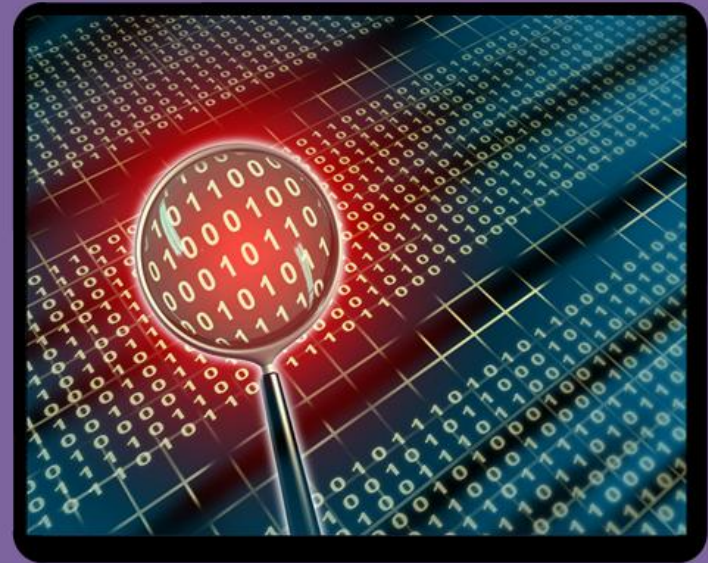
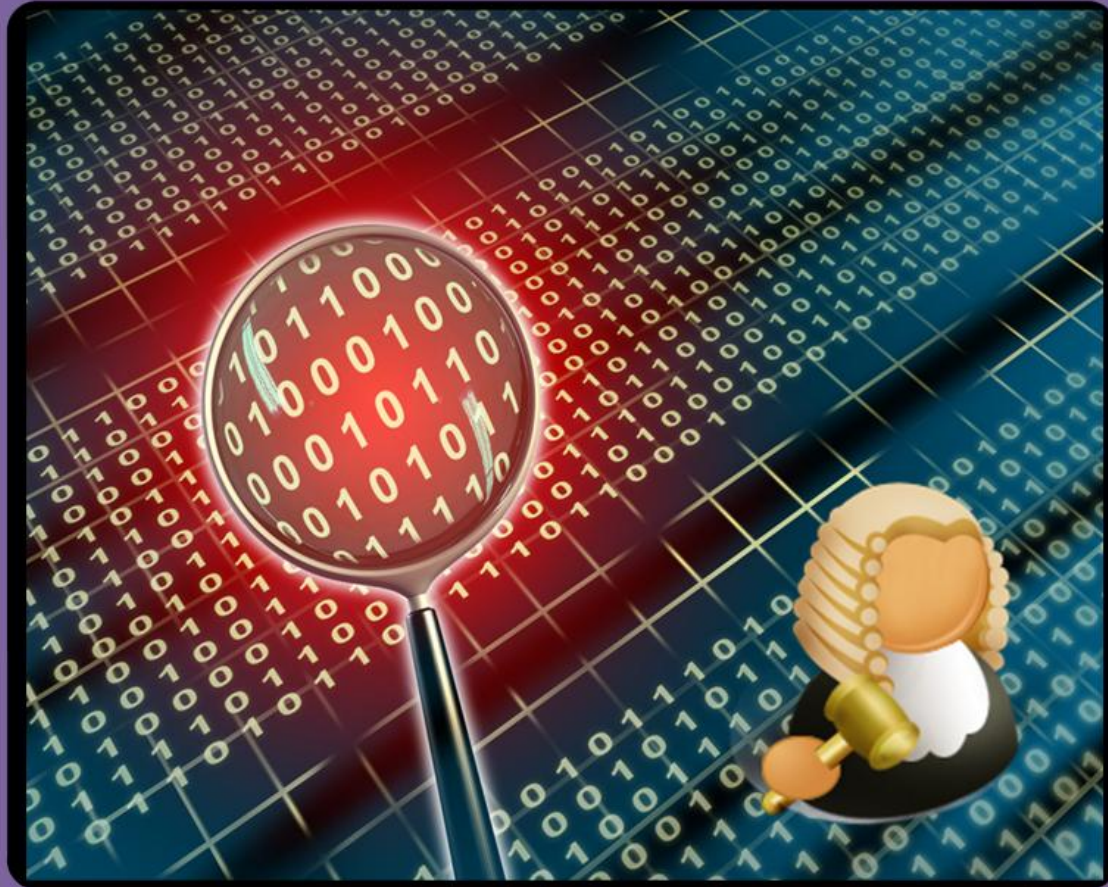


Data Hiding and Obfuscation

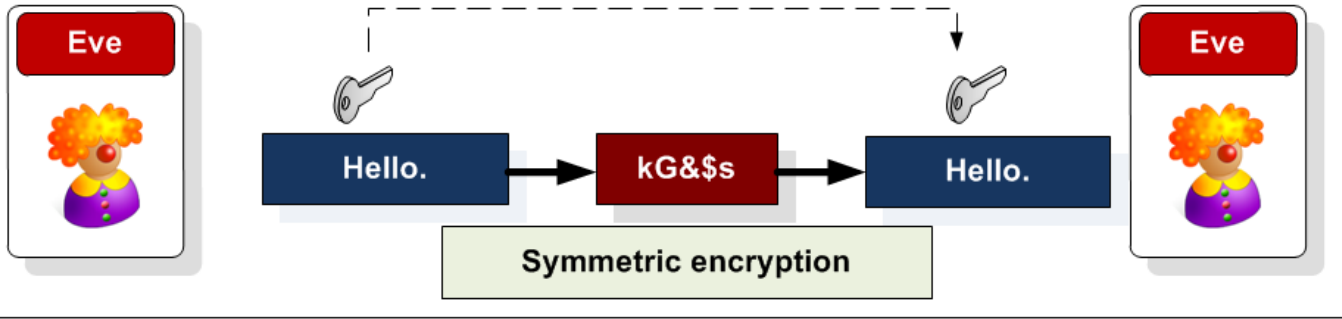
- Outline obfuscation methods.
- Define methods used to encode data in order to hide the original content.
- Understand encryption methods used to hide data, and possible methods to overcome this obfuscation.
- Define how file types can be discovered.



