Maladjusted
Hiding malware in plain sight

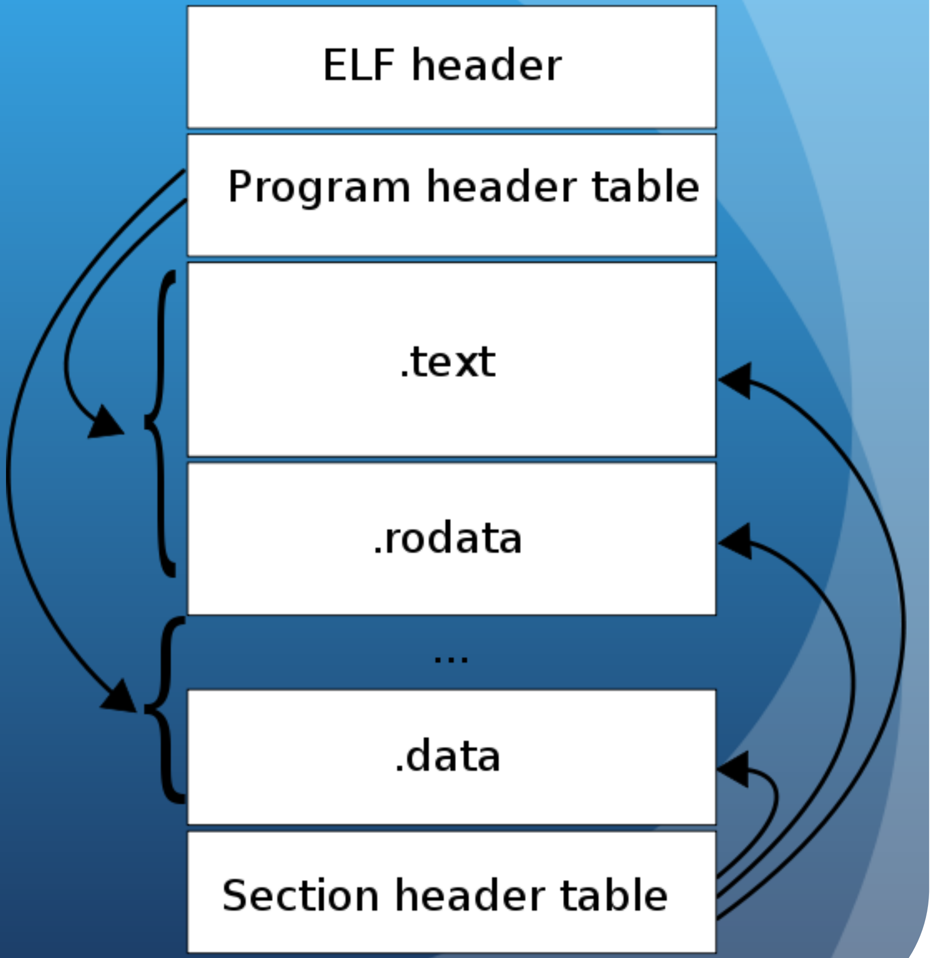
Eric Gragsone

How Unix Executables Work

Unix executables are split up into different parts based on their functionality.

Instruction code that dictates how a program functions is called Text.

