

Pi Hediyem Vardı, Verdim, Gitti #3 :)

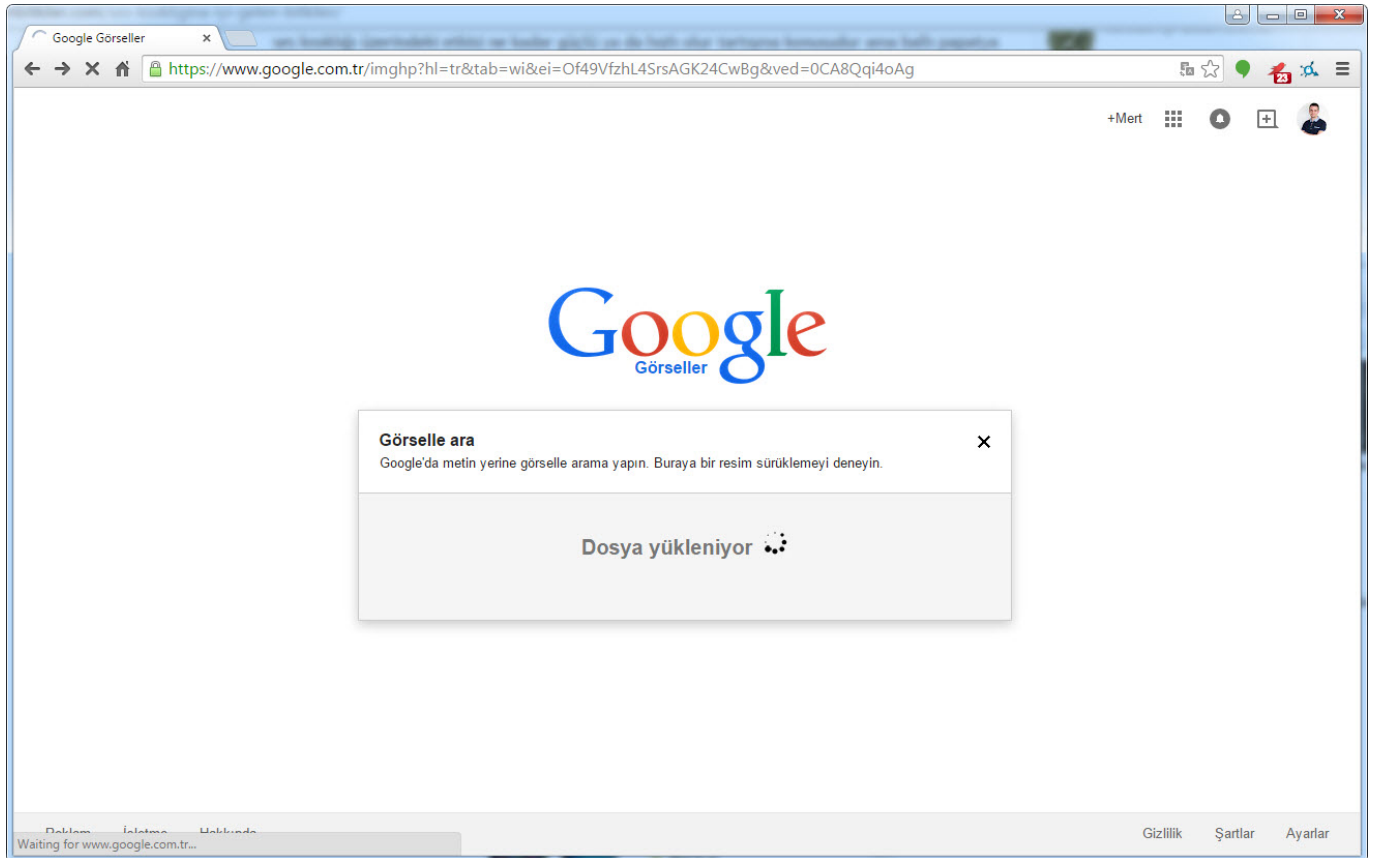
written by Mert SARICA | 5 May 2015

1 Mayıs 2015 tarihinde üçüncüsü düzenlenen Pi Hediyem Var oyununun çözüm yolu ve Raspberry Pi 2 kazanan talihli karşınızda!

