

Title:

Industrial Scale Hardware Hacking



Presented By: Anthony S. Clark

Introduction

- Name:** **Anthony S. Clark**
- Title:** Owner / Principal Researcher Red Crow Lab
- Contact:** asclark@redcrowlab.com
- Focus:** Reverse engineering, vulnerability discovery, PoC devel
- Background:**
- **LANL:** Red Team Founder, CSIRT Member, X-DIV Tech Sec, Int. Applied Tech - Research Scientist 4, Guest Scientist
 - **Founder / CEO Attack Research:** Security consulting (Exxon, Facebook, GM, Bridgewater, Panasonic Avionics, DOD, IC)
 - **Founder / CTO Boldend:** Software tooling for IC & FVEY
 - **Founder Red Crow Lab:** Hardware/Software RE, Tool Dev
 - **Speaker & Trainer:** Blackhat, Defcon, SANS, Infragard, BSides
 - **Original Contributor:** Metasploit, Cisco ThreatGrid, PTES, DARPA Cyber Fast Track



Specialty

Taking custom or proprietary technologies
Learning them,
Reversing them,
& **Leveraging** them.

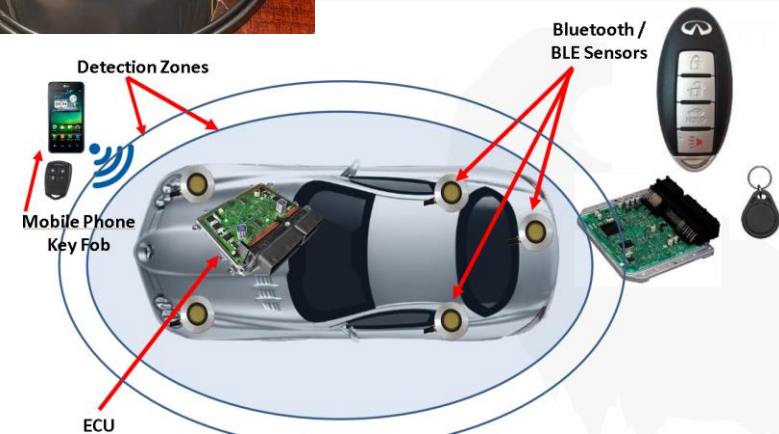


Types of Devices

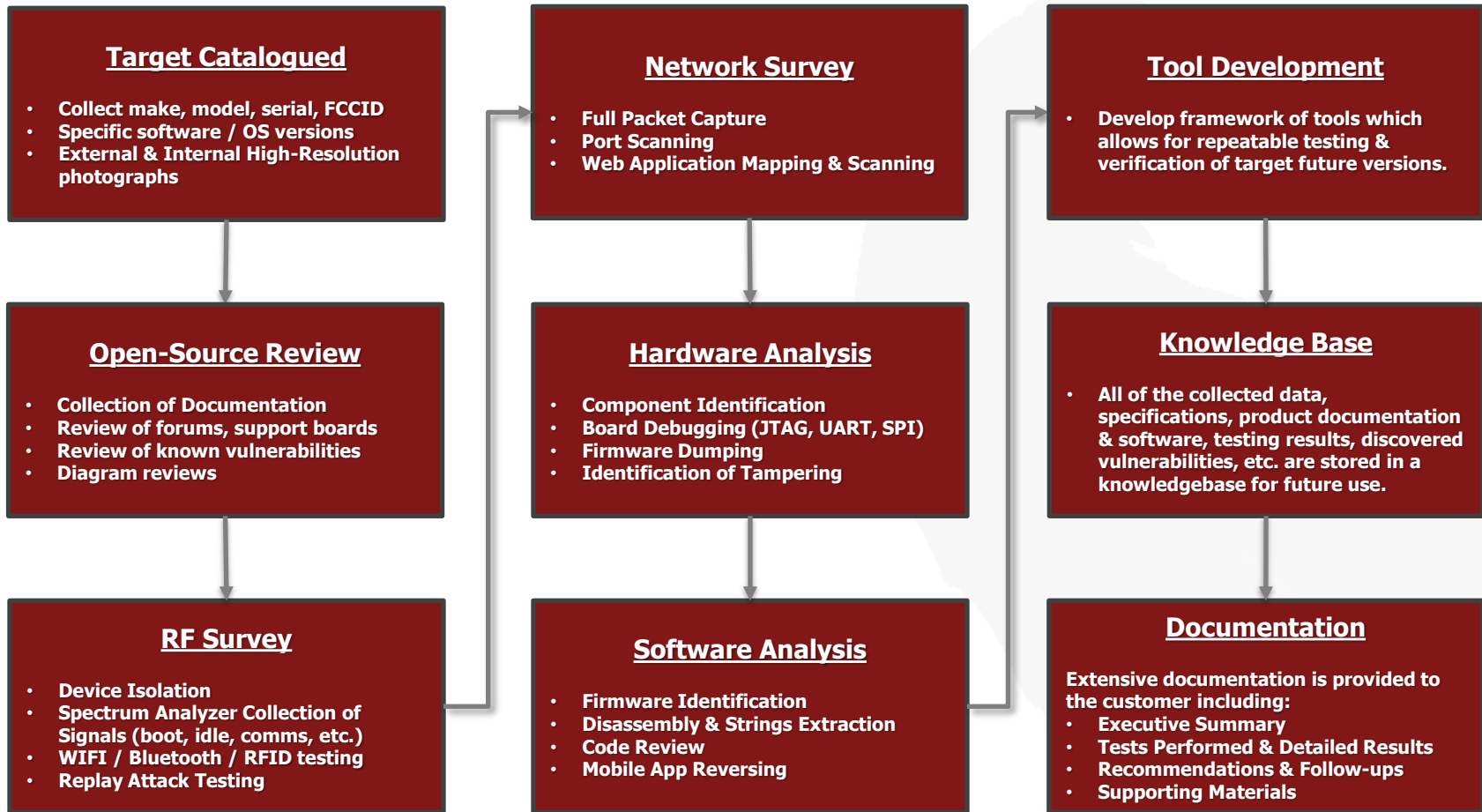
- Scientific Instruments
- Avionics
- Automotive
- Security (ex. Locks)
- Legacy (Ex. AS400)
- Satellite
 - sensors
- OT/ICS/SCADA
- Financial
 - ATMs
 - POS
- Telecom
 - Routers
 - Switches
- Mobile



System Control Unit (SCU)



Industrial Scale Hardware Hacking Process



Setting Up A Lab

BENCH CONCEPT

INSTRUMENTATION COLLECTION

- Modifications
 - Network
 - File System
 - Process Table
 - Registry
 - Memory
 - Signals

RF TEST BENCH



LAB GEAR

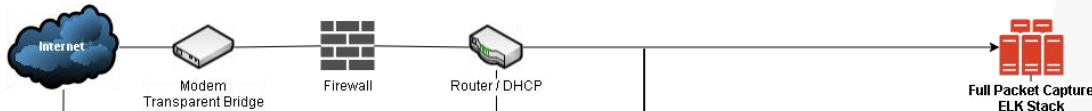
- Signal Isolation
- Spectrum Analysis
- Near Field Probing
- WIFI & Bluetooth Analysis
- Replay Tools
- RFID & Proxcard readers / writers
- SDRs

HARDWARE TEST BENCH



LAB GEAR

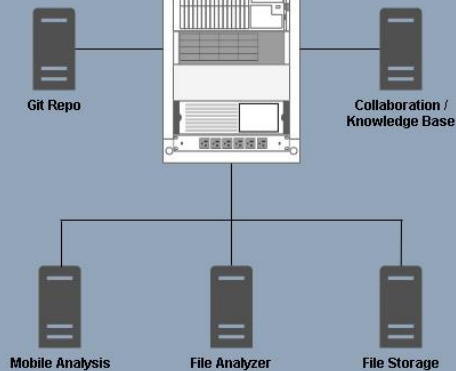
- Oscilloscopes
- Logic Analyzers
- JTAG/SPI/UART Debuggers
- Soldering & Hot Air Rework Stations
- Chip programmers / firmware dumpers
- Multimeters
- HID Emulators
- High Resolution Photography & Imaging



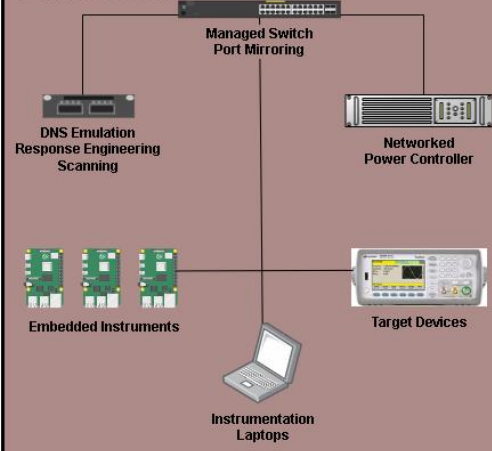
Internal LLM/AI
(In Process)

NVIDIA GeForce
RTX 3060 Ti
LAMA 3 Instruct

VIRTUALIZATION INFRASTRUCTURE

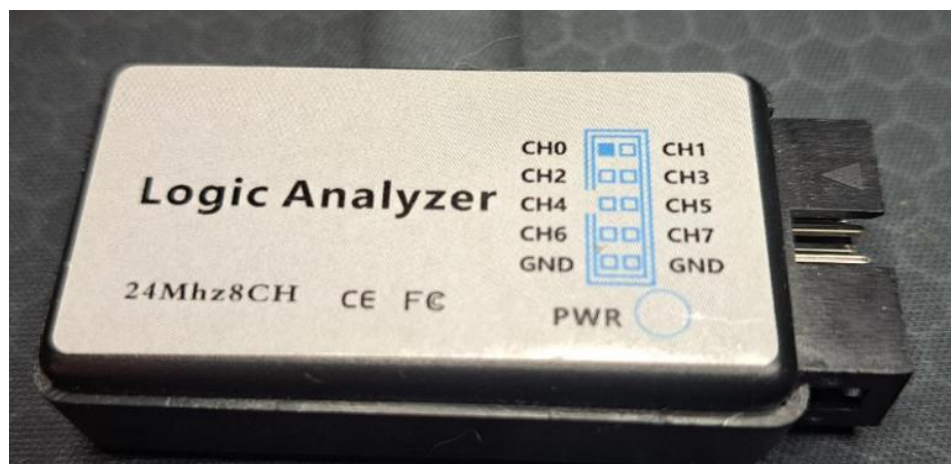


TEST NETWORK



Attribution Management

Lab Equipment



Lab Equipment

- **Network Gear**
 - Network Isolation / Network Switch With Port Mirroring / Router
 - Jump Hosts
 - DNS Control / Dynamic Host Configuration Protocol (DHCP) Server
 - Full Packet Capture
 - Man In The Middle (MiTM) Tools (fiddler, Ettercap, sslstrip)
- **Small Programmable Devices**
 - Arduino / Raspberry Pi / BeagleBone / Teensy / NanoPi / OrangePi
- **Radio Frequency Analysis**
 - HackRF / BladeRF / UberTooth / Proxmark / FlipperZero / Pineapple / SDR
- **Hardware Debugging & Measurement**
 - Multimeters
 - Oscilloscope
 - Logic Analyzer
 - Chip Reader - Dataman 48Pro2 Universal Programmer /
- **Imaging**
 - High Resolution Camera & Lighting
 - Electronics Microscope



Build a Kanban Board

Hardware Assessment Tasks

Backlog | 5

Build & compile C2 client to run on device.

Identify JTAG PIN outs

Attach to JTAG Debugging Port

Attack Bluetooth Interface

Create modified firmware

+

In progress | 5

Run Burp Scan on Web Interfaces

Run security tool on control software

Network MitM against command port

Build Hardware Implant

Crack Device WIFI Password

+

Blocked | 2

Analyze Mobile App - Need to acquire APK from vendor, waiting on NDA

Analyze Firmware, Firmware Encrypted

+

Done | 5

Take External Photos

Take Internal Photos

Analyze Photos & Identify Components / Inputs

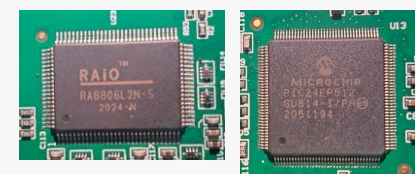
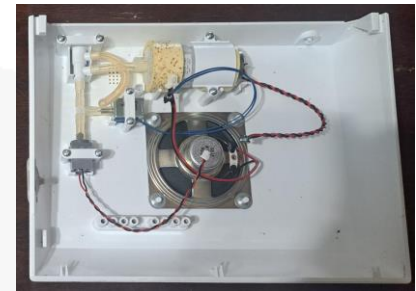
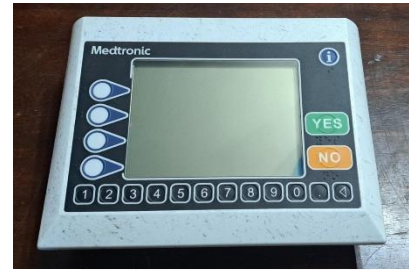
Collect RF Survey

Collect Network Survey (PCAP + Ports)

+

Target Catalogue

ITEM	VALUE
MAKE:	Medtronic
MODEL:	Commander Flex CD320-GV
SERIAL NUMBER:	1000869493
FCCID:	XTQ-CO320 IQOUBLE113
DESCRIPTION:	Medical Telemonitoring Device, is capable sending important medical information to your doctor, and or medical healthcare professional, via a wired telephone line. Measures weight, peak blood flow, oxygen saturation, blood pressure, and/or blood glucose levels
DATASHEET:	https://fccid.io/XTQ-CD320/User-Manual/User-Manual-2976121
IO:	USB RJ11 7V DC Power Audio PS2

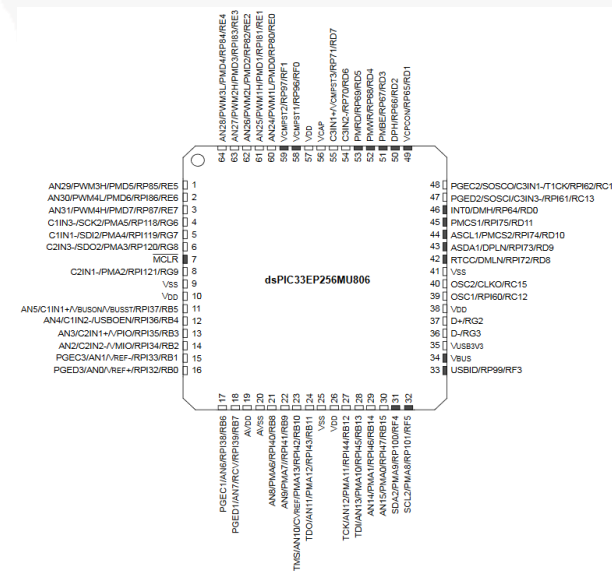


Target Catalogue

- Identify Critical Chips



ITEM	VALUE
MAKE:	Microchip
MODEL:	PIC24EP512
DESCRIPTION:	<p>Primary microcontroller. The PIC24EP512 has an 16-bit CPU core, (C and Assembly) based , with IEEE 1149.2 Compatible (JTAG) Boundary Scan. A well as 15-Channel DMA (Direct Memory Access) with User-Selectable Priority Arbitration:</p> <ul style="list-style-type: none">15-Channel DMA with 4 UART modules (15 Mbps), with support for UART, SPI, ADC, ECAN and OC.Four 4-Wire SPI modules (15 Mbps)Two ECAN™ modules (1 Mbaud) CAN 2.0B SupportTwo I2C modules (up to 1 Mbaud) with SMBus SupportData Converter Interface (DCI) module with Support for I2SProgrammable Cyclic Redundancy Check (CRC)Parallel Master Port (PMP)PPS to allow Function Remap
DATASHEET:	https://ww1.microchip.com/downloads/aemDocuments/documents/OTH/ProductDocuments/Datasheets/70616g.pdf



Open Source Review

← → ↻ cve.mitre.org/cgi-bin/cvekey.cgi?keyword=medtronic

CVE CVE List + CNAs + WGs + Board + About +

Search CVE List Downloads Data Feeds Update a CVE Record Request CVE IDs

HOME > CVE > SEARCH RESULTS

Search Results

There are 26 CVE Records that match your search.

