Sakarya Universitesi Bilgisayar ve Bilişim Bilimleri Fakültesi

Bilgisayar Mühendisliği Bölümü

İnternet Mühendisliği Ödevi

Öğretmen: Dr. öğretim üyesi Musa BALTA

Hazırlayan Öğrencinin

Adı: Furkan

Soyadı: Yanteri

Nu:b181210380

Şube:1A

Konu: SIP Potokolünün Analiz Edilmesi ve Wireshark İle Yakalanan Bir SIP Paketinin Gösterimi ve Açıklanması

İçerik

1. SIP Protokolü Tarihsel Süreci ve Oluşumu

- **1996** Henning Schulzrinne, Mark Handley ve Jonathan Rosenberg tarafından tasarlandı.
- **1999** RFC2543 olarak standartlaştırılmıştır.
- **2000** SIP, 3GPP sinyal protokolü ve hücresel ağlarda IP tabanlı akışlı multimedya hizmetleri için IP multimedya alt sistemi (IMS) mimarisinin kalıcı unsuru olarak kabul edildi.
- **2002** RFC3261 olarak kabul edildi ve o zamandan beri çeşitli uzantılar ve açıklamalar yayınlandı.

2. SIP Protokolü Nedir?

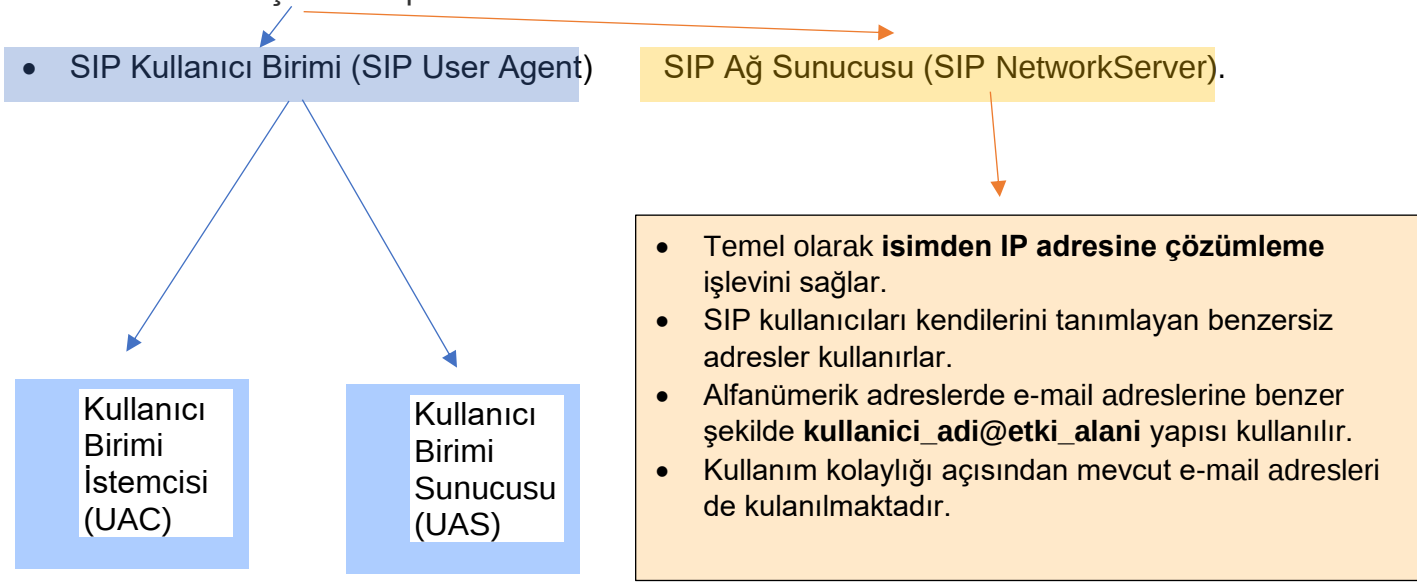
- SIP yani **S**ession **I**nitiation **P**rotocol (Oturum Başlatma Protokolü)
- VOIP **telefon aramalarını oluşturmak**, **ayarlamak** ve **bitirmek** için kullanılan bir **IP telefonculuğu işaretleşme protokolüdür.**

2.1 Kısaca VOIP den bahsetmek gerekirse:

- **VoIP = Volume Over IP** yani, **İnternet Protokolu üzerinden ses** demektir.
- Basitce **IP-temelli şebekeler üzerinden ses trafiğinin iletilmesidir.** İlk önce veri şebekeleri için tasarlandı, dünya standartında veri şebekelerinin başarılı konumlandırması ile, İnternet Protokolu (IP) daha sonra ses şebekeleri için de adapte edildi.
- VoIP PBX sistemleri, çalışanlara taşınırlık, bir işyeri genişlediğinde esneklik sağlar, çünkü **geleneksel PBX'e göre idare etmesi daha kolaydır** ve telefon idare **masraflarını da oldukça düşürür**.

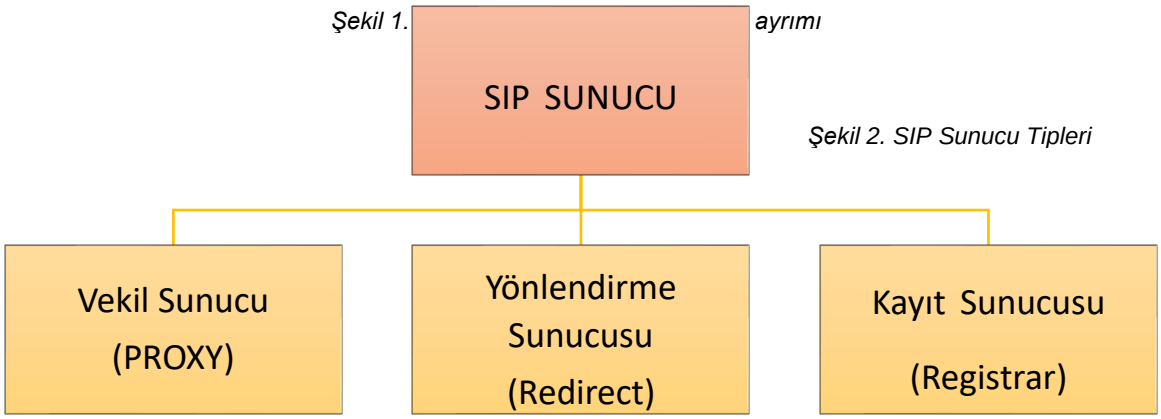
3. SIP Protokolü Bileşenleri

- SIP 2 ana bileşene sahiptir.



