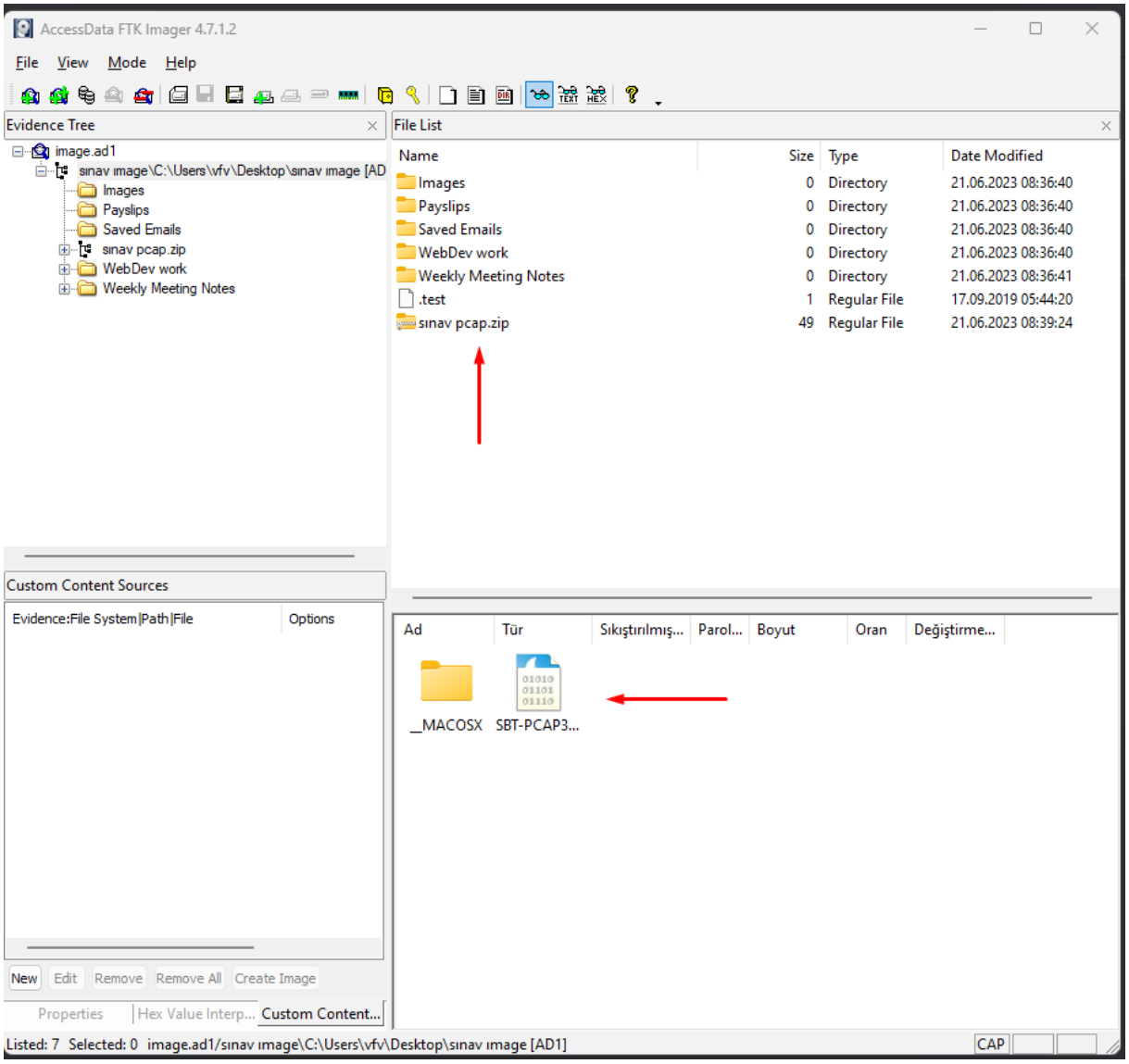
SORU 1: Sınav imaj isimli klasör içerisinde bir adet imaj dosyası bulunmakta, soru 4 ile ilgili soruları cevaplamanız için bu imaj içerisindeki “sınav pcap.zip” isimli zip dosyasını imaj içerisinden çıkarmanız gerekiyor. Bu dosyayı çıkarmak için kullandığınız programı>menüleri>örnekteki gibi yazınız. (10 puan)

Not: Ftk Imager ile açtım, file>add evidence item>image file ile dosyayı açtım ve ağaç yapısından ilgili dosyayı bulup çıkarttım. Dosya adı sınav pcap.zip şeklindeydi.



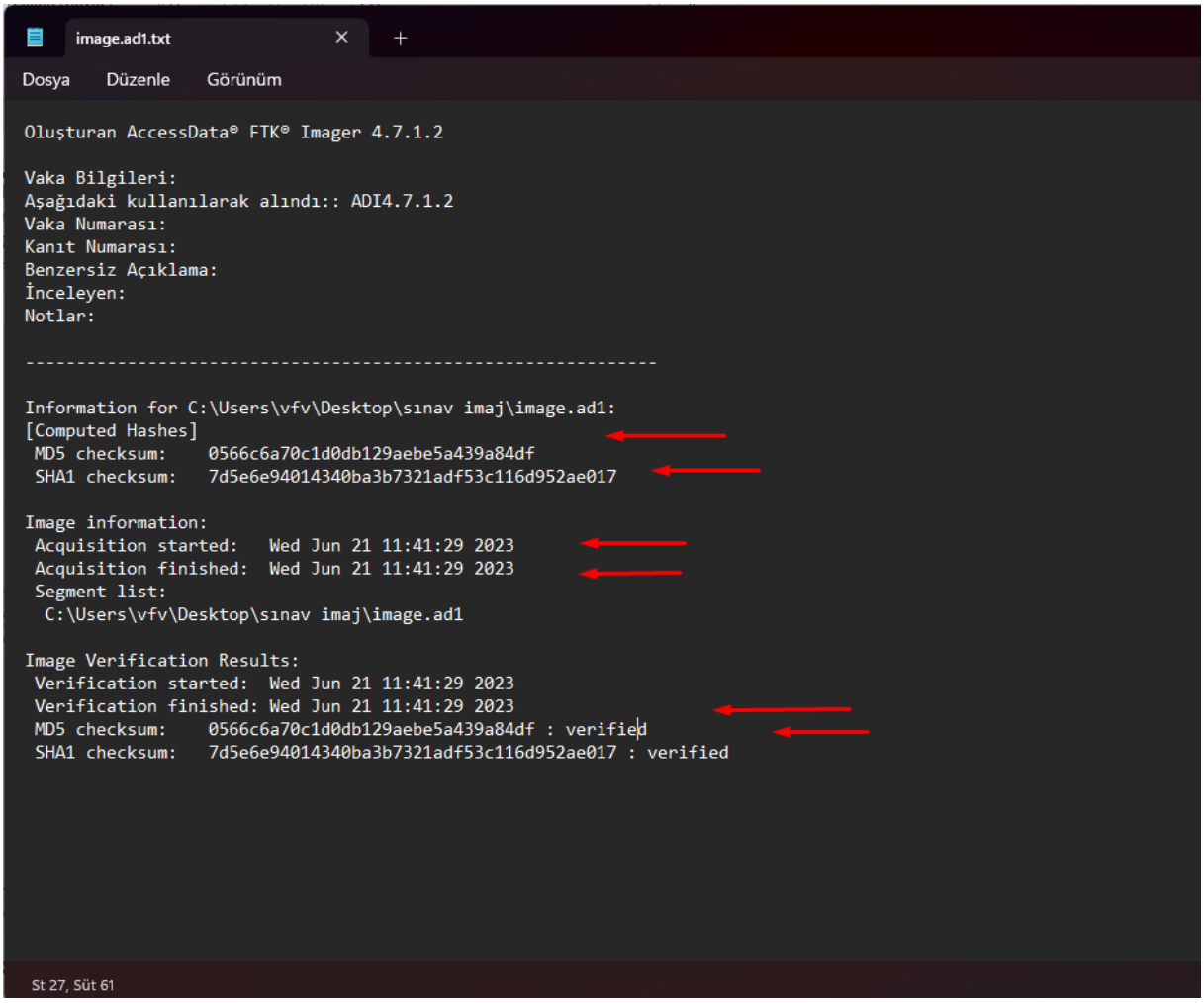
SORU 2: imajın oluşturma tarihini ve veri bütünlük değerini yazınız. (10 puan)

Oluşturulma tarihi → Wed Jun 21 11:41:29 2023

Veri bütünlük değerleri;

