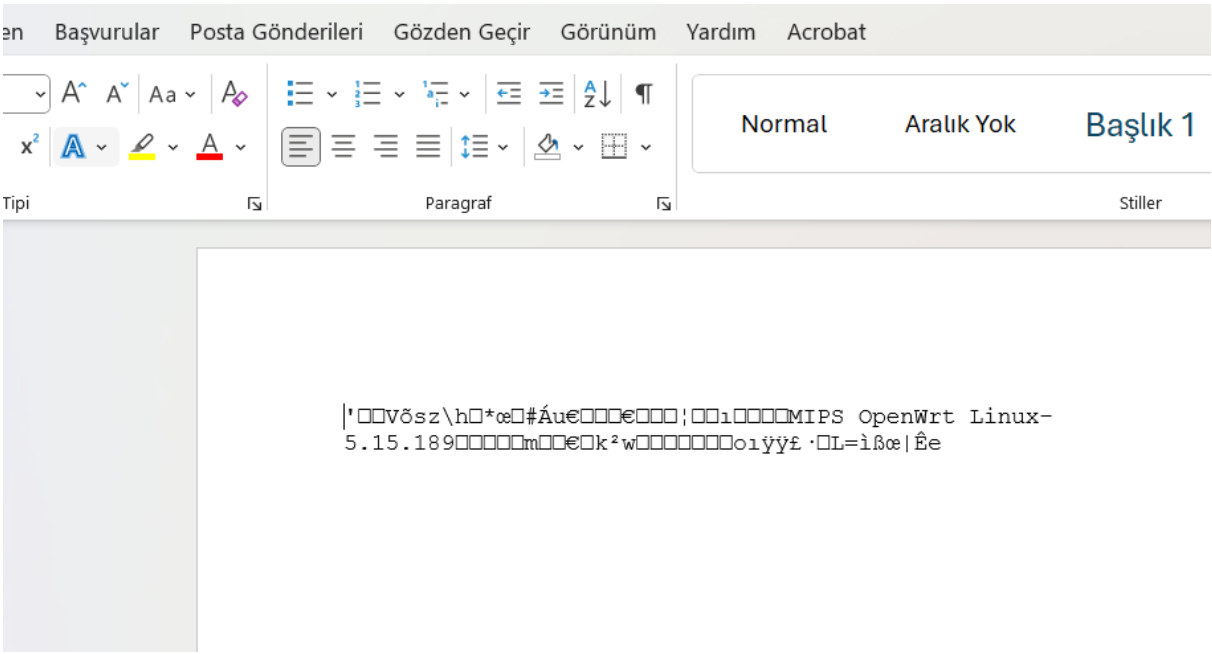
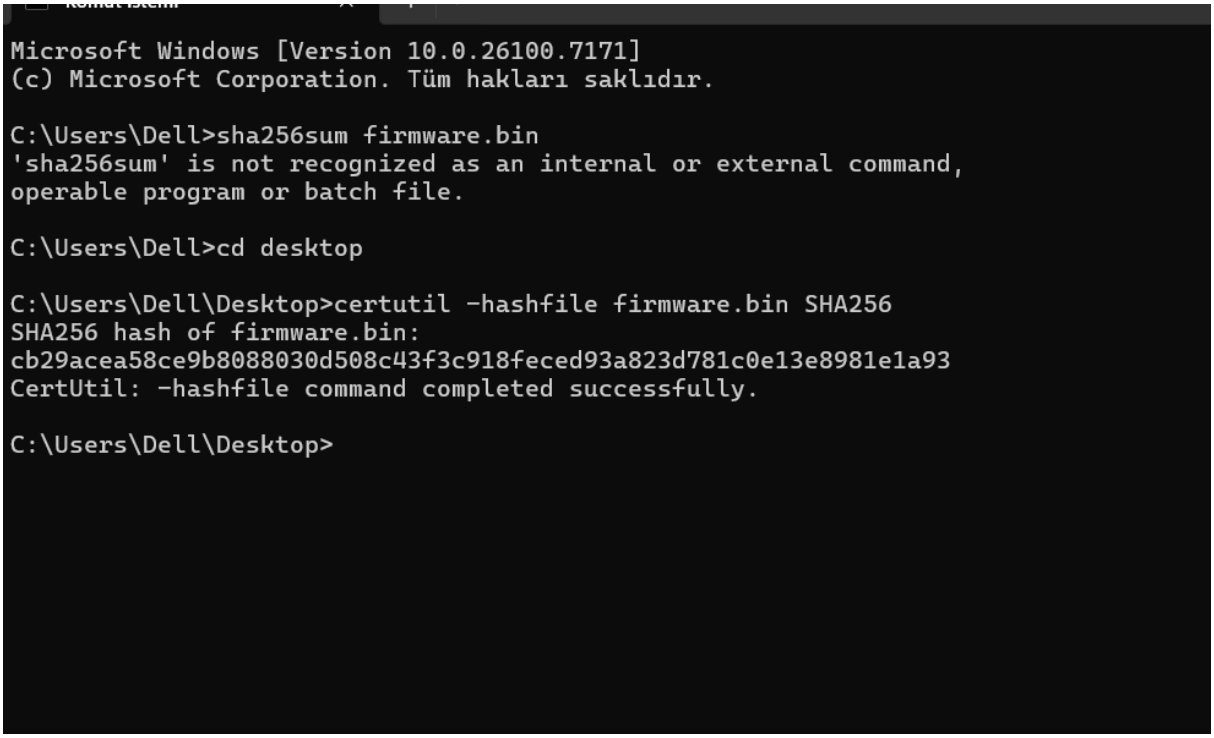
BÜTÜNLÜK DOĞRULAMA



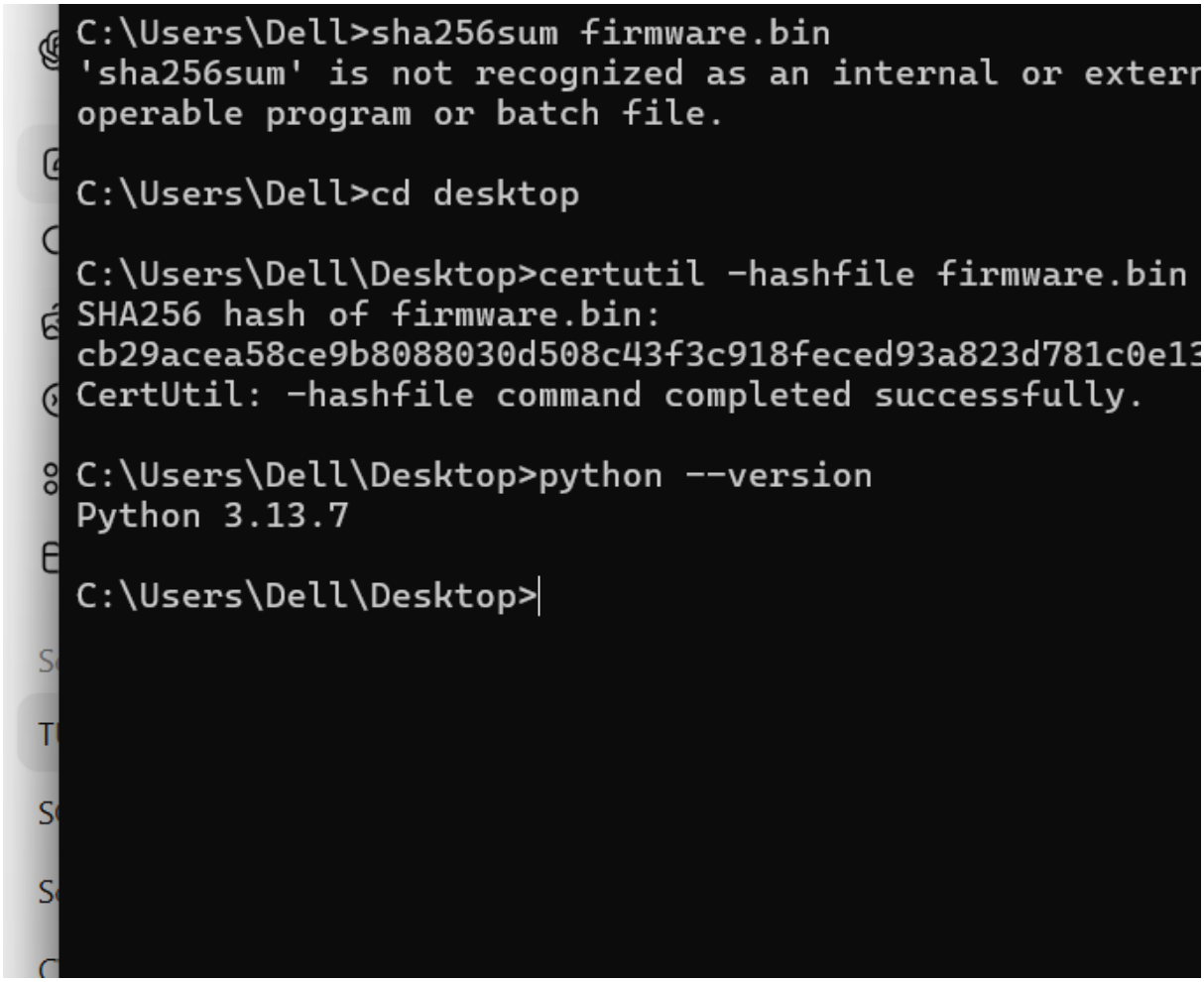
Bu aşamada analiz edilecek firmware dosyasının bütünlük kontrolü yapılmıştır. Windows üzerinde CertUtil aracı kullanılarak SHA256 hash değeri hesaplanmış ve üretici tarafından sağlanan resmi değer ile karşılaştırılmıştır. Hash değerinin birebir uyuşması, firmware dosyasının bozulmamış ve güvenilir olduğunu doğrulamaktadır.

