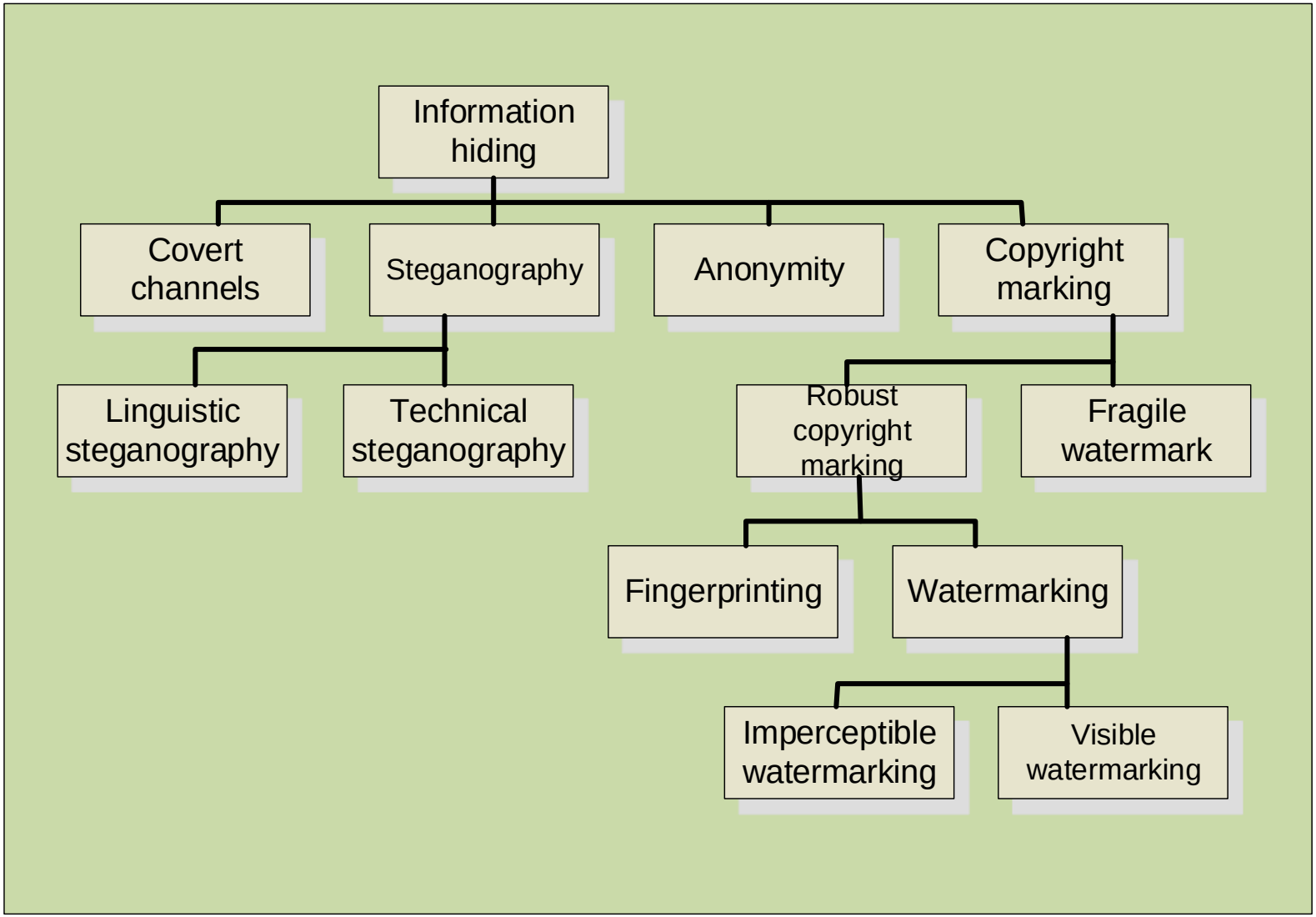
Steganography

- Some methods.
- Discriminators.
- Covert channels.
- Port knocking.
- Onion Routing.
- Dictionary.

Author: Prof Bill Buchanan



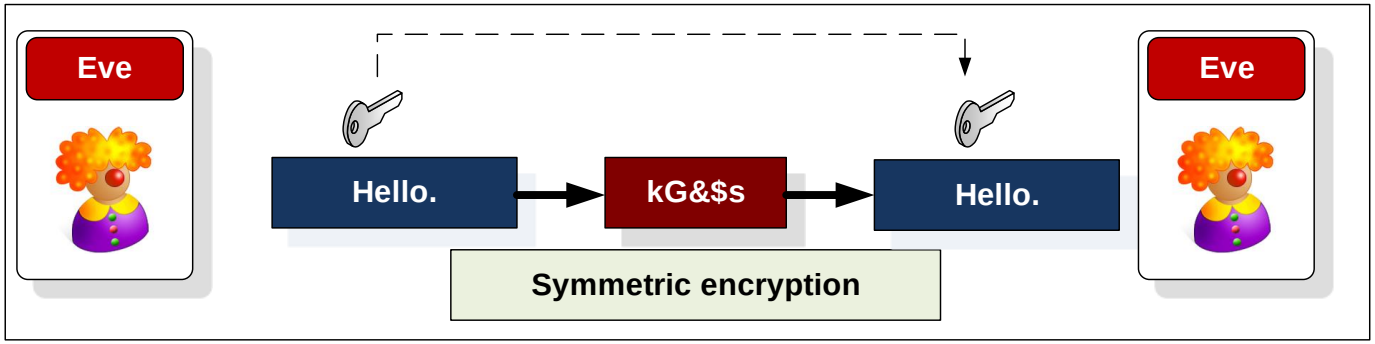
Data hiding

Forensic

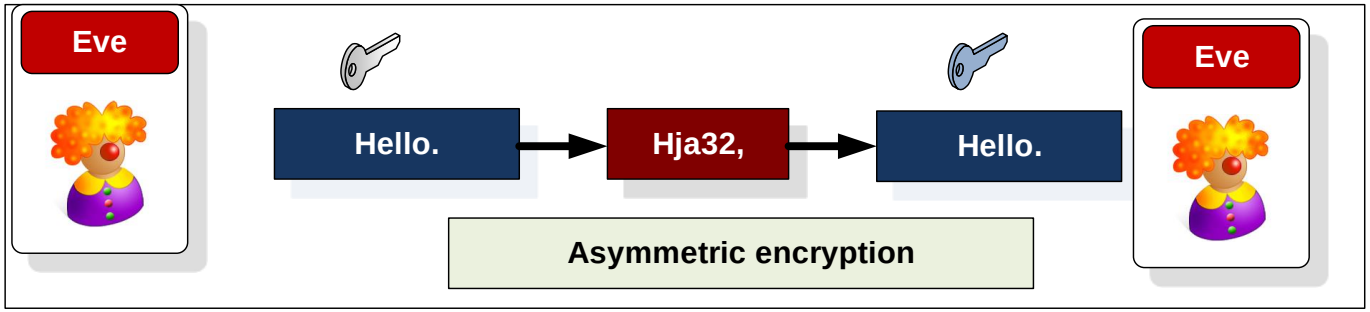
Author: Prof Bill Buchanan

Encryption

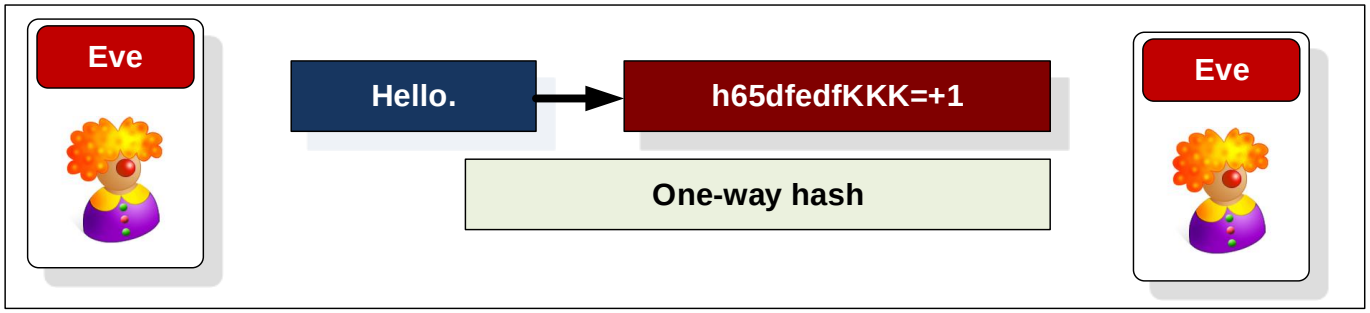
Data Hiding



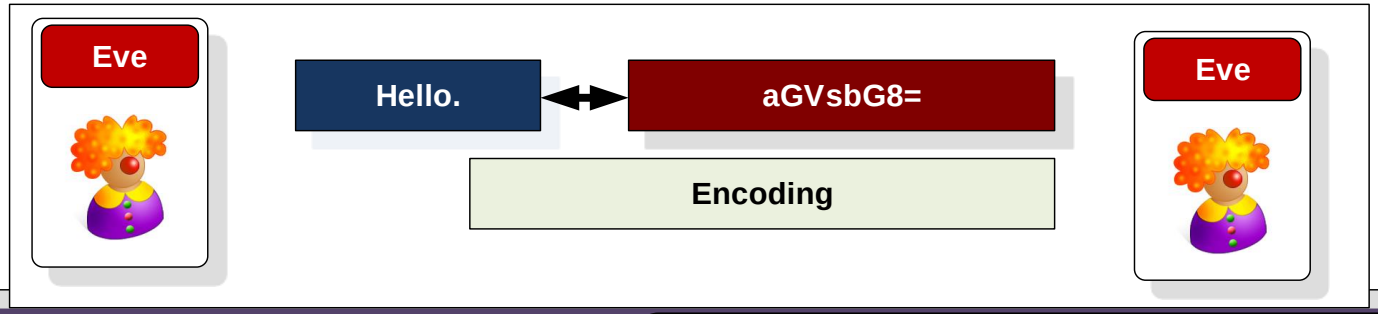
Private-key:
RC2, RC4, DES, 3DES, AES



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



Hashing:
MD5, SHA-1



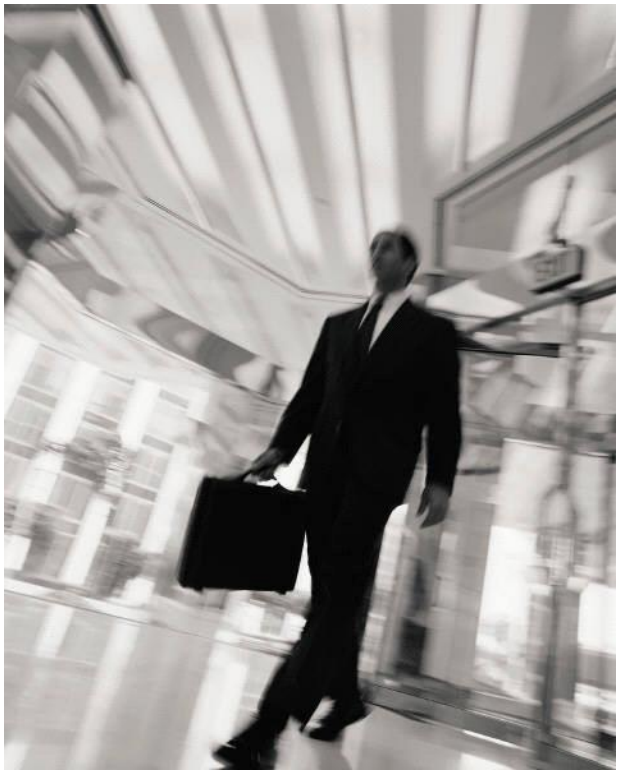
Encoding:
Hex, Base-64, ASCII, UTF-16

Author: Prof Bill Buchanan

Data Hiding

Covert channels have been used by secret operations for a long time,
such as:

- Passing a briefcase in a busy place.
- Hiding microfilms in objects.
- Using templates for typewritten text.



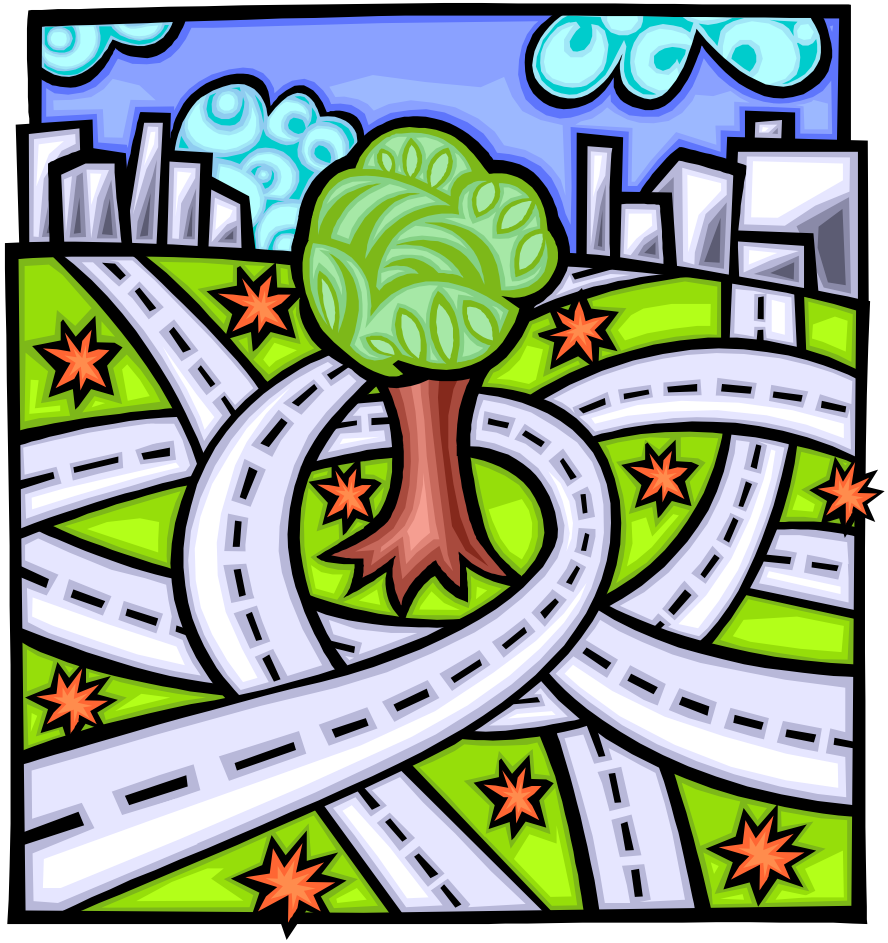
Let everyone tango. This has Edward's mind in some simple inquiry of nothing, before everyone gets into Nirvana.

What's the hidden message in this text? You have 1 minute to find it…

Let **e**veryone **t**ango. **T**his **h**as **E**dward's **m**ind **i**n **s**ome **s**imple **i**nquiry **o**f **n**othing, **b**efore **e**veryone **g**ets **i**nto **N**irvana.

Let the Mission Begin

With the Internet, we now have electronic communications, and sophisticated monitoring equipment…

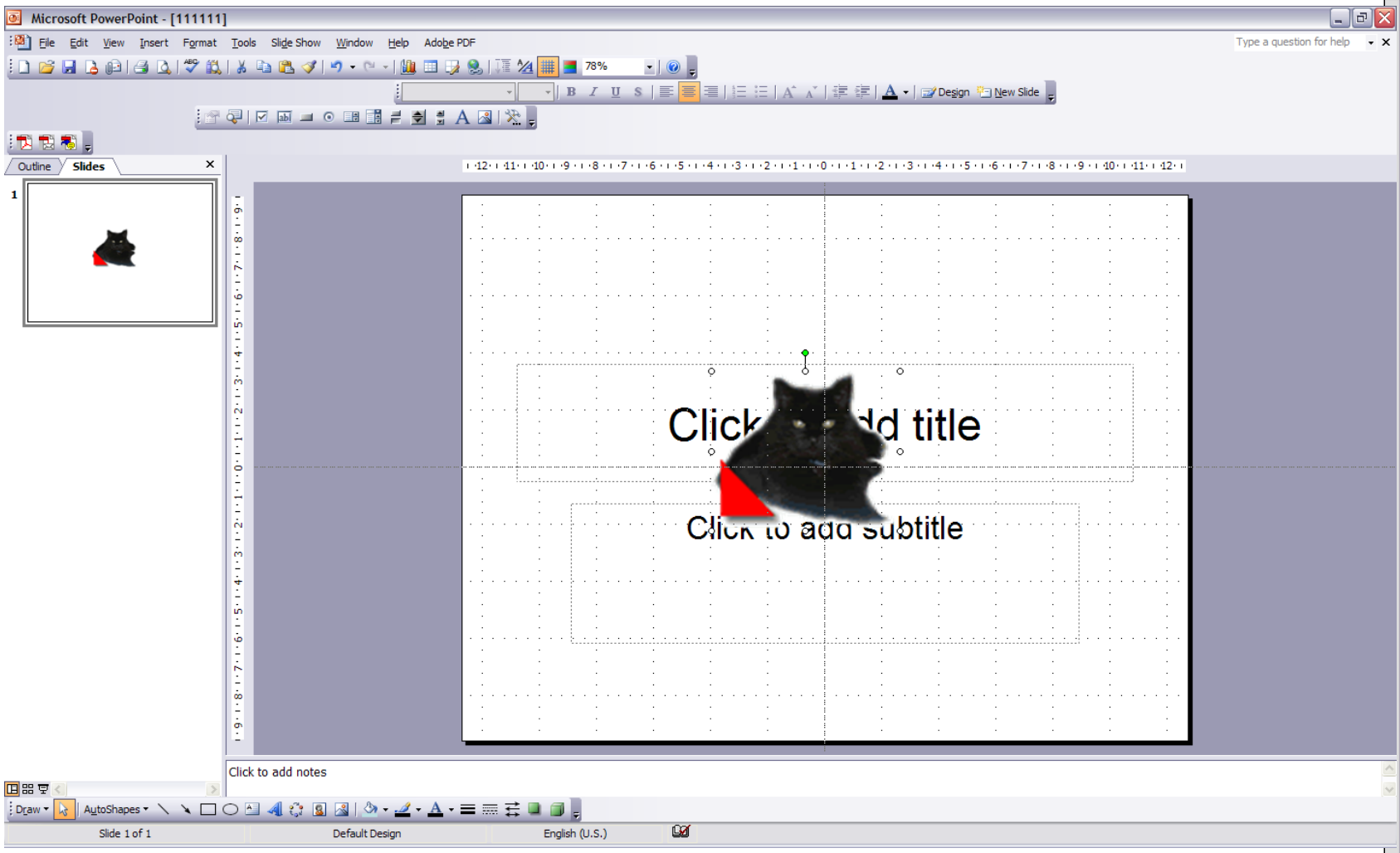


Author: Prof Bill Buchanan

Data Hiding

Author: Prof Bill Buchanan

Author: Prof Bill Buchanan



Author: Prof Bill Buchanan

Microsoft PowerPoint - [111111]

File Edit View Insert Format Tools Slide Show Window Help Adobe PDF

Outline Slides

111111.ppt - HHD Software Free Hex Editor

File Edit Tools Select Window Help

c:\111111.ppt

Hex

```
00002000:  00 00 00 10 f0 08 00 00 00 3e 05 b0 01 d0 14 dc    .....ð....>.°.Ð.Ü
00002010:  08 0f 00 11 f0 10 00 00 00 00 00 c3 0b 08 00 00    ....ð......Ã....
00002020:  00 00 00 00 00 0f 00 93 00 0f 00 0d f0 0c 00 00    .......“....ð...
00002030:  00 00 00 9e 0f 04 00 00 00 00 00 00 00 0f 00 04    ...ž............
00002040:  f0 72 00 00 00 12 00 0a f0 08 00 00 00 03 08 00    ðr......ð.......
00002050:  00 20 02 00 00 53 00 0b f0 1e 00 00 00 7f 00 00    . ...S..ð....□..
00002060:  00 04 00 80 00 34 02 52 07 bf 01 01 00 01 00 ff    ...€.4.R.¿.....ÿ
00002070:  01 01 00 01 00 01 03 03 04 00 00 00 00 10 f0 08    ..............ð.
00002080:  00 00 00 90 09 60 03 20 13 e0 0d 0f 00 11 f0 10    ...□.`. .à....ð.
00002090:  00 00 00 00 00 c3 0b 08 00 00 00 01 00 00 00 10    .....Ã..........
000020a0:  00 52 07 0f 00 0d f0 0c 00 00 00 00 00 9e 0f 04    .R....ð......ž..
000020b0:  00 00 00 01 00 00 00 0f 00 04 f0 82 00 00 00 b2    ..........ð,...²
000020c0:  04 0a f0 08 00 00 00 04 08 00 00 00 0a 00 00 43    ..ð............C
000020d0:  00 0b f0 5a 00 00 00 7f 00 80 00 80 00 04 41 01    ..ðZ...□.€.€..A.
000020e0:  00 00 00 05 c1 42 00 00 00 06 01 01 00 00 00 70    ....ÁB.........p
000020f0:  00 69 00 63 00 73 00 5f 00 63 00 6f 00 6f 00 6b    .i.c.s._.c.o.o.k
00002100:  00 69 00 65 00 5f 00 74 00 72 00 61 00 6e 00 73    .i.e._.t.r.a.n.s
00002110:  00 70 00 61 00 72 00 65 00 6e 00 74 00 5f 00 33    .p.a.r.e.n.t._.3
00002120:  00 32 00 63 00 6f 00 6c 00 6f 00 72 00 73 00 00    .2.c.o.l.o.r.s..
00002130:  00 00 00 10 f0 08 00 00 00 71 07 14 0a 6c 0c 6f    ....ð....q...l.o
00002140:  09 0f 00 04 f0 48 00 00 00 12 00 0a f0 08 00 00    ....ðH......ð...
00002150:  00 01 08 00 00 00 0c 00 00 83 00 0b f0 30 00 00    .........ƒ..ð0..
00002160:  00 81 01 00 00 00 08 83 01 05 00 00 08 93 01 8e    .□.....ƒ.....“.Ž
00002170:  9f 8b 00 94 01 de bd 68 00 bf 01 12 00 12 00 ff    Ÿ‹.”.Þ½h.¿.....ÿ
00002180:  01 00 00 08 00 04 03 09 00 00 00 3f 03 01 00 01    ...........?....
```

Ready | Pos. 0x00002000 of 0x00008000 | No selection | OVR

Draw AutoShapes

Slide 1 of 1

Data Hiding

Author: Prof Bill Buchanan

Digital

Steganography

Use Noise

Spreading out information

Define a structural profile eg make it look like a normal document by hide information

```
Man Utd 0 Man City 1
Celtic 1 Aberdeen 0
Liverpool 1 Stoke City 0
Hearts 0 Hibs 0
```

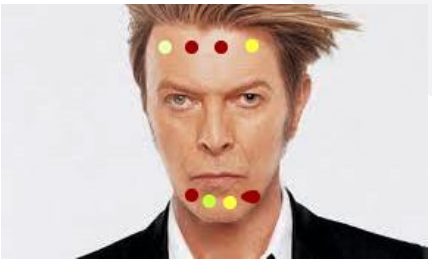
Define a statistical profile eg trick computer for statistical analysis

```
Help Everyone and Leave
Lots of Opportunity
```

