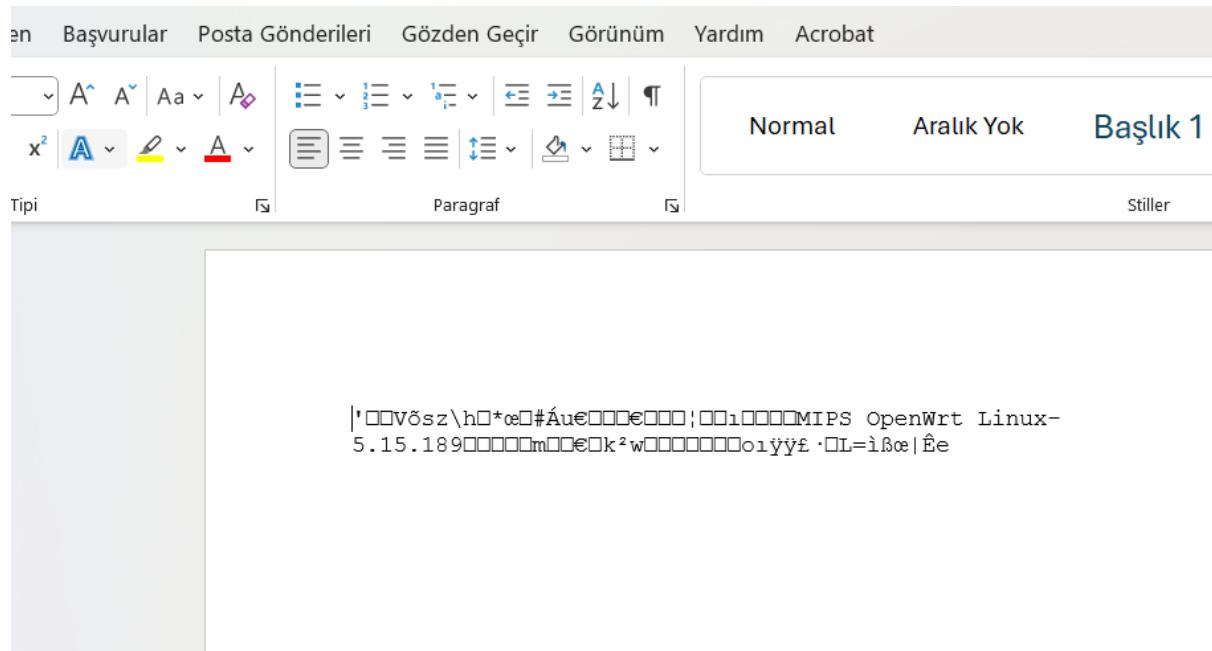


## BÜTÜNLÜK DOĞRULAMA



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

```
C:\ Komut İstemci  
Microsoft Windows [Version 10.0.26100.7171]  
(c) Microsoft Corporation. Tüm hakları saklıdır.  
  
C:\Users\Dell>sha256sum firmware.bin  
'sha256sum' is not recognized as an internal or external command,  
operable program or batch file.  
  
C:\Users\Dell>cd desktop  
  
C:\Users\Dell\Desktop>certutil -hashfile firmware.bin SHA256  
SHA256 hash of firmware.bin:  
cb29acea58ce9b8088030d508c43f3c918feced93a823d781c0e13e8981e1a93  
CertUtil: -hashfile command completed successfully.  
  
C:\Users\Dell\Desktop>
```

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

```
C:\Users\Dell>sha256sum firmware.bin
'sha256sum' is not recognized as an internal or external
operable program or batch file.

C:\Users\Dell>cd desktop

C:\Users\Dell\Desktop>certutil -hashfile firmware.bin
SHA256 hash of firmware.bin:
cb29acea58ce9b8088030d508c43f3c918feced93a823d781c0e13
CertUtil: -hashfile command completed successfully.

C:\Users\Dell\Desktop>python --version
Python 3.13.7

C:\Users\Dell\Desktop>
```

