



DR

---

ClamAV Bytecode Compiler  
*User Manual*

# Contents

---

<b>1</b>	<b>Installation</b>	<b>1</b>
1.1	Requirements	1
1.2	Obtaining the ClamAV Bytecode Compiler	2
1.3	Building	2
1.3.1	Disk space	2
1.3.2	Create build directory	2
1.4	Testing	3
1.5	Installing	3
1.5.1	Structure of installed files	3
<b>2</b>	<b>Tutorial</b>	<b>5</b>
2.1	Short introduction to the bytecode language	5
2.1.1	Types, variables and constants	5
2.1.2	Arrays and pointers	5
2.1.3	Arithmetics	5
2.1.4	Functions	5
2.1.5	Control flow	5
2.1.6	Common functions	5
2.2	Writing logical signatures	5
2.2.1	Structure of a bytecode for algorithmic detection	6
2.2.2	Virusnames	6
2.2.3	Patterns	7
2.2.4	Single subsignature	8
2.2.5	Multiple subsignatures	8
2.2.6	W32.Polipos.A detector rewritten as bytecode	10
2.2.7	Virut detector in bytecode	10
2.3	Writing unpackers	10
2.3.1	Structure of a bytecode for unpacking (and other hooks)	10
2.3.2	Detecting clam.exe via bytecode	12
2.3.3	Detecting clam.exe via bytecode (disasm)	12
2.3.4	A simple unpacker	12

2.3.5	Matching PDF javascript . . . . .	12
2.3.6	YC unpacker rewritten as bytecode . . . . .	12
<b>3</b>	<b>Usage</b>	<b>13</b>
3.1	Invoking the compiler . . . . .	13
3.1.1	Compiling C++ files . . . . .	14
3.2	Running compiled bytecode . . . . .	14
3.2.1	ClamBC . . . . .	14
3.2.2	clamscan, clamd . . . . .	14
3.3	Debugging bytecode . . . . .	15
3.3.1	“printf” style debugging . . . . .	15
3.3.2	Single-stepping . . . . .	15
<b>4</b>	<b>ClamAV bytecode language</b>	<b>17</b>
4.1	Differences from C99 and GNU C . . . . .	17
4.2	Limitations . . . . .	19
4.3	Logical signatures . . . . .	20
4.4	Headers and runtime environment . . . . .	22
<b>5</b>	<b>Bytecode security &amp; portability</b>	<b>23</b>
<b>6</b>	<b>Reporting bugs</b>	<b>25</b>
<b>7</b>	<b>Bytecode API</b>	<b>27</b>
7.1	Structure types . . . . .	27
7.1.1	cli_exe_info Struct Reference . . . . .	27
7.1.1.1	Detailed Description . . . . .	27
7.1.1.2	Member Function Documentation . . . . .	27
7.1.1.3	Field Documentation . . . . .	27
7.1.2	cli_exe_section Struct Reference . . . . .	28
7.1.2.1	Detailed Description . . . . .	28
7.1.2.2	Field Documentation . . . . .	28
7.1.3	cli_pe_hook_data Struct Reference . . . . .	29
7.1.3.1	Detailed Description . . . . .	29
7.1.3.2	Field Documentation . . . . .	29
7.1.4	DIS_arg Struct Reference . . . . .	30
7.1.4.1	Detailed Description . . . . .	30
7.1.4.2	Field Documentation . . . . .	31
7.1.5	DIS_fixed Struct Reference . . . . .	31
7.1.5.1	Detailed Description . . . . .	31
7.1.5.2	Field Documentation . . . . .	31

7.1.6	DIS_mem_arg Struct Reference . . . . .	32
7.1.6.1	Detailed Description . . . . .	32
7.1.6.2	Field Documentation . . . . .	32
7.1.7	DISASM_RESULT Struct Reference . . . . .	32
7.1.7.1	Detailed Description . . . . .	32
7.1.8	pe_image_data_dir Struct Reference . . . . .	32
7.1.8.1	Detailed Description . . . . .	32
7.1.9	pe_image_file_hdr Struct Reference . . . . .	33
7.1.9.1	Detailed Description . . . . .	33
7.1.9.2	Field Documentation . . . . .	33
7.1.10	pe_image_optional_hdr32 Struct Reference . . . . .	34
7.1.10.1	Detailed Description . . . . .	34
7.1.10.2	Field Documentation . . . . .	34
7.1.11	pe_image_optional_hdr64 Struct Reference . . . . .	35
7.1.11.1	Detailed Description . . . . .	36
7.1.11.2	Field Documentation . . . . .	36
7.1.12	pe_image_section_hdr Struct Reference . . . . .	37
7.1.12.1	Detailed Description . . . . .	37
7.1.12.2	Field Documentation . . . . .	37
7.2	Low level API . . . . .	38
7.2.1	bytecode_api.h File Reference . . . . .	38
7.2.1.1	Detailed Description . . . . .	40
7.2.1.2	Enumeration Type Documentation . . . . .	40
7.2.1.3	Function Documentation . . . . .	40
7.2.1.4	Variable Documentation . . . . .	51
7.2.2	bytecode_disasm.h File Reference . . . . .	51
7.2.2.1	Detailed Description . . . . .	54
7.2.2.2	Enumeration Type Documentation . . . . .	54
7.2.3	bytecode_execs.h File Reference . . . . .	64
7.2.3.1	Detailed Description . . . . .	64
7.2.4	bytecode_pe.h File Reference . . . . .	64
7.2.4.1	Detailed Description . . . . .	64
7.3	High level API . . . . .	64
7.3.1	bytecode_local.h File Reference . . . . .	64
7.3.1.1	Detailed Description . . . . .	67
7.3.1.2	Define Documentation . . . . .	67
7.3.1.3	Function Documentation . . . . .	68
<b>8</b>	<b>Copyright and License</b>	<b>79</b>
8.1	The ClamAV Bytecode Compiler . . . . .	79
8.2	Bytecode . . . . .	81

**A Predefined macros****83**

ClamAV Bytecode Compiler - Internals Manual,

© 2009 Sourcefire, Inc.

Authors: Török Edvin

This document is distributed under the terms of the GNU General Public License v2.

Clam AntiVirus is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; version 2 of the License.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA.

ClamAV and Clam AntiVirus are trademarks of Sourcefire, Inc.

# CHAPTER 1

## Installation

---

### 1.1. Requirements

---

The ClamAV Bytecode Compiler uses the LLVM compiler framework, thus requires an Operating System where building LLVM is supported:

- FreeBSD/x86
- Linux/{x86,x86\_64,ppc}
- Mac OS X/{x86,ppc}
- Solaris/sparcv9
- Windows/x86 using mingw32 or Visual Studio

The following packages are required to compile the ClamAV Bytecode Compiler:

- GCC C and C++ compilers (minimum 4.1.3, recommended: 4.3.4 or newer)<sup>1</sup>.
- Perl (version 5.6.0+)
- GNU make (version 3.79+, recommended 3.81)

The following packages are optional, but highly recommended:

- Python (version 2.5.4+?) - for running the tests

---

<sup>1</sup>Note that several versions of GCC have bugs when compiling LLVM, see <http://llvm.org/docs/GettingStarted.html#brokengcc> for a full list. Also LLVM requires support for atomic builtins for multithreaded mode, which gcc 3.4.x doesn't have

## 1.2. Obtaining the ClamAV Bytecode Compiler

---

You can obtain the source code in one of the following ways <sup>1</sup>

- Check out the source code using git native protocol:

```
git clone git://git.clamav.net/git/clamav-bytecode-compiler
```

- Check out the source code using HTTP:

```
git clone http://git.clamav.net/git/clamav-bytecode-compiler.git
```

You can keep the source code updated using:

```
git pull
```

## 1.3. Building

---

### 1.3.1. Disk space

---

A minimalistic release build requires 100M of disk space.

Testing the compiler requires a full build, 320M of disk space. A debug build requires significantly more disk space (1.4G for a minimalistic debug build).

Note that this is only needed during the build process, once installed only 12M is needed.

### 1.3.2. Create build directory

---

Building requires a separate object directory, building in the source directory is not supported. Create a build directory:

```
$ cd clamav-bytecode-compiler && mkdir obj
```

Run configure (you can use any prefix you want, this example uses /usr/local/clamav):

```
$ cd obj && ../llvm/configure --enable-optimized \
--enable-targets=host-only --disable-bindings \
--prefix=/usr/local/clamav
```

Run the build under ulimit <sup>2</sup>:

```
$ (ulimit -t 3600 -v 512000 && make clambc-only -j4)
```

---

<sup>1</sup>For now use the internal clamtools repository:

```
git clone username@git.clam.sourcify.com:/var/lib/git/clamtools.git
```

<sup>2</sup>compiling some files can be very memory intensive, especially with older compilers

## 1.4. Testing

---

```
$ (ulimit -t 3600 v 512000 && make -j4)
$ make check-all
```

If make check reports errors, check that your compiler is NOT on this list: <http://llvm.org/docs/GettingStarted.html#brokengcc>.

If it is, then your compiler is buggy, and you need to do one of the following: upgrade your compiler to a non-buggy version, upgrade the OS to one that has a non-buggy compiler, compile with `export OPTIMIZE_OPTION=-O2`, or `export OPTIMIZE_OPTION=-O1`, or `export OPTIMIZE_OPTION=-O1`.

If not you probably found a bug, report it at <http://bugs.clamav.net>

## 1.5. Installing

---

Install it:

```
$ make install-clambc -j8
```

### 1.5.1. Structure of installed files

---

1. The ClamAV Bytecode compiler driver: `$PREFIX/bin/clambc-compiler`
2. ClamAV bytecode header files:

```
$PREFIX/lib/clang/1.1/include:
bcfeatures.h
bytecode_{api_decl.c,api,disasm,execs,features}.h
bytecode.h
bytecode_{local,pe,types}.h
```

3. clang compiler (with ClamAV bytecode backend) compiler include files:

```
$PREFIX/lib/clang/1.1/include:
emmintrin.h
float.h
iso646.h
limits.h
{,p,t,x}mmmintrin.h
mm_malloc.h
std{arg,bool,def,int}.h
tgmath.h
```



#### 4. User manual

`$PREFIX/docs/clamav/clamav-user.pdf`

DRAFT

## CHAPTER 2

# Tutorial

---

### 2.1. Short introduction to the bytecode language

---

#### 2.1.1. Types, variables and constants

---

#### 2.1.2. Arrays and pointers

---

#### 2.1.3. Arithmetics

---

#### 2.1.4. Functions

---

#### 2.1.5. Control flow

---

#### 2.1.6. Common functions

---

### 2.2. Writing logical signature bytecodes <sup>1</sup>

---

Logical signatures can be used as triggers for executing bytecode. However, instead of describing a logical signature as a `.ldb` pattern, you use (simple) C code which is later translated to a `.ldb`-style logical signature by the ClamAV Bytecode Compiler.

A bytecode triggered by a logical signature is much more powerful than a logical signature itself: you can write complex algorithmic detections, and use the logical signature as a *filter* (to speed up matching). Thus another name for “logical signature bytecodes” is “algorithmic detection bytecodes”. The detection you write in bytecode has read-only access to the file being scanned and its metadata (PE sections, EP, etc.).

---

<sup>1</sup>See Section [4.3 on page 20](#) for more details about logical signatures in bytecode.

### 2.2.1. Structure of a bytecode for algorithmic detection

Algorithmic detection bytecodes are triggered when a logical signature matches. They can execute an algorithm that determines whether the file is infected and with which virus.

A bytecode can be either algorithmic or an unpacker (or other hook), but not both.

It consists of:

- Definition of virusnames used in the bytecode
- Pattern definitions (for logical subexpressions)
- The logical signature as C function: `bool logical_trigger(void)`
- The `int entrypoint(void)` function which gets executed when the logical signature matches
- (Optional) Other functions and global constants used in `entrypoint`

The syntax for defining logical signatures, and an example is described in Section [2.2.4 on page 8](#).

The function `entrypoint` must report the detected virus by calling `foundVirus` and returning 0. It is recommended that you always return 0, otherwise a warning is shown and the file is considered clean. If `foundVirus` is not called, then ClamAV also assumes the file is clean.

### 2.2.2. Virusnames

Each logical signature bytecode must have a virusname prefix, and one or more virusnames. The virusname prefix is used by the SI to ensure unique virusnames (a unique number is appended for duplicate prefixes).

---

#### Program 1 Declaring virusnames

---

```

1 /* Prefix, used for duplicate detection and fixing */
  VIRUSNAME_PREFIX("Trojan.Foo")
3 /* You are only allowed to set these virusnames as found */
  VIRUSNAMES("A", "B")
5 /* File type */
  TARGET(2)

```

---

In Program 1 3 predefined macros are used:

- `VIRUSNAME_PREFIX` which must have exactly one string argument

- VIRUSNAMES which must have one or more string arguments
- TARGET which must have exactly one integer argument

In this example, the bytecode could generate one of these virus-names: Trojan.Foo.A, or Trojan.Foo.B, by calling `foundVirus("A")` or `foundVirus("B")` respectively (notice that the prefix is not part of these calls).

### 2.2.3. Patterns

Logical signatures use `.ndb` style patterns, an example on how to define these is shown in Program 2.

---

#### Program 2 Declaring patterns

---

```

SIGNATURES_DECL_BEGIN
2 DECLARE_SIGNATURE( magic )
  DECLARE_SIGNATURE( check )
4 DECLARE_SIGNATURE( zero )
SIGNATURES_DECL_END

6
SIGNATURES_DEF_BEGIN
8 DEFINE_SIGNATURE( magic , "EP+0: aabb" )
  DEFINE_SIGNATURE( check , "f00d" )
10 DEFINE_SIGNATURE( zero , "ffff" )
SIGNATURES_END

```

---

Each pattern has a name (like a variable), and a string that is the hex pattern itself. The declarations are delimited by the macros `SIGNATURES_DECL_BEGIN`, and `SIGNATURES_DECL_END`. The definitions are delimited by the macros `SIGNATURES_DEF_BEGIN`, and `SIGNATURES_END`. Declarations must always come before definitions, and you can have only one declaration and declaration section! (think of declaration like variable declarations, and definitions as variable assignments, since that what they are under the hood). The order in which you declare the signatures is the order in which they appear in the generated logical signature.

You can use any name for the patterns that is a valid record field name in C, and doesn't conflict with anything else declared.

After using the above macros, the global variable `Signatures` will have two new fields: `magic`, and `zero`. These can be used as arguments to the functions `count_match()`, and `matches()` anywhere in the program as shown in Program 3 on the following page:

- `matches(Signatures.match)` will return true when the match signature matches (at least once)

- `count_match(Signatures.zero)` will return the number of times the zero signature matched
- `count_match(Signatures.check)` will return the number of times the check signature matched

The condition in the `if` can be interpreted as: if the `match` signature has matched at least once, and the number of times the `zero` signature matched is higher than the number of times the `check` signature matched, then we have found a virus A, otherwise the file is clean.

