2.3. <https://defendtheweb.net/playground/missile-codes>

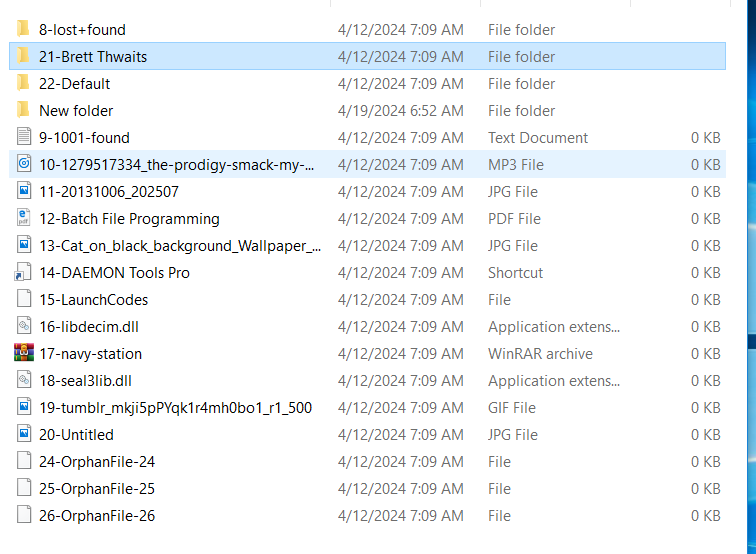
Missile codes / Forensics

We require your services once again. An employee from our company had recently been identified as a known criminal named Brett Thwaits. He is considered to have stolen missile launch codes from the US navy which unfortunately were handed to us for a brief period of time. As of now, we are accussed of the theft and unless we do something about it, we’re gonna end in some serious trouble. Before Brett left, he formatted the thumbdrive which used to store the launch codes. Fortunately, our system had made a backup image of the drive. See if you can recover the fourth launch code. Good luck! Download backup

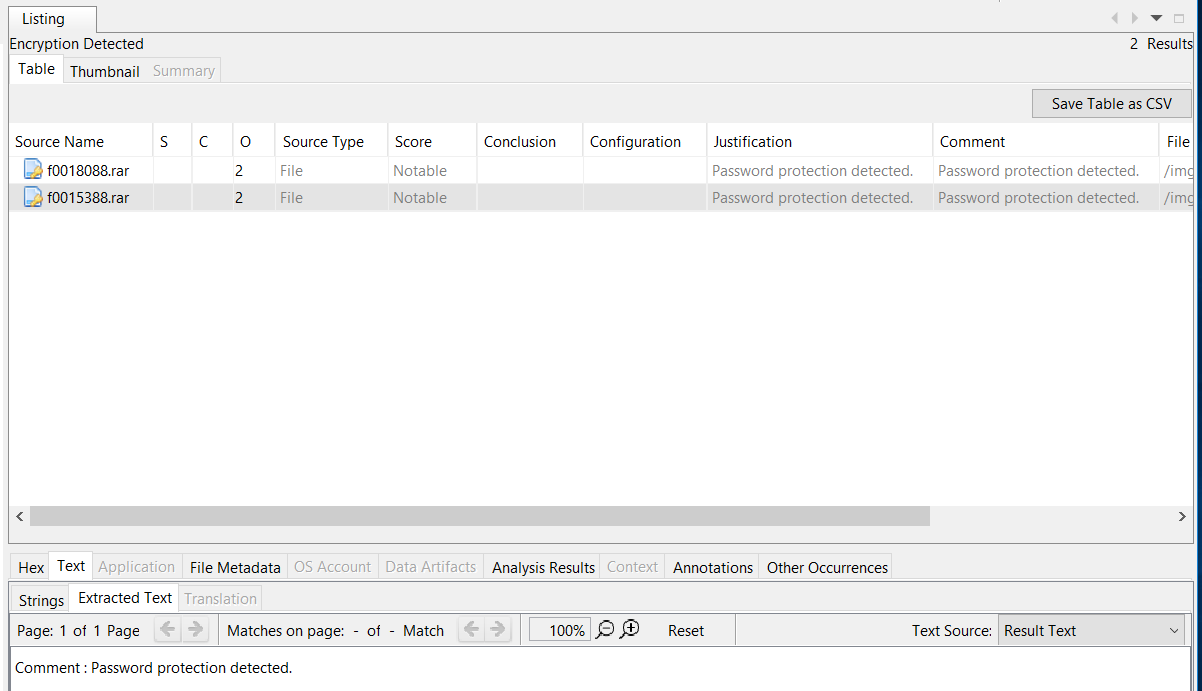
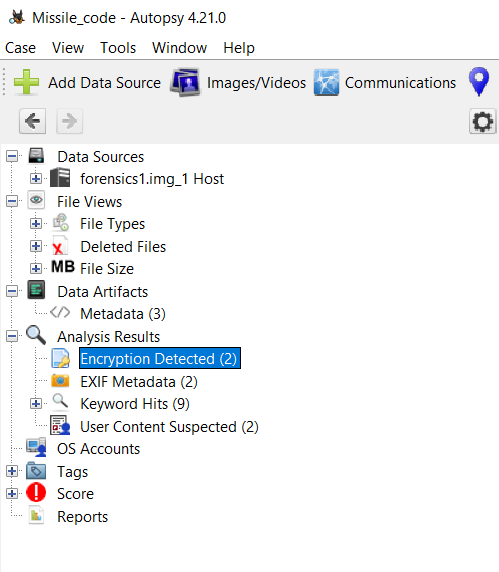
Solution

I downloaded the file and using Autopsy I created a case and opened the Forensic.img file.