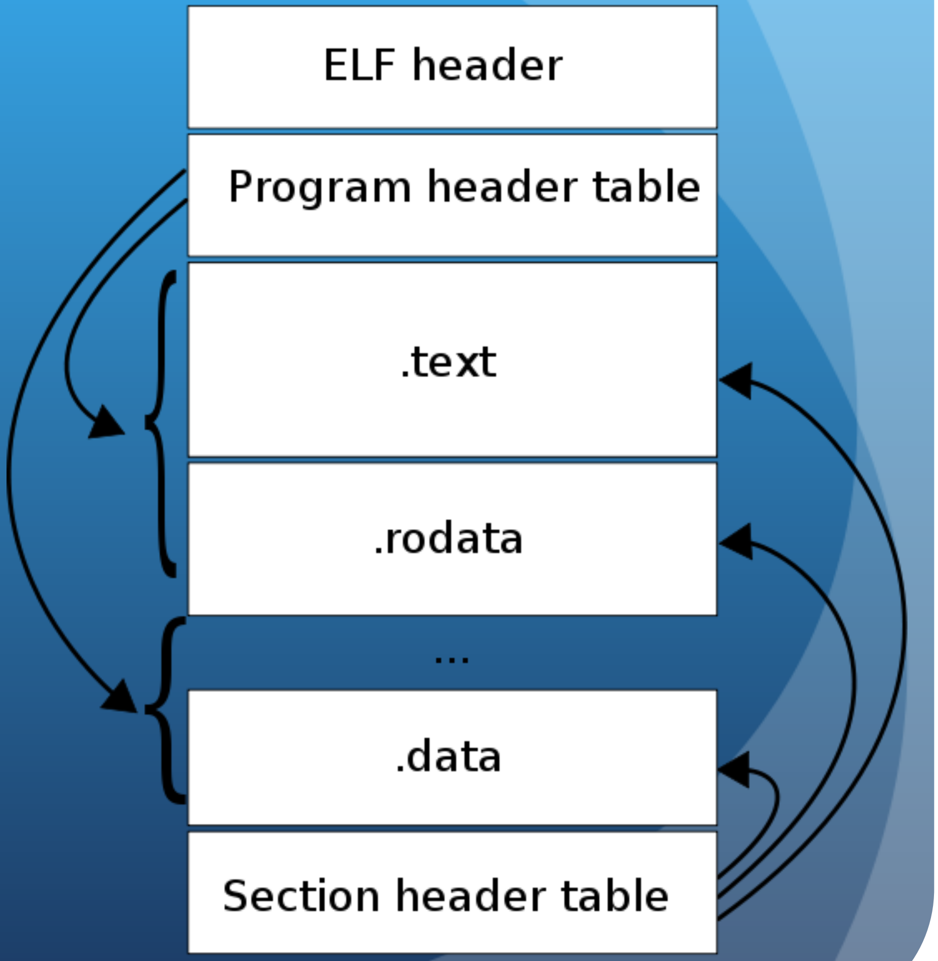
Values used to initiate variables is called Data. This part of the program is where the 'strings' utility looks into by default.



How Unix Executables Work

The Program and Section headers keep track of the different executable parts, both their offset in the file and the offset to load them in memory.

Additionally the ELF header keeps track of the location of these headers. The entire structure is referred to as an ELF executable.

