Protocol Deep Dive



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-ofservice 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.



"

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 lowerlevel 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 packetlevel corruption. This capability is particularly beneficial during 5G roll-outs, where it provides end-toend 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 thirdparty 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-toresolution 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

Т	Troubleshooting > (eoSearch											
	>>												
-	-	File Name: SIP_Dialogue-202	41016-105710-043.pca	Created: moments	ago File Size: 6.20	2 MB							Ω.
	Э	Packet Viewer Conver	rsations Packet Sec	uence Endpoints	Protocol Hierarch	hy							
	+												Apply Clear
		No. Time	Source	Destination	Protocol Lengt	th Via	SUWN	ARY		Info			Apply Clear
	E	2 0.036149056 3 0.040359329			SIP 765 SIP 765 SIP 765			4:5060;branch=29h64b8 4:5060;branch=29h64b8				odafone.ie (1 binding) odafone.ie (1 binding) odafone.ie (1 binding)	
	•	4 0.050219435 5 0.065863395	192.168.202.4	172.21.2.135	SIP 765 SIP 765	SIP/2.0/	UDP 192.168.202.	4:5060;branch=z9hG4b8 4:5060;branch=z9hG4b8	8kdbcq20cg21vegvh0k0	1 Request:	REGISTER sip:ims.v	odafone.ie (1 binding) odafone.ie (1 binding)	
	•	6 0.101985737 7 0.107373789	192.168.202.4	172.21.2.135	SIP 765 SIP 765	SIP/2.0/	UDP 192.168.202.	4:5060;branch=z9hG4b8 4:5060;branch=z9hG4b8	94kce730d011ffs0m6q0	1 Request:	REGISTER sip:ims.v	odafone.ie (1 binding) odafone.ie (1 binding)	
	E	8 0.116453575 9 0.132506928			SIP 765 SIP 765			4:5060;branch=29hG4bK 4:5060;branch=29hG4bK				odafone.ie (1 binding) odafone.ie (1 binding)	
	A.	10 0.170269706 > Frame 1: 765 bytes on wire > Ethernet II, Src: 00:00:00	(6120 bits), 765 bytes c	eptured (6120 bits)	SIP 765		UDP 192.168.202.	4:5060;branch=29hG4bx	ac1h2t30egv0ffc12110 00 00 00 00 00 00 00 00 00 00 00 00 00	1 Request:	······	odafone.ie (1 binding)	
	□ U	 Internet Protocol Version 4 User Datagram Protocol, Src Session Initiation Protocol 	<pre>i, Src: 192.168.202.4, Ds Port: 5060, Dst Port: 5 (REGISTER)</pre>	:: 172.21.2.135 NGO				0020 02 87 13 0030 45 52 20 0040 6f 6e 65 0050 56 69 61	00 00<	45 47 49 53 54 76 6f 64 61 66 32 2e 38 6d 63 38 2f 55 44 58	REGIST ER sip:1 ms.vodaf one.ie S IP/2.0 Via: SIP /2.0/UDP	RAW	
	DECODIN	> CSeq: 7367 REGISTER > Contact: "+353657000044 Expires: 3600	68.202.4:5860;branch=20h :+353657000040@ims.voda fp:+353657000040@ims.voda 00409735k312y03510 20+353657000040735k312y02 0° <sip:+353657000040-sbi 01P ViNE VINE2100V3 V3.3.