Protocol Deep Dive

Anritsu
Advancing beyond

Executive Summary

> “While rolling out 5G, it gave full visibility of all the network protocols and procedures, which helped us isolate the root cause to particular protocols that were simply impossible to see and understand with other tools.”

Anritsu’s Protocol Deep Dive provides complete visibility and clear decoding of lower-level stack protocols, providing new and deeper troubleshooting capabilities and use cases.

Drive Testing Support
Quickly decode PCAPs recorded during drive tests or by test equipment devices.

Security Threat Detection
Identify potential security threats such as unauthorised access attempts, malware, or denial-of-service attacks.

Protocol Compliance Verification
Verify if network devices and user equipment are complying with protocols and standards.

Security Policy Verification
Verify if network security policies are being implemented and enforced correctly.

New Equipment Validation
Validate the performance, conformance and compliance of new equipment roll-outs to the network.

Network Equipment Malfunction Analysis
Diagnose problems with routers, switches and other network equipment such as routing loops and traffic black-holing.

Overview

> “Troubleshooting often requires use of PCAP, but how do ensure that its use is secure.”

Anritsu’s Protocol Deep Dive is a sophisticated tool designed to provide telecom network professionals with comprehensive, low-level visibility into packet data, enabling complex troubleshooting and analysis. This solution is ideal for users needing to dissect and analyse protocol details within complex network environments, offering a seamless experience that integrates with existing tools and workflows.

Protocol Deep Dive allows users to access and decode lower-level protocol information that traditional call-trace tools miss. With advanced packet capture capabilities, users gain insights into TCP, RTP, and other protocol sequences, essential for identifying gaps, troubleshooting socket set-ups, and monitoring packet-level corruption. This capability is particularly beneficial during 5G roll-outs, where it provides end-to-end visibility across all protocols, supporting root cause analysis (RCA) when traditional tools fall short.

Beyond troubleshooting, Protocol Deep Dive supports diverse use cases, from drive testing and security threat detection to verifying compliance with protocol standards and diagnosing network equipment issues. The tool’s design allows users to follow streams, apply refined search filters, and view packet summaries and raw dumps, ensuring users can drill down to the essential details.

The user-friendly interface supports a range of usage scenarios and provides secure, embedded access without the need for third-party software, which enhances data security by keeping sensitive packet data within a protected environment.

Overall, Protocol Deep Dive stands out for its ability to streamline the process of in-depth network analysis. It minimises the time-to-resolution for network issues and offers a robust solution for anyone needing visibility into low-level network details.

Protocol Deep Dive is an invaluable asset for telecoms troubleshooting teams requiring efficient, secure, and comprehensive network management.

> “When establishing links with other operators, Protocol Deep Dive allows us to understand what is wrong at the signalling level between multiple network elements involved in the packet flows. Heartbeats, message duplications, and gaps in the traffic are clearly visible, and the analysis can be completed with only a few clicks.”

Value

> “Protocol Deep Dive is an invaluable asset for telecoms troubleshooting teams requiring efficient, secure, and comprehensive network management.”

Improved Visibility

Additional visibility of low-level protocols opens up all traffic for inspection and analysis. This exposes deeper root cause analysis to troubleshooting engineers.

Reduced MTTR

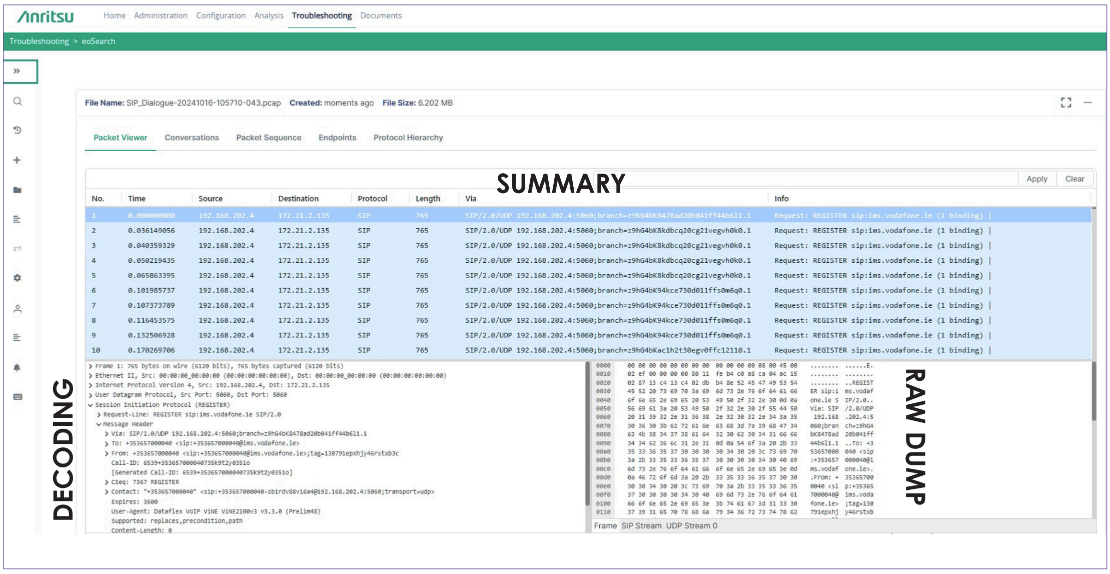
Seamless integration with Anritsu's solution suite ensures faster, more efficient troubleshooting workflows which has been shown to speed up MTTR by 65%.

Improved Security

Investigation happens within the controlled and safe solution environment without the requirements for 3rd-party software or insecure PCAP exports.

Screenshots

PACKET VIEWER



File Name: SIP_Dialogue-20241016-105710-043.pcap **Created:** moments ago **File Size:** 6.202 MB

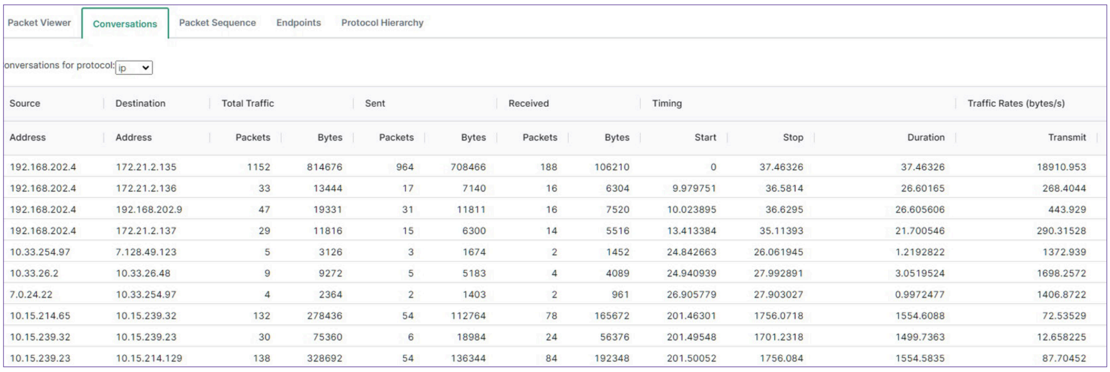
Packet Viewer | Conversations | Packet Sequence | Endpoints | Protocol Hierarchy

