

# IOT LINUX FORENSICS



## CHAMPLAIN COLLEGE Leahy Center for Digital Forensics & Cybersecurity



#### Ali Hadi,

Assistant Professor and Researcher at Champlain College.

#### Joseph McCormack,

HELLO!

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?



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



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



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

**X** They can be identified using their signature (still under research)



#### an exercise is used on exect devises due to lissited concer

Compression is used on most devices due to limited space:

- 🗶 Gzip
- × LZMA
- X Zlib
- **Χ** Ζίρ



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



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

#### Get root...



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



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



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



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





- 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

# loT Catalog (p1) ...

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

# loT Catalog (p2) ...

Portal	B81AO1BUS	Model No.	*	Facebook	Untouched	*	YES	*		*		*		*		*
Caseta Wireless Dimmer Kit with Smar	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.	- Ju	irky + General Electr	i Untouched	Ŧ	NO	*		*		*		*		*
Samsung Galaxy Tab A	R52M80B71CK	Serial No.	*	Samsung	Untouched	Ŧ	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	Ŧ	NO			*				*		*
Beam Alert	ZMD12IGC6000232	Serial No.	*	Zmodo	Untouched	*	YES	*		*		*		*		*
Greet Smart WiFi Doorbell	ZMD12EA48000087	Serial No.	*	Zmodo	Untouched	Ŧ	YES	*		*		*		*		*
Cujo	PRODUCT MISSING	PRODUCT MISSING	*	Cujo	Untouched	Ŧ		*		*				*		*
Hue Personal Lighting System	MP051503490184	Serial No.	*	Philips	Untouched	*	YES	-		*		*		*		*
Hue Personal Lighting System (White St	arter Kit)	Serial/Model No. Not Found		Philips	Being Researched/Worked On	Ŧ	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	Ŧ	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	Ŧ	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	Ŧ	YES	-		*		*		*		*
D-Link Wi-Fi Camera (Black)	RZZN1GC005522	Serial No.	*	D-Link	Untouched	*	YES	-		*		*		*		*
Lorex LCD monitor and recorder	WA0216103707	Serial No.	*	Flir	Untouched	Ŧ	NO	-		Ŧ		*		*		Ŧ
Lorex HD WiFi Security Camera	PRODUCT MISSING	PRODUCT MISSING		Flir	Untouched	Ŧ	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	Ŧ	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	Ŧ	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		Ŧ	-	•	T

# Surface Mapping (Ports & Services)

Device Name	Device Name MAC Address		Services	Operating System	Linux Access Method	
Canary USB100UK	D8:42:E2:03:08:68	none				
Samsung SmartCam HD Pro (Chinese)	Innsung SmartCam HD Pro hinese) 00:16:6C:85:04:76		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	IwIP 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)	<u>89</u> 2		1220		-22	
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	·			22 <sup>1010</sup>	
Canary Pro	ury 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

- **X** Installing Python
- X Installing Pyserial
- **X** Baudrate.py by DevTTYSO



#### 3. SETTING UP SERIAL PORTS IN LINUX

- X Connect the UART hardware to the computer
- X Confirm whether or not the device is connected
- **X** 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

X

#### SERIAL COMMUNICATION USING PUTTY

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

B COM8 - PuTTY	-	×
		-
U-Boot 1.1.3		
Board: Ralink APSoC DRAM: 128 MB relocate_code Pointer at: 87fb4000 flash manufacture id: c2, device id 20 17 find flash: MX25L6405D		
Ralink UBoot Version: 4.3.0.0		
ASIC 7628 MP (Port5<->None) DRAM component: 1024 Mbits DDR, width 16 DRAM bus: 16 bit Total memory: 128 MBytes Flash component: SPI Flash		
icache: sets:512, ways:4, linesz:32 ,total:65536 dcache: sets:256, ways:4, linesz:32 ,total:32768		
<pre>##### The CPU freq = 575 MHZ #### estimate memory size =128 Mbytes RESET MT7628 RHY!!!!! Signature: DCS-5030L Al Release 1.01 (2015-03-09)</pre>		
RT2880_AGPIOCFG_REG = fe00ff		
RT2880_GPIOMODE_REG = 55054025 RT280_GPIOMODE_REG+0x04 = 555 RT2880_REC_PIODIR = 37c000 RT2880_REC_6332PIODIR = 1640 RT2880_REG_6332PIODATA = 2c4f		
Please choose the operation:		

