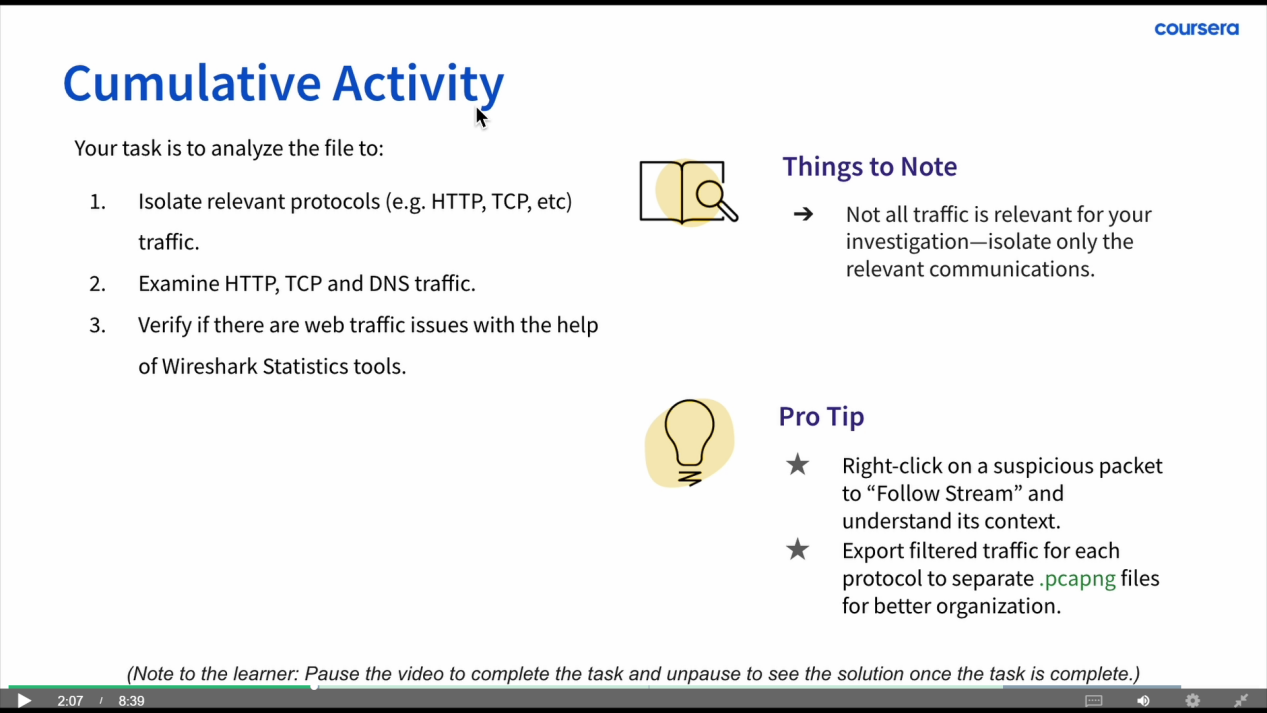
### Cumulative Activity Scenario

**Sən bir şəbəkə təhlükəsizliyi analizatorsusan. Son 48 saat ərzində şirkətin şəbəkə monitorinq sistemləri qeyri-adi fəaliyyətləri işarələyib.**

Təhlükəsizlik komandası şəbəkə problemlərini şübhəli bilib və sənə bu şübhəli dövrə aid olan bir .pcap faylı təqdim edib.