MD5 checksum: 0566c6a70c1d0db129aebe5a439a84df

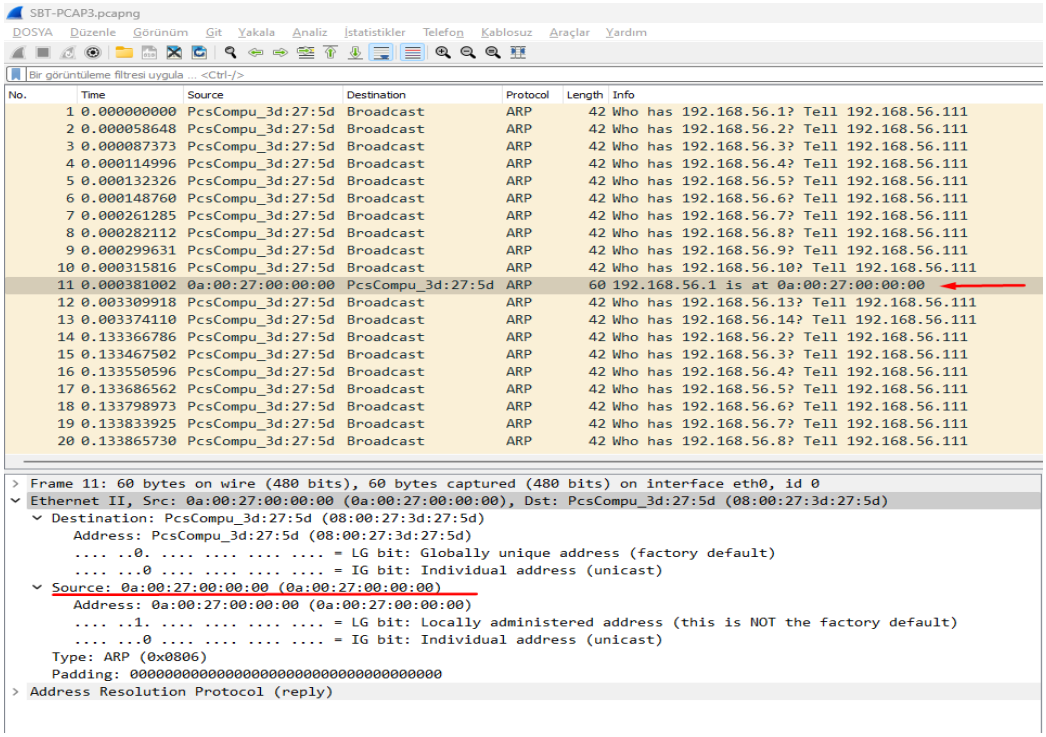
SHA1 checksum: 7d5e6e94014340ba3b7321adf53c116d952ae017



SORU 3: tcpdump yada Wireshark kullanarak Sınav.pcap isimli pcap dosyasını analizini ederek aşağıdaki soruları cevaplayınız.

1. Saldırganın MAC adresi nedir? (10) puan)

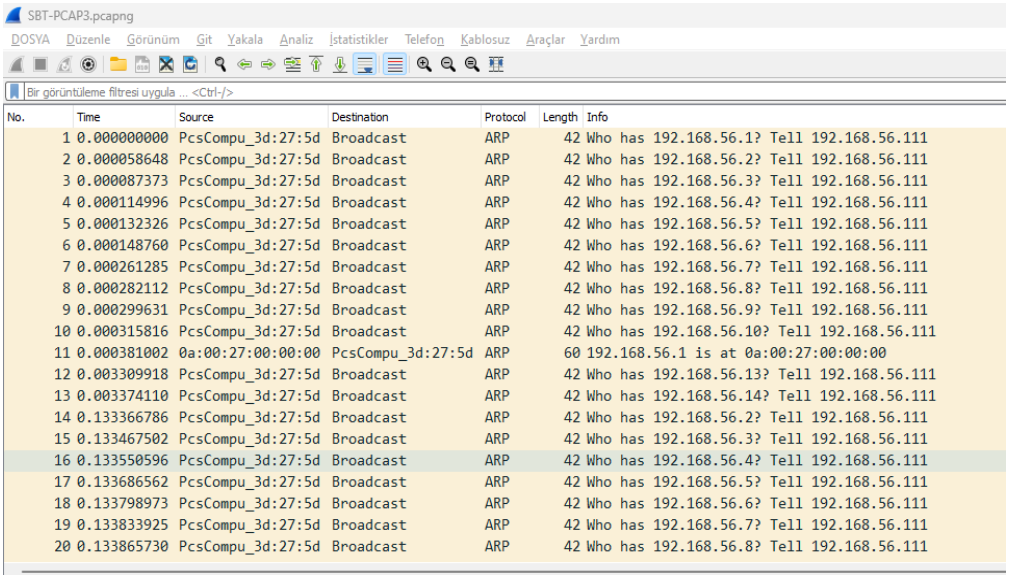
Mac address → 0a:00:27:00:00:00



2. Saldırganın merkezi sunucu ile başka bir ana bilgisayar arasındaki konuşmaları dinlemesine izin veren saldırı türü nedir? (5 puan)

