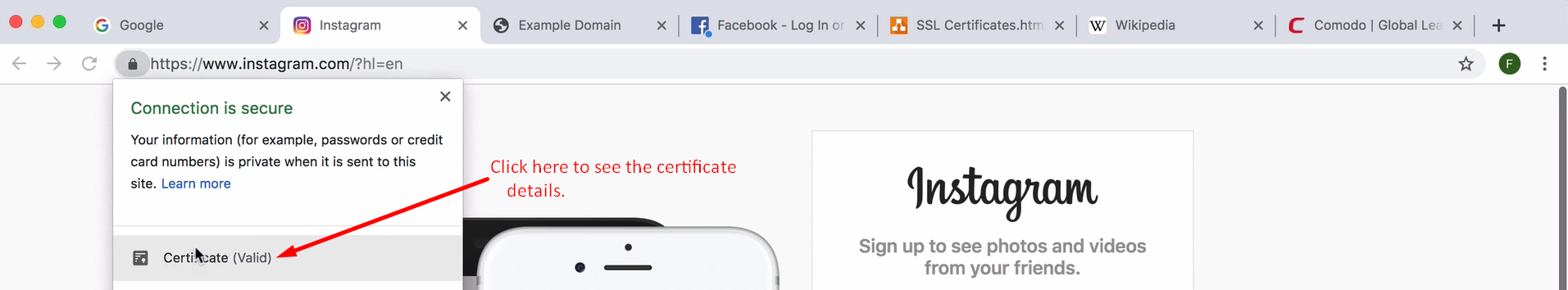
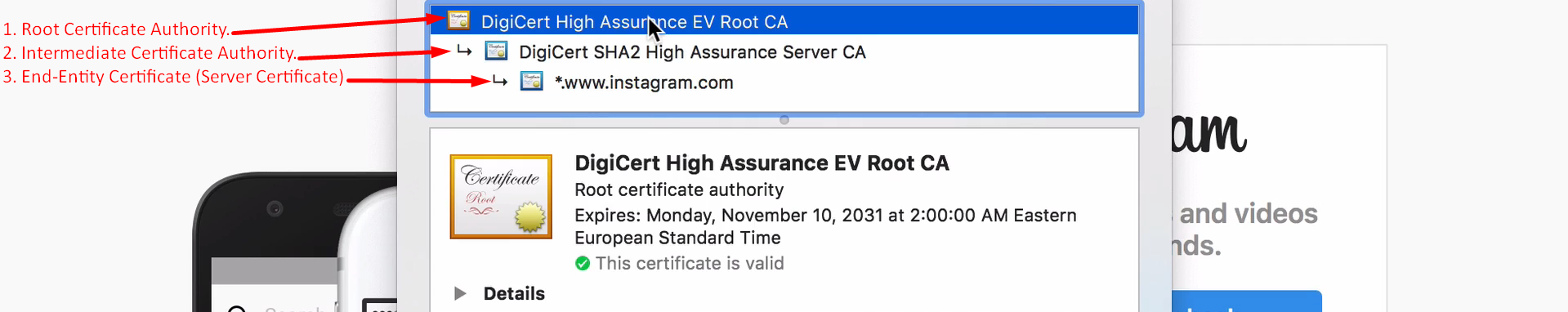
1. **Agenda**:
   1. Let’s explore certificate that is used to encrypt traffic to Instagram.com
2. 
3. 

This image shows the \*\*Certificate Authority (CA) chain\*\* for the domain \*\*instagram.com\*\*.

**### \*\*Certificate Chain Details:\*\***

**1. \*\*Root Certificate Authority (CA):\*\***

- \*\*DigiCert High Assurance EV Root CA\*\*

- This is the \*\*Root CA\*\*, which is at the top of the trust hierarchy.

- It is self-signed and trusted by browsers or operating systems.

- It verifies and signs intermediate certificates.

2. **\*\*Intermediate Certificate Authority (CA):\*\***

**- \*\*DigiCert SHA2 High Assurance Server CA\*\***

- This is an \*\*Intermediate CA\*\* issued by the \*\*Root CA\*\*.