Name	Description
CVE-2023-31222	Deserialization of untrusted data in Microsoft Messaging Queuing Service in Medtronic's Pacerat Optima versions 1.11 and earlier on WiR user to impact a healthcare delivery organization's Pacerat Optima system cardiac device causing data to be deleted, stolen, or system being used for further network penetration via network connectivity.
CVE-2023-25931	Medtronic identified that the Pelvic Health clinician apps, which are installed on the Smart Programmer mobile device, have a password v security update to fix. Not updating could potentially result in unauthorized control of the clinician therapy application, which has grea parameters than the patient app. Changes still cannot be made outside of the established therapy parameters of the programmer. For i individual would need physical access to the Smart Programmer.
CVE-2022-32537	A vulnerability exists which could allow an unauthorized user to learn aspects of the communication protocol used to pair system compa red with other system components. Exploitation requires nearby wireless signal proximity with the patient and the device; advanced for exploitation. Please refer to the Medtronic Product Security Bulletin for guidance.
CVE-2020-27252	Medtronic MyCareLink Smart 25000 all versions are vulnerable to a race condition in the MCL Smart Patient Reader software update sys firmware to be uploaded and executed on the Patient Reader. If exploited an attacker could remotely execute code on the MCL Smart P control of the device.
CVE-2020-25187	Medtronic MyCareLink Smart 25000 all versions are vulnerable when an attacker who gains auth runs a debug command, which is sent t overflow in the MCL Smart Reader stack. A heap overflow allows attacker to remotely execute code on the MCL Smart Reader, could le
CVE-2020-25183	Medtronic MyCareLink Smart 25000 all versions contain an authentication protocol vuln where the method used to auth between MCL S MyCareLink Smart mobile app is vulnerable to bypass. This vuln allows attacker to use other mobile device or malicious app on smartph patients's Smart Reader, fools the device into thinking its communicating with the actual smart phone application when execute

POWERLINE CONDUCTED EMISSIONS



EUT:	CD320 Commander Flex	Work Order:	CCOM0015
Serial Number:	900000009	Date:	06/29/2015
Customer:	Cardiocom	Temperature:	22.4°C
Attendees:	None	Relative Humidity:	57%
Customer Project:	None	Bar. Pressure:	980 mb
Tested By:	Dustin Sparks	Job Site:	MIN03
Power:	110VAC/60Hz	Configuration:	CCOM0015-3

TEST SPECIFICATIONS	
Specification:	Method:
FCC 15.207-2015	ANSI C63.10-2009

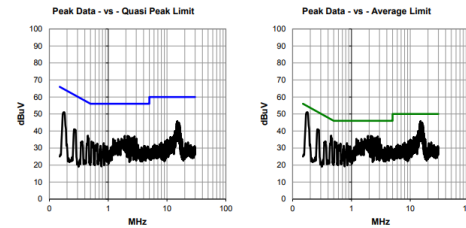
TEST PARAMETERS			
Band:	Line:	Neutral:	Add. Ext. Attenuation (dB):
5			0

COMMENTS
None

EUT OPERATING MODES
Transmitting channel 10

DEVIATIONS FROM TEST STANDARD
None

- Forums
- CVE / Vuln DBs
- FCCID Lookup
- Reddit



OR the Commander FLEX setup should look like this if a telephone is also plugged into the wall jack:



apps.fcc.gov/oetcf/eas/reports/ViewExhibitReport.cfm?mode=Sum&calledFromFrame=N&RequestTimeou...

Search | RSS | Updates | E-Filing | Initiatives | Consumers | End Page

FCC Federal Communications Commission

Office of Engineering and Technology

OET Home Page [FCC > FCC E-Filing > EAS > List Exhibits Page](#) [FCC Site Map](#)

Filing Options

- Grantee Registration
- Modify Grantee Information
- Reply to Grantee Name Change Correspondence
- Test Firm Accrediting Body Update
- Return to 159 J Pay for a Grantee Certificate

Reports

- Pending Application Status
- Authorization Search
- Grantee Search
- Pending Grantee Search

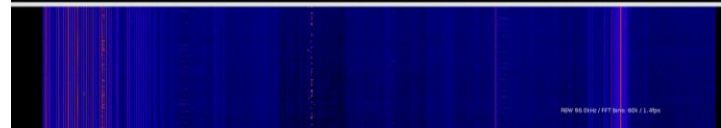
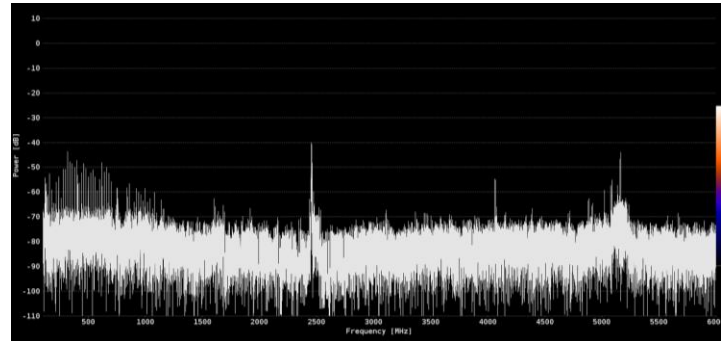
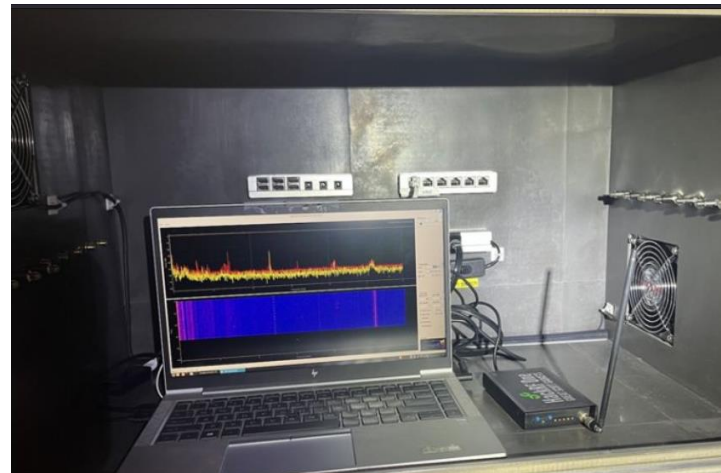
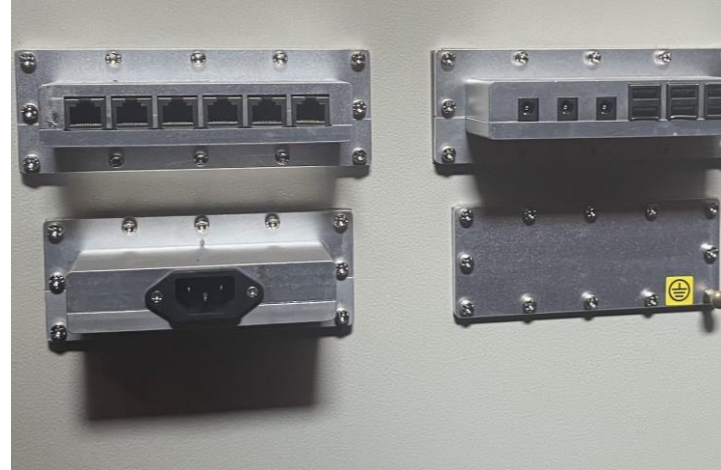
OET Exhibits Summary List

15 Matches found for FCC ID **XTQ-CD320**

Exhibit Type	File Type	File Size	Description	Submission Date	Permanent	Short-Term	Date Available
Block Diagram	Adobe Acrobat PDF103980	Frequency Block Diagram	04/29/2016	Yes	No	Confidential	04/29/2016
Cover Letter(s)	Adobe Acrobat PDF27780	Cover letter	04/29/2016	No	No	Confidential	04/29/2016
Cover Letter(s)	Adobe Acrobat PDF27257	Request for confidentiality	04/29/2016	No	No	Confidential	04/29/2016
External Photos	Adobe Acrobat PDF517644	External Photos	04/29/2016	No	No	Confidential	04/29/2016
ID Label/Location Info	Adobe Acrobat PDF110191	ID Label	04/29/2016	No	No	Confidential	04/29/2016
ID Label/Location Info	Adobe Acrobat PDF144184	ID Label	04/29/2016	No	No	Confidential	04/29/2016
Internal Photos	Adobe Acrobat PDF1052743	Internal Photos	04/29/2016	No	No	Confidential	04/29/2016
Operational Description	Adobe Acrobat PDF139983	Operational Description	04/29/2016	Yes	No	Confidential	04/29/2016
Operational Description	Adobe Acrobat PDF2396140	Operational Description	04/29/2016	Yes	No	Confidential	04/29/2016
Operational Description	Adobe Acrobat PDF51629	Antenna info	04/29/2016	No	No	Confidential	04/29/2016
Operational Description	Adobe Acrobat PDF40687	Antenna info	04/29/2016	No	No	Confidential	04/29/2016
Schematics	Adobe Acrobat PDF326694	Schematics	04/29/2016	Yes	No	Confidential	04/29/2016
Test Report	Adobe Acrobat PDF920898	Test Report	04/29/2016	No	No	Confidential	04/29/2016
Test Setup Photos	Adobe Acrobat PDF529392	Test setup Photos	04/29/2016	No	No	Confidential	04/29/2016
Users Manual	Adobe Acrobat PDF2136840	User Manual	04/29/2016	No	No	Confidential	04/29/2016

RF Survey

- Faraday Cage / Signal Isolation
- Spectrum Analyzer (1-6 GHz)
- Shielded Passthru Ports
- Look for signals that indicate RF coms
- Signals = Potential Attack Surfaces



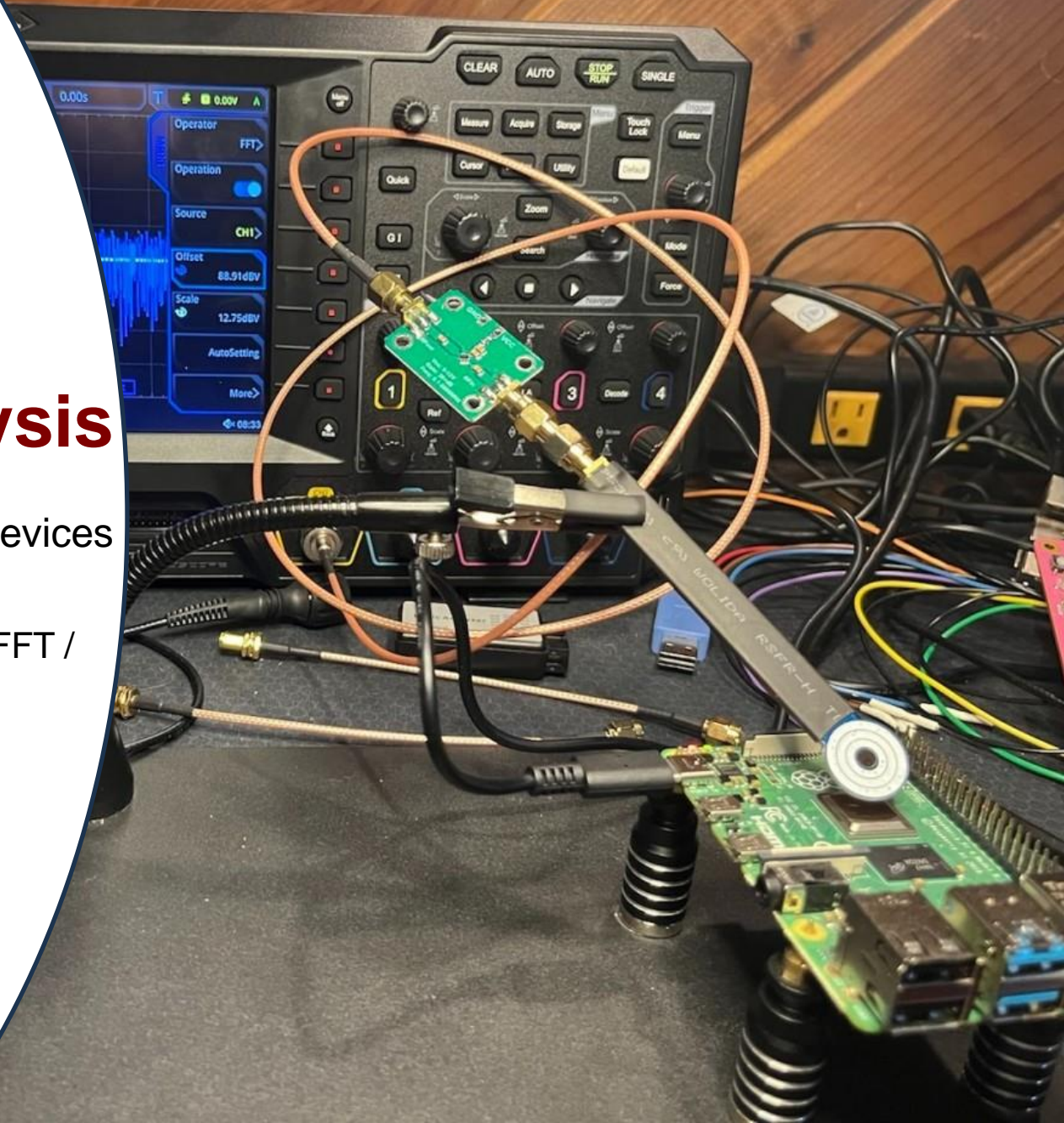
RF Survey

- HackRF
- QSpectrumAnalyzer in hackrf_sweep mode
- Signal Collection and Characterization
- Replay attacks
- Wifi testing
 - De-auth attacks
 - Traffic sniffing
 - Malicious AP attacks
- Bluetooth testing
- NFC, RFID, & other RF Tests



Near Field Analysis

- Look for emissions from devices
- Done using
 - Oscilloscope running in FFT / Spectrum Analyzer mode
 - HGLN Amplifier
 - Near field probes



Network Survey

- Internet controllable power switch
- Identify listening services

PORT	STATE	SERVICE
------	-------	---------

80/tcp	open	http
--------	------	------

443/tcp	open	https
---------	------	-------

MAC Address:

00:03:EA:06:68:10 (Mega System Technologies)