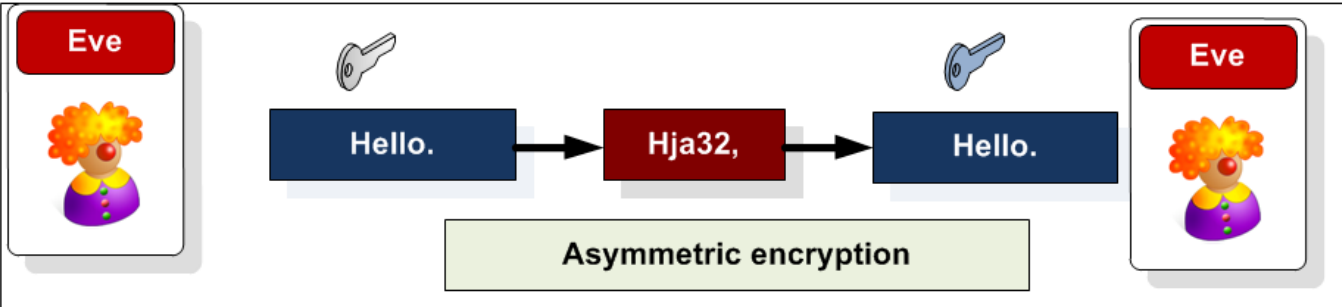
Data Hiding



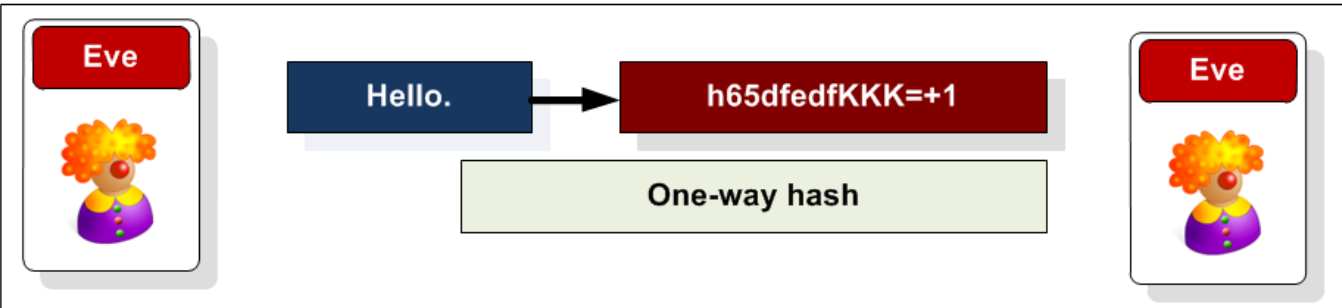
Obfuscation by
Encryption



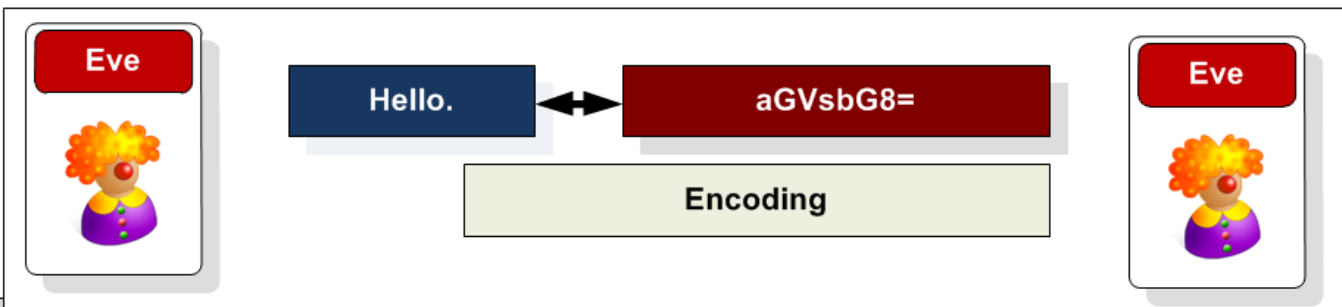
Private-key:
RC2, RC4,
DES, 3DES,
AES



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




Hashing:
MD5, SHA-1



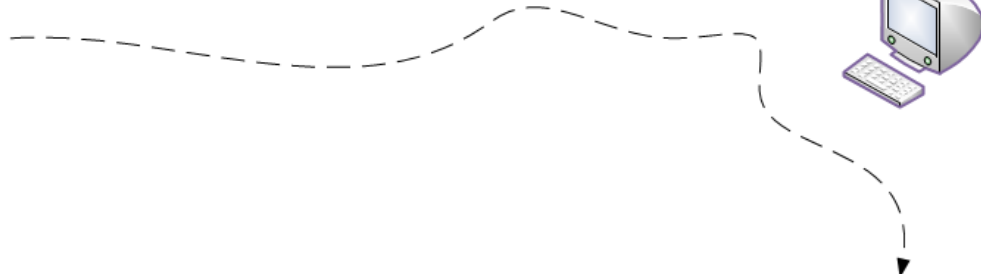
Encoding:
Hex, Base-64,
ASCII, UTF-16

Author: Prof Bill Buchanan

Eve



! Under suspect



test



**6XzX5ASPyIUE6K
thRc1UmA==**

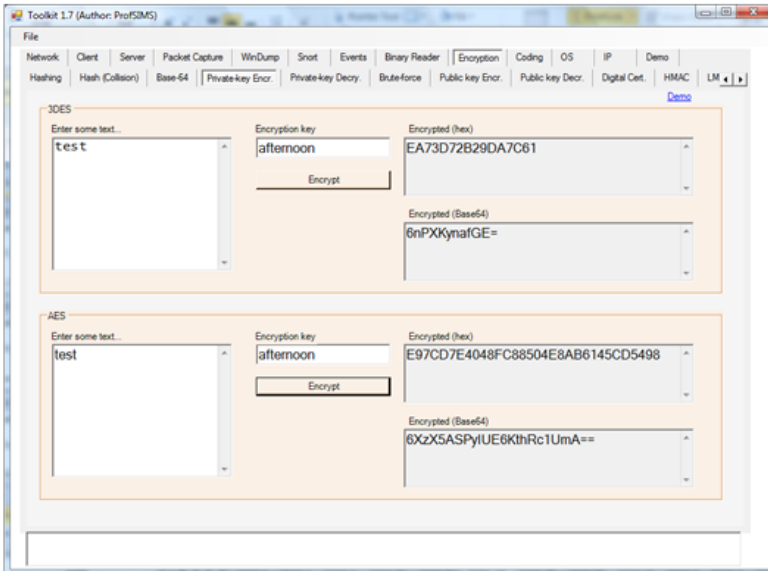
Search for key strings

crimedoesntpay
finaldemand
Mypassword
celticfc

Dictionary

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

Brute-force



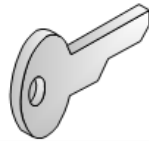
Eve



! Under suspect



test



6

Toolkit 1.7 (Author: ProfSims)

File Network Client Server Packet Capture WinDump Snort Events Binary Reader Encryption Coding OS IP Demo Hashing Hash (Collision) Base-64 Private-key Encr. Private-key Decry. Brute-force Public key Encr. Public key

3DES

Enter some text... Encryption key Encrypted (hex)

test afternoon EA73D72B29DA7C61

Encrypt

Encrypted (Base64)

6nPXKynafGE=

AES

Enter some text... Encryption key Encrypted (hex)

test afternoon E97CD7E4048FC88504E8AB6145CD5498

Encrypt

Encrypted (Base64)

6XzX5ASPyIUE6KthRc1UmA==

Toolkit 1.7 (Author: ProfSims)

File Network Client Server Packet Capture WinDump Snort Events Binary Reader Encryption Coding OS IP Demo Hashing Hash (Collision) Base-64 Private-key Encr. Private-key Decry. Brute-force Public key Encr. Public key Decr. Digital Cert. HMAC LM Demo

3DES

Enter encrypted (Hex) Encryption key Decrypted text

afternoon test

Decrypt

or ... Enter Base64 string

6nPXKynafGE=

AES

Enter hashed message Encryption key Decrypted text

afternoon test

Decrypt

or ... Enter Base64 string

6XzX5ASPyIUE6KthRc1UmA==

Brute-force

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

Eve



Toolkit 1.7 (Author: ProfSIMS)

File

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

Hashing Hash (Collision) Base-64 Private-key Encr. Private-key Decry. Brute-force Public key Encr. Public key Decr. Digital Cert. HMAC LM

[Brute force demo](#)

AES

1. First encrypt some AES text...

test

Encryption key: afternoon

Encrypted (hex): E97CD7E4048FC88504E8AB6145CD5498

Encrypt

Dictionary Attack

2. Next search for possible keys

Brute Force Attack

Trying... comess

Stop

Trying...

- Try
- Try a
- Try abilities
- Trying in a
- Try ability
- Try abilitys
- Try able
- Try about
- Try above
- Try absence
- Try absences
- Try absolute
- Try absolutely
- Try abuse
- Try academic

Possible

- afternoon [test]
- coded [JP*!LU>P\IIMO]

oesntpay
emand
word
fc

es
's
f

Encryption

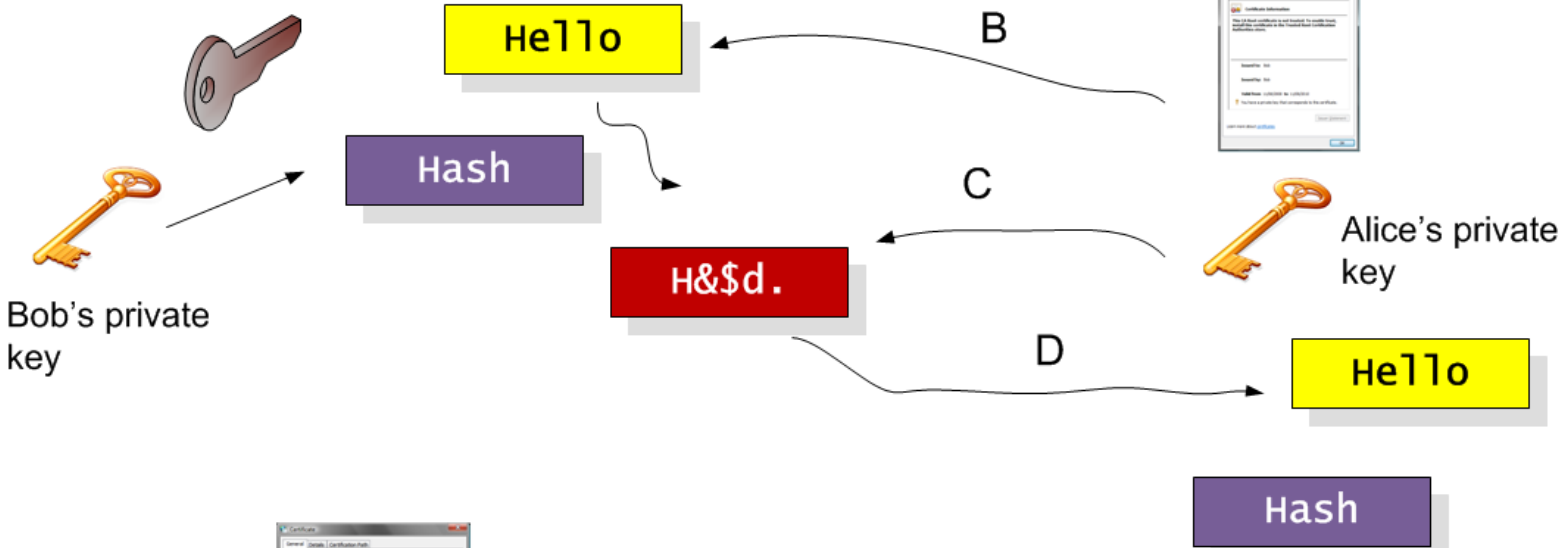
Data Hiding

Prof Bill Buchanan

Cracking the key



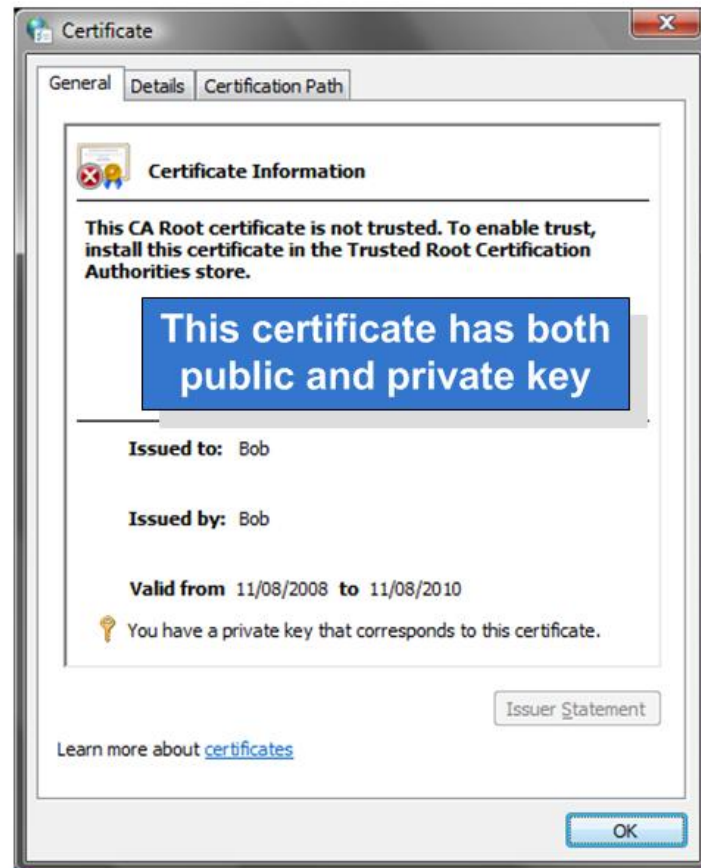
Encryption



Bob sends his Digital certificate to authenticate himself

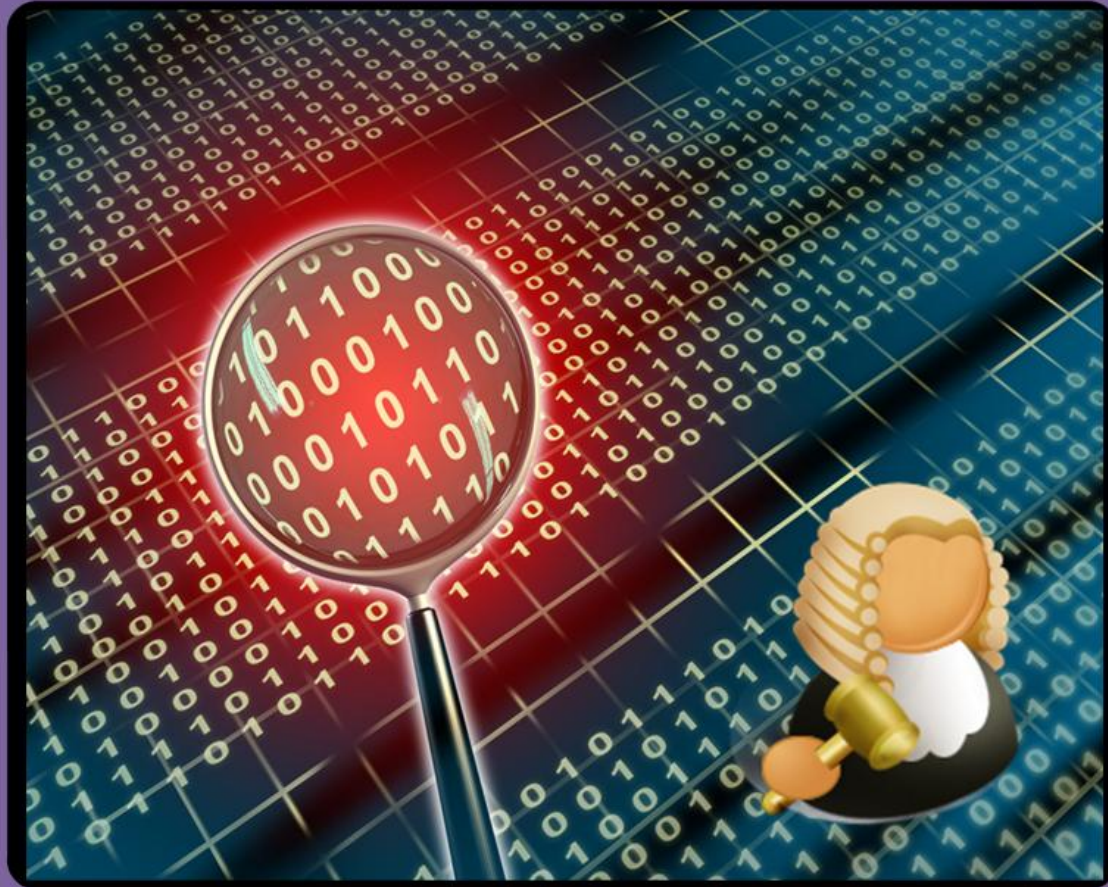
Alice checks the hash using Bob's public key from his certificate

Data Hiding



Author: Prof Bill Buchanan

Data Hiding



Obfuscation by Hashing



Hashing Algorithm (MD5) - 128 bit signature



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

Author: Prof. Dr. Bilal Durrani

Message Hash

Authentication



**Hashing
Algorithm (SHA-1)**
- 160 bit signature



hello

qvTGHdzF6KLavt4P00gs2a6pQ00=

Hello

9/+ei3uy4Jtwk1pdeF4MxdnQq/A=

Hello. How are you?

