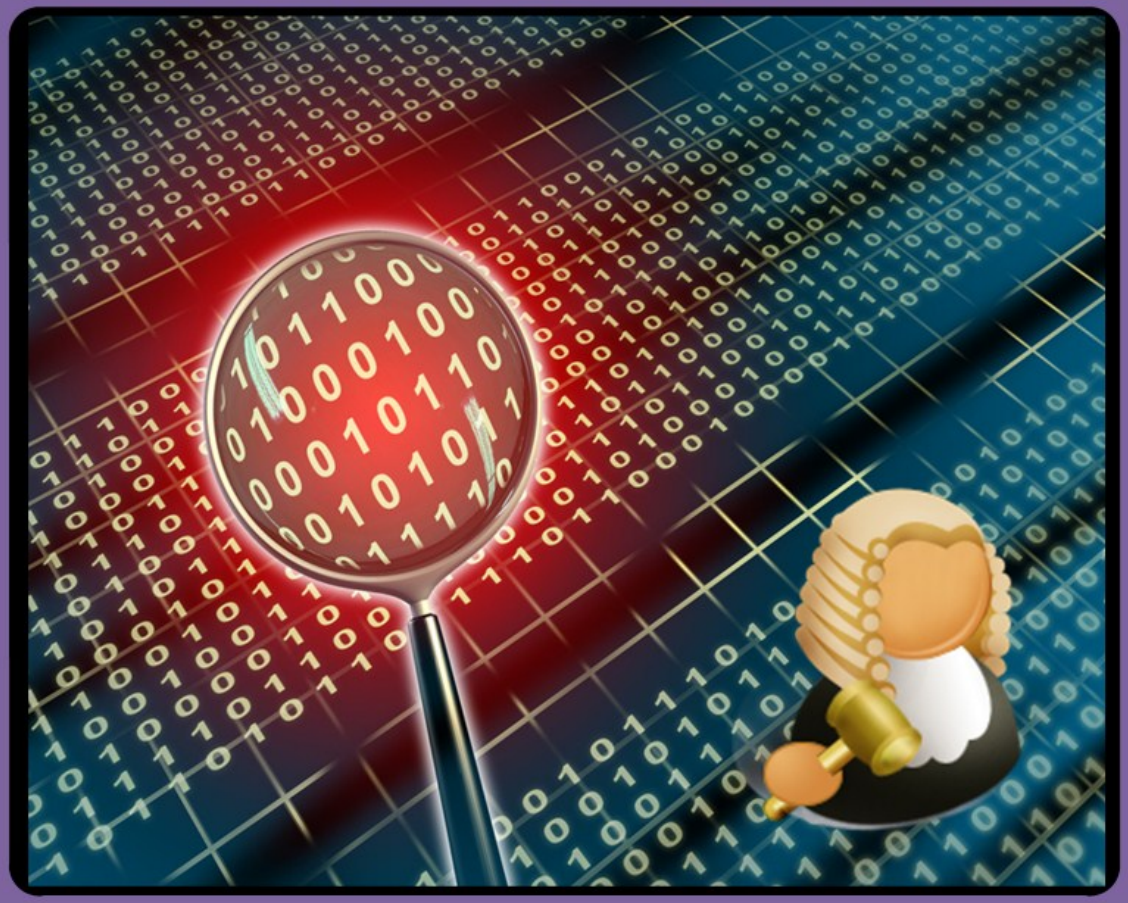
Data Hiding and Obfuscation

- Outline obfuscation methods.
- Define methods used to encode data in order to hide the original content.
- Understand encryption methods used to hide data, and possible methods to overcome this obfuscation.
- Define how file types can be discovered.

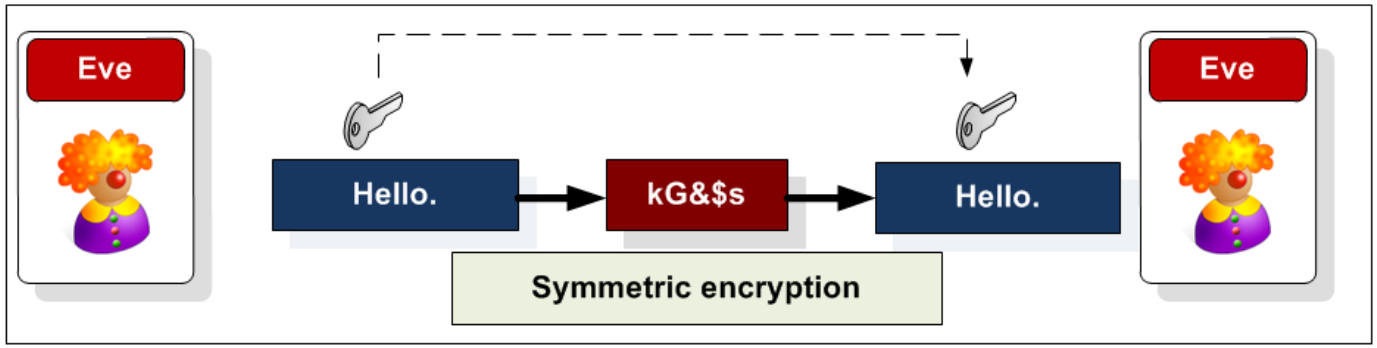
Author: Prof Bill Buchanan

Data Hiding

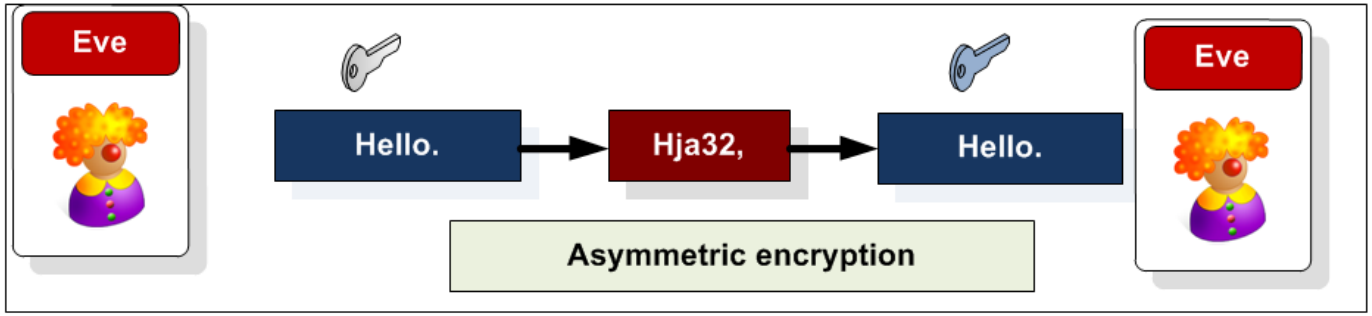


Obfuscation by Encryption

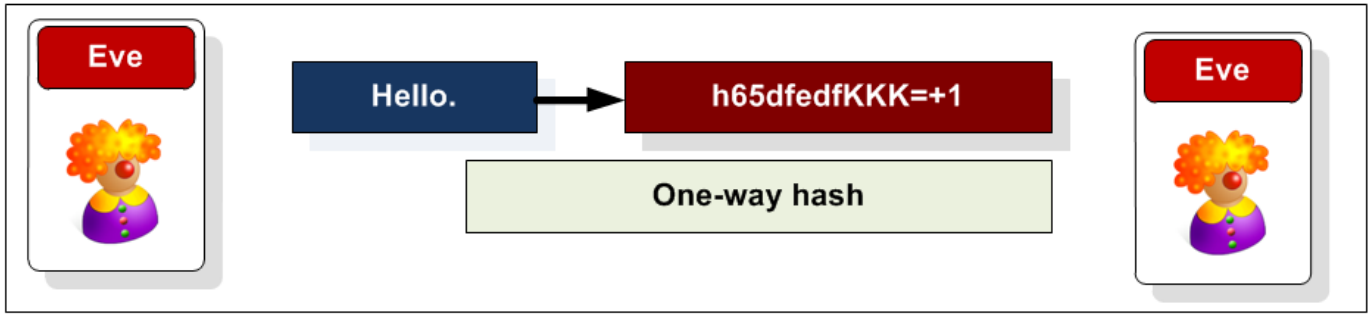
Author: Prof Bill Buchanan



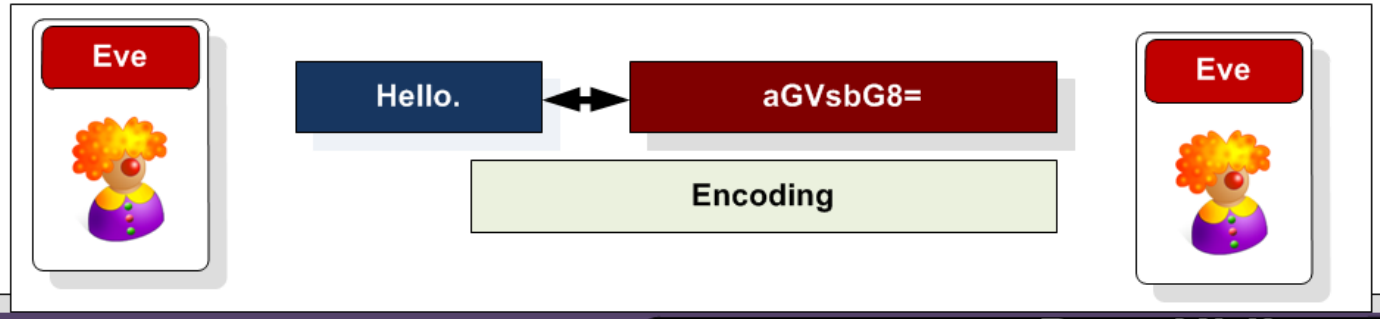
Private-key:
RC2, RC4,
DES, 3DES,
AES



Public-key:
RSA, DSA
(factoring prime
numbers)
FIPS 186-2,
ElGamal
(Elliptic curve)



Hashing:
MD5, SHA-1



Encoding:
Hex, Base-64,
ASCII, UTF-16

Encryption

Data Hiding

Author: Prof Bill Buchanan

test

6XzX5ASPylUE6K
thRc1UmA==

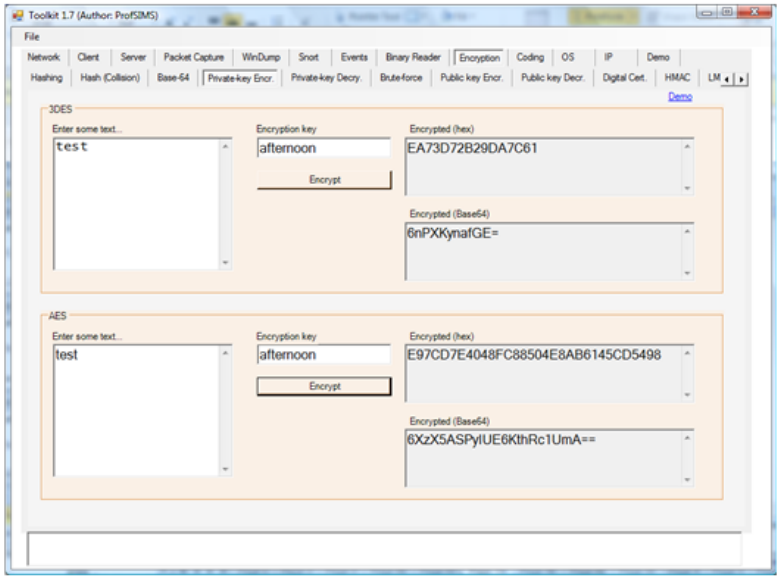
Search for key strings

```
crimedoesntpay
finaldemand
Mypassword
celticfc
```

Dictionary

```
a
abilities
ability
ability's
able
about
Above
….
young
your
yours
yourself
zero
zero's
```

