

# Challenge forensics DC3



S  
S  
T  
I  
C  
  
2  
0  
0  
9

Christophe GRENIER - [grenier@cgsecurity.org](mailto:grenier@cgsecurity.org)

# Challenge forensics DC3

- Challenge réalisé par le « Defense Cyber Crime Center » (DC3) plus particulièrement « Defense Computer Forensics Laboratory » (DCFL)
- « DC3 Challenge is a call to the digital forensics community to pioneer new investigative tools, techniques and methodologies. »

# Challenge forensics DC3

- The DC3 Challenge requires that all of its winning team participants hold **U.S. citizenship** and reside within (and travel from) the Continental US (CONUS); therefore the winning team must be comprised of all CONUS, U.S. citizens in order to claim the prize trip to the Conference.
- The DC3 Digital Forensics Challenge welcomes **non-US citizens** to participate for score and receive **bragging rights only**.

# Challenge forensics DC3



- Objectif réel: « United States Cyber Challenge - a talent search and development program for finding and nurturing the next generation of cyber experts »

# Challenge forensics DC3

- Conduct a forensic exam of the submitted media for evidence of violation(s) of:
- 26 USC Sec. 5812 (possession of automatic weapons),
- 10 USC Chapter 161 - Property Records And Report Of Theft Or Loss Of Certain Property (Weapons)
- 42 U.S.C. 3713 Computer Crime Enforcement Act
- 40 USC Sec. 5104 Sec. 5104. Unlawful activities
- 10 USC Sec. 881 Sec. 881. Art. 81. Conspiracy

Logiciels suspects

FLAG - Forensic Log Analysis GUI. 0.87-pre1 - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://127.0.0.1:8000/f?report=Browse Filesystem&family=Disk Fore



Case Management Load Data Configuration Disk Forensics Log Analysis Network Forensics Preview Test

Case: DC3\_2009

## Browsing Virtual Filesystem

Tree View Table View

- msdownld.tmp
- NVIDIA
- Program Files
  - Accessories
  - CHAT
  - Common Files
  - DIRECTX
  - DriveWiper Pro 1.10
  - EvidenceEliminator5.0
  - Internet Explorer
  - Messenger
  - MSN
  - MSN Messenger
  - NetMeeting
  - Online Services
  - Outlook Express
  - PLUS!
  - PowerQuest
  - Skype
  - Steg Creator Plus
  - STEG\_IT\_v7
  - SuperVault Encryntion Service 2.4

Inode	Filename	Del	File Size	Last Modified	Mode
<input type="checkbox"/>  <a href="#">IcJK517-0-0</a>	desktop.ini	✓	129	 2009-02-26 11:14:20	r/r

Done



N/A S Adblock

# Stéganographie



# Challenge forensics DC3

- Extrait du rapport du Special Agent H. Edward Cicop:  
« She stated that he would have pictures of Crystal Clocks up on the computer for hours and said he was 'working on them' like they were broken or he was fixing them somehow. »

Thumbnail	Filename	Type	Size	Timestamp
 <p data-bbox="31 957 351 997">Ic K2476426-0-0</p>	<p data-bbox="457 662 946 702"><a href="#">/c/IntelPRO/APPS/TOOLS/CC1.MDB</a></p>	<p data-bbox="1276 646 1585 718">JPEG image data, JFIF standard 1.01</p>	<p data-bbox="1702 662 1798 702">47780</p>	<p data-bbox="1830 662 2053 734">2008-12-26 23:16:46</p>
	<p data-bbox="457 1252 1159 1356"><a href="#">/c/System Volume Information/restore{2906B87C-A85F-43CD-91FA-1C1B08CE54E2}/RP31/log.ini</a></p>	<p data-bbox="1276 1268 1585 1340">JPEG image data, JFIF standard 1.01</p>	<p data-bbox="1702 1284 1798 1324">47191</p>	<p data-bbox="1830 1284 2053 1356">2008-12-26 23:37:26</p>

Systeme de fichier chiffré ?

FLAG - Forensic Log Analysis GUI. 0.87-pre1 - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://127.0.0.1:8000/f?report=Browse Filesystem&family=Disk Fore









Case Management Load Data Configuration Disk Forensics Log Analysis Network Forensics Preview Test

Case: DC3\_2009

## Browsing Virtual Filesystem

Tree View Table View

- + /
- + c
- d
  - + \$RECYCLE.BIN
  - + Documents and Settings
  - + Downloads
  - + ETHERNET
  - + i386
  - + IntelPRO
  - + msdownld.tmp
  - + NVIDIA
  - + Program Files
  - + Recycled
  - + System Volume Information
  - + WINDOWS
  - + Windows.old
  - + \_deleted\_
  - + \_unallocated\_
- + n

