

Attack

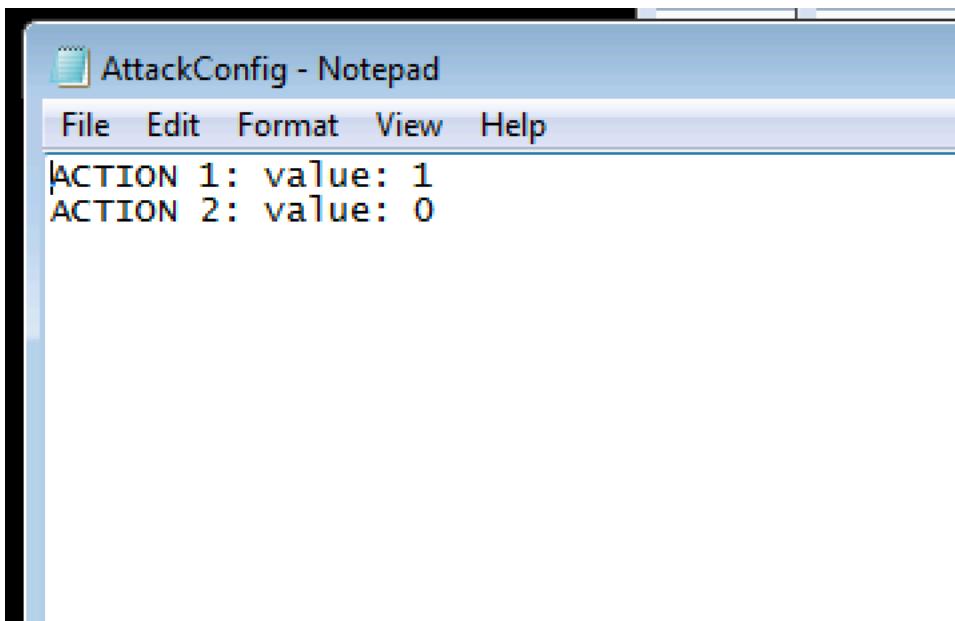
Define global variable for Config and Log path.

```
1 // Ting-Wei's code
// Two variables to store attack log path and attack config path
private String AttackLogPath = "C:\\\\Program Files\\\\ScadaBR\\\\tomcat\\\\logs\\\\AttackLog.txt";
private String AttackConfigPath = "C:\\\\Program Files\\\\ScadaBR\\\\tomcat\\\\conf\\\\AttackConfig.txt";
```

Here's my code for reading the Attack Config.

```
// Ting-Wei's Code
// Read Attack Config
public String ReadAttackConfig(int num_of_line) {
    String data = "";
    try {
        File myObj = new File(AttackConfigPath);
        Scanner myReader = new Scanner(myObj);
        int i = 1;
        // Find the Target line
        while (i != num_of_line) {
            myReader.nextLine();
            i++;
        }
        data = myReader.nextLine().split("value: ", 0)[1];
        myReader.close();
    } catch (FileNotFoundException e) {
        System.out.println("Read Attack Config error occurred");
    }
    return data;
}
```

The Attack Config.



The Read Config and Send Attack part.

I collected data under attack for 40 minutes.
Run the find WRITE API sequences script.

```
twang626@bird:~/Desktop/11_4$ python3 find_write_api_sequence.py
[+] Running USE_TIME_DB_READ_HEURISTIC Approach ... Finished!!
It takes 366.53 seconds
[+] Running USE_TCP_RECEIVE_HEURISTIC Approach ... Finished!!
It takes 3.12 seconds
USE_TIME_DB_READ_HEURISTIC Statistics
    Correctness Rate: 31.59%
    False Positive Rate: 7.39%
```

There are 1339 WRITE commands in total

[+] Exporting Files ... Finished!!
It takes 17.07 seconds

All: 4,645,778 API calls
SCADABR APIs: 1,387,445 API calls
SCADABR and Dependencies APIs: 1,387,499 API calls
READ commands: 2,266 API calls
WRITE commands: 1,339 API calls

Timing and Frequency Analysis.

```
twang626@bird:~/Desktop/11_4$ python3 timing_and_frequency_analysis.py
Write_to_Write_Timing:
    Count: 1338 in total
    Mean: 1788.03 milliseconds
    Standard Deviation: 2154.7 milliseconds
Read_to_Write_Timing:
    Count: 899 in total
    Mean: 71.91 milliseconds
    Standard Deviation: 99.15 milliseconds
Read_to_Read_Timing:
    Count: 2265 in total
    Mean: 1056.01 milliseconds
    Standard Deviation: 1273.2 milliseconds

Cycle Frequencies (Use a WRITE TO WRITE as a cycle)
    Cycle Count: 1338 in total
    Mean: (0.64681848, 0.03541519)
    Standard Deviation: (0.25556703, 0.09861156)
```

Factory I/O

I installed the free trial version (lasts for 30 days). But it's not able to be run on my VM because of performance issue. It hangs frequently and not responding.

