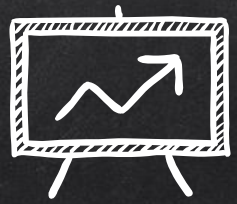


# IoT Linux Forensics

CHAMPLAIN COLLEGE
Leahy Center for Digital Forensics & Cybersecurity

# HELLO!

**Ali Hadi**,

Assistant Professor and Researcher at Champlain College.

Joseph McCormack,

Sophomore Digital Forensics student at Champlain College.

Austin Grupposo,

Sophomore Digital Forensics student at Champlain College.


# IoT Linux Forensics

is becoming Important to Digital Forensics Investigators; Are You Caught Up?

# A Primer

- ✘ IoT security issues are often overlooked
- ✘ Devices can interconnect throughout a consumer network
- ✘ Devices could be assembled from different components manufactured by different producers.

# Purpose and Scope

- ✘ Research and utilize access methods in a forensic setting
- ✘ Many devices available at the Leahy Center
- ✘ Software and Hardware level research
- ✘ Root access to look into file system
- ✘ Open-Source Linux tools
- ✘ Logs, config files, user artifacts

# IoT Device File Systems

- ✘ The most common file systems found on IoT firmwares:
  - Ext2
  - Cramfs
  - JFFS2
  - Squashfs
  - YAFFS2

- ✘ They can be identified using their signature (still under research)

# IoT Device Compression Methods

Compression is used on most devices due to limited space:

- ✘ Gzip
- ✘ LZMA
- ✘ Zlib
- ✘ Zip

# Access Methods to IoT Devices

- ✘ Software and Hardware exploits
  - Known exploits that can lead to root
- ✘ Different Interfaces to access the IoT device
  - Web
  - USB
  - Ethernet
- ✘ JTAG/UART

# Why UART Communication?

- ✘ Universal Asynchronous Receiver/Transmitter
- ✘ Allows interacting with devices:
  - Reading debug logs
  - Bootloader access
  - admin/admin, root/toor, admin/password
    - Get root...

# How Many UART Pins?

- ✘ Many devices use 8-pins for read/write
- ✘ 4-pins were used for the devices used in this research, since only reading was required
  - E.g. the camera only allows reading

# Serial Communication?

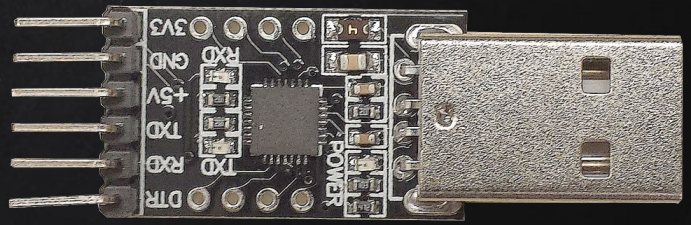
- ✘ Most IoT devices use Serial Communication and protocols
- ✘ Transfer 1-bit at a time
- ✘ Common Channels: RS232, USB, HDMI, etc

# Baud rate

- ✘ The rate at which information is transferred
- ✘ UART has no clock rate
- ✘ Ex. 9600 baud, 19200 baud, 115200 baud

# UART Converter

- ✘ Translates serial data into readable data via USB
- ✘ Requires additional cabling (often included)
- ✘ Purchased on Amazon



# Devices Researched

- Smart Home:
  - Philips Hue Lights
  - Pet Cube Play
  - Nest Thermostat
- Voice Assistants:
  - Amazon Echo
  - Google Home
  - Facebook Portal
- Security Systems:
  - Samsung SmartCam
  - D-Link 5030L Wifi Cam
  - Ring Video Doorbell
- Smart Hubs:
  - Samsung Smartthings Hub
  - Wink Hub 2
  - Circle by Disney

# IoT Catalog (p1) ...

| Device Name | Identifier No. | Identifier Type | Manufacturer | Status | Physical Factory Reset | Ethernet Port | USB Connector | JTAG Access | Remote Exploit |
|---|---|---|---|---|---|---|---|---|---|
| Echo | SK705DI | Model No. | Amazon | Untouched | YES | NO | NO | | |
| Echo Dot 2nd gen | RS03QR | Model No. | Amazon | Untouched | YES | NO | YES | YES | NO |
| Echo Look | PL67WR | Model No. | Amazon | Untouched | | | | | |
| Echo Spot | VN94DQ | Model No. | Amazon | Untouched | YES | | | | |
| Echo Show (10" Screen) | DW84JL | Model No. | Amazon | Untouched | YES | | | | |
| Echo Show | MW46WB | Model No. | Amazon | Untouched | YES | | | | |
| Cloud Cam | PB04JL | Model No. | Amazon | Untouched | YES | | | | |
| Google Home Hub | 8929AA0GS20 | Serial No. | Google | Being Researched/Worked On | YES | | | | |
| Home | 6C07AYWE00 | Serial No. | Google | Untouched | YES | | | | |
| Google WiFi Point | 3701HT0062F | Serial No. | Google | Untouched | YES | | | | |
| Nest Thermostat | 69EM02M10E01 | Serial No. | Google | Untouched | NO | | | | |
| Nest Thermostat | 09AB01AC461615CE | Serial No. | Google | Untouched | NO | NO | YES | YES | |
| Nest Cam Indoor | 18B4305A27C0 | Serial No. | Google | Untouched | NO | | | | |
| Nest Guard | 07AA01AD41170DBN | Serial No. | Google | Untouched | YES | | | | |
| Nest Protect | 06C | Model No. | Google | Untouched | YES | | | | |
| Nest Protect | 06A | Model No. | Google | Untouched | YES | | | | |
| Nest Cam Indoor | 18B4304E6DCE | Serial No. | Google | Untouched | | | | | |
| Ring Video Doorbell | BHL11637CH005687-1 | Serial No. | Ring | Untouched | YES | NO | NO | | |
| Ring Video Doorbell | BHR41652LH006322 | Serial No. | Ring | Untouched | YES | | | | |
| Ring Stick Up Cam | BHS2LH1646006907 | Serial No. | Ring | Untouched | | NO | YES | YES | |
| Kasa Cam | 2186004R02109 | Serial No. | TP-Link | Untouched | YES | NO | YES | YES | |
| Logi Circle | V-R0005 | Model No. | Logitech | Untouched | YES | NO | YES | | |
| Connect WiFi Camera | NS-CH1\|PC8 | Model No. | Insignia | Untouched | | | | | |
| SimpliCam | 007542E | Model No. | SimpliSafe | Untouched | YES | | | | |
| Canary Flex | C600K1703633 | Serial No. | Canary | Untouched | YES | | | | |
| Circle 2 | V-R0008 | Model No. | Logitech | Untouched | YES | | | | |
| WeMo Insight Switch | 221620K120014D | Serial No. | Belkin | Untouched | YES | | | | |
| WeMo Light Switch | 221624K130031A | Serial No. | Belkin | Untouched | YES | | | | |
| Ecobee 3 | EB-STATE3-02 | Model No. | Ecobee | Untouched | NO | | | | |
| Dojo Pebble + (Base) | DBB000042 | Model No. | Bullguard | Untouched | YES | | | | |
| SmartThings Hub | IM6001-V3P01 | Model No. | Zigbee | Being Researched/Worked On | YES | YES | YES | | |
| Blink XT Security Camera System | PRODUCT MISSING | PRODUCT MISSING | Blink | Untouched | | | | | |
| Nexus 7 | D80KBC769433 | Serial No. | Asus | Untouched | NO | | | | |
| Nexus 7 | D90KBC250069 | Serial No. | Asus | Being Researched/Worked On | YES | NO | YES | | |
| Nexus 7 | D80KBC758481 | Serial No. | Asus | Untouched | NO | | | | |
| iPad 6 | DMPRXHAVG5VJ | Serial No. | Apple | Untouched | NO | | | | |
| iPad 6 | GG7XKNGXJMVR | Serial No. | Apple | Untouched | NO | | | | |
| Tile Mates and Slim | M04P9000183013L | Serial No. | Anatel | Untouched | NO | | | | |
| Schlage Sense | BE479CAM619 | Model No. | Schlage | Untouched | YES | | | | |
| Circle with Disney | 8CE2DAF10D7F | Serial No. | Circle Media | Being Researched/Worked On | YES | YES | YES | | YES |
| Circle with Disney | 8CE2DAF053BA | Serial No. | Circle Media | Untouched | YES | | | | |

