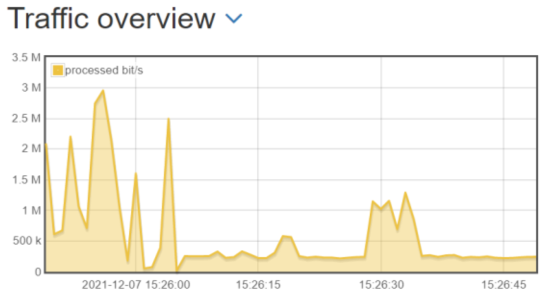
## Packet Captures have always been a part of the network engineer's tool set, but here are the top reasons people use them.

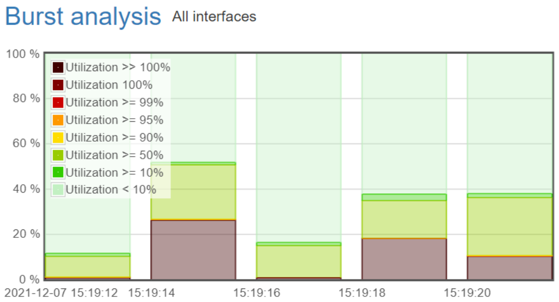
### 1. Utilization – Accurately!

There are many ways to get utilization figures but most are SNMP based which are not very accurate, averaging the numbers over several minutes. If you need to really know the utilization, including bursts and micro bursts then a packet capture is very useful tool.



*Utilization by the second*

It's these short bursts of high utilization that cause buffer overruns and lost packets which people can't see with other monitoring tools.



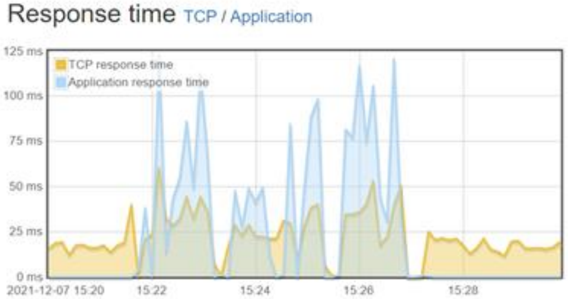
This table shows you down to 1ms how many times you have (briefly) hit 100% utilization.

### 2. Slow Response Times

The most frustrating thing in networking is slow response problems when the network is not busy. Packet captures contain the information you need to see how long it's taking the data to get from one end to the other, usually by looking at the TCP response times.

Better tools can help out with bounce charts and tables to make this easier to read.

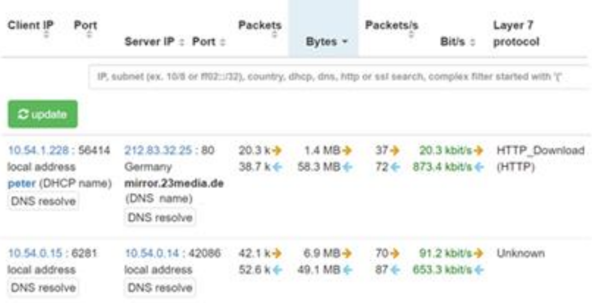
In this next graph we compare the network response times (in yellow) to the time it takes the server to react with a data frame (in blue).



### 3. Who's talking to who? Migrating sites and servers

Knowing who (or what) is taking up your bandwidth is always a popular piece of information.

Use cases we have seen include monitoring remote sites and old servers getting ready for migration and prepping firewall rules for such moves.

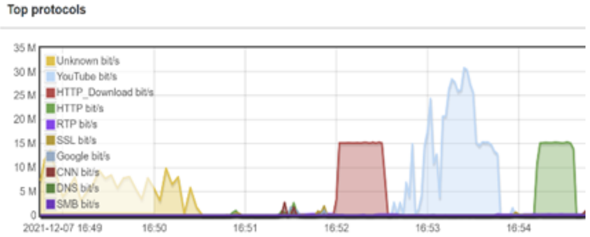


IP, subnet (ex. 10/8 or ff02::/32), country, dhcp, dns, http or ssl search, complex filter started with '('

| Client IP : Port | Server IP : Port | Packets | Bytes | Packets/s | Bit/s | Layer 7 protocol |
|---|---|---|---|---|---|---|
| 10.54.1.228 : 56414<br>local address<br>peter (DHCP name)<br>DNS resolve | 212.83.32.25 : 80<br>Germany<br>mirror.23media.de<br>(DNS name)<br>DNS resolve | 20.3 k →<br>38.7 k ← | 1.4 MB →<br>58.3 MB ← | 37 →<br>72 ← | 20.3 kbit/s →<br>873.4 kbit/s ← | HTTP_Download<br>(HTTP) |
| 10.54.0.15 : 6281<br>local address<br>DNS resolve | 10.54.0.14 : 42086<br>local address<br>DNS resolve | 42.1 k →<br>52.6 k ← | 6.9 MB →<br>49.1 MB ← | 70 →<br>87 ← | 91.2 kbit/s →<br>653.3 kbit/s ← | Unknown |

## 4. What Protocols are out there?

The mix of protocols on your network will always surprise you. Sometimes it's the percentage of social media content, other times its things you had never considered or forgotten about.