</sip:+353657000040-sbi 	4bk54-75ad29b041ff44b6] ne.ie> fone.ie>;tag=13079iep> Sio] rdv35vi6a4ĝ192.160.202	hjy46rstxb3c			esis 56 69 31 39 eera 20 31 39 56 30 11 39 eera 20 31 30 56 30 11 39 66 31 31 30 66 32 32 66 33 35 35 66 66 73 32 66 63 63 73 22 66 33 35 66 66 73 22 66 33 35 66 63 63 73 22 66 33 35 66 63 63 73 22 66 33 35 66 63 63 73 73 33 36 613 63 63 73 75 31 36 613 63 73 75 31 36 63 63 73 75 31 31 36 36 36 36 36 36 <	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	192.168 .202.415 000;tran ch21564 000;tran ch21564 00441ff 00441f1 .70: -3 5355700 446 <52 -53557 0044081 ms.vodsf one.1e>, .from: +353670 0044081 p:+35365 00440 421 p:+35365 00440 421 p:+35365 004404 p:+5356 004404 p:+5366 004404 p:+53	V DUMP	
P	Packet Viewer	Conversations Pa	cket Sequence	Endpoints Pro	tocol Hierarchy								
or	nversations for p	irotocol: ip 🗸											
S	Source	Destination	Total Traffic		Sent		Received) 1	iming			Traffic	Rates (bytes/s)
	Address	Address	Packets	Bytes	Packets	Bytes	Packets	Bytes	Start	Stop		Duration	Transmi
	192.168.202.4 192.168.202.4	172.21.2.135 172.21.2.136	1152	814676 13444	964 17	708466 7140	188	106210 6304	0 9.979751	37.46326 36.5814		37.46326 26.60165	18910.95 268.404
	192.168.202.4	192.168.202.9	47	19331	31	11811	16	7520	10.023895	36.6295		26.605606	443.92
	192.168.202.4 10.33.254.97	172.21.2.137 7.128.49.123	29	11816 3126	15 3	6300 1674	14	5516 1452	13.413384 24.842663	35.11393 26.061945		21.700546 1.2192822	290.3152 1372.93
	10.33.26.2	10.33.26.48	9	9272	5	5183	4	4089	24.940939	27.992891		3.0519524	1698.257
10. ⁻	7.0.24.22	10.33.254.97 10.15.239.32	4	2364 278436	2 54	1403 112764	2	961 165672	26.905779 201.46301	27.903027 1756.0718		0.9972477 1554.6088	1406.872 72.5352
	10.15.239.32	10.15.239.23 10.15.214.129	30 138	75360 328692	6 54	18984 136344	24 84	56376 192348	201.49548 201.50052	1701.2318 1756.084		1499.7363 1554.5835	12.65822
	192 168 172 21	172 21 2 192 168	SIP: Re	1 172 21 2	ac0::12 fac0::2	fector:3	⊁ੁ	acket Viewer	Conversations	Packet	Sequence	Endpoints Pro	tocol Hierarchy
	SIP: Re	(2) (¥2212) (¥2248	sep: Sum SP: Stan SP: Re SP: Re SP: Stan	SIP: Request: REGIS. P: Request: REGISTE SIP: Status: 401 Una	R sip:open-i SIP: F	fec0:3		acket Viewer protocol th ip udp sip sip sip		Packet Comment Co		ytes Bytes % 699 100.00% 517 24.36% 517 24.36% 517 24.36% 182 75.64%	tocol Hierarchy
	SIP: Re	Jiewer Conve	sp: sta sp: sta sp: sta sp: sta sp: sta sp: sta sp: sta sp: sta	SIP: Request: REGIS P: Request: REGISTE	a Bipopen L. SiP I	Re		th ip udp sip ipv6 udp	Frames I 7054 I 1579 I 1579 I 1579 I 5475 I 5475 I	Trames % 100.00% 22.38% 22.38% 22.38% 22.38% 77.62%	Br 6390 1556 1556 1556 4834 4834	ytes Bytes % 699 100.00% 517 24.36% 517 24.36% 517 24.36% 182 75.64%	tocol Hierarchy
	SIP: Re	Viewer Conve	SIP: Re SIP: Re SIP: Re SIP: Re SIP: Re SIP: Sta SIP: Sta SIP: Sta SIP: Sta SIP: Sta SIP: Sta SIP: Sta SIP: Sta SIP: Sta	SP: Request: REDIS P: Request: REDIST SIP: Status: 401 Una P: Status: 401 Una P: Status: 401 Una	a Bipopen L. SiP I	Re	Protocol HIERARC	rotocol th ip udp sip sip sip	Frames I 7054 1 1579 1 1579 1 5475 5 5475 5	I 00.00% 22.38% 22.38% 22.38% 77.62%	Br 6390 1556 1556 1556 4834 4834	ytes Bytes % 699 100.00% 517 24.36% 517 24.36% 517 24.36% 182 75.64%	City
	Packet V Endpoints t	Viewer Conve for protocol:	sp: sta sp: sta sp: sta sp: sta sp: sta sp: sta	SIP: Request REOIS SIP: Request REOISTE SIP: Status: 401 Una Packet Seque ts Tx	a sipopent. Sip- sipotent Sip- sipotent Sip- sipotent Sipotent Sipotent Sipotent Sipotent Sip	Re P: Sta	Protocol HIERARC	rrotocol th ip udp sip sip sip Hierarchy	Frames I 7054 1 1579 1 1579 1 5475 5 5475 5	rames % 100.00% 22.38% 22.38% 22.38% 77.62% 77.62%	B 6390 1556 1556 4834 4834 4834	ytes Bytes % 699 100.00% 517 24.36% 517 24.36% 517 24.36% 517 24.36% 182 75.64% 182 75.64%	
	Packet V Endpoints I	Viewer Conve for protocol:	sp: sta sp: sta	SP: Request: REDIST SP: Request: REDISTE SP: Status: 401 Una SP: Status: 401 Una Packet Seque ts Tx 1	spoorn-L spo	Re P: Sta	Protocol	rotocol th ip udp sip udp sip Hierarchy Total Bytes	Frames 1 7054 1 1579 1 1579 1 5475 5 5475 5 5475 1	Trames % 100.00% 22.38% 22.38% 77.62% 77.62% 77.62% Res	84 6390 1556 1556 4834 4834 4834 4834 8834	ytes Bytes % 699 100.00% 517 24.36% 517 24.36% 517 24.36% 517 24.36% 182 75.64% 182 75.64%	
	Packet V Endpoints I Address 192.166	Viewer Conve for protocol:	rsations F Total Packet 126 115	SP: Request: REDIST SP: Request: REDISTE SP: Status: 401 Una SP: Status: 401 Una Packet Seque ts Tx 1	sported = C Packets 1027	Re P: Sta	Protocol	rotocol th ip udp sip dip sip sip Hierarchy Total Bytes 859267	Frames I 7054 1 1579 1 1579 1 5475 5 5475 5 5475 1 Tx Byl 7337	rames % 100.00% 22.38% 22.38% 77.62% 77.62% 77.62% 17.62% 17.107 10	B 6390 1556 1556 4834 4834 4834 4834 4834 2834 8834 2835 125550	ytes Bytes % 699 100.00% 517 24.36% 517 24.36% 517 24.36% 517 24.36% 182 75.64% 182 75.64%	
	Packet V Endpoints I Address 192.166	Viewer Conve for protocol: s 8.202.4 .2.135 .2.136	rsations F Total Packet 126 115	SP: Request: REDIST P: Request: REDIST SIP: Status: 401 Una P: Status: 401 Una P: Status: 401 Una 1 2 3	series series ence Enc Packets 1027 188	Re P: Sta	Protocol	rotocol th ip udp sip bip bip bip bip bip bip bip b	Frames I 7054 1 1579 1 1579 1 5475 5 5475 1 5475 1 7054 1 70337 1062	rames % 100.00% 22.38% 22.38% 22.38% 77.62% 77.62% 77.62% 17.62% 17 10 04	B 6390 1556 1556 4834 4834 4834 4834 4834 12555 708466	ytes Bytes % 699 100.00% 517 24.36% 517 24.36% 517 24.36% 517 24.36% 182 75.64% 182 75.64%	
	Packet V Endpoints 1 Address 192.168 172.21. 192.168 172.21.	Viewer Conve for protocol: [jp s 8.202.4 2.135 2.136 8.202.9 2.137	Total Packet 1125 1125 1125 1125 1125 1125 1125 112	SIP: Request: REDIS: P: Request: REDIS: SIP: Statue: 401 Una P: Statue	Ripopent. SIP / I simulation SIP / I simulation SIP / I simulation SIP / I simulation Ence Packets I 1027 188 16 16 14 I	Re P: Sta	Protocol	rotocol th ip udp sip sip dup sip Hierarchy Total Bytes 859267 814676 13444	Frames I 7054 1 1579 1 1579 1 5475 1 5475 1 5475 1 7337 1062 63 1	rames % 100.00% 22.38% 22.38% 22.38% 77.62% 77.62% 77.62% 117 10 04 20	Rx Bytes 125550 708466 7140	ytes Bytes % 699 100.00% 517 24.36% 517 24.36% 517 24.36% 517 24.36% 182 75.64% 182 75.64%	
	Packet V Endpoints 1 Address 192.168 172.21. 192.168 172.21. 192.168	Viewer Conve for protocol: ip s 8.202.4 .2.135 .2.136 8.202.9 .2.137 .2.137	Total Packet 126 15 15 15 15 15 15 15 15 15 15 15 15 15	SIP: Request: REDIS: P: Request: REDISTE SIP: Status: 401 Una P: Statu	since Enc Packets 1027 188 16 16 16 14 5	Re P: Sta	Protocol	rotocol th ip udp sip sip dup sip Hierarchy Total Bytes 859267 814676 13444 19331 11816 5490	Frames I 7054 1 1579 1 1579 1 5475 5 5475 5 5475 1 7337 1062 63 75 55 26	rames % 100.00% 22.38% 22.38% 77.62% 77.62% 77.62% 10 10 04 20 16 35	Rx Bytes 125550 708466 7140 11811 6300 2855	ytes Bytes % 699 100.00% 517 24.36% 517 24.36% 182 75.64% 182 75.64% 182 75.64% 182 75.64%	
	Packet V Endpoints I Address 192.168 172.21. 172.21. 192.168 172.22. 10.33.2 7.128.4	Viewer Conve for protocol: ip s 8.202.4 .2.135 .2.136 8.202.9 .2.137 .554.97 19.123	reations F Total Packet 115 34 4	SIP: Request: REOISTE SIP: Status: 401 Una Pr: Status: 401 Una Pr: Status: 401 Una Pracket Seque 1 2 3 7 9 9 5	SB000m-L SB01 SB01 SB01 Sance Ence Packets 1027 188 16 16 14 5 2	Re P: Sta	Protocol	rotocol th ip udp sip ipv6 udp sip Hierarchy Total Bytes 859267 814676 13444 19331 11816 5490 3126	Frames I 7054 1 1579 1 1579 1 5475 5 5475 5 5475 5 7377 1062 63 75 55 55 26 14	rames % 100.00% 22.38% 22.38% 22.38% 77.62% 77.62% 77.62% 10 10 04 20 16 35 52	Rx Bytes 125550 708466 7140 11811 6300 2855 1674	ytes Bytes % 699 100.00% 517 24.36% 517 24.36% 517 24.36% 517 24.36% 182 75.64% 182 75.64%	
	Packet V Endpoints I Address 192.168 172.21. 172.21. 192.168 172.21. 10.33.2 7.128.4 10.33.2	Viewer Conve for protocol: s 8.202.4 2.135 2.136 8.202.9 2.137 554.97 9.123 16.2	recorts feed spr. sta. spr. spr. spr. spr. spr. spr. spr. spr.	SP: Request REOS SP: Request REOISTE SP: Status: 401 Una Packet Seque 1 2 3 7 9 9 9 9	Spooen-L. Spooen-L.	Re P: Sta	Protocol	rotocol th ip udp sip dip sip Hierarchy Total Bytes 859267 814676 13444 19331 11816 5490 3126 9272	Frames I 7054 1 1579 1 1579 1 5475 5 5475 5 5475 1 7337 1062 63 75 55 26 14 51	rames % 100.00% 22.38% 22.38% 22.38% 77.82% 77.82% 77.82% 117 10 04 20 16 35 52 83	Rx Bytes 125550 708466 7140 11811 6300 2855 1674 4089	ytes Bytes % 699 100.00% 517 24.36% 517 24.36% 182 75.64% 182 75.64% 182 75.64% 182 75.64%	
	Packet V Endpoints I Address 192.168 172.21. 172.21. 192.168 172.21. 10.33.2 7.128.4 10.33.2 10.33.2	Viewer Conve for protocol: s 202.4 2.135 2.136 8.202.9 2.137 154.97 19.123 16.2 16.48	record Packet SP: Sta SP: SP: SP: SP: SP: SP: SP: SP: SP: SP:	SIP: Request: REGIS SIP: Status: 401 Una Pr: Status: 401 Una Packet: Seque sauce 401 U	R Biospen-L. SIP 1 second SIP 1 second Ence Packets I 1027 188 16 16 14 5 2 5 4 1	Re P: Sta	Protocol	rotocol th ip udp sip ipv6 udp sip Hierarchy Hierarchy S59267 814676 13444 19331 11816 5490 3126 9272	Frames I 7054 1 1579 1 1579 1 5475 5 5475 5 5475 1 7337 1062 63 75 55 26 14 51 40 40	rames % 100.00% 22.38% 22.38% 22.38% 77.82% 77.82% 77.82% 117 10 04 20 16 35 52 83 89	Rx Bytes 125550 708466 1556 4834 4834 4834 4834 4834 4834 4834 483	Vites Bytes % 699 100.00% 517 24.36% 517 24.36% 182 75.64% 182 75.64% 182 75.64% 182 75.64% United States	
	Packet V Endpoints I Address 192.166 172.21. 172.21. 192.166 172.21. 10.33.2 7.128.4 10.33.2 7.024.2	Jiewer Conve for protocol: p s s 8.202.4	Total Packet 126 115 3 4 2	SIP: Request: REOIST SIP: Status: 401 Una SIP: Status: 401 Una P: Status: 401 Una	Signspen L Signspen L Signspen L Signspen L <t< td=""><td>Re P: Sta</td><td>Protocol</td><td>rotocol th ip udp sip ipv6 udp sip Hierarchy Hierarchy Total Bytes 859267 814676 13444 19331 11816 5490 3126 9272 9272 2364</td><td>Frames I 7054 1 1579 1 1579 1 5475 1 5475 1 5475 1 7337 1062 63 75 555 26 14 51</td><td>rames % 100.00% 22.38% 22.38% 22.38% 77.62% 77.62% 77.62% 17.62% 17.62% 16 16 15 52 83 89 03</td><td>Rx Bytes 125550 708466 1556 4834 4834 4834 4834 4834 4834 4834 483</td><td>ytes Bytes % 699 100.00% 517 24.36% 517 24.36% 182 75.64% 182 75.64% 182 75.64% 182 75.64%</td><td></td></t<>	Re P: Sta	Protocol	rotocol th ip udp sip ipv6 udp sip Hierarchy Hierarchy Total Bytes 859267 814676 13444 19331 11816 5490 3126 9272 9272 2364	Frames I 7054 1 1579 1 1579 1 5475 1 5475 1 5475 1 7337 1062 63 75 555 26 14 51	rames % 100.00% 22.38% 22.38% 22.38% 77.62% 77.62% 77.62% 17.62% 17.62% 16 16 15 52 83 89 03	Rx Bytes 125550 708466 1556 4834 4834 4834 4834 4834 4834 4834 483	ytes Bytes % 699 100.00% 517 24.36% 517 24.36% 182 75.64% 182 75.64% 182 75.64% 182 75.64%	
	Packet V Endpoints I Address 192.168 172.21. 172.21. 192.168 172.21. 10.33.2 7.128.4 10.33.2	Viewer Conve for protocol: ip s 8.202.4 .2.135 .2.136 8.202.9 .2.137 .5.4.97 .9.123 .6.2 .6.48 .22 .114.65	recorts feed spr sta spr spr spr spr spr spr spr spr spr spr	SP: Request: REOS SP: Request: REOSTE SIP: Status: 401 Una P: Status:	R Biospen-L. SIP 1 suborized - C SIP 1 ence Enc Packets I 1027 188 16 16 14 5 2 5 4 5	Re P: Sta	Protocol	rotocol th ip udp sip ipv6 udp sip Hierarchy Hierarchy S59267 814676 13444 19331 11816 5490 3126 9272	Frames I 7054 1 1579 1 1579 1 5475 5 5475 5 5475 1 7337 1062 63 75 55 26 14 51 40 40	rames % 100.00% 22.38% 22.38% 22.38% 77.62% 77.62% 77.62% 17.62% 17.62% 17.62% 16.35 52 83 89 03 64	Rx Bytes 125550 708466 1556 4834 4834 4834 4834 4834 4834 4834 483	Vites Bytes % 699 100.00% 517 24.36% 517 24.36% 182 75.64% 182 75.64% 182 75.64% 182 75.64% United States	

10.15.239.23

10.15.214.129

78

84

90

54

404052

328692

192720

192348

211332

136344

168

138

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