

Komunikasi Data dan Jaringan Komputer



Andhika Putra Ramadhan

09031181520015

DOSEN PEMBIMBING

Deris Stiawan, M.T. Ph.D.

SISTEM INFORMASI

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

The screenshot shows a packet capture analysis in Wireshark. The packet list pane at the top shows several packets, with packet 360 selected. The packet details pane shows the structure of the packet, including the Ethernet II header, Internet Protocol (IP) header, and Hypertext Transfer Protocol (HTTP) request. The HTTP request details show the method as GET, the path as /R/ASAKIGPhYzc3MTdmDdhZjZPaYVhVhNGUIZl, and the host as su.ff.avast.com. The packet bytes pane shows the raw data of the packet, including the flags, window, and request body.

Diketahui bahwa ip dari 10.102.224.65 adalah milik avast yang mengikuti alur internet dari pc yang telah terinstall avast tersebut.

The screenshot shows a packet capture analysis in Wireshark. The packet list pane at the top shows several packets, with packet 3277 selected. The packet details pane shows the structure of the packet, including the Ethernet II header, Internet Protocol (IP) header, and Hypertext Transfer Protocol (HTTP) response. The HTTP response details show the status as 200 OK, the content type as application/javascript, and the content length as 1420 bytes. The packet bytes pane shows the raw data of the packet, including the flags, window, and response body.

IP dari 216.239.32.65 adalah milik dari situs geotrust.com yang saling menghubungkan.

Top100 IPv4 Conversation(Full Analysis) - 172.217.24.227 - Packets

No.	Absolute Time	Source	Destination	Protocol	Size	Decode	Summary
1694	11:27:11.060042	10.102.224.65:50378	172.217.24.227:443	TCP	66		[SYN] Seq=3613121242,Ack=0000000000,L...
1695	11:27:11.060625	10.102.224.65:50379	172.217.24.227:443	TCP	66		[SYN] Seq=1962389537,Ack=0000000000,L...
1712	11:27:11.314123	10.102.224.65:50381	172.217.24.227:443	TCP	66		[SYN] Seq=3457332023,Ack=0000000000,L...
1755	11:27:12.093817	172.217.24.227:443	10.102.224.65:50379	TCP	68		[SYN, ACK] Seq=3088958518,Ack=1962389...
1756	11:27:12.093820	172.217.24.227:443	10.102.224.65:50378	TCP	68		[SYN, ACK] Seq=3034475979,Ack=3613121...
1757	11:27:12.094480	10.102.224.65:50379	172.217.24.227:443	TCP	54		[ACK] Seq=1962389538,Ack=3088958519,L...
1758	11:27:12.094658	10.102.224.65:50378	172.217.24.227:443	TCP	54		[ACK] Seq=3613121243,Ack=3034475980,L...
1760	11:27:12.097000	10.102.224.65:50379	172.217.24.227:443	HTTPS	259		Client Hello
1761	11:27:12.098700	10.102.224.65:50378	172.217.24.227:443	HTTPS	259		Client Hello
1793	11:27:12.432778	172.217.24.227:443	10.102.224.65:50378	TCP	68		[Retransmission] [SYN, ACK] Seq=3034475...
1794	11:27:12.432780	172.217.24.227:443	10.102.224.65:50379	TCP	68		[Retransmission] [SYN, ACK] Seq=3088958...
1795	11:27:12.433091	10.102.224.65:50378	172.217.24.227:443	TCP	66		[ACK] Seq=3613121448,Ack=3034475980,L...
1796	11:27:12.433292	10.102.224.65:50379	172.217.24.227:443	TCP	66		[ACK] Seq=1962389743,Ack=3088958519,L...
1822	11:27:12.528015	172.217.24.227:443	10.102.224.65:50381	TCP	68		[SYN, ACK] Seq=2156408772,Ack=3457332...
1825	11:27:12.529186	10.102.224.65:50381	172.217.24.227:443	TCP	54		[ACK] Seq=3457332024,Ack=2156408773,L...
1827	11:27:12.532937	10.102.224.65:50381	172.217.24.227:443	TCP	259		Client Hello
1895	11:27:14.302400	172.217.24.227:443	10.102.224.65:50379	TCP	56		[ACK] Seq=3088958519,Ack=1962389743,L...
1896	11:27:14.302403	172.217.24.227:443	10.102.224.65:50379	HTTPS	1,484		HTTPS stream, 1430 bytes payload data