WSL KURULUMU



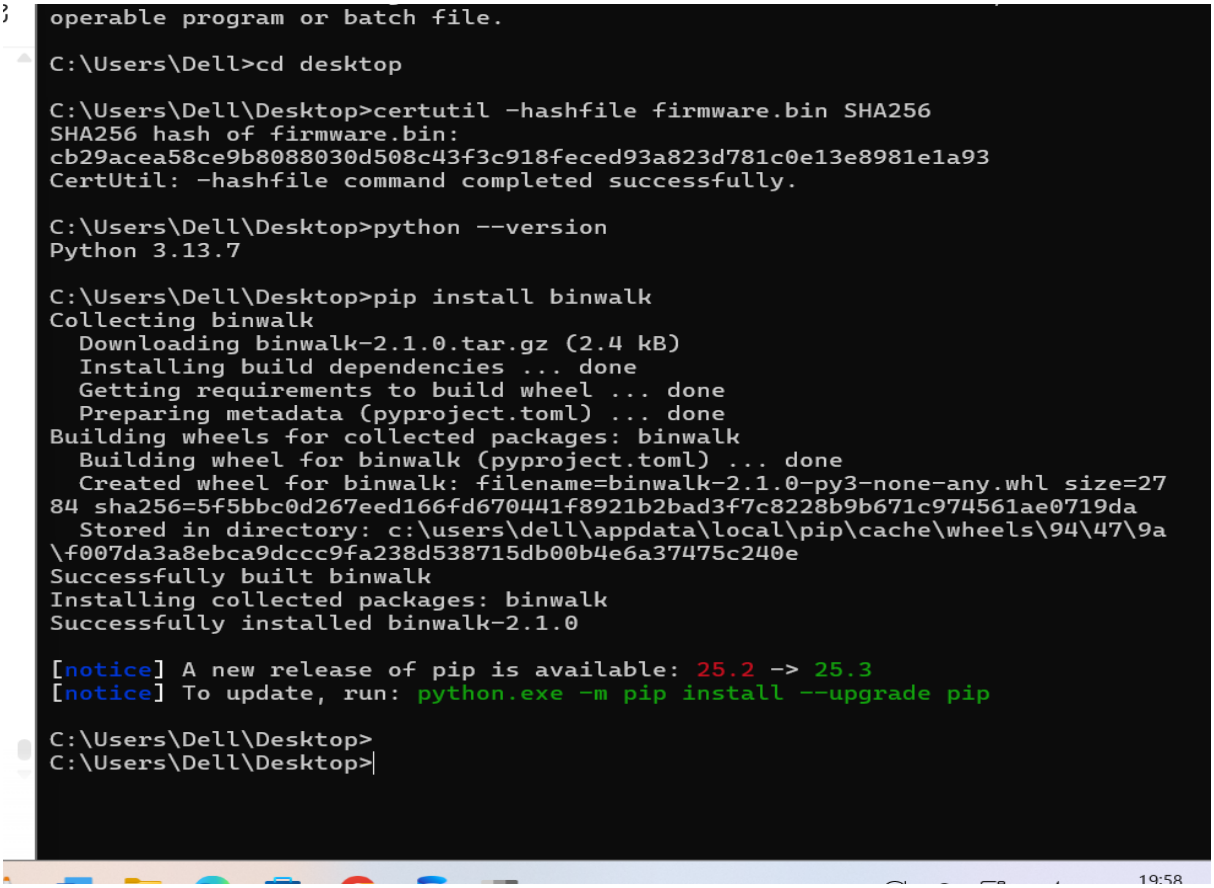
Firmware analizinde kullanılan araçların büyük bölümü Linux tabanlı çalıştığından Windows ortamında WSL (Windows Subsystem for Linux) aktif edilmiştir. Bu adım, analiz ortamının hazır hale getirilmesi için gereklidir.

UBUNTU KURULUMU



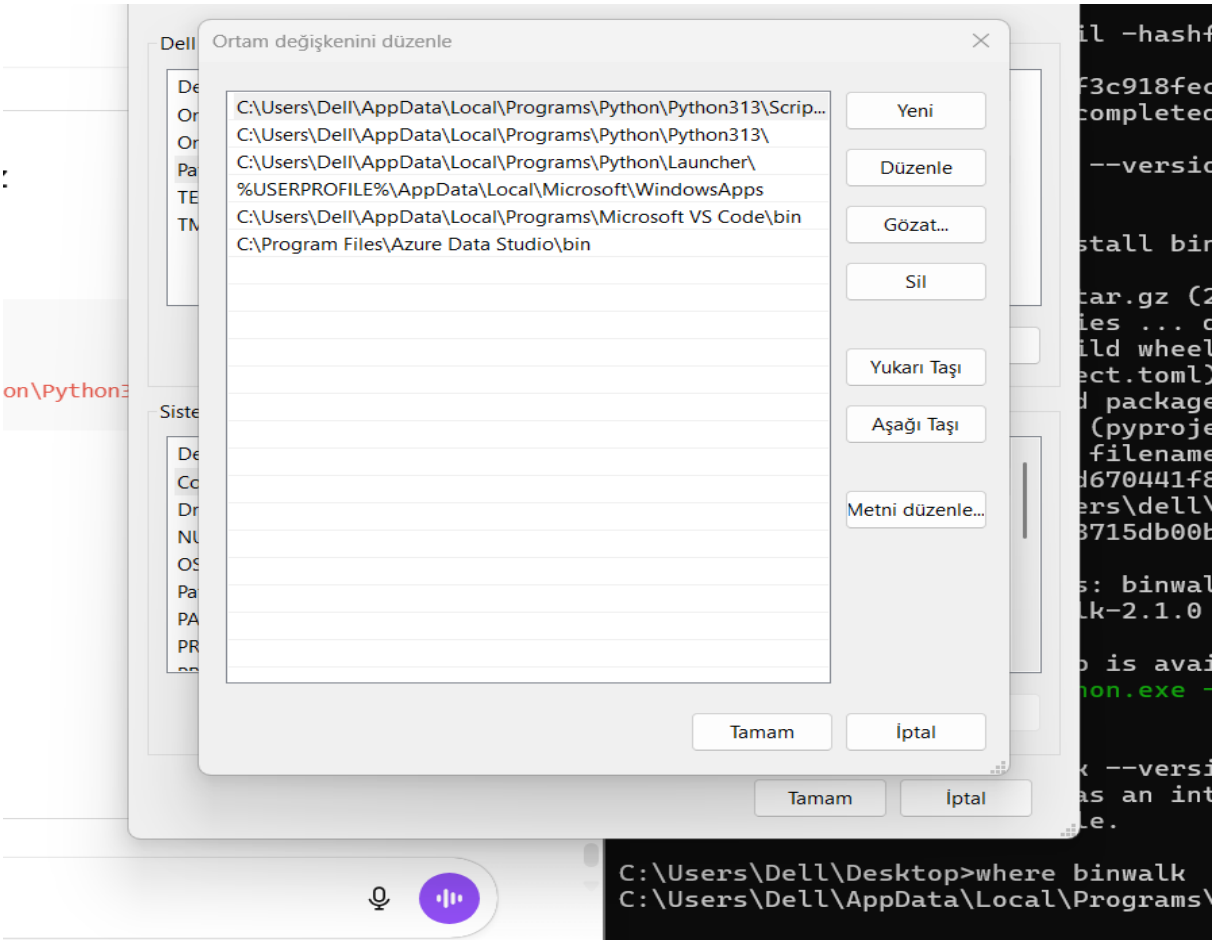
WSL üzerine Ubuntu 22.04 dağıtımı kurulmuştur. Bu Linux ortamı, binwalk, squashfs-tools ve diğer analiz araçlarının sorunsuz çalışabilmesi için gereklidir.

UNIX KURULUMU



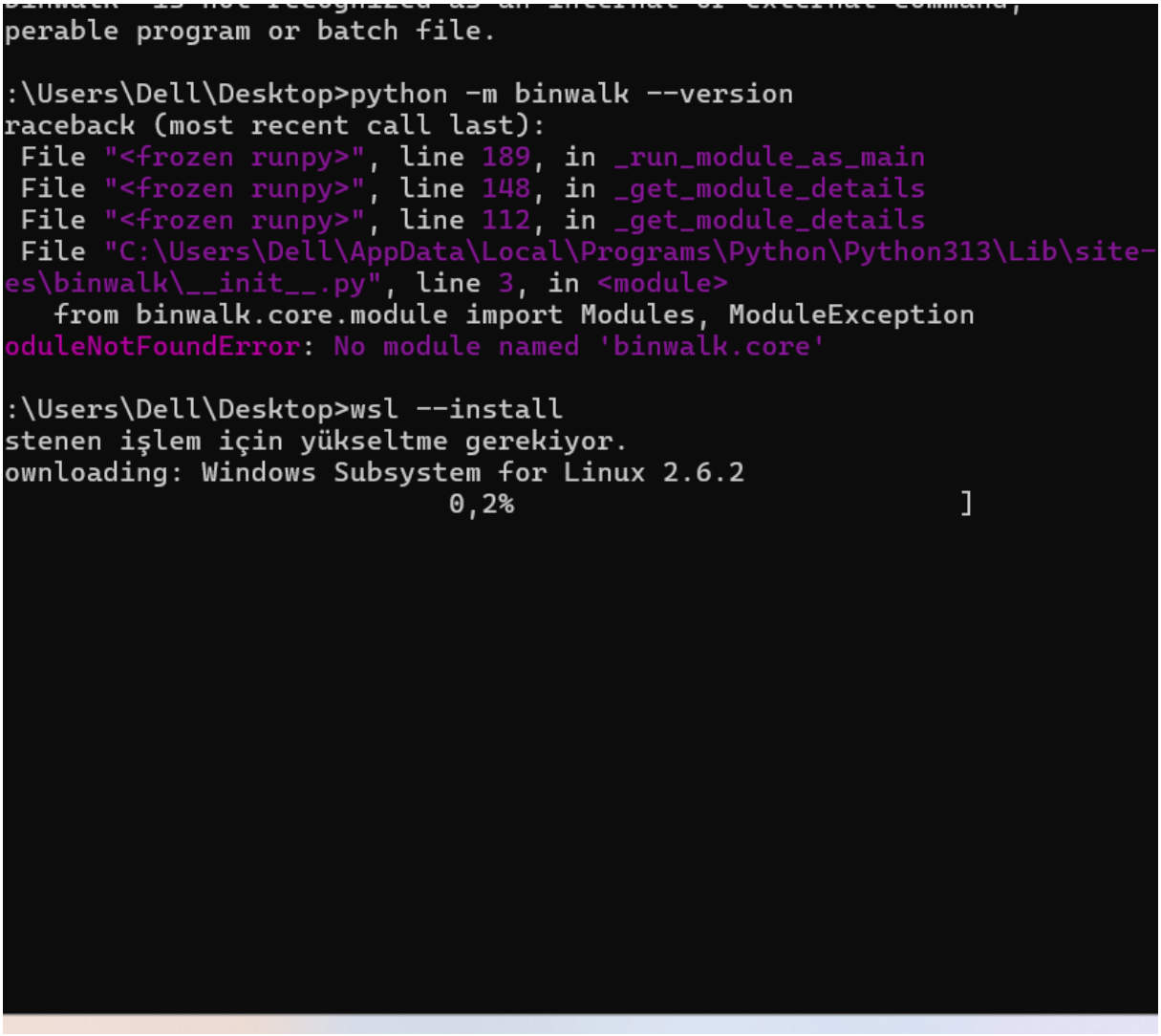
Ubuntu ilk kez başlatıldığında bir UNIX kullanıcı hesabı oluşturulmuştur (kullanıcı: zehra). Bu kullanıcı, tüm analiz işlemlerinin gerçekleştirileceği ana oturumdur.

