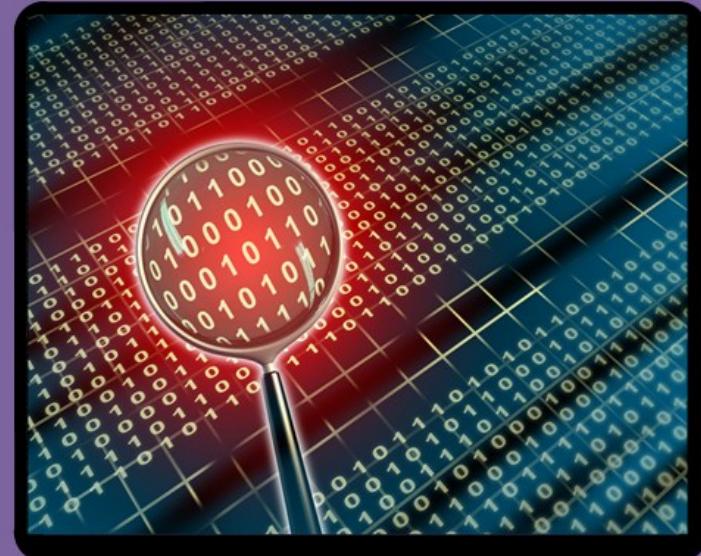
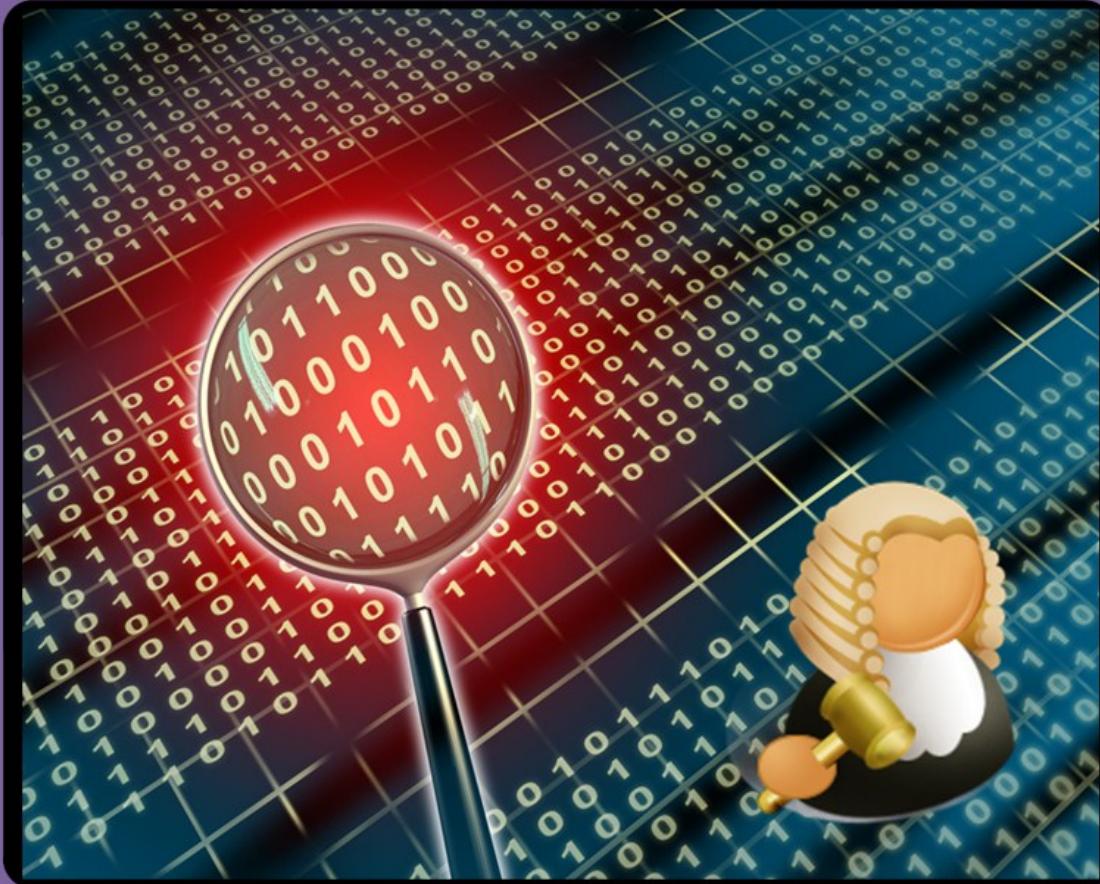


Data Hiding and Obfuscation

- 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.