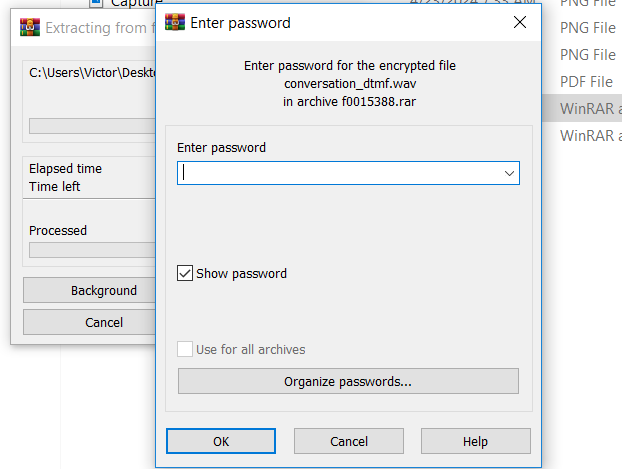
I exported the deleted files containing LaunchCodes but all turned out to be zero bytes.



On further investigations, Autopsy seems to have detected Encrypted files: **f0015388.rar** and **f0018088.rar**

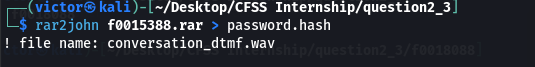


I successfully extracted this to my desktop but found a password wall.



After several failed attempts, I decided to brute force the rar files. using the command

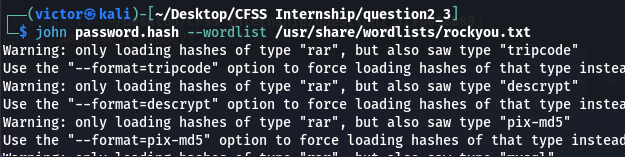
rar2john f0018088.rar > password.hash



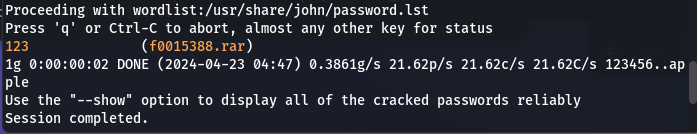
I got the hash of the file and redirected it to create a file **password.hash**

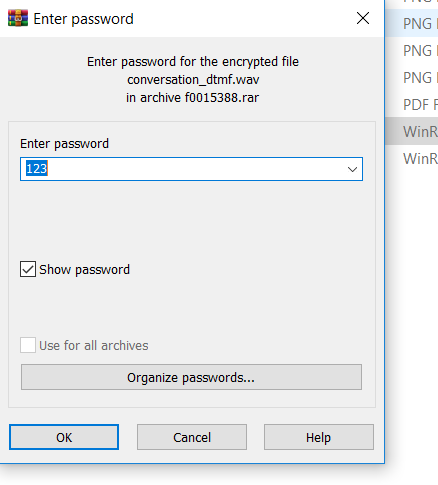
using the command

john password.hash --wordlist /usr/share/wordlists/rockyou.txt



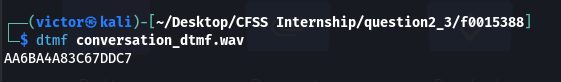
I got the password **'123'**

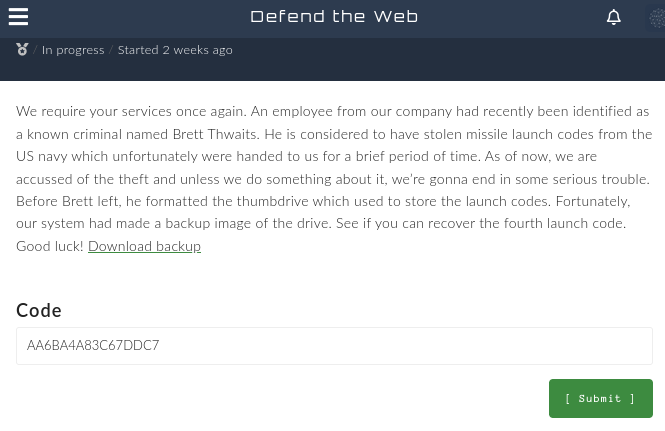




This revealed the file **conversation\_dtmf.wav**

using DTMF decoder, I ran the command

dtmf conversation\_dtmf.wav

I entered the code separated by '-' after every 4-byte to clear the challenge.

AA6B-A4A8-3C67-DDC7