# IoT Catalog (p2) ...

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Portal | B81AO1BUS | Model No. | Facebook | Untouched | YES | | | | |
| Caseta Wireless Dimmer Kit with Smai | 01923D90 | Serial No. | Lutron | Being Researched/Worked On | YES | YES | YES | YES | MAYBE |
| SmartThings Hub | ZM5304AU | Model No. | SmartThings | Untouched | YES | | | | |
| Eggminder | ABAA00027468 | Serial No. | Quirky + General Electri | Untouched | NO | | | | |
| Samsung Galaxy Tab A | R52M80B71CK | Serial No. | Samsung | Untouched | NO | | | | |
| Wink Hub 2 | WZE11642001191 | Serial No. | Wink | Untouched | YES | | | | |
| Wink Hub | 161801243WZD1 | Serial No. | Wink | Untouched | YES | | | | |
| Wink Hub | 151100501WZD1 | Serial No. | Wink | Untouched | YES | | | | |
| Ring Base Station | BHBS11744PG001975 | Serial No. | Ring | Untouched | YES | | | | |
| Wifi Smart Thermostat | 1649JA007682 | Serial No. | Honeywell | Untouched | NO | | | | |
| Beam Alert | ZMD12IGC6000232 | Serial No. | Zmodo | Untouched | YES | | | | |
| Greet Smart WiFi Doorbell | ZMD12EA48000087 | Serial No. | Zmodo | Untouched | YES | | | | |
| Cujo | PRODUCT MISSING | PRODUCT MISSING | Cujo | Untouched | | | | | |
| Hue Personal Lighting System | MP051503490184 | Serial No. | Philips | Untouched | YES | | | | |
| Hue Personal Lighting System (White Starter Kit) | | Serial/Model No. Not Found | Philips | Being Researched/Worked On | YES | YES | NO | YES | |
| LG Lucky | 508VTZC0431621 | Serial No. | LG | Untouched | YES | | | | |
| Samsung Smart Cam | KJD76V2F40002KW | Serial No. | Samsung | Being Researched/Worked On | YES | YES | NO | YES | YES |
| Samsung Smart Cam | KHNL6V2H60048PE | Serial No. | Samsung | Being Researched/Worked On | YES | | | | |
| ADT Security Hub | 1739020005764334 | Serial No. | Samsung | Untouched | YES | | | | |
| D-Link HD Pan WIFI Camera (White) | RZZK1G9002702 | Serial No. | D-Link | Being Researched/Worked On | YES | YES | YES | | YES |
| SimpliSafe Security System | 00005F83 | Serial No. | SimpliSafe | Untouched | | | | | |
| Petcube Play | PP211NV5LRV | Model No. | Petcube | Untouched | YES | | | | |
| Guardzilla All-In-One Security System | FCAX53UZ79E55NSW111A | Model No. | Guardzilla | Untouched | YES | | | | |
| **Canary 100USBK Indoor Camera** | **C100K1607590** | **Serial No.** | **Canary** | **Being Researched/Worked Or** | **NO** | **YES** | **YES** | **YES** | **NO** |
| D-Link WIFI Camera (Black) | QEEF1G8001327 | Serial No. | D-Link | Untouched | YES | | | | |
| D-Link WiFi Camera (White) | QXLB1I400877 | Serial No. | D-Link | Untouched | YES | | | | |
| D-Link Wi-Fi Camera (Black) | RZZN1GC005522 | Serial No. | D-Link | Untouched | YES | | | | |
| Lorex LCD monitor and recorder | WA0216103707 | Serial No. | Flir | Untouched | NO | | | | |
| Lorex HD WiFi Security Camera | PRODUCT MISSING | PRODUCT MISSING | Flir | Untouched | YES | | | | |
| Motorola baby monitor | VT16037003248 | Serial No. | Motorola | Untouched | NO | | | | |
| Arlo Pro Security System (Base) | 4R026A7FA1C19 | Serial No. | Netgear | Untouched | YES | | | | |
| Kwikset Kevo Smart Lock | | Serial/Model No. Not Found | Kwikset | Being Researched/Worked On | YES | | | | |
| Kevo Deadbolt 2nd Gen | | Serial/Model No. Not Found | Kwikset | Untouched | YES | | | | |
| Norton Core | COR11C779920 | Serial No. | Norton | Being Researched/Worked On | YES | YES | YES | | NO |
| OnHub | TGR1900 | Model No. | TP-Link / Google | Being Researched/Worked On | YES | YES | YES | YES | YES |
| Google Home | 6C07AYWE00 | Serial No. | Google | Being Researched/Worked On | YES | NO | YES | NO | NO |

# Available Interfaces for Access

| Device | Ethernet Port | USB Connector | Remote Exploit | Hardware Exploit | JTAG Access |
|---|---|---|---|---|---|
| Canary USB100UK | YES | YES | NO | NO | YES |
| Samsung SmartCam HD Pro (Chinese) | YES | NO | YES | NO | YES |
| Lutron Caseta | YES | YES | NO | YES | YES |
| D-Link HD Pan WIFI Camera (White) | YES | YES | YES | NO | YES |
| Philips Hue White Starter Kit | YES | NO | | YES | YES |
| Circle with Disney | YES | YES | YES | NO | YES |
| Wink Hub 2 | YES | NO | YES | YES | YES |
| Philips Hue Bridge (Old) | YES | NO | YES | NO | YES |
| Samsung SmartThings Hub | YES | YES | YES | NO | YES |
| Arlo | YES | YES | YES | YES | YES |
| Google OnHub | YES | YES | YES | YES | YES |
| Philips Hue Bridge (New) | YES | NO | YES | NO | YES |
| Norton Core | YES | YES | NO | NO | YES |
| Samsung SmartCam HD Pro | YES | NO | YES | NO | YES |
| Portal | NO | YES | | | |
| Amazon Echo | NO | NO | YES | YES | YES |
| Google Home | NO | YES | NO | YES | NO |
| Amazon Echo Dot | NO | YES | YES | YES | YES |
| Lorex | YES | YES | NO | NO | YES |
| Petcube Play | | | | | |

