Network Security Lab 17

<!-- pagebreak -->

Network Security Lab 17

David Ayeke April 10. 2017

1. TLS 1.2
2. 22 0x16
3. 23 0x17
4. 20 0x14
5. Client Hello, Server Hello, Certificate, and Application Data recieve their own frame. [Client Key Exchange, Change Cipher Spec, Hello Request] are bundled together as are [New Session Ticket, Change Cipher Spec and Hello Request]

6. Random Bytes: f714e47c551d5bf8d35fdaf2495c546a5e0c2723e85ce5c1...

7. Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)

8. Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)

9. Yes. Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) was selected again.