**CTF Topic: Certificate Transparency and Certificate Analysis**

**Introduction**

****

This CTF challenge revolves around analysing SSL certificates using the Certificate Transparency (CT) log search service provided by crt.sh. Participants will search for certificates related to "Ncell" and extract specific details from the provided certificates.

**Scenario**

****

You are a security analyst tasked with investigating the SSL certificates issued to Ncell. Using the crt.sh website, you need to find and analyse the certificates related to Ncell to uncover specific information.

**Process**

1. Search for Certificates:

* Visit crt.sh: <https://crt.sh>
* Use the search term "Ncell" to find all relevant certificates.
* Click on the crt.sh ID [13512776133](https://crt.sh/?id=13512776133)
* Capture the flag

**Questions**

Flag 1: What is the SHA256 fingerprint of the certificate issued to "NCELL AXIATA LIMITED" by "GlobalSign RSA OV SSL CA 2018"?

Answer:EE09CB4C0FA92C1F6CEAC1756E8E46F5EF372A62AC93C3BAC8CC4A90297EBFD3

Flag 2: What is the serial number of the certificate issued to "NCELL AXIATA LIMITED"?

Answer: 64:70:3b:71:e9:4e:50:fb:4d:b5:0a:1d

Flag 3: What is the Signature Algorithm of "NCELL AXIATA LIMITED"?

Answer: sha256WithRSAEncryption

**Hint**A screenshot of a computer

Description automatically generated