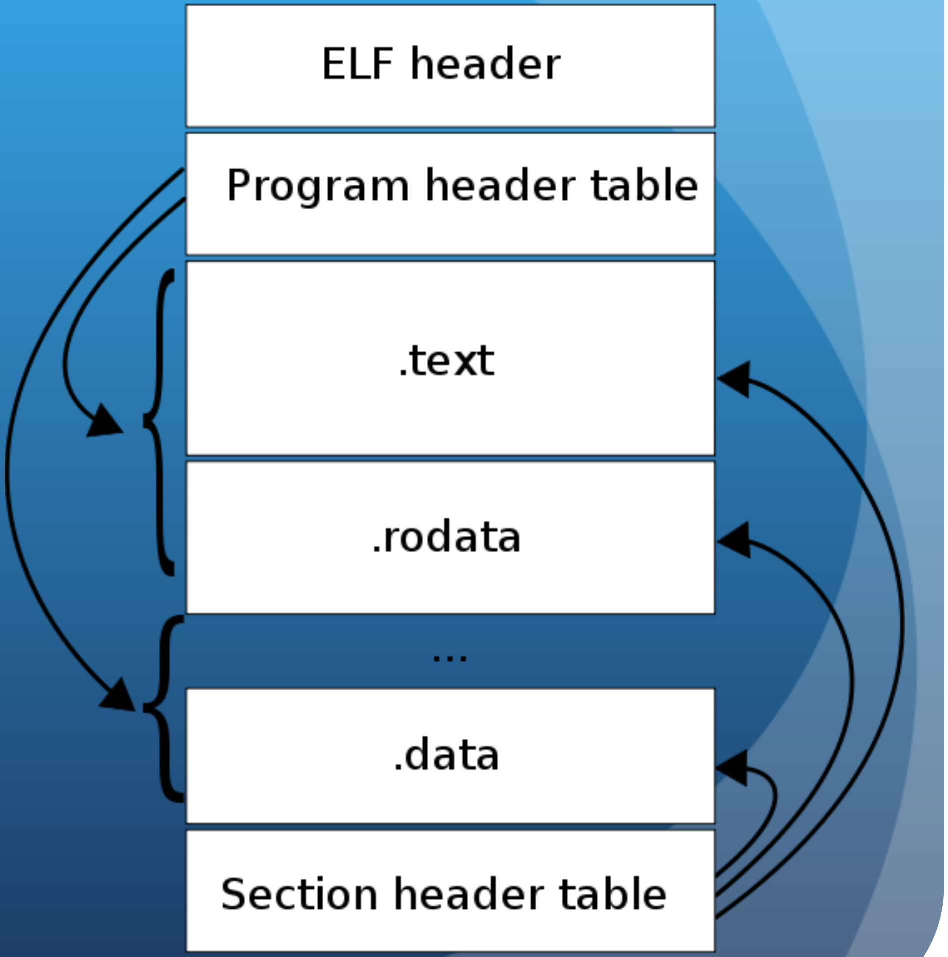


How Unix Executables Work

ELF File structure contains two ways to view the program.

Linkers (used for libraries) and Debuggers utilize the Section Header to dissect the file into numerous "sections."

However Loaders (used for executables) use the Program Header to dissect the file into a few "segments."



Maladjusted (2002)

Created a tool to prevent libBFD based programs (objdump & GDB) from analyzing ELF executables using my knowledge of the ELF file structure and the inner workings of Loader/Linkers.

Source:
http://dmca.cvs.sourceforge.net/viewvc/dmca/resh/swdev/DMCA/maladjusted/?view=tar

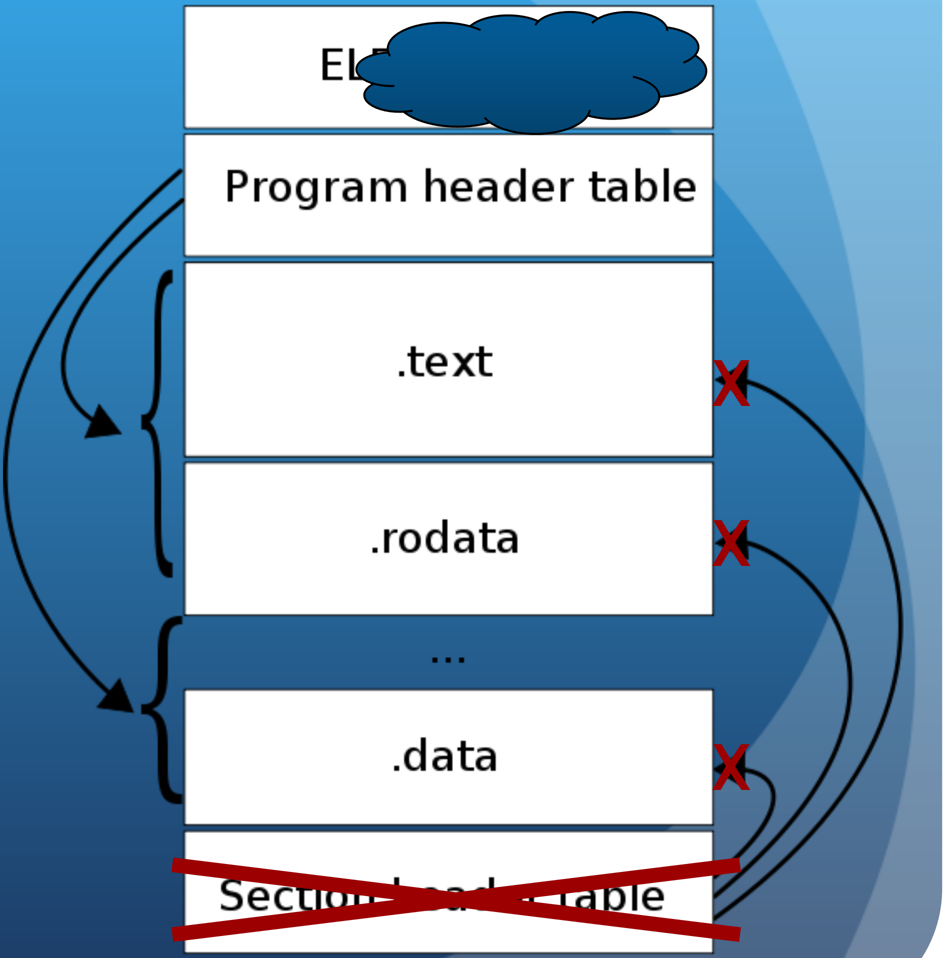
ELF Binary:
http://sourceforge.net/projects/dmca/files/test/maladjusted-i386-bin/maladjusted/download

Ten years later this technique still works.

