

List object file contents

```
$ cat hello.c # List example C file
#include <stdio.h>

int global;
static int local;

static void localfun() { }

main()
{
    fprintf(stdout, "hello, world: %p\n", localfun);
}
$ cc -c hello.c # Compile the file into object format
$ nm hello.o # List symbols in object file
                 U fprintf
0000000000000004 C global
0000000000000000 b local
0000000000000000 t localfun
0000000000000006 T main
                 U stdout
$
```

List executable file contents

```
$ cc -o hello hello.c # Compile and link file into executable
$ nm hello | head # List first ten symbols
00000000000600990 B __bss_start
00000000000600998 b completed.6661
00000000000600980 D __data_start
00000000000600980 W data_start
0000000000400480 t deregister_tm_clones
0000000000400500 t __do_global_dtors_aux
0000000000600768 t __do_global_dtors_aux_fini_array_entry
0000000000600988 D __dso_handle
0000000000600778 d _DYNAMIC
0000000000600990 D _edata
$ strip hello # Remove symbols
$ nm hello # Attempt to list symbols
nm: hello: no symbols
$ nm /bin/ls # Attempt to list symbols
nm: /bin/ls: no symbols
$
```

File with most global variables

```
$ nm -o $(find . -name \*.o) | head -3 # Run nm on all .o files
./modules/standard/mod_dir.o:00000000 t add_index
./modules/standard/mod_dir.o:          U ap_construct_url
./modules/standard/mod_dir.o:          U ap_destroy_sub_req
$ nm -o $(find . -name \*.o) |
> grep ' D ' | head -3 # Obtain only uninitialized global data definitions
./modules/standard/mod_dir.o:00000000 D dir_module
./modules/standard/mod_actions.o:00000000 D action_module
./modules/standard/mod_auth.o:00000000 D auth_module
$ nm -o $(find . -name \*.o) |
> grep ' D ' |
> cut -d: -f 1 | head -3 # Get file name
./modules/standard/mod_dir.o
./modules/standard/mod_actions.o
./modules/standard/mod_auth.o
$ nm -o $(find . -name \*.o) |
> grep ' D ' |
> cut -d: -f 1 |
> sort | uniq -c | sort -rn | head -5 # Order by number of global variables
 37 ./main/http_main.o
   2 ./modules.o
```

```
2 ./main/http_config.o
1 ./modules/standard/mod_userdir.o
1 ./modules/standard/mod_status.o
$
```

Find shared libraries

```
$ ldd /bin/ls # List dynamically linked libraries
linux-vdso.so.1 (0x00007ffe99964000)
libselinux.so.1 => /lib/x86_64-linux-gnu/libselinux.so.1 (0x00007f118c6b4000)
libacl.so.1 => /lib/x86_64-linux-gnu/libacl.so.1 (0x00007f118c4ab000)
libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007f118c102000)
libpcre.so.3 => /lib/x86_64-linux-gnu/libpcre.so.3 (0x00007f118be94000)
libdl.so.2 => /lib/x86_64-linux-gnu/libdl.so.2 (0x00007f118bc90000)
/lib64/ld-linux-x86-64.so.2 (0x00007f118c8d9000)
libattr.so.1 => /lib/x86_64-linux-gnu/libattr.so.1 (0x00007f118ba8b000)
libpthread.so.0 => /lib/x86_64-linux-gnu/libpthread.so.0 (0x00007f118b86e000)
$ ldd /bin/* | # Obtain shared libraries of all files
> sed 's/.*=>///;s/^\s*///;s/ .*//' | # Get absolute library path
> sort | uniq -c | sort -rn | head # Count
108 linux-vdso.so.1
108 /lib/x86_64-linux-gnu/libc.so.6
108 /lib64/ld-linux-x86-64.so.2
32 /lib/x86_64-linux-gnu/libdl.so.2
30 /lib/x86_64-linux-gnu/libpthread.so.0
29 not
21 /lib/x86_64-linux-gnu/libpcre.so.3
20 /lib/x86_64-linux-gnu/libselinux.so.1
15 /lib/x86_64-linux-gnu/libattr.so.1
11 /lib/x86_64-linux-gnu/libacl.so.1
$
```

List Java compiled files

```
$ javap -cp antlr-3.4-complete.jar org/antlr/runtime/ANTLRFileStream
Compiled from "ANTLRFileStream.java"
public class org.antlr.runtime.ANTRFileStream extends org.antlr.runtime.ANTRStringStream {
    protected java.lang.String fileName;
    public org.antlr.runtime.ANTRFileStream(java.lang.String) throws java.io.IOException;
    public org.antlr.runtime.ANTRFileStream(java.lang.String, java.lang.String) throws java.io.
IOException;
    public void load(java.lang.String, java.lang.String) throws java.io.IOException;
    public java.lang.String getSourceName();
}
$
```

List Windows compiled files

```
$ cd /cygdrive/c/Windows/
$ dumpbin /imports notepad.exe | head -20 # List imported symbols
Microsoft (R) COFF/PE Dumper Version 10.00.40219.01
Copyright (C) Microsoft Corporation. All rights reserved.
```

Dump of file notepad.exe

File Type: EXECUTABLE IMAGE

Section contains the following imports:

```
ADVAPI32.dll
    1000C000 Import Address Table
    1000D1E8 Import Name Table
    FFFFFFFF time date stamp
    FFFFFFFF Index of first forwarder reference

7FF7FF247B0    27F RegSetValueExW
7FF7FF2F050    26F RegQueryValueExW
```

```
7FF7FF247E0 23D RegCreateKeyW
7FF7FF34DE0 231 RegCloseKey
$ cd /cygdrive/c/Windows/System32
$ dumpbin /exports wsock32.dll | head -22 # List exported symbols
Microsoft (R) COFF/PE Dumper Version 10.00.40219.01
Copyright (C) Microsoft Corporation. All rights reserved.
```

Dump of file wsock32.dll

File Type: DLL

Section contains the following exports for WSOCK32.dll

```
00000000 characteristics
4A5BC955 time date stamp Tue Jul 14 02:55:01 2009
0.00 version
1 ordinal base
1142 number of functions
75 number of names
```

ordinal	hint	RVA	name
1141	0		AcceptEx (forwarded to MSWSOCK.AcceptEx)
1111	1		EnumProtocolsA (forwarded to MSWSOCK.EnumProtocolsA)
1112	2		EnumProtocolsW (forwarded to MSWSOCK.EnumProtocolsW)

\$