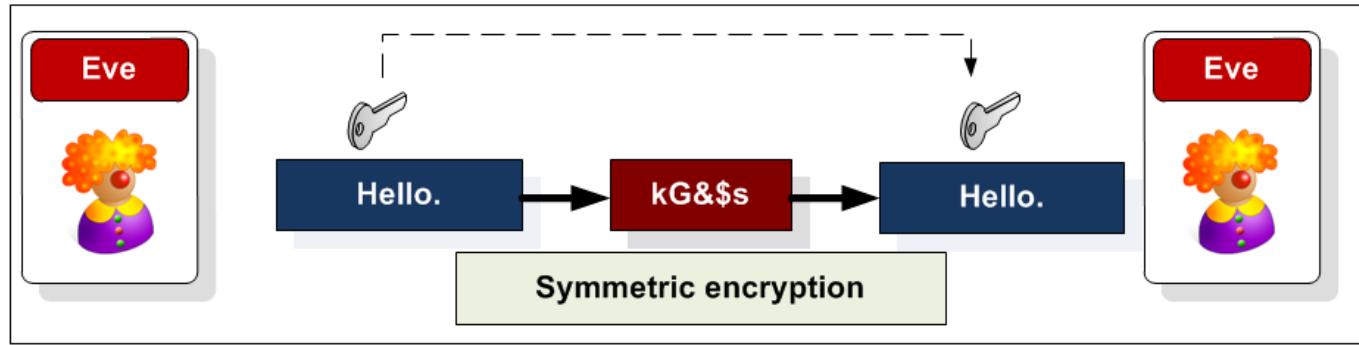


Data Hiding

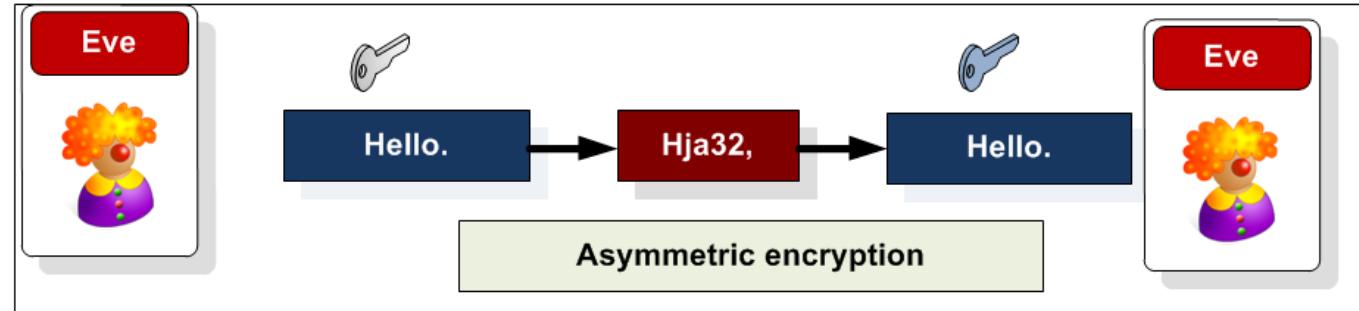


Obfuscation by
Encryption

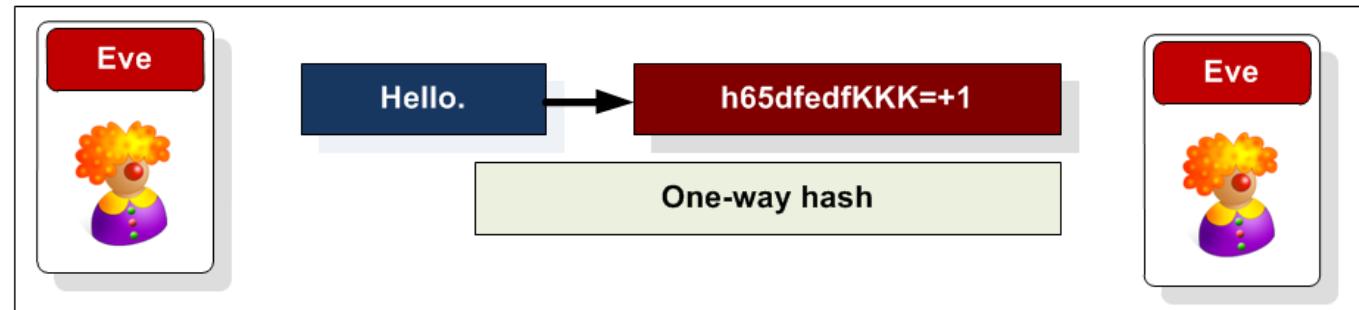
Encryption



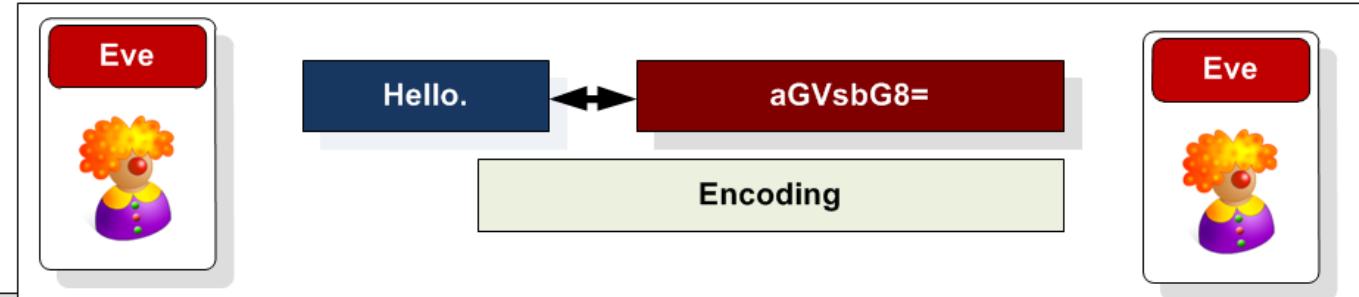
Private-key:
RC2, RC4,
DES, 3DES,
AES



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

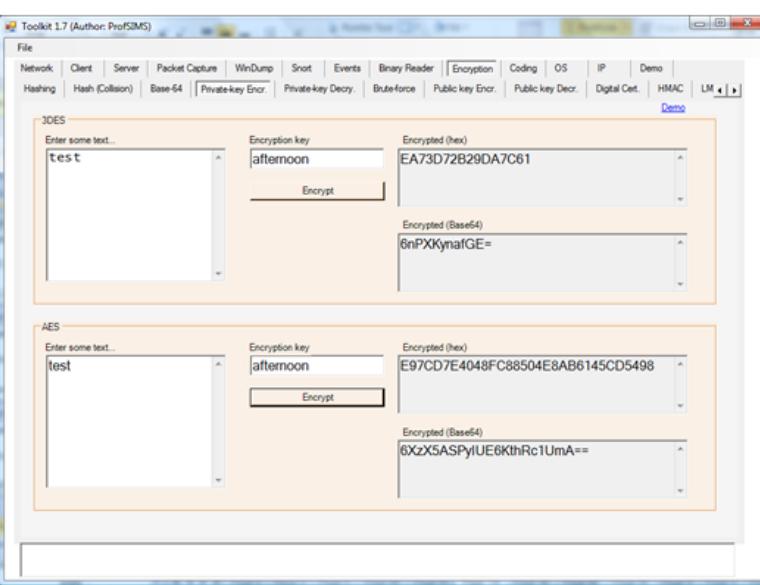


Hashing:
MD5, SHA-1

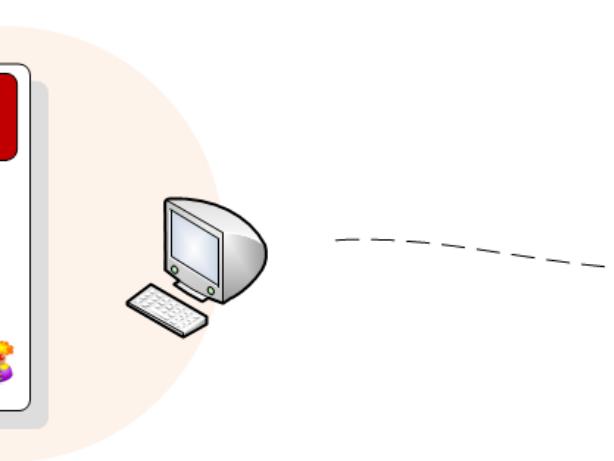


Encoding:
Hex, Base-64,
ASCII, UTF-16

Author: Prof Bill Buchanan



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

3DES

Enter encrypted (Hex): Encryption key: Decrypted text:

AES

Enter hashed message: Encryption key: Decrypted text:

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 Decr. Brute-force Public key Encr. Public key Decr. Digital Cert. HMAC Demo

Encryption

3DES

Enter some text...: Encryption key: Encrypted (hex): Encrypted (Base64): Encrypt

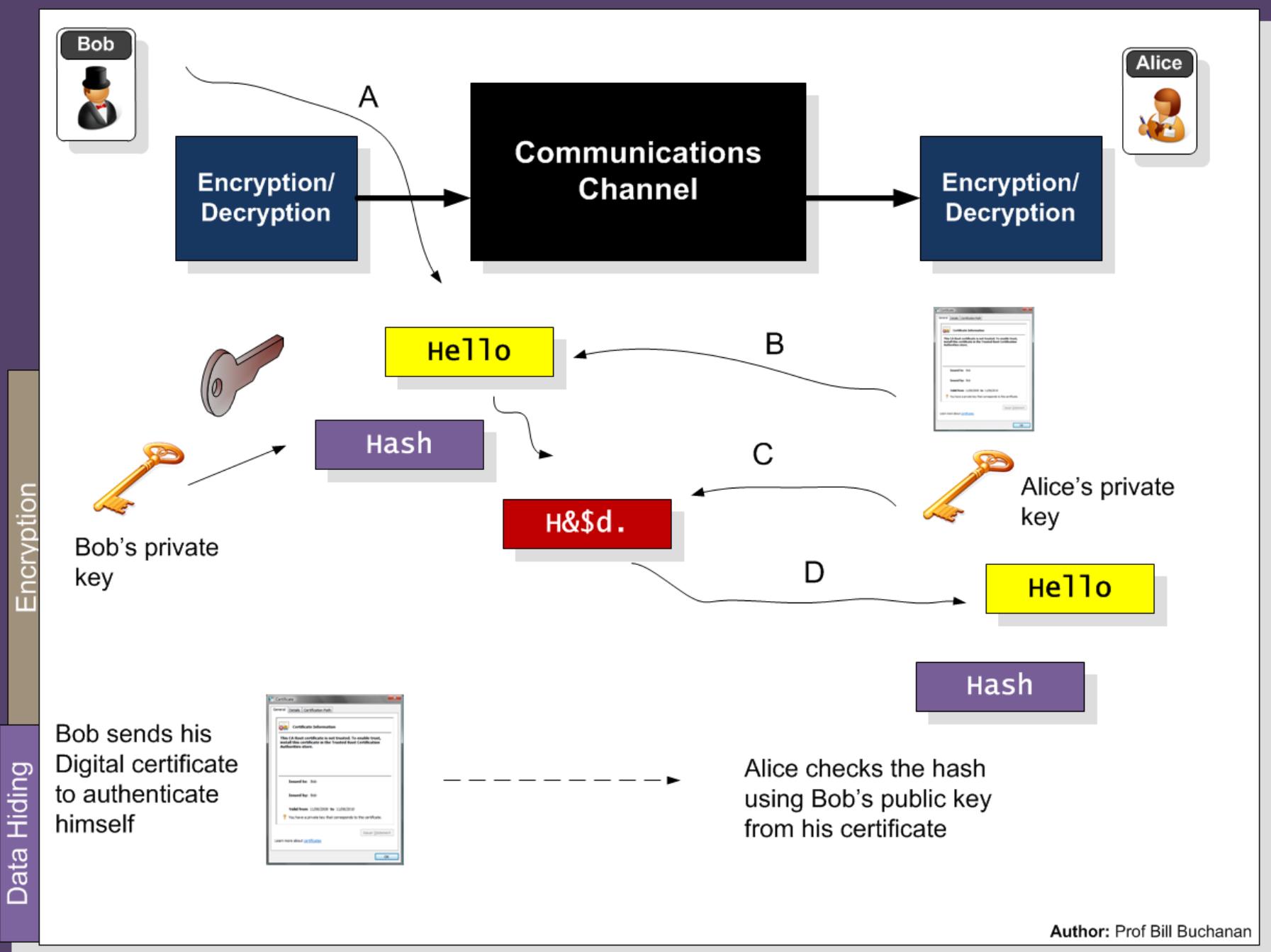
AES

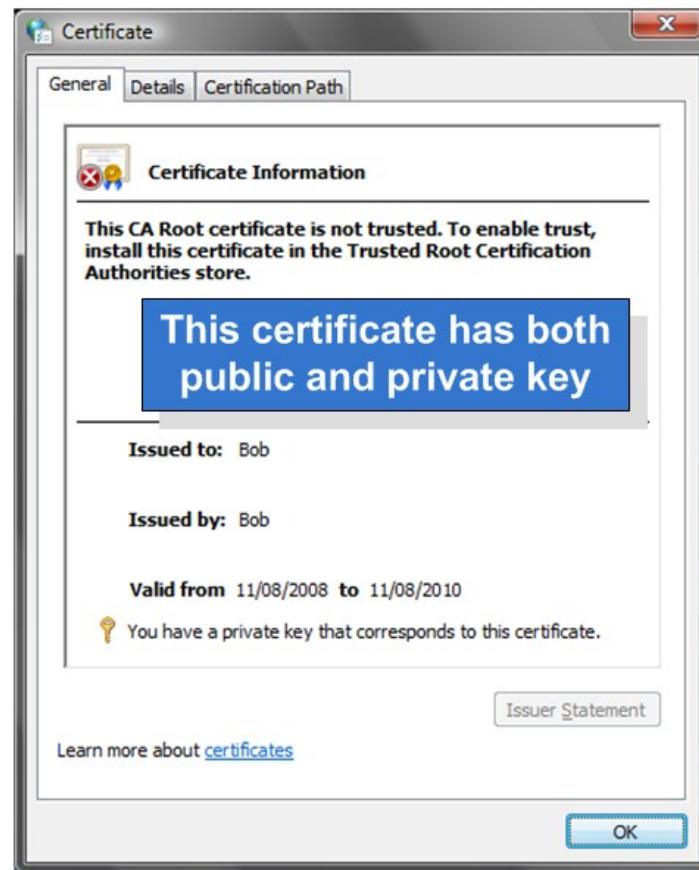
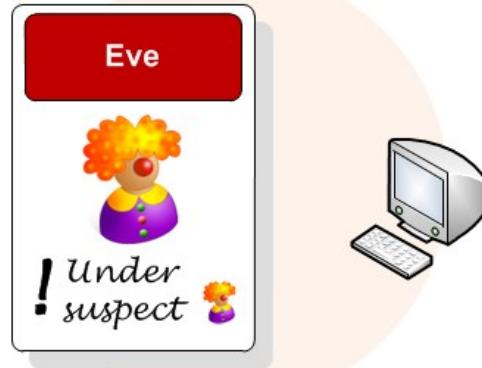
Enter some text...: Encryption key: Encrypted (hex): Encrypted (Base64): Encrypt