- Session	Basic options for your PuTTY session					
- Logging - Terminal - Keyboard - Bell - Features - Window - Mppearance - Behaviour - Translation	Specify the destination you w Serial line COM8 Connection type: O Raw O Telnet O Ric Load, save or delete a stored Saved Sessions	ant to connect to Speed 57600 Ingin O SSH   Seria session				
Selection     Colours     Connection     Data     Proxy     Telnet	Default Settings	Load Save Delete				
Rlogin ⊪-SSH Serial	Close window on exit: O Always O Never   Only on clean exit					
AL	-	0				

X

RepuTTY Configuration



3: Boot system code via Flash (default).

2: Load system code then write to Flash via TFTP.

#### BOOTLOADER

Booting System via Flash, opening MIPS Linux Kernel Image

				 	 	05520
RESET MT7628 PH	IY!!!!!					
Signature: DCS-	-5030L A1	Release 1.01 (2	2015-03-09)			
RT2880 AGPIOCEG	G REG = fe00ff					
RT2880 GPIOMODE	REG = 55054025					
RT2880 GPIOMODE	E = 555					
RT2880 REG PIOL	$\overline{DIR} = 3fc000$					
RT2880 REG 6332	PIODIR = 1640					
RT2880_REG_6332	PIODATA = 2c4f					
ni						
l. Lond	ne operation:	TIN TETD				
1: Load syst	em code to SDRAM	Via Ifif.				
2: Load syst	em code then writ	e co Flash via IFI	5.			
3: Boot syst	em code via Flash	(default).				
4. Fatr boot	command line int	eriace.				
1. Dirot 2000						
7: Load Boot	Loader code then	write to Flash via	a Serial.			
7: Load Boot 9: Load Boot	: Loader code then : Loader code then	write to Flash via write to Flash via	a Serial. a TFTP.			
7: Load Boot 9: Load Boot You choosed 3	: Loader code then : Loader code then	write to Flash via write to Flash via	a Serial. a TFTP.			
7: Load Boot 9: Load Boot You choosed 3	: Loader code then : Loader code then	write to Flash via write to Flash via	a Serial. a TFTP.			
7: Load Boot 9: Load Boot You choosed 3 3: System Boot	: Loader code then : Loader code then system code via F	write to Flash via write to Flash via lash.	a Serial. a TFTP.			
7: Load Boot 9: Load Boot You choosed 3 3: System Boot ## Booting imag	: Loader code then : Loader code then system code via F re at bc050000	write to Flash via write to Flash via lash.	a Serial. a TFTP.			
7: Load Boot 9: Load Boot You choosed 3 3: System Boot ## Booting imag Image Name:	: Loader code then : Loader code then system code via F ge at bc050000 Linux Kernel Im	write to Flash via write to Flash via lash. age	a Serial. a TFTP.			
7: Load Boot 9: Load Boot You choosed 3 3: System Boot ## Booting image Image Name: Image Type:	: Loader code then : Loader code then system code via F ge at bc050000 Linux Kernel Im MTPS Linux Kern	write to Flash via write to Flash via lash. age el Image (1zma comm	a Serial. a TFTP.			
7: Load Boot 9: Load Boot You choosed 3 3: System Boot ## Booting imag Image Name: Image Type: Data Size:	: Loader code then : Loader code then system code via F ge at bc050000 Linux Kernel Im MIPS Linux Kern 7653355 Bytes =	write to Flash via write to Flash via lash. age el Image (lzma comp 7.3 MB	a Serial. a TFTP. pressed)			
<ul> <li>3: System Boot</li> <li>4: Load Boot</li> <li>9: Load Boot</li> <li>9: Load Boot</li> <li>3: System Boot</li> <li>3: System Boot</li> <li>4: Booting image</li> <li>Image Name:</li> <li>Image Type:</li> <li>Data Side:</li> <li>Load Address</li> </ul>	: Loader code then : Loader code then system code via F ge at bc050000 Linux Kernel Im MIPS Linux Kern 7653355 Bytes = : 8000000	write to Flash via write to Flash via lash. age el Image (lzma comp 7.3 MB	a Serial. a TFTP. pressed)			