Original Packet

IP dari 172.217.24.227 milik dari situs google namun yang memiliki domain UK(united kingdom)

Top100 IPv4 Conversation(Full Analysis) - 52.43.52.166 - Packets

No.	Absolute Time	Source	Destination	Protocol	Size	Decode	Summary
878	11:27:06.065141	10.102.224.65:50364	52.43.52.166:443	TCP	66		[SYN] Seq=3785824697,Ack=0000000000,L...
879	11:27:06.065676	10.102.224.65:50365	52.43.52.166:443	TCP	66		[SYN] Seq=2275804870,Ack=0000000000,L...
955	11:27:06.323451	10.102.224.65:50368	52.43.52.166:443	TCP	66		[SYN] Seq=1731606231,Ack=0000000000,L...
972	11:27:06.435755	52.43.52.166:443	10.102.224.65:50364	TCP	68		[SYN, ACK] Seq=2353115146,Ack=3785824...
975	11:27:06.435760	52.43.52.166:443	10.102.224.65:50365	TCP	68		[SYN, ACK] Seq=1099918117,Ack=2275804...
979	11:27:06.436624	10.102.224.65:50364	52.43.52.166:443	TCP	54		[ACK] Seq=3785824698,Ack=2353115147,L...
981	11:27:06.437177	10.102.224.65:50365	52.43.52.166:443	TCP	54		[ACK] Seq=2275804871,Ack=1099918118,L...
984	11:27:06.451486	10.102.224.65:50364	52.43.52.166:443	HTTPS	266		Client Hello
985	11:27:06.453130	10.102.224.65:50365	52.43.52.166:443	HTTPS	266		Client Hello
1010	11:27:06.619903	52.43.52.166:443	10.102.224.65:50368	TCP	68		[SYN, ACK] Seq=3706353076,Ack=1731606...
1011	11:27:06.620686	10.102.224.65:50368	52.43.52.166:443	TCP	54		[ACK] Seq=1731606232,Ack=3706353077,L...
1012	11:27:06.623357	10.102.224.65:50368	52.43.52.166:443	HTTPS	266		Client Hello
1078	11:27:07.099293	52.43.52.166:443	10.102.224.65:50364	TCP	56		[ACK] Seq=2353115147,Ack=3785824910,L...
1079	11:27:07.099295	52.43.52.166:443	10.102.224.65:50364	HTTPS	1,514		Server Hello, Certificate
1080	11:27:07.099298	52.43.52.166:443	10.102.224.65:50364	HTTPS	1,514		HTTPS stream, 1460 bytes payload data
1084	11:27:07.100083	10.102.224.65:50364	52.43.52.166:443	TCP	54		[ACK] Seq=3785824910,Ack=2353118067,L...
1089	11:27:07.178600	52.43.52.166:443	10.102.224.65:50364	HTTPS	851		Server Key Exchange, Server Hello Done
1091	11:27:07.188804	10.102.224.65:50364	52.43.52.166:443	HTTPS	180		Client Key Exchange, Change Cipher Spec...

Original Packet

IP dari 10.102.224.65 adalah milik dari mozilla yang dibuka saat pertama kali (homepage) dan menyimpan data (cookies).

The screenshot displays a network capture in Wireshark. The main pane shows a list of packets with columns for No., Absolute Time, Source, Destination, Protocol, Size, Decode, and Summary. The source IP is 172.217.24.227 and the destination is 10.102.224.65. The protocols include TCP, HTTP, and HTTPS. The packet details pane for packet 1911 shows TCP flags: S, [46/1], 0x3F, and window size of 1430 bytes.

Sama dari ip 172.217.24.227 milik avast mengirim ke 10.102.224.65 terdeteksi, tetapi disini tidak hanya mengikuti alur surf, namun memberikan keamanan, terlihat pada symcd dan symcb.