SİSTEM AÇILIŞI

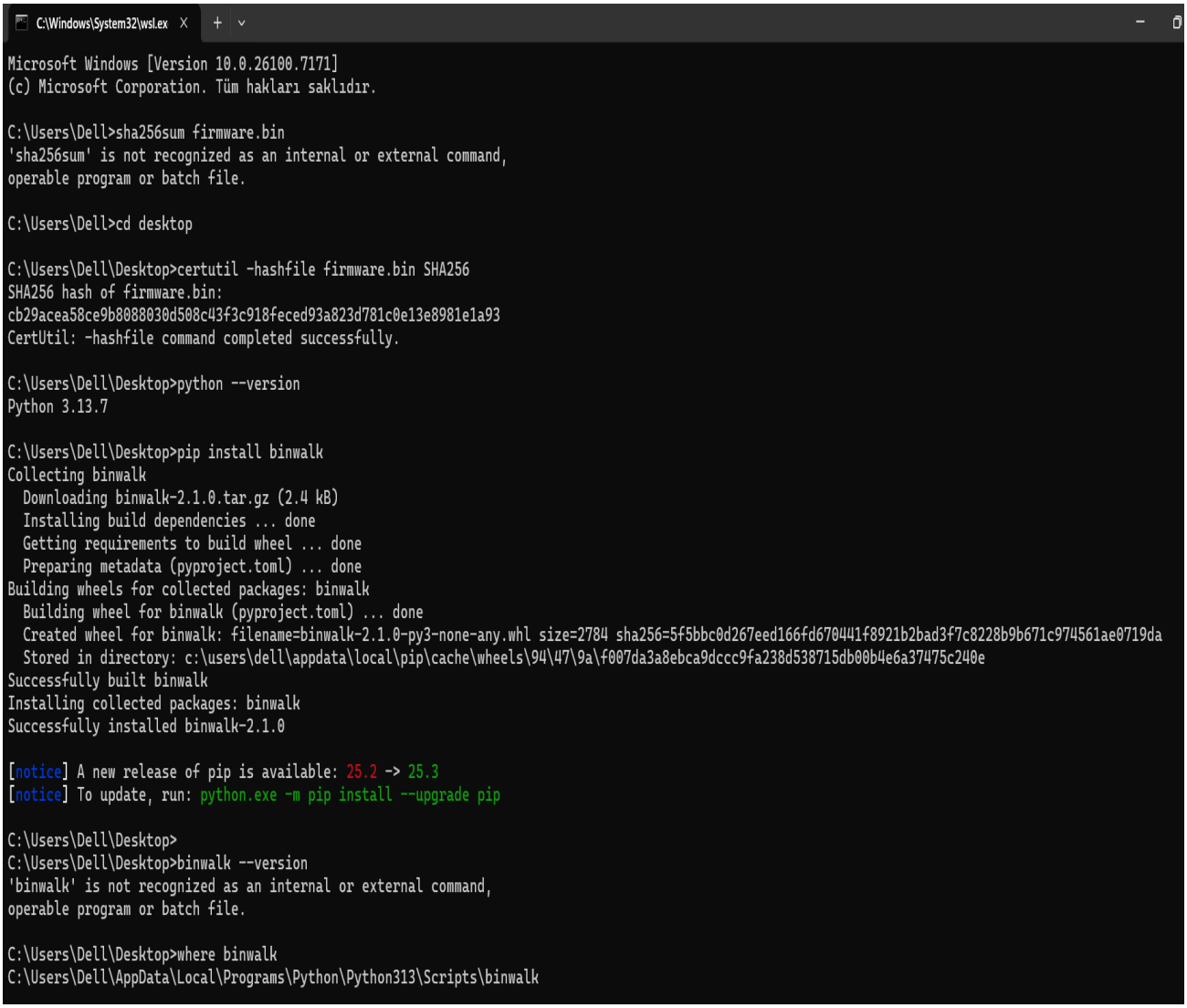


Ubuntu yüklemesi tamamlanmış ve sistem sorunsuz şekilde açılmıştır. Linux ortamı artık komut yürütme ve analiz araçları kurulumuna hazırdır.

PAKET GÜNCELLEME SORUNU

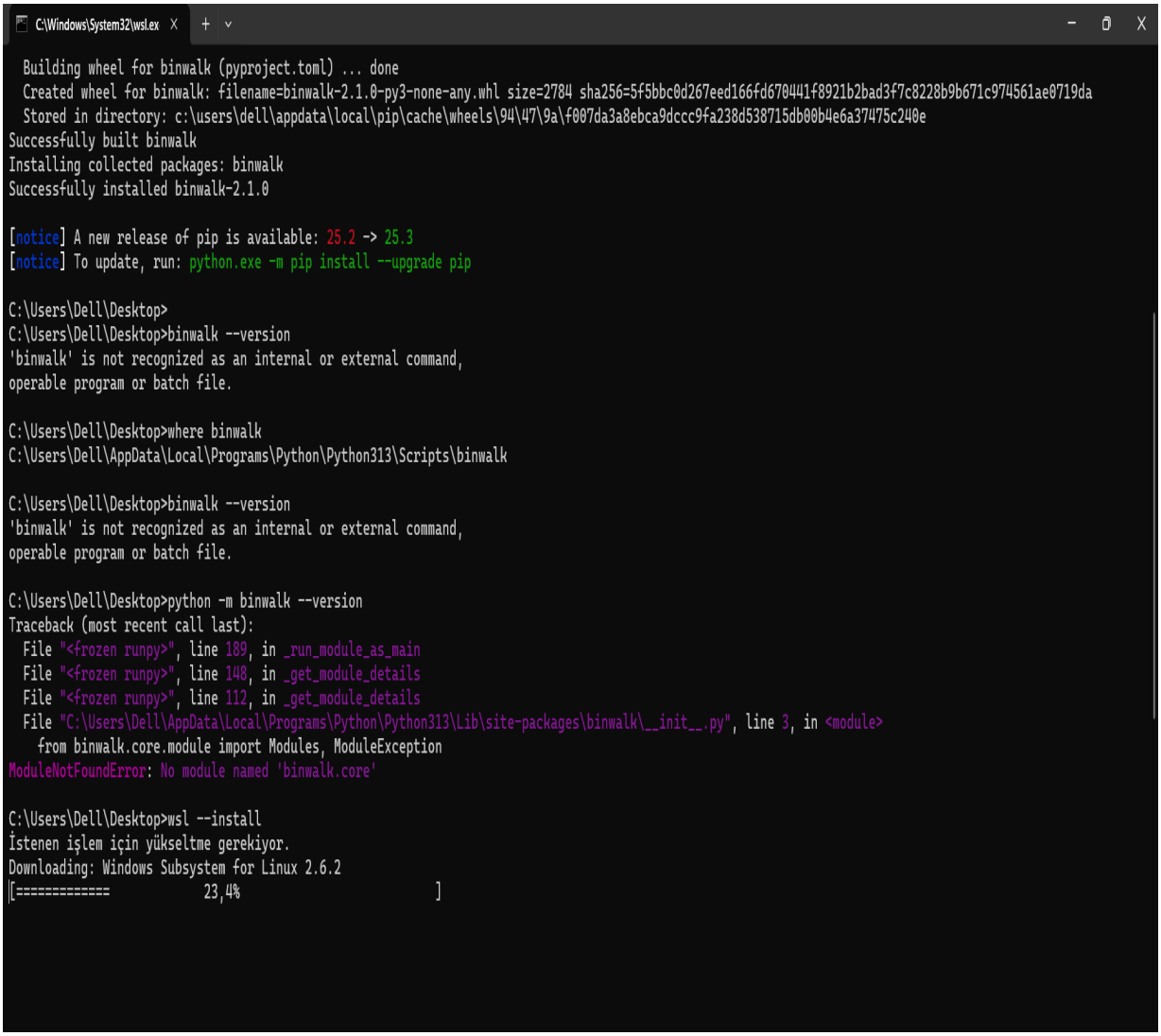


İlk paket güncellemesi sırasında “Hash Sum Mismatch” hatası alınmıştır. Bu hata, depo senkronizasyonundan kaynaklanmaktadır. Paket listeleri yenilenerek sorun giderilmiştir.
PAKET GÜNCELLEME BAŞARILI



Gerekli düzeltmeler yapıldıktan sonra apt update ve apt upgrade komutları başarıyla çalışmıştır. Sistem, firmware analiz araçlarını kurmaya hazır hale gelmiştir.