- Bir SIP uygulamasında üç tür sunucu bulunabilir

Şekil 1. ayrımı

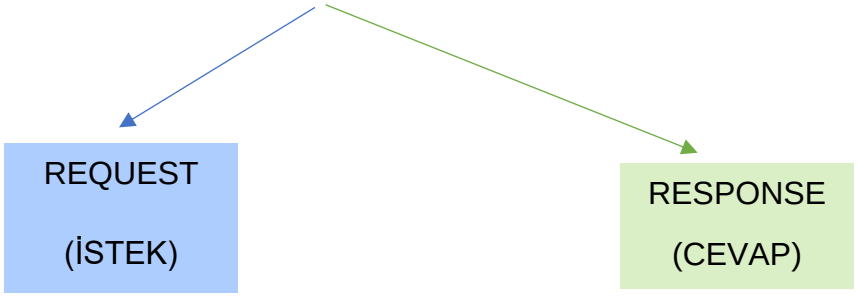


Şekil 2. SIP Sunucu Tipleri

- Vekil Sunucu (Proxy Server), diğer kullanıcılar adına talepte bulunabilen ve hem sunucu ve hem de kullanıcı rolünü üstlenebilen bir sunucu türüdür.Bir Vekil Sunucu, talebi yorumladıktan sonra gerekiyorsa talep mesajını yeniden yapılandırarak iletebilir. **Bu tür sunucular SIP olmayan uçlarla çoklu ortam oturumlarının kurulabilmesine de olanak sağlayabilirler**.Örneğin SIP'den H.323'e çevrim gibi.
- Yönlendirme Sunucusu (Redirect Server), **SIP talebini kabul eder, aranan tarafın adresini ya da aranan tarafın adresini bilmiyorsa adres olarak sıfırı geri döndürür.** Vekil Sunucunun aksine Yönlendirme Sunucusu talepleri diğer sunuculara aktarmaz.
- Kayıt Sunucusu (Registrar), Bir kayıt sunucusu, kullanıcıların kayıt taleplerini kabul ederek**, kullanıcıların konum bilgilerinin bulunduğu veri tabanını günceller**.

4. SIP Mesajları

- İki temel tür SIP mesajı bulunmaktadır.



Şekil 3. SIP Sunucu Tipleri

Kullanıcıdan sunucuya talep mesajları **Sunucudan kullanıcıya** cevap mesajları

MESAJ İSMİ	MESAJIN TANIMI
İnvite	Çağrıyı başlatır ve çağrı parametrelerini değiştirir (re-INVITE).
Ack	INVITE için nihai bir onaydır.
Bye	Bir çağrıyı sonlandırır.
Cancel	Araştırmayı ve çalmayı (Ring) iptal eder
Options	Karşı uç birimin yeteneklerini sorgular.
Register	Konum hizmetine kaydolunmasını sağlar.
İnfo	Oturum durumunu değiştirmeden oturum bilgisini gönderir.

Tablo1. SIP Mesajları

- CEVAP Mesajları

  - Cevap mesajları **HTTP cevap kodlarına dayanan** nümerik kodlar içerirler.
  - Cevap mesajlarının iki alt türü ve altı sınıfı vardır.
    - Kurulum aşaması (Provisional, 1xx sınıfı)
    - Bu cevaplar sunucu tarafından çağrı aşamalarını belirtmek için kullanılırlar.
    - Sonuç (Final, 2xx, 3xx, 4xx, 5xx ve 6xx sınıfları)
    - SIP iletimlerini sonlandıran sonuç cevaplarıdır.

1xx = Kurulum, araştırma, ring, kuyruğa alma vb.

2xx = Başarı.

3xx = Yeniden yönlendirme, aktarma.

4xx = Talep başarısızlığı (Kullanıcı hataları).

5xx = Sunucu başarısızlığı.

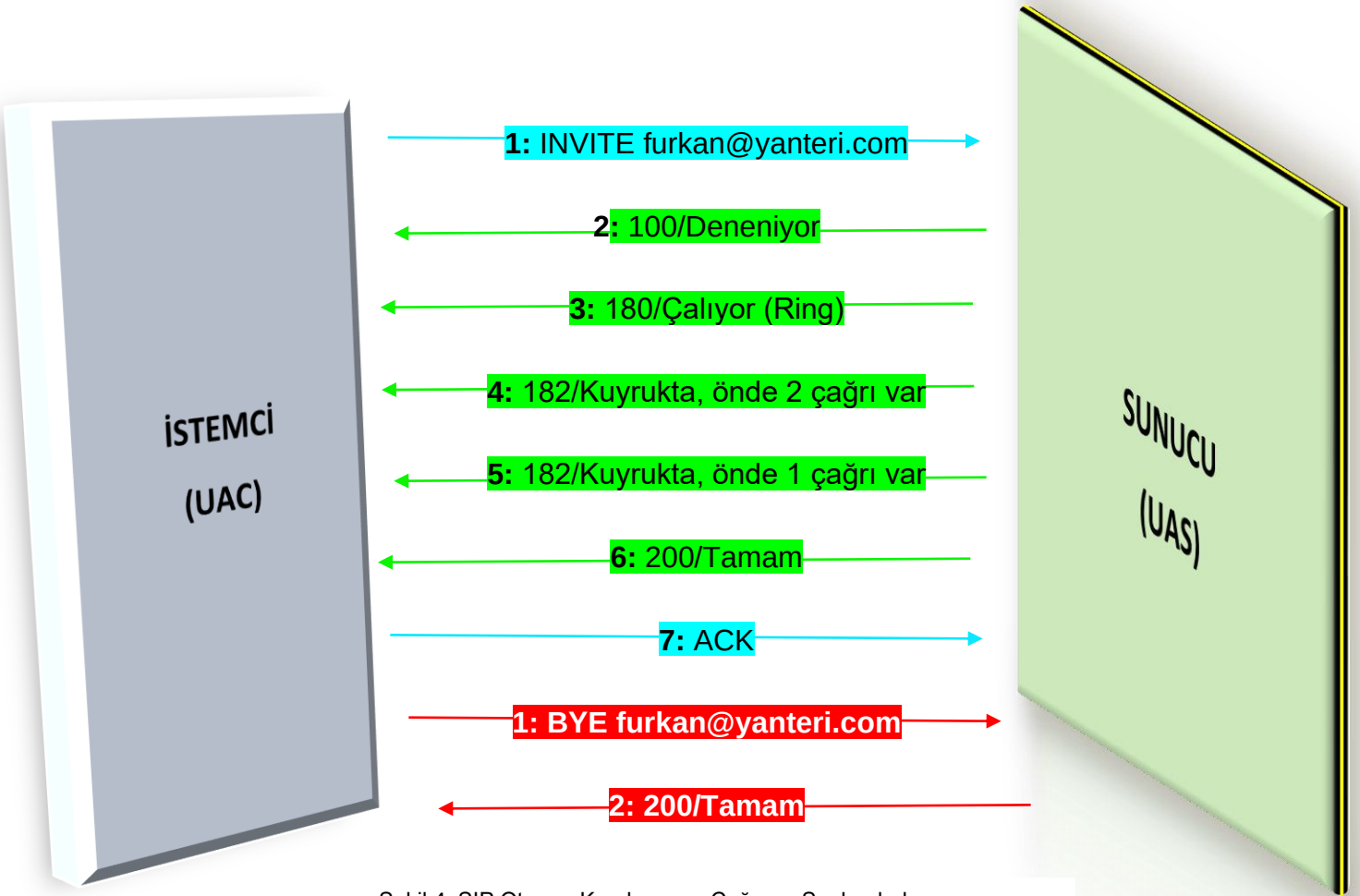
6xx = Genel başarısızlık (Meşgul, ret, hedef kullanıcı erişilemiyor)