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

## UNIX KURULUMU

```
operable program or batch file.

C:\Users\Dell>cd desktop

C:\Users\Dell\Desktop>certutil -hashfile firmware.bin SHA256
SHA256 hash of firmware.bin:
cb29acea58ce9b8088030d508c43f3c918feced93a823d781c0e13e8981e1a93
CertUtil: -hashfile command completed successfully.

C:\Users\Dell\Desktop>python --version
Python 3.13.7

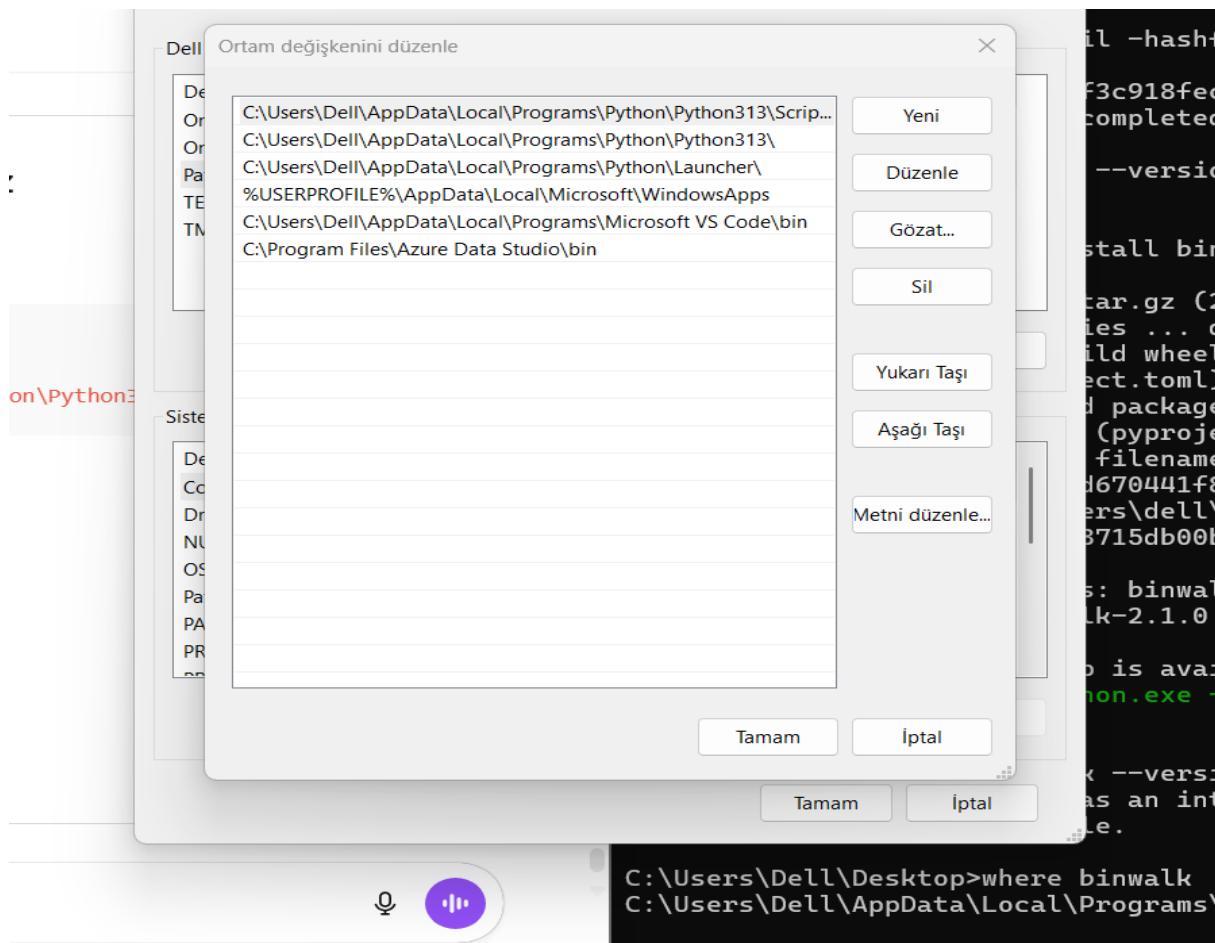
C:\Users\Dell\Desktop>pip install binwalk
Collecting binwalk
  Downloading binwalk-2.1.0.tar.gz (2.4 kB)
    Installing build dependencies ... done
    Getting requirements to build wheel ... done
    Preparing metadata (pyproject.toml) ... done
Building wheels for collected packages: binwalk
  Building wheel for binwalk (pyproject.toml) ... done
    Created wheel for binwalk: filename=binwalk-2.1.0-py3-none-any.whl size=27
84 sha256=5f5bbc0d267eed166fd670441f8921b2bad3f7c8228b9b671c974561ae0719da
     Stored in directory: c:\users\dell\appdata\local\pip\cache\wheels\94\47\9a
\f007da3a8ebca9dcc9fa238d538715db00b4e6a37475c240e
Successfully built binwalk
Installing collected packages: binwalk
Successfully installed binwalk-2.1.0

[notice] A new release of pip is available: 25.2 -> 25.3
[notice] To update, run: python.exe -m pip install --upgrade pip

C:\Users\Dell\Desktop>
C:\Users\Dell\Desktop|
```