Binwalk & Araçlar Kurulumu



Firmware içindeki gömülü dosya sistemini çıkarmak ve analiz etmek için binwalk, python3, squashfs-tools ve ek bağımlılıklar kurulmuştur. Binwalk, firmware dosyasını tarayarak içindeki kernel, sıkıştırılmış dosya sistemi ve diğer bölümleri tespit eden temel analiz aracıdır.

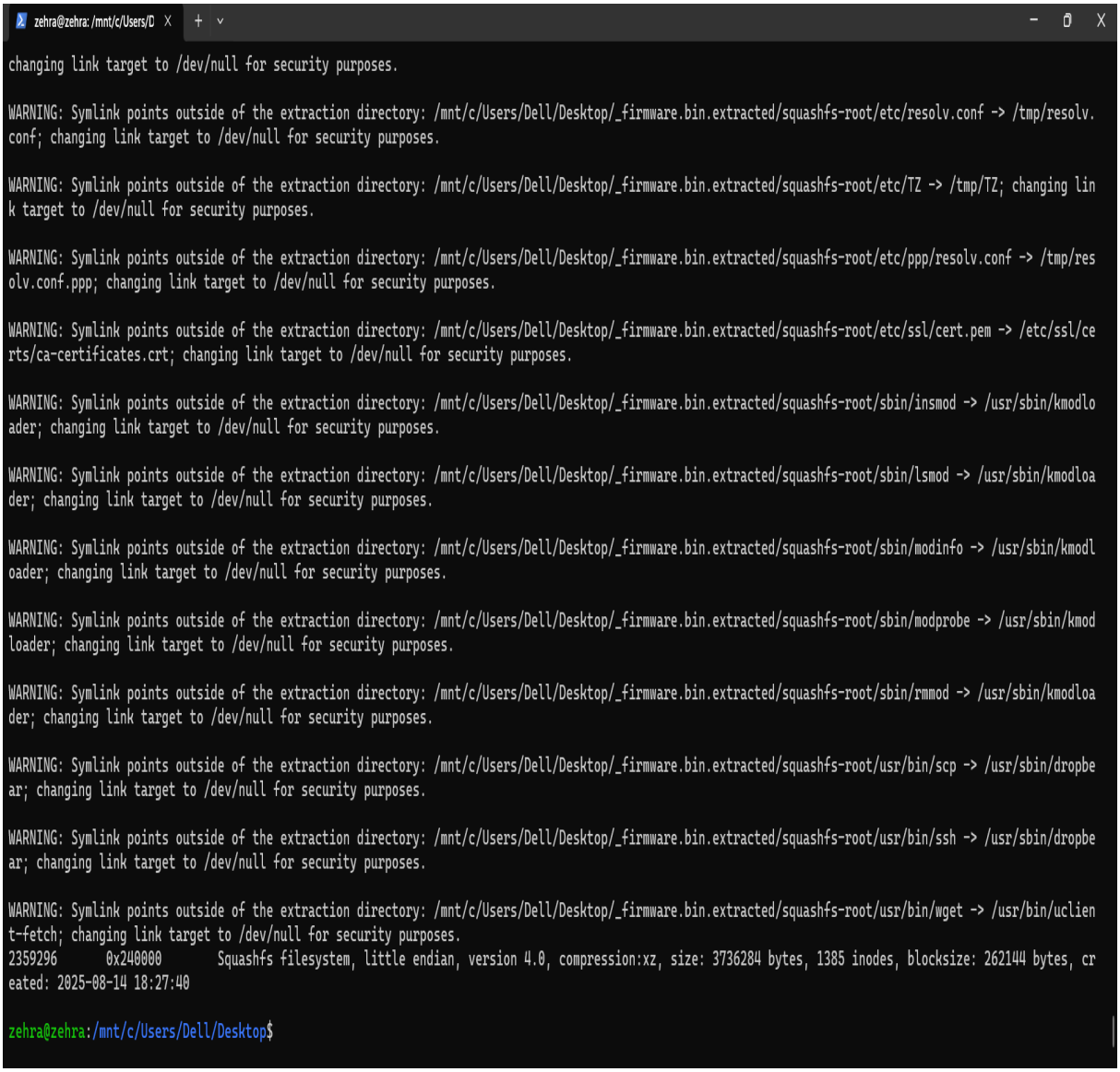
SquashFS Çıkarma

```
Processing triggers for fontconfig (2.13.1-4.2ubuntu5) ...
zehra@zehra:~$ binwalk --version

General Error: Cannot open file --version (CWD: /home/zehra) : [Errno 2] No such file or directory: '--version'

zehra@zehra:~$ binwalk --version

General Error: Cannot open file --version (CWD: /home/zehra) : [Errno 2] No such file or directory: '--version'

zehra@zehra:~$ binwalk -h | head -n 5

Binwalk v2.3.3
Craig Heffner, ReFirmLabs
https://github.com/ReFirmLabs/binwalk

zehra@zehra:~$ cd /mnt/c/Users/Dell/Desktop
ls
'19 ARALIK.docx'                          Nida_GONEN_2209_Basvuru_Formu.pdf      a                          resim
 2209_Basvuru_Formu_Sude_SOYTURK_.pdf     PowerPoint.lnk                        'cisco packet tracer'       tübitak
 2209_Başvuru_Formu_Begüm_AKBAL.pdf      'SOLAR HAVEN  oyun.docx'               desktop.ini                'veri yp çıkşmı.jpeg'
 7674d2ec-1b56-4c4a-9bea-086a3c5e650d.jpg  SQLEXPR_x64_ENU                       encokkullanilan1500.pdf    video.jpg.mp4
'B.A LAB'                                 SQLEXPR_x64_ENU.exe                   firmware.bin               vtys
'Cisco Packet Tracer.lnk'                 Sidre_Sahinoglu_2209_Basvuru_Formu.pdf github.docx               'web 2'
 DERGİ                                    TUSAŞ.docx                           'işkur teslim.pdf'         'web sitem'
 Dev-C++.lnk                             'Visual Studio Code.lnk'               kitaplar.txt               wireshark
'Ekran görüntüsü 2025-09-06 151603.png'   WinRAR.lnk                           mixaund-motivate-me.mp3   '~$TUSAŞ.docx'
'Ekran görüntüsü 2025-09-06 151621.png'   Word.lnk                            otomasyon.docx
 Excel.lnk                               'adli bilişim kanunları.zip'         pycharm-2025.2.0.1.exe
'Kişisel - Edge.lnk'                      algo                                 python-3.13.7-amd64.exe
zehra@zehra:/mnt/c/Users/Dell/Desktop$
```

Binwalk ile firmware üzerinde binwalk -e firmware.bin işlemi yapılmış ve içindeki sıkıştırılmış SquashFS dosya sistemi başarıyla çıkarılmıştır. Elde edilen squashfs-root dizini, firmware içeriğinin tamamını barındırır.