# Surface Mapping (Ports & Services)

| Device Name | MAC Address | Open Ports | Services | Operating System | Linux Access Method |
|---|---|---|---|---|---|
| Canary USB100UK | D8:42:E2:03:08:68 | none | -- | -- | |
| Samsung SmartCam HD Pro (Chinese) | 00:16:6C:85:04:76 | 80 / 443 / 554 / 943 / 4520 / 49152 | HTTP / HTTP / RTSP / Silverlight / RTSP / UPNP | Linux 2.6.32 | |
| Lutron Caseta | B0:D5:CC:00:C4:70 | 22 / 4548 / 8081 / 8083 | ssh / synchromesh / blackice-icecap / us-srv | Linux 3.11-4.1 | |
| D-Link HD Pan WIFI Camera (White) | B0:c5:54:35:e0:a0 | 80 / 443 | HTTP / HTTPS/ssl | -- | |
| Philips Hue White Starter Kit (Philips Hue Bridge) | 00:17:88:48:BB:B1 | 80 / 443 / 8080 /22 | HTTP / HTTPS/ssl / HTTP-Proxy | Linux (Specialized) (OpenWRT) | PuTTY |
| Circle with Disney | 8C:E2:DA:F0:53:B9 | 80 / 443 / 4444 / 4567 | rtsp / rtsp / rtsp / rtsp | Linux 3.0 (Specialized) | |
| Wink Hub 2 | 00:21:CC:4B:E1:7F | 1883 / 8886 | mqtt / unknown | Linux 3.2 - 4.9 | |
| Philips Hue Bridge (Old) | 00:17:88:1C:0F:78 | 80 | HTTP | lwIP Stack | |
| Smartthings Hub | 28:6D:97:7C:F5:EC | 443 / 8889 / 8890 / 39500 | http / ddi-tcp-2 / ddi-tcp-2 / hubCore | Linux 3.2 - 4.9 | |
| Arlo Pro | 10:DA:43:CD:12:D1 | 5061 | sip-tls | Linux 2.6.19-2.6.36 | |
| Google OnHub | A4:2B:B0:CE:B5:13 | none | - | - | Hardware Root |
| Google Home Hub | 1C:F2:9A:4A:FB:F3 | 7778 / 8008 / 8009 / 8443 / 9000 / 10001 | interwise / http / castv2 / https-alt / cslistener / scp-config | Fortninet FortiGate 100D Firewall | |
| Nest Thermostat | | | | | |
| Canary Flex (UNUSABLE) | -- | -- | -- | -- | -- |
| Facebook Portal | A4:0E:2B:00:A5:19 | none | -- | -- | |
| Amazon Echo | AC:63:BE:6B:37:50 | 4070 / 4071 / 55442 / 55443 | http/http/nagios-ncsa/ssl | FireOS | |
| Google Home | F4:F5:D8:C8:BB:04 | 8008 / 8009 / 8443 / 9000 / 10001 | http / ajp13 / https-alt / cslistener / scp-config | Linux 2.6.32-3.10 | |
| Logitech Circle | 44:73:D6:05:91:C4 | -- | -- | Unknown | |
| Guardzilla All-In-One HD | E0:B9:4D:21:0D:DB | 23 | telnet | Linux 2.6.32-3.10 | Telnet |
| Nest Thermostat | 18:B4:30:B7:45:29 | -- | -- | -- | -- |
| Canary Pro | D8:42:E2:02:E1:58 | none | -- | "Too many fingerprints match this host to give specific OS details" | |
| Amazon Cloud Cam | FC:A1:83:24:7B:14 | -- | | FireOS | |

# Devices Investigated

...


- ✘ Philips Hue Bridge
- ✘ D-Link HD Pan Wifi Cam 5030l

# Forensic Workflow

# Step One: Datagen and acquisition

1. Factory Reset
2. Utilize Device as normal
3. Document actions in Timeline
4. Connect device to UART converter
5. Use Linux machine to access shell (Kali/Ubuntu)

# Step Two: Finding the baud rate of a device

- ✘ Installing Python
- ✘ Installing Pyserial
- ✘ Baudrate.py by DevTTYS0

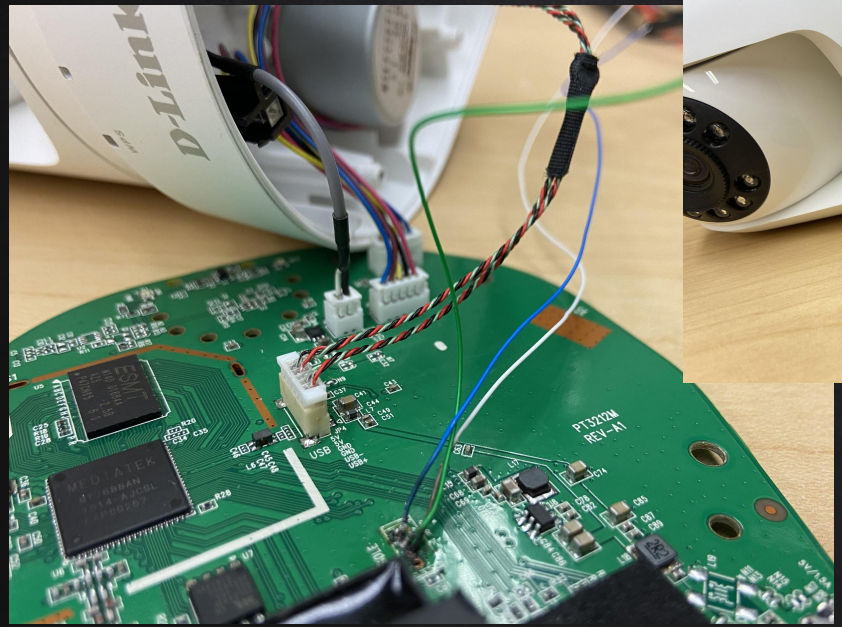
# 3. Setting up serial ports in Linux

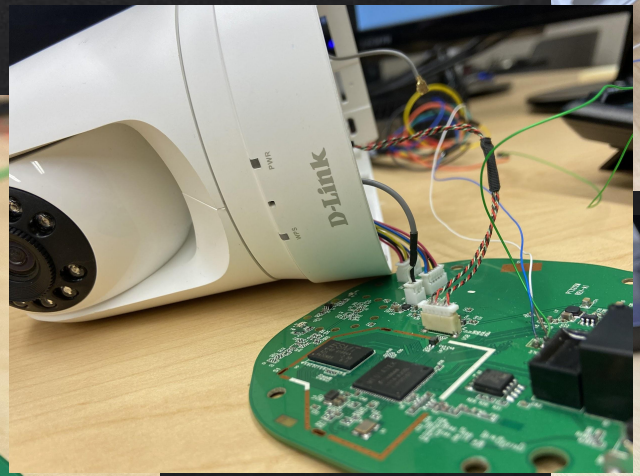
- ✘ Connect the UART hardware to the computer
- ✘ Confirm whether or not the device is connected
- ✘ Setserial
- ✘ chmod 666 /dev/ttyUSB0”
- ✘ cu –l /dev/ttyUSB0 –s 115200”

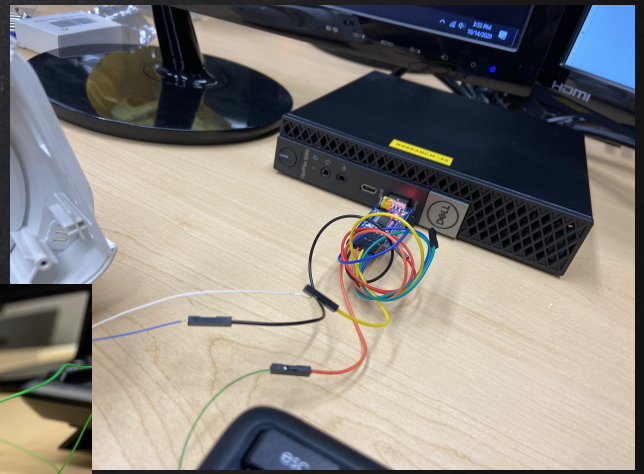
# D-Link DCS-5030L Security Camera

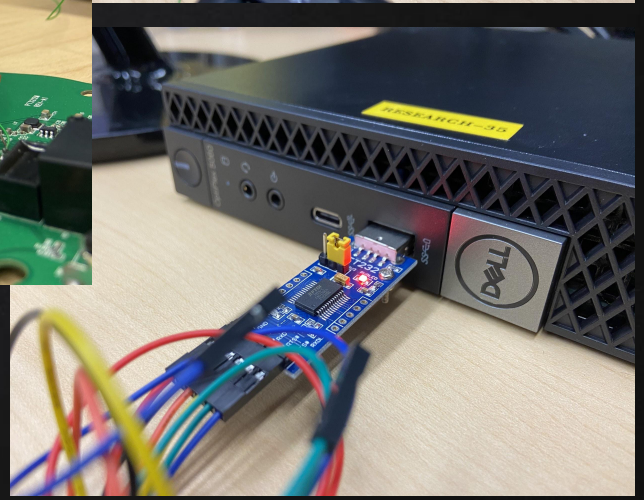
Accessing Backend Linux Systems via UART