How Maladjusted Works

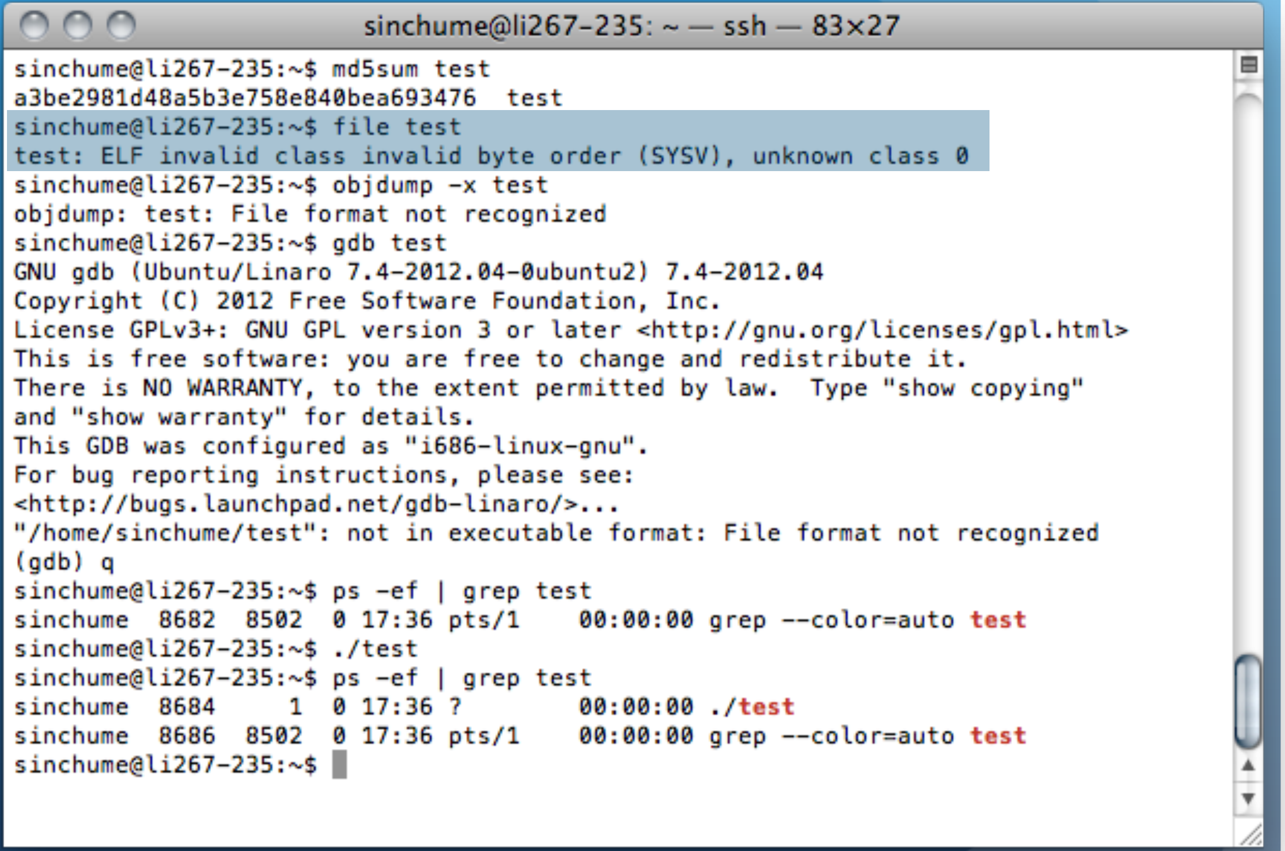
Maladjusted removes a program Section Header in order to blind libBFD based dissectors.

Additionally, Maladjusted mangles the ELF header just for good measure.



Maladjusted (2002)

File detects the ELF Magic bytes, but unable to recognize anything beyond that.

