**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?

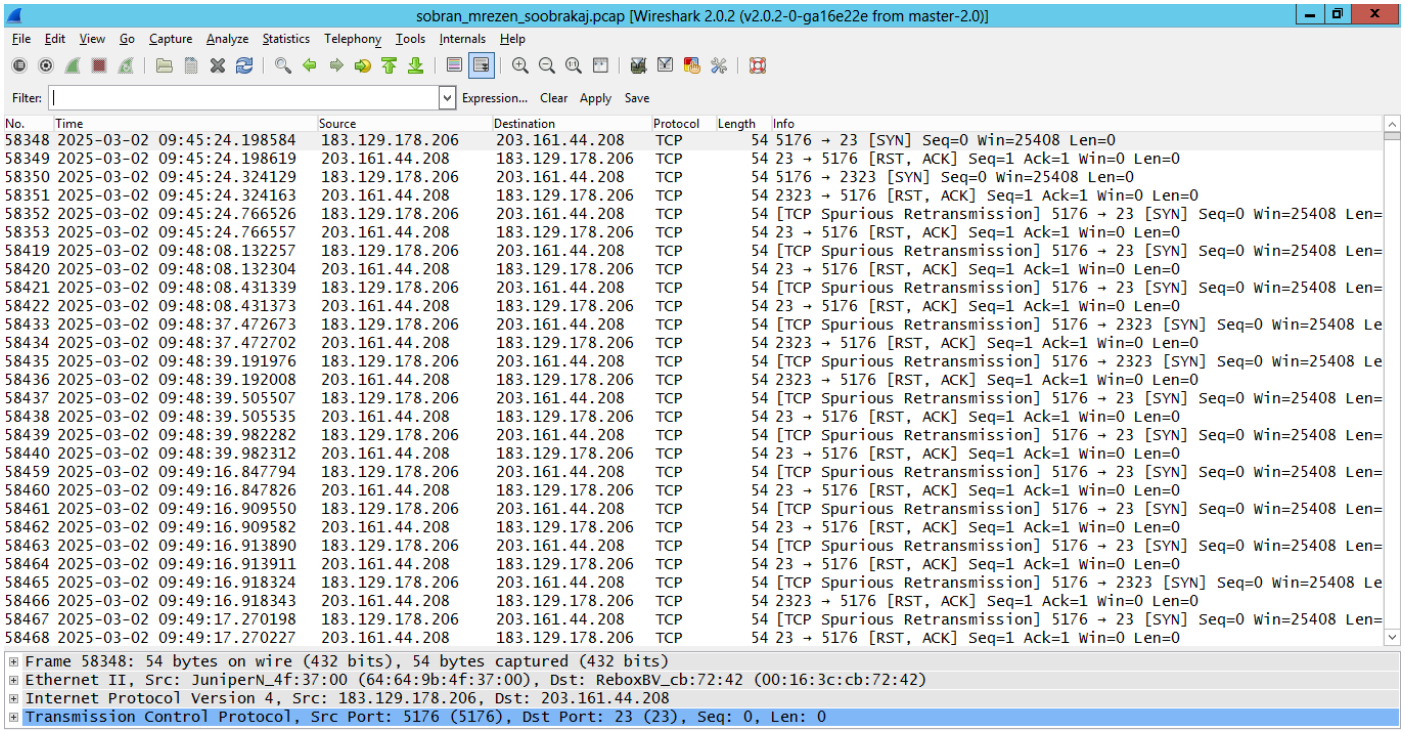
Во Вештиот наод и мислење треба да се изврши анализа и на снимен мрежен сообраќај и да се даде одговор на следните околности (6-10), кои се однесуваат на снимен мрежен сообраќај во алатката Wireshark прикажан на Слика 3, дадена во прилог на ова Барање.

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?

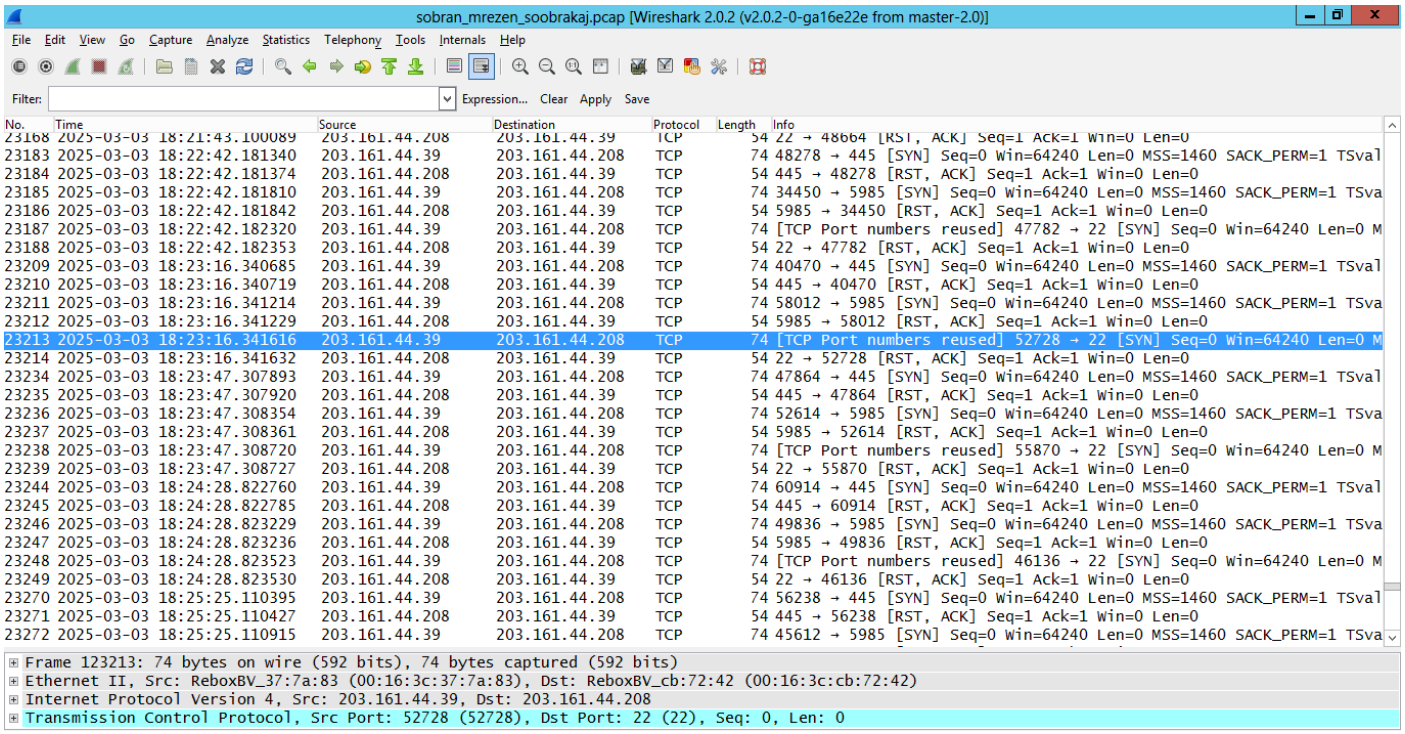
Со почит,

ББ

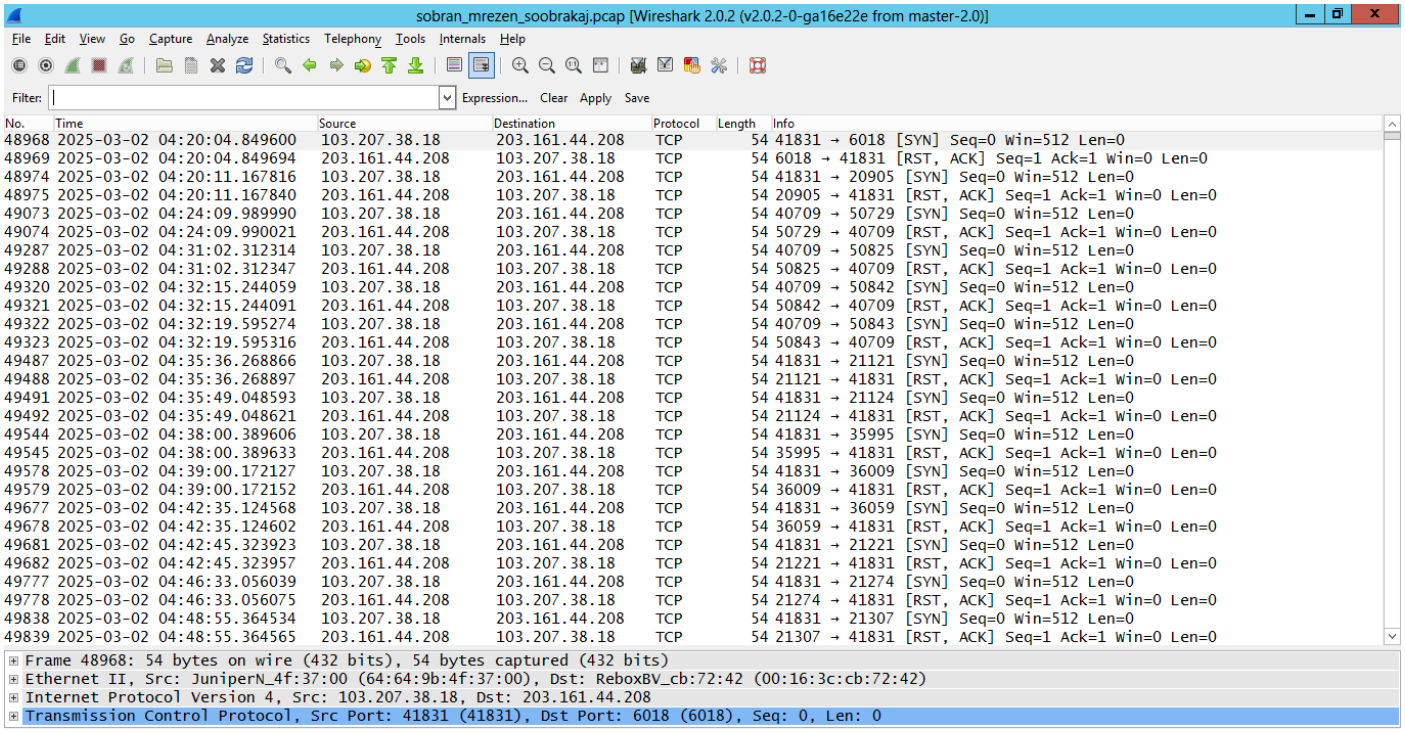
Прилог кон Барањето за вештачење:




Слика 1.




Слика 2.


sobran_mrezen_soobrakaj.pcap [Wireshark 2.0.2 (v2.0.2-0-ga16e22e from master-2.0)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
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: RaboxBV_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.