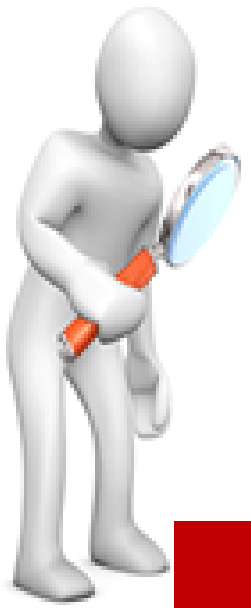
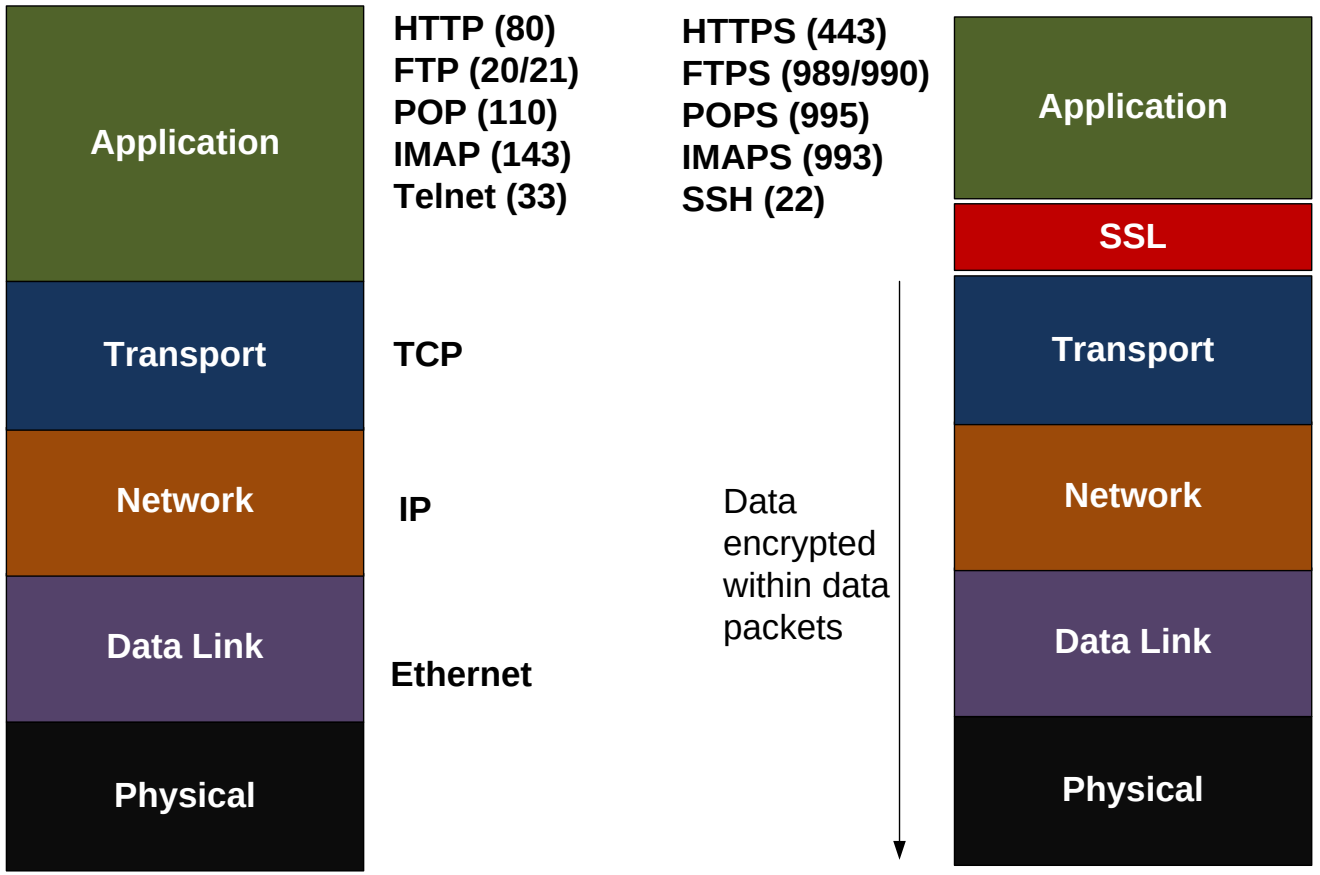