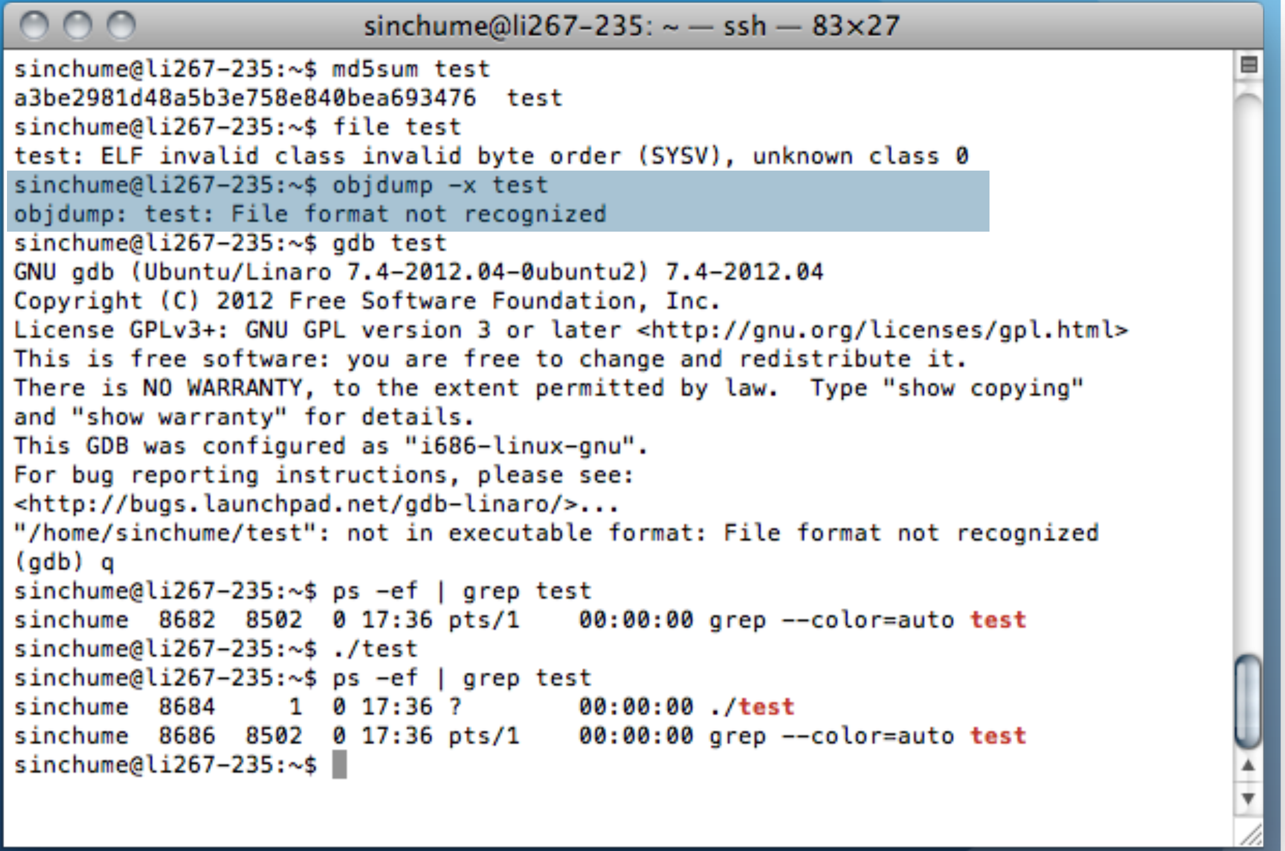


```
sinchume@li267-235:~$ md5sum test
a3be2981d48a5b3e758e840bea693476  test
sinchume@li267-235:~$ file test
test: ELF invalid class invalid byte order (SYSV), unknown class 0
sinchume@li267-235:~$ objdump -x test
objdump: test: File format not recognized
sinchume@li267-235:~$ gdb test
GNU gdb (Ubuntu/Linaro 7.4-2012.04-0ubuntu2) 7.4-2012.04
Copyright (C) 2012 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "i686-linux-gnu".
For bug reporting instructions, please see:
<http://bugs.launchpad.net/gdb-linaro/>...
"/home/sinchume/test": not in executable format: File format not recognized
(gdb) q
sinchume@li267-235:~$ ps -ef | grep test
sinchume  8682  8502  0 17:36 pts/1    00:00:00 grep --color=auto test
sinchume@li267-235:~$ ./test
sinchume@li267-235:~$ ps -ef | grep test
sinchume  8684     1  0 17:36 ?        00:00:00 ./test
sinchume  8686  8502  0 17:36 pts/1    00:00:00 grep --color=auto test
sinchume@li267-235:~$ 
```

Maladjusted (2002)

Objdump is completely unable to retrieve any information about this file.

