



Gray Market Medical Lab

Internal Report

Conor Walsh

Feb 2019



Agenda

- Why We're Here
- Building the Lab
- Hospira Abbot Plum A+ IV Pump
- Philips Intellivue MP50 Patient Monitor
- Data Export Interface Programming Guide

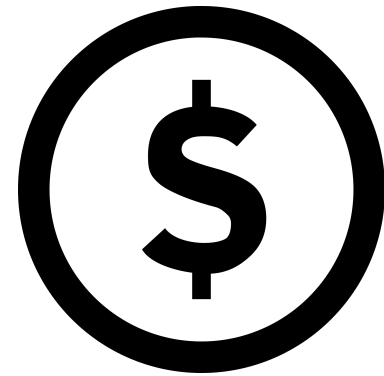


Why We're Here

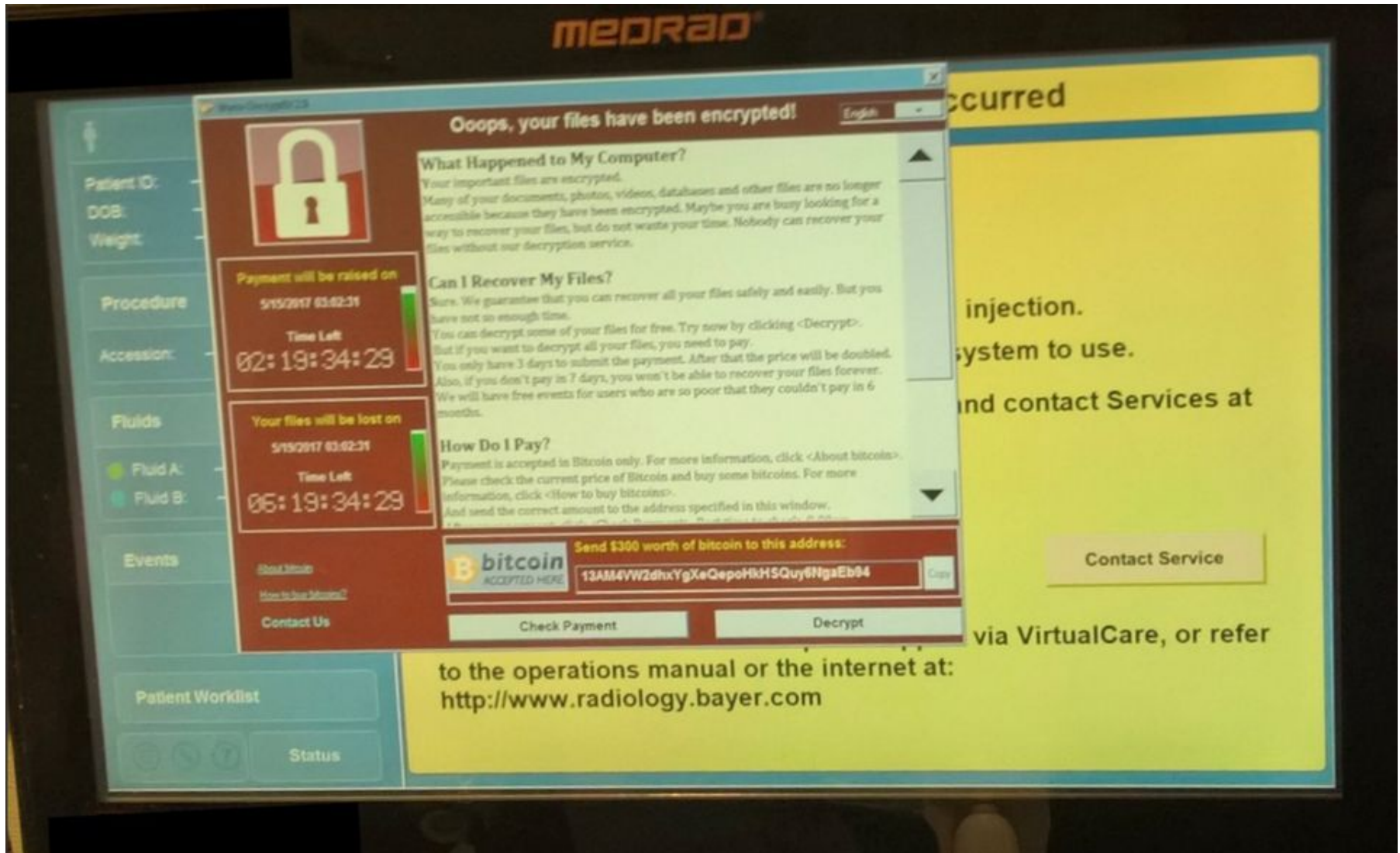
Why Medical Devices?

