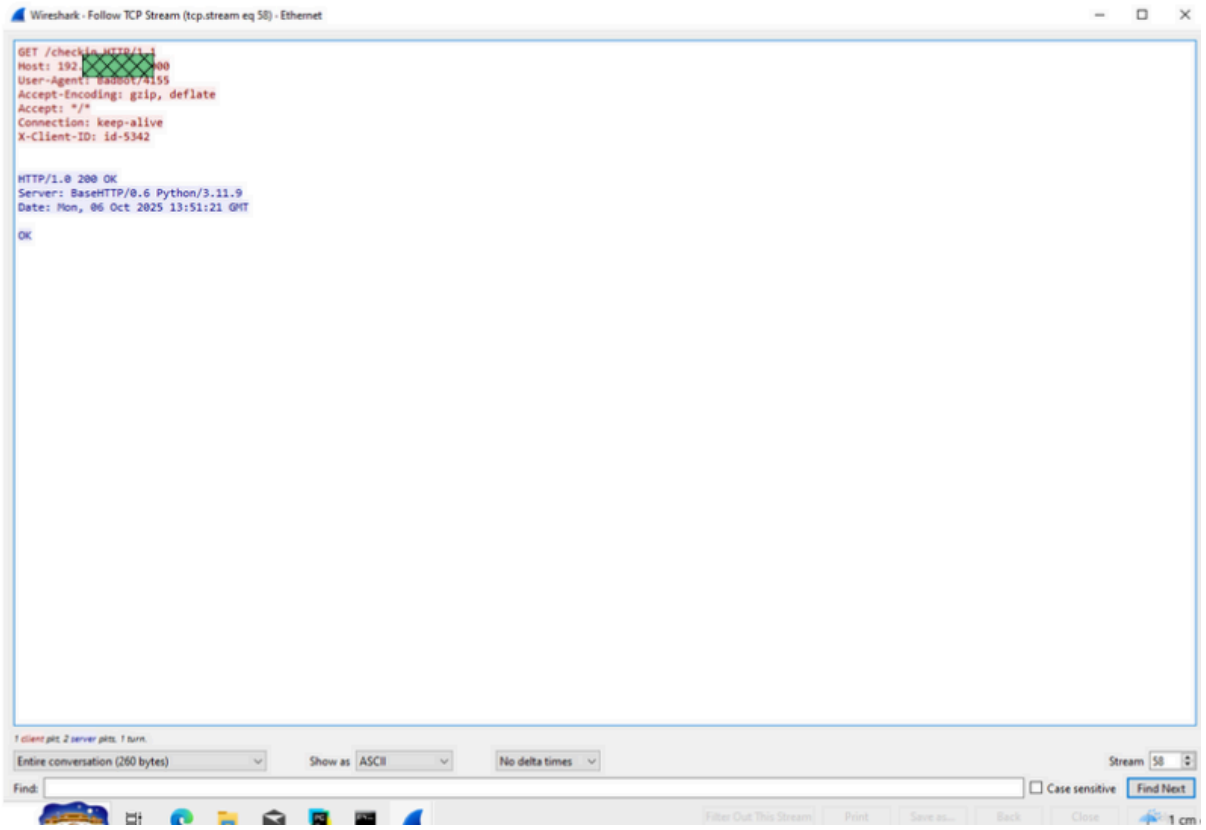


Packet list filtered for GET /checkin showing repeated requests and timestamps.

Description: Packet list filtered for GET requests.
Observation: Multiple `GET /checkin` entries spaced at ~1s intervals.
Interpretation: Confirms automated periodic beaconing behavior.
Wireshark Filter Used:

```
ip.addr == 10.0.2.15 && tcp.port == 8000 &&
http.request.method == "GET"
```