<ul> <li>3: System Boot</li> <li>9: Load Boot</li> <li>9: Load Boot</li> <li>9: Load Boot</li> <li>9: Load Boot</li> <li>3: System Boot</li> <li>4# Booting imag</li> <li>Image Name:</li> <li>Image Type:</li> <li>Data Sige:</li> <li>Load Address</li> <li>Entry Point:</li> </ul>	<pre>System code then System code via F ge at bc050000 Linux Kernel Im MIPS Linux Kern 7653355 Bytes = St 80000000 8000c150</pre>	write to Flash via write to Flash via lash. age el Image (lzma comp 7.3 MB	a Serial. a TFTP. pressed)			
<ul> <li>3: System Boot</li> <li>4# Booting image Image Name: Image Type: Data Size: Load Address Entry Point: Verifying Cf</li> </ul>	<pre>System code then System code via F te at bc050000 Linux Kernel Im MIPS Linux Kern 7653355 Bytes = St 80000000 8000c150 bccksum OK</pre>	write to Flash via write to Flash via lash. age el Image (lzma comp 7.3 MB	a Serial. a TFTP. pressed)			
3: System Boot 9: Load Boot 9: Load Boot You choosed 3 ## Booting imag Image Name: Image Type: Data Side: Load Address Entry Point: Verifying Ch Uncompression	<pre>System code then Loader code then system code via F ge at bc050000 Linux Kernel Im MIPS Linux Kern 7653355 Bytes = s: 80000000 80000150 becksum OK of Kernel Image</pre>	write to Flash via write to Flash via lash. age el Image (lzma comp 7.3 MB . OK	a Serial. a TFTP. pressed)			
3: System Boot 9: Load Boot 9: Load Boot You choosed 3 3: System Boot ## Booting imag Image Name: Image Type: Data Side: Load Address Entry Point: Verifying CP Uncompressir No initrd	<pre>System code then Loader code then system code via F ge at bc050000 Linux Kernel Im MIPS Linux Kern 7653355 Bytes = s: 80000000 8000c150 becksum OK ng Kernel Image</pre>	write to Flash via write to Flash via lash. age el Image (lzma comp 7.3 MB . OK	a Serial. a TFTP. pressed)			
3: System Boot 9: Load Boot 9: Load Boot 9: Load Boot 3: System Boot 1 mage Name: Image Name: Image Type: Data Side: Load Address Entry Point: Verifying Ct Uncompressir No initrd ## Transferring	<pre>System code then Loader code then System code via F ye at bc050000 Linux Kernel Im MIPS Linux Kern 7653355 Bytes = St 80000000 8000c150 mecksum OK ng Kernel Image a control to Linux</pre>	write to Flash via write to Flash via lash. age el Image (lzma comp 7.3 MB . OK	a Serial. a TFTP. pressed)			
3: System Boot 9: Load Boot 9: Load Boot You choosed 3 3: System Boot ## Booting imag Image Name: Image Type: Data Sige: Load Address Entry Point: Verifying Cf Uncompressir No initrd ## Transferring ## Giving Jinux	<pre>System code then Loader code then System code via F ge at bc050000 Linux Kernel Im MIPS Linux Kern 7653355 Bytes = S: 80000000 8000cl50 Becksum OK ag Kernel Image g control to Linux r memsize in MB l</pre>	write to Flash via write to Flash via lash. age el Image (lzma comp 7.3 MB . OK (at address 8000c)	a Serial. a TFTP. pressed) 150)			
<pre>3: System Boot 9: Load Boot 9: Load Boot 9: Load Boot 9: Load Boot 1: System Boot 1: System</pre>	<pre>System code then Loader code then System code via F ge at bc050000 Linux Kernel Im MIPS Linux Kern 7653355 Bytes = St 80000000 8000c150 hecksum OK ng Kernel Image g control to Linux t memsize in MB, 1</pre>	write to Flash via write to Flash via lash. age el Image (lzma comp 7.3 MB . OK (at address 8000c) 28	a Serial. a TFTP. pressed) 150)			
<pre>3: System Boot 9: Load Boot 9: Load Boot 9: Load Boot 9: Load Boot 1: System Boot 1: System Boot 1: System Boot 1: Image Name: 1: Image</pre>	<pre>System code then Loader code then System code via F ge at bc050000 Linux Kernel Im MIPS Linux Kern 7653355 Bytes = St 8000000 8000c150 mecksum OK ng Kernel Image g control to Linux t memsize in MB, l</pre>	write to Flash via write to Flash via lash. age el Image (lzma comp 7.3 MB . OK (at address 8000c: 28	a Serial. a TFTP. pressed) 150)			

