

Tue 10:30

Thur 10:30

Robot #301

역공학

Reverse Engineering

# Exploring a Suspicious File

---

Assignment #2

박 정 흠

Park, Jungheum

jungheumpark@korea.ac.kr



Korea University  
School of Cybersecurity

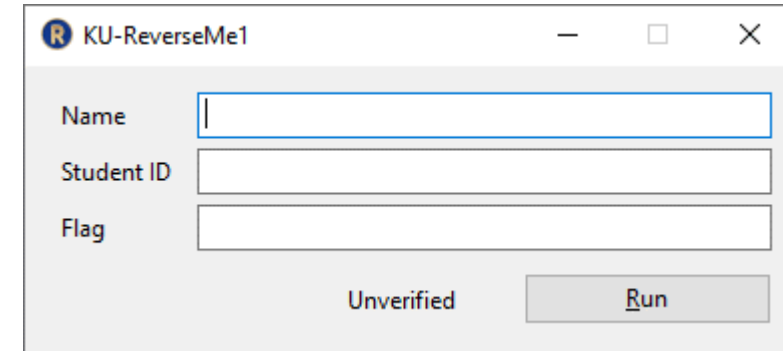
# What You Must Do

---

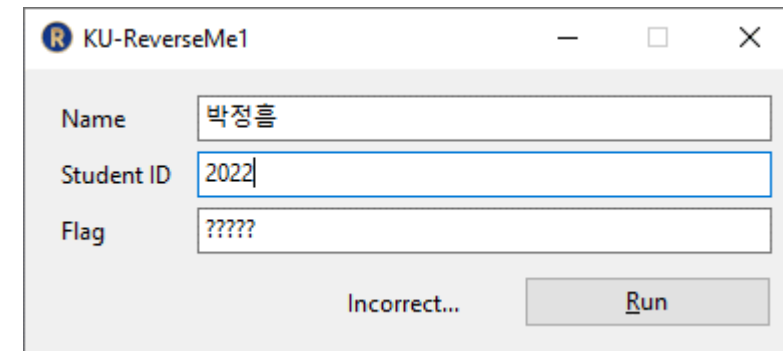
# What You Must Do

## Target PE File

- Overview of Target PE File
  - 'KU-ReverseMe1'
    - 32-bit & 64-bit applications
  - Portable Executable files



The screenshot shows the 'KU-ReverseMe1' application window. It has three input fields: 'Name', 'Student ID', and 'Flag'. The 'Name' field is empty. The 'Student ID' field is empty. The 'Flag' field is empty. Below the fields, there is a status indicator 'Unverified' and a 'Run' button.



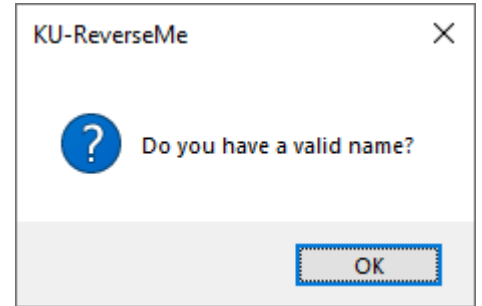
The screenshot shows the 'KU-ReverseMe1' application window. The 'Name' field is filled with '박정흠'. The 'Student ID' field is filled with '2022'. The 'Flag' field is filled with '?????'. Below the fields, there is a status indicator 'Incorrect...' and a 'Run' button.

# What You Must Do

## Questions

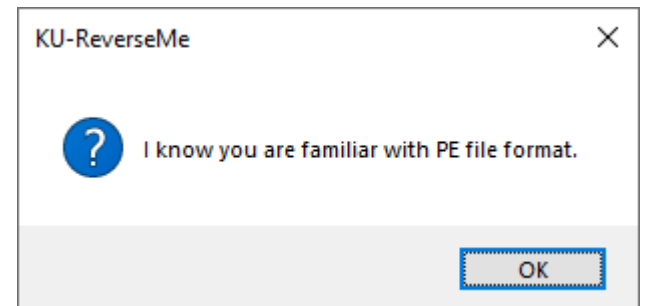
- [1] Execute the target PE file properly. How did you do that? (2)

- [Tool] **IDA**, Ghidra
- [API] GetModuleFileName, GetFileTitle



- [2] Execute the target PE file properly. How did you do that? (2)

