.NET DEVELOPER DAYS

Building Your Own Debugging Toolbox With ClrMD

Kevin Gosse **@kookiz**
Christophe Nasarre **@chnasarre**

Agenda

- Introduction to ClrMD
- From live process to memory dump
- ClrHeap, addresses and types
- Marshaling data from instance and static fields

Introduction: why ClrMD?

ClrMD helps you automate .NET application analysis in C#

Work on running process or memory dump

Sky is the limit!

DEMO

Why ClrMD?

ClrMD Basics

ClrMD = Microsoft.Diagnostics.Runtime Nuget package

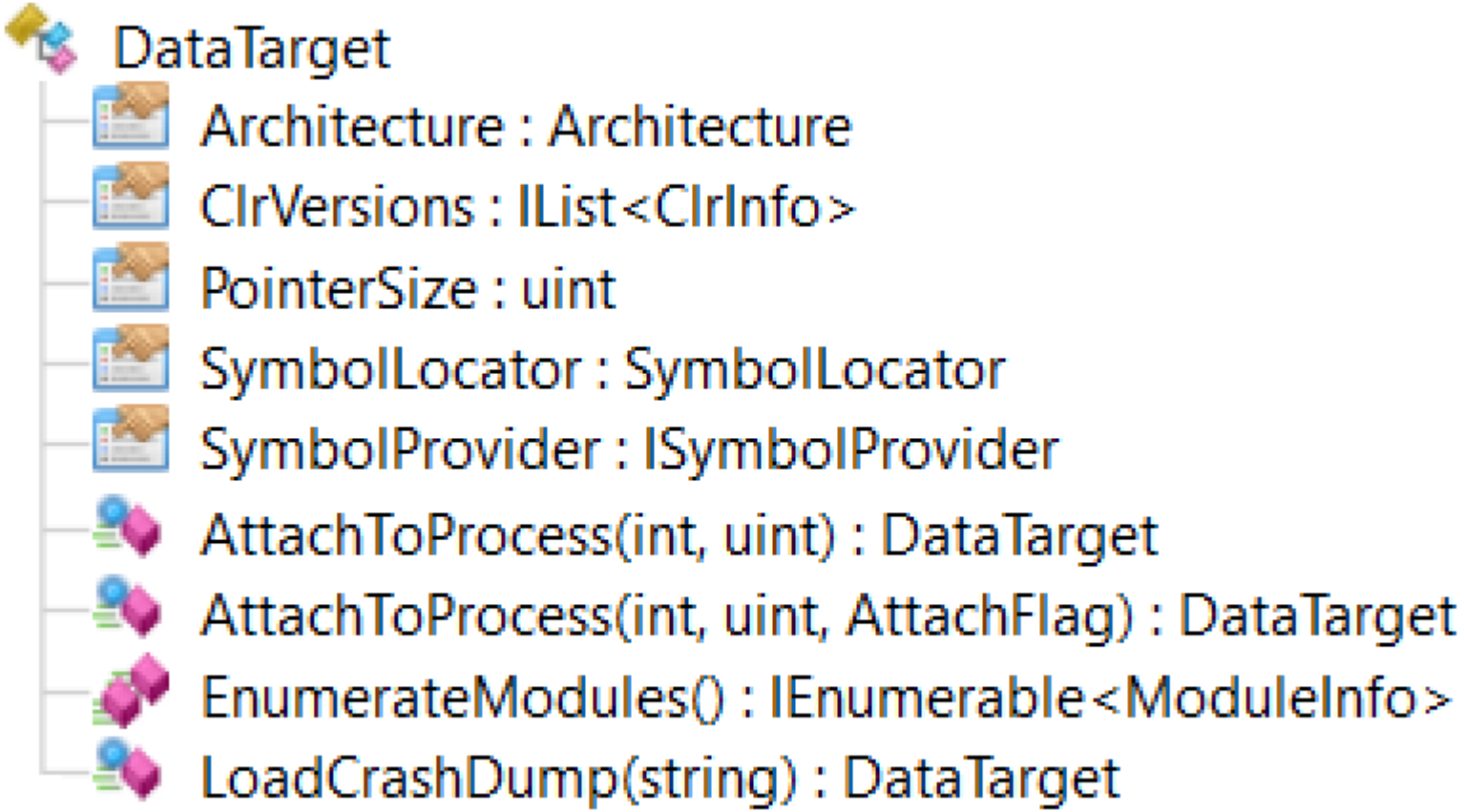
The source code is available on GitHub

Take a look at the samples and the implementation

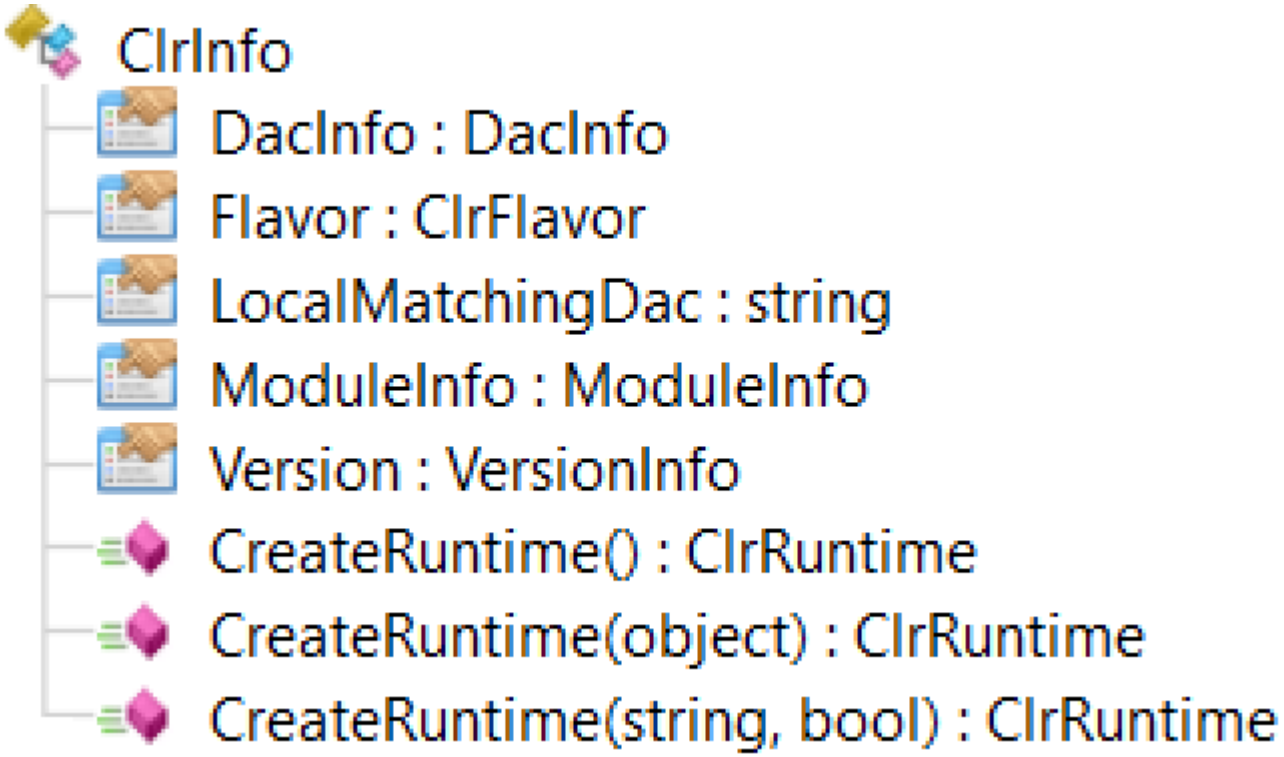
Agenda

- Introduction to ClrMD
- From live process to memory dump
- ClrHeap, addresses and types
- Marshaling data from instance and static fields