Digital

Investigator

Networking Infrastructures

Tunnelled Protocols: SSL and TLS



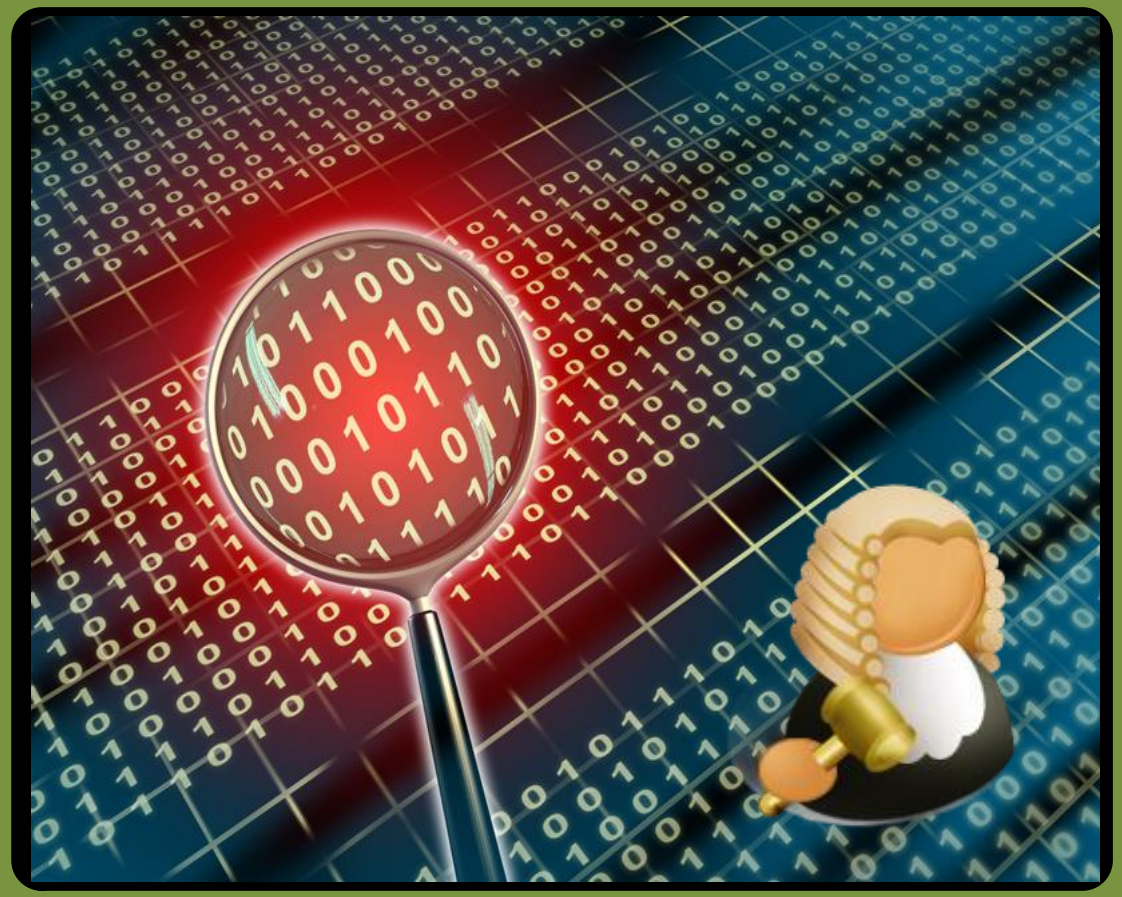
SSL

Net Forensics

Author: Prof Bill Buchanan

SSL

Net Forensics



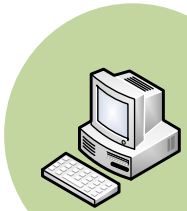
Background on Encryption

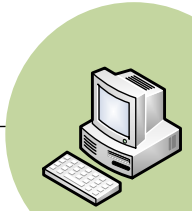
Author: Prof Bill Buchanan

Intruder

C

Confidentially: Secure the data
Risk: Someone listens to communications





Client

I

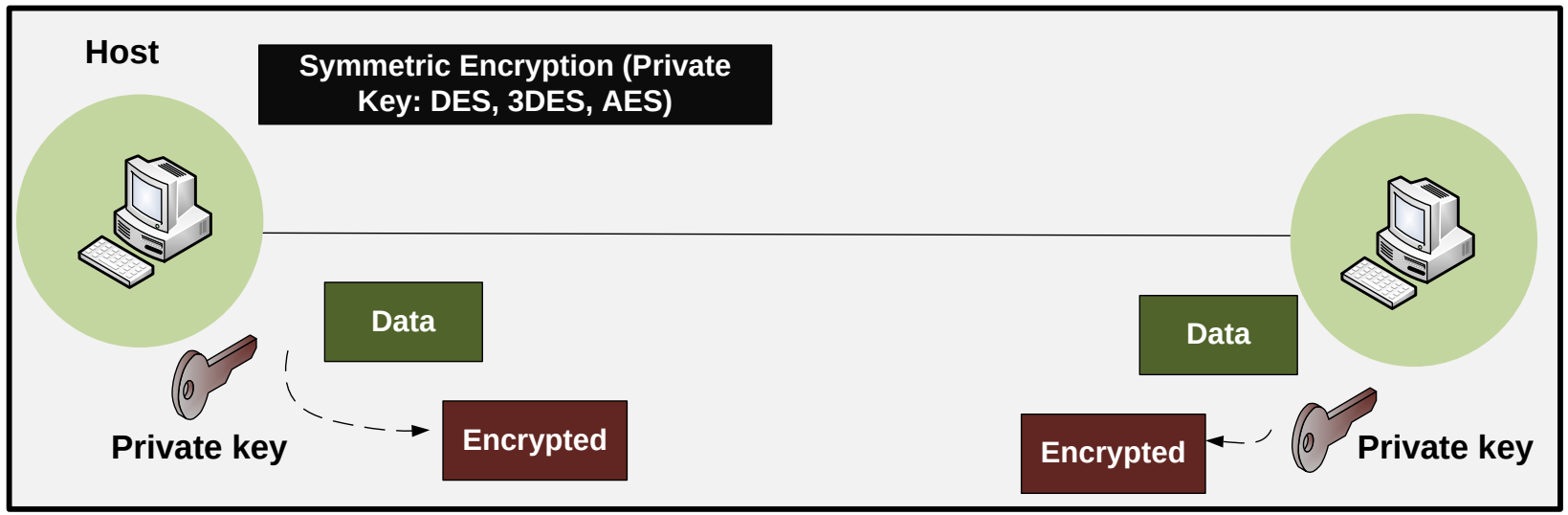
Integrity: Prove the data sent hasn't been changed.
Risk: Someone changes the data

