Write-up : Black Box Emergency Retrieval

This challenge purpose is to trigger students to phish and email that can be found publicly.

There are two flags together to complete the “mission”. The first flag is the retrieval of the **emergency recovery procedure** file. The second is the content of the black box.

Let’s go step by step to understand the wanted scenario for flag one.

Flag 1 : Finding the Emergency protocol

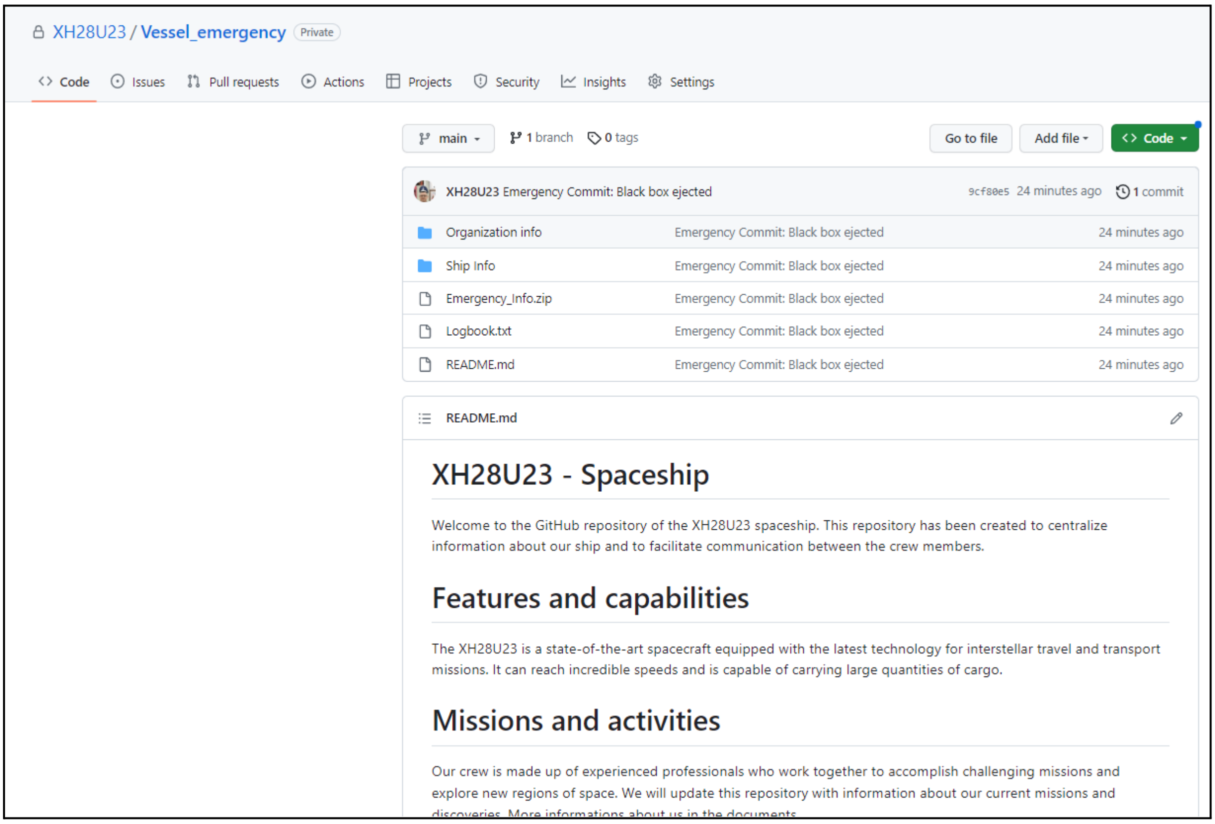
Step 1: read the description of the challenge

“The black box from the **XH28U23** vessel has been located on the campus of ESIEE. This box contains sensitive information that must not fall into the wrong hands. Your mission is to retrieve it before it’s too late. To succeed, you must be persuasive and have access to the right information. The fate of the mission rests on your shoulders. Will you rise to the challenge?”

The following description gives context. It is also going to be entry to understand the context.

Step 2: find the keyword to search for, spaceship name **“XH28U23”**

Step 3: Search for the github of XH28U23



XH28U23 Emergency Commit: Black box ejected 9cf80e5 24 minutes ago 1 commit

Organization info	Emergency Commit: Black box ejected	24 minutes ago
Ship Info	Emergency Commit: Black box ejected	24 minutes ago
Emergency_Info.zip	Emergency Commit: Black box ejected	24 minutes ago
Logbook.txt	Emergency Commit: Black box ejected	24 minutes ago
README.md	Emergency Commit: Black box ejected	24 minutes ago

README.md

XH28U23 - Spaceship

Welcome to the GitHub repository of the XH28U23 spaceship. This repository has been created to centralize information about our ship and to facilitate communication between the crew members.