ÇÖZÜM YOLU:


Dahi ile deli arasında ince bir çizgi olduğu söylenir.

Aşağıdaki resimde gördüğünüz bir dahi ise, yine bu resimde olan ama göremediğiniz deli kimdir ? sorusu bize aslında bu resim içinde başka bir resmin gizli olabileceğine yani steganografi kullanıldığına dair ipucu veriyordu. Bu ipucundan yola çıkarak Einstein'ın resmini (pihaber6.png) Google görseller üzerinde aratarak resmin orjinalina kısa bir sürede ulaşabilirdik.



Google'da Ara

https://www.google.com.tr/search?tbs=sbi:AMhZzitZvp857uVh9TVUa-XgOWUMH0hJw4kHM9II4s6KosP6fARuEQ



Eşleşen görselleri içeren sayfalar

İş - "Einstein Sizin İçin Çalışsaydı..." - Başlangıcın biraz ilerisi...
kmuratsimsek.blogspot.com/.../is-einstein-sizin-icin-calssayd-...
620 x 747 - 26 Nis 2014 - Muhteşem olurdu değil mi? Düşünsenize tarihin gelmiş geçmiş en büyük zekalarından birisi sizin için çalışıyor. Hangi departmanda olursa ...

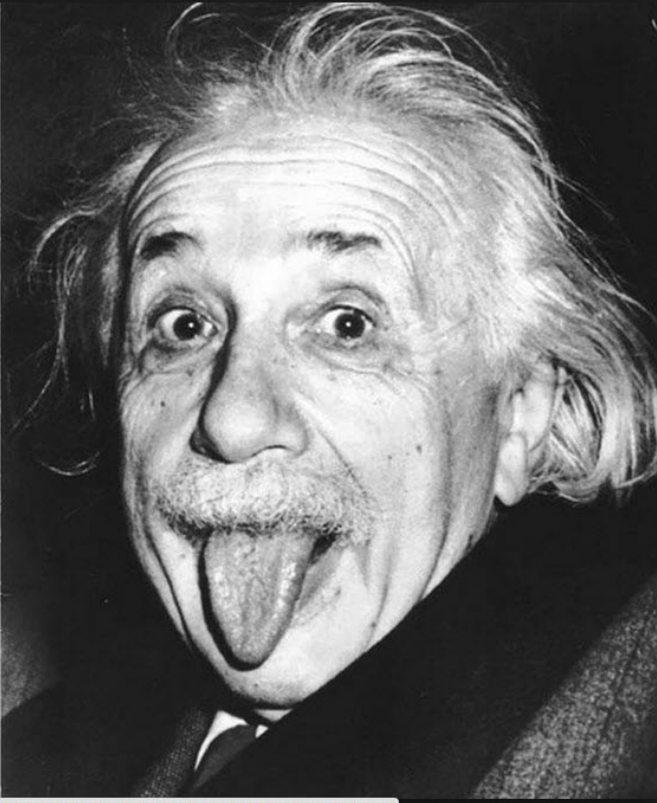
Poster APPLE Think Different Albert Einstein - 50X70 ...
https://www.pinterest.com/.../11603... - Bu sayfanın çevirisini yap
357 x 500 - Poster APPLE Think Different Albert Einstein - 50X70 !! | See more about albert einstein and posters.

Think different on Pinterest | Jane Goodall, Pablo Picasso ...
https://tr.pinterest.com/ericchan2017/think-different/
357 x 500 - Explore eric chan's board "Think different" on Pinterest, a visual bookmarking tool ... Apple •Think Different• ad campaign 1997 poster > Jane GOODALL (brit ...