Any of these are reasons to fight the good fight...

- Hospitals have money to spend
- HIPAA Regulations
- Sticking it to the FDA
- Heart-Stopping Drama
- Mainlining Substances
- Radiation Poisoning



WannaCry





Lodestone

Where do we stand?

- Just started, no healthcare clients yet
- No specifically MedDev past experience on team

How to Fix This

- Read the internet
- Follow Network Best Practices
- Get hands dirty...

Building the Lab

Acquiring Devices

- Healthcare Org vendor agreements and SLA's
- Group Purchasing Organizations
- Devices are expensive
- Software under lock and key



Ebay



Thanks for your order, Roger!

Your order is confirmed and we'll let you know when it's on the way. It will ship to 263 Tresser
[REDACTED] United States

[View order details](#)

Protected by

ebay™ MONEY BACK GUARANTEE



Hospira Abbott PLUM A+ IV Infusion Pump MedNet...

Item ID: 2[REDACTED]216

Quantity: 1

Estimated delivery: Wed. Mar. 21 - Mon. Mar. 26

Paid: \$55.00 with PayPal

✓ Seller: [REDACTED]

FDA Authorized Purchaser

Under the provision of Section 520(e) of the Amendments, the FDA is authorized to restrict the sale, distribution, or use of a device if there cannot otherwise be reasonable assurance of its safety and effectiveness.

A restricted device can only be sold on oral or written authorization by a licensed practitioner or under conditions specified by regulation. Devices such as cardiac pacemakers and heart valves, for example, require a practitioner's authorization....



FDA cont...



Description

Hospira Abbott PLUM A+ IV Infusion Pump MedNet v13.41.00.002

INCLUDES:

- Hospira Abbott Plum A+ IV Pump with MedNet Power Cord.

THESE UNITS ALL HAVE MARKS OR DENTS ON THE PLASTIC SCREEN.

ALL ARE IN PERFECT WORKING CONDITION, JUST COSMETIC MARKS ON THE PLASTIC.

FULLY TESTED-IN EXCELLENT WORKING CONDITION

**THE UNIT PHOTOED IS TO SHOW AVERAGE CONDITION
SEE PHOTOS**

30 DAY WARRANTY

FDA cont...

A PROVEN PERFORMER

With more than 325,000 pumps installed worldwide, the Plum A+™ general purpose infusion system is a proven choice for caregivers and clinicians alike. The scalable platform can be initially deployed, and then upgraded to include Hospira MedNet™ safety software to meet your evolving patient care needs. The innovative PlumSet™ cassette technology and time-saving features simplify medication delivery and enhance safety for patients, clinicians and caregivers.

THE PLUM A+ SYSTEM HELPS ENSURE SAFE AND ACCURATE INFUSIONS

- Deliver infusions with confidence with the unique PlumSet™ technology
 - Automated second-line delivery — eliminates the need to raise and lower infusion containers, improving ease-of-use and efficiency
 - Concurrent delivery of 2 medications through a single patient line
 - Air-in-Line detection and elimination — air trap captures up to 2 mLs of air
 - Accumulated air can be removed by automated back-priming without disconnecting the patient, reducing the risk of contamination
 - Deliver secondary infusions via IV container or syringe
- Reliable performance, steady, consistent and proven
 - One integrated system works across the entire spectrum of clinical care
 - Single channel (2 concurrent medications) or triple channel (6 concurrent medications) mode
 - Choose from a variety of programming options:
 - Automated piggyback and concurrent delivery

FDA cont...

International Buyers – Please Note:

Import duties, taxes, and charges are not included in the item price or shipping cost. These charges are the buyer's responsibility.

Please check with your country's customs office to determine what these additional costs will be prior to bidding or buying.

Terms of Sale

Return Policy:

Most items we sell come with a 30 day money back guarantee. Please review the eBay listing to determine the guarantee that we are providing for the item. Some items have a longer guarantee, some have a shorter guarantee, and some items are sold as is. Please review the eBay listing of the item you are interested in to determine guarantee. Contact us with any questions. Thank You!

