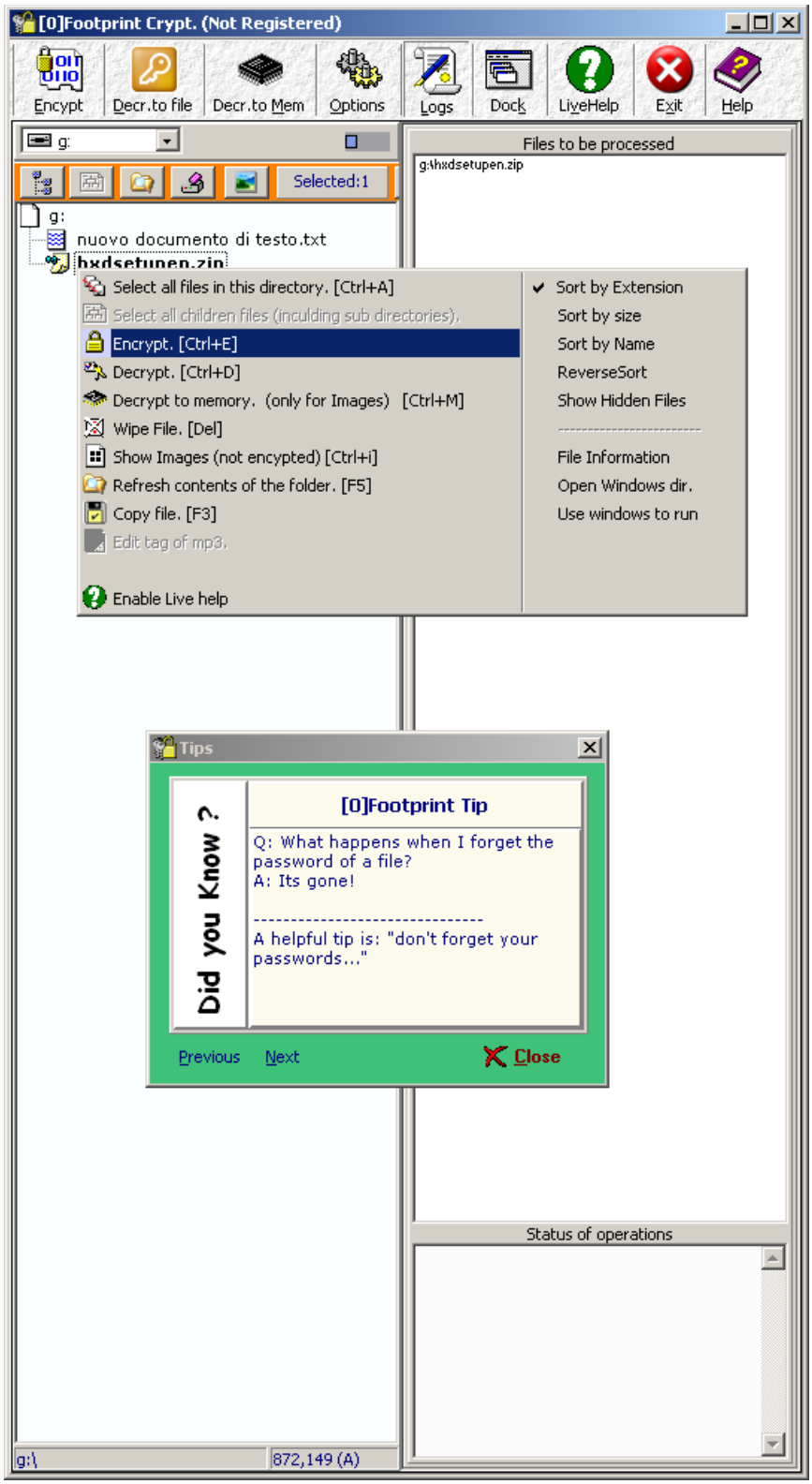
---::[[0]Footprint Crypt 1.5 password recovery]::---

Salve a tutti. Stavo creando alcune definizioni per l'ormai tool di defacto per l'analisi di file binary e non: **TrID** (*http://mark0.net/soft-trid.html*). Creando diverse migliaia di file crittografati con diversi software è stato notato un piccolo particolare, in questo caso nel software di cui il titolo. Apriamo il programma e crittografiamo un file a caso con password a caso. Attenzione da notare che il "Tip Of The Day" capita a pennello. La risposta degli autori non è proprio corretta del tutto. Si creerà un file .0ft.

Hi all. While creating some definitions to the defacto tool for analysing binary and not files: **TrID** (*http://mark0.net/soft-trid.html*), I encrypted some tousands of files with different softwares. Among all those utilities, a little bug appeared clearly. In this case in the encryption schema of the freeware in the title. Let's open the program and encrypt a random file with a random password. Please note that is was just random what the "Tip Of The Day" is telling us. The answer is not 100% right. It will create a .0ft file.