No.	Time	Source	Destination	Protocol	Length	Via	Info
1	0.000000000	192.168.202.4	172.21.2.135	SIP	765	SIP/2.0/UDP 192.168.202.4:5060;branch=z9hG4bK8478ad20b041ff44b6l1.1	Request: REGISTER sip:ims.vodafone.ie (1 binding) |
2	0.036149056	192.168.202.4	172.21.2.135	SIP	765	SIP/2.0/UDP 192.168.202.4:5060;branch=z9hG4bK8kdbcq20cg21vegvh0k0.1	Request: REGISTER sip:ims.vodafone.ie (1 binding) |
3	0.040359329	192.168.202.4	172.21.2.135	SIP	765	SIP/2.0/UDP 192.168.202.4:5060;branch=z9hG4bK8kdbcq20cg21vegvh0k0.1	Request: REGISTER sip:ims.vodafone.ie (1 binding) |
4	0.050219435	192.168.202.4	172.21.2.135	SIP	765	SIP/2.0/UDP 192.168.202.4:5060;branch=z9hG4bK8kdbcq20cg21vegvh0k0.1	Request: REGISTER sip:ims.vodafone.ie (1 binding) |
5	0.065863395	192.168.202.4	172.21.2.135	SIP	765	SIP/2.0/UDP 192.168.202.4:5060;branch=z9hG4bK8kdbcq20cg21vegvh0k0.1	Request: REGISTER sip:ims.vodafone.ie (1 binding) |
6	0.101985737	192.168.202.4	172.21.2.135	SIP	765	SIP/2.0/UDP 192.168.202.4:5060;branch=z9hG4bK94kce730d011ffs0m6q0.1	Request: REGISTER sip:ims.vodafone.ie (1 binding) |
7	0.107373789	192.168.202.4	172.21.2.135	SIP	765	SIP/2.0/UDP 192.168.202.4:5060;branch=z9hG4bK94kce730d011ffs0m6q0.1	Request: REGISTER sip:ims.vodafone.ie (1 binding) |
8	0.116453575	192.168.202.4	172.21.2.135	SIP	765	SIP/2.0/UDP 192.168.202.4:5060;branch=z9hG4bK94kce730d011ffs0m6q0.1	Request: REGISTER sip:ims.vodafone.ie (1 binding) |
9	0.132506928	192.168.202.4	172.21.2.135	SIP	765	SIP/2.0/UDP 192.168.202.4:5060;branch=z9hG4bK94kce730d011ffs0m6q0.1	Request: REGISTER sip:ims.vodafone.ie (1 binding) |
10	0.170269706	192.168.202.4	172.21.2.135	SIP	765	SIP/2.0/UDP 192.168.202.4:5060;branch=z9hG4bKac1h2t30egv0ffc12110.1	Request: REGISTER sip:ims.vodafone.ie (1 binding) |

```
> Frame 1: 765 bytes on wire (6120 bits), 765 bytes captured (6120 bits)
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 192.168.202.4, Dst: 172.21.2.135
> User Datagram Protocol, Src Port: 5060, Dst Port: 5060
v Session Initiation Protocol (REGISTER)
  > Request-Line: REGISTER sip:ims.vodafone.ie SIP/2.0
  v Message Header
    > Via: SIP/2.0/UDP 192.168.202.4:5060;branch=z9hG4bK8478ad20b041ff44b6l1.1
    > To: +353657000040 <sip:+353657000040@ims.vodafone.ie>
    > From: +353657000040 <sip:+353657000040@ims.vodafone.ie>;tag=130791epxhjy46rstxb3c
      Call-ID: 6539+353657000040735k9t2y0351o
      [Generated Call-ID: 6539+353657000040735k9t2y0351o]
    > CSeq: 7367 REGISTER
    > Contact: "+353657000040" <sip:+353657000040-sbirdv88vi6a4@192.168.202.4:5060;transport=udp>
      Expires: 3600
      User-Agent: Dataflex VoIP ViNE ViNE2100v3 v3.3.0 (Prelim48)
      Supported: replaces,precondition,path
      Content-Length: 0
```

```
0000   00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00   ........ ......E.
0010   02 ef 00 00 00 00 80 11  fe b4 c0 a8 ca 04 ac 15   ........ ........
0020   02 87 13 c4 13 c4 02 db  b4 8e 52 45 47 49 53 54   ........ ..REGIST
0030   45 52 20 73 69 70 3a 69  6d 73 2e 76 6f 64 61 66   ER sip:i ms.vodaf
0040   6f 6e 65 2e 69 65 20 53  49 50 2f 32 2e 30 0d 0a   one.ie S IP/2.0..
0050   56 69 61 3a 20 53 49 50  2f 32 2e 30 2f 55 44 50   Via: SIP /2.0/UDP
0060   20 31 39 32 2e 31 36 38  2e 32 30 32 2e 34 3a 35    192.168 .202.4:5
0070   30 36 30 3b 62 72 61 6e  63 68 3d 7a 39 68 47 34   060;bran ch=z9hG4
0080   62 4b 38 34 37 38 61 64  32 30 62 30 34 31 66 66   bK8478ad 20b041ff
0090   34 34 62 36 6c 31 2e 31  0d 0a 54 6f 3a 20 2b 33   44b6l1.1 ..To: +3
00a0   35 33 36 35 37 30 30 30  30 34 30 20 3c 73 69 70   53657000 040 <sip
00b0   3a 2b 33 35 33 36 35 37  30 30 30 30 34 30 40 69   :+353657 000040@i
00c0   6d 73 2e 76 6f 64 61 66  6f 6e 65 2e 69 65 3e 0d   ms.vodaf one.ie>.
00d0   0a 46 72 6f 6d 3a 20 2b  33 35 33 36 35 37 30 30   .From: + 35365700
00e0   30 30 34 30 20 3c 73 69  70 3a 2b 33 35 33 36 35   0040 <si p:+35365
00f0   37 30 30 30 30 34 30 40  69 6d 73 2e 76 6f 64 61   7000040@ ims.voda
0100   66 6f 6e 65 2e 69 65 3e  3b 74 61 67 3d 31 33 30   fone.ie> ;tag=130
0110   37 39 31 65 70 78 68 6a  79 34 36 72 73 74 78 62   791epxhj y46rstxb
```

CONVERSATIONS

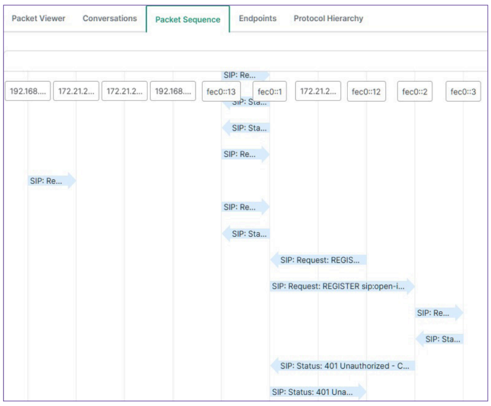


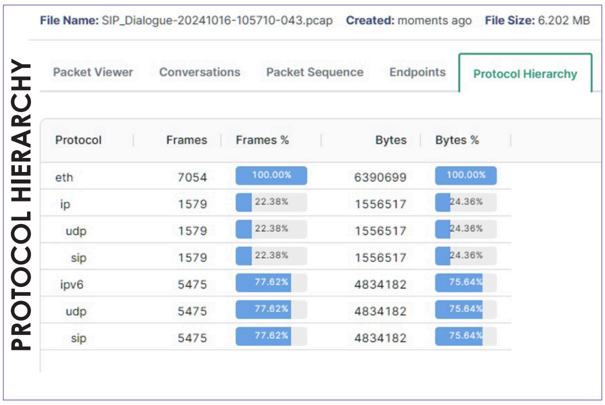
Packet Viewer | Conversations | Packet Sequence | Endpoints | Protocol Hierarchy

onversations for protocol: ip

Source	Destination	Total Traffic		Sent		Received		Timing			Traffic Rates (bytes/s)
Address	Address	Packets	Bytes	Packets	Bytes	Packets	Bytes	Start	Stop	Duration	Transmit
192.168.202.4	172.21.2.135	1152	814676	964	708466	188	106210	0	37.46326	37.46326	18910.953
192.168.202.4	172.21.2.136	33	13444	17	7140	16	6304	9.979751	36.5814	26.60165	268.4044
192.168.202.4	192.168.202.9	47	19331	31	11811	16	7520	10.023895	36.6295	26.605606	443.929
192.168.202.4	172.21.2.137	29	11816	15	6300	14	5516	13.413384	35.11393	21.700546	290.31528
10.33.254.97	7.128.49.123	5	3126	3	1674	2	1452	24.842663	26.061945	1.2192822	1372.939
10.33.26.2	10.33.26.48	9	9272	5	5183	4	4089	24.940939	27.992891	3.0519524	1698.2572
7.0.24.22	10.33.254.97	4	2364	2	1403	2	961	26.905779	27.903027	0.9972477	1406.8722
10.15.214.65	10.15.239.32	132	278436	54	112764	78	165672	201.46301	1756.0718	1554.6088	72.53529
10.15.239.32	10.15.239.23	30	75360	6	18984	24	56376	201.49548	1701.2318	1499.7363	12.658225
10.15.239.23	10.15.214.129	138	328692	54	136344	84	192348	201.50052	1756.084	1554.5835	87.70452