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

Author: Prof Bill Buchanan

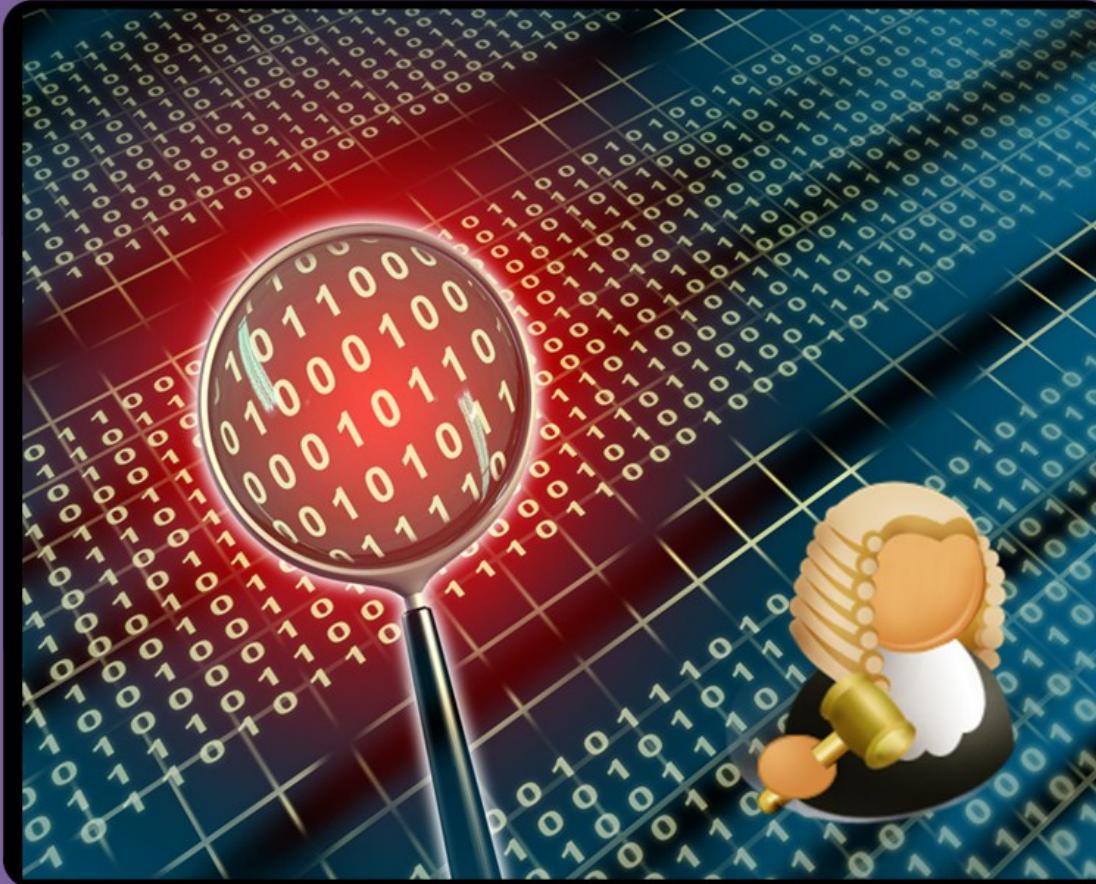
The image shows a screenshot of the Toolkit 1.7 software interface, version 1.7 (Author: ProfSIMS). The interface is titled "AES" and includes sections for "Encryption key" and "Encrypted (hex)". In the "Encryption key" section, the text "afternoon" is entered. In the "Encrypted (hex)" section, the hex value "E97CD7E4048FC88504E8AB6145CD5498" is displayed. Below this, a "Dictionary Attack" section is shown, with the text "comess" entered into a "Trying..." field. A list of words being tried includes: Try, Try a, Try abilities, Trying in a, Try ability, Try abilities, Try able, Try about, Try above, Try absence, Try absences, Try absolute, Try absolutely, Try abuse, and Try academic. To the right of this list, the text "afternoon [test] coded [üP*ILU>þ\IMO]" is visible. On the left side of the interface, there is a sidebar with the title "Encryption" and a cartoon character named "Eve". On the right side, there are several green rectangular boxes containing partial words: "oesntpay", "emand", "word", "fc", "es", "'s", and "f". At the bottom right of the interface, the text "Prof Bill Buchanan" is visible.





Author: Prof Bill Buchanan

Data Hiding



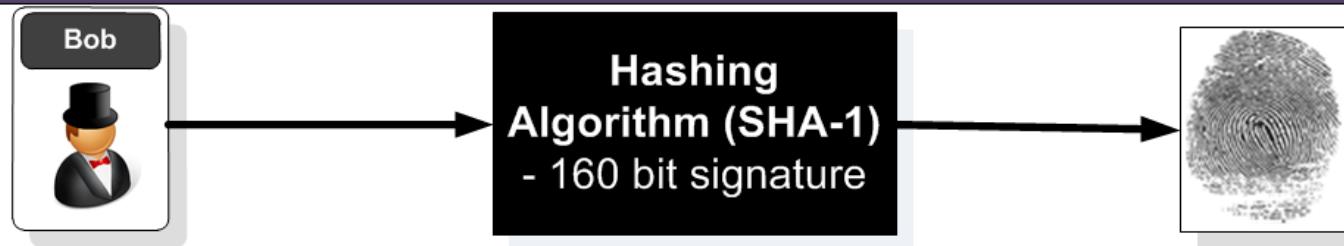
Obfuscation by Hashing



Message Hash	Base-64
hello	XUFAKrxLKna5cZ2REBfFkg
Hello	i xqZU8RhEpaoJ6v4xHgE1w
Hello. How are you?	CysDE5j+zOubCYztTdsFiw
Napier	j4NXH5Mkrk4j13N1MFxHtg

Authentication	Hex
Message Hash	Base-64
hello	5D41402ABC4B2A76B9719D911017C592
Hello	8B1A9953C4611296A827ABF8C47804D7
Hello. How are you?	CC708153987BF9AD833BEBF90239BF0F
Napier	8F83571F9324AE4E23D773753055C7B6

Author: Prof Bill Buchanan



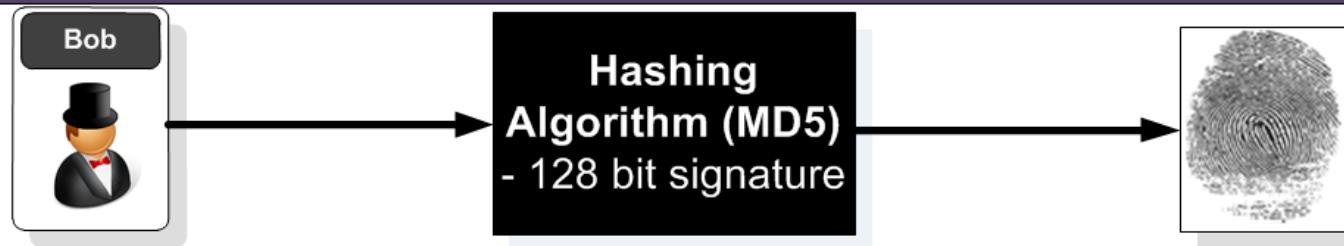
Message	Hash (Base-64)
hello	qVTGHdzF6KLavt4P00gs2a6pQ00=
Hello	9/+ei3uy4Jtwk1pdeF4MxdnQq/A=
Hello. How are you?	Puh2Am76bhjqE51bTwtsqbdFC8=
Napier	v4GxNaVod2b09GR2Tqw4yopOuro=

Base-64

Message	Hash (Hex)
hello	AAF4C61DDCC5E8A2DABEDE0F3B482CD9AEA9434D
Hello	F7FF9E8B7BB2E09B70935A5D785E0CC5D9D0ABF0
Hello. How are you?	3EE876026EFA6E18EA13995B4D6B70B2A6DD142F
Napier	BF81B135A5687766F4F464764EAC38CA8A4EBABA

Hex

Author: Prof Bill Buchanan



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 with physical connections.

8A8BDC3FF80A01917D0432800201CFBF

iovcP/gKAZF9BDKAAGHPVW==

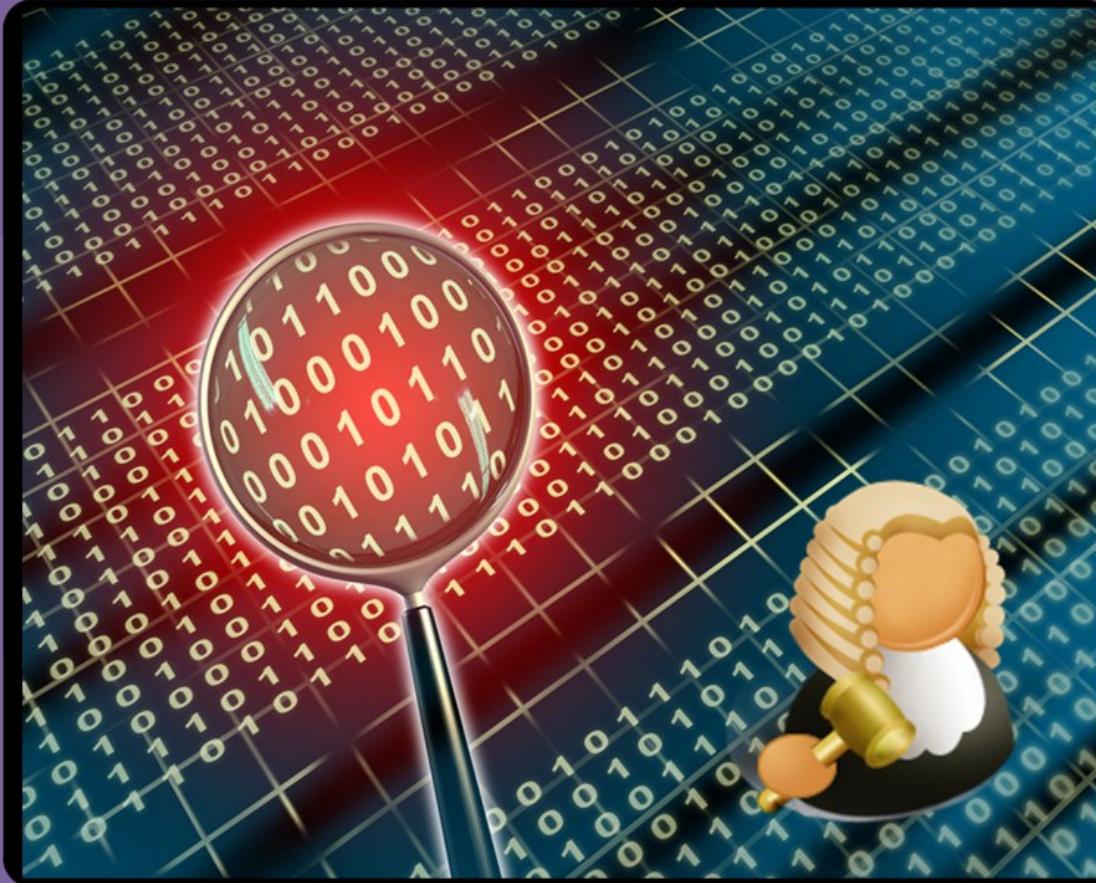
Hex



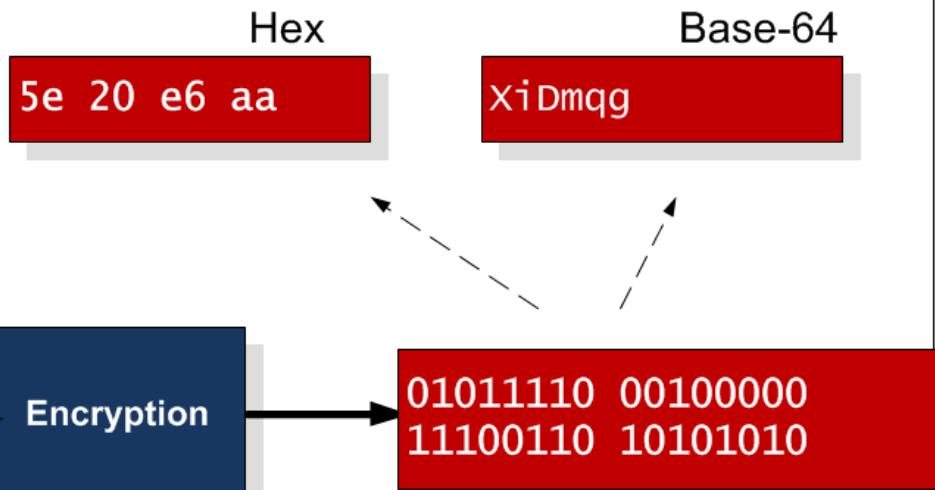
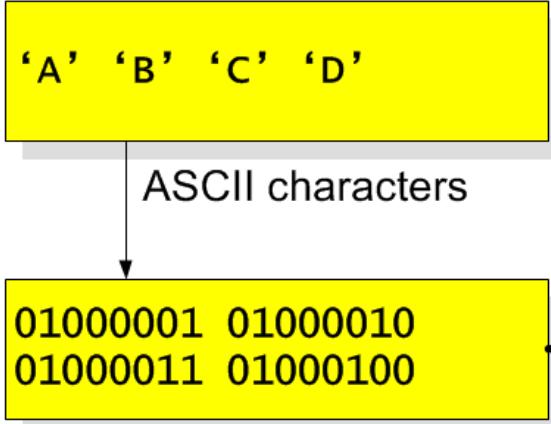
Base-64