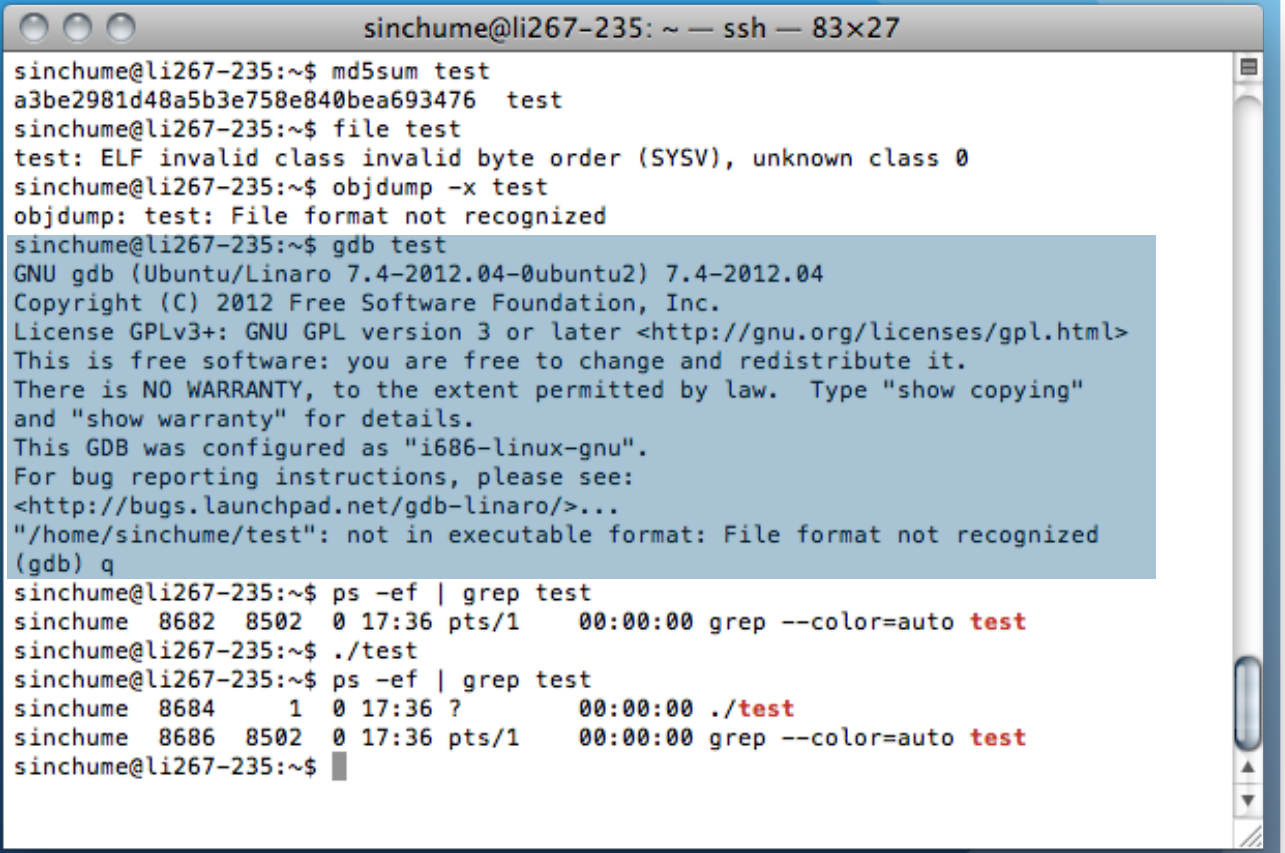
Note: Objdump fails even when explicitly told the file format with option ‘-b elf32-386’



```
sinchume@li267-235:~$ md5sum test
a3be2981d48a5b3e758e840bea693476  test
sinchume@li267-235:~$ file test
test: ELF invalid class invalid byte order (SYSV), unknown class 0
sinchume@li267-235:~$ objdump -x test
objdump: test: File format not recognized
sinchume@li267-235:~$ gdb test
GNU gdb (Ubuntu/Linaro 7.4-2012.04-0ubuntu2) 7.4-2012.04
Copyright (C) 2012 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "i686-linux-gnu".
For bug reporting instructions, please see:
<http://bugs.launchpad.net/gdb-linaro/>...
"/home/sinchume/test": not in executable format: File format not recognized
(gdb) q
sinchume@li267-235:~$ ps -ef | grep test
sinchume  8682  8502  0 17:36 pts/1    00:00:00 grep --color=auto test
sinchume@li267-235:~$ ./test
sinchume@li267-235:~$ ps -ef | grep test
sinchume  8684     1  0 17:36 ?        00:00:00 ./test
sinchume  8686  8502  0 17:36 pts/1    00:00:00 grep --color=auto test
sinchume@li267-235:~$ 
```

Maladjusted (2002)

Gnu Debugger 7.4 (my favorite debugger) states that this file is not in executable format.