Features and capabilities

The XH28U23 is a state-of-the-art spacecraft equipped with the latest technology for interstellar travel and transport missions. It can reach incredible speeds and is capable of carrying large quantities of cargo.

Missions and activities

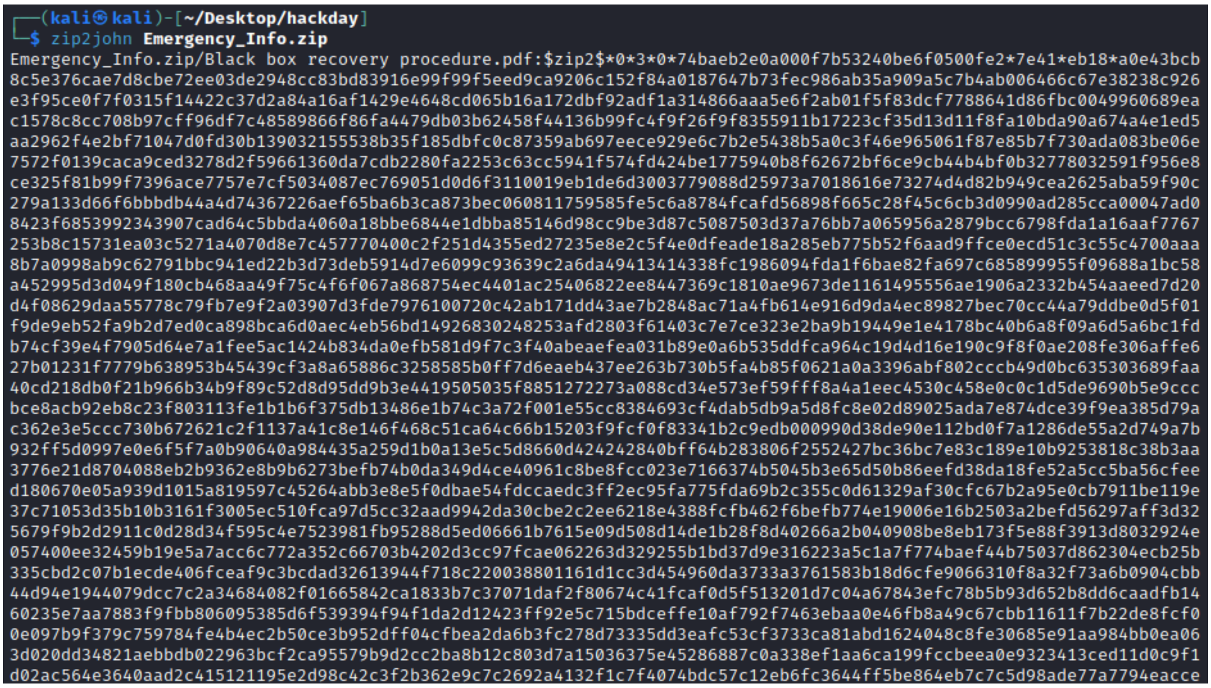
Our crew is made up of experienced professionals who work together to accomplish challenging missions and explore new regions of space. We will update this repository with information about our current missions and discoveries. More informations about us in the documents.

The github has one repository. This repository contains different information about the spaceship which will be important for the information gathering of the second flag.

Step 4: get the **Emergency_info.zip** which contains the flag.txt and the emergency recovery procedure

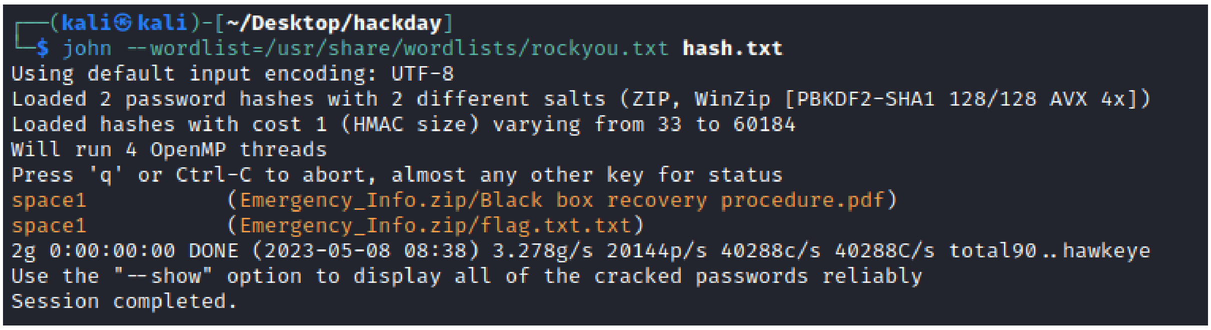
The Emergency_info.zip file is a password protected .zip. To open it, the participants have to use a bruteforcing tool.