Ilk http-leri analiz edek:

**HTTP Trafikini Niyə Analiz Edirik?**

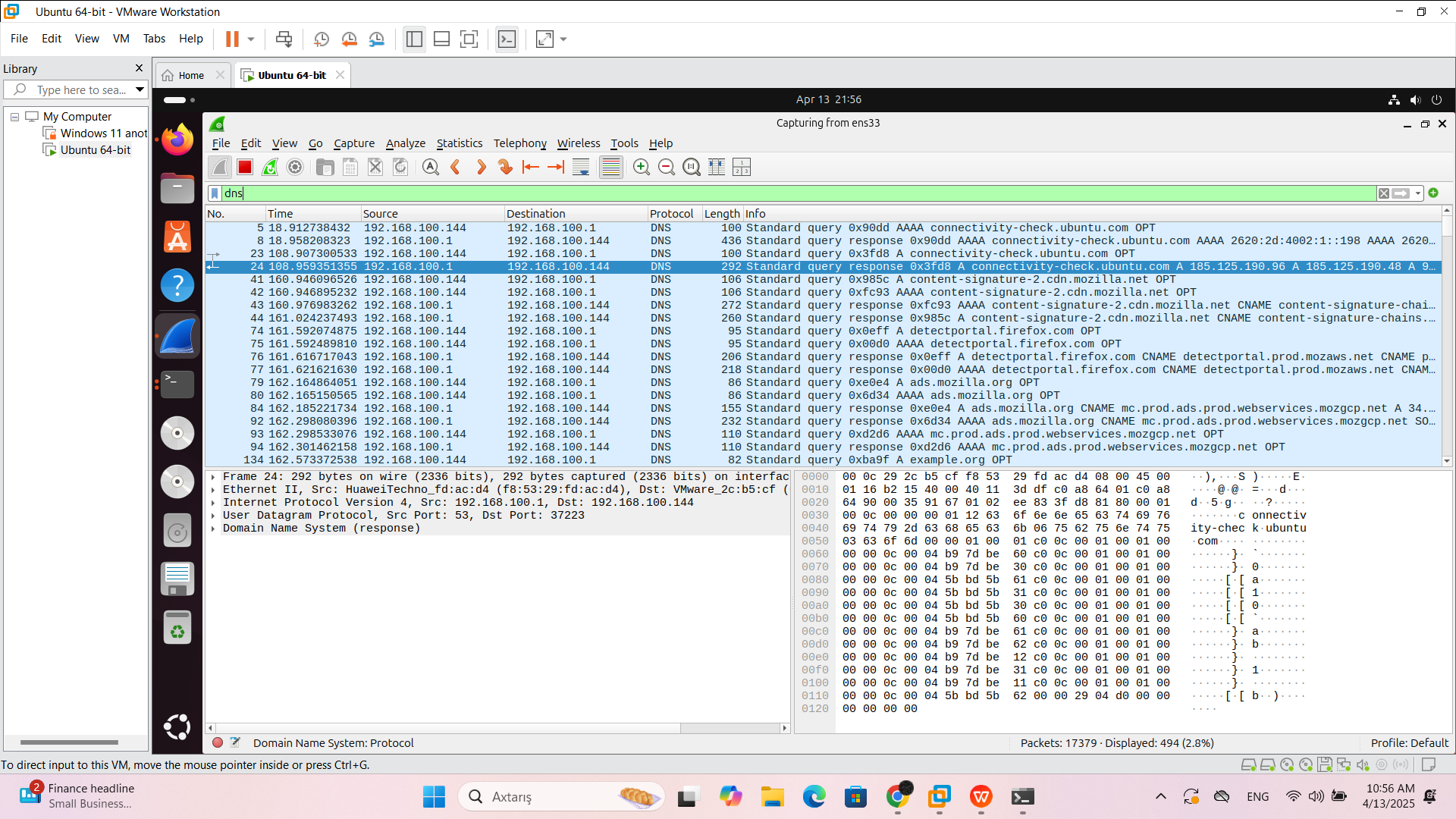
**Təhlükəsizlik:** HTTP trafikində **XSS**, **SQL injection** və **Cross-site scripting** kimi hücumları tapmaq mümkündür.

**Performans:** HTTP cavab zamanları və status kodları (200 OK, 404 Not Found, 503 Service Unavailable) trafikin düzgün işləyib-işləmədiyini göstərir.

**Məlumatın Bərpa Olunması:** HTTP vasitəsilə sistemin fəaliyyətində baş verən problemləri, məsələn, səhifələrin çox yavaş yüklənməsi və ya səhvlərin baş verməsi izlənilə bilər.

**Nəticə:** Wireshark-da **HTTP** trafiki açıq olduğu üçün, HTTP paketlərini izləmək asandır. **HTTPS** isə şifrələndiyi üçün, yalnız məlumatları açmaq üçün əlavə tədbirlər görülməlidir.

Daha sonra DNS traffikin izlemeliyik:



Filtr tətbiqi: dns filtrini tətbiq etməklə DNS sorğularını və cavablarını asanlıqla izləyə bilərsiniz.

Sorğuları analiz etmək: DNS sorğularının URL-lərini və cavablarını təhlil edərək şəbəkə fəaliyyətini izləyin.

Şəbəkə Problemlərini Aşkarlamaq: DNS cavablarının düzgünlüyünü yoxlayın, gecikmələri və ya səhvləri (404, 503 və s.) müşahidə edin.

Bu təhlillər DNS sorğularının düzgün işləməsini təmin etməyə və şəbəkə problemlərini müəyyən etməyə kömək edə bilər.

### ****Şəbəkə Hücumlarını Avtomatik Aşkarlamaq****

Şəbəkə üzərində MITM (Man in the Middle) və ya ARP Spoofing hücumlarını izləmək üçün Wireshark ilə şəbəkə trafiki yığıb, Python ilə analiz edərək avtomatik aşkarlama sistemi qurun.

#### ****Python Kitabxanaları****:

Wireshark tərəfindən toplanan məlumatları təhlil etmək üçün Python kitabxanası **PyShark** istifadə edə bilərsiniz. Bu kitabxana Wireshark-un .pcap fayllarını analiz etməyə imkan verir.

Quraşdırmaq üçün:

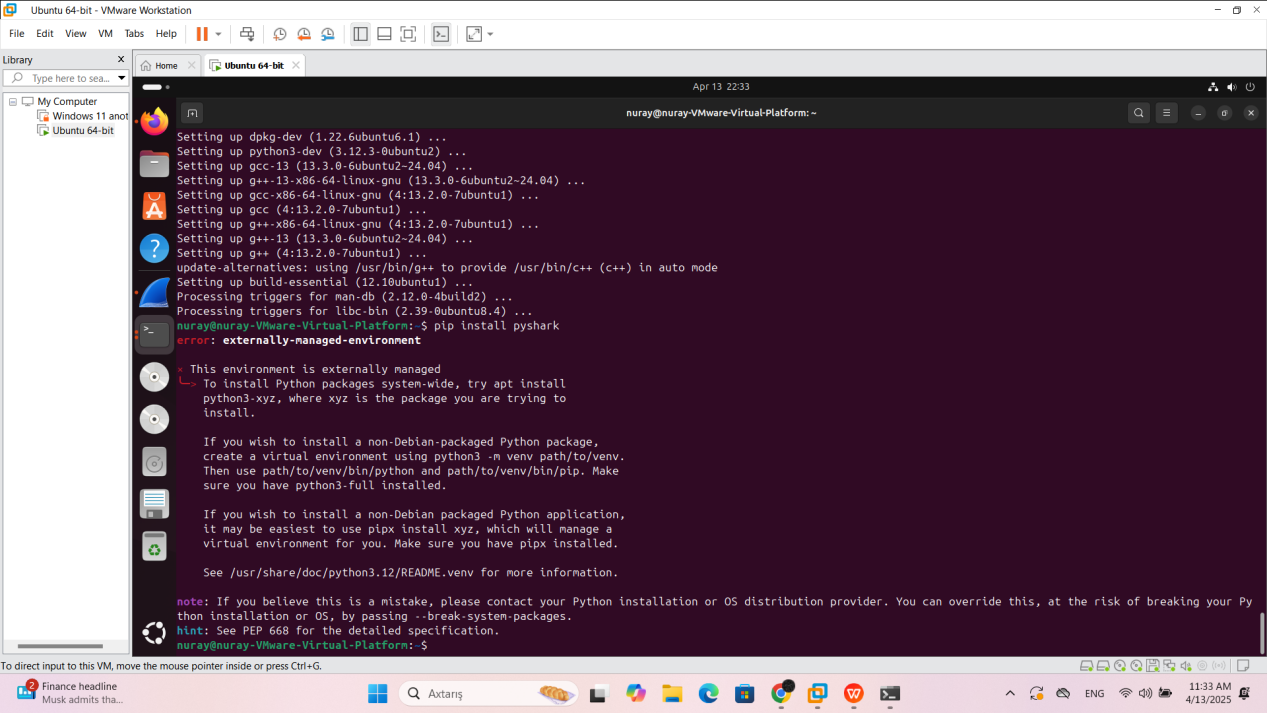
pip install pyshark

Bu cur errorla qarsilasa bilersiniz:

Eger qarsilassaniz sudo apt install python3-pip ile pythonun pip konfiqurasiyasini edin.