Change the order eg order of a shopping list

Replace randomness eg add imperfections in places in a picture

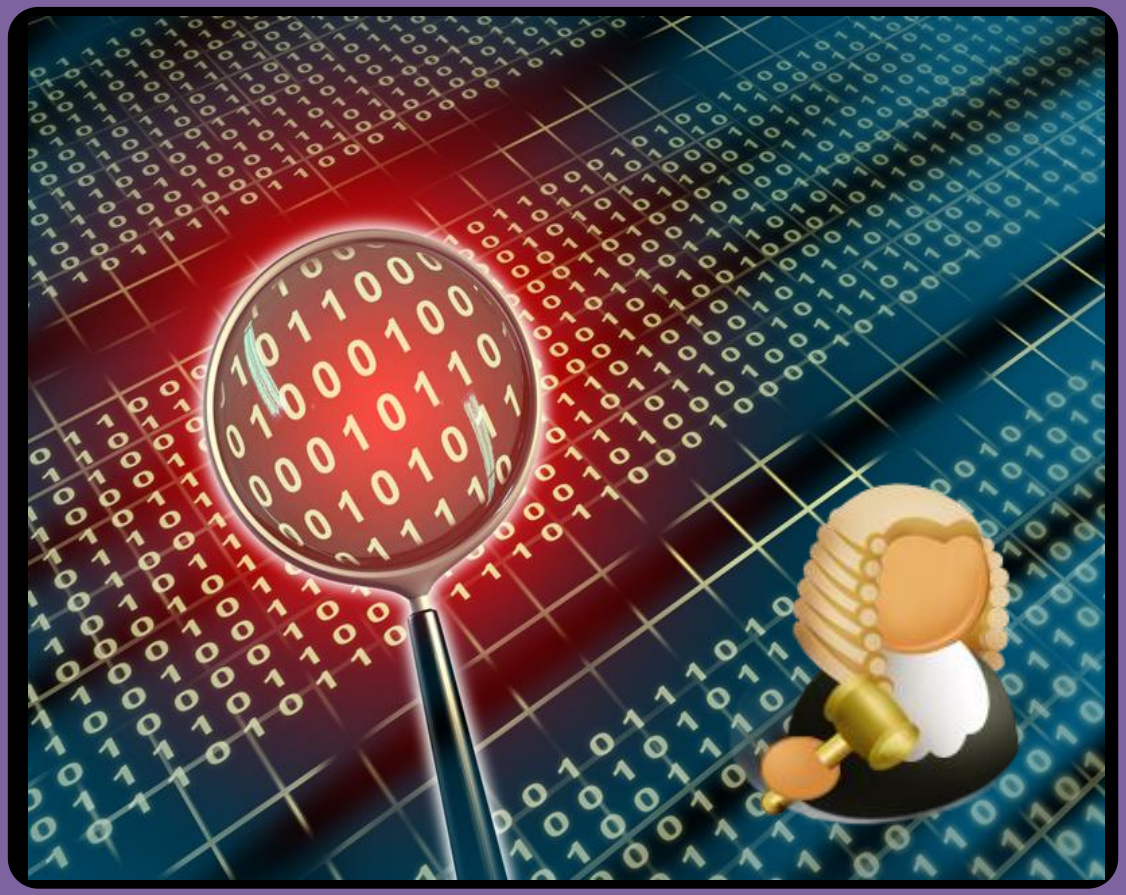
Split information eg first word on every page



Hide the souce eg Tor Onion Routing

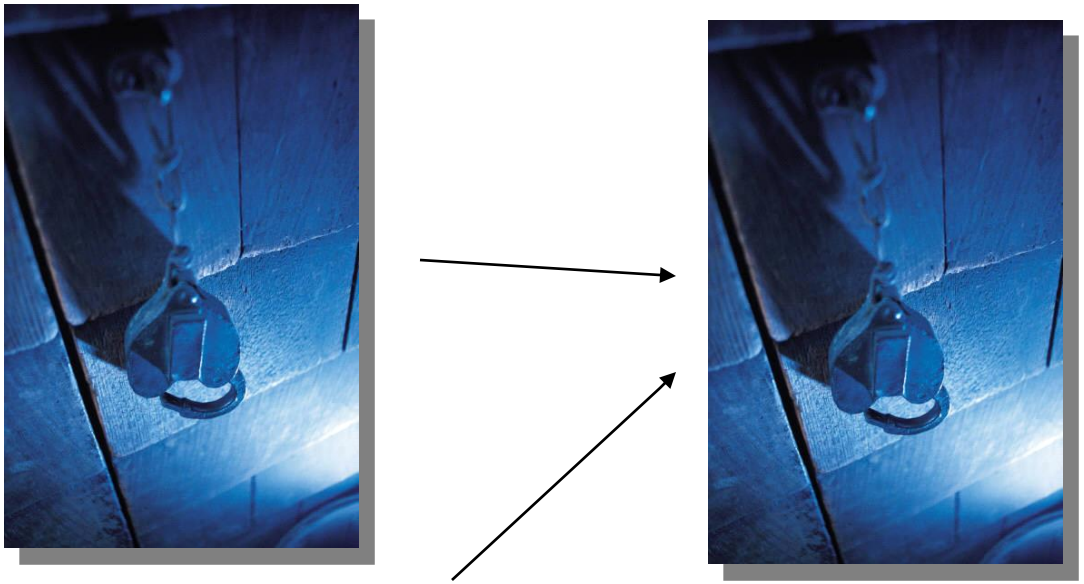
Methods

Data Hiding



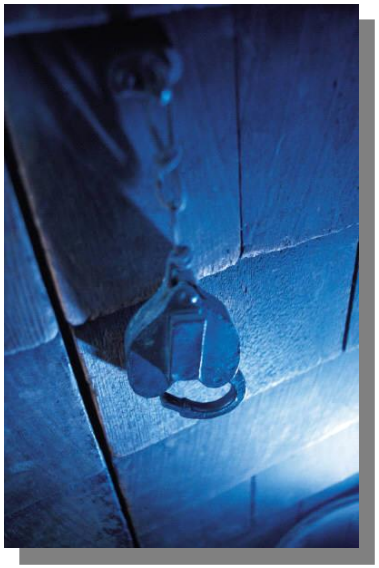
JPEG Data Hiding

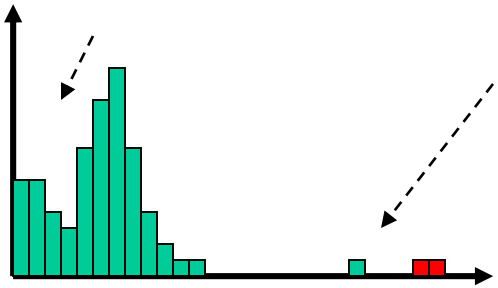
Author: Prof Bill Buchanan



Hello. How are You?

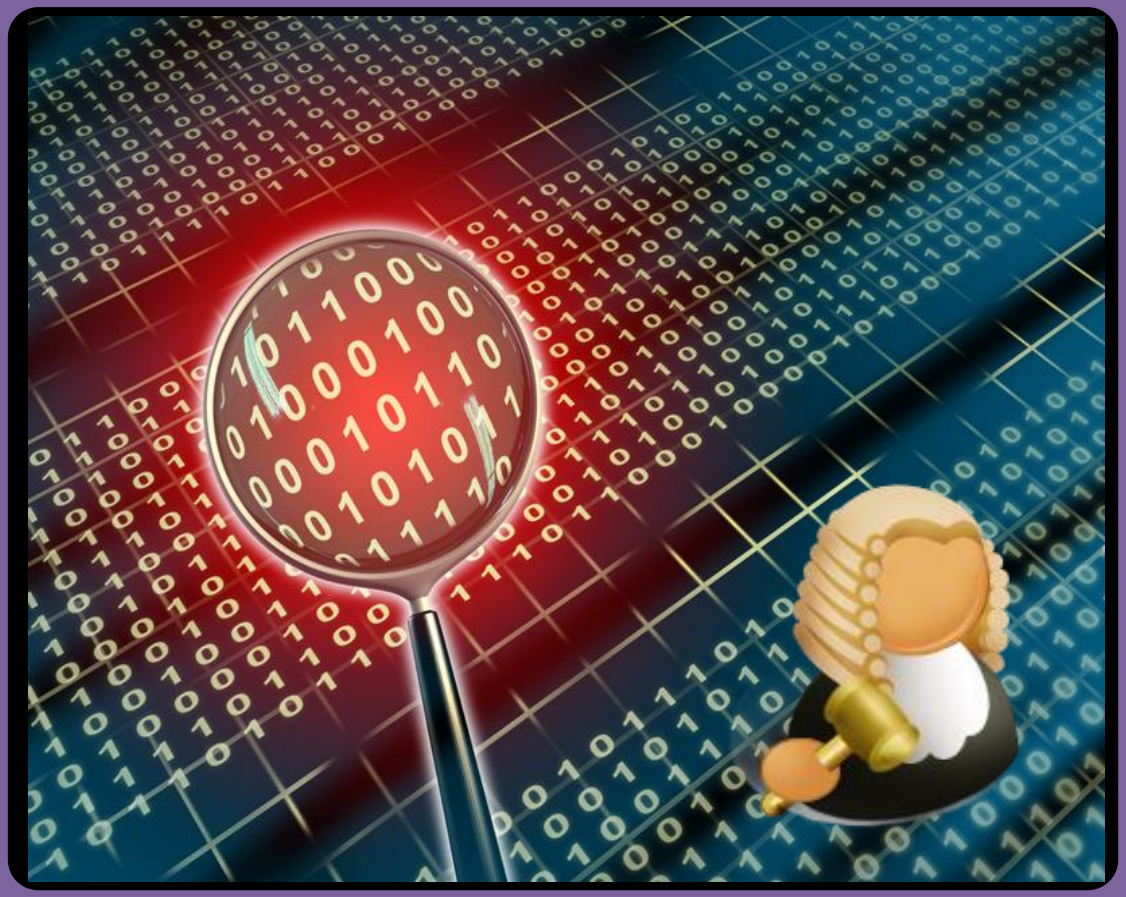
Author: Prof Bill Buchanan





Hello. How are You?

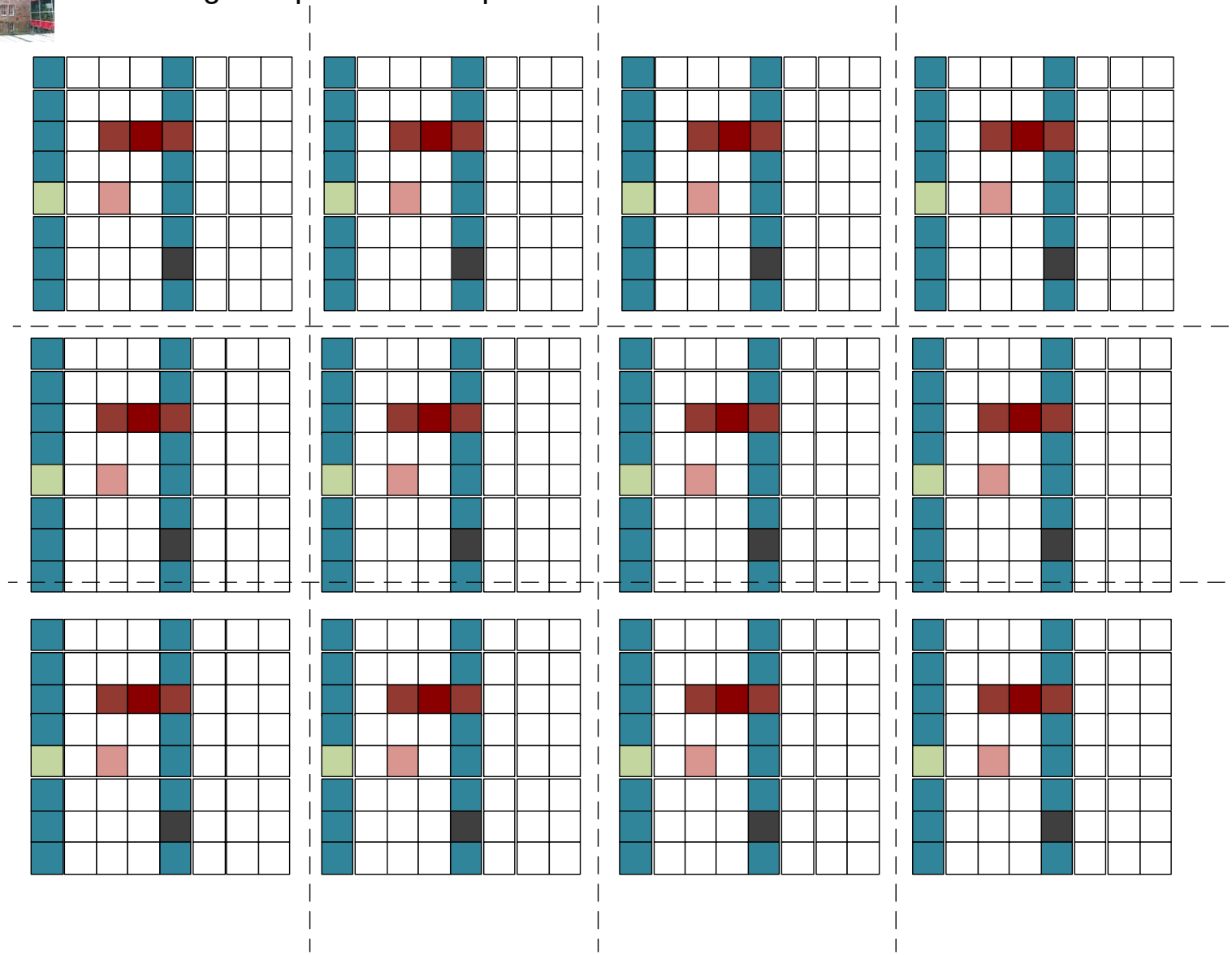
Data Hiding



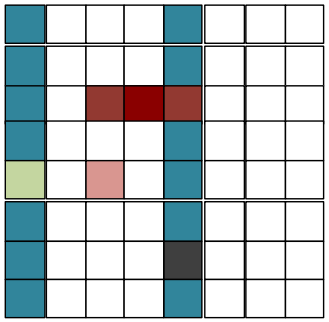
Discriminators

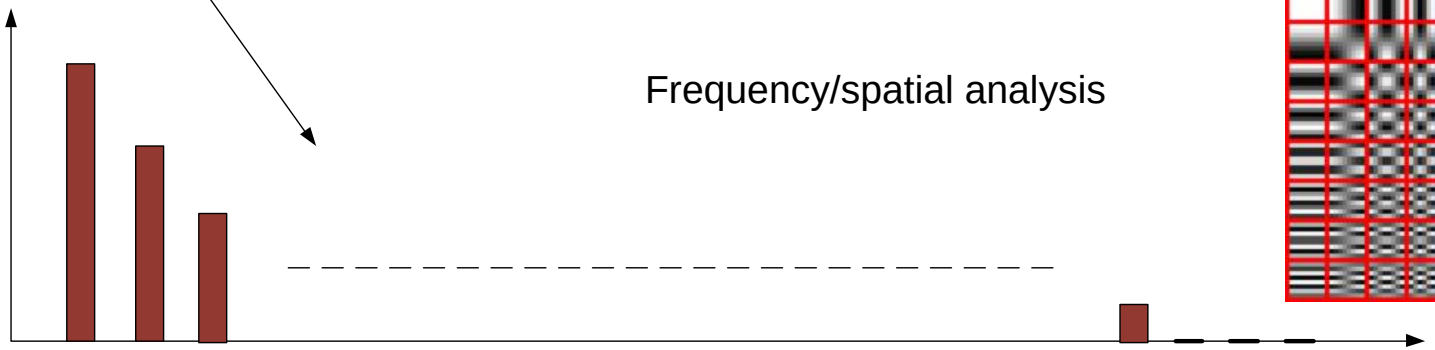
Author: Prof Bill Buchanan

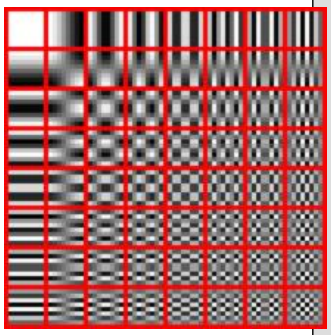
Image is split into 8 x 8 pixel blocks



Author: Prof Bill Buchanan







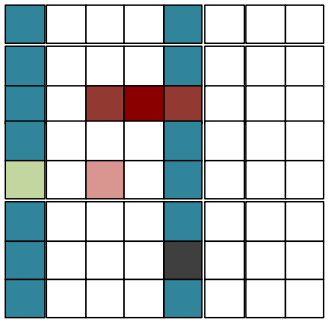
F(0,0)
Low frequency changes

F(7,7)
High frequency changes

Sample values

```
1257.9 2.3 -9.7 -4.1 3.9 0.6 -2.1 0.7
-21.0 -15.3 -4.3 -2.7 2.3 3.5 2.1 -3.1
-11.2 -7.6 -0.9 4.1 2.0 3.4 1.4 0.9
-4.9 -5.8 1.8 1.1 1.6 2.7 2.8 -0.7
0.1 -3.8 0.5 1.3 -1.4 0.7 1.0 0.9
0.9 -1.6 0.9 -0.3 -1.8 -0.3 1.4 0.8
-4.4 2.7 -4.4 -1.5 -0.1 1.1 0.4 1.9
-6.4 3.8 -5.0 -2.6 1.6 0.6 0.1 1.5
```

Author: Prof Bill Buchanan



After DCT

```
1257.9 2.3 -9.7 -4.1 3.9 0.6 -2.1 0.7
-21.0 -15.3 -4.3 -2.7 2.3 3.5 2.1 -3.1
-11.2 -7.6 -0.9 4.1 2.0 3.4 1.4 0.9
-4.9 -5.8 1.8 1.1 1.6 2.7 2.8 -0.7
0.1 -3.8 0.5 1.3 -1.4 0.7 1.0 0.9
0.9 -1.6 0.9 -0.3 -1.8 -0.3 1.4 0.8
-4.4 2.7 -4.4 -1.5 -0.1 1.1 0.4 1.9
-6.4 3.8 -5.0 -2.6 1.6 0.6 0.1 1.5
```

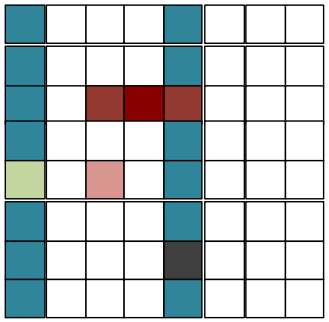
Divide by a certain value and find the nearest integer

```
5 3 4 4 4 3 5 4
4 4 5 5 5 6 7 12
8 7 7 7 7 15 11 11
9 12 13 15 18 18 17 15
20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20
```

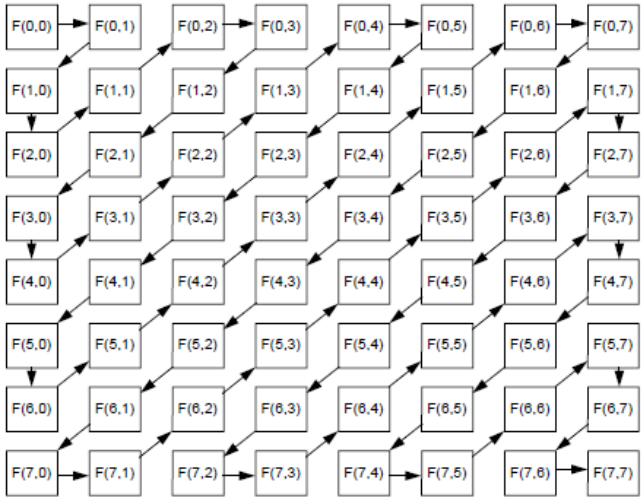
Result:

```
251 0 -2 -1 0 0 0 0
-5 -3 0 0 0 0 0 0
-1 -1 0 0 0 0 0 0
0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0
```

Author: Prof Bill Buchanan



```
251  0  -2  -1  0  0  0  0
-5  -3  0  0  0  0  0  0
-1  -1  0  0  0  0  0  0
0  0  0  0  0  0  0  0
0  0  0  0  0  0  0  0
0  0  0  0  0  0  0  0
0  0  0  0  0  0  0  0
0  0  0  0  0  0  0  0
```



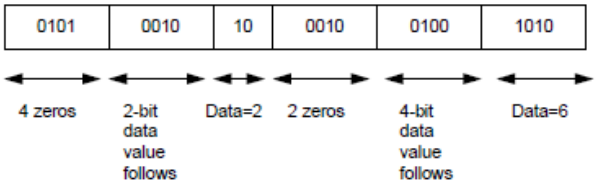
Order in Zig-zag

251, 0, -5, -1, -3, -2, 0, -1, 0, 0, 0, 0, -1, 0, 0, 0, 0,…,0

The binary value of 0000 0000 (00h) can never occur in the AC coding scheme. This code is used as a special code to identify that all of the values until the end of a block are zero. This is a common occurrence and thus saves coding bits.

Use Modified Huffman Code:

Data: 0, 0, 0, 0, 2, 0, 0, 6



Author: Prof Bill Buchanan

Toolkit 2.2 (Author: ProfSIMS)

File

Network | Encryption | Coding | Client | Server | Packet Capture | Snort | Events | Binary Reader | OS | IP | SQL | Test | Dem

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

C:\small.jpg

Tutorial

Hex viewer

00	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	01	01	2C
10	01	2C	00	00	FF	DB	00	43	00	01	01	01	01	01	01	01
20	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01
30	01	01	01	01	01	02	01	01	01	01	01	01	02	02	02	02
40	02	02	02	02	02	02	02	02	02	02	02	02	02	02	02	02
50	02	02	02	02	02	02	02	02	02	FF	DB	00	43	01	01	01
60	01	01	01	01	02	02	02	02	02	02	02	02	02	02	02	02
70	02	02	02	02	02	02	02	02	02	02	02	02	02	02	02	02
80	02	02	02	02	02	02	02	02	02	02	02	02	02	02	02	02
90	02	02	02	02	02	02	02	02	02	02	02	02	02	02	FF	C0
A0	00	11	08	00	A2	00	C8	03	01	11	00	02	11	01	03	11
B0	01	FF	C4	00	1F	00	00	01	04	02	03	01	01	00	00	00
C0	00	00	00	00	00	00	00	06	07	08	09	05	0A	01	03	04
D0	02	0B	FF	C4	00	62	10	00	00	06	02	00	04	03	01	09
E0	0A	06	09	0E	0F	00	00	01	02	03	04	05	06	07	08	00
F0	09	11	12	13	14	21	15	0A	18	22	23	31	37	41	75	B5
1...	16	24	32	51	55	56	95	96	D3	D4	17	36	38	42	61	71
1...	25	53	62	76	77	81	B1	B3	B4	19	1A	33	35	3A	59	72
1...	73	74	78	91	98	A6	B6	34	39	43	52	54	57	65	84	92
1...	94	B2	B7	C2	D1	D2	FF	C4	00	1D	01	01	01	01	00	02

Char viewer

.	.	.	.	.	.	J	F	I	F	.	.	.	.	.	.	.
.	.	.	.	.	.	.	C	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.	C	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	b	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	!	.	.	.	"	#	1	7	A	u	.
.	$	2	Q	U	V	.	.	.	.	.	6	8	B	a	q
%	S	b	v	w	.	.	.	.	.	.	3	5	:	Y	r
s	t	x	.	.	.	.	4	9	C	R	T	W	e	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.

Found FFD8 tag (Start of image). Pos: 0
Found FFE0 tag (JPEG file identifier). Pos: 2
Length: 16
Found FFDB tag (Quantization Table). Pos: 20, Block 0
Found FFDB tag (Quantization Table). Pos: 89, Block 0
Found FFC0 tag (Start Of Frame (Baseline DCT)). Pos: 158, Block 0
Found FFC4 tag (Huffman Table). Pos: 177, Block 0
Found FFC4 tag (Huffman Table). Pos: 210, Block 0
Found FFC4 tag (Huffman Table). Pos: 310, Block 0
Found FFC4 tag (Huffman Table). Pos: 341, Block 0
Found FFDA tag (Start Of Scan). Pos: 412, Block 0
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 1209, Block 2
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 3720, Block 7
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 3977, Block 7
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 4304, Block 8
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 5489, Block 10
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 5507, Block 10
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 5970, Block 11
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 7115, Block 13
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 7620, Block 14
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 7892, Block 15
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 8309, Block 16
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 8938, Block 17
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 9082, Block 17
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 10014, Block 19
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 10626, Block 20
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 10926, Block 21
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 11033, Block 21
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 11310, Block 22
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 11556, Block 22
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 11738, Block 22
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 11748, Block 22
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 11751, Block 22
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 11761, Block 22
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 11765, Block 22
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 12162, Block 23
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 12236, Block 23
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 12507, Block 24
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 12736, Block 24
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 12759, Block 24
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 13706, Block 26
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 13776, Block 26
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 13835, Block 27
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 14427, Block 28
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 14441, Block 28
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 14447, Block 28
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 14476, Block 28
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 14572, Block 28
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 14740, Block 28
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 15372, Block 30
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 15447, Block 30
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 15501, Block 30
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 15893, Block 31
...
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 18943, Block 36
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 19224, Block 37
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 19293, Block 37
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 19430, Block 37
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 19459, Block 38
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 19595, Block 38
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 19632, Block 38
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 19906, Block 38
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 19943, Block 38
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 20153, Block 39
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 20182, Block 39
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 20446, Block 39
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 20448, Block 39
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 20495, Block 40
Found FFD9 tag (End of image). Pos: 21684, Block 42

Discriminator

Authentication

FFC0 tag (Start Of Frame (Baseline DCT)).
FFC2 tag (Start Of Frame (Progressive DCT)).
FFC4 tag (Huffman Table).
FFDB tag (Quantization Table).
FFC2 tag (Define Restart Interval).
FFDA tag (Start Of Scan).
FFDE tag (Comment).
FF00 stuffed FF (Likely Huffman Coding).