Using **zip2john**, they will first have to gather the hash of the .zip files.



```
┌──(kali㉿kali)-[~/Desktop/hackday]
└─$ zip2john Emergency_Info.zip
Emergency_Info.zip/Black box recovery procedure.pdf:$zip2$*0*3*0*74baeb2e0a000f7b53240be6f0500fe2*7e41*eb18*a0e43bcb
8c5e376cae7d8cbe72ee03de2948cc83bd83916e99f99f5eed9ca9206c152f84a0187647b73fec986ab35a909a5c7b4ab006466c67e38238c926
e3f95ce0f7f0315f14422c37d2a84a16af1429e4648cd065b16a172dbf92adf1a314866aaa5e6f2ab01f5f83dcf7788641d86fbc0049960689ea
c1578c8cc708b97cff96df7c48589866f86fa4479db03b62458f44136b99fc4f9f26f9f8355911b17223cf35d13d11f8fa10bda90a674a4e1ed5
aa2962f4e2bf71047d0fd30b139032155538b35f185dbfc0c87359ab697eece929e6c7b2e5438b5a0c3f46e965061f87e85b7f730ada083be06e
7572f0139caca9ced3278d2f59661360da7cdb2280fa2253c63cc5941f574fd424be1775940b8f62672bf6ce9cb44b4bf0b32778032591f956e8
ce325f81b99f7396ace7757e7cf5034087ec769051d0d6f3110019eb1de6d3003779088d25973a7018616e73274d4d82b949cea2625aba59f90c
279a133d66f6bbbdb44a4d74367226aef65ba6b3ca873bec060811759585fe5c6a8784fcafd56898f665c28f45c6cb3d0990ad285cca00047ad0
8423f6853992343907cad64c5bbda4060a18bbe6844e1dbba85146d98cc9be3d87c5087503d37a76bb7a065956a2879bcc6798fda1a16aaf7767
253b8c15731ea03c5271a4070d8e7c457770400c2f251d4355ed27235e8e2c5f4e0dfeade18a285eb775b52f6aad9ffce0ecd51c3c55c4700aaa
8b7a0998ab9c62791bbc941ed22b3d73deb5914d7e6099c93639c2a6da49413414338fc1986094fda1f6bae82fa697c685899955f09688a1bc58
a452995d3d049f180cb468aa49f75c4f6f067a868754ec4401ac25406822ee8447369c1810ae9673de1161495556ae1906a2332b454aaeed7d20
d4f08629daa55778c79fb7e9f2a03907d3fde7976100720c42ab171dd43ae7b2848ac71a4fb614e916d9da4ec89827bec70cc44a79ddbe0d5f01
f9de9eb52fa9b2d7ed0ca898bca6d0aec4eb56bd14926830248253afd2803f61403c7e7ce323e2ba9b19449e1e4178bc40b6a8f09a6d5a6bc1fd
b74cf39e4f7905d64e7a1fee5ac1424b834da0efb581d9f7c3f40abeaefea031b89e0a6b535ddfca964c19d4d16e190c9f8f0ae208fe306affe6
27b01231f7779b638953b45439cf3a8a65886c3258585b0ff7d6eaeb437ee263b730b5fa4b85f0621a0a3396abf802cccb49d0bc635303689faa
40cd218db0f21b966b34b9f89c52d8d95dd9b3e4419505035f8851272273a088cd34e573ef59fff8a4a1eec4530c458e0c0c1d5de9690b5e9ccc
bce8acb92eb8c23f803113fe1b1b6f375db13486e1b74c3a72f001e55cc8384693cf4dab5db9a5d8fc8e02d89025ada7e874dce39f9ea385d79a
c362e3e5ccc730b672621c2f1137a41c8e146f468c51ca64c66b15203f9fcf0f83341b2c9edb000990d38de90e112bd0f7a1286de55a2d749a7b
932ff5d0997e0e6f5f7a0b90640a984435a259d1b0a13e5c5d8660d424242840bff64b283806f2552427bc36bc7e83c189e10b9253818c38b3aa
3776e21d8704088eb2b9362e8b9b6273befb74b0da349d4ce40961c8be8fcc023e7166374b5045b3e65d50b86eefd38da18fe52a5cc5ba56cfee
d180670e05a939d1015a819597c45264abb3e8e5f0dbae54fdccaedc3ff2ec95fa775fda69b2c355c0d61329af30cfc67b2a95e0cb7911be119e
37c71053d35b10b3161f3005ec510fca97d5cc32aad9942da30cbe2c2ee6218e4388fcfb462f6befb774e19006e16b2503a2befd56297aff3d32
5679f9b2d2911c0d28d34f595c4e7523981fb95288d5ed06661b7615e09d508d14de1b28f8d40266a2b040908be8eb173f5e88f3913d8032924e
057400ee32459b19e5a7acc6c772a352c66703b4202d3cc97fcae062263d329255b1bd37d9e316223a5c1a7f774baef44b75037d862304ecb25b
335cbd2c07b1ecde406fceaf9c3bcdad32613944f718c220038801161d1cc3d454960da3733a3761583b18d6cfe9066310f8a32f73a6b0904cbb
44d94e1944079dcc7c2a34684082f01665842ca1833b7c37071daf2f80674c41fcaf0d5f513201d7c04a67843efc78b5b93d652b8dd6caadfb14
60235e7aa7883f9fbb806095385d6f539394f94f1da2d12423ff92e5c715bdceffe10af792f7463ebaa0e46fb8a49c67cbb11611f7b22de8fcf0
0e097b9f379c759784fe4b4ec2b50ce3b952dff04cfbea2da6b3fc278d73335dd3eafc53cf3733ca81abd1624048c8fe30685e91aa984bb0ea06
3d020dd34821aebbdb022963bcf2ca95579b9d2cc2ba8b12c803d7a15036375e45286887c0a338ef1aa6ca199fccbeea0e9323413ced11d0c9f1
d02ac564e3640aad2c415121195e2d98c42c3f2b362e9c7c2692a4132f1c7f4074bdc57c12eb6fc3644ff5be864eb7c7c5d98ade77a7794eacce
```