- Setup hardware network tap



Hak5 Plunderbug



Network Survey

- Using a tap, collect full packet capture of interaction with the device

No.	Time	Source	Destination	Protocol	Length	Info
23	3.640417	192.168.101.175	192.168.101.228	TCP	66	56978 → 80 [SYN] Seq=0 Win=64240
25	3.640916	192.168.101.228	192.168.101.175	TCP	66	80 → 56978 [SYN, ACK] Seq=0 Ack=
26	3.640932	192.168.101.175	192.168.101.228	TCP	60	56978 → 80 [ACK] Seq=1 Ack=1 Win=
27	3.641161	192.168.101.175	192.168.101.228	HTTP	705	POST /goform/login HTTP/1.1 (ap
30	3.641700	192.168.101.228	192.168.101.175	TCP	60	80 → 56978 [ACK] Seq=1 Ack=652 W
31	3.646714	192.168.101.228	192.168.101.175	TCP	81	80 → 56978 [PSH, ACK] Seq=1 Ack=
32	3.648082	192.168.101.228	192.168.101.175	HTTP	485	HTTP/1.0 200 Data follows (text/html)
33	3.648091	192.168.101.175	192.168.101.228	TCP	60	56978 → 80 [ACK] Seq=652 Ack=460 Win=262144 Len=0
34	3.648673	192.168.101.175	192.168.101.228	TCP	60	56978 → 80 [FIN, ACK] Seq=652 Ack=460 Win=262144 Len=0
35	3.649102	192.168.101.228	192.168.101.175	TCP	60	80 → 56978 [ACK] Seq=460 Ack=653 Win=7142 Len=0

Frame 27: 705 bytes on wire (5640 bits), 705 bytes captured (5640 bits) on interface \Device\NPF_{2F98D...}

Ethernet II, Src: ASUSTekC_7e:db:e6 (50:eb:f6:7e:db:e6), Dst: MegaSyst_06:68:10 (00:03:ea:06:68:10)

Internet Protocol Version 4, Src: 192.168.101.175, Dst: 192.168.101.228

Transmission Control Protocol, Src Port: 56978, Dst Port: 80, Seq: 1, Ack: 1, Len: 651

Hypertext Transfer Protocol

HTML Form URL Encoded: application/x-www-form-urlencoded

```
POST /goform/login HTTP/1.1
Host: 192.168.101.228
Connection: keep-alive
Content-Length: 38
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.101.228
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://192.168.101.228/login.asp
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

login=1&user=admin&password=rcPassword
Server: GoAhead-Webs

login=1&user=admin&password=rcPassword HTTP/1.0 200 Data follows
Server: GoAhead-Webs
Date: Tue Jun 25 08:03:20 2024
Set-Cookie: MQKJhuEcnAVA3t7WE+ug6A=3wiURyFzHynJsIoLx; HttpOnly; Path=/
Pragma: no-cache
Cache-Control: no-cache
Content-Type: text/html
Location: /index.asp

```
<html><head>
  <meta http-equiv=Content-Type content='text/html; charset=utf-8'>
</head><body>
  <script language='JavaScript'>
window.top.location.href='/index.asp';
</script>
</body></html>
```

Network Survey

- Scan for low-hanging fruit vulnerabilities

Time	Source	Issue type	Host	Path	Insertion point	Severity	Confidence	Commer	
11:22:04	25 Jun 2024	Task 3	🔍	Input returned in response (stored)	http://192.168.101.228	/system.asp	WQK.JhuEcnAVA3t7W...	Information	Certain
11:13:43	25 Jun 2024	Task 3	🔍	Input returned in response (reflected)	http://192.168.101.228	/top2.htm	WQK.JhuEcnAVA3t7W...	Information	Certain
11:03:53	25 Jun 2024	Task 3	🔍	Open redirection (DOM-based)	http://192.168.101.228	/skype.asp		Low	Tentative
11:03:52	25 Jun 2024	Task 3	🔍	Open redirection (DOM-based)	http://192.168.101.228	/config.asp		Low	Tentative
11:03:45	25 Jun 2024	Task 3	🚨	Session token in URL	http://192.168.101.228	/view.asp		Medium	Firm
11:03:45	25 Jun 2024	Task 3	🔍	Private IP addresses disclosed	http://192.168.101.228	/network.asp		Information	Certain
11:03:45	25 Jun 2024	Task 3	🔍	HTML does not specify charset	http://192.168.101.228	/eventLog.asp		Information	Certain
11:03:45	25 Jun 2024	Task 3	🔍	Private IP addresses disclosed	http://192.168.101.228	/cgi-bin/ExportSettings.sh		Information	Certain
11:03:45	25 Jun 2024	Task 3	🚨	Cleartext submission of password	http://192.168.101.228	/mailSettings.asp		High	Certain
11:03:45	25 Jun 2024	Task 3	🔍	File upload functionality	http://192.168.101.228	/saveUpgrade.asp		Information	Certain
11:03:45	25 Jun 2024	Task 3	🚨	Session token in URL	http://192.168.101.228	/eventLog.asp		Medium	Firm
11:03:45	25 Jun 2024	Task 3	🔍	Private IP addresses disclosed	http://192.168.101.228	/config.asp		Information	Certain
11:03:45	25 Jun 2024	Task 3	🚨	Cleartext submission of password	http://192.168.101.228	/account.asp		High	Certain

Advisory Request **Response** Path to issue

Pretty Raw Hex Render

```
1 HTTP/1.0 200 OK
2 Date: Wed Jun 26 01:01:57 2024
3 Server: GoAhead-Webs
4 Pragma: no-cache
5 Cache-Control: no-cache
6 Content-type: text/html
7
8 <html>
9 <frameset frameborder="0" framespacing="0" border="0" rows="60,*">
10 <frame src="logChoose.asp" name="logchoose" scrolling="no" marginwidth="0" marginheight="0" noresize>
11 <frame src="/cgi-bin/eventlog.cgi?type=0&csrfToken=QJrwqx8Zb7QA32X80" name="eventlog" marginwidth="0"
12 marginheight="0" scrolling="no" target="right">
13 </frameset>
14 </html>
```

Inspector

Response headers 5

Name	Value
Date	Wed Jun 26 01:0...
Server	GoAhead-Webs
Pragma	no-cache
Cache-Control	no-cache
Content-type	text/html



HTTP Intercept

- Use Burp to identify useful actions
- Determine “effects”
- Create tool to generate effect

The screenshot displays the Burp Suite interface. The main window shows the raw HTTP request in the 'Pretty' view. A red arrow points from the 'control=3' parameter in the request body to the 'Request query parameters' section in the Inspector panel. The Inspector panel shows the following details:

Name	Value
target	1
control	3
time	1719274366948
csrftoken	deNSxgwGhP9VSI0s5

Network Effect Tool

- **msnEffect.py**

```
import requests

url = "http://192.168.101.228/cgi-
bin/control.cgi?target=1&control=3&time=1719274366948&csrftoken=deNSxgwGhP9VSlOs5"

headers = {
    "Host": "192.168.101.228",
    "Upgrade-Insecure-Requests": "1",
    "User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) Chrome/125.0.6422.112
Safari/537.36",
    "Accept":
"text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*
*;q=0.8,application/signed-exchange;v=b3;q=0.7",
    "Referer": "http://192.168.101.228/status.asp",
    "Accept-Encoding": "gzip, deflate, br",
    "Accept-Language": "en-US,en;q=0.9",
    "Connection": "keep-alive"
}

cookies = {
    "WQKJhuEcnAVA3t7WE+ug6A": "OPns8R7gSpJvsWo3F"
}

response = requests.get(url, headers=headers, cookies=cookies, verify=False)