Poster Apple Think Different Albert Einstein 50x70 | eBay
www.ebay.com/...-/250764766418 - Bu sayfanın çevirisini yap
€21,90 - Stokta Var
357 x 500 - Poster APPLE Think Different Albert Einstein - 50X70 !! in Computers/Tablets & Networking, Vintage Computing, Vintage Computers & Mainframes | eBay.

http://mentalfloss.com/sit

www.google.com.tr/imgres?imgurl=http://mentalfloss.com/sites/default/files/styles/insert_main_wide_image/pub

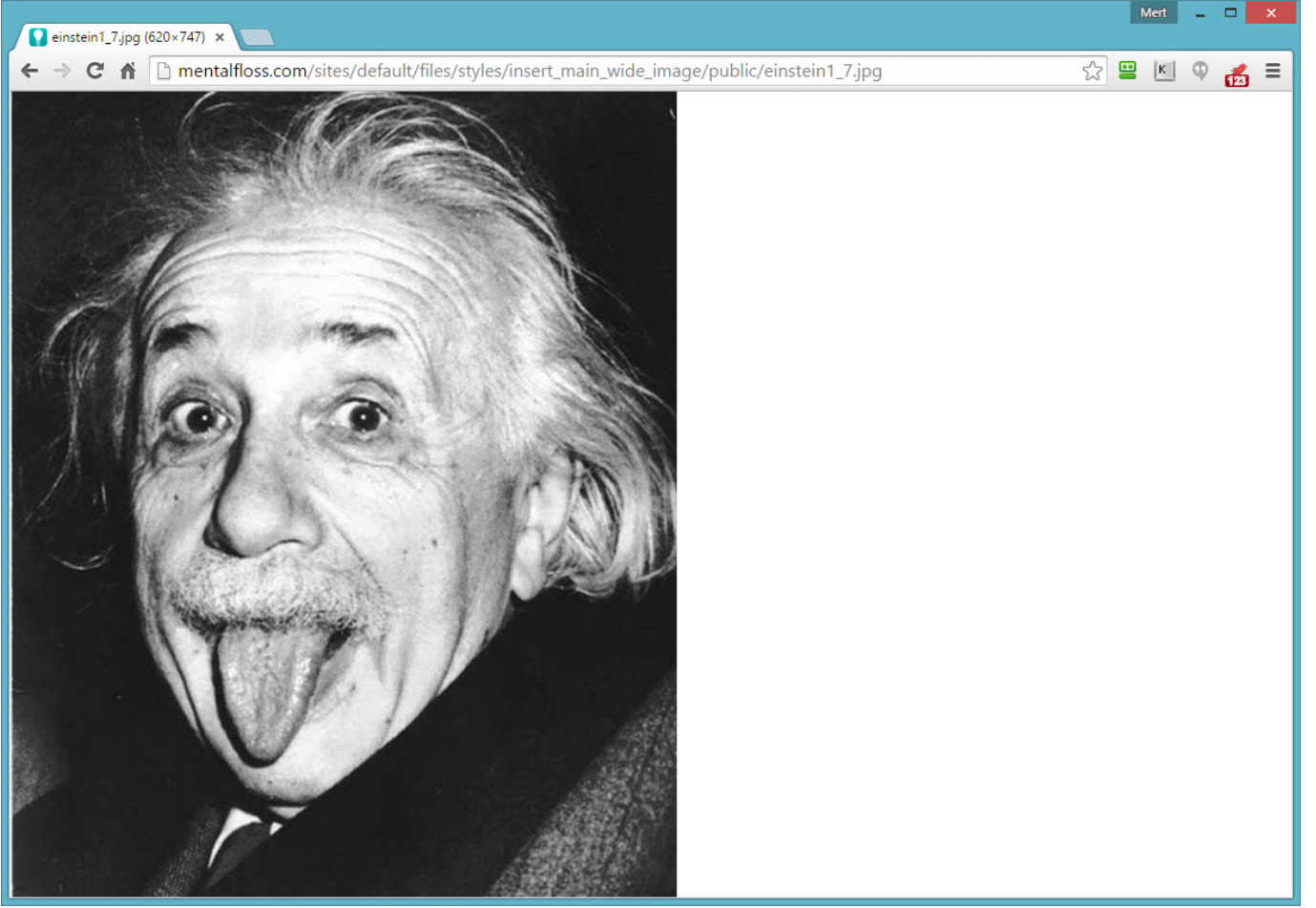


İş - "Einstein Sizin İçin Çalışsaydı..." ...
kmuratsimsek.blogspot.com - 620 x 747 - Görselle ara
Muhteşem olurdu değil mi? Düşünsenize tarihin gelmiş geçmiş en büyük zekalarından birisi sizin için çalışıyor. Hangi departmanda olursa olsun harikalar ...