✘ F232 UART Device Connection



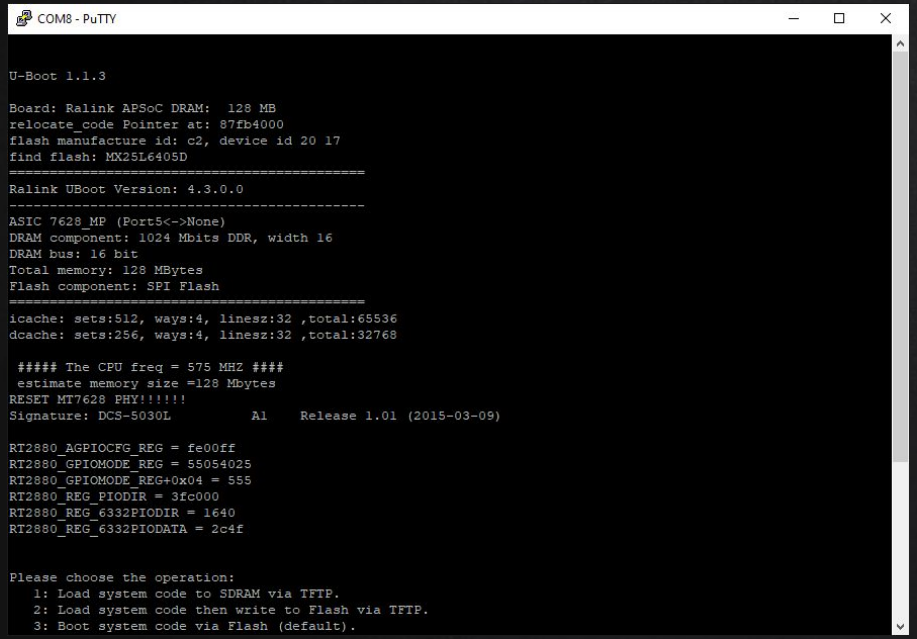



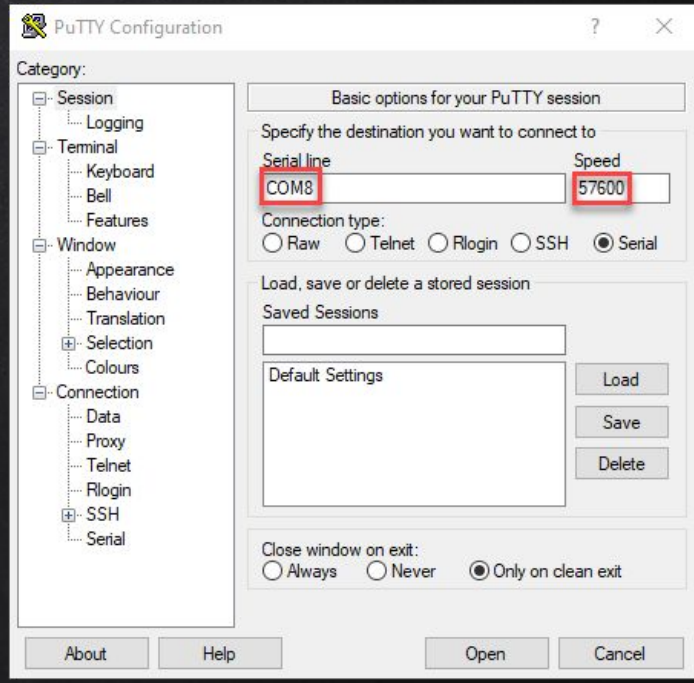



# Serial Communication using Putty

- ✘ COM8, F232 UART device location
- ✘ 57600, Baud rate of D-Link Smart Cameras

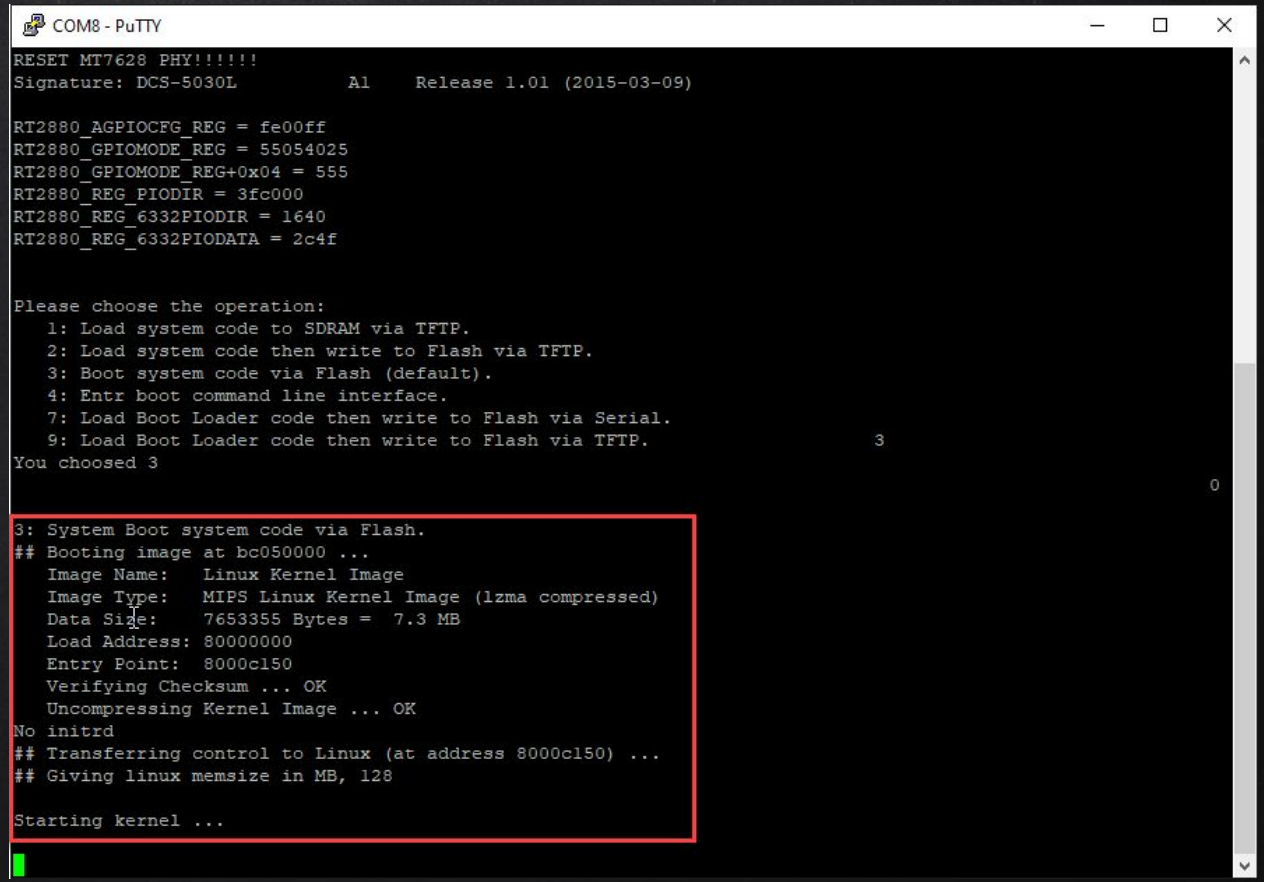



dlinkSerial.log

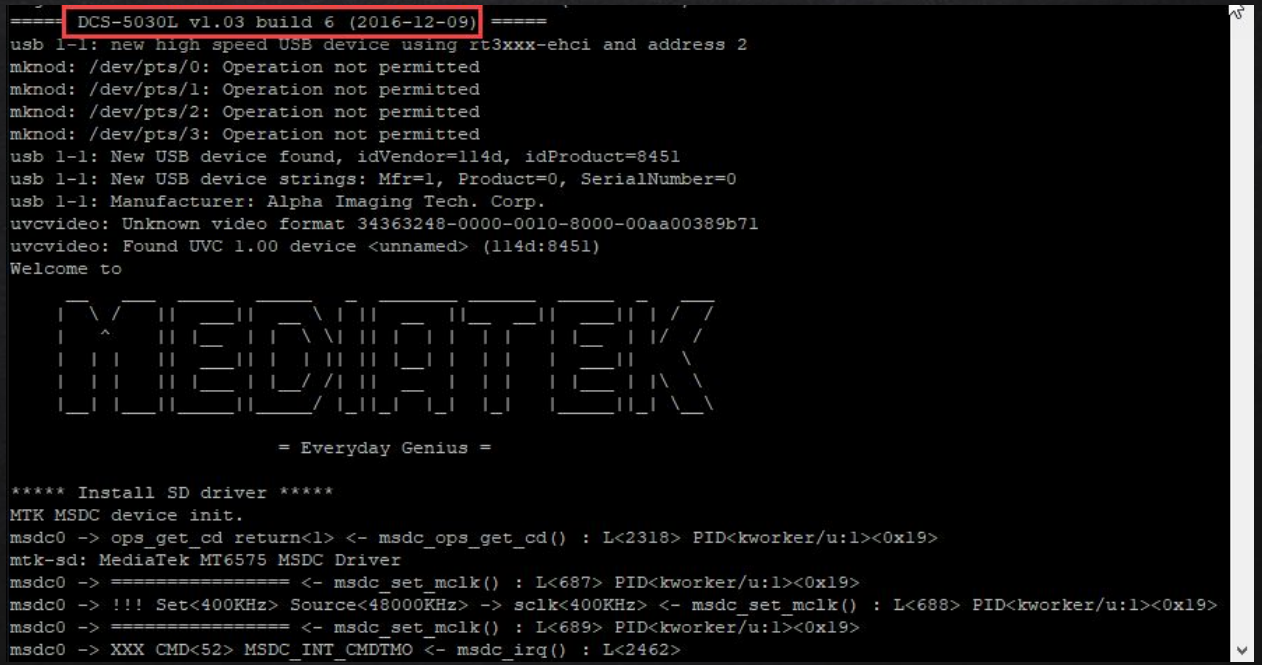
# Bootloader

Booting System via Flash, opening MIPS Linux Kernel Image