2011 UK IT INDUSTRY AWARDS
bcs The Chartered Institute for IT computing
FINALIST

Small.jpg

Detecting a JPEG file

512 Bytes **Segment 0**

512 Bytes **Segment 1**

512 Bytes **Segment 2**

512 Bytes **Seg 40**

512 Bytes **Seg 41**

512 Bytes **Seg 42**

Segment No	Detected
1	Not detected
2	1 Found
3	Not detected
4	Not detected
5	Not detected
6	Not detected

7 2 Found
8 1 Found
9 Not detect
10 2 Found
11 1 Found
12 Not detected
13 1 Found
14 1 Found
15 1 Found
16 1 Found
17 2 Found
18 Not detected
19 1 Found
20 1 Found
21 2 Found
22 7 Found
23 2 Found
24 3 Found
25 Not detected
26 2 Found
27 1 Found
28 6 Found
29 Not detected
30 3 Found
31 6 Found

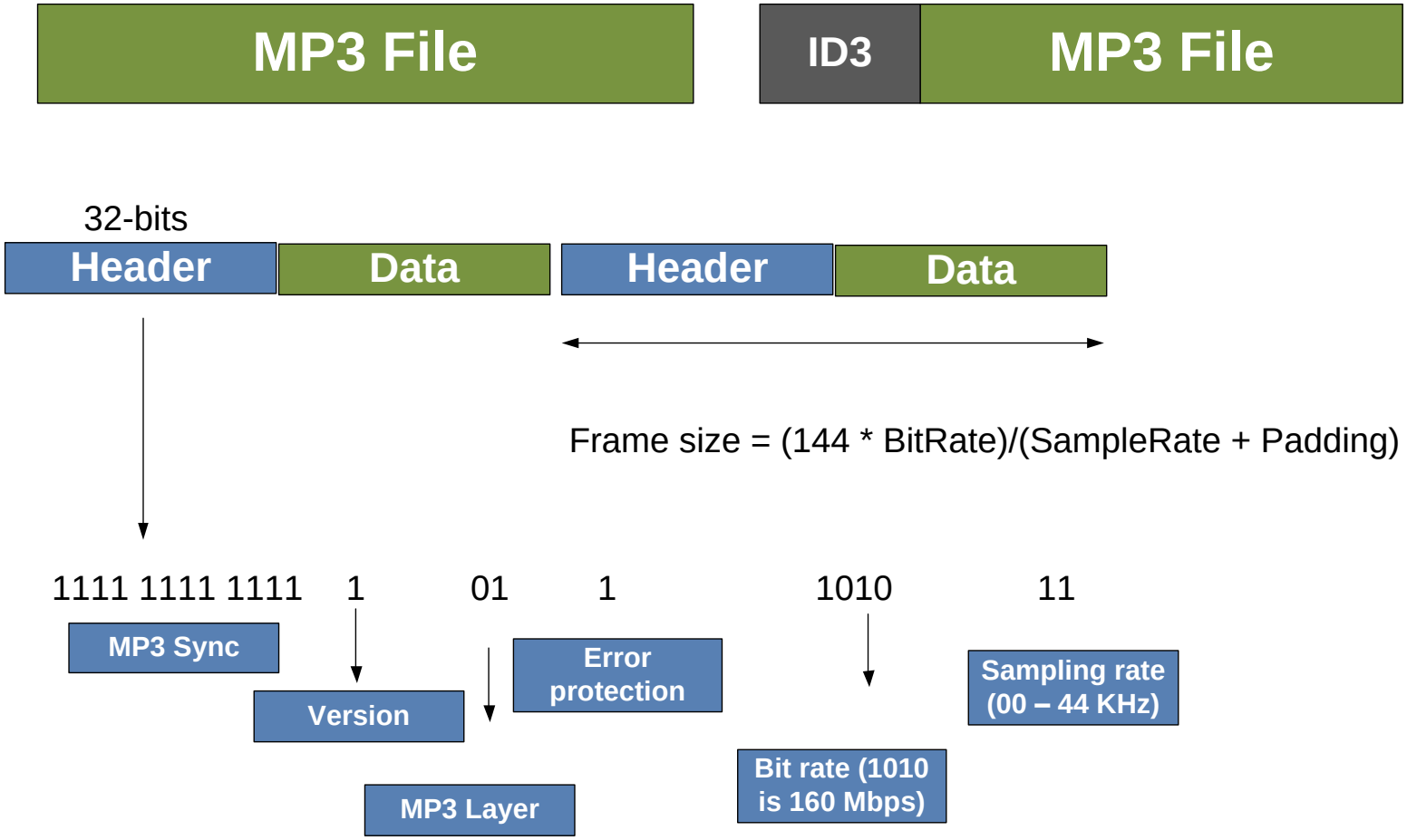
Result: 29 out of 40 (0 and 41 also detected)
With 2048 byte blocks: Nearly 100%

```
Found FFD8 tag (Start of image). Pos: 0
Found FFE0 tag (JPEG file identifier). Pos: 2
  Length: 16
Found FFDB tag (Quantization Table). Pos: 20, Segment 0
Found FFDB tag (Quantization Table). Pos: 89, Segment 0
Found FFC0 tag (Start Of Frame (Baseline DCT)). Pos: 158, Segment 0
Found FFC4 tag (Huffman Table). Pos: 177, Segment 0
Found FFC4 tag (Huffman Table). Pos: 210, Segment 0
Found FFC4 tag (Huffman Table). Pos: 310, Segment 0
Found FFC4 tag (Huffman Table). Pos: 341, Segment 0
Found FFDA tag (Start Of Scan). Pos: 412, Segment 0
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 1209, Segment 2
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 3720, Segment 7
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 3977, Segment 7
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 4304, Segment 8
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 5489, Segment 10
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 5507, Segment 10
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 5970, Segment 11
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 7115, Segment 13
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 7620, Segment 14
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 7892, Segment 15
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 8309, Segment 16
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 8938, Segment 17
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 9082, Segment 17
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 10014, Segment 19
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 10626, Segment 20
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 10926, Segment 21
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 11033, Segment 21
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 11310, Segment 22
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 11556, Segment 22
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 11738, Segment 22
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 11748, Segment 22
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 11751, Segment 22
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 11761, Segment 22
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 11765, Segment 22
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 12162, Segment 23
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 12236, Segment 23
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 12507, Segment 24
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 12736, Segment 24
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 12759, Segment 24
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 13706, Segment 26
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 13776, Segment 26
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 13835, Segment 27
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 14427, Segment 28
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 14441, Segment 28
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 14447, Segment 28
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 14476, Segment 28
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 14572, Segment 28
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 14740, Segment 28
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 15372, Segment 30
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 15447, Segment 30
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 15501, Segment 30
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 15893, Segment 31
...
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 18943, Segment 36
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 19224, Segment 37
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 19293, Segment 37
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 19430, Segment 37
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 19459, Segment 38
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 19595, Segment 38
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 19632, Segment 38
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 19906, Segment 38
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 19943, Segment 38
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 20153, Segment 39
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 20182, Segment 39
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 20446, Segment 39
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 20448, Segment 39
Found FF00 stuffed FF (Likely Huffman Coding). Pos: 20495, Segment 40
Found FFD9 tag (End of image). Pos: 21684, Segment 42
```

Discriminator

Authentication

Detecting an MP3 file



Discriminator

Authentication

Author: Prof Bill Buchanan

Track258.mp3

512 Bytes **Segment 0**

512 Bytes **Segment 1**

512 Bytes **Segment 2**

Segment No	Detected
0	Found
2	Found
...	
20	Found

Found in all segments

512 Bytes **Seg 18**

512 Bytes **Seg 19**

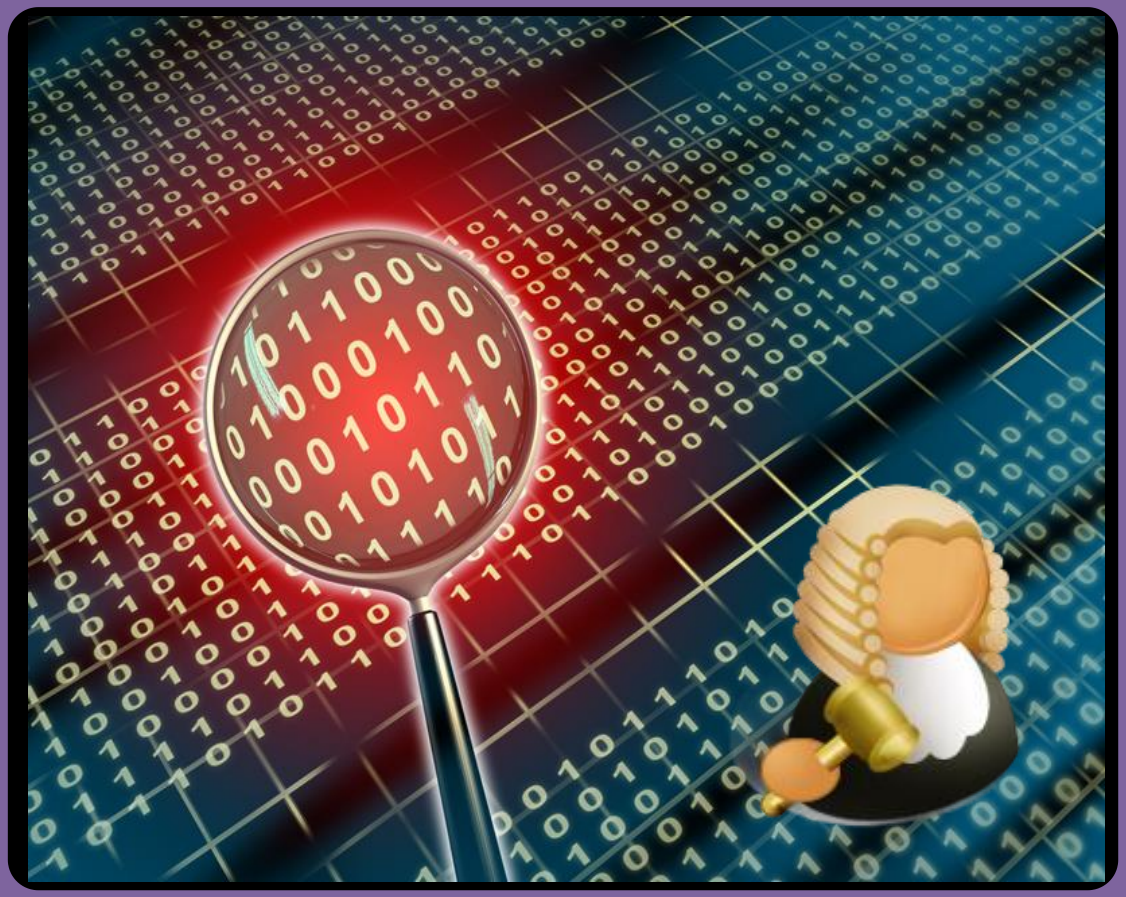
512 Bytes **Seg 20**

```
MP3 Analysis ... looking for 11 or 12-bit sequences for 1's for the frames in 512 byte sectors
MP3: Found 12-bit sequence. Pos: 63, Segment: 0 out of 21 segments
MP3: Found 11-bit sequence. Pos: 234, Segment: 0 out of 21 segments
MP3: Found 11-bit sequence. Pos: 704, Segment: 1 out of 21 segments
MP3: Found 12-bit sequence. Pos: 1152, Segment: 2 out of 21 segments
MP3: Found 12-bit sequence. Pos: 1228, Segment: 2 out of 21 segments
MP3: Found 12-bit sequence. Pos: 1239, Segment: 2 out of 21 segments
MP3: Found 11-bit sequence. Pos: 1488, Segment: 2 out of 21 segments
MP3: Found 12-bit sequence. Pos: 1755, Segment: 3 out of 21 segments
MP3: Found 12-bit sequence. Pos: 1802, Segment: 3 out of 21 segments
MP3: Found 12-bit sequence. Pos: 1862, Segment: 3 out of 21 segments
MP3: Found 12-bit sequence. Pos: 1928, Segment: 3 out of 21 segments
MP3: Found 11-bit sequence. Pos: 2015, Segment: 3 out of 21 segments
MP3: Found 12-bit sequence. Pos: 2145, Segment: 4 out of 21 segments
MP3: Found 12-bit sequence. Pos: 2146, Segment: 4 out of 21 segments
MP3: Found 12-bit sequence. Pos: 2489, Segment: 4 out of 21 segments
MP3: Found 12-bit sequence. Pos: 2622, Segment: 5 out of 21 segments
MP3: Found 11-bit sequence. Pos: 2765, Segment: 5 out of 21 segments
MP3: Found 12-bit sequence. Pos: 2866, Segment: 5 out of 21 segments
MP3: Found 12-bit sequence. Pos: 2977, Segment: 5 out of 21 segments
MP3: Found 12-bit sequence. Pos: 3005, Segment: 5 out of 21 segments
MP3: Found 12-bit sequence. Pos: 3011, Segment: 5 out of 21 segments
MP3: Found 11-bit sequence. Pos: 3080, Segment: 6 out of 21 segments
MP3: Found 12-bit sequence. Pos: 3081, Segment: 6 out of 21 segments
MP3: Found 11-bit sequence. Pos: 3086, Segment: 6 out of 21 segments
MP3: Found 12-bit sequence. Pos: 3087, Segment: 6 out of 21 segments
MP3: Found 12-bit sequence. Pos: 3134, Segment: 6 out of 21 segments
MP3: Found 12-bit sequence. Pos: 3212, Segment: 6 out of 21 segments
MP3: Found 12-bit sequence. Pos: 3231, Segment: 6 out of 21 segments
MP3: Found 12-bit sequence. Pos: 3499, Segment: 6 out of 21 segments
MP3: Found 12-bit sequence. Pos: 3500, Segment: 6 out of 21 segments
MP3: Found 12-bit sequence. Pos: 3704, Segment: 7 out of 21 segments
MP3: Found 12-bit sequence. Pos: 3761, Segment: 7 out of 21 segments
MP3: Found 11-bit sequence. Pos: 4044, Segment: 7 out of 21 segments
MP3: Found 12-bit sequence. Pos: 4231, Segment: 8 out of 21 segments
...
MP3: Found 12-bit sequence. Pos: 7312, Segment: 14 out of 21 segments
MP3: Found 12-bit sequence. Pos: 7366, Segment: 14 out of 21 segments
MP3: Found 12-bit sequence. Pos: 7495, Segment: 14 out of 21 segments
MP3: Found 11-bit sequence. Pos: 7666, Segment: 14 out of 21 segments
MP3: Found 12-bit sequence. Pos: 8031, Segment: 15 out of 21 segments
MP3: Found 12-bit sequence. Pos: 8164, Segment: 15 out of 21 segments
MP3: Found 12-bit sequence. Pos: 8195, Segment: 16 out of 21 segments
MP3: Found 11-bit sequence. Pos: 8427, Segment: 16 out of 21 segments
MP3: Found 12-bit sequence. Pos: 8497, Segment: 16 out of 21 segments
MP3: Found 12-bit sequence. Pos: 8634, Segment: 16 out of 21 segments
MP3: Found 11-bit sequence. Pos: 8716, Segment: 17 out of 21 segments
MP3: Found 11-bit sequence. Pos: 8907, Segment: 17 out of 21 segments
MP3: Found 12-bit sequence. Pos: 8973, Segment: 17 out of 21 segments
MP3: Found 12-bit sequence. Pos: 9279, Segment: 18 out of 21 segments
MP3: Found 12-bit sequence. Pos: 9474, Segment: 18 out of 21 segments
MP3: Found 12-bit sequence. Pos: 9761, Segment: 19 out of 21 segments
MP3: Found 12-bit sequence. Pos: 9776, Segment: 19 out of 21 segments
MP3: Found 12-bit sequence. Pos: 9777, Segment: 19 out of 21 segments
MP3: Found 12-bit sequence. Pos: 9778, Segment: 19 out of 21 segments
MP3: Found 11-bit sequence. Pos: 9795, Segment: 19 out of 21 segments
MP3: Found 11-bit sequence. Pos: 9952, Segment: 19 out of 21 segments
MP3: Found 12-bit sequence. Pos: 10264, Segment: 20 out of 21 segments
MP3: Found 12-bit sequence. Pos: 10265, Segment: 20 out of 21 segments
MP3: Found 12-bit sequence. Pos: 10407, Segment: 20 out of 21 segments
MP3: Found 11-bit sequence. Pos: 10422, Segment: 20 out of 21 segments
MP3: Found 12-bit sequence. Pos: 10657, Segment: 20 out of 21 segments
```

Author: Prof Bill Buchanan

Detecting an MP3 file

Data Hiding



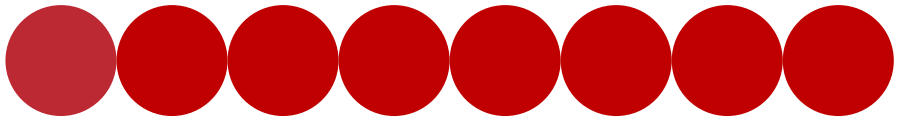
lsb hiding

Author: Prof Bill Buchanan

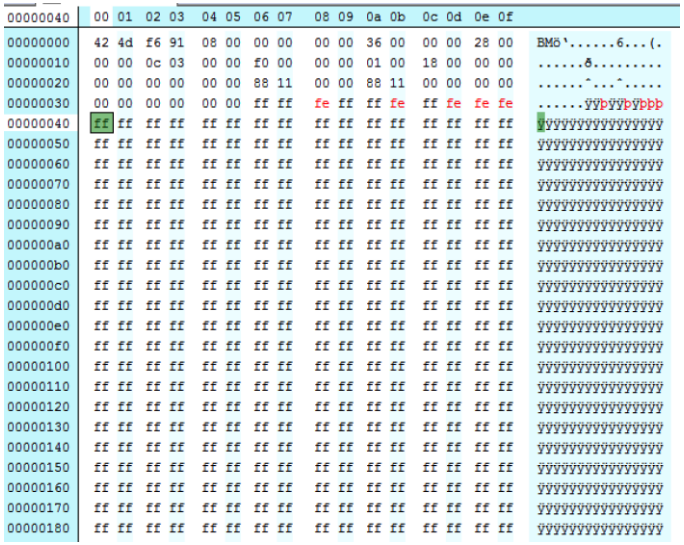
Edinburgh Napier UNIVERSITY

‘h’ - 68h – 0110 1000

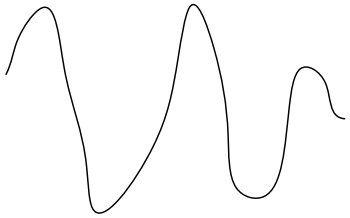
189 41 51 189 41 50 189 41 50 189 41 50



189 41 50 189 41 51 189 41 51 189 41 50



00000040	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00000000	42	4d	f6	91	08	00	00	00	00	00	36	00	00	00	28	00
00000010	00	00	0c	03	00	00	f0	00	00	00	01	00	18	00	00	00
00000020	00	00	00	00	00	00	88	11	00	00	88	11	00	00	00	00
00000030	00	00	00	00	00	00	ff	ff	fe	ff	ff	fe	ff	fe	fe	fe
00000040	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff
00000050	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff
00000060	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff
00000070	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff
00000080	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff
00000090	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff
000000a0	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff
000000b0	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff
000000c0	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff
000000d0	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff
000000e0	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff
000000f0	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff
00000100	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff
00000110	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff
00000120	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff
00000130	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff
00000140	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff
00000150	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff
00000160	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff
00000170	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff
00000180	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff	ff

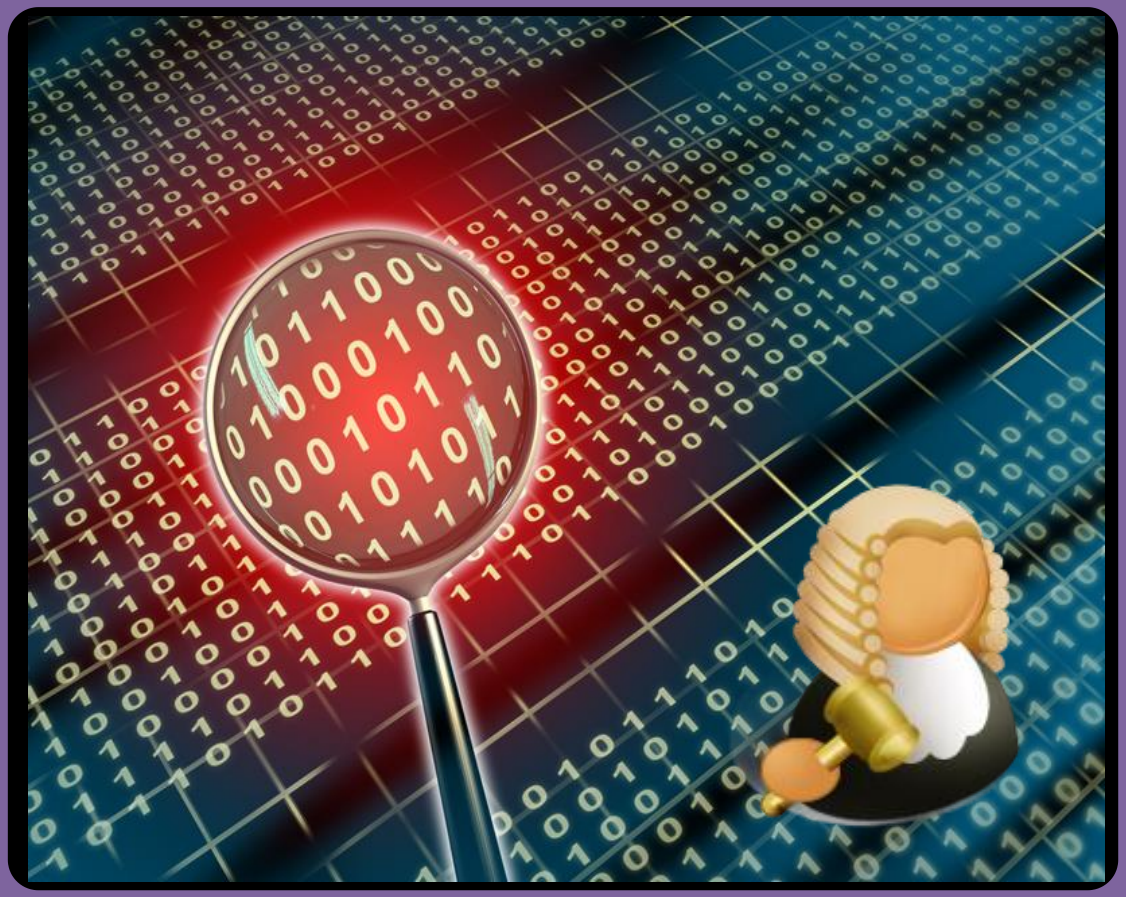


Modify the least significant bit (audio)