Sayfayı ziyaret et Resmi görüntüle

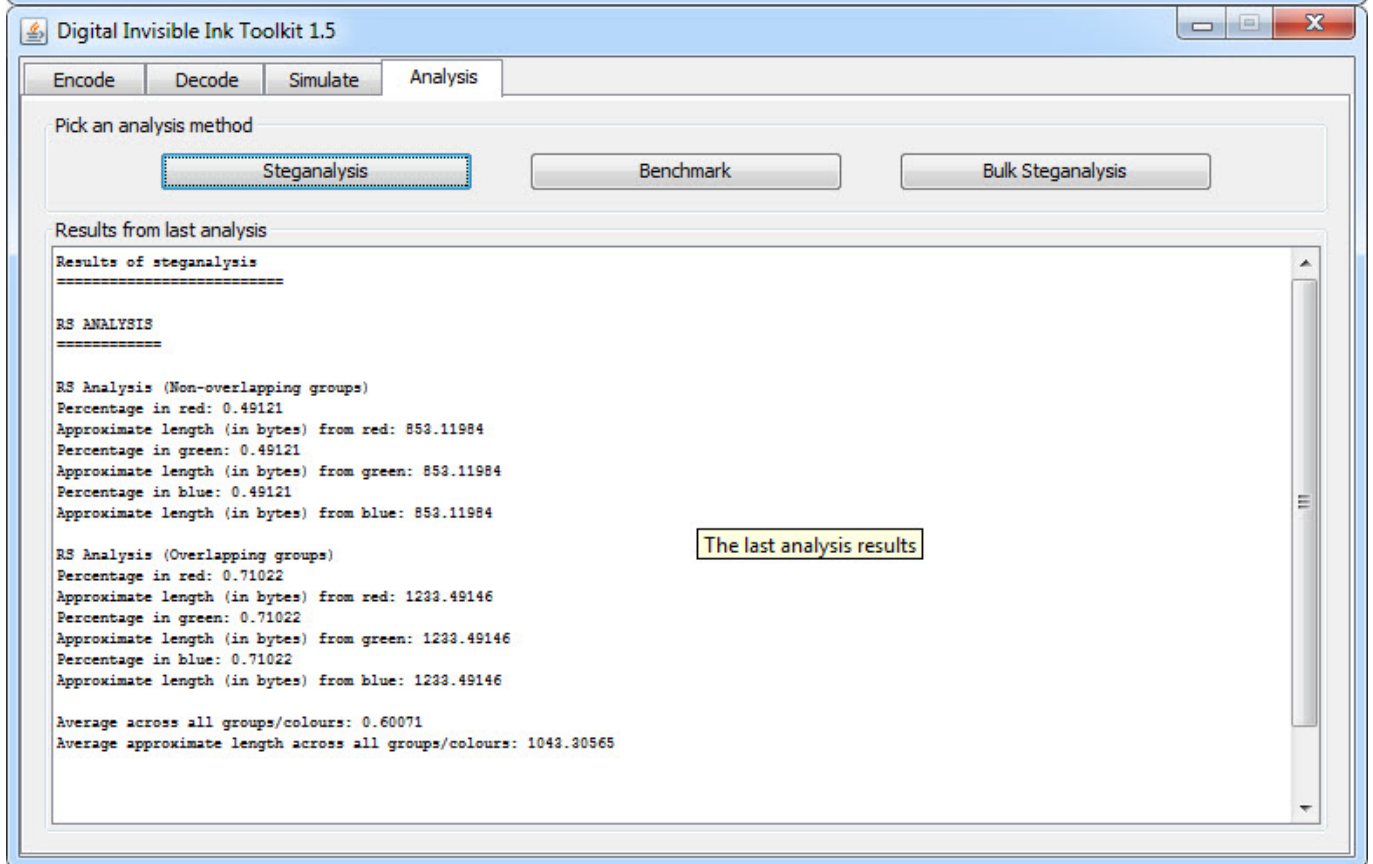