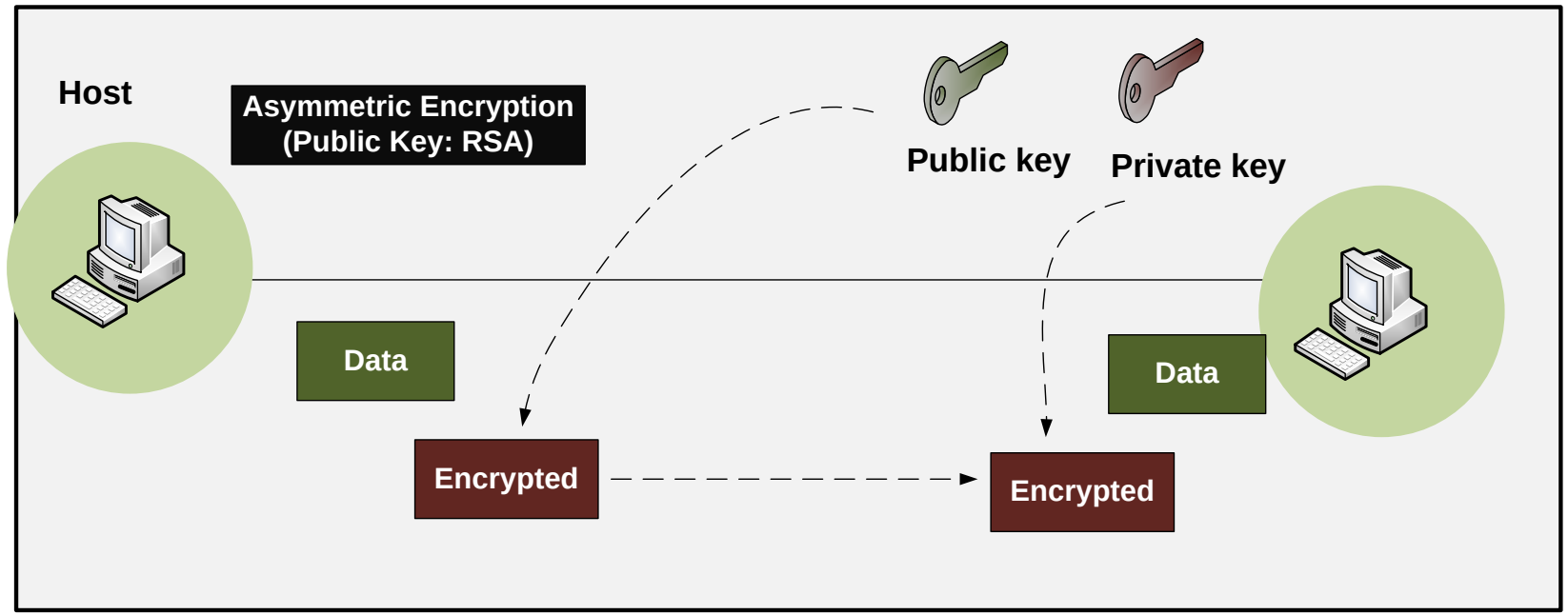
Server

A

Assurance: That the client is the client and the server is the server.
Risk: Some "spoofs" the client or the server or changes it.