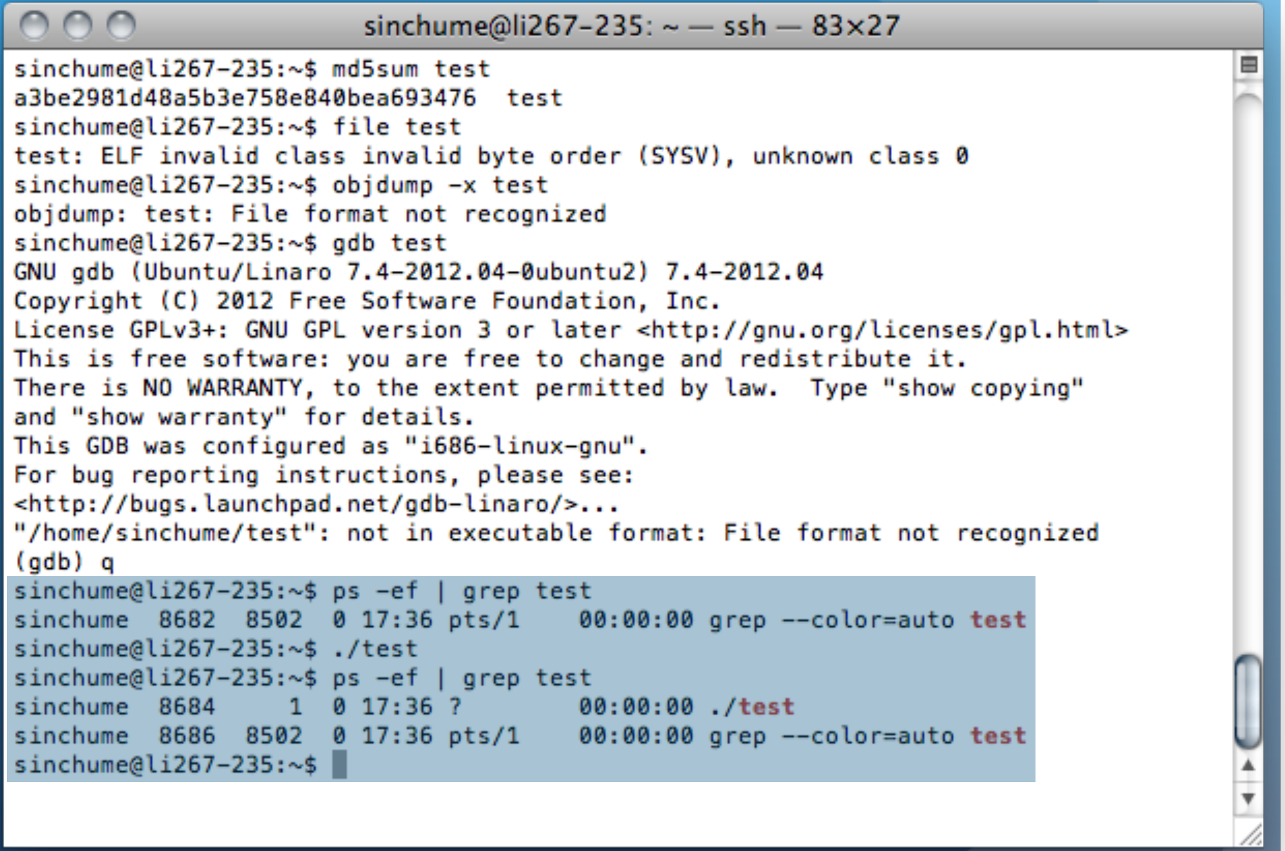


```
sinchume@li267-235:~$ md5sum test
a3be2981d48a5b3e758e840bea693476  test
sinchume@li267-235:~$ file test
test: ELF invalid class invalid byte order (SYSV), unknown class 0
sinchume@li267-235:~$ objdump -x test
objdump: test: File format not recognized
sinchume@li267-235:~$ gdb test
GNU gdb (Ubuntu/Linaro 7.4-2012.04-0ubuntu2) 7.4-2012.04
Copyright (C) 2012 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "i686-linux-gnu".
For bug reporting instructions, please see:
<http://bugs.launchpad.net/gdb-linaro/>...
"/home/sinchume/test": not in executable format: File format not recognized
(gdb) q
sinchume@li267-235:~$ ps -ef | grep test
sinchume  8682  8502  0 17:36 pts/1    00:00:00 grep --color=auto test
sinchume@li267-235:~$ ./test
sinchume@li267-235:~$ ps -ef | grep test
sinchume  8684     1  0 17:36 ?        00:00:00 ./test
sinchume  8686  8502  0 17:36 pts/1    00:00:00 grep --color=auto test
sinchume@li267-235:~$ 
```