- CEVAP Mesajı için yukarıdaki sınıflara dair örnekler:

100	Devam.	481	Çağrı bacağı mevcut değil.
180	Ring.	5**	Sunucu hatası.
200	Tamam.	600	Meşgul.
300	Çoklu seçim.	603	Ret.
302	Geçici olarak taşındı.	604	Mevcut değil.
400	Hatalı talep.	606	Kabul edilemez.

Tablo 2. SIP Cevap Mesajları Örneklendirme

- **SIP Protokolünü kullanan 2 kullanıcı arasındaki iletişimin başlatılması ve bitirilmesi nasıl işler?**



Şekil 4. SIP Oturum Kurulumu ve Çağrının Sonlandırılması

Oturum Kurulumu

1. Arayan UAC, **Furkan'ın SIP adresi** sip:**furkan@yanteri.com**'a bir **INVITE** mesajı gönderir.
2. UAS talebi alır ve hemen **"100"** cevap kodlu mesajı gönderir.
3. UAS uç birimi çaldırarak, **Ring, Furkan'a yeni bir çağrının geldiğini söyler** ve aynı anda UAC'ye "**180**" kodlu mesajı gönderir.
4. UAS "**182**" kodlu mesaj ile çağrının diğer iki çağrının arkasında kuyrukta olduğunu UAC'ye rapor eder.
5. UAS "**182**" kodlu mesaj ile çağrının diğer bir çağrının arkasında kuyrukta olduğunu UAC'ye rapor eder.
6. Furkan çağrıyı alır ve UAS arayan UA'a "**200**" kodlu mesajı gönderir. **Bu mesaj ayrıca Furkan'ın uç biriminin ortam yeteneklerini açıklayan bir SDP paketi içerir.**
7. Arayan UAC, "**200" kodlu mesaj ile cevabın alındığını onaylar**.

Oturumun Sonlandırılması

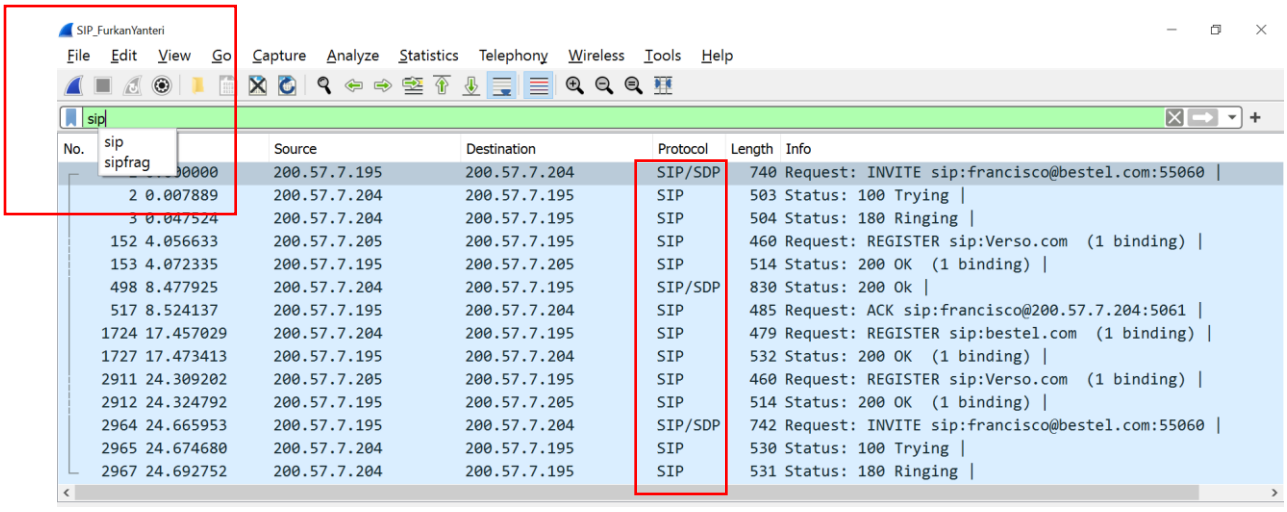
1. Arayan uç çağrıyı sonlandırmaya karar verir ve kapatır.
Furkan'ın **sip:furkan@yanteri.com** adresine **BYE** talebinin gönderilmesine neden olur.

2. Furkan'ın UAS'ı "**200**" kodlu mesaj ile cevap verir ve Furkan'a çağrının sona erdiğini bildirir.

- **SIP Protokolünde çağrı vekâleti**

1. Bir **INVITE** mesajı **furkan@yanteri.com'a** gönderilir ancak işaretleşme yolu üzerinde vekil sunucu **sip.yanteri.com** bulunur.
2. Vekil sunucu hemen "**100**" mesajı ile cevap verir.
3. Vekil sunucu Furkan'ın o anki konumuna SIP dışı bir servis üzerinden, örneğin LDAP, bakar.
4. Konum servisi Furkan'ın konumunu döndürür: SIP adresi **furkan@lab.yanteri.com.**
5. Vekil sunucu çağrıya **vekil olma kararı verir** ve asıl **INVITE** mesajında bulunan başlangıç satırındaki URI'ı **furkan@lab.yanteri.com** olarak değiştirerek yeni bir **INVITE** mesajı oluşturur. **Vekil sunucu** bu talebi lab.yanteri.com'daki UAS'ye gönderir.
6. UAS önce bir "**100**" ile cevap verir.
7. UAS sonra bir "**180**" cevabı gönderir.
8. Vekil sunucu "**180**" mesajını arayan UA'ya iletir.
9. Aranan kullanıcı çağrıyı cevapladığında (Örneğin ahizeyi kaldırdığında) **lab.yanteri.com'daki** UAS "200" cevabı gönderir. Bu örnekte Furkan'ın UAS'i cevaptaki erişim başlığına **furkan@lab.yanteri.com** değerini yerleştirir. Bundan sonraki haberleşme doğrudan gerçekleştirilerek **vekil sunucu** devre dışı bırakılır. Bu işlem seçime bağlıdır.
10. Vekil sunucu "**200**" cevabını arayan UAC'ye iletir.
11. Arayan UA ACK cevabını doğrudan Furkan'ın **lab.yanteri.com'daki** UA'sına gönderir.