Puh2Am76bhjqE51bTwtwsqbdFC8=

Napier

v4GxNaVod2b09GR2Tqw4yop0uro=

Base-64

hello

AAF4C61DDCC5E8A2DABEDE0F3B482CD9AEA9434D

Hello

F7FF9E8B7BB2E09B70935A5D785E0CC5D9D0ABF0

Hello. How are you?

3EE876026EFA6E18EA13995B4D6B70B2A6DD142F

Napier

BF81B135A5687766F4F464764EAC38CA8A4EBABA

Hex

Message Hash

Authentication



**Hashing
Algorithm (MD5)**
- 128 bit signature



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 **most** important issues on the Internet, as they will allow users to secure their data transmissions, and also break their link their physical connections.

8A8BDC3FF80A01917D0432800201CFBF

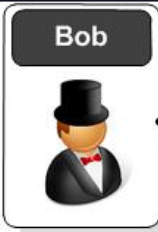
i ovCP/gKAZF9BDKAAGHPVW==

Hex

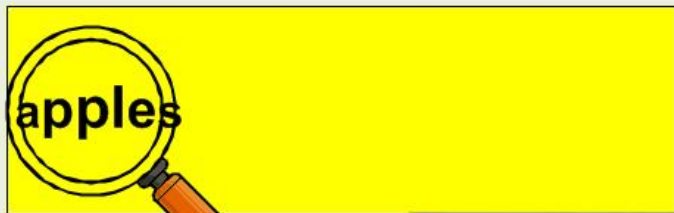
Author: T for Bill Buchanan

Message Hash

Authentication



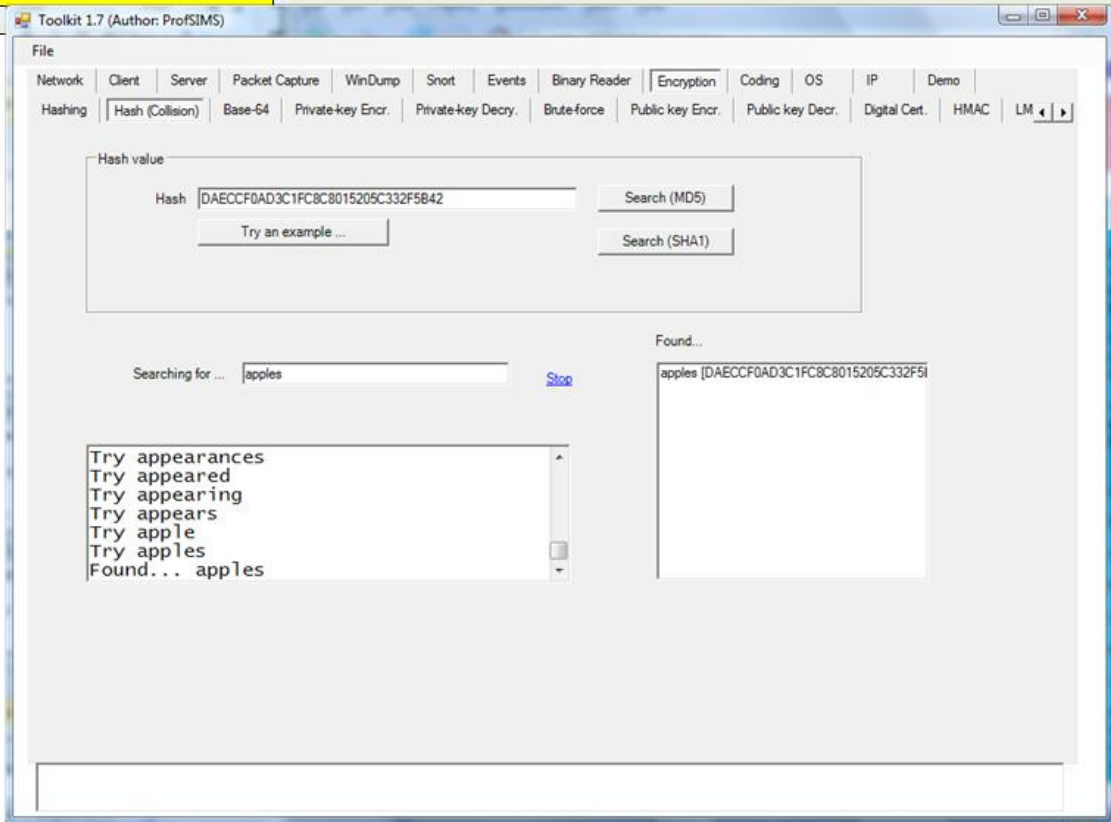
Hashing Algorithm (MD5) - 128 bit signature



DAECCF0AD3C1FC8C8015205C332F5B42

2uzPCTPB/IyAFSBcMy9bQg==

Base-64



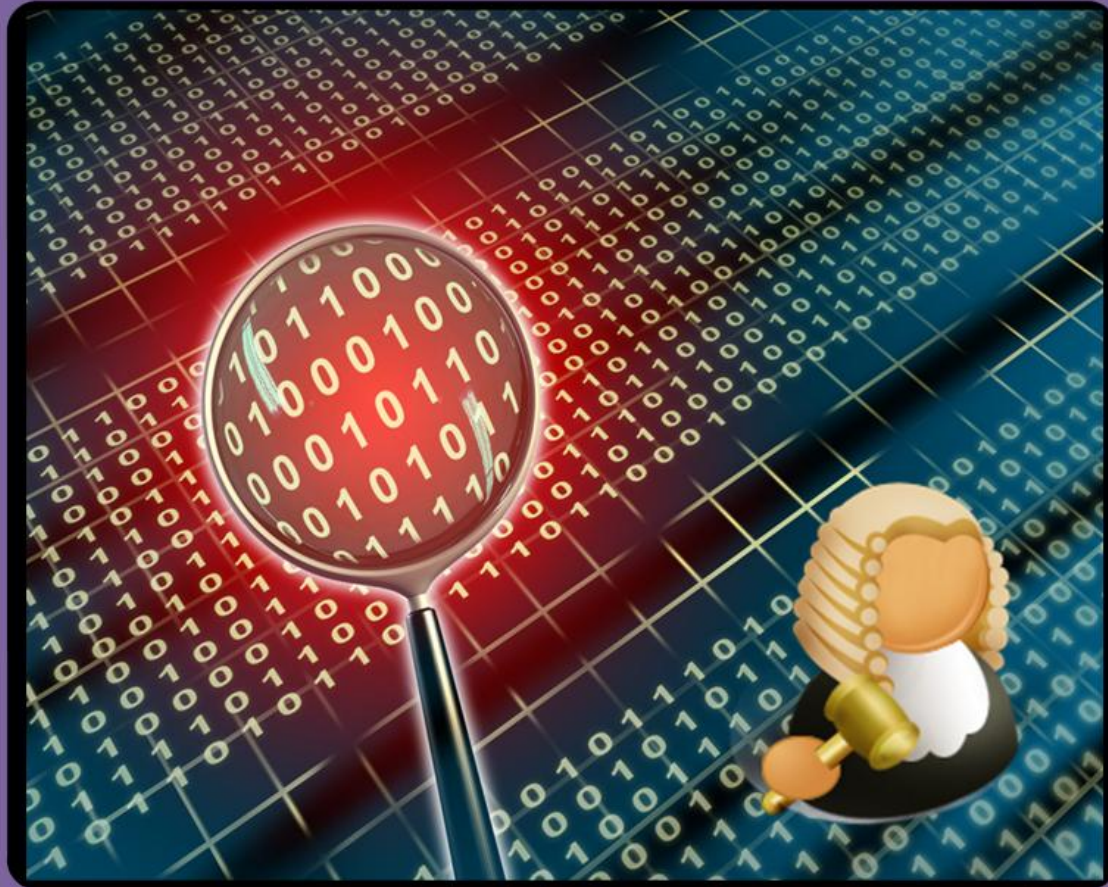
Message Hash

Authentication

Author: Prof Bill Buchanan

MD5 hash algorithm

Data Hiding



Obfuscation by Encoding



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

ASCII characters

01000001 01000010
01000011 01000100

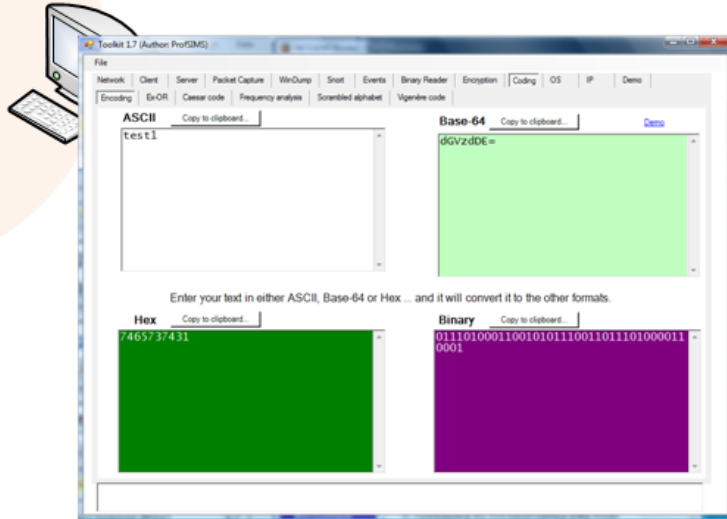
Encryption

01011110 00100000
11100110 10101010

Hex
5e 20 e6 aa

Base-64
xiDmqg





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

0111 0100 0110 0101 0111 0011 0111 0100 0011
0001

Bit stream

Data Hiding

7 4 6 5 7 3 7 4 3 1

Hex

Author: Prof Bill Buchanan

Hex conversion



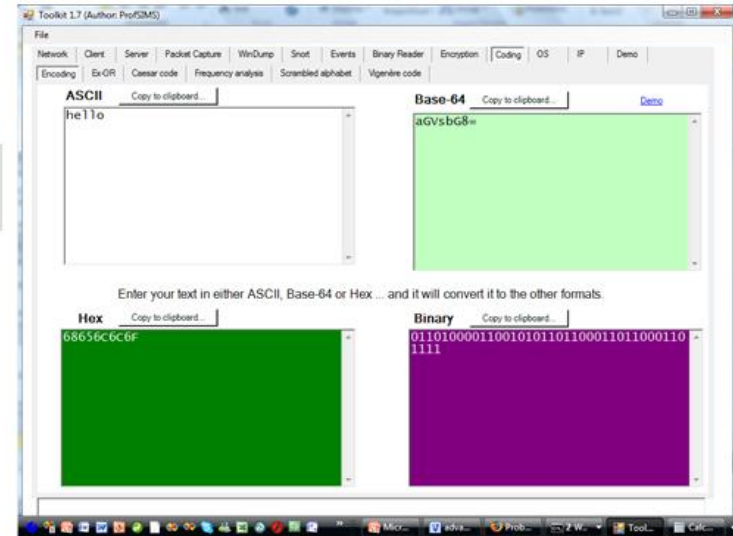
011010 000110 010101 101100 011011
000110 1111