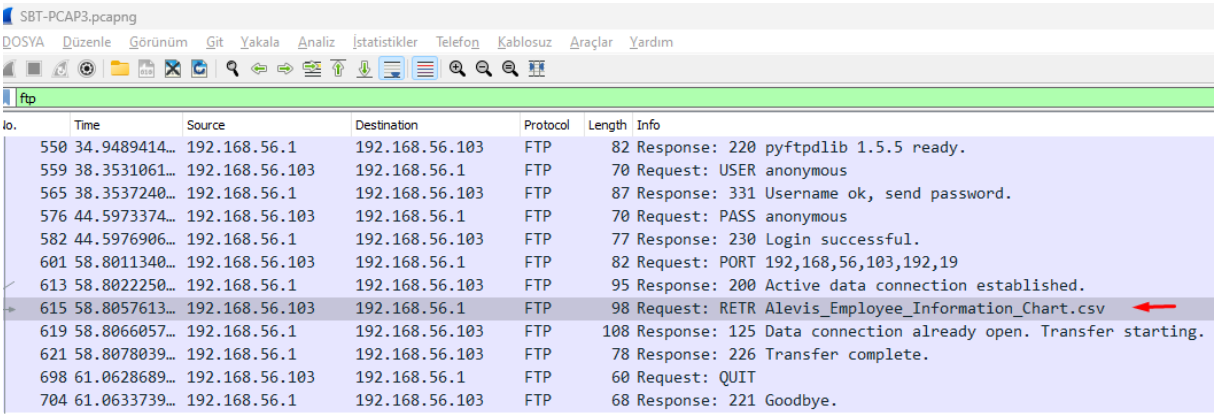
Man in the middle saldırısı, kısaca **MitM** yada türkçe adıyla ortadaki adam saldırısı denir.

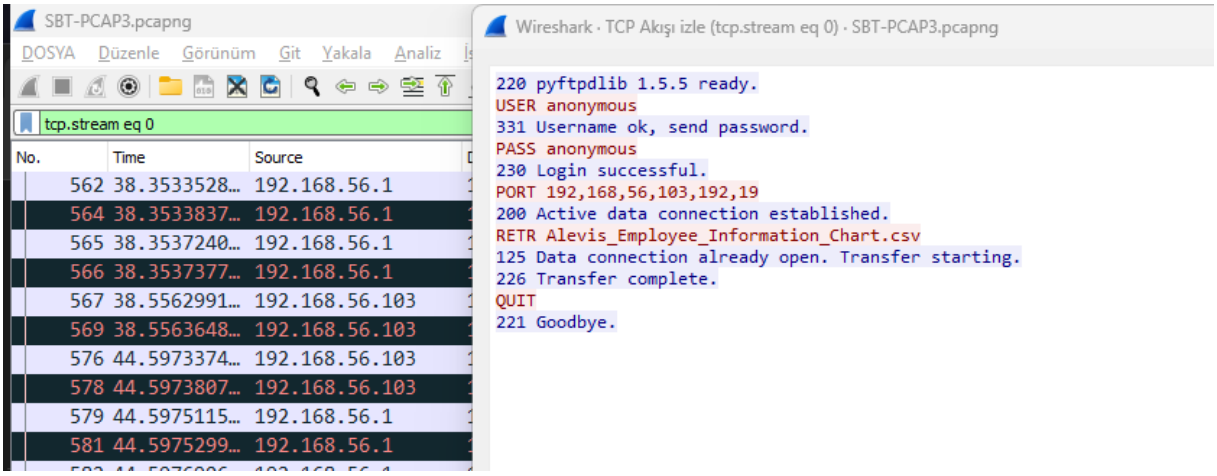
ARP zehirlenmesi bu pcap dosyasında yakalanmış MitM saldırı tekniğinin yöntemidir.