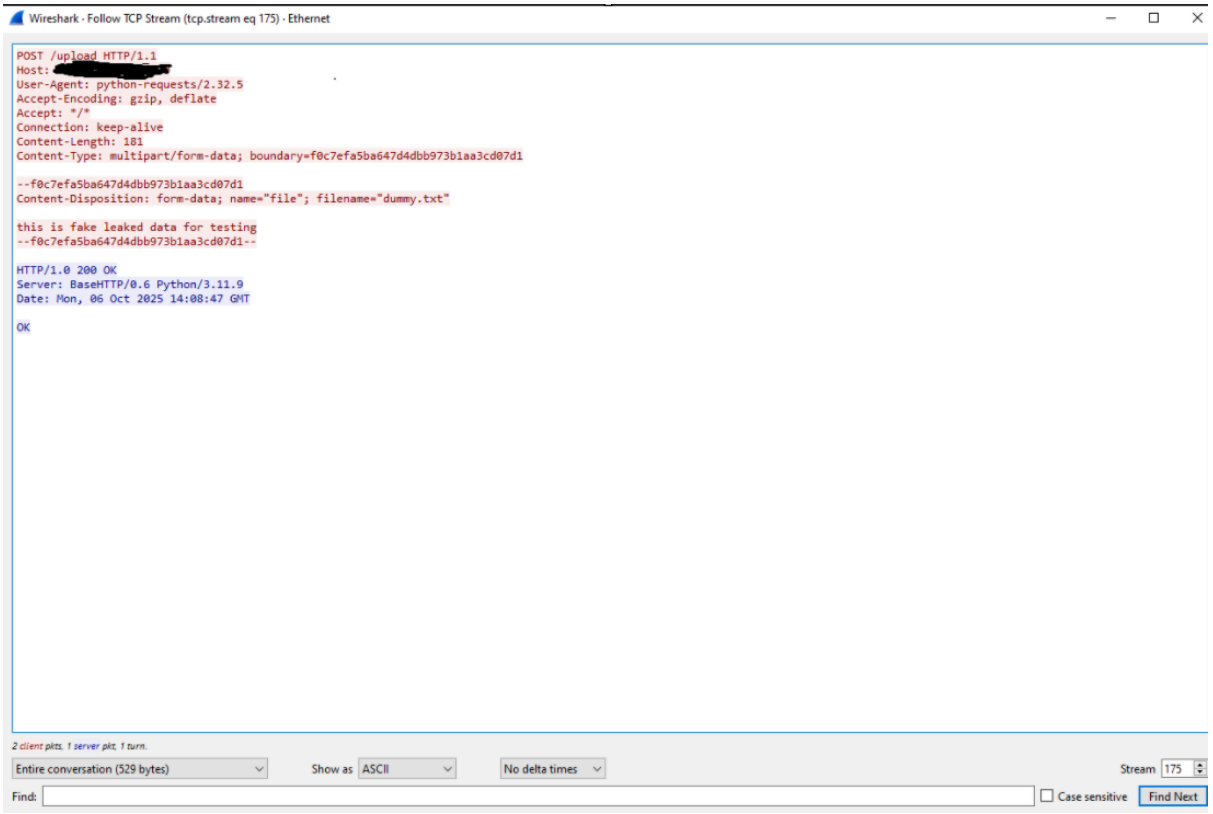
(note: Please read the README.md before opening this)
Some Pictures may be blurry this is intentional because I don't want to put sensitive raw information online, Raw files are available upon request including the PCAP
Packet list filtered for GET /checkin showing repeated requests and timestamps.



Follow TCP Stream (GET): plaintext `GET /checkin` and server `200 OK` — beaconing visible in the capture.

Description: Follow TCP Stream of `GET /checkin`.
Observation: Plaintext HTTP request with headers: `User-Agent: BadBot/4155`, `X-Client-ID: id-5342` and `HTTP/1.0 200 OK` response.
Interpretation: Confirms periodic beaconing from the VM to the host.

(note: Please read the README.md before opening this)
Some Pictures may be blurry this is intentional because I don't want to put sensitive raw information online, Raw files are available upon request including the PCAP



Follow TCP Stream (POST): multipart upload with file contents visible — plaintext exfiltration.

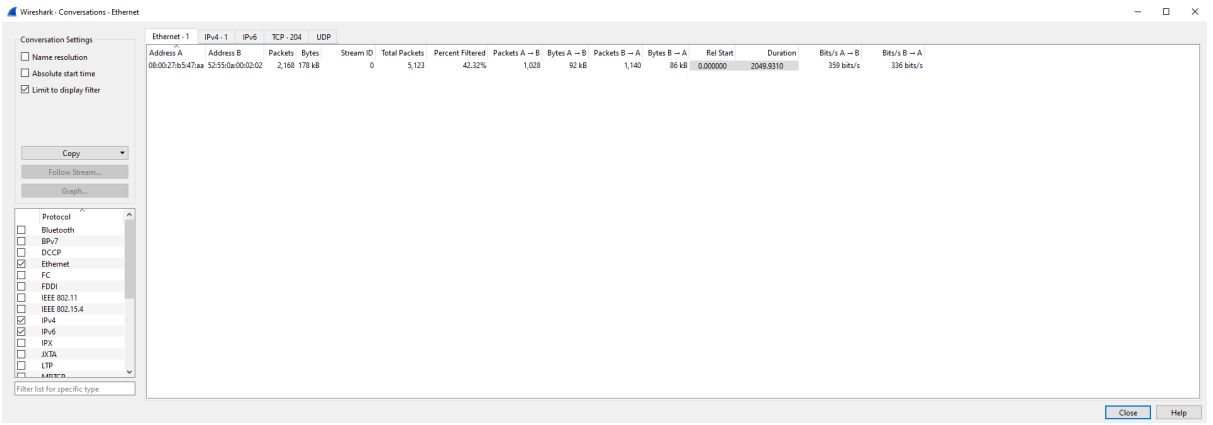
Description: Follow TCP Stream of `POST /upload`.