Digital

Steganography

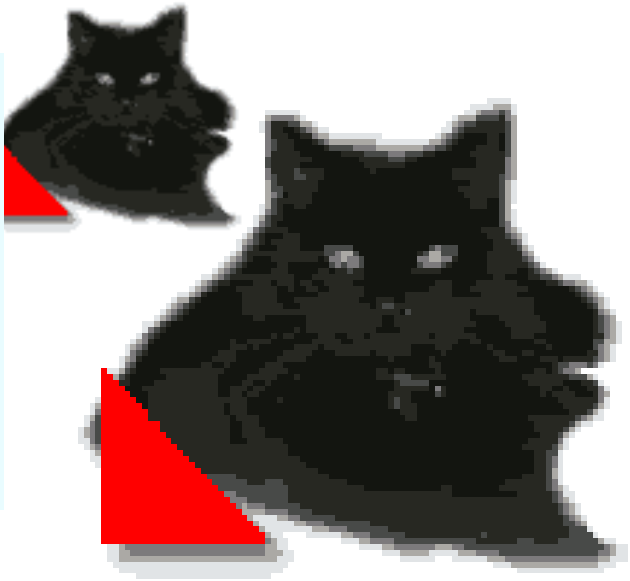
Data Hiding



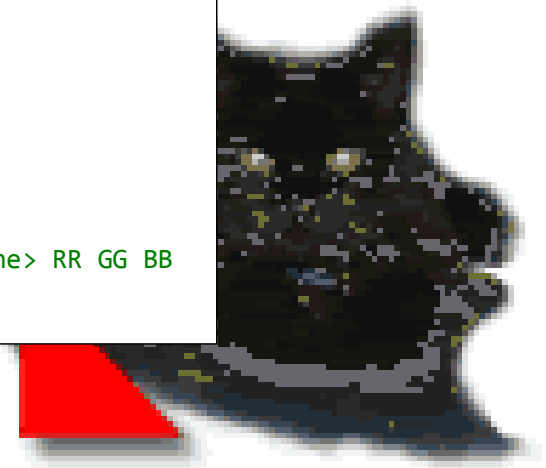
Hiding in Message Blocks

Author: Prof Bill Buchanan

```
47 49 46 38  39 61 64 00  55 00 c4 00  00 10 10 10   GIF89ad.U.A.....
cc cc cc e1  04 05 99 99  99 3a 3a 3c  66 66 66 ff   ÌÌÌá..™™™::<fffÿ
ff ff 21 21  21 51 5c 6c  f1 f4 f2 19  18 11 7a 84   ÿÿ!!!Q\lñôò...z„
8a 7a 0f 10  21 2e 38 d7  1f 1f e1 e4  e6 b5 b3 ae   Šz..!.8×..áäæµ³®
29 29 28 74  75 72 22 1a  19 37 45 52  7b 72 4d 57   ))(tur"..7ER{rMW
55 53 fc 20  20 13 15 10  ff 00 00 68  65 6c 6c 6f   USü  ...ÿ..hello
33 d5 d5 d5  21 21 19 a7  a5 9e 61 56  61 21 f9 04   3ÕÕÕ!!.§¥žaVa!ù.
05 14 00 06  00 2c 00 00  00 00 64 00  55 00 00 05   .....,....d.U...
ff a0 21 8e  64 69 9e 68  aa ae 67 c2  be 70 2c cf   ÿ !Ždižh ª®gÂ¾p,Ï
69 92 3c dc  43 ef bc 68  db bd 1a 2e  00 f1 40 74   i'<ÜCï¼hÛ½...ñ@t
c1 a4 ea 16  68 3e 1e 2e  a5 21 c1 21  0e 16 85 cf   Á¤ê.h>..¥!Á!...…Ï
82 23 ed 96  12 9e 82 78  01 e1 44 83  09 c8 60 f0   ,#í–.ž,x.áDƒ.È`ð
a1 50 08 91  42 c0 4b 37  3c 0a 9b 4d  84 f0 f1 04   ¡P.'BÀK7<.›M„ðñ.
```

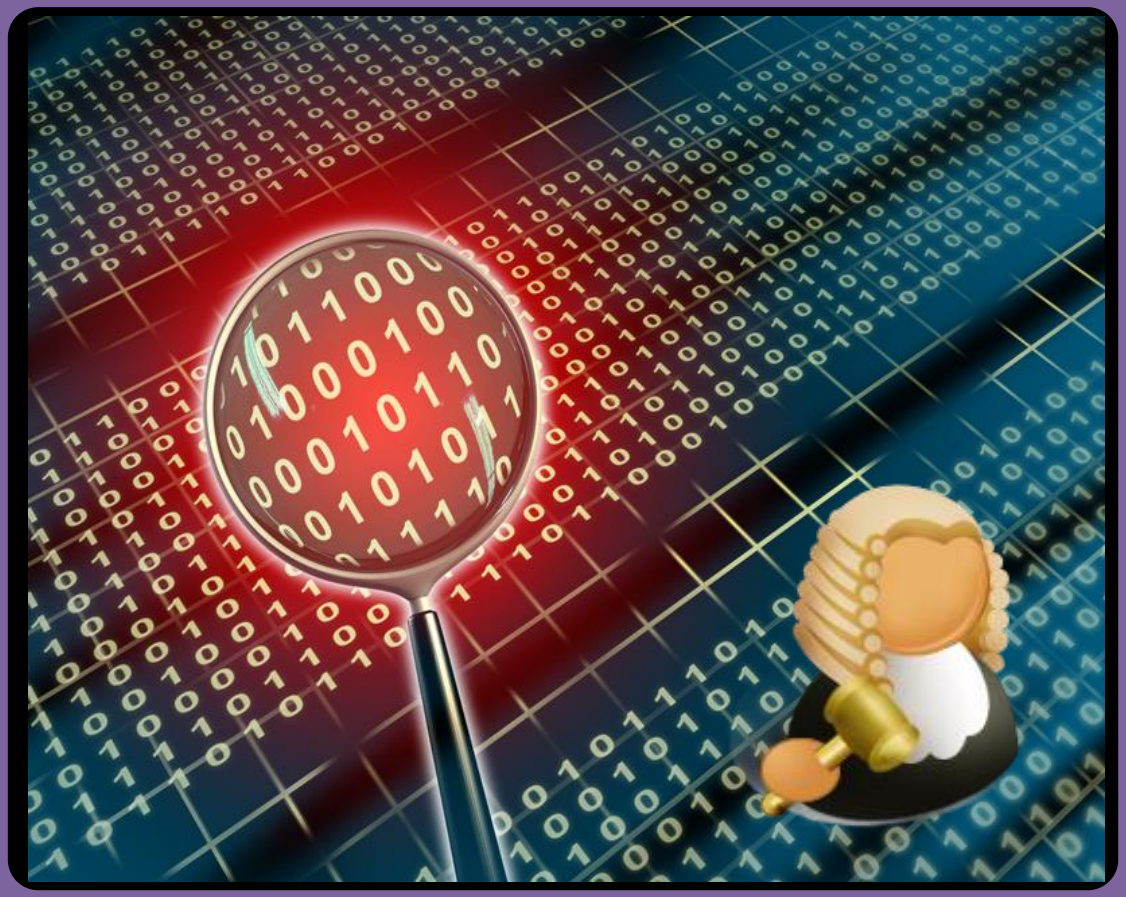


```
// Format for GIF header
//Offset   Length   Contents
//  0      3 bytes  "GIF"
//  3      3 bytes  "87a" or "89a"
//  6      2 bytes  <Logical Screen Width>
//  8      2 bytes  <Logical Screen Height>
// 10      1 byte   bit 0:    Global Color Table Flag (GCTF)
//                  bit 1..3: Color Resolution
//                  bit 4:    Sort Flag to Global Color Table
//                  bit 5..7: Size of Global Color Table: 2^(1+n)
// 11      1 byte   <Background Color Index>
// 12      1 byte   <Pixel Aspect Ratio>
// 13      ? bytes  <Global Color Table(0..255 x 3 bytes) if GCTF is one> RR GG BB
//         ? bytes  <Blocks>
//         1 bytes  <Trailer> (0x3b)
```



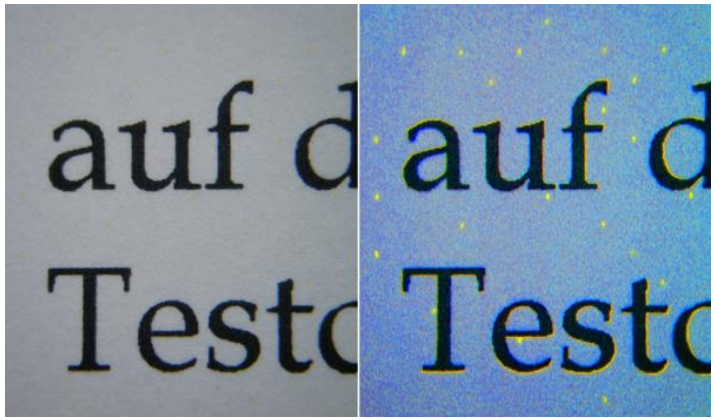
Hiding in message blocks

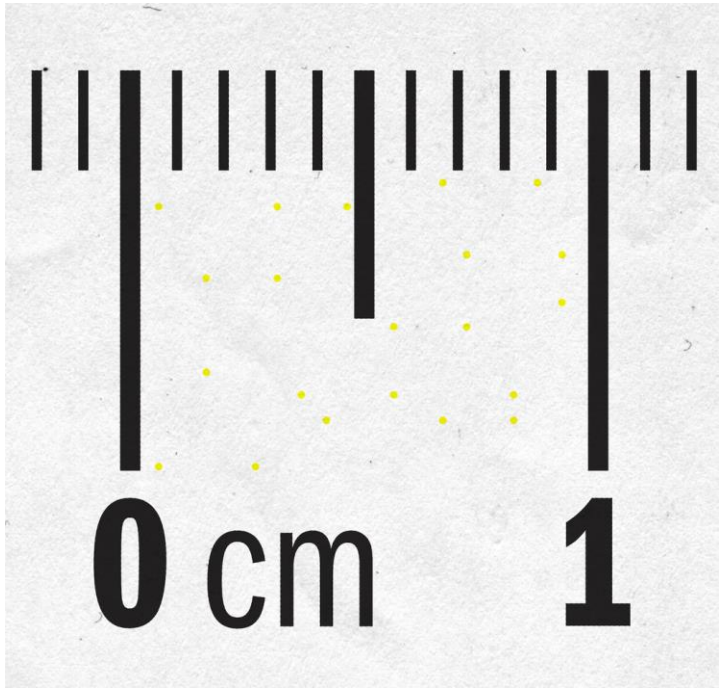
Data Hiding



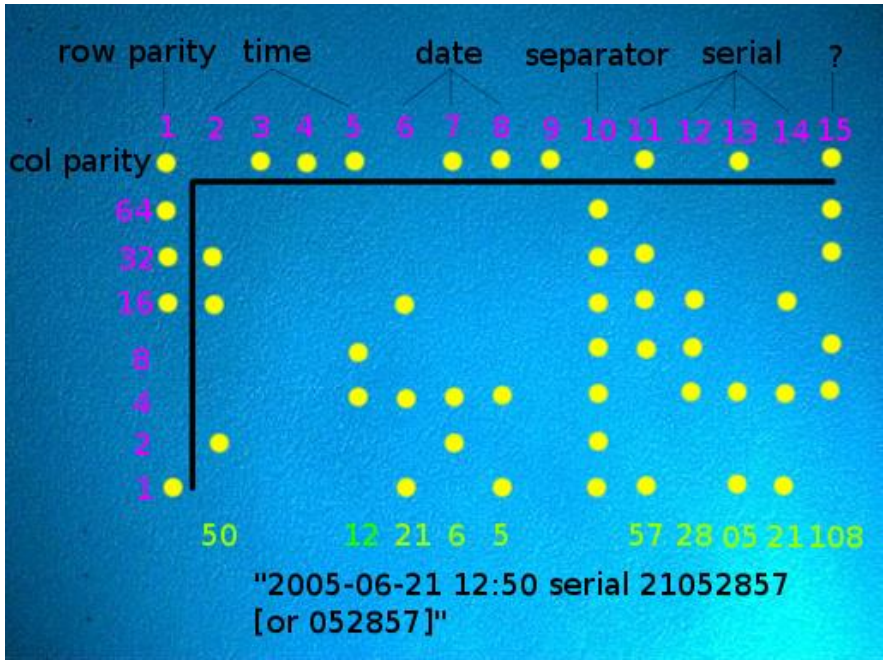
Hidden Messages

Author: Prof Bill Buchanan





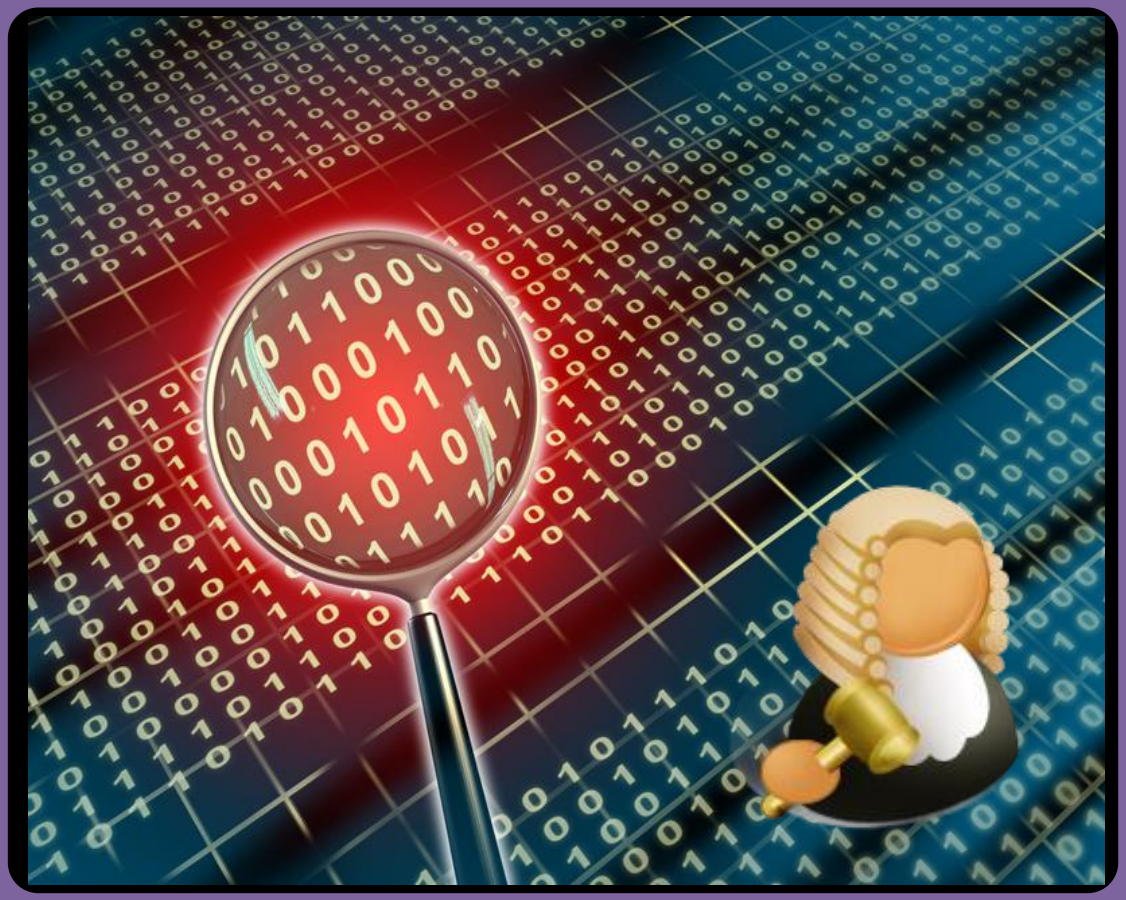
ELECTRONIC FRONTIER FOUNDATION



Hidden printer codes

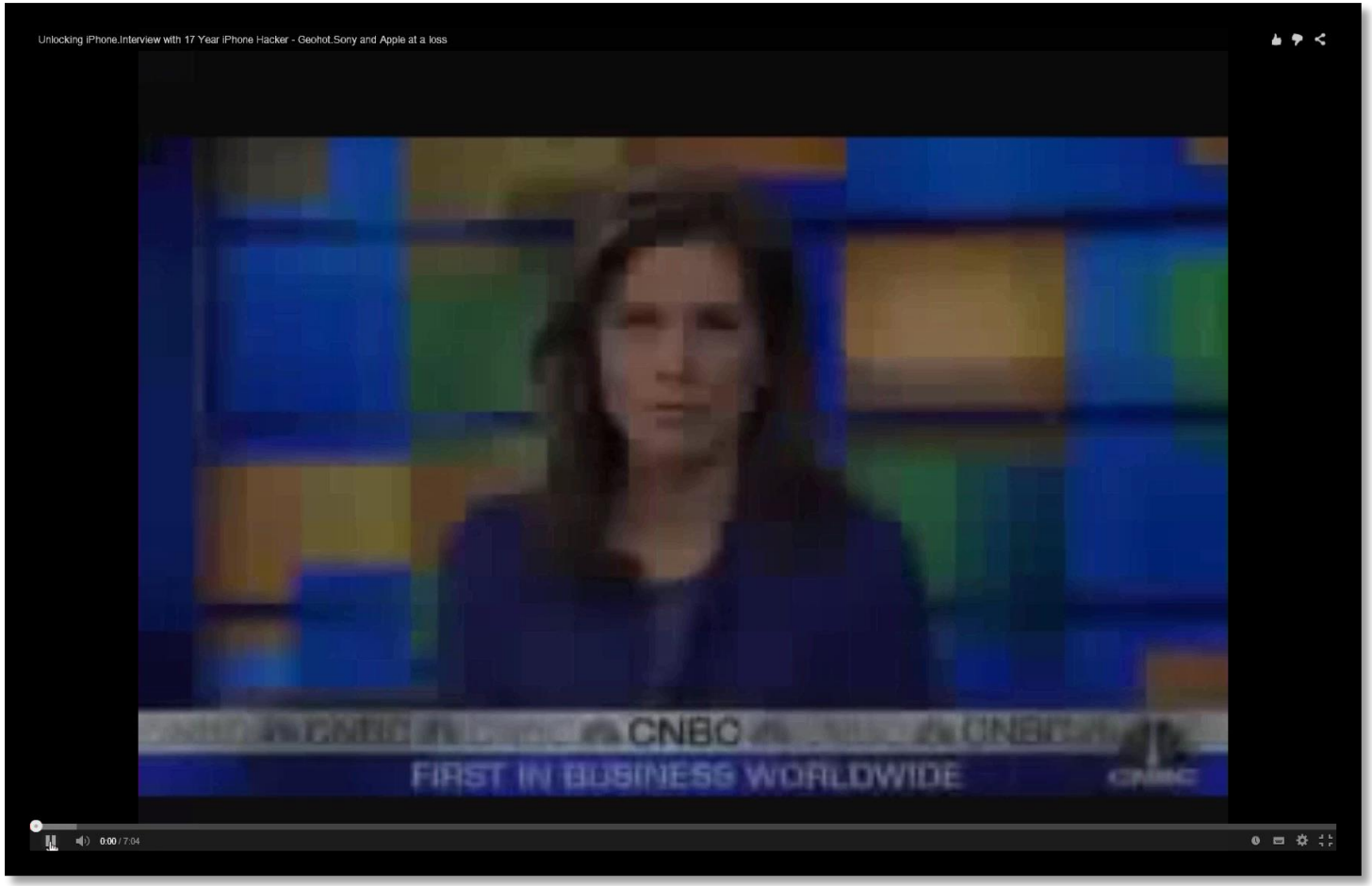
EFF cracked date, time, and printer serial number in a Xerox DocuColor color laser output

Data Hiding

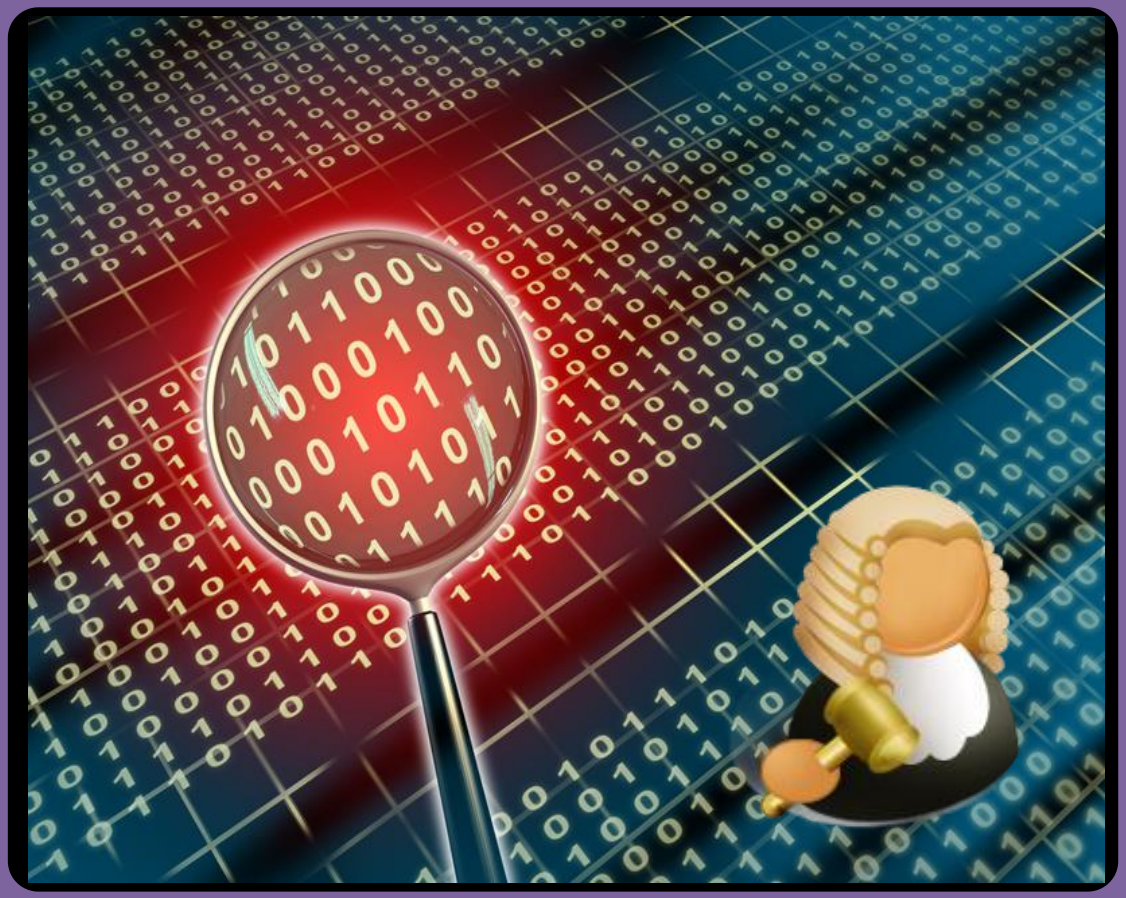


Static Messages in Video

Author: Prof Bill Buchanan

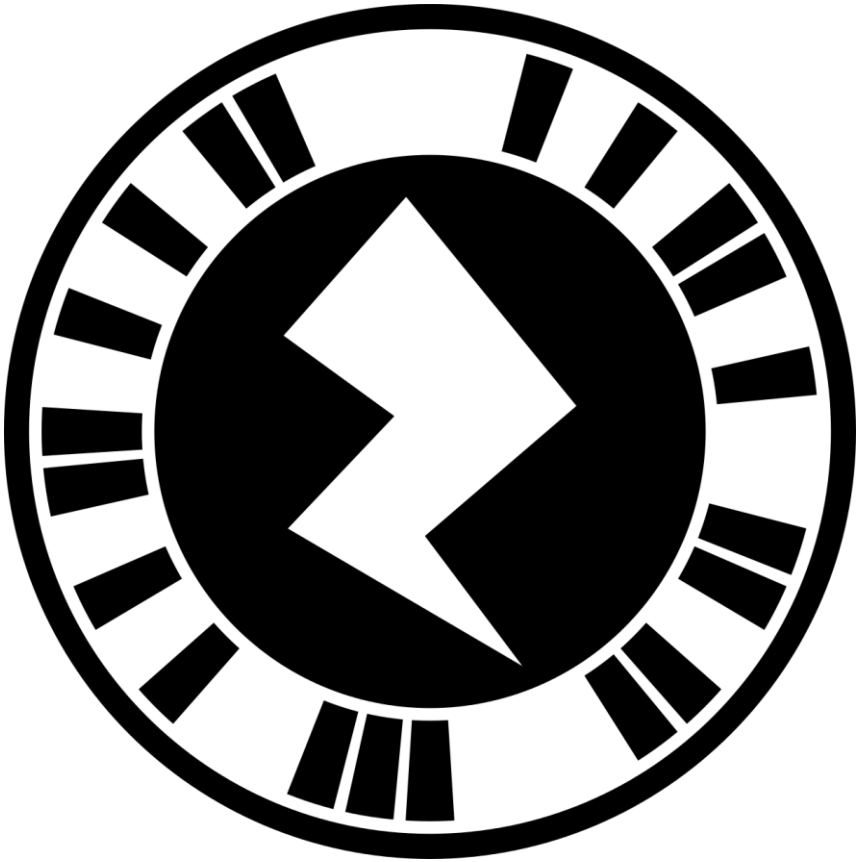

Unlocking iPhone.Interview with 17 Year iPhone Hacker - Geohot.Sony and Apple at a loss
CNBC
FIRST IN BUSINESS WORLDWIDE
0:00 / 7:04