Author: Prof Bill Buchanan



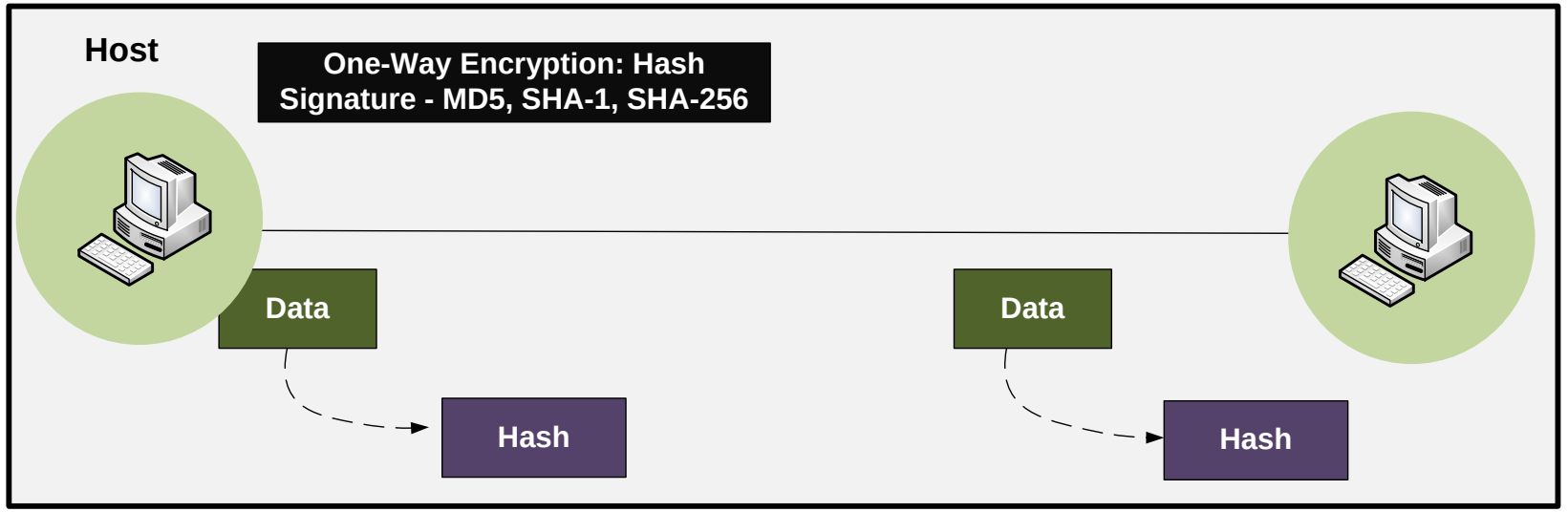


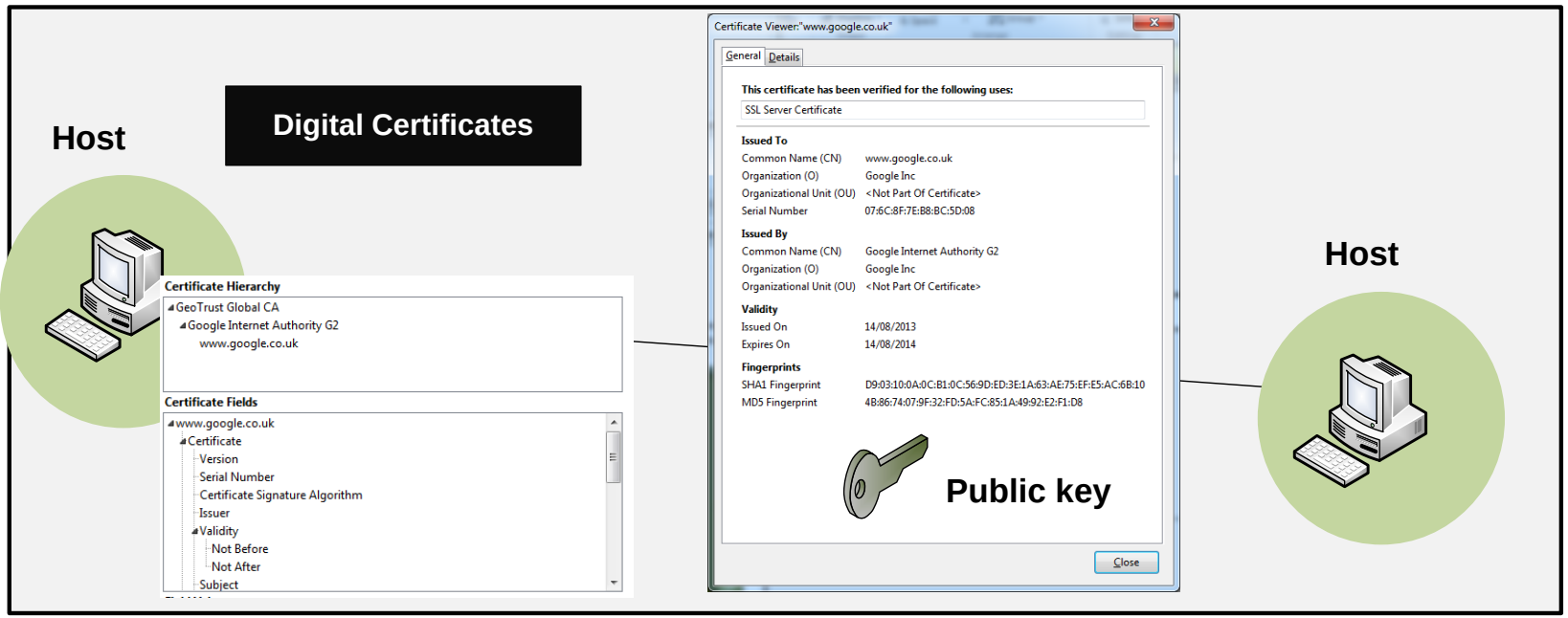
SSL/TLS

Net Forensics

Author: Prof Bill Buchanan

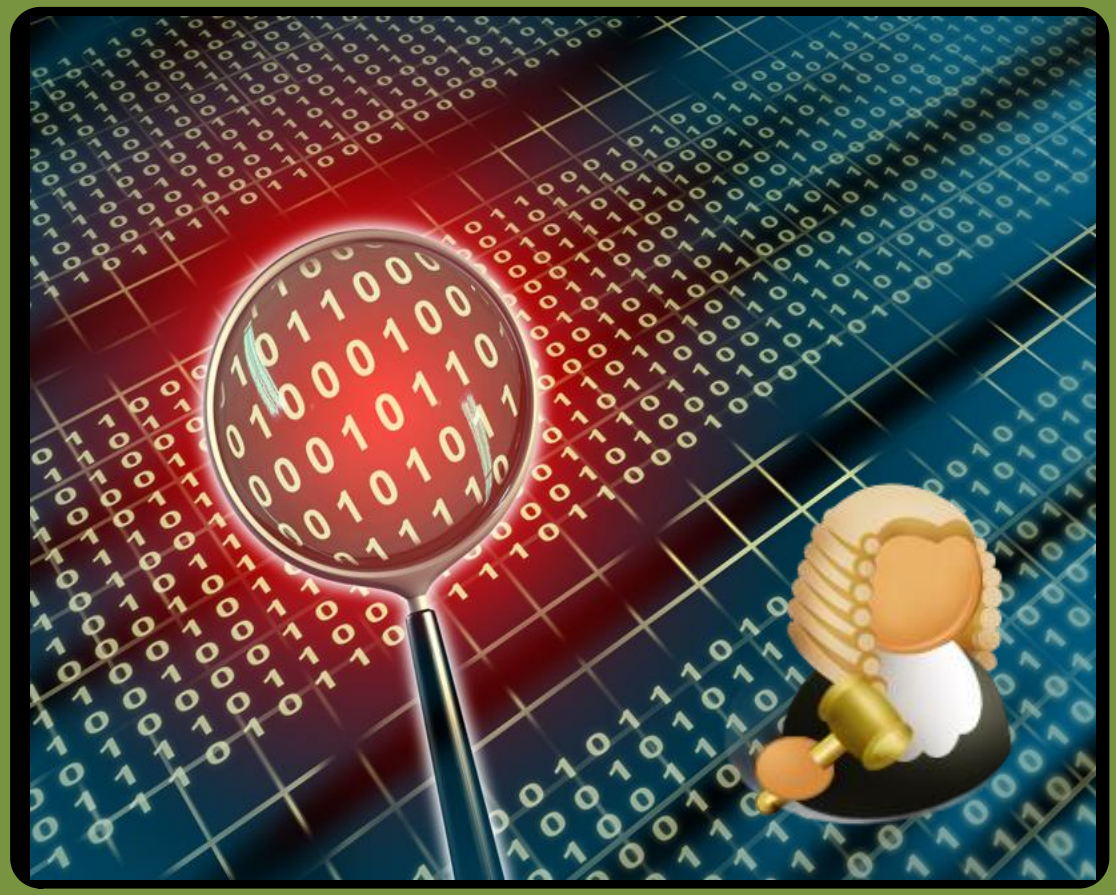
Encryption





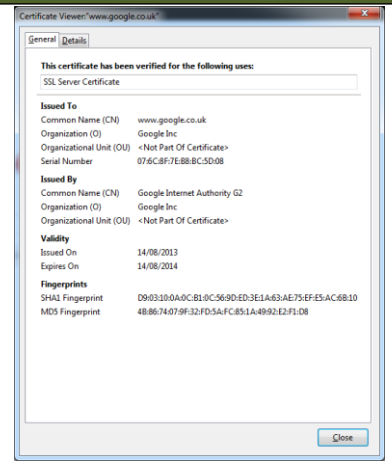
Author: Prof Bill Buchanan

Net Forensics



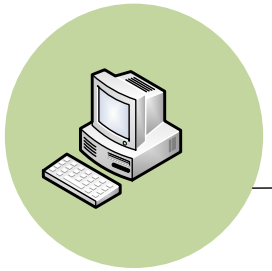
SSL/TLS

Author: Prof Bill Buchanan



Initial Handshake and Server Authentication. Negotiation of:

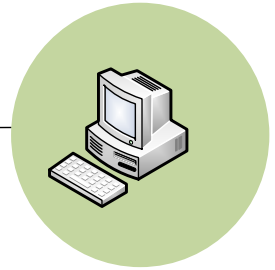
- Encryption methods.
- Key exchange.
- Authentication algorithms.



Client

Here is what I support (DES, AES)

I would like this one (DES).



Server

TLS_RSA_WITH_3DES_EDE_CBC_SHA
Session Key Passed with: RSA
Data Encryption: 3DES
Integrity: SHA

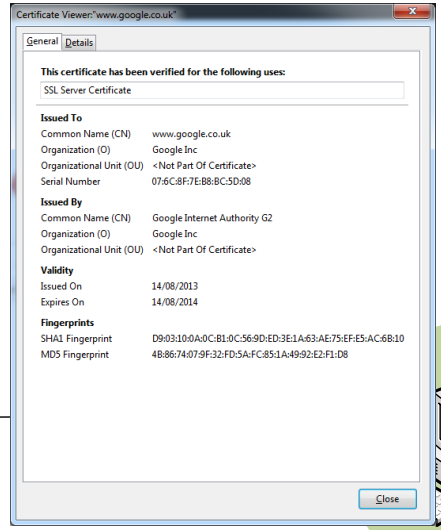
Data (Symmetric Encryption: DES, 3DES, ARCFOUR, AES, Camellia, RC2, IDEA, SEED, NULL).