5.Wireshark SIP Pcap İnceleme



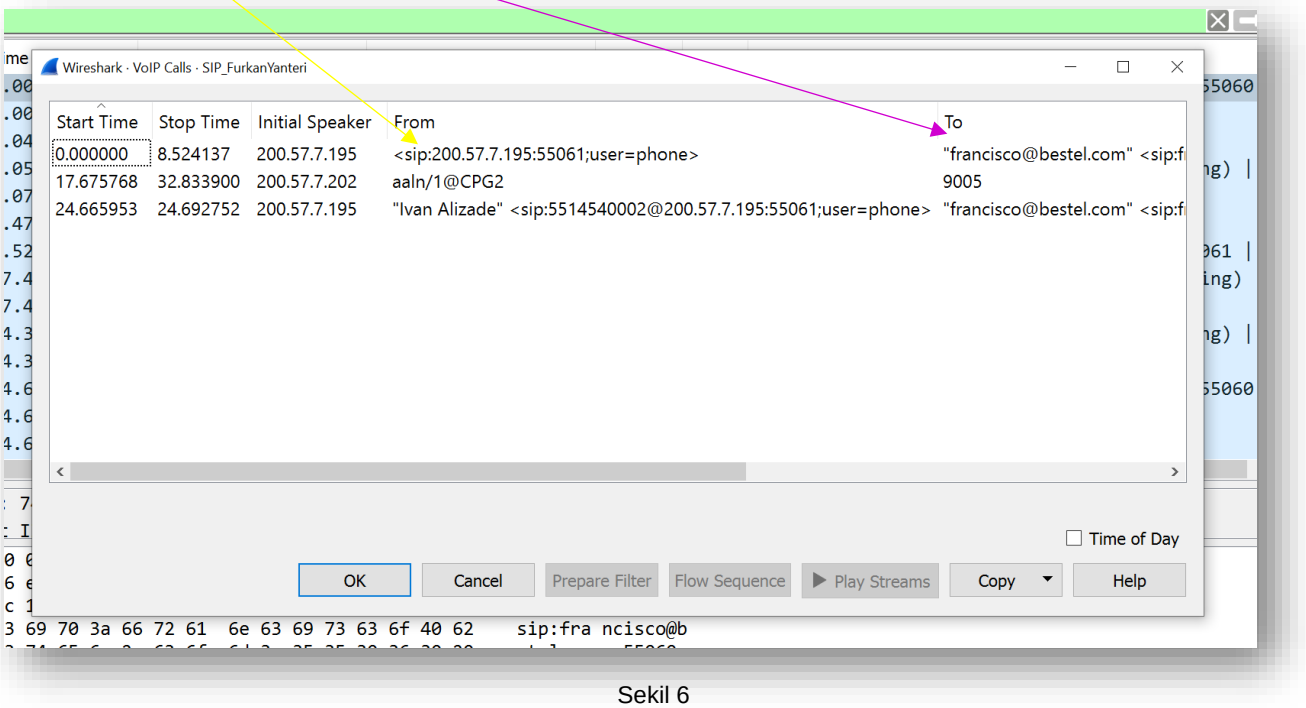
Sekil 5. Wireshark'da SIP dahil bir çok farklı türde paketlerin olduğu bir aralıkta capture edilmiş bir pcap için ekran ve SIP filtresiyle gösterim.

5.1 SIP aramalarını (SIP CALL) listeleme

Menü kısmından 'Telephony > VOIP Calls' kısmında SIP aramaları listesini görebiliriz.

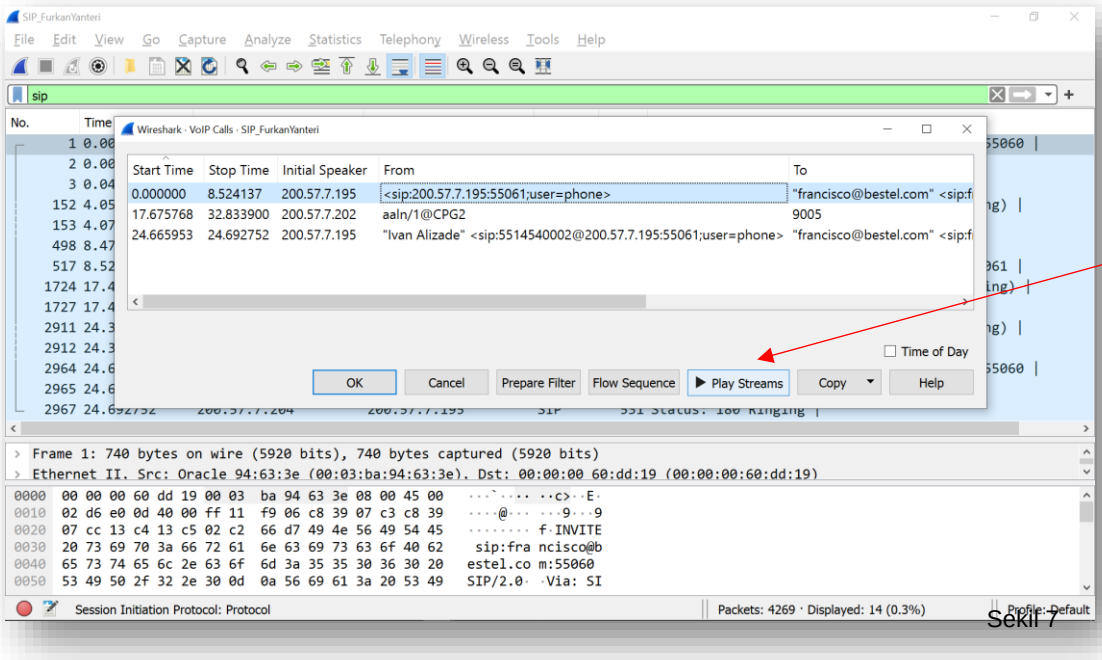
Elde edebileceğimiz bilgiler:

- Aramaların başlangıç ve bitiş zamanları.
- Konuşan kısmı arayanın IP adresidir.
- Arayan ve aranan kimlikleri.