Brute-force

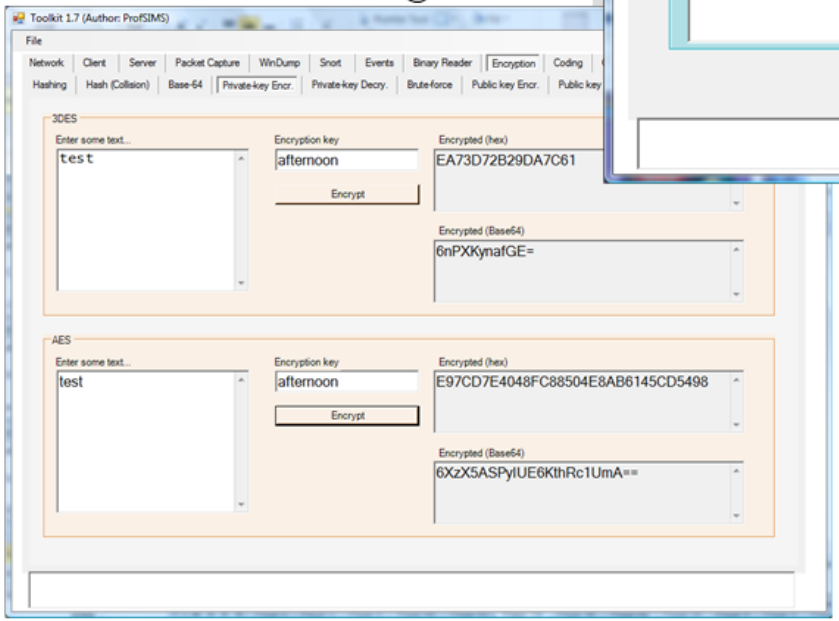


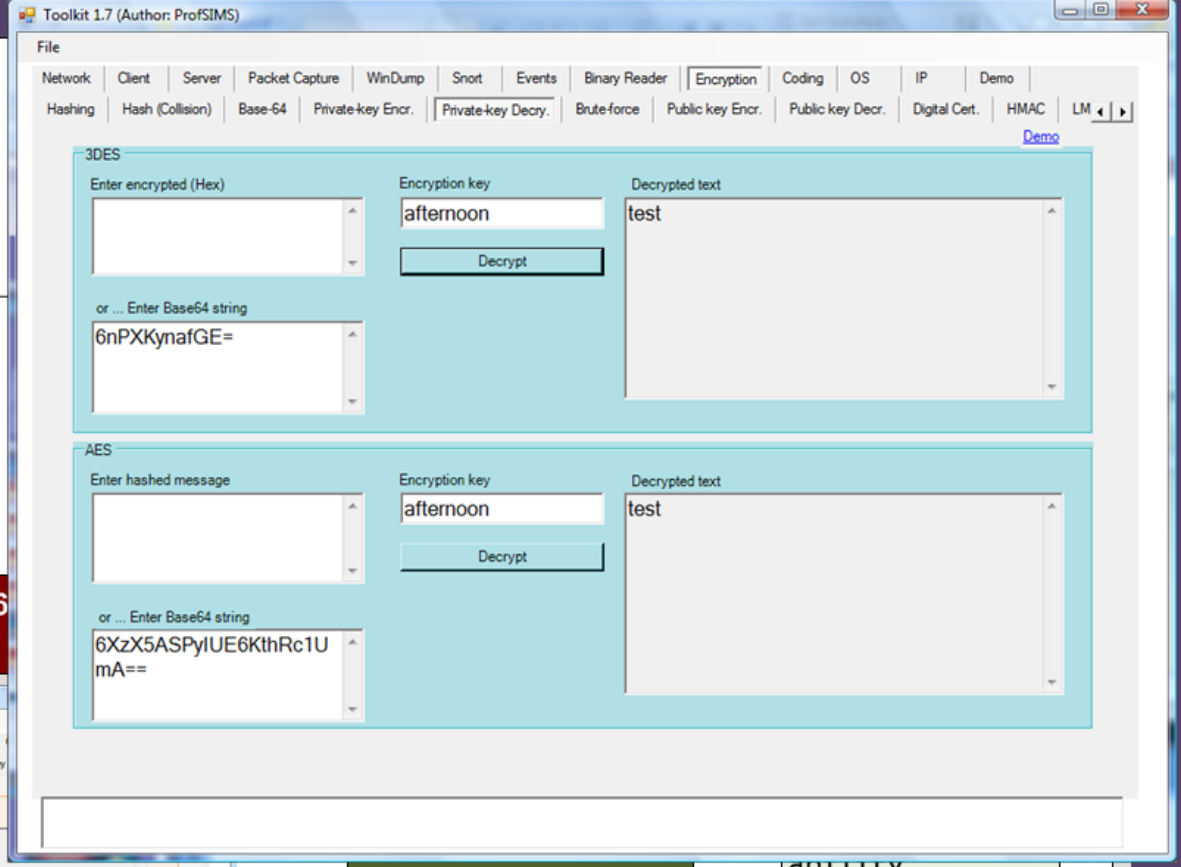
Author: Prof Bill Buchanan

Encryption

Data Hiding

test



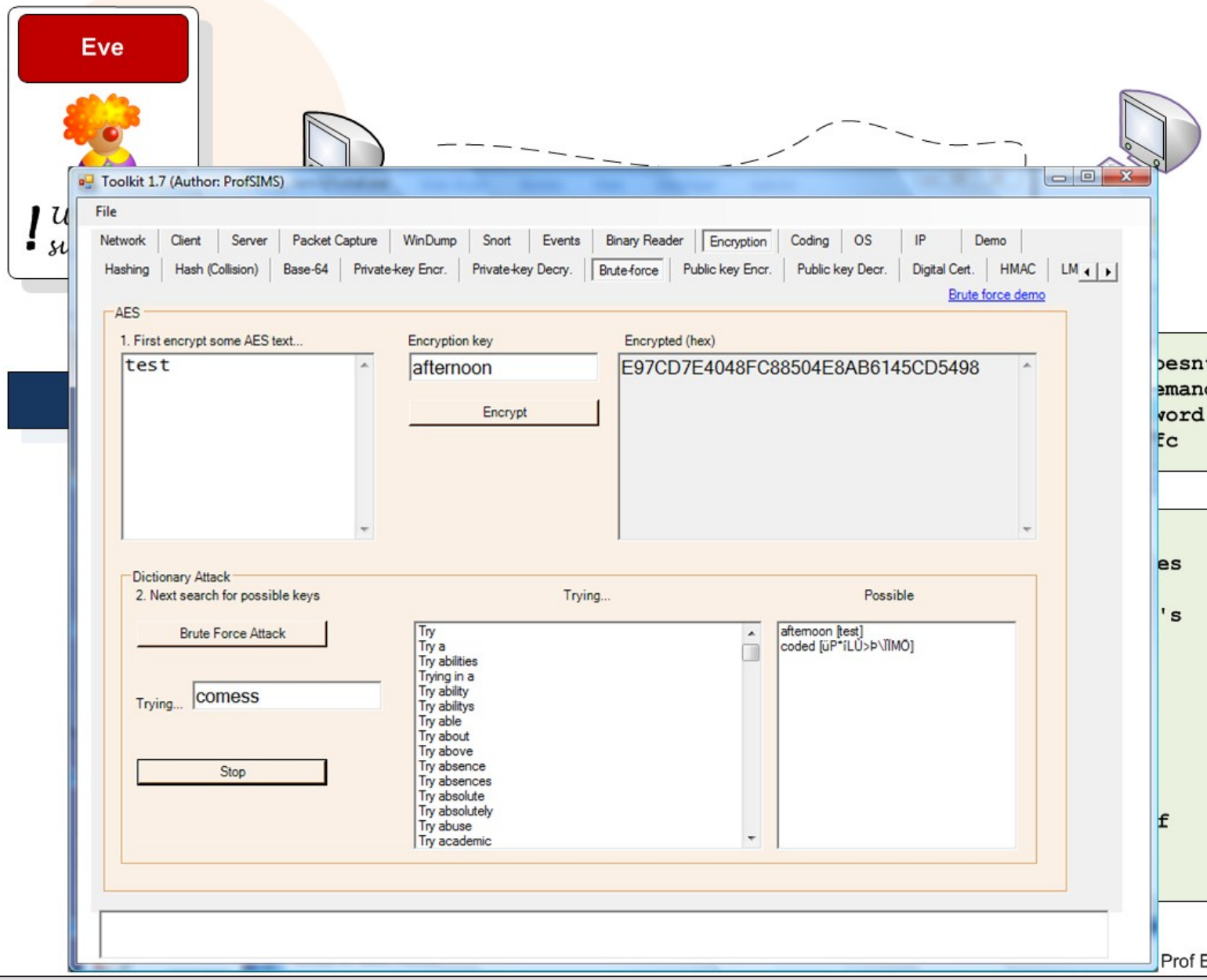


Brute-force

```
ability
ability's
able
about
Above
….
young
your
yours
yourself
zero
zero's
```

Author: Prof Bill Buchanan

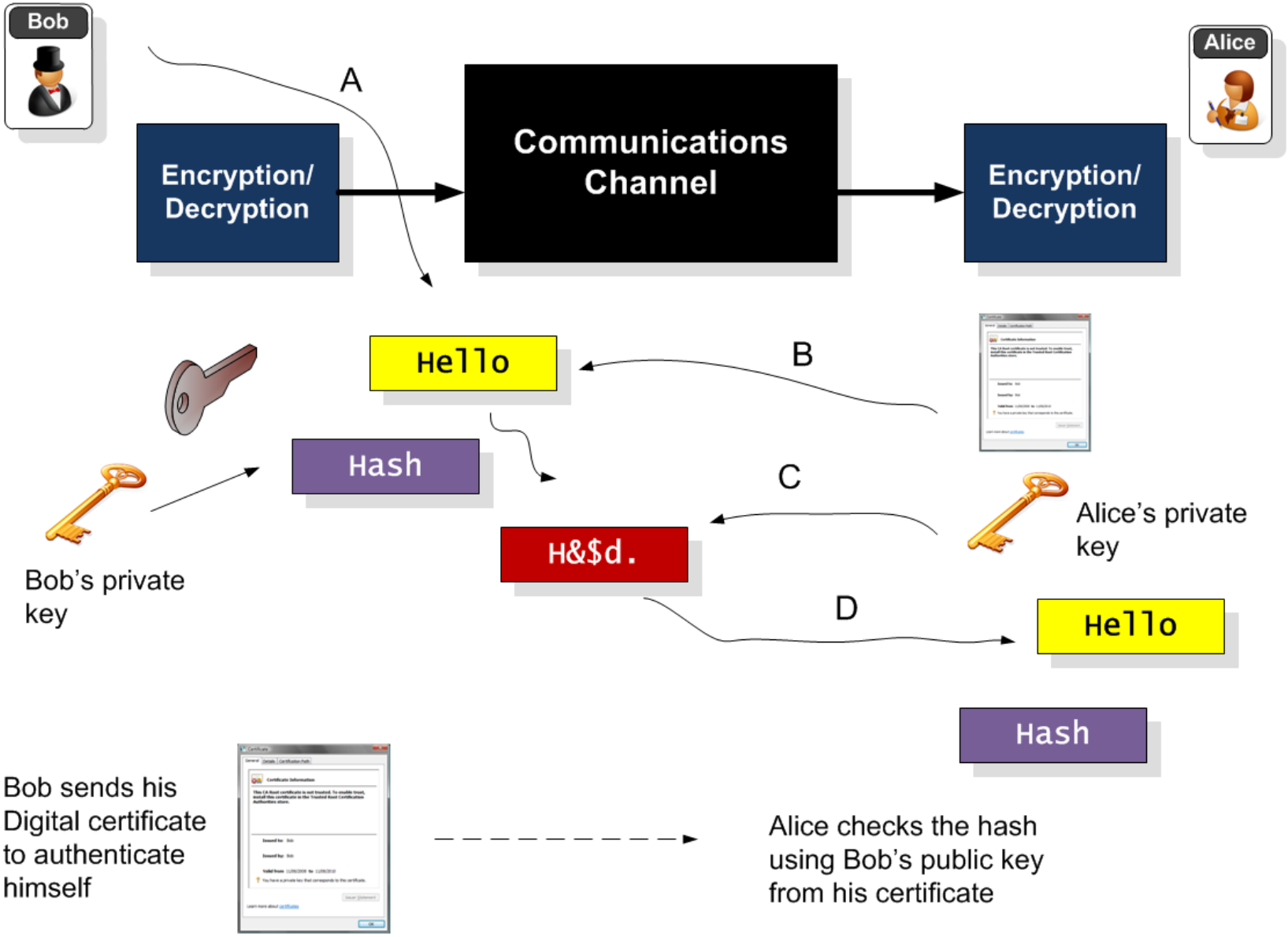
Cracking the key



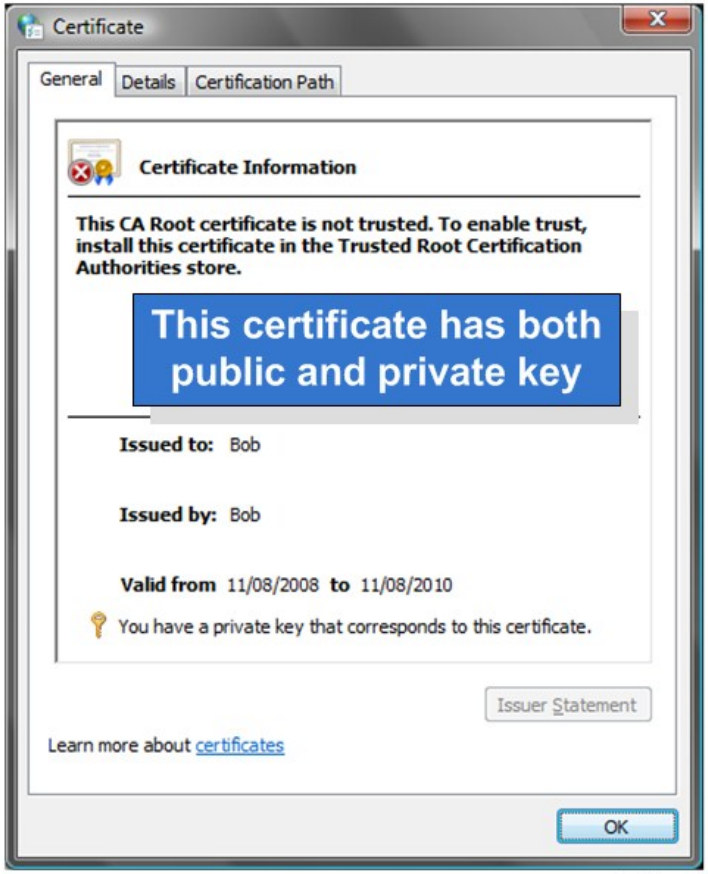
Encryption

Data Hiding

Cracking the key



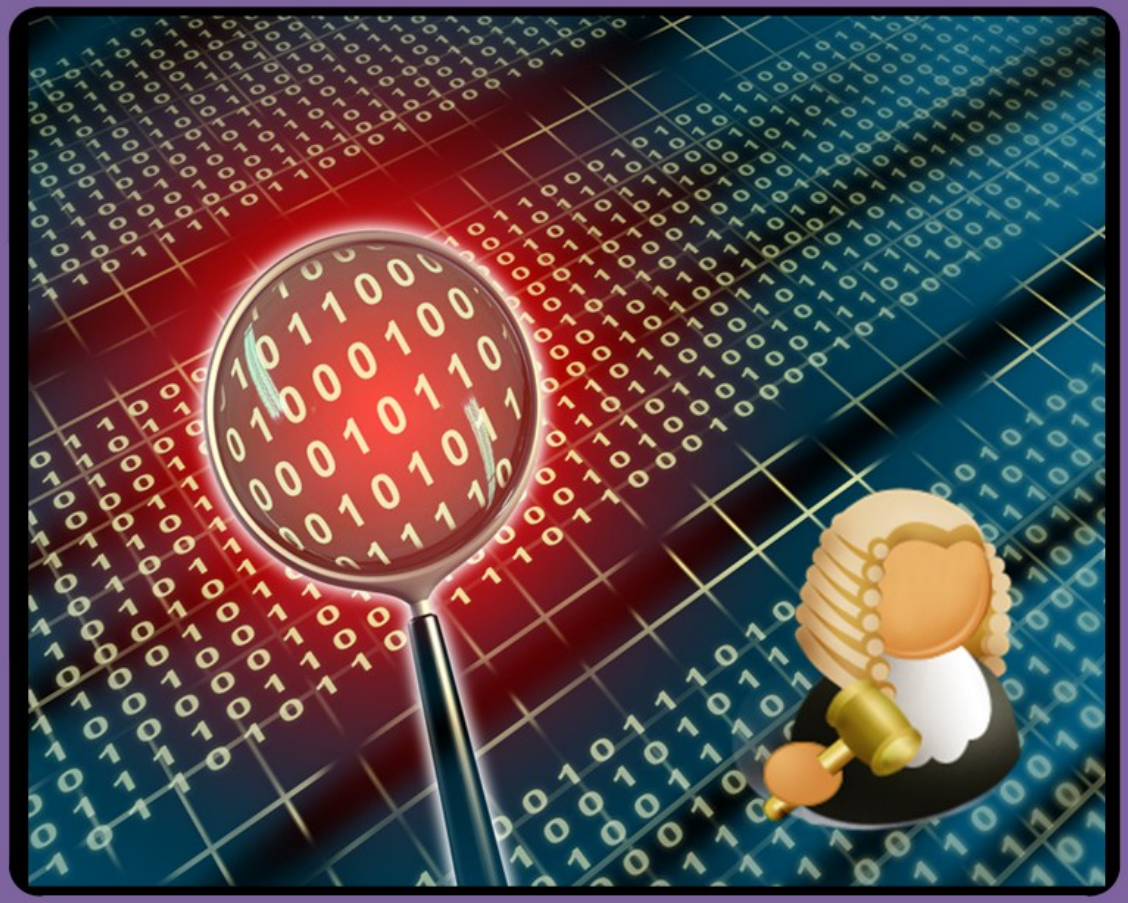
Author: Prof Bill Buchanan



Author: Prof Bill Buchanan

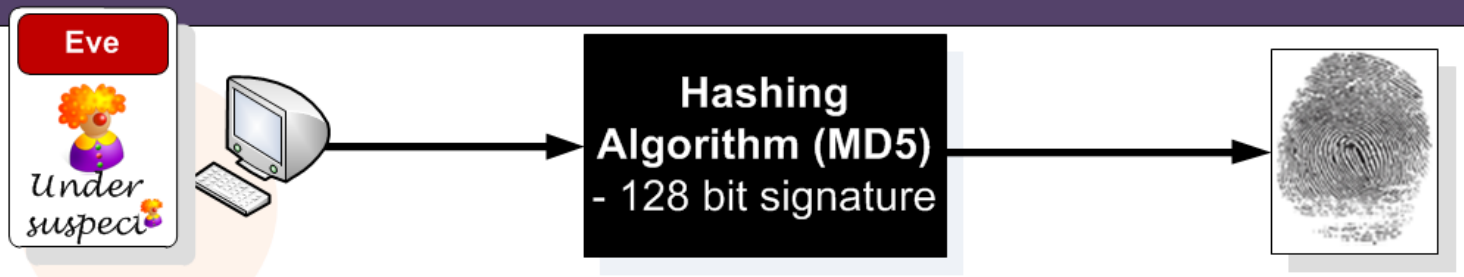
Cracking the key

Data Hiding



Obfuscation by Hashing

Author: Prof Bill Buchanan



hello	XUFAKrxLKna5cZ2REBfFkg
Hello	ixqZU8RhEpaoJ6v4xHgE1w
Hello. How are you?	CysDE5j+ZOUbCYZtTdsFiw
Napier	j4NXH5Mkrk4j13N1MFXHtg

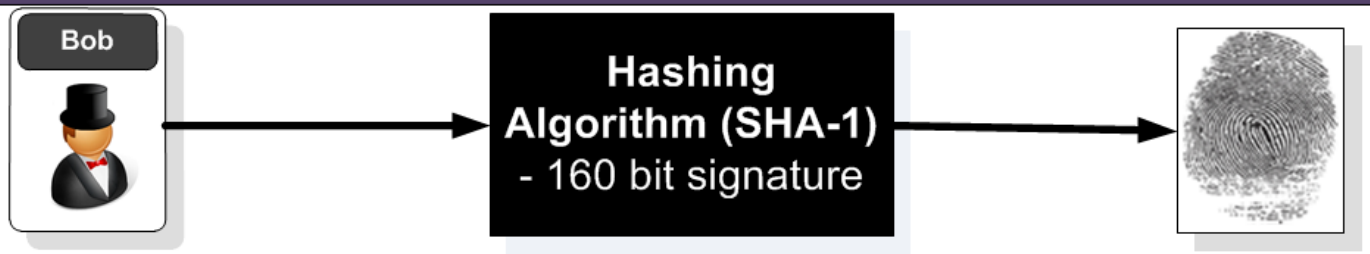
Base-64

hello	5D41402ABC4B2A76B9719D911017C592
Hello	8B1A9953C4611296A827ABF8C47804D7
Hello. How are you?	CC708153987BF9AD833BEBF90239BF0F
Napier	8F83571F9324AE4E23D773753055C7B6