print(response.text)
```



Test Effect

MSNswitch

Information
Status

Current Status >>>

Configuration
Settings

Configuration
Schedule
Network
E-mail
Skype
Account
System
Language

Logs
Data

Event Log

Help

System Status
Save / Upgrade
Online FAQ
Logout

Connection Status

Assign	Site Label	Target Site	IP Address	Response Time	Timeout
Both	Google	www.google.com	142.250.72.36	21 ms	13 %
	Yahoo	www.yahoo.com	69.147.71.248	Timeout	100 %
	Pingler	www.pingler.com	69.64.32.114	45 ms	14 %
	Ask.com	www.ask.com	151.101.70.114	21 ms	13 %
None	Router	192.168.101.1	192.168.101.1	1 ms	13 %

Status and Control

Item	On/Off Control
UIS Reset	<input type="checkbox"/>

Assigned outlet will auto reset when target site timeout. Only outlets that are On will reset.
 Assigned outlet will not reset when connection loss is detected.

Effect Resets
Power Outlet

Status and Control

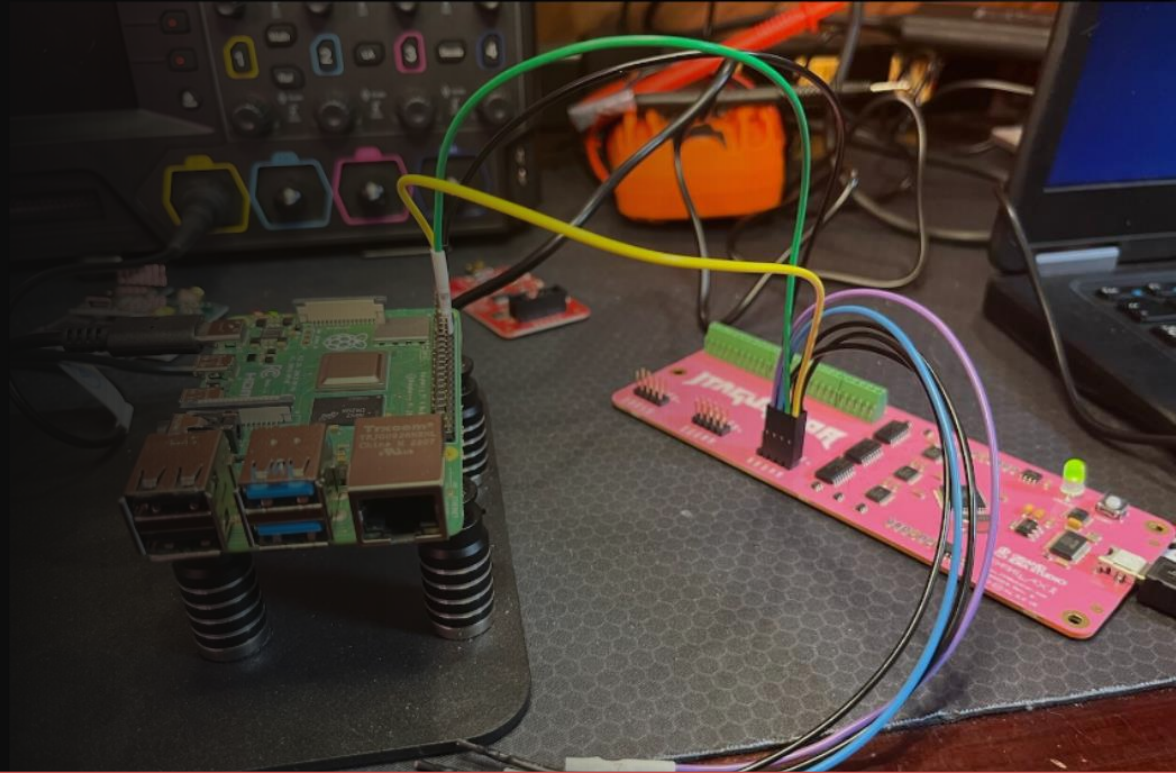
Outlet Name	Status	Control
Outlet 1	Off	<input type="checkbox"/>
Outlet 2	On	<input type="checkbox"/> <input type="button" value="Reset"/>

Outlet On Outlet Off Outlet is On, UIS Reset function is Off or Outlet is not Assigned

Command Prompt

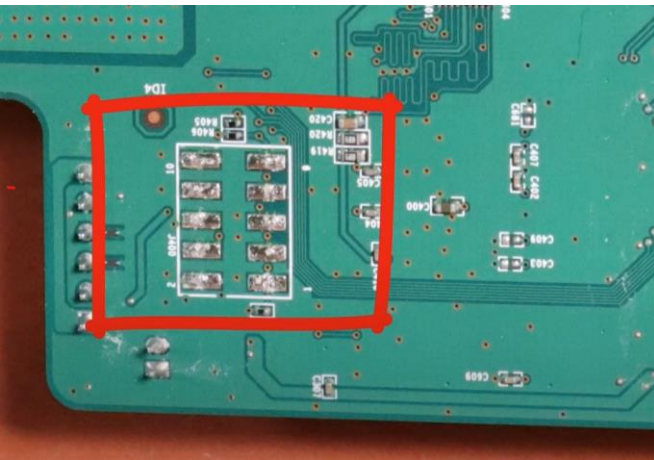
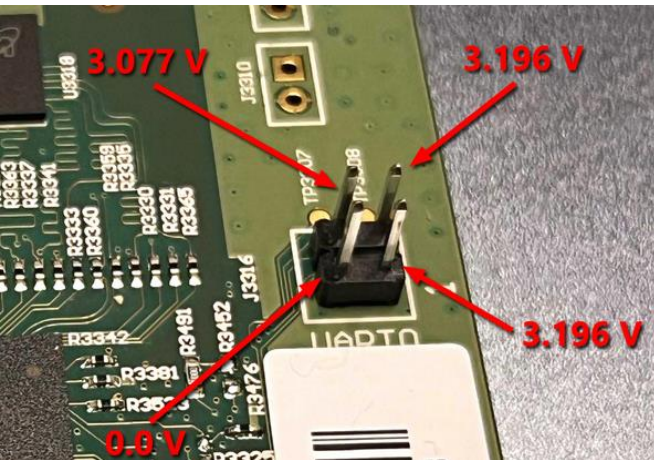
```
C:\Users\Admin>python msnSwitch_effect.py  
<?xml version="1.0"?><request><outlet_status>1,1</outlet_status><uis_s  
tatus>0</uis_status></request>
```

Hardware Analysis



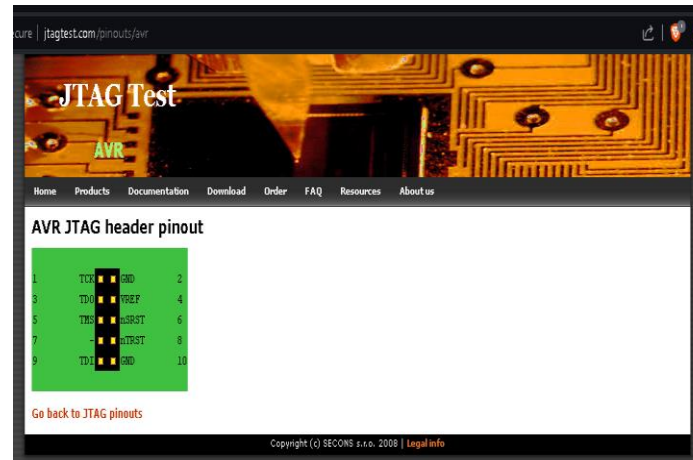
```
RT> p
te: UART pin naming is from the target's perspective
ter X to disable either pin, if desired.
ter TXD pin [0]: 1
ter RXD pin [0]: 2
ter baud rate [0]: 115200
able local echo? [y/N]: y
tering UART passthrough! Press Ctrl-X to exit...
[0.000000] Booting Linux on physical CPU 0x0
[0.000000] Linux version 5.15.61-v7l+ (dom@buildb
untu) 2.34) #1579 SMP Fri Aug 26 11:13:03 BST 2022
[0.000000] CPU: ARMv7 Processor [410fd083] revisi
[0.000000] CPU: div instructions available: patch
[0.000000] CPU: PIPT / VIPT nonaliasing data cach
[0.000000] OF: fdt: Machine model: Raspberry Pi 4
[0.000000] random: crng init done
```

Hardware Analysis



- **JTAG, UART, SPI**

1. Take resistance measurements against ground with board powered off. Set Multimeter to ohms Ω .
 2. Touch black probe to a ground point.
 3. Touch red probe led to each pin and record measurements on a table.
 4. Next take resistance measurements against VCC.
 5. Find data sheet, locate VCC pin
 6. Red probe on the VCC pin & touch the black probe to each candidate JTAG pins & record results in table
 7. Power on board, switch multimeter to volts, measure voltage on each pin. Black probe on ground & red probe on each pin
 8. Search <http://jtagtest.com/pinouts> for a pinout that matches findings.
1. Know the device's architecture (arm, mips, etc.)



PINout Lookup

Example Pinout Analysis Table

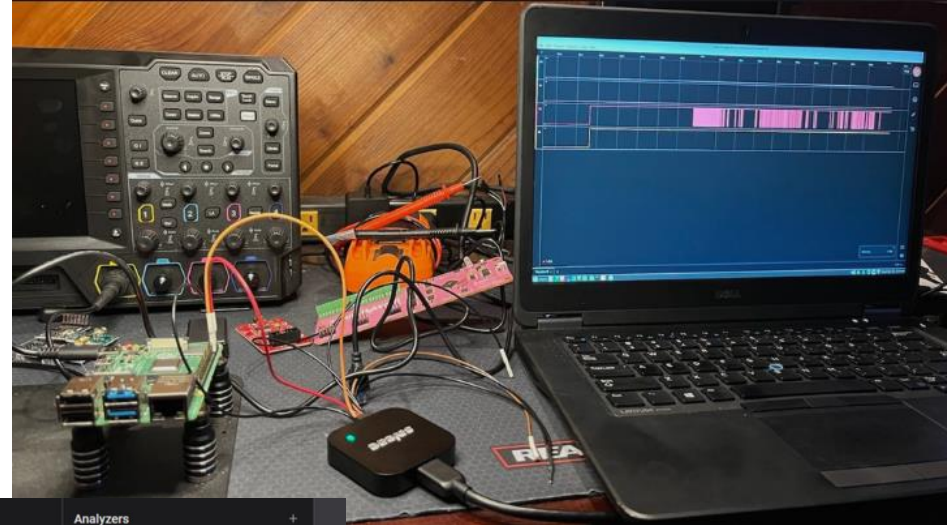
PIN	RGRND	RVCC	V	NOTES	PIN	RGND	RVCC	V	NOTES
1	1K Ω	1K Ω	0 V		2	0 Ω	90 Ω	0 V	Probably Ground (GND) because its all 0s
3	∞	∞	2.1 V	High Impedance PIN? Could be TDO	4	90 Ω	0 Ω	3.3 V	VCC because it has 0 resistance against VCC but 3.3 V
5	4.7K Ω	4.7K Ω	3.3 V		6	∞	∞	0 V	Not Connected?
7	5.7K Ω	5.7K Ω	3.3 V		8	∞	∞	0 V	Not Connected?
9	4.7K Ω	4.7K Ω	3.3 V		10	0 Ω	90 Ω	0 V	Probably Ground (GND)



Logic Analysis

Hex: "0x48, 0x65, 0x6C 0x6F, 0x20, 0x57,
0x6F, 0x72, 0x6C, 0x64, 0x0D 0x0D"

ASCII: "H" "e" "l" "l" "o" "space" "W" "o"
"r" "l" "d"



Dec	Hex	Oct	Char	Dec	Hex	Oct	Char	Dec	Hex	Oct	Char
0	0000	000	(null)	32	20	040	Space	64	40	100	@
1	0001	001	(start of heading)	33	21	041	!	65	41	101	A
2	0002	002	(start of text)	34	22	042	"	66	42	102	B
3	0003	003	(end of text)	35	23	043	#	67	43	103	C
4	0004	004	(end of transmission)	36	24	044	\$	68	44	104	D
5	0005	005	(enquiry)	37	25	045	%	69	45	105	E
6	0006	006	(acknowledge)	38	26	046	&	70	46	106	F
7	0007	007	(bell)	39	27	047	'	71	47	107	G
8	0010	010	(backspace)	40	28	050	()	72	48	110	H
9	0011	011	(horizontal tab)	41	29	051	!	73	49	111	I
10	A 012	LF	(line feed, new line)	42	2A	052	"	74	4A	112	J
11	B 013	VT	(vertical tab)	43	2B	053	#	75	4B	113	K
12	C 014	FF	(form feed, new page)	44	2C	054	\$	76	4C	114	L
13	D 015	CR	(carriage return)	45	2D	055	%	77	4D	115	M
14	E 016	SO	(shift out)	46	2E	056	&	78	4E	116	N
15	F 017	SI	(shift in)	47	2F	057	'	79	4F	117	O
16	10 020	DL	(data link escape)	48	30	060	()	80	50	120	P
17	11 001	DC1	(device control 1)	49	31	061	!	81	51	121	Q
18	12 002	DC2	(device control 2)	50	32	062	"	82	52	122	R
19	13 003	DC3	(device control 3)	51	33	063	#	83	53	123	S
20	14 004	DC4	(device control 4)	52	34	064	\$	84	54	124	T
21	15 025	NAK	(negative acknowledge)	53	35	065	%	85	55	125	U
22	16 026	SYN	(synchronous idle)	54	36	066	&	86	56	126	V
23	17 027	ETB	(end of trans. block)	55	37	067	'	87	57	127	W
24	18 030	CAN	(cancel)	56	38	070	()	88	58	130	X
25	19 031	EM	(end of medium)	57	39	071	!	89	59	131	Y
26	1A 032	SUB	(substitute)	58	3A	072	"	90	5A	132	Z
27	1B 033	ESC	(escape)	59	3B	073	#	91	5B	133	[
28	1C 034	FS	(file separator)	60	3C	074	\$	92	5C	134	\
29	1D 035	GS	(group separator)	61	3D	075	%	93	5D	135]
30	1E 036	RS	(record separator)	62	3E	076	&	94	5E	136	^
31	1F 037	US	(unit separator)	63	3F	077	'	95	5F	137	_

Software Analysis

- Windows Device Software
 - PE (.exe) & DLL files
- Linux Device Software
 - ELF binaries and .so files
- Firmware Reverse Engineering
 - Firmware format identification
 - OS & file extraction





Static Software Analysis Example

FILE NAME:	CareLinkUploader-ACC-7350-3.11.0-windows-installer.exe
FILE SIZE:	174372 / 171M
FILE TYPE:	PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows
MD5SUM:	cf0a57d5441239da426922e481a2a85e
SHA256SUM:	62b9e6928b3884bc67868423dc9a63d76bb05118ae7c5ada1ee453355981f383
COMPILE TIME:	2023-01-04 15:12:35
COMPILE SECURITY:	DEP: True ASLR: True NX: True SEH: True CFG: False
DEPENDENCIES:	'GDI32.dll', 'SHELL32.DLL', 'OLEAUT32.DLL', 'WS2_32.dll', 'OLE32.dll', 'USER32.dll', 'COMCTL32.DLL', 'msvcrt.dll', 'COMDLG32.DLL', 'IMM32.DLL', 'ADVAPI32.DLL', 'KERNEL32.dll'
SECTIONS:	11, '.text', '.data', '.rdata', '.eh_fram', '.bss', '.edata', '.idata', '.CRT', '.tls', '.rsrc', '.reloc'
ENTROPY:	7.9983 (High Entropy, likely contains compressed/encrypted data)
IMPORTS:	GetSecurityDescriptorOwner, GetSidIdentifierAuthority, GetUserNameA, GetUserNameW, RegCloseKey, RegOpenKeyExA, RegQueryValueExA, CopyFileA, CreateDirectoryA, CreateEventA, CreateFileA, CreateFileW, CreatePipe, CreateProcessA, CreateProcessW, CreateThread, DeleteFileA, DeleteFileW, ExitProcess, FindClose, FindFirstFileA, FindFirstFileW, FindNextFileA, FindNextFileW, WriteConsoleW, WriteFile, lstrcpYA, lstrcpYW, lstrcpynA, lstrlenA, lstrlenW, _getpid, _stricmp, _strnicmp, _timezone, _tzset, _write, fputc, fputs, fread, free, frexp, fseek, ftell, fwrite, getenv, gmtime, isalnum, ldexp, localtime, log, log10, malloc, memcmp, memcpy, memmove, memset, mktime, modf, pow, printf, puts, qsort, realloc, setlocale, signal, sin, sinh, sprintf, sqrt, sscanf, strcat, strchr, strcmp, strcpy, strcspn, strerror, strlen, strncmp, strncpy, strpbrk, strrchr, strspn, strstr, strtod, strtol, strtoul, swprintf, tan, tanh, time, tolower, toupper, vfprintf, vsprintf, wcschr, wcsncmp, wcsncpy, wcslen, wcsncmp, GetAsyncKeyState, GetCapture, GetClipboardData, GetClipboardOwner, GetFocus, GetForegroundWindow, GetKeyState, GetKeyboardLayout, GetWindow, MessageBoxA, OpenClipboard, PeekMessageA, PostMessageA, PostQuitMessage, SendMessageW, accept, bind, closesocket, connect, gethostbyaddr, gethostbyname, gethostname, getpeername, getservbyname, getsockname, getsockopt, htons, inet_addr, inet_ntoa, ioctlsocket, listen, ntohs, recv, select, send, setsockopt, socket

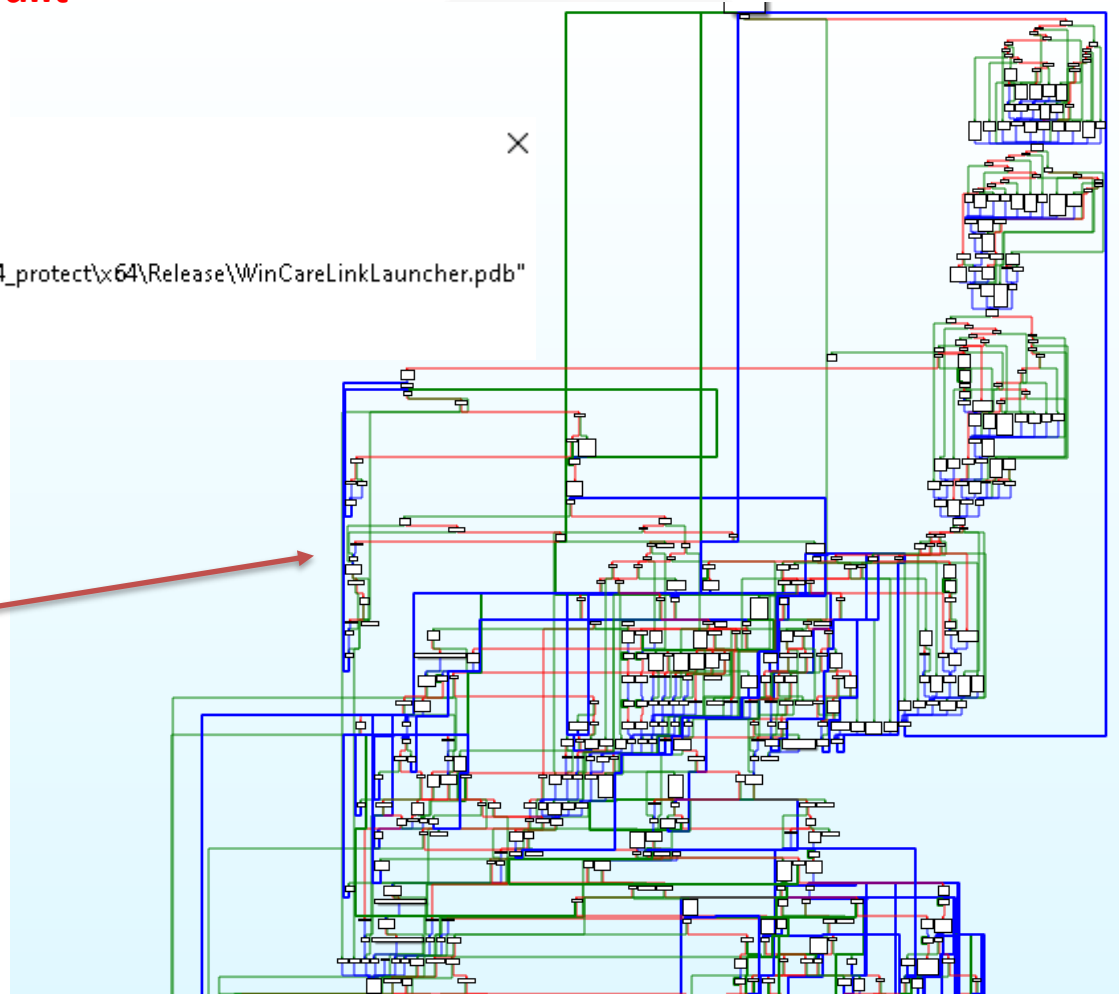
Static Software Analysis Example

Interesting Error from IDA Indicating how the program was built

 Please confirm

 The input file was linked with debug information and the symbol filename is:
"D:\Jenkins\workspace\uploader_pipeline\build\scp.x64_protect\x64\Release\WinCareLinkLauncher.pdb"
Do you want to look for this file at the specified path and the Microsoft Symbol Server?

View Flow Graph to begin to understand the program



Static Software Analysis Example

- Look at potentially useful imports
 - CreateFile, WriteFile, RegSetValue, fopen
 - Malloc, free, strcpy, gets, CreateProcess
 - Socket, connect, bind, CryptGenKey