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 hazırlıdır.

## PAKET GÜNCELLEME SORUNU

```
binwalk is not recognized as an internal or external command,  
operable program or batch file.  
  
:\Users\DELL\Desktop>python -m binwalk --version  
raceback (most recent call last):  
  File "<frozen runpy>", line 189, in _run_module_as_main  
  File "<frozen runpy>", line 148, in _get_module_details  
  File "<frozen runpy>", line 112, in _get_module_details  
  File "C:\Users\DELL\AppData\Local\Programs\Python\Python313\Lib\site-  
es\binwalk\__init__.py", line 3, in <module>  
    from binwalk.core.module import Modules, ModuleException  
ModuleNotFoundError: No module named 'binwalk.core'  
  
:\Users\DELL\Desktop>wsl --install  
stehen işlem için yükseltme gerekiyor.  
ownloading: Windows Subsystem for Linux 2.6.2  
          0,2% ]
```

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

PAKET GÜNCELLEME BAŞARILI

```
C:\Windows\System32\wsl.exe X + ▾

Microsoft Windows [Version 10.0.26100.7171]
(c) Microsoft Corporation. Tüm hakları saklıdır.

C:\Users\Dell>sha256sum firmware.bin
'sha256sum' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Dell>cd desktop

C:\Users\Dell\Desktop>certutil -hashfile firmware.bin SHA256
SHA256 hash of firmware.bin:
cb29acea58ce9b80889030d508c43f3c918feced93a823d781c0e13e8981e1a93
CertUtil: -hashfile command completed successfully.

C:\Users\Dell\Desktop>python --version
Python 3.13.7

C:\Users\Dell\Desktop>pip install binwalk
Collecting binwalk
  Downloading binwalk-2.1.0.tar.gz (2.4 kB)
    Installing build dependencies ... done
    Getting requirements to build wheel ... done
    Preparing metadata (pyproject.toml) ... done
Building wheels for collected packages: binwalk
  Building wheel for binwalk (pyproject.toml) ... done
  Created wheel for binwalk: filename=binwalk-2.1.0-py3-none-any.whl size=2784 sha256=5f5bbc0d267eed166fd670441f8921b2bad3f7c8228b9b671c974561ae0719da
  Stored in directory: c:\users\dell\appdata\local\pip\cache\wheels\94\47\9a\f007da3a8ebca9dcc9fa238d538715db00b4e6a37475c240e
Successfully built binwalk
Installing collected packages: binwalk
Successfully installed binwalk-2.1.0

[notice] A new release of pip is available: 25.2 → 25.3
[notice] To update, run: python.exe -m pip install --upgrade pip

C:\Users\Dell\Desktop>
C:\Users\Dell\Desktop>binwalk --version
'binwalk' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Dell\Desktop>where binwalk
C:\Users\appData\Local\Programs\Python\Python313\Scripts\binwalk
```

