Todo

**General**

* Move ‘internal’ code to ‘detail’ folder/namespace.
* Review compiler support.
  + GCC via MinGW is quite unstable, investigate dropping support. Furthermore, this will allow a move back to a VS-based build system… Alternatively, add VS-based build system as a ‘secondary’ system, and retain Boost.Build system to keep code standards conformant and be ready for Clang support.
* Documentation.
  + Full documentation of all components.
  + Threading docs.
  + Exception guarantee docs.
* Unit tests.
  + Extra sanity checks to ensure not only that functions return without exception, but also that the returned data is valid. (e.g. GetName in ImpThunk.)
  + Expand tests to be more thorough and use Boost.Test checks such as BOOST\_CHECK\_NO\_THROW, BOOST\_CHECK\_THROW, BOOST\_CHECK\_EQUAL\_COLLECTION, etc.
  + Extra tests on library usage that should fail to compile (because of static assertions, type traits, etc). Needed to ensure library misuse is not ‘possible’.
* Examples.
  + All components.
  + Cleanup and in-source documentation.
* Improve quality of existing code.
  + Improve exception-safety guarantees. (Rollback support etc)
  + Improve thread-safety guarantees and threading model.
  + Throw custom error codes as part of exceptions. Use a different tag type.
  + Investigate Boost.Exception’s support for multiple exception info objects which share the same tag type, and how to ‘extract’ them at the catch site. Potentially rewrite some exceptions which use multiple ‘ErrorCodeWin’ objects to use unique tags instead.
  + Use more ‘localized’ exception types where possible.
  + Proper localization and internationalization support/framework.
  + Consider moving from UTF-16 internally to UTF-8, and only using UTF-16 at API boundaries. If implemented, all files and other IO should be in UTF-8.
  + Template concept checking and improved error messages.
  + Compile time checks to ensure MSVC, GCC, Boost, etc meet the minimum requirements.
  + Value-type style uniform initialization (e.g. std::set<T> = GetT()).
  + Use virtual function ‘override’ keyword.
  + Assertions where appropriate (for ‘impossible’ cases).
  + Improved error reporting via exceptions.
  + Support move semantics where appropriate.
  + Support swapping where appropriate (and use to simplify operator= if possible).
  + Support extra operator overloads where appropriate (such as < or > on Module to make it closer to the built in HMODULE type).
  + Support perfect forwarding where appropriate.
  + Style cleanup (e.g. LLVM).
  + Const support for iterators (template iterators on ValueT, add cbegin/cend to parent).
  + Fix conversion to bool in classes (e.g. EnsureCleanup) to use an unspecified bool type and prevent implicit conversion to int, and also to remove the reliance on HandleType’s implicit conversion to bool, which we cannot guarantee.
  + Const correctness.
  + Clean up iterators to be more lightweight, and shift most of the processing to the parent object.
  + Clean up APIs returning pairs/tuples/etc to return objects with named fields and/or getters.
  + Investigate DLL build.
  + Review and ‘rewrite’ in-code documentation/comments.
  + Tests for remaining ‘detail’ components such as EnsureCleanup, StringBuffer, etc.
  + Investigate support for optional error reporting via error codes to avoid littering code with try-catch blocks in certain scenarios.
  + Improve API genericity.
    - Instead of taking or returning a vector<T>, instead use a C<T> where ‘C’ is a template parameter representing an arbitrary container.
    - Use ‘ranges’ over direct containers where possible.
* Improved binary generation and distribution.
  + Binaries with update server.
  + Automatic binary versioning using SVN revision.
  + Automatic build bot.
  + Digital signature (for build bot, WER, etc).
* Reduce compile time.
  + Reduce include dependencies.
    - Pointer-to-impl idiom.
  + PCH support using Boost.Build.
  + Decouple components if possible.
* Todo list.
  + Consider porting to Google Code issue tracker.
* Performance improvements in potential bottlenecks (e.g. Iterators, Scanner, PeLib, FindPattern, etc).
* .NET interop.
* Investigate a template header-only approach.

**New Modules**

* Cheat Engine ‘replacement’.
* Helper service to run HadesMem tools as ‘SYSTEM’ for when manipulation certain protected/critical processes (running in separate desktops, sessions, etc.).
  + Ensure service is secure from abuse.
* Debugging.
  + Software breakpoint.
  + Hardware breakpoint (including memory read/write detection).
  + Conditional breakpoints.
  + Single stepping.
  + Stack trace.
* Anti-anti-cheat.
* Thread/process information and enumeration.
* Manual mapper.
  + Windows PE loader reversing.
  + TLS support.
  + Exception handling support. (Safe, rather than catch-all.)
  + No ‘external’ (read: MMHelper) dependencies.
  + Extensive sanity checking on PE file.
  + Manually map dependencies and ‘link’.
* Remote code ‘emulator’.
* Custom GetModuleHandle, GetProcAddress, etc.
* C++ WinAPI wrapper.
* Memory iterators/functors.

