INTRODUCTION TO INFORMATION SECURITY & FORENSICS

ASSIGNMENT 03

MUHAMMAD HARRIS BCS203193

—

29th December, 2022

INTRODUCTION TO INFORMATION SECURITY & FORENSICS

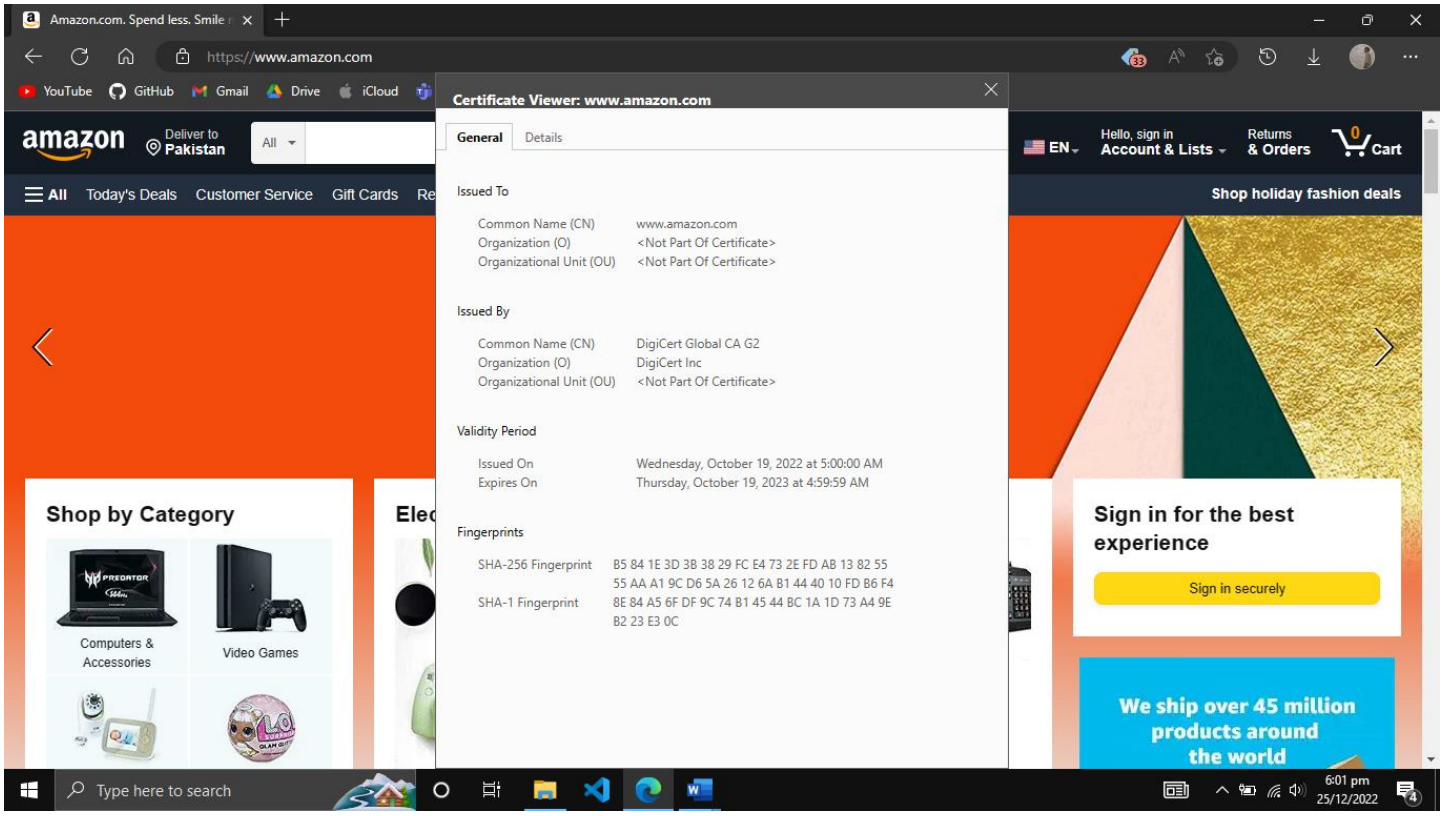
ASSIGNMENT 03

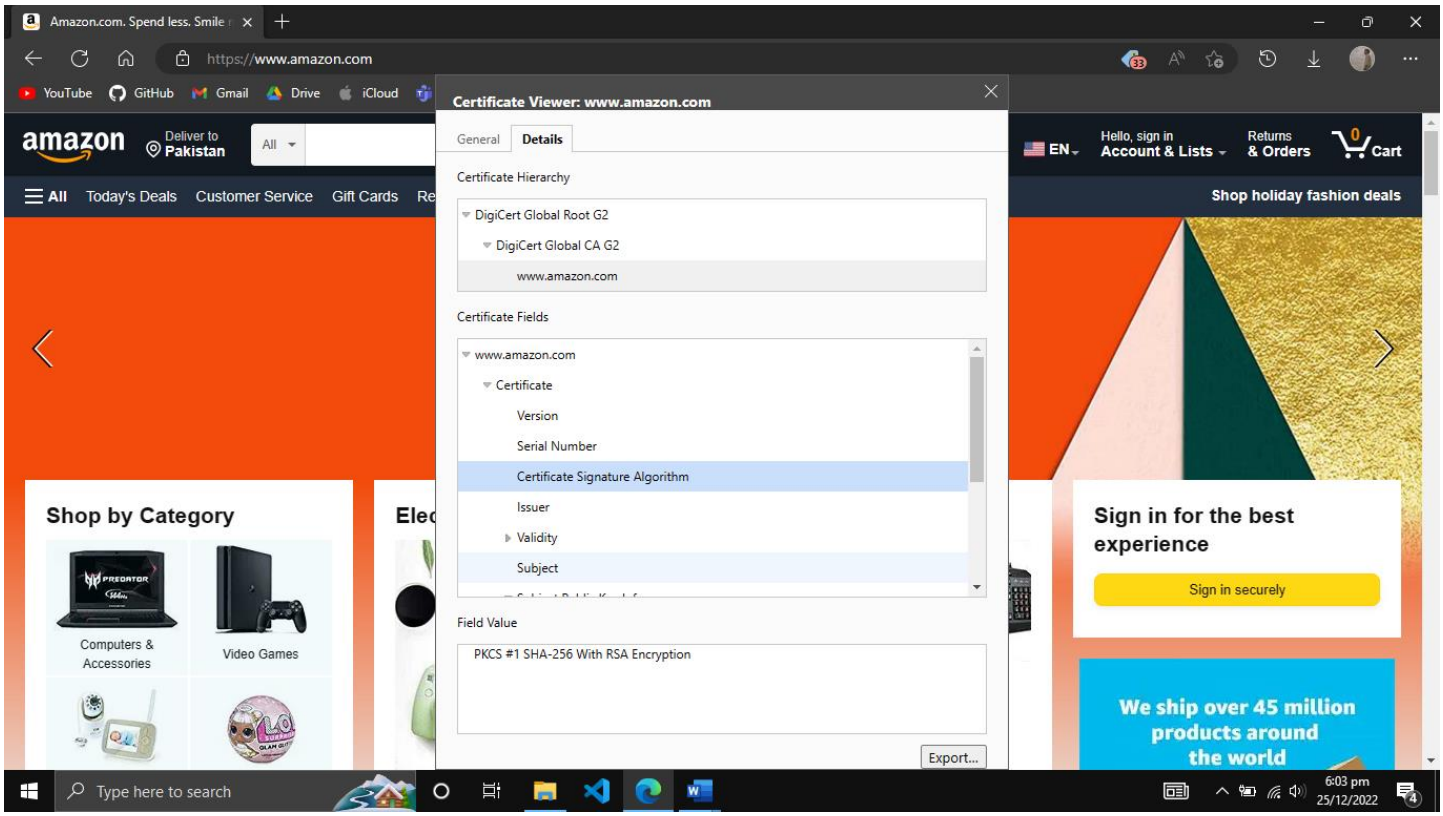
PART 1:

Examine and inspect the details of amazon.com's Certificate and answer the following:

1. What is the root certificate authority for amazon.com?
2. What is the intermediate certificate authority for amazon.com?
3. What algorithm does Amazon certificate use for public key?
4. What certificate signature algorithm does Amazon use?
5. What is the key size of Amazon certificate's public key?

1. Root Certificate Authority of Amazon.com is DigiCert Global Root G2.
2. Intermediate Certificate Authority of Amazon.com is DigiCert Global CA G2.
3. Amazon Certificate uses RSA Encryption Algorithm for public key.
4. Amazon Certificate uses SHA-256 with RSA Encryption Algorithm for Certificate Signature.
5. The length of public key for Amazon Certificate is 2048 bits (modulus) + 17 bits (exponents).


Amazon.com. Spend less. Smile
https://www.amazon.com
YouTube
GitHub
Gmail
Drive
iCloud
Certificate Viewer: www.amazon.com
General
Details
Issued To
Common Name (CN) www.amazon.com
Organization (O) <Not Part Of Certificate>
Organizational Unit (OU) <Not Part Of Certificate>
Issued By
Common Name (CN) DigiCert Global CA G2
Organization (O) DigiCert Inc
Organizational Unit (OU) <Not Part Of Certificate>
Validity Period
Issued On Wednesday, October 19, 2022 at 5:00:00 AM
Expires On Thursday, October 19, 2023 at 4:59:59 AM
Fingerprints
SHA-256 Fingerprint B5 84 1E 3D 3B 38 29 FC E4 73 2E FD AB 13 82 55 55 AA A1 9C D6 5A 26 12 6A B1 44 40 10 FD B6 F4
SHA-1 Fingerprint 8E 84 A5 6F DF 9C 74 B1 45 44 BC 1A 1D 73 A4 9E B2 23 E3 0C
amazon
Deliver to Pakistan
All
Today's Deals
Customer Service
Gift Cards
EN
Hello, sign in Account & Lists
Returns & Orders
Cart
Shop holiday fashion deals
Shop by Category
Computers & Accessories
Video Games
Sign in for the best experience
Sign in securely
We ship over 45 million products around the world
Type here to search
6:01 pm
25/12/2022

