

M1:

ClientHello:

ClientRandom[28]

Suggested Cipher Suites:

TLS_RSA_WITH_IDEA_CBC_SHA

TLS_RSA_WITH_3DES_EDE_CBC_SHA

TLS_DH_DSS_WITH_AES_128_CBC_SHA

Suggested Compression Algorithm: NONE