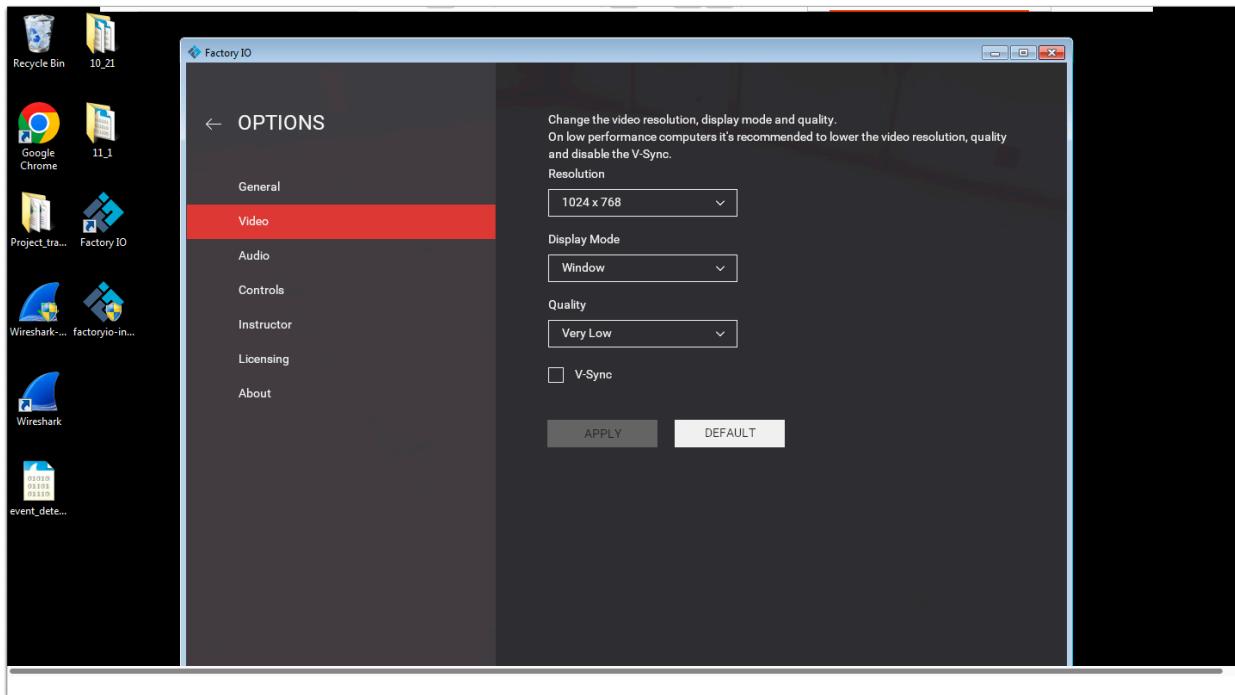
I've tried

More Processors (Total Processor Cores: 4 -> 8): Whole computer hangs, wait a long time to execute VMware.

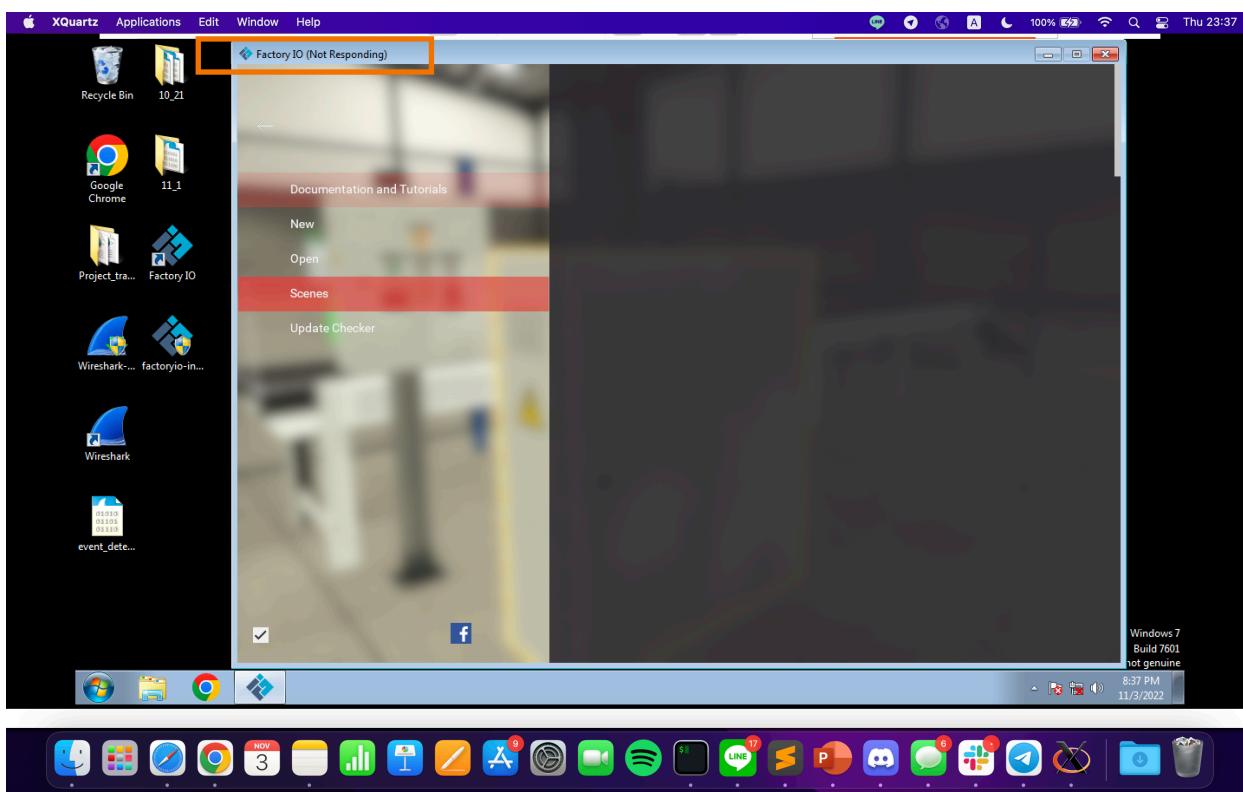
More RAM (20 GB -> 48 GB): Not getting better

Lower resolution and reduce video quality: 1 FPS to 3 FPS. It's still not applicable.

Video Configuration in Factory I/O, I changed everything to the lowest.



Not Responding and Hangs (Shown in the orange box)



Low Performance 3 FPS (Shown in the orange box)