Author: Prof Bill Buchanan

Server sends its digital certificate

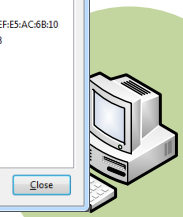
Client

Public key

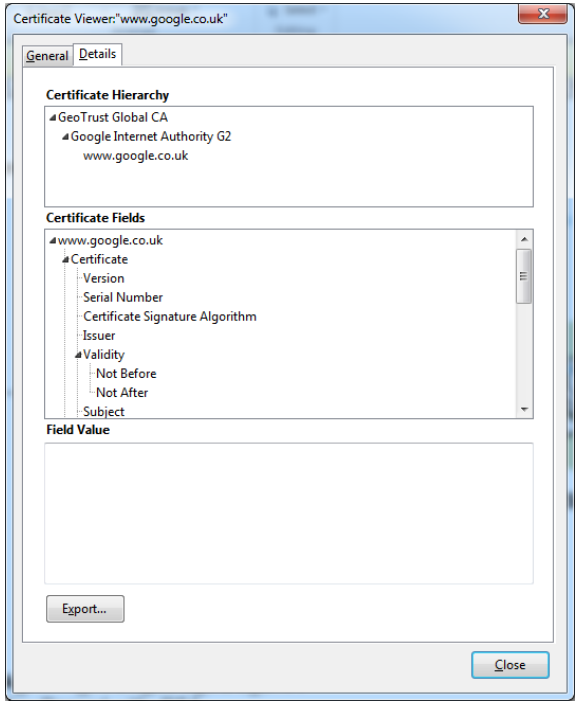


Private key

Server



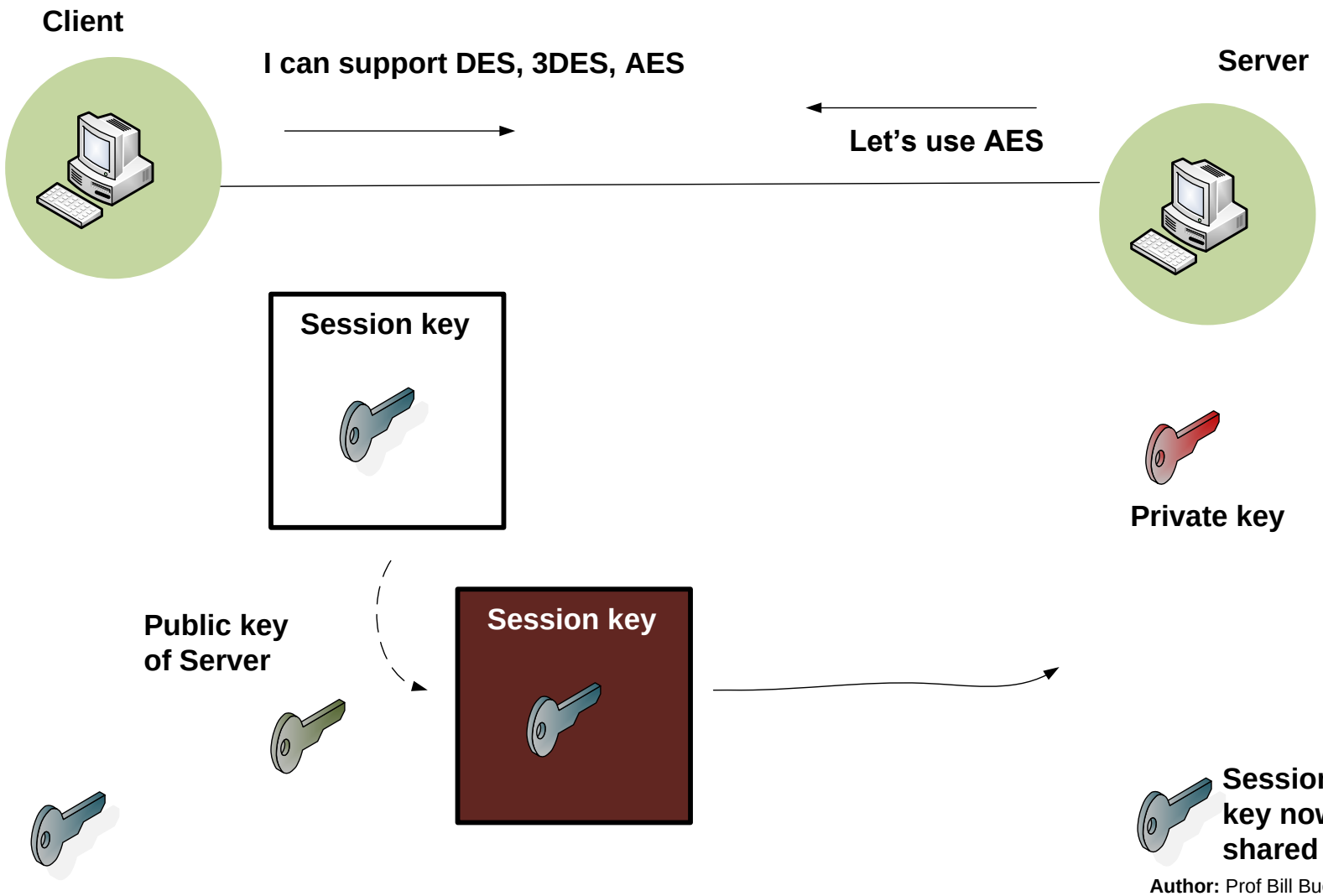
Client check the certificate for its credibility



