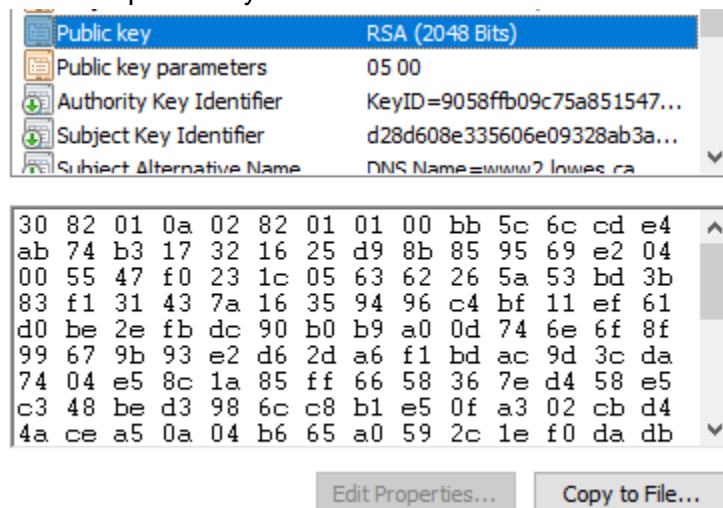


1. What server was the certificate assigned to? Answer
 - a. www1.lowes.com
2. What is the validity date of the cert? Answer
 - a. 1/24/22-11/11/22
3. What is the Certificate Authority for the certificate? Answer
 - a. GeoTrust RSA CA 2018
4. Can you find the public key? Post Screenshot



a.

2. Use Wireshark to capture connections to a HTTPS site

1. Describe the packet exchange for the HTTPS negotiation - how many packets, what order...
 - a. 9 Packets
 - b. Client Hello, Server Hello, Cert., Server hello done, client key exchange, change cypher spec, finished, change cypher spec, finished.
2. Post details about the certificate:
 - a. Validity Date

```

▼ validity
  ▼ notBefore: utcTime (0)
    utcTime: 2020-09-24 00:00:00 (UTC)
  ▼ notAfter: utcTime (0)
    utcTime: 2030-09-23 23:59:59 (UTC)
  i.
  ▼ subject: cn=www1.lowes.ca
  
```

b. Certificate Authority (Issuer)

- ▼ issuer: rdnSequence (0)
 - ▼ rdnSequence: 4 items (id-at-commonName=DigiCert Global Root CA,id-at-organizationalUnitName=www.digicert.com)
 - ▼ RDNSequence item: 1 item (id-at-countryName=US)
 - ▼ RelativeDistinguishedName item (id-at-countryName=US)
 - Id: 2.5.4.6 (id-at-countryName)
 - CountryName: US
 - ▼ RDNSequence item: 1 item (id-at-organizationName=DigiCert Inc)
 - ▼ RelativeDistinguishedName item (id-at-organizationName=DigiCert Inc)
 - Id: 2.5.4.10 (id-at-organizationName)
 - DirectoryString: printableString (1)

i.

c. Public Key

- ▼ subjectPublicKeyInfo: rsaEncryption
 - ▼ algorithm (rsaEncryption)
 - Algorithm Id: 1.2.840.113549.1.1.1 (rsaEncryption)
 - ▼ subjectPublicKey: 3082010a0282010100c80ff543bee06b47fd8f4bdf75d30d9a5b4b9e4cc677379881b591bd421081a543b2a2...
 - modulus: 0x00c80ff543bee06b47fd8f4bdf75d30d9a5b4b9e4cc677379881b591bd421081a543b2a2...
 - publicExponent: 65537

i.