---

### Program 3 Using patterns

---

```

1 int entrypoint(void)
  {
3   if ( matches( Signatures.match ) && count_match( Signatures.zero )
        > count_match( Signatures.check ) )
        foundVirus( "A" );
5   return 0;
  }

```

---

#### 2.2.4. Single subsignature

---

The simplest logical signature is like a `.ndb` signature: a virus name, signature target, 0 as logical expression <sup>1</sup>, and a `ndb`-style pattern.

The code for this is shown in Program 4 on the next page

The logical signature (created by the compiler) looks like this:

```
Trojan.Foo.{A};Target:2;0;aabb
```

Of course you should use a `.ldb` signature in this case when all the processing in `entrypoint` is only setting a virusname and returning. However, you can do more complex checks in `entrypoint`, once the bytecode was triggered by the `logical_trigger`

In the example in Program 4 on the facing page the pattern was used without an anchor; such a pattern matches at any offset. You can use offsets though, the same way as in `.ndb` signatures, see Program 5 on page 11 for an example.

#### 2.2.5. Multiple subsignatures

---

An example for this is shown in Program 5 on page 11. Here you see the following new features used: <sup>2</sup>

---

<sup>1</sup>meaning that subexpression 0 must match

<sup>2</sup>In case of a duplicate virusname the prefix is appended a unique number by the SI

---

**Program 4** Single subsignature example
 

---

```

/* Declare the prefix of the virusname */
2 VIRUSNAME_PREFIX("Trojan.Foo")
/* Declare the suffix of the virusname */
4 VIRUSNAMES("A")
/* Declare the signature target type (1 = PE) */
6 TARGET(1)

8 /* Declare the name of all subsignatures used */
SIGNATURES_DECL_BEGIN
10 DECLARE_SIGNATURE(magic)
SIGNATURES_DECL_END
12
/* Define the pattern for each subsignature */
14 SIGNATURES_DEF_BEGIN
DEFINE_SIGNATURE(magic, "aabb")
16 SIGNATURES_END

18 /* All bytecode triggered by logical signatures must have this
function */
20 bool logical_trigger(void)
{
22 /* return true if the magic subsignature matched,
* its pattern is defined above to "aabb" */
24 return count_match(Signatures.magic) != 2;
}
26
/* This is the bytecode function that is actually executed when
the logical
28 * signature matched */
int entrypoint(void)
30 {
/* call this function to set the suffix of the virus found */
32 foundVirus("A");
/* success, return 0 */
34 return 0;
}

```

---

- Multiple virusnames returned from a single bytecode (with common prefix)
- Multiple subsignatures, each with a name of your choice
- A pattern with an anchor (EP+0:aabb)
- More subsignatures defined than used in the logical expression

The logical signature looks like this:

```
Trojan.Foo.{A,B};Target:2;(((0|1|2)=42,2)|(3=10));EP+0:aabb;ffff;aaccee;f00d;dead
```

Notice how the subsignature that is not used in the logical expression (number 4, dead) is used in `entrypoint` to decide the virus name. This works because ClamAV does collect the match counts for all subsignatures (regardless if they are used or not in a signature). The `count_match(Signatures.check2)` call is thus a simple memory read of the count already determined by ClamAV.

Also notice that comments can be used freely: they are ignored by the compiler. You can use either C-style multiline comments (start comment with `/*`, end with `*/`), or C++-style single-line comments (start comment with `//`, automatically ended by newline).

### 2.2.6. W32.Polipos.A detector rewritten as bytecode

### 2.2.7. Virut detector in bytecode

## 2.3. Writing unpackers

### 2.3.1. Structure of a bytecode for unpacking (and other hooks)

When writing an unpacker, the bytecode should consist of:

- Define which hook you use (for example `PE_UNPACKER_DECLARE` for a PE hook)
- An `int entrypoint(void)` function that reads the current file and unpacks it to a new file
- Return 0 from `entrypoint` if you want the unpacked file to be scanned
- (Optional) Other functions and global constants used by `entrypoint`

**Program 5** Multiple subsignatures

```

1  /* You are only allowed to set these virusnames as found */
   VIRUSNAME_PREFIX("Test")
3  VIRUSNAMES("A", "B")
   TARGET(1)
5
   SIGNATURES_DECL_BEGIN
7  DECLARE_SIGNATURE(magic)
   DECLARE_SIGNATURE(zero)
9  DECLARE_SIGNATURE(check)
   DECLARE_SIGNATURE(fivetoten)
11 DECLARE_SIGNATURE(check2)
   SIGNATURES_DECL_END
13
   SIGNATURES_DEF_BEGIN
15 DEFINE_SIGNATURE(magic, "EP+0:aabb")
   DEFINE_SIGNATURE(zero, "ffff")
17 DEFINE_SIGNATURE(fivetoten, "aaccee")
   DEFINE_SIGNATURE(check, "f00d")
19 DEFINE_SIGNATURE(check2, "dead")
   SIGNATURES_END
21
   bool logical_trigger(void)
23 {
       unsigned sum_matches = count_match(Signatures.magic)+
25         count_match(Signatures.zero) +
           count_match(Signatures.fivetoten);
       unsigned unique_matches = matches(Signatures.magic)+
27         matches(Signatures.zero)+
           matches(Signatures.fivetoten);
       if (sum_matches == 42 && unique_matches == 2) {
29         // The above 3 signatures have matched a total of 42
           times, and at least
           // 2 of them have matched
31         return true;
       }
33     // If the check signature matches 10 times we still have a
       match
       if (count_match(Signatures.check) == 10)
35         return true;
       // No match
37     return false;
   }
39
   int entrypoint(void)
41 {
       unsigned count = count_match(Signatures.check2);
43       if (count >= 2)
           // foundVirus(count == 2 ? "A" : "B");
45       if (count == 2)
           foundVirus("A");           11
47       else
           foundVirus("B");
49       return 0;
   }

```



### **2.3.2. Detecting clam.exe via bytecode**

---

Example provided by aCaB:

### **2.3.3. Detecting clam.exe via bytecode (disasm)**

---

Example provided by aCaB:

### **2.3.4. A simple unpacker**

---

### **2.3.5. Matching PDF javascript**

---

### **2.3.6. YC unpacker rewritten as bytecode**

---

## CHAPTER 3

# Usage

---

### 3.1. Invoking the compiler

---

Compiling is similar to gcc <sup>1</sup>:

```
$ /usr/local/clamav/bin/clamc-compiler foo.c -o foo.cbc -O2
```

This will compile the file `foo.c` into a file called `foo.cbc`, that can be loaded by ClamAV, and packed inside a `.cvd` file.

The compiler by default has all warnings turned on.

Supported optimization levels: `-O0`, `-O1`, `-O2`, `-O3`. <sup>2</sup> It is recommended that you always compile with at least `-O1`.

Warning options: `-Werror` (transforms all warnings into errors).

Preprocessor flags:

**-I <directory>** Searches in the given directory when it encounters a `#include "headerfile"` directive in the source code, in addition to the system defined header search directories.

**-D <MACRONAME>=<VALUE>** Predefine given `<MACRONAME>` to be equal to `<VALUE>`.

**-U <MACRONAME>** Undefine a predefined macro

The compiler also supports some other commandline options (see `clamc-compiler --help` for a full list), however some of them have no effect when using the ClamAV bytecode backend (such as the X86 backend options). You shouldn't need to use any flags not documented above.

---

<sup>1</sup>Note that the ClamAV bytecode compiler will refuse to compile code it considers insecure

<sup>2</sup>Currently `-O0` doesn't work

### 3.1.1. Compiling C++ files

Filenames with a `.cpp` extension are compiled as C++ files, however `clang++` is not yet ready for production use, so this is EXPERIMENTAL currently. For now write bytecodes in C.

## 3.2. Running compiled bytecode

After compiling a C source file to bytecode, you can load it in ClamAV:

### 3.2.1. ClamBC

ClamBC is a tool you can use to test whether the bytecode loads, compiles, and can execute its entrypoint successfully. Usage:

```
clambc <file> [function] [param1 ...]
```

For example loading a simple bytecode with 2 functions is done like this:

```
$ clambc foo.cbc
LibClamAV debug: searching for unrar, user-searchpath: /usr/local/lib
LibClamAV debug: unrar support loaded from libclamunrar_iface.so.6.0.4 libclan
LibClamAV debug: bytecode: Parsed 0 APICalls, maxapi 0
LibClamAV debug: Parsed 1 BBs, 2 instructions
LibClamAV debug: Parsed 1 BBs, 2 instructions
LibClamAV debug: Parsed 2 functions
Bytecode loaded
Running bytecode function :0
Bytecode run finished
Bytecode returned: 0x8
Exiting
```

### 3.2.2. clamscan, clamd

You can tell clamscan to load the bytecode as a database directly:

```
$ clamscan -dfoo.cbc
```

Or you can instruct it to load all databases from a directory, then clamscan will load all supported formats, including files with bytecode, which have the `.cbc` extension.

```
$ clamscan -ddirectory
```

You can also put the bytecode files into the default database directory of ClamAV (usually `/usr/local/share/clamav`) to have it loaded automatically from there. Of course, the bytecode can be stored inside CVD files, too.

## 3.3. Debugging bytecode

---

### 3.3.1. “printf” style debugging

---

You can use `debug_print_str` and `debug_print_int` API calls to print debug messages during the execution of the bytecode.

### 3.3.2. Single-stepping

---

If you have GDB 7.0 (or newer) you can single-step <sup>1</sup> <sup>2</sup> during the execution of the bytecode.

- Run `clambc` or `clamscan` under `gdb`:

```
$ ./libtool --mode=execute gdb clamscan/clamscan
...
(gdb) b cli_vm_execute_jit
Are you sure ....? y
(gdb) run -dfoo.cbc
...
Breakpoint ....

(gdb) step
(gdb) next
```

You can single-step through the execution of the bytecode, however you can't (yet) print values of individual variables, you'll need to add debug statements in the bytecode to print interesting values.

---

<sup>1</sup>not yet implemented in `libclamav`

<sup>2</sup>assuming you have JIT support

DRAFT

## CHAPTER 4

# ClamAV bytecode language

---

The bytecode that ClamAV loads is a simplified form of the LLVM Intermediate Representation, and as such it is language-independent.

However currently the only supported language from which such bytecode can be generated is a simplified form of C <sup>1</sup>

The language supported by the ClamAV bytecode compiler is a restricted set of C99 with some GNU extensions.

## 4.1. Differences from C99 and GNU C

---

These restrictions are enforced at compile time:

- No standard include files. <sup>2</sup>
- The ClamAV API header files are preincluded.
- No external function calls, except to the ClamAV API <sup>3</sup>
- No inline assembly <sup>4</sup>
- Globals can only be readonly constants <sup>5</sup>
- `inline` is C99 inline (equivalent to GNU C89 `extern inline`), thus it cannot be used outside of the definition of the ClamAV API, you should use `static inline`

---

<sup>1</sup>In the future more languages could be supported, see the Internals Manual on language frontends

<sup>2</sup>For portability reasons: preprocessed C code is not portable

<sup>3</sup>For safety reasons we can't allow the bytecode to call arbitrary system functions

<sup>4</sup>This is both for safety and portability reasons

<sup>5</sup>For thread safety reasons

- `sizeof(int) == 4` always
- `sizeof(long) == sizeof(long long) == 8` always
- `ptrdiff_t = int, intptr_t = int, intmax_t = long, uintmax_t = unsigned long`<sup>1</sup>
- No pointer to integer casts and integer to pointer casts (pointer arithmetic is allowed though)
- No `__thread` support
- Size of memory region associated with each pointer must be known in each function, thus if you pass a pointer to a function, you must also pass its allocated size as a parameter.
- Endianness must be handled via the `__is_bigendian()` API function call, or via the `cli_{read,write}int{16,32}` wrappers, and not by casting pointers
- Predefines `__CLAMBC__`
- All integer types have fixed width
- `main` or `entrypoint` must have the following prototype: `int main(void)`, the prototype `int main(int argc, char *argv[])` is not accepted

They are meant to ensure the following:

- Thread safe execution of multiple different bytecodes, and multiple instances of the same bytecode
- Portability to multiple CPU architectures and OSes: the bytecode must execute on both the libclamav/LLVM JIT where that is supported (x86, x86\_64, ppc, arm?), and on the libclamav interpreter where that is not supported.
- No external runtime dependency: libclamav should have everything needed to run the bytecode, thus no external calls are allowed, not even to libc!
- Same behaviour on all platforms: fixed size integers.

These restrictions are checked at runtime (checks are inserted at compile time):

---

<sup>1</sup>Note that a pointer's `sizeof` is runtime-platform dependent, although at compile time `sizeof(void*) == 4`, at runtime it can be something else. Thus you should avoid using `sizeof(pointer)`

- Accessing an out-of-bounds pointer will result in a call to `abort()`
- Calling `abort()` interrupts the execution of the bytecode in a thread safe manner, and doesn't halt ClamAV <sup>1</sup>.

The ClamAV API header has further restriction, see the Internals manual.

Although the bytecode undergoes a series of automated tests (see Publishing chapter in Internals manual), the above restrictions don't guarantee that the resulting bytecode will execute correctly! You must still test the code yourself, these restrictions only avoid the most common errors. Although the compiler and verifier aims to accept only code that won't crash ClamAV, no code is 100% perfect, and a bug in the verifier could allow unsafe code be executed by ClamAV.

## 4.2. Limitations

---

The bytecode format has the following limitations:

- At most 64k bytecode kinds (hooks)
- At most 64k types (including pointers, and all nested types)
- At most 16 parameters to functions, no vararg functions
- At most 64-bit integers
- No vector types or vector operations
- No opaque types
- No floating point
- Global variable initializer must be compile-time computable
- At most 32k global variables (and at most 32k API globals)
- Pointer indexing at most 15 levels deep (can be worked around if needed by using temporaries)
- No struct return or byval parameters
- At most 32k instructions in a single function
- No Variable Length Arrays

---

<sup>1</sup>in fact it calls a ClamAV API function, and not the libc abort function.



## 4.3. Logical signatures

---

Logical signatures can be used as triggers for executing a bytecode. Instead of describing a logical signatures as a `.ldb` pattern, you use C code which is then translated to a `.ldb`-style logical signature.

Logical signatures in ClamAV support the following operations:

- Sum the count of logical subsignatures that matched inside a subexpression
- Sum the number of different subsignatures that matched inside a subexpression
- Compare the above counts using the `>`, `=`, `<` relation operators
- Perform logical `&&`, `||` operations on above boolean values
- Nest subexpressions
- Maximum 64 subexpressions

Out of the above operations the ClamAV Bytecode Compiler doesn't support computing sums of nested subexpressions, (it does support nesting though).