Bit stream

a G V s b G 8 =

Base-64

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	/



Author: Prof Bill Buchanan

Encoding

Data Hiding



hello

01101000 01100101 01101100 01101100

+

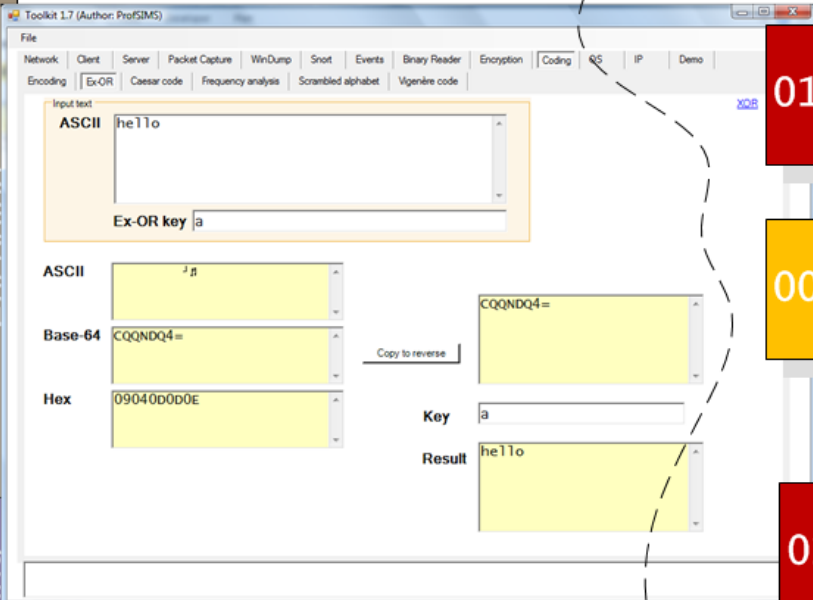
01100001 01100001 01100001 01100001

00001001 0000100 00001101 00001101

09 04 0D 0D 0E

01100001 01100001 01100001 01100001

01101000 01100101 01101100 01101100



Encoding

Data Hiding

Ex-OR

Eve

hello

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

The future of the Internet, especially in expanding the range of applications, involves a much deeper degree of privacy, and authentication. Without these the Internet cannot be properly used to replace existing applications such as in voting, finance, and

Try sample English

Most prob. Least prob.

Stand. Eng.	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
... from text	e	t	i	o	n	a	s	r	h	c	l	d	u	p	m	y	g	b	w	f	k	v	x	q	j	z

Letter	Occurance
e	170
t	128
i	112
o	100
n	96
a	94
s	80
r	66
h	65
c	62
l	44
d	40
u	39
p	39
m	30
y	30
g	25
b	21
w	21
f	21
k	17
v	16
x	2

Encode

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, NH0EO VQZEXPVTQ UOZOFZVTQ BA
 ZEBGGVF, BQU QOZNTJ/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

Input text

ASCII GTEFO NTXKU POZXI PIVOP NHTPO ZBPJ VZ VP ZT
 UOZOFZ VQZEXPVTQP, BQU BQC FTMOEZ BFZVMVZVOP.
 GVAXEO 2.3 VKKXPZEBZOP ZHVP FTQFOIZ, NH0EO
 VQZEXPVTQ UOZOFZVTQ BAOQZP BEO XPOU ZT KVPZOQ
 ZT QOZNTJ ZEBGGVF, BQU QOZNTJ/XPOE BFZVMVZC
 ZT ZEC BQU UOZOFZ BQC LEOBFHOP VQ POFXEVZC.

Try sample English

Most prob. Least prob.

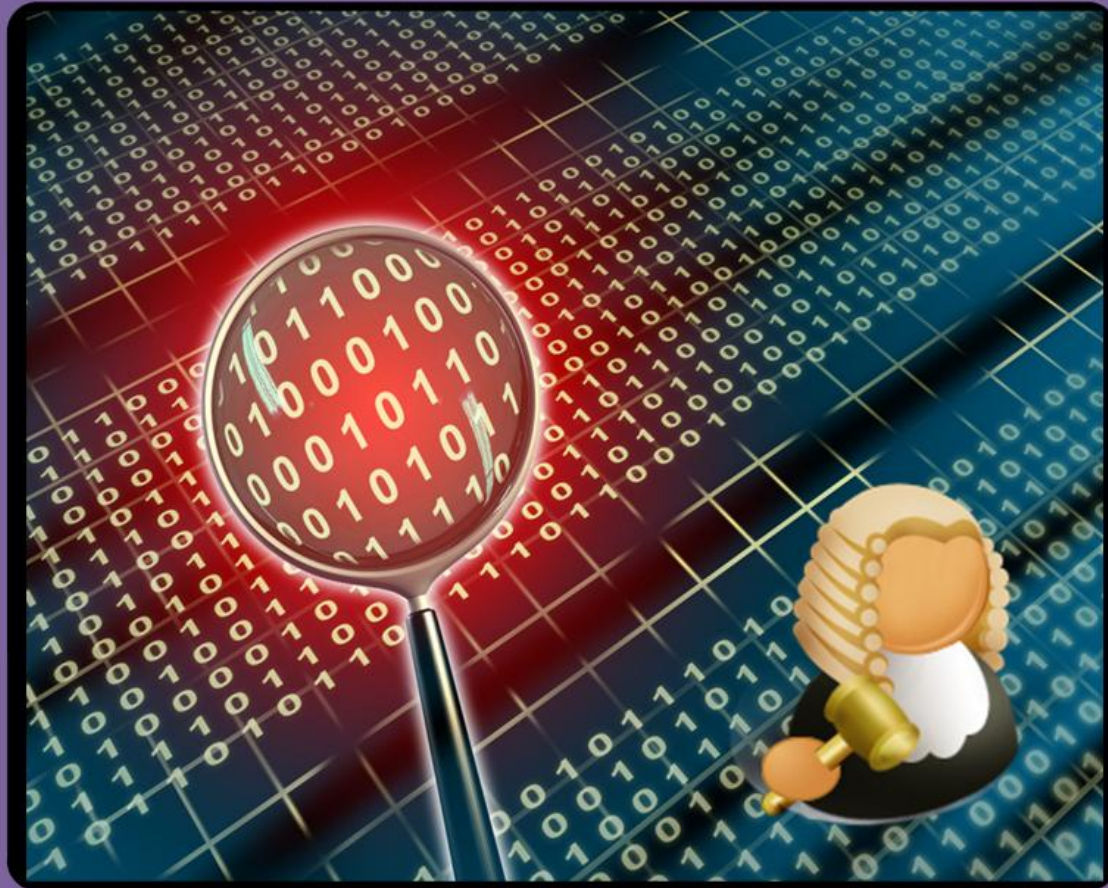
Stand. Eng. E T O A N I R S H D L C F U M P Y W G B V K X J Q Z

... from text

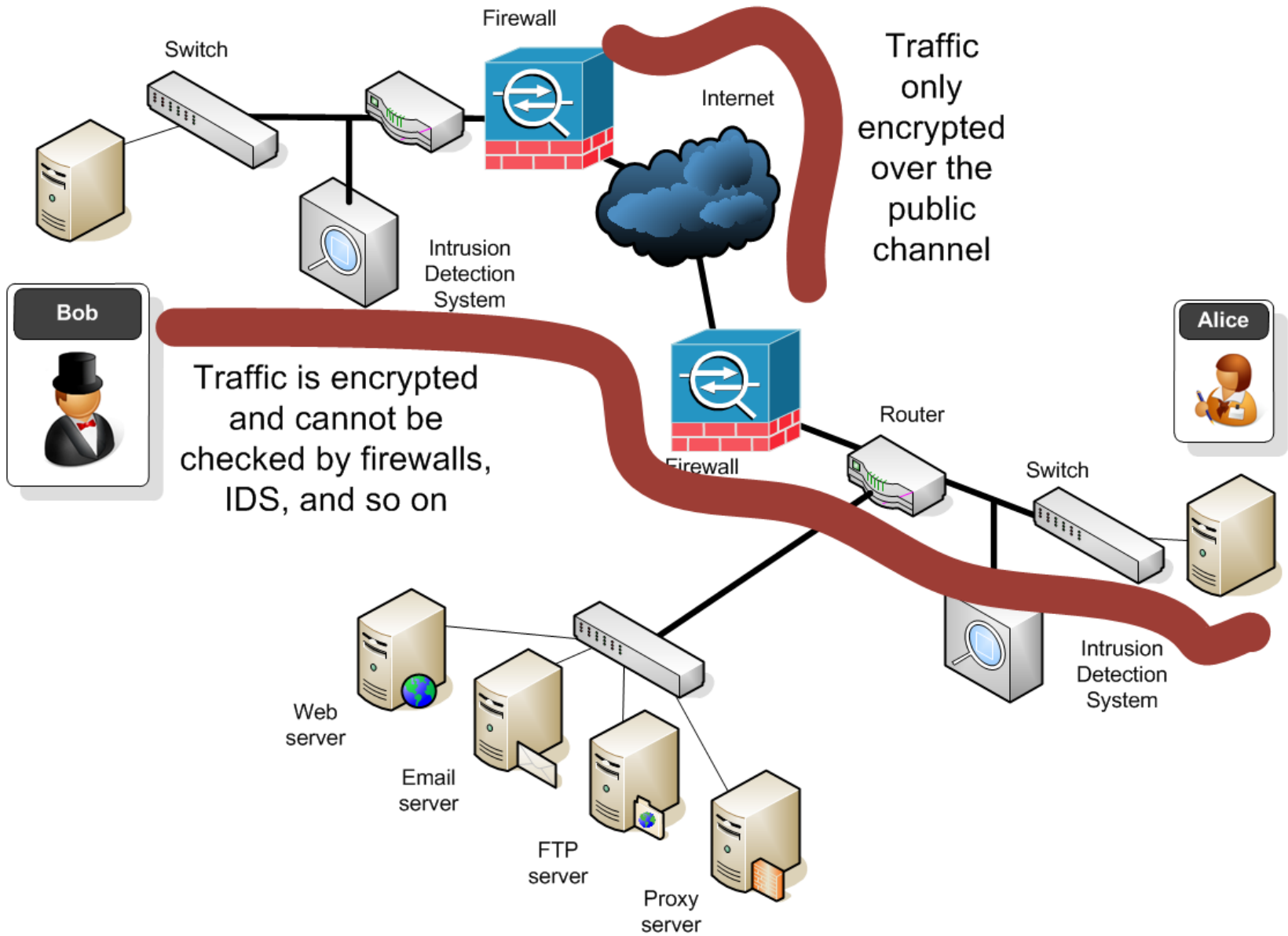
o	z	b	p	q	v	e	t	h	f	k	c	x	u	g	a	n	y	i	m	j	l	s	w	r	d
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

