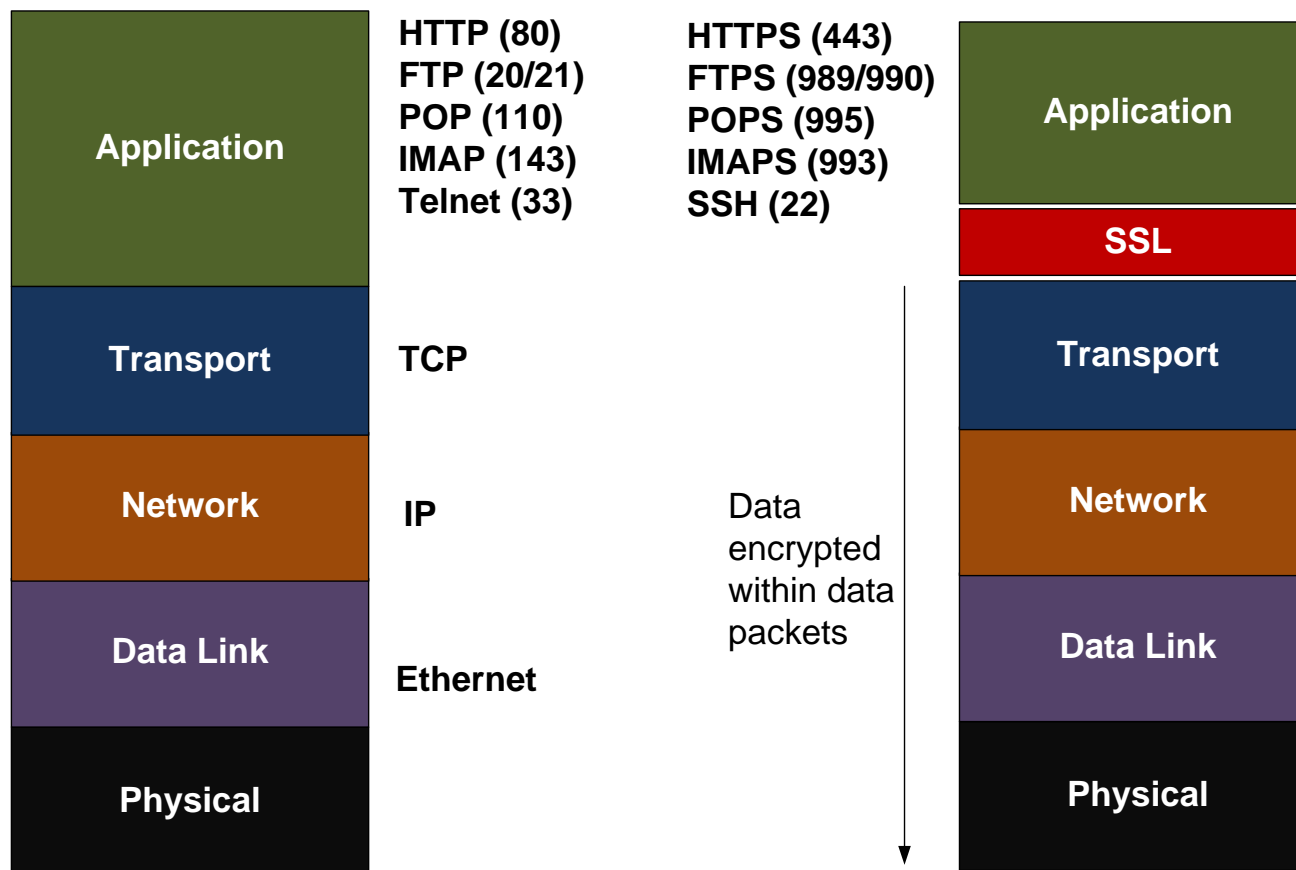


# Digital

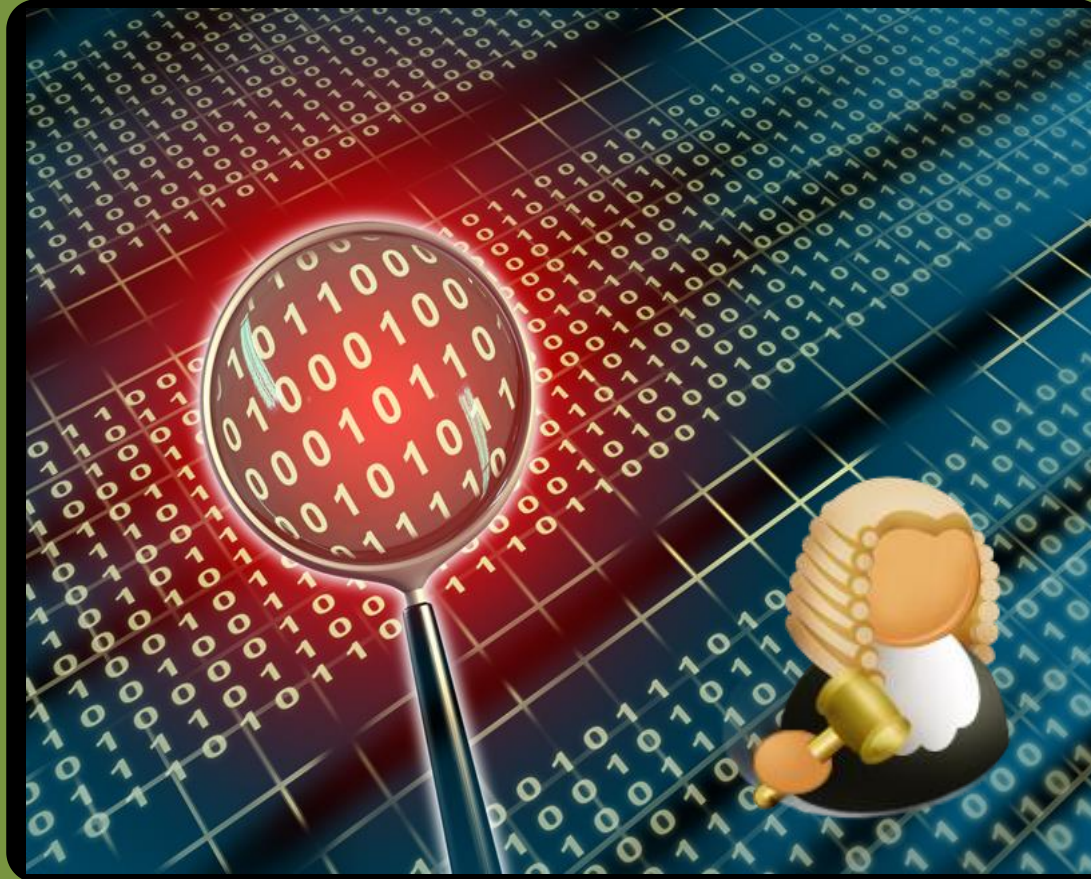