3. Merkezi sunucudan indirilen dosya nedir? (10 puan)

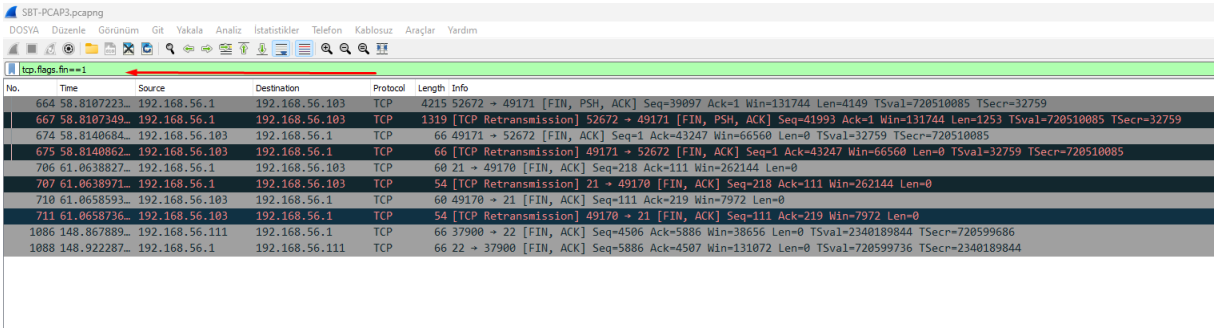
Merkezi sunucudan indirilen dosyanın adı → Alevis_Employee_Information_Chart.csv

