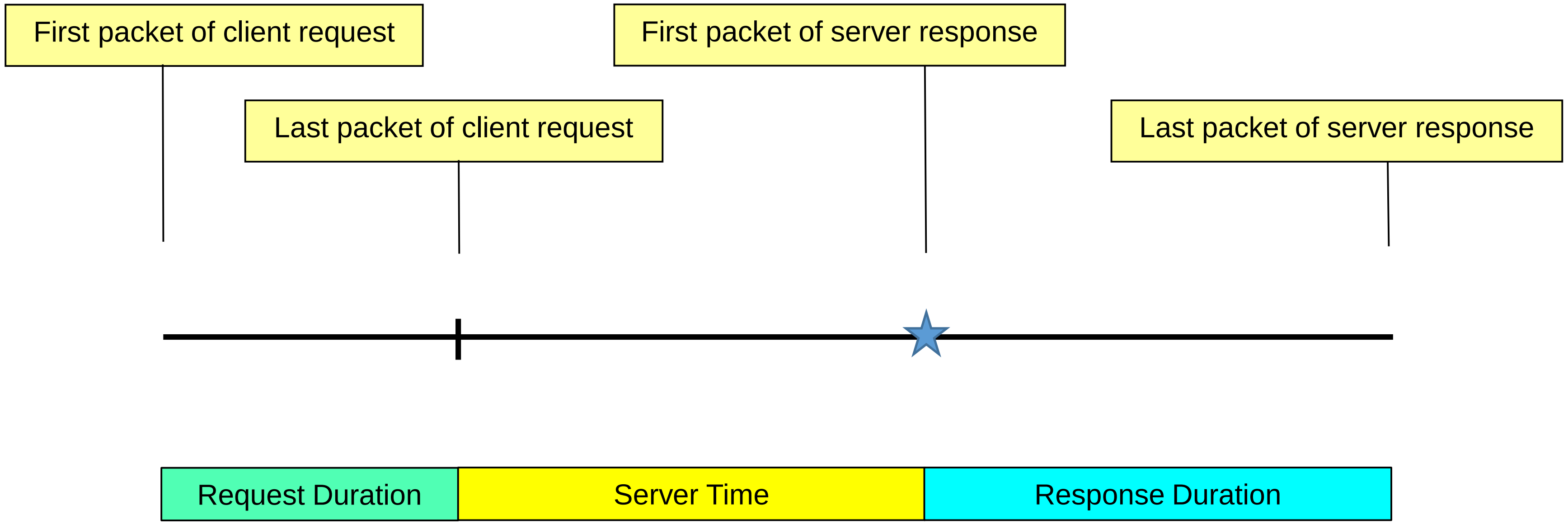
Understanding Performance Chart Transaction Symbols

NetData measures and reproduces individual application-layer transactions. The Performance chart plots each transaction as a horizontal line that represents the overall transaction duration, adding symbols within the line to indicate timings of transaction components. The main symbol's colour reflects the transaction's server (or client) and its shape indicates transaction type.

The x-axis is time-of-day and the y-axis is transaction duration. Each transactions is plotted at a height that usually represents the transaction's overall duration (the full length of the horizontal line).

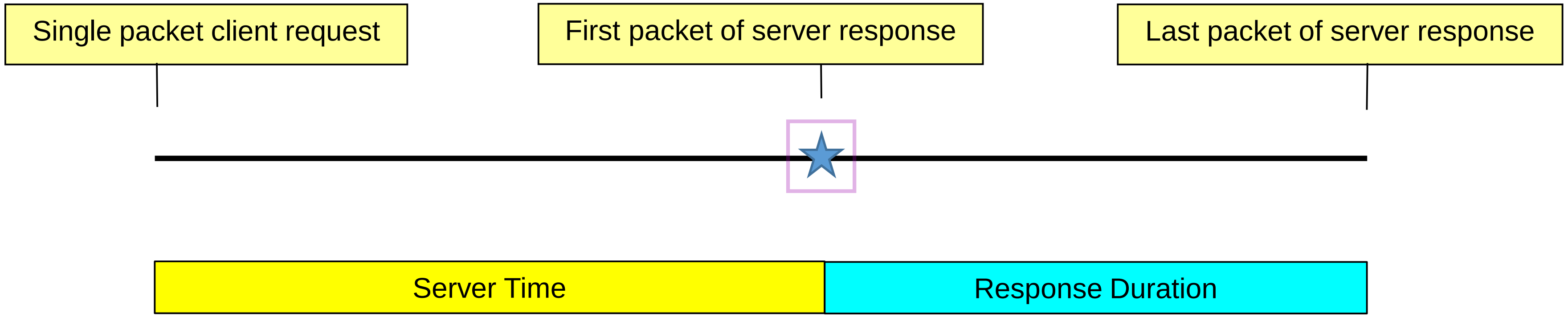


These green, yellow and blue colours are applied consistently to transaction bars on Timing and Waterfall charts to represent the same time components.

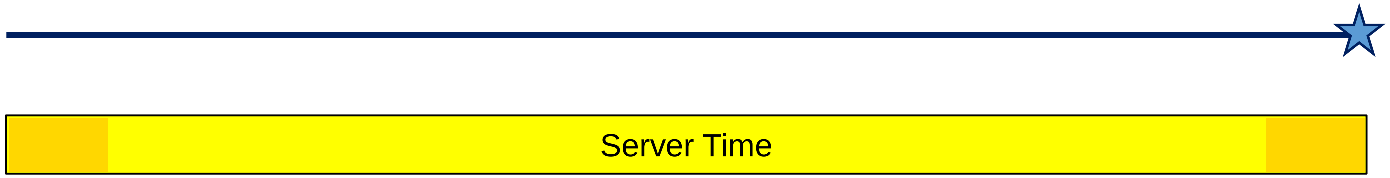
Understanding Performance Chart Transaction Symbols

When the client's request is small enough to be transferred in a single packet, there is no vertical tick and the whole length of the horizontal line before the coloured symbol represents 'Server Time'.