Then using john and rockyou wordlist, it is possible to get the password used to protect the zip folder.



```
┌──(kali㉿kali)-[~/Desktop/hackday]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (ZIP, WinZip [PBKDF2-SHA1 128/128 AVX 4x])
Loaded hashes with cost 1 (HMAC size) varying from 33 to 60184
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
space1           (Emergency_Info.zip/Black box recovery procedure.pdf)
space1           (Emergency_Info.zip/flag.txt.txt)
2g 0:00:00:00 DONE (2023-05-08 08:38) 3.278g/s 20144p/s 40288c/s 40288C/s total90..hawkeye
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Flag 2 : Phishing the mail to get the black box password

Once the password is found for the zip, the participants have now new information to proceed further.

Note : We will not talk about physically finding the black box, as it is independent of these steps. It can be done directly or with the tips from the github file “radius_map”.

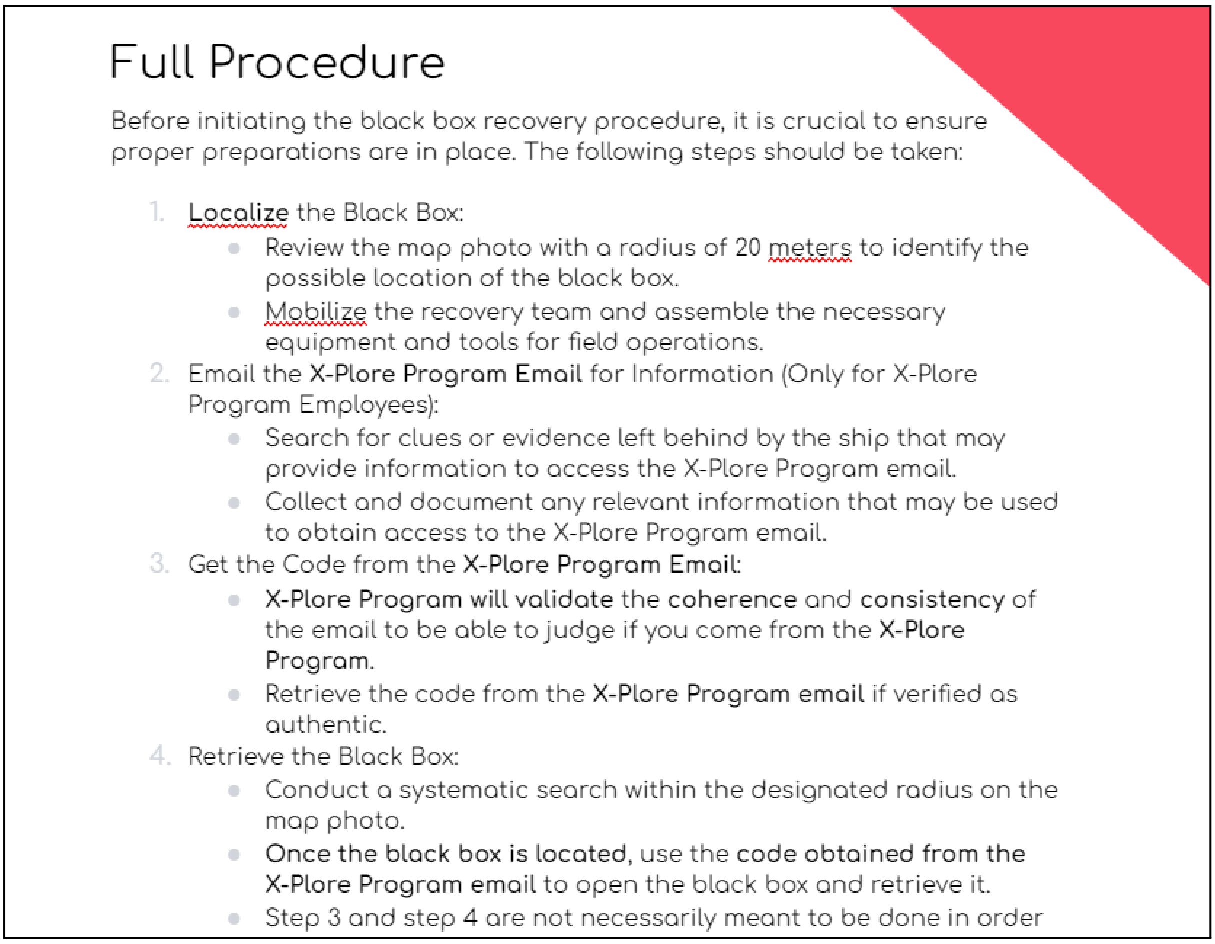
The objective here is to open the black box, using phishing methods. They’ll have to:

- Understand the emergency procedure
- Find the email to phish (X-PLORE program email) - agent_XH28U23@protonmail.com
- Gather information on the ship and create a real scenario
- Phish the email to get the code

Step 1: Understand the **emergency recovery procedure**

Black box : Emergency Recovery Procedure

The Black Box Emergency Recovery Procedure can be found with the first flag. This document explains step-by-step how to recover the black-box and its information.



Full Procedure

Before initiating the black box recovery procedure, it is crucial to ensure proper preparations are in place. The following steps should be taken:

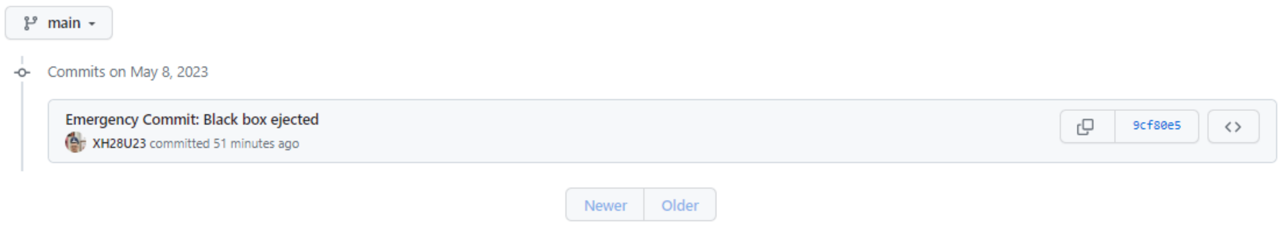
1. Localize the Black Box:
   - Review the map photo with a radius of 20 meters to identify the possible location of the black box.
   - Mobilize the recovery team and assemble the necessary equipment and tools for field operations.