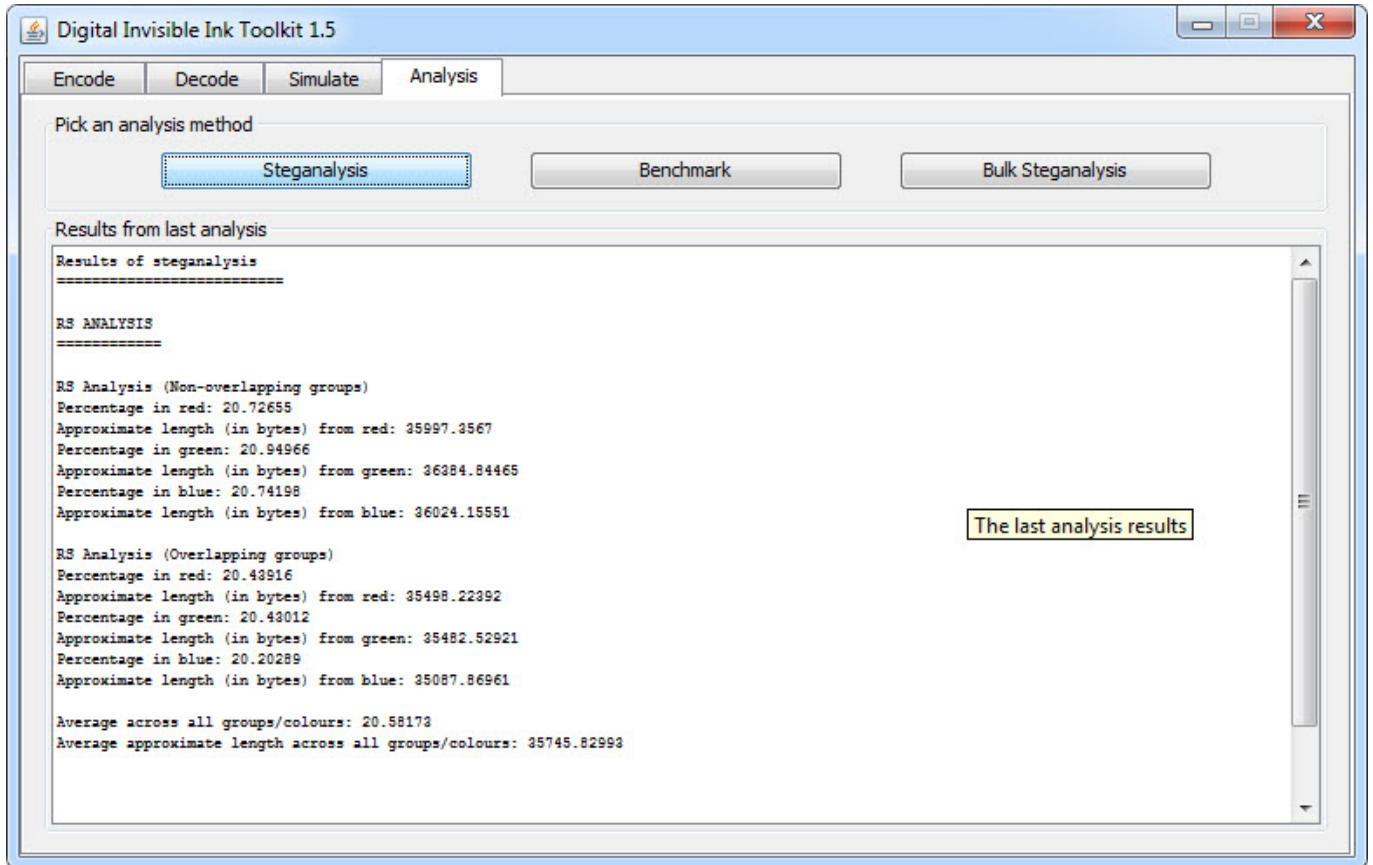
Görseller telif hakkına tabi olabilir. - Geri bildirim gönder