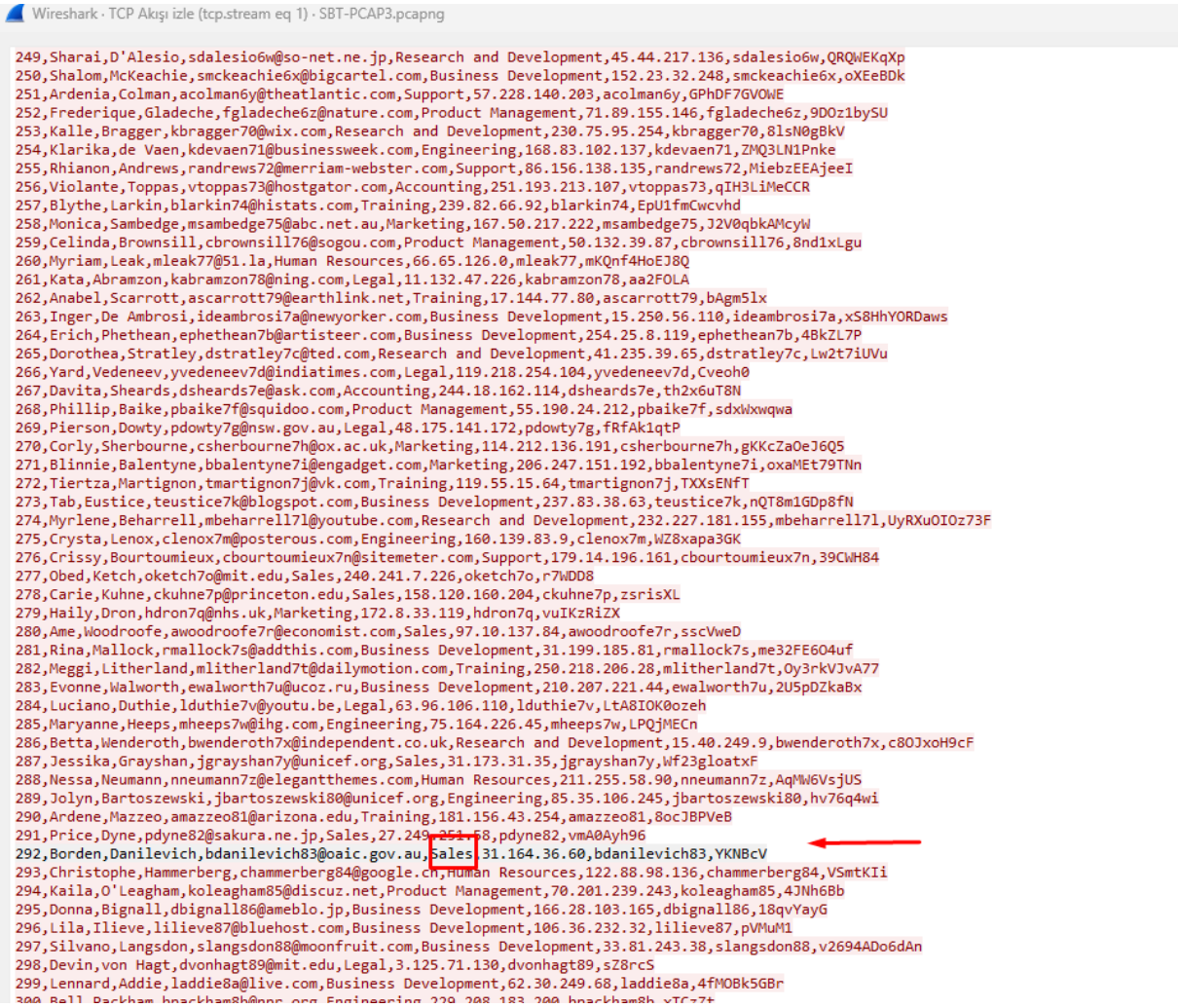




4. Borden Danilevich hangi departmanda çalışıyor? (20 puan)

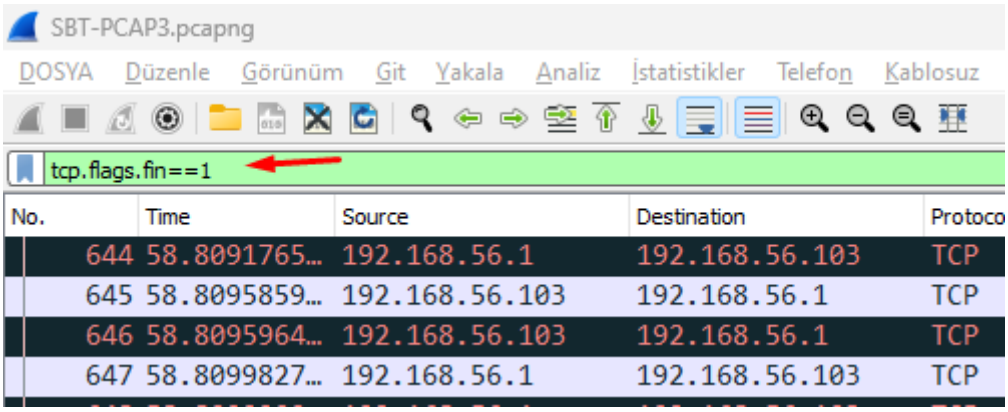
Sale departmant , Satış departmanında çalışıyor.

