

# FUN WITH FIREWIRE BY KAGURE.

**kagure (500 pts)**

AED Tower, Innovation City, Pennsylvania, USA  
99th Floor Layout Diagram

(C) 2011, Amalgamated Construction Corporation  
All Rights Reserved.

**Last Opened Mission:**  
[1] "Division is HARD!!" ([details](#)) [trivia] [20pts]  
Opened 121:24 hours ago.

**Selected Mission:**  
"Fun with firewire" ([details](#))  
forensics [500pts]

Este ctf se desarrolló el pasado fin de semana, y la verdad que complicado si estaba, como una de las cosas que mas me gusta son las ciencias forenses aplicadas a maquinas sea teléfonos, pc's, u otros. Me fui por el más alto a ver que podía hacer, para mejorar los 100 puntos del codegate.

1. Leer descripción del reto.

## 2. Description

3. Category: forensics

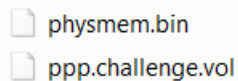
All of the machines at the AED office are encrypted using the amazing Truecrypt software.

When we grabbed one of their USB sticks from a computer, we also grabbed the memory using the Firewire port.

Recover the key using the truecrypt image and the memory dump.

2. Descargar archivo <http://www.plaidctf.com/chals/81d9467f812d2fbb32e9d4b915cccfe457245f25.tar.bz2>

3. extraer contenido.



El primero es la imagen de la memoria en formato binario y el segundo el volumen truecrypt para comprobar esto lo paso a una virtual y miro con [volatility](#) obteniendo lo siguiente.

```
root@laboratorio:/usr/local/volatility# python volatility ident -f /root/physmem
.bin
/usr/local/Volatility-1.3_Beta/forensics/win32/crashdump.py:31: DeprecationWarni
ng: the sha module is deprecated; use the hashlib module instead
  import sha
      Image Name: /root/physmem.bin
      Image Type: Service Pack 3
      VM Type: nopae
      DTB: 0x39000
      Datetime: Wed Dec 29 14:20:47 2010
```

Paso a seguir identificar los procesos que había corriendo.

```

root@laboratorio:/usr/local/volatility# python volatility pslist -f /root/physm
em_bin
/usr/local/Volatility-1.3.Beta/forensics/win32/crashdump.py:31: DeprecationWarni
ng: the sha module is deprecated; use the hashlib module instead
import sha
Name                Pid      Ppid     Thds     Hnds     Time
System              4         0        47       225     Thu Jan 01 00:00:00 1970
smss.exe            268        4         3         19     Wed Dec 29 23:18:07 2010
csrss.exe           328       268        11        323     Wed Dec 29 23:18:08 2010
winlogon.exe        360       268        23        514     Wed Dec 29 23:18:10 2010
services.exe        404       360        15        247     Wed Dec 29 23:18:11 2010
lsass.exe           416       360        23        327     Wed Dec 29 23:18:11 2010
svchost.exe         568       404        22        177     Wed Dec 29 23:18:12 2010
svchost.exe         628       404         9        213     Wed Dec 29 23:18:12 2010
UNKNOWN            664       404        53        979     Wed Dec 29 23:18:12 2010
svchost.exe         704       404         5         59     Wed Dec 29 23:18:12 2010
svchost.exe         756       404         4         86     Wed Dec 29 23:18:13 2010
spoolsv.exe         840       404        15        114     Wed Dec 29 23:18:14 2010
vmssvc.exe          916       404         5         45     Wed Dec 29 23:18:23 2010
vpcmap.exe         1060      404         3         27     Wed Dec 29 23:18:23 2010
alg.exe            1280      404         7        104     Wed Dec 29 23:18:27 2010
explorer.exe        1508     1432        15        349     Wed Dec 29 23:18:37 2010
vmssvc.exe         1720     1508         2         44     Wed Dec 29 21:18:39 2010
ctfmon.exe          1728     1508         1         79     Wed Dec 29 21:18:39 2010
wscntfy.exe         1740     664         1         37     Wed Dec 29 21:18:39 2010
TrueCrypt.exe      1892     1508         1         41     Wed Dec 29 21:19:25 2010
cmd.exe             1952     1508         1         33     Wed Dec 29 21:20:20 2010
win32dd.exe         1980     1952         1         22     Wed Dec 29 21:20:45 2010

```

Interesante win32dd.exe, truecrypt.exe. y después de eso estuve un rato atascado mentalmente hasta que recordé haber leído algo a cerca de el más exactamente aquí <http://www.kriptopolis.org/passware-kit-rompe-truecrypt> y leyendo los comentarios había uno que decía Passware kit no rompe nada de TrueCrypt, simplemente extrae contraseñas mientras están en uso; no usa GPU para nada. Y mas abajo decía que tambie atacaba por fuerza bruta lógicamente en un comienzo lo pensé pero era gastar demasiado tiempo en nada asi que me baje la herramienta en cuestión [Passware kit](#) y a trabajar.