kmuratsimsek.blogspot.com/2014/04/is-einstein-sizin-icin-calssayd-yazs.html



Steganografi kullanıldığından şüphe ederek resim üzerinde Digital Invisible Ink Toolkit aracı ile RS LSB steganalizi yaptığımızda Red, Green ve Blue renk grubunun değerlerinin orjinaline kıyasla yüksek çıktığını görebilirdik. Bu durum da bize LSB yöntemi ile resim üzerinde bir verinin gizlendiği bilgisini verirdi.

Stegsolve aracı ile



Stegsolve aracı ile Red, Green ve Blue Bitplane değerleri için sıfır seçtiğimizde karşımıza sayısal görüntü kodlama biçimi olan JPEG başlık bilgisi çıkıyordu. JPEG dosyasının başlangıç (0xFFD8) ve bitiş değeri (0xFFD9) arasındaki veriyi kopyalayıp çalıştırdığımızda ise Einstein'in resmine gizlenmiş bir deli resmi ortaya çıkıyor ve oyunu başarıyla tamamlamış

oluyorduk :)

The screenshot shows the StegSolve 1.3 by Caesum application. The main window displays a black and white image of Albert Einstein sticking his tongue out. An 'Extract Preview' dialog box is open, showing a hex dump of the image data. The hex dump includes the following text: 'fed00000ffd8ffe0 00104a4649460001JFIF..', '0001009600960000 fffe001f4c454144LEAD', '20546563686e6f6c 6f6769657320496e Technol ogies In', '632e2056312e3031 00ffdb0084000505 c. V1.01', and several lines of '0c0c0d0d0d0d0d0d 0c090909c0d0c0c'. The dialog box also features 'Bit Planes' settings for Alpha, Red, Green, and Blue, each with checkboxes for bits 7 through 0. The 'Order settings' section includes 'Extract By' (Row selected), 'Bit Order' (MSB First selected), and 'Bit Plane Order' (RGB selected). The 'Preview Settings' section has 'Include Hex Dump In Preview' checked. Buttons for 'Preview', 'Save Text', 'Save Bin', and 'Cancel' are at the bottom.

Hex Workshop - [C:\Users\Mert\Desktop\stega\deli-ext.jpg]

File Edit Disk Options Tools Plug-Ins Window Help

Legacy ASCII

	0	1	2	3	4	5	6	7	8	9	A	B	0123456789AB
00000000	FE	D0	00	00	FF	D8	FE	E0	00	10	4A	46JF
0000000C	49	46	00	01	00	01	00	96	00	96	00	00	IF.....
00000018	FF	FE	00	1F	4C	45	41	44	20	54	65	63LEAD Tec
00000024	68	6E	6F	6C	6F	67	69	65	73	20	49	6E	hnologies In
00000030	63	2E	20	56	31	2E	30	31	00	FF	DB	00	c. V1.01....
0000003C	84	00	05	05	05	08	05	08	0C	07	07	0C
00000048	0C	09	09	09	0C	0D	0C	0C	0C	0D	0D	0D
00000054	0D	0D	0D	0D	0D	0D	0D	0D	0D	0D	0D	0D
00000060	0D	0D	0D	0D	0D	0D	0D	0D	0D	0D	0D	0D
0000006C	0D	0D	0D	0D	0D	0D	0D	0D	0D	0D	0D	0D
00000078	0D	0D	0D	0D	0D	0D	01	05	08	08	0A	07
00000084	0A	0C	07	07	0C	0D	0C	0A	0C	0D	0D	0D
00000090	0D	0D	0D	0D	0D	0D	0D	0D	0D	0D	0D	0D
0000009C	0D	0D	0D	0D	0D	0D	0D	0D	0D	0D	0D	0D
000000A8	0D	0D	0D	0D	0D	0D	0D	0D	0D	0D	0D	0D
000000B4	0D	0D	0D	0D	0D	0D	0D	0D	0D	0D	0D	FF

deli-ext.jpg

Data Inspector

Data at offset 0x00000004:

- int8 -1
- uint8 255
- int16 -9985
- uint16 55551
- int32 -520103681
- uint32 3774863615
- int64
- uint64

Expression Calc

Signed 32 bit

Eval

Compare Results

Type	Source	Count	Count	Target	Count	Count

Compare Checksum Find Bookmarks Output

Structure Viewer

Ready Cursor: 00000044 Caret: 00000004 Sel: 00000004 OVR MOD READ

Hex Workshop - [C:\Users\Mert\Desktop\stega\deli-ext.jpg]

File Edit Disk Options Tools Plug-Ins Window Help

Legacy ASCII

	0	1	2	3	4	5	6	7	8	9	A	B	0	1	2	3	4	5	6	7	8	9	A	B
0000D0F8	50	03	BB	52	28	05	30	3F	FF	D9	0F	F8	P	.	.	R	(.	0	?
0000D104	1C	0F	C0	E3	8F	F8	E3	8F	F8	03	80	3F
0000D110	E3	80	07	00	7E	3F	1C	7F	C0	03	F1	FF	.	.	.	~	?
0000D11C	FF	8F	F8	FF	F0	3F	00	0E	38	03	FE	3F	.	.	.	?	.	.	8	.	?	.	.	.
0000D128	FF	FF	FF	E0	70	07	03	8F	F8	00	01	C0	.	.	.	p
0000D134	1C	7F	F8	FF	81	C7	03	FE	38	00	7E	3F	8	.	~	?	.	.
0000D140	E3	F0	00	FC	01	F8	FC	0F	C0	1F	8E	38
0000D14C	E3	FE	00	1C	7F	F8	FC	7E	38	1F	80	00	~	8
0000D158	03	8F	FF	00	0F	C0	FC	01	F8	E3	81	C7
0000D164	03	8F	C7	FF	FE	00	00	7F	F8	E0	00	00
0000D170	E3	81	C7	1C	71	C0	FC	71	C7	1C	0E	38	.	.	.	q	.	.	q	8
0000D17C	FF	F1	FF	FF	F0	07	1F	8F	F8	E3	80	3F
0000D188	1C	0E	00	E3	80	00	FF	81	FF	FC	01	C7
0000D194	E3	80	3F	E0	00	07	1F	FF	FF	FF	FF	FF	.	.	.	?
0000D1A0	1C	01	FF	03	F0	07	1C	00	00	1F	8E	3F
0000D1AC	FC	7E	3F	E0	7E	3F	E0	7F	FF	1C	7E	00	.	.	~	?	.	~	?

deli-ext.jpg

Data Inspector

Data at offset 0x0000D102:

int8	15
uint8	15
int16	-2033
uint16	63503
int32	253556751
uint32	253556751
int64	-535959416607...
uint64	1791078465710...

Expression Calc

Signed 32 bit

Eval

1 instances of 'FFD9' found in C:\Users\Mert\Desktop\stega\deli-ext.jpg

Address	Length	Length
0000D100	2	02

Compare Checksum Find Bookmarks Output

Structure Viewer

Find All Complete. Cursor: 0000D11A Caret: 0000D102 173678 bytes OVR MOD READ

Hex Workshop - [C:\Users\Mert\Desktop\stega\deli-ext.jpg]