## Investigator

**Networking  
Infrastructures**

**Tunnelled Protocols: SSL and TLS**

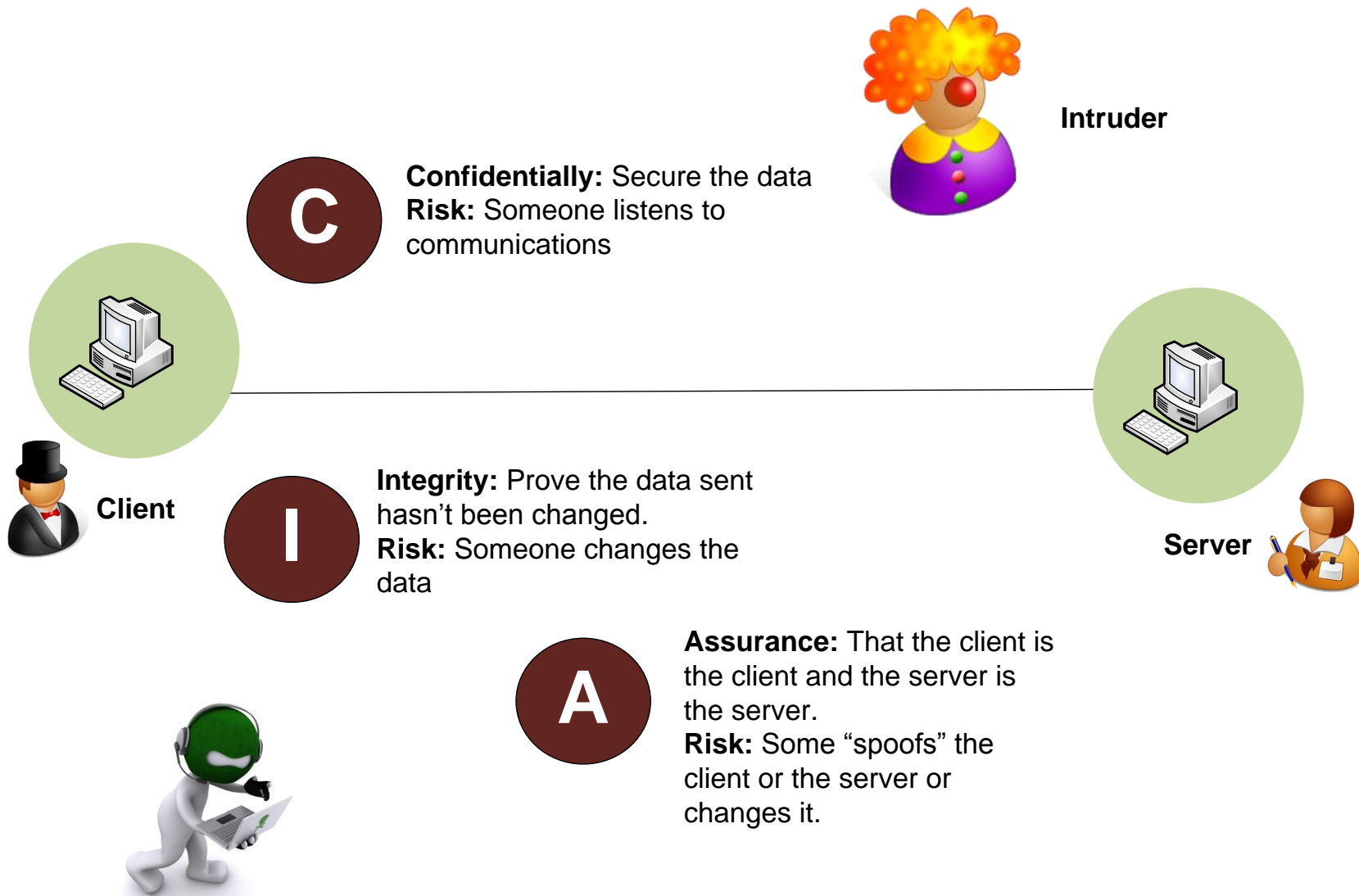