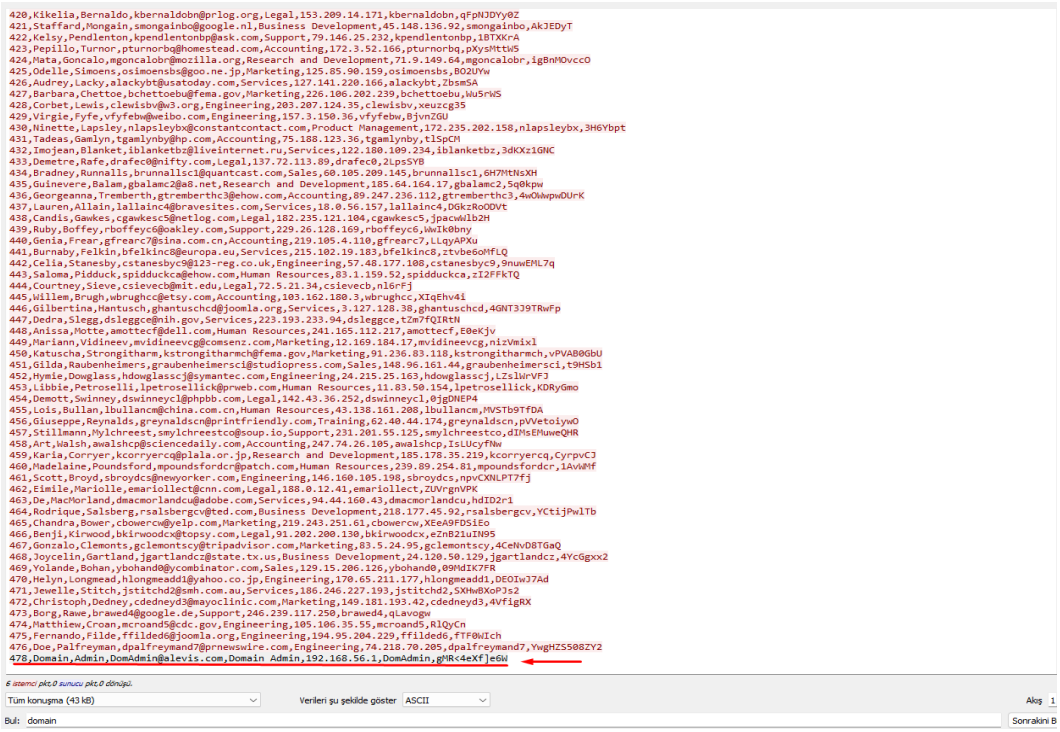




5. Domain Admin nin SSH parolası nedir? (20 puan)

PAROLA → gMR<4eXf]e6W

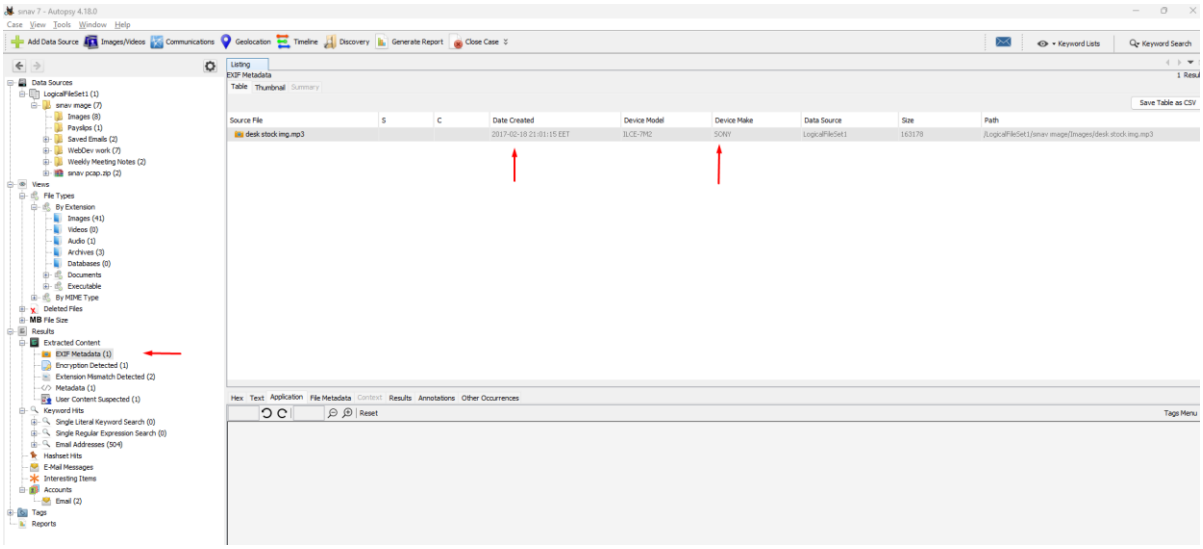




SORU 4: 2_Autopsy Case isimli klasör içerisinde case autopsy kullanarak açınız ve aşağıdaki soruları cevaplayınız (15 PUAN)

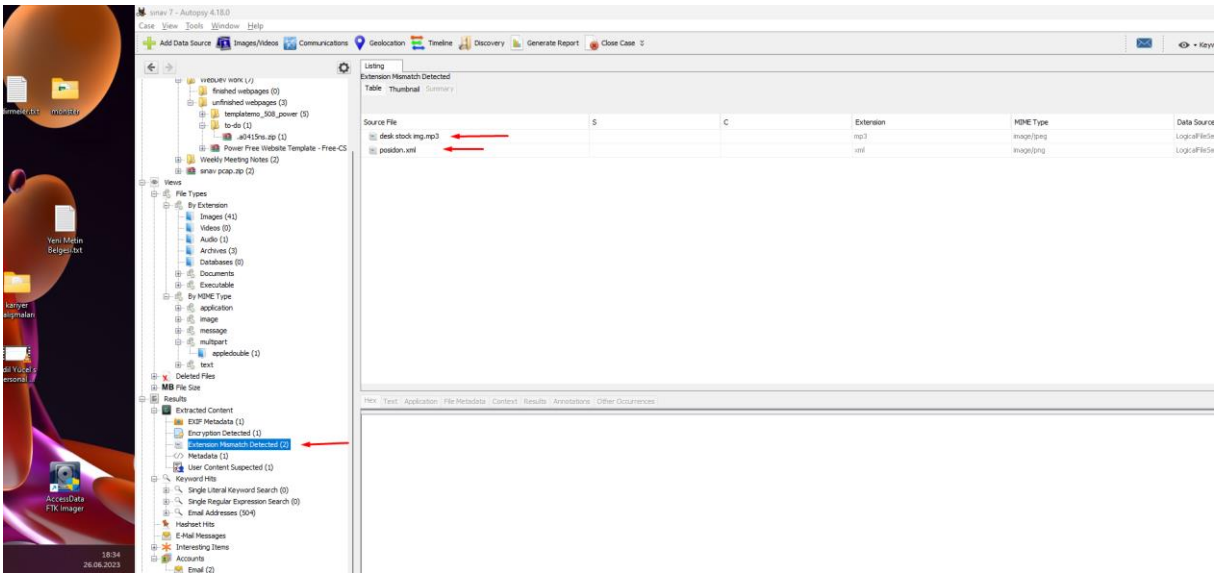
1. SONY marka bir makineden 2017-02-18 21:01:15 tarihinde çekilen fotoğraf dosyasının adı nedir. (İp ucu: Fotoğraflar sizi her zaman jpg, jpeg, gif vb. uzantıları ile beklemez)

