ATTACK DEFENSE

by PentesterAcademy

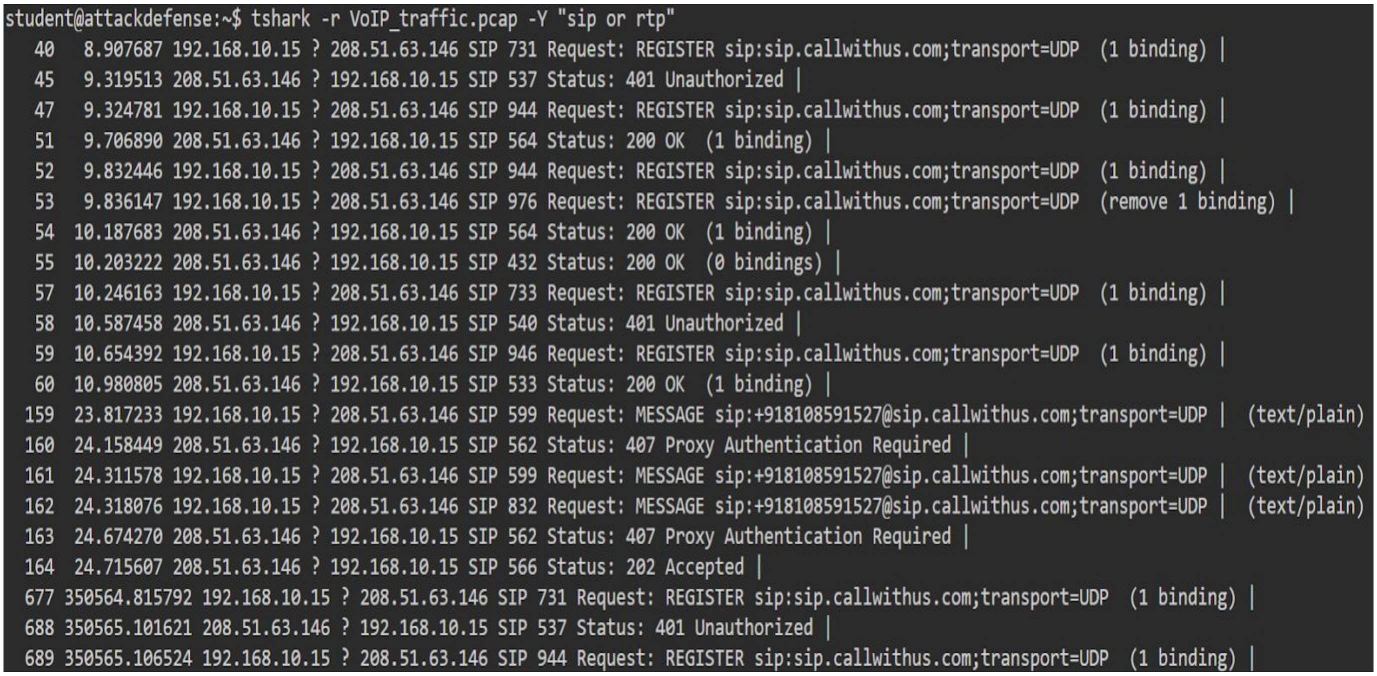
Name	Filtering Advanced: VoIP
URL	https://www.attackdefense.com/challengedetails?cid=5
Type	Traffic Analysis: Tshark Fu

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Set A:

Q1. What command can be used to only show VoIP traffic?

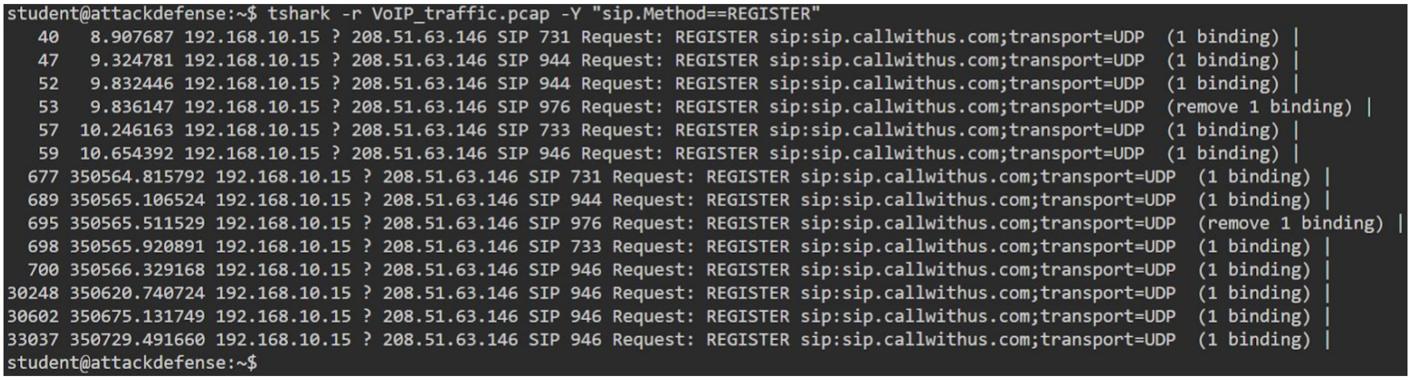
Answer: tshark -r VoIP_traffic.pcap -Y "sip or rtp"



```
student@attackdefense:~$ tshark -r VoIP_traffic.pcap -Y "sip or rtp"
   40   8.907687 192.168.10.15 ? 208.51.63.146 SIP 731 Request: REGISTER sip:sip.callwithus.com;transport=UDP  (1 binding) |
   45   9.319513 208.51.63.146 ? 192.168.10.15 SIP 537 Status: 401 Unauthorized |
   47   9.324781 192.168.10.15 ? 208.51.63.146 SIP 944 Request: REGISTER sip:sip.callwithus.com;transport=UDP  (1 binding) |
   51   9.706890 208.51.63.146 ? 192.168.10.15 SIP 564 Status: 200 OK  (1 binding) |
   52   9.832446 192.168.10.15 ? 208.51.63.146 SIP 944 Request: REGISTER sip:sip.callwithus.com;transport=UDP  (1 binding) |
   53   9.836147 192.168.10.15 ? 208.51.63.146 SIP 976 Request: REGISTER sip:sip.callwithus.com;transport=UDP  (remove 1 binding) |
   54  10.187683 208.51.63.146 ? 192.168.10.15 SIP 564 Status: 200 OK  (1 binding) |
   55  10.203222 208.51.63.146 ? 192.168.10.15 SIP 432 Status: 200 OK  (0 bindings) |
   57  10.246163 192.168.10.15 ? 208.51.63.146 SIP 733 Request: REGISTER sip:sip.callwithus.com;transport=UDP  (1 binding) |
   58  10.587458 208.51.63.146 ? 192.168.10.15 SIP 540 Status: 401 Unauthorized |
   59  10.654392 192.168.10.15 ? 208.51.63.146 SIP 946 Request: REGISTER sip:sip.callwithus.com;transport=UDP  (1 binding) |
   60  10.980805 208.51.63.146 ? 192.168.10.15 SIP 533 Status: 200 OK  (1 binding) |
  159  23.817233 192.168.10.15 ? 208.51.63.146 SIP 599 Request: MESSAGE sip:+918108591527@sip.callwithus.com;transport=UDP |  (text/plain)
  160  24.158449 208.51.63.146 ? 192.168.10.15 SIP 562 Status: 407 Proxy Authentication Required |
  161  24.311578 192.168.10.15 ? 208.51.63.146 SIP 599 Request: MESSAGE sip:+918108591527@sip.callwithus.com;transport=UDP |  (text/plain)
  162  24.318076 192.168.10.15 ? 208.51.63.146 SIP 832 Request: MESSAGE sip:+918108591527@sip.callwithus.com;transport=UDP |  (text/plain)
  163  24.674270 208.51.63.146 ? 192.168.10.15 SIP 562 Status: 407 Proxy Authentication Required |
  164  24.715607 208.51.63.146 ? 192.168.10.15 SIP 566 Status: 202 Accepted |
  677 350564.815792 192.168.10.15 ? 208.51.63.146 SIP 731 Request: REGISTER sip:sip.callwithus.com;transport=UDP  (1 binding) |
  688 350565.101621 208.51.63.146 ? 192.168.10.15 SIP 537 Status: 401 Unauthorized |
  689 350565.106524 192.168.10.15 ? 208.51.63.146 SIP 944 Request: REGISTER sip:sip.callwithus.com;transport=UDP  (1 binding) |
```

Q2. What command can be used to print all REGISTER packets?

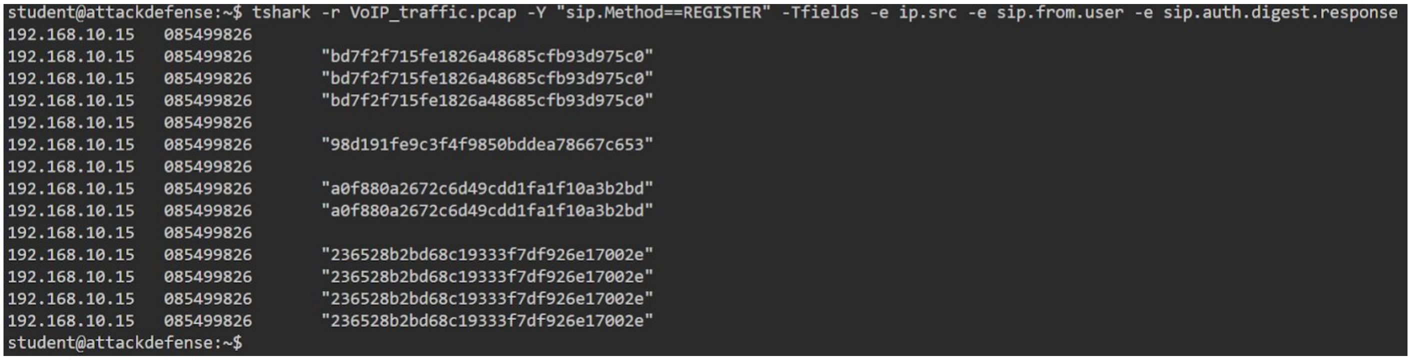
Answer: tshark -r VoIP_traffic.pcap -Y "sip.Method==REGISTER"



```
student@attackdefense:~$ tshark -r VoIP_traffic.pcap -Y "sip.Method==REGISTER"
   40   8.907687 192.168.10.15 ? 208.51.63.146 SIP 731 Request: REGISTER sip:sip.callwithus.com;transport=UDP  (1 binding) |
   47   9.324781 192.168.10.15 ? 208.51.63.146 SIP 944 Request: REGISTER sip:sip.callwithus.com;transport=UDP  (1 binding) |
   52   9.832446 192.168.10.15 ? 208.51.63.146 SIP 944 Request: REGISTER sip:sip.callwithus.com;transport=UDP  (1 binding) |
   53   9.836147 192.168.10.15 ? 208.51.63.146 SIP 976 Request: REGISTER sip:sip.callwithus.com;transport=UDP  (remove 1 binding) |
   57  10.246163 192.168.10.15 ? 208.51.63.146 SIP 733 Request: REGISTER sip:sip.callwithus.com;transport=UDP  (1 binding) |
   59  10.654392 192.168.10.15 ? 208.51.63.146 SIP 946 Request: REGISTER sip:sip.callwithus.com;transport=UDP  (1 binding) |
  677 350564.815792 192.168.10.15 ? 208.51.63.146 SIP 731 Request: REGISTER sip:sip.callwithus.com;transport=UDP  (1 binding) |
  689 350565.106524 192.168.10.15 ? 208.51.63.146 SIP 944 Request: REGISTER sip:sip.callwithus.com;transport=UDP  (1 binding) |
  695 350565.511529 192.168.10.15 ? 208.51.63.146 SIP 976 Request: REGISTER sip:sip.callwithus.com;transport=UDP  (remove 1 binding) |
  698 350565.920891 192.168.10.15 ? 208.51.63.146 SIP 733 Request: REGISTER sip:sip.callwithus.com;transport=UDP  (1 binding) |
  700 350566.329168 192.168.10.15 ? 208.51.63.146 SIP 946 Request: REGISTER sip:sip.callwithus.com;transport=UDP  (1 binding) |
30248 350620.740724 192.168.10.15 ? 208.51.63.146 SIP 946 Request: REGISTER sip:sip.callwithus.com;transport=UDP  (1 binding) |
30602 350675.131749 192.168.10.15 ? 208.51.63.146 SIP 946 Request: REGISTER sip:sip.callwithus.com;transport=UDP  (1 binding) |
33037 350729.491660 192.168.10.15 ? 208.51.63.146 SIP 946 Request: REGISTER sip:sip.callwithus.com;transport=UDP  (1 binding) |
student@attackdefense:~$
```

Q3. What command can be used to only print the source IP, sender extension and authorization digest response for REGISTER packets?

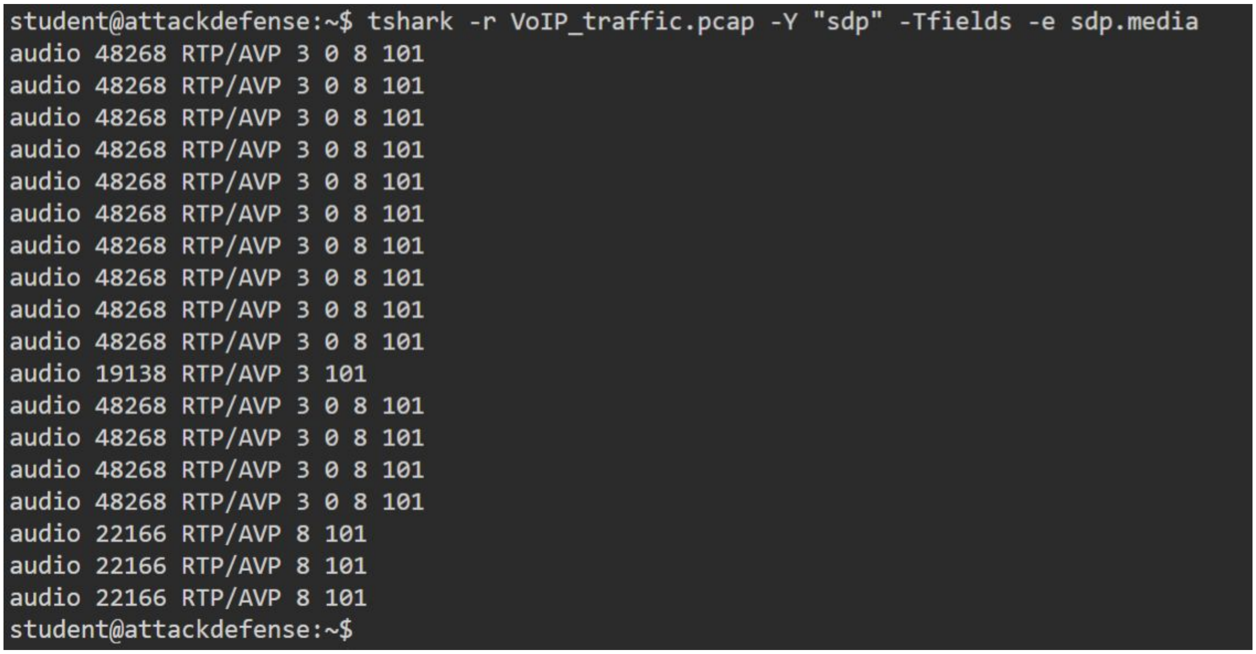
Answer: tshark -r VoIP_traffic.pcap -Y "sip.Method==REGISTER" -Tfields -e ip.src -e sip.from.user -e sip.auth.digest.response



```
student@attackdefense:~$ tshark -r VoIP_traffic.pcap -Y "sip.Method==REGISTER" -Tfields -e ip.src -e sip.from.user -e sip.auth.digest.response
192.168.10.15   085499826
192.168.10.15   085499826       "bd7f2f715fe1826a48685cfb93d975c0"
192.168.10.15   085499826       "bd7f2f715fe1826a48685cfb93d975c0"
192.168.10.15   085499826       "bd7f2f715fe1826a48685cfb93d975c0"
192.168.10.15   085499826
192.168.10.15   085499826       "98d191fe9c3f4f9850bddea78667c653"
192.168.10.15   085499826
192.168.10.15   085499826       "a0f880a2672c6d49cdd1fa1f10a3b2bd"
192.168.10.15   085499826       "a0f880a2672c6d49cdd1fa1f10a3b2bd"
192.168.10.15   085499826
192.168.10.15   085499826       "236528b2bd68c19333f7df926e17002e"
192.168.10.15   085499826       "236528b2bd68c19333f7df926e17002e"
192.168.10.15   085499826       "236528b2bd68c19333f7df926e17002e"
192.168.10.15   085499826       "236528b2bd68c19333f7df926e17002e"
student@attackdefense:~$
```

Q4. What command can be used to print all codecs being used by RTP protocol?

Answer: tshark -r VoIP_traffic.pcap -Y "sdp" -Tfields -e sdp.media



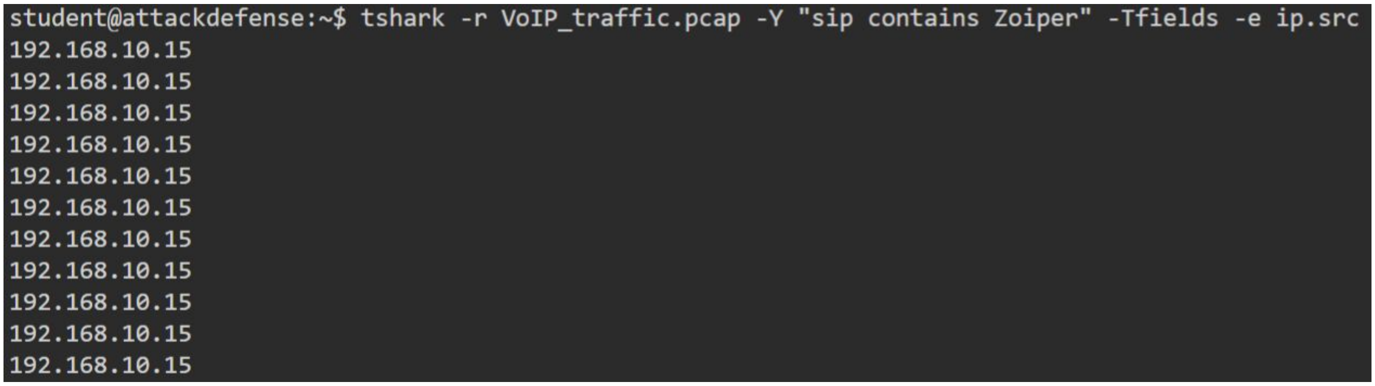
```
student@attackdefense:~$ tshark -r VoIP_traffic.pcap -Y "sdp" -Tfields -e sdp.media
audio 48268 RTP/AVP 3 0 8 101
audio 48268 RTP/AVP 3 0 8 101
audio 48268 RTP/AVP 3 0 8 101
audio 48268 RTP/AVP 3 0 8 101
audio 48268 RTP/AVP 3 0 8 101
audio 48268 RTP/AVP 3 0 8 101
audio 48268 RTP/AVP 3 0 8 101
audio 48268 RTP/AVP 3 0 8 101
audio 48268 RTP/AVP 3 0 8 101
audio 48268 RTP/AVP 3 0 8 101
audio 19138 RTP/AVP 3 101
audio 48268 RTP/AVP 3 0 8 101
audio 48268 RTP/AVP 3 0 8 101
audio 48268 RTP/AVP 3 0 8 101
audio 48268 RTP/AVP 3 0 8 101
audio 22166 RTP/AVP 8 101
audio 22166 RTP/AVP 8 101
audio 22166 RTP/AVP 8 101
student@attackdefense:~$
```

Set B:

Q1. What is the IP address of the user who is using the Zoiper VoIP client?

Answer: 192.168.10.15

Command: tshark -r VoIP_traffic.pcap -Y "sip contains Zoiper" -Tfields -e ip.src

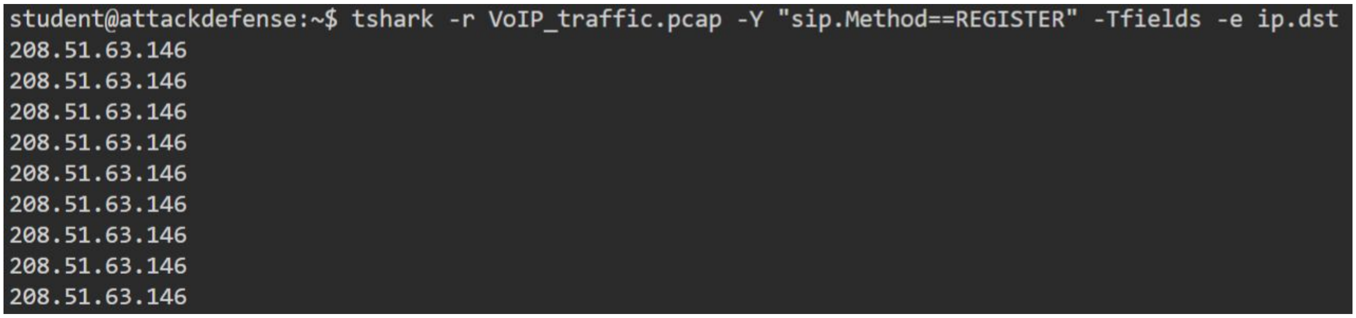


```
student@attackdefense:~$ tshark -r VoIP_traffic.pcap -Y "sip contains Zoiper" -Tfields -e ip.src
192.168.10.15
192.168.10.15
192.168.10.15
192.168.10.15
192.168.10.15
192.168.10.15
192.168.10.15
192.168.10.15
192.168.10.15
192.168.10.15
192.168.10.15
```

Q2. What is the IP address of the SIP server used to place calls?

Answer: 208.51.63.146

Command: tshark -r VoIP_traffic.pcap -Y "sip.Method==REGISTER" -Tfields -e ip.dst

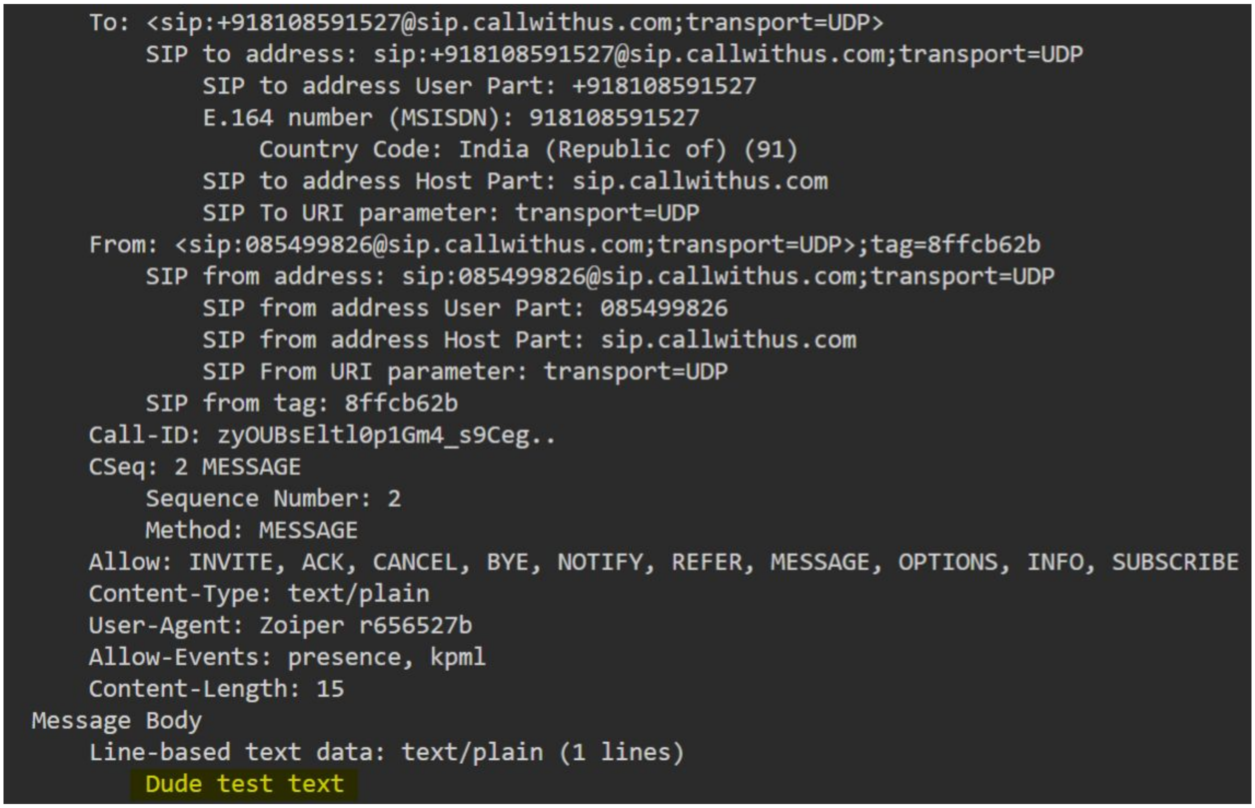


```
student@attackdefense:~$ tshark -r VoIP_traffic.pcap -Y "sip.Method==REGISTER" -Tfields -e ip.dst
208.51.63.146
208.51.63.146
208.51.63.146
208.51.63.146
208.51.63.146
208.51.63.146
208.51.63.146
208.51.63.146
208.51.63.146
```

Q3. What is the content of the text message sent to +918108591527?

Answer: Dude test text

Command: tshark -r VoIP_traffic.pcap -Y "sip.Method == MESSAGE" -V (Read the content)

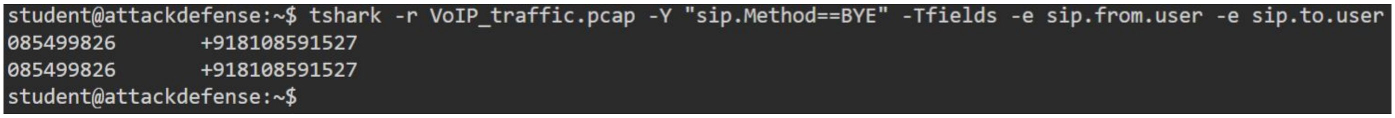


```
    To: <sip:+918108591527@sip.callwithus.com;transport=UDP>
        SIP to address: sip:+918108591527@sip.callwithus.com;transport=UDP
            SIP to address User Part: +918108591527
            E.164 number (MSISDN): 918108591527
                Country Code: India (Republic of) (91)
            SIP to address Host Part: sip.callwithus.com
            SIP To URI parameter: transport=UDP
    From: <sip:085499826@sip.callwithus.com;transport=UDP>;tag=8ffcb62b
        SIP from address: sip:085499826@sip.callwithus.com;transport=UDP
            SIP from address User Part: 085499826
            SIP from address Host Part: sip.callwithus.com
            SIP From URI parameter: transport=UDP
        SIP from tag: 8ffcb62b
    Call-ID: zyOUBsEltl0p1Gm4_s9Ceg..
    CSeq: 2 MESSAGE
        Sequence Number: 2
        Method: MESSAGE
    Allow: INVITE, ACK, CANCEL, BYE, NOTIFY, REFER, MESSAGE, OPTIONS, INFO, SUBSCRIBE
    Content-Type: text/plain
    User-Agent: Zoiper r656527b
    Allow-Events: presence, kpml
    Content-Length: 15
Message Body
    Line-based text data: text/plain (1 lines)
        Dude test text
```

Q4.Which extensions completed a call successfully?

Answer: 085499826   918108591527

Command: tshark -r VoIP_traffic.pcap -Y "sip.Method==BYE" -Tfields -e sip.from.user -e sip.to.user



```
student@attackdefense:~$ tshark -r VoIP_traffic.pcap -Y "sip.Method==BYE" -Tfields -e sip.from.user -e sip.to.user
085499826       +918108591527
085499826       +918108591527
student@attackdefense:~$
```

References:

1. Tshark (https://www.wireshark.org/docs/man-pages/tshark.html)
2. Wireshark (https://www.wireshark.org/)