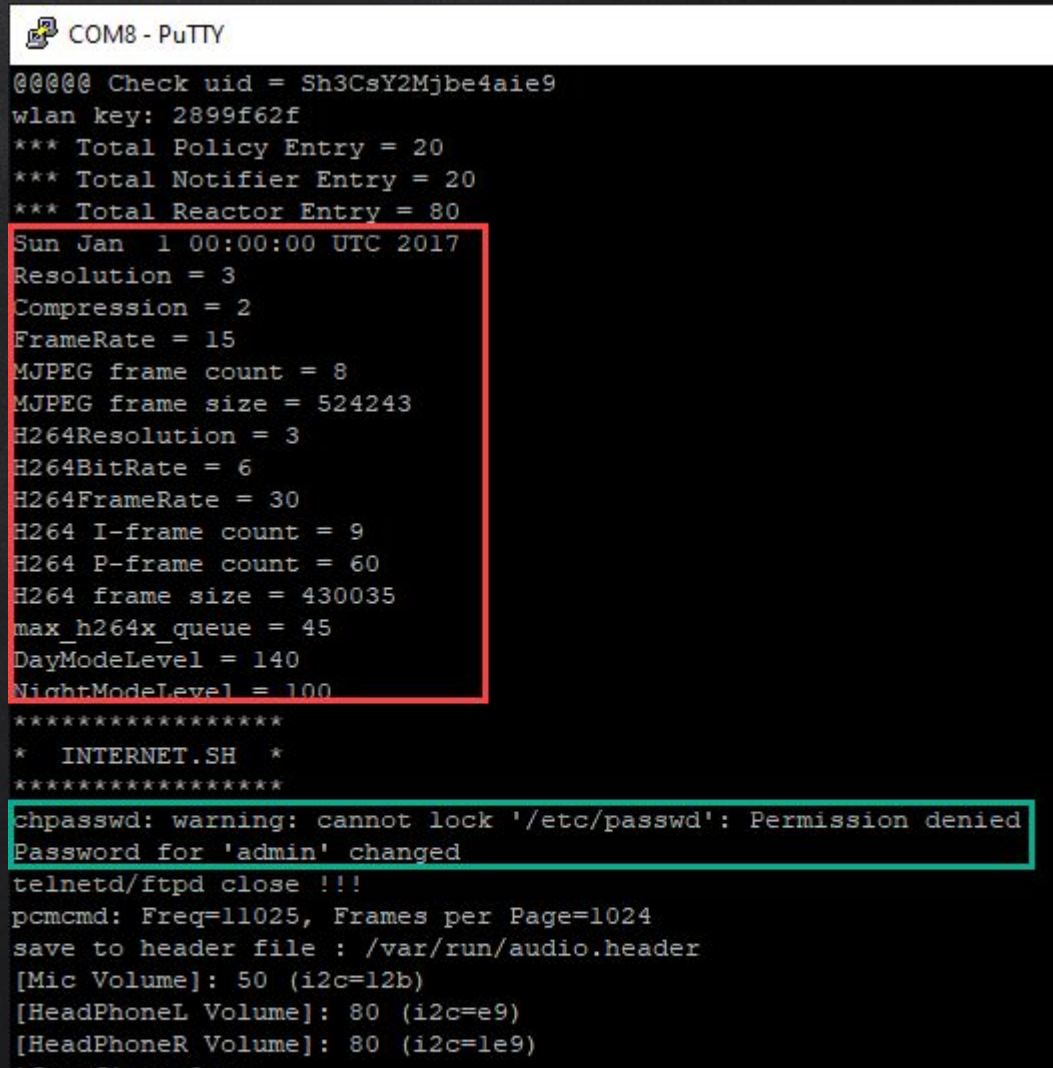
# Success!

## Device Bootloader

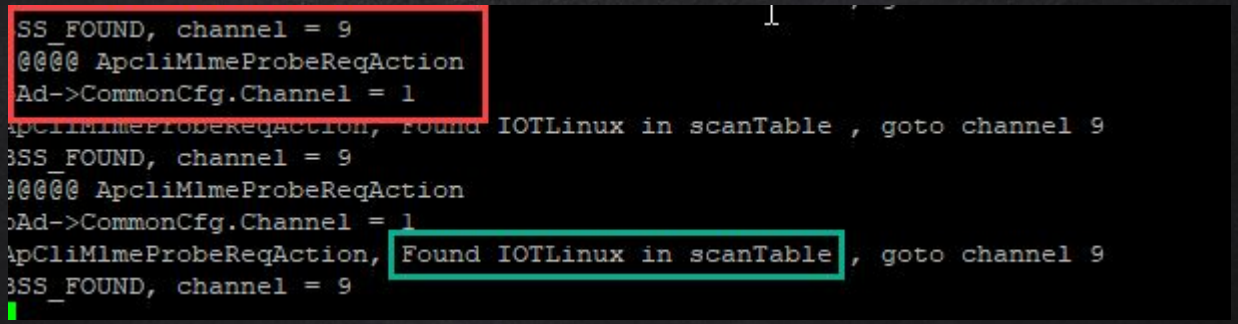


# Metadata Revealed on First Login

- ✘ Saved JPEG images, Saved MP4 video settings
- ✘ Files appear to be cached locally until Reset Button is pushed
- ✘ Admins password changed automatically after login, cannot elevate to sudo once logged in, but resets to [u:admin p: ] after every boot, leaving root shell vulnerable