DOSYA ADI: desk.stock.img.**mp3**



2. Uzantısı değiştirilmiş multimedya dosyasının adı nedir?

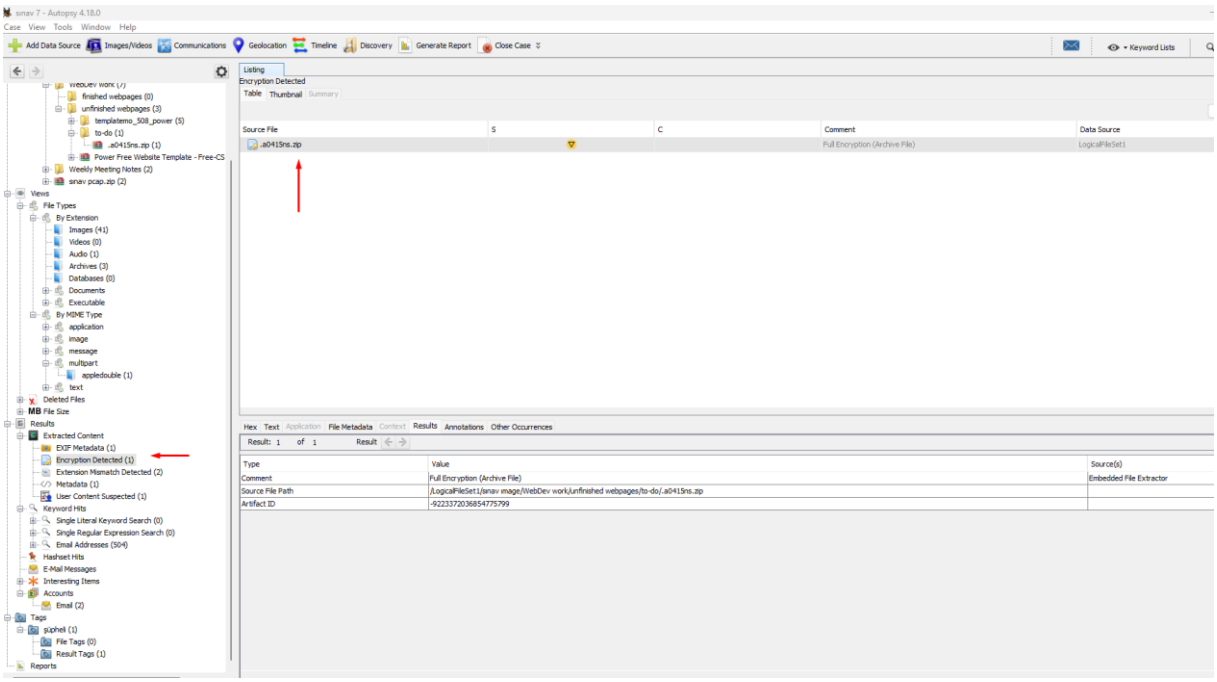
Multimedya dosyasının adı → desk.stock.img.**mp3**
Diğer uzantısı değiştirilmiş dosya → posidon**.xml**



3. Şifreli zip dosyasının adı nedir?

Zip dosyasını adı → .a0415ns.zip

Not: Zip dosyasının içindeki dosyanın adı ise “employeedump” ‘dır.



ÖMER KIZILGEDİK - Bilişim Güvenliği Mimarlığı Eğitimi - SoftİTo

Teşekkürler.