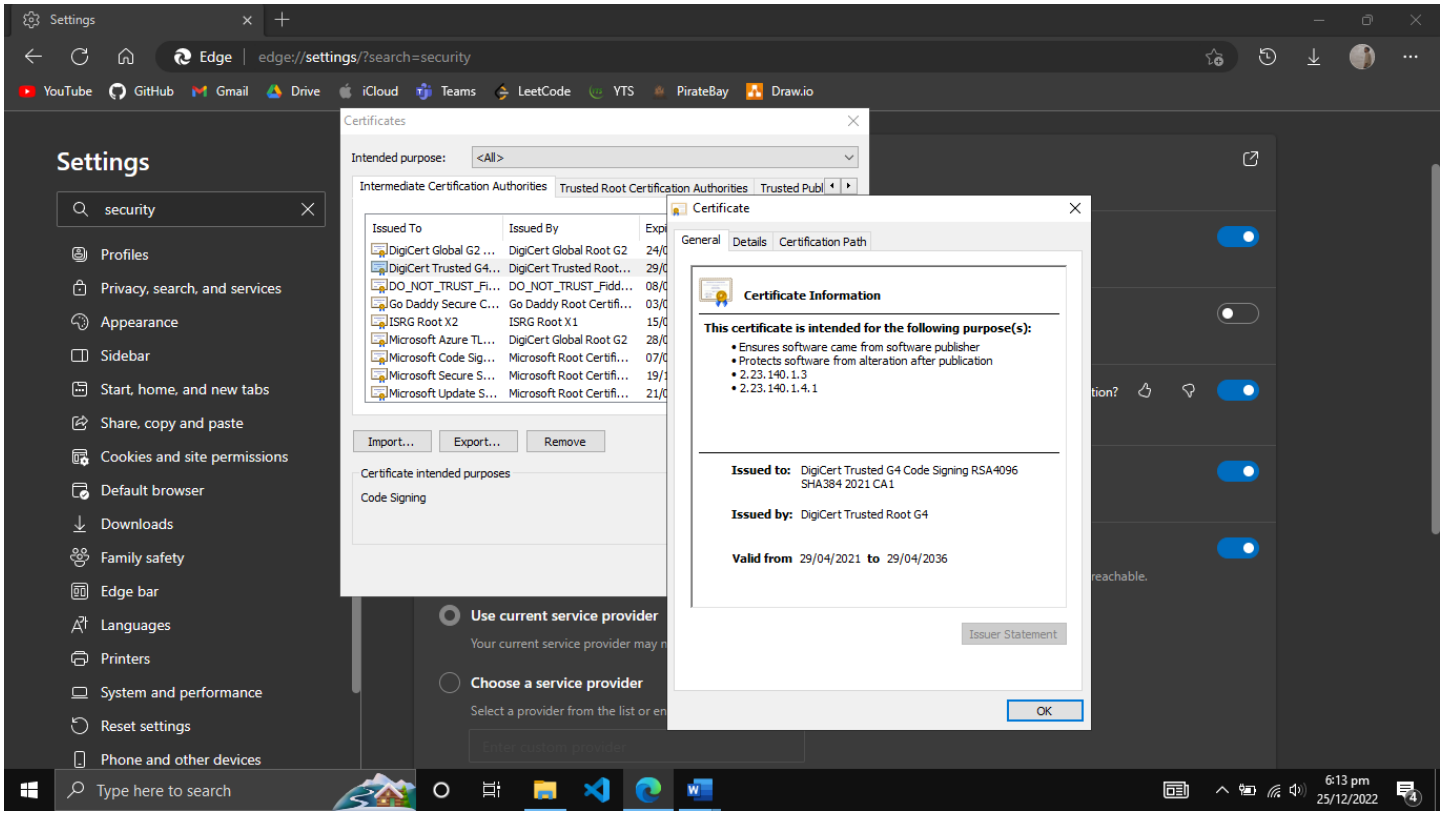

Amazon.com. Spend less. Smile
https://www.amazon.com
YouTube
GitHub
Gmail
Drive
iCloud
Certificate Viewer: www.amazon.com
General
Details
Certificate Hierarchy
DigiCert Global Root G2
DigiCert Global CA G2
www.amazon.com
Certificate Fields
www.amazon.com
Certificate
Version
Serial Number
Certificate Signature Algorithm
Issuer
Validity
Subject
Field Value
PKCS #1 SHA-256 With RSA Encryption
Export...
amazon
Deliver to Pakistan
All
Today's Deals
Customer Service
Gift Cards
EN
Hello, sign in Account & Lists
Returns & Orders
Cart
Shop holiday fashion deals
Shop by Category
Computers & Accessories
Video Games
Sign in for the best experience
Sign in securely
We ship over 45 million products around the world
Type here to search
6:03 pm
25/12/2022