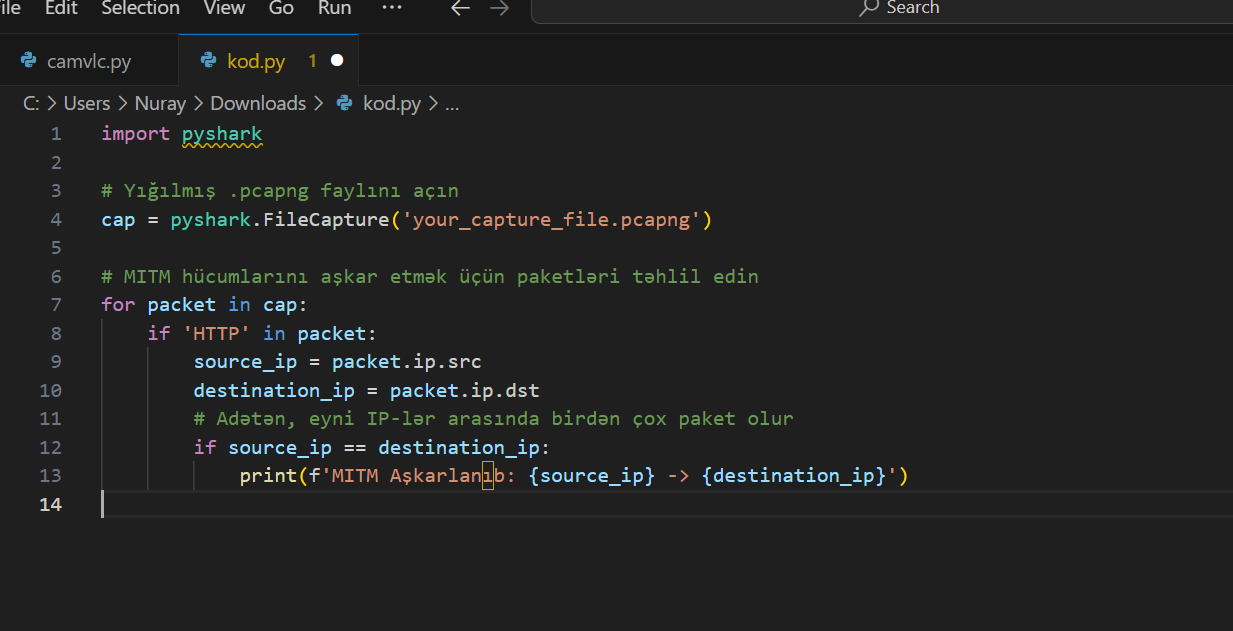


Novbeti ve meshur error python enviromentin aktivlesdirmeliyik



#### ****MITM Aşkarlanması:****

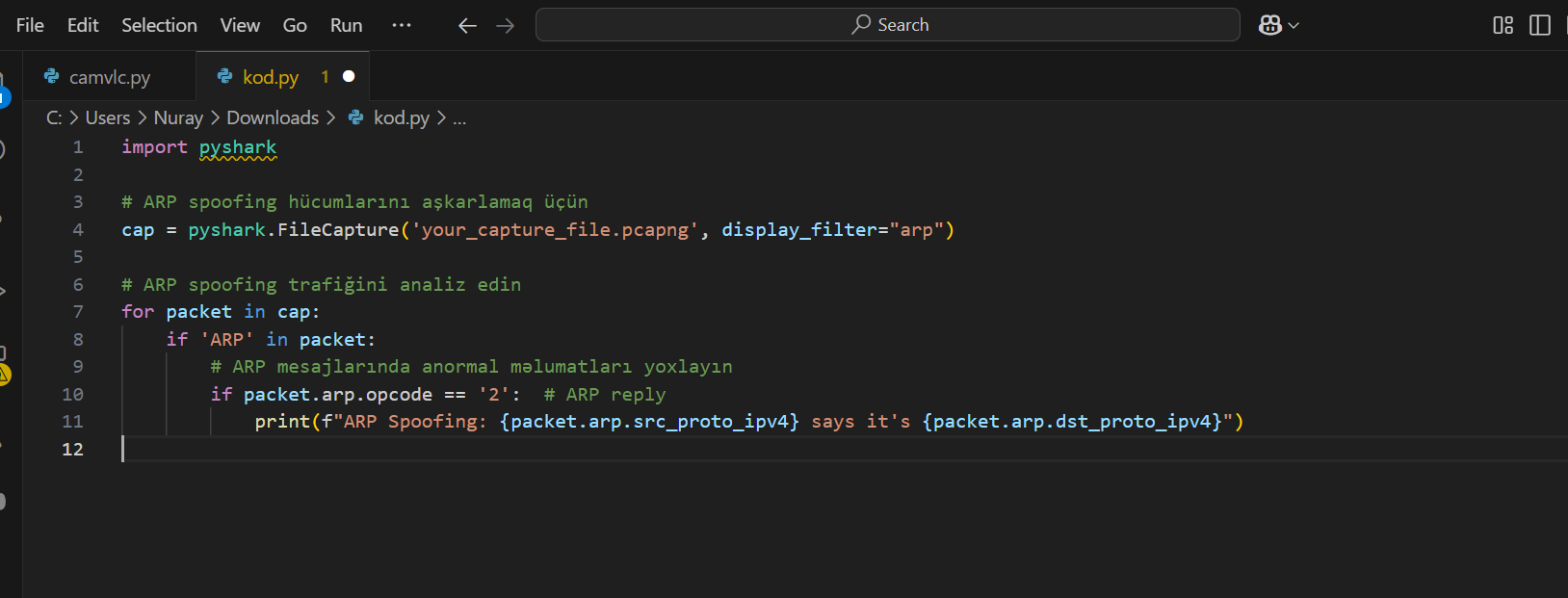
MITM hücumlarını aşkar etmək üçün TCP trafiğində anormal bağlantıları izləyin. Hücum zamanı server və müştəri arasında əlaqə yerinə üçüncü tərəf (hücum edən şəxs) müdaxilə edir.



Burada, **source\_ip** və **destination\_ip** təkrarlanması yoxlanılır. Əgər eyni IP-lərdən gələn paketlər varsa, bu, MITM hücumunun əlaməti ola bilər.

#### ****ARP Spoofing Aşkarlanması:****

ARP Spoofing hücumları zamanı şəbəkədəki cihazlar yanlış ARP (Address Resolution Protocol) məlumatları alır, bu da digər cihazların trafikinə nəzarət etmək üçün istifadə edilir.



Burada, ARP reply mesajları təhlil edilir və **ARP Spoofing** aşkarlanır. Bu zaman cihazların ARP cədvəlində olan məlumatlar zərərli şəkildə dəyişdirilir.