2. Email the **X-Plore Program Email** for Information (Only for X-Plore Program Employees):
   - Search for clues or evidence left behind by the ship that may provide information to access the X-Plore Program email.
   - Collect and document any relevant information that may be used to obtain access to the X-Plore Program email.
3. Get the Code from the **X-Plore Program Email**:
   - **X-Plore Program will validate** the **coherence** and **consistency** of the email to be able to judge if you come from the **X-Plore Program**.
   - Retrieve the code from the **X-Plore Program email** if verified as authentic.
4. Retrieve the Black Box:
   - Conduct a systematic search within the designated radius on the map photo.
   - **Once the black box is located**, use the **code obtained from the X-Plore Program email** to open the black box and retrieve it.
   - Step 3 and step 4 are not necessarily meant to be done in order

Using the information it is to be understood that the steps you have to follow are such as :

- Finding the Black Box
- Emailing the X-PLORE Program by making a legit enough mail
- Get the code of the box from the email
- Open the box
- Give the info inside the box to agent 00 by presenting a valid XPLORE ID format
- End

Step 2: Find the **email**

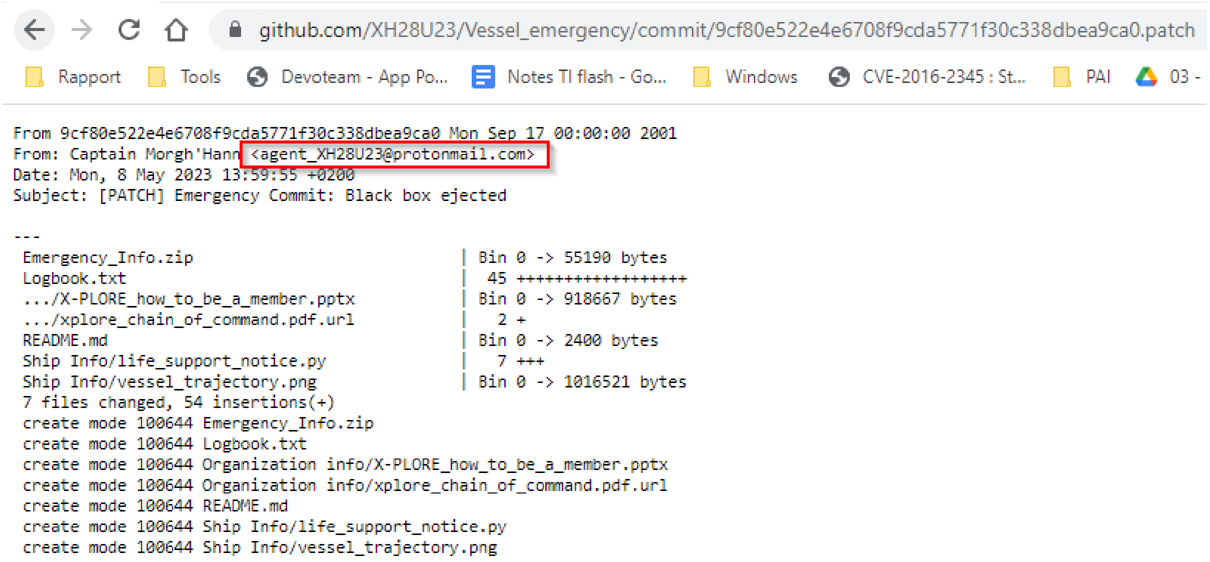
To find the email let’s look into the Github repository commits.



Commits on May 8, 2023

Emergency Commit: Black box ejected
XH28U23 committed 51 minutes ago

By clicking the commit and accessing its patch, it is possible to find the email of the github.



github.com/XH28U23/Vessel_emergency/commit/9cf80e522e4e6708f9cda5771f30c338dbea9ca0.patch
Rapport
Tools
Devoteam - App Po...
Notes TI flash - Go...
Windows
CVE-2016-2345 : St...
PAI
03 -

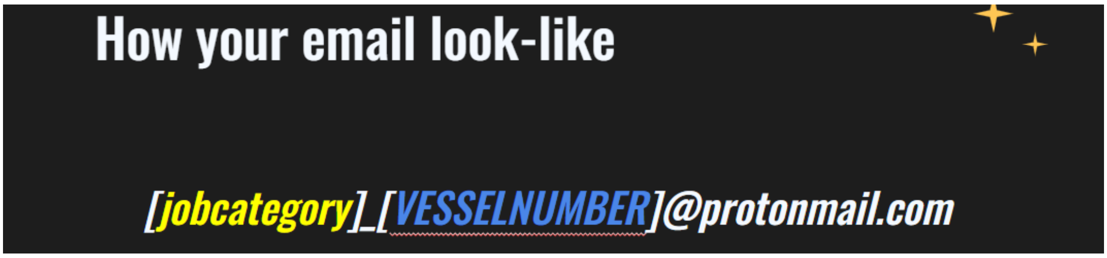
```
From 9cf80e522e4e6708f9cda5771f30c338dbea9ca0 Mon Sep 17 00:00:00 2001
From: Captain Morgh'Hann <agent_XH28U23@protonmail.com>
Date: Mon, 8 May 2023 13:59:55 +0200
Subject: [PATCH] Emergency Commit: Black box ejected

