

ОБЛАСТ ИНФОРМАТИЧКИ ТЕХНОЛОГИИ

ПРАКТИЧЕН СЛУЧАЈ БР. 1 - Анализа на мрежен сообраќај

До вешто лице: АА

Нарачател: ББ

Барање за изготвување на Вешт наод и мислење од област информатички технологии

Почитуван,

Пред Основниот суд ВВ, се води постапка 11/2025, каде што како тужител се јавува ДД, а тужен е ББ. За потребите на постапката, потребно е да се изготви Вешт наод и мислење од областа на информатичките технологии, во кои треба да се изврши анализа на снимен мрежен сообраќај и да се даде одговор на следните околности (1-5), кои се однесуваат на снимен мрежен сообраќај во алатката Wireshark прикажани на Слика 1 и Слика 2, дадени во прилог на ова Барање.

1. Која е IP адресата на клиентите кои иницираат воспоставувањето на TCP конекции?
2. Која е IP адресата на серверот кон кој се испратени овие барања за воспоставување на конекција?
3. На кои комуникациски порти на страната на серверот, се обидуваат клиентите да воспостави конекција?
4. Дали врз основа на идентификуваните целни комуникациски порти може да препознаете за кои протоколи/сервиси се работи?
5. Дали е успешно воспоставена конекција помеѓу клиентите и серверот?

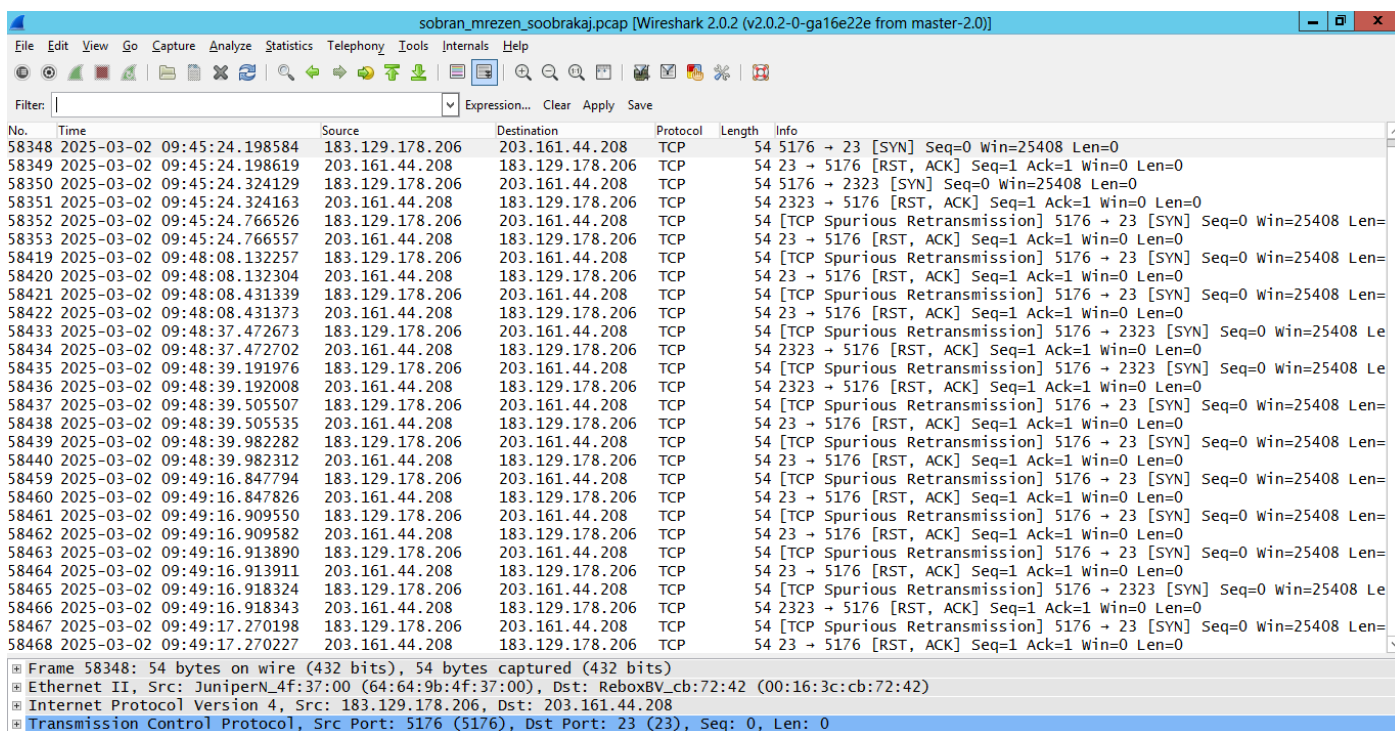
Во Вештиот наод и мислење треба да се изврши анализа и на снимен мрежен сообраќај и да се даде одговор на следните околности (6-10), кои се однесуваат на снимен мрежен сообраќај во алатката Wireshark прикажан на Слика 3, дадена во прилог на ова Барање.