`DataTarget` to bootstrap them all



`ClrInfo` and a little bit of black magic



Use **DataTarget.SymbolLocator** to setup symbols/dll locations

srv*c:\symbols*http://msdl.microsoft.com/download/symbols

ClrRuntime

AppDomains
Assemblies (modules)
Threads
Thread Pool
Heap

More advanced
- finalizers
- pinned objects
- methods

Lab

.NET DEVELOPER DAYS

Getting started with ClrMD

Agenda

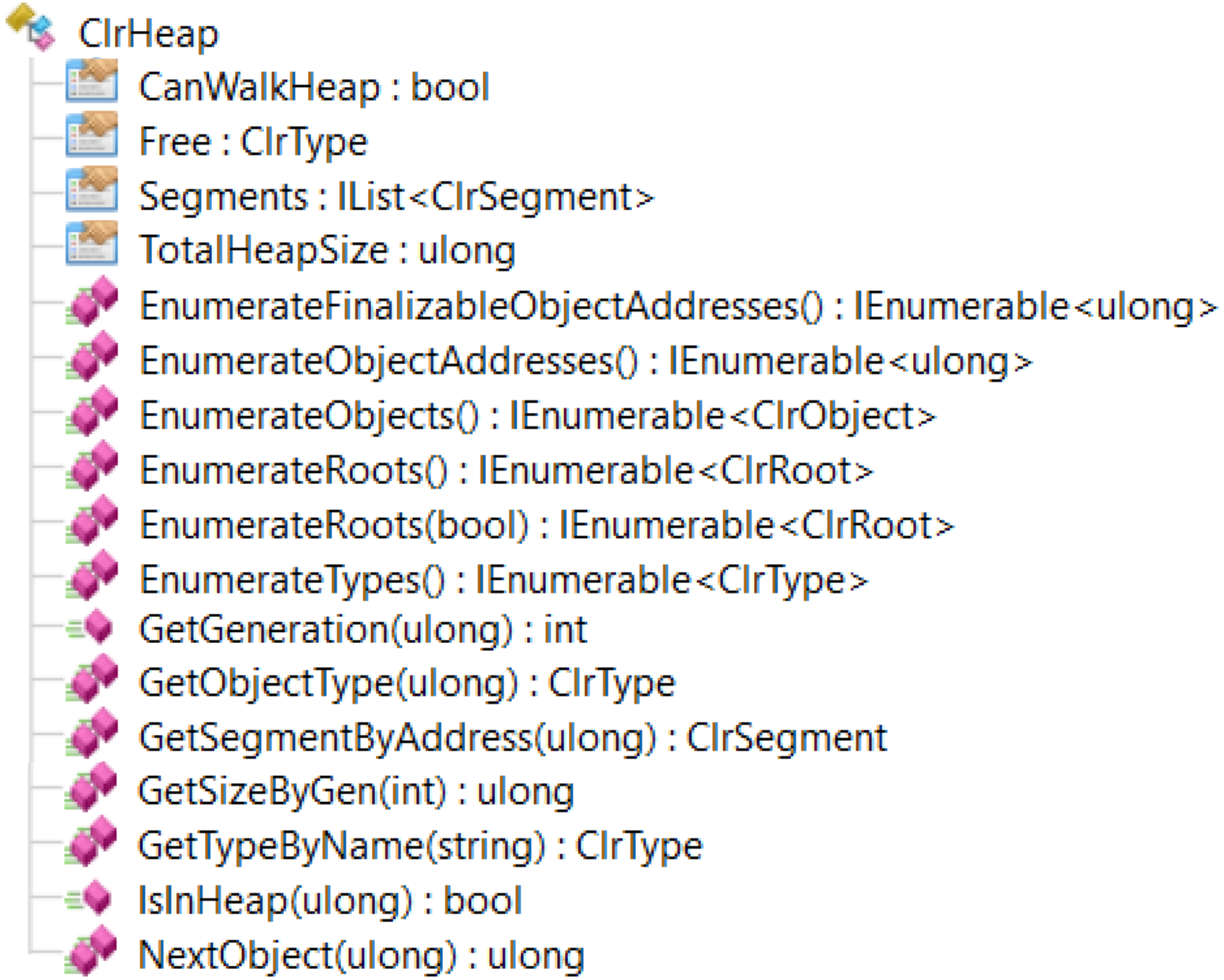
- Introduction to ClrMD
- From live process to memory dump
- ClrHeap, addresses and types
- Marshaling data from instance and static fields

