|  |
| --- |
| Cyber Defenders |
| Intel101 |
| Threat Intelligence |

|  |
| --- |
| Abdallah Chbaro  09/04/2023 |

Table des matières

[Scenario 2](#_Toc131969738)

[Tools 2](#_Toc131969739)

[Write Up 3](#_Toc131969740)

# Scenario

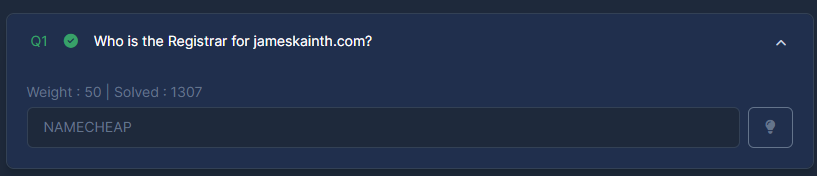
Open-source intelligence (OSINT) exercise to practice mining and analyzing public data to produce meaningful intel when investigating external threats.

# Tools

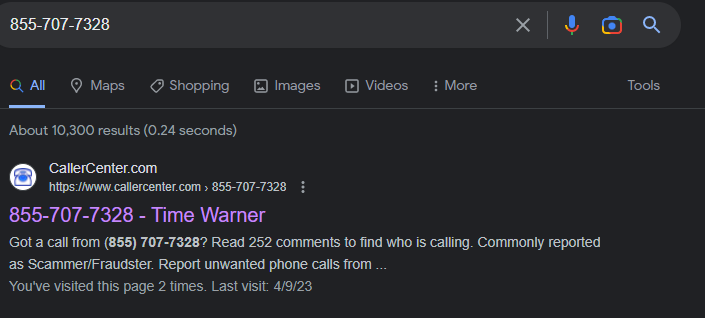
* Google Lens
* archive.org
* WhoIS

# Write Up

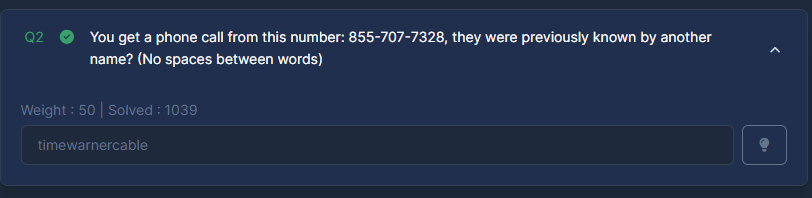
Looking for the domain on who.is, we find that the name of the registrat is NAMECHEAP:



Looking for the phone number on google, we find the following:

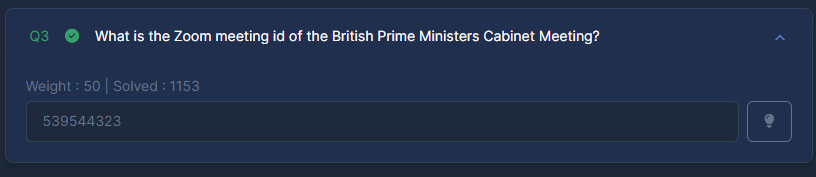


Scrolling through, we find it is for Spectrum. Doing a google search, we find that previously it was known as Time Warner Cable. As for the answer, we need to write it without spaces:

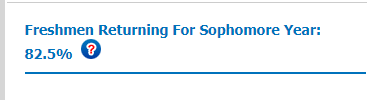


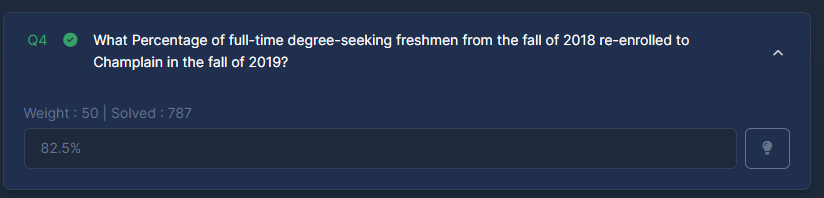
Doing a google search on the British prime ministers zoom meeting ID, we get the following:



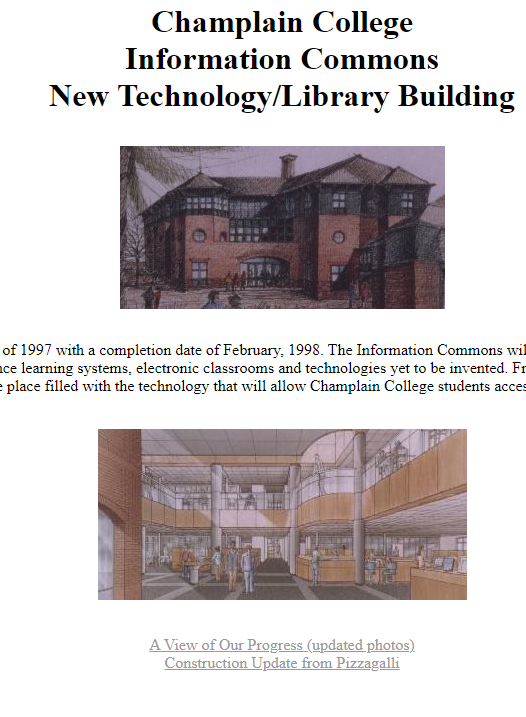


In question 4, they are asking about data from 2018. To do so, we need to use the way back machine:

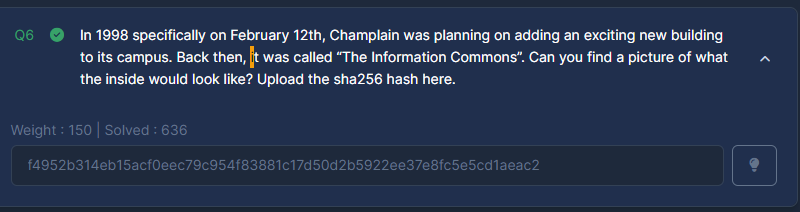




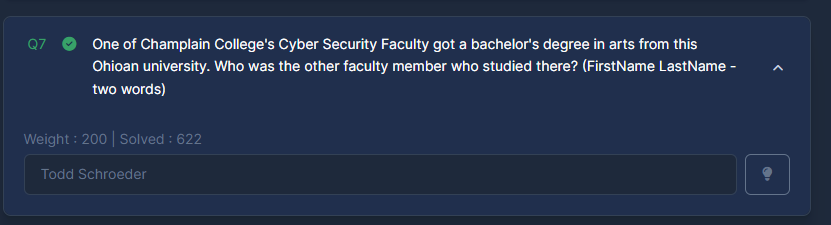
For question 6, we need to use the way back machine again:



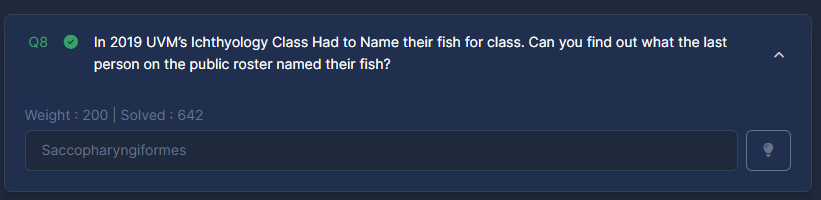
Downloading the interior image, we can calculate the checksum and submit it:



Next, searching for the faculty members, we found out that Joe Eastman has a Bachelor of Arts from the University of Toledo. I searched ‘“University of Toledo”. Then we seach of ‘University of Toledo’ site:champlain.edu, and we find Todd Schroeder:



A google search will lead us to an excel file containing the names. We need to check the last fish name:



For the last question, doing a Yandex search will give the answer:

