در زیر تحلیل مربوط به بسته‌های TCP که در لاگ وایرشارک مشاهده می‌شود، آورده شده است:

- اتصال اول: (127.0.0.1:43555 به 127.0.0.10:5050)

1. بسته 1:

- [SYN] 127.0.0.10:5050 → 127.0.0.1:43555

- ایجاد اتصال با ارسال درخواست همزمان‌سازی .(SYN)

2. بسته 2:

- [SYN, ACK] 127.0.0.1:43555 → 127.0.0.10:5050

- تأیید درخواست اتصال با ارسال .SYN-ACK

3. بسته 3:

- [ACK] 127.0.0.10:5050 → 127.0.0.1:43555

- تأیید نهایی و تکمیل هم‌دستی (Handshake)سه‌گانه .TCP

4. بسته 4:

- [PSH, ACK] 127.0.0.10:5050 → 127.0.0.1:43555

- ارسال داده به همراه تأیید دریافت.

5. بسته 5:

- [ACK] 127.0.0.1:43555 → 127.0.0.10:5050

- تأیید دریافت داده‌های ارسالی.

6. بسته 6:

- [PSH, ACK] 127.0.0.1:43555 → 127.0.0.10:5050

- ارسال داده به همراه تأیید دریافت.

7. بسته 7:

- [ACK] 127.0.0.10:5050 → 127.0.0.1:43555

- تأیید دریافت داده‌های ارسالی.

8. بسته 8:

- [PSH, ACK] [127.0.0.1:43555 → 127.0.0.10:5050]بسته ناسالم

- ارسال داده به همراه تأیید دریافت، ولی بسته دارای خطا یا نقص است.

9. بسته 9:

- [ACK] 127.0.0.10:5050 → 127.0.0.1:43555

- تأیید دریافت داده‌های ارسالی.

- اتصال دوم: (127.0.0.1:43556 به 127.0.0.10:5050)

10. بسته 10:

- [SYN] 127.0.0.10:5050 → 127.0.0.1:43556

- ایجاد اتصال با ارسال درخواست همزمان‌سازی .(SYN)

11. بسته 11:

- [SYN, ACK] 127.0.0.1:43556 → 127.0.0.10:5050

- تأیید درخواست اتصال با ارسال .SYN-ACK

12. بسته 12:

- [ACK] 127.0.0.10:5050 → 127.0.0.1:43556

- تأیید نهایی و تکمیل هم‌دستی سه‌گانه .TCP

13. بسته 13:

- [PSH, ACK] 127.0.0.10:5050 → 127.0.0.1:43556

- ارسال داده به همراه تأیید دریافت.

14. بسته 14:

- [ACK] 127.0.0.1:43556 → 127.0.0.10:5050

- تأیید دریافت داده‌های ارسالی.

15. بسته 15:

- [PSH, ACK] 127.0.0.1:43556 → 127.0.0.10:5050

- ارسال داده به همراه تأیید دریافت.

16. بسته 16:

- [ACK] 127.0.0.10:5050 → 127.0.0.1:43556

- تأیید دریافت داده‌های ارسالی.

17. بسته 17:

- [PSH, ACK] 127.0.0.1:43556 → 127.0.0.10:5050

- ارسال داده به همراه تأیید دریافت.

18. بسته 18:

- [ACK] 127.0.0.10:5050 → 127.0.0.1:43556

- تأیید دریافت داده‌های ارسالی.

- تحلیل:

1. اتصال موفق:

- هر دو اتصال با سه‌گانه TCP (SYN, SYN-ACK, ACK) به‌درستی انجام شده است.

2. ارسال داده:

– داده‌ها به‌درستی بین کلاینت و سرور ارسال و دریافت شده‌اند.

3. بسته ناسالم:

– در اتصال اول، بسته 8 دارای نقص یا خطا بوده است که ممکن است نیاز به بررسی بیشتر داشته باشد.

4. تاخیر در ارسال:

– در هر دو اتصال، تاخیر قابل توجهی بین ایجاد اتصال و ارسال داده‌های PSH مشاهده می‌شود (بیش از 20 ثانیه).

این تحلیل نشان می‌دهد که دو اتصال TCP به‌درستی ایجاد شده‌اند و داده‌ها بین کلاینت و سرور تبادل شده‌اند، اما وجود بسته ناسالم نیاز به بررسی بیشتری دارد.