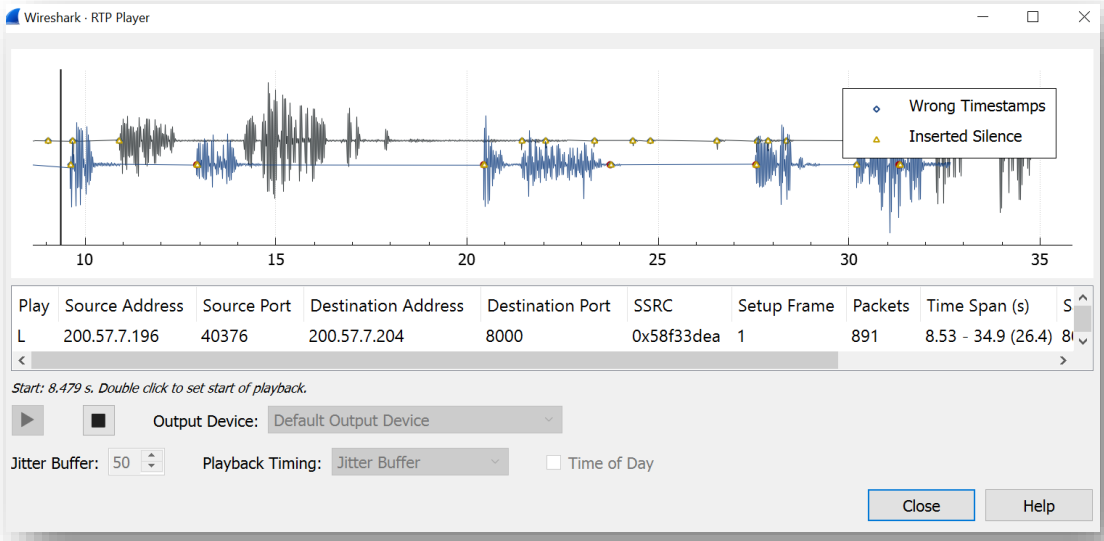
Sekil 6

5.2 SIP görüşmelerini dinleme



Sekil 7

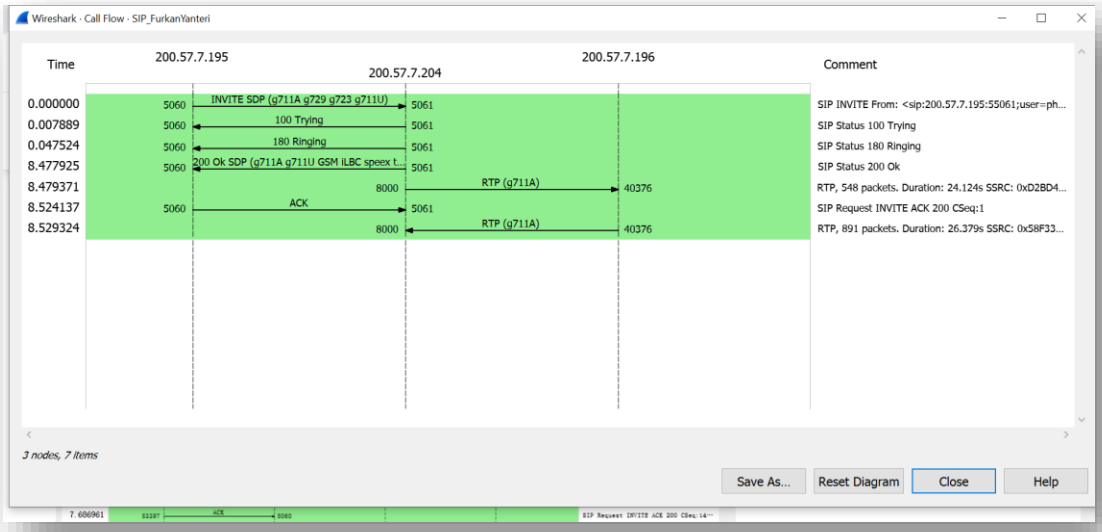
Bu ekranda aramalardan birini seçinde burada Play Streams kısmı aktif olur.Play streamse tıklayararak **konuşmaları dinleyebiliriz.**



Yandaki şekilde SIP üzerinden gerçekleştirilmiş VOIP sesli görüşme dinleniyor.

Sekil 7

5.3 SIP Flow sequence kısmından detaylı inceleme

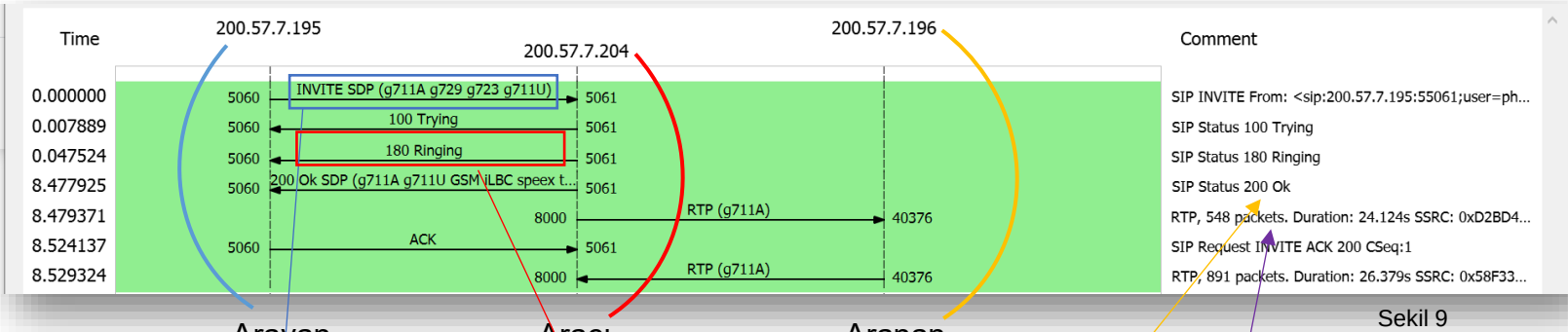


Bir önceki menüde flow sequence kısmına basarak ilgili SIP paketlerine dair detaylı bilgi elde edebiliriz.

SIP sinyal akışları(mesajlar)

Kaynek ve hedef portların adresleri

Sekil 8



Sekil 9

Arayan

İnvite(Davet) mesajı

Arayanın aramaya başladığı an

Aracı

Arayana,arananın telefonunun çaldığı bilgisi dönüyor.

(RİNGİNG 180)

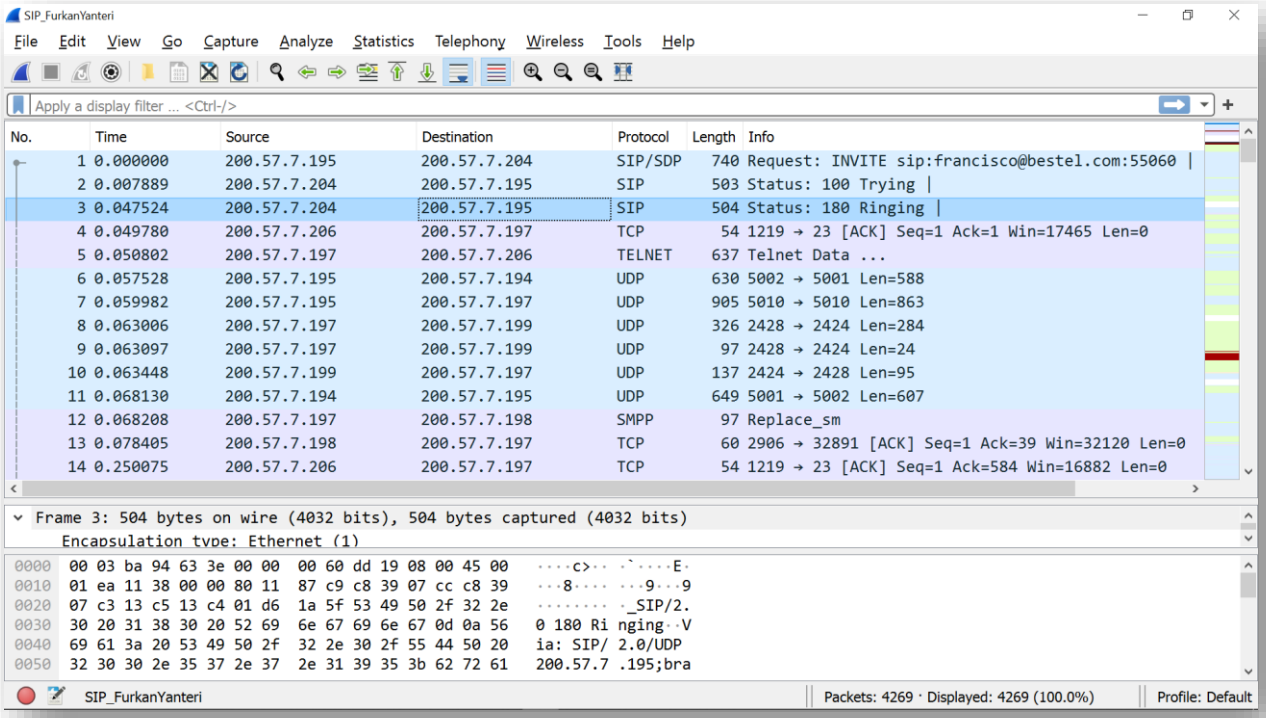
Aranan

Bağlanılan an

24.14 saniye boyunca gönderilen

Karşılıklı paketler sayısı.

5.4 Tek bir SIP paketinden detaylı inceleme



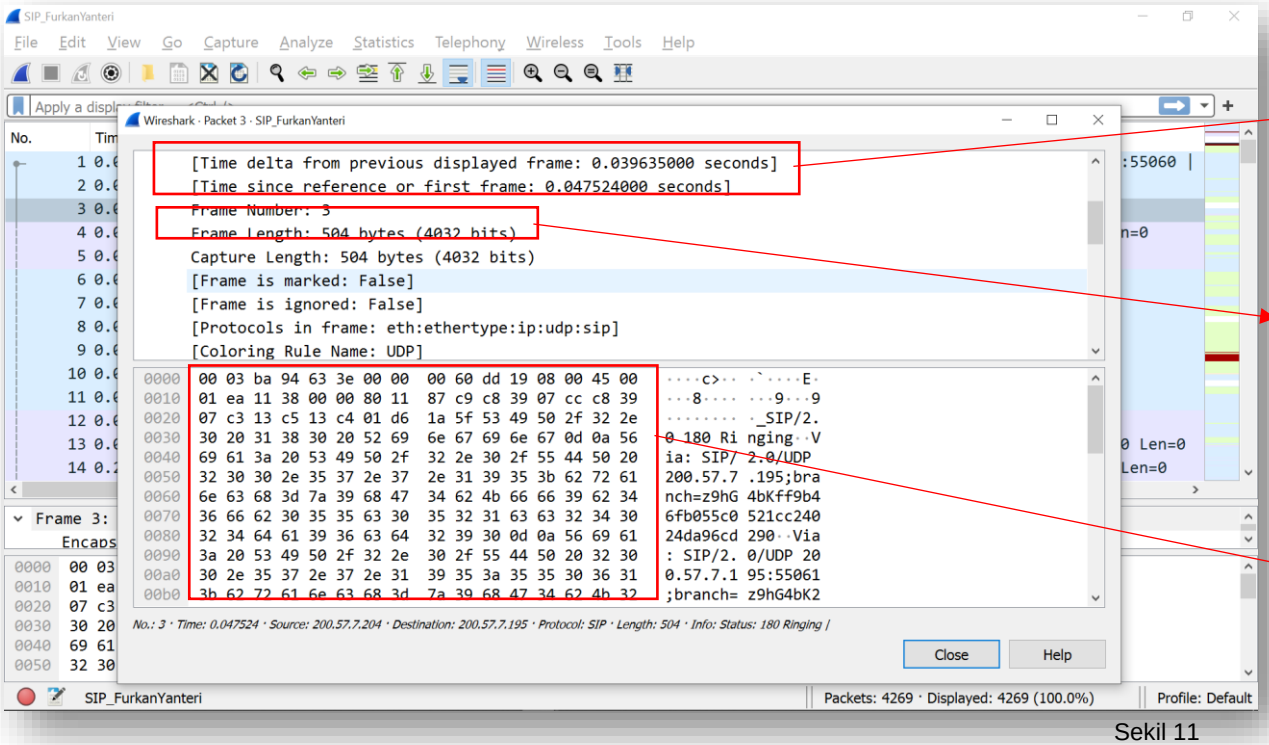
Sekil 10

Pcap dosyasından,

Capture ettiğimiz aralıktaki paketler listesinde bir çok paket var.Tek bir SIP paketi incelemek için bir tanesini seçelim.Zaten paketler listelenirken kaynak(source) ve hedef(destination)

bilgileriyle beraber tutulmakta.

200.57.7.204 cihazından gönderilen **180** paketini inceleyelim.