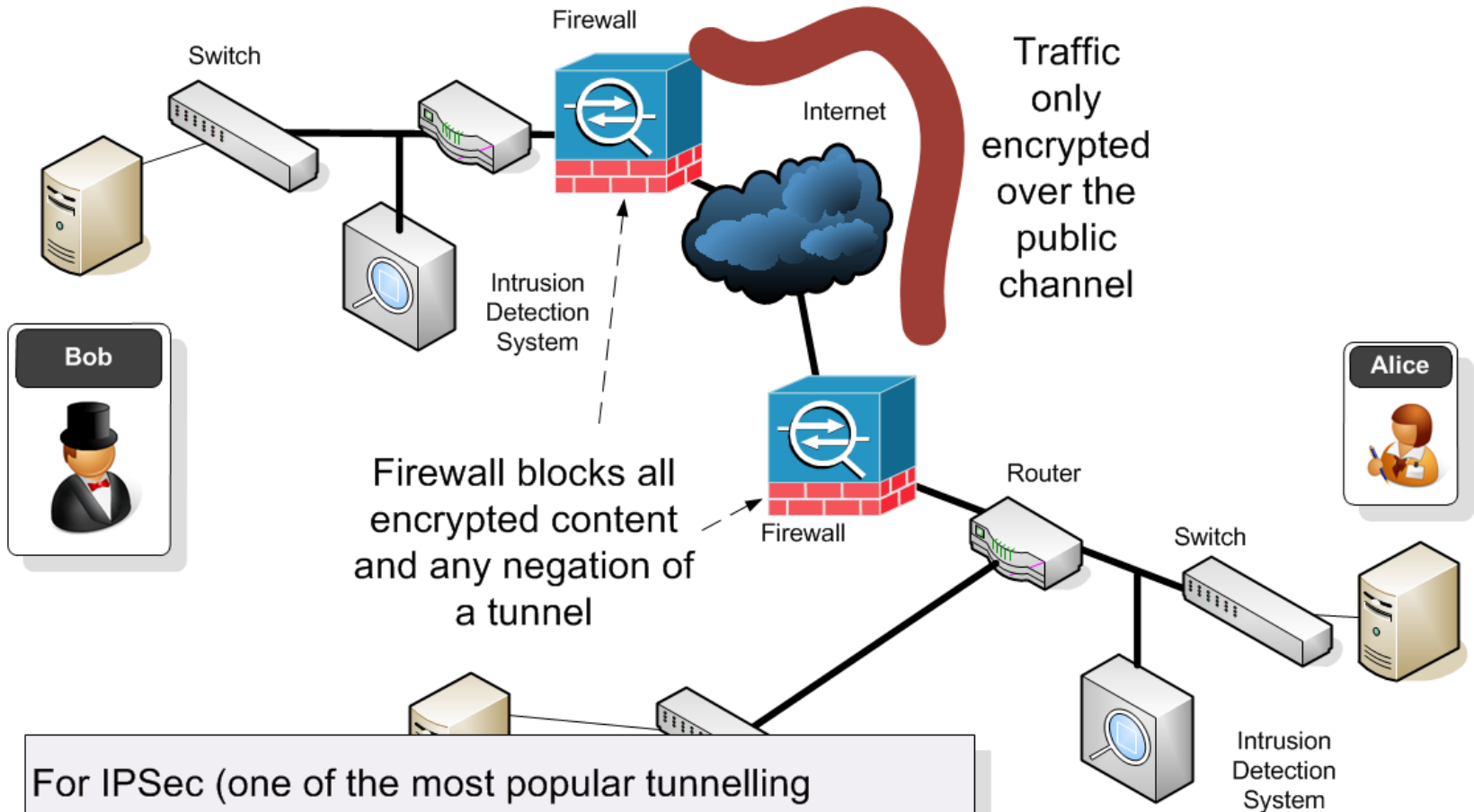
Letter	Occurance
o	145
z	128
b	116
p	104
q	98
v	87
e	70
t	65
h	52
f	51
k	41
c	37
x	36
u	36
g	27
a	25
n	25
y	23
l	20
m	11
j	11
i	9
r	1

Data Hiding



Obfuscation by
Tunnelling





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)

Switch

Firewall

Traffic

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\client\Toolkit\log\ipsec.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	UDP		16:45	192.168.0.20	65340	146.176.210.2	62515	~?K~
2	UDP		16:45	192.168.0.20	65341	146.176.210.2	500	~?C9?~d~
3	UDP		16:45	146.176.210.2	500	192.168.0.20	65341	~?C9?~d??Hm~.~?~8~
4	UDP		16:45	192.168.0.20	65342	146.176.210.2	4500	~?C9?~d??Hm~.~?~??~
5	UDP		16:45	192.168.0.20	65342	146.176.210.2	4500	?
6	UDP		16:45	146.176.210.2	4500	192.168.0.20	65342	~?C9?~d??Hm~.~?~??~d%~
7	UDP		16:45	192.168.0.20	65342	146.176.210.2	4500	~?C9?~d??Hm~.~?~??~TD~
8	UDP		16:45	146.176.210.2	4500	192.168.0.20	65342	~?C9?~d??Hm~.~?~4a?/~<~
9	UDP		16:45	192.168.0.20	65342	146.176.210.2	4500	~?C9?~d??Hm~.~?~4a?/~<9?~
10	UDP		16:45	192.168.0.20	65342	146.176.210.2	4500	~?C9?~d??Hm~.~?~??a~?p~
11	UDP		16:45	146.176.210.2	4500	192.168.0.20	65342	~?C9?~d??Hm~.~?~??a~T?~
12	UDP		16:45	146.176.210.2	57442	192.168.0.20	5442	~?~?4^?& ~?~?S?S?????o1T?Q~+?~

VPN

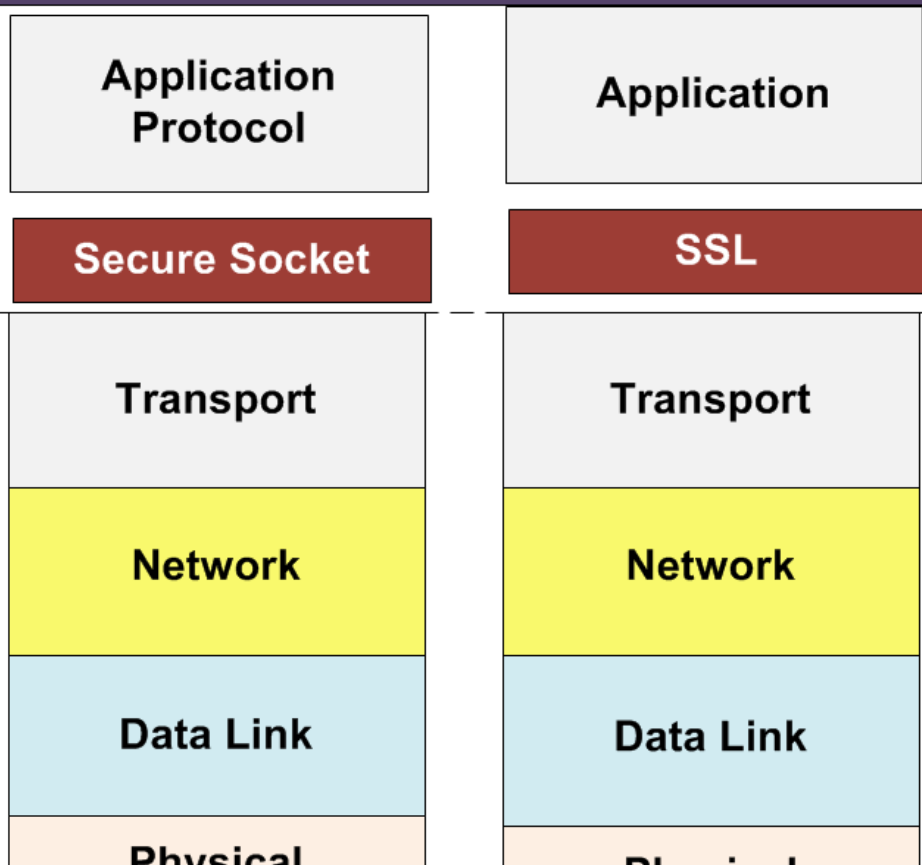
Data Hiding

methods):

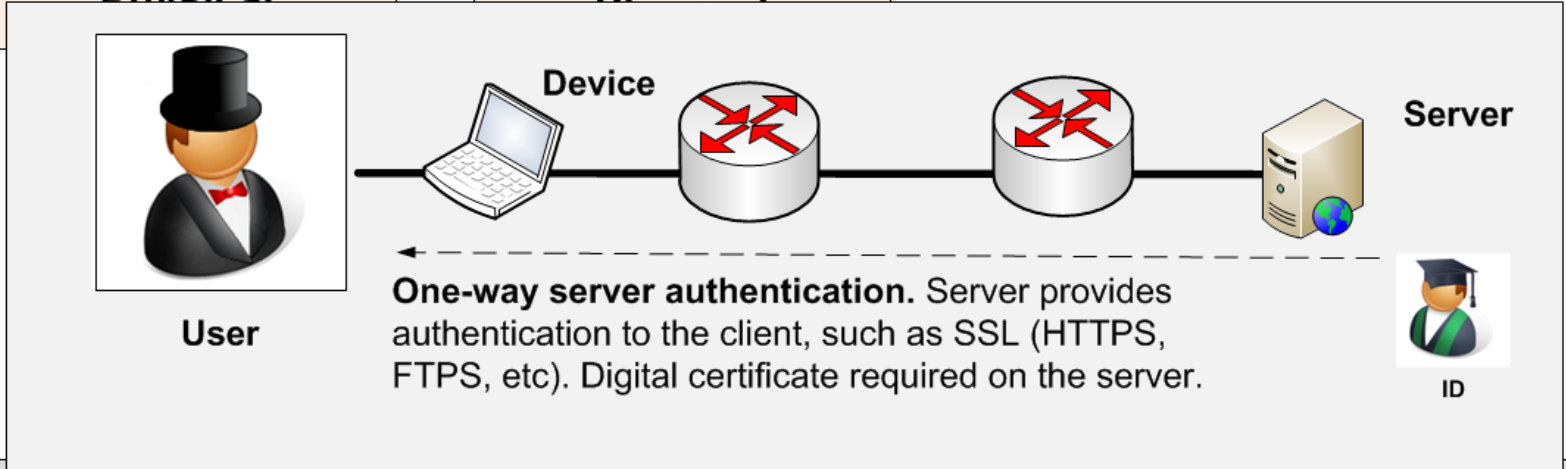
- UDP Port 500 is the key exchange port. If it is blocked there can be no tunnel.
- TCP Port 50 for IPsec ESP (Encapsulated Security Protocol).
- TCP Port 51 for IPsec AH (Authentication Header)