```
.idata:00000001400733A8      extrn GetModuleHandleExW:qword
.idata:00000001400733A8      ; CODE XREF: sub_14005BE40+25?p
.idata:00000001400733A8      ; DATA XREF: sub_14005BE40+25?r
.idata:00000001400733B0 ; BOOL __stdcall WriteFile(HANDLE hfile, LPCVOID lpBuffer, DWORD nNumberOfBytesToWrite, LPDWORD lpNumberOfBytesWritten, LPOVERLAPPED lpOverlapped)
.idata:00000001400733B0      extrn WriteFile:qword          ; CODE XREF: sub_1400623C0+34E?p
.idata:00000001400733B0      ; sub_1400623C0+397?p ...
.idata:00000001400733B8 ; LPVOID
.idata:00000001400733B8
.idata:00000001400733B8
.idata:00000001400733B8
.idata:00000001400733C0 ; BOOL __st
.idata:00000001400733C0
.idata:00000001400733C0 ; int __std
.idata:00000001400733C8
.idata:00000001400733C8
.idata:00000001400733C8
.idata:00000001400733D0 ; int __std
.idata:00000001400733D0
.idata:00000001400733D0
.idata:00000001400733D0
.idata:00000001400733D0
.idata:00000001400733D0 ; BOOL __st
.idata:00000001400733D8
.idata:00000001400733D8
.idata:00000001400733D8
.idata:00000001400733D8 ; LCID __st
.idata:00000001400733E0
.idata:00000001400733E0
.idata:00000001400733E0
.idata:00000001400733E0
.idata:00000001400733E0 ; BOOL __st
.idata:00000001400733E8
.idata:00000001400733E8
```

Direction	Type	Address	Text
Up	p	sub_1400623C0+34E	call cs:WriteFile
Up	p	sub_1400623C0+397	call cs:WriteFile
Up	p	write_text_ansi_nolock(int,c...	call cs:WriteFile
Up	p	write_text_utf16le_nolock(in...	call cs:WriteFile
Up	p	write_text_utf8_nolock(int,c...	call cs:WriteFile
Up	p	sub_140062D9C+262	call cs:WriteFile
Up	r	sub_1400623C0+34E	call cs:WriteFile
Up	r	sub_1400623C0+397	call cs:WriteFile
Up	r	write_text_ansi_nolock(int,c...	call cs:WriteFile
Up	r	write_text_utf16le_nolock(in...	call cs:WriteFile
Up	r	write_text_utf8_nolock(int,c...	call cs:WriteFile
Up	r	sub_140062D9C+262	call cs:WriteFile

Map out and review all calls to useful imported functions

Static Software Analysis Example

- Map out installed files security: **EXEs, DLLs, Drivers, Services, Reg Keys**

FILE NAME	C:\Program Files\Medtronic\Carelink\Uploader\DSS\WinCareLinkLauncher.exe
IS PE	yes
FILE SIZE	0.767120361328125MB
MDSUM	2BCF5A8589360C5A9794774AD558A7C1
FILE PERMISSIONS	NT AUTHORITY\SYSTEM FullControl; BUILTIN\Administrators FullControl; BUILTIN\Users ReadAndExecute, Synchronize; APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES ReadAndExecute, Synchronize; APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES ReadAndExecute, Synchronize;
USED AS SERVICE	no
ARCHITECTURE	32BIT
SECURITY FEATURES	ASLR, DEP, SafeSEH, StrongNaming

Static Software Analysis Example

- Identify files with:
 - Keys
 - Passwords
 - Secrets
 - Operation hints
 - Ips / Servers

The screenshot shows a Windows file explorer window displaying the directory structure: C:\Program Files\Medtronic\Carelink\Uploader\DSS\localweb. The files listed are configuration, data_tokens, greylis, latestversion, metadata_token, patientinfo, servertime, uploadstatus, and whitelist. Two Notepad windows are open. The top window, titled 'patientinfo - Notepad', displays a JSON object with fields like 'firstName', 'lastName', 'country', 'clinicName', 'dateOfBirth', 'locale', 'tokenExpirationTime', 'sakeKey', 'controlCodes', 'deviceList', and 'diagnosticControlCode'. A red circle highlights the 'sakeKey' field. The bottom window, titled 'data_tokens - Notepad', displays a JSON object with fields like 'kind', 'repositories', and 'version'. A red circle highlights the 'secureToken' field within the 'repositories' array.

```
patientinfo - Notepad
{
  "firstName": "Paul",
  "lastName": "Smith",
  "country": "USA",
  "clinicName": "San Lupine Diabetes Center",
  "dateOfBirth": "1991-08-24",
  "locale": "en-US",
  "tokenExpirationTime": "2017-12-31T08:49:12.132Z",
  "sakeKey": "7D8v/FxUCW/shdEIPB4TiqtPysH74dCQC AOo3ARRzfI8uS1AgbY5psDAKNoojOf2Cc",
  "controlCodes": {
    "connectionTimeout": 3,
    "logLevel": 2,
    "traceUpload": "NONE",
    "encryptionKey": "thisisasimpleencryptionkeyandisverylong",
    "diagnosticControlCode": false
  },
  "deviceList": [
  ]
}

data_tokens - Notepad
{
  "kind": "BLENGP_SECURE_SNAPSHOT_CONTROL_RESPONSE",
  "repositories": [
    {
      "repositoryType": "USER_SETTINGS",
      "secureToken": "FwMDACcAAAAAAAAAu9Zav++x++PYrTuQezEeO/37htnaFuDvyNdTBzMU1/",
      "recache": false
    },
    {
      "repositoryType": "PUMP_HISTORY",
      "secureToken": "FwMDACcAAAAAAAAA211oP8UX+SdRv/cjM68k6iI4133eumG0Xvpk8axVOSv",
      "recache": false
    },
    {
      "repositoryType": "PUMP_SENSOR_HISTORY",
      "secureToken": "FwMDACcAAAAAAAAABBLWamN7e1u2YKRe9ZwWQ+J5ACSt42xjOisAzQ+Fx8E",
      "recache": false
    }
  ],
  "version": "1"
}
```

Static Software Analysis Example

- Disassemble JAVA files and look for device controls & secrets

SECRET HANDLING

```
package com.medtronic.diabetes.utils;  
  
import com.whitecrypton.skb.Cipher;  
import com.whitecrypton.skb.SkbException;  
import java.util.UUID;  
import libuploader.Loader;  
  
public abstract class SecurityUtils {  
    public static native byte[] encryptWithPadding(Cipher paramCipher, byte[] paramArrayOfbyte1, byte[] paramArrayOfbyte2);  
  
    public static native byte[] getCipherIv(UUID paramUUID);  
  
    public static native byte[] decryptWithNoPadding(Cipher paramCipher, byte[] paramArrayOfbyte1, byte[] paramArrayOfbyte2);  
  
    public static native byte[] getRandomIv();  
  
    public static native byte[] encrypt(Cipher paramCipher, byte[] paramArrayOfbyte1, byte[] paramArrayOfbyte2);  
  
    public static native byte[] encryptWithPadding(Cipher paramCipher, byte[] paramArrayOfbyte1, byte[] paramArrayOfbyte2);  
  
    public static native String iiiiiiiiiiiiii(object paramObject);  
  
    public static native byte[] xorArrays(byte[] paramArrayOfbyte1, byte[] paramArrayOfbyte2);  
  
    public static native byte[] decryptWithPadding(Cipher paramCipher, byte[] paramArrayOfbyte1, byte[] paramArrayOfbyte2);  
  
    public static native byte[] encryptWithBlockSizeExtension(Cipher paramCipher, byte[] paramArrayOfbyte1, byte[] paramArrayOfbyte2);  
  
    public static native byte[] encrypt(Cipher paramCipher, byte[] paramArrayOfbyte1, byte[] paramArrayOfbyte2);  
  
    public static native UUID retrieveSystemId();  
}
```

HARDWARE CONTROL

```
package com.ftdi;  
  
import com.medtronic.diabetes.fusion.device.common.Util;  
import com.sun.jna.Library;  
import com.sun.jna.Memory;  
import com.sun.jna.Platform;  
import com.sun.jna.Pointer;  
import com.sun.jna.Structure;  
import com.sun.jna.Structure.FieldOrder;  
import com.sun.jna.ptr.ByteByReference;  
import com.sun.jna.ptr.IntByReference;  
import com.sun.jna.ptr.PointerByReference;  
import com.sun.jna.ptr.ShortByReference;  
import java.nio.file.Path;  
import java.nio.file.Paths;  
import java.util.Objects;  
  
public interface FTD2XX extends Library {  
    public static final int DEVICE_INFO_LEN = 104;  
  
    static String getLibraryPath() {  
        String FTDI_DRIVER = "FTDI-Driver";  
        String DRIVERS = "Drivers";  
        Path path = null;  
        if (Platform.isWindows()) {  
            if (Platform.is64Bit()) {  
                path = Paths.get("Drivers", new String[] { "usb", "FTDI-Driver", "amd64", "ftd2xx64" });  
            } else {  
                path = Paths.get("Drivers", new String[] { "usb", "FTDI-Driver", "i386", "ftd2xx" });  
            }  
        } else if (Platform.isMac()) {  
            path = Paths.get("Uploader.bundle", new String[] { "Contents", "Home", "Drivers", "usb", "FTDI-Driver" });  
        } else if (Platform.isLinux()) {  
            path = Paths.get("/home/android/Projects/GL/uploader/deployment/layouts/lin.x64/Drivers/usb/FTDI-Driver/");  
        }  
        Objects.requireNonNull(path, "Error during initialization of path in FTD2XX");  
        return path.toAbsolutePath().toString();  
    }  
}
```

Dynamic Software Analysis Example

- Monitor everything the application does

- Registry modifications
- File system modifications
- Process table changes
- Network connections

Sysinternals for windows system monitoring

3:38:47.9212878 PM	M	WinCareLinkLauncher.exe	5068	Load Image	C:\Windows\System32\crypt32.dll
3:38:47.9231303 PM	M	WinCareLinkLauncher.exe	5068	CreateFileMapping	C:\Windows\System32\version.dll
3:38:47.9231539 PM	M	WinCareLinkLauncher.exe	5068	CreateFileMapping	C:\Windows\System32\version.dll
3:38:47.9232705 PM	M	WinCareLinkLauncher.exe	5068	Load Image	C:\Windows\System32\version.dll
3:38:47.9249084 PM	M	WinCareLinkLauncher.exe	5068	CreateFileMapping	C:\Windows\System32\imm32.dll
3:38:47.9249216 PM	M	WinCareLinkLauncher.exe	5068	QueryStandardInformation...	C:\Windows\System32\imm32.dll
3:38:47.9249414 PM	M	WinCareLinkLauncher.exe	5068	CreateFileMapping	C:\Windows\System32\imm32.dll
3:38:47.9260144 PM	M	WinCareLinkLauncher.exe	5068	Load Image	C:\Windows\System32\imm32.dll
3:38:47.9309343 PM	M	WinCareLinkLauncher.exe	5068	CreateFileMapping	C:\Windows\System32\msasn1.dll
3:38:47.9309631 PM	M	WinCareLinkLauncher.exe	5068	CreateFileMapping	C:\Windows\System32\msasn1.dll
3:38:47.9311194 PM	M	WinCareLinkLauncher.exe	5068	Load Image	C:\Windows\System32\msasn1.dll
3:38:47.9320743 PM	M	WinCareLinkLauncher.exe	5068	QueryNameInformationFile	C:\Program Files\Medtronic\Carelink\Uploader\DSS\WinCareLinkLauncher.exe
3:38:47.9323933 PM	M	WinCareLinkLauncher.exe	5068	Load Image	C:\Windows\System32\SHCore.dll
3:38:47.9325684 PM	M	WinCareLinkLauncher.exe	5068	Load Image	C:\Windows\System32\combase.dll
3:38:47.9370315 PM	M	WinCareLinkLauncher.exe	5068	CreateFileMapping	C:\Windows\System32\TextShaping.dll
3:38:47.9370578 PM	M	WinCareLinkLauncher.exe	5068	CreateFileMapping	C:\Windows\System32\TextShaping.dll
3:38:47.9371417 PM	M	WinCareLinkLauncher.exe	5068	Load Image	C:\Windows\System32\TextShaping.dll
3:38:47.9459782 PM	M	WinCareLinkLauncher.exe	5068	QueryStandardInformation...	C:\Windows\Fonts\StaticCache.dat
3:38:47.9460460 PM	M	WinCareLinkLauncher.exe	5068	CreateFileMapping	C:\Windows\Fonts\StaticCache.dat
3:38:47.9460607 PM	M	WinCareLinkLauncher.exe	5068	QueryStandardInformation...	C:\Windows\Fonts\StaticCache.dat
3:38:47.9460845 PM	M	WinCareLinkLauncher.exe	5068	CreateFileMapping	C:\Windows\Fonts\StaticCache.dat

Dynamic Software Analysis Example

- Run software in debugger
- Identify useful imports, set breakpoints

Base	Module	Party	Path	Address	Type	Ordinal	Symbol
00007FF78E010000	wincarelink1launcher	User	C:\Program Files\Medtronic\Carelink1\wincarelink1launcher.exe	00007FF80F9B9030	Symbol		WriteConsoleInputVDMA
00007FF805810000	version.dll	System	C:\Windows\System32\version.dll	00007FF80F9B9030	Export	1566	WriteConsoleInputVDMA
00007FF80AA50000	apphelp.dll	System	C:\Windows\System32\apphelp.dll	00007FF80F9B90C0	Symbol		WriteConsoleInputVDMW
00007FF80D100000	win32u.dll	System	C:\Windows\System32\win32u.dll	00007FF80F9B90C0	Export	1567	WriteConsoleInputVDMW
00007FF80D1C0000	ucrtbase.dll	System	C:\Windows\System32\ucrtbase.dll	00007FF80F9758F0	Symbol		WriteConsoleInputW
00007FF80D2C0000	msvc_p_win.dll	System	C:\Windows\System32\msvc_p_win.dll	00007FF80F9758F0	Export	1568	WriteConsoleInputW
00007FF80D460000	gdi32full.dll	System	C:\Windows\System32\gdi32full.dll	00007FF80F975900	Symbol		WriteConsoleOutputA
00007FF80D580000	crypt32.dll	System	C:\Windows\System32\crypt32.dll	00007FF80F975900	Export	1569	WriteConsoleOutputA
00007FF80D6E0000	wintrust.dll	System	C:\Windows\System32\wintrust.dll	00007FF80F975910	Symbol		WriteConsoleOutputAttribute
00007FF80D750000	kernelbase.dll	System	C:\Windows\System32\kernelbase.dll	00007FF80F975910	Export	1570	WriteConsoleOutputAttribute
00007FF80DA50000	bcrypt.dll	System	C:\Windows\System32\bcrypt.dll	00007FF80F975930	Symbol		WriteConsoleOutputCharacterA
00007FF80DA80000	user32.dll	System	C:\Windows\System32\user32.dll	00007FF80F975920	Export	1571	WriteConsoleOutputCharacterA
00007FF80DCD0000	msvcrt.dll	System	C:\Windows\System32\msvcrt.dll	00007FF80F975930	Symbol		WriteConsoleOutputCharacterW
00007FF80DD00000	gdi32.dll	System	C:\Windows\System32\gdi32.dll	00007FF80F975930	Export	1572	WriteConsoleOutputCharacterW
00007FF80DF20000	advapi32.dll	System	C:\Windows\System32\advapi32.dll	00007FF80F975940	Symbol		WriteConsoleOutputW
00007FF80E350000	shlwapi.dll	System	C:\Windows\System32\shlwapi.dll	00007FF80F975940	Export	1573	WriteConsoleOutputW
00007FF80E640000	shell32.dll	System	C:\Windows\System32\shell32.dll	00007FF80F975600	Symbol		WriteConsoleW
00007FF80EE30000	rpcrt4.dll	System	C:\Windows\System32\rpcrt4.dll	00007FF80F975600	Export	1574	WriteConsoleW
00007FF80F720000	sechost.dll	System	C:\Windows\System32\sechost.dll	00007FF80F9752E0	Symbol		WriteFile
00007FF80F950000	kernel32.dll	System	C:\Windows\System32\kernel32.dll	00007FF80F9752E0	Export	1575	WriteFile
00007FF80FA50000	ntdll.dll	System	C:\Windows\System32\ntdll.dll	00007FF80F9752F0	Symbol		WriteFileEx
				00007FF80F9752F0	Export	1576	WriteFileEx

Type	Address	Module/Label/Exception	State	Disassembly	Hits	Summary
Software	00007FF778E058270	<wincarelink1launcher.exe.OptionalHeader.AddressOfEntryPoint>	One-time	sub rsp,28	0	entry breakpoint
	00007FF800AA8890	<user32.dll.LoadStringW>	Enabled	sub rsp,38	0	
	00007FF80DF36900	<advapi32.dll.CryptCreateHashStub>	Enabled	jmp qword ptr ds:[7FF80DFCC088]	0	
	00007FF80F96BA80	<kernel32.dll.lstrncmpwStub>	Enabled	jmp qword ptr ds:[&lstrncmpw]	0	
	00007FF80F96C790	<kernel32.dll.lstrncmpAStub>	Enabled	jmp <kernel32.lstrncmpA>	0	
	00007FF80F96D370	<kernel32.dll.GetExitCodeProcessImplementation>	Enabled	mov qword ptr ss:[rsp+8],rbx	0	
	00007FF80F96E360	<kernel32.dll.FatalExit>	Enabled	sub rsp,28	0	
	00007FF80F972160	<kernel32.dll.lstrncpyw>	Enabled	mov r8,rcx	0	
	00007FF80F9751F0	<kernel32.dll.ReadFile>	Enabled	jmp qword ptr ds:[&ReadFile]	0	
	00007FF80F9752E0	<kernel32.dll.WriteFile>	Enabled	jmp qword ptr ds:[&WriteFile]	0	
	00007FF80FA0D880	<ntdll.dll.lstrncmp>	Enabled	sub rsp,28	0	
	00007FF80FA0D9A0	<ntdll.dll.lstrncmp>	Enabled	sub rsp,28	0	



Dynamic Software Analysis Example

- Look for clues when breakpoints are hit

Paused INT3 breakpoint at <kernel32.ReadFile> (00007FF80F9751F0)!

<http://blest.inrange.me:7095/api/dataupload>

```
RAX 0000000000000000
RBX 0000000000000000
RCX 00000000000001BC
RDX 000002684896C310
RBP 0000000000000100
RSP 000000D0E9AFE6F8
RSI 000002684896BDC0
RDI 0000000000000000

R8 0000000000000100
R9 000000D0E9AFE7B8
R10 000000000000000A
R11 0000000000000000
R12 0000000000000003
R13 0000000000000100
R14 000000000000001B
R15 000002684896C310

RIP 00007FF80F9751F0
RFLAGS 0000000000000344
ZF 1 PF 1 AF 0
OF 0 SF 0 DF 0
CF 0 TF 1 IF 1
```

L'S'
"threadPriority=true\nble.base.url=http://blest.inrange.me:7095/api/dataupload/v1\
&"threadPriority=true\nble.base.url=http://blest.inrange.me:7095/api/dataupload/v1\
"threadPriority=true\nble.base.url=http://blest.inrange.me:7095/api/dataupload/v1\
<ker> • 00007FF80F9751F0 - FF25 7ABF0500 jmp qword ptr ds:[<&ReadFile>] ReadFile
• 00007FF80F9751F6 CC int3
• 00007FF80F9751F7 CC int3
• 00007FF80F9751F8 CC int3
• 00007FF80F9751F9 CC int3
• 00007FF80F9751FA CC int3
• 00007FF80F9751FB CC int3
• 00007FF80F9751FC CC int3
• 00007FF80F9751FD CC int3
• 00007FF80F9751FE CC int3
• 00007FF80F9751FF CC int3
• 00007FF80F975200 - FF25 72BF0500 jmp qword ptr ds:[<&ReadFileEx>] ReadFileEx
• 00007FF80F975206 CC int3
• 00007FF80F975207 CC int3
• 00007FF80F975208 CC int3
• 00007FF80F975209 CC int3
• 00007FF80F97520A CC int3
• 00007FF80F97520B CC int3
• 00007FF80F97520C CC int3
• 00007FF80F97520D CC int3
• 00007FF80F97520E CC int3
• 00007FF80F97520F CC int3

Dynamic Software Analysis Example

- Identify app communications & analyze

The image displays the Wireshark network protocol analyzer interface. The top pane shows a list of captured packets, including TCP and DNS traffic. The middle pane shows the 'Endpoint Settings' for Ethernet, with a table of IP addresses and their corresponding traffic statistics. The bottom pane shows the 'I/O Graphs' for Ethernet, which is a line graph plotting 'Packets/1 sec' against 'Time (s)'. The graph shows a significant spike in traffic around 9.5 seconds. Below the graph, there is a table of enabled graphs and various settings for the I/O graph.

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
13.107.246.66	4	299 bytes	3	245 bytes	1	54 bytes
13.248.212.111	6	378 bytes	3	198 bytes	3	180 bytes
20.7.215.90	22	7,532 KiB	12	2,483 KiB	10	5,049 KiB
20.42.144.52	2	126 bytes	1	66 bytes	1	60 bytes
34.214.65.117	2	126 bytes	1	66 bytes	1	60 bytes
35.186.224.24	3	180 bytes	1	60 bytes	2	120 bytes
44.196.121.44	3	335 bytes	1	149 bytes	2	186 bytes
52.177.83.91	3	238 bytes	1	87 bytes	2	151 bytes
54.85.240.191	3	335 bytes	1	149 bytes	2	186 bytes
57.144.104.141	1	86 bytes	0	0 bytes	1	86 bytes
57.144.104.145	12	888 bytes	4	316 bytes	8	572 bytes
99.83.181.31	2	126 bytes	1	66 bytes	1	60 bytes
104.244.42.194	12	950 bytes	7	534 bytes	5	416 bytes
142.250.72.3	18	8,288 KiB	10	4,795 KiB	8	3,493 KiB
142.250.72.10	20	8,169 KiB	11	4,562 KiB	9	3,607 KiB
142.250.72.42	13	1,746 KiB	7	818 bytes	6	970 bytes
142.250.72.46	35	13,337 KiB	17	3,470 KiB	18	9,867 KiB
142.250.72.66	20	8,872 KiB	11	4,716 KiB	9	4,156 KiB
142.250.72.67	8	808 bytes	4	412 bytes	4	396 bytes
162.254.193.74	2	173 bytes	1	60 bytes	1	113 bytes
173.194.54.168	1,099	1,198 MiB	971	1,166 MiB	128	32,778 KiB
184.105.99.43	11	1,761 KiB	6	988 bytes	5	815 bytes
192.168.101.1	4	446 bytes	2	280 bytes	2	166 bytes
192.168.101.43	1	101 bytes	1	101 bytes	0	0 bytes
192.168.101.69	7	1,969 KiB	4	1,678 KiB	3	298 bytes
192.168.101.152	5	395 bytes	5	395 bytes	0	0 bytes
192.168.101.173	5	353 bytes	2	108 bytes	3	245 bytes
192.168.101.175	1,310	1,254 MiB	232	63,751 KiB	1,078	1,192 MiB
192.168.101.214	20	3,891 KiB	20	3,891 KiB	0	0 bytes
192.168.101.255	4	252 bytes	0	0 bytes	4	252 bytes
199.232.73.140	2	147 bytes	1	67 bytes	1	80 bytes
224.0.0.22	1	54 bytes	0	0 bytes	1	54 bytes
224.0.0.251	17	3,146 KiB	0	0 bytes	17	3,146 KiB
239.255.255.250	5	1,007 bytes	0	0 bytes	5	1,007 bytes

Mobile App Analysis

- Static Analysis
 - MobSF
 - IDA Pro, Ghidra, Radare2, JD-GUI
- Dynamic Analysis
 - Android Studio
 - Logcat, adb, Profiler
 - Fiddler
 - APK-MITM

```
public final void apply(Bitmap bitmap) {
    PowerManager pm = (PowerManager) myContext.getSystemService(Context.POWER_SERVICE);
    PowerManager.WakeLock wakeLock = pm.newWakeLock(PARTIAL_WAKE_LOCK, tag: "filter:" + getClass().getSimpleName());
    wakeLock.acquire();
    int[] pixelsDst = new int[bitmap.getWidth() * bitmap.getHeight()];
    int[] pixelsSrc = new int[bitmap.getWidth() * bitmap.getHeight()];
}
```

System Event	Description	Called By	Timeline
Wake Lock: Partial	filter:GrayscaleFilter	Filter.apply	45.0

Mobile App Static Analysis

1. Acquire APK
2. Scan APK with MobSF

The screenshot displays the MobSF web interface for the analysis of an APK file named 'MiniMed™ Mobile_2.5.0_APKPure.apk'. The interface is divided into several sections:

- APP SCORES:** Shows a Security Score of 55/100 and Trackers Detection of 0/432. A 'MobSF Scorecard' button is visible.
- FILE INFORMATION:** Lists file details: File Name (MiniMed™ Mobile_2.5.0_APKPure.apk), Size (46.34MB), MD5 (b72ab77eed2741cf101e41d2b069cb17), SHA1 (ddac3e5845a1e9ba8670aa5395c3ff4bc70b60c5), and SHA256 (7192079be349ef50a07803133b0ad1bfb5b1f37f83f97e4a1926d594a20df69).
- APP INFORMATION:** Lists app metadata: App Name (MiniMed™ Mobile), Package Name (com.medtronic.diabetes.minimedmobile.eu), Main Activity (com.medtronic.minimed.ui.startupwizard.SplashScreenActivity), Target SDK (33), Min SDK (28), Max SDK, Android Version Name (2.5.0), and Android Version Code (917).
- Summary Cards:** Four cards show counts for Activities (54), Services (16), Receivers (6), and Providers (5). Each card has a 'View' button.
- Exported Elements:** Below the summary cards, four boxes show 'Exported' counts: Activities (4), Services (0), Receivers (2), and Providers (0).
- SCAN OPTIONS:** Includes buttons for 'Rescan', 'Manage Suppressions', and 'Start Dynamic Analysis'.
- DECOMPILED CODE:** Includes buttons for 'View AndroidManifest.xml', 'View Source', 'View Smali', 'Download Java Code', 'Download Smali Code', and 'Download APK'.

APPLICATION PERMISSIONS

Search:

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.AUTHENTICATE_ACCOUNTS	dangerous	act as an account authenticator	Allows an application to use the account authenticator capabilities of the Account Manager, including creating accounts as well as obtaining and setting their passwords.

Mobile App Dynamic Analysis

1. Create Android Emulator (not all APKs will work)
2. Install MITMProxy Certificate
3. Configure Android Web Proxy Settings
4. Use MITMProxy to analyze/modify web traffic
 1. Can use Burp and Burp Cert
5. If App Uses Cert Pinning use apk-mitm to strip cert from APK
 1. Large APKs can be stripped on a temporary high resource AWS node

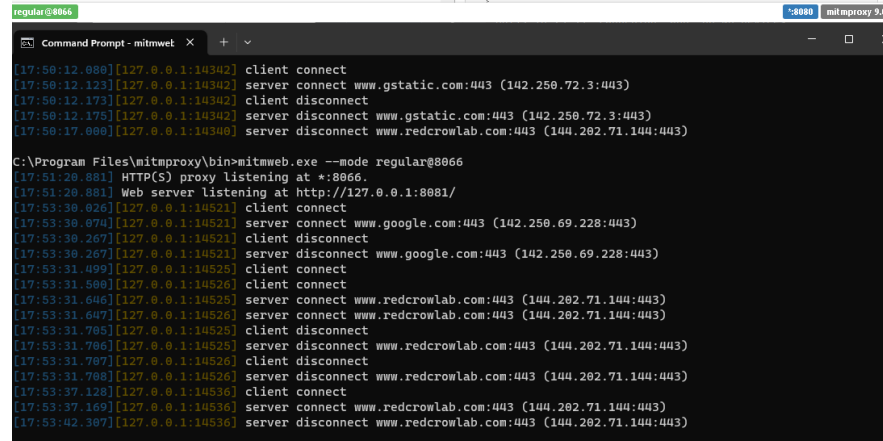
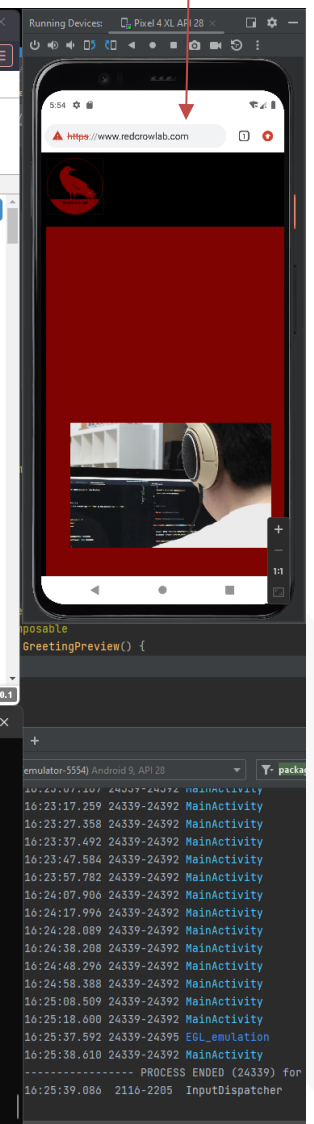
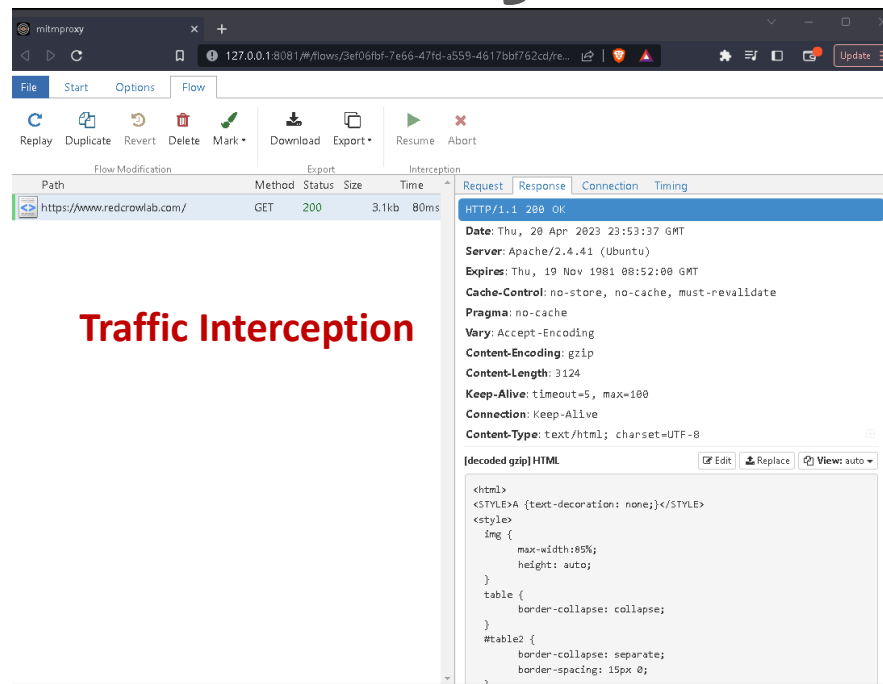
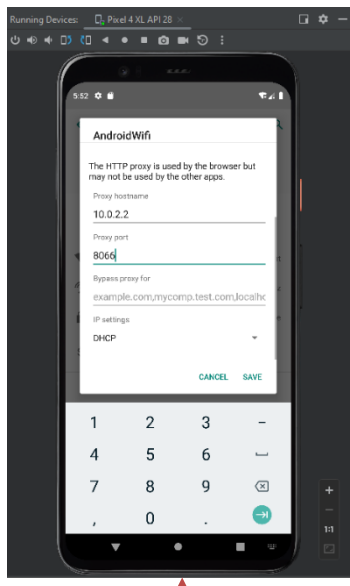
```
user@ubuntu:~$ apk-mitm tiktok-29-1-16.apk
[ apk-mitm v1.2.1
  apktool v2.6.1
  uber-apk-signer v1.2.1