**MemoryMgr**

* Improve ‘safety’ of remote function caller via EH to minimize risk of crashing the target.
* Improve genericity of parameter passing in remote function caller.
* Memory reading via expression templates.
* Support floating point parameters and return values in remote function caller.
* Support 64-bit parameters under x86 in remote function caller.
* Support non-MSVC compilers in remote function caller (e.g. in calling convention specification).

**Injector**

* .NET injection.
  + Without DLL dependency if possible.
* Cross-section injection.
* IAT injection.
* Get address of Kernel32!LoadLibrary ‘manually’ rather than using a local GetProcAddress and pointer arithmetic.
  + Whilst this works in all normal cases, it doesn’t work when the target has shims enabled which hook LoadLibrary.

**Patcher**

* VEH hooking (both INT3 and DR).
* Transactional hooking.
* Improved relative instruction rebuilding (including conditionals). x64 has far more IP relative instructions than x86.
* Freeze target when hooking (except calling thread if applicable – e.g. in injected code).
* When hooking on x64 try to find a free memory block for the trampoline that is within RIP-relative range of the detour. Only if one cannot be acquired should we fall back to a system-provided address and an absolute jump.
* Uncopyable, so make moveable.
* VMT hooking.
* IAT/EAT hooking.
* Explicitly support hook chains (and write test).
* Use relative jumps where possible (detect delta at runtime).
* Detect cases where hooking may overflow past the end of a function, and fail. (Provide policy or flag to allow overriding this behaviour.) Examples may be instructions such as ‘int 3’, ‘ret’, ‘jmp’, etc.

**FindPattern**

* Pattern generator.
* ‘Multi-pass’ support (e.g. search for pattern, apply for manipulators, use as starting point for second search).
* Arbitrary region support.

**PeLib**

* Support for working on x86 PE files from x64 and vice versa.
* Investigate use of virtual functions for file vs memory access (RvaToVa).
  + Alternatively, investigate use of templates, which may ‘merge’ better with x86/x64 cross compatibility.
  + Note: May cause problems when copying ‘PeFile’ type.
* Extra sanity checking in all components.
  + E.g. Check NumberOfRvaAndSizes in NtHeaders before attempting to retrieve a data dir.
* Cache base pointers etc rather than retrieving it manually in every getter/setter. Slightly less ‘robust’, but due to the typically ‘read-only’ nature of the data this is the expected behaviour in all known cases anyway.
* Support more of the PE file format.
  + Overlay data.
  + Resource directory.
  + Exception directory.
  + Relocation directory.
  + Security directory.
  + Debug directory.
  + Load config directory.
  + Delay import directory.
  + Bound import directory.
  + IAT (as opposed to Import) directory.
  + CLR runtime directory support.
* Full support for writing back to PE file, including automatically performing adjustments where required to fit in new data or remove unnecessary space.
* Improve export forwarding code to detect and handle forward-by-ordinal explicitly rather than forcing the user to detect it and do string manipulation and conversion.
* Helper functions such as FindExport, FindImport, HasDataDir, GetArchitecture, IsDotNet, GetPDB, etc.

**Disassembler**

* Decode calls/jumps to function names if possible.
* NOP/UnNOP support.
* ASM searching API with ‘wildcards’. (MetaASM?)
* String based assembler with x64 support.
* Disassemble function API.

**Scanner**

* Rewrite to be more reliable and robust.
* Refactor to reduce code duplication.
* Use a file view with a small memory cache rather than consuming large amounts of RAM.
* Multi-threaded scanning options.
* Wildcard support for vector/string scanning.
* Regex support for string scanning.
* Memory protection filters (read, write, exec).
* Memory type filters (private, mapped, image).
* Support pausing target while scanning.
* Support injected scanning.
* Configurable scan buffer size.
* Pointer scanner.
* Unknown value scan.
* Progressive scan filtering based on either value or criteria.
* Scan history and undo.
* Support case insensitive string scanning.
* Binary scanning.
* Custom scanning via user-supplied predicate.
* Improved floating point support (configurable or ‘smart’ epsilon).
* Group search support.