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

```
C:\Windows\System32\wsl.exe X + v

Building wheel for binwalk (pyproject.toml) ... done
Created wheel for binwalk: filename=binwalk-2.1.0-py3-none-any.whl size=2784 sha256=5f5bbc0d267eed166fd670441f8921b2bad3f7c8228b9b671c974561ae0719da
Stored in directory: c:\users\dell\appdata\local\pip\cache\wheels\94\47\9a\f007da3a8ebca9dcc9fa238d538715db00b4e6a37475c240e
Successfully built binwalk
Installing collected packages: binwalk
Successfully installed binwalk-2.1.0

[notice] A new release of pip is available: 25.2 → 25.3
[notice] To update, run: python.exe -m pip install --upgrade pip

C:\Users\Dell\Desktop>
C:\Users\Dell\Desktop>binwalk --version
'binwalk' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Dell\Desktop>where binwalk
C:\Users\Dell\AppData\Local\Programs\Python\Python313\Scripts\binwalk

C:\Users\Dell\Desktop>binwalk --version
'binwalk' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Dell\Desktop>python -m binwalk --version
Traceback (most recent call last):
  File "<frozen runpy>", line 189, in _run_module_as_main
  File "<frozen runpy>", line 148, in _get_module_details
  File "<frozen runpy>", line 112, in _get_module_details
  File "C:\Users\Dell\AppData\Local\Programs\Python\Python313\Lib\site-packages\binwalk\__init__.py", line 3, in <module>
    from binwalk.core.module import Modules, ModuleException
ModuleNotFoundError: No module named 'binwalk.core'

C:\Users\Dell\Desktop>wsl --install
İstenen işlem için yükselte gerekiyor.
Downloading: Windows Subsystem for Linux 2.6.2
|[=====          23,4%                  ]
```

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
2209_Basvuru_Formu_Sude_SOYTURK_.pdf   PowerPoint.Lnk
2209_Basvuru_Formu_Begüm_AKBAL.pdf     'SOLAR HAVEN _oyun.docx'
767d2ec-1b56-4c4a-9bea-086a3c5e650d.jpg SOLEXPR_x64_ENU
'TE A LNK'                   SOLEXPR_x64_ENU.exe
'Cisco Packet Tracer.lnk'      Sidre_Sahinoglu_2209_Basvuru_Formu.pdf
'DERO'                      TUSAŞ.docx
'Dev-C++.lnk'                'Visual Studio Code.Lnk'
'Ekran görüntüsü 2025-09-06 151603.png' WinRAR.Lnk
'Ekran görüntüsü 2025-09-06 151621.png' Word.Lnk
'Excel.lnk'                  'adlı bilişim kanunları.zip'
'Kişisel - Edge.lnk'         algo
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

