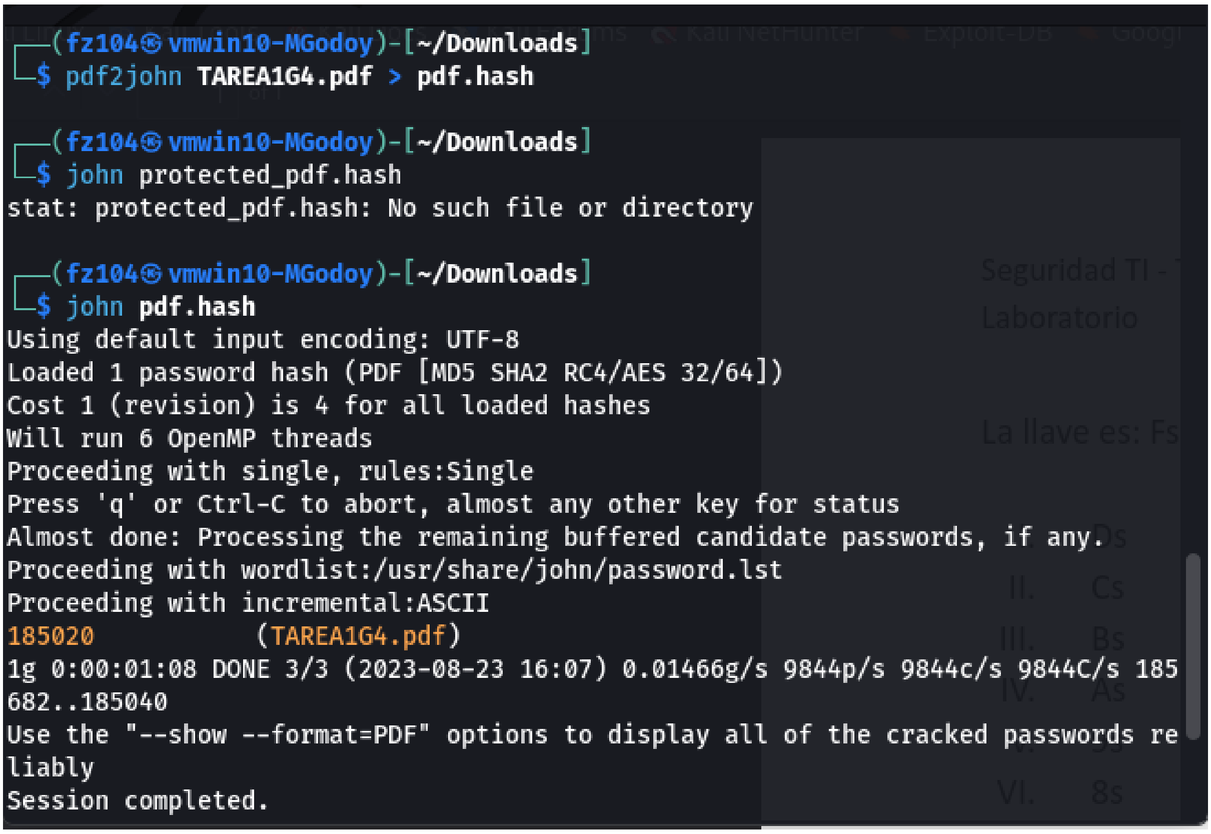
Informe

Sofia Prado
Sebastian Velasquez

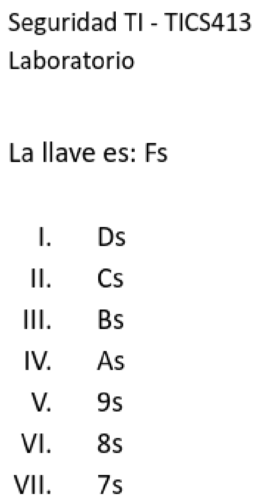


```
┌──(fz104㉿vmwin10-MGodoy)-[~/Downloads]
└─$ pdf2john TAREA1G4.pdf > pdf.hash

┌──(fz104㉿vmwin10-MGodoy)-[~/Downloads]
└─$ john protected_pdf.hash
stat: protected_pdf.hash: No such file or directory

┌──(fz104㉿vmwin10-MGodoy)-[~/Downloads]
└─$ john pdf.hash
Using default input encoding: UTF-8
Loaded 1 password hash (PDF [MD5 SHA2 RC4/AES 32/64])
Cost 1 (revision) is 4 for all loaded hashes
Will run 6 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
185020           (TAREA1G4.pdf)
1g 0:00:01:08 DONE 3/3 (2023-08-23 16:07) 0.01466g/s 9844p/s 9844c/s 9844C/s 185
682..185040
Use the "--show --format=PDF" options to display all of the cracked passwords re
liably
Session completed.
```

