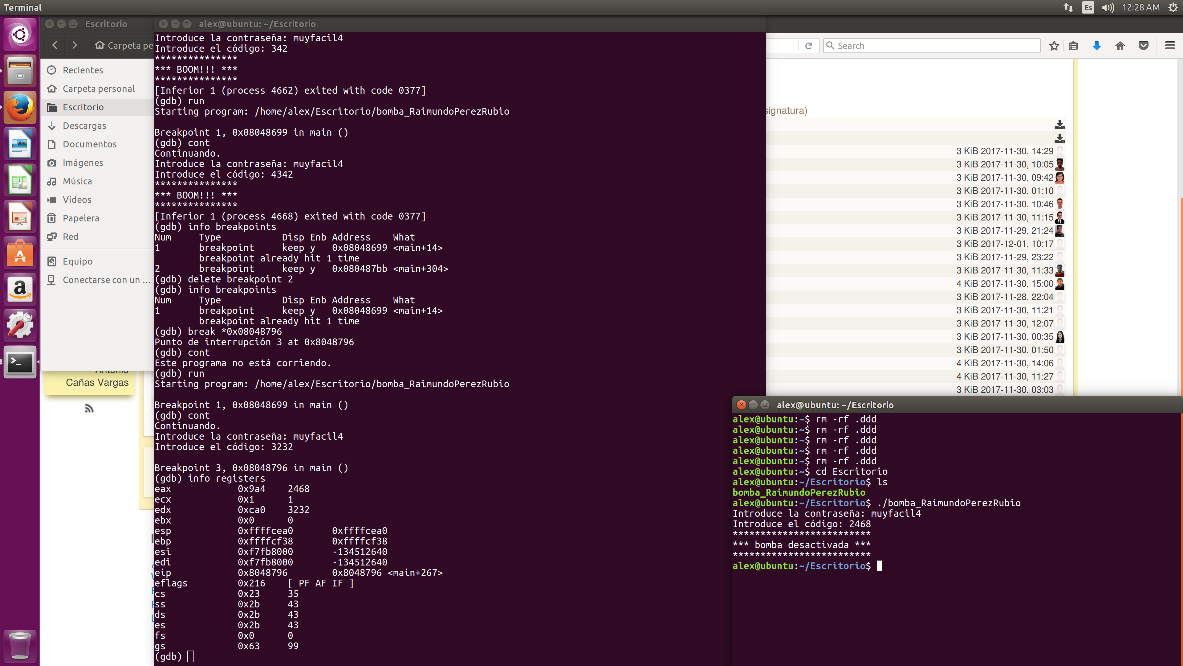
Práctica 4 Alejandro Poyatos López Segunda Parte

Resolución de las bombas de los alumnos de la clase

He resuelto la bomba del compañero Raimundo Perez Rubio, siguiendo los siguientes pasos, para comenzar he observado que no existe codificación externa a la del main, por lo que lo he abierto con ddd y he colocado un breakpoint justo despúes de la comparación de strlen como se observa en la siguiente foto:



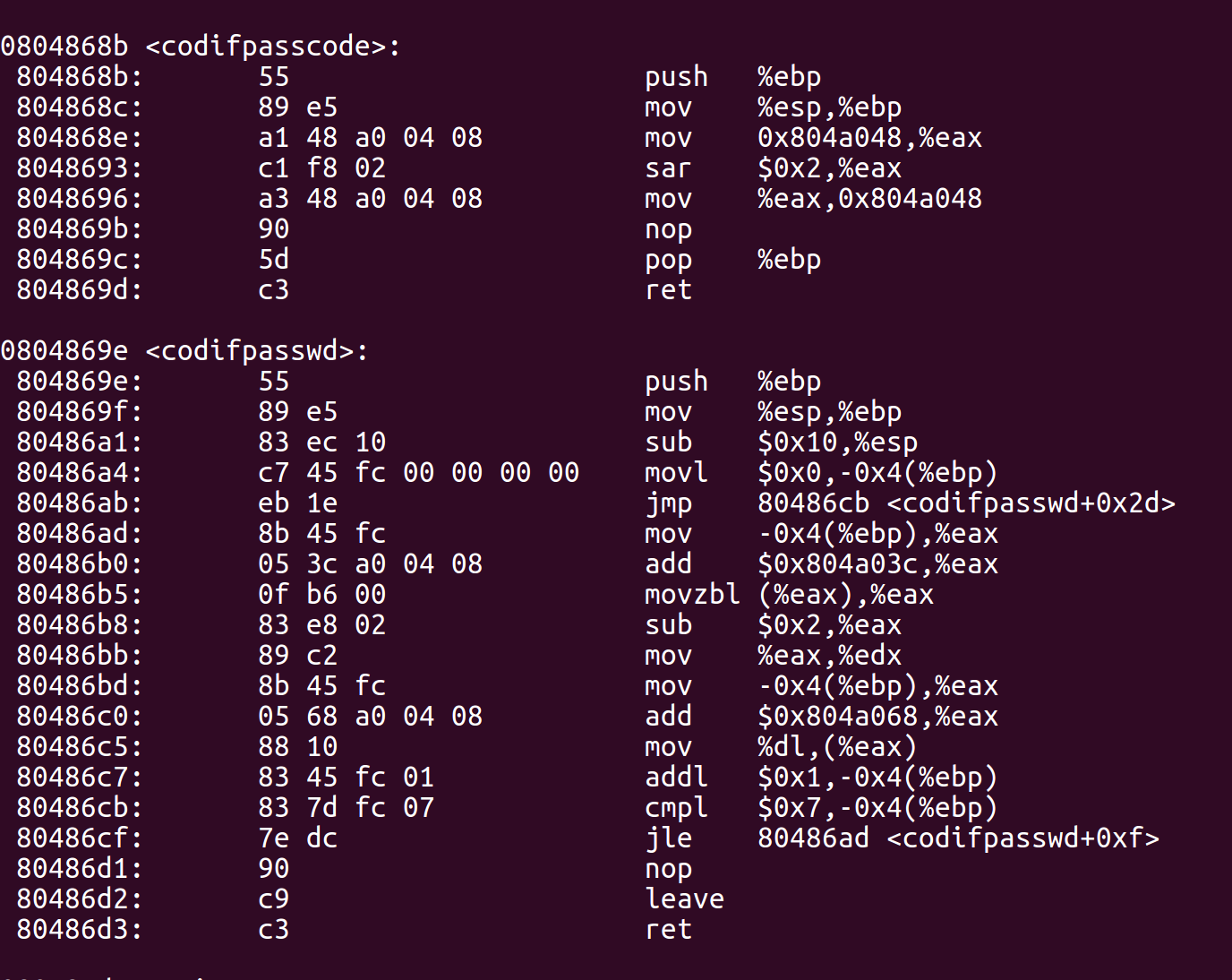
Y observando los datos de tipo char de la dirección que hace push inmediatamente antes sacamos la password directamente: muyfacil4