Ebay required FDA Statement:

The below statement is required by eBay when listing in medical categories. For most items we sell there are no restrictions to purchase but please contact us if you are unsure.

"The sale of this item may be subject to regulation by the U.S. Food and Drug Administration and state and local regulatory agencies. If so, do not bid on this item unless you are an authorized purchaser. If the item is subject to FDA regulation, I will verify your status as an authorized purchaser of this item before shipping of the item."

FDA... FAIL





Hospira A+ IV Pump

Hospira

- **Hospira - Now Pfizer Injectables**
- **Builds a number of IV Pumps**
- **Very popular throughout the medical industry**
 - And Ebay...
- **Security Flaws in the Pumps reported**
 - Billy Rios, Symbiq and LifeCare PCA pumps, 2015



Plum A+ IV Pump

- Older gen of hospital bed-side IV pump
- Purportedly Affected by some reported vulnerabilities
 - Static Auth Key, Improper Encryption
- Cheap, Ethernet and Wifi capable
- Manuals Available Online

6.4.2

RESETTING THE ETHERNET IP ADDRESS AND SUBNET MASK

This section applies to List Number **20791-04** and above, and List Number **20677-04** and above.

If the CE has been misconfigured and WebConfig cannot communicate with the CE, the **Reset** button can be used to reset the Ethernet IP address (**192.168.0.100**) and Subnet Mask (**255.255.0.0**) to the factory default (*see Figure 6-2*).

To reset the Ethernet IP address and Subnet Mask, proceed as follows:

1. Turn on the infuser, and connect to Ethernet.
2. Confirm the configuration is **not** the factory default.
3. Turn off the infuser, disconnect from AC power, and wait two minutes.
4. Press and hold the **Reset** button.
5. Connect the infuser to AC power and start the timer.
6. Release the **Reset** button after a measured 20 seconds.
7. Wait two minutes for the CE to completely reboot.
8. Verify that the infuser network is now set to the factory default.



Plum A+

- **Takes DHCP Address**
- **Webserver listening on 80, 443 and 8443**
 - Running thttpd version from 2012
 - Only port 80 responds
 - 401 Unauthorized, requests Basic Auth credentials
 - 3 tries, port shuts off
 - All other
- **Secret code unlock Admin mode**

According to discussions with Healthcare Professionals

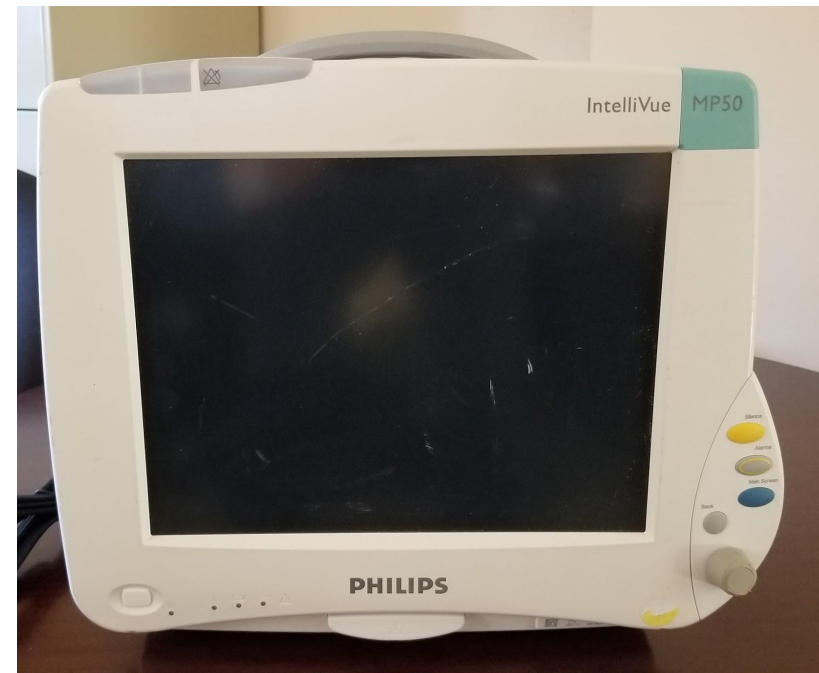
- Hospira software only updates settings and profiles
- They don't have, know, or are able to change the login key



Philips Intellivue MP50

Philips IntelliVue MP50 Patient Monitor

- Popular patient monitor, found in both hospitals and home-care
- Ethernet capability
- Philips IntelliVue Information Center
- Three CWE's reported by Philips in 2018
 - Identified by Medigate, reported through Philips "Hall of Honors"
 - ICS CERT Advisory ICSMA-18-156-01
 - Improper Authentication, Information Exposure, Buffer Overflow



Philips Hall of Honors



An error occurred while processing your request.