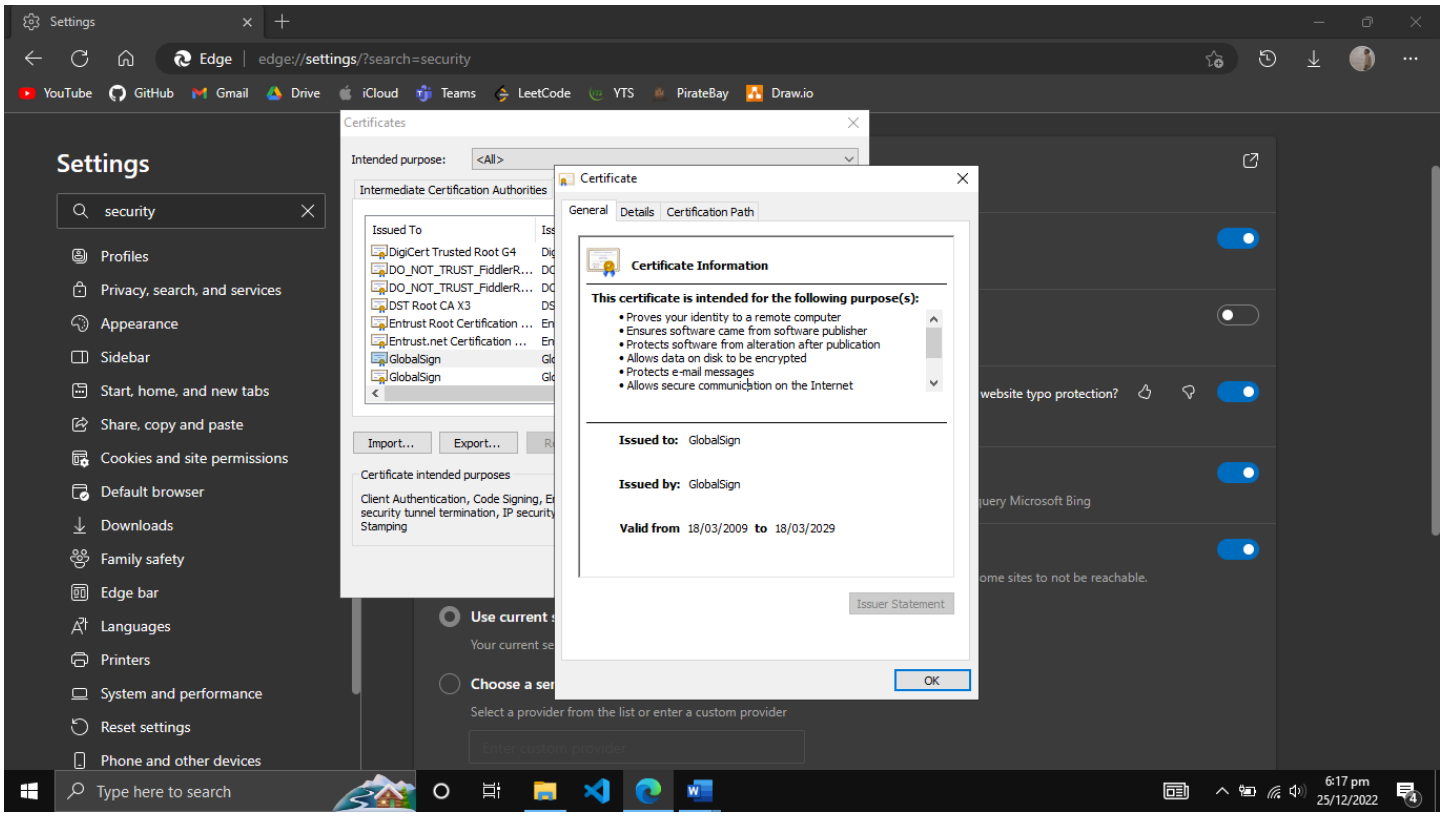
PART 2:

Explore the certificate authorities of Google Chrome and answer the following:

1. **Navigate to any DigiCert certificate. What are the purposes the certificate's key is used for?**
2. **What is the certificate key's enhanced usage?**
3. **Navigate to GlobalSign certificate and mention its enhanced key usage?**
4. **Navigate to any trusted certificate and mention its intended purpose(s).**
5. **What are the types of certificates signing algorithms supported by Google?**