ClrHeap

CanWalkHeap!

address != object

Low level details
- segments
- finalizables
- roots



How to browse all objects in the heap


```
foreach (ulong address in heap.EnumerateObjectAddresses())
{
    try
    {
        var objType = heap.GetObjectType(address);
        if (objType == null)
            continue;

        var obj = objType.GetValue(address);

        ...

    }
    catch (Exception x)
    {
        WriteLine(x);
        // some InvalidOperationException might occur sometimes
    }
}
```

Lab

.NET DEVELOPER DAYS

Count duplicated strings

Agenda

- Introduction to ClrMD
- From live process to memory dump
- ClrHeap, addresses and types
- Marshaling data from instance and static fields

Problem of class instance marshalling

All addresses are meaningless in the current process

`ClrType.GetValue()` automatically marshals basic types

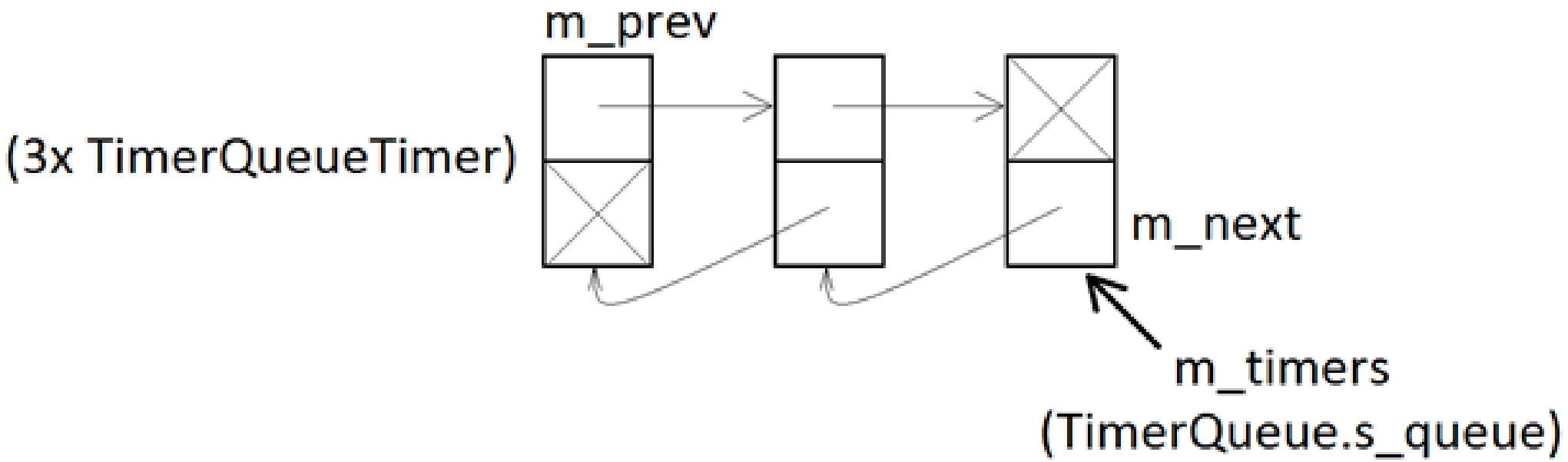
- numbers
- Bool
- String

All reference type instances must be marshalled by hand
→ field by field!