Paso 1.



#### Recover Hard Disk Passwords (Ctrl+D)

Recover encryption keys or passwords to unlock BitLocker and TrueCrypt drives.

Paso 2.



#### BitLocker (Ctrl+B)

Recover encryption keys to unlock a BitLocker volume.



#### TrueCrypt (Ctrl+T)

Decrypt a TrueCrypt volume.

#### Additional Tools

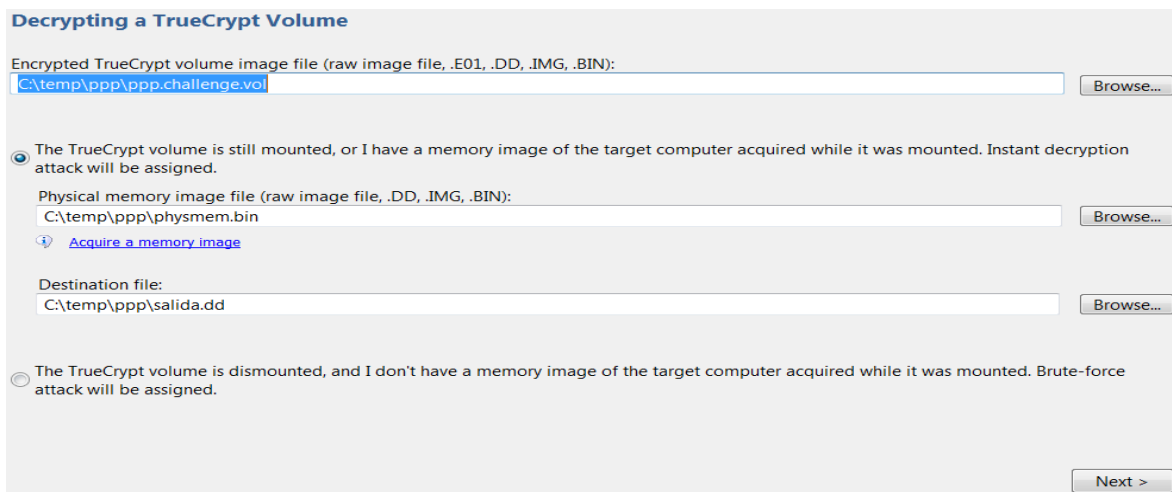


#### Passware FireWire Memory Imager

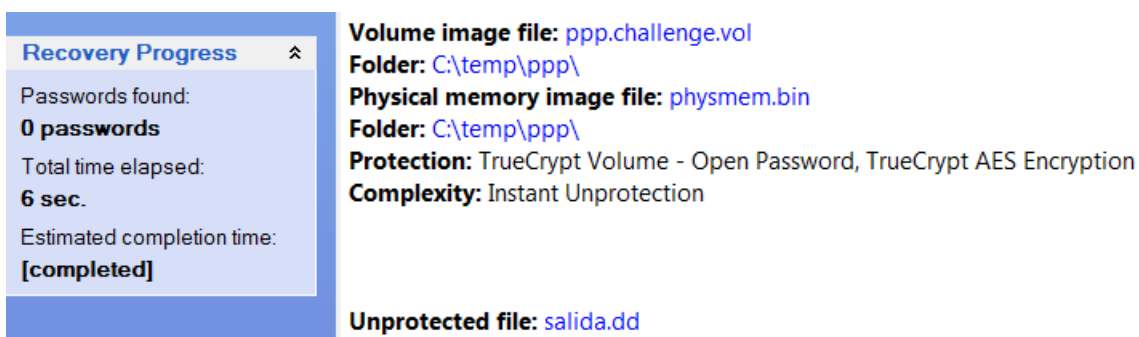
Acquire a memory image of a computer with a mounted BitLocker or TrueCrypt volume.

Click en truecrypt.

Paso 3.



Escoger primero el container de truecrypt luego el dump de la memoria y por ultimo donde debe quedar el container sin contraseña. Click en next y el hace un análisis y luego el resultado



Así que salida.dd es el container de truecrypt sin contraseña. Pero en formato dd así que debo montarla para saber que contiene así que me baje el [mount image pro](#) en versión de prueba 14 días más que suficiente.

Y aja hay un único archivo

 KEY.TXT

Que contiene el flag = jha0IMn58keAlpueeNCPVSO9dk que por fuerza bruta hubiera sido imposible.

Gracias. Y saludos a @hades @hecky @zarek y a @RicTeam.