Using temporary directory:
/tmp/apk-mitm-027242973f6dc4336bb3b1b625ae0644

✓ Checking prerequisites
✚ Decoding APK file
  → Loading resource table from file: /tmp/apk-mitm-027242973f6dc4336bb3b1b625ae0644/framework/1.apk
Applying patches
Encoding patched APK file
Signing patched APK file
```

Mobile Analysis

Analyzed Website



MITM Certificate Install

Android Emulator Web Proxy Setup

Tool Development

- Build tools to automate tasks, replicate attacks, and collect instrumentation data

Popular repositories Customize your pins

rcDetectVirtual Public
PoC Code to detect if running in a virtual machine
● C

rcPCAPanalyzer Public
Anomaly detection in Full Packet Captures
● Python

rcNixRecon Public
Automates recon of Unix based system
● Shell

rcHTTPExfil Public
Exfiltrates base64 encoded data over HTTP
● Python

rcProcDump Public
Dumps a Linux process memory
● Shell

rcFileScan Public
Collects ELF File Format data
● Python

Anthony S. Clark
redcrowlab
Reverse Engineer, Greybeard Hacker. I am not a coder so please be kind.



Tool Development

```
rcWinFileScan.ps1 X
1 #####
2 # rcWinFileScan - PowerShell Script for analyzing a programs directory security.
3
4 # Import required module for PE analysis
5 #Install-Module -Name PEsecurity -Force -SkipPublisherCheck
6
7 param ([string]$dirPath)
8
9 #####
10 # Function to get file hashes
11 function Get-FileHashes {
12     param ([string]$filePath)
13     $md5 = Get-FileHash -Path $filePath -Algorithm MD5
14     $sha256 = Get-FileHash -Path $filePath -Algorithm SHA256
15     return $md5.Hash, $sha256.Hash
16 }
17
18 #####
19 # Function to get PE file info
20 function Get-PEInfo {
21     param ([string]$filePath)
22
23     $peInfo = Get-PESecurity -file $filePath
24     $arch = if ($peInfo.Is64Bit) { "64BIT" } else { "32BIT" }
25     $secFeatures = @()
26
27     if ($peInfo.ASLR) { $secFeatures += "ASLR" }
28     if ($peInfo.DEP) { $secFeatures += "DEP" }
29     if ($peInfo.SEH) { $secFeatures += "SEH" }
30     if ($peInfo.SafeSEH) { $secFeatures += "SafeSEH" }
31     if ($peInfo.StrongNaming) { $secFeatures += "StrongNaming" }
```

```
[* FILE NAME *] C:\Program Files\Medtronic\Carelink\Uploader\DSS\vc_redist.exe
[* FILE SIZE *] 24.0657730102539MB
[* MDSUM * ] CDC5D5EE259D8071FA82F522C5C7D6E
[* SHA256 * ] CE6593A1520591E7DEA2B93FD03116E3FC3B3821A0525322B0A430FAA6B3C0B4
[* FILE PERMISSIONS *] NT AUTHORITY\SYSTEM FullControl; BUILTIN\Administrators FullControl; BUILTIN\Users ReadAndExecute, Synchronize; APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES ReadAndExecute, Synchronize;
[* IS PE *] yes
[* USED AS SERVICE *] no
[* ARCHITECTURE *] 32BIT
[* SECURITY FEATURES * ] ASLR, DEP, SafeSEH, StrongNaming

[* FILE NAME *] C:\Program Files\Medtronic\Carelink\Uploader\DSS\WinCareLinkLauncher.exe
[* FILE SIZE *] 0.767120361328125MB
[* MDSUM * ] 2BCF5A8589360C5A9794774AD558A7C1
[* SHA256 * ] 04CA6F0B8300C2032A8C97DC16CC2E414B66551ED332F00A376077FFAD26B486
[* FILE PERMISSIONS *] NT AUTHORITY\SYSTEM FullControl; BUILTIN\Administrators FullControl; BUILTIN\Users ReadAndExecute, Synchronize; APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES ReadAndExecute, Synchronize;
[* IS PE *] yes
[* USED AS SERVICE *] no
[* ARCHITECTURE *] 32BIT
[* SECURITY FEATURES * ] ASLR, DEP, SafeSEH, StrongNaming

[* FILE NAME *] C:\Program Files\Medtronic\Carelink\Uploader\DSS\Drivers\serial
[* FILE SIZE *] 9.5367431640625E-07MB
[* MDSUM * ]
[* SHA256 * ]
[* FILE PERMISSIONS *] NT SERVICE\TrustedInstaller FullControl; NT SERVICE\TrustedInstaller 268435456; NT AUTHORITY\SYSTEM FullControl; NT AUTHORITY\SYSTEM 268435456; BUILTIN\435456; BUILTIN\Users ReadAndExecute, Synchronize; BUILTIN\Users -1610612736; CREATOR OWNER 268435456; APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES ReadAndExecute, Synchronize; APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES ReadAndExecute, Synchronize; APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES ReadAndExecute, Synchronize;
[* IS PE *] no
```


Tool Development

```
root@~:~/data/medtronic/rcFileScan# python rcPEfileScan.py CareLinkUploader-AC
C-7350-3.11.0-windows-installer.exe
[+] File Type: PE
[+] File Size: 178548960 bytes
[+] MD5: cf0a57d5441239da426922e481a2a85e
[+] SHA256: 62b9e6928b3884bc67868423dc9a63d76bb05118ae7c5ada1ee453355981f383
[+] Entropy: 7.9983
[+] Number of Sections: 11
[+] Section Names: ['.text', '.data', '.rdata', '.eh_frame', '.bss', '.edata', '.idata',
'.CRT', '.tls', '.rsrc', '.reloc']
[+] Imports:
  ADVAPI32.DLL
  GetSecurityDescriptorOwner
  GetSidIdentifierAuthority
  GetUserNameA
  GetUserNameW
  RegCloseKey
  RegOpenKeyExA
  RegQueryValueExA
  listen
  ntohs
  recv
  select
  send
  setsockopt
  socket
[+] Exports:
  TclKit_AppInit
  TclKit_SetKitPath
[+] Dependencies: {'GDI32.dll', 'SHELL32.DLL', 'OLEAUT32.DLL', 'WS2_32.dll', 'OLE32.dll',
'USER32.dll', 'COMCTL32.DLL', 'msvcrt.dll', 'COMDLG32.DLL', 'IMM32.DLL', 'ADVAPI32.DLL',
'KERNEL32.dll'}
[+] Security Options:
  DEP: True
  ASLR: True
  NX: True
  SEH: True
  CFG: False
[+] Compile Time: 2023-01-04 15:12:35
[+] Compiler Version: 2.22
```

Knowledge Base

Home New Device

🔍 search for device, component, filename, m5sum 🗣️

- MikroTik mAP2nd Router
- + Catalog
 - Make: MikroTik
 - Model: RBmAP2m0
 - Serial Number: DE500FA1A1D4/141/r2
- + Open Source Research
- + Manuals & Datasheets

- Firmware Analysis

- + Components
 - NANYA2113 NT5TU32M16FG-AC
 - Winbond 250128JVSM 3121

+ Debugging Interfaces & Steps

- + RF Survey Results
 - Spectrum Analysis
 - Bluetooth
 - Wifi
 - GSM

- + Network Survey
 - Open Ports
 - Full Packet Capture
 - Burp Scan

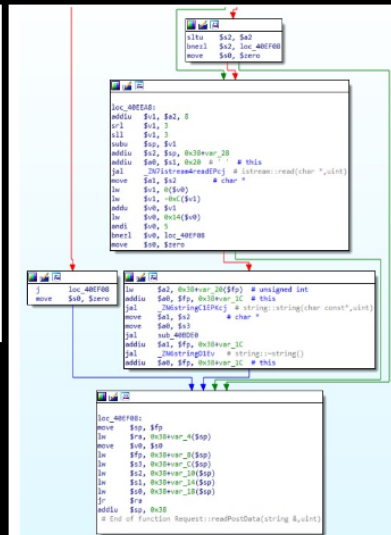
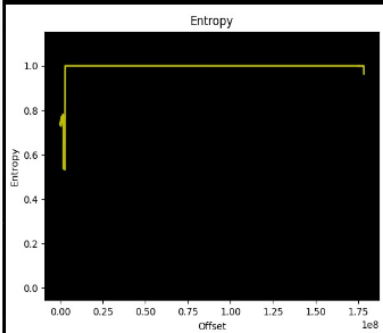
+ Vulnerabilities

+ Testing Tools

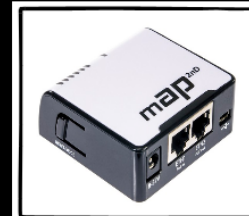
Firmware Analysis

Firmware Type: Nova Package
Firmware Version: 6.38
Architecture: MIPS
Checksum: df0a57d5463239da426922e481a2a85f

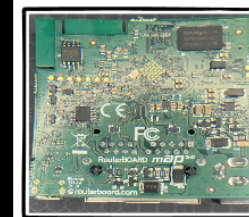
Firmware Call Graph



EXTERNAL PHOTOS



INTERNAL PHOTOS



← Upload & Scan Images

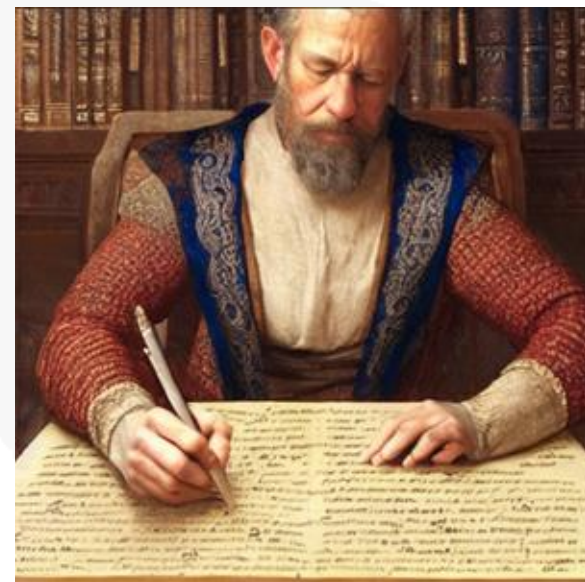
Click to zoom

Edit Device

Documentation

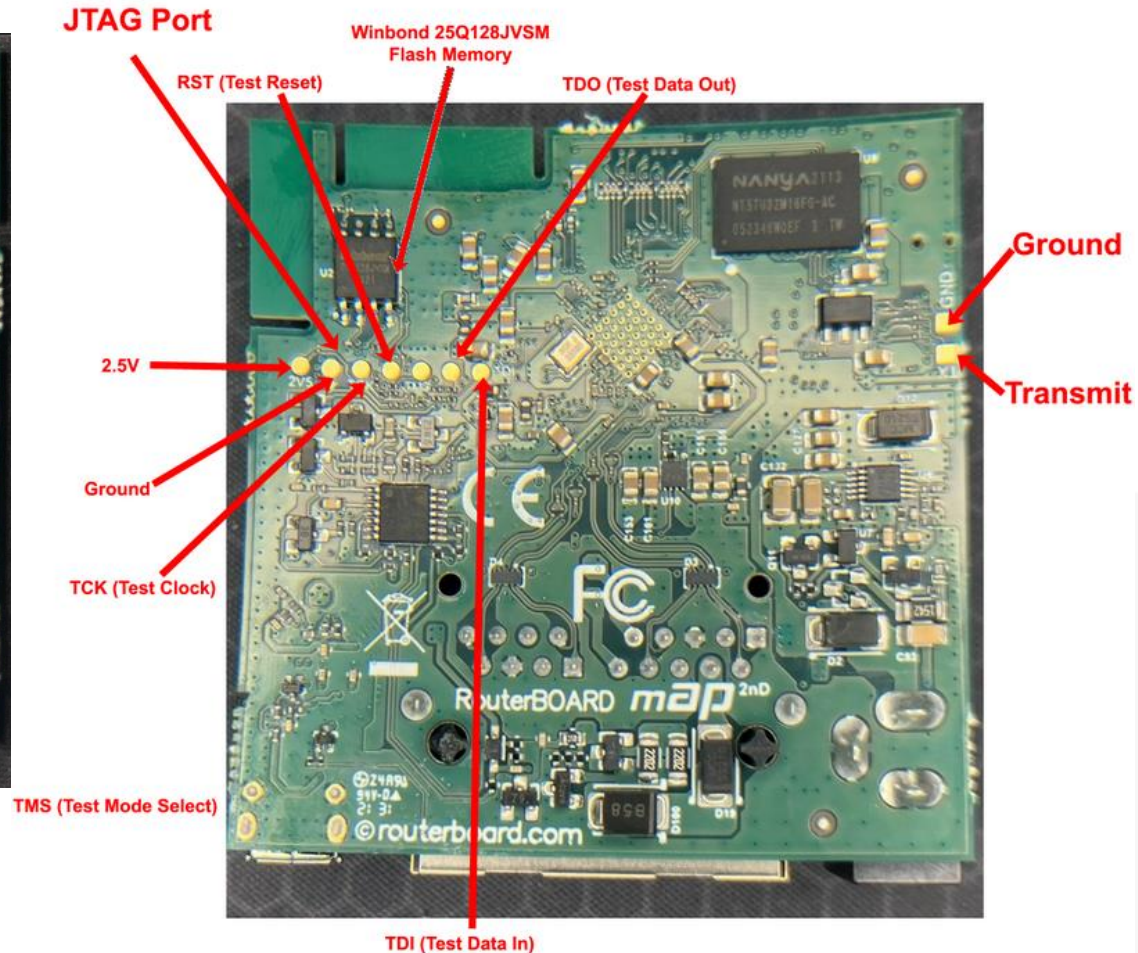
“If You Didn’t Document It, You Didn’t Do It”

- Sections of report for different audiences
 - Executive Summary (**Management**)
 - High level technical details (**Devs & Sysadmins**)
 - Deep technical details (**other RE’s**)
- Photos & device catalog
- Every test & results
 - Description of test conditions & steps to reproduce
- 1 Page per \$1000
- CD, USB, Zip with all supporting data
 - PCAPS, RF captures, debug logs, scans



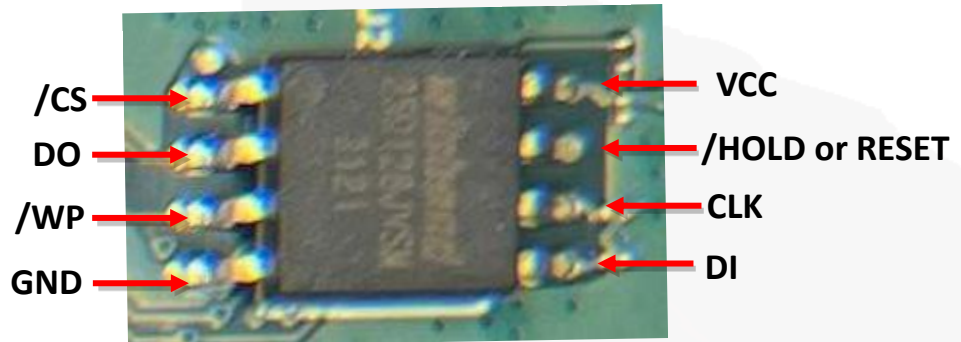
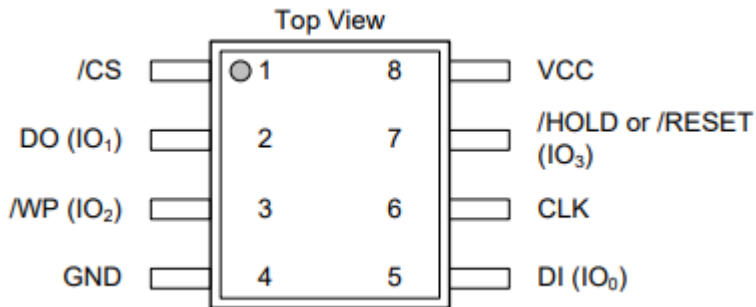
Example Case Study

- Mikrotik mAP2nd Router

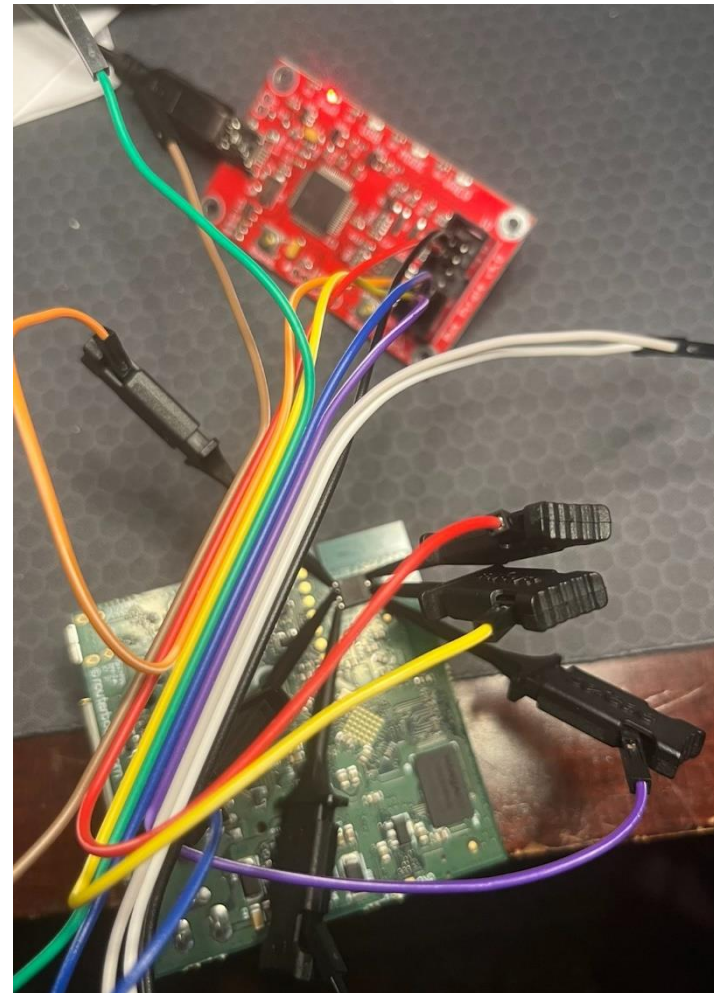
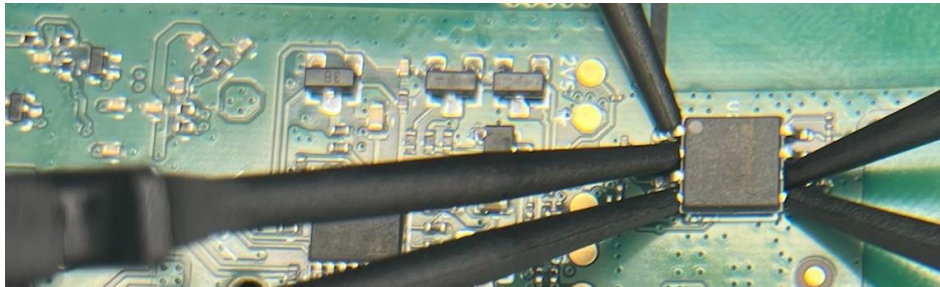


Example Case Study

- Winbond 25Q128JVSM
 - 3V 128M-BIT SERIAL FLASH MEMORY
 - Datasheet: <https://datasheetspdf.com/pdf-file/1462146/Winbond/25Q128JVSM/1>
 - Pin Configuration From Data Sheet:



Example Case Study



WIRE COLOR	WB CHIP PINS	BUSPIRATE PINS
- Yellow	- CS	- CS
- Green	- DO	- MISO
- Blue	- WP	
- Purple	- GND	- GND
- Black	- VCC	- +3.3
- Brown	- RES	
- Red	- CLK	- CLK
- Orange	- DI	- MOSI

Example Case Study

- **Firmware Dump:**