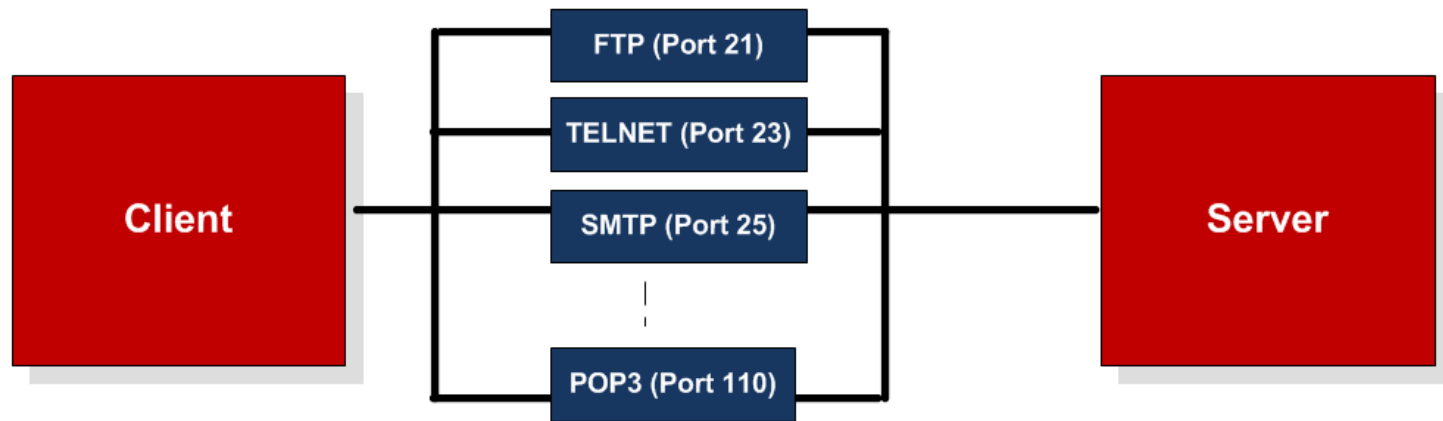
Tunnelling

Data hiding

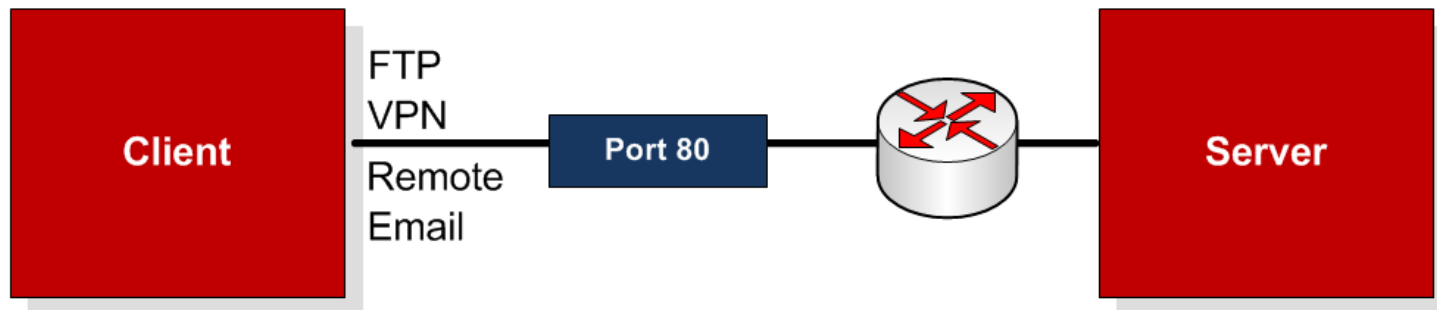


Secure protocols:
Port: 443. https (HTTP + SSL).
Port: 465. ssmtp (SMTP + SSL).
Port: 563. snntp (NNTP + SSL).
Port: 995. spop (POP-3 + SSL).
Port: 993. simap (IMAP + SSL).



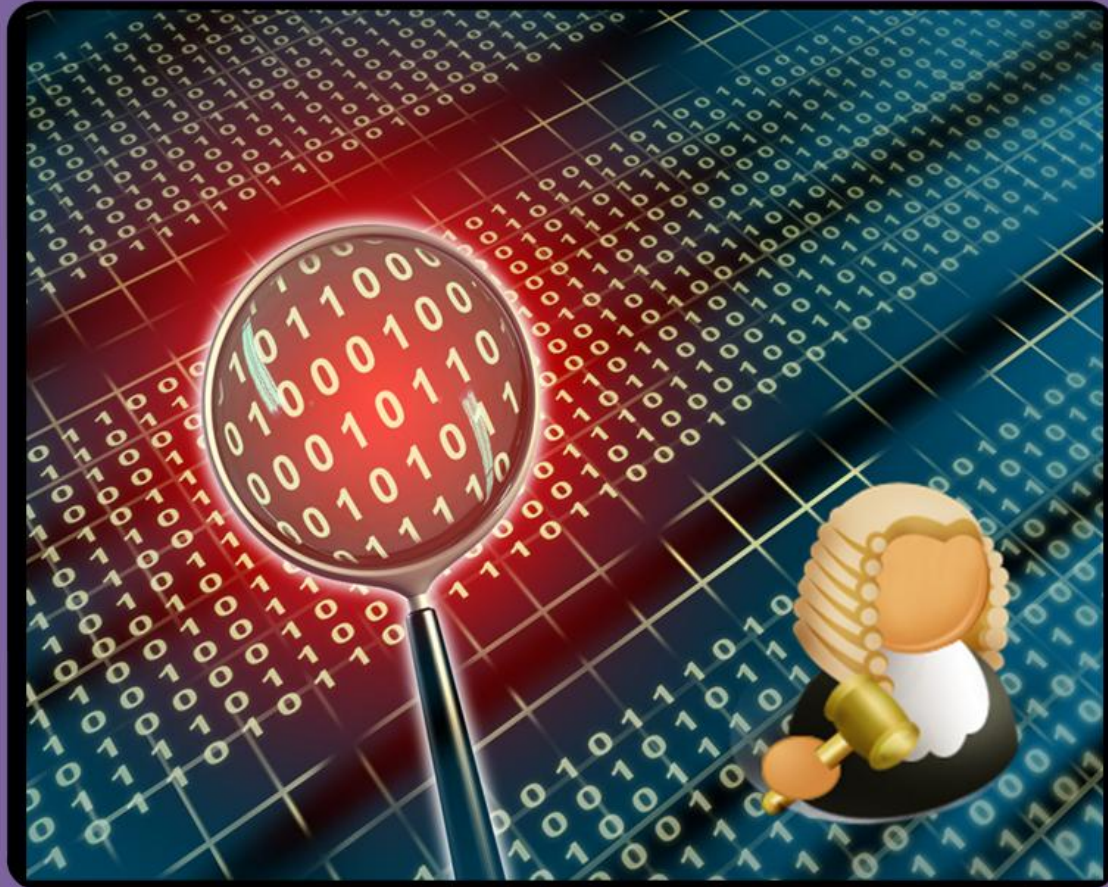


Applications use a wide range of TCP ports to communicate. Each of these ports could be blocked.

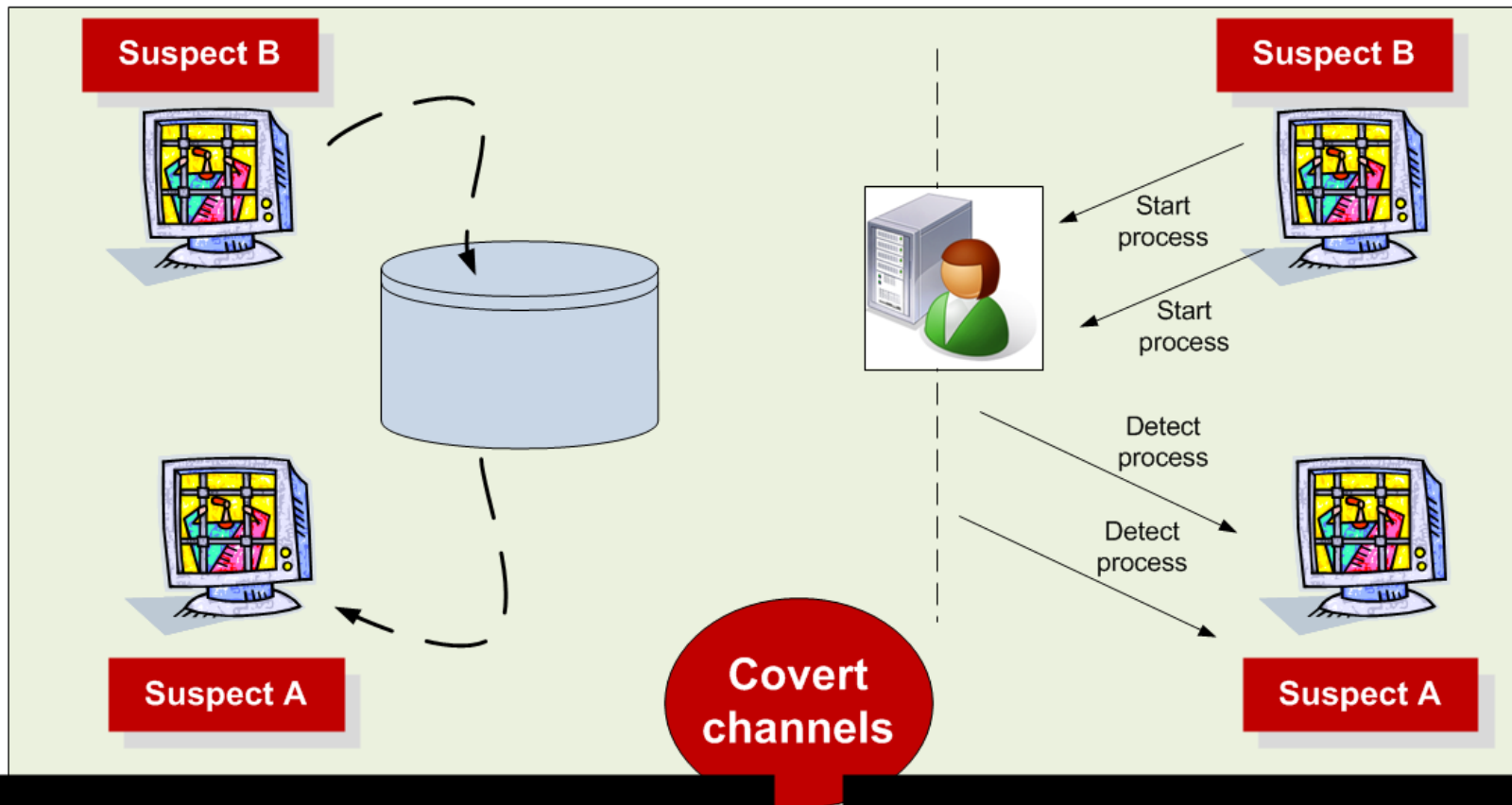


Applications communicate for a wide range of services through port 80 (Web port)... port 80 traffic is allowed through the firewall ... but can cause security problems as the firewall cannot check the usage