6. Која е IP адресата на клиентот кои иницираат воспоставувањето на TCP конекции?
7. Кој е бројот на комуникациска порта која ја користи клиентот за воспоставување на конекција со серверот?
8. Дали клиентот точно знае на која комуникациска порта серверот очекува барања за нови конекции или се обидува по случаен избор да најде активен сервис на страната на серверот?
9. Дали е вообичаено клиентот да користи една иста комуникациска порта за воспоставување TCP конекција за различни сервиси и различни комуникациски протоколи?
10. Дали од снимениот мрежен сообраќај може активноста на клиентот да се окарактеризира како некој тип на малициозно однесување односно мрежен напад и доколку да за каков тип на напад се работи?

Со почит,

ББ

Прилог кон Барањето за вештачење:

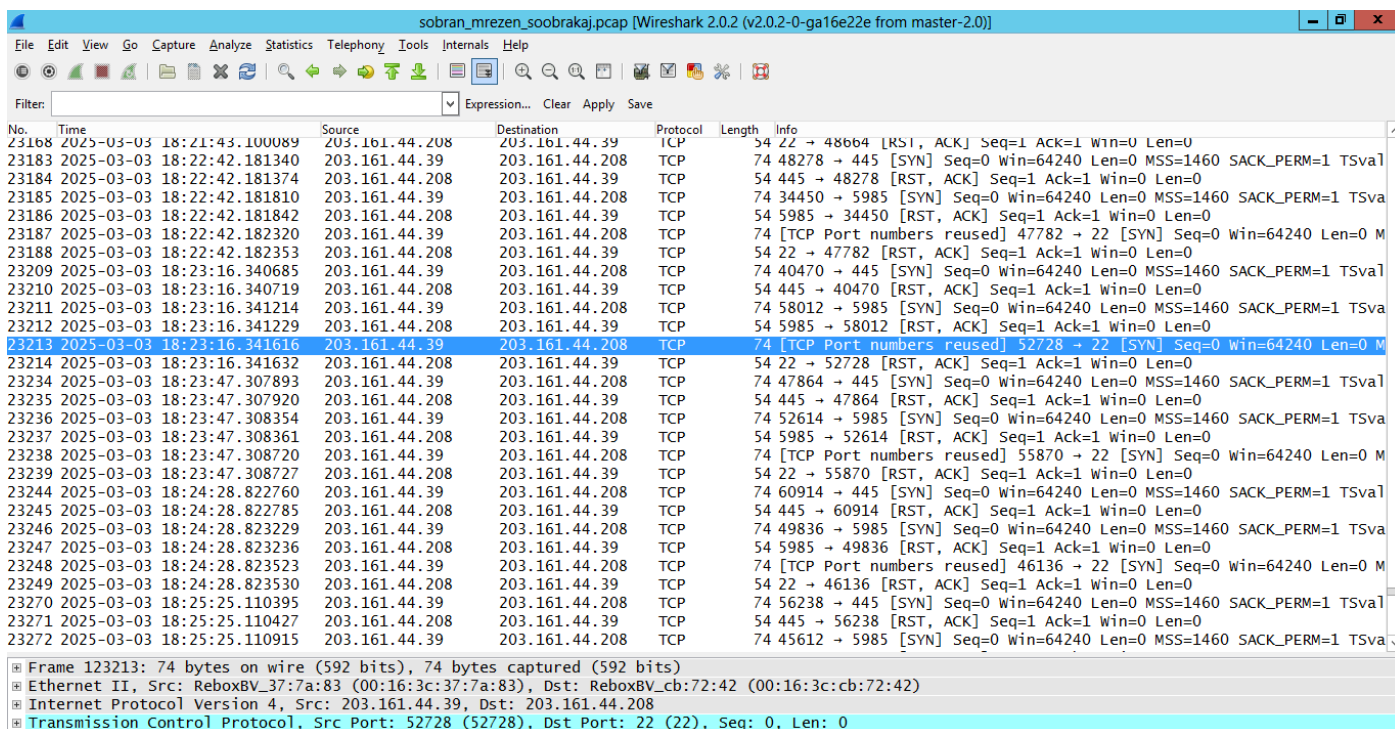


The screenshot shows a Wireshark capture of a network packet. The packet list on the left shows a series of TCP packets. The selected packet, number 58348, is a SYN packet from 183.129.178.206 to 203.161.44.208. The packet details pane on the right shows the structure of the packet: Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes pane at the bottom shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
58348	2025-03-02 09:45:24.198584	183.129.178.206	203.161.44.208	TCP	54	5176 → 23 [SYN] Seq=0 Win=25408 Len=0
58349	2025-03-02 09:45:24.198619	203.161.44.208	183.129.178.206	TCP	54	23 → 5176 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
58350	2025-03-02 09:45:24.324129	183.129.178.206	203.161.44.208	TCP	54	5176 → 2323 [SYN] Seq=0 Win=25408 Len=0
58351	2025-03-02 09:45:24.324163	203.161.44.208	183.129.178.206	TCP	54	2323 → 5176 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
58352	2025-03-02 09:45:24.766526	183.129.178.206	203.161.44.208	TCP	54	[TCP Spurious Retransmission] 5176 → 23 [SYN] Seq=0 Win=25408 Len=0
58353	2025-03-02 09:45:24.766557	203.161.44.208	183.129.178.206	TCP	54	23 → 5176 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
58419	2025-03-02 09:48:08.132257	183.129.178.206	203.161.44.208	TCP	54	[TCP Spurious Retransmission] 5176 → 23 [SYN] Seq=0 Win=25408 Len=0
58420	2025-03-02 09:48:08.132304	203.161.44.208	183.129.178.206	TCP	54	23 → 5176 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
58421	2025-03-02 09:48:08.431339	183.129.178.206	203.161.44.208	TCP	54	[TCP Spurious Retransmission] 5176 → 23 [SYN] Seq=0 Win=25408 Len=0
58422	2025-03-02 09:48:08.431373	203.161.44.208	183.129.178.206	TCP	54	23 → 5176 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
58433	2025-03-02 09:48:37.472673	183.129.178.206	203.161.44.208	TCP	54	[TCP Spurious Retransmission] 5176 → 2323 [SYN] Seq=0 Win=25408 Le