Reference #97.249733b8.1544739996.42a28e47

MP50

- Requires Static IP config?
- No listening ports
- UDP Broadcast on port 24005

5	65.213979	192.168.88.111	192.168.88.255	UDP	50
6	126.618233	192.168.88.111	192.168.88.255	UDP	50

> Frame 10: 500 bytes on wire (4000 bits), 500 bytes captured (4000 bits)									
> Ethernet II, Src: PhilipsP_03:49:13 (00:09:fb:03:49:13), Dst: Broadcast (f									
> Internet Protocol Version 4, Src: 192.168.88.111, Dst: 192.168.88.255									
> User Datagram Protocol, Src Port: 24005, Dst Port: 24005									

0110	37 34 35 38 00 09 00 02	00 08 00 0e 4d 38 30 30	7458....	...M800
0120	34 41 00 00 00 00 00 00	00 00 00 03 00 08 00 08	4A.....
0130	20 41 2e 30 30 2e 30 33	00 05 00 78 00 08 2d 2d	A.00.03	...x---
0140	2d 2d 2d 2d 2d 2d 00 02	00 58 00 0e 53 2d 4d 38	-----	...X...S-M8
0150	30 30 33 2d 31 35 30 31	41 20 00 04 00 58 00 08	003-1501 A	...X..
0160	47 2e 30 31 2e 37 39 20	00 07 00 86 00 01 00 08	G.01.79
0170	00 0c 44 45 33 34 37 30	37 34 35 38 00 09 00 02	..DE3470	7458....
0180	00 08 00 0e 4d 38 30 30	34 41 00 00 00 00 00 00	...M800	4A.....
0190	00 00 00 03 00 08 00 08	20 41 2e 30 30 2e 30 33	A.00.03
01a0	00 05 00 78 00 08 2d 2d	2d 2d 2d 2d 2d 2d 00 02	...x---	-----
01b0	00 58 00 0e 53 2d 4d 38	30 30 33 2d 31 35 30 31	...X...S-M8	003-1501
01c0	41 20 00 04 00 58 00 08	47 2e 30 31 2e 37 39 20	A ...X..	G.01.79
01d0	00 02 00 58 00 0e 53 2d	4d 38 30 30 09 28 00 14	...X...S-	M800.(...
01e0	00 08 50 68 69 6c 69 70	73 00 00 07 4d 38 30 30	..Philip s...	M800
01f0	34 41 00 00		4A..	

