Meet Stratoshark: Wireshark's Baby Brother

Josh Clark

https://github.com/je-clark/self-25-stratoshark

Agenda

- Introduction
- What are system calls?
- What data do Wireshark and Stratoshark examine?
- Demo

https://github.com/je-clark/self-25-stratoshark

Introduction

- B.S. and M.S. in Computer Engineering
  - Spent several semesters breaking Linux trying to optimize networking
- Principal Performance Engineer
  - Uses expertise in network protocols and Linux internals to identify bottlenecks in distributed systems

www.jeclark.net | www.github.com/je-clark

What are System Calls?

```
With open(r'./file.txt') as file:
    contents = read(file)
```

What are System Calls?

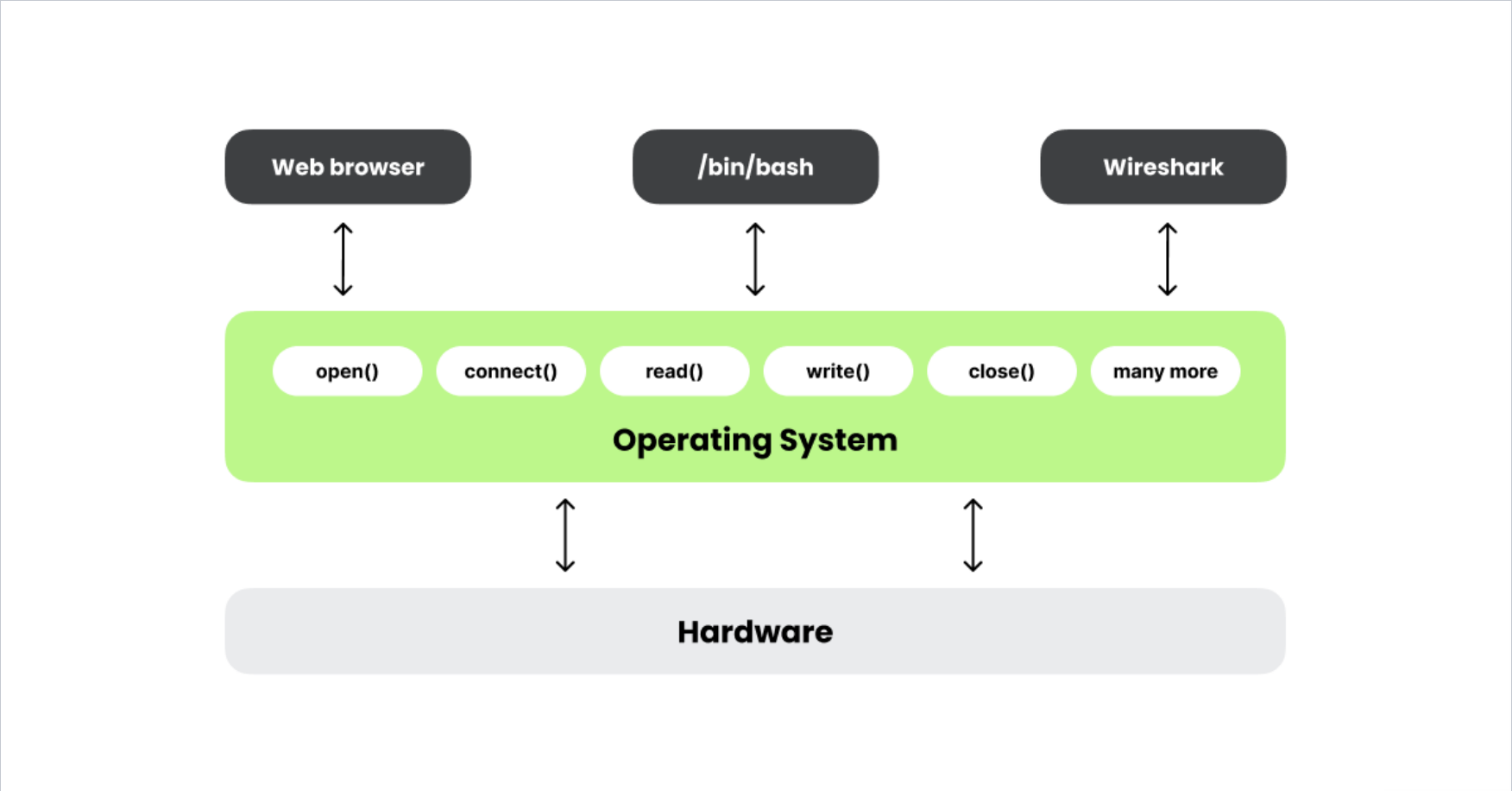
```
#include <stdio.h>
#include <stdlib.h>

int main() {
    FILE *file = fopen("./file.txt", "r");
    char *contents = malloc(filesize + 1);

    fread(contents, 1, filesize, file);
    contents[filesize] = '\0';

    fclose(file);
    return 0;
}
```

What are System Calls?