The C code that can be converted into a logical signature must obey these restrictions:

- a function named `logical_trigger` with the following prototype:  

```
bool logical_trigger(void)
```
- no function calls, except for `count_match` and `matches`
- no global variable access (except as done by the above 2 functions internally)
- return true when signature should trigger, false otherwise
- use only integer compare instructions, branches, integer *add*, logical *and*, logical *or*, logical *xor*, zero extension, store/load from local variables
- the final boolean expression must be convertible to disjunctive normal form without negation
- the final logical expression must not have more than 64 subexpressions
- it can have early returns (all true returns are unified using `||`)

- you can freely use comments, they are ignored
- the final boolean expression cannot be a `true` or `false` constant

The compiler does the following transformations (not necessarily in this order):

- convert shortcircuit boolean operations into non-shortcircuit ones (since all operands are boolean expressions or local variables, it is safe to execute these unconditionally)
- propagate constants
- simplify control flow graph
- (sparse) conditional constant propagation
- dead store elimination
- dead code elimination
- instruction combining (arithmetic simplifications)
- jump threading

If after this transformation the program meets the requirements outlined above, then it is converted to a logical signature. The resulting logical signature is simplified using basic properties of boolean operations, such as associativity, distributivity, De Morgan's law.

The final logical signature is not unique (there might be another logical signature with identical behavior), however the boolean part is in a canonical form: it is in disjunctive normal form, with operands sorted in ascending order.

For best results the C code should consist of:

- local variables declaring the sums you want to use
- a series of `if` branches that `return true`, where the `if`'s condition is a single comparison or a logical *and* of comparisons
- a final `return false`

You can use `||` in the `if` condition too, but be careful that after expanding to disjunctive normal form, the number of subexpressions doesn't exceed 64.

Note that you do not have to use all the subsignatures you declared in `logical_trigger`, you can do more complicated checks (that wouldn't obey the above restrictions) in the bytecode itself at runtime. The `logical_trigger` function is fully compiled into a logical signature, it won't be a runtime executed function (hence the restrictions).

## 4.4. Headers and runtime environment

---

When compiling a bytecode program, `bytecode.h` is automatically included, so you don't need to explicitly include it. These headers (and the compiler itself) predefine certain macros, see [Appendix A on page 83](#) for a full list. In addition the following types are defined:

```
typedef unsigned char uint8_t;  
2 typedef char int8_t;  
typedef unsigned short uint16_t;  
4 typedef short int16_t;  
typedef unsigned int uint32_t;  
6 typedef int int32_t;  
typedef unsigned long uint64_t;  
8 typedef long int64_t;  
typedef unsigned int size_t;  
10 typedef int off_t;  
typedef struct signature { unsigned id } __Signature;
```

As described in [Section 4.1 on page 17](#) the width of integer types are fixed, the above typedefs show that.

A bytecode's entrypoint is the function `entrypoint` and it's required by ClamAV to load the bytecode.

Bytecode that is triggered by a logical signature must have a list of virusnames and patterns defined. Bytecodes triggered via hooks can optionally have them, but for example a PE unpacker doesn't need virus names as it only processes the data.

## CHAPTER 5

# Bytecode security & portability

---

DRAFT

DRAFT

## CHAPTER 6

# Reporting bugs

---

DRAFT

DRAFT

## CHAPTER 7

# Bytecode API

## 7.1. Structure types

### 7.1.1. cli\_exe\_info Struct Reference

## Public Member Functions

- struct cli\_exe\_section \*section EBOUNDS (nsections)

## Data Fields

- uint32\_t offset
- uint32\_t ep
- uint16\_t nsections
- struct cli\_hashset \* vinfo

#### 7.1.1.1. Detailed Description

## Executable file information

### 7.1.1.2. Member Function Documentation

#### 7.1.1.2.1. struct cli\_exe\_section\* section EBOUNDS (nsections) [read]

Information about all the sections of this file. This array has `nsection` elements

### 7.1.1.3. Field Documentation

#### 7.1.1.3.1. uint32\_t ep

## Entrypoint of executable



**7.1.1.3.2. uint16\_t nsections** Number of sections

**7.1.1.3.3. uint32\_t offset** Offset where this executable start in file (nonzero if embedded)

**7.1.1.3.4. struct cli\_hashset\* vinfo** Hashset for versioninfo matching

## 7.1.2. cli\_exe\_section Struct Reference

---

### Data Fields

- uint32\_t [rva](#)
- uint32\_t [vsz](#)
- uint32\_t [raw](#)
- uint32\_t [rsz](#)
- uint32\_t [chr](#)
- uint32\_t [urva](#)
- uint32\_t [uvsz](#)
- uint32\_t [uraw](#)
- uint32\_t [ursz](#)

### 7.1.2.1. Detailed Description

Section of executable file

### 7.1.2.2. Field Documentation

**7.1.2.2.1. uint32\_t chr** Section characteristics

**7.1.2.2.2. uint32\_t raw** Raw offset (in file)

**7.1.2.2.3. uint32\_t rsz** Raw size (in file)

**7.1.2.2.4. uint32\_t rva** Relative VirtualAddress

**7.1.2.2.5. uint32\_t uraw** PE - unaligned PointerToRawData

**7.1.2.2.6. uint32\_t ursz** PE - unaligned SizeOfRawData

**7.1.2.2.7. uint32\_t urva** PE - unaligned VirtualAddress

**7.1.2.2.8. uint32\_t uvsz** PE - unaligned VirtualSize

**7.1.2.2.9. uint32\_t vsz** VirtualSize

### 7.1.3. cli\_pe\_hook\_data Struct Reference

#### Data Fields

- uint32\_t [ep](#)
- uint16\_t [nsections](#)
- struct [pe\\_image\\_file\\_hdr](#) [file\\_hdr](#)
- struct [pe\\_image\\_optional\\_hdr32](#) [opt32](#)
- struct [pe\\_image\\_optional\\_hdr64](#) [opt64](#)
- struct [pe\\_image\\_data\\_dir](#) [dirs](#) [16]
- uint32\_t [e\\_lfanew](#)
- uint32\_t [overlays](#)
- int32\_t [overlays\\_sz](#)
- uint32\_t [hdr\\_size](#)

#### 7.1.3.1. Detailed Description

Data for the bytecode PE hook

#### 7.1.3.2. Field Documentation

**7.1.3.2.1. struct [pe\\_image\\_data\\_dir](#) [dirs](#)[16]** PE data directory header

- 7.1.3.2.2. `uint32_t e_lfanew` address of new exe header
- 7.1.3.2.3. `uint32_t ep` EntryPoint as file offset
- 7.1.3.2.4. `struct pe_image_file_hdr file_hdr` Header for this PE file
- 7.1.3.2.5. `uint32_t hdr_size` internally needed by rawaddr
- 7.1.3.2.6. `uint16_t nsections` Number of sections
- 7.1.3.2.7. `struct pe_image_optional_hdr32 opt32` 32-bit PE optional header
- 7.1.3.2.8. `struct pe_image_optional_hdr64 opt64` 64-bit PE optional header
- 7.1.3.2.9. `uint32_t overlays` number of overlays
- 7.1.3.2.10. `int32_t overlays_sz` size of overlays

#### 7.1.4. DIS\_arg Struct Reference

---

##### Data Fields

- enum [DIS\\_ACCESS](#) `access_type`
- enum [DIS\\_SIZE](#) `access_size`
- struct [DIS\\_mem\\_arg](#) `mem`
- enum [X86REGS](#) `reg`
- `uint64_t other`

##### 7.1.4.1. Detailed Description

disassembled operand

**7.1.4.2. Field Documentation**

**7.1.4.2.1. enum DIS\_SIZE access\_size** size of access

**7.1.4.2.2. enum DIS\_ACCESS access\_type** type of access

**7.1.4.2.3. struct DIS\_mem\_arg mem** memory operand

**7.1.4.2.4. uint64\_t other** other operand

**7.1.4.2.5. enum X86REGS reg** register operand

**7.1.5. DIS\_fixed Struct Reference****Data Fields**

- enum [X86OPS x86\\_opcode](#)
- enum [DIS\\_SIZE operation\\_size](#)
- enum [DIS\\_SIZE address\\_size](#)
- uint8\_t [segment](#)

**7.1.5.1. Detailed Description**

disassembled instruction

**7.1.5.2. Field Documentation**

**7.1.5.2.1. enum DIS\_SIZE address\_size** size of address

**7.1.5.2.2. enum DIS\_SIZE operation\_size** size of operation

**7.1.5.2.3. uint8\_t segment** segment

**7.1.5.2.4. enum X86OPS x86\_opcode** opcode of X86 instruction

### 7.1.6. DIS\_mem\_arg Struct Reference

---

#### Data Fields

- enum [DIS\\_SIZE](#) `access_size`
- enum [X86REGS](#) `scale_reg`
- enum [X86REGS](#) `add_reg`
- [uint8\\_t](#) `scale`
- [int32\\_t](#) `displacement`

#### 7.1.6.1. Detailed Description

disassembled memory operand:  $\text{scale\_reg} * \text{scale} + \text{add\_reg} + \text{displacement}$

#### 7.1.6.2. Field Documentation

**7.1.6.2.1. enum DIS\_SIZE access\_size** size of access

**7.1.6.2.2. enum X86REGS add\_reg** register used as displacement

**7.1.6.2.3. int32\_t displacement** displacement as immediate number

**7.1.6.2.4. uint8\_t scale** scale as immediate number

**7.1.6.2.5. enum X86REGS scale\_reg** register used as scale

### 7.1.7. DISASM\_RESULT Struct Reference

---

#### 7.1.7.1. Detailed Description

disassembly result, 64-byte, matched by type-8 signatures

### 7.1.8. pe\_image\_data\_dir Struct Reference

---

#### 7.1.8.1. Detailed Description

PE data directory header

## 7.1.9. pe\_image\_file\_hdr Struct Reference

### Data Fields

- uint32\_t [Magic](#)
- uint16\_t [Machine](#)
- uint16\_t [NumberOfSections](#)
- uint32\_t [TimeDateStamp](#)
- uint32\_t [PointerToSymbolTable](#)
- uint32\_t [NumberOfSymbols](#)
- uint16\_t [SizeOfOptionalHeader](#)

### 7.1.9.1. Detailed Description

Header for this PE file

### 7.1.9.2. Field Documentation

**7.1.9.2.1. uint16\_t Machine** CPU this executable runs on, see libclamav/pe.c for possible values

**7.1.9.2.2. uint32\_t Magic** PE magic header: PE\0\0

**7.1.9.2.3. uint16\_t NumberOfSections** Number of sections in this executable

**7.1.9.2.4. uint32\_t NumberOfSymbols** debug

**7.1.9.2.5. uint32\_t PointerToSymbolTable** debug

**7.1.9.2.6. uint16\_t SizeOfOptionalHeader** == 224

**7.1.9.2.7. uint32\_t TimeDateStamp** Unreliable

### 7.1.10. pe\_image\_optional\_hdr32 Struct Reference

---

#### Data Fields

- uint8\_t [MajorLinkerVersion](#)
- uint8\_t [MinorLinkerVersion](#)
- uint32\_t [SizeOfCode](#)
- uint32\_t [SizeOfInitializedData](#)
- uint32\_t [SizeOfUninitializedData](#)
- uint32\_t [ImageBase](#)
- uint32\_t [SectionAlignment](#)
- uint32\_t [FileAlignment](#)
- uint16\_t [MajorOperatingSystemVersion](#)
- uint16\_t [MinorOperatingSystemVersion](#)
- uint16\_t [MajorImageVersion](#)
- uint16\_t [MinorImageVersion](#)
- uint32\_t [Checksum](#)
- uint32\_t [NumberOfRvaAndSizes](#)

#### 7.1.10.1. Detailed Description

32-bit PE optional header

#### 7.1.10.2. Field Documentation

- |   |                   |
|---|-------------------|
| <b>7.1.10.2.1. uint32_t CheckSum</b>          | NT drivers only   |
| <b>7.1.10.2.2. uint32_t FileAlignment</b>     | usually 32 or 512 |
| <b>7.1.10.2.3. uint32_t ImageBase</b>         | multiple of 64 KB |
| <b>7.1.10.2.4. uint16_t MajorImageVersion</b> | unreliable        |

<b>7.1.10.2.5. uint8_t MajorLinkerVersion</b>	unreliable
<b>7.1.10.2.6. uint16_t MajorOperatingSystemVersion</b>	not used
<b>7.1.10.2.7. uint16_t MinorImageVersion</b>	unreliable
<b>7.1.10.2.8. uint8_t MinorLinkerVersion</b>	unreliable
<b>7.1.10.2.9. uint16_t MinorOperatingSystemVersion</b>	not used
<b>7.1.10.2.10. uint32_t NumberOfRvaAndSizes</b>	unreliable
<b>7.1.10.2.11. uint32_t SectionAlignment</b>	usually 32 or 4096
<b>7.1.10.2.12. uint32_t SizeOfCode</b>	unreliable
<b>7.1.10.2.13. uint32_t SizeOfInitializedData</b>	unreliable
<b>7.1.10.2.14. uint32_t SizeOfUninitializedData</b>	unreliable

### 7.1.11. pe\_image\_optional\_hdr64 Struct Reference

---

#### Data Fields

- uint8\_t [MajorLinkerVersion](#)
- uint8\_t [MinorLinkerVersion](#)
- uint32\_t [SizeOfCode](#)
- uint32\_t [SizeOfInitializedData](#)
- uint32\_t [SizeOfUninitializedData](#)
- uint64\_t [ImageBase](#)
- uint32\_t [SectionAlignment](#)
- uint32\_t [FileAlignment](#)
- uint16\_t [MajorOperatingSystemVersion](#)
- uint16\_t [MinorOperatingSystemVersion](#)
- uint16\_t [MajorImageVersion](#)
- uint16\_t [MinorImageVersion](#)
- uint32\_t [Checksum](#)
- uint32\_t [NumberOfRvaAndSizes](#)



**7.1.11.1. Detailed Description**

PE 64-bit optional header

**7.1.11.2. Field Documentation**

<b>7.1.11.2.1. uint32_t CheckSum</b>	NT drivers only
<b>7.1.11.2.2. uint32_t FileAlignment</b>	usually 32 or 512
<b>7.1.11.2.3. uint64_t ImageBase</b>	multiple of 64 KB
<b>7.1.11.2.4. uint16_t MajorImageVersion</b>	unreliable
<b>7.1.11.2.5. uint8_t MajorLinkerVersion</b>	unreliable
<b>7.1.11.2.6. uint16_t MajorOperatingSystemVersion</b>	not used
<b>7.1.11.2.7. uint16_t MinorImageVersion</b>	unreliable
<b>7.1.11.2.8. uint8_t MinorLinkerVersion</b>	unreliable
<b>7.1.11.2.9. uint16_t MinorOperatingSystemVersion</b>	not used
<b>7.1.11.2.10. uint32_t NumberOfRvaAndSizes</b>	unreliable
<b>7.1.11.2.11. uint32_t SectionAlignment</b>	usually 32 or 4096
<b>7.1.11.2.12. uint32_t SizeOfCode</b>	unreliable
<b>7.1.11.2.13. uint32_t SizeOfInitializedData</b>	unreliable