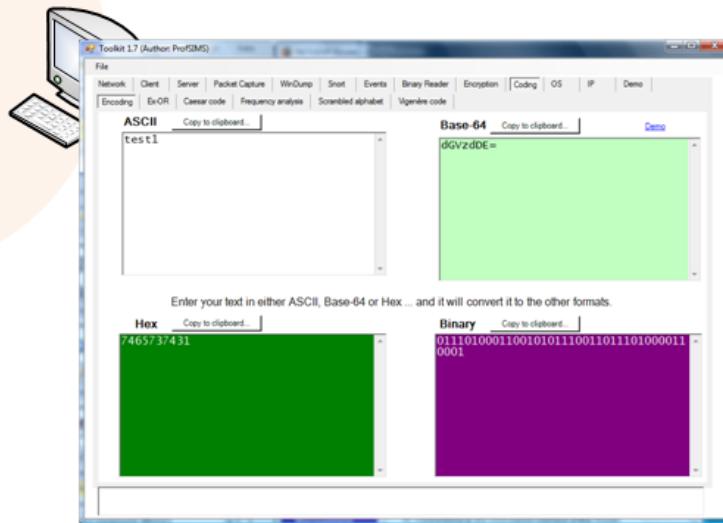
Screenshot of Toolkit 1.7 (Author: ProfSIMS) showing a search for the MD5 hash DAECCF0AD3C1FC8C8015205C332F5B42. The interface includes a navigation bar with Network, Client, Server, Packet Capture, WinDump, Snort, Events, Binary Reader, Encryption, Coding, OS, IP, Demo, Hashing, Hash (Collision), Base-64, Private-key Encr., Private-key Decry., Brute-force, Public key Encr., Public key Decr., Digital Cert., HMAC, and LM tabs. The Hash value field contains the hash DAECCF0AD3C1FC8C8015205C332F5B42. Below it are buttons for Search (MD5) and Search (SHA1). A search bar below shows "apples". The results pane displays "Found..." with the entry "apples [DAECCF0AD3C1FC8C8015205C332F51]". A list of search terms is shown in the bottom-left pane, including "Try appearances", "Try appeared", "Try appearing", "Try appears", "Try apple", "Try apples", and "Found... apples".

Data Hiding



Obfuscation by Encoding





0111 0100 0110 0101 0111 0011 0111 0100 0011
0001

Bit stream

7 4 6 5 7 3 7 4 3 1

Hex

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

Data Hiding

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	/

Bit stream

Base-64

Encoder

Author: Prof Bill Buchanan

Toolkit 1.7 (Author: ProfSMS)

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

Encoding XOR Caesar code Frequency analysis Scrambled alphabet Vigenère code

ASCII Copy to clipboard... Base-64 Copy to clipboard... Demo

hello aGVsbG8=

Enter your text in either ASCII, Base-64 or Hex ... and it will convert it to the other formats.

Hex Copy to clipboard... Binary Copy to clipboard...

68656C6C6F 011010000110010101101100011011000110



hello

01101000 01100101 01101100 01101100

Toolkit 1.7 (Author: ProfSIMS)

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

Encoding Ex-OR Caesar code Frequency analysis Scrambled alphabet Vigenère code

Input text ASCII hello

Ex-OR key [a]

XOR 01100001 01100001 01100001 01100001

ASCII jfl

Base-64 CQQNDQ4=

Hex 09040D0D0E

Copy to reverse

Result hello

Key a

00001001 00000100 00001101 00001101
09 04 0D 0D 0E

01100001 01100001 01100001 01100001

01101000 01100101 01101100 01101100

Data Hiding

Ex-OR

The screenshot shows the Toolkit 1.7 application window titled "Toolkit 1.7 (Author: ProfSIMS)". The menu bar includes File, Network, Client, Server, Packet Capture, WinDump, Snort, Events, Binary Reader, Encryption, Coding, OS, IP, and Demo. The Coding tab is selected, and the Frequency analysis sub-tab is active. The main interface displays the input text "hello" and the frequency analysis results.

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**

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

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 FTQZVQAQFC IKBQP.
 TEABQVPBZVTQP HBMO QT IKBQP GTE AVMQO
 NHVFH BEO VQ YTPZ UBQAOE TG B UBYBAVQ
 BQ BKKVOU GTEFO NTXKU POZXI PIVOP NHT
 VQZEXPVTQP, BQU BQC FTMOEZ BFZVMVZVOP
 FTQFOIZ, NHOEQ 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 VQZEXPVTOP, BQU BQC FTMOEZ BFZVMVZVOP.
 GVAXEO 2.3 VKKXPZEBZOP ZHVP FTQFOIZ, NHOEQ
 VQZEXPVTQ UOZOFZVTQ BAOQZP BEO XPOU ZT KVPZQZ
 ZT QOZNTej ZEBGGVF, BQU QOZNTej/XPOE BFZVMVZC
 ZT ZEC BQU UOZOFZ BQC LEOBFHOP VQ POFXEVZC.

[Try sample English](#)

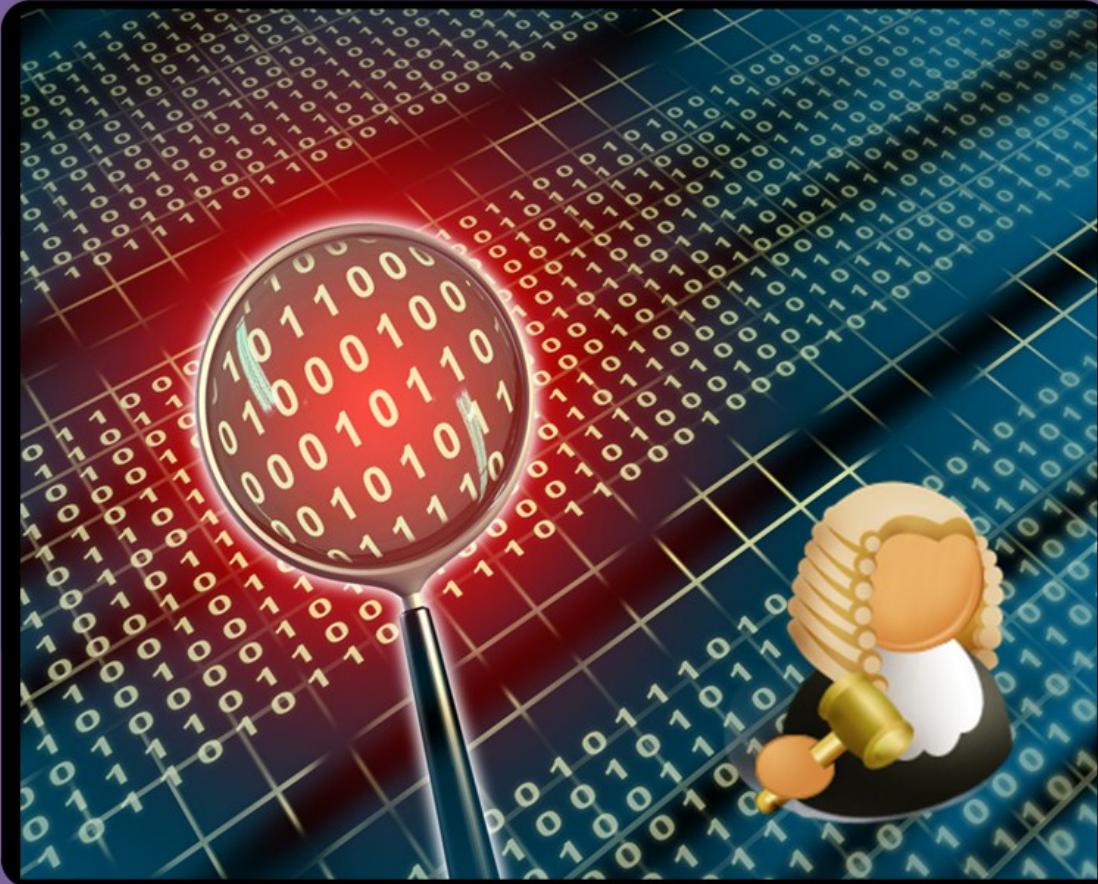
Most prob. Least prob.