#### SUCCESS! Device Bootloader

DCS-5030L vl.03 build 6 (2016-12-09) ===== usb 1-1: new high speed USB device using rt3xxx-ehci and address 2 mknod: /dev/pts/0: Operation not permitted mknod: /dev/pts/1: Operation not permitted mknod: /dev/pts/2: Operation not permitted usb 1-1: New USB device found, idVendor=114d, idProduct=8451 usb 1-1: New USB device strings: Mfr=1, Product=0, SerialNumber=0 usb 1-1: Manufacturer: Alpha Imaging Tech. Corp. uvcvideo: Unknown video format 34363248-0000-0010-8000-00aa00389b71 uvcvideo: Found UVC 1.00 device <unnamed> (114d:8451) Welcome to



= Everyday Genius =

\*\*\*\*\* Install SD driver \*\*\*\*\*

MTK MSDC device init.

msdc0 -> ops\_get\_cd return<1> <- msdc\_ops\_get\_cd() : L<2318> PID<kworker/u:1><0x19>

mtk-sd: MediaTek MT6575 MSDC Driver

msdc0 -> ============ <- msdc set mclk() : L<687> PID<kworker/u:1><0x19>

msdc0 -> !!! Set<400KHz> Source<48000KHz> -> sclk<400KHz> <- msdc set mclk() : L<688> PID<kworker/u:l><0x19>

msdc0 -> ============= <- msdc set mclk() : L<689> PID<kworker/u:1><0x19>

msdc0 -> XXX CMD<52> MSDC INT CMDTMO <- msdc irq() : L<2462>

#### 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

#### COM8 - PuTTY

```
00000 Check uid = Sh3CsY2Mjbe4aie9
wlan key: 2899f62f
*** Total Policy Entry = 20
   Total Notifier Entry = 20
*** Total Reactor Entry = 80
Sun Jan 1 00:00:00 UTC 2017
Resolution = 3
Compression = 2
FrameRate = 15
MJPEG frame count = 8
MJPEG frame size = 524243
H264Resolution = 3
H264BitRate = 6
H264FrameRate = 30
H264 I-frame count = 9
H264 P-frame count = 60
H264 frame size = 430035
max h264x queue = 45
DavModeLevel = 140
NightModeLevel = 100
   INTERNET.SH
chpasswd: warning: cannot lock '/etc/passwd': Permission denied
Password for 'admin' changed
telnetd/ftpd close !!!
pcmcmd: Freq=11025, Frames per Page=1024
save to header file : /var/run/audio.header
[Mic Volume]: 50 (i2c=12b)
[HeadPhoneL Volume]: 80 (i2c=e9)
[HeadPhoneR Volume]: 80 (i2c=le9)
```

#### AUTORUNNING FS SCRIPTS WITHOUT SHELL INPUT



- SS\_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
- X Shorting contact to bypass bootloader
- **X** Accessing root shell

shell

**X** Using dropbear to remotely connect to root



#### SPLASH SCREEN W/ SSH

- Uses outdated algorithm, makes accessing system much easier X
- Connected at 10.0.0.2/24 X
- Access shell using

default user and

kali@kali:~\$ sudo ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 root@10.0.0.2 The authenticity of host '10.0.0.2 (10.0.0.2)' can't be established. RSA key fingerprint is SHA256:t32HaEKdaj0gzu6f0Ew48EVQkZWF4K+/XkVTxZMeCrE. Are you sure you want to continue connecting (yes/no/[fingerprint])? yes Warning: Permanently added '10.0.0.2' (RSA) to the list of known hosts. root@10.0.0.2's password:

BusyBox v1.25.1 (2020-08-19 08:14:38 UTC) built-in shell (ash)



Version: 1941056000 Hardware Hacked by IoTLinuxForensics

#### **Device Bootloader**

password





#### GETTING OS INFORMATION

- ✗ cat /etc/\*release; uname −a
- X 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_CODENAME='chaos_calmer'
DISTRIB_TARGET='ar71xx/generic'
DISTRIB_TARGET='ar71xx/generic'
DISTRIB_DESCRIPTION='OpenWrt Chaos Calmer 15.05.1'
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)

lo

eth1

#### **Device Bod**

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

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

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:/#

#### CHECKING FOR MOUNT POINTS

× mount

X 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

 X Timestamps and access permissions

coot@Philips	s-hue	e:/# ls	-al
irwxrwxrwx	1	root	root
irwxrwxrwx	1	root	root
irwxr-xr-x	2	root	root
irwxr-xr-x	4	root	root
irwxr-xr-x	1	root	root
lrwxr-xr-x	1	root	root
-rwxr-xr-x	1	root	root
irwxr-xr-x	11	root	root
irwxr-xr-x	2	root	root
irwxr-xr-x	4	root	root
lr-xr-xr-x	64	root	root
irwxr-xr-x	17	root	root
irwxr-xr-x	1	root	root
irwxr-xr-x	2	root	root
lr-xr-xr-x	11	root	root
-rw-rr	1	root	root
irwxrwxrwt	20	root	root
-rwxr-xr-t	1	root	root
irwxr-xr-x	7	root	root
rwxrwxrwx	1	root	root
lrwxr-xr-x	4	root	root
coot@Philips	s-hue	e:/#	

480	Nov	11	20:34	
480	Nov	11	20:34	
777	Aug	28	11:38	bin
1280	Oct	14	21:09	dev
560	Aug	28	11:38	etc
432	Feb	27	2020	home
78	Aug	19	07:43	init
854	Aug	28	11:38	lib
3	Aug	19	08:12	mnt
360	Feb	27	2020	overlay
0	Jan	1	1970	proc
247	Aug	28	11:38	rom
224	Nov	8	18:41	root
702	Aug	28	11:38	sbin
0	Jan	1	1970	sys
0	0ct	14	21:33	temp
660	Nov	11	10:53	tmp
20	0ct	21	19:47	tmp.gz
89	Aug	28	11:37	usr
4	Aug	28	11:38	$var \rightarrow /tm$
230	Aug	28	11:38	www

#### LISTING ACTIVE SERVICES

tcp tcp tcp

tcp tc tc

ud udp roo

- Netstat -tulpn X
- Showing open ports and tree X services being used by the device while running

oota	Philips-	-hue:/#	netstat -tulpn	
ctiv	e Intern	net conr	nections (only servers	)
roto	Recv-Q	Send-Q	Local Address	Foreign Add
ср	0	0	127.0.0.1:9001	0.0.0.0:*
cn	a	0	127 0 0 1.0002	0 0 0 0.+