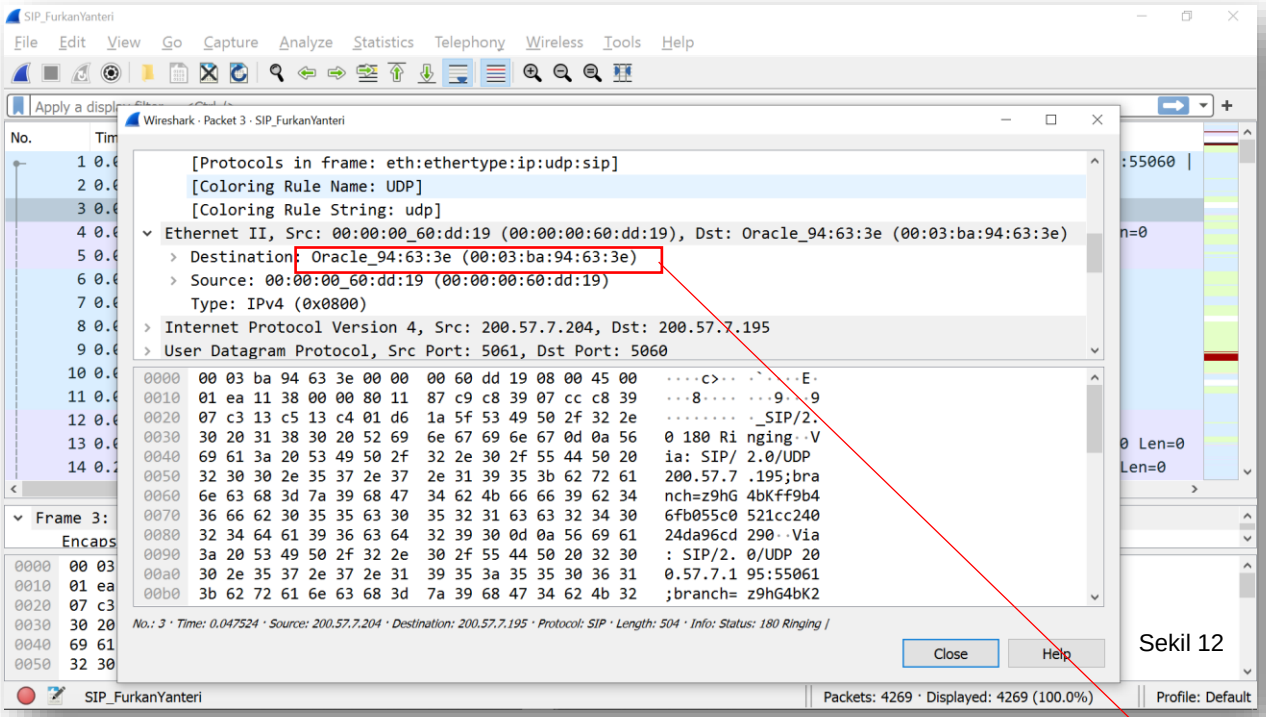
Sekil 11

Pakete çift tıklayarak paket içerik bölümüne girelim.Buradan paketlerin ulaşım zamanları hakkında bilgi almak da mümkün.

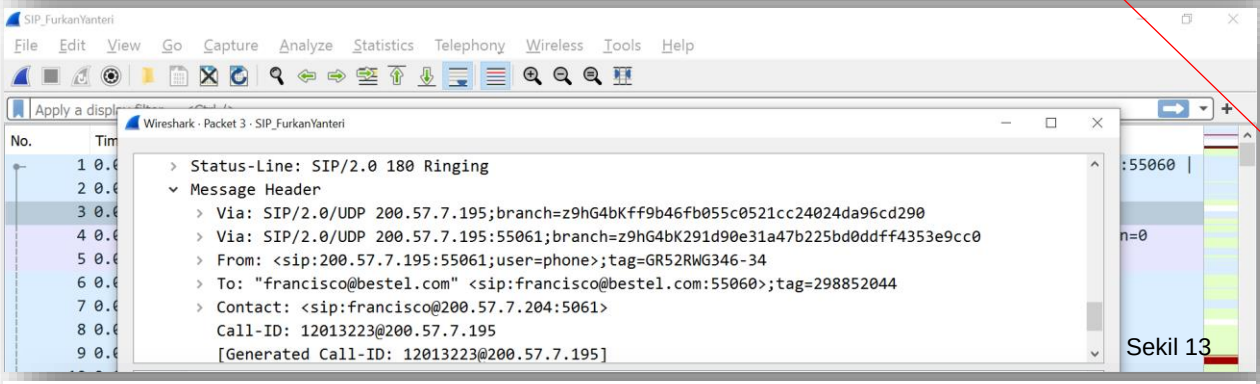
Çerçeve 504 byte.

Çerçevedeki protokoller **ip, udp** ve **SIP**.

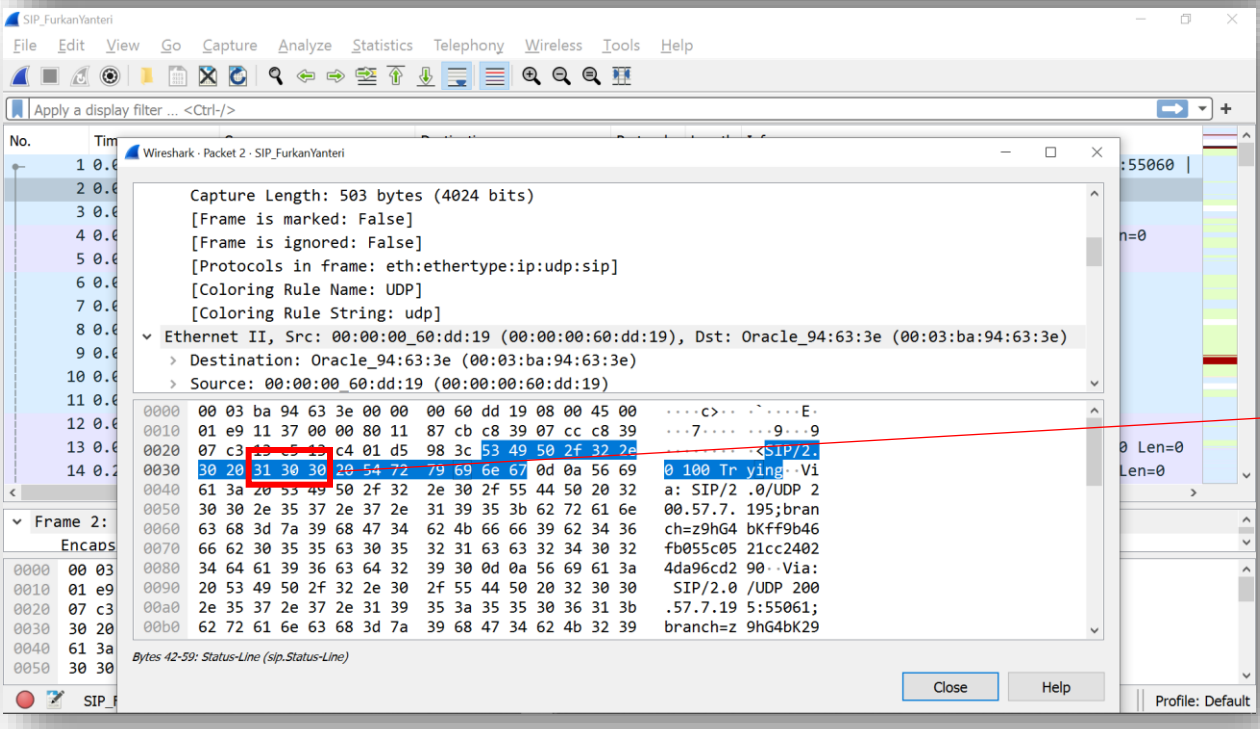
Paketler tabi ki binary formatta iletiliyor.Burada **hex** formatta paket içeriğinin tamamen gösterimi mevcut.Buradaki hex sayılar toplam **504 byte** dır.