Data Hiding

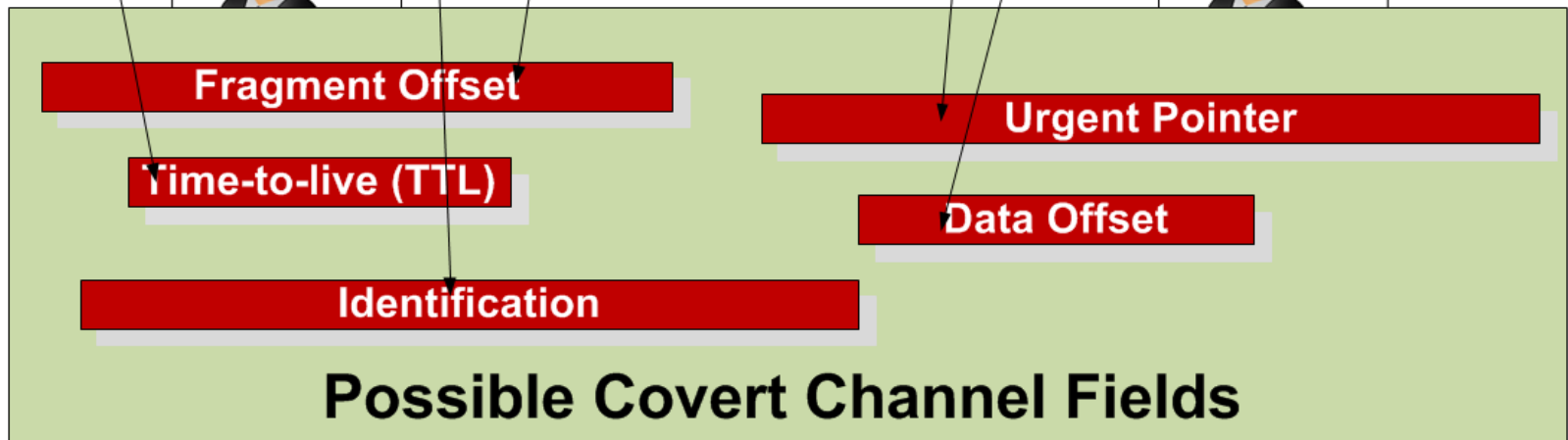
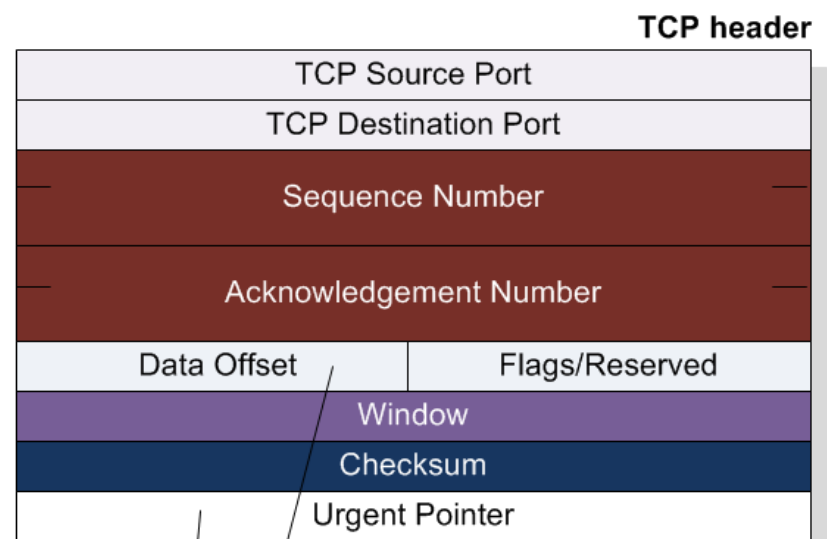
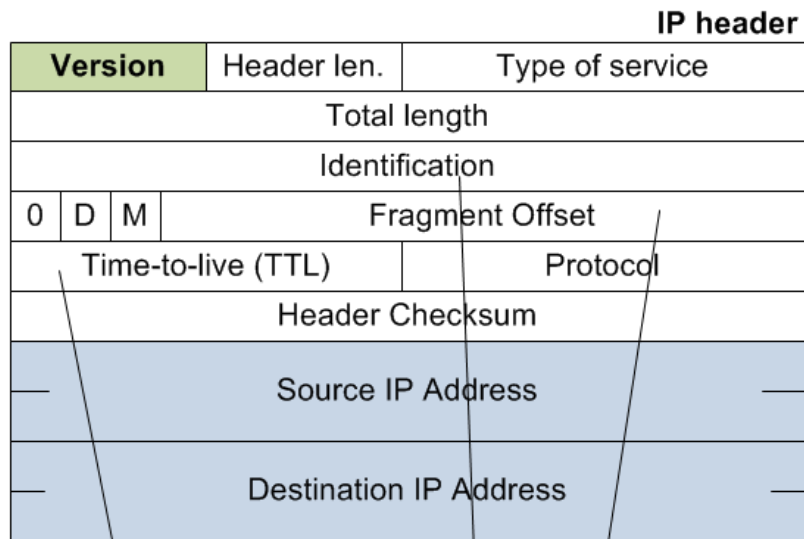


Covert Channels

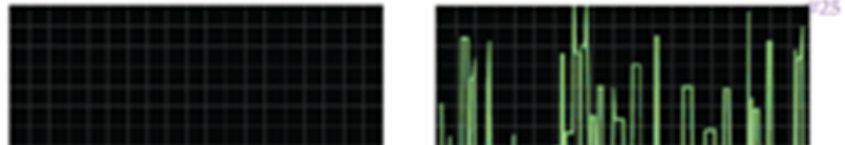


Storage covert channels are where one process uses direct (or indirect) data writing, whilst another process reads the data. It generally uses a finite system resource that is shared between entities with different privileges.

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)

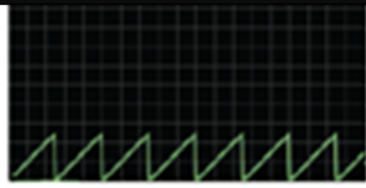
... Packets missed out ...

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)