---
 Emergency_Info.zip                               | Bin 0 -> 55190 bytes
 Logbook.txt                                      |  45 ++++++++++++++++++
 .../X-PLORE_how_to_be_a_member.pptx              | Bin 0 -> 918667 bytes
 .../xplore_chain_of_command.pdf.url              |   2 +
 README.md                                        | Bin 0 -> 2400 bytes
 Ship Info/life_support_notice.py                 |   7 +++
 Ship Info/vessel_trajectory.png                  | Bin 0 -> 1016521 bytes
 7 files changed, 54 insertions(+)
 create mode 100644 Emergency_Info.zip
 create mode 100644 Logbook.txt
 create mode 100644 Organization info/X-PLORE_how_to_be_a_member.pptx
 create mode 100644 Organization info/xplore_chain_of_command.pdf.url
 create mode 100644 README.md
 create mode 100644 Ship Info/life_support_notice.py
 create mode 100644 Ship Info/vessel_trajectory.png
```

Step 3: Gather informations about the ship to **create a scenario**

There is a lot of information in the repository to be used to create a legit scenario.

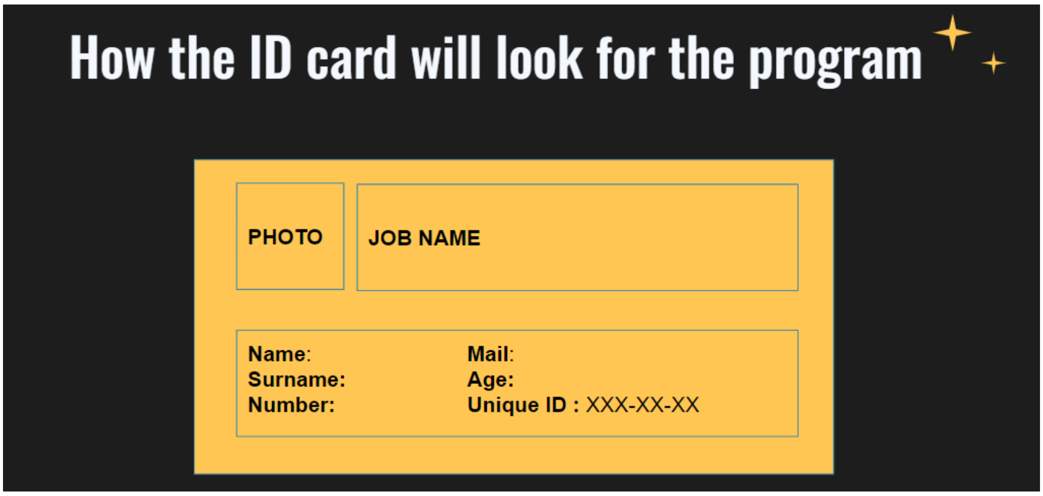