# Net Forensics

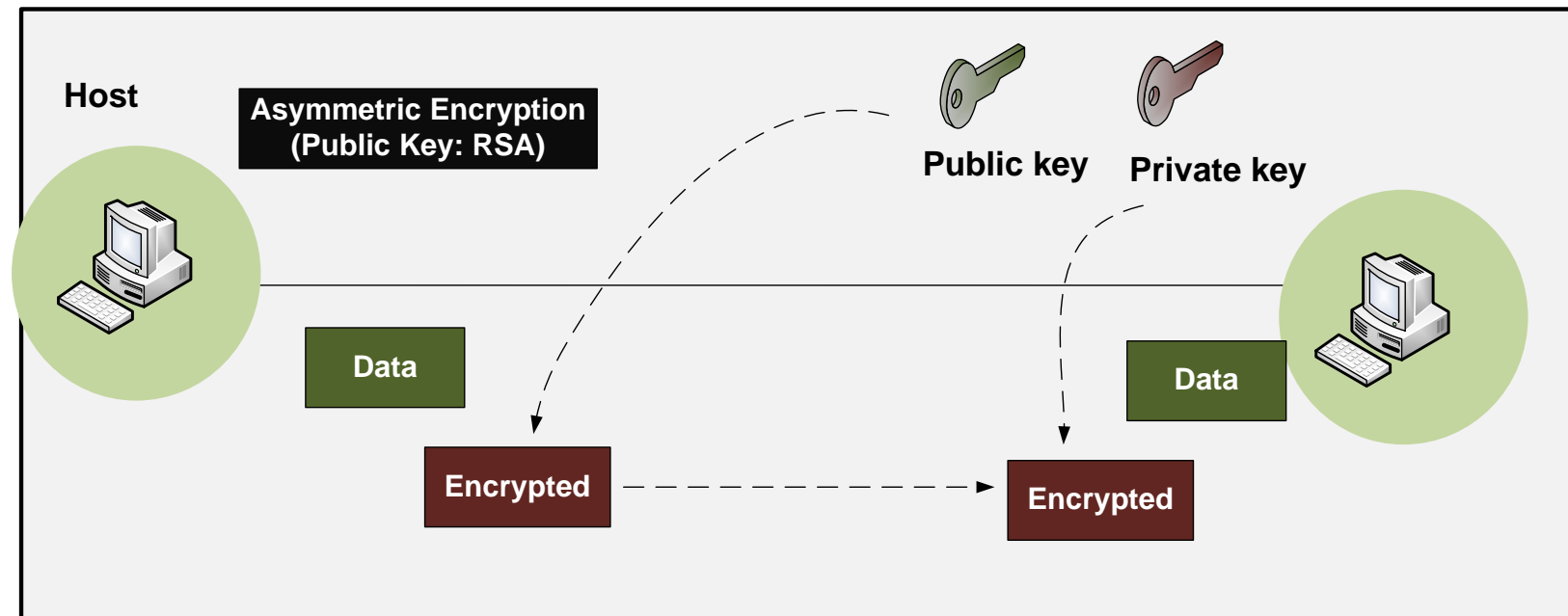
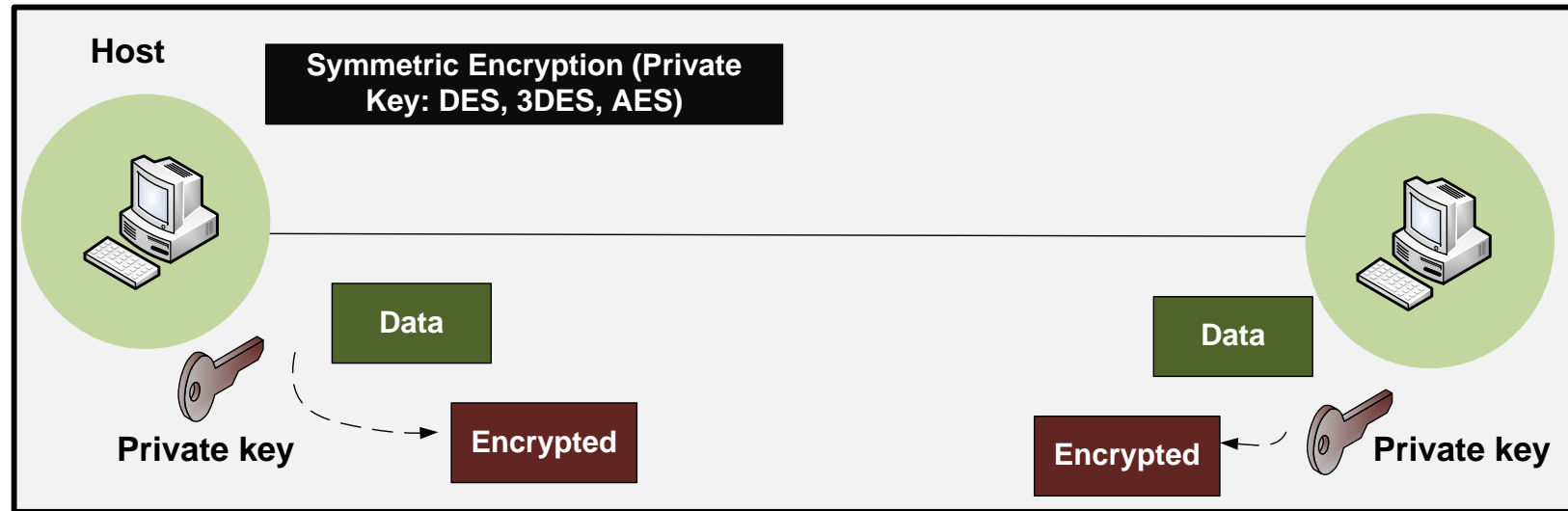