File Edit Disk Options Tools Plug-Ins Window Help

Legacy ASCII

Data Visualizer

Address	0	1	2	3	4	5	6	7	8	9	A	B	0123456789AB
00000000	FE	D0	00	00	FF	D8	FF	E0	00	10	4A	46JF
0000000C	49	46	00	01	00	01	00	96	00	96	00	00	IF.....
00000018	FF	FE	00	1F	4C	45	41	44	20	54	65	63	...LEAD Tec
00000024	68	6E	6F	6C	6F	67	69	65	73	20	49	6E	hnologies In
00000030	63	2E	20	56	31	2E	30	31	00	FF	DB	00	c. V1.01....
0000003C	84	00	05	05	05	08	05	08	0C	07	07	0C
00000048	0C	09	09	0C	0D	0C	0C	0C	0C	0D	0D	0D
00000054	0D	0D	0D	0D	0D	0D	0D	0D	0D	0D	0D	0D
00000060	0D	0D	0D	0D	0D	0D	0D	0D	0D	0D	0D	0D
0000006C	0D	0D	0D	0D	0D	0D	0D	0D	0D	0D	0D	0D
00000078	0D	0D	0D	0D	0D	01	05	08	08	0A	07	
00000084	0A	0C	07	07	0C	0D	0C	0A	0C	0D	0D	0D
00000090	0D	0D	0D	0D	0D	0D	0D	0D	0D	0D	0D	0D
0000009C	0D	0D	0D	0D	0D	0D	0D	0D	0D	0D	0D	0D
000000A8	0D	0D	0D	0D	0D	0D	0D	0D	0D	0D	0D	0D
000000B4	0D	0D	0D	0D	0D	0D	0D	0D	0D	0D	0D	FF

Data Inspector

Data at offset 0x00000004:

int8	-1
uint8	255
int16	-9985
uint16	55551
int32	-520103681
uint32	3774863615
int64	5064878326892...
uint64	5064878326892...

Expression Calc

Signed 32 bit

Eval

1 instances of 'FFD9' found in C:\Users\Mert\Desktop\stega\deli-ext.jpg

Address	Length	Length
0000D100	2	02

Compare Checksum Find Bookmarks Output

Structure Viewer

Ready Cursor: 0000002B Caret: 0000D102 Sel: -0000D0FE OVR MOD READ

deli.jpg - Windows Photo Viewer

deli.jpg Properties

General Security Details

deli.jpg

Type of file: JPEG image (jpg)

Opens with: Windows Photo Viewer

Location: C:\Users\Mert\Desktop\stega

Size: 52.2 KB (53,502 bytes)

Size on disk: 56.0 KB (57,344 bytes)

Created: 27 Nisan 2015 Yesterday, 17:44:18

Modified: 27 Nisan 2015 Yesterday, 13:17:04

Accessed: 27 Nisan 2015 Yesterday, 17:44:18

Attributes: Read-only Hidden

OK Cancel Apply



deli.jpg Properties

General Security Details

deli.jpg

Type of file: JPEG image (jpg)

Opens with: Windows Photo Viewer

Location: C:\Users\Mert\Desktop

Size: 52.2 KB (53,502 bytes)

Size on disk: 56.0 KB (57,344 bytes)

Created: 28 Nisan 2015 Today, 1 minute ago

Modified: 28 Nisan 2015 Today, 1 minute ago

Accessed: 28 Nisan 2015 Today, 1 minute ago

Attributes: Read-only Hidden

OK Cancel Apply

OYUNU BAŞARIYLA TAMAMLAYANLAR: Harun GÜLEÇ, Melih Burak Sarı, Ahmet Cihan

ÇEKİLİŞ ve KAZANAN TALİHLİ: Melih Burak Sarı

The image shows a text editor window titled 'Çekiliş.txt' with the following content:

```
1 Harun GÜLEÇ
2 Melih Burak Sarı
3 Ahmet Cihan
```

A red arrow points to the second line, 'Melih Burak Sarı'. Below the text editor is a command prompt window titled 'Administrator: C:\WINDOWS\system32\cmd.exe - python'. The command prompt shows the following output:

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\>python
Python 2.7.9 (default, Dec 10 2014, 12:24:55) [MSC v.1500 32 bit (Intel)] on win
32
Type "help", "copyright", "credits" or "license" for more information.
>>> from random import randint
>>> print randint(1,3)
2
>>> _
```

Başta kazanan talihli Melih Burak Sarı olmak üzere oyunu başarıyla çözen, katılan, destekleyen, sponsor olan herkese teşekkür eder, yeni oyunlarda görüşmek dileğiyle herkese güvenli günler dilerim.