Client will now use the public key to send encryption key for data

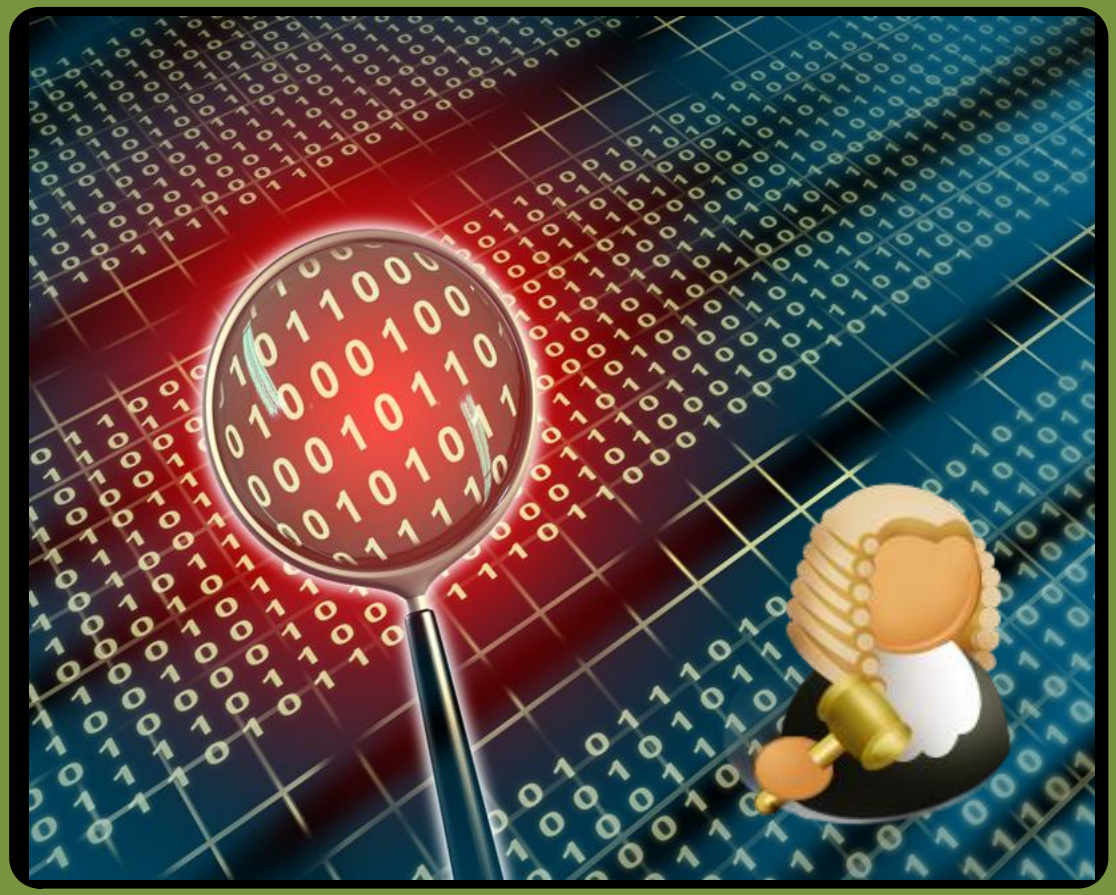
TLS_RSA_WITH_3DES_EDE_CBC_SHA
Session Key Passed with: RSA
Data Encryption: 3DES
Integrity: SHA

Author: Prof Bill Buchanan



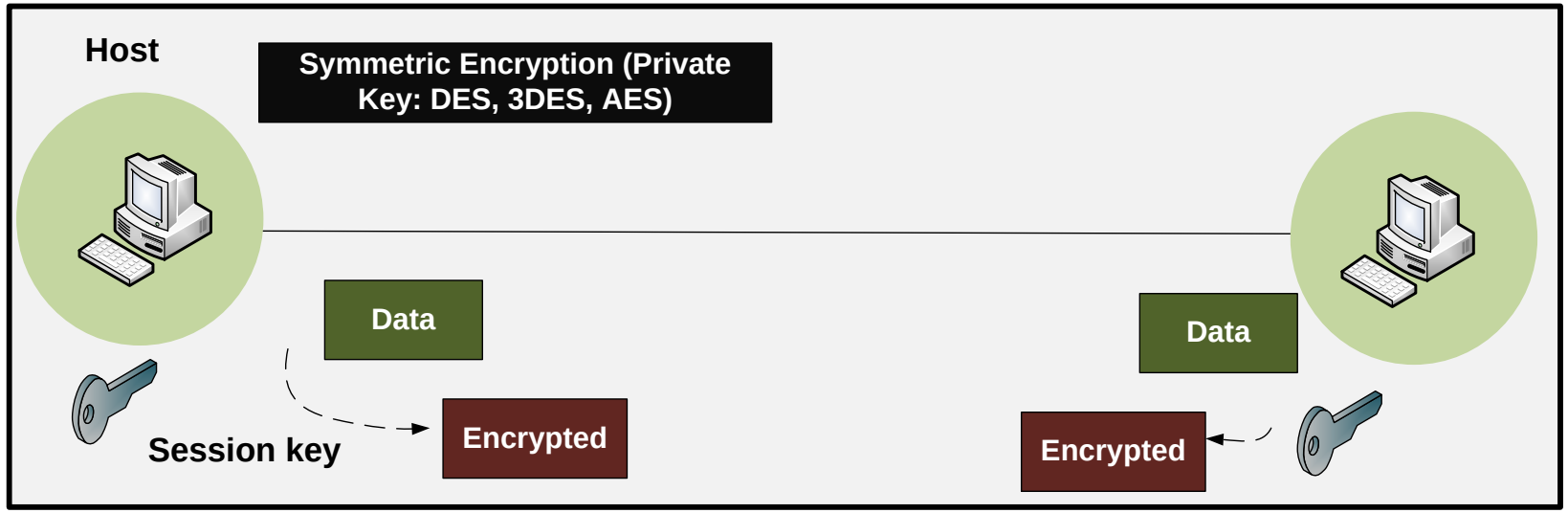
Getting encryption method and session key