Hex

Message Hash

Authentication



hello	qvTGHdzF6KLavt4PO0gs2a6pQ00=
Hello	9/+ei3uy4Jtwk1pdeF4MxdnQq/A=
Hello. How are you?	Puh2Am76bhjqE5lbTWtwsqbdFC8=
Napier	v4GxNaVod2b09GR2Tqw4yopOuro=

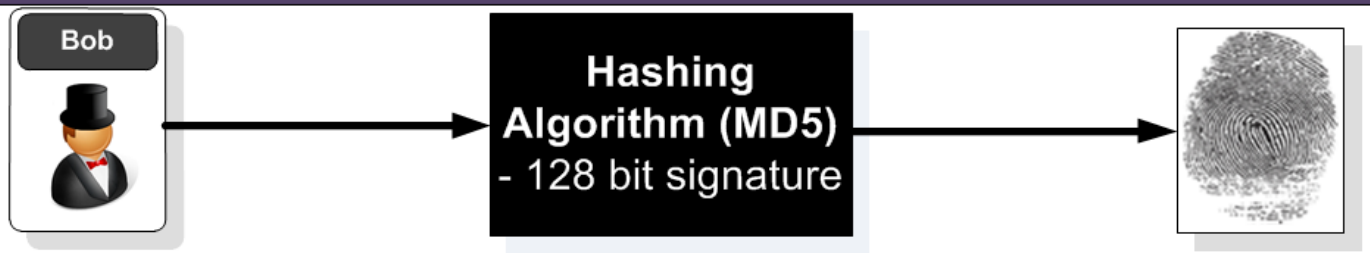
Base-64

hello	AAF4C61DDCC5E8A2DABEDE0F3B482CD9AEA9434D
Hello	F7FF9E8B7BB2E09B70935A5D785E0CC5D9D0ABF0
Hello. How are you?	3EE876026EFA6E18EA13995B4D6B70B2A6DD142F
Napier	BF81B135A5687766F4F464764EAC38CA8A4EBABA

Hex

Message Hash

Authentication



Security and mobility are two of the most important issues on the Internet, as they will allow users to secure their data transmissions, and also break their link with physical connections.

F94FBED3DAE05D223E6B963B9076C4EC

+U++09rgXSI+a5Y7kHbE7A==

Base-64

Security and mobility are two of the mast important issues on the Internet, as they will allow users to secure their data transmissions, and also break their link their physical connections.

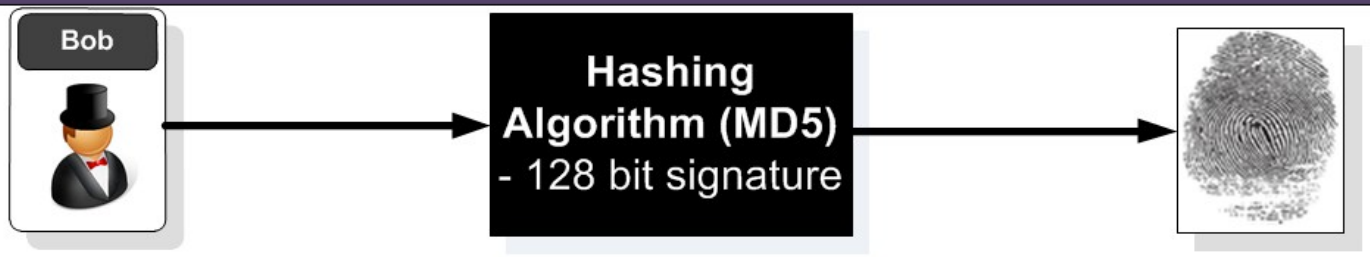
8A8BDC3FF80A01917D0432800201CFBF

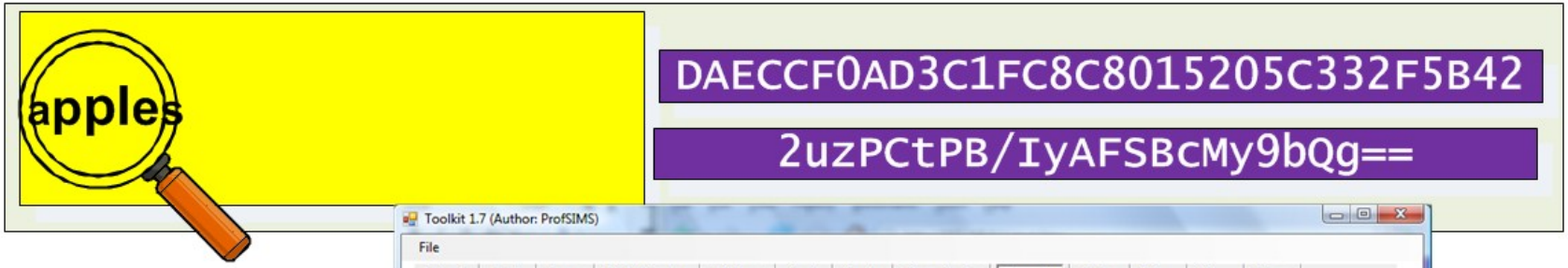
iovcP/gKAZF9BDKAAgHPvw==

Hex

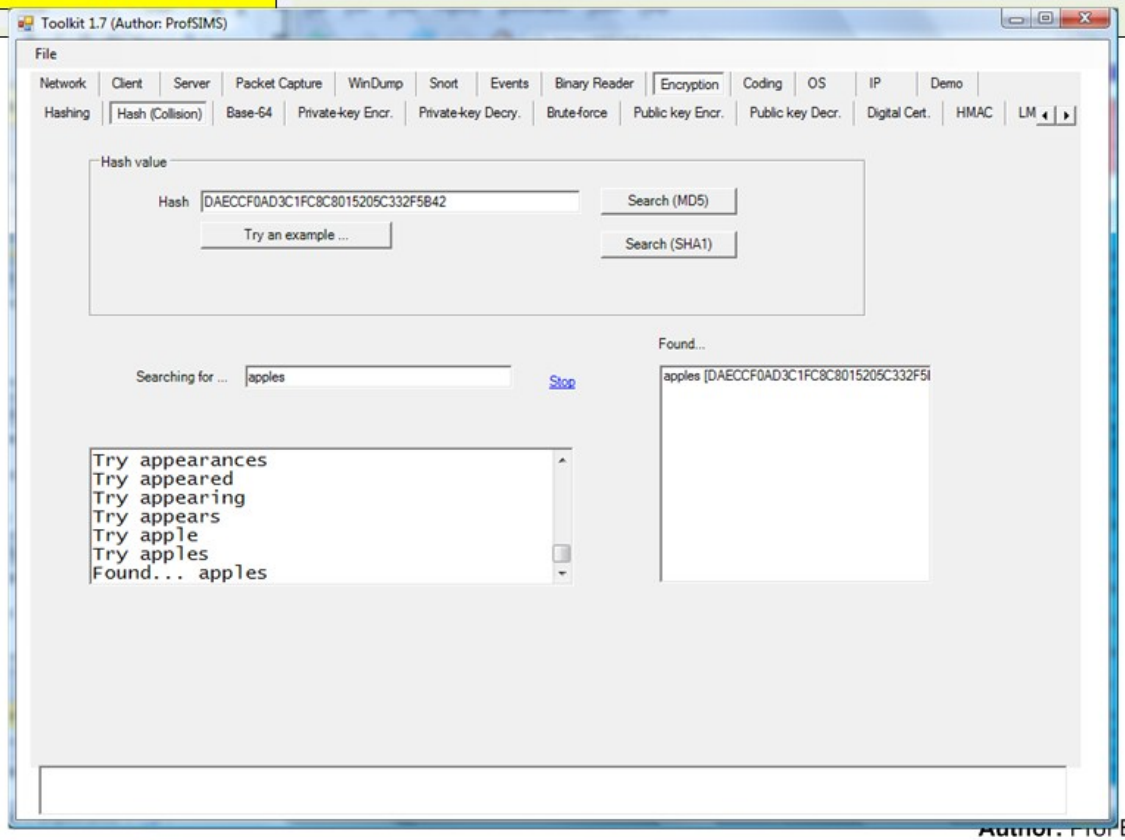
Message Hash

Authentication





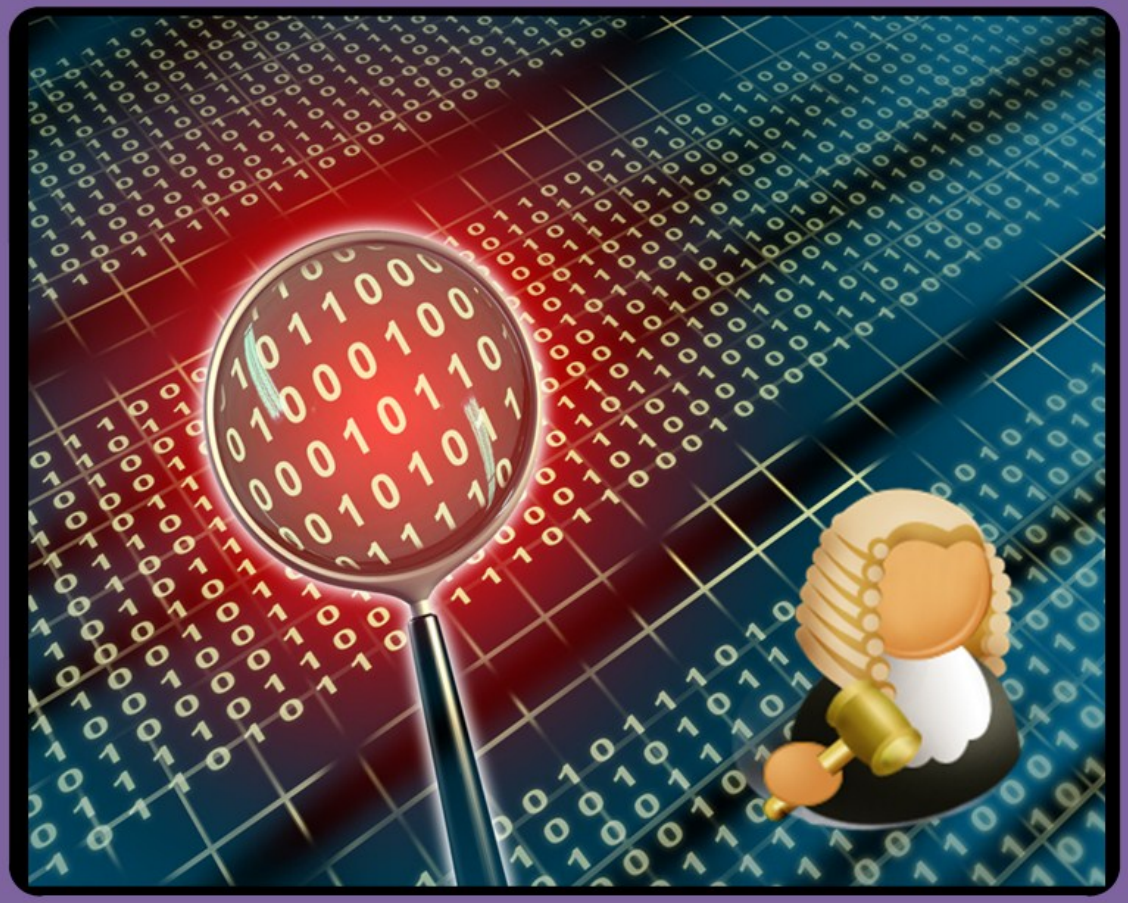
Base-64



Message Hash

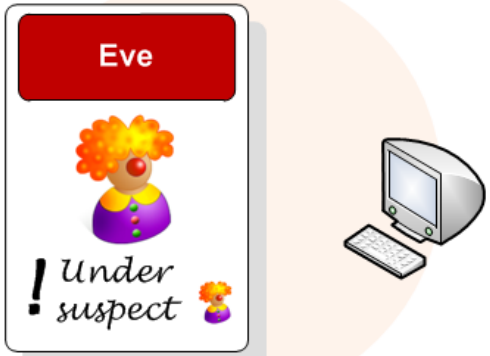
Authentication

Data Hiding



Obfuscation by Encoding

Author: Prof Bill Buchanan



Hex

Base-64

5e 20 e6 aa

XiDmqg

'A' 'B' 'C' 'D'

ASCII characters

01000001 01000010
01000011 01000100

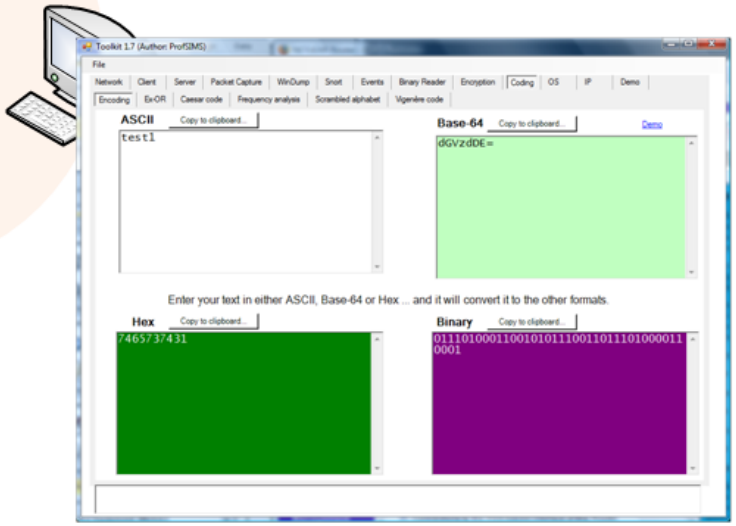
Encryption

01011110 00100000
11100110 10101010

Encoding

Data Hiding

Author: Prof Bill Buchanan



Decimal	Binary	Hex
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

Encryption

Data Hiding

0111 0100 0110 0101 0111 0011 0111 0100 0011 0001

Bit stream

7 4 6 5 7 3 7 4 3 1

Hex

Author: Prof Bill Buchanan

Hex conversion

Val	Enc	Val	Enc	Val	Enc	Val	Enc
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/

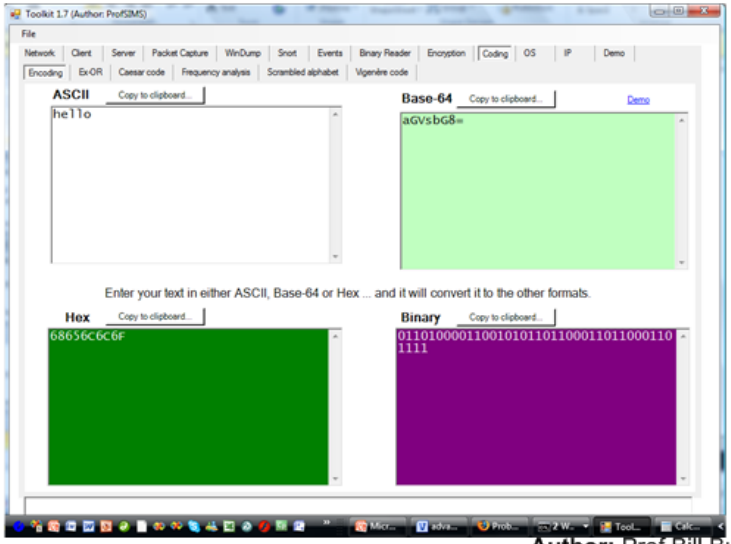
Encoding

```
011010 000110 010101 101100 011011
000110 1111
```

Bit stream

```
a G V s b G 8 =
```

Base-64

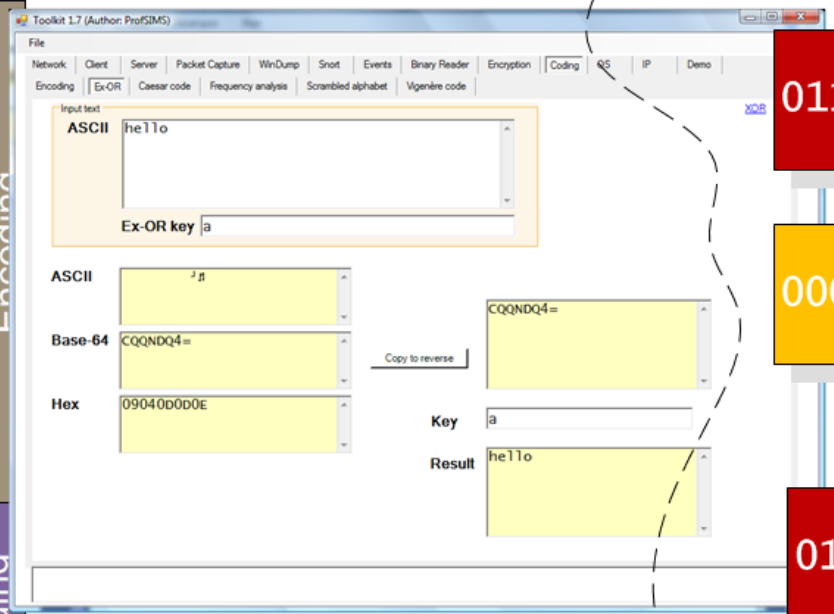


Author: Prof Bill Buchanan

hello

01101000 01100101 01101100 01101100

+



01100001 01100001 01100001 01100001

00001001 00000100 00001101 00001101

09 04 0D 0D 0E

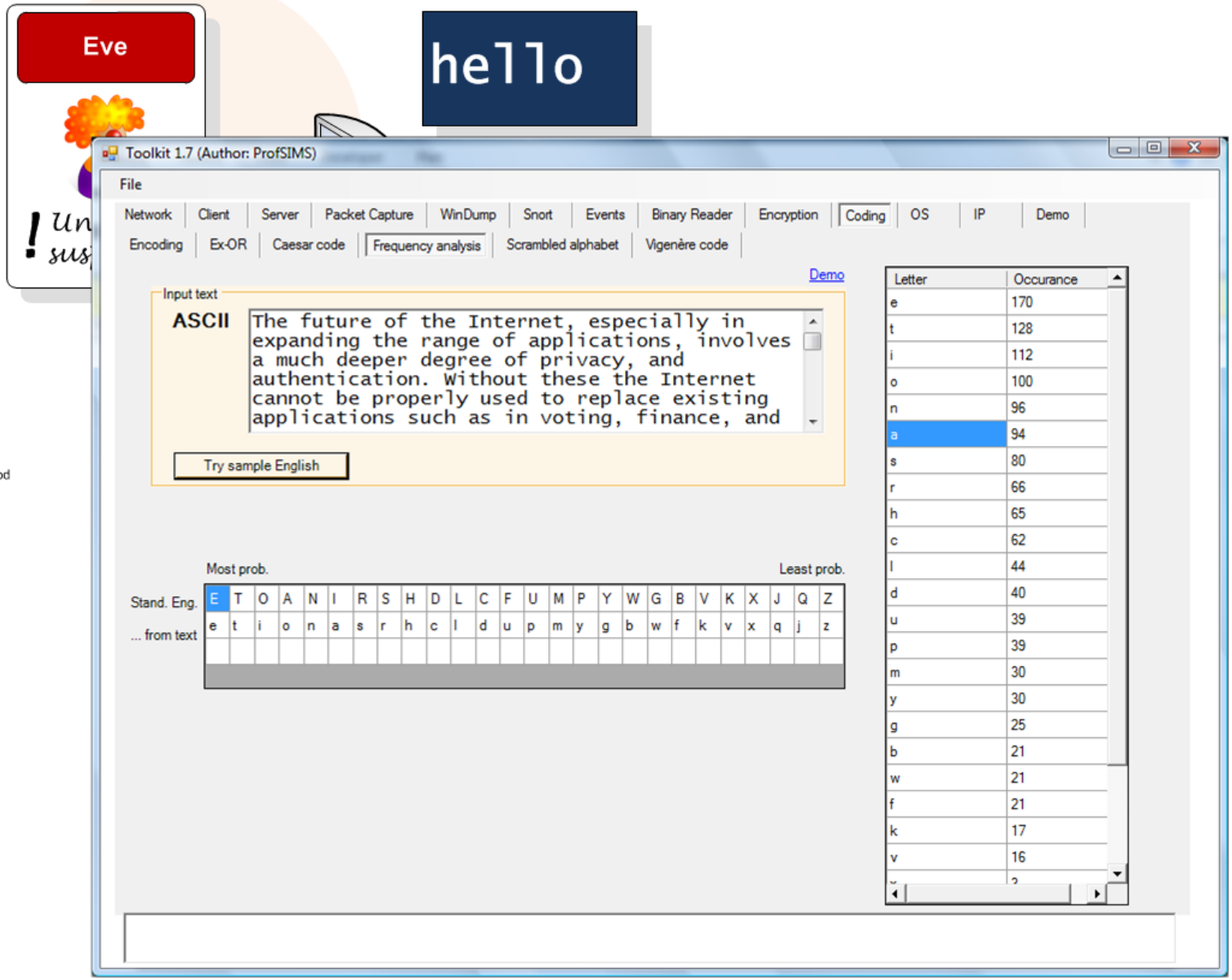
01100001 01100001 01100001 01100001

01101000 01100101 01101100 01101100

Encoding

Data Hiding

Ex-OR

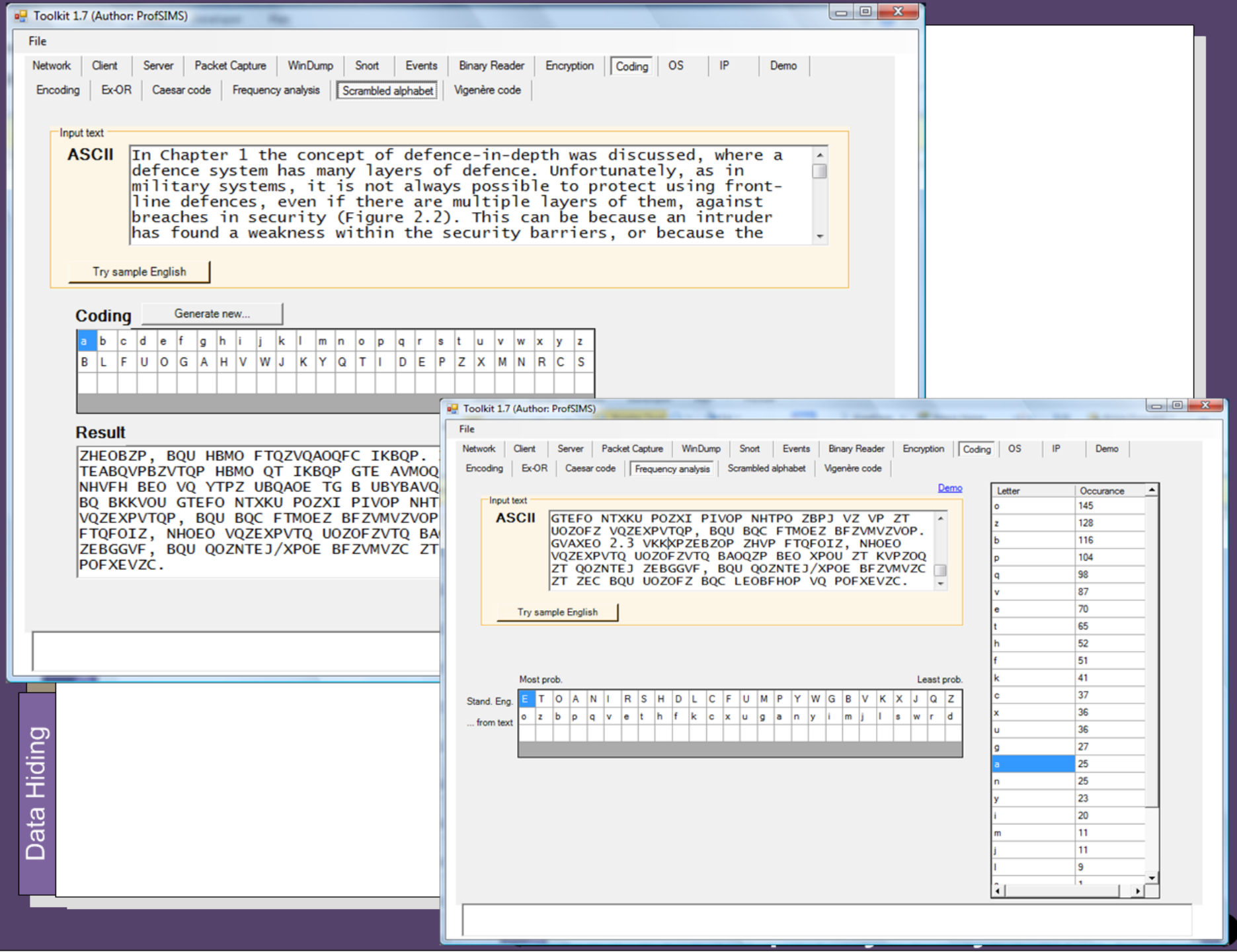


Encoding

Data Hiding

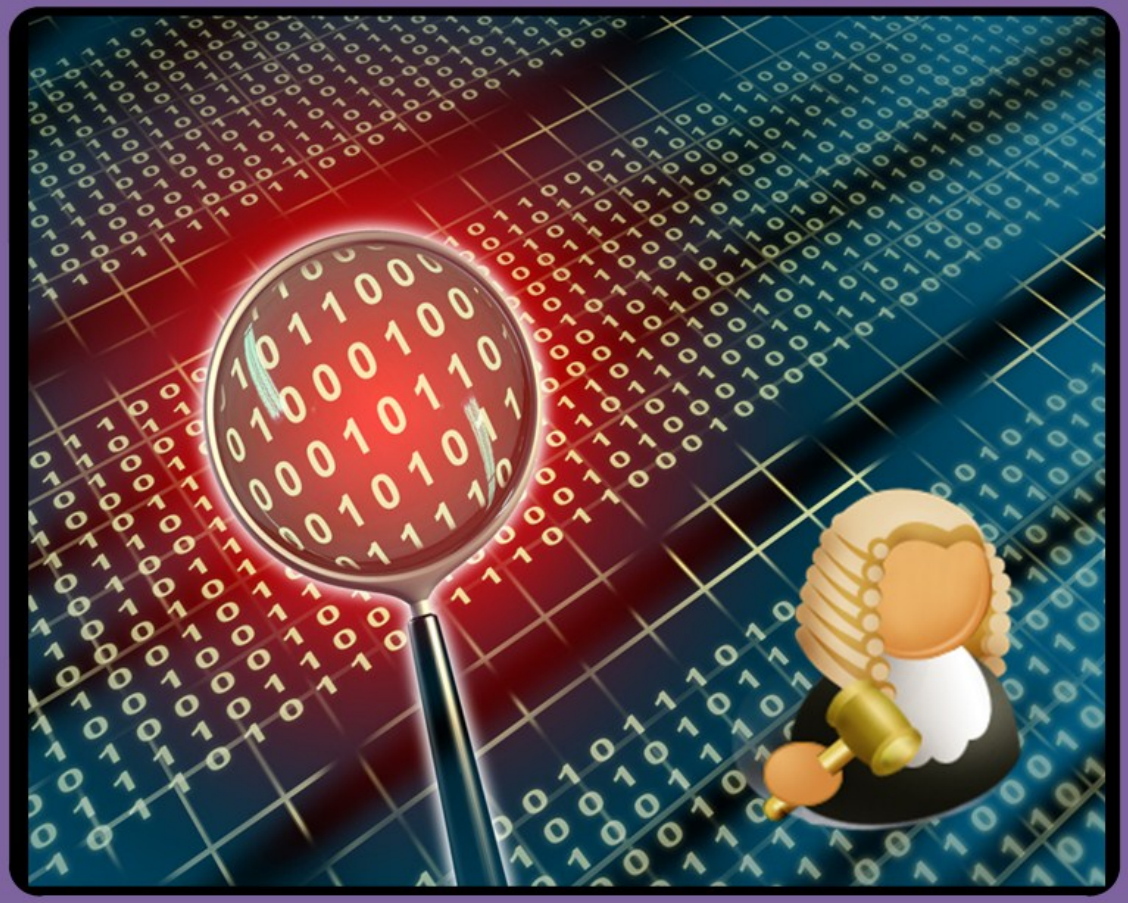
Author: Prof Bill Buchanan

Frequency Analysis


Toolkit 1.7 (Author: ProfSIMS)
File
Network
Client
Server
Packet Capture
WinDump
Snort
Events
Binary Reader
Encryption
Coding
OS
IP
Demo
Encoding
Ex-OR
Caesar code
Frequency analysis
Scrambled alphabet
Vigenère code
Input text
ASCII
In Chapter 1 the concept of defence-in-depth was discussed, where a defence system has many layers of defence. Unfortunately, as in military systems, it is not always possible to protect using front-line defences, even if there are multiple layers of them, against breaches in security (Figure 2.2). This can be because an intruder has found a weakness within the security barriers, or because the
Try sample English
Coding
Generate new...
a b c d e f g h i j k l m n o p q r s t u v w x y z
B L F U O G A H V W J K Y Q T I D E P Z X M N R C S
Result
ZHEOBZP, BQU HBMO FTQZVQAOQFC IKBQP.
TEABQVPBZVTQP HBMO QT IKBQP GTE AVMOQ
NHVFH BEO VQ YTPZ UBQAOE TG B UBYBAVQ
BQ BKKVOU GTEFO NTXKU POZXI PIVOP NHT
VQZEXPVTQP, BQU BQC FTMOEZ BFZVMVZVOP
FTQFOIZ, NHOEO VQZEXPVTQ UOZOFZVTQ BA
ZEBGGVF, BQU QOZNTEJ/XPOE BFZVMVZC ZT
POFXEVZC.
Toolkit 1.7 (Author: ProfSIMS)
File
Network
Client
Server
Packet Capture
WinDump
Snort
Events
Binary Reader
Encryption
Coding
OS
IP
Demo
Encoding
Ex-OR
Caesar code
Frequency analysis
Scrambled alphabet
Vigenère code
Demo
Input text
ASCII
GTEFO NTXKU POZXI PIVOP NHTPO ZBPJ VZ VP ZT UOZOFZ VQZEXPVTQP, BQU BQC FTMOEZ BFZVMVZVOP. GVAXEO 2.3 VKKXPZEBZOP ZHVP FTQFOIZ, NHOEO VQZEXPVTQ UOZOFZVTQ BAOQZP BEO XPOU ZT KVPZOQ ZT QOZNTEJ ZEBGGVF, BQU QOZNTEJ/XPOE BFZVMVZC ZT ZEC BQU UOZOFZ BQC LEOBFHOP VQ POFXEVZC.
Try sample English
Most prob.
Least prob.
Stand. Eng.
... from text
E T O A N I R S H D L C F U M P Y W G B V K X J Q Z
o z b p q v e t h f k c x u g a n y i m j l s w r d
Letter
Occurance
o 145
z 128
b 116
p 104
q 98
v 87
e 70
t 65
h 52
f 51
k 41
c 37
x 36
u 36
g 27
a 25
n 25
y 23
i 20
m 11
j 11
l 9