Data Hiding

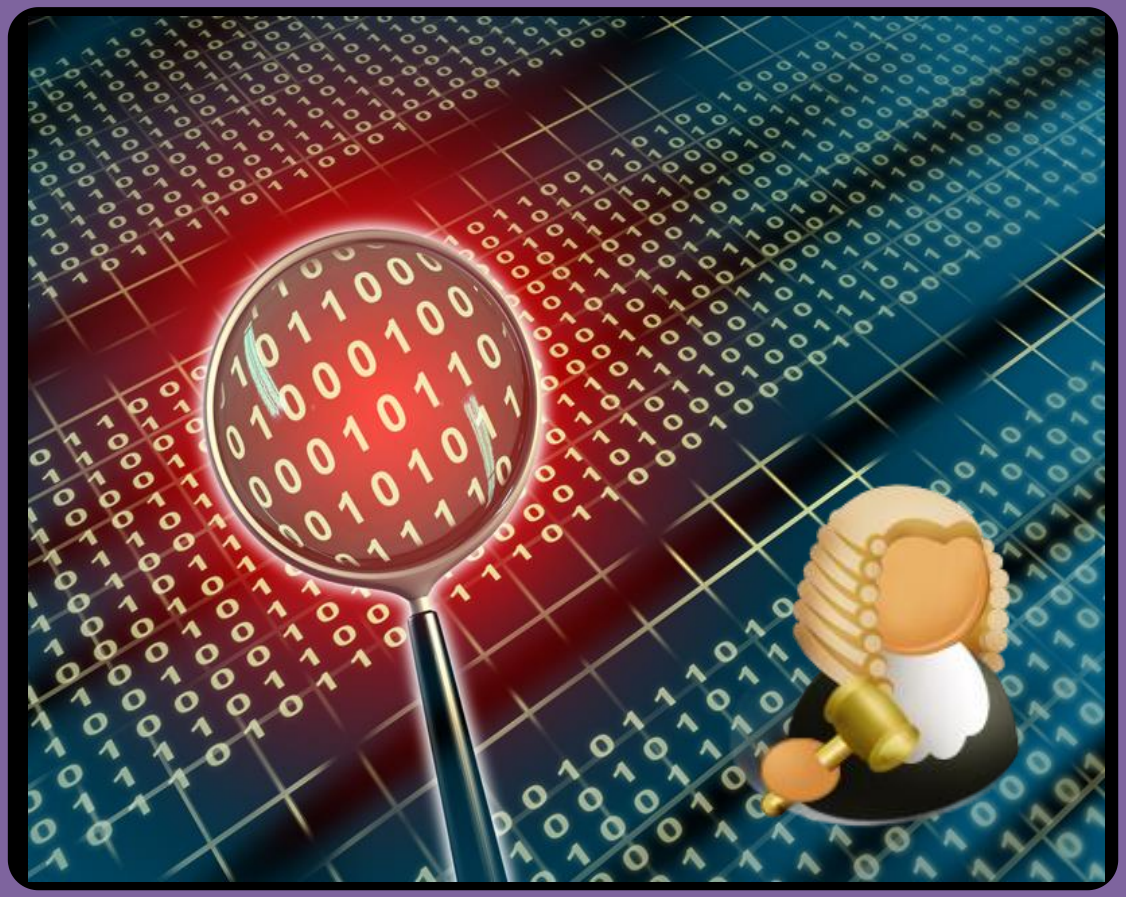


Codes in Messages

Author: Prof Bill Buchanan



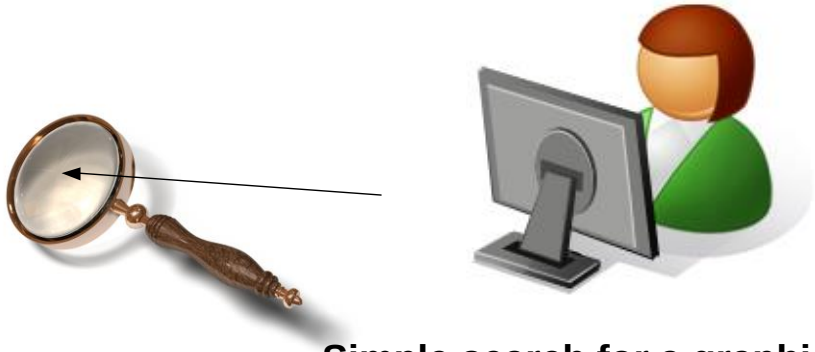
Data Hiding



File Carving

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)

Deep Analysis

Forensic

Author: Prof Bill Buchanan

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\clientToolkit\log\cat01_with_hidden_text.gif

Tutorial

Hex viewer

00	47	49	46	38	39	61	64	00	55	00	E6	00	00	FF	FF	FF
10	F7	F7	F6	F1	F4	F2	EE	EE	EF	E7	E7	E7	E1	E4	E6	DF
20	DE	DF	D7	DA	DD	EF	CE	CE	D5	D5	D5	D5	D3	D0	D9	D1
30	A1	CC	CC	CC	C4	C8	CC	68	65	6C	6C	6F	C0	D1	C6	84
40	C0	BF	BD	BD	BB	B8	B8	B6	B5	B5	B3	AE	AA	B1	B6	AB
50	AC	AD	AB	A9	A5	A6	A6	A6	A7	A5	9E	AB	A8	70	AC	9C
60	9F	99	99	99	94	9A	A0	8B	95	9C	93	92	8E	8C	8D	8A
70	86	8C	96	98	8B	66	90	87	82	83	83	83	7A	84	8A	CB
80	5E	5E	FB	48	48	82	7C	73	7C	7A	7C	85	7A	5E	73	7C
90	82	99	66	66	74	75	72	61	80	66	6A	73	80	7B	72	4D
A0	7D	6E	52	6B	6A	6E	77	63	5F	F8	2A	2A	74	68	45	66
B0	66	66	5C	66	74	FC	20	20	55	62	6B	6B	5F	3F	E9	22
C0	22	82	4D	4F	55	5D	66	61	56	61	51	5C	6C	55	58	5A
D0	57	55	53	4B	55	62	63	4A	4A	55	51	48	D8	17	17	4A
E0	52	58	F2	09	09	30	50	86	FF	00	00	43	4B	56	48	4A
F0	48	7B	33	36	E1	04	05	44	45	42	37	45	52	42	41	39
1...	26	43	78	47	3A	2C	34	3F	49	52	30	31	3A	3A	3C	AC
1...	09	09	3C	38	35	66	25	28	2F	3A	42	2F	3A	3C	33	33
1...	33	6B	18	19	29	31	41	2A	31	39	34	2F	2A	7A	0F	10
1...	29	2D	31	30	2B	28	21	2E	38	33	28	22	29	29	28	21

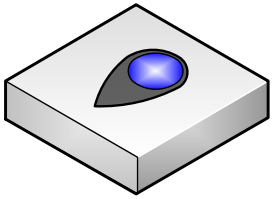
Char viewer

G	I	F	8	9	a	d	.	U.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	h	e	l	l	o	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.	p	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	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	(	"	)	)	(	!

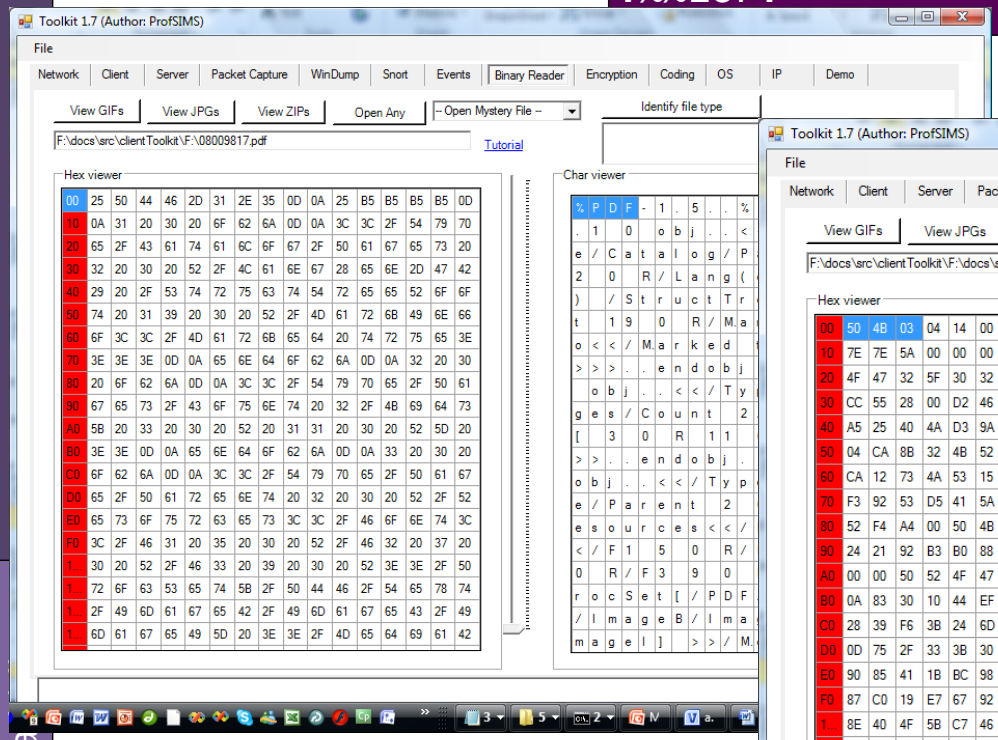
Obfuscation

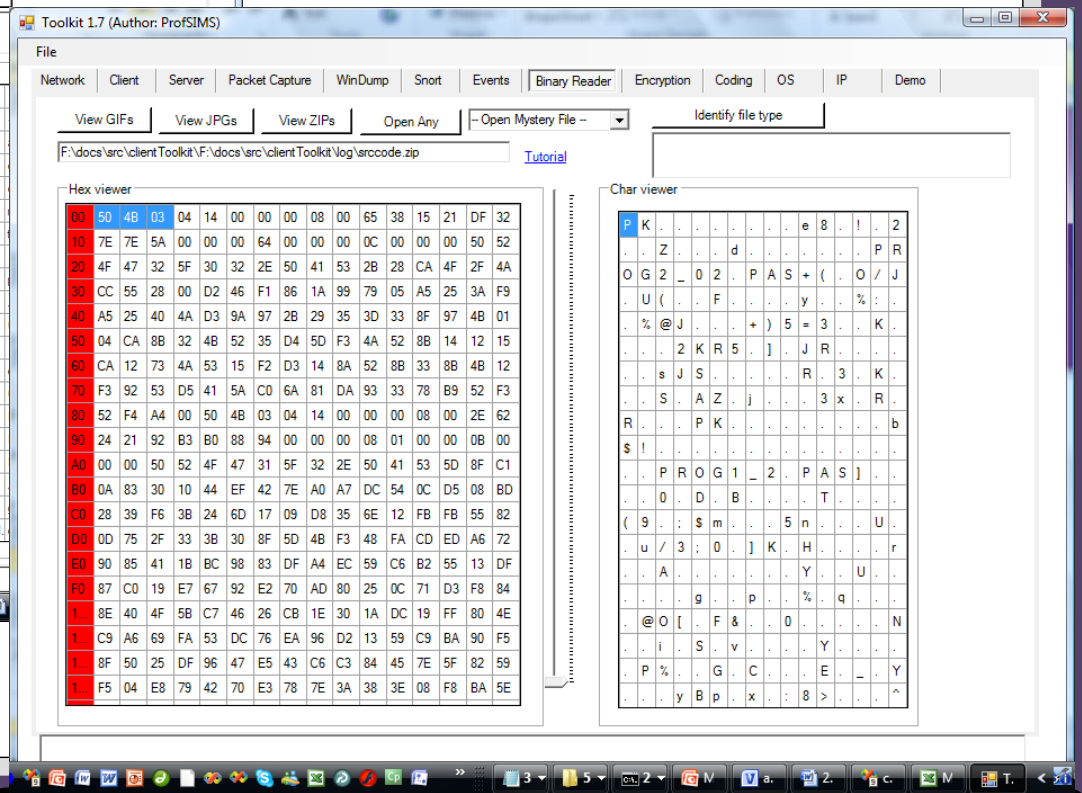
Forensic

File Analysis



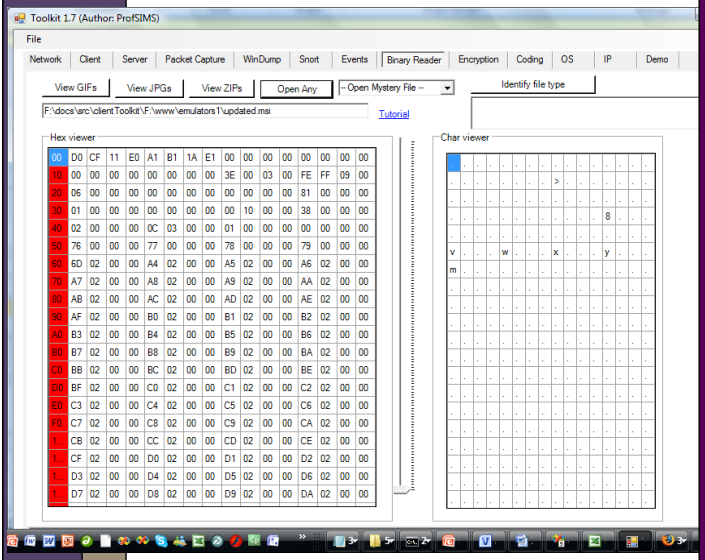
Sig	File ext	File type
0x474946	*.gif	GIF files
GIF89a	*.gif	GIF files
0xFFD8FF	*.jpg	JPEG files
JFIF	*.jpg	JPEG files
0x504B03	*.zip	ZIP files
0x25504446	*.pdf	PDF files
%PDF	*.pdf	PDF files
0x0A2525454F460A	*.pdf	PDF file
.%%EOF.	*.pdf	PDF file

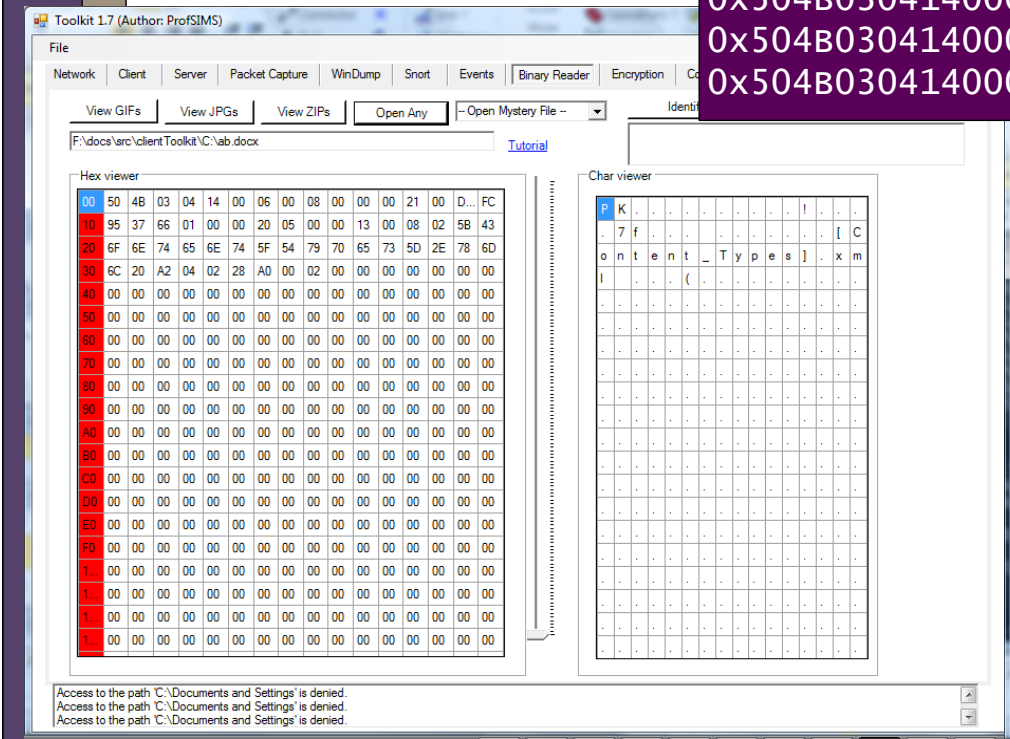


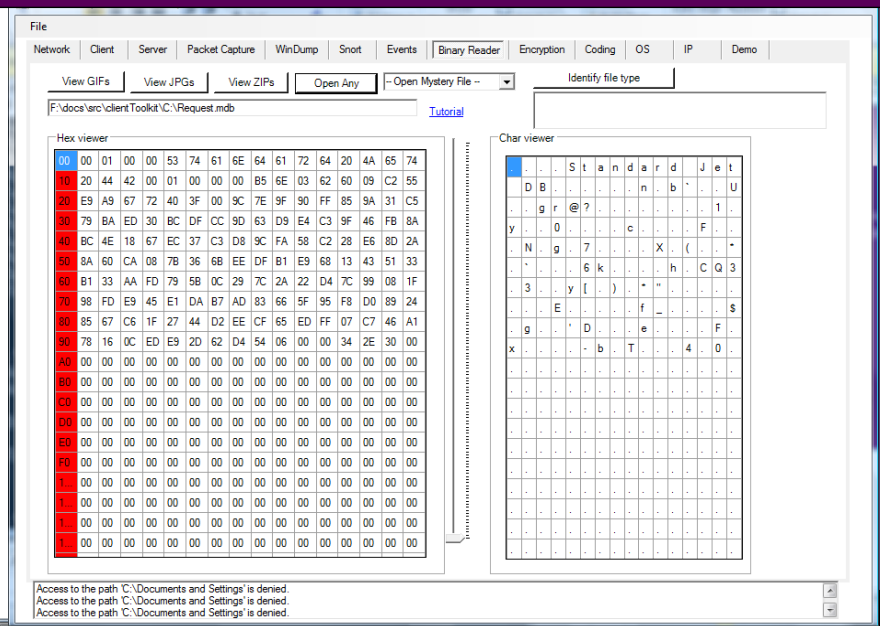


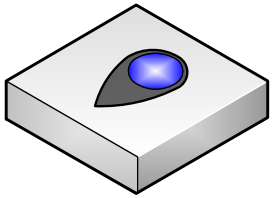
File signature

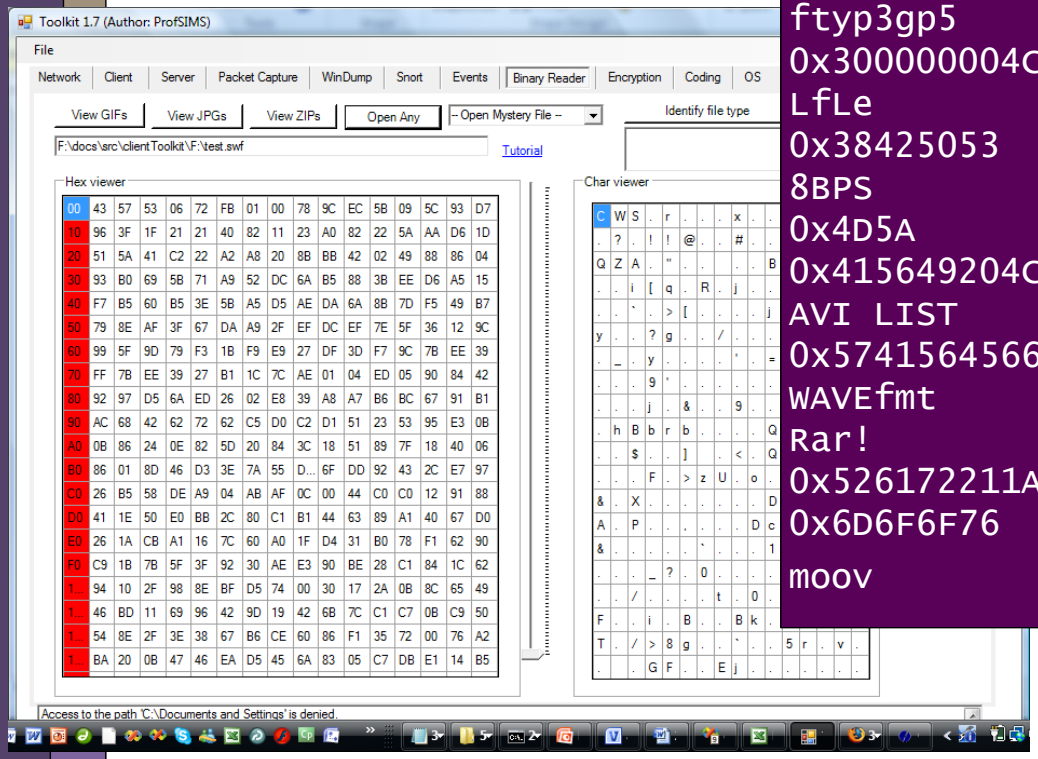
Sig	File ext	File type
0x006E1EF0	*.ppt	PPT
0xA0461DF0	*.ppt	PPT
0xECA5C100	*.doc	Doc file
0x00010000 5374616E 64617264 204A6574 204442		
	*.mdb	Microsoft database
Standard Jet DB	*.mdb	Microsoft database
0x2142444E	*.pst	PST file
!BDN	*.pst	PST file
0x0908100000060500	*.xls	XLS file
0xD0CF11E0A1B11AE1	*.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











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
0x0000001866747970336770 35	*.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