58434	2025-03-02 09:48:37.472702	203.161.44.208	183.129.178.206	TCP	54	2323 → 5176 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
58435	2025-03-02 09:48:39.191976	183.129.178.206	203.161.44.208	TCP	54	[TCP Spurious Retransmission] 5176 → 2323 [SYN] Seq=0 Win=25408 Le
58436	2025-03-02 09:48:39.192008	203.161.44.208	183.129.178.206	TCP	54	2323 → 5176 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
58437	2025-03-02 09:48:39.505507	183.129.178.206	203.161.44.208	TCP	54	[TCP Spurious Retransmission] 5176 → 23 [SYN] Seq=0 Win=25408 Len=0
58438	2025-03-02 09:48:39.505535	203.161.44.208	183.129.178.206	TCP	54	23 → 5176 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
58439	2025-03-02 09:48:39.982282	183.129.178.206	203.161.44.208	TCP	54	[TCP Spurious Retransmission] 5176 → 23 [SYN] Seq=0 Win=25408 Len=0
58440	2025-03-02 09:48:39.982312	203.161.44.208	183.129.178.206	TCP	54	23 → 5176 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
58459	2025-03-02 09:49:16.847794	183.129.178.206	203.161.44.208	TCP	54	[TCP Spurious Retransmission] 5176 → 23 [SYN] Seq=0 Win=25408 Len=0
58460	2025-03-02 09:49:16.847826	203.161.44.208	183.129.178.206	TCP	54	23 → 5176 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
58461	2025-03-02 09:49:16.909550	183.129.178.206	203.161.44.208	TCP	54	[TCP Spurious Retransmission] 5176 → 23 [SYN] Seq=0 Win=25408 Len=0
58462	2025-03-02 09:49:16.909582	203.161.44.208	183.129.178.206	TCP	54	23 → 5176 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
58463	2025-03-02 09:49:16.913890	183.129.178.206	203.161.44.208	TCP	54	[TCP Spurious Retransmission] 5176 → 23 [SYN] Seq=0 Win=25408 Len=0
58464	2025-03-02 09:49:16.913911	203.161.44.208	183.129.178.206	TCP	54	23 → 5176 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
58465	2025-03-02 09:49:16.918324	183.129.178.206	203.161.44.208	TCP	54	[TCP Spurious Retransmission] 5176 → 2323 [SYN] Seq=0 Win=25408 Le
58466	2025-03-02 09:49:16.918343	203.161.44.208	183.129.178.206	TCP	54	2323 → 5176 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
58467	2025-03-02 09:49:17.270198	183.129.178.206	203.161.44.208	TCP	54	[TCP Spurious Retransmission] 5176 → 23 [SYN] Seq=0 Win=25408 Len=0
58468	2025-03-02 09:49:17.270227	203.161.44.208	183.129.178.206	TCP	54	23 → 5176 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Frame 58348: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: JuniperN_4f:37:00 (64:64:9b:4f:37:00), Dst: ReboxBV_cb:72:42 (00:16:3c:cb:72:42)
Internet Protocol Version 4, Src: 183.129.178.206, Dst: 203.161.44.208
Transmission Control Protocol, Src Port: 5176 (5176), Dst Port: 23 (23), Seq: 0, Len: 0