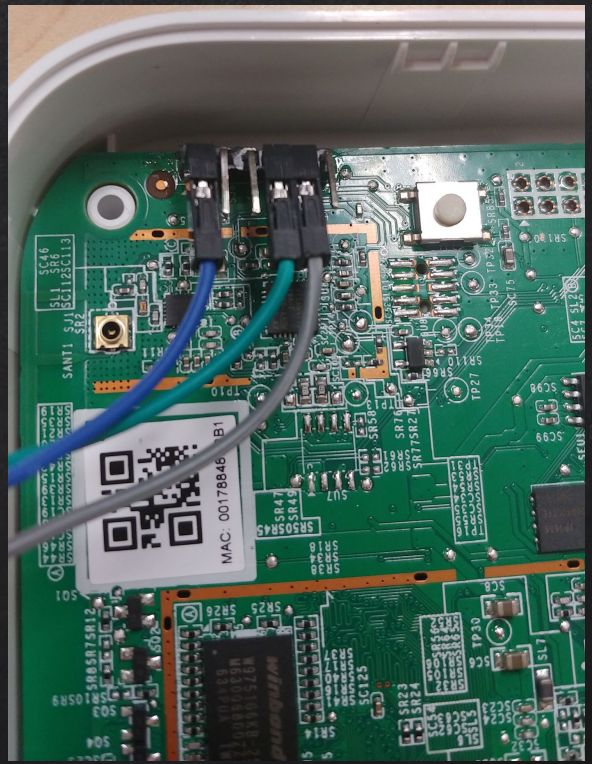


# Autorunning FS Scripts without Shell Input



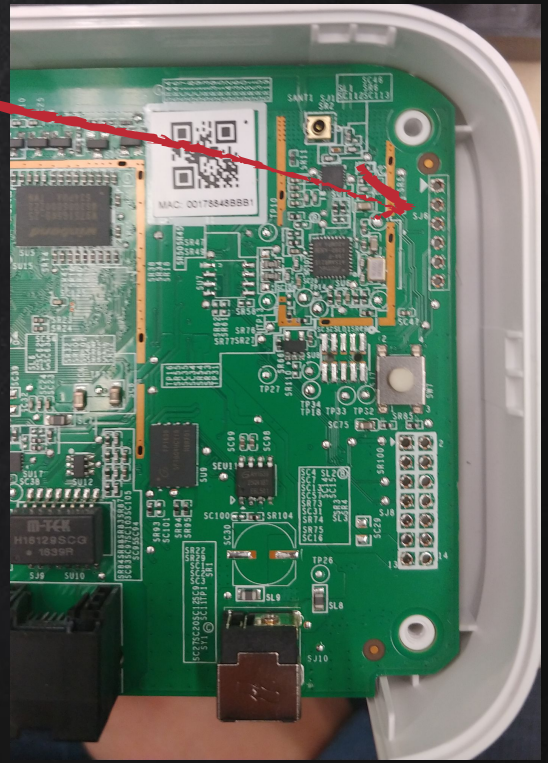

- ✘ BSS_FOUND/BSS_NOT_FOUND showing the radio antenna actively searching for previously established connections, even when antenna is unplugged from board
- ✘ Found IOTLinux, showing that previously connected WiFi network data/IP tables are stored internally. Active connections were disabled during this serial session, meaning D-Link could not have scanned for available SSIDs

# Philips Hue Bridge


# Philips Hue Bridge – Accessing through Hardware Hacking

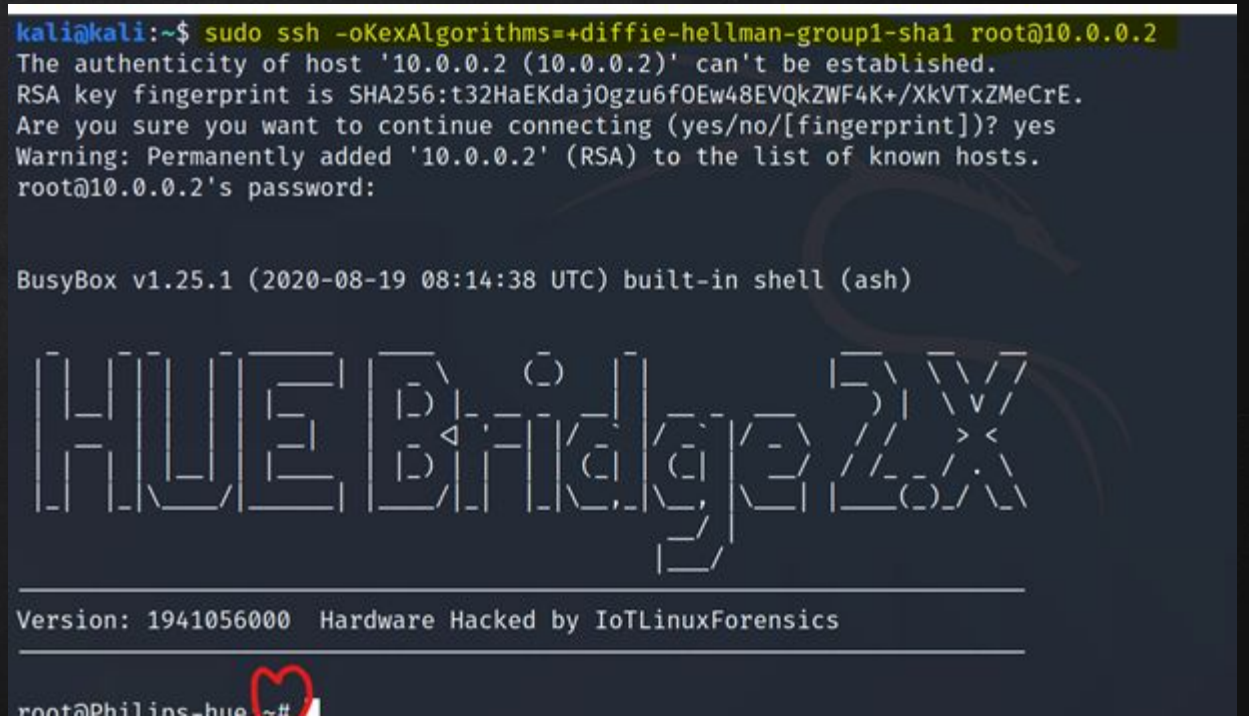
- ✘ F232 UART device location
- ✘ 115200 baud rate
- ✘ Shorting contact to bypass bootloader
- ✘ Accessing root shell
- ✘ Using dropbear to remotely connect to root shell



# Splash Screen w/ SSH

- ✘ Uses outdated algorithm, makes accessing system much easier
- ✘ Connected at 10.0.0.2/24
- ✘ Access shell using default user and password

Device Bootloader



# Getting OS Information

- ✘ cat /etc/*release; uname –a
- ✘ Will list the distro information and version of Linux

```
root@Philips-hue:/# cat /etc/*release
DISTRIB_ID='OpenWrt'
DISTRIB_RELEASE='Chaos Calmer'
DISTRIB_REVISION='r46875'
DISTRIB_CODENAME='chaos_calmer'
DISTRIB_TARGET='ar71xx/generic'
DISTRIB_DESCRIPTION='OpenWrt Chaos Calmer 15.05.1'
DISTRIB_TAINTS='no-all busybox override'
root@Philips-hue:/# uname -a
Linux Philips-hue 4.4.60 #1 Wed Aug 19 08:23:25 UTC 2020 mips GNU/Linux
root@Philips-hue:/#
```

# Network information

- ✘ Ifconfig –a
- ✘ Lists network location for Remote access (Important for quarantine)

```
root@Philips-hue:/# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:03:7F:11:20:CE
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Interrupt:4

eth1      Link encap:Ethernet  HWaddr 00:17:88:48:BB:B1
          inet addr:10.0.0.2  Bcast:10.0.0.255  Mask:255.255.255.0
          inet6 addr: fe80::217:88ff:fe48:bbb1/64 Scope:Link
          inet6 addr: fd6a:6429:8e27::1/60 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:729238 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1109305 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:73315728 (69.9 MiB)  TX bytes:295099822 (281.4 MiB)
          Interrupt:5

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:1480233 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1480233 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:64846118 (61.8 MiB)  TX bytes:64846118 (61.8 MiB)

root@Philips-hue:/#
```