A pink square around the symbol indicates that the transaction has been affected by a network abnormality.



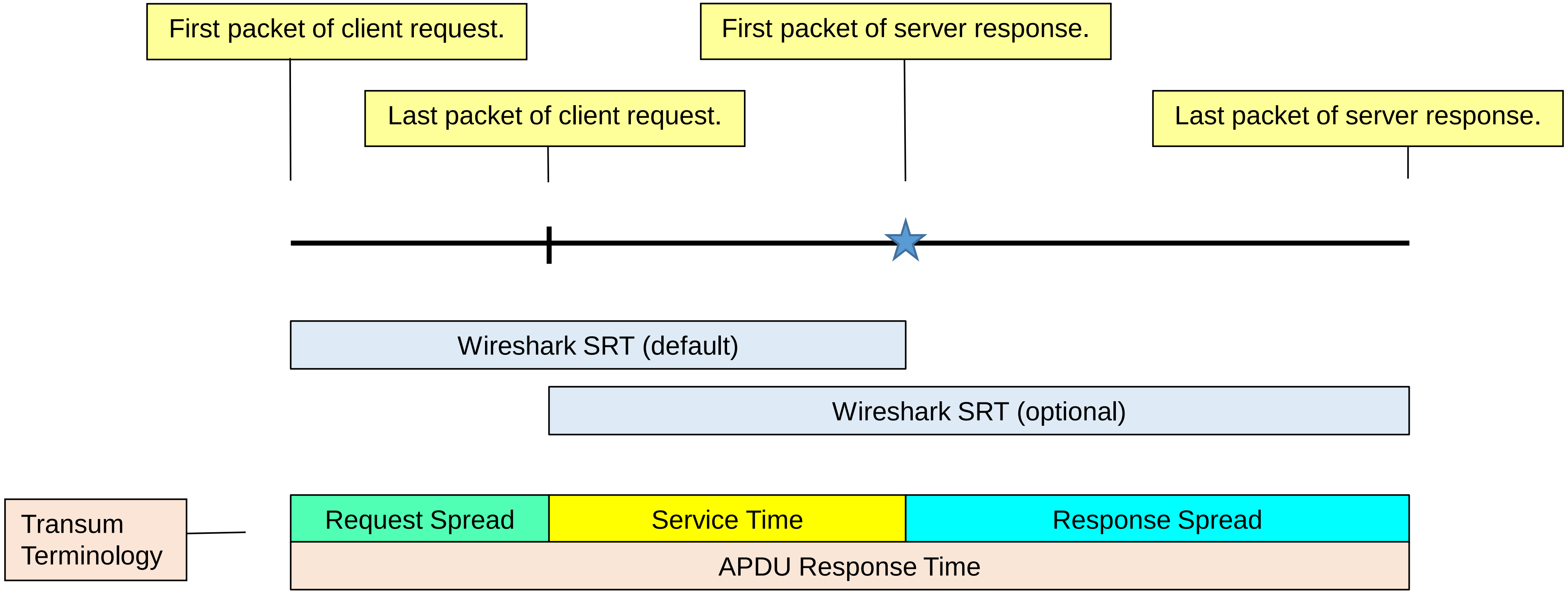
If the server response is also small (or relatively fast), then the coloured symbol will be at the very end of the line and the whole transaction duration appears to be 'Server Time'. In client-side captures, orange bars visualise propagation delay..