**7.1.11.2.14. uint32\_t SizeOfUninitializedData**

unreliable

**7.1.12. pe\_image\_section\_hdr Struct Reference**

---

**Data Fields**

- uint8\_t [Name](#) [8]
- uint32\_t [SizeOfRawData](#)
- uint32\_t [PointerToRawData](#)
- uint32\_t [PointerToRelocations](#)
- uint32\_t [PointerToLinenumbers](#)
- uint16\_t [NumberOfRelocations](#)
- uint16\_t [NumberOfLinenumbers](#)

**7.1.12.1. Detailed Description**

PE section header

**7.1.12.2. Field Documentation**

- |  |                              |
|--|------------------------------|
| <b>7.1.12.2.1. uint8_t Name[8]</b>               | may not end with NULL        |
| <b>7.1.12.2.2. uint16_t NumberOfLinenumbers</b>  | object files only            |
| <b>7.1.12.2.3. uint16_t NumberOfRelocations</b>  | object files only            |
| <b>7.1.12.2.4. uint32_t PointerToLinenumbers</b> | object files only            |
| <b>7.1.12.2.5. uint32_t PointerToRawData</b>     | offset to the section's data |
| <b>7.1.12.2.6. uint32_t PointerToRelocations</b> | object files only            |
| <b>7.1.12.2.7. uint32_t SizeOfRawData</b>        | multiple of FileAlignment    |

## 7.2. Low level API

---

### 7.2.1. bytecode\_api.h File Reference

---

#### Enumerations

- enum `BytecodeKind` { `BC_GENERIC` = 0 , `BC_LOGICAL` = 256, `BC_PE_UNPACKER` }
- enum { `SEEK_SET` = 0, `SEEK_CUR`, `SEEK_END` }

#### Functions

- `uint32_t test1` (`uint32_t a`, `uint32_t b`)
- `int32_t read` (`uint8_t *data`, `int32_t size`)  
*Reads specified amount of bytes from the current file into a buffer. Also moves current position in the file.*
- `int32_t write` (`uint8_t *data`, `int32_t size`)  
*Writes the specified amount of bytes from a buffer to the current temporary file.*
- `int32_t seek` (`int32_t pos`, `uint32_t whence`)  
*Changes the current file position to the specified one.*
- `uint32_t setvirusname` (`const uint8_t *name`, `uint32_t len`)
- `uint32_t debug_print_str` (`const uint8_t *str`, `uint32_t len`)
- `uint32_t debug_print_uint` (`uint32_t a`)
- `uint32_t disasm_x86` (`struct DISASM_RESULT *result`, `uint32_t len`)
- `uint32_t pe_rawaddr` (`uint32_t rva`)
- `int32_t file_find` (`const uint8_t *data`, `uint32_t len`)
- `int32_t file_byteat` (`uint32_t offset`)
- `void * malloc` (`uint32_t size`)
- `uint32_t test2` (`uint32_t a`)
- `int32_t get_pe_section` (`struct cli_exe_section *section`, `uint32_t num`)
- `int32_t fill_buffer` (`uint8_t *buffer`, `uint32_t len`, `uint32_t filled`, `uint32_t cursor`, `uint32_t fill`)
- `int32_t extract_new` (`int32_t id`)
- `int32_t read_number` (`uint32_t radix`)
- `int32_t hashset_new` (`void`)

- `int32_t hashset_add` (`int32_t hs`, `uint32_t key`)
- `int32_t hashset_remove` (`int32_t hs`, `uint32_t key`)
- `int32_t hashset_contains` (`int32_t hs`, `uint32_t key`)
- `int32_t hashset_done` (`int32_t id`)
- `int32_t hashset_empty` (`int32_t id`)
- `int32_t buffer_pipe_new` (`uint32_t size`)
- `int32_t buffer_pipe_new_fromfile` (`uint32_t pos`)
- `uint32_t buffer_pipe_read_avail` (`int32_t id`)
- `uint8_t * buffer_pipe_read_get` (`int32_t id`, `uint32_t amount`)
- `int32_t buffer_pipe_read_stopped` (`int32_t id`, `uint32_t amount`)
- `uint32_t buffer_pipe_write_avail` (`int32_t id`)
- `uint8_t * buffer_pipe_write_get` (`int32_t id`, `uint32_t size`)
- `int32_t buffer_pipe_write_stopped` (`int32_t id`, `uint32_t amount`)
- `int32_t buffer_pipe_done` (`int32_t id`)
- `int32_t inflate_init` (`int32_t from_buffer`, `int32_t to_buffer`, `int32_t window-Bits`)
- `int32_t inflate_process` (`int32_t id`)
- `int32_t inflate_done` (`int32_t id`)
- `int32_t bytecode_rt_error` (`int32_t locationid`)
- `int32_t jsnorm_init` (`int32_t from_buffer`)
- `int32_t jsnorm_process` (`int32_t id`)
- `int32_t jsnorm_done` (`int32_t id`)

## Variables

- `const uint32_t __clambc_match_counts` [64]  
*Logical signature match counts.*
- `struct cli_pe_hook_data __clambc_pdata`
- `const uint32_t __clambc_filesize` [1]
- `const uint16_t __clambc_kind`

### 7.2.1.1. Detailed Description

### 7.2.1.2. Enumeration Type Documentation

#### 7.2.1.2.1. anonymous enum

##### Enumerator:

**SEEK\_SET** set file position to specified absolute position

**SEEK\_CUR** set file position relative to current position

**SEEK\_END** set file position relative to file end

#### 7.2.1.2.2. enum BytecodeKind

Bytecode trigger kind

##### Enumerator:

**BC\_GENERIC** generic bytecode, not tied a specific hook

**BC\_LOGICAL** triggered by a logical signature

**BC\_PE\_UNPACKER** a PE unpacker

### 7.2.1.3. Function Documentation

**7.2.1.3.1. int32\_t buffer\_pipe\_done (int32\_t id)** Deallocate memory used by buffer. After this all attempts to use this buffer will result in error. All buffer\_pipes are automatically deallocated when bytecode finishes execution.

##### Parameters:

*id* ID of buffer\_pipe

##### Returns:

0 on success

**7.2.1.3.2. int32\_t buffer\_pipe\_new (uint32\_t size)** Creates a new pipe with the specified buffer size

##### Parameters:

*size* size of buffer

##### Returns:

ID of newly created buffer\_pipe

**7.2.1.3.3. `int32_t buffer_pipe_new_fromfile (uint32_t pos)`** Same as `buffer_pipe_new`, except the pipe's input is tied to the current file, at the specified position.

**Parameters:**

*pos* starting position of pipe input in current file

**Returns:**

ID of newly created `buffer_pipe`

**7.2.1.3.4. `uint32_t buffer_pipe_read_avail (int32_t id)`** Returns the amount of bytes available to read.

**Parameters:**

*id* ID of `buffer_pipe`

**Returns:**

amount of bytes available to read

**7.2.1.3.5. `uint8_t* buffer_pipe_read_get (int32_t id, uint32_t amount)`** Returns a pointer to the buffer for reading. The 'amount' parameter should be obtained by a call to [buffer\\_pipe\\_read\\_avail\(\)](#).

**Parameters:**

*id* ID of `buffer_pipe`

*amount* to read

**Returns:**

pointer to buffer, or NULL if buffer has less than specified amount

**7.2.1.3.6. `int32_t buffer_pipe_read_stopped (int32_t id, uint32_t amount)`** Updates read cursor in `buffer_pipe`.

**Parameters:**

*id* ID of `buffer_pipe`

*amount* amount of bytes to move read cursor

**Returns:**

0 on success

**7.2.1.3.7. `uint32_t buffer_pipe_write_avail (int32_t id)`** Returns the amount of bytes available for writing.

**Parameters:**

*id* ID of buffer\_pipe

**Returns:**

amount of bytes available for writing

**7.2.1.3.8. `uint8_t* buffer_pipe_write_get (int32_t id, uint32_t size)`** Returns pointer to writable buffer. The 'amount' parameter should be obtained by a call to [buffer\\_pipe\\_write\\_avail\(\)](#).

**Parameters:**

*id* ID of buffer\_pipe

*size* amount of bytes to write

**Returns:**

pointer to write buffer, or NULL if requested amount is more than what is available in the buffer

**7.2.1.3.9. `int32_t buffer_pipe_write_stopped (int32_t id, uint32_t amount)`** Updates the write cursor in buffer\_pipe.

**Parameters:**

*id* ID of buffer\_pipe

*amount* amount of bytes to move write cursor

**Returns:**

0 on success

**7.2.1.3.10. `int32_t bytecode_rt_error (int32_t locationid)`** Report a runtime error at the specified locationID.

**Parameters:**

*locationid* (line << 8) | (column&0xff)

**Returns:**

0

**7.2.1.3.11. uint32\_t debug\_print\_str (const uint8\_t \* *str*, uint32\_t *len*)**

Prints a debug message.

**Parameters:**

- ← *str* Message to print
- ← *len* length of message to print

**Returns:**

0

**7.2.1.3.12. uint32\_t debug\_print\_uint (uint32\_t *a*)**

Prints a number as a debug message.

**Parameters:**

- ← *a* number to print

**Returns:**

0

**7.2.1.3.13. uint32\_t disasm\_x86 (struct DISASM\_RESULT \**result*, uint32\_t *len*)**  
Disassembles starting from current file position, the specified amount of bytes.**Parameters:**

- *result* pointer to struct holding result
- ← *len* how many bytes to disassemble

**Returns:**

0 for success

You can use `lseek` to disassemble starting from a different location. This is a low-level API, the result is in ClamAV type-8 signature format (64 bytes/instruction).

**See also:**

[DisassembleAt](#)



**7.2.1.3.14. `int32_t extract_new (int32_t id)`** Prepares for extracting a new file, if we've already extracted one it scans it.

**Parameters:**

← *id* an id for the new file (for example position in container)

**Returns:**

1 if previous extracted file was infected

**7.2.1.3.15. `int32_t file_byteat (uint32_t offset)`** Read a single byte from current file

**Parameters:**

*offset* file offset

**Returns:**

byte at offset *off* in the current file, or -1 if offset is invalid

**7.2.1.3.16. `int32_t file_find (const uint8_t * data, uint32_t len)`** Looks for the specified sequence of bytes in the current file.

**Parameters:**

← *data* the sequence of bytes to look for

*len* length of data, cannot be more than 1024

**Returns:**

offset in the current file if match is found, -1 otherwise

**7.2.1.3.17. `int32_t fill_buffer (uint8_t * buffer, uint32_t len, uint32_t filled, uint32_t cursor, uint32_t fill)`** Fills the specified buffer with at least *fill* bytes.

**Parameters:**

→ *buffer* the buffer to fill

← *len* length of buffer

← *filled* how much of the buffer is currently filled

- ← *cursor* position of cursor in buffer
- ← *fill* amount of bytes to fill in (0 is valid)

**Returns:**

<0 on error, 0 on EOF, number bytes available in buffer (starting from 0) The character at the cursor will be at position 0 after this call.

**7.2.1.3.18. `int32_t get_pe_section (struct cli_exe_section * section, uint32_t num)`** Gets information about the specified PE section.

**Parameters:**

- *section* PE section information will be stored here
- ← *num* PE section number

**7.2.1.3.19. `int32_t hashset_add (int32_t hs, uint32_t key)`** Add a new 32-bit key to the hashset.

**Parameters:**

- hs* ID of hashset (from `hashset_new`)
- key* the key to add

**Returns:**

0 on success

**7.2.1.3.20. `int32_t hashset_contains (int32_t hs, uint32_t key)`** Returns whether the hashset contains the specified key.

**Parameters:**

- hs* ID of hashset (from `hashset_new`)
- key* the key to lookup

**Returns:**

1 if found, 0 if not found, <0 on invalid hashset ID

**7.2.1.3.21. `int32_t` `hashset_done` (`int32_t` *id*)** Deallocates the memory used by the specified hashset. Trying to use the hashset after this will result in an error. The hashset may not be used after this. All hashsets are automatically deallocated when bytecode finishes execution.

**Parameters:**

*id* ID of hashset (from `hashset_new`)

**Returns:**

0 on success

**7.2.1.3.22. `int32_t` `hashset_empty` (`int32_t` *id*)** Returns whether the hashset is empty.

**Parameters:**

*id* of hashset (from `hashset_new`)

**Returns:**

0 on success

**7.2.1.3.23. `int32_t` `hashset_new` (`void`)** Creates a new hashset and returns its id.

**Returns:**

ID for new hashset

**7.2.1.3.24. `int32_t` `hashset_remove` (`int32_t` *hs*, `uint32_t` *key*)** Remove a 32-bit key from the hashset.

**Parameters:**

*hs* ID of hashset (from `hashset_new`)

*key* the key to add

**Returns:**

0 on success

**7.2.1.3.25. `int32_t inflate_done (int32_t id)`** Deallocates inflate data structure. Using the inflate data structure after this will result in an error. All inflate data structures are automatically deallocated when bytecode finishes execution.

**Parameters:**

*id* ID of inflate data structure

**Returns:**

0 on success.

**7.2.1.3.26. `int32_t inflate_init (int32_t from_buffer, int32_t to_buffer, int32_t windowBits)`** Initializes inflate data structures for decompressing data 'from\_buffer' and writing uncompressed data 'to\_buffer'.

**Parameters:**

*from\_buffer* ID of buffer\_pipe to read compressed data from

*to\_buffer* ID of buffer\_pipe to write decompressed data to

*windowBits* (see zlib documentation)

**Returns:**

ID of newly created inflate data structure, <0 on failure

**7.2.1.3.27. `int32_t inflate_process (int32_t id)`** Inflate all available data in the input buffer, and write to output buffer. Stops when the input buffer becomes empty, or write buffer becomes full. Also attempts to recover from corrupted inflate stream (via `inflateSync`). This function can be called repeatedly on success after filling the input buffer, and flushing the output buffer. The inflate stream is done processing when 0 bytes are available from output buffer, and input buffer is not empty.

**Parameters:**

*id* ID of inflate data structure

**Returns:**

0 on success, zlib error code otherwise

**7.2.1.3.28. `int32_t jsnorm_done (int32_t id)`** Flushes JS normalizer.

**Parameters:**

*id* ID of js normalizer to flush

**7.2.1.3.29. `int32_t jsnorm_init (int32_t from_buffer)`** Initializes JS normalizer for reading 'from\_buffer'. Normalized JS will be written to a single tempfile, one normalized JS per line, and automatically scanned when the bytecode finishes execution.

**Parameters:**

*from\_buffer* ID of buffer\_pipe to read javascript from

**Returns:**

ID of JS normalizer, <0 on failure

**7.2.1.3.30. `int32_t jsnorm_process (int32_t id)`** Normalize all javascript from the input buffer, and write to tempfile. You can call this function repeatedly on success, if you (re)fill the input buffer.

**Parameters:**

*id* ID of JS normalizer

**Returns:**

0 on success, <0 on failure

**7.2.1.3.31. `void* malloc (uint32_t size)`** Allocates memory. Currently this memory is freed automatically on exit from the bytecode, and there is no way to free it sooner.