## Background on Encryption

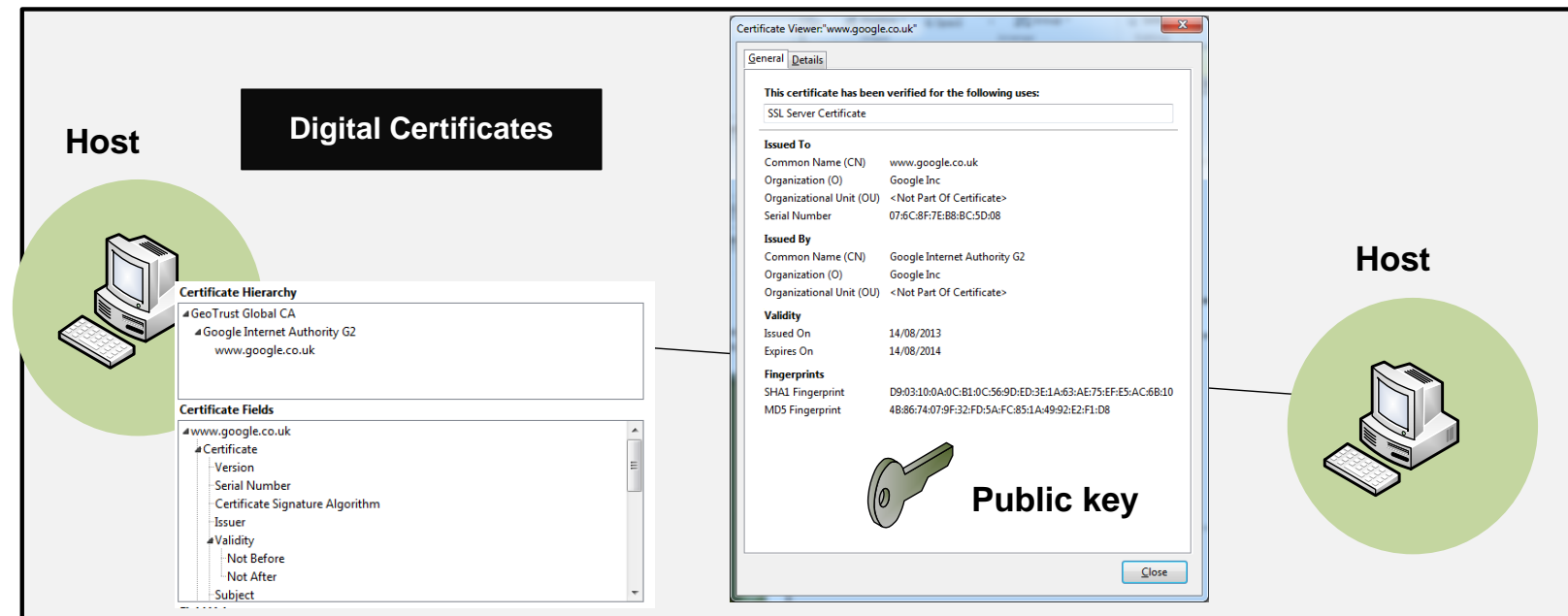
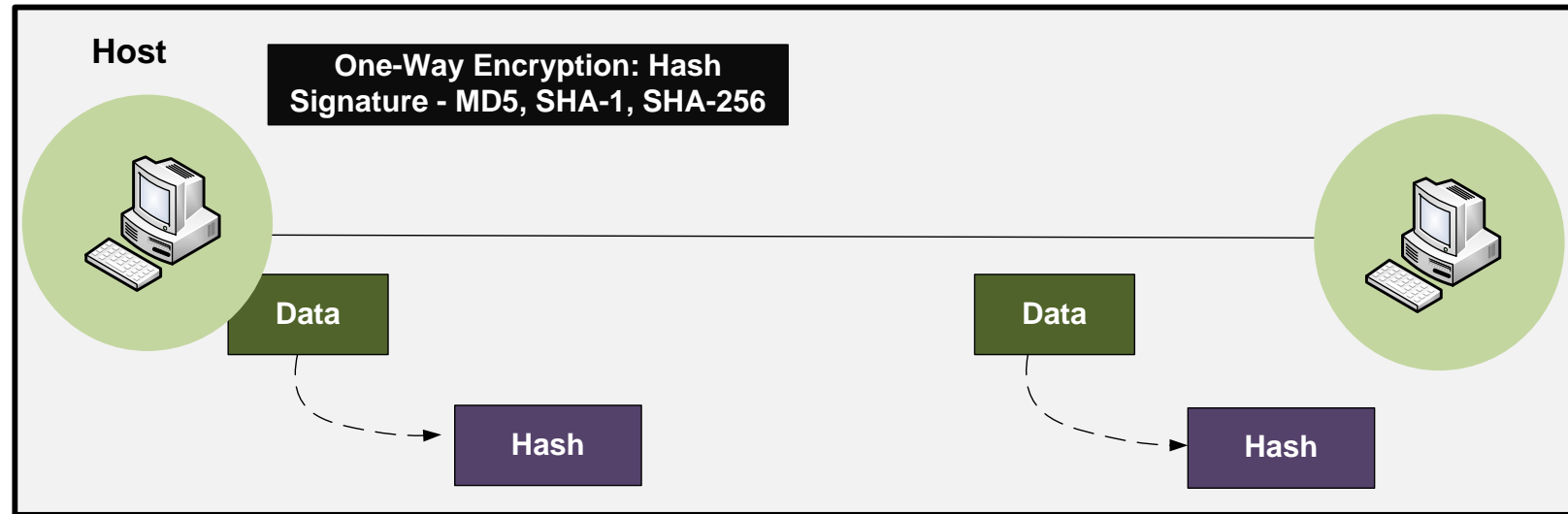
Author: Prof Bill Buchanan