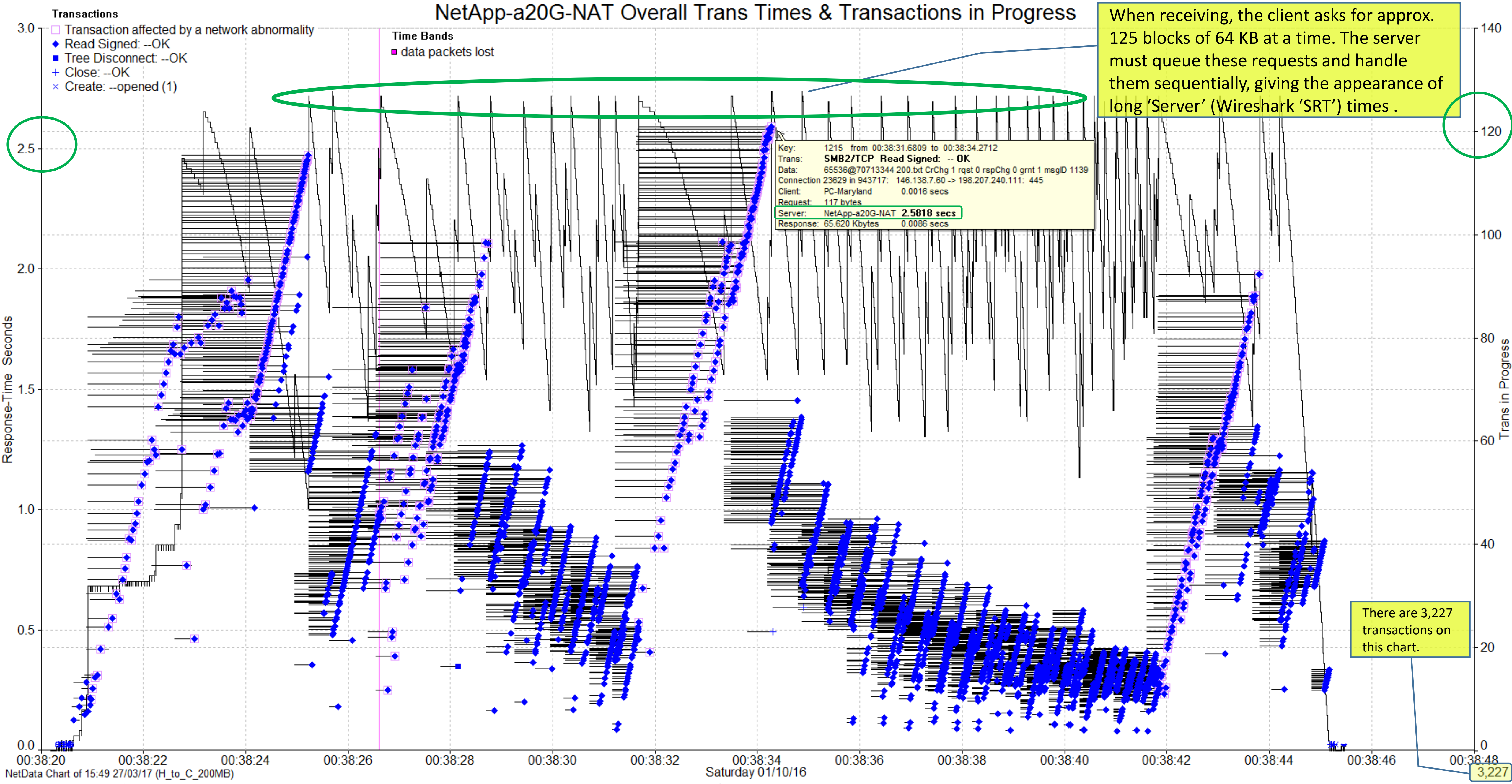
Comparison with Wireshark & Transum

Wireshark has two settings for measuring 'Service Response Times' (SRT) for several application protocols.

A newer feature, Transum (originally developed by Tribelab in the UK but now built into Wireshark), can also calculate the timing of request-, server-, response- and overall-transaction durations for some protocols.



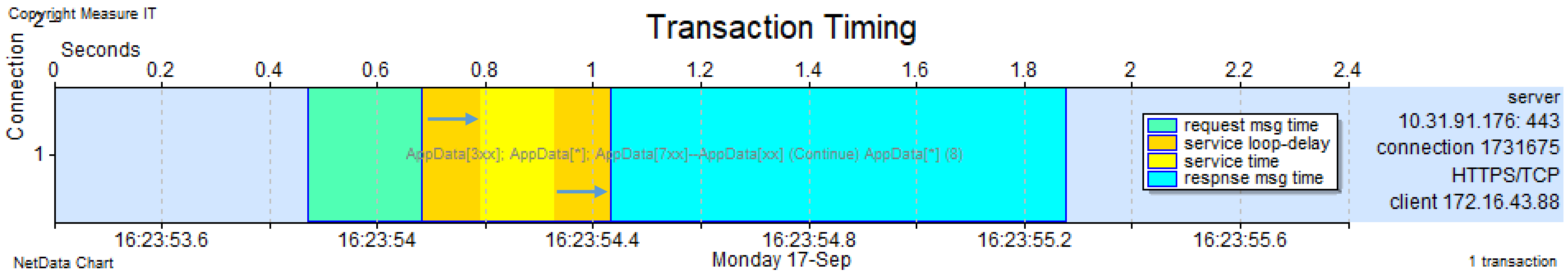
Performance Chart with Bursts of SMB2 Read Transactions



Simple Transaction Timing Chart

The transaction–timing chart represents the durations of transaction phases with horizontal bars in the standard colours, drawn on pale-coloured bands dedicated to the activity of different connections. The connections are described in the chart's right-hand column and a floating box of legends tells what the colours represent.

In this simple example we have only one TCP connection and one transaction. Later we'll see many of each.