Device Boo

# Checking for Mount points

- ✘ mount
- ✘ Lists the location of file to image

```
root@Philips-hue:/# mount
/dev/root on /rom type squashfs (ro,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,noatime)
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,noatime)
tmpfs on /tmp type tmpfs (rw,nosuid,nodev,noatime)
/dev/ubi1_1 on /overlay type ubifs (rw,noatime)
overlayfs:/overlay on / type overlay (rw,noatime,lowerdir=/,upperdir=/overlay/upper,workdir=/overlay/work)
tmpfs on /dev type tmpfs (rw,nosuid,relatime,size=512k,mode=755)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,mode=600)
debugfs on /sys/kernel/debug type debugfs (rw,noatime)
root@Philips-hue:/#
```

# Listing Root Directory

- ✘ Ls –al /
- ✘ Listing all directories in root Directory
- ✘ Timestamps and access permissions

```
root@Philips-hue:/# ls -al
drwxrwxrwx    1 root     root           480 Nov 11 20:34 .
drwxrwxrwx    1 root     root           480 Nov 11 20:34 ..
drwxr-xr-x    2 root     root           777 Aug 28 11:38 bin
drwxr-xr-x    4 root     root          1280 Oct 14 21:09 dev
drwxr-xr-x    1 root     root           560 Aug 28 11:38 etc
drwxr-xr-x    1 root     root           432 Feb 27  2020 home
-rwxr-xr-x    1 root     root            78 Aug 19 07:43 init
drwxr-xr-x   11 root     root           854 Aug 28 11:38 lib
drwxr-xr-x    2 root     root             3 Aug 19 08:12 mnt
drwxr-xr-x    4 root     root           360 Feb 27  2020 overlay
dr-xr-xr-x   64 root     root             0 Jan  1  1970 proc
drwxr-xr-x   17 root     root           247 Aug 28 11:38 rom
drwxr-xr-x    1 root     root           224 Nov  8 18:41 root
drwxr-xr-x    2 root     root           702 Aug 28 11:38 sbin
dr-xr-xr-x   11 root     root             0 Jan  1  1970 sys
-rw-r--r--    1 root     root             0 Oct 14 21:33 temp
drwxrwxrwt   20 root     root           660 Nov 11 10:53 tmp
-rwxr-xr-t    1 root     root            20 Oct 21 19:47 tmp.gz
drwxr-xr-x    7 root     root            89 Aug 28 11:37 usr
lrwxrwxrwx    1 root     root             4 Aug 28 11:38 var -> /tmp
drwxr-xr-x    4 root     root           230 Aug 28 11:38 www
root@Philips-hue:/#
```

# Listing Active Services

- ✘ Netstat –tulpn
- ✘ Showing open ports and services being used by the device while running

```
root@Philips-hue:/# netstat -tulpn
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:9001          0.0.0.0:*               LISTEN      1241/ipbridge
tcp        0      0 127.0.0.1:9002          0.0.0.0:*               LISTEN      1285/behaviord
tcp        0      0 127.0.0.1:9003          0.0.0.0:*               LISTEN      1296/clipd
tcp        0      0 0.0.0.0:3245            0.0.0.0:*               LISTEN      1264/nginx.conf -g
tcp        0      0 127.0.0.1:3246          0.0.0.0:*               LISTEN      1296/clipd
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      1264/nginx.conf -g
tcp        0      0 0.0.0.0:8083            0.0.0.0:*               LISTEN      1264/nginx.conf -g
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      989/dropbear
tcp        0      0 0.0.0.0:1338            0.0.0.0:*               LISTEN      1241/ipbridge
tcp        0      0 0.0.0.0:1339            0.0.0.0:*               LISTEN      1241/ipbridge
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN      1264/nginx.conf -g
tcp        0      0 0.0.0.0:1883            0.0.0.0:*               LISTEN      1033/mosquitto
tcp        0      0 :::50051                :::*                    LISTEN      1241/ipbridge
tcp        0      0 :::8080                 :::*                    LISTEN      1344/hk_hap
tcp        0      0 :::80                   :::*                    LISTEN      1264/nginx.conf -g
tcp        0      0 :::8083                 :::*                    LISTEN      1264/nginx.conf -g
tcp        0      0 :::22                   :::*                    LISTEN      989/dropbear
tcp        0      0 :::443                  :::*                    LISTEN      1264/nginx.conf -g
tcp        0      0 :::1883                 :::*                    LISTEN      1033/mosquitto
udp        0      0 0.0.0.0:46611           0.0.0.0:*                           1069/mdnsd
udp        0      0 0.0.0.0:1900            0.0.0.0:*                           1241/ipbridge
udp        0      0 0.0.0.0:5353            0.0.0.0:*                           1069/mdnsd
udp        0      0 :::5353                 :::*                                1069/mdnsd
udp        0      0 :::48108                :::*                                1069/mdnsd
root@Philips-hue:/# @sS
```

# Busybox

```
root@Philips-hue:/# ls -al bin
drwxr-xr-x    2 root     root           777 Aug 28 11:38 .
drwxrwxrwx    1 root     root           480 Nov 11 20:34 ..
lrwxrwxrwx    1 root     root             7 Aug 28 11:38 ash → busybox
-rwxr-xr-x    1 root     root           265 Aug 19 07:43 board_detect
-rwxr-xr-x    1 root     root        312640 Aug 19 08:14 busybox
lrwxrwxrwx    1 root     root             7 Aug 28 11:38 cat → busybox
lrwxrwxrwx    1 root     root             7 Aug 28 11:38 chgrp → busybox
lrwxrwxrwx    1 root     root             7 Aug 28 11:38 chmod → busybox
lrwxrwxrwx    1 root     root             7 Aug 28 11:38 chown → busybox
-rwxr-xr-x    1 root     root          3311 Aug 19 07:43 config_generate
lrwxrwxrwx    1 root     root             7 Aug 28 11:38 cp → busybox
lrwxrwxrwx    1 root     root             7 Aug 28 11:38 date → busybox
lrwxrwxrwx    1 root     root             7 Aug 28 11:38 dd → busybox
lrwxrwxrwx    1 root     root             7 Aug 28 11:38 df → busybox
lrwxrwxrwx    1 root     root             7 Aug 28 11:38 dmesg → busybox
lrwxrwxrwx    1 root     root             7 Aug 28 11:38 echo → busybox
lrwxrwxrwx    1 root     root             7 Aug 28 11:38 egrep → busybox
lrwxrwxrwx    1 root     root             7 Aug 28 11:38 false → busybox
lrwxrwxrwx    1 root     root             7 Aug 28 11:38 fgrep → busybox
lrwxrwxrwx    1 root     root             7 Aug 28 11:38 fsync → busybox
lrwxrwxrwx    1 root     root             7 Aug 28 11:38 grep → busybox
lrwxrwxrwx    1 root     root             7 Aug 28 11:38 gunzip → busybox
lrwxrwxrwx    1 root     root             7 Aug 28 11:38 gzip → busybox
-rwxr-xr-x    1 root     root          1550 Aug 19 07:43 ipcalc.sh
lrwxrwxrwx    1 root     root             7 Aug 28 11:38 kill → busybox
lrwxrwxrwx    1 root     root             7 Aug 28 11:38 ln → busybox
lrwxrwxrwx    1 root     root             7 Aug 28 11:38 lock → busybox
lrwxrwxrwx    1 root     root             7 Aug 28 11:38 login → busybox
-rwxr-xr-x    1 root     root           424 Aug 19 07:43 login.sh
lrwxrwxrwx    1 root     root             7 Aug 28 11:38 ls → busybox
```