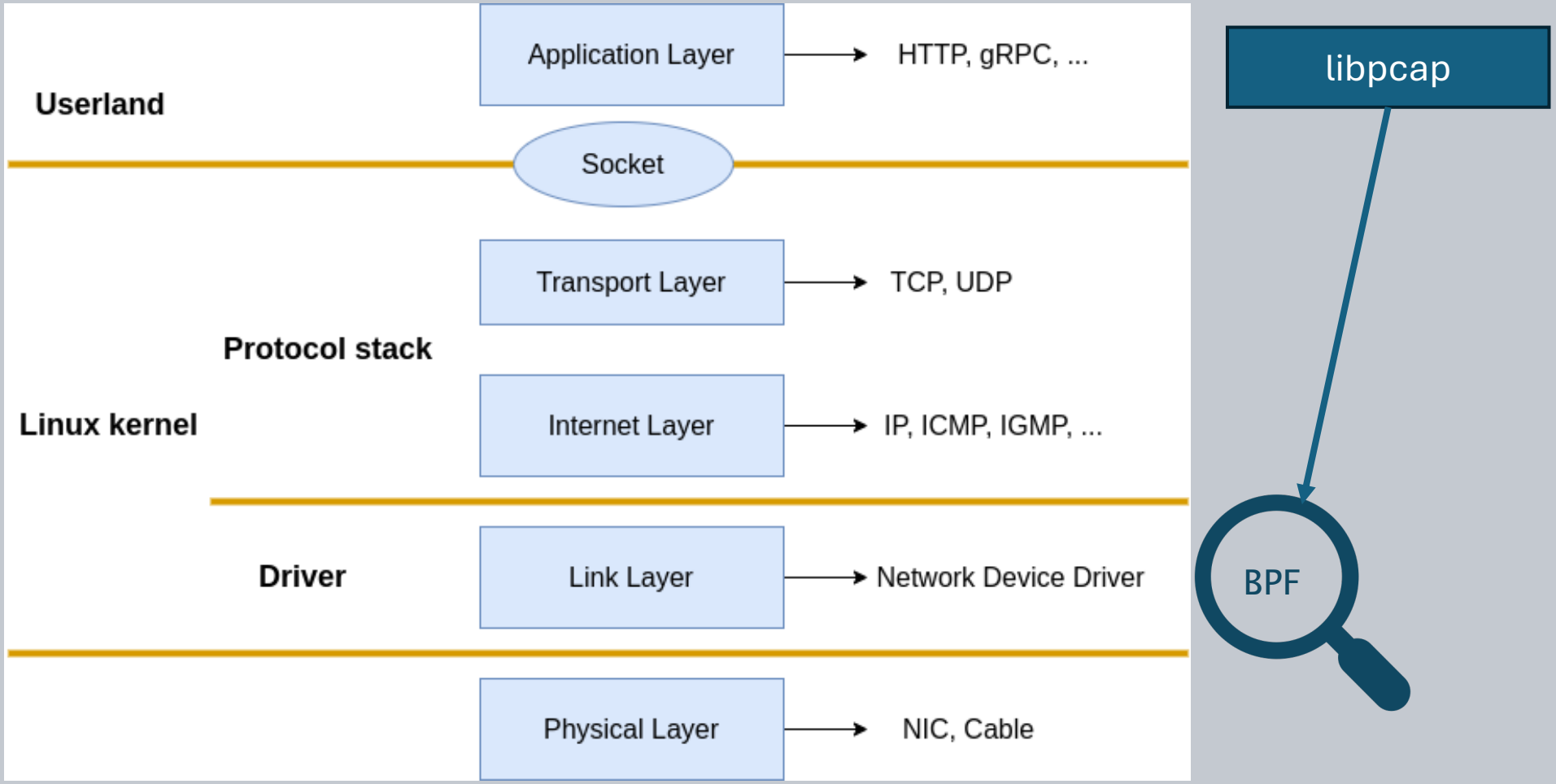


https://blog.wireshark.org/2025/01/those-arent-packets/

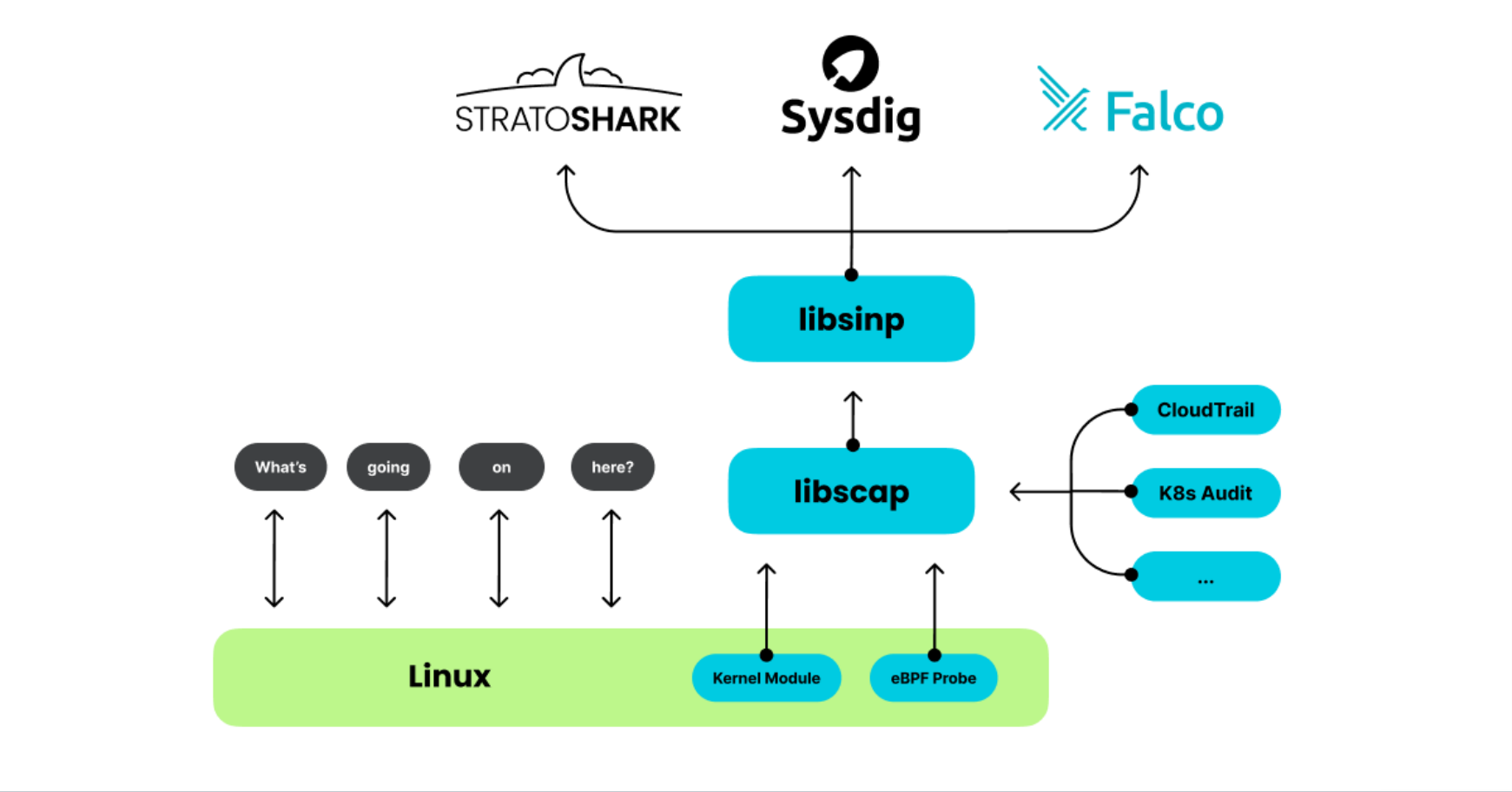
What System Calls Are Out There?

https://filippo.io/linux-syscall-table/

How Do We Capture Packets?