Maladjusted (2002)

Yet the file is recognized by the loader and is executed correctly.

Sadly, IDA Pro is able to correctly disassemble this file without manual loading.

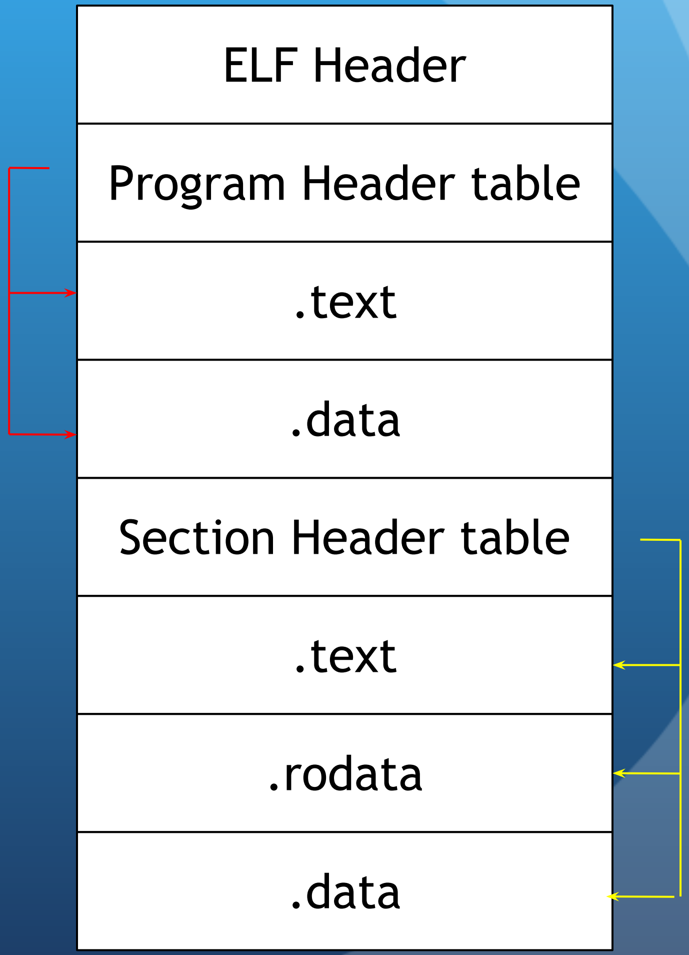


```
sinchume@li267-235:~$ md5sum test
a3be2981d48a5b3e758e840bea693476  test
sinchume@li267-235:~$ file test
test: ELF invalid class invalid byte order (SYSV), unknown class 0
sinchume@li267-235:~$ objdump -x test
objdump: test: File format not recognized
sinchume@li267-235:~$ gdb test
GNU gdb (Ubuntu/Linaro 7.4-2012.04-0ubuntu2) 7.4-2012.04
Copyright (C) 2012 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "i686-linux-gnu".
For bug reporting instructions, please see:
<http://bugs.launchpad.net/gdb-linaro/>...
"/home/sinchume/test": not in executable format: File format not recognized
(gdb) q
sinchume@li267-235:~$ ps -ef | grep test
sinchume  8682  8502  0 17:36 pts/1    00:00:00 grep --color=auto test
sinchume@li267-235:~$ ./test
sinchume@li267-235:~$ ps -ef | grep test
sinchume  8684     1  0 17:36 ?        00:00:00 ./test
sinchume  8686  8502  0 17:36 pts/1    00:00:00 grep --color=auto test
sinchume@li267-235:~$ 
```

The Future?

Based on this experience

Can we append a benign program and have the Section Header point to it in order to completely hide the malicious program?



ELF Header

Program Header table

.text

.data

Section Header table

.text

.rodata

.data