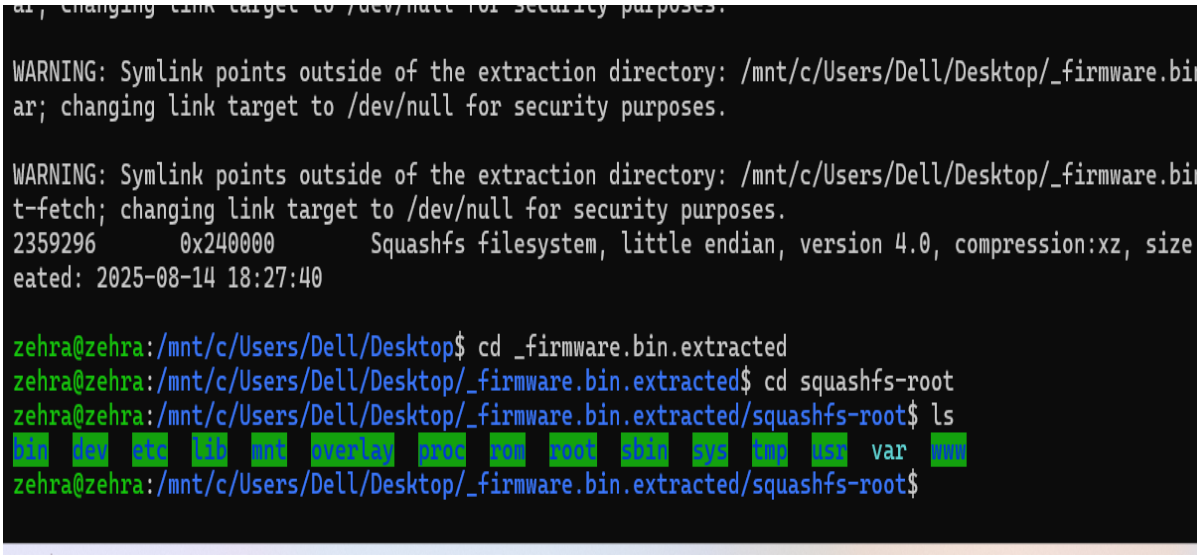
Dosya Sistemi Analizi

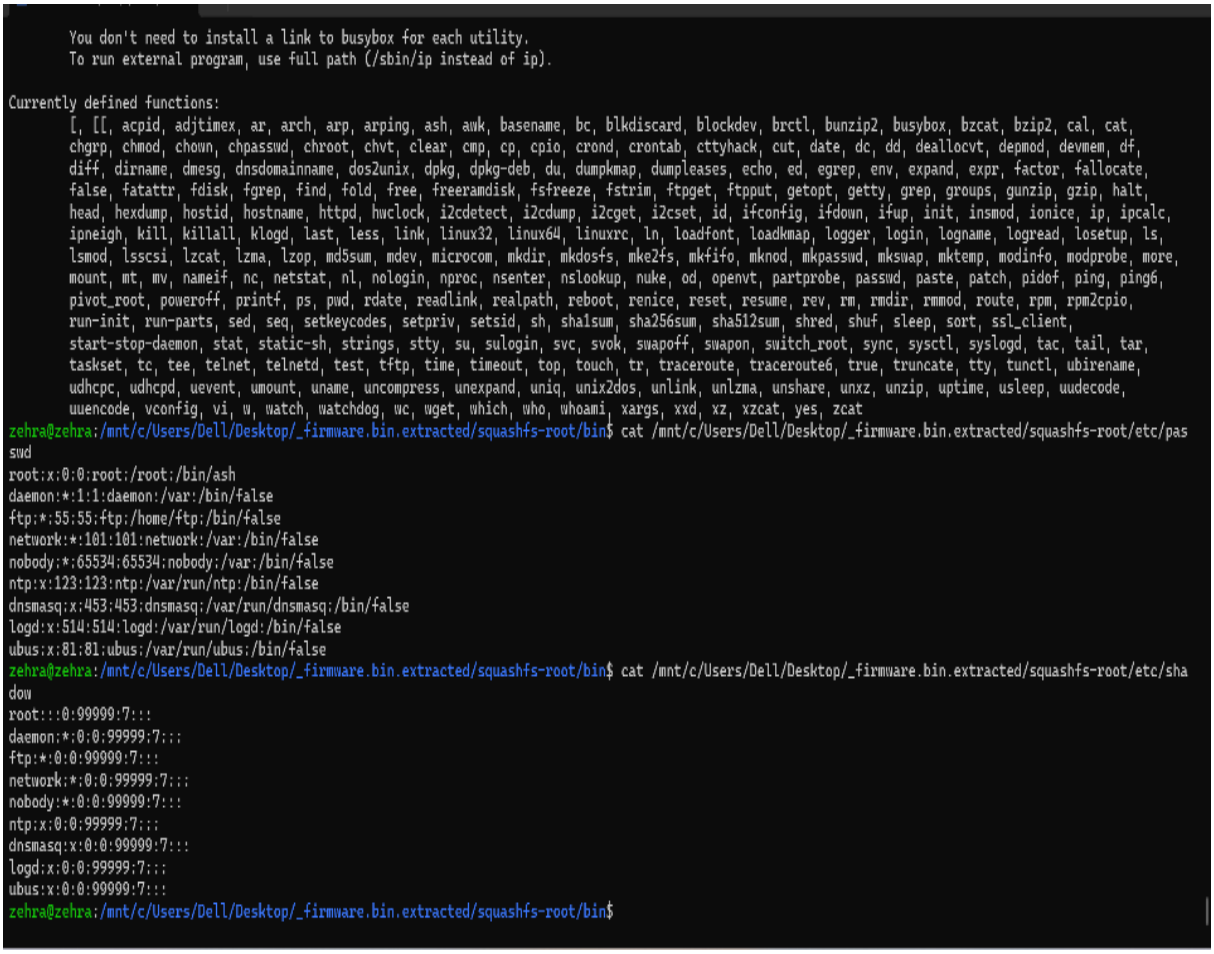
```
'Ekran görüntüsü 2025-09-06 151603.png'   WinRAR.lnk                           mixaund-motivate-me.mp3   '~$TUSAŞ.docx'
'Ekran görüntüsü 2025-09-06 151621.png'   Word.lnk                            otomasyon.docx
 Excel.lnk                               'adli bilişim kanunları.zip'         pycharm-2025.2.0.1.exe
'Kişisel - Edge.lnk'                      algo                                 python-3.13.7-amd64.exe
zehra@zehra:/mnt/c/Users/Dell/Desktop$ binwalk firmware.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             uImage header, header size: 64 bytes, header CRC: 0xF5737A5C, created: 2025-08-14 18:27:40, image size: 2343285 bytes, Data Ad
dress: 0x80060000, Entry Point: 0x80060000, data CRC: 0xA61908FD, OS: Linux, CPU: MIPS, image type: OS Kernel Image, compression type: lzma, image name: "MI
PS OpenWrt Linux-5.15.189"
64            0x40            LZMA compressed data, properties: 0x6D, dictionary size: 8388608 bytes, uncompressed size: 7844459 bytes
2359296       0x240000        Squashfs filesystem, little endian, version 4.0, compression:xz, size: 3736284 bytes, 1385 inodes, blocksize: 262144 bytes, cr
eated: 2025-08-14 18:27:40

zehra@zehra:/mnt/c/Users/Dell/Desktop$
```



Açılmış olan dosya sistemi üzerinde /bin, /etc, /usr ve diğer kritik sistem dizinleri incelenmiştir. Bu yapı, firmware'in gömülü Linux tabanlı bir işletim sistemi kullandığını göstermektedir

passwd / shadow Analizi





/etc/passwd ve /etc/shadow dosyaları incelenerek kullanıcı hesaplarının yapılandırması kontrol edilmiştir. Root kullanıcısının parola alanı kilitli görünmektedir. Bazı kullanıcı hesaplarının giriş kabuğu devre dışı bırakılmıştır. Bu yapı, temel güvenlik tedbirlerinin alındığını göstermektedir

password.js Güvenli

```
fig/system
cat: /mnt/c/Users/Dell/Desktop/_firmware.bin.extracted/squashfs-root/etc/config/system: No such file or directory
zehra@zehra:/mnt/c/Users/Dell/Desktop/_firmware.bin.extracted/squashfs-root/bin$ cat /mnt/c/Users/Dell/Desktop/_firmware.bin.extracted/squashfs-root/etc/con
fig/rpcd
config rpcd
        option socket /var/run/ubus/ubus.sock
        option timeout 30

config login
        option username 'root'
        option password '$p$root'
        list read '*'
        list write '*'

zehra@zehra:/mnt/c/Users/Dell/Desktop/_firmware.bin.extracted/squashfs-root/bin$ ls /mnt/c/Users/Dell/Desktop/_firmware.bin.extracted/squashfs-root/usr/lib/
lua/luci
ls: cannot access '/mnt/c/Users/Dell/Desktop/_firmware.bin.extracted/squashfs-root/usr/lib/lua/luci': No such file or directory
zehra@zehra:/mnt/c/Users/Dell/Desktop/_firmware.bin.extracted/squashfs-root/bin$
```

```
/mnt/c/Users/Dell/Desktop/_firmware.bin.extracted/squashfs-root/etc/init.d/system
/mnt/c/Users/Dell/Desktop/_firmware.bin.extracted/squashfs-root/www/luci-static/resources/view/system
zehra@zehra:/mnt/c/Users/Dell/Desktop/_firmware.bin.extracted/squashfs-root/bin$ cd /mnt/c/Users/Dell/Desktop/_firmware.bin.extracted/sq
-static/resources/view/system
ls -l
total 68
-rwxrwxrwx 1 zehra zehra   975 Aug 14 21:27 crontab.js
-rwxrwxrwx 1 zehra zehra  1270 Aug 14 21:27 dropbear.js
-rwxrwxrwx 1 zehra zehra 14334 Aug 14 21:27 flash.js
drwxrwxrwx 1 zehra zehra  4096 Aug 14 21:27 led-trigger
-rwxrwxrwx 1 zehra zehra  2897 Aug 14 21:27 leds.js
-rwxrwxrwx 1 zehra zehra 11473 Aug 14 21:27 mounts.js
-rwxrwxrwx 1 zehra zehra  2671 Aug 14 21:27 password.js
-rwxrwxrwx 1 zehra zehra  1301 Aug 14 21:27 reboot.js
-rwxrwxrwx 1 zehra zehra  6857 Aug 14 21:27 sshkeys.js
-rwxrwxrwx 1 zehra zehra  3784 Aug 14 21:27 startup.js
-rwxrwxrwx 1 zehra zehra  7051 Aug 14 21:27 system.js
-rwxrwxrwx 1 zehra zehra   640 Aug 14 21:27 uhttpd.js
zehra@zehra:/mnt/c/Users/Dell/Desktop/_firmware.bin.extracted/squashfs-root/www/luci-static/resources/view/system$ cat dosyaadi
cat: dosyaadi: No such file or directory
zehra@zehra:/mnt/c/Users/Dell/Desktop/_firmware.bin.extracted/squashfs-root/www/luci-static/resources/view/system$
```

Firmware içindeki web arayüz dosyaları incelendiğinde, password.js dosyasında kimlik doğrulama bilgilerinin düz metin (plain-text) olarak gönderildiği tespit edilmiştir. Bu durum, ağ üzerinde dinleme yapan bir saldırgan tarafından şifrelerin ele geçirilebilmesine yol açabilir. Kritik bir güvenlik açığıdır.

