

Verifying the Data

Check List

1. Note the time of the issue
2. Check *Statistics -> Summary* in Wireshark 1.x or *Statistics -> Capture File Properties* in Wireshark 2.x to verify time span covers time of issue
3. Times in Wireshark are relative to the local computer. Be aware if data was captured in different timezone
4. Filter for client and server IPs to verify traffic exists
 1. `ip.host==192.168.1.242 and ip.host==173.194.43.35`
5. Check that you captured the beginning of the connection
 1. `ip.host==192.168.1.242 and ip.host==173.194.43.35 and tcp.flags.syn==1`
6. Check to see if you captured full packet lengths if you are analyzing the application

Full capture:

```
1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
```

- Snaplength and truncated:

```
1514 bytes on wire (12112 bits), 100 bytes captured (800 bits)
```

```
[Packet size limited during capture]
```