1. Certificate's public key is used for,
    - Ensuring that software came from software publisher
    - Protecting software against alterations
2. Certificate's public key was intended for code signing.
3. GlobalSign key is used for the following purposes:
    - Proves your identity to a remote computer
    - Ensures software came from software publisher
    - Protects software from alteration after publication
    - Allows data on disk to be encrypted
    - Protects e-mail messages
    - Allows secure communication on the Internet
    - Ensures the identity of a remote computer
    - Allows data to be signed with the current time
    - All issuance policies
4. Trusted Certificate had the following purposes:
    - Proves your identity to a remote computer
    - Ensures software came from software publisher
    - Protects software from alteration after publication
    - Allows data on disk to be encrypted
    - Protects e-mail messages
    - Allows secure communication on the Internet
    - Ensures the identity of a remote computer
    - Allows data to be signed with the current time
    - All issuance policies
5. Algorithms supported by Google are AES-256, RSA, SHA-256, SHA-384 and SHA-512.


Settings
Edge | edge://settings/?search=security
YouTube GitHub Gmail Drive iCloud Teams LeetCode YTS PirateBay Draw.io
Settings
security
Profiles
Privacy, search, and services
Appearance
Sidebar
Start, home, and new tabs
Share, copy and paste
Cookies and site permissions
Default browser
Downloads
Family safety
Edge bar
Languages
Printers
System and performance
Reset settings
Phone and other devices
Certificates
Intended purpose: <All>
Intermediate Certification Authorities
Trusted Root Certification Authorities
Issued To
Issued By
DigiCert Global G2 ...
DigiCert Global Root G2
DigiCert Trusted G4...
DigiCert Trusted Root...
DO_NOT_TRUST_Fi...
DO_NOT_TRUST_Fidd...
Go Daddy Secure C...
Go Daddy Root Certifi...
ISRG Root X2
ISRG Root X1
Microsoft Azure TL...
DigiCert Global Root G2
Microsoft Code Sig...
Microsoft Root Certifi...
Microsoft Secure S...
Microsoft Root Certifi...
Microsoft Update S...
Microsoft Root Certifi...
Import... Export... Remove
Certificate intended purposes
Code Signing
Certificate
General Details Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures software came from software publisher
• Protects software from alteration after publication
• 2.23.140.1.3
• 2.23.140.1.4.1
Issued to: DigiCert Trusted G4 Code Signing RSA4096 SHA384 2021 CA1
Issued by: DigiCert Trusted Root G4
Valid from 29/04/2021 to 29/04/2036
Issuer Statement
OK
Use current service provider
Your current service provider may r
Choose a service provider
Select a provider from the list or en
Enter custom provider
Type here to search
6:13 pm
25/12/2022


Settings
Edge | edge://settings/?search=security
YouTube GitHub Gmail Drive iCloud Teams LeetCode YTS PirateBay Draw.io
Settings
security
Profiles
Privacy, search, and services
Appearance
Sidebar
Start, home, and new tabs
Share, copy and paste
Cookies and site permissions
Default browser
Downloads
Family safety
Edge bar
Languages
Printers
System and performance
Reset settings
Phone and other devices
Certificates
Intended purpose: <All>
Intermediate Certification Authorities
Issued To
DigiCert Trusted Root G4
DO_NOT_TRUST_FiddlerR...
DO_NOT_TRUST_FiddlerR...
DST Root CA X3
Entrust Root Certification ...
Entrust.net Certification ...
GlobalSign
GlobalSign
Import... Export...
Certificate intended purposes
Client Authentication, Code Signing, E
security tunnel termination, IP securit
Stamping
Certificate
General Details Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Proves your identity to a remote computer
• Ensures software came from software publisher
• Protects software from alteration after publication
• Allows data on disk to be encrypted
• Protects e-mail messages
• Allows secure communication on the Internet
Issued to: GlobalSign
Issued by: GlobalSign
Valid from 18/03/2009 to 18/03/2029
Issuer Statement
OK
Choose a ser
Select a provider from the list or enter a custom provider
Enter custom provider
Type here to search
6:17 pm
25/12/2022