The screenshot displays a network capture in Wireshark. The main pane shows a list of packets with columns for No., Absolute Time, Source, Destination, Protocol, Size, Decode, and Summary. The source IP is 10.100.130.5 and the destination is 10.100.130.53. The protocols include DNS_QUERY and DNS_RESPONSE. The packet details pane for packet 1866 shows DNS query information, including the domain www.googleadservices.com.

IP 10.100.130.5 merupakan domain yang digunakan google untuk iklan.

Top100 IPv4 Conversation(Full Analysis) - 10.100.130.10 - Packets

No.	Absolute Time	Source	Destination	Protocol	Size	Decode	Summary
437	11:27:02.951590	10.102.224.65:64247	10.100.130.10:53	DNS_QUERY	83		C: Q=saf
442	11:27:02.970845	10.100.130.10:53	10.102.224.65:64247	DNS_RESPONSE	254		S: Q=saf
447	11:27:02.979716	10.102.224.65:63024	10.100.130.10:53	DNS_QUERY	75		C: Q=sb.
454	11:27:03.131703	10.100.130.10:53	10.102.224.65:63024	DNS_RESPONSE	227		S: Q=sb.l
462	11:27:03.136505	10.102.224.65:56980	10.100.130.10:53	DNS_QUERY	75		C: Q=sb.
463	11:27:03.156529	10.102.224.65:57382	10.100.130.10:53	DNS_QUERY	79		C: Q=sup
465	11:27:03.241155	10.100.130.10:53	10.102.224.65:56980	DNS_RESPONSE	239		S: Q=sb.l
478	11:27:03.388073	10.102.224.65:55862	10.100.130.10:53	DNS_QUERY	79		C: Q=clie
480	11:27:03.413570	10.100.130.10:53	10.102.224.65:55862	DNS_RESPONSE	351		S: Q=clie
486	11:27:03.421040	10.102.224.65:52334	10.100.130.10:53	DNS_QUERY	80		C: Q=clie
499	11:27:03.493456	10.100.130.10:53	10.102.224.65:57382	DNS_RESPONSE	288		S: Q=sup

Recursion Desired: 1
 Recursion Available: 0
 Authenticated Data: 0
 Checking: 0
 Response Code: 0
 Questions: 1
 Answers: 0
 Authority: 0
 Additional: 0
 Question: [54/17] sb.l.google.com
 Domain Name: sb.l.google.com

IP dari 10.100.130.10 adalah security yang dilakukan dari google, untuk mengecek apakah pada perangkat terdapat scam atau tidak, dapat dilihat dari sb.l.google.com

Top100 IPv4 Conversation(Full Analysis) - 10.102.224.65 - Packets

No.	Absolute Time	Source	Destination	Protocol	Size	Decode	Summary
383	11:27:02.110706	10.102.224.65:50349	216.58.196.196:443	HTTPS	257		Client Hello
384	11:27:02.185239	10.102.224.65:50350	216.58.196.196:443	TCP	66		[SYN] Seq=2042910389, Ack=000000000, L...
387	11:27:02.303642	216.58.196.196:443	10.102.224.65:50349	TCP	56		[ACK] Seq=2419740063, Ack=3148546549, L...
390	11:27:02.354654	216.58.196.196:443	10.102.224.65:50349	HTTPS	1,484		Server Hello, Certificate
391	11:27:02.354665	216.58.196.196:443	10.102.224.65:50349	HTTPS	1,484		HTTPS stream, 1430 bytes payload data
392	11:27:02.354669	216.58.196.196:443	10.102.224.65:50349	HTTPS	671		Server Key Exchange, Server Hello Done
393	11:27:02.354673	216.58.196.196:443	10.102.224.65:50350	TCP	68		[SYN, ACK] Seq=2069474543, Ack=2042910...
394	11:27:02.355534	10.102.224.65:50349	216.58.196.196:443	TCP	54		[ACK] Seq=3148546549, Ack=2419743540, L...
395	11:27:02.355791	10.102.224.65:50350	216.58.196.196:443	TCP	54		[ACK] Seq=2042910390, Ack=2069474544, L...
396	11:27:02.358104	10.102.224.65:50350	216.58.196.196:443	HTTPS	257		Client Hello
397	11:27:02.381011	10.102.224.65:55862	10.100.130.5:3	DNS_QUERY	79		C: Q=clients1.google.com(A)
400	11:27:02.436593	10.102.224.65:50349	216.58.196.196:443	HTTPS	147		Client Key Exchange, Change Cipher Spec, ...
401	11:27:02.567952	216.58.196.196:443	10.102.224.65:50350	TCP	56		[ACK] Seq=2069474544, Ack=2042910593, L...
424	11:27:02.716311	10.102.224.65:50351	216.58.196.196:443	TCP	66		[SYN] Seq=3466562107, Ack=000000000, L...
428	11:27:02.825782	216.58.196.196:443	10.102.224.65:50349	HTTPS	316		New Session Ticket, Change Cipher Spec, ...
429	11:27:02.825791	216.58.196.196:443	10.102.224.65:50349	HTTPS	110		Application Data
430	11:27:02.826342	10.102.224.65:50349	216.58.196.196:443	TCP	54		[ACK] Seq=3148546642, Ack=2419743858, L...
431	11:27:02.861005	216.58.196.196:443	10.102.224.65:50349	HTTPS	96		Application Data