Author: Prof Bill Buchanan



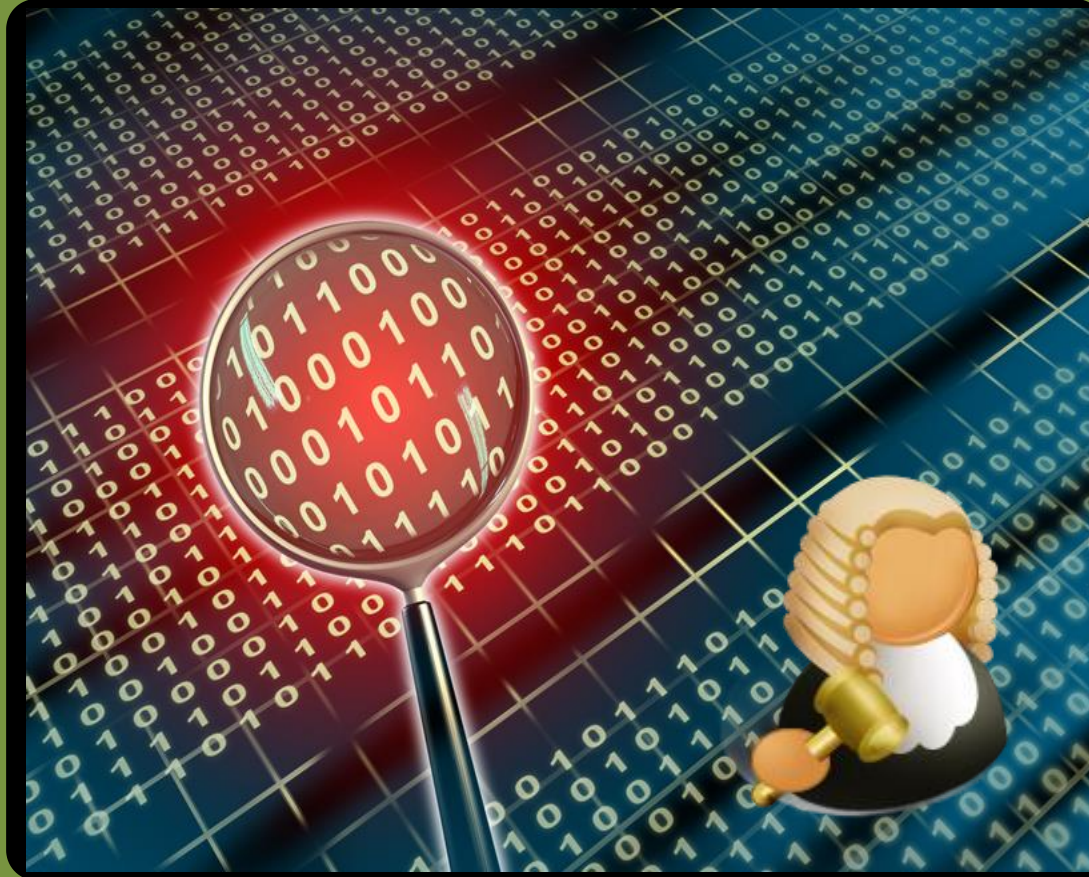
Author: Prof Bill Buchanan



Author: Prof Bill Buchanan



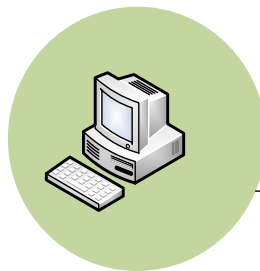
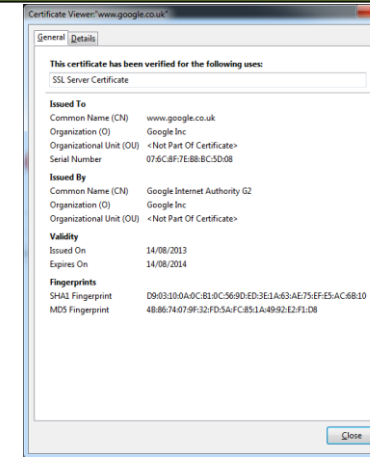
# Net Forensics



SSL/TLS

### Initial Handshake and Server Authentication. Negotiation of:

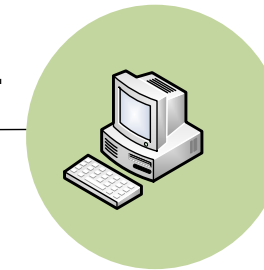
- Encryption methods.
- Key exchange.
- Authentication algorithms.



Client

Here is what  
I support (DES, AES)

I would like this one (DES).