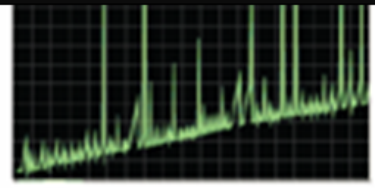
```

Data hiding

identifying fragments of an original IP
Source: David Llamas



Real Covert channel based on IPv4ID



Unknown

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

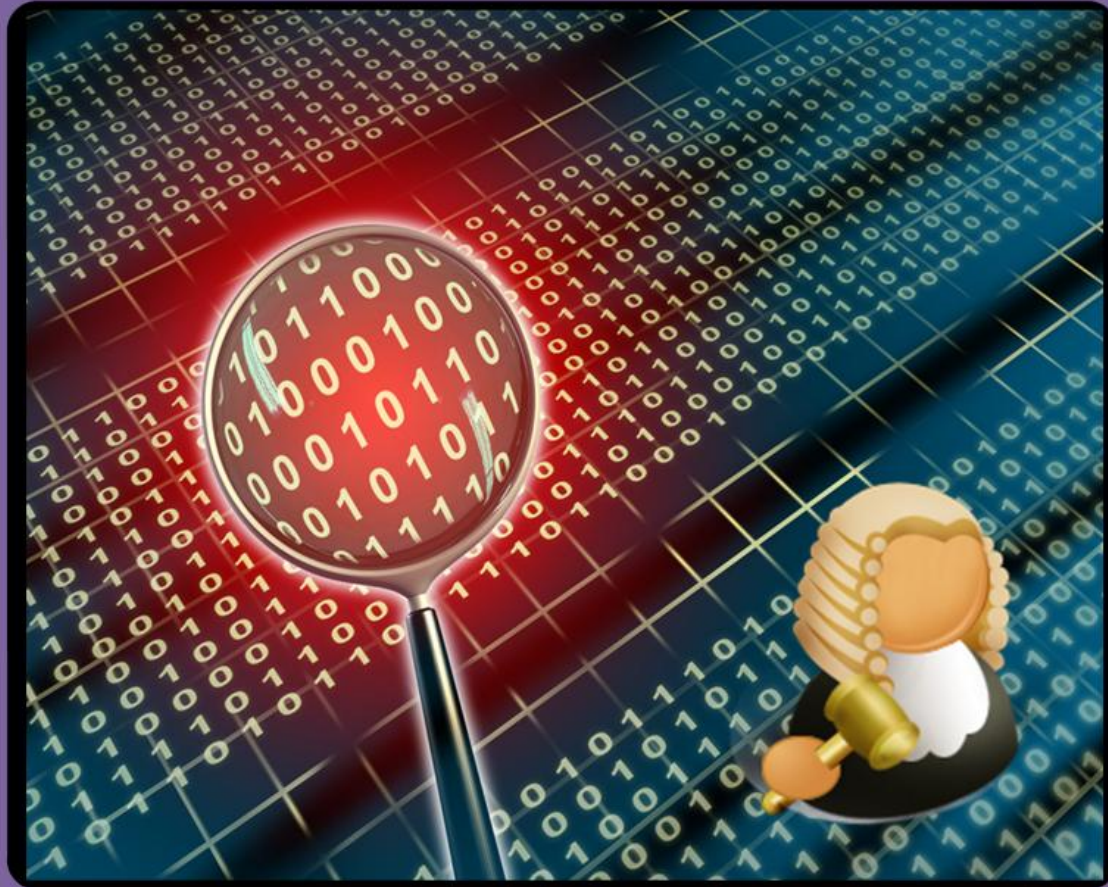
Identification: 0x0050 (80)

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)

Data Hiding



File Signatures

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

Obfuscation



Mypic.gif



Mypic.dll

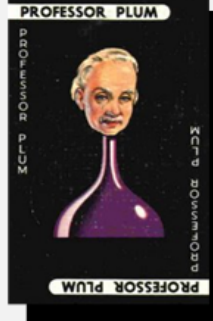
Change name from:

Mypic.gif

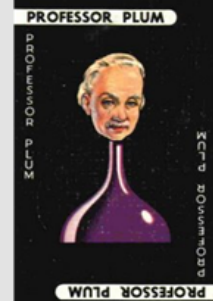
To

Mypic.dll

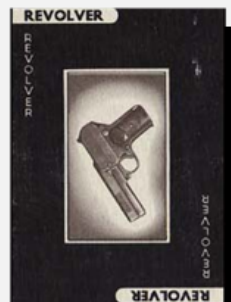
Prof. PLUM



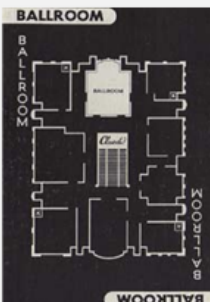
Prof. PLUM



REVOLVER



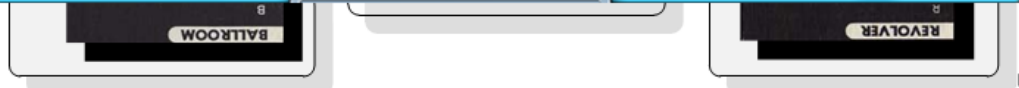
BALLROOM

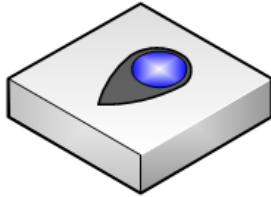


Data hiding

File name changing

The screenshot shows the Toolkit 1.7 interface. At the top, there are menu tabs: File, Network, Client, Server, Packet Capture, WinDump, Snort, Events, Binary Reader, Encryption, Coding, OS, IP, and Demo. Below these are buttons for 'View GIFs', 'View JPGs', 'View ZIPs', 'Open Any', and a dropdown menu for '-- Open Mystery File --'. An 'Identify file type' button is also present. The file path 'F:\docs\src\client\Toolkit\log\cat01_with_hidden_text.gif' is entered in the address bar, with a 'Tutorial' link next to it. The main area is split into two panes: 'Hex viewer' on the left and 'Char viewer' on the right. The hex viewer shows a grid of hexadecimal values, with the first column highlighted in red. The char viewer shows the corresponding ASCII characters, revealing the text 'GIF89a d. U.', 'h e l l o', 'f z . . .', '^ ^ . H H . . s . z . . z ^ s .', '. . f f t u r a . f j s . . r M.', '. n R k j n w c _ . * * t h E f', 'f f \ f t . U . b k k _ ? . "', '" . M . O U] f a V a Q \ I U X Z', 'W U S K U b c J J U Q H . . . J', 'R X . . . 0 P . . . C K V H J', 'H . 3 6 . . . D E B 7 E R B A 9', '& C x G : . 4 ? I R 0 1 : : < .', '. . < 8 5 f % (/ : B / : < 3 3', '3 k . .) 1 A * 1 9 4 / * z . .', ') - 1 0 + (! . 8 3 (")) (!'.





Sig

0x474946
 GIF89a
 0xFFD8FF
 JFIF
 0x504B03
 0x25504446
 %PDF
 0x0A2525454F460A
 .%%EOF.

File ext

*.gif
 *.gif
 *.jpg
 *.jpg
 *.zip
 *.pdf
 *.pdf
 *.pdf

File type

GIF files
 GIF files
 JPEG files
 JPEG files
 ZIP files
 PDF files
 PDF files
 PDF file
 PDF file

Toolkit 1.7 (Author: ProfsIMS)

File

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

View GIFs View JPGs View ZIPs Open Any - Open Mystery File - Identify file type

F:\docs\src\client\Toolkit\F:\08009817.pdf Tutorial

Hex viewer

00	25	50	44	46	20	31	2E	35	0D	0A	25	B5	B5	B5	B5	0D
10	0A	31	20	30	20	6F	62	6A	0D	0A	3C	3C	2F	54	79	70
20	65	2F	43	61	74	61	6C	6F	67	2F	50	61	67	65	73	20
30	32	20	30	20	52	2F	4C	61	6E	67	28	65	6E	2D	47	42
40	29	20	2F	53	74	72	75	63	74	54	72	65	65	52	6F	6F
50	74	20	31	39	20	30	20	52	2F	4D	61	72	68	49	6E	66
60	6F	3C	3C	2F	4D	61	72	68	65	64	20	74	72	75	65	3E
70	3E	3E	3E	0D	0A	65	6E	64	6F	62	6A	0D	0A	32	20	30
80	20	6F	62	6A	0D	0A	3C	3C	2F	54	79	70	65	2F	50	61
90	67	65	73	2F	43	6F	75	6E	74	20	32	2F	48	69	64	73
A0	5B	20	33	20	30	20	52	20	31	31	20	30	20	52	50	20
B0	3E	3E	0D	0A	65	6E	64	6F	62	6A	0D	0A	33	20	30	20
C0	6F	62	6A	0D	0A	3C	3C	2F	54	79	70	65	2F	50	61	67
D0	65	2F	50	61	72	65	6E	74	20	32	20	30	20	52	2F	52
E0	65	73	6F	75	72	63	65	73	3C	3C	2F	46	6F	6E	74	3C
F0	3C	2F	46	31	20	35	20	30	20	52	2F	46	32	20	37	20
1.	30	20	52	2F	46	33	20	39	20	30	20	52	3E	3E	2F	50
1.	72	6F	63	53	65	74	5B	2F	50	44	46	2F	54	65	78	74
1.	2F	49	6D	61	67	65	42	2F	49	6D	61	67	65	43	2F	49
1.	6D	61	67	65	49	5D	20	3E	3E	2F	4D	65	64	69	61	42

Char viewer

P	.	D	.	F
.	.	1	.	0
e	/	C	a	t	a	l	o	g	/	P
2	0	R	/	L	a	n	g	(.
)	/	S	t	r	u	c	t	T	r
t	1	9	0	R	/	M	a
o	<	<	<	M	a	r	k	e	d
>	>	>	.	e	n	d
o	b	j
g	e	s	/	C	o	u	n	t
[3	0	R	1	1
>	>	.	e	n	d
o	b	j
e	/	P	a	r	e	n	t
e	s	o	u	r	c	e	s	<	<
<	/	F	1	5	0	R	/
0	R	/	F	3	9	0
r	o	c	S	e	t	[/	P	D	F
/	i	m	a	g	e	B	/	i	m	a	g	e
m	a	g	e	l]

Toolkit 1.7 (Author: ProfsIMS)

File

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

View GIFs View JPGs View ZIPs Open Any - Open Mystery File - Identify file type

F:\docs\src\client\Toolkit\F:\docs\src\client\Toolkit\log\arcode.zip Tutorial

Hex viewer

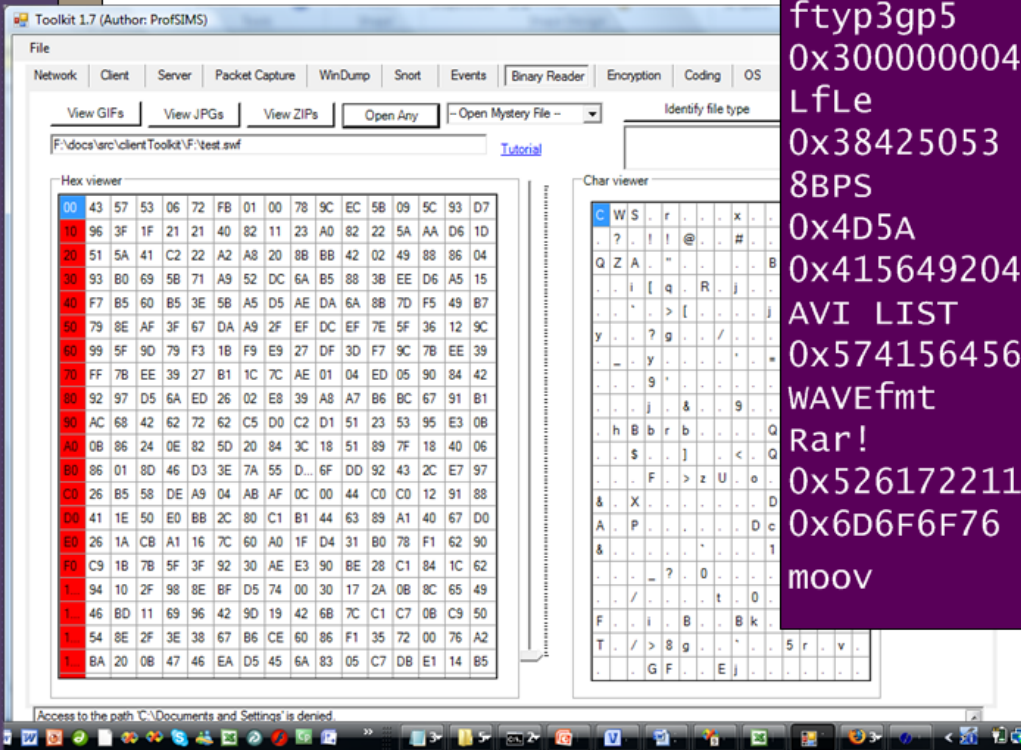
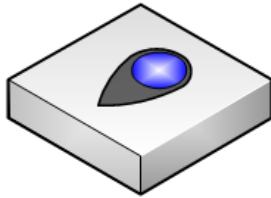
60	50	4B	03	04	14	00	00	00	08	00	65	38	15	21	DF	32
10	7E	7E	5A	00	00	00	64	00	00	0C	00	00	00	00	50	52
20	4F	47	32	5F	30	32	2E	50	41	53	2B	28	CA	4F	2F	4A
30	CC	55	28	00	D2	46	F1	86	1A	99	79	05	A5	25	3A	F9
40	A5	25	40	4A	D3	9A	97	2B	29	35	3D	33	8F	97	4B	01
50	04	CA	8B	32	4B	52	35	D4	5D	F3	4A	52	8B	14	12	15
60	CA	12	73	4A	53	15	F2	D3	14	8A	52	8B	33	8B	4B	12
70	F3	92	53	D5	41	5A	C0	6A	81	DA	93	33	78	B9	52	F3
80	52	F4	A4	00	50	4B	03	04	14	00	00	00	08	00	2E	62
90	24	21	92	B3	B0	88	94	00	00	00	08	01	00	00	0B	00
A0	00	00	50	52	4F	47	31	5F	32	2E	50	41	53	5D	8F	C1
B0	0A	83	30	10	44	EF	42	7E	A0	DC	54	0C	D5	08	0B	0D
C0	28	39	F6	38	24	6D	17	09	D8	35	6E	12	FB	FB	55	82
D0	00	75	2F	33	38	30	8F	5D	4B	F3	48	FA	CD	ED	A6	72
E0	90	85	41	1B	BC	98	83	DF	A4	EC	59	C6	B2	55	13	DF
F0	87	C0	19	E7	67	92	E2	70	AD	80	25	0C	71	D3	F8	84
1.	8E	40	4F	5B	C7	46	26	CB	1E	30	1A	DC	19	FF	80	4E
1.	C9	A6	69	FA	53	DC	7E	EA	96	D2	13	59	C9	BA	90	F5
1.	8F	50	25	DF	96	47	E5	43	C6	C3	84	45	7E	5F	82	59
1.	F5	04	E8	79	42	70	E3	78	7E	3A	38	3E	08	F8	BA	5E

Char viewer

P	K
.	.	Z
O	G	2	_	0	2	.	P	A	S	+	(.	O	/	J	.
U	(.	F
!	@	J
.	.	2	K	R	5	.]	.	J	R
.	.	s	J	S
.	.	S	A	Z
R
\$!
.	.	P	R	O	G	1	_	2	.	P	A	S]	.	.	.
.	.	0
(.	9
.	.	u	/	3	.	0	.]	.	K	.	H
.	.	A
.	.	g
.	.	@	[.	F	&
.	.	i	.	.	S
.	.	P	%	.	G
.	.	y	B	p

Data

File signature



Sig

0x465753
 FWS
 0x494433
 ID3
 0x4c0000001140200
 0x4C01
 0x4D4D002A
 MM
 0x000000186674797033677035
 ftyp3gp5
 0x30000004C664C65
 LfLe
 0x38425053
 8BPS
 0x4D5A
 0x415649204C495354
 AVI LIST
 0x57415645666D7420
 WAVEfmt
 Rar!
 0x526172211A0700
 0x6D6F6F76
 moov

File ext

*.swf
 *.swf
 *.mp3
 *.mp3
 *.lnk
 *.obj
 *.tif
 *.tif
 *.mp4
 *.mp4
 *.evt
 *.evt
 *.psd
 *.psd
 *.ocx
 *.avi
 *.avi
 *.wav
 *.wav
 *.rar
 *.rar
 *.mov
 *.mov

File type

SWF file
 SWF file
 MP3 file
 MP3 file
 Link file
 OBJ file
 TIF graphics
 TIF graphics
 MP4 video
 MP4 video
 Event file
 Event file
 Photoshop file
 Photoshop file
 Active X
 AVI file
 AVI file
 WAV file
 WAV file
 RAR file
 RAR file
 MOV file
 MOV file

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.