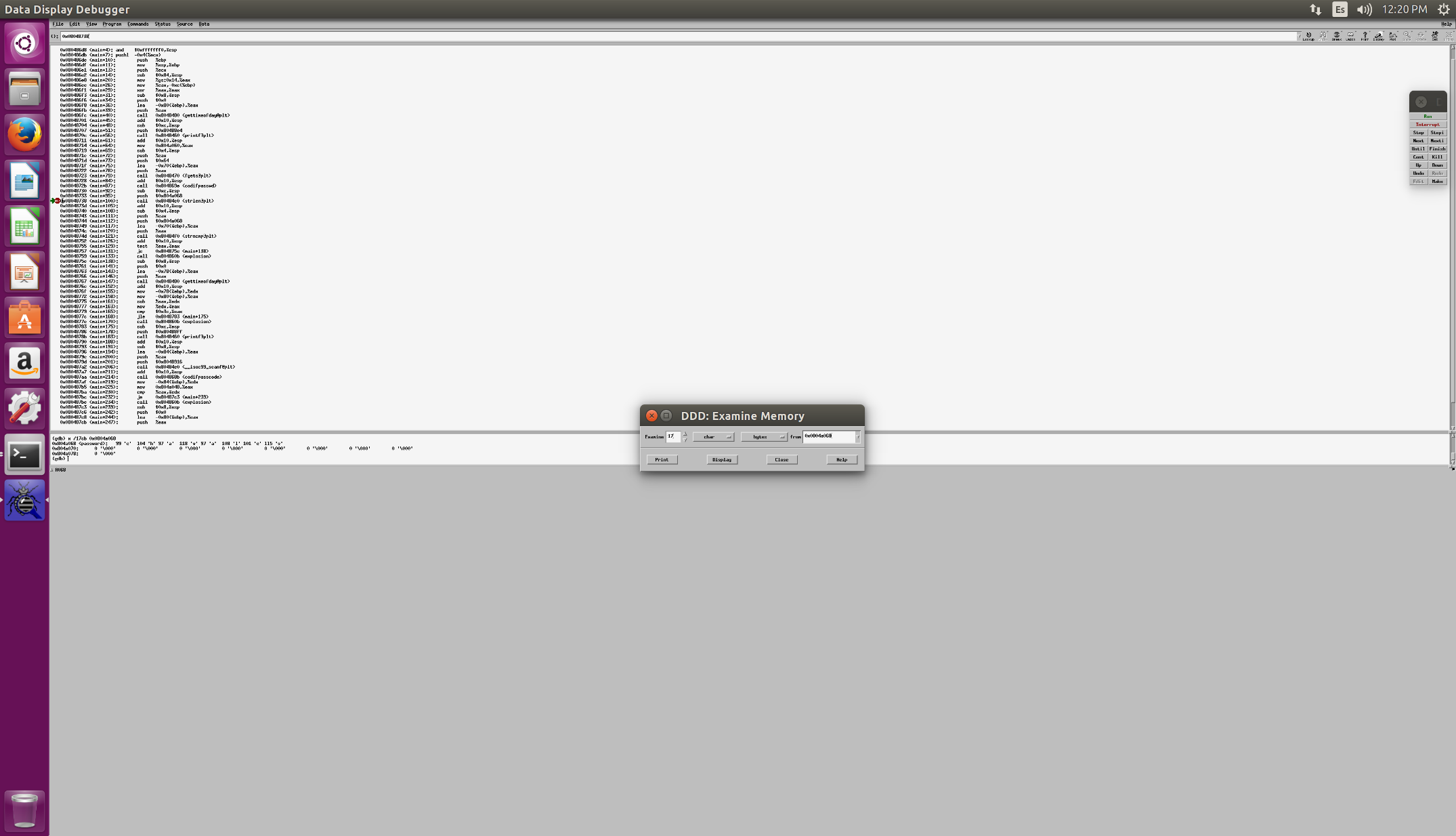
Por otro lado para para la cifra numérica he usado gdb y he colocado un breakpoint en el salto antes de la segunda llamada a boom para ver el valor del registro eax:

Como podemos observar el código esta a simple vista 2468, por lo que ya esta resuelta la bomba.

La segunda bomba es la del compañero David Carrasco Chicharro, que tiene dos funciones externas al main para codificar la password y el passcode:



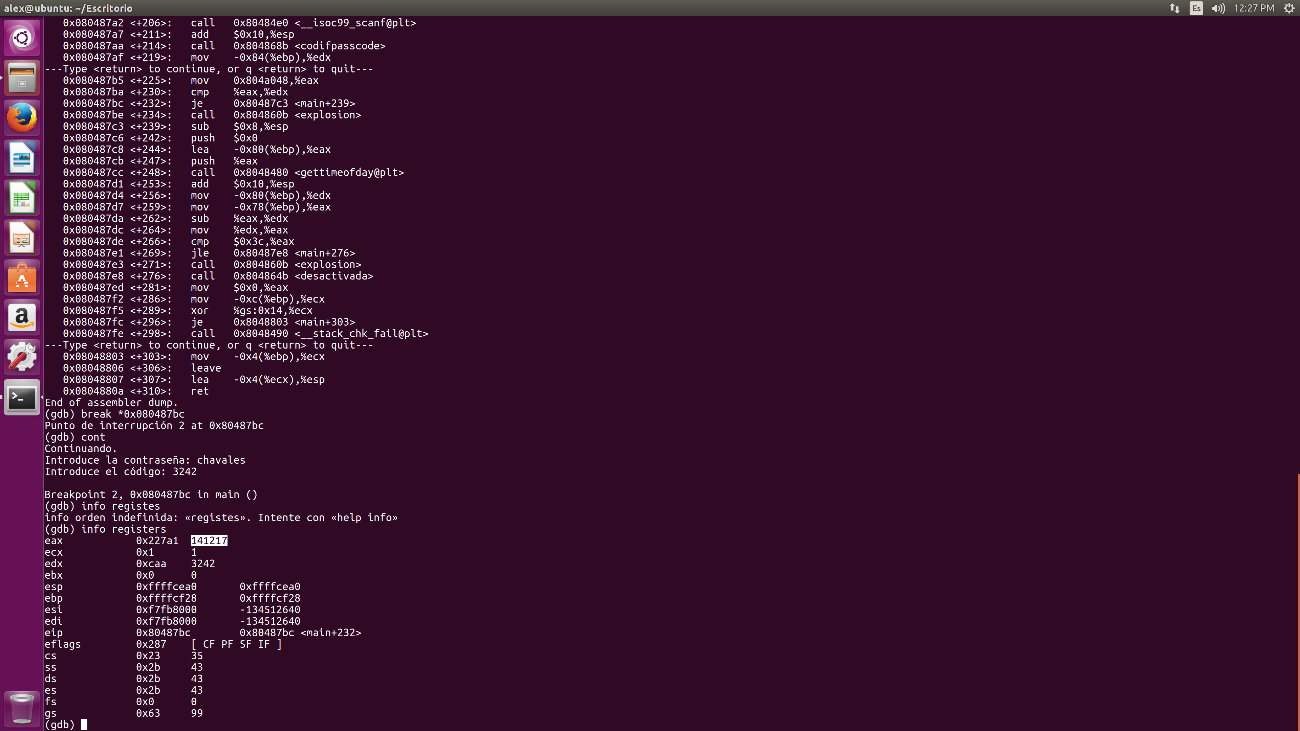
Aunque no me ha hecho falta descifrar el funcionamiento de ambos, ya que he conseguido averiguar la password de vuelta como se muestra en la siguiente imagen:



Obteniendo ya la password descodificada: chavales

La compruebo veo que funciona y continuo hacia el passcode.

Para el passcode me situo con gdb en la última comparación antes de la llamada a la explosión, observando que se comparan dos registros el eax y el edx, siendo el edx el que yo introduje, observo que el eax contiene el passcode descifrado:



Compruebo el código y veo que ya esta descifrada:

