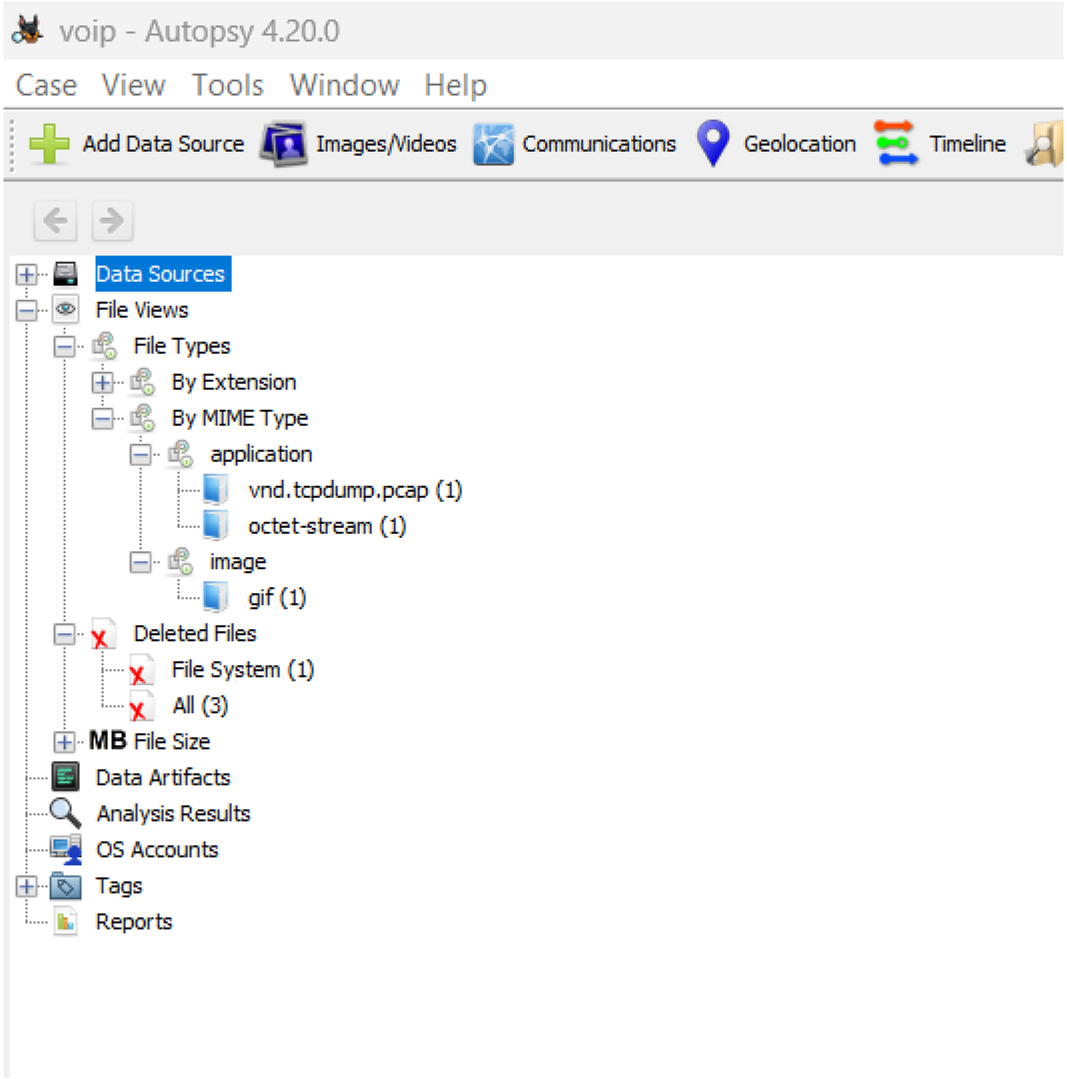
Steps to solve this challenge :

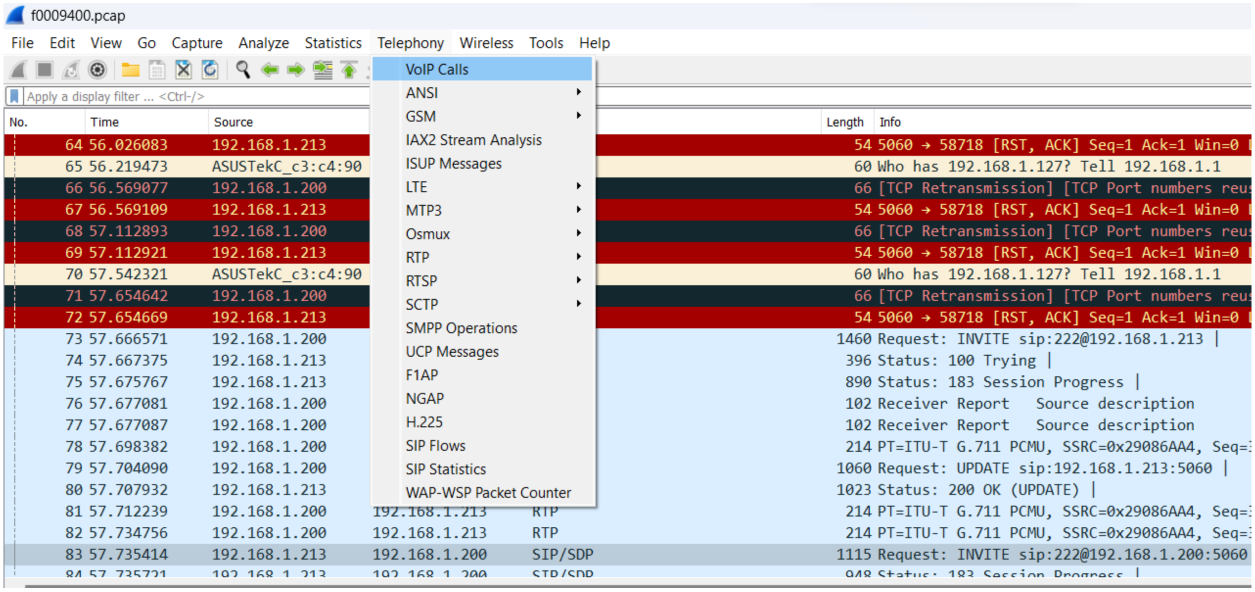
Step - 1 : Download and extract the .zip file

Step - 2 : Inside the zip file there is a disk image file called chal.img , Open that file with autopsy for analysis.

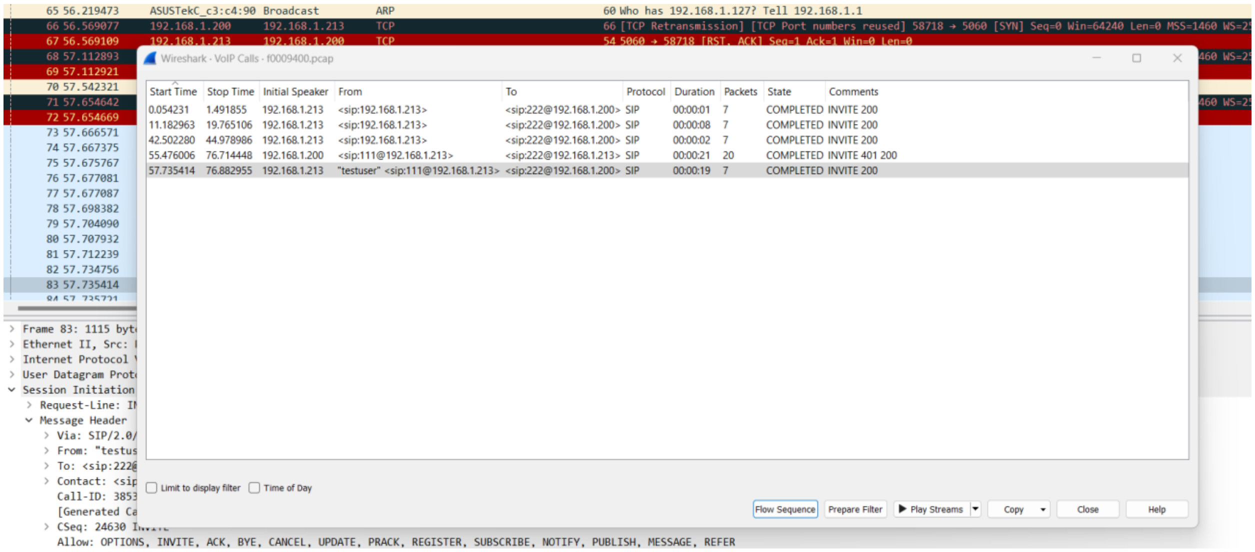
Step - 3 : After opening the file into the autopsy, Go to > Deleted File System and there you will get one .pcap file, extract that file.



Step 4 : Open that file in wireshark you will get the VOIP packet capture file which includes the SIP and RTP packets, To get the flag go to Telephony option in the top menu and select VOIP calls. This wireshark plugin composes a audio file from the RTP packets of the pcap file.



```
No.  Time        Source              Length Info
  64 56.026083   192.168.1.213          54 5060 → 58718 [RST, ACK] Seq=1 Ack=1 Win=0 L
  65 56.219473   ASUSTekC_c3:c4:90      60 Who has 192.168.1.127? Tell 192.168.1.1
  66 56.569077   192.168.1.200          66 [TCP Retransmission] [TCP Port numbers reus
  67 56.569109   192.168.1.213          54 5060 → 58718 [RST, ACK] Seq=1 Ack=1 Win=0 L
  68 57.112893   192.168.1.200          66 [TCP Retransmission] [TCP Port numbers reus
  69 57.112921   192.168.1.213          54 5060 → 58718 [RST, ACK] Seq=1 Ack=1 Win=0 L
  70 57.542321   ASUSTekC_c3:c4:90      60 Who has 192.168.1.127? Tell 192.168.1.1
  71 57.654642   192.168.1.200          66 [TCP Retransmission] [TCP Port numbers reus
  72 57.654669   192.168.1.213          54 5060 → 58718 [RST, ACK] Seq=1 Ack=1 Win=0 L
  73 57.666571   192.168.1.200        1460 Request: INVITE sip:222@192.168.1.213 |
  74 57.667375   192.168.1.213         396 Status: 100 Trying |
  75 57.675767   192.168.1.213         890 Status: 183 Session Progress |
  76 57.677081   192.168.1.200         102 Receiver Report   Source description
  77 57.677087   192.168.1.200         102 Receiver Report   Source description
  78 57.698382   192.168.1.200         214 PT=ITU-T G.711 PCMU, SSRC=0x29086AA4, Seq=
  79 57.704090   192.168.1.200        1060 Request: UPDATE sip:192.168.1.213:5060 |
  80 57.707932   192.168.1.213        1023 Status: 200 OK (UPDATE) |
  81 57.712239   192.168.1.200      192.168.1.213      RTP        214 PT=ITU-T G.711 PCMU, SSRC=0x29086AA4, Seq=
  82 57.734756   192.168.1.200      192.168.1.213      RTP        214 PT=ITU-T G.711 PCMU, SSRC=0x29086AA4, Seq=
  83 57.735414   192.168.1.213      192.168.1.200      SIP/SDP   1115 Request: INVITE sip:222@192.168.1.200:5060
  84 57.735721   192.168.1.213      192.168.1.200      SIP/SDP    948 Status: 183 Session Progress |
```



```
65 56.219473  ASUSTekC_c3:c4:90 Broadcast      ARP   60 Who has 192.168.1.127? Tell 192.168.1.1
66 56.569077  192.168.1.200     192.168.1.213  TCP   66 [TCP Retransmission] [TCP Port numbers reused] 58718 → 5060 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=2
67 56.569109  192.168.1.213     192.168.1.200  TCP   54 5060 → 58718 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
68 57.112893
69 57.112921
70 57.542321
71 57.654642
72 57.654669
73 57.666571
74 57.667375
75 57.675767
76 57.677081
77 57.677087
78 57.698382
79 57.704090
80 57.707932
81 57.712239
82 57.734756
83 57.735414
84 57.735721
```

Start Time	Stop Time	Initial Speaker	From	To	Protocol	Duration	Packets	State	Comments
0.054231	1.491855	192.168.1.213	<sip:192.168.1.213>	<sip:222@192.168.1.200>	SIP	00:00:01	7	COMPLETED	INVITE 200
11.182963	19.765106	192.168.1.213	<sip:192.168.1.213>	<sip:222@192.168.1.200>	SIP	00:00:08	7	COMPLETED	INVITE 200
42.502280	44.978986	192.168.1.213	<sip:192.168.1.213>	<sip:222@192.168.1.200>	SIP	00:00:02	7	COMPLETED	INVITE 200
55.476006	76.714448	192.168.1.200	<sip:111@192.168.1.213>	<sip:222@192.168.1.213>	SIP	00:00:21	20	COMPLETED	INVITE 401 200
57.735414	76.882955	192.168.1.213	"testuser" <sip:111@192.168.1.213>	<sip:222@192.168.1.200>	SIP	00:00:19	7	COMPLETED	INVITE 200

```
> Frame 83: 1115 byt
> Ethernet II, Src: 
> Internet Protocol 
> User Datagram Prot
v Session Initiation
  > Request-Line: IN
  v Message Header
    > Via: SIP/2.0/
    > From: "testus
    > To: <sip:222@
    > Contact: <sip
      Call-ID: 3853
      [Generated Ca
    > CSeq: 24630 Invite
      Allow: OPTIONS, INVITE, ACK, BYE, CANCEL, UPDATE, PRACK, REGISTER, SUBSCRIBE, NOTIFY, PUBLISH, MESSAGE, REFER
```

Play the audio from test user and after playing the audio you retrieve the Flag

Note: If you cannot determine the information present in the audio you can use any online tool which converts audio into text and retrieve the ciphertext.

Step 8 : Submit your flag in chtctf{d3v3l0p3d_vo1c3_0v3r_1p**} format.**