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 Address: 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, created: 2025-08-14 18:27:40

```

zehra@zehra:/mnt/c/Users/Dell/Desktop$ binwalk firmware.bin
```

```
zehra@zehra:/mnt/c/Users/D ~ + ▾
changing link target to /dev/null for security purposes.

WARNING: Symlink points outside of the extraction directory: /mnt/c/Users/Dell/Desktop/_firmware.bin.extracted/squashfs-root/etc/resolv.conf -> /tmp/resolv.conf; changing link target to /dev/null for security purposes.

WARNING: Symlink points outside of the extraction directory: /mnt/c/Users/Dell/Desktop/_firmware.bin.extracted/squashfs-root/etc/TZ -> /tmp/TZ; changing link target to /dev/null for security purposes.

WARNING: Symlink points outside of the extraction directory: /mnt/c/Users/Dell/Desktop/_firmware.bin.extracted/squashfs-root/etc/ppp/resolv.conf -> /tmp/resolv.conf.ppp; changing link target to /dev/null for security purposes.

WARNING: Symlink points outside of the extraction directory: /mnt/c/Users/Dell/Desktop/_firmware.bin.extracted/squashfs-root/etc/ssl/cert.pem -> /etc/ssl/certs/ca-certificates.crt; changing link target to /dev/null for security purposes.

WARNING: Symlink points outside of the extraction directory: /mnt/c/Users/Dell/Desktop/_firmware.bin.extracted/squashfs-root/sbin/insmod -> /usr/sbin/kmodloader; changing link target to /dev/null for security purposes.

WARNING: Symlink points outside of the extraction directory: /mnt/c/Users/Dell/Desktop/_firmware.bin.extracted/squashfs-root/sbin/lsmod -> /usr/sbin/kmodloader; changing link target to /dev/null for security purposes.

WARNING: Symlink points outside of the extraction directory: /mnt/c/Users/Dell/Desktop/_firmware.bin.extracted/squashfs-root/sbin/modinfo -> /usr/sbin/kmodloader; changing link target to /dev/null for security purposes.

WARNING: Symlink points outside of the extraction directory: /mnt/c/Users/Dell/Desktop/_firmware.bin.extracted/squashfs-root/sbin/modprobe -> /usr/sbin/kmodloader; changing link target to /dev/null for security purposes.

WARNING: Symlink points outside of the extraction directory: /mnt/c/Users/Dell/Desktop/_firmware.bin.extracted/squashfs-root/sbin/rmmod -> /usr/sbin/kmodloader; changing link target to /dev/null for security purposes.

WARNING: Symlink points outside of the extraction directory: /mnt/c/Users/Dell/Desktop/_firmware.bin.extracted/squashfs-root/usr/bin/scp -> /usr/sbin/dropbear; changing link target to /dev/null for security purposes.

WARNING: Symlink points outside of the extraction directory: /mnt/c/Users/Dell/Desktop/_firmware.bin.extracted/squashfs-root/usr/bin/ssh -> /usr/sbin/dropbear; changing link target to /dev/null for security purposes.

WARNING: Symlink points outside of the extraction directory: /mnt/c/Users/Dell/Desktop/_firmware.bin.extracted/squashfs-root/usr/bin/wget -> /usr/bin/uclient-fetch; changing link target to /dev/null for security purposes.
2359296      0x240000      Squashfs filesystem, little endian, version 4.0, compression:xz, size: 3736284 bytes, 1385 inodes, blocksize: 262144 bytes, created: 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'ın gömülü Linux tabanlı bir işletim sistemi kullandığını göstermektedir

## passwd / shadow Analizi

```
dr, changing link target to /dev/null for security purposes.

WARNING: Symlink points outside of the extraction directory: /mnt/c/Users/Dell/Desktop/_firmware.bin
ar; changing link target to /dev/null for security purposes.

WARNING: Symlink points outside of the extraction directory: /mnt/c/Users/Dell/Desktop/_firmware.bi
t-fetch; changing link target to /dev/null for security purposes.
2359296      0x240000      Squashfs filesystem, little endian, version 4.0, compression:xz, size
eated: 2025-08-14 18:27:40

zehra@zehra:/mnt/c/Users/Dell/Desktop$ cd _firmware.bin.extracted
zehra@zehra:/mnt/c/Users/Dell/Desktop/_firmware.bin.extracted$ cd squashfs-root
zehra@zehra:/mnt/c/Users/Dell/Desktop/_firmware.bin.extracted/squashfs-root$ ls
bin dev etc lib mnt overlay proc rom root sbin sys tmp usr var www
zehra@zehra:/mnt/c/Users/Dell/Desktop/_firmware.bin.extracted/squashfs-root$
```

```
You don't need to install a link to busybox for each utility.
To run external program, use full path (/sbin/ip instead of ip).
```

