FLIRT

김영철

2016. 7. 15.

Idea

- 프로그램 내부의 각각의 function들은 pattern으로 표현됨
- pattern은 function의 첫 32바이트를 가리킴

Idea

Example

패턴이 같음

558BEC0EFF7604.....59595DC3558BEC0EFF7604.....59595DC3 _registerbgidriver
558BEC1E078A66048A460E8B5E108B4E0AD1E9D1E980E1C0024E0C8A6E0A8A76 _biosdisk
558BEC1EB41AC55604CD211F5DC3..... _setdta
558BEC1EB42FCD210653B41A8B5606CD21B44E8B4E088B5604CD219C5993B41A _findfirst

558BEC
0EFF7604.....59595DC3558BEC0EFF7604.....59595DC3 _registerbgidriver
1E
078A66048A460E8B5E108B4E0AD1E9D1E980E1C0024E0C8A6E0A8A76 _biosdisk
B4
1AC55604CD211F5DC3 _setdta
2FCD210653B41A8B5606CD21B44E8B4E088B5604CD219C5993B41A _findfirst

Idea

- tree structure
  - 메모리 사용량을 줄일 수 있음
  - fast fast pattern matching에 적절함

558BEC
0EFF7604.....59595DC3558BEC0EFF7604.....59595DC3 _registerbgidriver
1E
078A66048A460E8B5E108B4E0AD1E9D1E980E1C0024E0C8A6E0A8A76 _biosdisk
B4
1AC55604CD211F5DC3 _setdta
2FCD210653B41A8B5606CD21B44E8B4E088B5604CD219C5993B41A _findfirst

Idea

- pattern이 같은 경우
  - CRC16 값 비교
  - CRC16 값도 같은 경우에는 다른 바이트를 갖는 leaf 안에 있는 모든 function들에 대한 position을 찾음
  - 그래도 같은 경우에는 “collision” 이라고 함
    - 효율성과 속도를 위해 collision을 구별하는 일은 나중에 생각

Idea

pattern 같은 경우
558BEC561EB8....8ED833C050FF7608FF7606.....83C4068BF083FEFF
0. _chmod (20 5F33)
1. _access (18 9A62)

pattern + CRC 값 같은 경우
05B8FFFFEB278A4606B4008BD8B8....8EC0
0. _tolower (03 41CB) (000C:00)
1. _toupper (03 41CB) (000C:FF)

pattern + CRC 값 + offset 같은 경우
0D8A049850E8....83C402880446803C0075EE8BC7:
0. _strupr (04 D19F) (REF 0011: _toupper)
1. _strlwr (04 D19F) (REF 0011: _tolower)