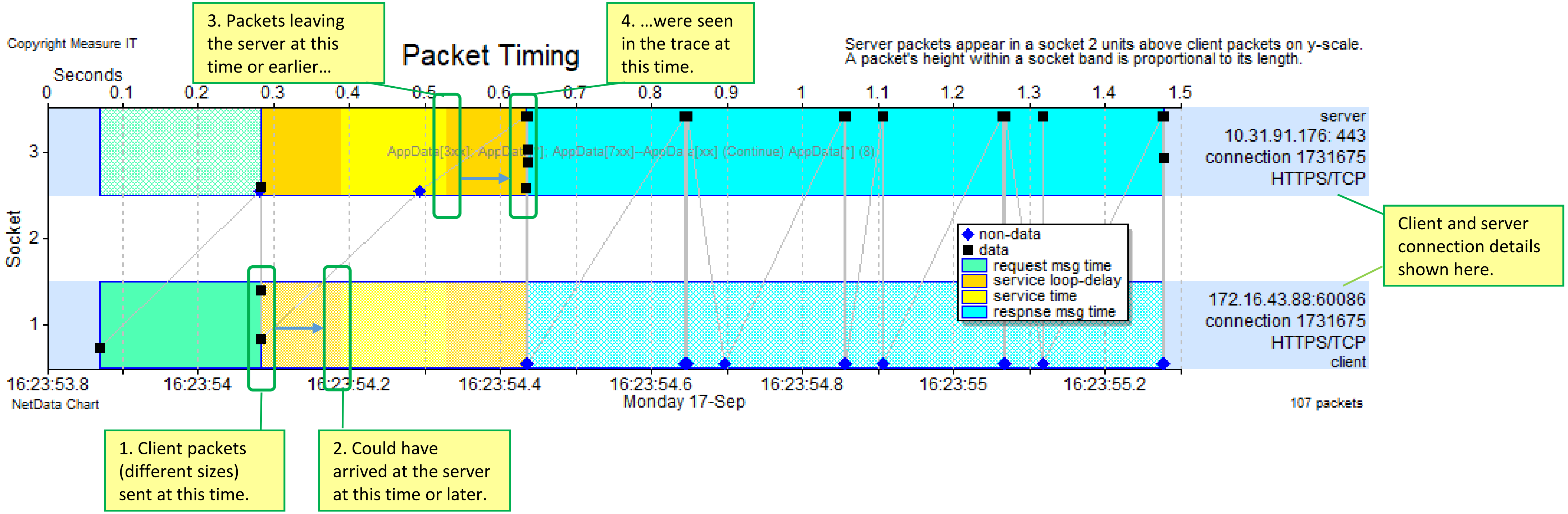


Optional orange bars indicate propagation delay associated with the service round-trip. The first orange bar represents the time for the last request packet to propagate from the sniffer to the server (arriving no earlier than the right-side of the bar); the second bar represents the time for the first response packet to propagate from the server(starting no later that the left-side of the bar) to the sniffer.

Simple Packet Timing Chart (One TCP Connection)

When packet markers are overlaid on transaction bars, the chart becomes a packet-timing chart. This is similar to a Wireshark Flow chart or "Ladder" diagram in other tools – but rotated onto its side. Packets are plotted at the times read from the capture file, making time intervals between packets easy to see.

There is no need for arrows to indicate packet direction because each connection band is split into two horizontal *socket* bands. Client packets are always plotted on the lower band and server packets always on the upper band. The height of a marker within its band is proportional to its length.

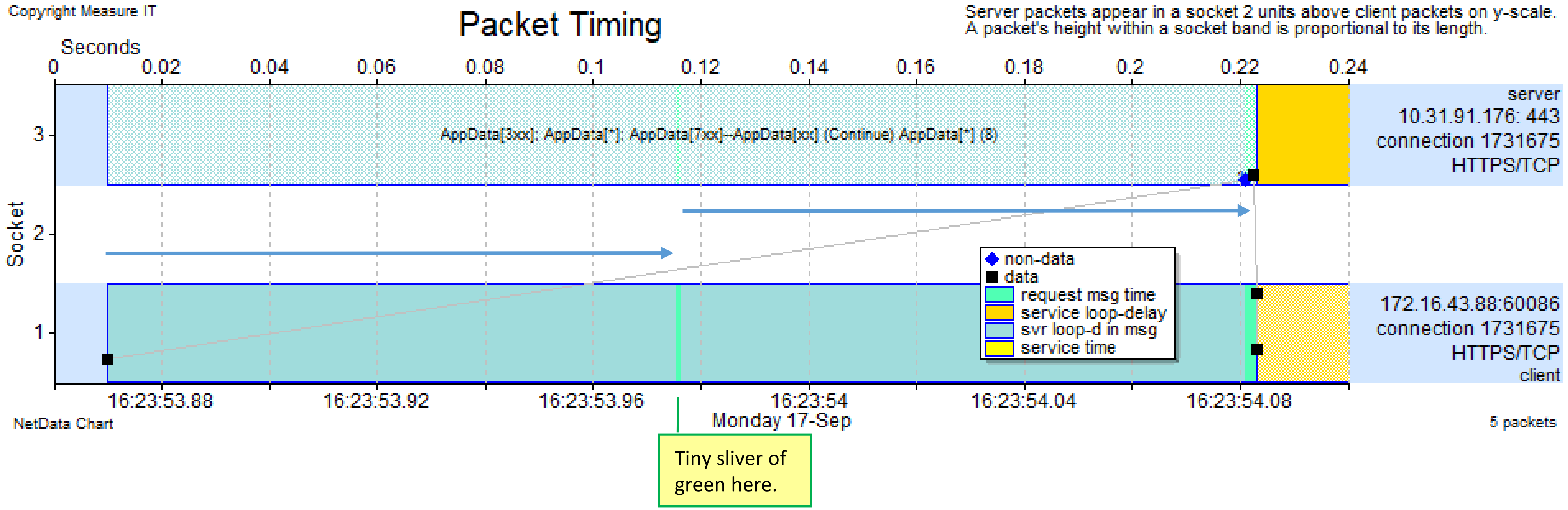


The optional grey lines link packets in chronological order. Different packet-marker shapes and colours (as indicated by the legend box) make it easy to identify different packet types: black squares for data packets, blue diamonds for acknowledgements. Many more are not shown here.

The server and response-message bars are drawn on the client band with paler colours, as is the request-message bar on the server band.