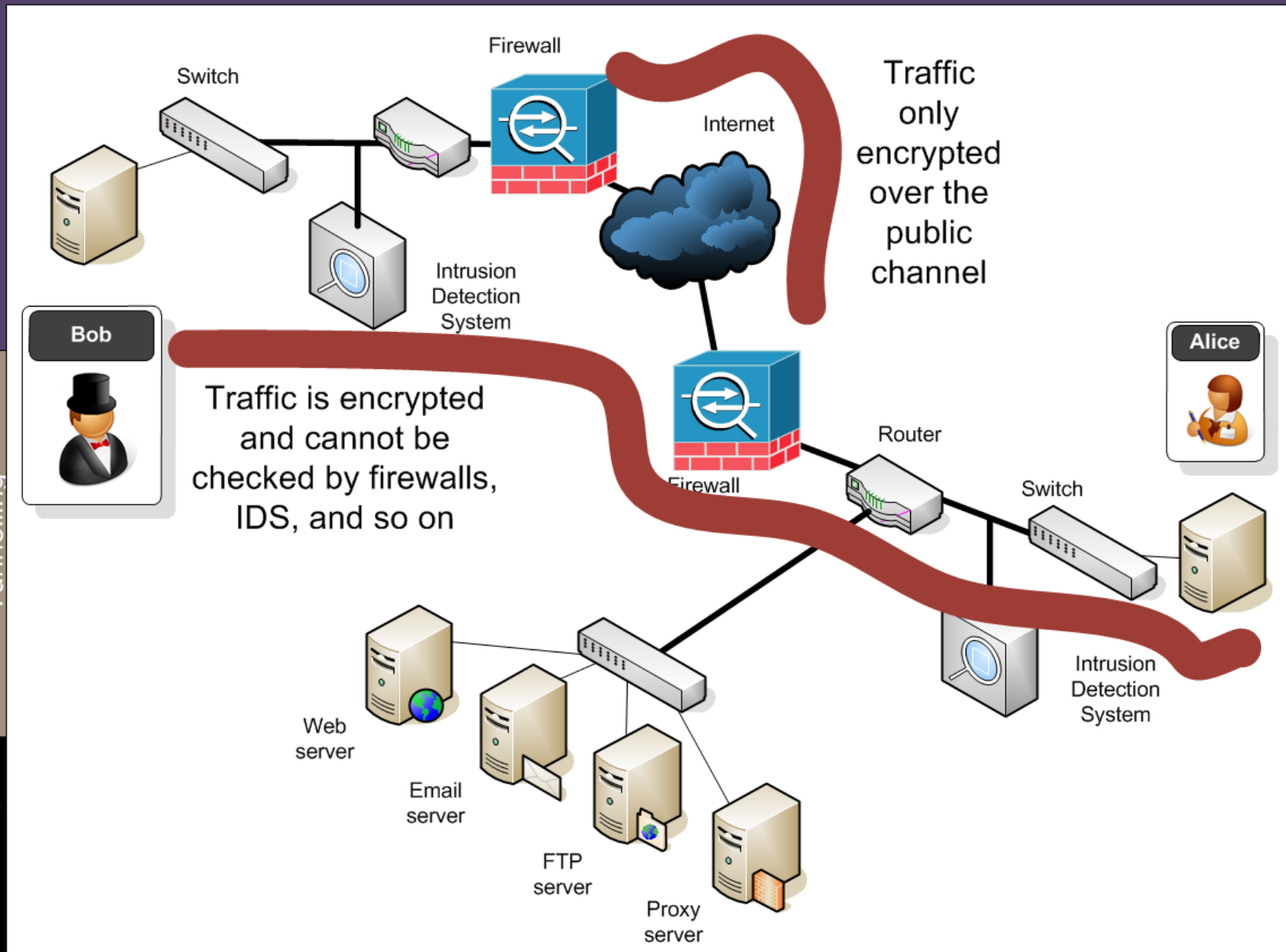
Data Hiding

Data Hiding

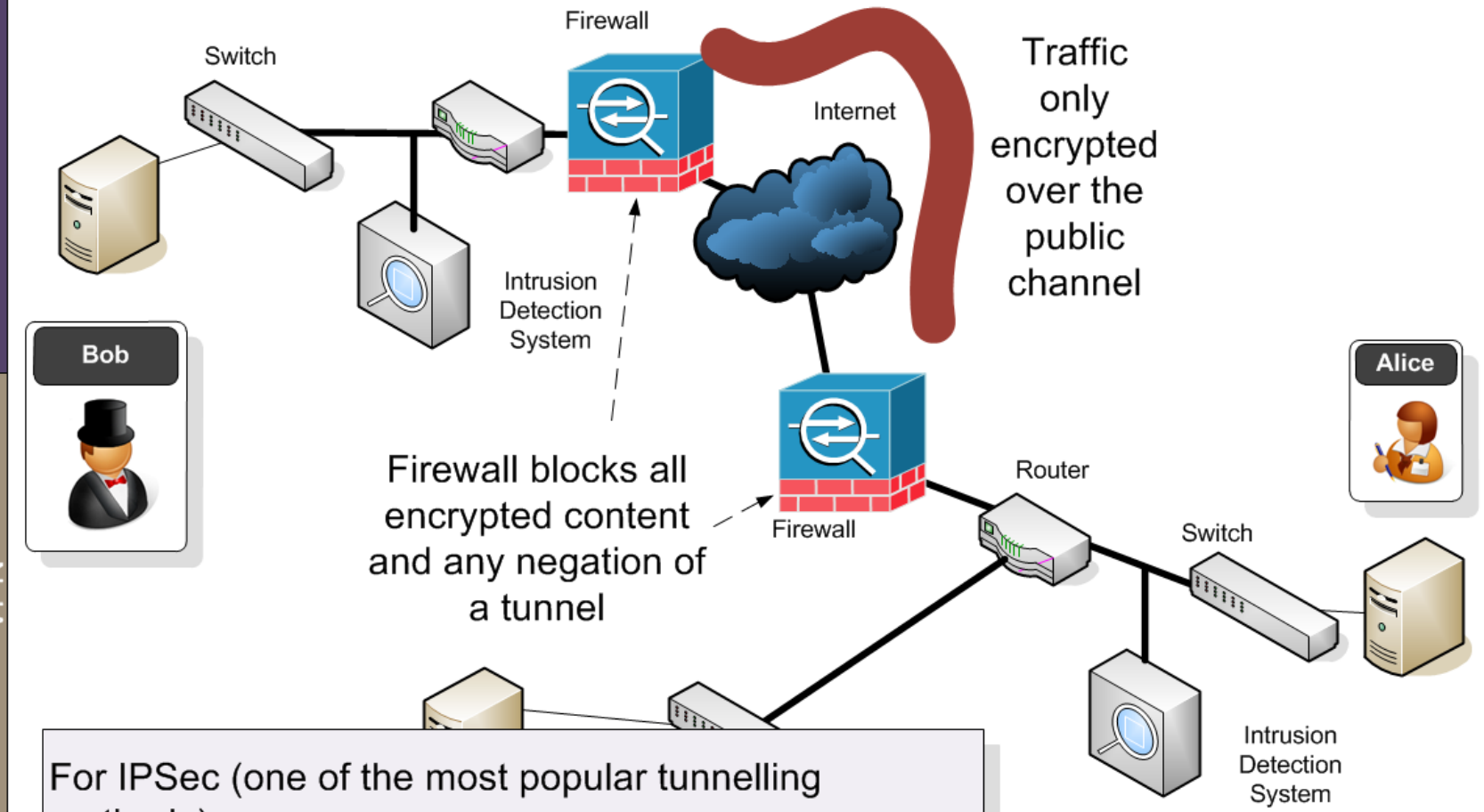


Obfuscation by Tunnelling

Author: Prof Bill Buchanan

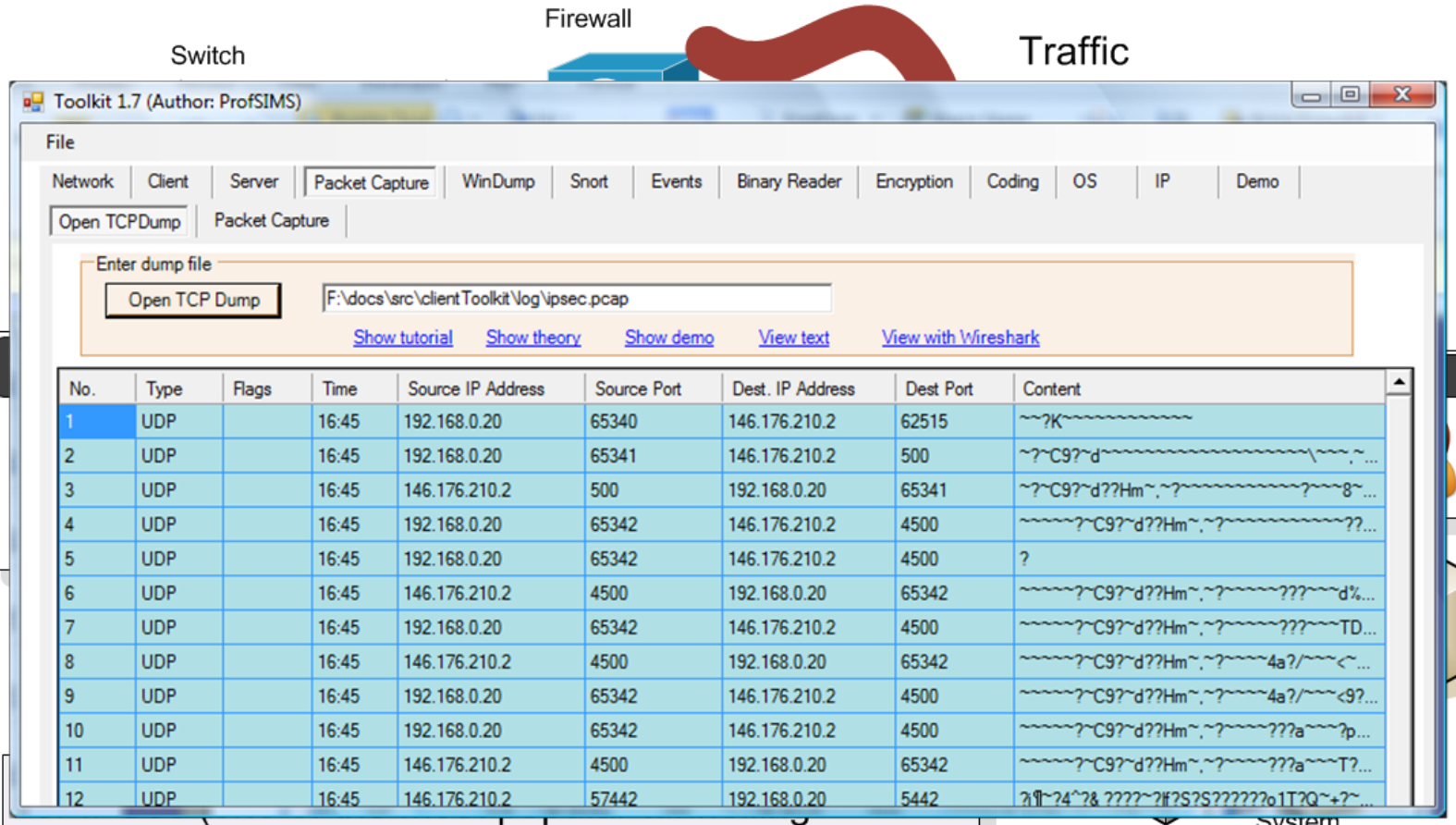


Tunnelling mode or transport mode



For IPSec (one of the most popular tunnelling methods):

- UDP Port 500 is the key exchange port. If it is blocked there can be no tunnel.
- TCP Port 50 for IPSec ESP (Encapsulated Security Protocol).
- TCP Port 51 for IPSec AH (Authentication Header)

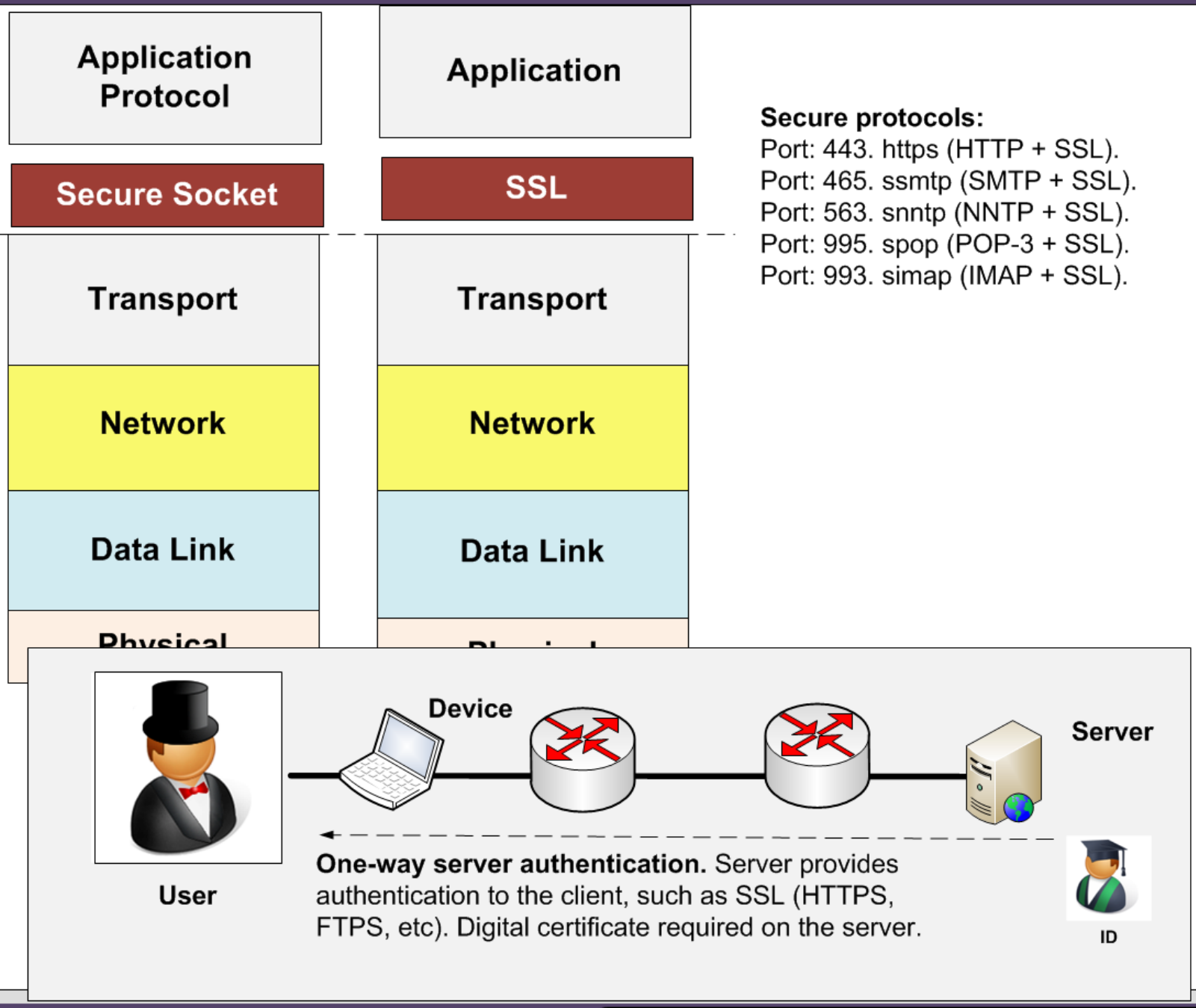


VPN

Data Hiding

methods):

- UDP Port 500 is the key exchange port. If it is blocked there can be no tunnel.
- TCP Port 50 for IPSec ESP (Encapsulated Security Protocol).
- TCP Port 51 for IPSec AH (Authentication Header)


Application Protocol
Application
Secure Socket
SSL
Transport
Transport
Network
Network
Data Link
Data Link
Physical
Tunnelling
Data hiding
Secure protocols:
Port: 443. https (HTTP + SSL).
Port: 465. ssmtp (SMTP + SSL).
Port: 563. snntp (NNTP + SSL).
Port: 995. spop (POP-3 + SSL).
Port: 993. simap (IMAP + SSL).
Device
Server
User
ID
One-way server authentication. Server provides authentication to the client, such as SSL (HTTPS, FTPS, etc). Digital certificate required on the server.

Application Protocol

Application

Secure protocols:
Port: 443. https (HTTP + SSL).

