

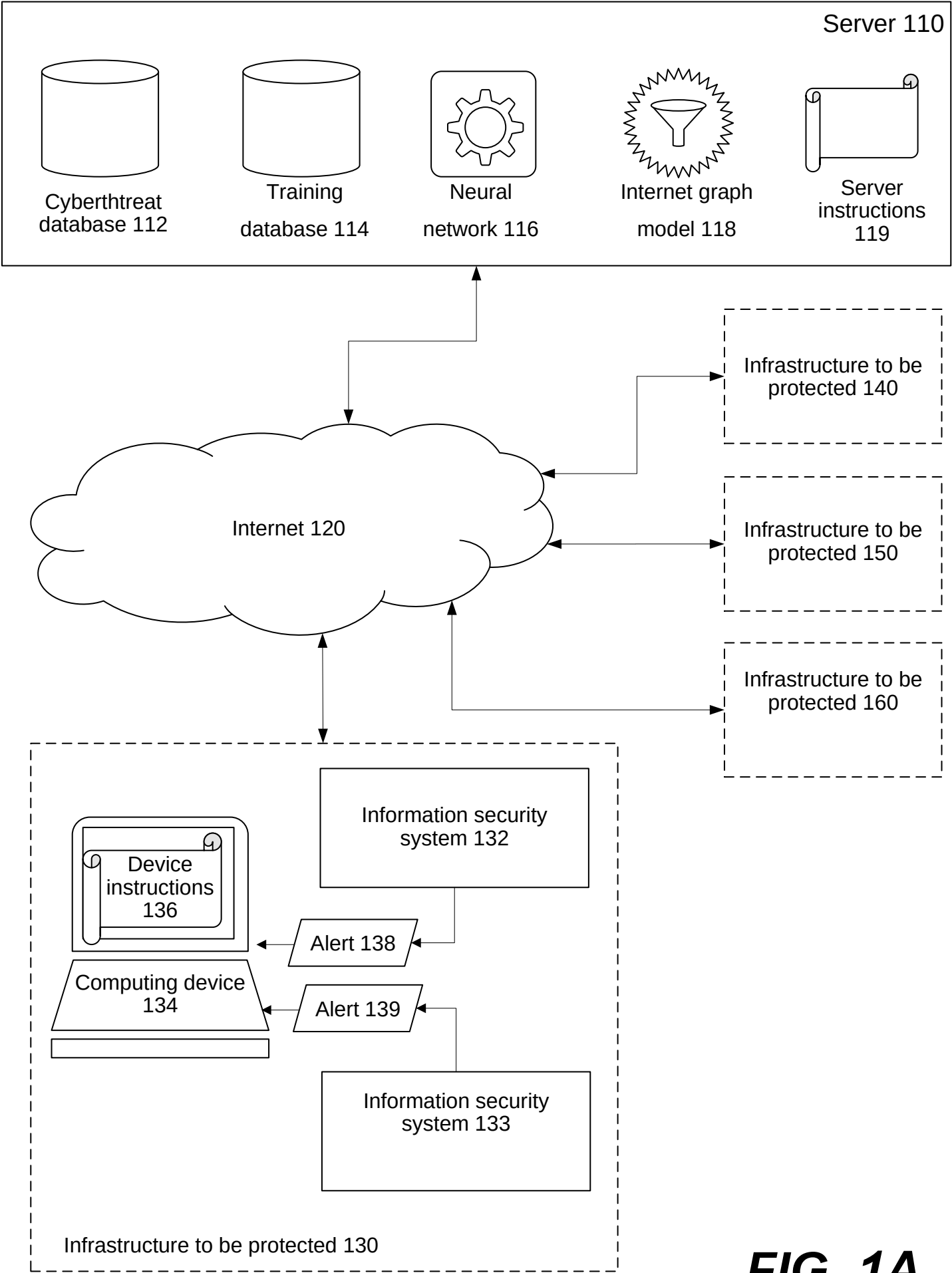


FIG. 1A

Alert 138

Malicious file WTF.zip

Hazard level: High

General information: email received from the address email@cybercrime.com comprises 1 malicious file and 1 malicious link.