**Parameters:**

*size* amount of memory to allocate in bytes

**Returns:**

pointer to allocated memory

**7.2.1.3.32. `uint32_t pe_rawaddr (uint32_t rva)`**      Converts a RVA (Relative Virtual Address) to an absolute PE file offset.

**Parameters:**

*rva* a rva address from the PE file

**Returns:**

absolute file offset mapped to the *rva*, or `PE_INVALID_RVA` if the *rva* is invalid.

**7.2.1.3.33. `int32_t read (uint8_t * data, int32_t size)`**

Reads specified amount of bytes from the current file into a buffer. Also moves current position in the file.

**Parameters:**

← *size* amount of bytes to read

→ *data* pointer to buffer where data is read into

**Returns:**

amount read.

**7.2.1.3.34. `int32_t read_number (uint32_t radix)`**      Reads a number in the specified radix starting from the current position. Non-numeric characters are ignored.

**Parameters:**

← *radix* 10 or 16

**Returns:**

the number read

**7.2.1.3.35. `int32_t seek (int32_t pos, uint32_t whence)`**

Changes the current file position to the specified one.

**See also:**

[SEEK\\_SET](#), [SEEK\\_CUR](#), [SEEK\\_END](#)

**Parameters:**

- ← *pos* offset (absolute or relative depending on *whence* param)
- ← *whence* one of SEEK\_SET, SEEK\_CUR, SEEK\_END

**Returns:**

absolute position in file

**7.2.1.3.36. `uint32_t setvirusname (const uint8_t * name, uint32_t len)`** Sets the name of the virus found.

**Parameters:**

- ← *name* the name of the virus
- ← *len* length of the virusname

**Returns:**

0

**7.2.1.3.37. `uint32_t test1 (uint32_t a, uint32_t b)`** Test api.

**Parameters:**

- a* 0xf00dbeef
- b* 0xbeeff00d

**Returns:**

0x12345678 if parameters match, 0x55 otherwise

**7.2.1.3.38. `uint32_t test2 (uint32_t a)`** Test api2.

**Parameters:**

- a* 0xf00d

**Returns:**

0xd00f if parameter matches, 0x5555 otherwise

**7.2.1.3.39. `int32_t write (uint8_t * data, int32_t size)`**

Writes the specified amount of bytes from a buffer to the current temporary file.

**Parameters:**

- ← *data* pointer to buffer of data to write
- ← *size* amount of bytes to write *size* bytes to temporary file, from the buffer pointed to byte

**Returns:**

amount of bytes successfully written

**7.2.1.4. Variable Documentation**

**7.2.1.4.1. `const uint32_t __clambc_filesize[1]`** File size (max 4G)

**7.2.1.4.2. `const uint16_t __clambc_kind`** Kind of the bytecode

**7.2.1.4.3. `const uint32_t __clambc_match_counts[64]`**

Logical signature match counts.

This is a low-level variable, use the Macros in [bytecode\\_local.h](#) instead to access it.

**7.2.1.4.4. `struct cli_pe_hook_data __clambc_pdata`** PE data, if this is a PE hook

**7.2.2. `bytecode_disasm.h` File Reference****Data Structures**

- struct [DISASM\\_RESULT](#)

**Enumerations**

- enum [X86OPS](#) { ,  
[OP\\_AAA](#), [OP\\_AAD](#), [OP\\_AAM](#), [OP\\_AAS](#),  
[OP\\_ADD](#), [OP\\_ADC](#), [OP\\_AND](#), [OP\\_ARPL](#),  
[OP\\_BOUND](#), [OP\\_BSF](#), [OP\\_BSR](#), [OP\\_BSWAP](#),  
[OP\\_BT](#), [OP\\_BTC](#), [OP\\_BTR](#), [OP\\_BTS](#),  
[OP\\_CALL](#), [OP\\_CDQ](#) , [OP\\_CWDE](#), [OP\\_CBW](#),



OP\_CLC, OP\_CLD, OP\_CLI, OP\_CLTS,  
OP\_CMC, OP\_CMOVO, OP\_CMOVNO, OP\_CMOVC,  
OP\_CMOVNC, OP\_CMOVZ, OP\_CMOVNZ, OP\_CMOVBE,  
OP\_CMOVA, OP\_CMOVS, OP\_CMOVNS, OP\_CMOVP,  
OP\_CMOVNP, OP\_CMOVL, OP\_CMOVGE, OP\_CMOVLE,  
OP\_CMOVG, OP\_CMP, OP\_CMPSD, OP\_CMPSW,  
OP\_CMPSB, OP\_CMPXCHG, OP\_CMPXCHG8B, OP\_CPUID,  
OP\_DAA, OP\_DAS, OP\_DEC, OP\_DIV,  
OP\_ENTER, OP\_FWAIT, OP\_HLT, OP\_IDIV,  
OP\_IMUL, OP\_INC, OP\_IN, OP\_INSD,  
OP\_INSW, OP\_INSB, OP\_INT, OP\_INT3,  
OP\_INT0, OP\_INVD, OP\_INVLPG, OP\_IRET,  
OP\_JO, OP\_JNO, OP\_JC, OP\_JNC,  
OP\_JZ, OP\_JNZ, OP\_JBE, OP\_JA,  
OP\_JS, OP\_JNS, OP\_JP, OP\_JNP,  
OP\_JL, OP\_JGE, OP\_JLE, OP\_JG,  
OP\_JMP, OP\_LAHF, OP\_LAR, OP\_LDS,  
OP\_LES, OP\_LFS, OP\_LGS, OP\_LEA,  
OP\_LEAVE, OP\_LGDT, OP\_LIDT, OP\_LLDT,  
OP\_PREFIX\_LOCK, OP\_LODSD, OP\_LODSW, OP\_LODSB,  
OP\_LOOP, OP\_LOOPE, OP\_LOOPNE, OP\_JECXZ,  
OP\_LSL, OP\_LSS, OP\_LTR, OP\_MOV,  
OP\_MOVSD, OP\_MOVSX, OP\_MOVSB, OP\_MOVSX,  
OP\_MOVZX, OP\_MUL, OP\_NEG, OP\_NOP,  
OP\_NOT, OP\_OR, OP\_OUT, OP\_OUTSD,  
OP\_OUTSW, OP\_OUTSB, OP\_PUSH, OP\_PUSHAD ,  
OP\_PUSHFD , OP\_POP, OP\_POPAD, OP\_POPFD ,  
OP\_RCL, OP\_RCR, OP\_RDMSR, OP\_RDPMC,  
OP\_RDTSC, OP\_PREFIX\_REPE, OP\_PREFIX\_REPNB, OP\_RETF,  
OP\_RETN, OP\_ROL, OP\_ROR, OP\_RSM,  
OP\_SAHF, OP\_SAR, OP\_SBB, OP\_SCASD,

OP\_SCASW, OP\_SCASB, OP\_SETO, OP\_SETNO,  
OP\_SETC, OP\_SETNC, OP\_SETZ, OP\_SETNZ,  
OP\_SETBE, OP\_SETA, OP\_SETS, OP\_SETNS,  
OP\_SETP, OP\_SETNP, OP\_SETL, OP\_SETGE,  
OP\_SETLE, OP\_SETG, OP\_SGDT, OP\_SIDT,  
OP\_SHL, OP\_SHLD, OP\_SHR, OP\_SHRD,  
OP\_SLDT, OP\_STOSD, OP\_STOSW, OP\_STOSB,  
OP\_STR, OP\_STC, OP\_STD, OP\_STI,  
OP\_SUB, OP\_SYSCALL, OP\_SYSENTER, OP\_SYSEXIT,  
OP\_SYSRET, OP\_TEST, OP\_UD2, OP\_VERR,  
OP\_VERRW, OP\_WBINVD, OP\_WRMSR, OP\_XADD,  
OP\_XCHG, OP\_XLAT, OP\_XOR, OP\_FPU,  
OP\_F2XM1, OP\_FABS, OP\_FADD, OP\_FADDP,  
OP\_FBLD, OP\_FBSTP, OP\_FCHS, OP\_FCLEX,  
OP\_FCMOVB, OP\_FCMOVBE, OP\_FCMOVE, OP\_FCMOVNB,  
OP\_FCMOVNBE, OP\_FCMOVNE, OP\_FCMOVNU, OP\_FCMOVU,  
OP\_FCOM, OP\_FCOMI, OP\_FCOMIP, OP\_FCOMP,  
OP\_FCOMPP, OP\_FCOS, OP\_FDECSTP, OP\_FDIV,  
OP\_FDIVP, OP\_FDIVR, OP\_FDIVRP, OP\_FFREE,  
OP\_FIADD, OP\_FICOM, OP\_FICOMP, OP\_FIDIV,  
OP\_FIDIVR, OP\_FILD, OP\_FIMUL, OP\_FINCSTP,  
OP\_FINIT, OP\_FIST, OP\_FISTP, OP\_FISTTP,  
OP\_FISUB, OP\_FISUBR, OP\_FLD, OP\_FLD1,  
OP\_FLDCW, OP\_FLDENV, OP\_FLDL2E, OP\_FLDL2T,  
OP\_FLDLG2, OP\_FLDLN2, OP\_FLDPI, OP\_FLDZ,  
OP\_FMUL, OP\_FMULP, OP\_FNOP, OP\_FPATAN,  
OP\_FPREM, OP\_FPREM1, OP\_FPTAN, OP\_FRNDINT,  
OP\_FRSTOR, OP\_FSCALE, OP\_FSINCOS, OP\_FSQRT,  
OP\_FSAVE, OP\_FST, OP\_FSTCW, OP\_FSTENV,  
OP\_FSTP, OP\_FSTSW, OP\_FSUB, OP\_FSUBP,  
OP\_FSUBR, OP\_FSUBRP, OP\_FTST, OP\_FUCOM,

OP\_FUCOMI, OP\_FUCOMIP, OP\_FUCOMP, OP\_FUCOMPP,  
 OP\_FXAM, OP\_FXCH, OP\_FXTRACT, OP\_FYL2X,  
 OP\_FYL2XP1 }

- enum **DIS\_ACCESS** {  
 ACCESS\_NOARG, ACCESS\_IMM, ACCESS\_REL, ACCESS\_REG,  
 ACCESS\_MEM }
- enum **DIS\_SIZE** {  
 SIZEB, SIZEW, SIZED, SIZEF,  
 SIZEQ, SIZET, SIZEPTR }
- enum **X86REGS**

#### 7.2.2.1. Detailed Description

#### 7.2.2.2. Enumeration Type Documentation

##### 7.2.2.2.1. enum DIS\_ACCESS

Access type

##### Enumerator:

**ACCESS\_NOARG** arg not present  
**ACCESS\_IMM** immediate  
**ACCESS\_REL** +/- immediate  
**ACCESS\_REG** register  
**ACCESS\_MEM** [memory]

##### 7.2.2.2.2. enum DIS\_SIZE

for mem access, immediate and relative

##### Enumerator:

**SIZEB** Byte size access  
**SIZEW** Word size access  
**SIZED** Doubleword size access  
**SIZEF** 6-byte access (seg+reg pair)  
**SIZEQ** Quadword access  
**SIZET** 10-byte access  
**SIZEPTR** ptr

**7.2.2.2.3. enum X86OPS**

X86 opcode

**Enumerator:**

***OP\_AAA*** Ascii Adjust after Addition  
***OP\_AAD*** Ascii Adjust AX before Division  
***OP\_AAM*** Ascii Adjust AX after Multiply  
***OP\_AAS*** Ascii Adjust AL after Subtraction  
***OP\_ADD*** Add  
***OP\_ADC*** Add with Carry  
***OP\_AND*** Logical And  
***OP\_ARPL*** Adjust Requested Privilege Level  
***OP\_BOUND*** Check Array Index Against Bounds  
***OP\_BSF*** Bit Scan Forward  
***OP\_BSR*** Bit Scan Reverse  
***OP\_BSWAP*** Byte Swap  
***OP\_BT*** Bit Test  
***OPBTC*** Bit Test and Complement  
***OPBTR*** Bit Test and Reset  
***OPBTS*** Bit Test and Set  
***OP\_CALL*** Call  
***OP\_CDQ*** Convert DoubleWord to QuadWord  
***OP\_CWDE*** Convert Word to DoubleWord  
***OP\_CBW*** Convert Byte to Word  
***OP\_CLC*** Clear Carry Flag  
***OP\_CLD*** Clear Direction Flag  
***OP\_CLI*** Clear Interrupt Flag  
***OP\_CLTS*** Clear Task-Switched Flag in CR0  
***OP\_CMC*** Complement Carry Flag  
***OP\_CMOVO*** Conditional Move if Overflow  
***OP\_CMOVNO*** Conditional Move if Not Overflow  
***OP\_CMOVC*** Conditional Move if Carry

***OP\_CMOVNC*** Conditional Move if Not Carry  
***OP\_CMOVZ*** Conditional Move if Zero  
***OP\_CMOVNZ*** Conditional Move if Non-Zero  
***OP\_CMOVBE*** Conditional Move if Below or Equal  
***OP\_CMOVA*** Conditional Move if Above  
***OP\_CMOVS*** Conditional Move if Sign  
***OP\_CMOVNS*** Conditional Move if Not Sign  
***OP\_CMOVP*** Conditional Move if Parity  
***OP\_CMOVNP*** Conditional Move if Not Parity  
***OP\_CMOVL*** Conditional Move if Less  
***OP\_CMOVGE*** Conditional Move if Greater or Equal  
***OP\_CMOVLE*** Conditional Move if Less than or Equal  
***OP\_CMOVG*** Conditional Move if Greater  
***OP\_CMP*** Compare  
***OP\_CMPSD*** Compare String DoubleWord  
***OP\_CMPSW*** Compare String Word  
***OP\_CMPSB*** Compare String Byte  
***OP\_CMPXCHG*** Compare and Exchange  
***OP\_CMPXCHG8B*** Compare and Exchange Bytes  
***OP\_CPUID*** CPU Identification  
***OP\_DAA*** Decimal Adjust AL after Addition  
***OP\_DAS*** Decimal Adjust AL after Subtraction  
***OP\_DEC*** Decrement by 1  
***OP\_DIV*** Unsigned Divide  
***OP\_ENTER*** Make Stack Frame for Procedure Parameters  
***OP\_FWAIT*** Wait  
***OP\_HLT*** Halt  
***OP\_IDIV*** Signed Divide  
***OP\_IMUL*** Signed Multiply  
***OP\_INC*** Increment by 1  
***OP\_IN*** INput from port