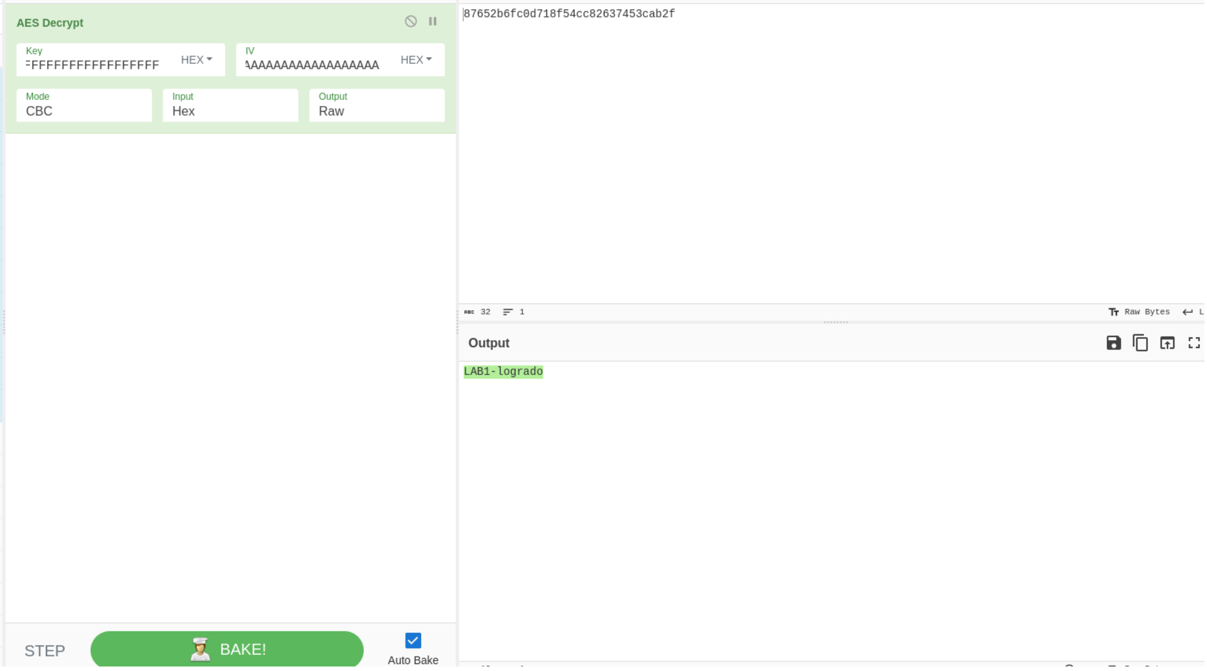
En el primero se creó el hash usando john the ripper, para luego desencriptar la clave a través de fuerza bruta, lo que nos entregó el valor del segundo paso. Adjuntamos copia del resultado.



Seguridad TI - TICS413
Laboratorio

La llave es: Fs

I. Ds
II. Cs
III. Bs
IV. As
V. 9s
VI. 8s
VII. 7s



AES Decrypt

Key: FFFFFFFFFFFFFFFFF HEX

IV: AAAAAAAAAAAAAAAAAA HEX

Mode: CBC

Input: Hex

Output: Raw

```
87652b6fc0d718f54cc82637453cab2f
```

Output

```
LAB1-logrado
```

En cyberchef utilizamos la clave encontrada anteriormente y desciframos el mensaje.