Tales of a System Call Spelunker

An Introduction to System Call Analysis with Stratoshark

https://github.com/je-clark/sharkfest-25-us-stratoshark

Josh Clark | www.jeclark.net | #sf25us

- Introduction
- What are system calls?
- How do Wireshark and Stratoshark capture data?
- What does a Stratoshark capture look like?
- BREAK
- Demo   –   HTTP Analysis
- Practice   –   HTTPS Analysis
- Demo   –   SCP Analysis
- Practice   –   SFTP Analysis
- Practice   –   Distributed System Troubleshooting

https://github.com/je-clark/sharkfest-25-us-stratoshark

- 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

  https://github.com/je-clark/sharkfest-25-us-stratoshark

Opening and reading a file in Python

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

Opening and reading a file in C

```c
#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;
}
```
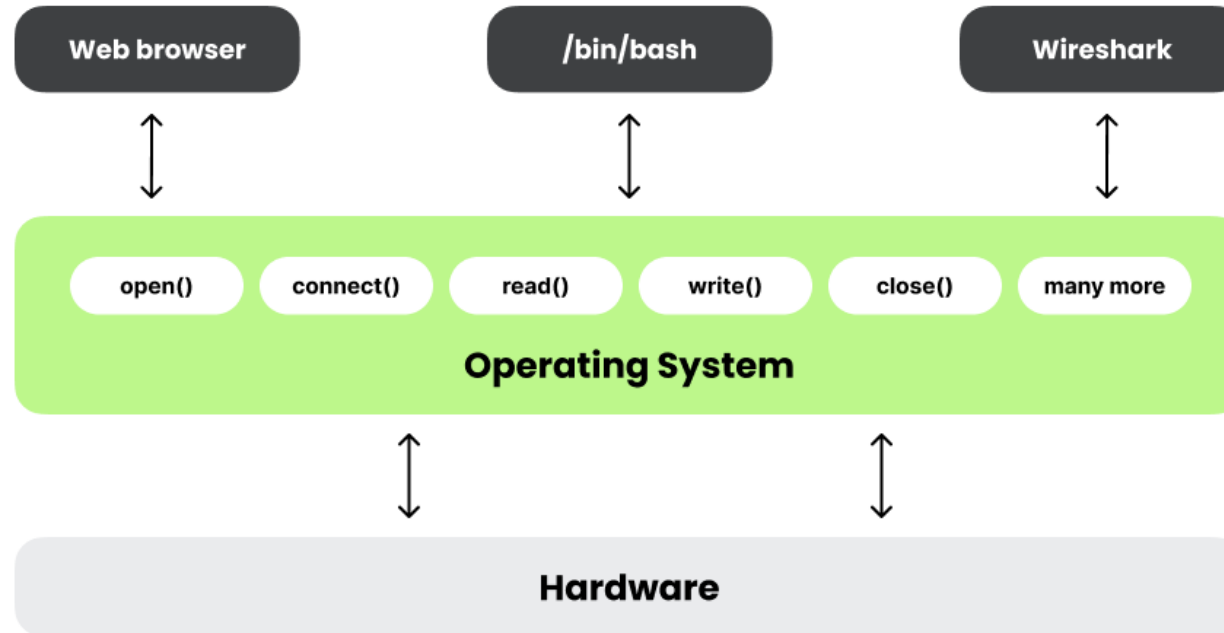
Josh Clark | www.jeclark.net | #sf25us

Playing Music in MATLAB

```
[y, Fs] = audioread('success.wav');
sound(y, Fs);
```

What are System Calls?

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

Josh Clark | www.jeclark.net | #sf25us

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

Userland

Application Layer → HTTP, gRPC, ...

Socket

libpcap

Protocol stack

Transport Layer → TCP, UDP

Linux kernel

Internet Layer → IP, ICMP, IGMP, ...

Driver

Link Layer → Network Device Driver

BPF

Physical Layer → NIC, Cable

Josh Clark | www.jeclark.net | #sf25us

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

Josh Clark | www.jeclark.net | #sf25us

https://github.com/draios/sysdig/wiki/How-to-Install-Sysdig-for-Linux

```
curl -s https://download.sysdig.com/stable/install-sysdig
| sudo bash
```

```
Sudo sysdig -w capture.scap
```

```
Sudo sysdig –s 1000 -w capture.scap
```

```
Sudo sysdig -w capture.scap proc.name=nginx or
proc.name=python3
```

```
Sudo sysdig -w capture.scap evt.type=open
```

Stratoshark Interface

Event list

Event details

Event bytes

Josh Clark | www.jeclark.net | #sf25us

Direction:
> Enters a syscall
< Exits a syscall

```
∨  Event Information
      Event Source: syscall
      Latency: 833
      Latency (s): 0
      Latency (ns): 833
      Human-Readable Latency: 833ns
      Direction: <
      Type: close
```

Arguments:
Syscall-specific
Discoverable in reference docs

```
>  Event Information
∨  Event Arguments
      fd: <4t>192.168.64.1:52641–>192.168.64.4:22
      size: 262144
```

SYNOPSIS

```
       #include <unistd.h>

       ssize_t read(int fd, void buf[.count], size_t count);
```

Josh Clark | www.jeclark.net | #sf25us

- 1_top.scap

- Use the 'in {}' filter syntax as a first choice
- /proc is a directory where the kernel writes process and system statistics
- getdents64() writes information about contents of a directory to a memory map created with the mmap() call
- The terminal window uses the file descriptor /dev/pts/0

- 2_http_packets.pcapng
- 2_http_syscalls.scap

- 3_https_packets.pcapng
- 3_https_syscalls.scap
- 3_https_worksheet.pdf

- 4_scp_packets.pcapng
- 4_scp _syscalls.scap

- 5_sftp_packets.pcapng
- 5_sftp_syscalls.scap
- 5_sftp_worksheet.pdf

- Distributed_system_worksheet.pdf
  - If you feel confident, try using only page 1
  - If you want a guided tour, use the entire worksheet
- Josh_web_store.har
- Web_packets.pcapng
- Web_syscalls.scap
- Nas_packets.pcapng
- Nas_syscalls.scap
- Db_packets.pcapng
- Db_syscalls.scap

- 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

- In this session, we
  - Learned what system calls are and how to capture them with sysdig
  - Learned the basic Stratoshark interface
  - Examined several common Linux applications in both Wireshark and Stratoshark
  - Found the bottlenecks in a distributed system using both Wireshark and Stratoshark

Feedback

Josh Clark | www.jeclark.net | #sf25us