```
Currently defined functions:
[, [[, acpid, adjtimex, ar, arch, arp, arping, ash, awk, basename, bc, blkdiscard, blockdev, brctl, bunzip2, busybox, bzcat, bzip2, cal, cat,
chgrp, chmod, chown, chpasswd, chroot, chvt, clear, cmp, cp, cpio, cron, crontab, cttyhack, cut, date, dc, dd, deallocvt, depmod, devmem, df,
diff, dirname, dmesg, dnsdomainname, dos2unix, dpkg, dpkg-deb, du, dumpkmap, dumpleases, echo, ed, egrep, env, expand, expr, factor, fallocate,
false, fattr, fdisk, fgrep, find, fold, free, freeramdisk, fsfreeze, fstrim, ftpput, getopt, getty, grep, groups, gunzip, gzip, halt,
head, hexdump, hostid, hostname, httpd, hwclock, i2cdetect, i2cdump, i2cget, i2cset, id, ifconfig, ifdown, ifup, init, insmod, ionice, ip, ipcalc,
ipneigh, kill, killall, klogd, last, less, link, linux32, linux64, linuxrc, ln, loadfont, loadmap, logger, login, logname, logread, losetup, ls,
lsmod, lsscsi, lzcat, lzma, lzop, md5sum, mdev, microcom, mkdir, mkdosfs, mke2fs, mkfifo, mknod, mkpasswd, mkswap, mktemp, modinfo, modprobe, more,
mount, mt, mv, nameif, nc, netstat, nl, nologin, nproc, nslookup, nuke, od, openpty, partprobe, passwd, paste, patch, pidof, ping, ping6,
pivot_root, poweroff, printf, ps, pwd, rdate, readlink, realpath, reboot, renice, reset, resume, rev, rm, rmdir, rmmod, route, rpm, rpm2cpio,
run-init, run-parts, sed, seq, setkeycodes, setpriv, setsid, sh, shasum, sha256sum, sha512sum, shred, shuf, sleep, sort, ssl_client,
start-stop-daemon, stat, static-sh, strings, stty, su, sulogin, svc, svok, swapoff, swapon, switch_root, sync, systemctl, syslogd, tac, tail, tar,
taskset, tc, tee, telnet, telnetd, test, tftp, time, timeout, top, touch, tr, traceroute, traceroute6, true, truncate, tty, tunctl, ubirename,
udhcp, udhcpd, uevent, umount, uname, uncompress, unexpand, uniq, unix2dos, unlink, unlzma, unshare, unxz, unzip, uptime, usleep, uudecode,
uuencode, vconfig, vi, w, watch, watchdog, wc, wget, which, who, whoami, xargs, xxd, xz, xzcat, yes, zcat
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/pas
swd
root:x:0:0:root:/root:/bin/ash
daemon:*:1:1:daemon:/var:/bin/false
ftp:*:55:55:ftp:/home/ftp:/bin/false
network:*:101:101:network:/var:/bin/false
nobody:*:65534:65534:nobody:/var:/bin/false
ntp:x:123:ntp:/var/run/ntp:/bin/false
dnsmasq:x:453:453:dnsmasq:/var/run/dnsmasq:/bin/false
logd:x:514:514:logd:/var/run/logd:/bin/false
ubus:x:81:81:ubus:/var/run/ubus:/bin/false
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/sha
dow
root:::0:99999:7:::
daemon:*:0:0:99999:7:::
ftp:*:0:0:99999:7:::
network:*:0:0:99999:7:::
nobody:*:0:0:99999:7:::
ntp:x:0:0:99999:7:::
dnsmasq:x:0:0:99999:7:::
logd:x:0:0:99999:7:::
ubus:x:0:0:99999:7:::
zehra@zehra:/mnt/c/Users/Dell/Desktop/_firmware.bin.extracted/squashfs-root/bin$
```

/etc/passwd ve /etc/shadow dosyaları incelenerek kullanıcı hesaplarının yapılandırması kontrol edilmiştir. Root kullanıcısının parola alanı kilitli görülmektedir. 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/so
-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  
Zayıflığı**

```

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]).*$","g"),mediumRe
gex=new RegExp("(?=.{7,})((?=.*[A-Z])(?=.*[a-z])(?=.*[0-9]))|((?=.*[a-z])(?=.*[0-9]))|((?=.*[a-z])(?=.*[0-9]))).*,$","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),_('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

```
6     def compute_hash(path):
7         with open(path, "rb") as f:
8             data = f.read()
9             return hashlib.sha256(data).hexdigest()
10
11     def list_extracted_files(base_path):
12
13         print("-----")
14
15         for f in files[:20]:
16             print(f)
17
18         print("\nAnaliz tamamlandi.")
19
20
21
22
23
24
25
26     print("-----")
27
28     for f in files[:20]:
29         print(f)
30
31     print("\nAnaliz tamamlandi.")
32
```