Detected on June 9, 2024, at 10.17:24. Last updated on June 9, 2024, at 10.17:24.

EDR verdict: malicious file (statistical rules), probability 86%

Verdict of the mail analyzer: malicious address email@cybercrime.com

Hash of the malicious file: 4ce0c876c63f7e3e733dd89e14c31646d6e4 (SHA-256)

Related network resources:

https://CYBER-EVIL.SITE/hacking_tools/trojans/WTF.zip

Related network resources:

111.222.333.444

Alert 139

Data leakage threat SCAN BMAP -sS window 1024

Hazard level: Critical

Sensor that detected the threat: [sensor identifier]

Threat source: network traffic

Detection time: 09.06.2024 10:41

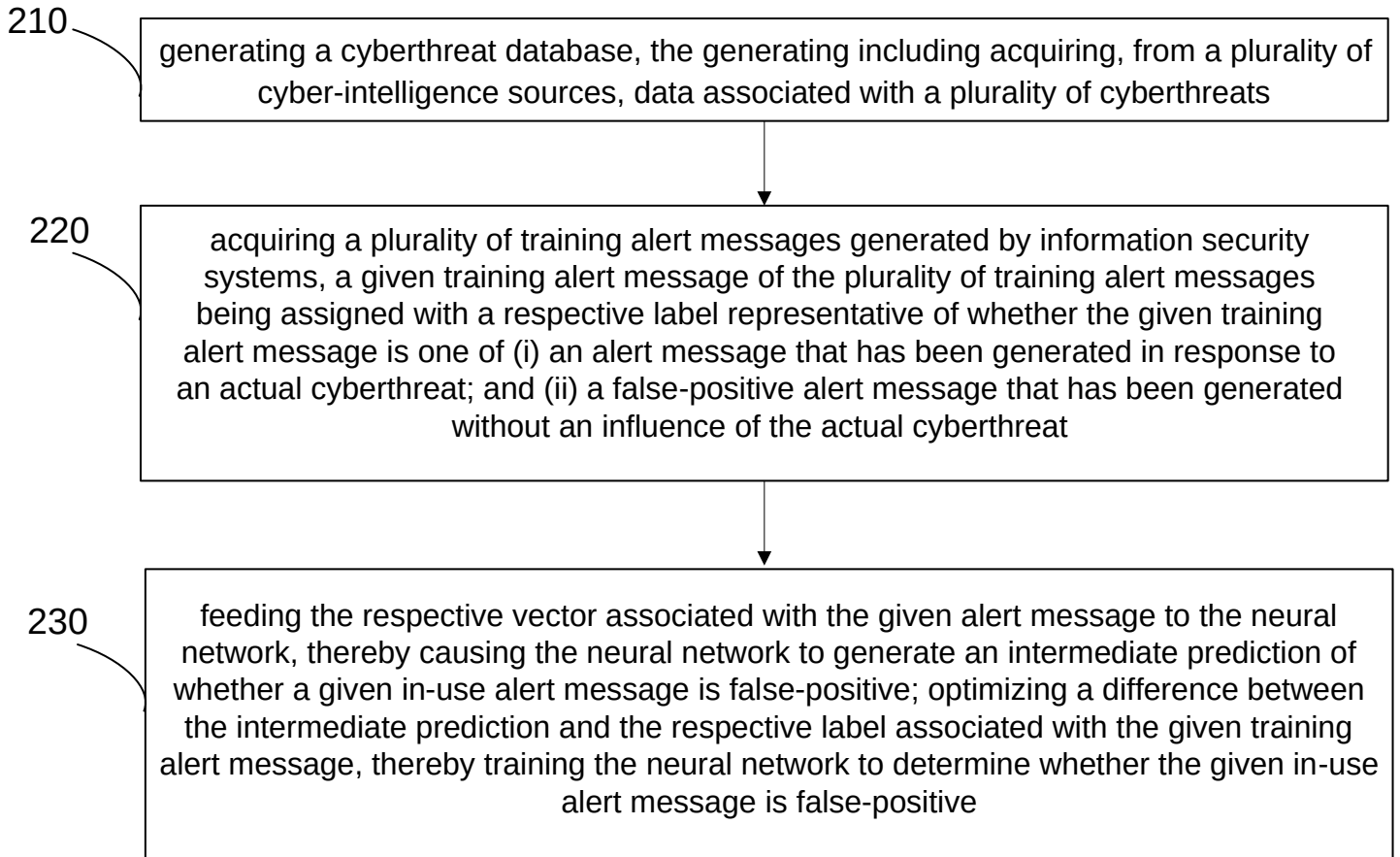
Recipient IP address: 111.222.333.444

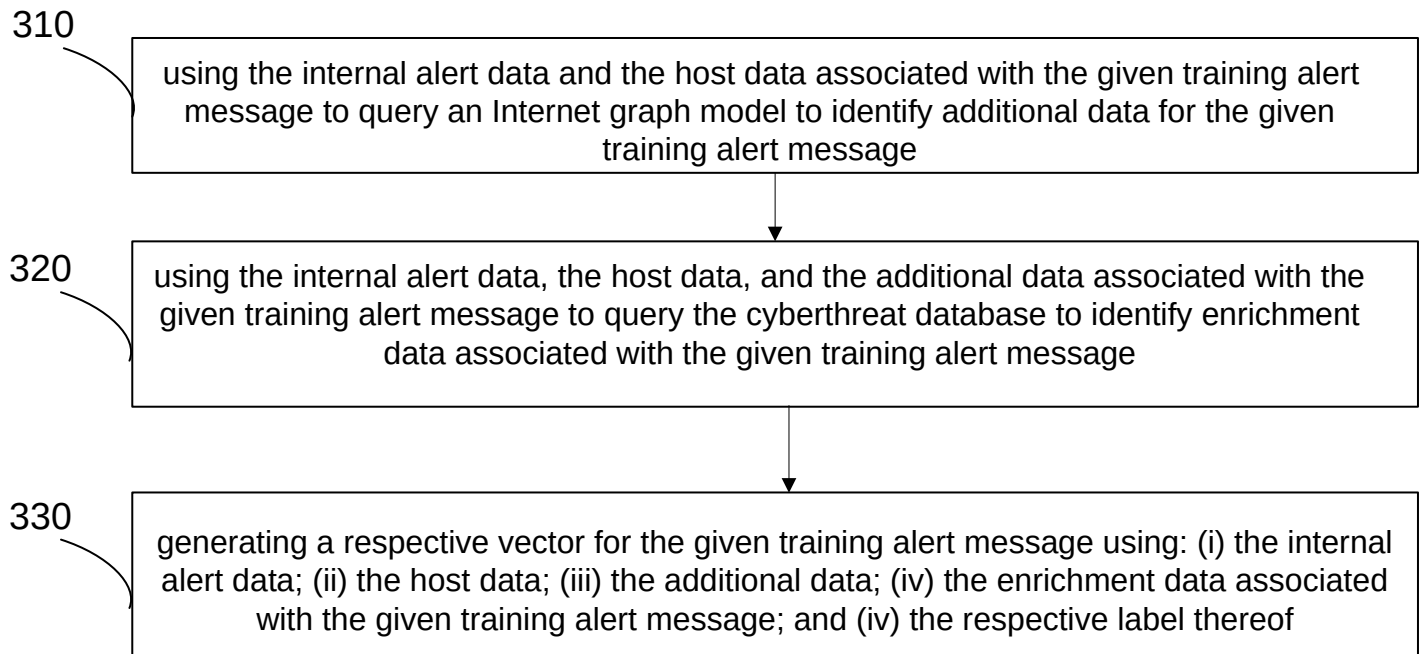
Sender IP address: 555.666.777.888

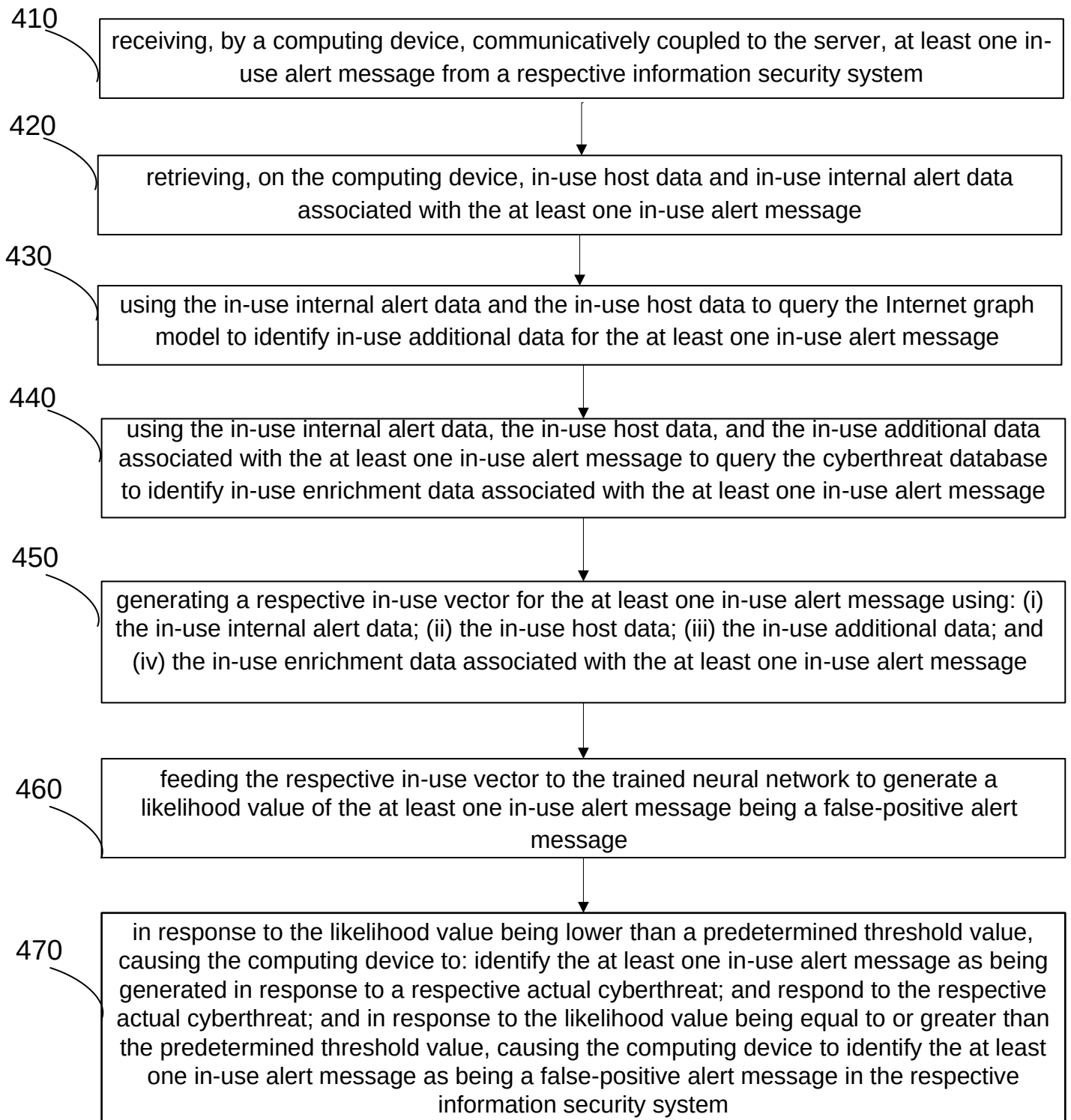
Signature that detected the threat: WEB-SPECIFIC_APPS ELF File magic encoded
Base64 Inbound Web Servers Likely Command Execution