- It acts as a link between the root certificate and the domain's certificate.

- It provides an extra layer of security and scalability, reducing the risk of exposing the root certificate.

3. **\*\*End-Entity Certificate (Server Certificate):\*\***

**- \*.instagram.com\*\***

- This is the **server certificate** issued for the specific domain.

- This is the actual SSL/TLS certificate for the website.

- It is signed by the **Intermediate CA** and used to establish SSL/TLS connections with clients.

**Trust Verification Process:**

1. The \*\*Root CA\*\* is inherently trusted by the browser.

2. The \*\*Intermediate CA\*\* is validated by the \*\*Root CA\*\*.

3. The \*\*Server Certificate\*\* is validated by the \*\*Intermediate CA\*\*.

4. The browser checks this chain to confirm the server's identity and establish a secure connection.

This chain ensures a hierarchical trust system for secure communication.

**Flow of Trust:**

The browser first checks the end-entity certificate (for www.instagram.com).

It then validates the intermediate CA (DigiCert SHA2 High Assurance Server CA) to confirm it is signed by the Root CA (DigiCert High Assurance EV Root CA).

Finally, the root CA is verified because it is pre-installed in the browser or OS trust store.

1. There are many blocks in the **Server Certificate**.
2. Let’s take a look **Detail Block**:
3. **Detail Block**: Contains info about the owner of the certificate in other words.

**1. Subject Name**

This field identifies the entity the certificate was issued to (the website or organization).

**Common Name** (CN): \*.www.instagram.com

Represents the domain name the certificate secures.

The \* indicates it is a **wildcard certificate**, meaning it secures all subdomains (e.g., www.instagram.com and login.instagram.com).

**2**. **Country or Region**

Value: US

Specifies the country code where the **organization is registered**.

It follows the ISO 3166-1 alpha-2 standard.

**3. State/Province**

Value: CA

Indicates the state or province where the organization operates.

In this case, California (CA) in the United States.

**4. Locality**

Value: Menlo Park

Specifies the city where the organization is located.

Menlo Park is the headquarters of Facebook, Inc..

**5. Organization**

Value: Facebook, Inc.

The name of the **legal entity** that owns the domain and certificate.

Facebook, Inc. owns Instagram.

1. **Issue Details:**
2. The Issuer Information section in the snapshot provides details about the entity (Certificate Authority - CA) that issued the certificate. Here's a detailed explanation of each field:
3. **Issuer Name:** This field describes the entity responsible for issuing the certificate, which acts as the Certificate Authority (CA)
4. **Country or Region: US:** Specifies the country where the CA is based, in this case, the United States.
5. **Organization**
   1. **Value**: DigiCert Inc
   2. Identifies the name of the CA organization that issued the certificate.
   3. DigiCert Inc is a well-known and trusted CA.
6. Common Name (CN)
   1. Value: DigiCert SHA2 High Assurance Server CA
   2. This is the name of the CA or intermediate CA used to issue the certificate.
   3. It reflects the type and purpose of the certificate, in this case, a SHA2 High Assurance Server Certificate.
7. **Serial Number**
   1. Value: 09 18 1C BE EB 73 D4 F3 26 9C 9F CF 09 DC 20 3E
   2. A unique identifier assigned to this certificate by the issuer.
   3. This number helps uniquely track and manage the certificate, especially in revocation scenarios.
8. **Version**
   1. Value: 3
   2. Indicates the X.509 version of the certificate standard being followed.
   3. Version 3 is widely used as it supports extensions for more advanced features like key usage constraints.
9. **Signature Algorithm**
   1. Value: SHA-256 with RSA Encryption
   2. Specifies the algorithm **used to sign the certificate**.
   3. SHA-256 (Secure Hash Algorithm) ensures integrity, and RSA is used for encryption.
      1. SHA-256: Algo was used to generate hashcode.
      2. RSA: To encrypt the above hashcode using this CA’s private key and eventually the output is the certificate’s signature = Hashcode + its encryption
   4. The OID (1.2.840.113549.1.1.11) is a unique identifier for this algorithm.
10. Validity Period