Implementation details of **`Timer`**

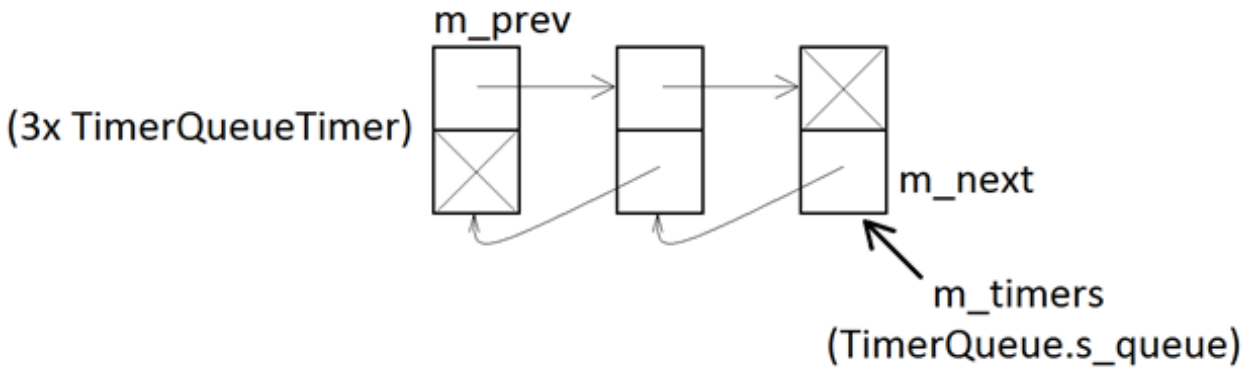
A `Timer` stores its details in a `TimerQueueTimer`

A static `_queue` field of `TimerQueue` points to the list head



How to list all timers?

1. Get the `ClrType` corresponding to `TimerQueue`
2. Reaching the static `s_queue` field description
3. Reading the static `s_queue` field value to get the list head
4. Reading an instance field to get the next `TimerQueueTimer`
5. Decyphering a callback method name and target



How to access a class static field? (1/2)

Access directly to a specific `ClrType`

- Look for the defining module
- Call `ClrModule.GetTypeByName` with the name

```
foreach (ClrModule module in runtime.Modules)
    if (module.AssemblyName.Contains("mscorlib.dll"))
        return module.GetTypeByName("System.Threading.TimerQueue");
```

How to access a class static field? (2/2)

Access a static field via `ClrType.GetStaticFieldByName`

Each AppDomain has a different value for all statics

- List all AppDomain
- Check if the static has a value or not

```
ClrStaticField staticField =
    timerQueueType.GetStaticFieldByName("s_queue");
foreach (ClrAppDomain domain in runtime.AppDomains)
{
    ulong? timerQueue = (ulong?)staticField.GetValue(domain);
    if (!timerQueue.HasValue || timerQueue.Value == 0)
        continue;
```

How to get instance field value?

Get the `ClrInstanceField` from `ClrType`

- Get the type from the instance address

Call `ClrInstanceField.GetValue()` with the instance address

```
var type = heap.GetObjectType(address);
ClrInstanceField field = type.GetFieldByName(fieldName);
return field?.GetValue(address);
```

How to decipher a delegate?

Difference between an instance and a static method

- Look for the value of **`_target`** field

The callback is stored in the **`_methodPtr`** field

- Use `ClrRuntime.GetMethodByAddress` to get a `ClrMethod`

```
var methodPtr = GetFieldValue(heap, timerCallbackRef, "_methodPtr");
ClrMethod method = clr.GetMethodByAddress((ulong)(long)methodPtr);
var thisPtr = GetFieldValue(heap, timerCallbackRef, "_target");
if ((thisPtr != null) && ((ulong)thisPtr) != 0)
{
    ...
```

Lab

.NET DEVELOPER DAYS

Get Timer info

Resources

Criteo blog series and source code

- http://labs.criteo.com/2017/12/clrmd-part-9-deciphering-tasks-thread-pool-items/
- https://github.com/chrisnas/DebuggingExtensions

ClrMD on github for source code and samples

https://github.com/Microsoft/clrmd

DynaMD on github

https://github.com/kevingosse/DynaMD

Please rate this session using

Developer Days Mobile App

login.developerdays.pl

or at

the booth in the Exhibition Hall