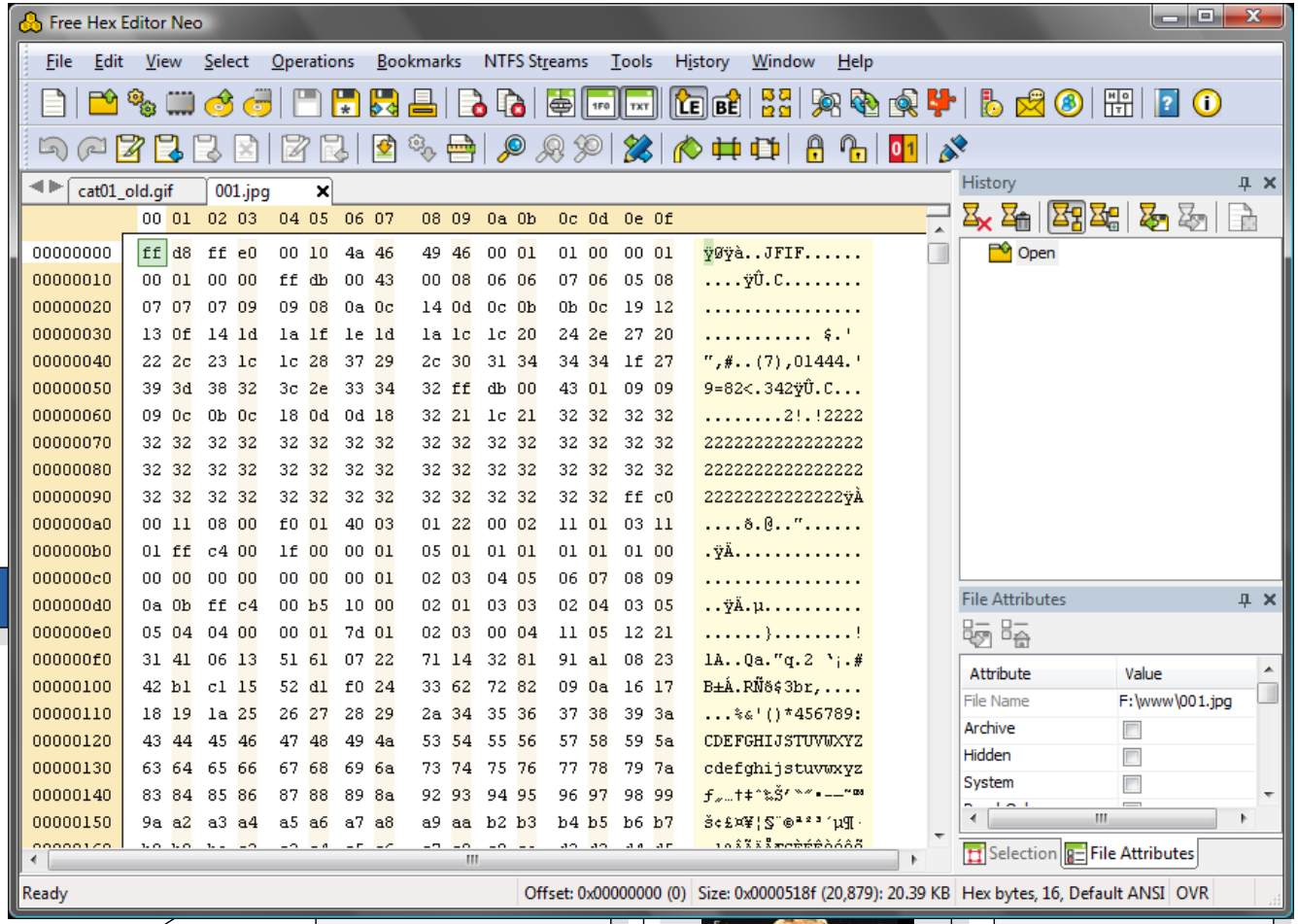
File signature

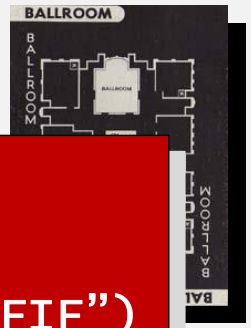
Myphoto.jpg

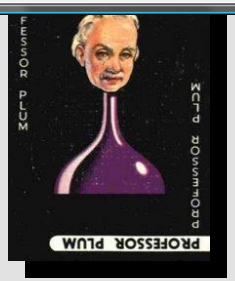
↓

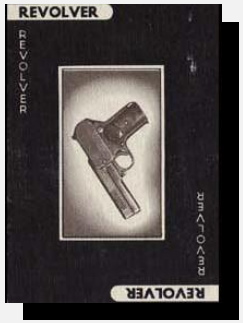
Myphoto.dll

Obfuscation





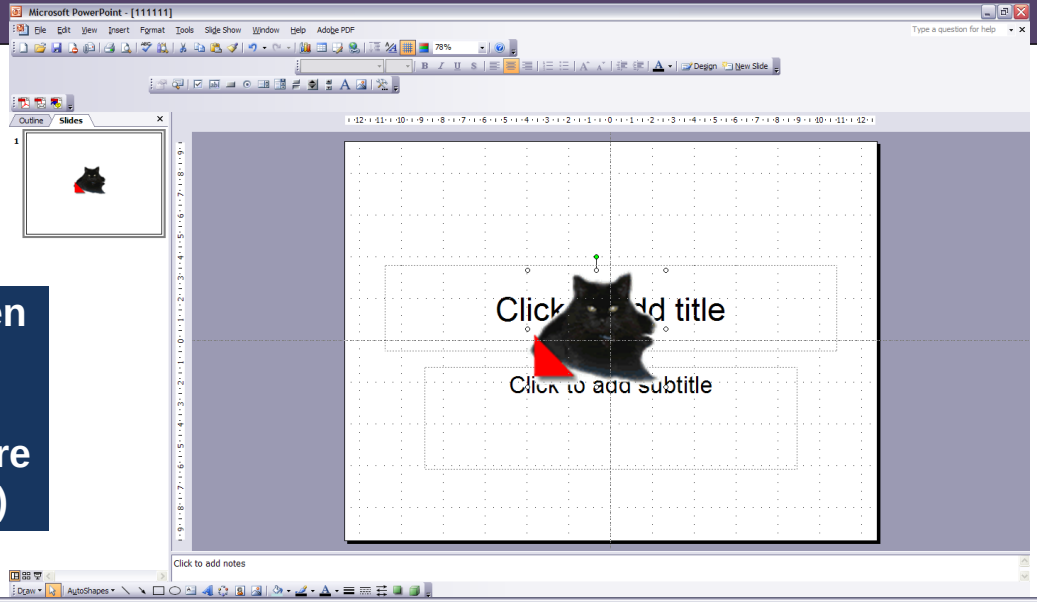




….JFIF...

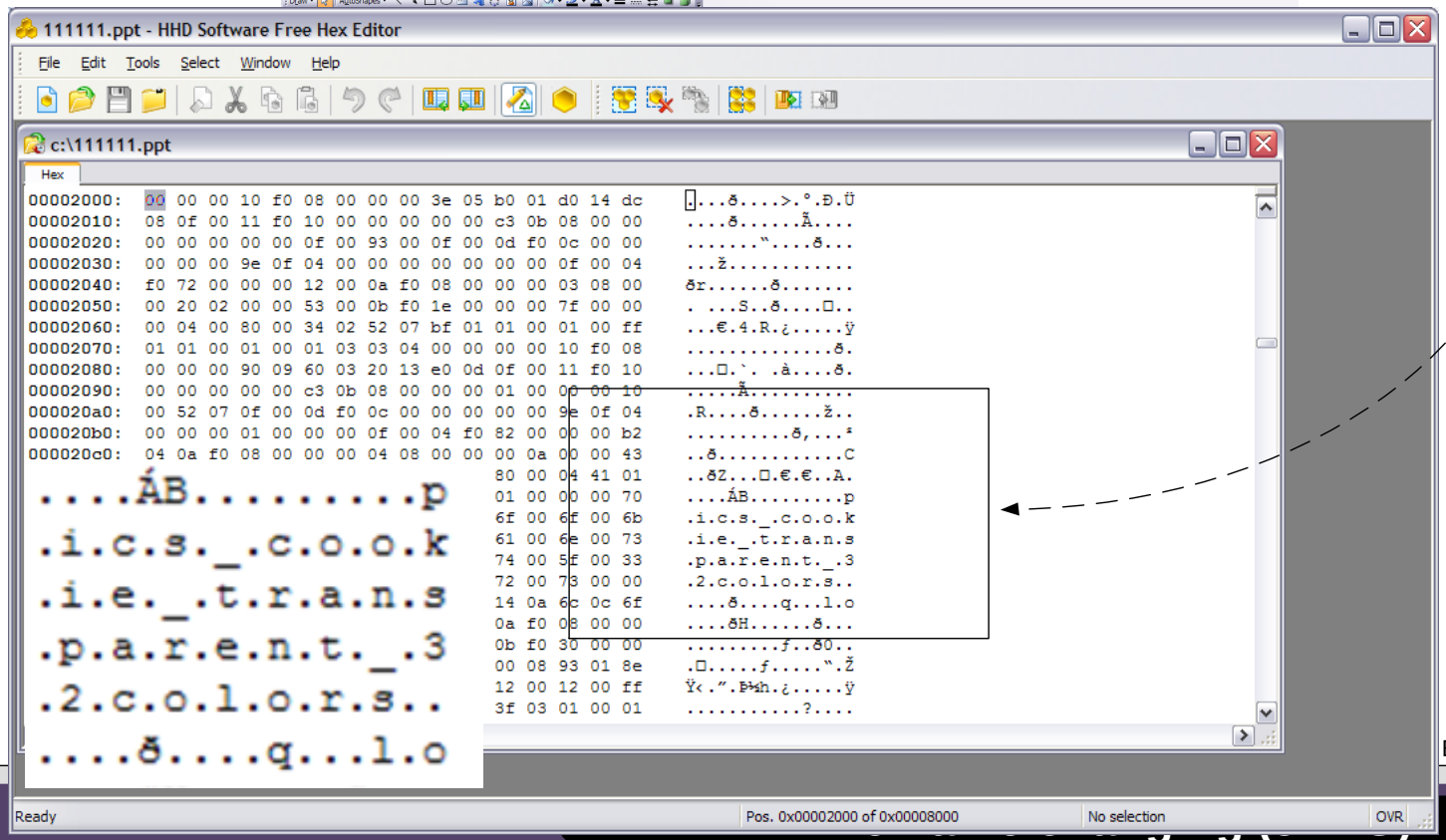
```
Header:   FFD8
Length:   <2 bytes>
Next:     4A,46,49,46,00 ("JFIF")
```

File name changing (JPEG)



Graphic has been imported into PowerPoint (cookie_transparent_32colors.gif)

Meta-data Is still stored in file (but 16-bit character format)



Obfuscation

Forensic

Myzip.zip

Myzip.doc

Obfuscation

Forensic

Free Hex Editor Neo

File Edit View Select Operations Bookmarks NTFS Streams Tools History Window Help

go.zip

```
00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
00000000  50 4b 03 04 14 00 02 00 08 00 50 72 49 39 9e de  PK........PrI9žÞ
00000010  b7 35 a9 00 00 00 5c 01 00 00 06 00 00 00 67 6f  ·5©...\.......go
00000020  2e 62 61 74 6d cf 5f 0b 82 40 0c 00 f0 f7 a0 ef  .batmÏ_.‚@..ð÷ ï
00000030  b0 3e 80 04 bd 08 be d9 79 92 a0 79 dc b4 0c f6  °>€.½.¾Ùy' yÜ´.ö
00000040  22 26 15 85 81 a7 20 7d fa ba fc 43 c6 71 b0 1b  "&.… § }úºüCÆq°.
00000050  6c 3f b6 55 65 03 ad 2a e1 e6 00 51 51 3f 2c f5  l?¶Ue.-*áæ.QQ?,õ
00000060  2c ce 79 93 53 a1 ba 0e d6 9f 52 ed e8 74 b9 58  ,Îy"S¡º.ÖŸRíèt¹X
00000070  55 43 eb 45 b7 46 5c 5a ae 10 48 99 f8 7e c7 60  UCëE·F\Z®.H™ø~Ç`
00000080  9f 09 3c c8 89 d8 9b 1f 72 1d 09 26 ae ef 53 1f  Ÿ.<È‰Ø›.r..&®ïS.
00000090  53 e4 12 09 d9 8e c5 91 20 86 f6 c6 8c ef 13 96  Sä..ÙŽÅ' †öÆŒï.–
                                  56 7d 36 13 23 50 f3 69 1e 17  $9sÃ Of}6.#Póï..
                                  3b 0e 00 e6 65 5e 0e 0c c2 0b  .,ù-Öt<..æe^..Â.
                                  36 0c d8 1f d0 ef 0d 50 4b 01  ¤MxB.é6.Ø.Ðï.PK.
000000d0  02 14 00 14 00 02 00 08 00 50 72 49 39 9e de b7  .........PrI9žÞ·
000000e0  35 a9 00 00 00 5c 01 00 00 06 00 24 00 00 00 00  5©...\.....$....
000000f0  00 01 00 20 00 00 00 00 00 00 00 67 6f 2e 62 61  ... .......go.ba
00000100  74 0a 00 20 00 00 00 00 00 01 00 18 00 60 56 e5  t.. .........`Vå
```

History

Open

File Attributes

Attribute	Value
File Name	C:\go.zip

```
00    ZIPLOCSIG    HEX   04034B50     ;Local File Header Signature
04    ZIPVER       DW    0000         ;Version needed to extract
06    ZIPGENFLG    DW    0000         ;General purpose bit flag
08    ZIPMTHD      DW    0000         ;Compression method
0A    ZIPTIME      DW    0000         ;Last mod file time (MS-DOS)
0C    ZIPDATE      DW    0000         ;Last mod file date (MS-DOS)
0E    ZIPCRC       HEX   00000000     ;CRC-32
12    ZIPSIZE      HEX   00000000     ;Compressed size
16    ZIPUNCMP     HEX   00000000     ;Uncompressed size
1A    ZIPFNLN      DW    0000         ;Filename length
1C    ZIPXTRALN    DW    0000         ;Extra field length
1E    ZIPNAME      DS    ZIPFNLN      ;filename
```

File name changing (ZIP)

```
c:\SMALL_~1>scalpel.exe "nps-2010-emails (1).raw" -o out5
Scalpel version 2.0
Written by Golden G. Richard III and Lodovico Marziale.
Multi-core CPU threading model enabled.
Initializing thread group data structures.
Creating threads...
Thread creation completed.

Opening target "c:\SMALL_~1\nps-2010-emails (1).raw"

Image file pass 1/2.
nps-2010-emails (1).raw: 100.0% |**********************|   10.0 MB    00:00 ETA
Allocating work queues...
Work queues allocation complete. Building work queues...
Work queues built.  Workload:
jpg with header "\xff\xd8\xff\xe0\x00\x10" and footer "\xff\xd9" --> 19 files
Carving files from image.
Image file pass 2/2.
nps-2010-emails (1).raw: 100.0% |**********************|   10.0 MB    00:00 ETA
nps-2010-emails (1).raw: 100.0% |**********************|   10.0 MB    00:00 ETA
Processing of image file complete. Cleaning up...
Done.
Scalpel is done, files carved = 19, elapsed  = 1 secs.
```

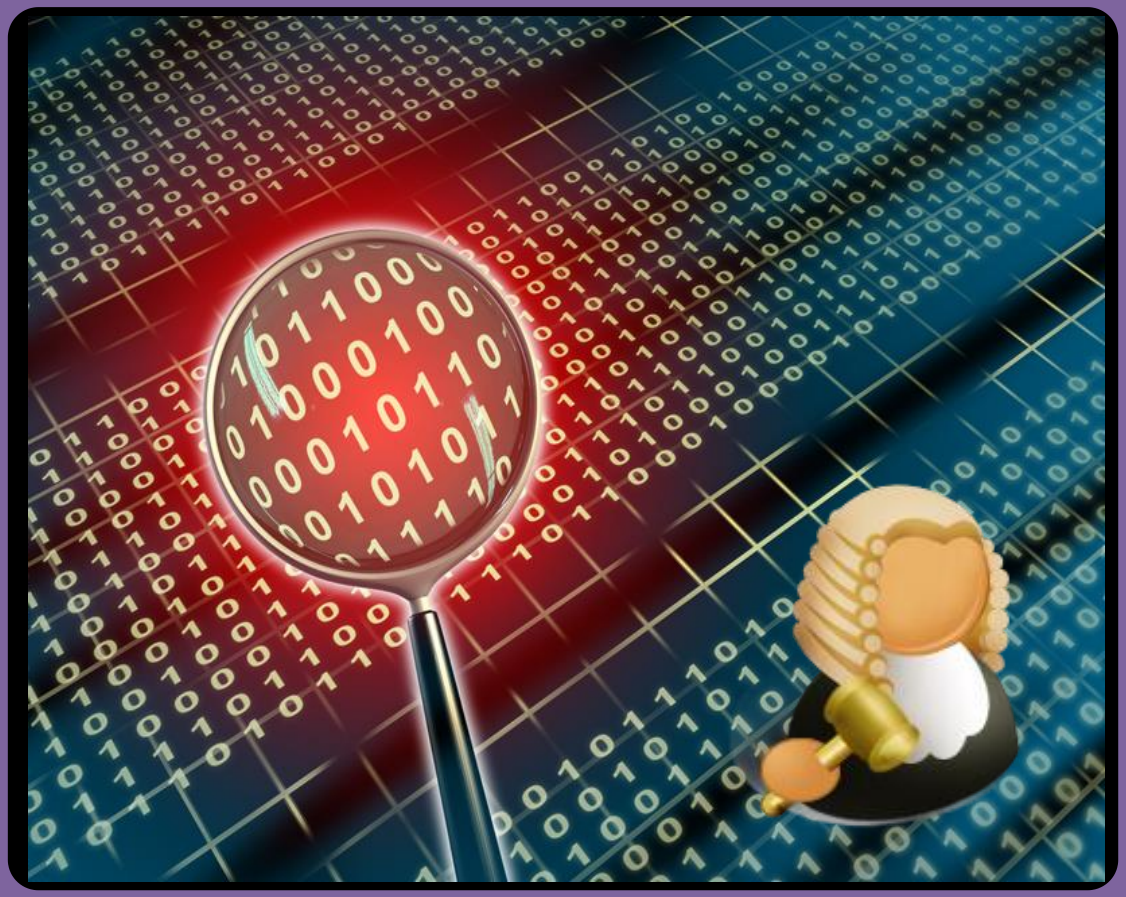
Maximum carve size

	case	size	header	footer
jpg	y	5000:100000	\xff\xd8\xff\xe0\x00\x10	\xff\xd9
avi	y	50000000	RIFF????AVI	
mov	y	10000000	????moov	
fws	y	4000000	FWS	
mp3	y	8000000	\xFF\xFB??\x44\x00\x00	

Author: Prof Bill Buchanan

Using scalpel

Steganography



Huffman Coding/XOR

Author: Prof Bill Buchanan

Letter:	'b'	'c'	'e'	'i'	'o'	'p'
No. of occurrences:	12	3	57	51	33	20

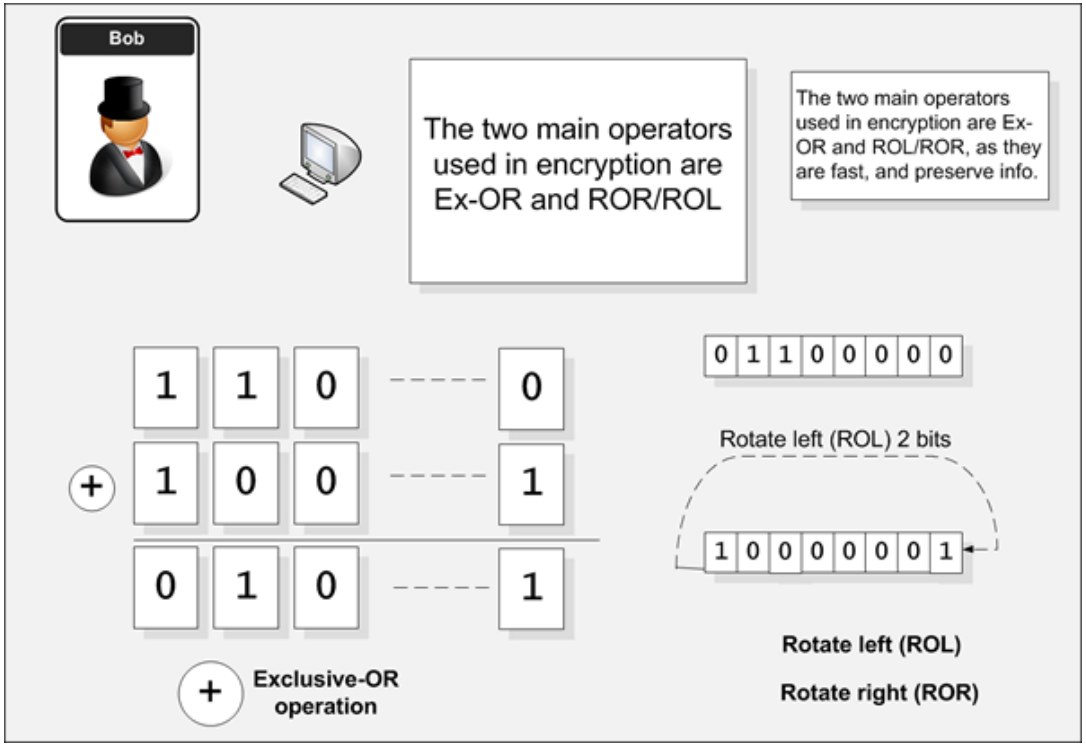
Letter:	'e'	'i'	'o'	'p'	'b'	'c'
No.	57	51	33	20	12	3

```
'e' 57 ----------------------→  57 [1]→ 108 [1]
'i' 51 ----------------------→ 51 [0]
'o' 33                → 33 [0] →       ->  68 [0]
'p' 20      →20 [1] → 35 [1]
'b' 12 [1] →15 [0]
'e' 3  [0]
```

'e' 11 'i' 10
'o' 00 'p' 011
'b' 0101 'c' 0100

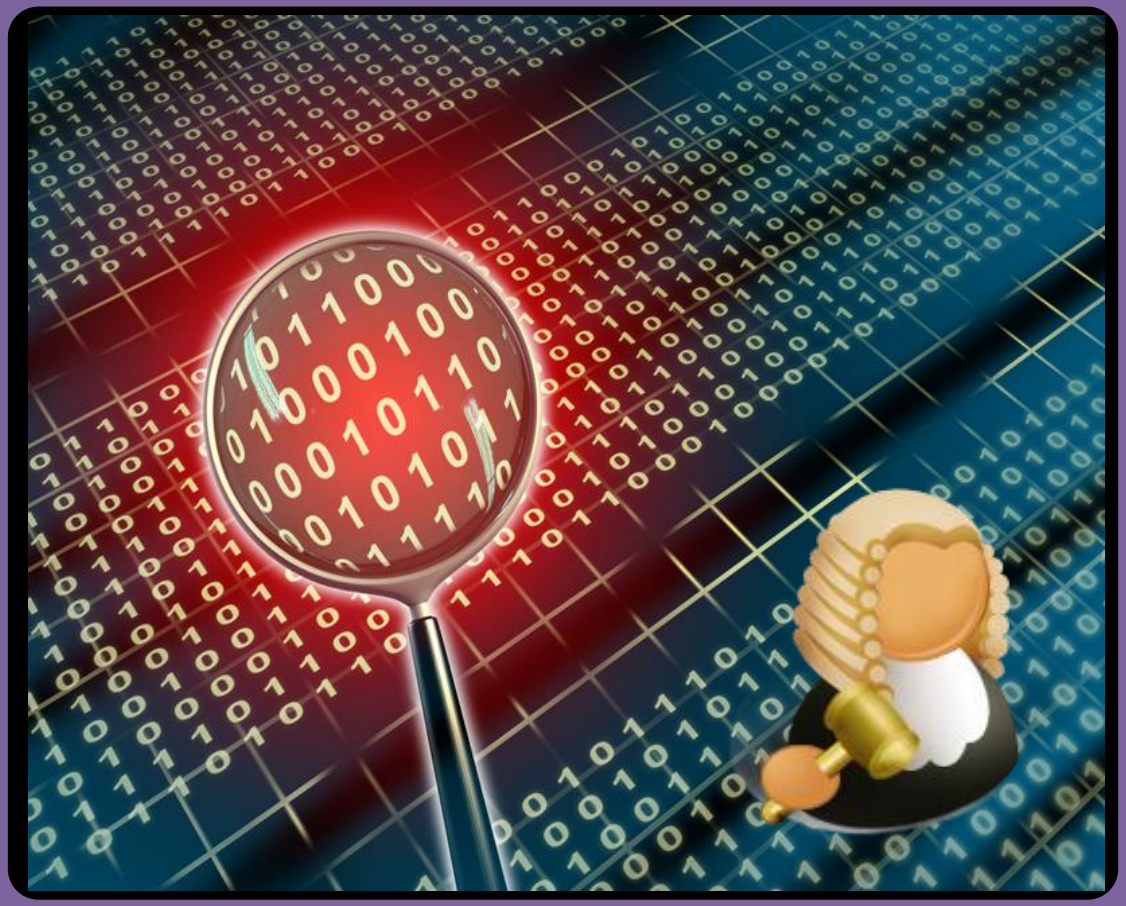
0110011

String	ASCII (Result)	Hex (Result)	Hex (Base-64)	Hex (Binary)
Input	napier	6E6170696572	bmFwaWVy	01101110 01100001 01110000 01101001 01100101 01110010
Key	tttttt			01110100 01110100 01110100 01110100 01110100 01110100
Encoded		1A15041D1106	GhUEHREG	00011010 00010101 00000100 00011101 00010001 00000110