Data Export Interface Programing Guide



DATA EXPORT INTERFACE PROGRAMMING GUIDE

Data Export Guide



IntelliVue Patient Monitor & Avalon Fetal Monitor

**X2, MP Series, MX Series,
FM Series**

Patient Monitoring



many 08/15

PHILIPS

Lodestone
SECURITY

Programing Guide

- **How-To Building a Computer Client**

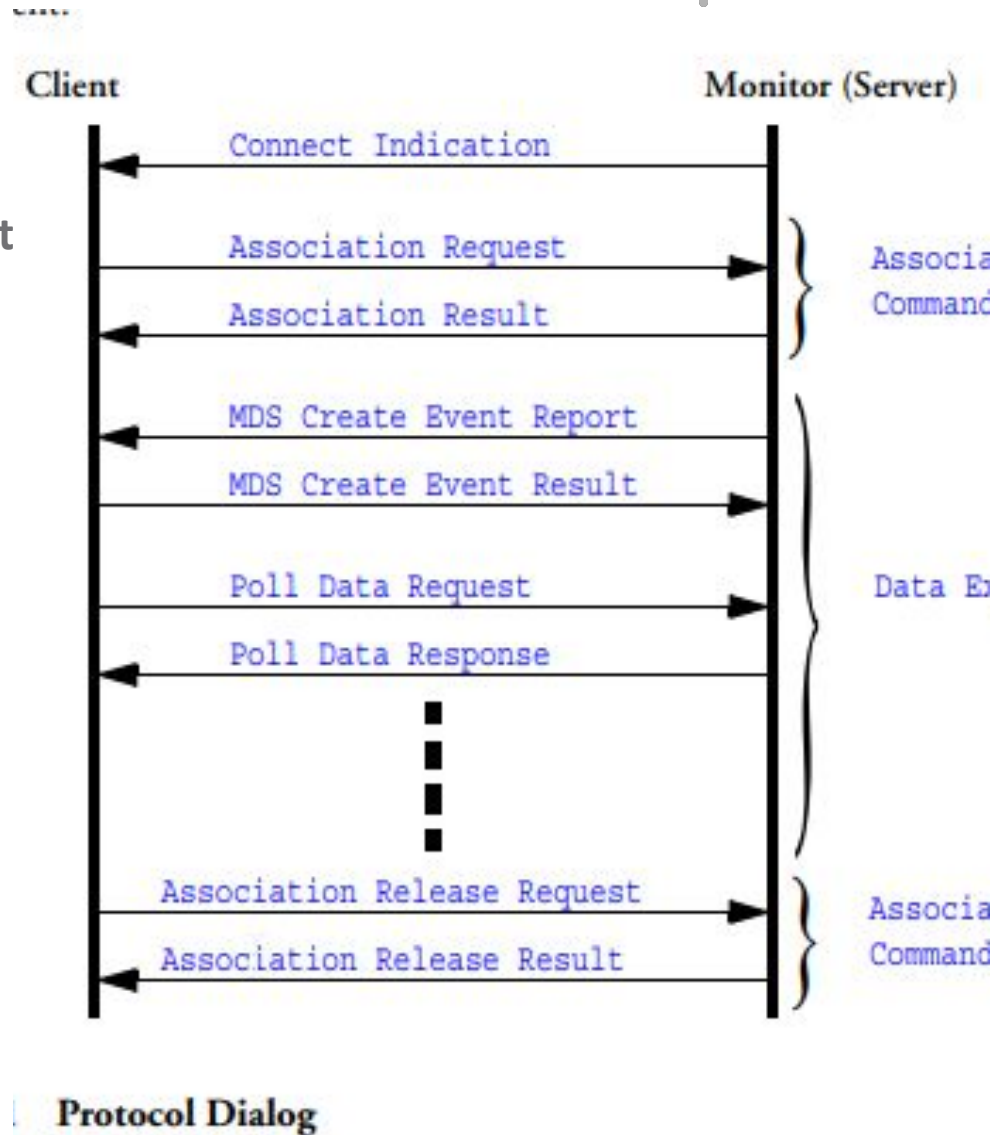
- Protocol design
- Packet order
- Byte-codes

- **No Authorization**

- Simply follow proctocol

- **Varied data types available**

- Numeric (Hear rate, etc.)
- Alerts
- Enumeration
- Medical Device System
- Waves (ECG, etc.)
- Patient Demographics
 - You mean PHI...



Hacking a Client (together)

```
if(attr_id == 'f101'):
    attribute['val'] = parse_protocol_support(val)
elif(attr_id == 'f100'):
    attribute['val'] = parse_network_address(val)
elif(attr_id == '0986'):
    attribute['system_type'] = parse_system_type(val)
elif(attr_id == '092d'):
    attribute['val'] = parse_product_specification(val)
elif(attr_id == '0928'):
    attribute['model'] = parse_model(val)
elif(attr_id == '0937'):
    attribute['locale'] = parse_localization(val, le)
elif(attr_id == '0984'):
    attribute['label'] = 'NOM_ATTR_SYS_ID'
    attribute['system_id'] = parse_sys_id(val)
elif(attr_id == '091d'):
    attribute['label'] = 'NOM_ATTR_ID_ASSOC_NO'
    attribute['association_invoke_id'] = parse_association_invoke_id(val)
elif(attr_id == '0948'):
    attribute['label'] = 'NOM_ATTR_NOM_VERS'
    attribute['nomenclature'] = parse_nomenclature(val)
elif(attr_id == '0946'):
    attribute['label'] = 'NOM_ATTR_MODE_OP'
    attribute['operating_mode'] = parse_mode_op(val)
elif(attr_id == '090d'):
    attribute['label'] = 'NOM_ATTR_AREA_APPL'
    attribute['application_area'] = parse_app_area(val)
elif(attr_id == '0935'):
    attribute['label'] = 'NOM_ATTR_LINE_FREQ'
    attribute['line_freq'] = parse_line_freq(val)
elif(attr_id == '0982'):
    attribute['label'] = 'NOM_ATTR_STD_SAFETY'
    attribute['safety_standard'] = parse_safety(val)
elif(attr_id == '090c'):
    attribute['label'] = 'NOM_ATTR_ALTITUDE'
    attribute['altitude'] = parse_altitude(val)
elif(attr_id == 'f1fa'):
    attribute['label'] = 'NOM_ATTR_MDS_GEN_INFO'
    attribute['mds_gen_info'] = parse_mds_gen_info(val)
```

- Plodding through the manual
- Enough BioMed for one lifetime
 - Anyone need their IV pump calibrated?
- Tell her what she wants to hear...
- And she'll give you her secrets
 - Can I assume gender for inanimate objects?