***OP\_INSD*** INput from port to String Doubleword

***OP\_INSW*** INput from port to String Word

***OP\_INSB*** INput from port to String Byte

***OP\_INT*** INTerrupt

***OP\_INT3*** INTerrupt 3 (breakpoint)

***OP\_INT0*** INTerrupt 4 if Overflow

***OP\_INVD*** Invalidate Internal Caches

***OP\_INVLPG*** Invalidate TLB Entry

***OP\_IRET*** Interrupt Return

***OP\_JO*** Jump if Overflow

***OP\_JNO*** Jump if Not Overflow

***OP\_JC*** Jump if Carry

***OP\_JNC*** Jump if Not Carry

***OP\_JZ*** Jump if Zero

***OP\_JNZ*** Jump if Not Zero

***OP\_JBE*** Jump if Below or Equal

***OP\_JA*** Jump if Above

***OP\_JS*** Jump if Sign

***OP\_JNS*** Jump if Not Sign

***OP\_JP*** Jump if Parity

***OP\_JNP*** Jump if Not Parity

***OP\_JL*** Jump if Less

***OP\_JGE*** Jump if Greater or Equal

***OP\_JLE*** Jump if Less or Equal

***OP\_JG*** Jump if Greater

***OP\_JMP*** Jump (unconditional)

***OP\_LAHF*** Load Status Flags into AH Register

***OP\_LAR*** load Access Rights Byte

***OP\_LDS*** Load Far Pointer into DS

***OP\_LES*** Load Far Pointer into ES

***OP\_LFS*** Load Far Pointer into FS

***OP\_LGS*** Load Far Pointer into GS  
***OP\_LEA*** Load Effective Address  
***OP\_LEAVE*** High Level Procedure Exit  
***OP\_LGDT*** Load Global Descript Table Register  
***OP\_LIDT*** Load Interrupt Descriptor Table Register  
***OP\_LLDT*** Load Local Descriptor Table Register  
***OP\_PREFIX\_LOCK*** Assert LOCK# Signal Prefix  
***OP\_LODSD*** Load String Dword  
***OP\_LODSW*** Load String Word  
***OP\_LODSB*** Load String Byte  
***OP\_LOOP*** Loop According to ECX Counter  
***OP\_LOOPE*** Loop According to ECX Counter and ZF=1  
***OP\_LOOPNE*** Loop According to ECX Counter and ZF=0  
***OP\_JECXZ*** Jump if ECX is Zero  
***OP\_LSL*** Load Segment Limit  
***OP\_LSS*** Load Far Pointer into SS  
***OP\_LTR*** Load Task Register  
***OP\_MOV*** Move  
***OP\_MOVSD*** Move Data from String to String Doubleword  
***OP\_MOVSW*** Move Data from String to String Word  
***OP\_MOVSB*** Move Data from String to String Byte  
***OP\_MOVSX*** Move with Sign-Extension  
***OP\_MOVZX*** Move with Zero-Extension  
***OP\_MUL*** Unsigned Multiply  
***OP\_NEG*** Two's Complement Negation  
***OP\_NOP*** No Operation  
***OP\_NOT*** One's Complement Negation  
***OP\_OR*** Logical Inclusive OR  
***OP\_OUT*** Output to Port  
***OP\_OUTSD*** Output String to Port Doubleword  
***OP\_OUTSW*** Output String to Port Word

***OP\_OUTSB*** Output String to Port Bytes  
***OP\_PUSH*** Push Onto the Stack  
***OP\_PUSHAD*** Push All Double General Purpose Registers  
***OP\_PUSHFD*** Push EFLAGS Register onto the Stack  
***OP\_POP*** Pop a Value from the Stack  
***OP\_POPAD*** Pop All Double General Purpose Registers from the Stack  
***OP\_POPFD*** Pop Stack into EFLAGS Register  
***OP\_RCL*** Rotate Carry Left  
***OP\_RCR*** Rotate Carry Right  
***OP\_RDMSR*** Read from Model Specific Register  
***OP\_RDPMC*** Read Performance Monitoring Counters  
***OP\_RDTSC*** Read Time-Stamp Counter  
***OP\_PREFIX\_REPE*** Repeat String Operation Prefix while Equal  
***OP\_PREFIX\_REPNE*** Repeat String Operation Prefix while Not Equal  
***OP\_RETF*** Return from Far Procedure  
***OP\_RETN*** Return from Near Procedure  
***OP\_ROL*** Rotate Left  
***OP\_ROR*** Rotate Right  
***OP\_RSM*** Resumse from System Management Mode  
***OP\_SAHF*** Store AH into Flags  
***OP\_SAR*** Shift Arithmetic Right  
***OP\_SBB*** Subtract with Borrow  
***OP\_SCASD*** Scan String Doubleword  
***OP\_SCASW*** Scan String Word  
***OP\_SCASB*** Scan String Byte  
***OP\_SETO*** Set Byte on Overflow  
***OP\_SETNO*** Set Byte on Not Overflow  
***OP\_SETC*** Set Byte on Carry  
***OP\_SETNC*** Set Byte on Not Carry  
***OP\_SETZ*** Set Byte on Zero  
***OP\_SETNZ*** Set Byte on Not Zero



***OP\_SETBE*** Set Byte on Below or Equal  
***OP\_SETA*** Set Byte on Above  
***OP\_SETS*** Set Byte on Sign  
***OP\_SETNS*** Set Byte on Not Sign  
***OP\_SETP*** Set Byte on Parity  
***OP\_SETNP*** Set Byte on Not Parity  
***OP\_SETL*** Set Byte on Less  
***OP\_SETGE*** Set Byte on Greater or Equal  
***OP\_SETLE*** Set Byte on Less or Equal  
***OP\_SETG*** Set Byte on Greater  
***OP\_SGDT*** Store Global Descriptor Table Register  
***OP\_SIDT*** Store Interrupt Descriptor Table Register  
***OP\_SHL*** Shift Left  
***OP\_SHLD*** Double Precision Shift Left  
***OP\_SHR*** Shift Right  
***OP\_SHRD*** Double Precision Shift Right  
***OP\_SLDT*** Store Local Descriptor Table Register  
***OP\_STOSD*** Store String Doubleword  
***OP\_STOSW*** Store String Word  
***OP\_STOSB*** Store String Byte  
***OP\_STR*** Store Task Register  
***OP\_STC*** Set Carry Flag  
***OP\_STD*** Set Direction Flag  
***OP\_STI*** Set Interrupt Flag  
***OP\_SUB*** Subtract  
***OP\_SYSCALL*** Fast System Call  
***OP\_SYSENTER*** Fast System Call  
***OP\_SYSEXIT*** Fast Return from Fast System Call  
***OP\_SYSRET*** Return from Fast System Call  
***OP\_TEST*** Logical Compare  
***OP\_UD2*** Undefined Instruction

***OP\_VERR*** Verify a Segment for Reading  
***OP\_VERRW*** Verify a Segment for Writing  
***OP\_WBINVD*** Write Back and Invalidate Cache  
***OP\_WRMSR*** Write to Model Specific Register  
***OP\_XADD*** Exchange and Add  
***OP\_XCHG*** Exchange Register/Memory with Register  
***OP\_XLAT*** Table Look-up Translation  
***OP\_XOR*** Logical Exclusive OR  
***OP\_FPU*** FPU operation  
***OP\_F2XMI*** Compute  $2x-1$   
***OP\_FABS*** Absolute Value  
***OP\_FADD*** Floating Point Add  
***OP\_FADDP*** Floating Point Add, Pop  
***OP\_FBLD*** Load Binary Coded Decimal  
***OP\_FBSTP*** Store BCD Integer and Pop  
***OP\_FCHS*** Change Sign  
***OP\_FCLEX*** Clear Exceptions  
***OP\_FCMOVB*** Floating Point Move on Below  
***OP\_FCMOVBE*** Floating Point Move on Below or Equal  
***OP\_FCMOVE*** Floating Point Move on Equal  
***OP\_FCMOVNB*** Floating Point Move on Not Below  
***OP\_FCMOVNBE*** Floating Point Move on Not Below or Equal  
***OP\_FCMOVNE*** Floating Point Move on Not Equal  
***OP\_FCMOVNU*** Floating Point Move on Not Unordered  
***OP\_FCMOVU*** Floating Point Move on Unordered  
***OP\_FCOM*** Compare Floating Pointer Values and Set FPU Flags  
***OP\_FCOMI*** Compare Floating Pointer Values and Set EFLAGS  
***OP\_FCOMIP*** Compare Floating Pointer Values and Set EFLAGS, Pop  
***OP\_FCOMP*** Compare Floating Pointer Values and Set FPU Flags, Pop  
***OP\_FCOMPP*** Compare Floating Pointer Values and Set FPU Flags, Pop  
Twice

***OP\_FCOS*** Cosine  
***OP\_FDECSTP*** Decrement Stack Top Pointer  
***OP\_FDIV*** Floating Point Divide  
***OP\_FDIVP*** Floating Point Divide, Pop  
***OP\_FDIVR*** Floating Point Reverse Divide  
***OP\_FDIVRP*** Floating Point Reverse Divide, Pop  
***OP\_FFREE*** Free Floating Point Register  
***OP\_FIADD*** Floating Point Add  
***OP\_FICOM*** Compare Integer  
***OP\_FICOMP*** Compare Integer, Pop  
***OP\_FIDIV*** Floating Point Divide by Integer  
***OP\_FIDIVR*** Floating Point Reverse Divide by Integer  
***OP\_FILD*** Load Integer  
***OP\_FIMUL*** Floating Point Multiply with Integer  
***OP\_FINCSTP*** Increment Stack-Top Pointer  
***OP\_FINIT*** Initialize Floating-Point Unit  
***OP\_FIST*** Store Integer  
***OP\_FISTP*** Store Integer, Pop  
***OP\_FISTTP*** Store Integer with Truncation  
***OP\_FISUB*** Floating Point Integer Subtract  
***OP\_FISUBR*** Floating Point Reverse Integer Subtract  
***OP\_FLD*** Load Floating Point Value  
***OP\_FLD1*** Load Constant 1  
***OP\_FLDCW*** Load x87 FPU Control Word  
***OP\_FLDENV*** Load x87 FPU Environment  
***OP\_FLDL2E*** Load Constant  $\log_2(e)$   
***OP\_FLDL2T*** Load Constant  $\log_2(10)$   
***OP\_FLDLG2*** Load Constant  $\log_{10}(2)$   
***OP\_FLDLN2*** Load Constant  $\log_e(2)$   
***OP\_FLDPI*** Load Constant PI  
***OP\_FLDZ*** Load Constant Zero

***OP\_FMUL*** Floating Point Multiply  
***OP\_FMULP*** Floating Point Multiply, Pop  
***OP\_FNOP*** No Operation  
***OP\_FPATAN*** Partial Arctangent  
***OP\_FPREM*** Partial Remainder  
***OP\_FPREMI*** Partial Remainder  
***OP\_FPTAN*** Partial Tangent  
***OP\_FRNDINT*** Round to Integer  
***OP\_FRSTOR*** Restore x86 FPU State  
***OP\_FSCALE*** Scale  
***OP\_FSINCOS*** Sine and Cosine  
***OP\_FSQRT*** Square Root  
***OP\_FSAVE*** Store x87 FPU State  
***OP\_FST*** Store Floating Point Value  
***OP\_FSTCW*** Store x87 FPU Control Word  
***OP\_FSTENV*** Store x87 FPU Environment  
***OP\_FSTP*** Store Floating Point Value, Pop  
***OP\_FSTSW*** Store x87 FPU Status Word  
***OP\_FSUB*** Floating Point Subtract  
***OP\_FSUBP*** Floating Point Subtract, Pop  
***OP\_FSUBR*** Floating Point Reverse Subtract  
***OP\_FSUBRP*** Floating Point Reverse Subtract, Pop  
***OP\_FTST*** Floating Point Test  
***OP\_FUCOM*** Floating Point Unordered Compare  
***OP\_FUCOMI*** Floating Point Unordered Compare with Integer  
***OP\_FUCOMIP*** Floating Point Unorder Compare with Integer, Pop  
***OP\_FUCOMP*** Floating Point Unorder Compare, Pop  
***OP\_FUCOMPP*** Floating Point Unorder Compare, Pop Twice  
***OP\_FXAM*** Examine ModR/M  
***OP\_FXCH*** Exchange Register Contents  
***OP\_FXTRACT*** Extract Exponent and Significand  
***OP\_FYL2X*** Compute  $y \cdot \log_2 x$   
***OP\_FYL2XP1*** Compute  $y \cdot \log_2(x+1)$

#### 7.2.2.2.4. enum X86REGS

X86 registers

### 7.2.3. bytecode\_execs.h File Reference

---

#### Data Structures

- struct [cli\\_exe\\_section](#)
- struct [cli\\_exe\\_info](#)

#### 7.2.3.1. Detailed Description

### 7.2.4. bytecode\_pe.h File Reference

---

#### Data Structures

- struct [pe\\_image\\_file\\_hdr](#)
- struct [pe\\_image\\_data\\_dir](#)
- struct [pe\\_image\\_optional\\_hdr32](#)
- struct [pe\\_image\\_optional\\_hdr64](#)
- struct [pe\\_image\\_section\\_hdr](#)
- struct [cli\\_pe\\_hook\\_data](#)

#### 7.2.4.1. Detailed Description

## 7.3. High level API

---

### 7.3.1. bytecode\_local.h File Reference

---

#### Data Structures

- struct [DIS\\_mem\\_arg](#)
- struct [DIS\\_arg](#)
- struct [DIS\\_fixed](#)

#### Defines

- #define [VIRUSNAME\\_PREFIX](#)(name) const char \_\_clambc\_virusname\_prefix[] = name;
- #define [VIRUSNAMES](#)(...) const char \*const \_\_clambc\_virusnames[] = {\_\_VA\_ARGS\_\_};

- #define SIGNATURES\_DECL\_BEGIN struct \_\_Signatures {
- #define DECLARE\_SIGNATURE(name)
- #define SIGNATURES\_DECL\_END };
- #define TARGET(tgt) const unsigned short \_\_Target = (tgt);
- #define SIGNATURES\_DEF\_BEGIN
- #define DEFINE\_SIGNATURE(name, hex)
- #define SIGNATURES\_END };\

## Functions

- static force\_inline uint32\_t count\_match (\_\_Signature sig)
- static force\_inline uint32\_t matches (\_\_Signature sig)
- static force\_inline void foundVirus (const char \*virusname)
- static force\_inline uint32\_t getFileSize (void)
- bool \_\_is\_bigendian (void) \_\_attribute\_\_((const)) \_\_attribute\_\_((nothrow))
- static uint32\_t force\_inline le32\_to\_host (uint32\_t v)
- static uint16\_t force\_inline le16\_to\_host (uint16\_t v)
- static uint32\_t force\_inline cli\_readint32 (const void \*buff)
- static uint16\_t force\_inline cli\_readint16 (const void \*buff)
- static void force\_inline cli\_writeint32 (void \*offset, uint32\_t v)
- static force\_inline bool hasExeInfo (void)
- static force\_inline bool isPE64 (void)
- static force\_inline uint8\_t getPEMajorLinkerVersion (void)
- static force\_inline uint8\_t getPEMinorLinkerVersion (void)
- static force\_inline uint32\_t getPESizeOfCode (void)
- static force\_inline uint32\_t getPESizeOfInitializedData (void)
- static force\_inline uint32\_t getPESizeOfUninitializedData (void)
- static force\_inline uint32\_t getPEBaseOfCode (void)
- static force\_inline uint32\_t getPEBaseOfData (void)
- static force\_inline uint64\_t getPEImageBase (void)
- static force\_inline uint32\_t getPESectionAlignment (void)
- static force\_inline uint32\_t getPEFileAlignment (void)
- static force\_inline uint16\_t getPEMajorOperatingSystemVersion (void)
- static force\_inline uint16\_t getPEMinorOperatingSystemVersion (void)
- static force\_inline uint16\_t getPEMajorImageVersion (void)
- static force\_inline uint16\_t getPEMinorImageVersion (void)
- static force\_inline uint16\_t getPEMajorSubsystemVersion (void)