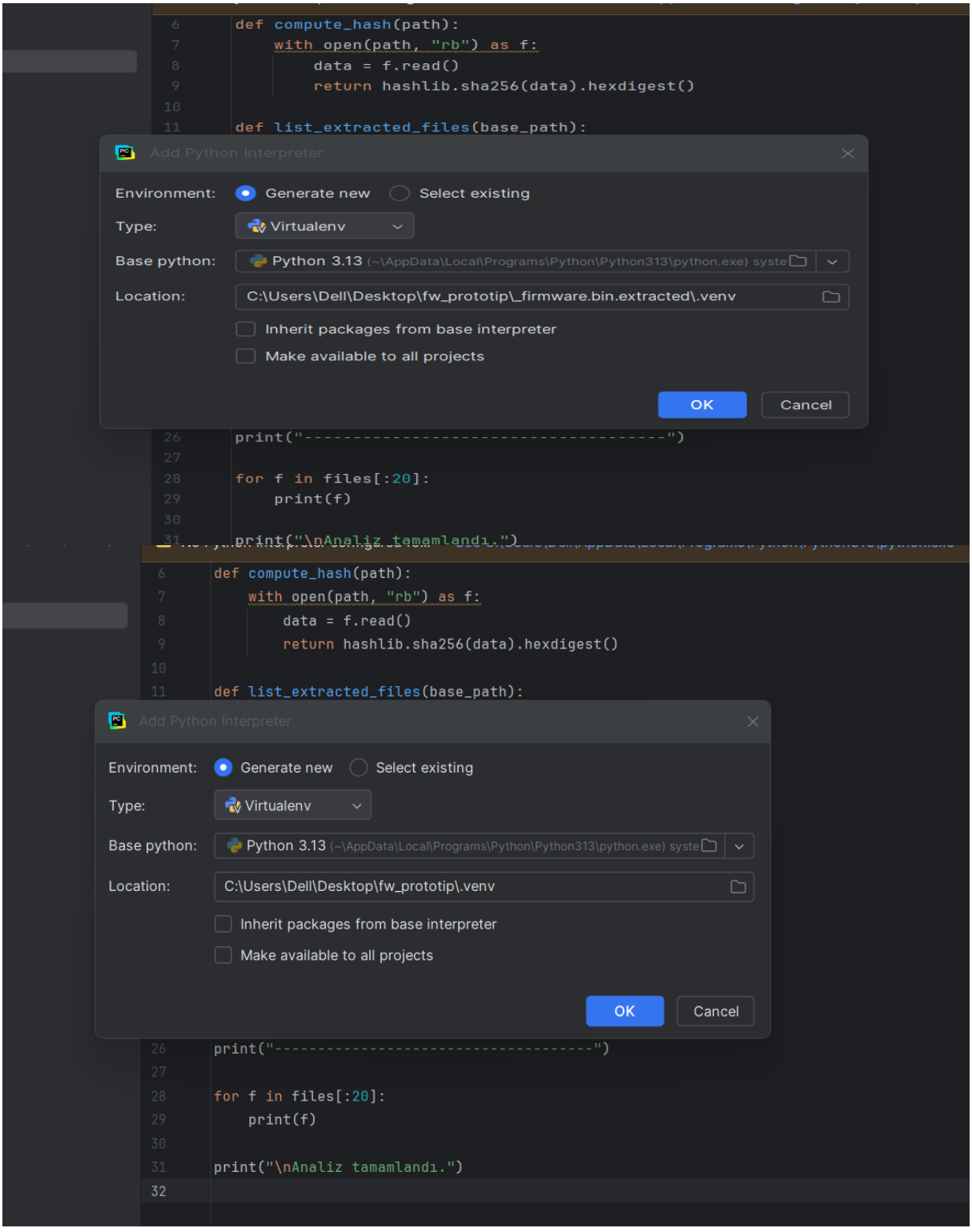
Kimlik Doğrulama
Zafiyeti

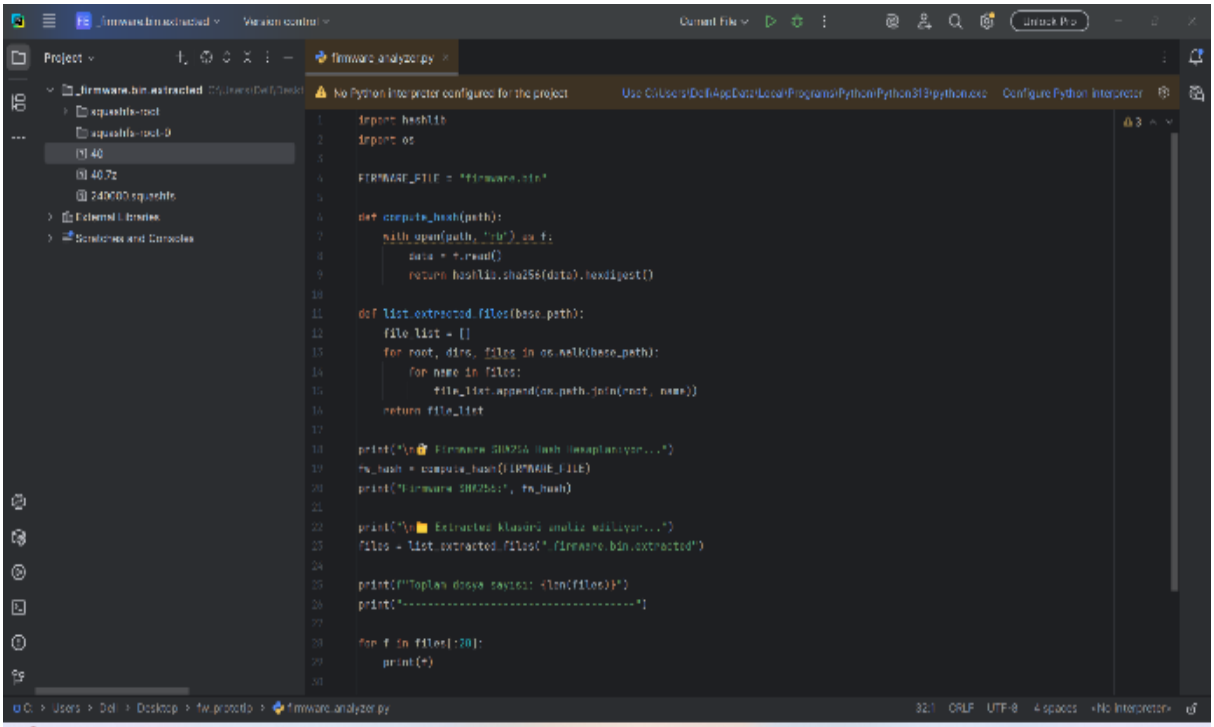
```
zehra@zehra:/mnt/c/Users/Dell/Desktop/_firmware.bin.extracted/squashfs-root/www/luci-static/resources/view/system$ cat dosyaadi
cat: dosyaadi: No such file or directory
zehra@zehra:/mnt/c/Users/Dell/Desktop/_firmware.bin.extracted/squashfs-root/www/luci-static/resources/view/system$ cat password.js
'use strict';'require view';'require dom';'require ui';'require form';'require rpc';var formData={password:{pw1:null,pw2:null}};var callSetPassword=rpc.decl
are({object:'luci',method:'setPassword',params:['username','password'],expect:{result:false}});return view.extend({checkPassword:function(section_id,value){
var strength=document.querySelector('.cbi-value-description'),strongRegex=new RegExp("^(?=.{8,})(?=.*[A-Z])(?=.*[a-z])(?=.*[0-9])(?=.*\\W).*$","g"),mediumRe
gex=new RegExp("^(?=.{7,})(((?=.*[A-Z])(?=.*[a-z]))|((?=.*[A-Z])(?=.*[0-9]))|((?=.*[a-z])(?=.*[0-9]))).*$","g"),enoughRegex=new RegExp("(?=.{6,}).*","g");if
(strength&&value.length){if(false==enoughRegex.test(value))
strength.innerHTML='%s: <span style="color:red">%s</span>'.format(_('Password strength'),_('More Characters'));else if(strongRegex.test(value))
strength.innerHTML='%s: <span style="color:green">%s</span>'.format(_('Password strength'),_('Strong'));else if(mediumRegex.test(value))
strength.innerHTML='%s: <span style="color:orange">%s</span>'.format(_('Password strength'),_('Medium'));else
strength.innerHTML='%s: <span style="color:red">%s</span>'.format(_('Password strength'),_('Weak'));}
return true;},render:function(){var m,s,o;m=new form.JSONMap(formData,_('Router Password'),_('Changes the administrator password for accessing the device'))
;m.readonly=!L.hasViewPermission();s=m.section(form.NamedSection,'password','password');o=s.option(form.Value,'pw1',_('Password'));o.password=true;o.validat
e=this.checkPassword;o=s.option(form.Value,'pw2',_('Confirmation'),' ');o.password=true;o.renderWidget=function(){var node=form.Value.prototype.renderWidget
.apply(this,arguments);node.querySelector('input').addEventListener('keydown',function(ev){if(ev.keyCode==13&&!ev.currentTarget.classList.contains('cbi-inpu
t-invalid'))
document.querySelector('.cbi-button-save').click();});return node;};return m.render();},handleSave:function(){var map=document.querySelector('.cbi-map');ret
urn dom.callClassMethod(map,'save').then(function(){if(formData.password.pw1==null||formData.password.pw1.length==0)
return;if(formData.password.pw1!=formData.password.pw2){ui.addNotification(null,E('p',_('Given password confirmation did not match, password not changed!'))
,'danger');return;}
return callSetPassword('root',formData.password.pw1).then(function(success){if(success)
ui.addNotification(null,E('p',_('The system password has been successfully changed.')),'info');else
ui.addNotification(null,E('p',_('Failed to change the system password.')),'danger');formData.password.pw1=null;formData.password.pw2=null;dom.callClassMetho
d(map,'render');});});},handleSaveApply:null,handleReset:null});zehra@zehra:/mnt/c/Users/Dell/Desktop/_firmware.bin.extracted/squashfs-root/www/luci-static/
resources/view/system$
```