	0	0 127.0.0.1:9001	0.0.0:*	LISTEN	1241/ipbridge
	0	0 127.0.0.1:9002	0.0.0:*	LISTEN	1285/behaviord
	0	0 127.0.0.1:9003	0.0.0:*	LISTEN	1296/clipd
	0	0 0.0.0.0:3245	0.0.0:*	LISTEN	1264/nginx.conf -g
	0	0 127.0.0.1:3246	0.0.0:*	LISTEN	1296/clipd
	0	0 0.0.0.0:80	0.0.0:*	LISTEN	1264/nginx.conf -g
	0	0 0.0.0.0:8083	0.0.0.0:*	LISTEN	1264/nginx.conf -g
	0	0 0.0.0.0:22	0.0.0:*	LISTEN	989/dropbear
	0	0 0.0.0.0:1338	0.0.0:*	LISTEN	1241/ipbridge
	0	0 0.0.0.0:1339	0.0.0:*	LISTEN	1241/ipbridge
	0	0 0.0.0.0:443	0.0.0:*	LISTEN	1264/nginx.conf -g
	0	0 0.0.0.0:1883	0.0.0:*	LISTEN	1033/mosquitto
	0	0 ::: 50051	:::*	LISTEN	1241/ipbridge
	0	0 :::8080	:::*	LISTEN	1344/hk_hap
	0	0 :::80	:::*	LISTEN	1264/nginx.conf -g
	0	0 :::8083	:::*	LISTEN	1264/nginx.conf -g
	0	0 :::22	:::*	LISTEN	989/dropbear
	0	0 ::: 443	:::*	LISTEN	1264/nginx.conf -g
	0	0 ::: 1883	:::*	LISTEN	1033/mosquitto
	0	0 0.0.0.0:46611	0.0.0:*		1069/mdnsd
	0	0 0.0.0.0:1900	0.0.0:*		1241/ipbridge
	0	0 0.0.0.0:5353	0.0.0:*		1069/mdnsd
	0	0 :::5353	:::*		1069/mdnsd
	0	0 ::: 48108	:::*		1069/mdnsd
taPhi	lips-hu	e:/# @sS			
		100			

state

PID/Program name

#### BUSYBOX

root@Philips	-hue:/# ls	; -al bin	
drwxr-xr-x	2 root	root	777
drwxrwxrwx	1 root	root	480
lrwxrwxrwx	1 root	root	7
-rwxr-xr-x	1 root	root	265
-rwxr-xr-x	1 root	root	312640
lrwxrwxrwx	1 root	root	7
lrwxrwxrwx	1 root	root	7
lrwxrwxrwx	1 root	root	7
lrwxrwxrwx	1 root	root	7
-rwxr-xr-x	1 root	root	3311
lrwxrwxrwx	1 root	root	7
lrwxrwxrwx	1 root	root	7
lrwxrwxrwx	1 root	root	7
lrwxrwxrwx	1 root	root	7
lrwxrwxrwx	1 root	root	7
lrwxrwxrwx	1 root	root	7
lrwxrwxrwx	1 root	root	7
lrwxrwxrwx	1 root	root	7
lrwxrwxrwx	1 root	root	7
lrwxrwxrwx	1 root	root	7
lrwxrwxrwx	1 root	root	7
lrwxrwxrwx	1 root	root	7
lrwxrwxrwx	1 root	root	7
-rwxr-xr-x	1 root	root	1550
lrwxrwxrwx	1 root	root	7
lrwxrwxrwx	1 root	root	7
lrwxrwxrwx	1 root	root	7
lrwxrwxrwx	1 root	root	7
-rwxr-xr-x	1 root	root	424
lrwxrwxrwx	1 root	root	7

