

GDB

```
set disassembly-flavor intel
$ cat ~/.bash_aliases | grep gdb
alias gdb='gdb -quiet'

Running gdb
-----
$ gdb      ■■- run, then use file command to load object
$ gdb -quiet      - supress copyright information
$ gdb object      ■- normal debug
$ gdb object core ■- analyze core dump
$ gdb object pid  ■- attach to running process

General commands
-----
set args          - set program arguments
show args         - show program arguments
run               - run the program
run < file        - run with input from file
set follow-exec-mode new/sam
set write          - set debugger response to an exec call
set write off      - set write into executables
continue          - unset write int oexecutables
finish             - continue running until break
source FILE        - execute until current stack frame ends
shell  [cmd]       - read commands from script file
display /5i $eip   - run cmd in a shell
undisplay <expr #> - display expression everytime execution stops
info functions    - display expression number
info variables    - list all the functions
info registers    - list all the variables
info all-registers - list most common registers
info display       - list all registers
backtrace          - print the list of displayed expressions
where              - print backtrace of all stack frames
set disassembly-flavor intel
define hook-[cmd] - same as backtrace
define hooopost-[cmd] - set disassembly style to intel/att
define hook-stop   - actions to execute before command
                     - actions to execute after command
                     - actions to execute when execution stops

Breakpoints
-----
info breakpoints    - list all breakpoints
break [func]        - break function name
break *[addr]       - break at address
delete [bnum]        - delete breakpoint bnum
break if [cond]     - break if condition
ignore [bnum] [count] - ignore breakpoint bnum count times
condition [bnum] $eax == 0x22 - add condition for breakpoint 1
condition [bnum]     - delete condition for breakpoint 1

Watchpoints
-----
info watchpoints   - list all the watchpoint
watch variable==value - break when variable equals ..
watch $eax == 0x0000ffaa - break when register equals ..
rwatch *[addr]     - break on read memory location
awatch *[addr]     - break on read/write memory location
```