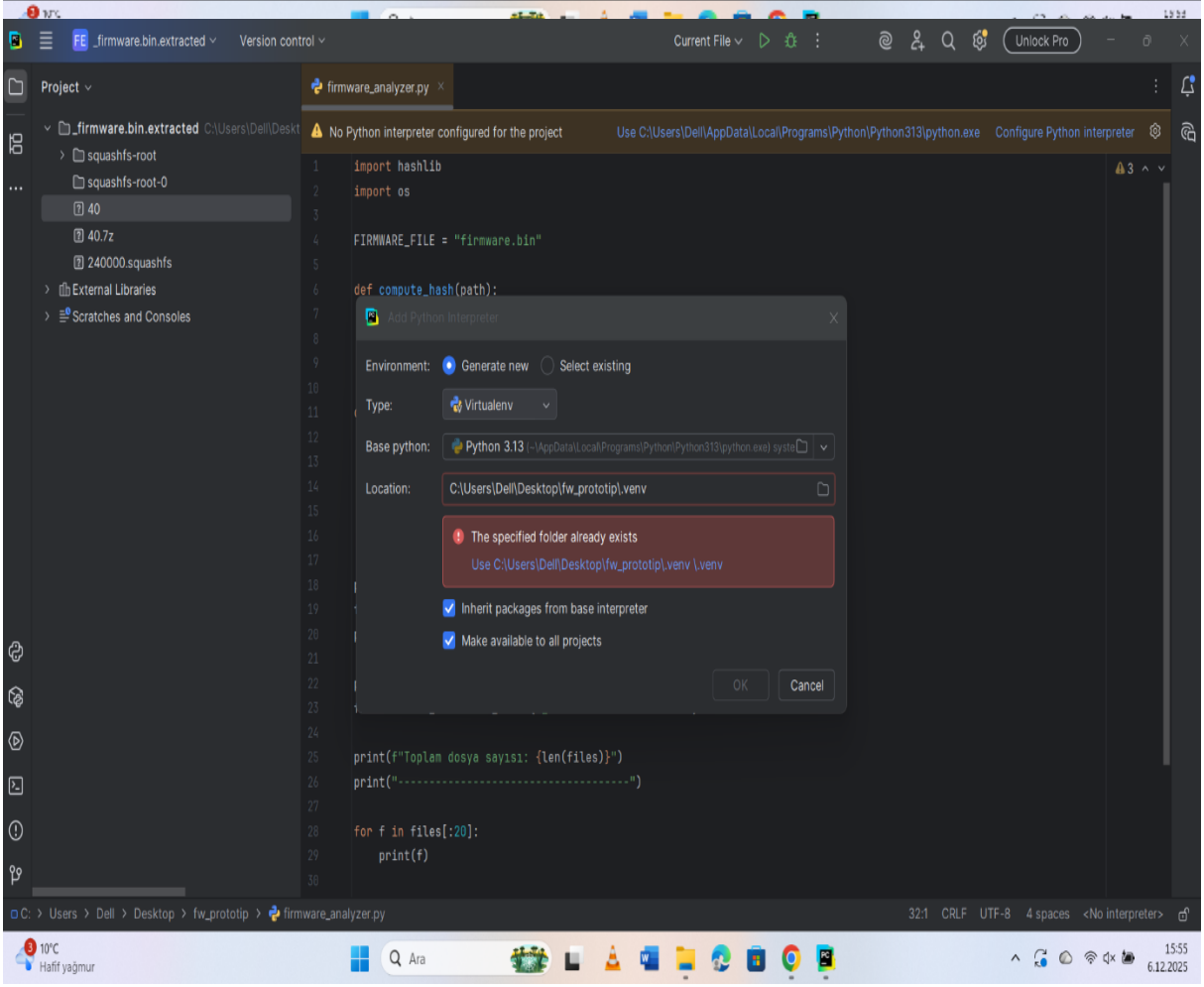
```
zehra@zehra:/mnt/c/Users/Dell/Desktop/_firmware.bin.extracted/squashfs-root/www/luci-static/resources/view/system$ cat /mnt/c/Users/Dell/Desktop/_firmware.b
in.extracted/squashfs-root/etc/config/uhttpd
# Server configuration
config uhttpd main

        # HTTP listen addresses, multiple allowed
        list listen_http        0.0.0.0:80
        list listen_http        [::]:80

        # HTTPS listen addresses, multiple allowed
        list listen_https       0.0.0.0:443
        list listen_https       [::]:443

        # Redirect HTTP requests to HTTPS if possible
        option redirect_https   0

        # Server document root
        option home             /www

        # Reject requests from RFC1918 IP addresses
        # directed to the servers public IP(s).
        # This is a DNS rebinding countermeasure.
        option rfc1918_filter 1

        # Maximum number of concurrent requests.
        # If this number is exceeded, further requests are
        # queued until the number of running requests drops
        # below the limit again.
        option max_requests 3

        # Maximum number of concurrent connections.
        # If this number is exceeded, further TCP connection
        # attempts are queued until the number of active
        # connections drops below the limit again.
        option max_connections 100

        # Certificate and private key for HTTPS.
```

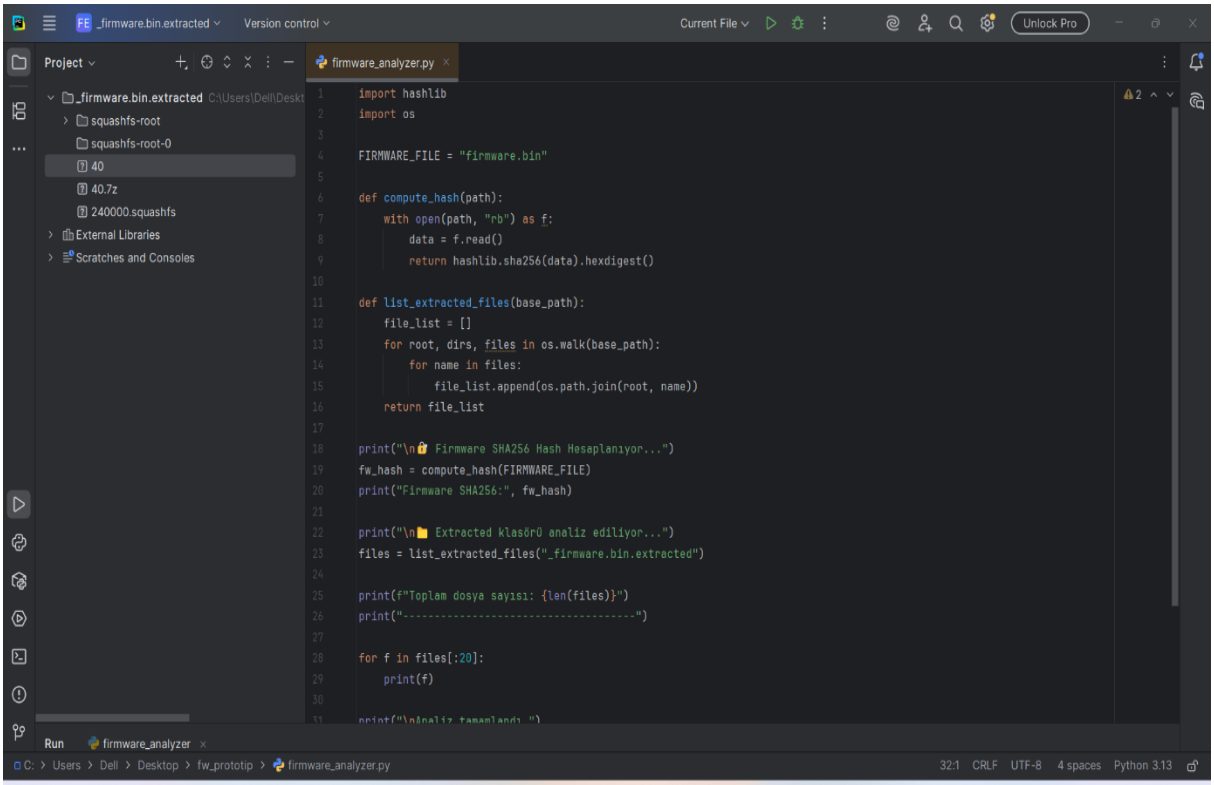
Web arayüzünün RPC tabanlı kimlik doğrulama mekanizmasının şifreyi şifrelemeden taşıdığı tespit edilmiştir. Bu yapı, man-in-the-middle (MITM) saldırılarına karşı savunmasızdır.

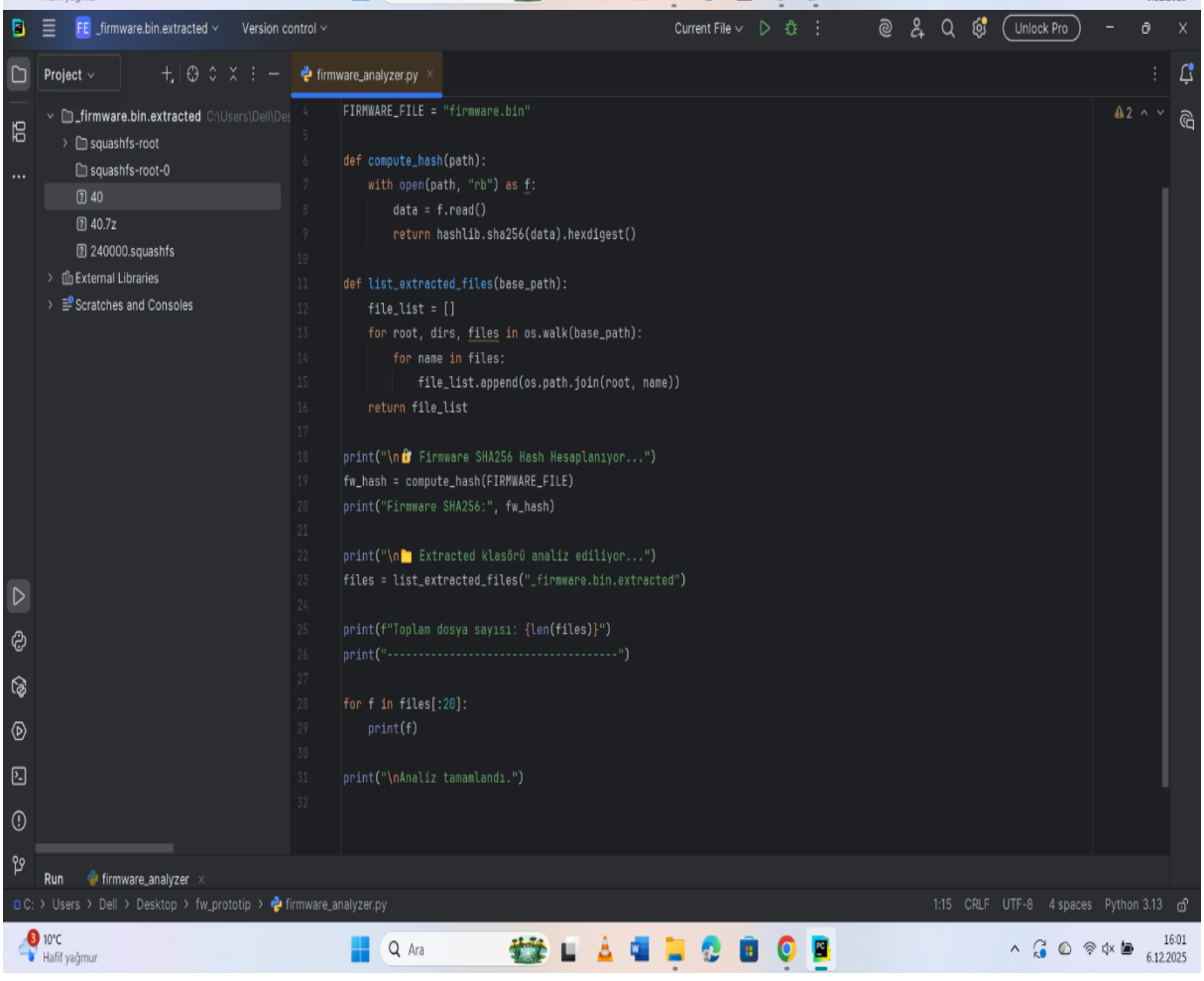
Python Otomatik Analiz

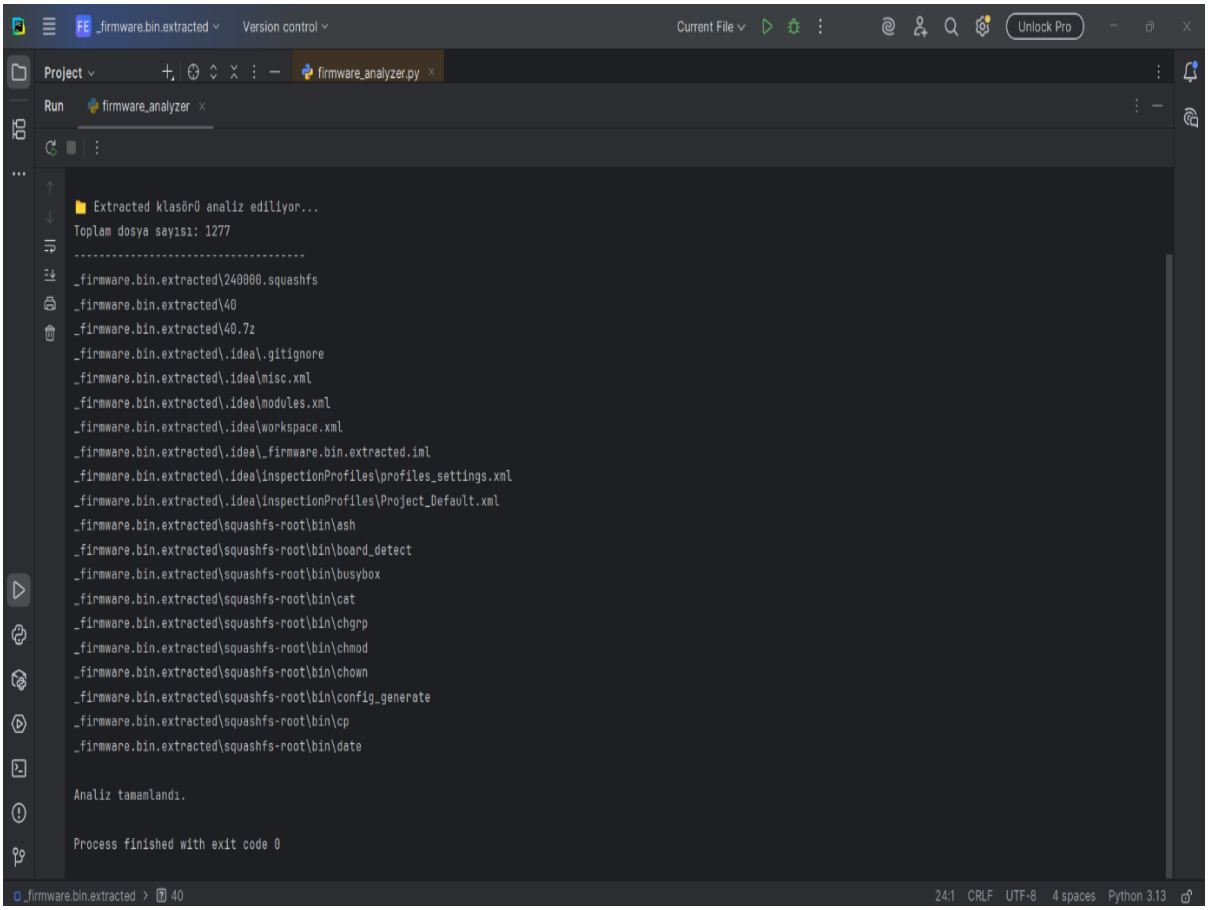

def compute_hash(path):
with open(path, "rb") as f:
data = f.read()
return hashlib.sha256(data).hexdigest()
def list_extracted_files(base_path):
Add Python Interpreter
Environment:
Generate new
Select existing
Type:
Virtualenv
Base python:
Python 3.13 (~\AppData\Local\Programs\Python\Python313\python.exe) syste
Location:
C:\Users\Dell\Desktop\fw_prototip_firmware.bin.extracted\.venv
Inherit packages from base interpreter
Make available to all projects
OK
Cancel
print("----------")
for f in files[:20]:
print(f)
print("\nAnaliz tamamlandı.")
def compute_hash(path):
with open(path, "rb") as f:
data = f.read()
return hashlib.sha256(data).hexdigest()
def list_extracted_files(base_path):
Add Python Interpreter
Environment:
Generate new
Select existing
Type:
Virtualenv
Base python:
Python 3.13 (~\AppData\Local\Programs\Python\Python313\python.exe) syste
Location:
C:\Users\Dell\Desktop\fw_prototip\.venv
Inherit packages from base interpreter
Make available to all projects
OK
Cancel
print("----------")
for f in files[:20]:
print(f)
print("\nAnaliz tamamlandı.")




_firmware.bin.extracted
Version control
Current File
Unlock Pro
Project
firmware_analyzer.py
No Python interpreter configured for the project
Use C:\Users\Dell\AppData\Local\Programs\Python\Python313\python.exe
Configure Python interpreter
_firmware.bin.extracted C:\Users\Dell\Deskt
squashfs-root
squashfs-root-0
40
40.7z
240000.squashfs
External Libraries
Scratches and Consoles
import hashlib
import os
FIRMWARE_FILE = "firmware.bin"
def compute_hash(path):
Add Python Interpreter
Environment:
Generate new
Select existing
Type:
Virtualenv
Base python:
Python 3.13 (~\AppData\Local\Programs\Python\Python313\python.exe) syste
Location:
C:\Users\Dell\Desktop\fw_prototip\.venv
The specified folder already exists
Use C:\Users\Dell\Desktop\fw_prototip\.venv \.venv
Inherit packages from base interpreter
Make available to all projects
OK
Cancel
print(f"Toplam dosya sayısı: {len(files)}")
print("-----------------------------------")
for f in files[:20]:
print(f)
C: › Users › Dell › Desktop › fw_prototip › firmware_analyzer.py
32:1
CRLF
UTF-8
4 spaces
<No interpreter>
10°C
Hafif yağmur
Ara
15:55
6.12.2025


_firmware.bin.extracted
Version control
Current File
Unlock Pro
Project
firmware_analyzer.py
_firmware.bin.extracted C:\Users\Dell\Deskt
squashfs-root
squashfs-root-0
40
40.7z
240000.squashfs
External Libraries
Scratches and Consoles
import hashlib
import os
FIRMWARE_FILE = "firmware.bin"
def compute_hash(path):
with open(path, "rb") as f:
data = f.read()
return hashlib.sha256(data).hexdigest()
def list_extracted_files(base_path):
file_list = []
for root, dirs, files in os.walk(base_path):
for name in files:
file_list.append(os.path.join(root, name))
return file_list
print("\n Firmware SHA256 Hash Hesaplanıyor...")
fw_hash = compute_hash(FIRMWARE_FILE)
print("Firmware SHA256:", fw_hash)
print("\n Extracted klasörü analiz ediliyor...")
files = list_extracted_files("_firmware.bin.extracted")
print(f"Toplam dosya sayısı: {len(files)}")
print("-----------------------------------")
for f in files[:20]:
print(f)
print("\nAnaliz tamamlandı.")
Run
firmware_analyzer
C: › Users › Dell › Desktop › fw_prototip › firmware_analyzer.py
32:1 CRLF UTF-8 4 spaces Python 3.13
10°C
Hafif yağmur
Ara
16:01
6.12.2025


_firmware.bin.extracted
Version control
Current File
Unlock Pro
Project
firmware_analyzer.py
_firmware.bin.extracted C:\Users\Dell\Des
squashfs-root
squashfs-root-0
40
40.7z
240000.squashfs
External Libraries
Scratches and Consoles
FIRMWARE_FILE = "firmware.bin"
def compute_hash(path):
with open(path, "rb") as f:
data = f.read()
return hashlib.sha256(data).hexdigest()
def list_extracted_files(base_path):
file_list = []
for root, dirs, files in os.walk(base_path):
for name in files:
file_list.append(os.path.join(root, name))
return file_list
print("\n Firmware SHA256 Hash Hesaplanıyor...")
fw_hash = compute_hash(FIRMWARE_FILE)
print("Firmware SHA256:", fw_hash)
print("\n Extracted klasörü analiz ediliyor...")
files = list_extracted_files("_firmware.bin.extracted")
print(f"Toplam dosya sayısı: {len(files)}")
print("-----------------------------------")
for f in files[:20]:
print(f)
print("\nAnaliz tamamlandı.")
Run
firmware_analyzer
C: › Users › Dell › Desktop › fw_prototip › firmware_analyzer.py
1:15 CRLF UTF-8 4 spaces Python 3.13
10°C
Hafif yağmur
Ara
16:01
6.12.2025



Projenin bir parçası olarak geliştirilen Python tabanlı prototip, firmware dosyasının SHA256 hash'ini hesaplamakta, extract edilen dizin içindeki dosyaları listelemekte ve temel statik analiz çıktıları üretmektedir. Bu araç, firmware inceleme sürecini otomatikleştirmeyi amaçlamaktadır