Net Forensics



SSL/TLS Traffic

Author: Prof Bill Buchanan



SSL/TLS

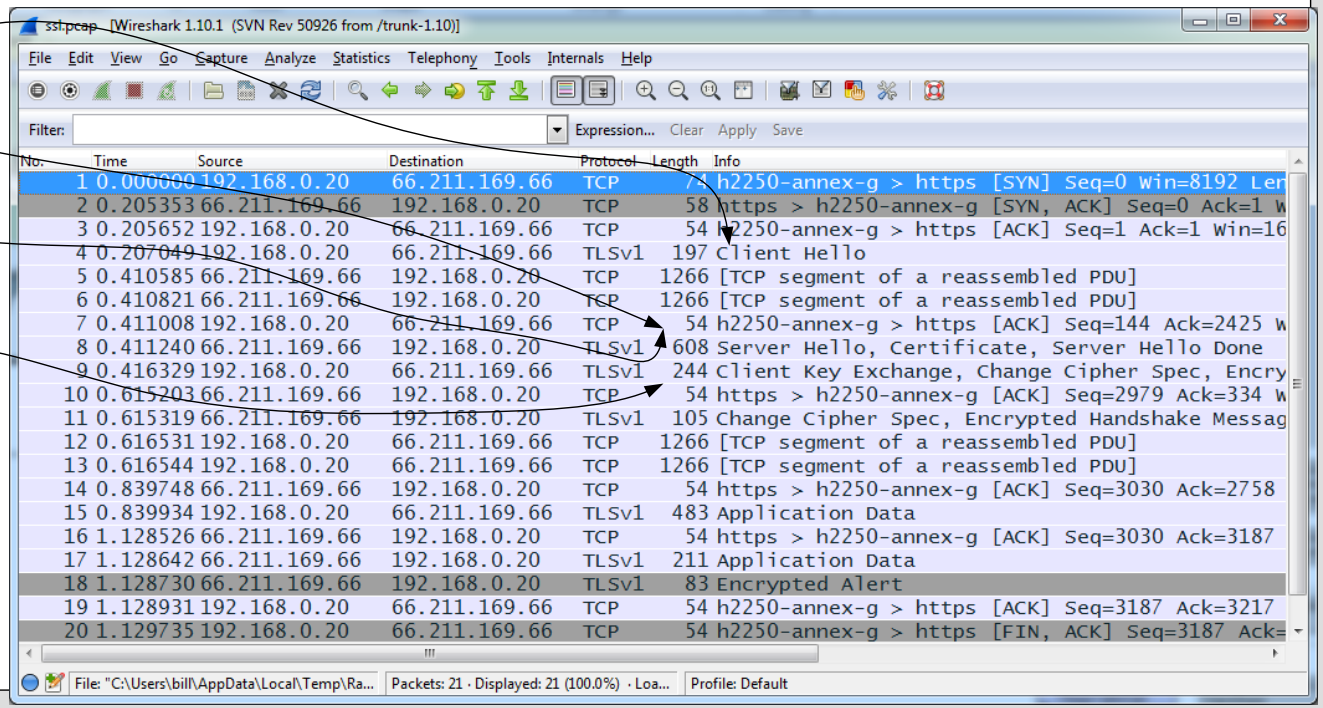
Net Forensics

ClientHello

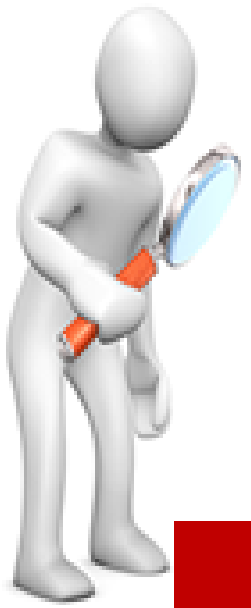
ServerHello

Certificate

Key Exchange



Traffic Flow



Digital

Investigator

Networking Infrastructures

Tunnelled Protocols: SSL and TLS