# /etc

```
root@Philips-hue:/# ls -al /etc
drwxr-xr-x    1 root     root           560 Aug 28 11:38 .
drwxrwxrwx    1 root     root           480 Nov 11 20:34 ..
lrwxrwxrwx    1 root     root             7 Aug 28 11:38 TZ → /tmp/TZ
drwxr-xr-x    2 root     root            43 Aug 28 11:38 avahi
-rwxr-xr-x    1 root     root           768 Nov  4 20:14 banner
-rw-r--r--    1 root     root           408 Aug 19 07:43 banner.failsafe
drwxr-xr-x    2 root     root            47 Aug 28 11:38 ca-certificates
drwxr-xr-x    2 root     root           853 Aug 28 11:38 clipd
drwxr-xr-x    1 root     root           768 Nov  4 20:37 config
drwxr-xr-x    2 root     root             3 Aug 19 08:12 crontabs
-rw-r--r--    1 root     root            76 Aug 19 08:12 device_info
-rw-r--r--    1 root     root          6449 Aug 19 07:43 diag.sh
drwx------    1 root     root           392 Feb 27  2020 dropbear
-rw-r--r--    1 root     root           352 Aug 19 08:11 firewall.user
lrwxrwxrwx    1 root     root            10 Aug 28 11:38 fstab → /tmp/fstab
-rwxr-xr-x    1 root     root            70 Aug 28 11:36 fw_env.config
-rw-r--r--    1 root     root           140 Aug 28 11:38 group
-rw-r--r--    1 root     root            20 Aug 19 07:43 hosts
-rw-r--r--    1 root     root           326 Aug 19 08:11 hotplug-preinit.json
drwxr-xr-x    6 root     root            66 Aug 28 11:38 hotplug.d
-rw-r--r--    1 root     root          1657 Aug 19 08:11 hotplug.json
drwxr-xr-x    2 root     root            61 Aug 28 11:38 hue-diagcd
drwxr-xr-x    2 root     root           436 Aug 28 11:38 init.d
-rwxr-xr-x    1 root     root           107 Aug 28 11:36 inittab
drwxr-xr-x    3 root     root            34 Aug 28 11:38 iot-field-test
drwxr-xr-x    2 root     root            70 Aug 28 11:38 modules-boot.d
drwxr-xr-x    2 root     root           328 Aug 28 11:38 modules.d
drwxr-xr-x    2 root     root            37 Aug 28 11:38 mosquitto
lrwxrwxrwx    1 root     root            12 Aug 28 11:38 mtab → /proc/mounts
drwxr-xr-x    2 root     root           290 Aug 28 11:38 nginx
drwxr-xr-x    2 root     root            34 Aug 28 11:38 ntpd
-rw-r--r--    1 root     root           234 Aug 19 08:12 openwrt_release
-rw-r--r--    1 root     root             8 Aug 19 08:12 openwrt_version
```

# Custom Firewall Rules

```
root@Philips-hue:/# cat /etc/config/firewall

config defaults
        option input 'REJECT'
        option output 'ACCEPT'
        option forward 'REJECT'
        option synflood_protect '1'

config zone 'lan'
        option name 'lan'
        list network 'lan'
        option input 'REJECT'
        option output 'ACCEPT'
        option forward 'REJECT'
        option masq '1'
        option mtu_fix '1'

config rule 'clip'
        option name 'Allow-CLIP'
        option src 'lan'
        option proto 'tcp'
        option dest_port '80'
        option target 'ACCEPT'
        option family 'ipv4'

config rule 'factory'
        option name 'Allow-Factory'
        option src 'lan'
        option proto 'tcp'
        option dest_port '30000'
        option target 'ACCEPT'
        option family 'ipv4'
```

Root user has read and write permissions to change any settings in the firewall config files

```
root@Philips-hue:~# cat /etc/firewall.user
# This file is interpreted as shell script.
# Put your custom iptables rules here, they will
# be executed with each firewall (re-)start.

# Internal uci firewall chains are flushed and recreated on reload, so
# put custom rules into the root chains e.g. INPUT or FORWARD or into the
# special user chains, e.g. input_wan_rule or postrouting_lan_rule
root@Philips-hue:~#
```

```
root@Philips-hue:~# cat /etc/group
root:x:0:
daemon:x:1:
adm:x:4:
mail:x:8:
audio:x:29:
www-data:x:33:
ftp:x:55:
users:x:100:
network:x:101:
nogroup:x:65534:
mosquitto:x:200:
root@Philips-hue:~#
```

kali@kali: ~

File Actions Edit View Help

```
root@Philips-hue:/etc# cat /etc/passwd
root:x:0:0:root:/root:/bin/ash
daemon:*:1:1:daemon:/var:/bin/false
ftp:*:55:55:ftp:/home/ftp:/bin/false
network:*:101:101:network:/var:/bin/false
nobody:x:65534:65534:nobody:/var:/bin/false
mosquitto:x:200:200:mosquitto:/var/run/mosquitto:/bin/false
root@Philips-hue:/etc# sw
```

# Imaging on the Linux side

```
root@Philips-hue:/# ls
bin         etc         init        mnt         proc        root        sys         test.tar.gz  tmp.gz      var
dev         home        lib         overlay     rom         sbin        temp        tmp          usr         www
root@Philips-hue:/# nc 10.0.0.3 2222 < test.tar.gz
```

```
Select Command Prompt - nc  -p 2222 -l
Microsoft Windows [Version 10.0.18362.1082]
(c) 2019 Microsoft Corporation. All rights reserved.

H:\>cd Desktop

H:\Desktop>cd netcat

H:\Desktop\netcat>nc -p 2222 -l > PhilipsImage.tar.gz
```

Saving the result to our target system

The result of the compressed tar will be something similar to what is listed below:

| Name | Size | Packed Size | Modified | Mode | User | Group | Symbolic Link | Hard Link | Folders | Files |
|---|---|---|---|---|---|---|---|---|---|---|
| bin | 326 467 | 328 192 | 2020-08-28 07:38 | drwxr-xr-x | root | root | | | 0 | 58 |
| dev | 20 | 0 | 2020-10-14 17:09 | drwxr-xr-x | root | root | | | 4 | 62 |
| etc | 556 644 | 606 720 | 2020-08-28 07:38 | drwxr-xr-x | root | root | | | 35 | 199 |
| home | 351 773 | 378 880 | 2020-02-27 12:55 | drwxr-xr-x | root | root | | | 20 | 135 |
| lib | 1 707 010 | 1 741 312 | 2020-08-28 07:38 | drwxr-xr-x | root | root | | | 12 | 135 |
| mnt | 0 | 0 | 2020-08-19 04:12 | drwxr-xr-x | root | root | | | 0 | 0 |
| overlay | 292 237 | 317 440 | 2020-02-27 12:57 | drwxr-xr-x | root | root | | | 21 | 168 |
| proc | 53 329 | 0 | | dr-xr-xr-x | root | root | | | 1 525 | 18 692 |
| rom | 29 892 044 | 30 207 488 | 2020-08-28 07:38 | drwxr-xr-x | root | root | | | 94 | 1 264 |
| root | 0 | 0 | 2020-08-19 04:12 | drwxr-xr-x | root | root | | | 0 | 0 |
| sbin | 320 105 | 326 656 | 2020-08-28 07:38 | drwxr-xr-x | root | root | | | 0 | 44 |
| sys | 4 128 | 4 096 | 1969-12-31 20:00 | dr-xr-xr-x | root | root | | | 6 | 2 |
| init | 78 | 512 | 2020-08-19 03:43 | -rwxr-xr-x | root | root | | | | |

# Challenge(s)

- ✘ COVID-19 Lockdown
  - Leahy Center Locked down from March – late September
- ✘ Smaller Team
  - Ali, Joseph, Austin, Sid
  - Zero previous IoT Experience!
- ✘ Lack of resources
  - Cloud vs. On-Board

# What Comes Next?

- ✘ IoT File Systems
- ✘ Detailed forensic acquisitions
- ✘ Automated forensics
- ✘ IoT Forensics Toolkit

# THANKS!

## Questions/Suggestions?

#hadi-linuxforensics-iot on the OSDFCon Discord Server

Ali Hadi, @binaryz0ne via Twitter
Austin Grupposo, via LinkedIn
Joseph McCormack, via LinkedIn