**CyberX – Chennai Cyber Hackathon 2.o - Problem Statements – 2023**

**May 19th and 20th, 2023**

**Problem1: Cryptocurrency Security: An interface/solution for crypto currency data analysis.**

Crypto transaction data comes from a variety of places, including wallets like Metamask, Coinbase, and exchanges like WazirX, and CoinDCX.

Aim is to identify and analyze the owner of these transactions and the purpose of the transaction??

Other transaction made by the id to be retrieved.

Those transactions mapped to the wallets have to be identified.

The proposed system should be able to do the following:

1. Cryptocurrency address validator
2. Note down the transactions and verify, the address.
3. Search for Wallet address from ID

<https://www.blockchain.com/explorer>

**Problem2: Mobile forensic Triage (quick method to find the evidence)**

In general, to know the details of the mobile:

Connect the mobile to the system

Extract data from the mobile

Export the extracted data to separate software like Cellebrite Physical analyser

Manually understand the report generated by the analyser,

The hackathon problem statement is to simply the above process by simply connecting the mobile to the system where the proposed solution is installed. That software should be able to give a checklist of details (call logs, Normal messages, Messages that could be filtered based on some parameter from any Chat Application, Photos, Videos, etc) that could be retrieved from the connected mobile. The user could preview the required data by selecting the appropriate checklist item. Based on the preview results the data could be extracted from the mobile if required.

**Problem 3:** **Social media monitoring tool**

Social media platforms have set up a mix of automated and human driven editorial processes to promote or filter certain types of content. In addition to that, their users are increasingly using these platforms as the primary source of getting their news. It is also important to consider how recommendation algorithms on social media platforms may inadvertently promote fake and hateful speech. At their core, these recommendation systems group users based on their shared interests and then promote the same type of content to all users within each group. If most of the users in one group have interests in, say, flat-earth theory and anti-vaccination hoaxes, then the algorithm will promote the anti-vaccination content to the users in the same group who may only be interested in flat-earth theory.

Currently, social media companies have adopted two approaches to fight misinformation. The first one is to block such content outright. For example, [Pinterest](https://www.fastcompany.com/90310970/the-tech-giant-fighting-anti-vaxxers-isnt-twitter-or-facebook-its-pinterest) bans anti-vaccination content and [Facebook](https://www.nbcnews.com/tech/tech-news/facebook-bans-white-nationalism-after-pressure-civil-rights-groups-n987991?cid=sm_npd_nn_tw_ma) bans white supremacist content. The other is to provide alternative information alongside the content with fake information so that the users are exposed to the truth and correct information. This approach, which is implemented by YouTube, encourages users to click on the links with verified and vetted information that would debunk the misguided claims made in fake or hateful content. If you search “Vaccines cause autism” on YouTube, while you still can view the videos posted by anti-vaxxers, you will also be presented with a link to the Wikipedia page of MMR vaccine that debunks such beliefs.

The proposed system of this hackathon is expected to perform the following. With a specified keyword (Tamil and English language) given as input to the software, it should be able to search across various social media platforms such as Instagram, Facebook, Twitter and identify the owners’ of the keyword, of textual data, with the timestamp.

**Problem 4: Anomaly Detection**

The detection of abnormal events in surveillance video systems remains challenging despite significant advancements in modern science. Anomaly detection is a time-critical application of computer vision. Design a system capable of detecting anomalies like the following:

1. a new person coming to the specified area who is not the resident of that area at any time
2. whether a person has any weapon during his visit at night time
3. a two wheeler towed manually in an abnormal night time
4. a person or a gang running fast in the night
5. over speed of vehicle in the night time
6. attack in night time
7. fire in the night time
8. a person staying in the same place or frequently visiting a place at night.

The system should be able to categorise the abnormally and it should be able to inform the same with a snap to the concerned officers mobile or through mail with the GPS based detailed location.

**Problem 5: Telegram live location tracing**

Telegram tracks your activities when you turn on the location feature within the app. Since you’ve granted it permission to track you, it will use the location service on your device automatically. Another way Telegram tracks you is if you turn on your location services on or switch on your GPS. Since the Android OS can already track you this way, Telegram can access that data. Besides that, the most common way Telegram keeps track of your location is if you use its Live location feature. Once turned on, you give Telegram permission to access your location information and share it with the people you choose.

Without depending on the phone service providers, the proposed system should be able to trace the callee’s current location based on the live call in Telegram application. Basically this is to monitor someone else's location using this app via Telegram. The proposed solution should not use the telegram application’s live location feature for providing the demo.