Observation: `multipart/form-data` request with `dummy.txt` contents visible.
Example body snippet:

```
Content-Disposition: form-data; name="file";
filename="dummy.txt"
this is fake leaked data for testing
```

Interpretation: Demonstrates plaintext data exfiltration.

(note: Please read the README.md before opening this)
Some Pictures may be blurry this is intentional because I don't want to put sensitive raw information online, Raw files are available upon request including the PCAP

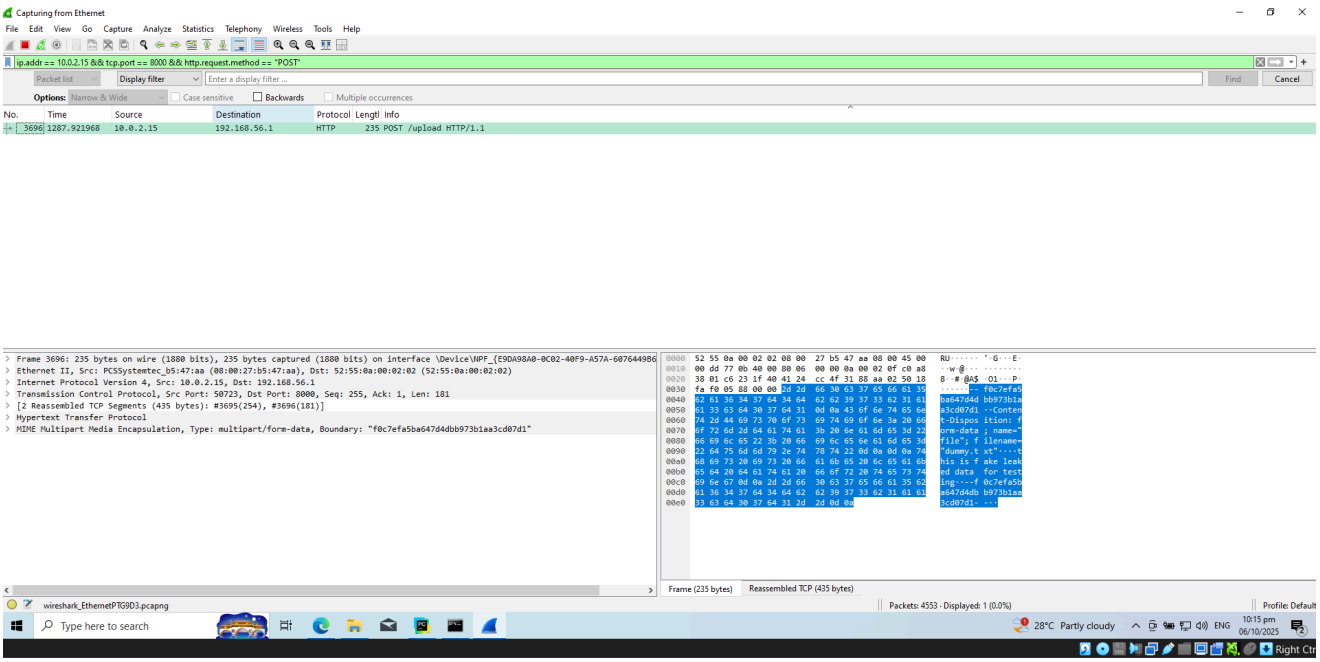


Conversations: quantifies packet count, bytes, and session duration between attacker VM and host.

Description: *Wireshark "Conversations" view showing IP pairs, packet counts, bytes, and duration.*

Observation: *One dominant conversation between VM (attacker) and host (receiver).*

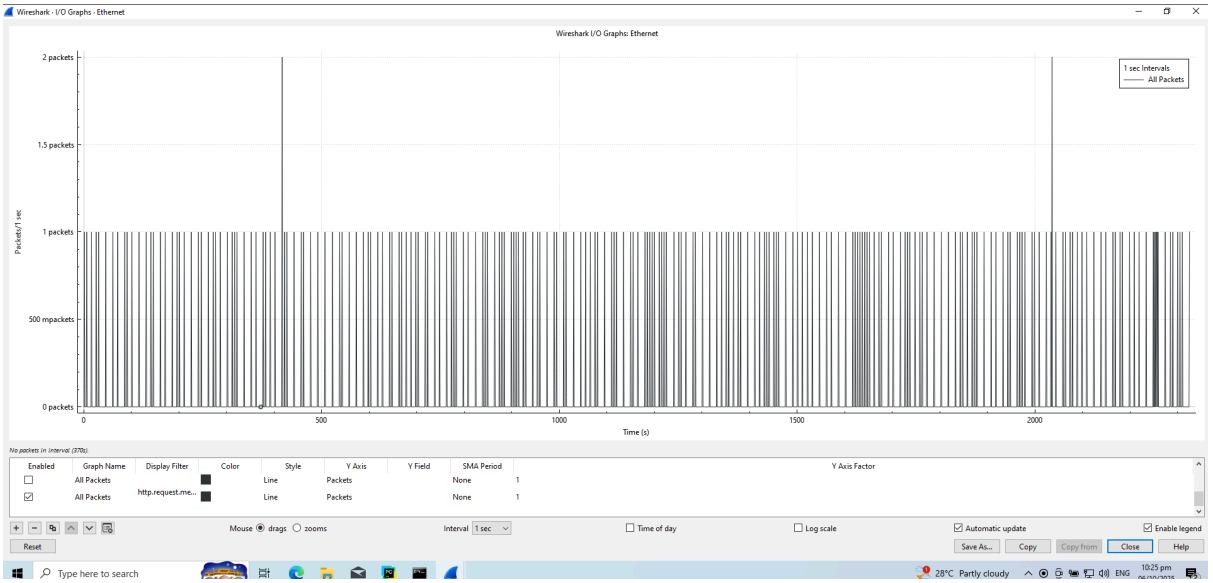
Interpretation: *Quantifies total traffic exchanged during the C2/exfil session.*



Confirms payload reconstruction and visible data content.

(note: Please read the README.md before opening this)
Some Pictures may be blurry this is intentional because I don't want to put sensitive raw information online, Raw files are available upon request including the PCAP

Description: Packet detail pane for POST reassembly.
Observation: Shows “Reassembled TCP Segments” and MIME multipart decode.
Interpretation: Confirms payload reconstruction and visible data content.



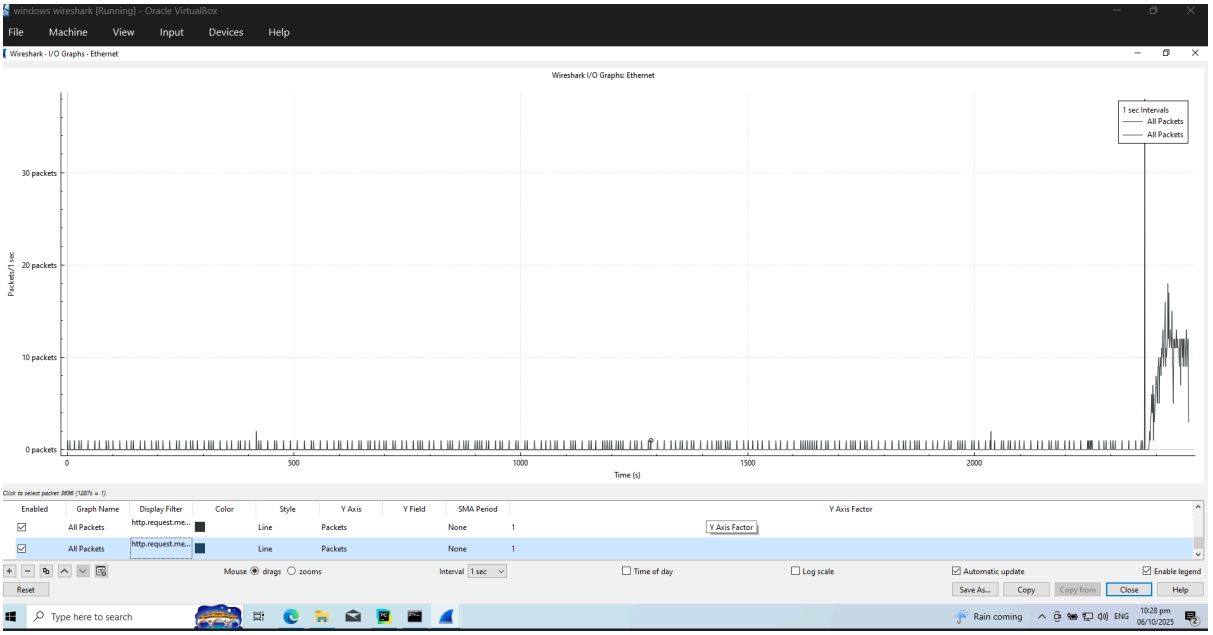
Repeated requests at regular intervals; evidence of automated beaconing.