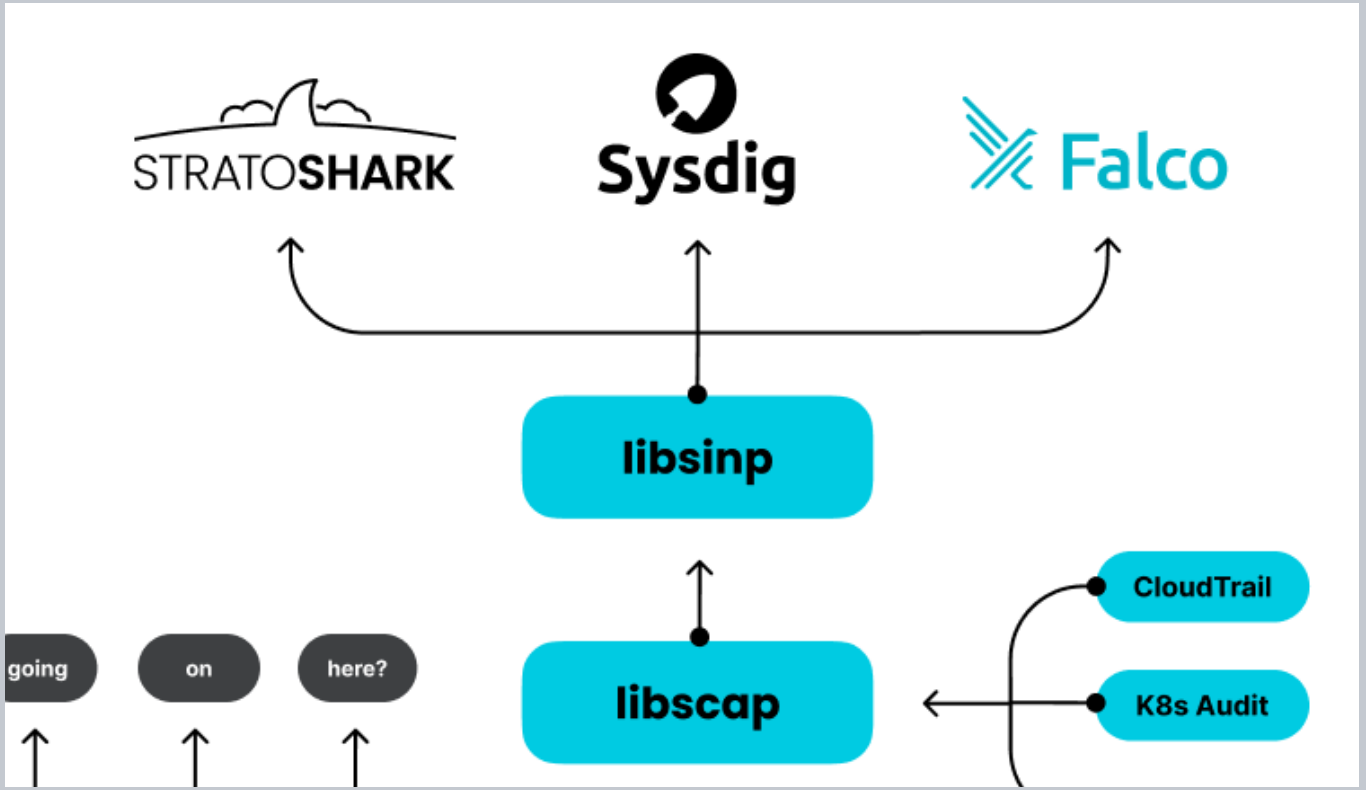
How Do We Capture System Calls?



https://blog.wireshark.org/2025/01/those-arent-packets/

How Do We Capture System Calls?

https://github.com/draios/sysdig



https://blog.wireshark.org/2025/01/those-arent-packets/

Demo: HTTP

- http_packets.pcapng
- http_syscalls.scap

Current Limitations

- Unable to see some inter-process and kernel communication
  - Statically linked libraries (e.g. nginx and openssl)
  - Shared memory locations (e.g. getdents64())
- sysdig missing features that other syscall tools include
  - Strace gives you more data for getdents64() than sysdig
- No Windows or MacOS support
  - Gitlab issue is open for Windows procmon support

Questions & Feedback

Josh Clark | www.jeclark.net