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	l	m	j	i	s	w	r	d

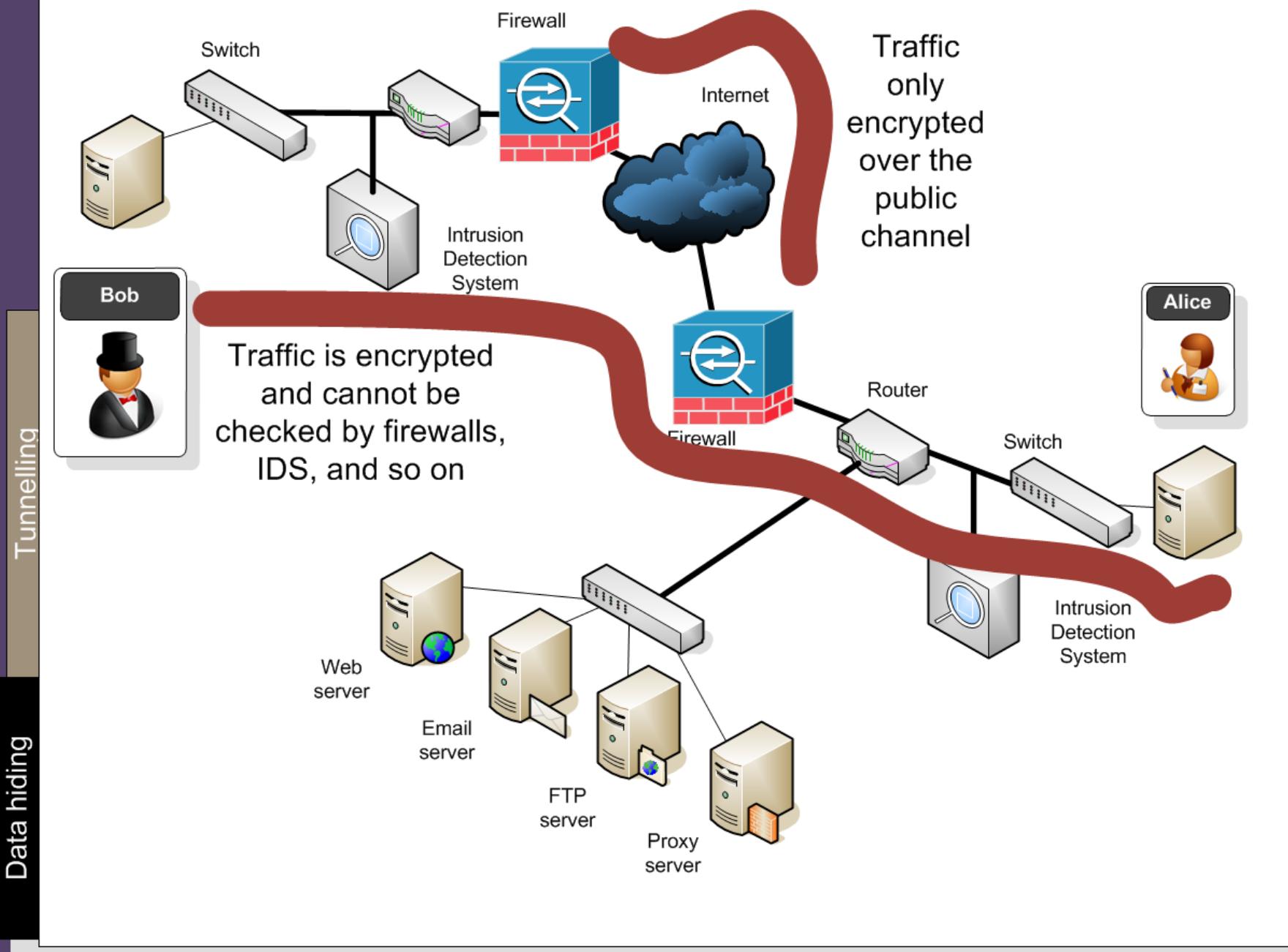
Letter	Occurance
o	145
z	128
b	116
p	104
q	98
v	87
e	70
t	65
h	52
f	51
k	41
c	37
x	36
u	36
g	27
a	25
n	25
y	23
i	20
m	11
j	11
l	9
^	1

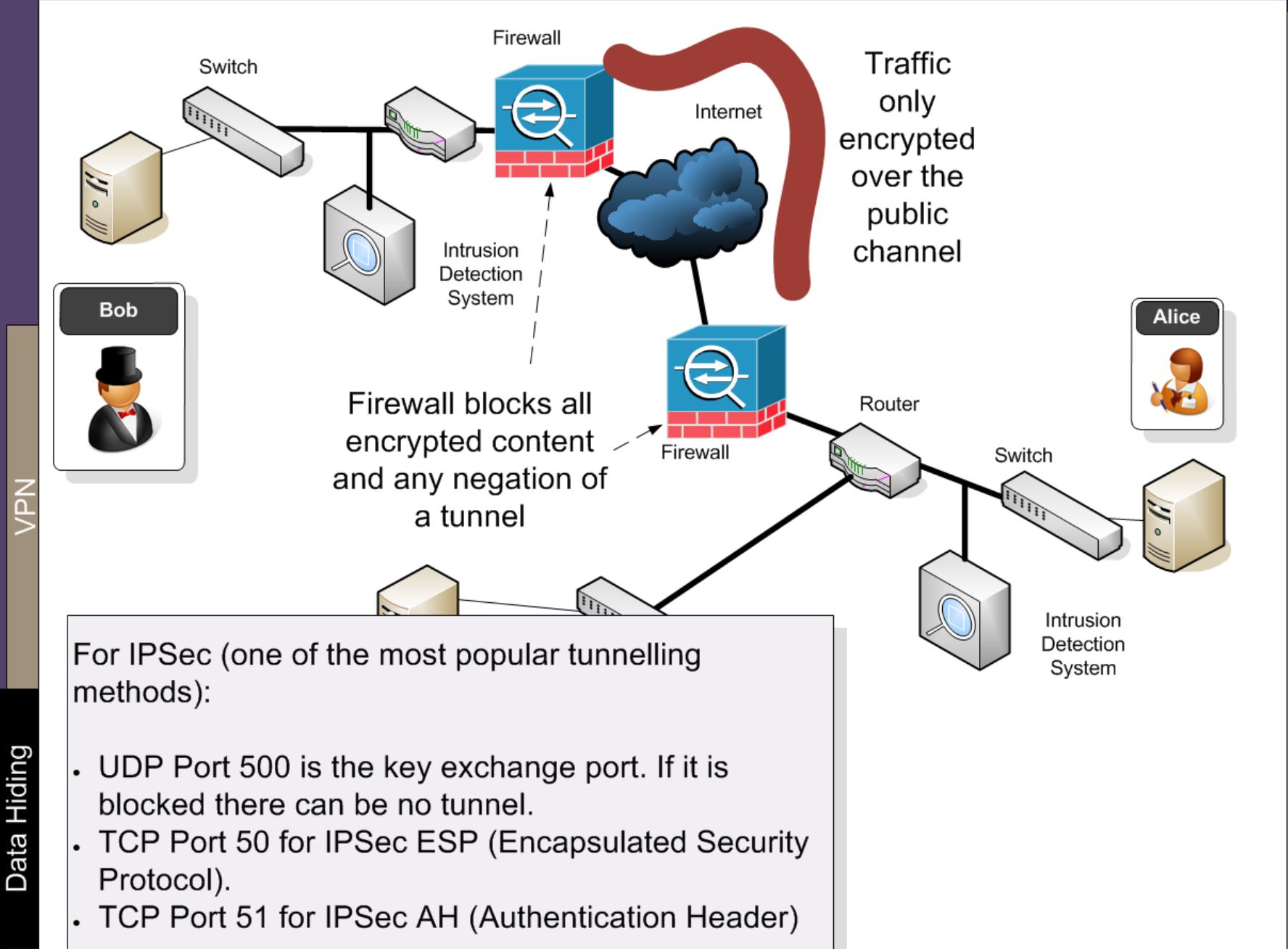
Data Hiding



Obfuscation by
Tunnelling

Data hiding





Switch

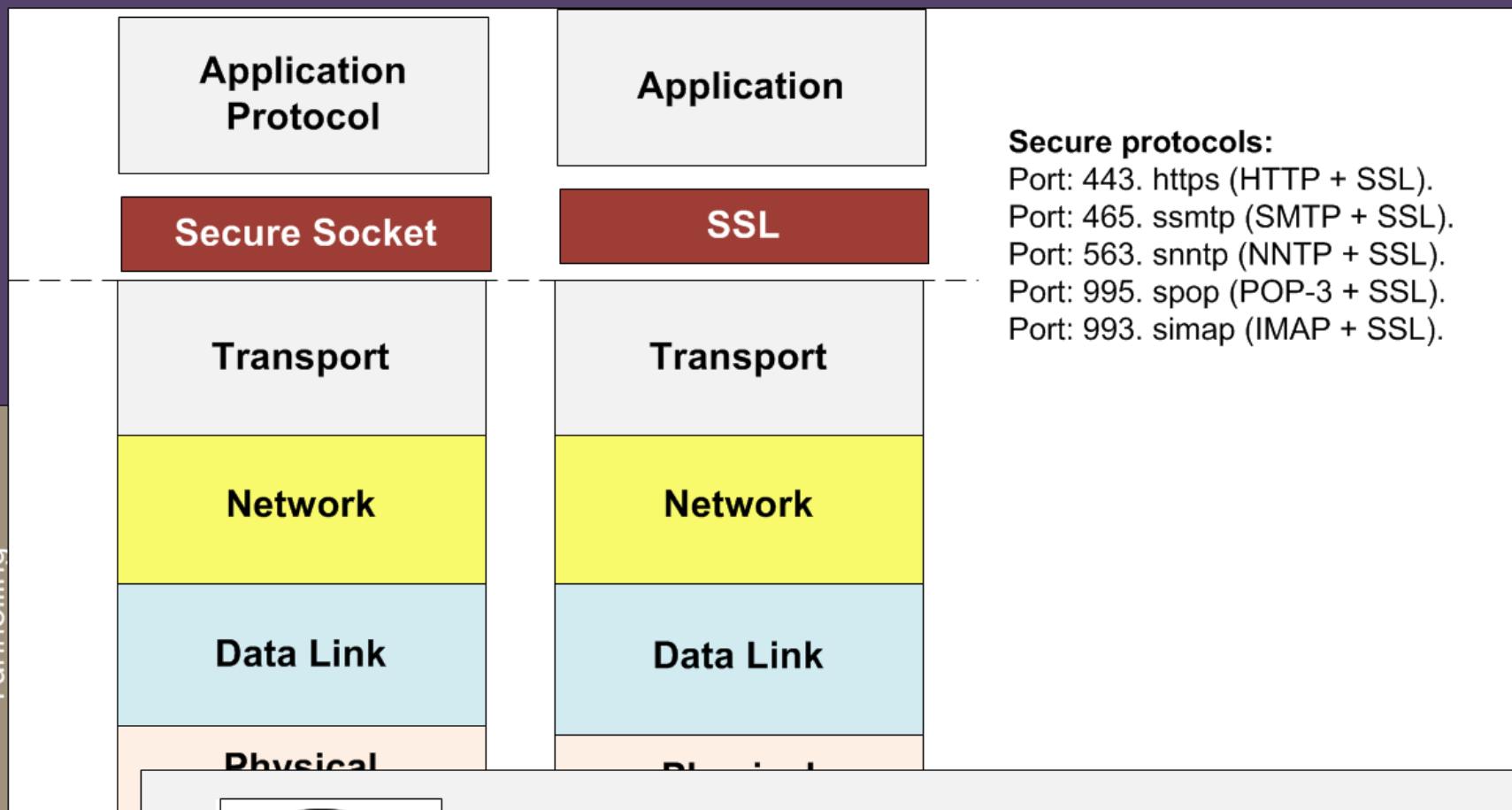
Firewall

Traffic

The screenshot shows the Toolkit 1.7 application window. The title bar reads "Toolkit 1.7 (Author: ProfSIMS)". The menu bar includes File, Network, Client, Server, Packet Capture (selected), WinDump, Snort, Events, Binary Reader, Encryption, Coding, OS, IP, Demo, Open TCPDump, and Packet Capture. Below the menu is a search bar labeled "Enter dump file" with "F:\docs\src\client Toolkit\log\ipsec.pcap" entered. Below the search bar are links: Show tutorial, Show theory, Show demo, View text, and View with Wireshark. The main content area is a table with the following columns: No., Type, Flags, Time, Source IP Address, Source Port, Dest. IP Address, Dest Port, and Content. The table contains 12 rows of UDP traffic. Row 1 shows a UDP packet from 192.168.0.20 to 146.176.210.2 on port 65340. Row 2 shows a UDP packet from 192.168.0.20 to 146.176.210.2 on port 65341. Row 3 shows a UDP packet from 146.176.210.2 to 192.168.0.20 on port 500. Row 4 shows a UDP packet from 192.168.0.20 to 146.176.210.2 on port 65342. Row 5 shows a UDP packet from 192.168.0.20 to 146.176.210.2 on port 65342. Row 6 shows a UDP packet from 146.176.210.2 to 192.168.0.20 on port 4500. Row 7 shows a UDP packet from 192.168.0.20 to 146.176.210.2 on port 65342. Row 8 shows a UDP packet from 146.176.210.2 to 192.168.0.20 on port 4500. Row 9 shows a UDP packet from 192.168.0.20 to 146.176.210.2 on port 65342. Row 10 shows a UDP packet from 192.168.0.20 to 146.176.210.2 on port 65342. Row 11 shows a UDP packet from 146.176.210.2 to 192.168.0.20 on port 4500. Row 12 shows a UDP packet from 146.176.210.2 to 192.168.0.20 on port 57442.