Propagation Delay

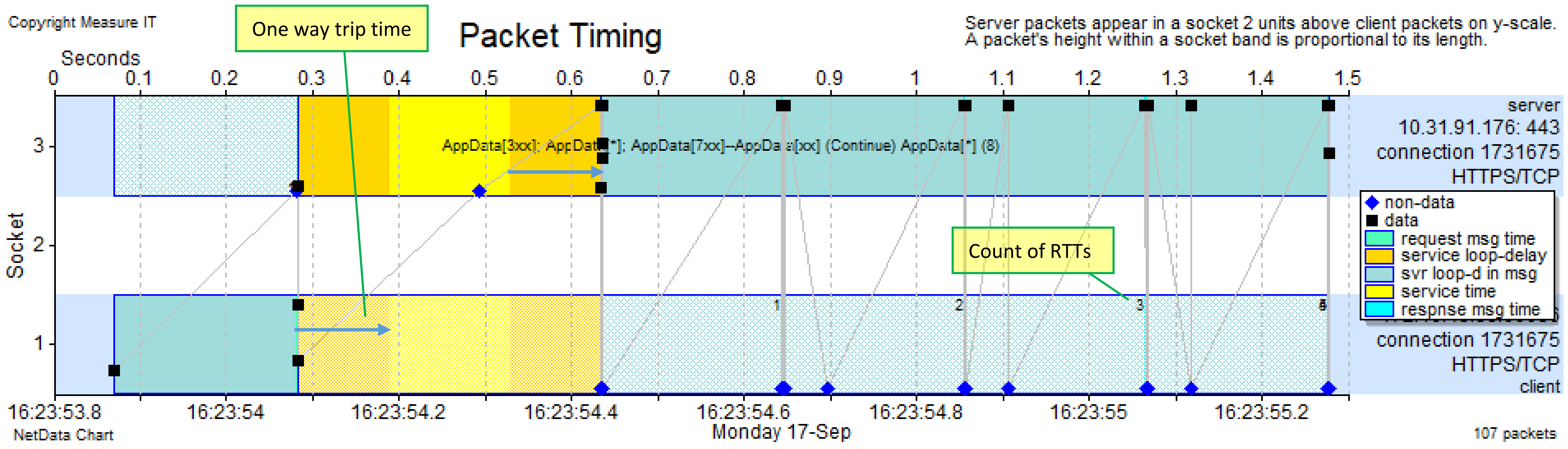
NetData can also indicate the time spent in signal propagation during request and response message transfers. During a transfer there are likely to be many concurrent activities; while some packets are being transmitted over different links, others might be queued in routers awaiting transmission, and many signals will be propagating. NetData identifies a ‘critical path’ through all the activities to avoid counting any time period twice. In effect it tracks the times for a single data packet to cross the network, say from server to client; then the times for the Ack packet prompted by that data packet to return across the network; and, if data is waiting, subsequent data packets as they are prompted when a responding Ack opens the window.



In this chart two grey-blue propagation bars are separated by a very short green bar. The first grey-blue bar represents the time for the first request packet to propagate from the sniffer to the server (arriving no earlier than the right-side of the bar); the second bar represents the time for the first Ack packet to propagate from the server (starting no later that the left-side of the bar) to the sniffer. In this case the client was waiting for a short data packet containing an HTTP 100-Continue message from the server before sending the remainder of the request.

Response Propagation Delay

Just as orange bars indicate propagation delay (half the minimum RTT) within the yellow server time areas, grey-blue bars indicate propagation delay during request and response message transfers.



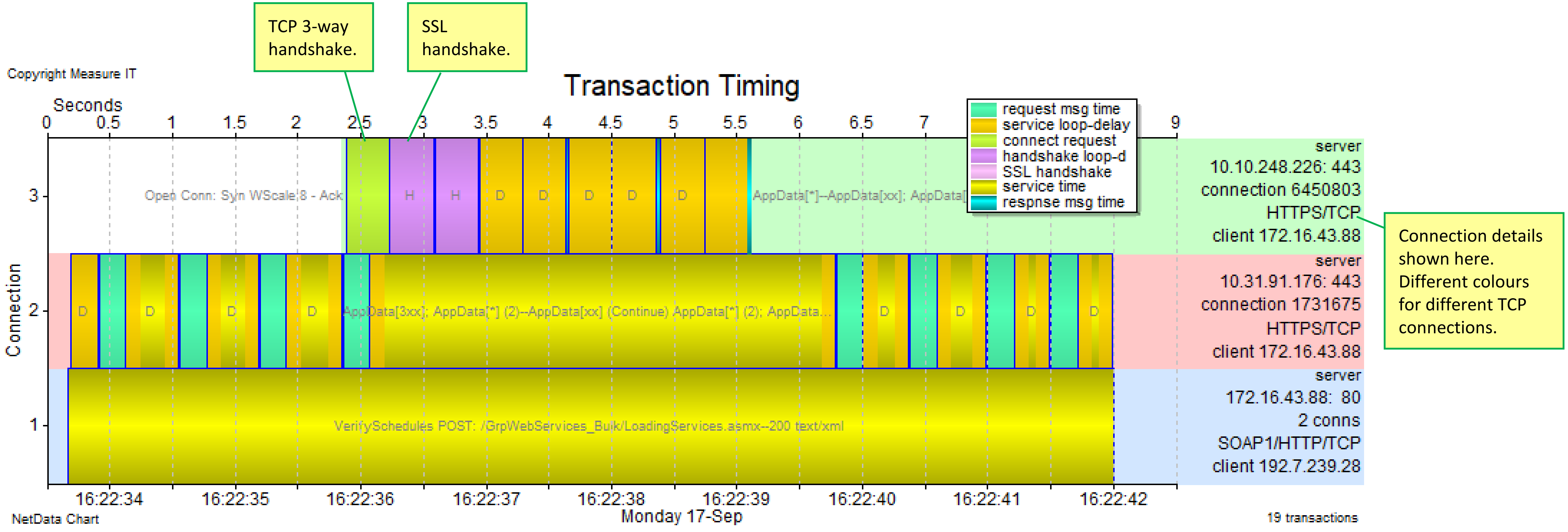
In this case the response message required four TCP round-trips, each trip starting with a data packet from the server and ending with an Ack from the client. At this scale it appears that all the message-transfer time was propagation time, with one loop-delay for the request message and four times the loop-delay for the response message. When the orange propagation time is added, it is seen that this transaction's overall response time included six times the path's loop-delay.