PACKET SEQUENCE





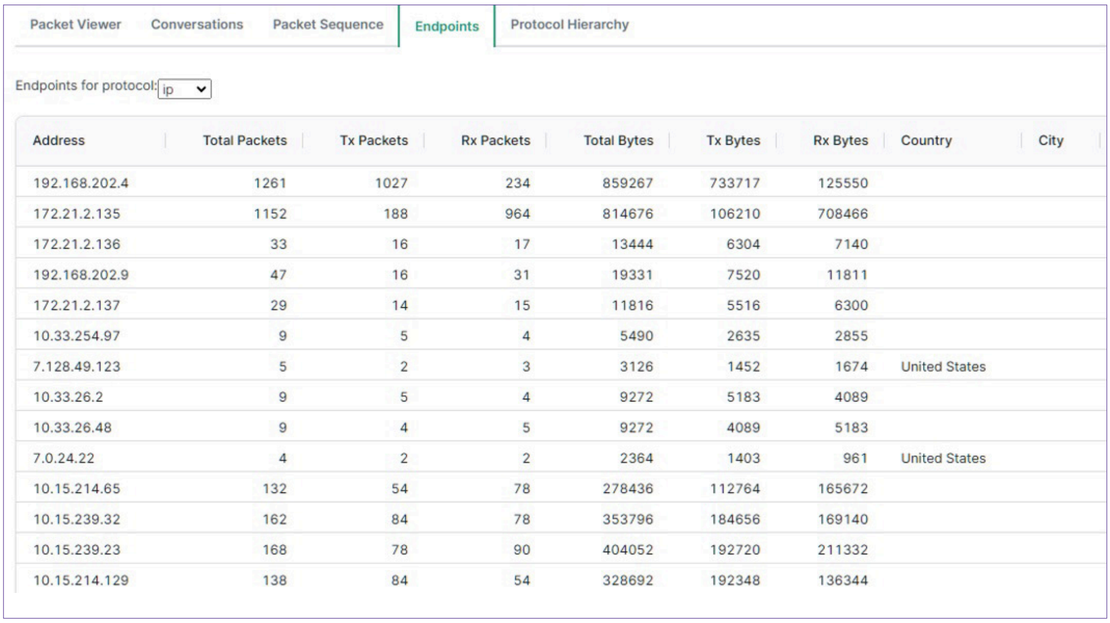
PROTOCOL HIERARCHY

File Name: SIP_Dialogue-20241016-105710-043.pcap **Created:** moments ago **File Size:** 6.202 MB

Packet Viewer | Conversations | Packet Sequence | Endpoints | Protocol Hierarchy

Protocol	Frames	Frames %	Bytes	Bytes %
eth	7054	100.00%	6390699	100.00%
ip	1579	22.38%	1556517	24.36%
udp	1579	22.38%	1556517	24.36%
sip	1579	22.38%	1556517	24.36%
ipv6	5475	77.62%	4834182	75.64%
udp	5475	77.62%	4834182	75.64%
sip	5475	77.62%	4834182	75.64%

ENDPOINTS



Packet Viewer | Conversations | Packet Sequence | Endpoints | Protocol Hierarchy

Endpoints for protocol: ip

Address	Total Packets	Tx Packets	Rx Packets	Total Bytes	Tx Bytes	Rx Bytes	Country	City
192.168.202.4	1261	1027	234	859267	733717	125550		
172.21.2.135	1152	188	964	814676	106210	708466		
172.21.2.136	33	16	17	13444	6304	7140		
192.168.202.9	47	16	31	19331	7520	11811		
172.21.2.137	29	14	15	11816	5516	6300		
10.33.254.97	9	5	4	5490	2635	2855		
7.128.49.123	5	2	3	3126	1452	1674	United States	
10.33.26.2	9	5	4	9272	5183	4089		
10.33.26.48	9	4	5	9272	4089	5183		
7.0.24.22	4	2	2	2364	1403	961	United States	
10.15.214.65	132	54	78	278436	112764	165672		
10.15.239.32	162	84	78	353796	184656	169140		
10.15.239.23	168	78	90	404052	192720	211332		
10.15.214.129	138	84	54	328692	192348	136344		

Anritsu

Advancing beyond

Anritsu A/S
c/o Regus Winghouse
Ørestads Boulevard 73, 4th floor
2300 Copenhagen S
Denmark
Phone: +45 (0) 7211-2200

info@anritsu.com