Let's look into each file/folders

1. *Organisation Info (folder)*:
    a. X-PLORE: a presentation of the xplore program containing information about the emails used by the program, the crew members that work there, and also the template for a legitimate ID.



How your email look-like

[jobcategory]_[VESSELNUMBER]@protonmail.com

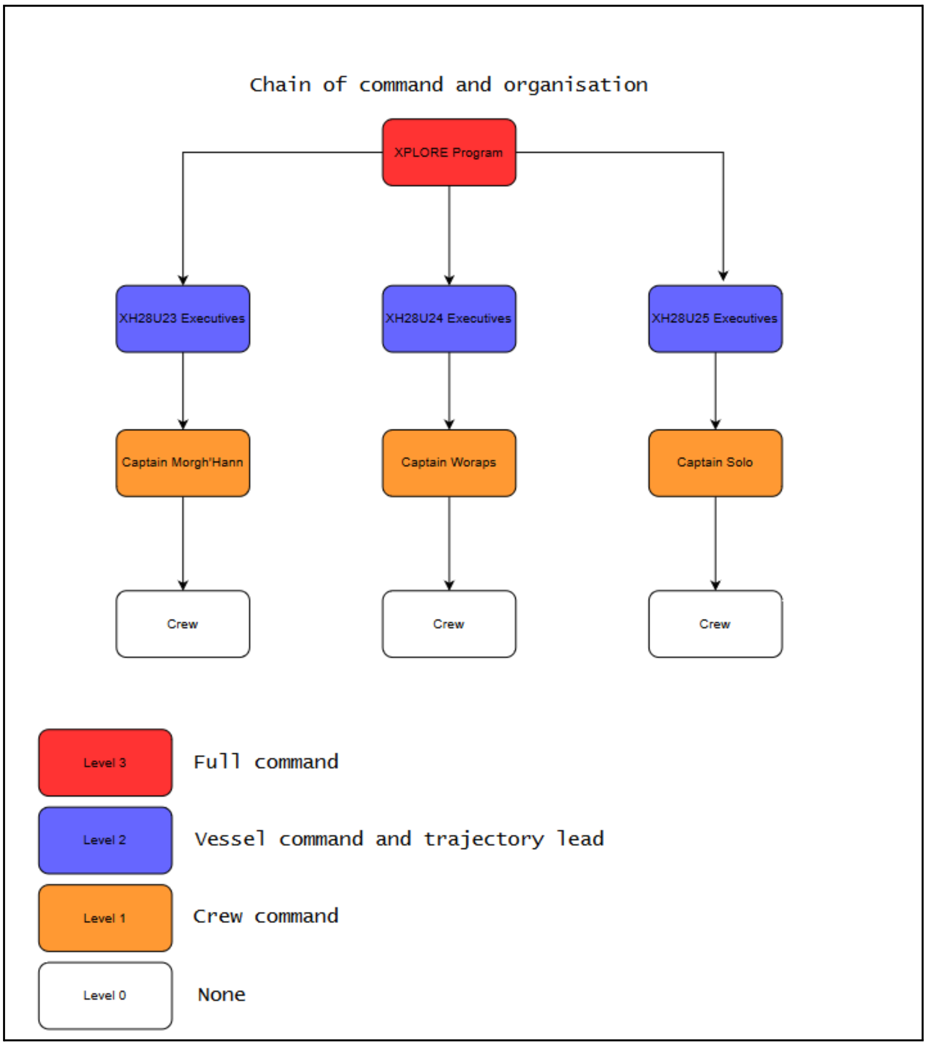


How the ID card will look for the program

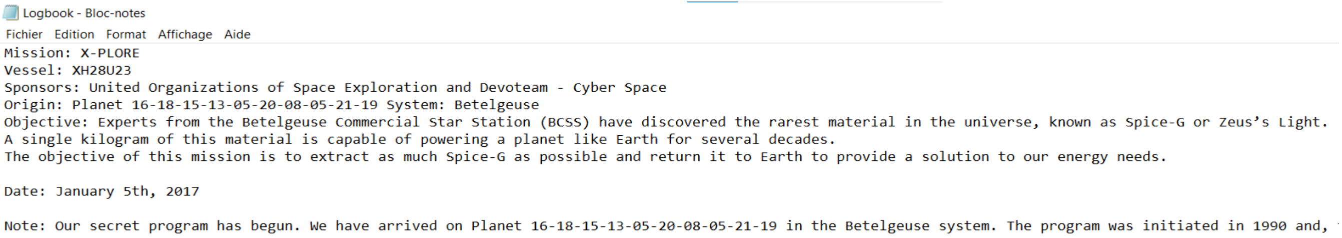
PHOTO	JOB NAME

Name:	**Mail**:
Surname:	**Age:**
Number:	**Unique ID :** XXX-XX-XX

b. X-PLORE Chain of command : a chain of command diagram containing hierarchical information on the program



2. *Ship info (folder)*:
    a. Life_support_notice.py: an obfuscated pythoncode that only contains a print command that talks about when the crew from the spaceship is on hibernation (could be used for scenario making)
    b. Vessel_trajectory: a picture of the trajectory followed by the XH28U23 (could be used for scenario)
3. Logbook (file): containing information about the XH28U23 adventure (could be used for scenario)



