

## SSL Certificate Analysis Project –Submission template

Please answer the below questions to complete the submission report. Please add screenshots of the certificate wherever necessary.

1. The certificate indicates **two fingerprints**. Identify the certificate fingerprints and complete the following table. (5 points)

**Answer-**

Certificate Fingerprint	Field Value
SHA-256 Fingerprint	92 A3 7F BD 5E 21 A5 3A 95 C7 16 E1 14 4F 44 2F 58 2B 94 D0 FA FC 67 3E B6 71 7A 4E B5 1A 88 A7
SHA-1 Fingerprint	A3 B5 9E 5F E8 84 EE 1F 34 D9 8E EF 85 8E 3F B6 62 AC 10 4A

2. Are there any Subject Alternative Names? If yes, please mention. (5 points)

**Answer-**

DNS Name: github.com

DNS Name: www.github.com

3. Complete the following table: (15 points)

**Answer-**

Certificate level	Issued to (Common Name)	Serial Number
Server	github.com	0C:D0:A8:BE:C6:32:CF:E6:45:EC:A0:A9:B0:84:FB:1C
Intermediary	DigiCert TLS Hybrid ECC SHA384 2020 CA1	07:F2:F3:5C:87:A8:77:AF:7A:EF:E9:47:99:35:25:BD
Root	DigiCert Global Root CA	08:3B:E0:56:90:42:46:B1:A1:75:6A:C9:59:91:C7:4A

4. On which date was the following serial number revoked? (15 points)

077937c0eca34a544de4424e66f4b8de

(Hint: Check for the certificates revoked in the month of August 2022)

**Answer-**

Serial number : 077937c0eca34a544de4424e66f4b8de

revocation date : Friday, August 5, 2022 2:36:55 AM