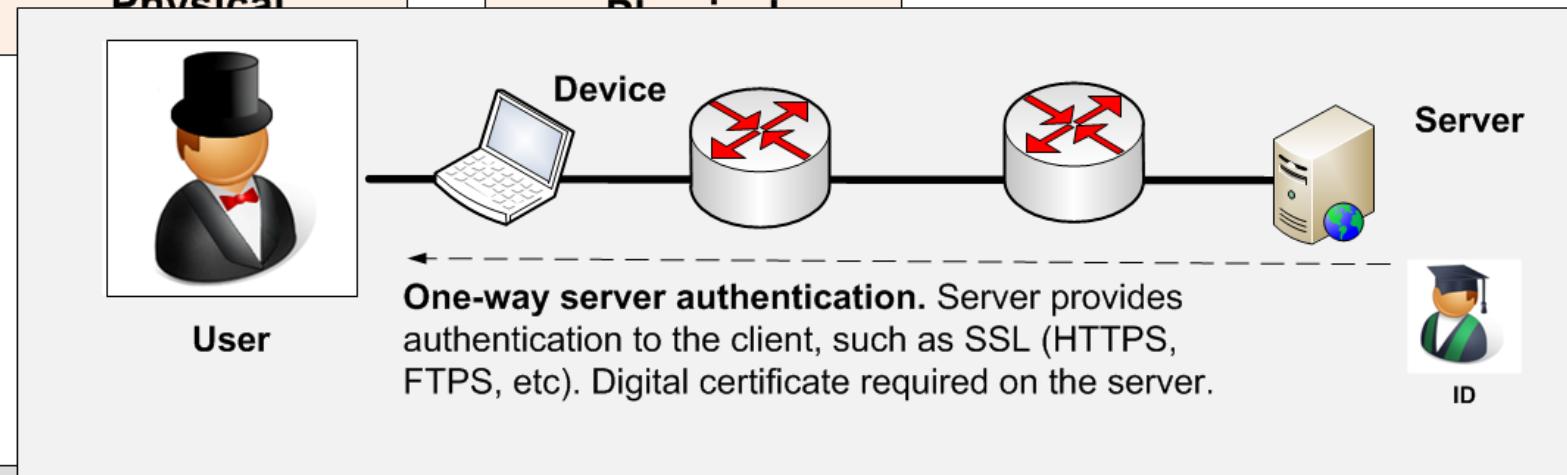
methods):

- 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)



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).



Application Protocol

Application

Secure protocols:

Port: 443. https (HTTP + SSL).

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

[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?l~6~~?~eISS...
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~!??~?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?YY??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??~?#>...

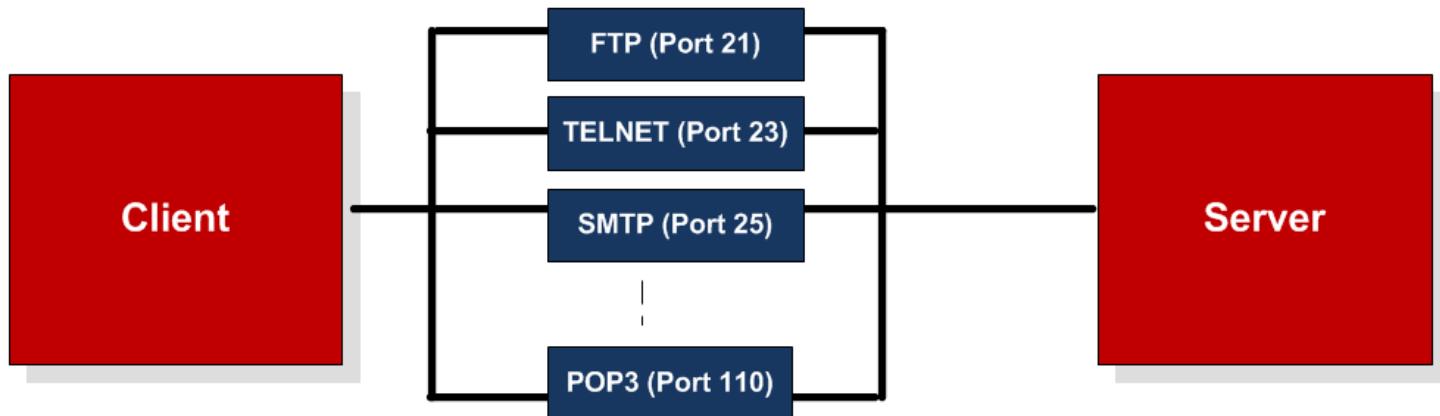


User

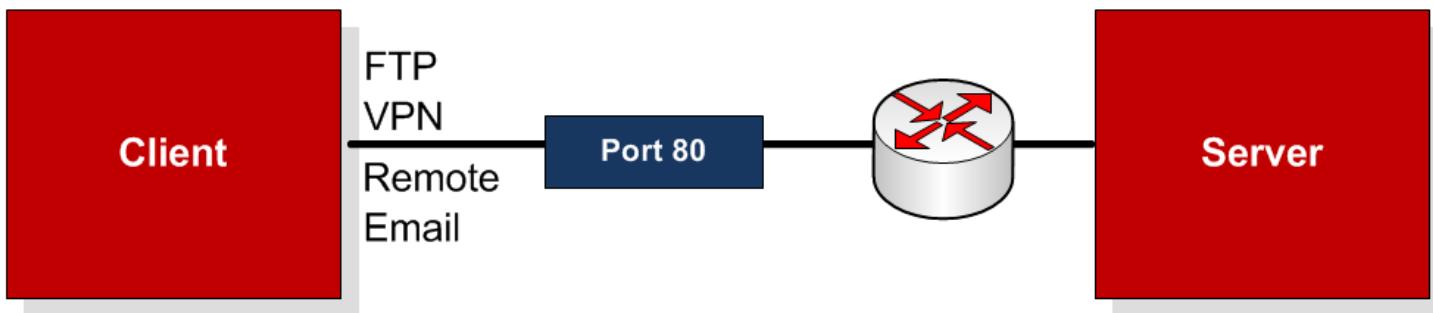


ID

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

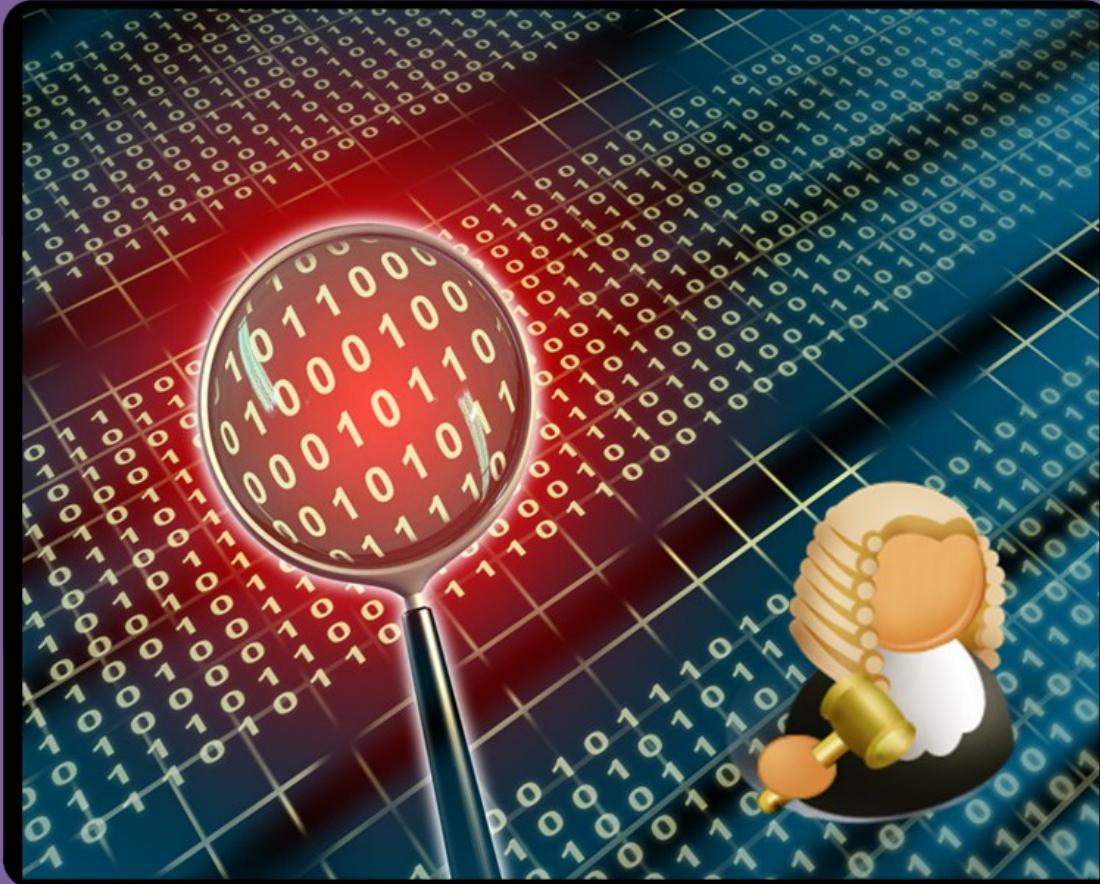


Applications use a wide range of TCP ports to communicate. Each of these ports could be blocked.