Inode	Filename	Del	File Size	Last Modified	Mode
<input type="checkbox"/>  <a href="#">IdJK209688-0-0</a>	SystemDatabase	<input checked="" type="checkbox"/>	4194304	2008-03-11 13:08:36	r/r
<input type="checkbox"/>  <a href="#">IdJK209793-0-0</a>	MSI8b9e2.tmp	<input checked="" type="checkbox"/>	4096	2008-04-01 08:52:50	d/-
<input type="checkbox"/>  <a href="#">IdJK209791-0-0</a>	MSI6bd37.tmp	<input checked="" type="checkbox"/>	4096	2008-04-01 08:50:44	d/-
<input type="checkbox"/>  <a href="#">IdJK209789-0-0</a>	MSIf7202.tmp	<input checked="" type="checkbox"/>	4096	2008-04-01 08:50:18	d/-
<input type="checkbox"/>  <a href="#">IdJK209787-0-0</a>	MSI5961c.tmp	<input checked="" type="checkbox"/>	4096	2008-04-01 08:49:22	d/-
<input type="checkbox"/>  <a href="#">IdJK209785-0-0</a>	MSIf53b0.tmp	<input checked="" type="checkbox"/>	4096	2008-04-01 08:42:30	d/-
<input type="checkbox"/>  <a href="#">IdJK209783-0-0</a>	MSIccfb9.tmp	<input checked="" type="checkbox"/>	4096	2008-04-01 08:31:26	d/-
<input type="checkbox"/>  <a href="#">IdJK209781-0-0</a>	MSI15fcb.tmp	<input checked="" type="checkbox"/>	4096	2008-04-01 08:27:18	d/-

Done

N/A Adblock

**Des Armes automatiques!**



[/d/Documents and Settings/TallTower/Local Settings/Temporary InternetFiles/Content.IE5/4N3PE2T1/Restricted%20Receiverx.jpg](#)

JPEG image data, JFIF standard 1.01

[..K19144257-0-0](#)



[/d/Documents and Settings/TallTower/Local Settings/Temporary InternetFiles/Content.IE5/4N3PE2T1/LWRC%20M6A2%20Rx.jpg](#)

JPEG image data, JFIF standard 1.01

[..K19144254-0-0](#)



[/d/Documents and Settings/TallTower/Local Settings/Temporary InternetFiles/Content.IE5/4N3PE2T1/LWRC%20M6A2%20Lx.jpg](#)

JPEG image data, JFIF standard 1.01

[..K19144251-0-0](#)



[/d/Documents and Settings/TallTower/Local Settings/Temporary InternetFiles/Content.IE5/4N3PE2T1/LE6933%20M402%20Rx.jpg](#)

JPEG image data, JFIF standard 1.01

[..K19144248-0-0](#)



[/d/Documents and Settings/TallTower/Local Settings/Temporary InternetFiles/Content.IE5/4N3PE2T1/LE6933%20M402%20R%20M402%20offx.jpg](#)

JPEG image data, JFIF standard 1.01

[..K19144245-0-0](#)

## Viewing file in inode [Id|K42784656-0-0](#)

Classified as XML document text by magic

[Statistics](#)[HexDump](#)[TextDump](#)[Download](#)[Summary](#)[Explain](#)

```
over</Text></Message><Message Date="4/3/2008" Time="12:28:48 PM"
DateTime="2008-04-03T19:28:48.953Z" SessionID="3"><From><User Friendl
yName="blane"/></From><To><User FriendlyName="bob"/></To><Text Style
="font-family:MS Shell Dlg; color:#000000; ">I don't rat, ut maybe we
better not. Least not now.</Text></Message><Message Date="4/3/2008"
Time="12:30:15 PM" DateTime="2008-04-03T19:30:15.968Z"
SessionID="3"><From><User FriendlyName="bob"/></From><To><User
FriendlyName="blane"/></To><Text Style="font-family:MS Shell Dlg;
color:#000000; ">It goes as planned and youre gonna be there too. I
didn't spend all this time and effort for you to chicken out at the
last nimute. If youre too yellow to work this with me ill get
somebody else to pull it with. You just give me the guns and gear u
got]</Text></Message><Message Date="4/3/2008" Time="12:30:55 PM"
DateTime="2008-04-03T19:30:55.125Z" SessionID="3"><From><User
FriendlyName="blane"/></From><To><User FriendlyName="bob"/></To><Text
Style="font-family:MS Shell Dlg; color:#000000; ">I aint no mor yellow
thatn you. You think your so bad, just remember I can wip your tail
anyday, did a year ago</Text></Message><Message Date="4/3/2008"
Time="12:31:25 PM" DateTime="2008-04-03T19:31:25.671Z"
```