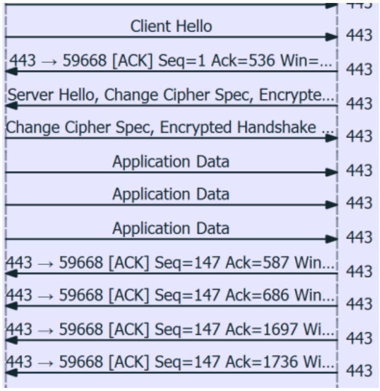


This information is key to keeping control of the work / life / security balance in the LAN and WAN.

Here we are displaying the top 10 protocols and their profiles over time.

## 5. Is it an Application Issue?

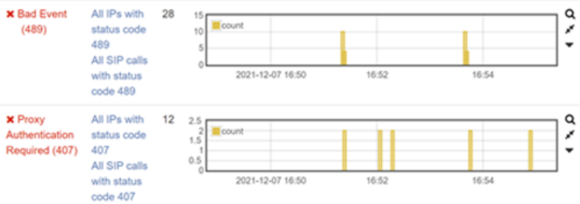
Working out how the application is communicating can give you solid information on how its responding and whether it's waiting on back-end services to fulfil the user's requests. One of the great ways to see this is with a bounce chart.



```
Client Hello                                    443
443 → 59668 [ACK] Seq=1 Ack=536 Win=...         443
Server Hello, Change Cipher Spec, Encrypte...   443
Change Cipher Spec, Encrypted Handshake ...     443
Application Data                                443
Application Data                                443
Application Data                                443
443 → 59668 [ACK] Seq=147 Ack=587 Win...        443
443 → 59668 [ACK] Seq=147 Ack=686 Win...        443
443 → 59668 [ACK] Seq=147 Ack=1697 Wi...        443
443 → 59668 [ACK] Seq=147 Ack=1736 Wi...        443
```

## 6. Poor Quality Voice and Video

We rely on good quality voice and video now, whether at work or at the home office, so when call quality becomes an issue we need to see where in the system things have gone wrong.



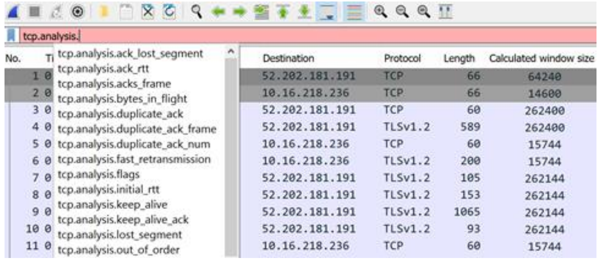
| | | | |
|---|---|---|---|
| ✖ Bad Event (489) | All IPs with status code 489<br>All SIP calls with status code 489 | 28 | |
| ✖ Proxy Authentication Required (407) | All IPs with status code 407<br>All SIP calls with status code 407 | 12 | |

Here we have two different call set up issues identified and can drill in to see the IP addresses involved.

## 7. Finding IPs / Protocols / Errors that you want / don't want to see

Once you have the capture data you can mine it for more detailed information you need to know.

Below is an example of the options for searching for TCP errors in a capture.

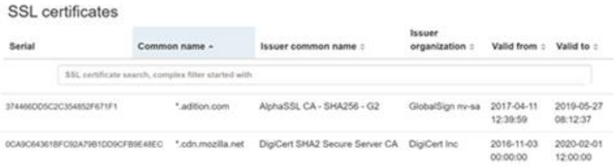


```
tcp.analysis.

No.  Ti  tcp.analysis.ack_lost_segment       Destination      Protocol  Length  Calculated window size
  1 0   tcp.analysis.ack_rtt                 52.202.181.191   TCP           66    64240
  2 0   tcp.analysis.acks_frame              10.16.218.236    TCP           66    14600
  3 0   tcp.analysis.bytes_in_flight         52.202.181.191   TCP           60   262400
  4 0   tcp.analysis.duplicate_ack           52.202.181.191   TLSv1.2      589   262400
  5 0   tcp.analysis.duplicate_ack_frame     10.16.218.236    TCP           60    15744
  6 0   tcp.analysis.duplicate_ack_num       10.16.218.236    TLSv1.2      200    15744
  7 0   tcp.analysis.fast_retransmission     52.202.181.191   TLSv1.2      105   262144
  8 0   tcp.analysis.flags                   52.202.181.191   TLSv1.2      153   262144
  9 0   tcp.analysis.initial_rtt             52.202.181.191   TLSv1.2     1065   262144
 10 0   tcp.analysis.keep_alive              52.202.181.191   TLSv1.2       93   262144
 11 0   tcp.analysis.keep_alive_ack          10.16.218.236    TCP           60    15744
        tcp.analysis.lost_segment
        tcp.analysis.out_of_order
```

## 8. Network Security

Captures have always been something security teams fall back on. Most modern solutions will monitor for log events and "threats" and then reference the part of the capture that contains the details they need to see.



SSL certificates

| Serial | Common name ▴ | Issuer common name ⇕ | Issuer organization ⇕ | Valid from ⇕ | Valid to ⇕ |
|---|---|---|---|---|---|
| SSL certificate search, complex filter started with | | | | | |
| 374460D05C2C354852F671F1 | *.adition.com | AlphaSSL CA - SHA256 - G2 | GlobalSign nv-sa | 2017-04-11 12:39:59 | 2019-05-27 08:12:37 |
| 0CA9C643618FC92A79B1DD9CFB9E48EC | *.cdn.mozilla.net | DigiCert SHA2 Secure Server CA | DigiCert Inc | 2016-11-03 00:00:00 | 2020-02-01 12:00:00 |

In this example we are checking that SSL certificates are valid and not about to expire.