- static force\_inline uint16\_t [getPEMinorSubsystemVersion](#) (void)
- static force\_inline uint32\_t [getPEWin32VersionValue](#) (void)
- static force\_inline uint32\_t [getPESizeOfImage](#) (void)
- static force\_inline uint32\_t [getPESizeOfHeaders](#) (void)
- static force\_inline uint32\_t [getPEChecksum](#) (void)
- static force\_inline uint16\_t [getPESubsystem](#) (void)
- static force\_inline uint16\_t [getPEDllCharacteristics](#) (void)
- static force\_inline uint32\_t [getPESizeOfStackReserve](#) (void)
- static force\_inline uint32\_t [getPESizeOfStackCommit](#) (void)
- static force\_inline uint32\_t [getPESizeOfHeapReserve](#) (void)
- static force\_inline uint32\_t [getPESizeOfHeapCommit](#) (void)
- static force\_inline uint32\_t [getPELoaderFlags](#) (void)
- static force\_inline uint16\_t [getPEMachine](#) ()
- static force\_inline uint32\_t [getPEPointerToSymbolTable](#) ()
- static force\_inline uint32\_t [getPENumberOfSymbols](#) ()
- static force\_inline uint16\_t [getPESizeOfOptionalHeader](#) ()
- static force\_inline uint16\_t [getPECharacteristics](#) ()
- static force\_inline uint32\_t [getPEImageDataVA](#) (unsigned n)
- static force\_inline uint32\_t [getPEImageDataSize](#) (unsigned n)
- static force\_inline uint16\_t [getNumberOfSections](#) (void)
- static uint32\_t [getPELFANew](#) (void)
- static force\_inline int [readPESectionName](#) (unsigned char name[8], unsigned n)
- static force\_inline uint32\_t [getEntryPoint](#) (void)
- static force\_inline uint32\_t [getExeOffset](#) (void)
- static force\_inline uint32\_t [getImageBase](#) (void)
- static void \* [memchr](#) (const void \*s, int c, size\_t n)
- void \* [memset](#) (void \*src, int c, uintptr\_t n) \_\_attribute\_\_((nothrow)) \_\_attribute\_\_((nonnull\_\_(1)))
- void \* [memmove](#) (void \*dst, const void \*src, uintptr\_t n) \_\_attribute\_\_((nothrow)) \_\_attribute\_\_((nonnull\_\_(1)))
- void \*void \* [memcpy](#) (void \*restrict dst, const void \*restrict src, uintptr\_t n) \_\_attribute\_\_((nothrow)) \_\_attribute\_\_((nonnull\_\_(1)))
- void \*void \*int [memcmp](#) (const void \*s1, const void \*s2, uint32\_t n) \_\_attribute\_\_((nothrow)) \_\_attribute\_\_((pure)) \_\_attribute\_\_((nonnull\_\_(1)))
- static force\_inline uint32\_t [DisassembleAt](#) (struct [DIS\\_fixed](#) \*result, uint32\_t offset, uint32\_t len)

**7.3.1.1. Detailed Description****7.3.1.2. Define Documentation****7.3.1.2.1. #define DECLARE\_SIGNATURE(name)****Value:**

```
const char *name##_sig;\n    __Signature name;
```

Declares a name for a subsignature

**7.3.1.2.2. #define DEFINE\_SIGNATURE(name, hex)****Value:**

```
.name##_sig = (hex),\n    .name = {__COUNTER__ - __signature_bias},
```

Defines the pattern for a previously declared subsignature.

See also:

[DECLARE\\_SIGNATURE](#)

**Parameters:**

*name* the name of a previously declared subsignature

*hex* the pattern for this subsignature

**7.3.1.2.3. #define SIGNATURES\_DECL\_BEGIN struct \_\_Signatures {**

Marks the beginning of the subsignature name declaration section

**7.3.1.2.4. #define SIGNATURES\_DECL\_END };**

Marks the end of the

subsignature name declaration section

**7.3.1.2.5. #define SIGNATURES\_DEF\_BEGIN****Value:**

```
static const unsigned __signature_bias = __COUNTER__+1;\nconst struct __Signatures Signatures = {\n
```

Marks the beginning of subsignature pattern definitions.

See also:

[SIGNATURES\\_DECL\\_BEGIN](#)



**7.3.1.2.6. #define SIGNATURES\_END ;\** Marks the end of the subsignature pattern definitions.

**7.3.1.2.7. #define TARGET(tgt) const unsigned short \_\_Target = (tgt);** Defines the ClamAV file target.

**Parameters:**

*tgt* ClamAV signature type (0 - raw, 1 - PE, etc.)

**7.3.1.2.8. #define VIRUSNAME\_PREFIX(name) const char \_\_clambc\_virusname\_prefix[] = name;** Declares the virusname prefix.

**Parameters:**

*name* the prefix common to all viruses reported by this bytecode

**7.3.1.2.9. #define VIRUSNAMES( ...) const char \*const \_\_clambc\_virusnames[] = {\_\_VA\_ARGS\_\_};** Declares all the virusnames that this bytecode can report.

**Parameters:**

... a comma-separated list of strings interpreted as virusnames

### 7.3.1.3. Function Documentation

**7.3.1.3.1. bool \_\_is\_bigendian (void) const** Returns true if the bytecode is executing on a big-endian CPU.

**Returns:**

true if executing on bigendian CPU, false otherwise

This will be optimized away in libclamav, but it must be used when dealing with endianness for portability reasons. For example whenever you read a 32-bit integer from a file, it can be written in little-endian convention (x86 CPU for example), or big-endian convention (PowerPC CPU for example). If the file always contains little-endian integers, then conversion might be needed. ClamAV bytecodes by their nature must only handle known-endian integers, if endianness can change, then both situations must be taken into account (based on a 1-byte field for example).

**7.3.1.3.2. static uint16\_t force\_inline cli\_readint16 (const void \* *buff*)**  
**[static]** Reads from the specified buffer a 16-bit of little-endian integer.

**Parameters:**

← *buff* pointer to buffer

**Returns:**

16-bit little-endian integer converted to host endianness

**7.3.1.3.3. static uint32\_t force\_inline cli\_readint32 (const void \* *buff*)**  
**[static]** Reads from the specified buffer a 32-bit of little-endian integer.

**Parameters:**

← *buff* pointer to buffer

**Returns:**

32-bit little-endian integer converted to host endianness

**7.3.1.3.4. static void force\_inline cli\_writeint32 (void \* *offset*, uint32\_t *v*)**  
**[static]** Writes the specified value into the specified buffer in little-endian order

**Parameters:**

→ *offset* pointer to buffer to write to

← *v* value to write

**7.3.1.3.5. static force\_inline uint32\_t count\_match (\_\_Signature *sig*)**  
**[static]** Returns how many times the specified signature matched.

**Parameters:**

*sig* name of subsignature queried

**Returns:**

number of times this subsignature matched in the entire file

This is a constant-time operation, the counts for all subsignatures are already computed.

**7.3.1.3.6. static force\_inline uint32\_t DisassembleAt (struct DIS\_fixed \* *result*, uint32\_t *offset*, uint32\_t *len*) [static]** Disassembles one X86 instruction starting at the specified offset.

**Parameters:**

- *result* disassembly result
- ← *offset* start disassembling from this offset, in the current file
- ← *len* max amount of bytes to disassemble

**Returns:**

offset where disassembly ended

**7.3.1.3.7. static force\_inline void foundVirus (const char \* *virusname*) [static]** Sets the specified virusname as the virus detected by this bytecode.

**Parameters:**

- virusname* the name of the virus, excluding the prefix, must be one of the virusnames declared in VIRUSNAMES.

**See also:**

[VIRUSNAMES](#)

**7.3.1.3.8. static force\_inline uint32\_t getEntryPoint (void) [static]** Returns the offset of the EntryPoint in the executable file.

**Returns:**

offset of EP as 32-bit unsigned integer

**7.3.1.3.9. static force\_inline uint32\_t getExeOffset (void) [static]** Returns the offset of the executable in the file.

**Returns:**

offset of embedded executable inside file.

**7.3.1.3.10. static force\_inline uint32\_t getFilesize (void) [static]** Re-  
turns the currently scanned file's size.

**Returns:**

file size as 32-bit unsigned integer

**7.3.1.3.11. static force\_inline uint32\_t getImageBase (void) [static]**  
Returns the ImageBase with the correct endian conversion

**7.3.1.3.12. static force\_inline uint16\_t getNumberOfSections (void) [static]**  
Returns the number of sections in this executable file.

**Returns:**

number of sections as 16-bit unsigned integer

**7.3.1.3.13. static force\_inline uint32\_t getPEBaseOfCode (void) [static]**  
Return the PE BaseOfCode.

**7.3.1.3.14. static force\_inline uint32\_t getPEBaseOfData (void) [static]**  
Return the PE BaseOfData.

**7.3.1.3.15. static force\_inline uint16\_t getPECharacteristics () [static]**  
Returns PE characteristics.

**7.3.1.3.16. static force\_inline uint32\_t getPEChecksum (void) [static]**  
Return the PE CheckSum.

**7.3.1.3.17. static force\_inline uint16\_t getPEDllCharacteristics (void) [static]**  
Return the PE DllCharacteristics.

**7.3.1.3.18. static force\_inline uint32\_t getPEFileAlignment (void) [static]**  
Return the PE FileAlignment.

**7.3.1.3.19. static force\_inline uint64\_t getPEImageBase (void) [static]**  
Return the PE ImageBase as 64-bit integer.

**7.3.1.3.20. static force\_inline uint32\_t getPEImageDataSize (unsigned *n*) [static]** Gets the size of the specified image data directory.

**Parameters:**

*n* image directory requested

**Returns:**

Size of requested image directory

**7.3.1.3.21. static force\_inline uint32\_t getPEImageDataVA (unsigned *n*) [static]** Gets the virtual address of specified image data directory.

**Parameters:**

*n* image directory requested

**Returns:**

Virtual Address of requested image directory

**7.3.1.3.22. static uint32\_t getPELFANew (void) [static]** Gets the offset to the PE header.

**7.3.1.3.23. static force\_inline uint32\_t getPELoaderFlags (void) [static]**  
Return the PE LoaderFlags.

**7.3.1.3.24. static force\_inline uint16\_t getPEMachine () [static]** Returns the CPU this executable runs on, see libclamav/pe.c for possible values

**7.3.1.3.25. static force\_inline uint16\_t getPEMajorImageVersion (void) [static]**  
Return the PE MajorImageVersion

**7.3.1.3.26. static force\_inline uint8\_t getPEMajorLinkerVersion (void) [static]** Returns MajorLinkerVersion for this PE file.

**7.3.1.3.27. static force\_inline uint16\_t getPEMajorOperatingSystemVersion (void) [static]** Return the PE MajorOperatingSystemVersion.

**7.3.1.3.28. static force\_inline uint16\_t getPEMajorSubsystemVersion (void) [static]** Return the PE MajorSubsystemVersion

**7.3.1.3.29. static force\_inline uint16\_t getPEMinorImageVersion (void) [static]** Return the PE MinorImageVersion

**7.3.1.3.30. static force\_inline uint8\_t getPEMinorLinkerVersion (void) [static]** Returns MinorLinkerVersion for this PE file.

**7.3.1.3.31. static force\_inline uint16\_t getPEMinorOperatingSystemVersion (void) [static]** Return the PE MinorOperatingSystemVersion.

**7.3.1.3.32. static force\_inline uint16\_t getPEMinorSubsystemVersion (void) [static]** Return the PE MinorSubsystemVersion

**7.3.1.3.33. static force\_inline uint32\_t getPENumberOfSymbols () [static]** Returns the PE number of debug symbols

**7.3.1.3.34. static force\_inline uint32\_t getPEPointerToSymbolTable () [static]** Returns pointer to the PE debug symbol table

**7.3.1.3.35. static force\_inline uint32\_t getPESectionAlignment (void) [static]** Return the PE SectionAlignment.

**7.3.1.3.36. static force\_inline uint32\_t getPESizeOfCode (void) [static]** Return the PE SizeOfCode.

**7.3.1.3.37. static force\_inline uint32\_t getPESizeOfHeaders (void)**  
**[static]** Return the PE SizeOfHeaders.

**7.3.1.3.38. static force\_inline uint32\_t getPESizeOfHeapCommit (void)**  
**[static]** Return the PE SizeOfHeapCommit.

**7.3.1.3.39. static force\_inline uint32\_t getPESizeOfHeapReserve (void)**  
**[static]** Return the PE SizeOfHeapReserve.

**7.3.1.3.40. static force\_inline uint32\_t getPESizeOfImage (void) [static]**  
Return the PE SizeOfImage.

**7.3.1.3.41. static force\_inline uint32\_t getPESizeOfInitializedData (void)**  
**[static]** Return the PE SizeofInitializedData.

**7.3.1.3.42. static force\_inline uint16\_t getPESizeOfOptionalHeader ()**  
**[static]** Returns the size of PE optional header.

**7.3.1.3.43. static force\_inline uint32\_t getPESizeOfStackCommit (void)**  
**[static]** Return the PE SizeOfStackCommit.

**7.3.1.3.44. static force\_inline uint32\_t getPESizeOfStackReserve (void)**  
**[static]** Return the PE SizeOfStackReserve.

**7.3.1.3.45. static force\_inline uint32\_t getPESizeOfUninitializedData (void)**  
**[static]** Return the PE SizeofUninitializedData.

**7.3.1.3.46. static force\_inline uint16\_t getPESubsystem (void) [static]**  
Return the PE Subsystem.

**7.3.1.3.47. static force\_inline uint32\_t getPEWin32VersionValue (void)**  
**[static]** Return the PE Win32VersionValue.

**7.3.1.3.48. static force\_inline bool hasExeInfo (void) [static]** Returns whether the current file has executable information.

**Returns:**

true if the file has exe info, false otherwise

**7.3.1.3.49. static force\_inline bool isPE64 (void) [static]** Returns whether this is a PE32+ executable.

**Returns:**

true if this is a PE32+ executable

**7.3.1.3.50. static uint16\_t force\_inline le16\_to\_host (uint16\_t v) [static]** Converts the specified value if needed, knowing it is in little endian order.

**Parameters:**

← *v* 16-bit integer as read from a file

**Returns:**

integer converted to host's endianness

**7.3.1.3.51. static uint32\_t force\_inline le32\_to\_host (uint32\_t v) [static]** Converts the specified value if needed, knowing it is in little endian order.