Source port: 55862 [34/2]
 Destination port: 53 [36/2]
 Length: 45 [38/2]
 Checks: 0xPSP2 (Correct) [40/2]
 DNS - Domain Name System Protocol
 Identification: 0x7F62 [42/2]
 Code and Flag: 0000 0001 0000 0000 [44/2] 0xFFFF
 Query/Response: 0... (Query) [44/2] 0:
 Operator Code: .000 0... (QUERY) [44/2] 0:
 Authoritative Answer: ...0... (No) [44/2] 0x04:
 Truncation: ...0... (No) [44/2] 0x02:
 Recursion Desired: ...1... (Yes) [44/2] 0x0:
 Recursion Available: ...0... (No) [44/2] 0x00:
 Authenticated Data: ...0... (No) [44/2] 0x00:
 Checking: ...0... (Checking Enable)
 Response Code: ...0000 (No Error) [44/2]
 Questions: 1 [46/2]

Ip dari 10.100.130.5 adalah milik dari client google.

Top100 IPv4 Conversation(Full Analysis) - 216.58.216.46 - Packets

No.	Absolute Time	Source	Destination	Protocol	Size	Decode	Summary
818	11:27:05.821568	10.102.224.65:50363	www.google-analytics.com:443	TCP	66		[SYN] Seq=2443308076,Ack=0000000000,L...
940	11:27:06.267162	www.google-analytics.com:443	10.102.224.65:50363	TCP	68		[ACK] Seq=3779216629,Ack=2443308...
945	11:27:06.268306	10.102.224.65:50363	www.google-analytics.com:443	TCP	54		[ACK] Seq=2443308077,Ack=3779216630,L...
949	11:27:06.272185	10.102.224.65:50363	www.google-analytics.com:443	HTTPS	272		ClientHello
976	11:27:06.435762	www.google-analytics.com:443	10.102.224.65:50363	TCP	68		[Retransmission] [SYN, ACK] Seq=3779216...
980	11:27:06.437053	10.102.224.65:50363	www.google-analytics.com:443	TCP	66		[ACK] Seq=2443308295,Ack=3779216630,L...
991	11:27:06.498841	www.google-analytics.com:443	10.102.224.65:50363	TCP	56		[ACK] Seq=3779216630,Ack=2443308295,L...
992	11:27:06.498842	www.google-analytics.com:443	10.102.224.65:50363	HTTPS	1,484		Server Hello, Certificate
993	11:27:06.498843	www.google-analytics.com:443	10.102.224.65:50363	HTTPS	1,484		HTTPS stream, 1430 bytes payload data
994	11:27:06.498845	www.google-analytics.com:443	10.102.224.65:50363	HTTPS	1,167		Server Key Exchange, Server Hello Done
997	11:27:06.499681	10.102.224.65:50363	www.google-analytics.com:443	TCP	54		[ACK] Seq=2443308295,Ack=3779220603,L...
1002	11:27:06.520326	10.102.224.65:50363	www.google-analytics.com:443	HTTPS	147		Client Key Exchange, Change Cipher Spec, ...
1019	11:27:06.667581	10.102.224.65:50363	www.google-analytics.com:443	HTTPS	1,366		Application Data
1104	11:27:07.195337	www.google-analytics.com:443	10.102.224.65:50363	HTTPS	332		New Session Ticket, Change Cipher Spec, ...
1105	11:27:07.195339	www.google-analytics.com:443	10.102.224.65:50363	HTTPS	110		Application Data
1108	11:27:07.195955	10.102.224.65:50363	www.google-analytics.com:443	TCP	54		[ACK] Seq=2443309700,Ack=3779220937,L...
1110	11:27:07.210967	10.102.224.65:50363	www.google-analytics.com:443	HTTPS	92		Application Data
1112	11:27:07.224168	www.google-analytics.com:443	10.102.224.65:50363	HTTPS	96		Application Data

