Win32API Interceptor
Monitoring Windows API calls

The project’s goal: To create an application that is able to log all Win32API function calls that were issued by a user specified process/application

Kfir Karmon (skarmont2.technion.ac.il)
Polina Shafran (shpolina@t2.technion.ac.il)

Supervisors:
Dr. Ilana David (ilana@ee.technion.ac.il)
Ben Bernstein, Microsoft (bbern@microsoft.com)
The Detours Technology

The system is built using the Detours technology, that was developed by Microsoft researchers.

- No access to source code is needed.
- Interception code is applied dynamically at runtime.
- The original code is modified in memory only.

Diagram: How Detours change the original functions' calling sequence
Win32API Interceptor – Architecture

1. Create COM Object
2. Create COM Object
3a. Spawn
3b. Inject
4. Post function call logging data
5. Extract logging data
6. Log function call data

Win32API Interceptor (MS Access Data Base)

DllInjectionAppLoader (COM Object)

InterceptLogger (COM Object)

TraceAPI. DLL (Binary DLL with the Detours functions)

Spawned process (with the TraceAPI.DLL injected)

\pipe\Win32APIInterceptor (OS pipe)
Win32API Interceptor – Screenshot