```
# flashrom -p buspirate_spi:dev=/dev/ttyUSB0,spispeed=500k -r firmware_dump.bin -vvv
```

```
0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff
0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff
0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff
0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff
0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff
0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff
0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff 0xff
```

done.

```
programmer_unmap_flash_region: unmapped 0x0000000000000000
```

```
buspirate_sendrecv: write 1, read 0 Sending 0x00
```

```
buspirate_sendrecv: write 0, read 4 , receiving 0x42 0x42 0x49 0x4f
```

```
buspirate_sendrecv: write 0, read 1 , receiving 0x31
```

```
Raw bitbang mode version 1
```

```
buspirate_sendrecv: write 1, read 0 Sending 0x0f
```

```
Bus Pirate shutdown completed.
```

```
-rw-r--r-- 1 root root 16777216 Sep 9 17:47 firmware_dump.bin
```

Alternative Tools:

- OpenOCD
- PyOCD

Example Case Study

- Search file for signatures:

```
# binwalk -B firmware_dump.bin
```

DECIMAL	HEXADECIMAL	DESCRIPTION
1936	0x790	CRC32 polynomial table, little endian
950480	0xE80D0	xz compressed data
6369136	0x612F70	gzip compressed data, has original file name: "roteros.dll", from Unix, last modified: 2021-05-31
9013347	0x898863	gzip compressed data, has original file name: "secure.dll", from Unix, last modified: 2021-05-31
9052581	0x8A21A5	gzip compressed data, has original file name: "wlan6.dll", from Unix, last modified: 2021-05-31
9130578	0x8B5252	gzip compressed data, has original file name: "iframe.html", from Unix, last modified: 2021-05-31
9131091	0x8B5453	PNG image, 7 x 7, 8-bit/color RGBA, non-interlaced
9132652	0x8B5A6C	PNG image, 512 x 64, 8-bit/color RGBA, non-interlaced
9218884	0x8CAB44	xz compressed data
9248368	0x8D1E70	xz compressed data
9288416	0x8DBAE0	xz compressed data
9288447	0x8DBAFF	gzip compressed data, has original file name: "dhcp.dll", from Unix, last modified: 2021-05-31 07:33:47
9368892	0x8EF53C	gzip compressed data, has original file name: "ipv6.dll", from Unix, last modified: 2021-05-31 07:36:07
9451262	0x9036FE	gzip compressed data, has original file name: "ppp.dll", from Unix, last modified: 2021-05-31 07:35:12
9551692	0x91BF4C	xz compressed data
9612800	0x92AE00	xz compressed data
9612831	0x92AE1F	gzip compressed data, has original file name: "master-min.js", from Unix, last modified: 2021-05-31
07:12:40		
9698952	0x93FE88	gzip compressed data, has original file name: "curve255-min.js", from Unix, last modified: 2021-05-31
07:12:39		
9784725	0x954D95	gzip compressed data, has original file name: "ipv6.jg", from Unix, last modified: 2021-05-31 07:36:07
9791354	0x95677A	gzip compressed data, has original file name: "mpls.jg", from Unix, last modified: 2021-05-31 07:35:47
11049606	0xA89A86	ELF, 32-bit MSB MIPS64 executable, MIPS, version 1 (SYSV)
13527889	0xCE6B51	Neighborly text, "neighbor discovery-settings set discover-interface-list=LAN /tool mac-server set
allowed-interface-list=LAN"		

Example Case Study

- Extract the files:

```
# binwalk --run-as=root -e -M firmware_dump.bin
```

DECIMAL	HEXADECIMAL	DESCRIPTION
1936	0x790	CRC32 polynomial table, little endian

Scan Time: 2023-09-09 17:54:59
Target File: /root/_firmware_dump.bin.extracted/E80D0
MD5 Checksum: 6eb40faa97ee5e0dd7d68c8fe51cd770
Signatures: 411

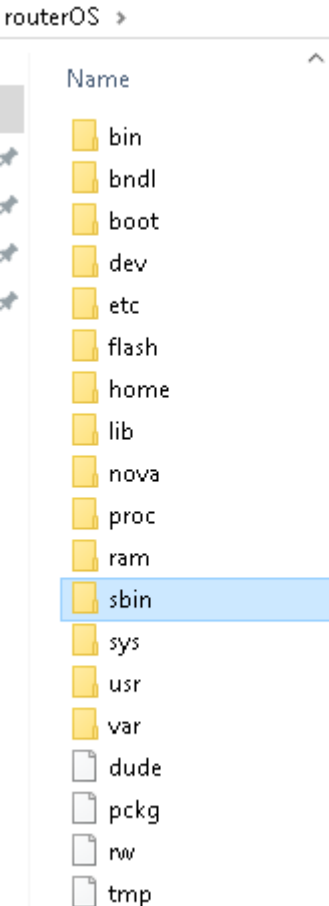
DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	ELF, 32-bit MSB MIPS64 executable, MIPS, version 1 (SYSV)

Scan Time: 2023-09-09 17:54:59
Target File: /root/_firmware_dump.bin.extracted/FD1FC
MD5 Checksum: 3c4464073496b309285d7339526e58ed
Signatures: 411

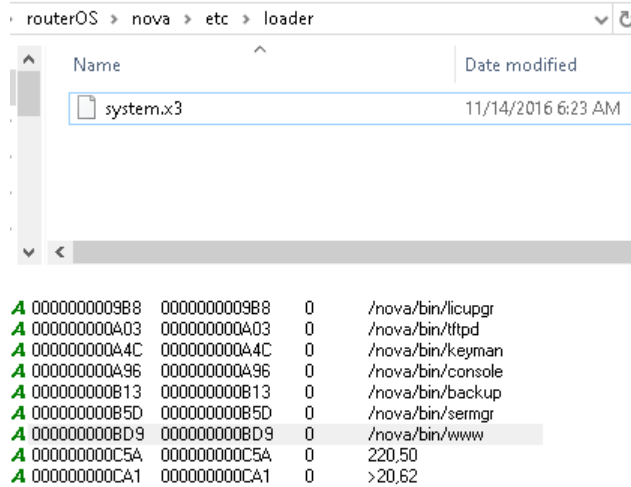


Example Case Study

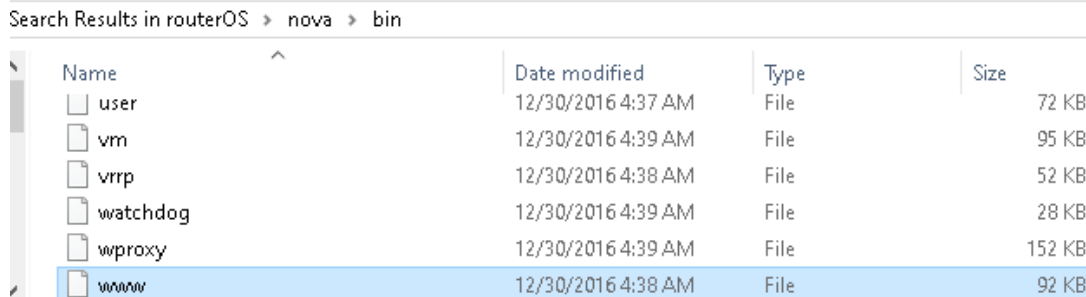
1. Filesystem Extracted From Firmware



2. Identify Loaded Binaries by looking at strings in the system.x3 binary



3. Find the www binary



4. Disassemble the MIPS www binary & identify potential vulns



Example Case Study

- Check extracted files:

```
$ cat iframe.html
```

```
<html>
<body
onload="parent.generateContent(parent.location.hash.substr(1));"
>
</body>
</html>
<html>
<head>
  <link rel="stylesheet" type="text/css"
href="master.css"></link>
</head>
<style>
  form {
    display: inline;
    width: 100%;
  }
  input {
    width: 100%;
    height: 26px;
    background: #fff;
    border: 1px solid #888;
    margin: 0;
    padding: 1px;
    font-family: verdana, arial, helvetica, sans-serif;
    font-size: 12px;
    box-shadow: none;
    -moz-box-shadow: none;
  }
</style>
<body style="margin:0; white-space: nowrap">
  <form id="form" action="/jsproxy/upload" method="post"
  enctype="multipart/form-data">
    <input id="file" type="file" name="file">
  </form>
</body>
</html>
```

- Analyze binaries:

```
$ strings A89A86.elf |more
mips
RouterOS for mipsbe RouterBOARDS, bridgeports.dat
bridgeports.idx
switch-config.dat
ether2
wlan10

#| Welcome to RouterOS!
#| RouterMode:
#| * WAN port is protected by firewall and enabled DHCP client
#| * Wireless and Ethernet interfaces (except WAN port/s)
#| LAN Configuration:
#|   IP address 192.168.88.1/24 is set on bridge (LAN port)
#|   DHCP Server: enabled;
#|   DNS: enabled;
#| wlan1 Configuration:
#|   mode:                ap-bridge;
#|   band:                 2ghz-b/g/n;
#|   wpa2:                 no;
#|   ht-extension:        20/40mhz-XX;
:if ($action = "apply") do={
  # wait for interfaces
  :local count 0;
  :while ([/interface ethernet find] = "") do={
    :if ($count = 30) do={
      :log warning "DefConf: Unable to find ethernet interfaces";
      /quit;
    }
    :delay 1s; :set count ($count +1);
  };
  :local count 0;
  :while ([/interface wireless print count-only] < 1) do={
    :set count ($count +1);
    :if ($count = 40) do={
      :log warning "DefConf: Unable to find wireless
interface(s)";
      /ip address add address=192.168.88.1/24 interface=ether1
comment="defconf";
      /quit
```

Questions



If you have questions or need further details
please contact:

<https://www.redcrowlab.com>

asclark@redcrowlab.com