Слика 1.



The screenshot shows a Wireshark capture of a network packet. The packet list on the left shows a series of TCP packets. The selected packet, number 23213, is a SYN packet from 203.161.44.39 to 203.161.44.208. The packet details pane on the right shows the structure of the packet: Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes pane at the bottom shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
23168	2025-03-03 18:21:43.100089	203.161.44.208	203.161.44.39	TCP	54	22 → 48664 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23183	2025-03-03 18:22:42.181340	203.161.44.39	203.161.44.208	TCP	74	48278 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval
23184	2025-03-03 18:22:42.181374	203.161.44.208	203.161.44.39	TCP	54	445 → 48278 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23185	2025-03-03 18:22:42.181810	203.161.44.39	203.161.44.208	TCP	74	34450 → 5985 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSva
23186	2025-03-03 18:22:42.181842	203.161.44.208	203.161.44.39	TCP	54	5985 → 34450 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23187	2025-03-03 18:22:42.182320	203.161.44.39	203.161.44.208	TCP	74	[TCP Port numbers reused] 47782 → 22 [SYN] Seq=0 Win=64240 Len=0 M
23188	2025-03-03 18:22:42.182353	203.161.44.208	203.161.44.39	TCP	54	22 → 47782 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23209	2025-03-03 18:23:16.340685	203.161.44.39	203.161.44.208	TCP	74	40470 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval
23210	2025-03-03 18:23:16.340719	203.161.44.208	203.161.44.39	TCP	54	445 → 40470 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23211	2025-03-03 18:23:16.341214	203.161.44.39	203.161.44.208	TCP	74	58012 → 5985 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSva
23212	2025-03-03 18:23:16.341229	203.161.44.208	203.161.44.39	TCP	54	5985 → 58012 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23213	2025-03-03 18:23:16.341616	203.161.44.39	203.161.44.208	TCP	74	[TCP Port numbers reused] 52728 → 22 [SYN] Seq=0 Win=64240 Len=0 M
23214	2025-03-03 18:23:16.341632	203.161.44.208	203.161.44.39	TCP	54	22 → 52728 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23234	2025-03-03 18:23:47.307893	203.161.44.39	203.161.44.208	TCP	74	47864 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval
23235	2025-03-03 18:23:47.307920	203.161.44.208	203.161.44.39	TCP	54	445 → 47864 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23236	2025-03-03 18:23:47.308354	203.161.44.39	203.161.44.208	TCP	74	52614 → 5985 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSva
23237	2025-03-03 18:23:47.308361	203.161.44.208	203.161.44.39	TCP	54	5985 → 52614 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23238	2025-03-03 18:23:47.308720	203.161.44.39	203.161.44.208	TCP	74	[TCP Port numbers reused] 55870 → 22 [SYN] Seq=0 Win=64240 Len=0 M
23239	2025-03-03 18:23:47.308727	203.161.44.208	203.161.44.39	TCP	54	22 → 55870 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23244	2025-03-03 18:24:28.822760	203.161.44.39	203.161.44.208	TCP	74	60914 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval
23245	2025-03-03 18:24:28.822785	203.161.44.208	203.161.44.39	TCP	54	445 → 60914 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23246	2025-03-03 18:24:28.823229	203.161.44.39	203.161.44.208	TCP	74	49836 → 5985 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSva
23247	2025-03-03 18:24:28.823236	203.161.44.208	203.161.44.39	TCP	54	5985 → 49836 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23248	2025-03-03 18:24:28.823523	203.161.44.39	203.161.44.208	TCP	74	[TCP Port numbers reused] 46136 → 22 [SYN] Seq=0 Win=64240 Len=0 M
23249	2025-03-03 18:24:28.823530	203.161.44.208	203.161.44.39	TCP	54	22 → 46136 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23270	2025-03-03 18:25:25.110395	203.161.44.39	203.161.44.208	TCP	74	56238 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval
23271	2025-03-03 18:25:25.110427	203.161.44.208	203.161.44.39	TCP	54	445 → 56238 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23272	2025-03-03 18:25:25.110915	203.161.44.39	203.161.44.208	TCP	74	45612 → 5985 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSva

Frame 23213: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: ReboxBV_37:7a:83 (00:16:3c:37:7a:83), Dst: ReboxBV_cb:72:42 (00:16:3c:cb:72:42)
Internet Protocol Version 4, Src: 203.161.44.39, Dst: 203.161.44.208
Transmission Control Protocol, Src Port: 52728 (52728), Dst Port: 22 (22), Seq: 0, Len: 0

Слика 2.

sobran_mrezen_soobrakaj.pcap [Wireshark 2.0.2 (v2.0.2-0-ga16e22e from master-2.0)]									
No.	Time	Source	Destination	Protocol	Length	Info			
48968	2025-03-02 04:20:04.849600	103.207.38.18	203.161.44.208	TCP	54	41831 → 6018	[SYN]	Seq=0	Win=512 Len=0
48969	2025-03-02 04:20:04.849694	203.161.44.208	103.207.38.18	TCP	54	6018 → 41831	[RST, ACK]	Seq=1 Ack=1	Win=0 Len=0
48974	2025-03-02 04:20:11.167816	103.207.38.18	203.161.44.208	TCP	54	41831 → 20905	[SYN]	Seq=0	Win=512 Len=0
48975	2025-03-02 04:20:11.167840	203.161.44.208	103.207.38.18	TCP	54	20905 → 41831	[RST, ACK]	Seq=1 Ack=1	Win=0 Len=0
49073	2025-03-02 04:24:09.989990	103.207.38.18	203.161.44.208	TCP	54	40709 → 50729	[SYN]	Seq=0	Win=512 Len=0
49074	2025-03-02 04:24:09.990021	203.161.44.208	103.207.38.18	TCP	54	50729 → 40709	[RST, ACK]	Seq=1 Ack=1	Win=0 Len=0
49287	2025-03-02 04:31:02.312314	103.207.38.18	203.161.44.208	TCP	54	40709 → 50825	[SYN]	Seq=0	Win=512 Len=0
49288	2025-03-02 04:31:02.312347	203.161.44.208	103.207.38.18	TCP	54	50825 → 40709	[RST, ACK]	Seq=1 Ack=1	Win=0 Len=0
49320	2025-03-02 04:32:15.244059	103.207.38.18	203.161.44.208	TCP	54	40709 → 50842	[SYN]	Seq=0	Win=512 Len=0
49321	2025-03-02 04:32:15.244091	203.161.44.208	103.207.38.18	TCP	54	50842 → 40709	[RST, ACK]	Seq=1 Ack=1	Win=0 Len=0
49322	2025-03-02 04:32:19.595274	103.207.38.18	203.161.44.208	TCP	54	40709 → 50843	[SYN]	Seq=0	Win=512 Len=0
49323	2025-03-02 04:32:19.595316	203.161.44.208	103.207.38.18	TCP	54	50843 → 40709	[RST, ACK]	Seq=1 Ack=1	Win=0 Len=0
49487	2025-03-02 04:35:36.268866	103.207.38.18	203.161.44.208	TCP	54	41831 → 21121	[SYN]	Seq=0	Win=512 Len=0
49488	2025-03-02 04:35:36.268897	203.161.44.208	103.207.38.18	TCP	54	21121 → 41831	[RST, ACK]	Seq=1 Ack=1	Win=0 Len=0