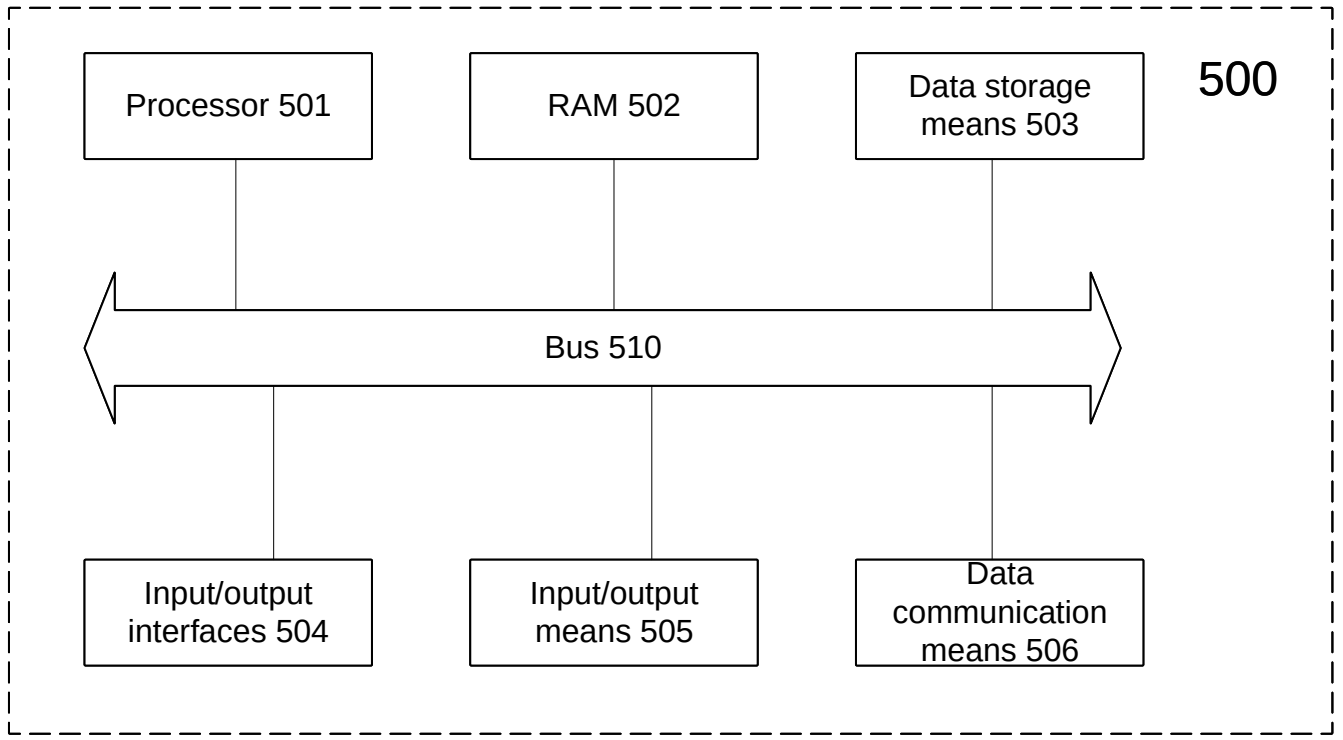
Traffic fragment: [fragment of the network traffic, where this signature has been activated]

200

**FIG. 2**

**FIG. 3**

**FIG. 4**

**FIG. 5**