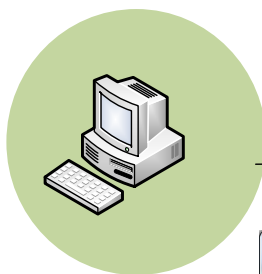
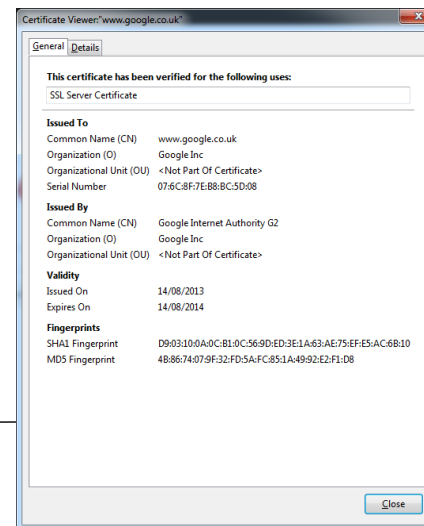
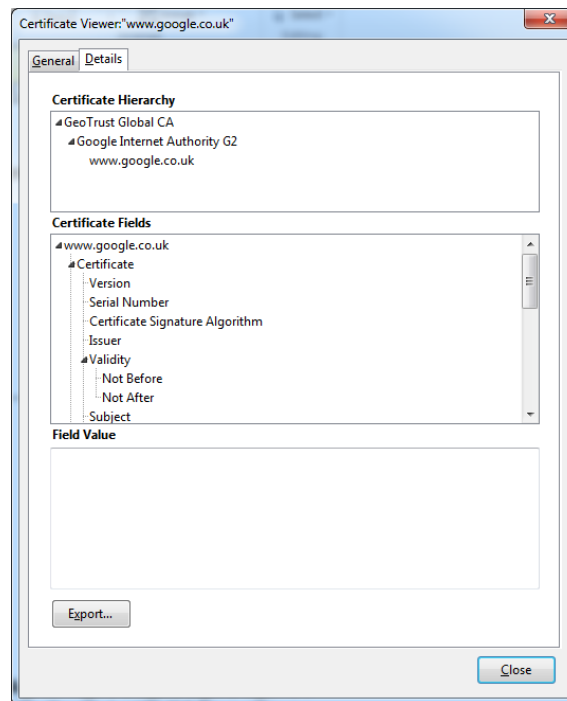
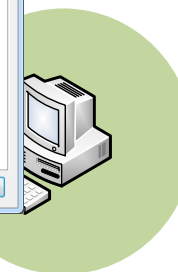