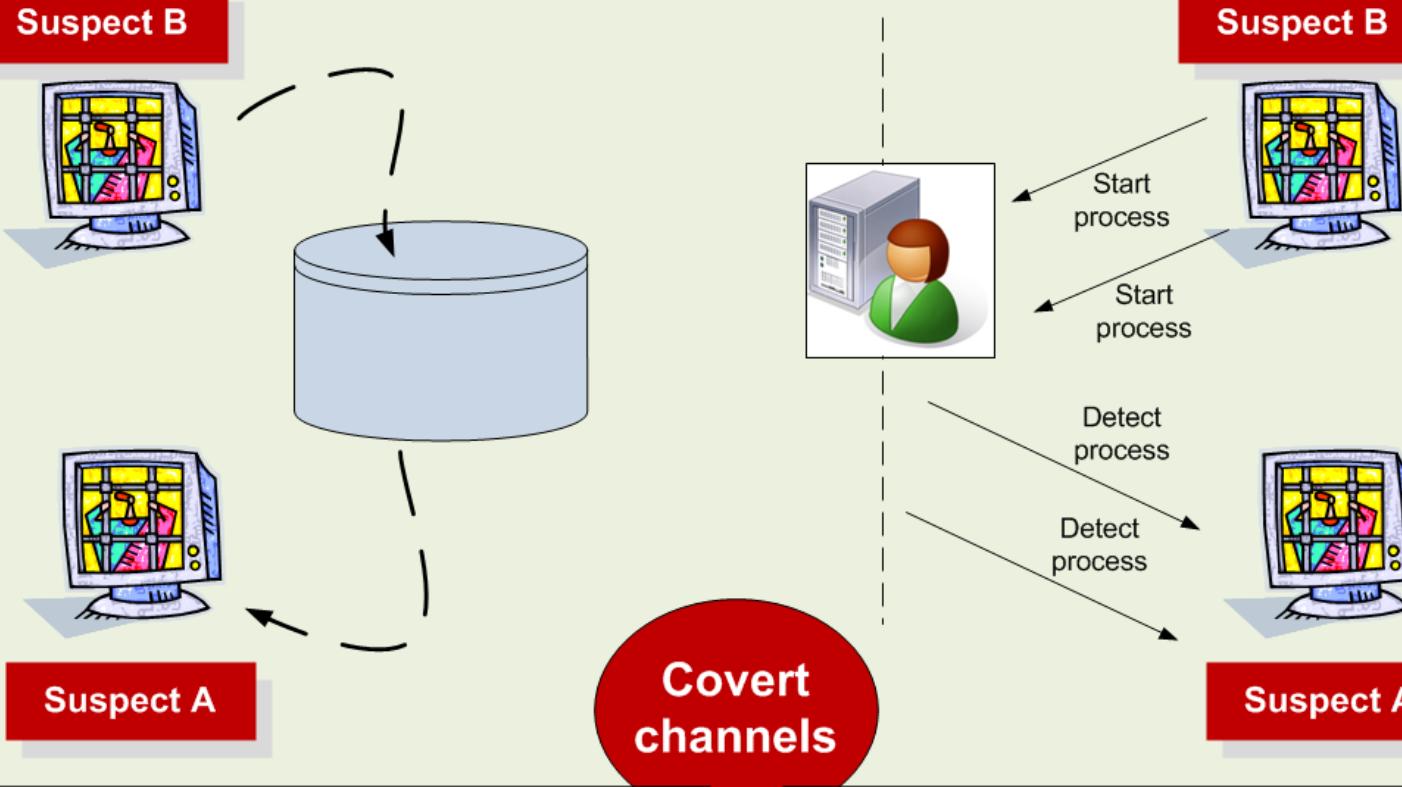


Applications communicate for a wide range of services through port 80 (Web port)... port 80 traffic is allowed through the firewall ... but can cause security problems as the firewall cannot check the usage

Data Hiding

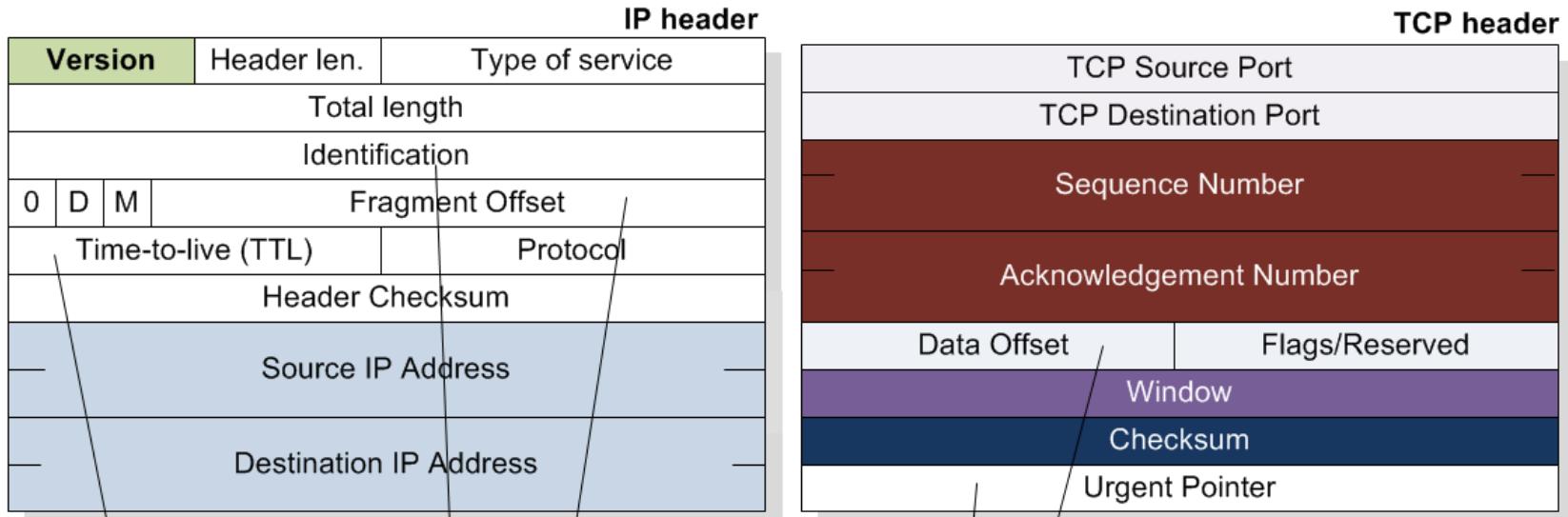


Covert Channels



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.



Covert Channels

Forensic

Police

Police



Fragment Offset

Urgent Pointer

Time-to-live (TTL)

Data Offset

Identification

Possible Covert Channel Fields

Author: Prof Bill Buchanan



Version	Header len.	Type of service
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)					

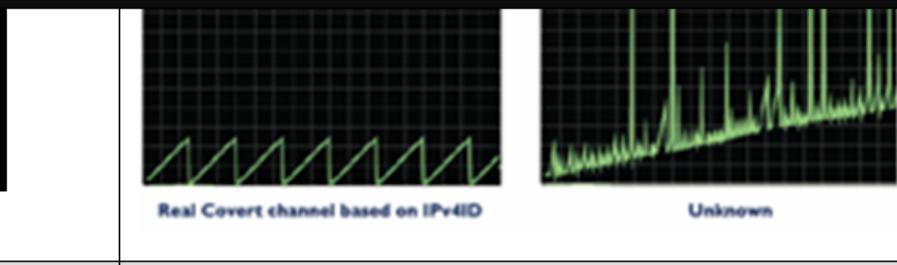
No.	Time	Source	Destination	Protocol	Info
7	8.968288	192.168.75.132	192.168.75.1	TCP	afrog >
http [SYN] Seq=0 Win=64240 Len=0 MSS=1460					
Identification: 0x008f (143)					

.... 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



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)

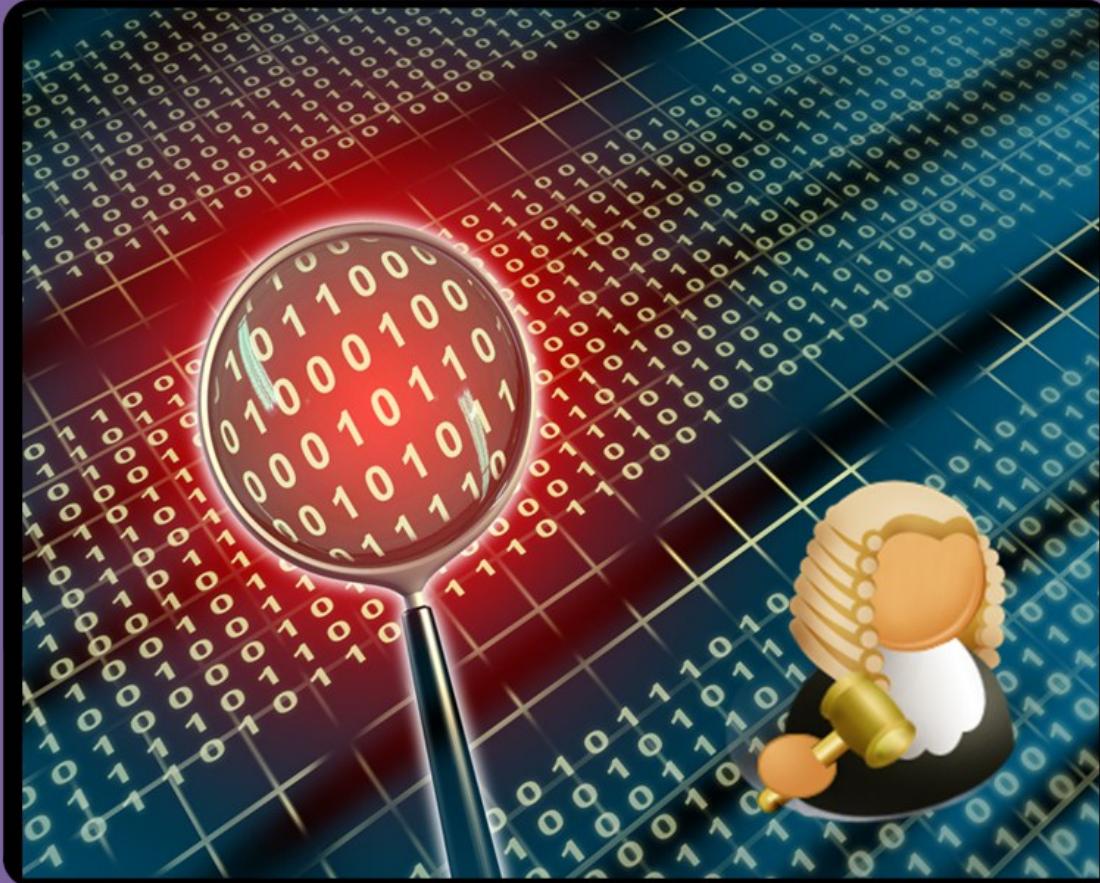
No.	Time	Source	Destination	Protocol	Info
55	23.979951	192.168.75.138	192.168.75.1	TCP	54065 > icslap [SYN]
Seq=0	Win=5840	Len=0	MSS=1460	TSV=18847	TSER=0 WS=5