Add Python Interpreter

Environment:  Generate new  Select existing

Type:  Virtualenv

Base python: Python 3.13 (~\AppData\Local\Programs\Python\Python313\python.exe) system

Location: C:\Users\Dell\Desktop\fw\_prototip\firmware.bin.extracted\venv

Inherit packages from base interpreter

Make available to all projects

OK Cancel

Add Python Interpreter

Environment:  Generate new  Select existing

Type:  Virtualenv

Base python: Python 3.13 (~\AppData\Local\Programs\Python\Python313\python.exe) system

Location: C:\Users\Dell\Desktop\fw\_prototip\venv

Inherit packages from base interpreter

Make available to all projects

OK Cancel

**firmware\_analyzer.py**

```
1 import hashlib
2 import os
3
4 FIRMWARE_FILE = "firmware.bin"
5
6 def compute_hash(path):
7     with open(path, "rb") as f:
8         data = f.read()
9     return hashlib.sha256(data).hexdigest()
10
11 def list_extracted_files(base_path):
12     file_list = []
13     for root, dirs, files in os.walk(base_path):
14         for name in files:
15             file_list.append(os.path.join(root, name))
16     return file_list
17
18 print("\nfirmware SHA256 hash: " + compute_hash(FIRMWARE_FILE))
19 rh_hash = compute_hash("firmware.bin")
20 print("Firmware SHA256: ", rh_hash)
21
22 print("\nExtracted klasör analizi başlıyor...")
23 files = list_extracted_files("_firmware.bin.extracted")
24
25 print(f"Toplam dosya sayısı: {len(files)}")
26 print("-----")
27
28 for f in files[:20]:
29     print(f)
```

**firmware\_analyzer.py**

```
1 import hashlib
2 import os
3
4 FIRMWARE_FILE = "firmware.bin"
5
6 def compute_hash(path):
7     Add Python Interpreter
8
9 Environment:  Generate new  Select existing
10 Type:  Virtualenv
11 Base python: Python 3.13 (C:\Users\...Python\Python313\python.exe)
12 Location: C:\Users\...fw_prototip\venv
13
14 ! The specified folder already exists
15 Use C:\Users\...fw_prototip\venv\venv
16
17  Inherit packages from base interpreter
18  Make available to all projects
19
20 OK Cancel
21
22
23
24
25 print(f"Toplam dosya sayısı: {len(files)}")
26 print("-----")
27
28 for f in files[:20]:
29     print(f)
```

```
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.")
```

The screenshot shows a terminal window with the following output:

```
Extracted klasörÜ analiz ediliyor...
Toplam dosya sayısı: 1277
-----
_firmware.bin.extracted\240000.squashfs
_firmware.bin.extracted\40.7z
_firmware.bin.extracted\.idea\.gitignore
_firmware.bin.extracted\.idea\misc.xml
_firmware.bin.extracted\.idea\modules.xml
_firmware.bin.extracted\.idea\workspace.xml
_firmware.bin.extracted\.idea\_firmware.bin.extracted.iml
_firmware.bin.extracted\.idea\inspectionProfiles\profiles_settings.xml
_firmware.bin.extracted\.idea\inspectionProfiles\Project_Default.xml
_firmware.bin.extracted\squashfs-root\bin\ash
_firmware.bin.extracted\squashfs-root\bin\board_detect
_firmware.bin.extracted\squashfs-root\bin\busybox
_firmware.bin.extracted\squashfs-root\bin\cat
_firmware.bin.extracted\squashfs-root\bin\chgrp
_firmware.bin.extracted\squashfs-root\bin\chmod
_firmware.bin.extracted\squashfs-root\bin\chown
_firmware.bin.extracted\squashfs-root\bin\config_generate
_firmware.bin.extracted\squashfs-root\bin\cp
_firmware.bin.extracted\squashfs-root\bin\date
Analiz tamamlandı.
Process finished with exit code 0
```

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