The individual TCP round-trips are counted with numbers displayed on the chart.

Activity on Many Connections

The timing chart scales to visualise the activity of possibly hundreds of connections with thousands of transactions (and optionally all their packets). In this case a single front-end SOAP transaction on the bottom band (connection 1) generated transactions on backend connections to two different servers (connection bands 2 and 3). The overall timing of the front-end transaction was determined by the timing of the nine back-end transactions on connection 2.

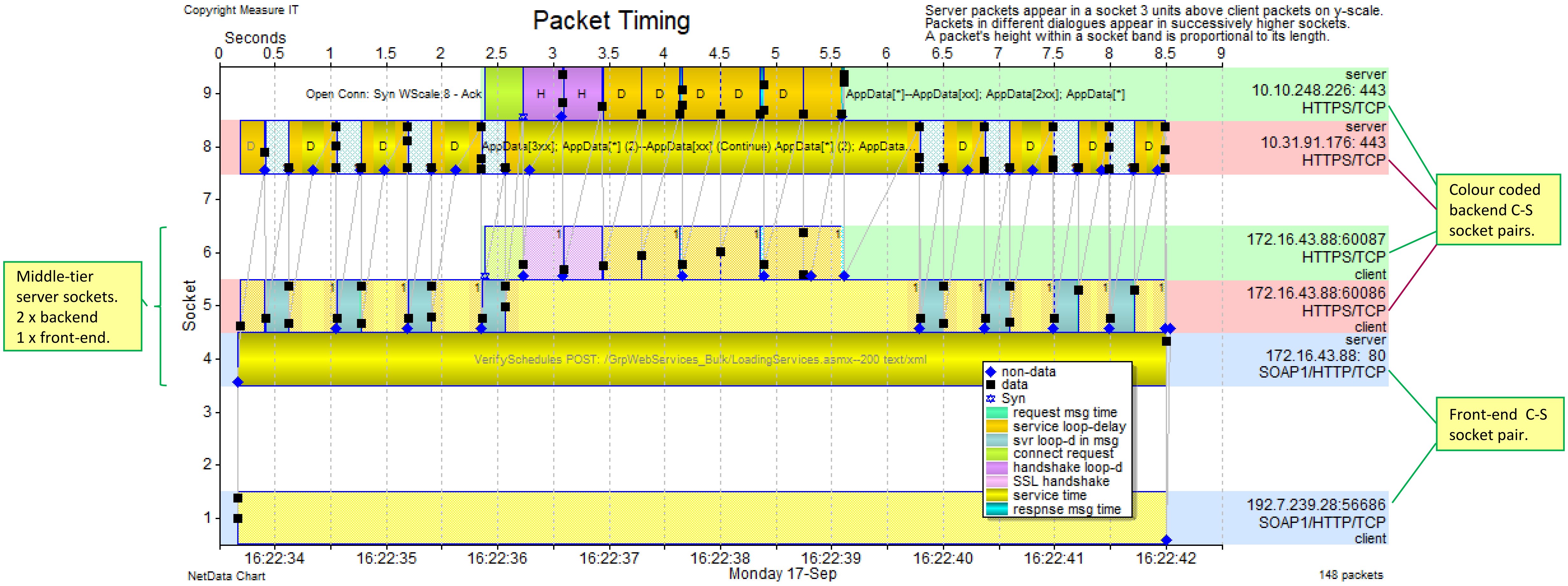
As always, the floating legend box describes the bar colours, including here a green bar for a TCP three-way handshake and two purple bars representing round-trips for an SSL handshake.



Characterising a Multi-Tier Transaction

Adding packets to the chart splits each *connection* band into two (client and server) *socket* bands. The connection pairs are further separated to emphasise the multi-tier nature of configurations by placing front-end connections below backend connections where possible. In this chart the front-end connection pair (blue) is at the bottom and the corresponding backend connection pairs (red and green) appear at the top. All three bands clustered in the middle describe the streams of packets transmitted from three sockets of the middle-tier server.

Adding packets also allows NetData to count and display propagation delay in message transfers.