Author: Prof Bill Buchanan

Steganography



Lempel-Ziv/RLE

Author: Prof Bill Buchanan

00000 ‘ ‘
00001 The
00002 boy
00003 stood
00004 on
00005 the
00006 burning
00007 deck
00008 .
00009 end

```
The boy stood on the burning
deck. The end.
```

```
00001 00000 00003 00000 00004 00000 00005
00000 00006 00000 00007 00008 00000 00001
00000 00009 00008
```

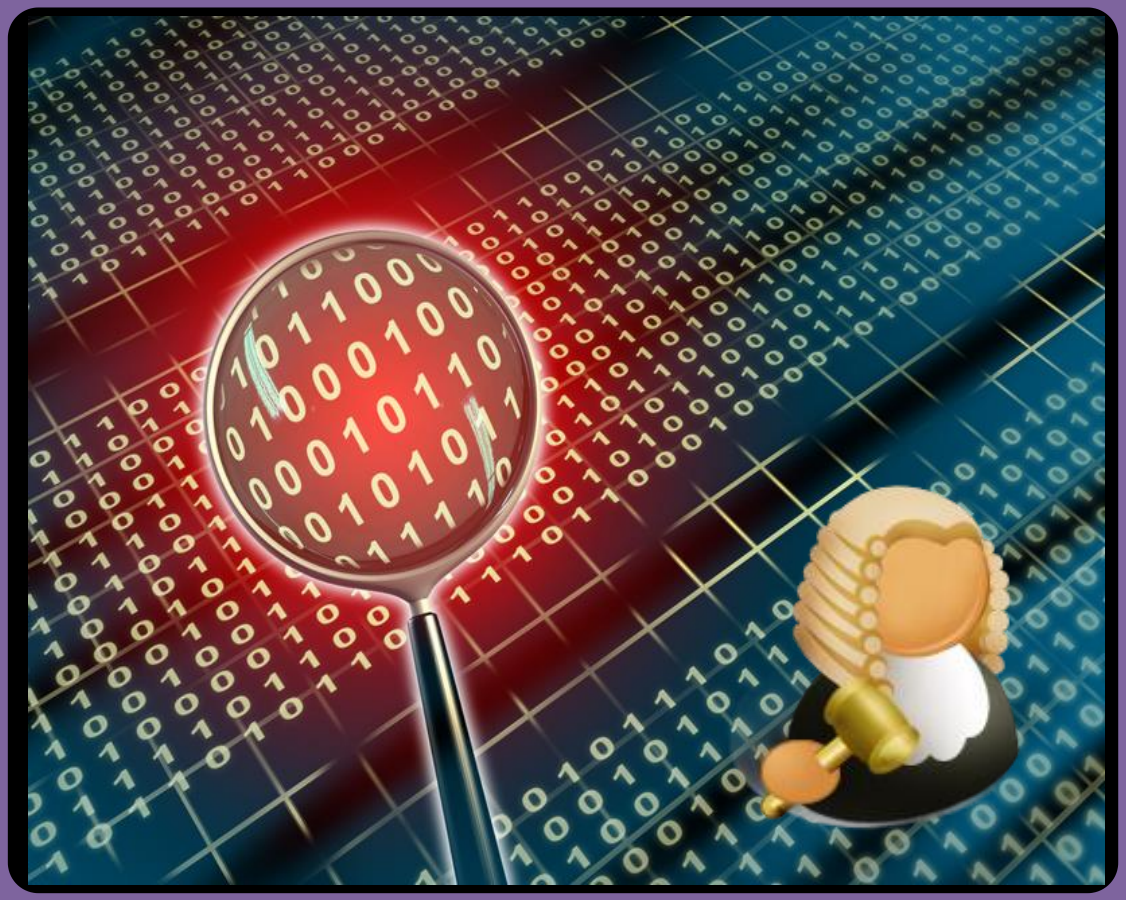
1	1	1	1
1	2	1	1
1	1	1	2
1	1	1	1

```
00001 00001 00001 00001
00001 00002 00001 00001
00001 00001 00001 00002
00001 00001 00001 00001
```

Run Length Encoding (RLE)

```
000001{4} 00002 00001{5} 00002 00001{4}
```

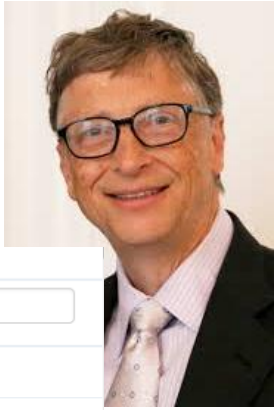
Steganography



Zero-knowledge

Author: Prof Bill Buchanan

Two billionaire problem: How can the billionaires discuss without revealing how much they have and reveal the one with most money?



Bob:	Alice	Carol
2	2	8

Next Bob creates three random values which give a sum of (his vote+100) to give:

Bob 1	Bob 2	Bob 3
72	23	7

Next Alice creates three random values which give a sum of (her vote+100) to give:

Alice 1	Alice 2	Alice 3
42	44	16

Next Carol creates three random values which give a sum of (her vote+100) to give:

Carol 1	Carol 2	Carol 3
91	14	3

Bob gets Alice's second value, and Carol's second value, and adds it to his first value and calculates the sum as: 130

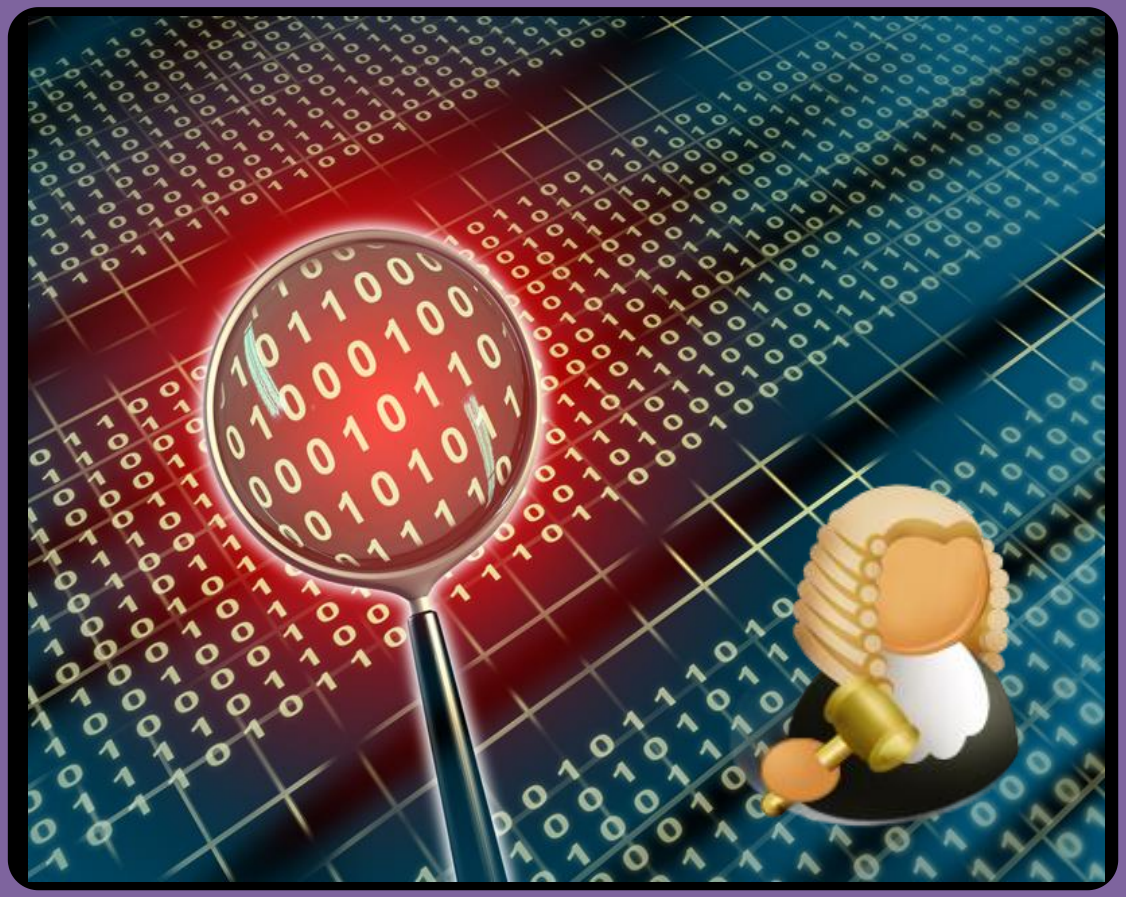
Alice gets Bob's second value, and Carol's third value, and adds it to her first value and calculates the sum as: 68

Carol gets Alice's third value, and Bob's third value, and adds it to her first value and calculates the sum as: 114

Finally Bob, Alice and Carol announce their calculations, and it is added up to: 312

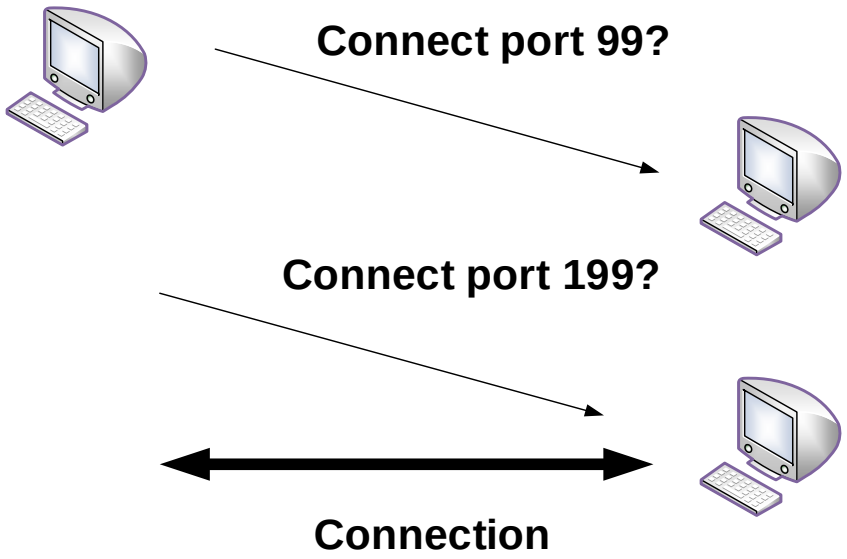
which taken with modulo 100 gives: 12 which should be the total of the votes!!!!! Check the original votes for Bob, Alice Carol and make sure that it totals this value. So ... Bob, Alice and Carol know the total, but not any of votes of the others.

Steganography

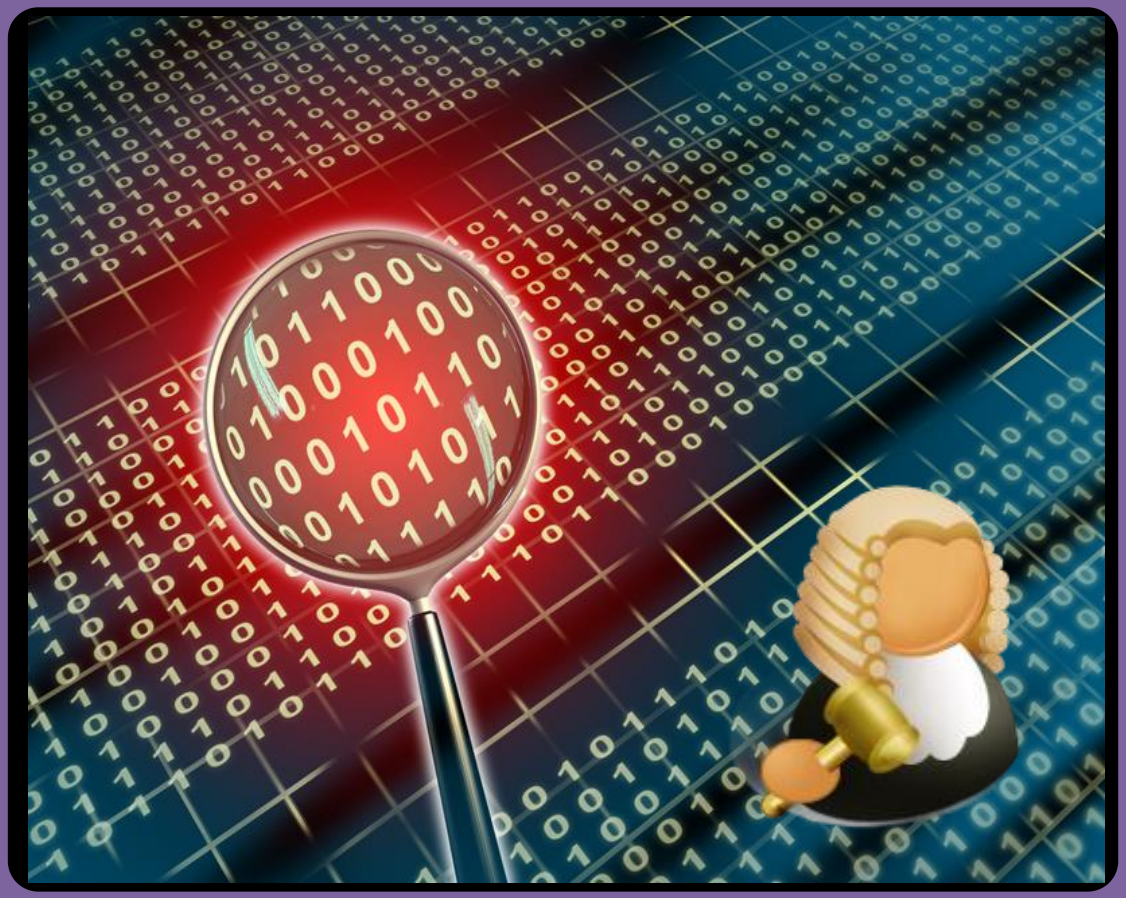


Port Knocking

Author: Prof Bill Buchanan


Connect port 99?
Connect port 199?
Connection

Steganography



Secret Shares

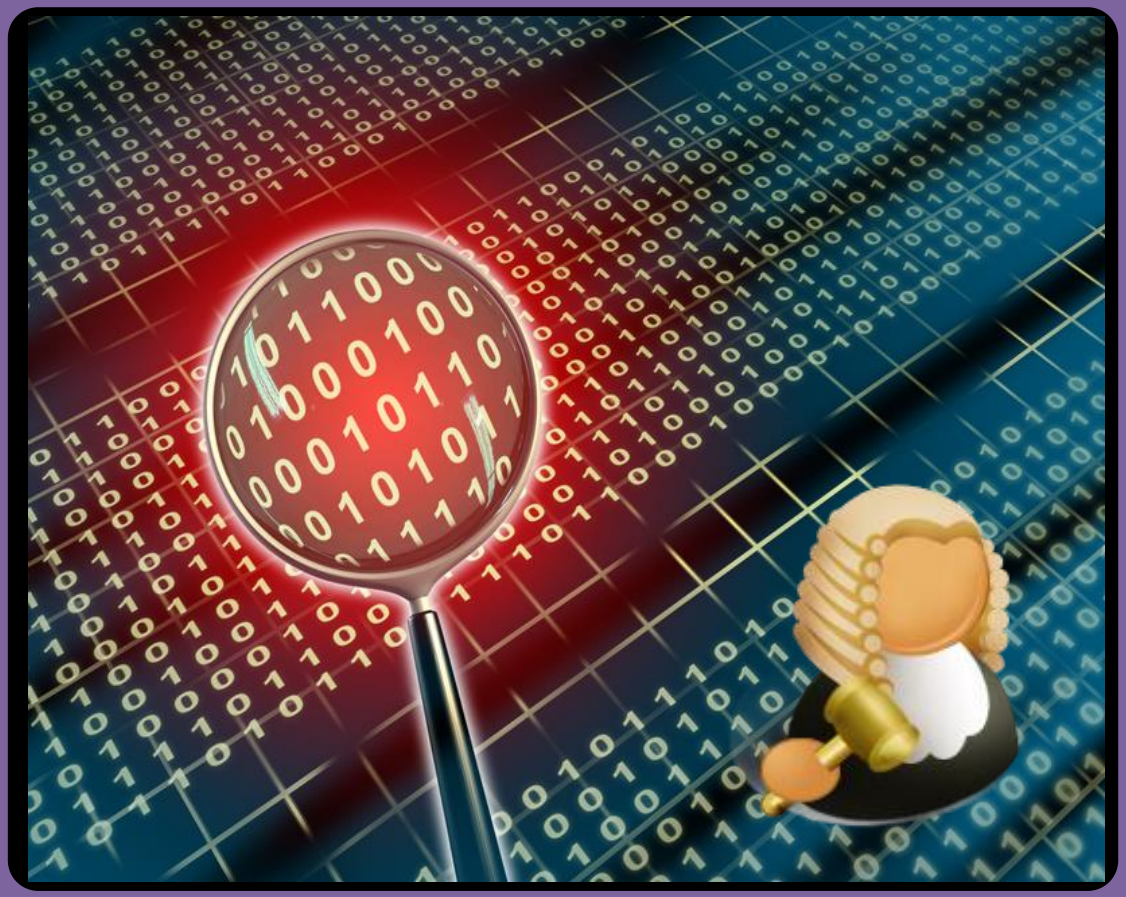
Author: Prof Bill Buchanan

[n,k] - Any k from n shares
k – Threshold, n - shares

X marks the spot (2 from 4):

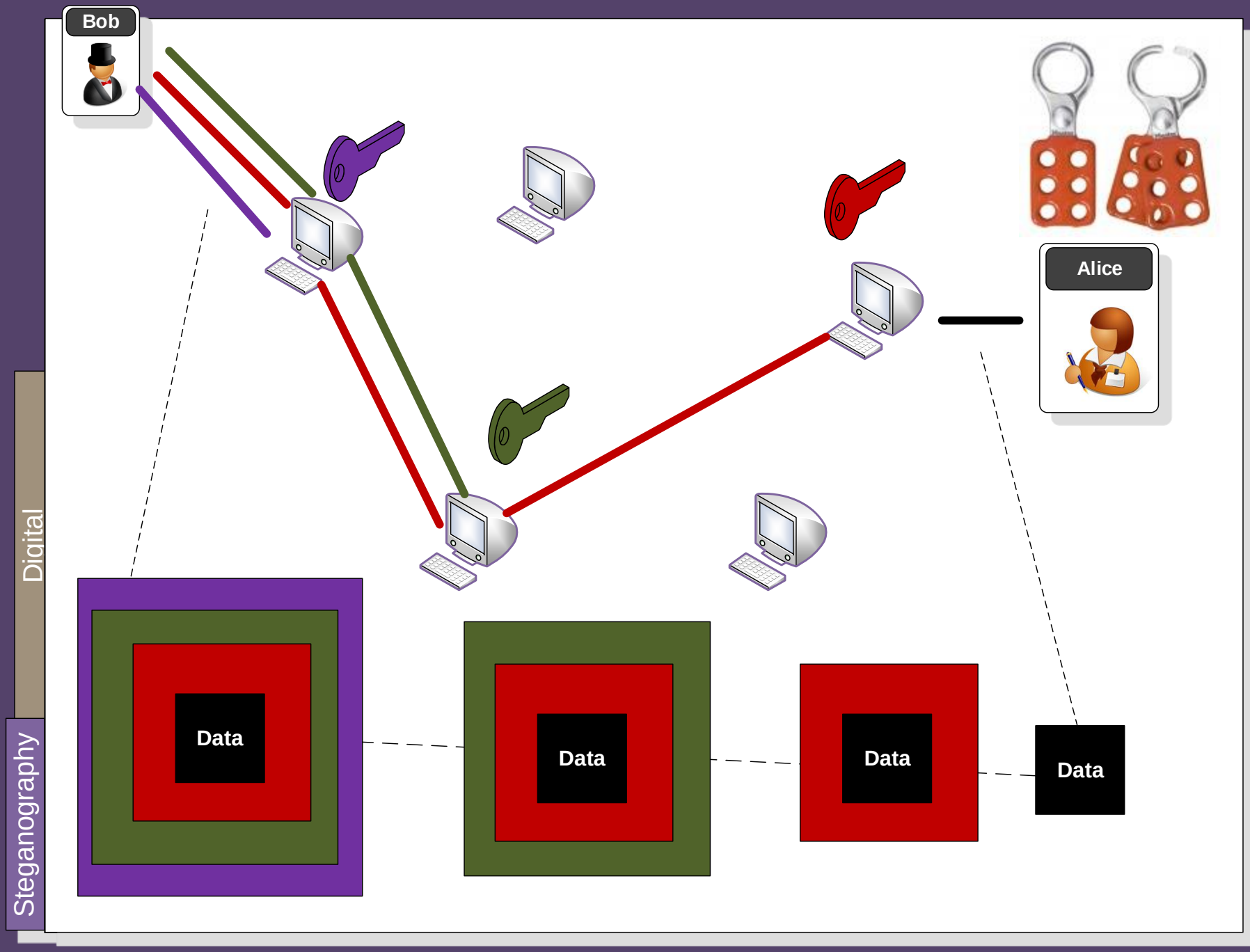
000/EJk2GcZ70S1xLxr/UyWWg==
001jc+Y9wIejQkDhRFjA1R0Yw==
002H1mchq0XK97ZR+b2AX1SpQ==
003btRgqcgQSZNvBkv+/2WwnA==