**Parameters:**

← *v* 32-bit integer as read from a file

**Returns:**

integer converted to host's endianness

**7.3.1.3.52. static force\_inline uint32\_t matches (\_\_Signature sig) [static]** Returns whether the specified subsignature has matched at least once.

**Parameters:**

*sig* name of subsignature queried

**Returns:**

1 if subsignature one or more times, 0 otherwise



**7.3.1.3.53. static void\* memchr (const void \* *s*, int *c*, size\_t *n*) [static]**  
Scan the first *n* bytes of the buffer *s*, for the character *c*.

**Parameters:**

- ← *s* buffer to scan
- c* character to look for
- n* size of buffer

**Returns:**

a pointer to the first byte to match, or NULL if not found.

**7.3.1.3.54. void\* void\* int memcmp (const void \* *s1*, const void \* *s2*, uint32\_t *n*)**  
Compares two memory buffers.

**Parameters:**

- ← *s1* buffer one
- ← *s2* buffer two
- ← *n* amount of bytes to copy

**Returns:**

an integer less than, equal to, or greater than zero if the first *n* bytes of *s1* are found, respectively, to be less than, to match, or be greater than the first *n* bytes of *s2*.

**7.3.1.3.55. void\* void\* memcpy (void \*restrict *dst*, const void \*restrict *src*, uintptr\_t *n*)**  
Copies data between two non-overlapping buffers.

**Parameters:**

- *dst* destination buffer
- ← *src* source buffer
- ← *n* amount of bytes to copy

**Returns:**

*dst*

**7.3.1.3.56. void\* memmove (void \* *dst*, const void \* *src*, uintptr\_t *n*)**  
Copies data between two possibly overlapping buffers.

**Parameters:**

- *dst* destination buffer
- ← *src* source buffer
- ← *n* amount of bytes to copy

**Returns:**

*dst*

**7.3.1.3.57. void\* memset (void \* *src*, int *c*, uintptr\_t *n*)** Fills the specified buffer to the specified value.

**Parameters:**

- *src* pointer to buffer
- ← *c* character to fill buffer with
- ← *n* length of buffer

**Returns:**

*src*

**7.3.1.3.58. static force\_inline int readPESectionName (unsigned char *name*[8], unsigned *n*) [static]** Read name of requested PE section.

**Parameters:**

- *name* name of PE section
- ← *n* PE section requested

**Returns:**

0 if successful, <0 otherwise

DRAFT

## CHAPTER 8

# Copyright and License

---

### 8.1. The ClamAV Bytecode Compiler

---

The ClamAV Bytecode Compiler is released under the GNU General Public License version 2.

The following directories are under the GNU General Public License version 2: ClamBC, docs, driver, editor, examples, ifacegen.

Copyright (C) 2009 Sourcefire, Inc.

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License version 2 as published by the Free Software Foundation.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA.

It uses the LLVM compiler framework, contained in the following directories: llvm, clang. They have this copyright:

```
=====
LLVM Release License
=====
```

```
University of Illinois/NCSA
Open Source License
```

```
Copyright (c) 2003-2009 University of Illinois at Urbana-Champaign.
All rights reserved.
```

Developed by:

LLVM Team

University of Illinois at Urbana-Champaign

<http://llvm.org>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal with the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

- \* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimers.
- \* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimers in the documentation and/or other materials provided with the distribution.
- \* Neither the names of the LLVM Team, University of Illinois at Urbana-Champaign, nor the names of its contributors may be used to endorse or promote products derived from this Software without specific prior written permission.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE CONTRIBUTORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS WITH THE SOFTWARE.

=====  
Copyrights and Licenses for Third Party Software Distributed with LLVM:  
=====

The LLVM software contains code written by third parties. Such software will have its own individual LICENSE.TXT file in the directory in which it appears. This file will describe the copyrights, license, and restrictions which apply to that code.

The disclaimer of warranty in the University of Illinois Open Source License applies to all code in the LLVM Distribution, and nothing in any of the other licenses gives permission to use the names of the LLVM Team or the University of Illinois to endorse or promote products derived from this Software.

The following pieces of software have additional or alternate copyrights, licenses, and/or restrictions:

Program	Directory
-----	-----
Autoconf	llvm/autoconf llvm/projects/ModuleMaker/autoconf llvm/projects/sample/autoconf
CellSPU backend	llvm/lib/Target/CellSPU/README.txt
Google Test	llvm/utils/unittest/googletest
OpenBSD regex	llvm/lib/Support/{reg*, COPYRIGHT.regex}

It also uses re2c, contained in driver/clamdriver/re2c. This code is public domain:

Originally written by Peter Bumbulis (peter@csg.uwaterloo.ca)

Currently maintained by:

- \* Dan Nuffer <nuffer@users.sourceforge.net>
- \* Marcus Boerger <helly@users.sourceforge.net>
- \* Hartmut Kaiser <hkaiser@users.sourceforge.net>

The re2c distribution can be found at:

<http://sourceforge.net/projects/re2c/>

re2c is distributed with no warranty whatever. The code is certain to contain errors. Neither the author nor any contributor takes responsibility for any consequences of its use.

re2c is in the public domain. The data structures and algorithms used in re2c are all either taken from documents available to the general public or are inventions of the author. Programs generated by re2c may be distributed freely. re2c itself may be distributed freely, in source or binary, unchanged or modified. Distributors may charge whatever fees they can obtain for re2c.

If you do make use of re2c, or incorporate it into a larger project an acknowledgement somewhere (documentation, research report, etc.) would be appreciated.

## 8.2. Bytecode

The headers used when compiling bytecode have these license (clang/lib/Headers/{bcfeatures, bytecode\*}.h):

Copyright (C) 2009 Sourcefire, Inc.  
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

**The other header files in clang/lib/Headers/ are from clang with this license (see individual files for copyright owner):**

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

**When using the ClamAV bytecode compiler to compile your own bytecode programs, you can release it under the license of your choice, provided that you comply with the license of the above header files.**

## APPENDIX A

# Predefined macros

---

```
1 #define __llvm__ 1
2 #define __clang__ 1
3 #define __GNUC_MINOR__ 2
4 #define __GNUC_PATCHLEVEL__ 1
5 #define __GNUC__ 4
6 #define __GXX_ABI_VERSION 1002
7 #define __VERSION__ "4.2.1 Compatible Clang Compiler"
8 #define __STDC__ 1
9 #define __STDC_VERSION__ 199901L
10 #define __STDC_HOSTED__ 0
11 #define __CONSTANT_CFSTRINGS__ 1
12 #define __CHAR_BIT__ 8
13 #define __SCHAR_MAX__ 127
14 #define __SHRT_MAX__ 32767
15 #define __INT_MAX__ 2147483647
16 #define __LONG_MAX__ 9223372036854775807L
17 #define __LONG_LONG_MAX__ 9223372036854775807LL
18 #define __WCHAR_MAX__ 2147483647
19 #define __INTMAX_MAX__ 9223372036854775807L
20 #define __INTMAX_TYPE__ long int
21 #define __UINTMAX_TYPE__ long unsigned int
22 #define __INTMAX_WIDTH__ 64
23 #define __PTRDIFF_TYPE__ int
24 #define __PTRDIFF_WIDTH__ 32
25 #define __INTPTR_TYPE__ long int
26 #define __INTPTR_WIDTH__ 64
27 #define __SIZE_TYPE__ unsigned int
28 #define __SIZE_WIDTH__ 32
29 #define __WCHAR_TYPE__ int
30 #define __WCHAR_WIDTH__ 32
31 #define __WINT_TYPE__ int
32 #define __WINT_WIDTH__ 32
33 #define __SIG_ATOMIC_WIDTH__ 32
34 #define __FLT_DENORM_MIN__ 1.40129846e-45F
35 #define __FLT_HAS_DENORM__ 1
36 #define __FLT_DIG__ 6
37 #define __FLT_EPSILON__ 1.19209290e-7F
38 #define __FLT_HAS_INFINITY__ 1
39 #define __FLT_HAS_QUIET_NAN__ 1
40 #define __FLT_MANT_DIG__ 24
41 #define __FLT_MAX_10_EXP__ 38
42 #define __FLT_MAX_EXP__ 128
43 #define __FLT_MAX__ 3.40282347e+38F
44 #define __FLT_MIN_10_EXP__ (-37)
45 #define __FLT_MIN_EXP__ (-125)
46 #define __FLT_MIN__ 1.17549435e-38F
47 #define __DBL_DENORM_MIN__ 4.9406564584124654e-324
48 #define __DBL_HAS_DENORM__ 1
49 #define __DBL_DIG__ 15
50 #define __DBL_EPSILON__ 2.2204460492503131e-16
51 #define __DBL_HAS_INFINITY__ 1
52 #define __DBL_HAS_QUIET_NAN__ 1
53 #define __DBL_MANT_DIG__ 53
54 #define __DBL_MAX_10_EXP__ 308
55 #define __DBL_MAX_EXP__ 1024
56 #define __DBL_MAX__ 1.7976931348623157e+308
57 #define __DBL_MIN_10_EXP__ (-307)
58 #define __DBL_MIN_EXP__ (-1021)
59 #define __DBL_MIN__ 2.2250738585072014e-308
60 #define __LDBL_DENORM_MIN__ 4.9406564584124654e-324
61 #define __LDBL_HAS_DENORM__ 1
```



```

#define __LDBL_DIG__ 15
63 #define __LDBL_EPSILON__ 2.2204460492503131e-16
#define __LDBL_HAS_INFINITY__ 1
65 #define __LDBL_HAS_QUIET_NAN__ 1
#define __LDBL_MANT_DIG__ 53
67 #define __LDBL_MAX_10_EXP__ 308
#define __LDBL_MAX_EXP__ 1024
69 #define __LDBL_MAX__ 1.7976931348623157e+308
#define __LDBL_MIN_10_EXP__ (-307)
71 #define __LDBL_MIN_EXP__ (-1021)
#define __LDBL_MIN__ 2.2250738585072014e-308
73 #define __POINTER_WIDTH__ 64
#define __INT8_TYPE__ char
75 #define __INT16_TYPE__ short
#define __INT32_TYPE__ int
77 #define __INT64_TYPE__ long int
#define __INT64_C_SUFFIX__ L
79 #define __USER_LABEL_PREFIX__ _
#define __FINITE_MATH_ONLY__ 0
81 #define __GNUC_STDC_INLINE__ 1
#define __NO_INLINE__ 1
83 #define __FLT_EVAL_METHOD__ 0
#define __FLT_RADIX__ 2
85 #define __DECIMAL_DIG__ 17
#define __CLAMBC__ 1
87 #define BYTECODE_API_H
#define __EXECS_H
89 #define BC_FEATURES_H
#define EBOUNDS(x)
91 #define __PE_H
#define DISASM_BC_H
93 #define __STDBOOL_H
#define bool _Bool
95 #define true 1
#define false 0
97 #define __bool_true_false_are_defined 1
#define force_inline inline __attribute__((always_inline))
99 #define VIRUSNAME_PREFIX(name) const char __clambc_virusname_prefix[] = name;
#define VIRUSNAMES(...) const char *const __clambc_virusnames[] = {__VA_ARGS__};
101 #define PE_UNPACKER_DECLARE const uint16_t __clambc_kind = BC_PE_UNPACKER;
#define SIGNATURES_DECL_BEGIN struct __Signatures {
103 #define DECLARE_SIGNATURE(name) const char *name##_sig; __Signature name;
#define SIGNATURES_DECL_END };
105 #define TARGET(tgt) const unsigned short __Target = (tgt);
#define SIGNATURES_DEF_BEGIN static const unsigned __signature_bias = __COUNTER__ + 1; const struct
__Signatures Signatures = {
107 #define DEFINE_SIGNATURE(name, hex) .name##_sig = (hex), .name = {__COUNTER__ - __signature_bias,
#define SIGNATURES_END };
109 #define RE2C_BSIZE 128
#define YYCTYPE unsigned char
111 #define YYCURSOR re2c_scur
#define YYLIMIT re2c_slim
113 #define YYMARKER re2c_smrk
#define YYCONTEXT re2c_sctx
115 #define YYPILL(n) { RE2C_FILLBUFFER(n); if (re2c_sres <= 0) break;}
#define REGEX_SCANNER unsigned char *re2c_scur, *re2c_stok, *re2c_smrk, *re2c_sctx, *re2c_slim; int
re2c_sres; int32_t re2c_stokstart; unsigned char re2c_sbuffer[RE2C_BSIZE]; re2c_scur = re2c_slim =
re2c_smrk = re2c_sctx = &re2c_sbuffer[0]; re2c_sres = 0; RE2C_FILLBUFFER(0);
117 #define REGEX_POS (-(re2c_slim - re2c_scur) + seek(0, SEEK_CUR))
#define REGEX_LOOP_BEGIN do { re2c_stok = re2c_scur; re2c_stokstart = REGEX_POS; } while (0);
119 #define REGEX_RESULT (re2c_sres)
#define RE2C_DEBUG_PRINT do { char buf[81]; uint32_t here = seek(0, SEEK_CUR); uint32_t d = re2c_slim -
re2c_scur; uint32_t end = here - d; unsigned len = end - re2c_stokstart; if (len > 80) { unsigned
skipped = len - 74; seek(re2c_stokstart, SEEK_SET); if (read(buf, 37) == 37) break; memcpy(buf+37,
"[...]", 5); seek(end-37, SEEK_SET); if (read(buf, 37) != 37) break; buf[80] = '\0'; } else {
seek(re2c_stokstart, SEEK_SET); if (read(buf, len) != len) break; buf[len] = '\0'; } buf[80] = '\0';
debug_print_str(buf, 0); seek(here, SEEK_SET); } while (0)
121 #define DEBUG_PRINT_REGEX_MATCH RE2C_DEBUG_PRINT
#define BUFFER_FILL(buf, cursor, need, limit) do { (limit) = fill_buffer((buf), sizeof((buf)), (limit),
(cursor), (need)); } while (0);
123 #define BUFFER_ENSURE(buf, cursor, need, limit) do { if ((cursor) + (need) >= (limit)) { BUFFER_FILL(buf,
cursor, need, limit) (cursor) = 0; } } while (0);
#define RE2C_FILLBUFFER(need) do { uint32_t cursor = re2c_stok - &re2c_sbuffer[0]; int32_t limit =
re2c_slim - &re2c_sbuffer[0]; limit = fill_buffer(re2c_sbuffer, sizeof(re2c_sbuffer), limit,
(cursor), (need)); if (!limit) { re2c_sres = 0; } else if (limit <= (need)) { re2c_sres = -1; } else
{ uint32_t curoff = re2c_scur - re2c_stok; uint32_t mrkoff = re2c_smrk - re2c_stok; uint32_t ctxoff =
re2c_sctx - re2c_stok; re2c_slim = &re2c_sbuffer[0] + limit; re2c_stok = &re2c_sbuffer[0]; re2c_scur
= &re2c_sbuffer[0] + curoff; re2c_smrk = &re2c_sbuffer[0] + mrkoff; re2c_sctx = &re2c_sbuffer[0] +
ctxoff; re2c_sres = limit; } } while (0);

```