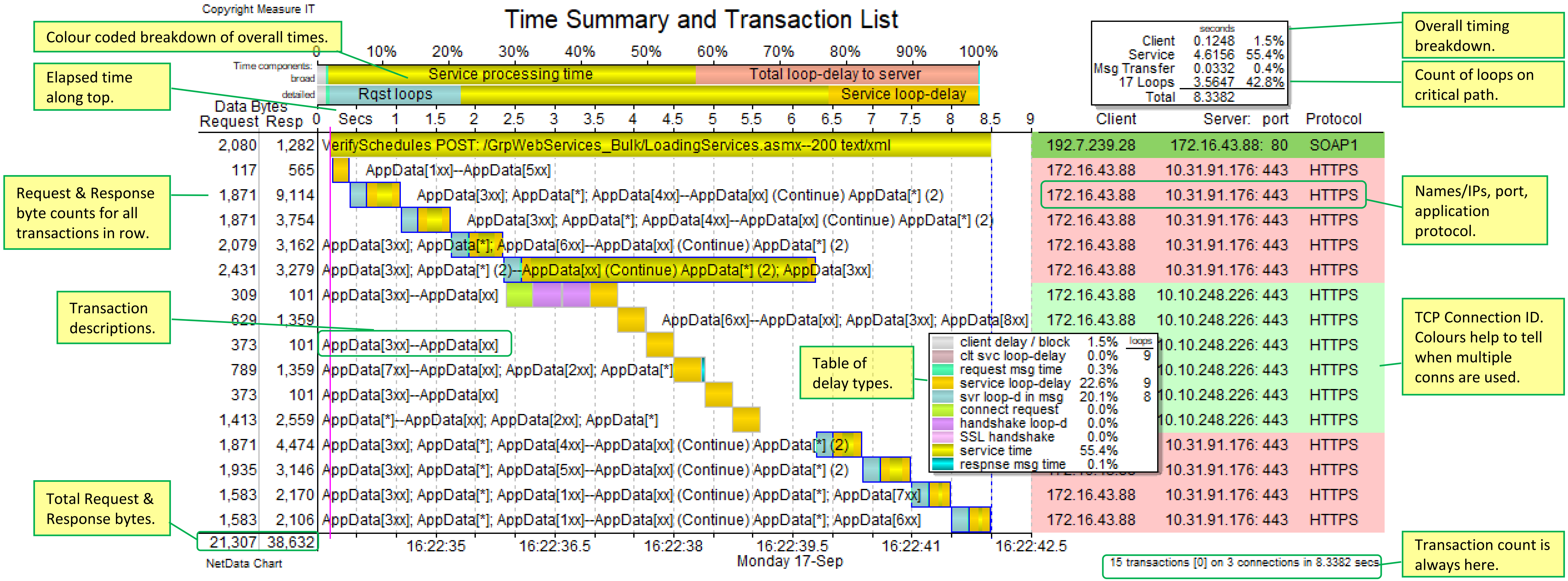


Interpreting Waterfall Charts

All the back-end activity generated by the single front-end transaction can also be characterised on a waterfall chart, with one application transaction on each row. The top row is the same front-end transaction as before and subsequent rows describe the various backend transactions.

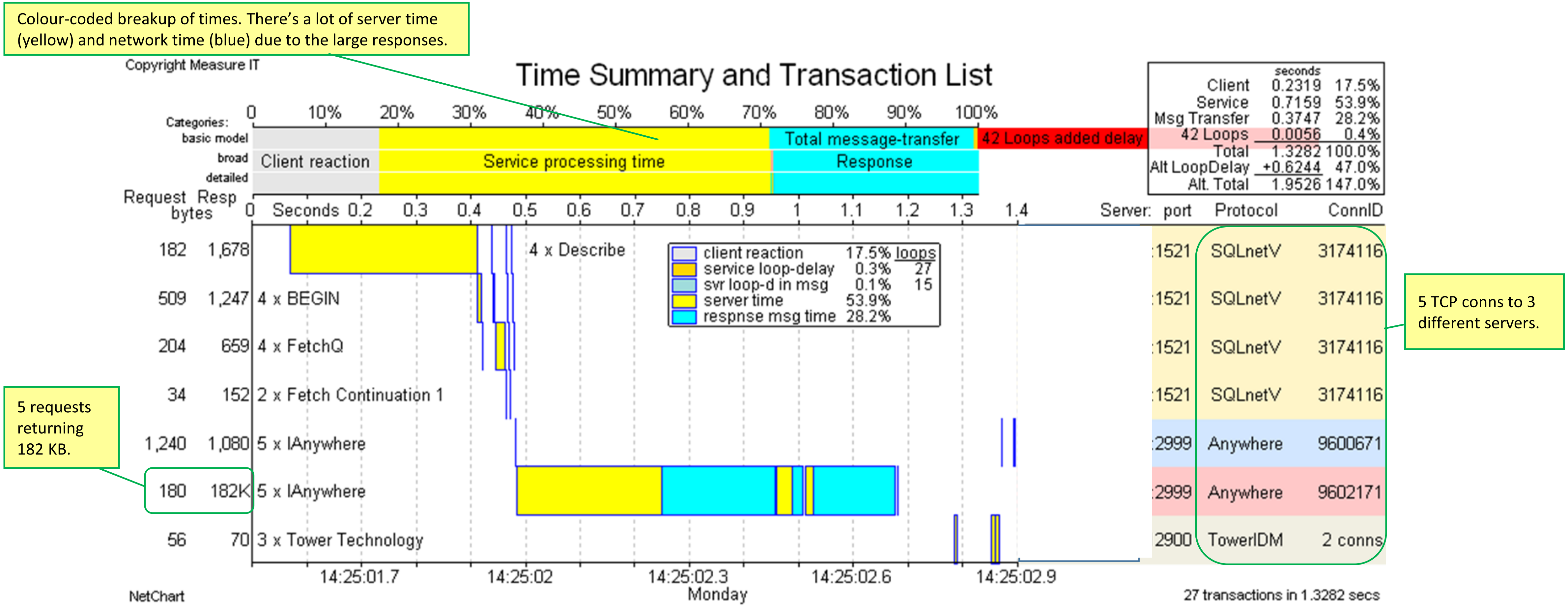
Time summary bars and their table above the waterfall tells that backend propagation delay accounted for 42% of the overall response time.