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

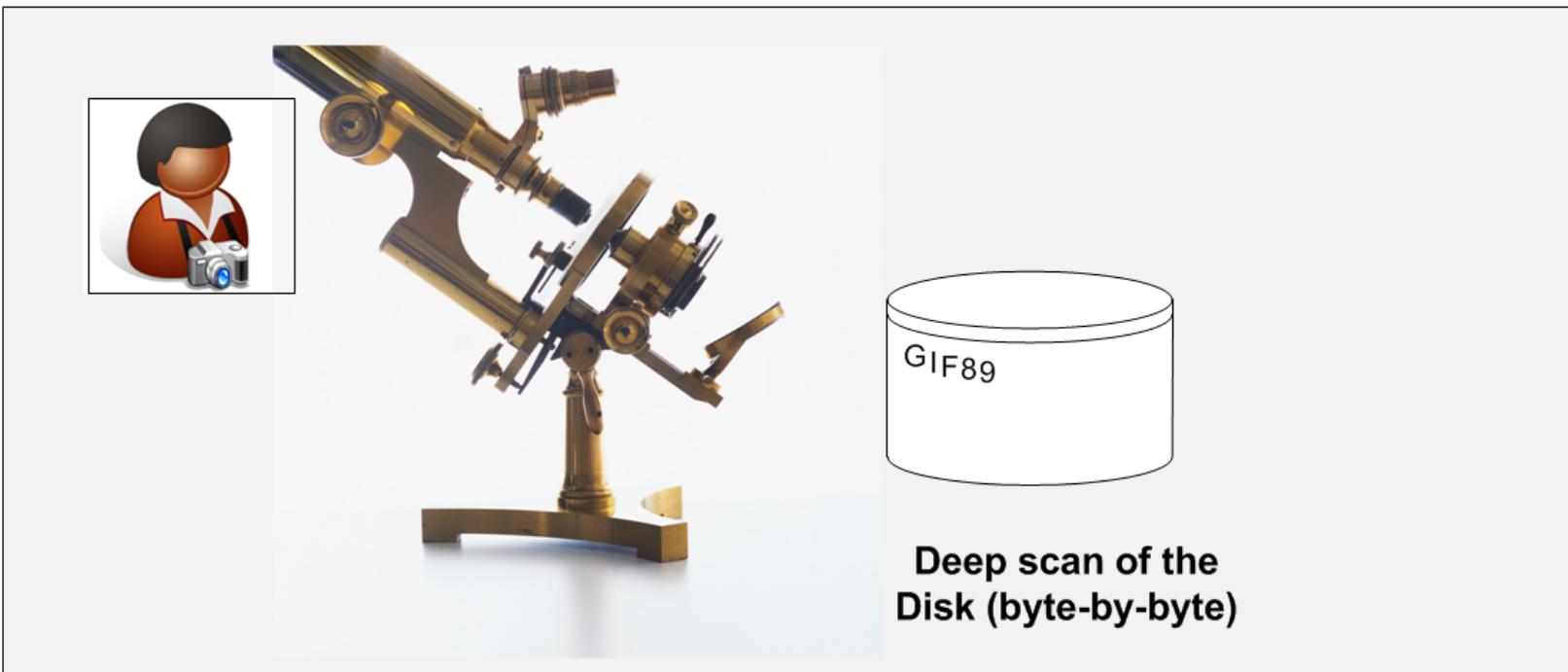


File Signatures

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



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





Mypic.gif



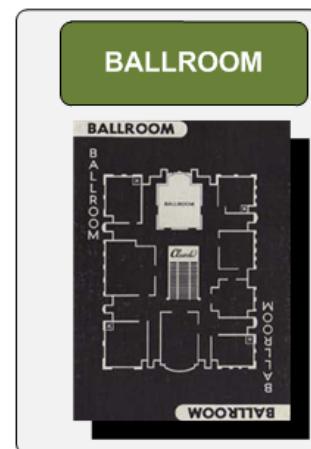
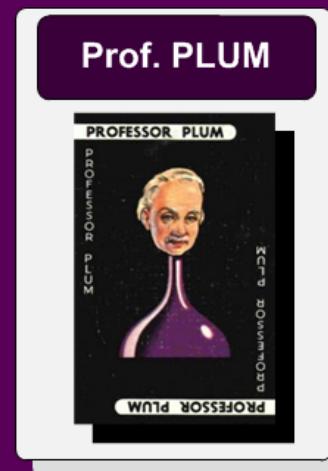
Mypic.dll

Change name from:

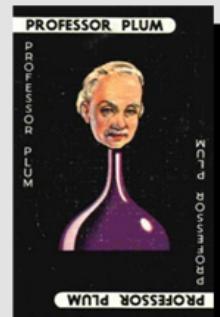
Mypic.gif

To

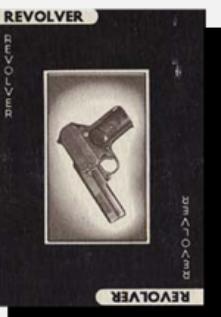
Mypic.dll

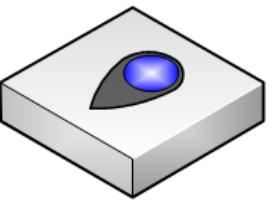


Prof. PLUM



REVOLVER





Sig

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

File ext

*.gif
 *.gif
 *.jpg
 *.jpg
 *.zip
 *.pdf
 *.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 - Tutorial

F:\docs\src\clientToolkit\F:\08009817.pdf

Identify file type

Hex viewer

```

00 25 50 44 46 2D 31 2E 35 0D 0A 25 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 6B 49 6E 66
60 6F 3C 3C 2F 4D 61 72 6B 65 64 20 74 72 75 65 3E
70 3E 3E 00 0A 65 6E 64 6F 62 6A 0D 0A 32 20 30
80 20 6F 62 6A 0D 04 3C 3C 2F 54 79 70 65 2F 50 61
90 67 65 73 2F 43 6F 75 6E 74 20 32 2F 4B 69 64 73
A0 5B 20 33 20 30 20 52 20 31 31 20 30 20 52 5D 20
B0 3E 3E 00 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
10 30 20 52 2F 46 33 20 39 20 30 20 52 3E 3E 2F 50
20 72 6F 63 53 65 74 5B 2F 50 44 46 2F 54 65 78 74
30 2F 49 6D 61 67 65 42 49 6D 61 67 65 43 2F 49
40 6D 61 67 65 49 50 20 3E 3E 2F 4D 65 64 69 61 42

```

Char viewer

```

% P O F . 1 . 5 . . %
. 1 0 o b j . . <
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 t
> > . . e n d o b j
o b j . . < < / T y
g e s / C o u n t 2
[ 3 0 R 1 1
> > . . e n d o b j .
o b j . . < < / T y p e
e / P a r e n t 2
r 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 g l ] > > / M

```

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 - Tutorial

F:\docs\src\clientToolkit\F:\docs\src\clientToolkit\log\barcode.zip

Identify file type

Hex viewer

```

00 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 00 00 0C 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 50 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 60 81 DA 93 33 78 89 52 F3
80 52 F4 A4 00 50 4B 03 04 14 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 A7 DC 54 0C D5 08 BD
C0 28 39 F6 38 24 6D 17 09 D8 35 6E 12 FB FB 55 82
D0 0D 75 2F 33 3B 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
2 C9 A6 69 FA 53 DC 76 EA 96 D2 13 59 C9 BA 90 F5
3 8F 50 25 DF 96 47 E5 43 C6 C3 84 45 7E 5F 82 59
4 F5 04 E8 79 42 70 E3 78 7E 3A 38 3E 08 F8 BA 5E

```

Char viewer

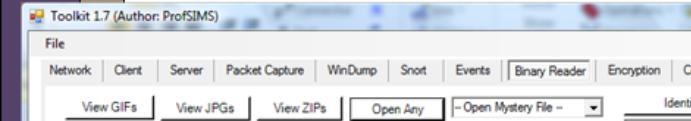
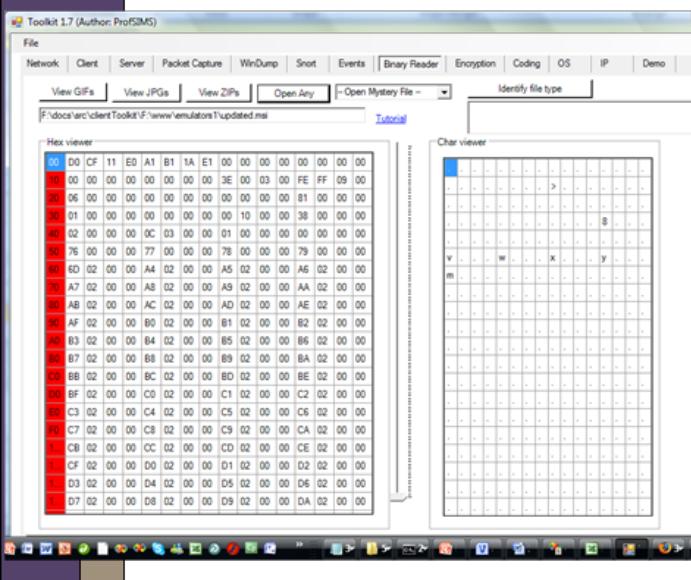
```

P K . . . . . . e 8 . ! . 2
. Z . . . d . . . . . P R
O G 2 _ 0 2 . P A S + ( . 0 / J
. U ( . . F . . . y . . % . .
. % @ J . . . + ) 5 = 3 . . K .
. . 2 K R 5 . ] . J R . . .
. . s J S . . . . R . 3 . K .
. . S . A Z . j . . . 3 x . R .
R . . P K . . . . . . b
$ ! . . . . . . . . . .
. . P R O G 1 _ 2 . P A S ] . .
. . 0 . D . B . . . . T . .
( 9 . . $ m . . . 5 n . . . U .
. . u / 3 ; 0 . ] K . H . . . r
. . A . . . . Y . . . U .
. . g . . . p . . . % . q . .
@ O [ . F & . . 0 . . . . N
. . i . S . v . . . Y . . .
P % . . G . C . . . E . . . Y
. . y B p . x : 8 > . . ^

```

Data

File signature



Sig	File ext	File type
0x006E1EF0	*.ppt	PPT
0xA0461DF0	*.ppt	PPT
0xECA5C100	*.doc	Doc file
0x000100005374616E64617264204A6574204442	*.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
0x504B030414000600	*.docx	Microsoft DOCX file
0x504B030414000600	*.pptx	Microsoft PPTX file
0x504B030414000600	*.xlsx	Microsoft XLSX file

This screenshot shows the Toolkit 1.7 interface with a third file. The main window title is "Toolkit 1.7 (Author: ProfSIMS)". The menu bar and toolbar are identical. The status bar at the bottom displays the path F:\docs\arc\client\Toolkit\I:\Request.mdb and a Tutorial link. The main area contains two panes: a "Hex viewer" on the left showing binary data and a "Char viewer" on the right showing ASCII characters.

Access to the path 'C:\Documents and Settings' is denied.
Access to the path 'C:\Documents and Settings' is denied.
Access to the path 'C:\Documents and Settings' is denied.

Access to the path 'C:\Documents and Settings' is denied.
Access to the path 'C:\Documents and Settings' is denied.
Access to the path 'C:\Documents and Settings' is denied.

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.