Server

**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).**

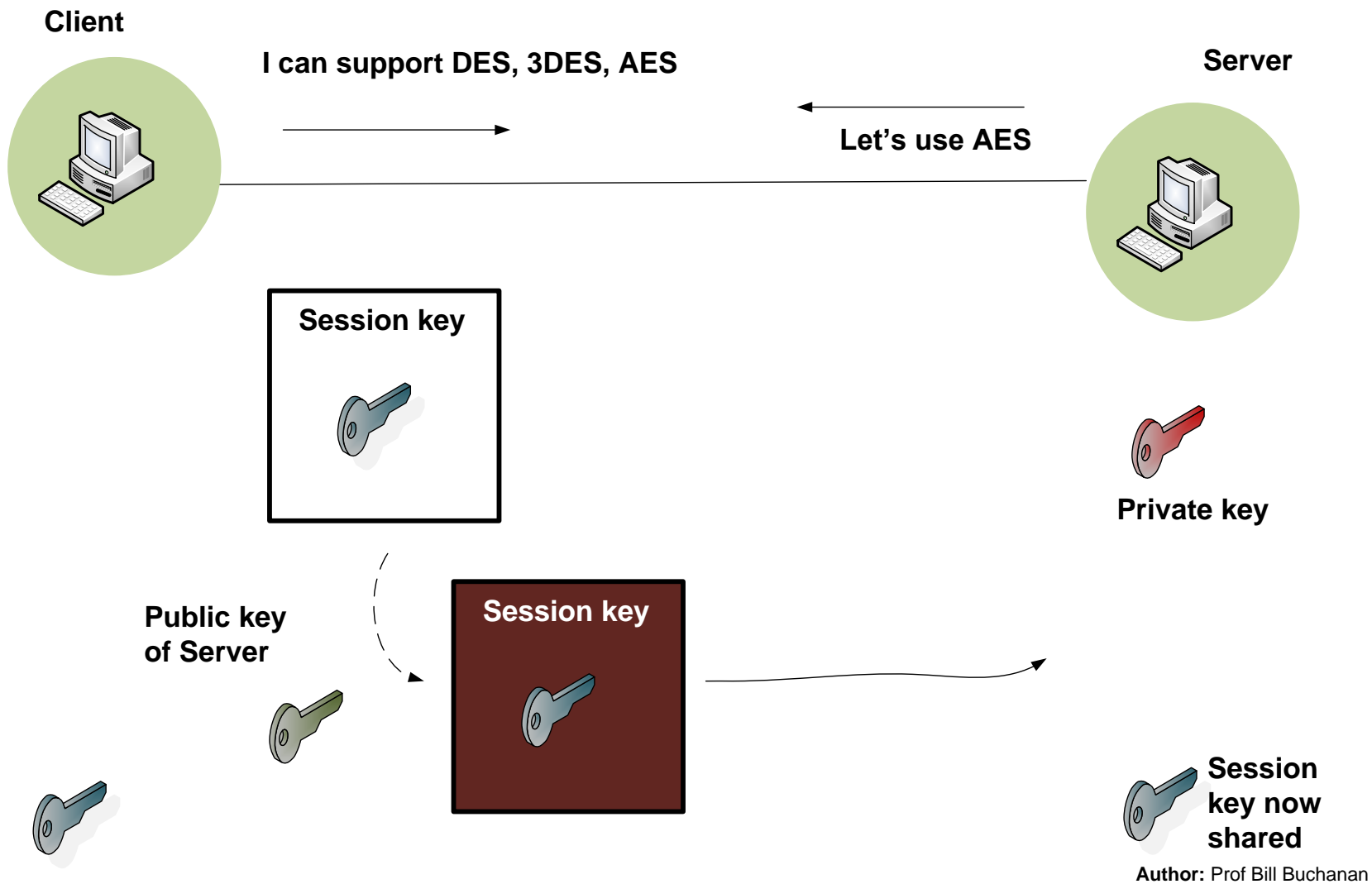


**Client****Client  
check the  
certificate  
for its  
credibility****Client will  
now use the  
public key  
to send  
encryption  
key for data****Server sends its digital certificate****Public key****Private key****Server**

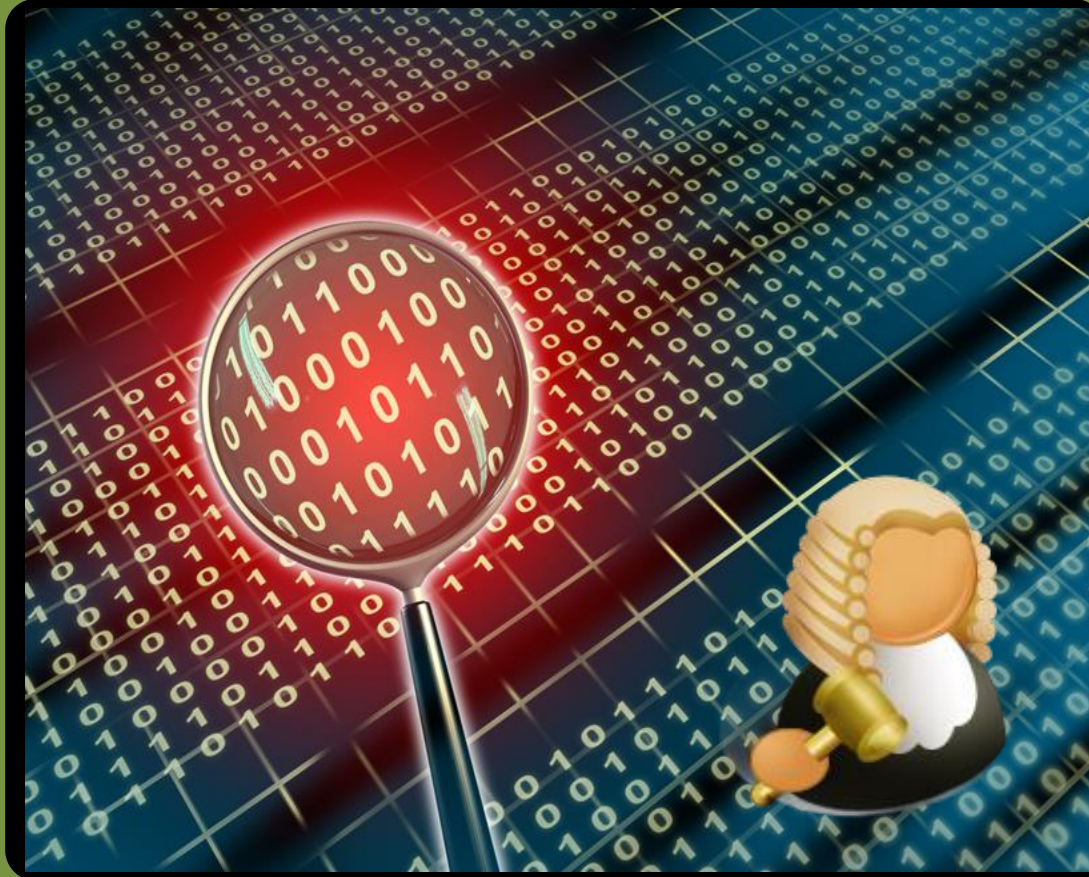
**TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA**  
Session Key Passed with: RSA  
Data Encryption: 3DES  
Integrity: SHA