Tunnelling

Data hiding

Toolkit 1.7 (Author: ProfSIMS)

File

Network | Client | Server | Packet Capture | WinDump | Snort | Events | Binary Reader | Encryption | Coding | OS | IP | Demo

Open TCPDump | Packet Capture

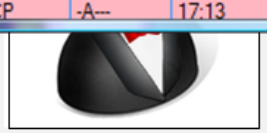
Enter dump file

Open TCP Dump

F:\docs\src\clientToolkit\log\ssl.pcap

Show tutorial | Show theory | Show demo | View text | View with Wireshark

No.	Type	Flags	Time	Source IP Address	Source Port	Dest. IP Address	Dest Port	Content
1	TCP	S----	17:13	192.168.0.20	2099	66.211.169.66	443	
2	TCP	SA---	17:13	66.211.169.66	443	192.168.0.20	2099	
3	TCP	-A---	17:13	192.168.0.20	2099	66.211.169.66	443	
4	TCP	-A-P-	17:13	192.168.0.20	2099	66.211.169.66	443	~~~~?~~~?~~~~~R?Bs?/?4?!~6~~?~elSS...
5	TCP	-A-P-	17:13	66.211.169.66	443	192.168.0.20	2099	~~~~?~~~F~~KJ~????a5???o??~|~~??~6?...
6	TCP	-A-P-	17:13	66.211.169.66	443	192.168.0.20	2099	???:@?Lg???]~=??;?a~I??~?chy?U~L~??]}...
7	TCP	-A---	17:13	192.168.0.20	2099	66.211.169.66	443	
8	TCP	-A-P-	17:13	66.211.169.66	443	192.168.0.20	2099	?]?[0Y0W0U~~image/gif0!00~~~+~~~~~¶??...
9	TCP	-A-P-	17:13	192.168.0.20	2099	66.211.169.66	443	~~~~?~~~?~?~?k???)??HF&'???4?tYY??C?...
10	TCP	-A---	17:13	66.211.169.66	443	192.168.0.20	2099	
11	TCP	-A-P-	17:13	66.211.169.66	443	192.168.0.20	2099	¶~~~~~~~~~(?T??????~?m~?8?P?g(??'?~...
12	TCP	-A---	17:13	192.168.0.20	2099	66.211.169.66	443	~~~~ ?????R???"??n?1?2A?~~¶uZ??~?#>...

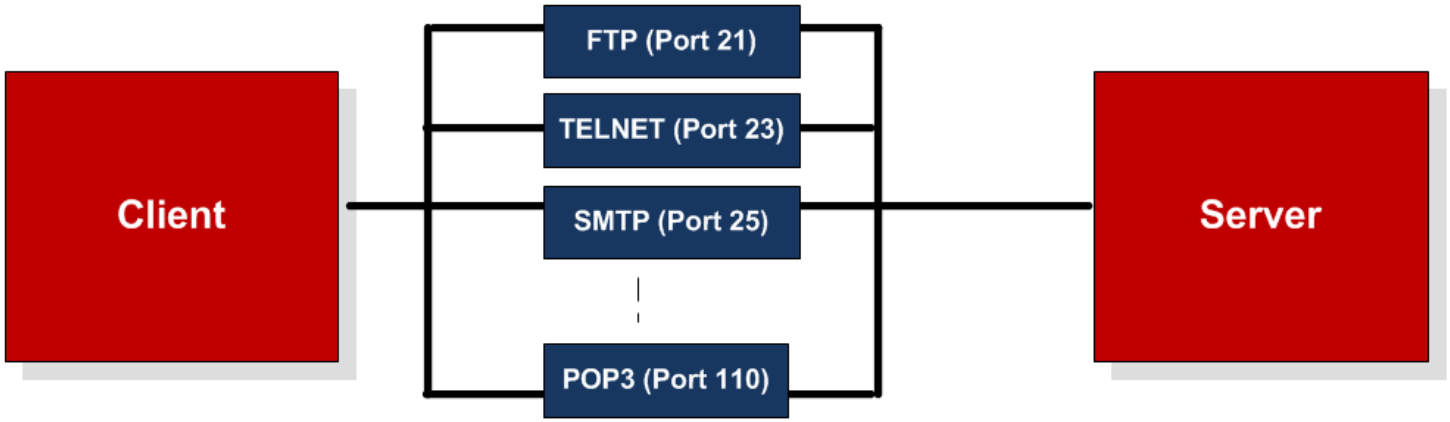


User

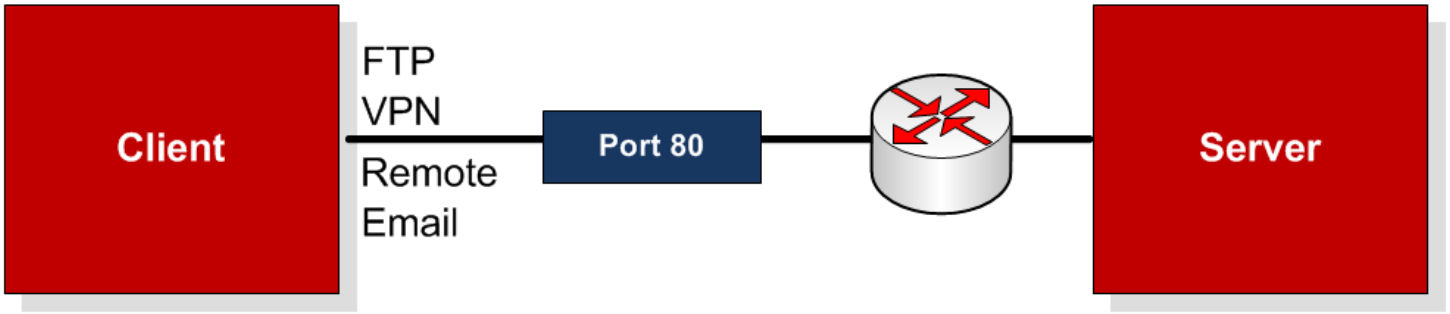
One-way server authentication. Server provides authentication to the client, such as SSL (HTTPS, FTPS, etc). Digital certificate required on the server.

ID

Secure Sockets (SSL)

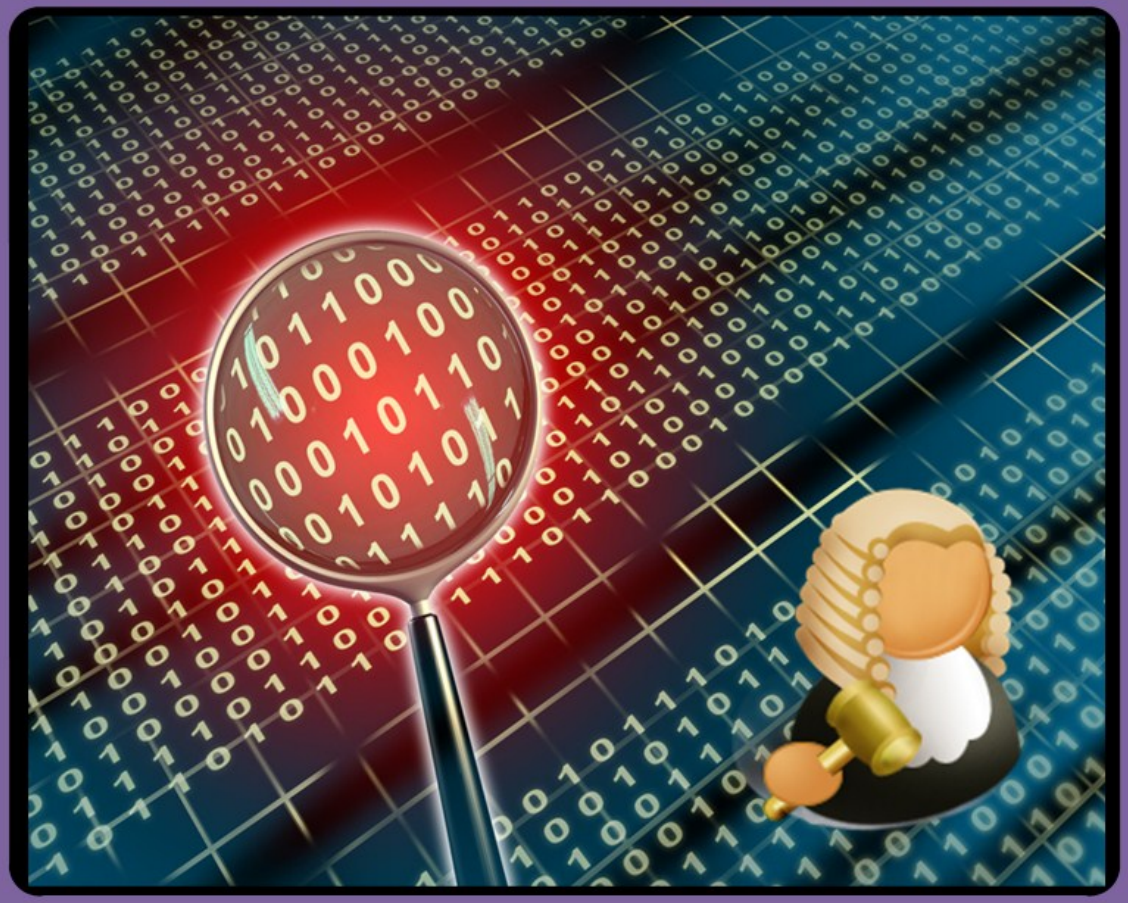


Applications use a wide range of TCP ports to communicate. Each of these ports could be blocked.



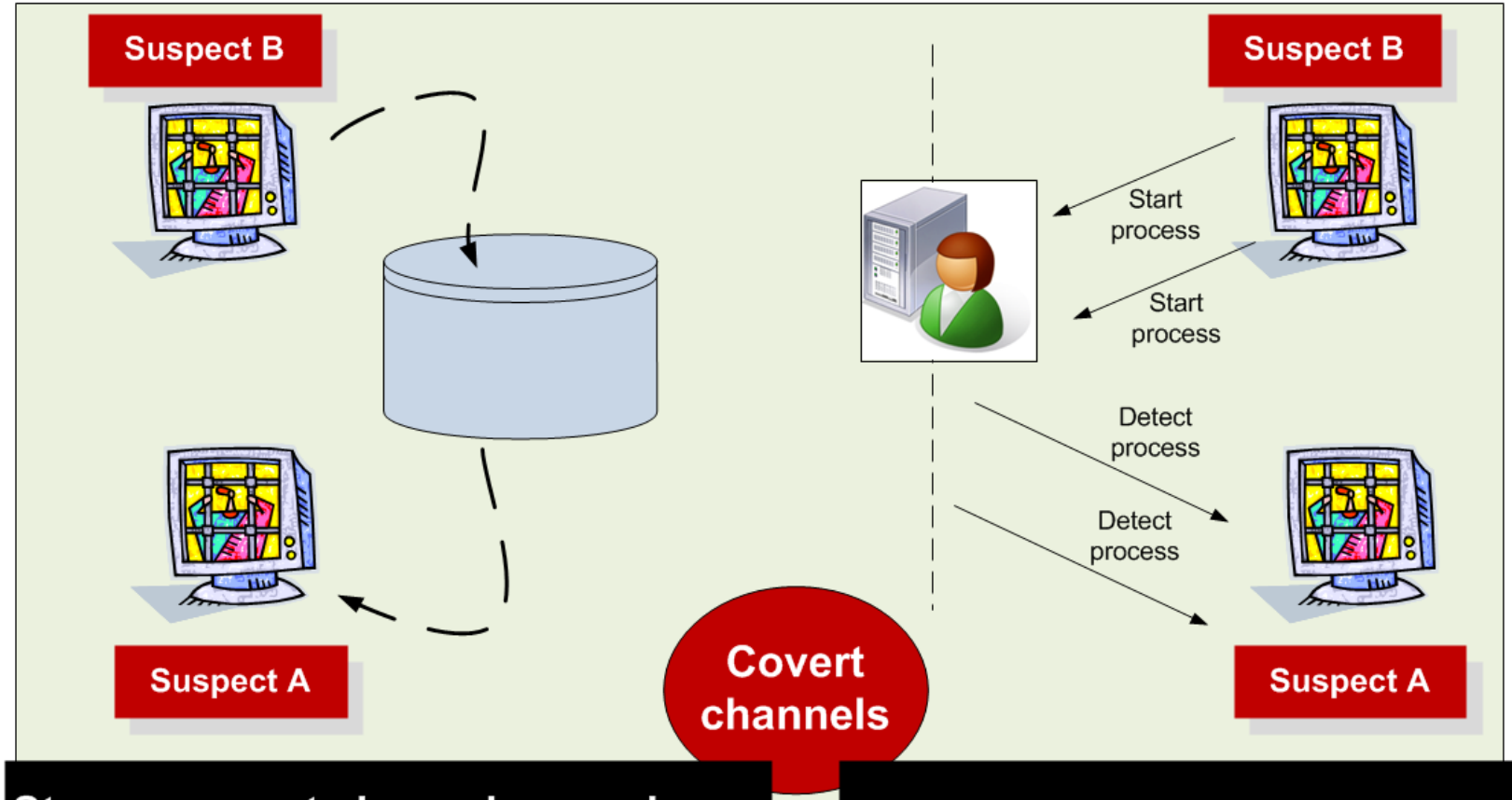
Applications communicate for a wide range of services through port 80 (Web port)… port 80 traffic is allowed through the firewall … but can cause security problems as the firewall cannot check the usage

Data Hiding



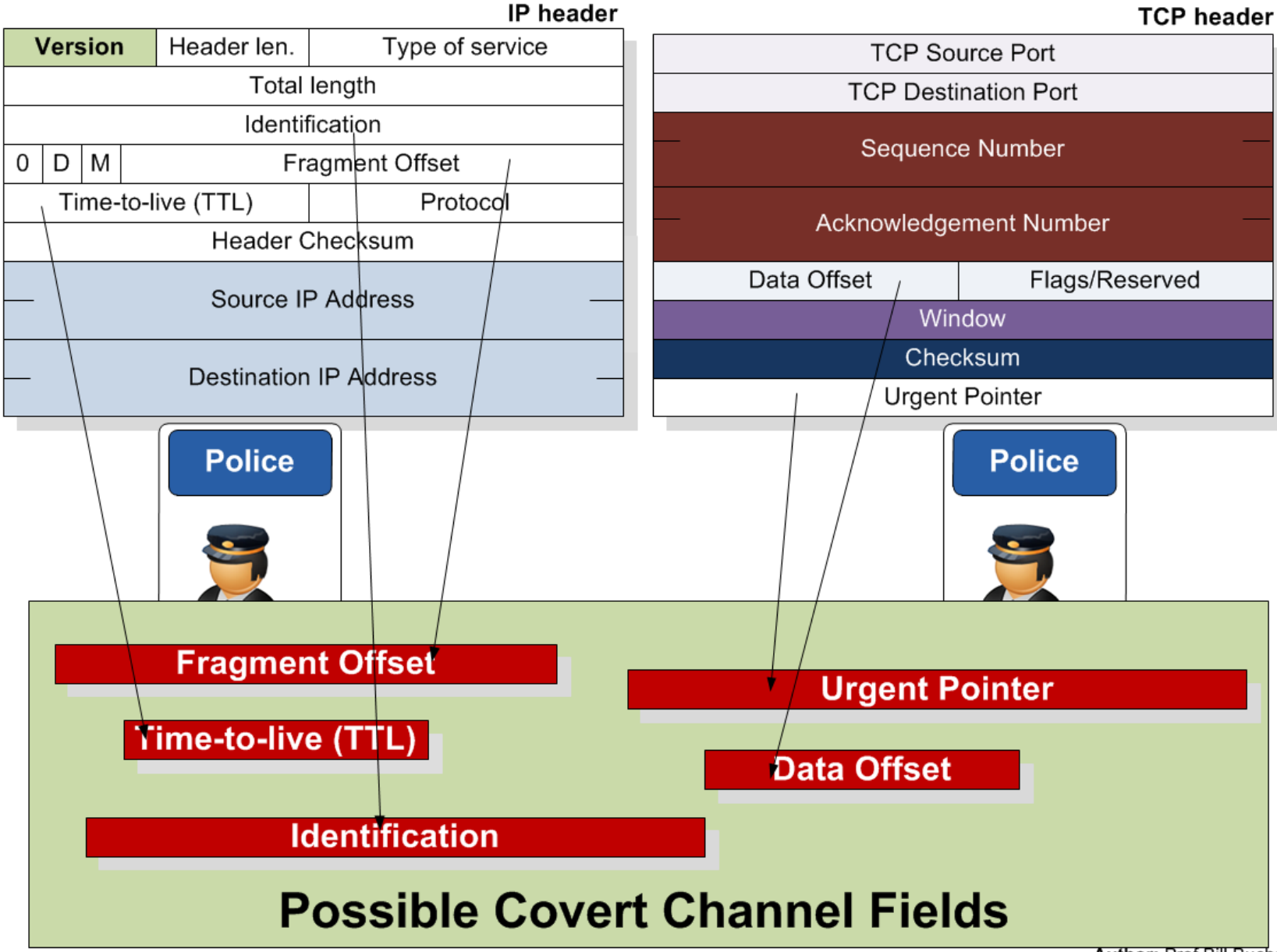
Covert Channels

Author: Prof Bill Buchanan

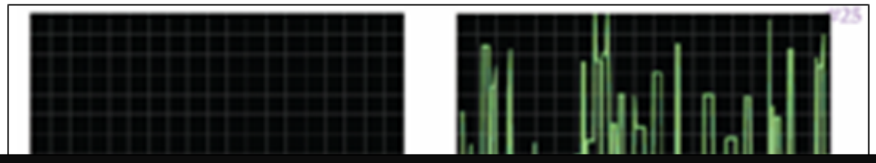


Storage covert channels are where one process uses direct (or indirect) data writing, whilst another process reads the data. It generally uses a finite system resource that is shared between entities with different privileges.