Sekil 12



Sekil 13



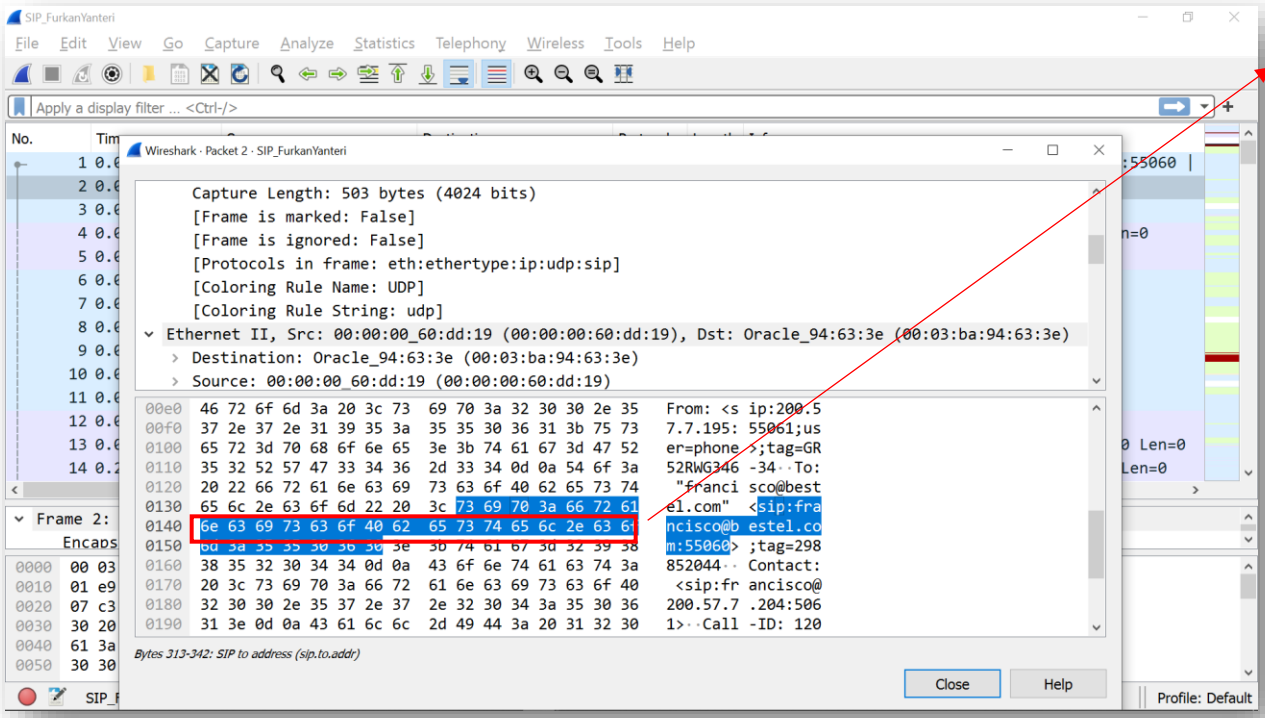
Sekil 14

VOIP görüşmeler için ara yönendirici sistemler oracle üzerinden kiralanmış sunuculardan yapılıyor.Bu çok güvenli değildir.Çünkü bir yerel ağda (ortalama 400 makine için) böyle bir sistemle kurup çağrıyı harici bir sunucu üzerinden (dış ağ / fiziksel bağlantısız dinlenebilir internet trafiği) yaptıklarına göre yüksek gizlilik seviyesi taşıyan görüşmeler bu hattan yapılmamaktadır.

Burada hem sunucu hem de port adı var.Fiziksel adrese yani görüşmeyi başlatan kişiye ulaşılabilir.

Paketin fiziksek olarak göründüğü kısımda sayıların üzerine gelerek anlamlandırılmış hali yanda görünmektedir.

Buradaki **31 30 30** kısmı bizzat mesajın adıdır.Yani **100** yani **TRYING** yani arama isteğinin sunucu tarafından kabul edilmiş olup hedef cihaza gerekli işlemlerin başlatılacağı anlamında.



Sekil 15

Burada hedef(aranmak istenen) cihazın sanal adresi bulunmaktadır.Tabi ki **Çerçevenin bu kısmındaki isim, aranan uçta** router kısmındaki **tablodan bakılıp fiziksel adrese dönüştürülerek iletim gerçekleştirilir.**Fakat uygulama katmanında fiziksek olarak adres bulundurma zorunluluğu yoktur.

6.Yararlanılan Kaynaklar

- **İnternet Siteleri**
  - https://www.voip-info.org/sip (ana kaynak)
  - https://www.3cx.com.tr/voip-sip/
  - https://support.yeastar.com/hc/en-us/articles/360007606533-How-to-Analyze-SIP-Calls-in-Wireshark
  - https://allegro-packets.com/en/network-multimeter/analysis-modules/sip-analysis
  - https://www.tutorialspoint.com/session_initiation_protocol/session_initiation_protocol_introduction.htm
- **Akademik Dökümanlar**
  - SIP Saldırıları ve Güvenlik Yöntemleri(Merve YÜKSEL, Nihat ÖZTÜRK (Gazi Universitesi)
  - SIP Basics Dennis Baron January 5, 2005/MIT
- **Diğer**(youtube, tutorialspoint, vb. video eğitimleri)

Saygılarımla
Son