What the image shows: Packet list filtered to show `GET /checkin` packets (with timestamps). You can see many lines of `GET /checkin` and their time column.

What to point at:

- The repeated `GET /checkin` entries in the Info column.
- The Time column — intervals between requests (use this to show ~1s periodicity).
- The bottom packet details/hex if you want to show payload.

(note: Please read the README.md before opening this)
Some Pictures may be blurry this is intentional because I don't want to put sensitive raw information online, Raw files are available upon request including the PCAP



I/O Graph (filtered): steady 1s beaconing intervals followed by a higher-volume transfer.

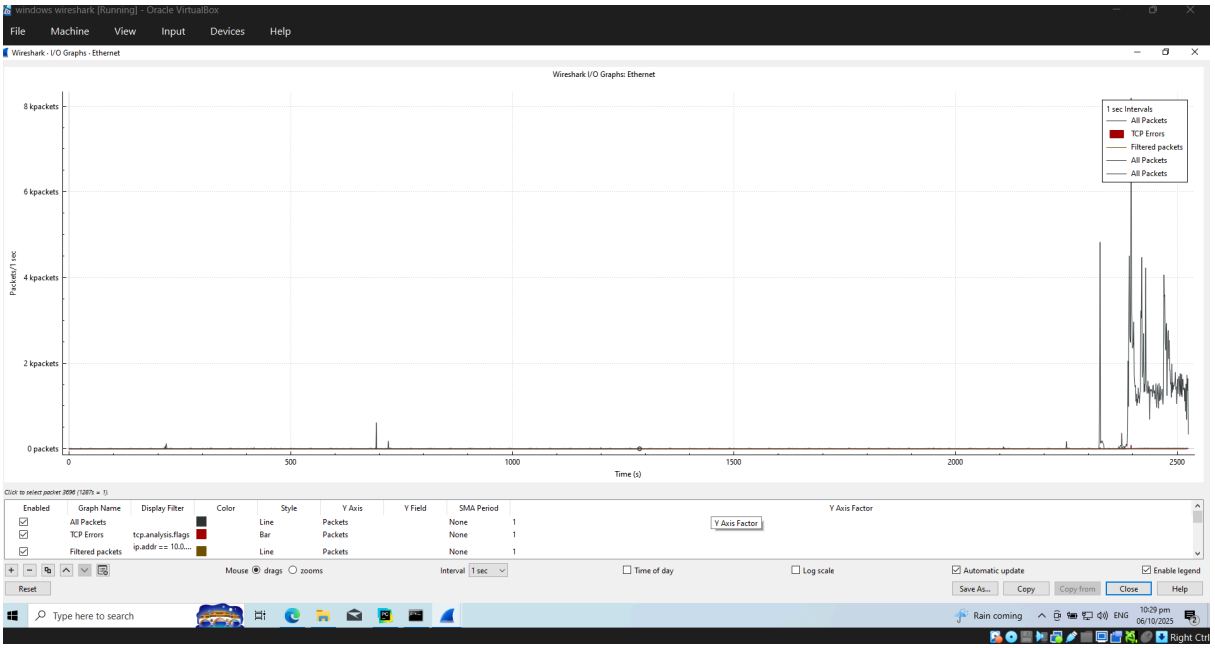
What the image shows: Zoomed I/O Graph (filtered) showing the periodic GET spikes (around 1/sec) followed later by increased traffic. Probably two plotted series (GET filter vs all packets).

What to point at:

- The repeated 1/sec spikes spread across the capture (shows periodicity).
- The later section where amplitude increases (switch to bulk/ upload).

What it proves: The GETs are automated and periodic, and later traffic increases — typical behavior for a callback then data transfer.

(note: Please read the README.md before opening this)
Some Pictures may be blurry this is intentional because I don't want to put sensitive raw information online, Raw files are available upon request including the PCAP



I/O Graph: baseline idle activity followed by a burst consistent with beaconing and subsequent data transfer

What the image shows: Wireshark I/O Graph for “All Packets” over the entire capture. Most of the capture is near-zero traffic, then near the far right you see a clear cluster of traffic spikes (a burst).

What to point at in the screenshot:

- The long baseline of near-zero packet rate (normal/idle).
- The cluster of high spikes at the right edge (time of beaconing/exfiltration).

What it proves: There was a prolonged quiet period followed by a sudden increase in traffic — consistent with periodic beaconing that later escalates into a burst/upload.