Author: Prof Bill Buchanan

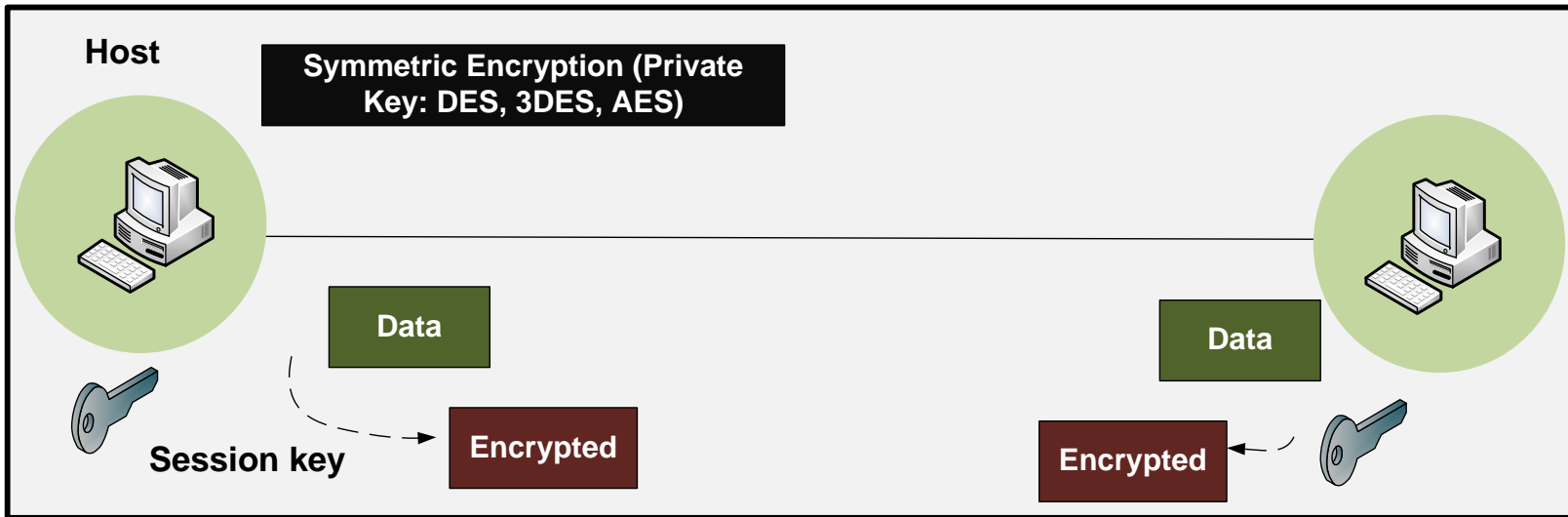
**Authenticating the server and getting key**



# Net Forensics



SSL/TLS Traffic



SSL/TLS

Net Forensics

**ClientHello**

**ServerHello**

**Certificate**

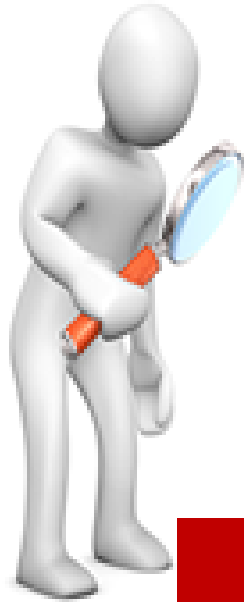
**Key Exchange**

Wireshark 1.10.1 (SVN Rev 50926 from /trunk-1.10)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.20	66.211.169.66	TCP	74	h2250-annex-g > https [SYN] Seq=0 Win=8192 Len=0
2	0.205353	66.211.169.66	192.168.0.20	TCP	58	https > h2250-annex-g [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0
3	0.205652	192.168.0.20	66.211.169.66	TCP	54	h2250-annex-g > https [ACK] Seq=1 Ack=1 Win=16 Len=0
4	0.207049	192.168.0.20	66.211.169.66	TLSv1	197	Client Hello
5	0.410585	66.211.169.66	192.168.0.20	TCP	1266	[TCP segment of a reassembled PDU]
6	0.410821	66.211.169.66	192.168.0.20	TCP	1266	[TCP segment of a reassembled PDU]
7	0.411008	192.168.0.20	66.211.169.66	TCP	54	h2250-annex-g > https [ACK] Seq=144 Ack=2425 Win=0 Len=0
8	0.411240	66.211.169.66	192.168.0.20	TLSv1	608	Server Hello, Certificate, Server Hello Done
9	0.416329	192.168.0.20	66.211.169.66	TLSv1	244	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
10	0.615203	66.211.169.66	192.168.0.20	TCP	54	https > h2250-annex-g [ACK] Seq=2979 Ack=334 Win=0 Len=0
11	0.615319	66.211.169.66	192.168.0.20	TLSv1	105	Change Cipher Spec, Encrypted Handshake Message
12	0.616531	192.168.0.20	66.211.169.66	TCP	1266	[TCP segment of a reassembled PDU]
13	0.616544	192.168.0.20	66.211.169.66	TCP	1266	[TCP segment of a reassembled PDU]
14	0.839748	66.211.169.66	192.168.0.20	TCP	54	https > h2250-annex-g [ACK] Seq=3030 Ack=2758 Win=0 Len=0
15	0.839934	192.168.0.20	66.211.169.66	TLSv1	483	Application Data
16	1.128526	66.211.169.66	192.168.0.20	TCP	54	https > h2250-annex-g [ACK] Seq=3030 Ack=3187 Win=0 Len=0
17	1.128642	66.211.169.66	192.168.0.20	TLSv1	211	Application Data
18	1.128730	66.211.169.66	192.168.0.20	TLSv1	83	Encrypted Alert
19	1.128931	192.168.0.20	66.211.169.66	TCP	54	h2250-annex-g > https [ACK] Seq=3187 Ack=3217 Win=0 Len=0
20	1.129735	192.168.0.20	66.211.169.66	TCP	54	h2250-annex-g > https [FIN, ACK] Seq=3187 Ack=3217 Win=0 Len=0

File: "C:\Users\bill\AppData\Local\Temp\R... Packets: 21 · Displayed: 21 (100.0%) · Load Profile: Default

**Traffic Flow**



# Digital

## Investigator

**Networking  
Infrastructures**

**Tunnelled Protocols: SSL and TLS**