```
Mission: X-PLORE
Vessel: XH28U23
Sponsors: United Organizations of Space Exploration and Devoteam - Cyber Space
Origin: Planet 16-18-15-13-05-20-08-05-21-19 System: Betelgeuse
Objective: Experts from the Betelgeuse Commercial Star Station (BCSS) have discovered the rarest material in the universe, known as Spice-G or Zeus’s Light.
A single kilogram of this material is capable of powering a planet like Earth for several decades.
The objective of this mission is to extract as much Spice-G as possible and return it to Earth to provide a solution to our energy needs.

Date: January 5th, 2017

Note: Our secret program has begun. We have arrived on Planet 16-18-15-13-05-20-08-05-21-19 in the Betelgeuse system. The program was initiated in 1990 and,
```

To be validated the phishing email has to contain at least two or three informations from the repository.

To be accepted a mail would have:

- To follow the format used by the X-PLORE mission (as shown in the XPLORE presentation pdf)
- Contain a correct scenario:
    - “I am a gerontologist from the XH28U24 vessel, I have retrieve the black box and followed the emergency procedure. I was in the BCSS and arrived to earth to catch the box.”
    - Sent from a : scientist_XH28U24@protonmail.com
- Imagination, the scenario is pretty open

If phishing is successful you’ll receive :

“Hello from the X-PLORE Program,

We have authenticated you as a member of the X-PLORE program.
Here is the code to open the box

- CODE : XXXX

Follow the full procedure to be able to get the informations out of the box.

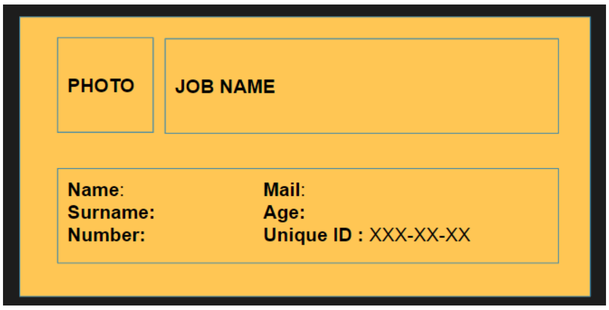
Good luck,

Best regards”

Step 4: Open the box and bring its content to the agent 00

Once the content of the box is opened, you’ll have to find agent-00 and bring him the flag. However, it is written in the procedure that you have to bring an X-PLORE ID.

To do so participants will have to come with a fake ID using the template of given in the presentation file of X-PLORE.



PHOTO

JOB NAME

Name:
Surname:
Number:

Mail:
Age:
Unique ID : XXX-XX-XX

Once the template given, with the fake ID the agent 00 will be able to give the last flag.