**MARYMOUNT UNIVERSITY**

**Assignment:** IT520; Enterprise Infrastructure and Networks [Lab 8]

**Assigned:** April 17, 2018

**Instructor:** Dr. Ibrahim Waziri

**Student Name:** George Boakye

Source Host’s IP Address: **192.168.1.10**

**A screenshot of a social media post

Description generated with very high confidence**

**QUESTIONS**

1. What is the SSL/TLS version of the of the Client Hello frame? **CLIENT HELLO RECORD**

**ANSWER:** TLSVersion 1.2

A screenshot of a social media post

Description generated with very high confidence

1. What is the value of the content type?

**ANSWER:** Handshake (22)

A screenshot of a cell phone

Description generated with very high confidence

1. Does the Client Hello record contain a nonce (also known as a “challenge”)? If so, what is the value of the challenge in hexadecimal notation?

**ANSWER:** Nonce is not set

A screenshot of a social media post

Description generated with very high confidence

­­­

1. Does the ClientHello record advertise the cypher suites it supports? If so, in the first listed suite, what are the public-key algorithm, the symmetric-key algorithm, and the hash algorithm?

**ANSWER:** Yes, the ClientHello record advertises the cypher suites it supports.

Public key algorithm: RSA; Symmetric key algorithm: AES; and Hash algorithm: SHA

A screenshot of a social media post

Description generated with very high confidence

1. Locate the ServerHello SSL record. Does this record specify a chosen cipher suite? What are the algorithms in the chosen cipher suite?

**ANSWER:** Yes, the ServerHello record specify a chosen cypher suite. TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256

Server has an RSA keypair used to calculate pre-master secret

**SERVER HELLO RECORD**

A screenshot of a social media post

Description generated with very high confidence