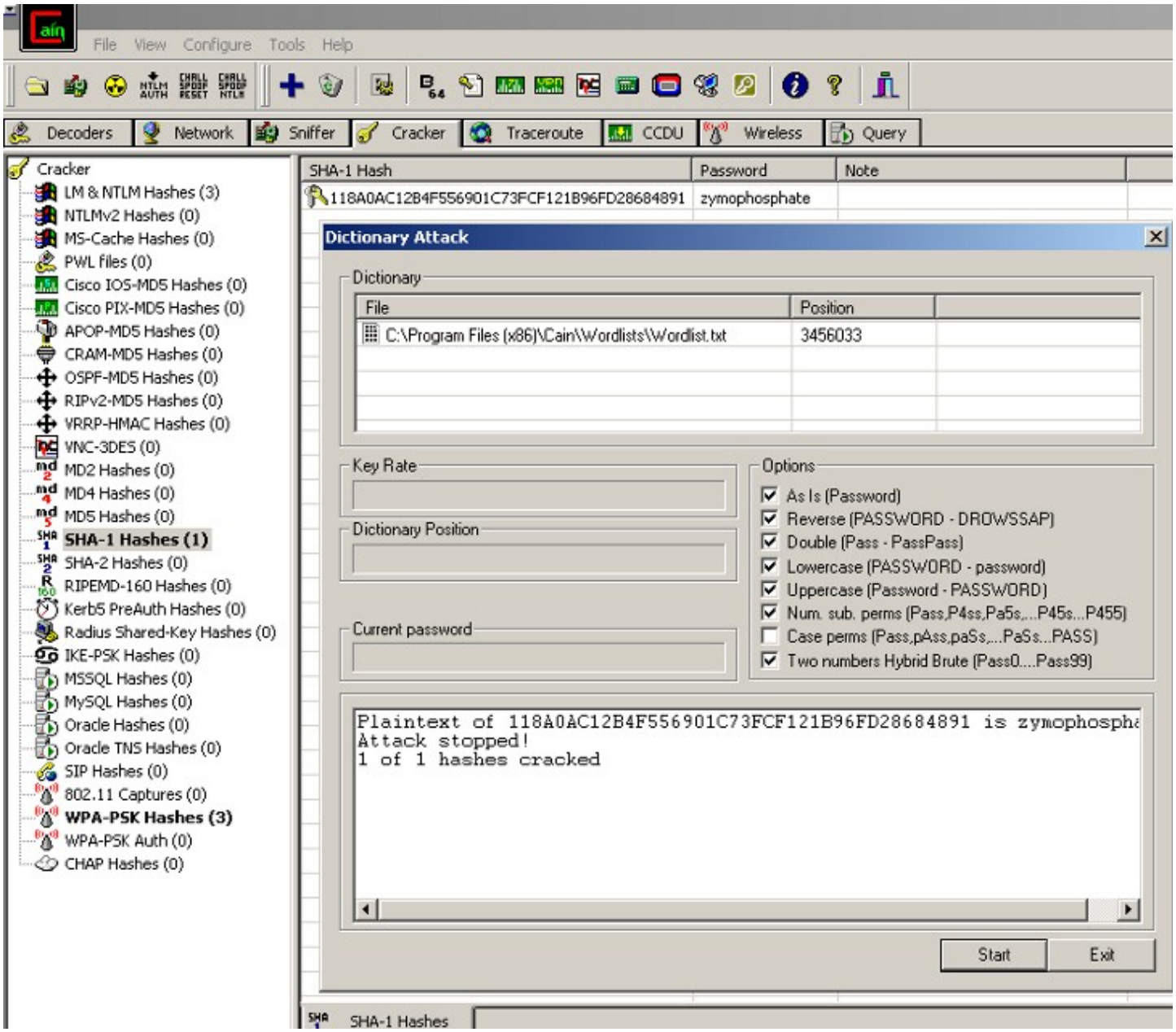
Bene. La password inserita per crittografare il file viene passata alla semplice funzione tipo: **SHA-1('*pass*')**. Poi viene inserita in 'chiaro' nel header del file. Aprendo il file, del quale facciamo finta di aver dimenticato la password, con un hexeditor, copiamo i primi 40 byte oppure direttamente il testo in ascii:

So far so good. The inserted password will go through a function like: **SHA-1('*pass*')** and inserted into the header of the file. Let's assume we forgot the pwd, then simply copy the first 40 bytes or directly the ascii string:

```
Hex: 31 31 38 41 30 41 43 31 32 42 34 46 35 35 36 39 30 31 43 37 33 46 43 46 31 32 31 42 39 36 46 44 32 38 36 38 34 38 39 31
Hash: 1  1  8  A  0  A  C  1  2  B  4  F  5  5  6  9  0  1  C  7  3  F  C  F  1  2  1  B  9  6  F  D  2  8  6  8  4  8  9  1
Hash to feed the cracker: 118A0AC12B4F556901C73FCF121B96FD28684891
```

Ci sono così tanti hash-crackers nella rete che non sto a elencare. Avendolo già aperto prima, uso Cain (http://www.oxid.it) con la sua wordlist predefinita.

There are so many hash-crackers out there, no need to tell which works faster or better. Since Cain (http://www.oxid.it) is already opened, let's take that one and run a simple dictionary attack.



Per molti questo articolo è inutile, ma per newbies è senz'altro una piccola e brevissima lettura interessante :) Saluto cordialmente tutti e a presto.

For most, this article isn't interesting at all. Mainly for newbies this could be a short and interesting lecture :) Kindest regards to everybody and c u...