- [Tool] IDA, **Ghidra**
- [API] GetModuleFileName, CreateFile, GetFileSize



# What You Must Do

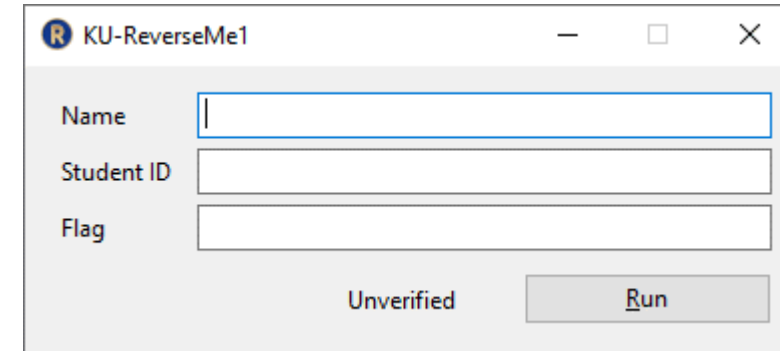
## Questions

- **After the 'Run' button is pressed once, you can answer the following questions:**
  - **[3] What is the full path of a file automatically generated? (1)**
    - [Tool] Process Monitor
    - [API] CreateFile
  - **[4] How many times was the file generated in total per pressing the button? (1)**
    - [Tool] Process Monitor
  - **[5] Identify and describe an algorithm that determines the number of times. (1)**
    - [Tool] IDA or Ghidra
    - [API] GetDlgItemText

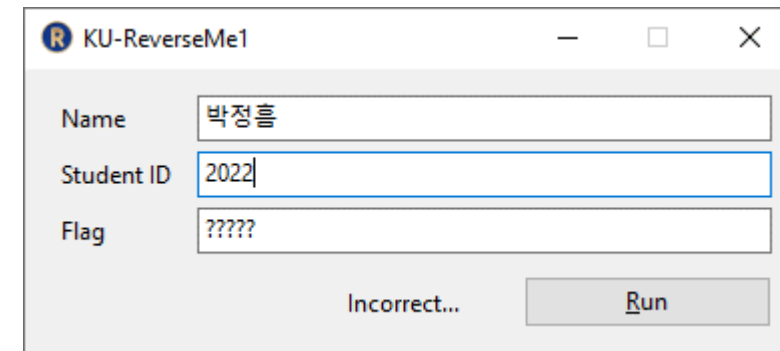
# What You Must Do

## Questions

- [6] Find a valid flag. (3)
  - [Tool] IDA or Ghidra
  - [API] GetDlgItemText



The screenshot shows the 'KU-ReverseMe1' application window. It has three input fields: 'Name', 'Student ID', and 'Flag'. The 'Name' field is empty. The 'Student ID' field is empty. The 'Flag' field is empty. Below the fields, there is a status indicator 'Unverified' and a 'Run' button.



The screenshot shows the 'KU-ReverseMe1' application window after an attempt. The 'Name' field contains the text '박정흠'. The 'Student ID' field contains the text '2022'. The 'Flag' field contains the text '?????'. Below the fields, the status indicator has changed to 'Incorrect...' and the 'Run' button is still present.

# What You Must Do

## [REF] Useful Tools

### ■ Basic Static Analysis

- HxD, CyberChef, HashMyFiles
- strings, FLOSS
- Exeinfo PE, pestudio, PPEE, PE-bear
- Resource Hacker
- YARA
- capa

### ■ Static Code Analysis

- IDA
- Ghidra

### ■ Basic Dynamic Analysis

- Process Hacker, Process Explorer
- Process Monitor
- System Monitor
- Wireshark
- Sandboxie-Plus

### ■ Dynamic Code Analysis

- x32dbg / x64dbg
- Frida

# How to Submit

---



# How to Submit

## Documentation Rules

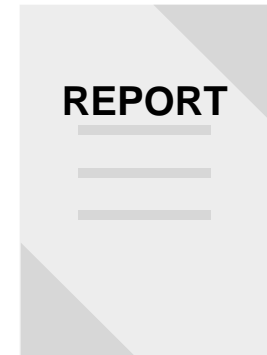
- **Write a Technical Report using Markdown**
  - You should explain your step-by-step processes
  - Report structure
    - For this assignment, you can freely design your own report
  - [REF] Apps/Services for writing Markdown files:
    - You can choose anyone such as *VS Code*, *R*, *Typora*, *Notion* ...
      - Syntax: <https://support.typora.io/Markdown-Reference>



# How to Submit

## Submission Rules

- **Submit Your Files to the Blackboard** ('Assignments and Tests' page)
  - File format: PDF
  - File name: [2022-RE]-[ID]-[NAME]
- **Deadline**
  - 2022.11.29. (Tue) 10:29
- **Points (10)**
  - Answers + Report's Quality



THANK YOU  
for Listening!

**jungheumpark@korea.ac.kr**

KOREA UNIVERSITY Digital Forensic Research Center | [dfrc.korea.ac.kr](http://dfrc.korea.ac.kr)

Questions?