Covert timing channels use the modulation of certain resources, such as the CPU timing, in order to exchange information between processes.



Author: Prof Bill Buchanan



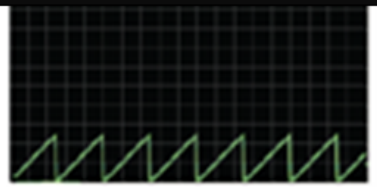
Version	Header len.	Type of service
Total length		
Identification		

```
No.     Time        Source                Destination           Protocol Info
      3 0.001525    192.168.75.132        192.168.75.1          TCP      afrog >
http [SYN] Seq=0 Win=64240 Len=0 MSS=1460
    Identification: 0x008c (140)

No.     Time        Source                Destination           Protocol Info
      4 3.019628    192.168.75.132        192.168.75.1          TCP      afrog >
http [SYN] Seq=0 Win=64240 Len=0 MSS=1460
    Identification: 0x008e (142)

No.     Time        Source                Destination           Protocol Info
      7 8.968288    192.168.75.132        192.168.75.1          TCP      afrog >
http [SYN] Seq=0 Win=64240 Len=0 MSS=1460
    Identification: 0x008f (143)
…. Packets missed out …

No.     Time        Source                Destination           Protocol Info
    129 30.598774   192.168.75.132        84.53.138.18          TCP      dcutility >
http [ACK] Seq=4751 Ack=28096 Win=63188 Len=0
    Identification: 0x00d1 (209)
```

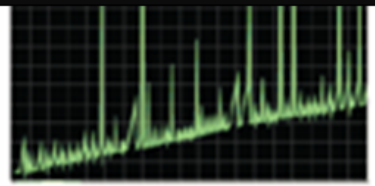
Data hiding

identifying fragments of an original IP

Source: David Llamas



Real Covert channel based on IPv4ID



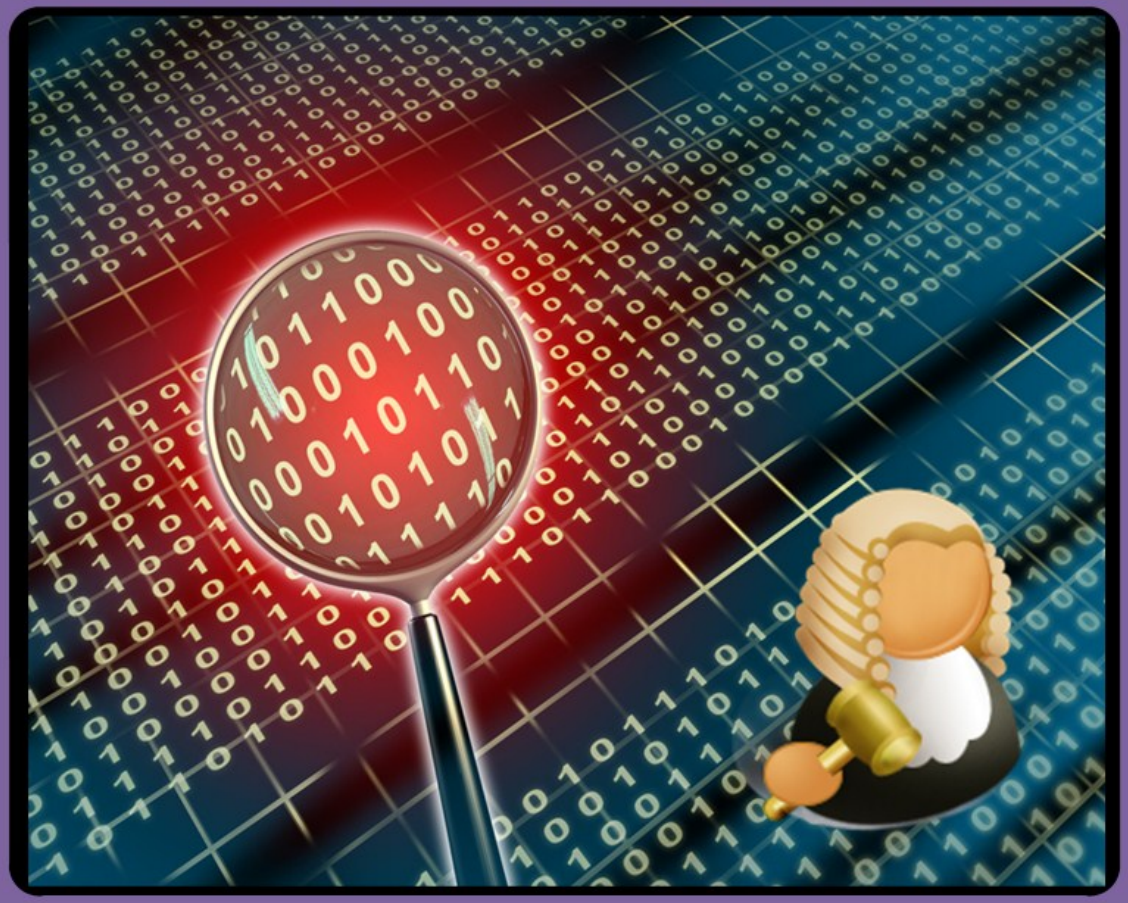
Unknown

IPv4 ID Field

```
No.     Time        Source                Destination           Protocol Info
     49 23.974294   192.168.75.138        192.168.75.1          TCP      54064 > icslap [ACK]
Seq=134 Ack=225 Win=6912 Len=0 TSV=18845 TSER=2182534

    Identification: 0x1643 (5699)

No.     Time        Source                Destination           Protocol Info
     50 23.974900   192.168.75.138        192.168.75.1          TCP      54064 > icslap [ACK]
Seq=134 Ack=1673 Win=9824 Len=0 TSV=18845 TSER=2182534
    Identification: 0x1644 (5700)

No.     Time        Source                Destination           Protocol Info
     51 23.975155   192.168.75.138        192.168.75.1          TCP      54064 > icslap [ACK]
Seq=134 Ack=1807 Win=12704 Len=0 TSV=18845 TSER=2182534
    Identification: 0x1645 (5701)

No.     Time        Source                Destination           Protocol Info
     53 23.977703   192.168.75.138        192.168.75.1          TCP      54064 > icslap [FIN,
ACK] Seq=134 Ack=1808 Win=12704 Len=0 TSV=18846 TSER=2182534
    Identification: 0x1646 (5702)

No.     Time        Source                Destination           Protocol Info
     55 23.979951   192.168.75.138        192.168.75.1          TCP      54065 > icslap [SYN]
Seq=0 Win=5840 Len=0 MSS=1460 TSV=18847 TSER=0 WS=5
    Identification: 0x0050 (80)

No.     Time        Source                Destination           Protocol Info
     57 23.981798   192.168.75.138        192.168.75.1          TCP      54065 > icslap [ACK]
Seq=1 Ack=1 Win=5856 Len=0 TSV=18847 TSER=2182535
    Identification: 0x0051 (81)
```

IPv4 ID Field

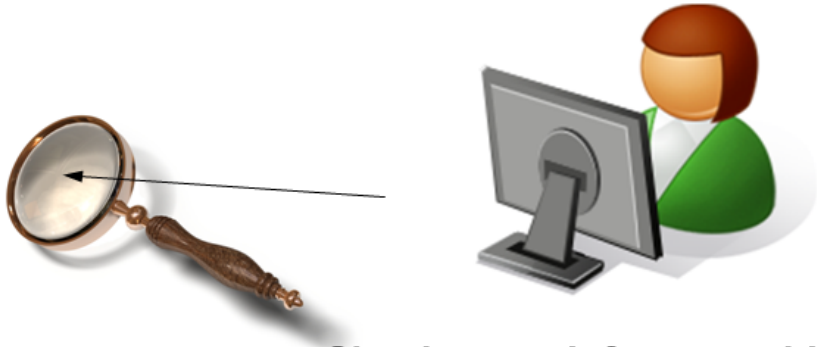
Data Hiding



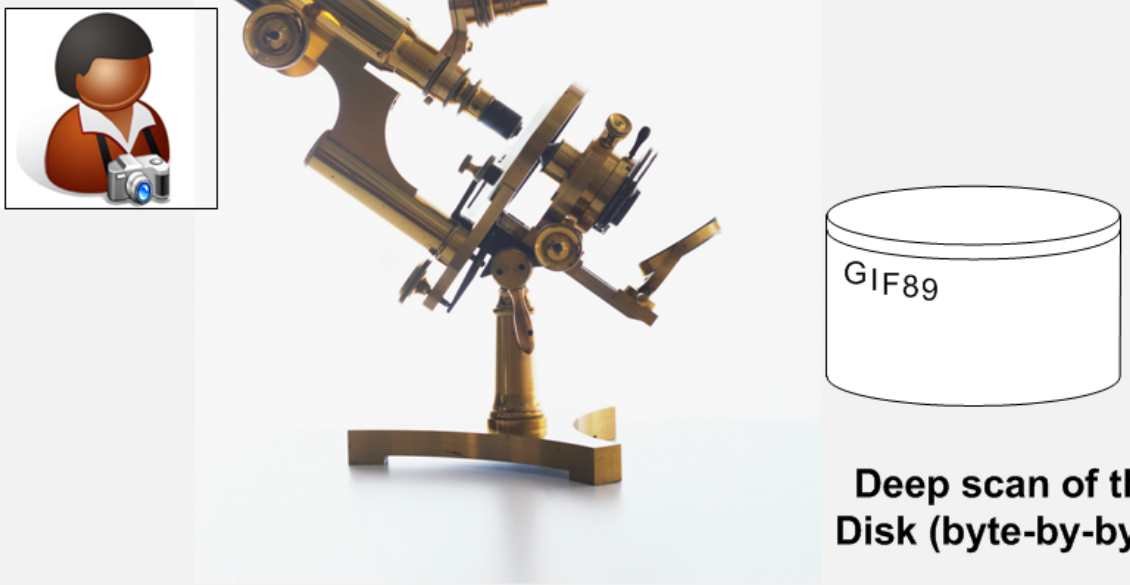
File Signatures

Author: Prof Bill Buchanan

File Allocation Table:
1.txt
2.doc
Test.doc
-Delete.gif [deleted]



Simple search for a graphic file will not find the deleted file



Deep scan of the Disk (byte-by-byte)

Author: Prof Bill Buchanan

Mypic.gif

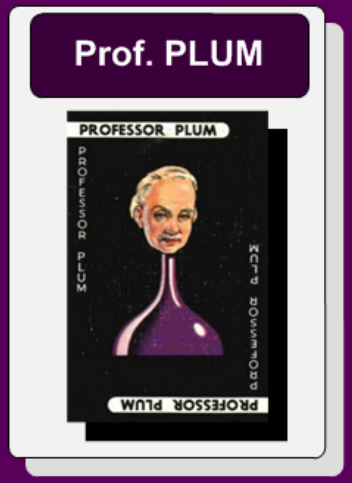
Mypic.dll

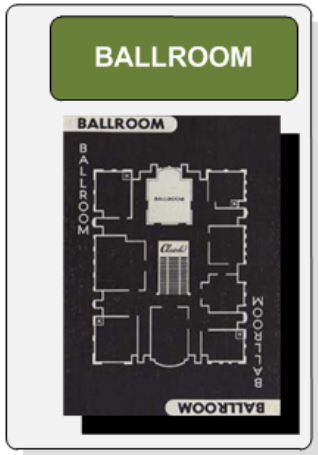
Change name from:

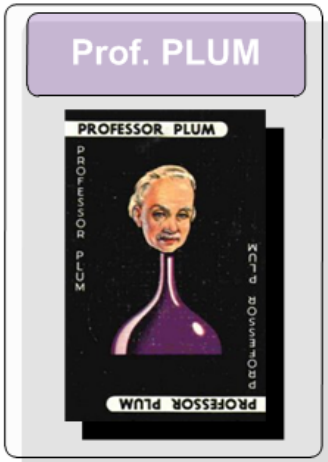
Mypic.gif

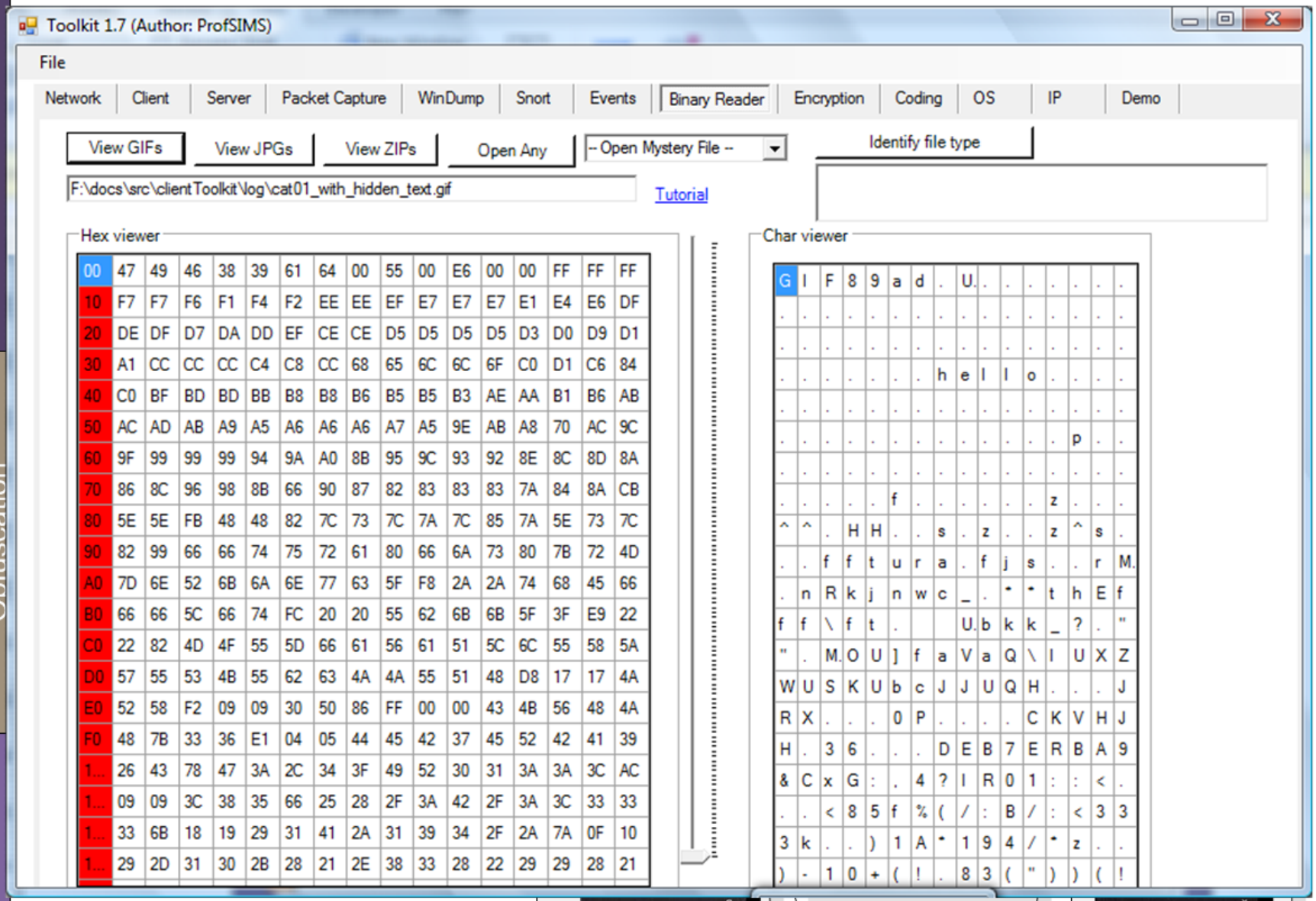
To

Mypic.dll





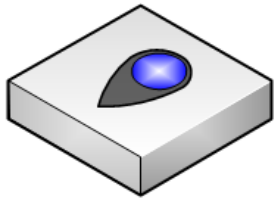




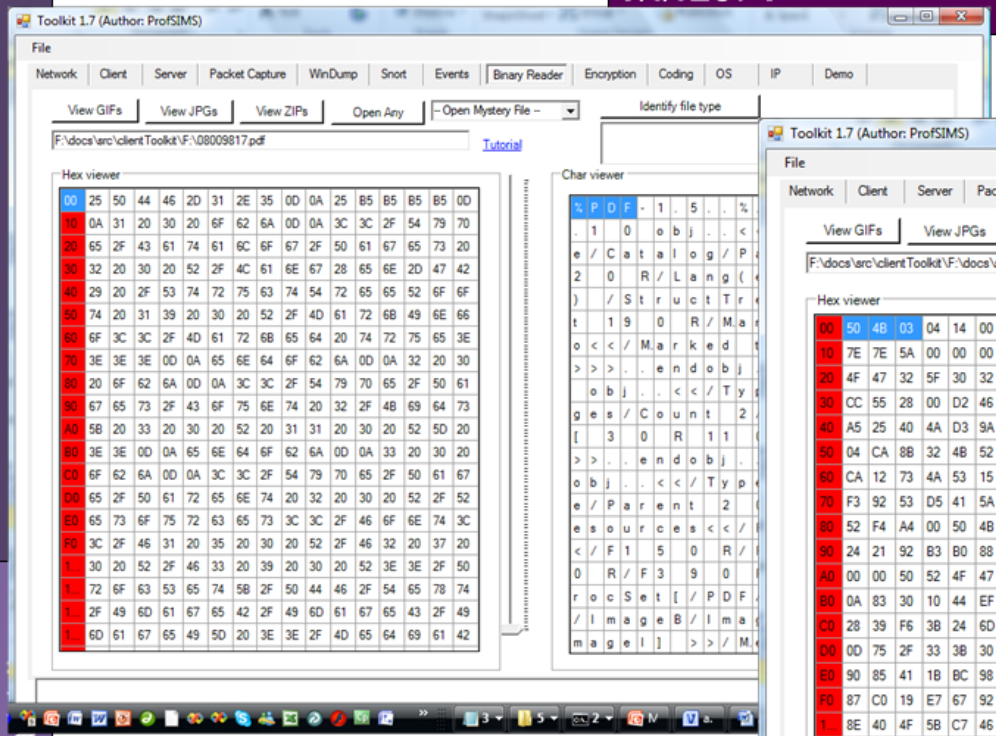
Obfuscation

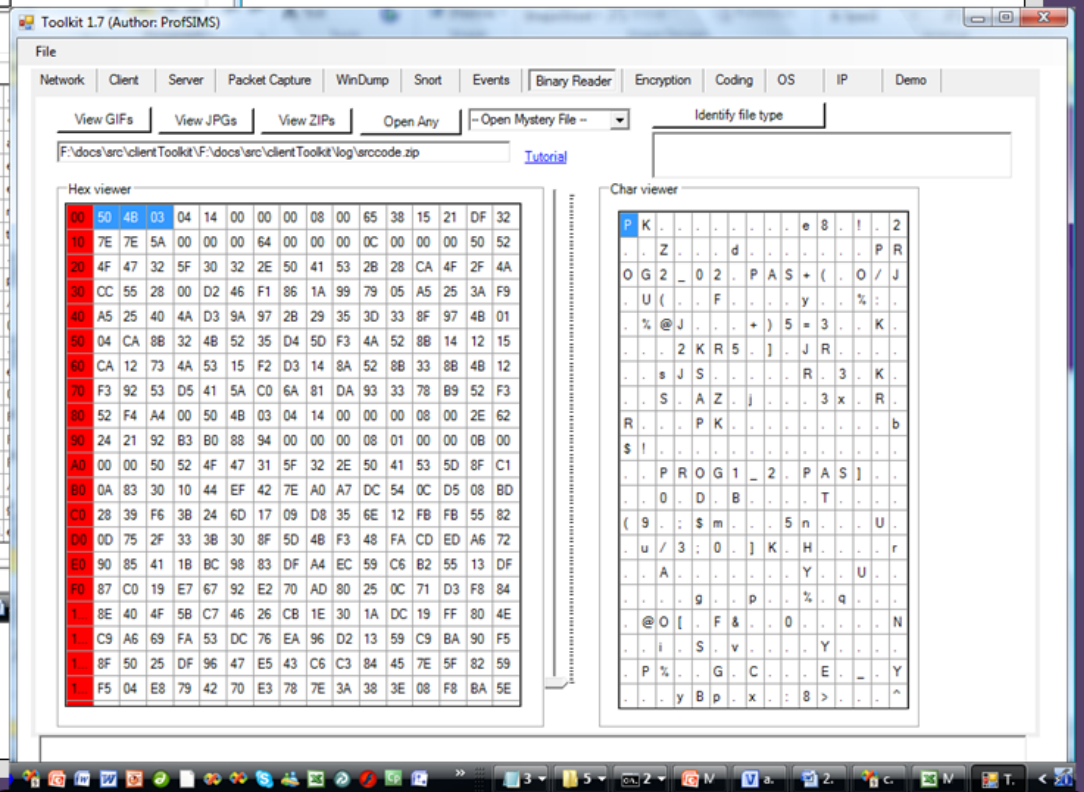
Forensic

File name changing



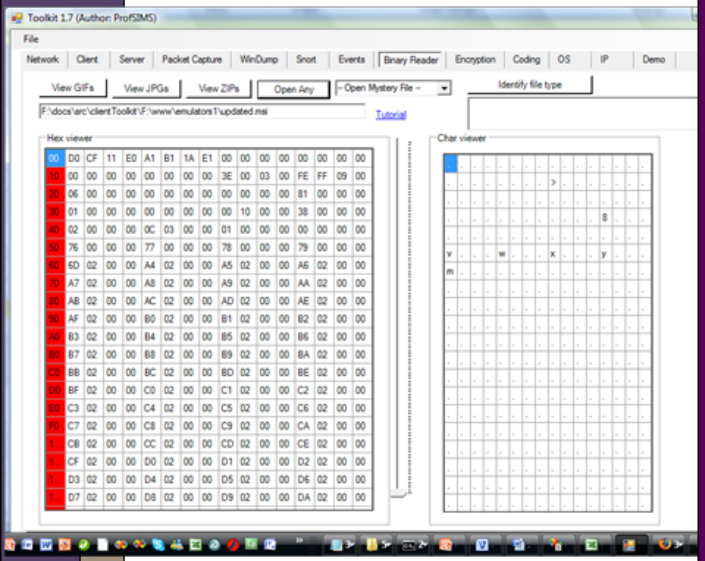
Sig	File ext	File type
0x474946	*.gif	GIF files
GIF89a	*.gif	GIF files
0xFFD8FF	*.jpg	JPEG files
JFIF	*.jpg	JPEG files
0x504B03	*.zip	ZIP files
0x25504446	*.pdf	PDF files
%PDF	*.pdf	PDF files
0x0A2525454F460A	*.pdf	PDF file
.%%EOF.	*.pdf	PDF file



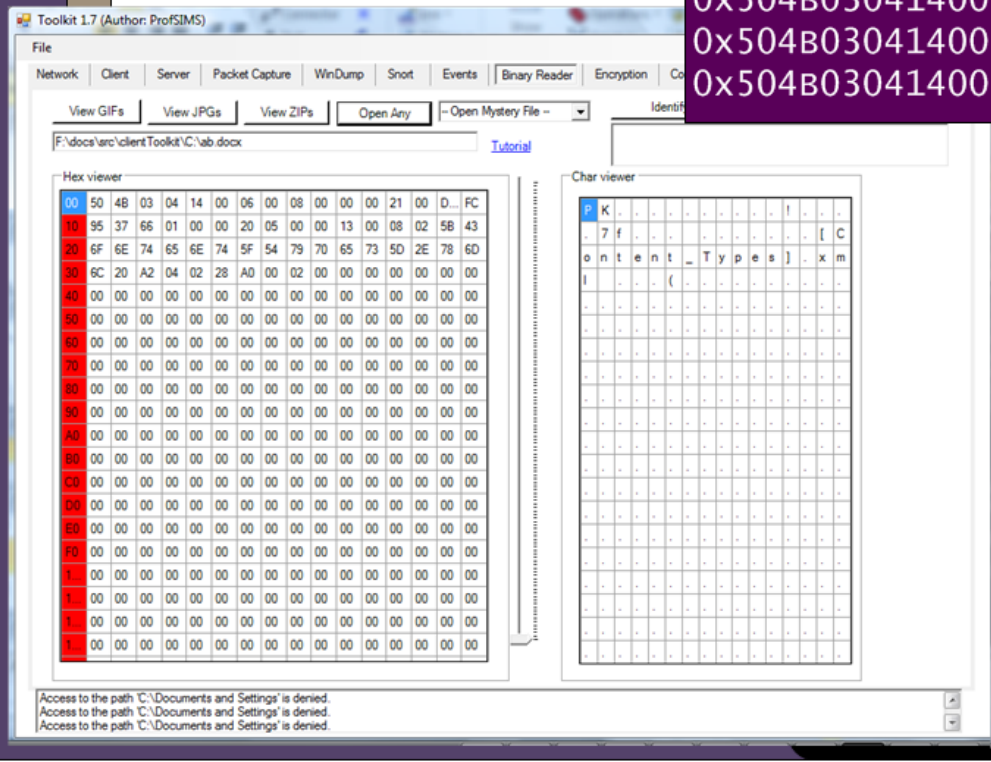


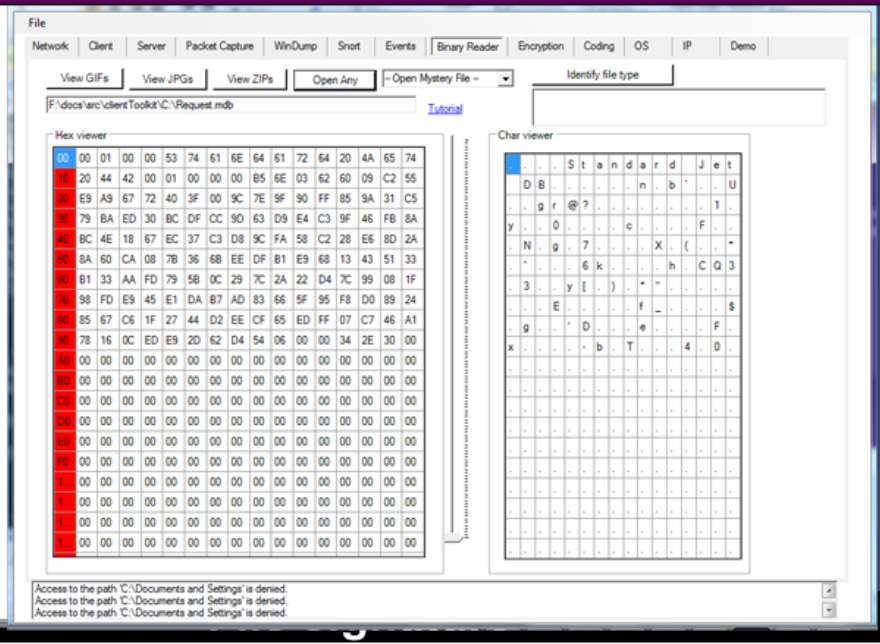
Data

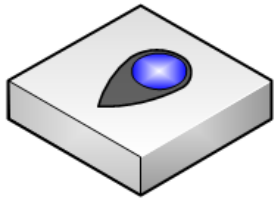
File signature



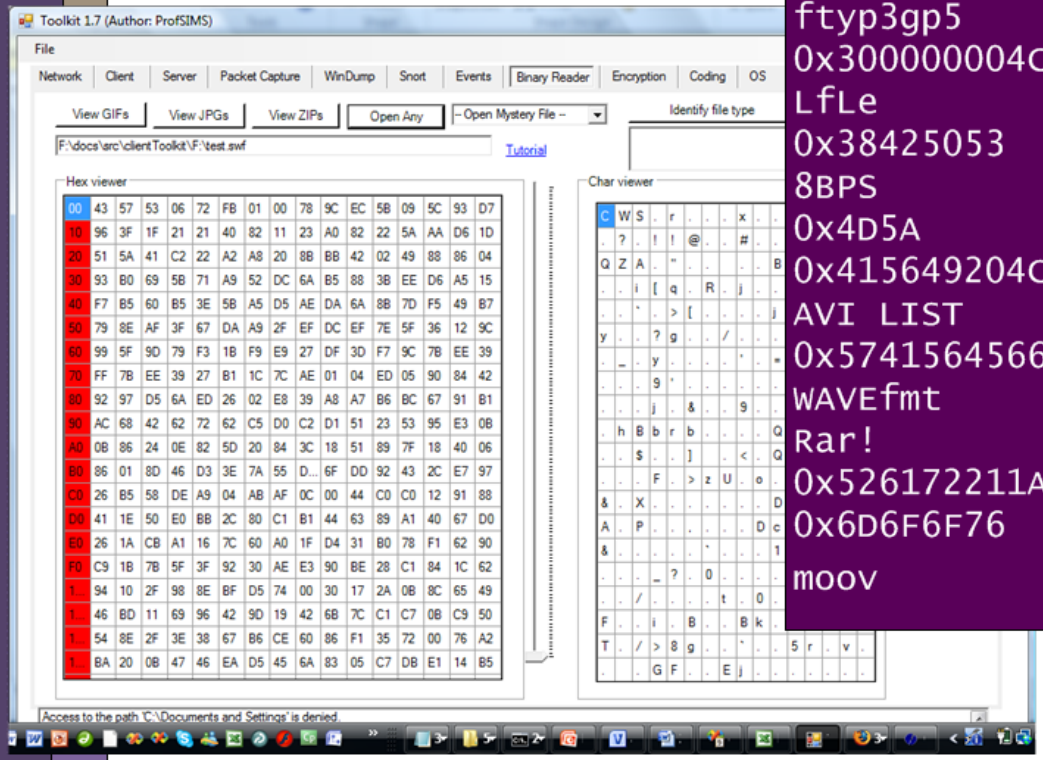
Sig	File ext	File type
0x006E1EF0	*.ppt	PPT
0xA0461DF0	*.ppt	PPT
0xECA5C100	*.doc	Doc file
0x00010000 5374616E 64617264 204A6574 20444200	*.mdb	Microsoft database
Standard Jet DB	*.mdb	Microsoft database
0x2142444E	*.pst	PST file
!BDN	*.pst	PST file
0x0908100000060500	*.xls	XLS file
0xD0CF11E0A1B11AE1	*.msi	MSI file
0xD0CF11E0A1B11AE1	*.doc	DOC
0xD0CF11E0A1B11AE1	*.xls	Excel
0xD0CF11E0A1B11AE1	*.vsd	Visio
0xD0CF11E0A1B11AE1	*.ppt	PPT
0x504B0304 14000600	*.docx	Microsoft DOCX file
0x504B0304 14000600	*.pptx	Microsoft PPTX file
0x504B0304 14000600	*.xlsx	Microsoft XLSX file







Sig	File ext	File type
0x465753	*.swf	SWF file
FWS	*.swf	SWF file
0x494433	*.mp3	MP3 file
ID3	*.mp3	MP3 file
0x4C00000001140200	*.lnk	Link file
0x4C01	*.obj	OBJ file
0x4D4D002A	*.tif	TIF graphics
MM	*.tif	TIF graphics
0x000000186674797033677035	*.mp4	MP4 Video
ftyp3gp5	*.mp4	MP4 Video
0x300000004C664C65	*.evt	Event file
LfLe	*.evt	Event file
0x38425053	*.psd	Photoshop file
8BPS	*.psd	Photoshop file
0x4D5A	*.ocx	Active X
0x415649204C495354	*.avi	AVI file
AVI LIST	*.avi	AVI file
0x57415645666D7420	*.wav	WAV file
WAVEfmt	*.wav	WAV file
Rar!	*.rar	RAR file
0x526172211A0700	*.rar	RAR file
0x6D6F6F76	*.mov	MOV file
moov	*.mov	MOV file



Author: Prof Bill Buchanan

Data Hiding and Obfuscation

- Outline obfuscation methods.
- Define methods used to encode data in order to hide the original content.
- Understand encryption methods used to hide data, and possible methods to overcome this obfuscation.
- Define how file types can be discovered.

Author: Prof Bill Buchanan