Steganography



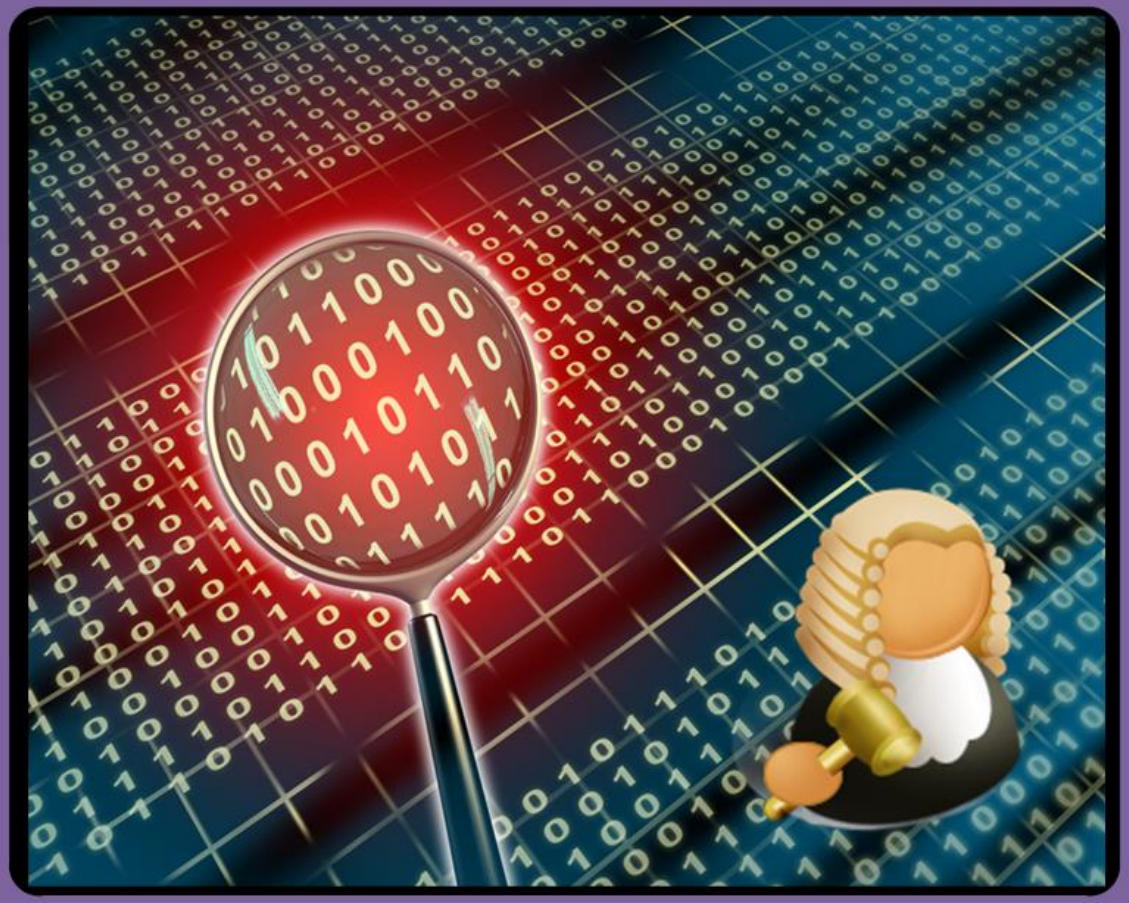
Hidding Source

Author: Prof Bill Buchanan



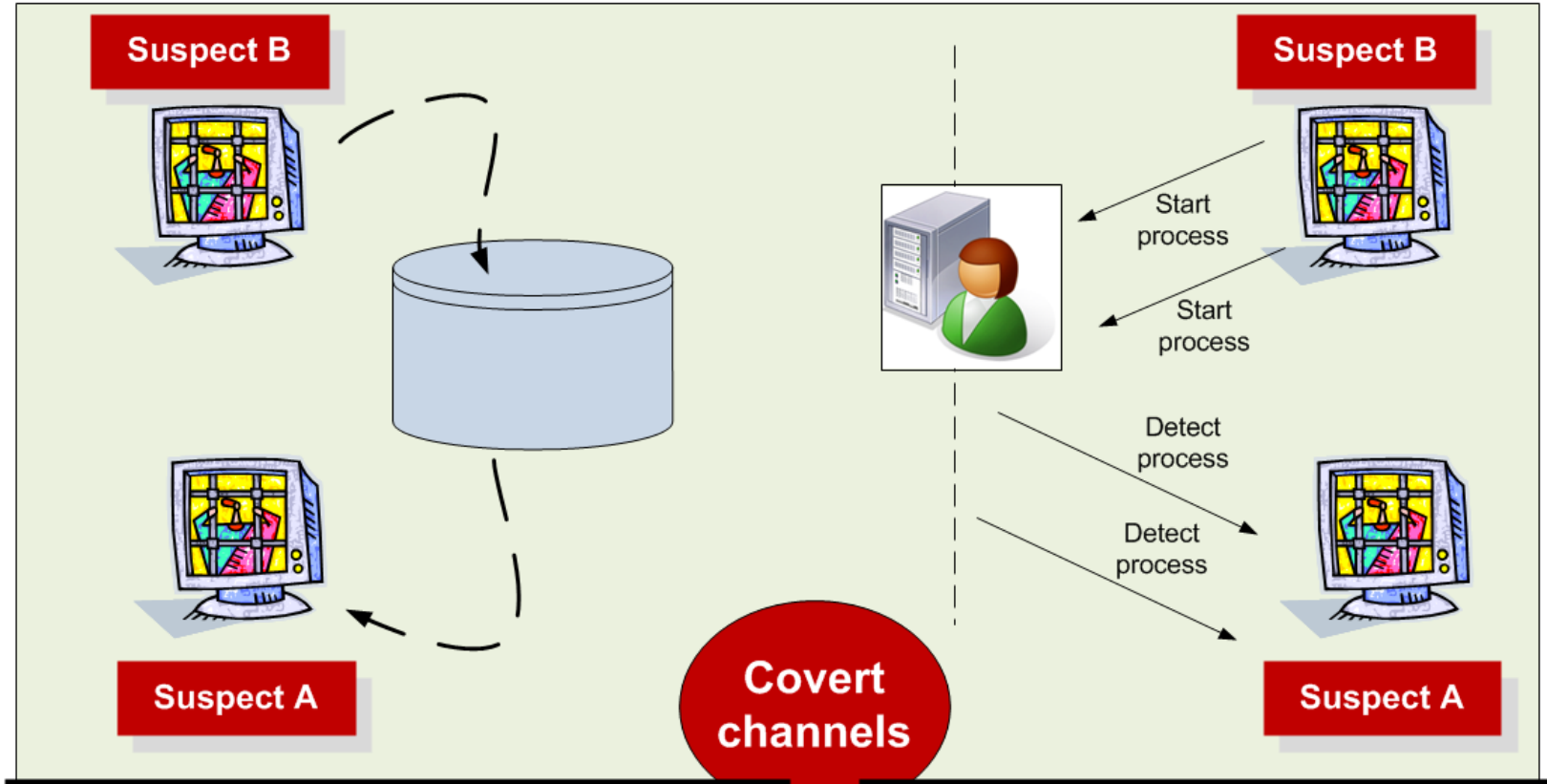
Tor Onion Routing

Data Hiding



Covert Channels

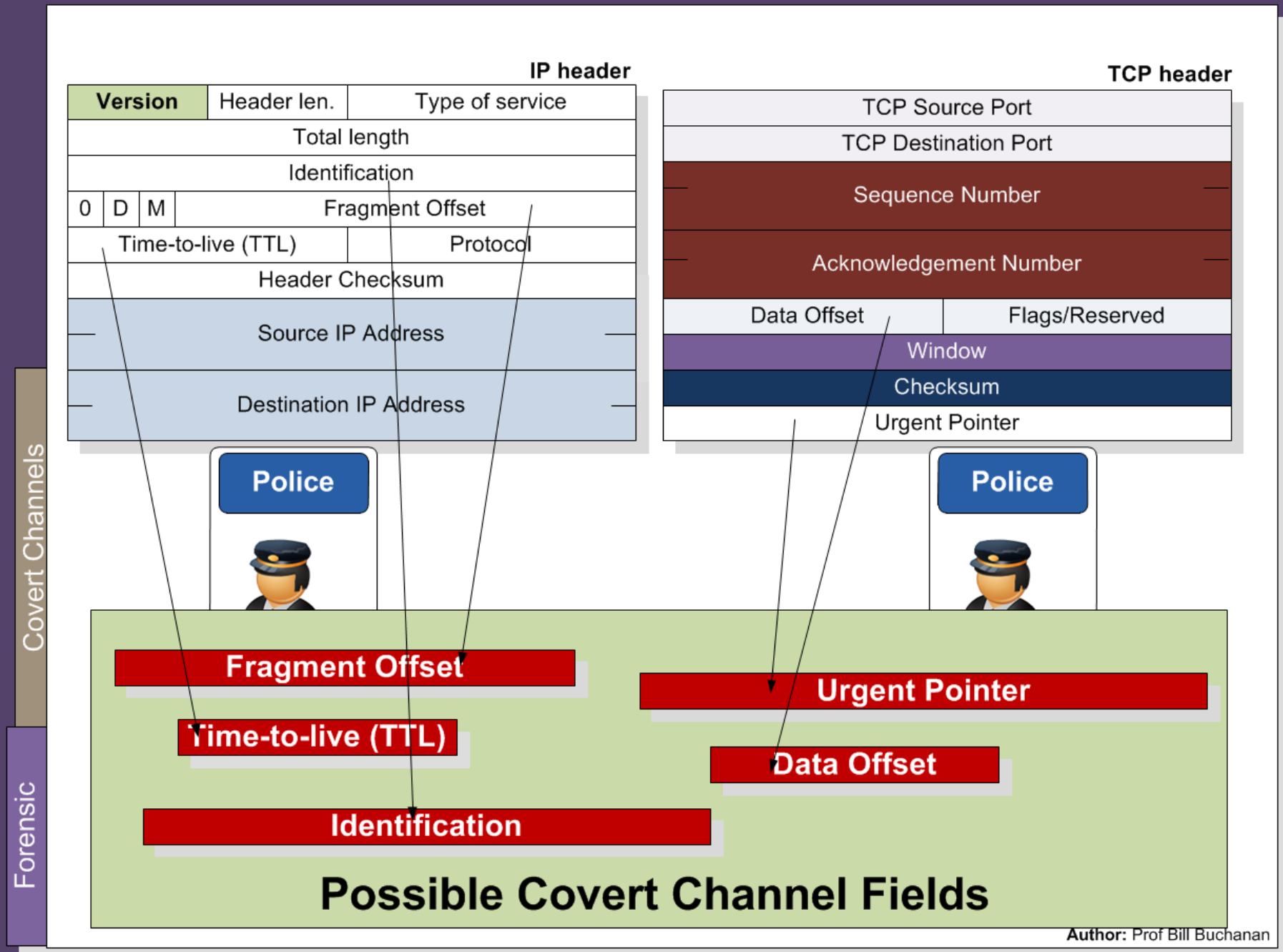
Author: Prof Bill Buchanan



Covert channels

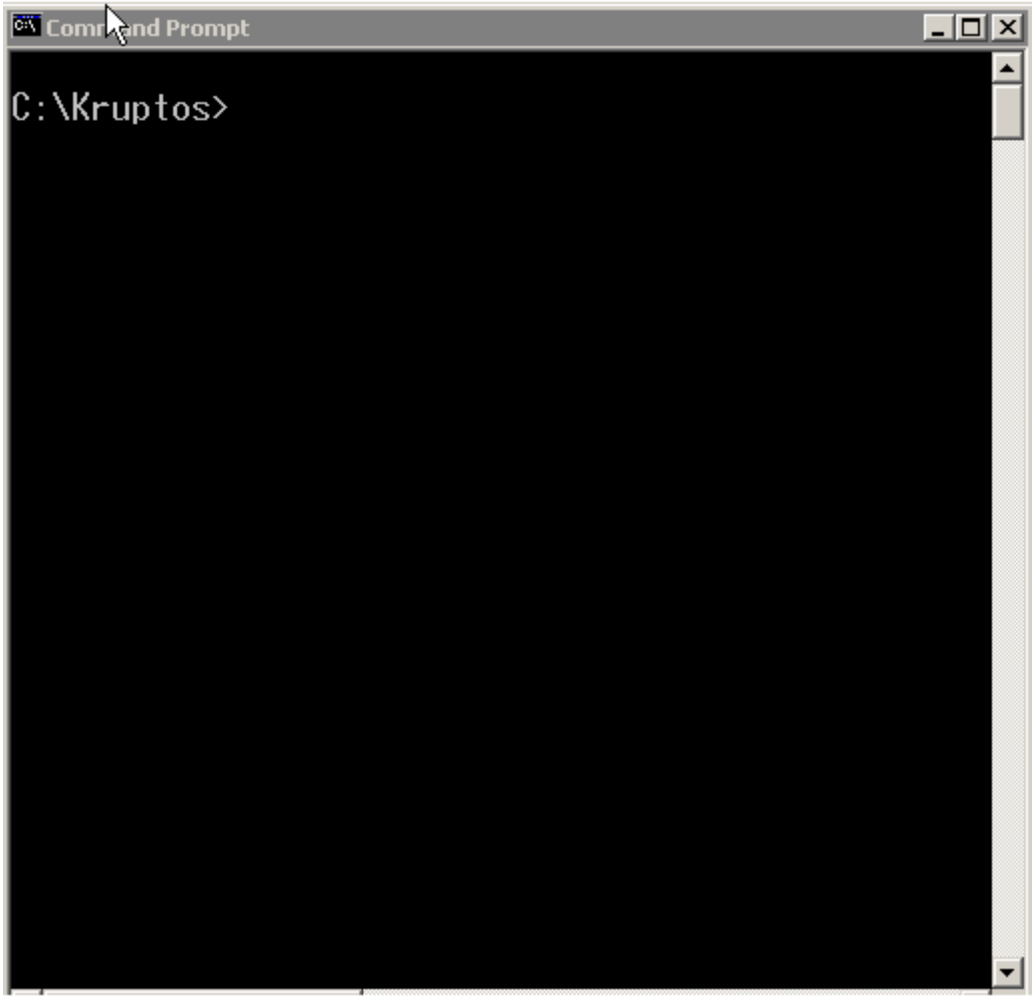
Storage covert channels are where one process uses direct (or indirect) data writing, whilst another process reads the data. It generally uses a finite system resource that is shared between entities with different privileges.

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

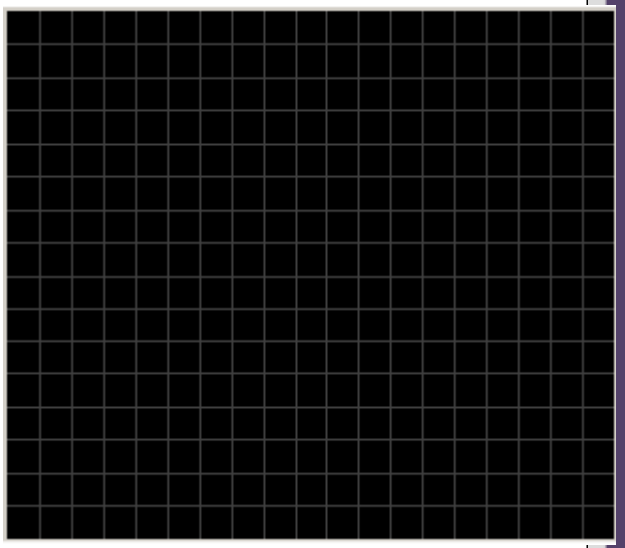


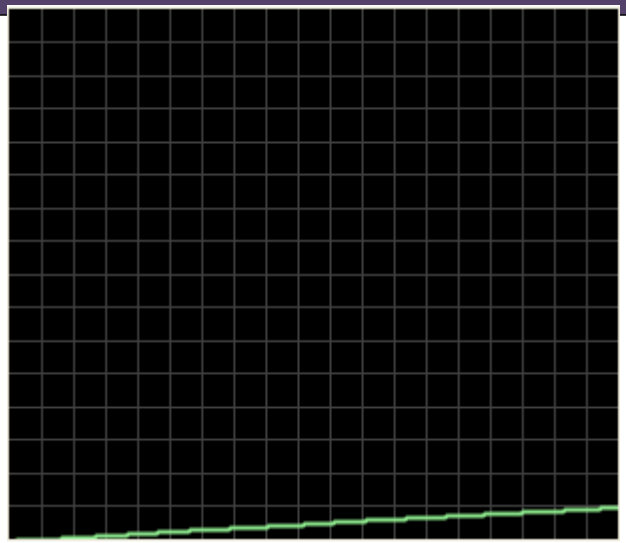
IP and TCP Covert Channels

IPv4ID – Authoritative definition - Monitoring traffic

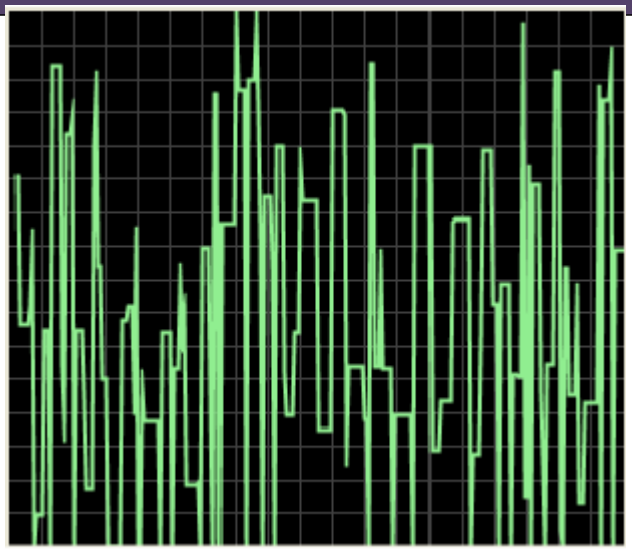


המוסד למודיעין ולתפקידים מיוחדים
ISRAEL SECRET INTELLIGENCE SERVICE

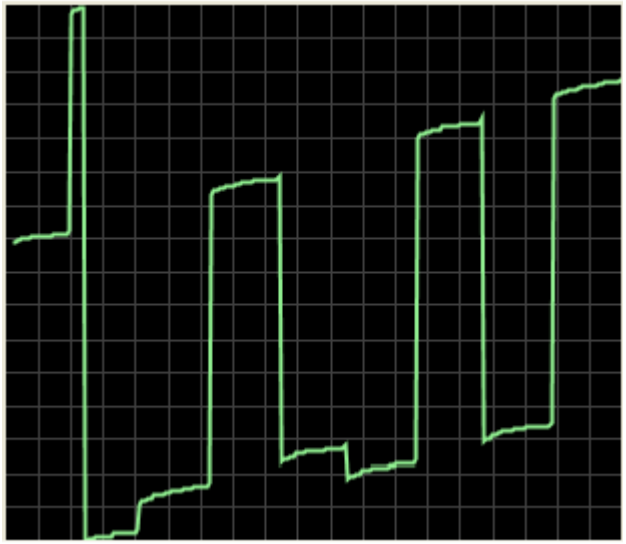




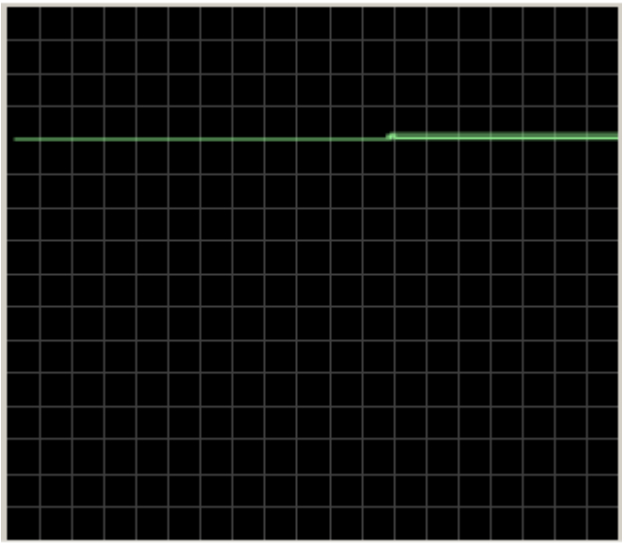
MS Windows – http://www.covertchannels.org



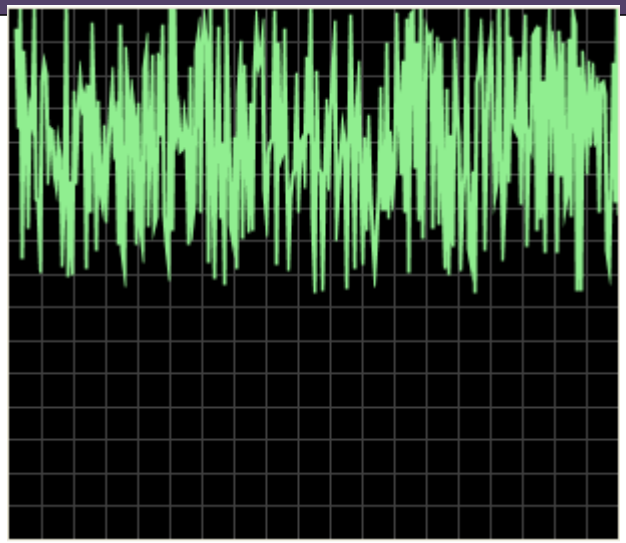
Linux 2.4.x



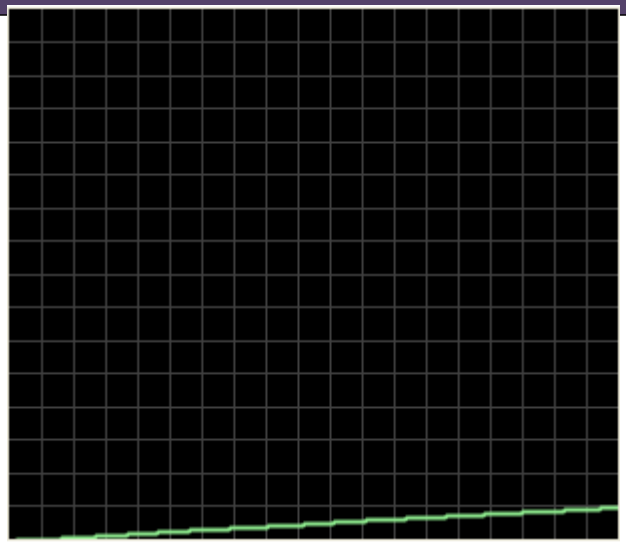
SUN Solaris – http://www.ebay.co.uk



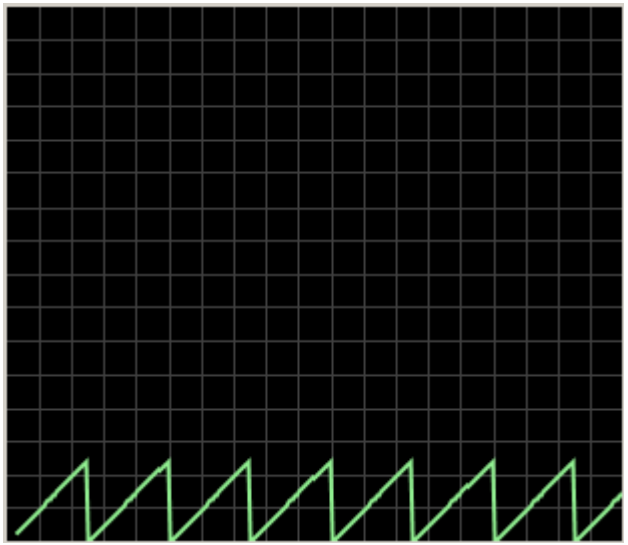
OpenBSD – http://www.openbsd.org



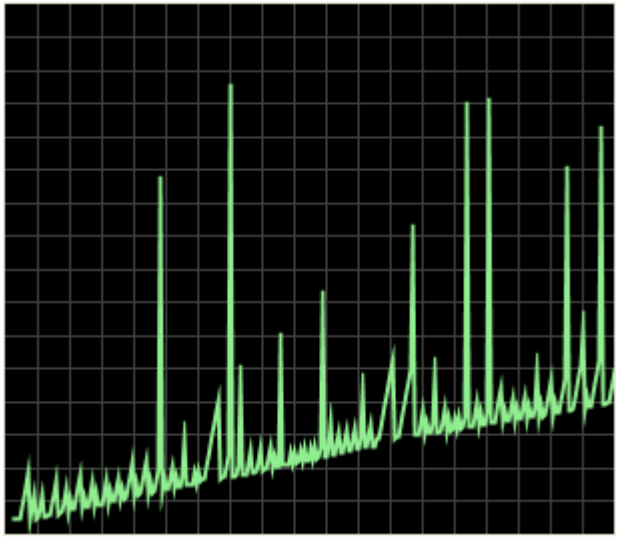
Webwall - http://www.dstl.gov.uk



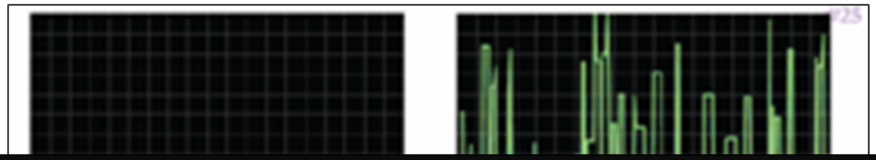
Reverse Proxy Server – http://test.dstl.info



Real Covert channel based on IPv4ID



Unknown



Version	Header len.	Type of service
Total length		
Identification		

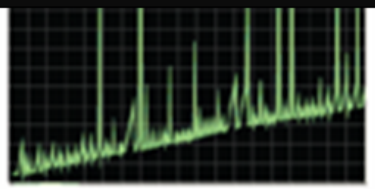
```
No.     Time        Source              Destination         Protocol Info
      3 0.001525    192.168.75.132      192.168.75.1        TCP      afrog >
http [SYN] Seq=0 Win=64240 Len=0 MSS=1460
    Identification: 0x008c (140)

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

Steganography

- Some methods.
- Discriminators.
- Covert channels.
- Port knocking.
- Onion Routing.
- Dictionary.

Author: Prof Bill Buchanan