**Windbg Quiz**

**1. What is WinDbg primarily used for?**

a) Game development.

b) Web browsing.

c) System and application debugging.

d) Spreadsheet calculations.

**2. Which command in WinDbg displays the call stack?**

a) `.stack`

b) `!stack`

c) `stack()`

d) `k`

**3. Which of the following commands lists all loaded modules?**

a) `lm`

b) `mods`

c) `listm`

d) `.modules`

**4. What does the `.reload` command do?**

a) Restarts WinDbg.

b) Reloads symbols.

c) Refreshes the UI.

d) Exits the debugger.

**5. What does the `g` command do in WinDbg?**

a) Generates a report.

b) Goes to a function.

c) Resumes execution.

d) Lists global variables.

**6. Which command helps set breakpoints?**

a) `setbp`

b) `mark`

c) `bp`

d) `interrupt`

**7. To which mode does WinDbg NOT attach?**

a) Kernel mode.

b) User mode.

c) Game mode.

d) Both user and kernel mode.

**8. How do you start a new debugging session?**

a) File > New Session.

b) File > Open Executable.

c) File > Start.

d) Debugger > New Session.

**9. Which command loads debugger extensions?**

a) `!load`

b) `.extload`

c) `.load`

d) `extension.load`

**10. If you have a memory address and want to view its content, which command would you use?**

a) `va`

b) `d`

c) `ma`

d) `view`

**11. What does the `t` command do in WinDbg?**

a) Trace into the next call.

b) Terminate execution.

c) View type information.

d) Test the application.

**12. Which command in WinDbg is used for displaying local variables?**

a) `dv`

b) `lv`

c) `locals`

d) `vl`

**13. To view the available processors in a multiprocessor system, you use:**

a) `!cpus`

b) `~`

c) `!processors`

d) `#`

**14. What does `ub` command do?**

a) Unload breakpoints.

b) Disassemble backwards.

c) Unbox a value.

d) Update the binary.

**15. If you want to search memory for a specific pattern, you would use:**

a) `s`

b) `f`

c) `m`

d) `?`

**16. The `dt` command in WinDbg stands for:**

a) Display Type.

b) Define Table.

c) Debug Trace.

d) Data Tracker.

**17. To see all current breakpoints, which command is used?**

a) `lbs`

b) `bps`

c) `lists`

d) `bl`

**18. The `!analyze -v` command is used for:**

a) Variable analysis.

b) Verbose allocation.

c) Verbose analysis of exceptions or crashes.

d) None of the above.

**19. The `e` command in WinDbg stands for:**

a) Execute.

b) Enter (to modify memory).

c) Exit.

d) Enumerate.

**20. In order to see all threads, which command would you use?**

a) `!threads`

b) `.threads`

c) `~\*`

d) `threads()`

**21. Which of the following is NOT a type of breakpoint in WinDbg?**

a) Hardware.

b) Data.

c) Software.

d) Conditional.

**22. Which command evaluates expressions?**

a) `expr`

b) `!calc`

c) `?`

d) `=`

**23. What does the `r` command do in WinDbg?**

a) Display or modify registers.

b) Restart the debugger.

c) Run the application.

d) Refresh the view.

**24. The `!peb` command displays:**

a) Process Environment Block.

b) Program Error Buffer.

c) Previous Execution Block.

d) None of the above.

**25. The command `.symfix` in WinDbg is used to:**

a) Set the symbol path to Microsoft's symbol server.

b) Fix broken symbols.

c) Synchronize all symbols.

d) None of the above.

Answers:

1. System and application debugging.
2. k
3. lm
4. Reloads symbols.
5. Resumes execution.
6. bp
7. Game mode.
8. File > Open Executable.
9. .load
10. d
11. Trace into the next call.
12. dv
13. ~
14. Disassemble backwards.
15. s
16. Display Type.
17. bl
18. Verbose analysis of exceptions or crashes.
19. Enter (to modify memory).
20. ~\*
21. Software.
22. ?
23. Display or modify registers.
24. Process Environment Block.
25. Set the symbol path to Microsoft's symbol server.