NetData also identifies a 'critical path' through the various system activities and counts round-trip times (loops) along this path. The absence of blue borders to the transaction bars on the light green connection indicates that their activity was not counted on the critical path.



Three Different Server Types

Here's a completely different example, where the overall function took 1.33 seconds.
On this chart each row contains multiple transactions of the same general category to a particular server.
It is easy to see when server time occurred (yellow) and when response network data delivery occurred (blue).
The extra red bar is showing how much the overall user function would be affected if the servers were moved to a more distant location.

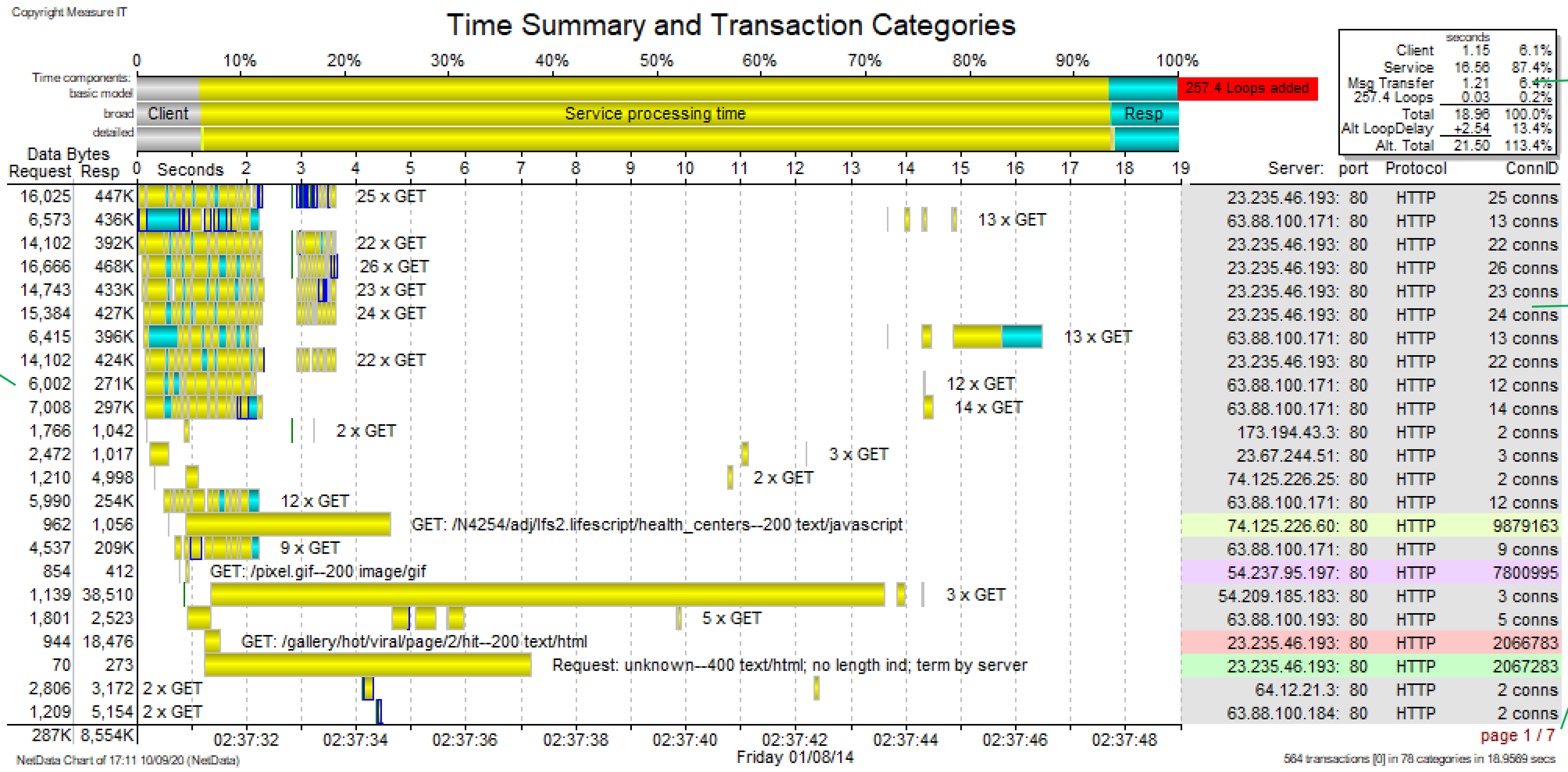


HTTP Protocol

This is an example showing HTTP transactions. With 257 round trips, the servers being 10 ms away would add 2.5 seconds to this 19 second set of transactions (a 13.4% increase). 87% of the overall time is “Server (yellow)” with 6.4% being “Msg Transfer (blue)” – which is time taken to deliver the packets of the large responses.

It is worth noting that this chart was produced with NetDataLite. Further, that this is just page 1 of 7.

287 KB of requests returning 8.5 MB of responses.



Mostly server time but some packet delivery time.

Many TCP connections to many servers.

This is page 1 of 7 overall pages.

Phil Storey

Phil@NetworkDetective.com.au

www.NetworkDetective.com.au

au.linkedin.com/in/philipstorey3

@PhilStorey24

www.youtube.com/c/NetworkDetective

ask.wireshark.org @philst