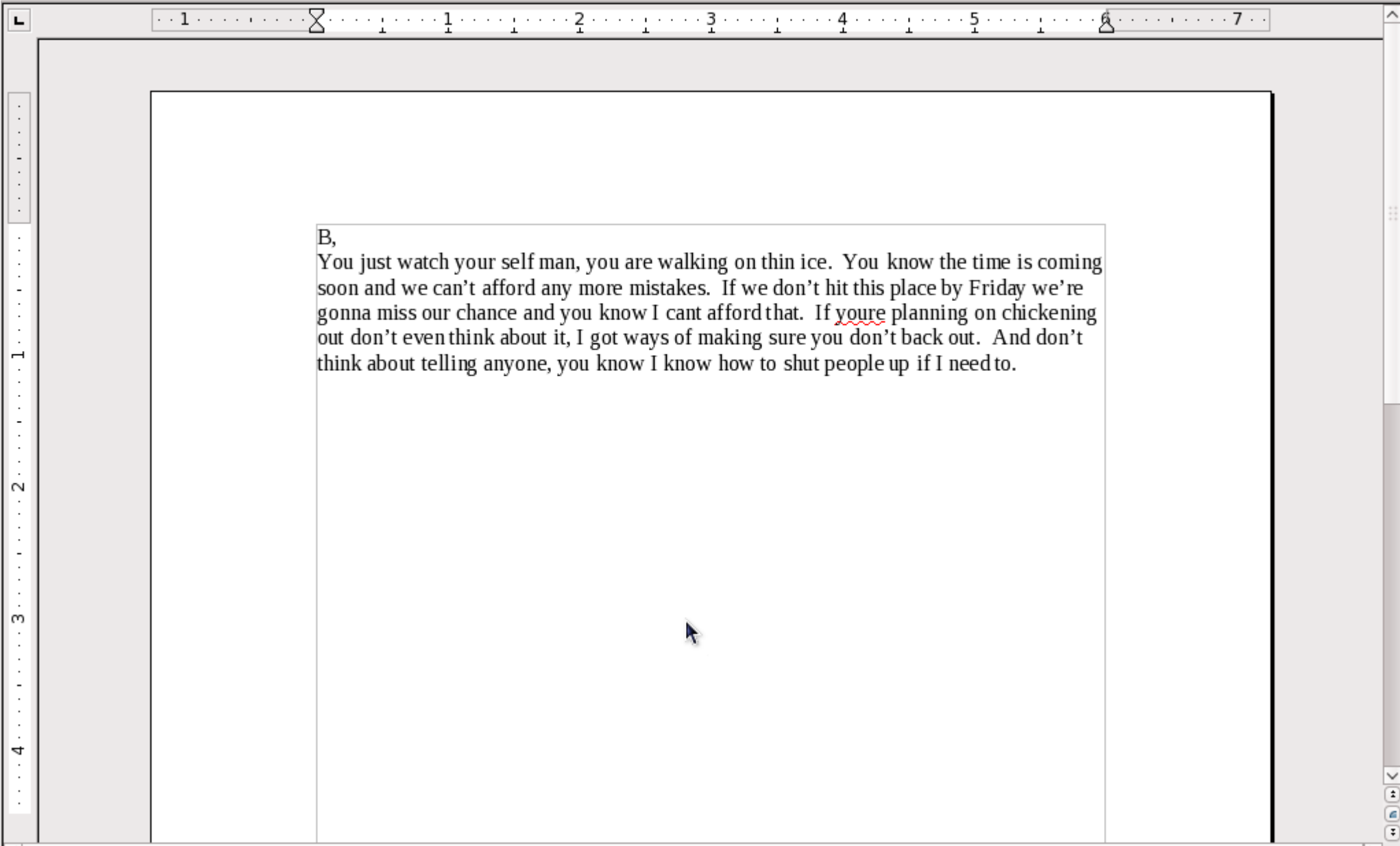
Find: gun Previous Next Highlight all Match case

Done

N/A S Adblock

**Un casse!**





Un problème ?

```
[kmaster@adsl ~]$ cd /data2/DC3_2009/cgr/RECYCLER/
[kmaster@adsl RECYCLER]$ exiftool letter.doc
ExifTool Version Number      : 7.67
File Name                    : letter.doc
Directory                   : .
File Size                    : 24 kB
File Modification Date/Time  : 2009:02:19 13:16:30+01:00
File Type                   : DOC
MIME Type                    : application/msword
Title                       :
Subject                      :
Author                      : jennifer.reichwein
Keywords                    :
Template                    : Normal.dot
Last Saved By               : jennifer.reichwein
Revision Number             : 2
Software                    : Microsoft Office Word
Total Edit Time             : 10.0 minutes
Create Date                 : 2009:02:10 17:09:00
Modify Date                 : 2009:02:10 17:19:00
Page Count                  : 1
Word Count                  : 65
Char Count                  : 373
Security                   : 0
Code Page                   : 1252
Company                     : DCFL
Lines                      : 3
Paragraphs                  : 1
Char Count With Spaces     : 437
App Version                 : 11 (270f)
Scale Crop                  : 0
Links Up To Date           : 0
Shared Doc                  : 0
Hyperlinks Changed         : 0
Title Of Parts              :
Heading Pairs               : Title, 1
Comp Obj User Type Len     : 31
Comp Obj User Type        : Microsoft Office Word Document
[kmaster@adsl RECYCLER]$
```