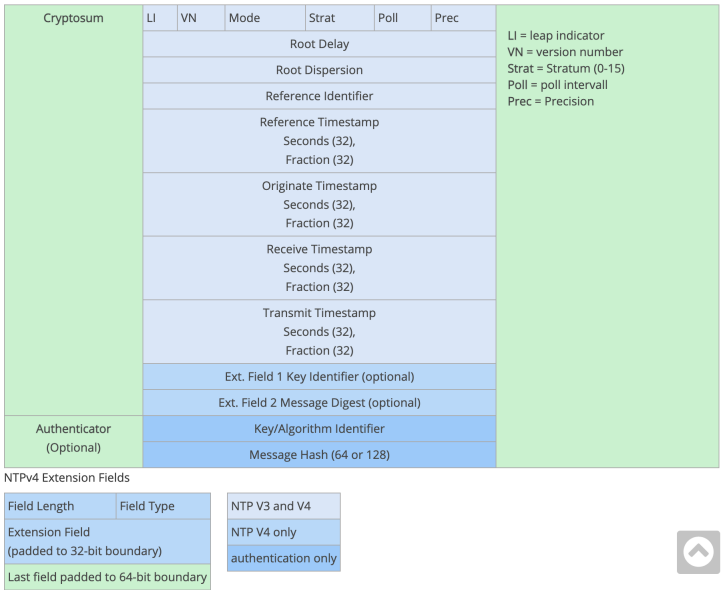
CCDC Inject

INJECT NAME	Create Forensic Analysis Request - NTPa Log File Extract
INJECT ID	SOCS04A

INJECT DESCRIPTION:
A recent packet capture obtained an NTP packet, which the Security Operations staff think it is a malware beacon. They have asked the Security Analyst to make a ruling as to whether this is the case.

Give the NTP Packet Layout



The fields contain:

Leap Indicator: No

Version Number: 4

Mode: Client

Stratum: 52

Poll: 10

Precision: -24

Root Delay: .001846

Root Dispersion: .034897

Reference ID: 106.20.14.218

Reference Timestamp: Jan 5, 2024 13:04.22.655333004 UTC

Originate Timestamp: Jan5, 2024 13:04.22.653850915 UTC

Receive Timestamp: Jan 5, 2024 13:04.22.655333004 UTC

Transmit Timestamp: Jan5, 2024 13:04.22.675517085 UTC

Key Identifier: 00000001

Message Digest: 646f776e6c6f6164207061796c6f636433

INJECT DELIVERABLE

Respond with a business memo clearly making a judgement as to whether this is a normal NTP packet or potentially a malware beacon. Be specific with your analysis.