Aug 28 11:38 . Nov 11 20:34 ... Aug 28 11:38 ash → busybox Aug 19 07:43 board\_detect Aug 19 08:14 busybox Aug 28 11:38 cat  $\rightarrow$  busybox Aug 28 11:38 chgrp  $\rightarrow$  busybox Aug 28 11:38 chmod → busybox Aug 28 11:38 chown → busybox Aug 19 07:43 config generate Aug 28 11:38 cp  $\rightarrow$  busybox Aug 28 11:38 date → busybox Aug 28 11:38 dd  $\rightarrow$  busybox Aug 28 11:38 df → busybox Aug 28 11:38 dmesg  $\rightarrow$  busybox Aug 28 11:38 echo → busybox Aug 28 11:38 egrep → busybox Aug 28 11:38 false → busybox Aug 28 11:38 fgrep  $\rightarrow$  busybox Aug 28 11:38 fsync → busybox Aug 28 11:38 grep  $\rightarrow$  busybox Aug 28 11:38 gunzip  $\rightarrow$  busybox Aug 28 11:38 gzip  $\rightarrow$  busybox Aug 19 07:43 ipcalc.sh Aug 28 11:38 kill  $\rightarrow$  busybox Aug 28 11:38  $ln \rightarrow busybox$ Aug 28 11:38 lock → busybox Aug 28 11:38 login → busybox Aug 19 07:43 login.sh Aug 28 11:38 ls  $\rightarrow$  busybox

|--|

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	$TZ \rightarrow /tmp/TZ$
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-rr	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-rr	1 root	root	76	Aug	19	08:12	device_info
-rw-rr	1 root	root	6449	Aug	19	07:43	diag.sh
drwx——	1 root	root	392	Feb	27	2020	dropbear
-rw-rr	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-rr	1 root	root	140	Aug	28	11:38	group
-rw-rr	1 root	root	20	Aug	19	07:43	hosts
-rw-rr	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-rr	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	<pre>mtab → /proc/mounts</pre>
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-rr	1 root	root	234	Aug	19	08:12	openwrt_release
-rw-rr	1 root	root	8	Aug	19	08:12	openwrt_version

#### CUSTOM FIREWALL RULES



Root user has read and write permissions to change any settings in the firewall config files 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@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.						
	<pre># Internal uci firewall ch # put custom rules into th # special user chains, e.g root@Philips-hue:~#</pre>	ains are flushed and recreated on reload, so e root chains e.g. INPUT or FORWARD or into the root@Philips-hue:~# cat /etc/group root:x:0:					
<pre>e Actions Edit View Help bot@Philips-hue:/etc# cat /etc/ oot:x:0:0:root:/root:/bin/ash aemon:*:1:1:daemon:/var:/bin/fa tp:*:55:55:ftp:/home/ftp:/bin/f etwork:*:101:101:network:/var:/ obody:x:65534:65534:nobody:/var osquitto:x:200:200:mosquitto:/v oot@Philips-hue:/etc# sw</pre>	kali@kali:- passwd lse alse bin/false :/bin/false ar/run/mosquitto:/bin/false	<pre>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:</pre>					

root@Philips-hue:~#

-

Imaging on the Linux side	root@Philip bin dev root@Philip	ps-hue:/# ls etc home ps-hue:/# nc	init 1ib 10.0.0.3 222	mnt overlay 2 < test.tar.ç	proc rom jz		sys temp	test.tar.gz tmp	tmp.gz usr	var www
Select Command Prompt - nc -p 2222 -I				2	>	<				
Microsoft Windows [Version 10.0.18362.1082] (c) 2019 Microsoft Corporation. All rights reserved.						^				
H:\>cd Desktop	Savin	o the	rosul	t to o	ur					
H:\Desktop>cd netcat										
H:\Desktop\netcat>nc -p 2222 -l > PhilipsImage.tar.gz	targe	et sys	tem							
· •		•								

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

holow	Name	Size	Packed Size	Modified	Mode	User	Group	Symbolic Link	Hard Link	Folders	Files
Ueluw.	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				



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



- **X** IoT File Systems
- **X** Detailed forensic acquisitions
- **X** Automated forensics
- X IoT Forensics Toolkit



# Questions/Suggestions?

#hadi-linuxforensics-iot on the OSDFCon Discord Server

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