49491	2025-03-02 04:35:49.048593	103.207.38.18	203.161.44.208	TCP	54	41831 → 21124	[SYN]	Seq=0	Win=512 Len=0
49492	2025-03-02 04:35:49.048621	203.161.44.208	103.207.38.18	TCP	54	21124 → 41831	[RST, ACK]	Seq=1 Ack=1	Win=0 Len=0
49544	2025-03-02 04:38:00.389606	103.207.38.18	203.161.44.208	TCP	54	41831 → 35995	[SYN]	Seq=0	Win=512 Len=0
49545	2025-03-02 04:38:00.389633	203.161.44.208	103.207.38.18	TCP	54	35995 → 41831	[RST, ACK]	Seq=1 Ack=1	Win=0 Len=0
49578	2025-03-02 04:39:00.172127	103.207.38.18	203.161.44.208	TCP	54	41831 → 36009	[SYN]	Seq=0	Win=512 Len=0
49579	2025-03-02 04:39:00.172152	203.161.44.208	103.207.38.18	TCP	54	36009 → 41831	[RST, ACK]	Seq=1 Ack=1	Win=0 Len=0
49677	2025-03-02 04:42:35.124568	103.207.38.18	203.161.44.208	TCP	54	41831 → 36059	[SYN]	Seq=0	Win=512 Len=0
49678	2025-03-02 04:42:35.124602	203.161.44.208	103.207.38.18	TCP	54	36059 → 41831	[RST, ACK]	Seq=1 Ack=1	Win=0 Len=0
49681	2025-03-02 04:42:45.323923	103.207.38.18	203.161.44.208	TCP	54	41831 → 21221	[SYN]	Seq=0	Win=512 Len=0
49682	2025-03-02 04:42:45.323957	203.161.44.208	103.207.38.18	TCP	54	21221 → 41831	[RST, ACK]	Seq=1 Ack=1	Win=0 Len=0
49777	2025-03-02 04:46:33.056039	103.207.38.18	203.161.44.208	TCP	54	41831 → 21274	[SYN]	Seq=0	Win=512 Len=0
49778	2025-03-02 04:46:33.056075	203.161.44.208	103.207.38.18	TCP	54	21274 → 41831	[RST, ACK]	Seq=1 Ack=1	Win=0 Len=0
49838	2025-03-02 04:48:55.364534	103.207.38.18	203.161.44.208	TCP	54	41831 → 21307	[SYN]	Seq=0	Win=512 Len=0
49839	2025-03-02 04:48:55.364565	203.161.44.208	103.207.38.18	TCP	54	21307 → 41831	[RST, ACK]	Seq=1 Ack=1	Win=0 Len=0
* Frame 48968: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)									
* Ethernet II, Src: JuniperN_4f:37:00 (64:64:9b:4f:37:00), Dst: ReboxBV_cb:72:42 (00:16:3c:cb:72:42)									
* Internet Protocol Version 4, Src: 103.207.38.18, Dst: 203.161.44.208									
* Transmission Control Protocol, Src Port: 41831 (41831), Dst Port: 6018 (6018), Seq: 0, Len: 0									

Слика 3.