Original Packet

Dari destination www.google-analytics.com merupakan filter dari google yang dilewati.

Top100 IPv4 Conversation(Full Analysis) - 172.217.27.14 - Packets

No.	Absolute Time	Source	Destination	Protocol	Size	Decode	Summary
445	11:27:02.977787	10.102.224.65:50352	172.217.27.14:443	TCP	66		[SYN] Seq=3672959746,Ack=0000000000,L...
446	11:27:02.978815	10.102.224.65:50353	172.217.27.14:443	TCP	66		[SYN] Seq=2548898392,Ack=0000000000,L...
455	11:27:03.131711	172.217.27.14:443	10.102.224.65:50352	TCP	68		[ACK] Seq=1611624756,Ack=3672959...
456	11:27:03.131713	172.217.27.14:443	10.102.224.65:50353	TCP	68		[SYN, ACK] Seq=0440554981,Ack=2548898...
458	11:27:03.132529	10.102.224.65:50352	172.217.27.14:443	TCP	54		[ACK] Seq=3672959747,Ack=1611624757,L...
459	11:27:03.132768	10.102.224.65:50353	172.217.27.14:443	TCP	54		[ACK] Seq=2548898393,Ack=0440554982,L...
460	11:27:03.134495	10.102.224.65:50352	172.217.27.14:443	HTTPS	266		ClientHello
461	11:27:03.134495	10.102.224.65:50353	172.217.27.14:443	HTTPS	266		ClientHello
466	11:27:03.269115	172.217.27.14:443	10.102.224.65:50353	TCP	56		[ACK] Seq=0440554982,Ack=2548898605,L...
469	11:27:03.345995	172.217.27.14:443	10.102.224.65:50353	HTTPS	1,484		Server Hello, Certificate
470	11:27:03.362780	172.217.27.14:443	10.102.224.65:50353	HTTPS	1,484		HTTPS stream, 1430 bytes payload data
471	11:27:03.362791	172.217.27.14:443	10.102.224.65:50352	HTTPS	1,484		HTTPS stream, 1430 bytes payload data
472	11:27:03.362806	172.217.27.14:443	10.102.224.65:50353	HTTPS	1,163		Server Key Exchange, Server Hello Done
474	11:27:03.363291	10.102.224.65:50352	172.217.27.14:443	TCP	66		[ACK] Seq=3672959959,Ack=1611624757,L...
475	11:27:03.363998	10.102.224.65:50353	172.217.27.14:443	TCP	54		[ACK] Seq=2548898605,Ack=0440558951,L...
497	11:27:03.466200	10.102.224.65:50353	172.217.27.14:443	HTTPS	147		Client Key Exchange, Change Cipher Spec, ...
503	11:27:03.593587	172.217.27.14:443	10.102.224.65:50352	HTTPS	1,484		[Retransmission] Server Hello, Encrypted H...
543	11:27:03.782734	10.102.224.65:50353	172.217.27.14:443	HTTPS	211		Application Data

Original Packet Reassembled Packet

IP 172.217.27.14 merupakan IP yang memanggil perintah untuk semua content pada google.