Oh my, P.H.I.

```

ute_id': '0ala', 'length': 2, 'val': '2000'}, {'attribute_id': 'f001', 'length': 10, 'label': 'NOM_ATTR_PT_ID_I
F', 'internal_patient_id': '0009fb034912la6403lf'}, {'attribute_id': '0962', 'length': 2, 'label': 'NOM_ATTR_PT
TYPE', 'patient_type': 'PEDIATRIC'}, {'attribute_id': '0ale', 'length': 2, 'label': 'NOM_ATTR_PT_PACED_MODE', '
paced_mode': '0001'}, {'attribute_id': '095d', 'length': 22, 'label': 'NOM_ATTR_PT_NAME_GIVEN', 'given_name': {
'length': 20, 'label': b'\x00L\x00o\x00d\x00e\x00s\x00t\x00o\x00n\x00e\x00\x00'}}, {'attribute_id': '095f', 'leng
n': 4, 'val': '00020000'}, {'attribute_id': '095c', 'length': 20, 'label': 'NOM_ATTR_PT_NAME_FAMILY', 'family_n
me': {'length': 18, 'label': b'\x00S\x00e\x00c\x00u\x00r\x00i\x00t\x00y\x00\x00'}}, {'attribute_id': '095a', 'l
ngth': 20, 'label': 'NOM_ATTR_PT_ID', 'patient_id': '0012004e00530053002d00310033003300370000'}, {'attribute_id
': 'f2e1', 'length': 24, 'val': '00160065006e0063002d00690064002d0030003000310000'}, {'attribute_id': 'fl29', 'l
ngth': 32, 'label': 'NOM_ATTR_PT_NOTES1', 'patient_notes_1': {'length': 30, 'label': b'\x00P\x00a\x00t\x00i\x00
\x00n\x00t\x00 \x00u\x00n\x00r\x00u\x00l\x00y\x00\x00'}}, {'attribute_id': 'fl2a', 'length': 44, 'label': 'NOM
ATTR_PT_NOTES2', 'patient_notes_2': {'length': 42, 'label': b'\x00S\x00e\x00d\x00a\x00t\x00i\x00o\x00n\x00 \x00R
\x00c\x00c\x00c\x00m\x00m\x00e\x00n\x00d\x00e\x00d\x00\x00'}}, {'attribute_id': '0961', 'length': 2, 'label': 'N
M_ATTR_PT_SEX', 'patient_sex': '0001'}, {'attribute_id': '0958', 'length': 8, 'label': 'NOM_ATTR_PT_DOB', 'pati
nt_dob': {'century': 32, 'year': 19, 'month': 5, 'day': 5, 'hour': 0, 'minute': 0, 'second': 0, 'sec_fractions'
: 0}}, {'attribute_id': '09d8', 'length': 6, 'label': 'NOM_ATTR_PT_AGE', 'patient_age': {'value': '00000005', 'm
unit': 2368}}, {'attribute_id': '09dc', 'length': 6, 'label': 'NOM_ATTR_PT_HEIGHT', 'patient_height': {'value':
'000000036', 'm_unit': 1376}}, {'attribute_id': '09df', 'length': 6, 'label': 'NOM_ATTR_PT_WEIGHT', 'patient_wi
ght': {'value': 'ff000834', 'm_unit': 1760}}, {'attribute_id': '0956', 'length': 6, 'label': 'NOM_ATTR_PT_BSA',
': {'value': 'fe0000bl', 'm_unit': 1472}}, {'attribute_id': 'flec', 'length': 2, 'label': 'NOM_ATTR_PT_BSA_FORM
LA', ': 'BSA_FORMULA_DUBOIS'}, {'attribute_id': 'f2e2', 'length': 4, 'val': '80752095'}, {'attribute_id': 'f2e
', 'length': 4, 'val': '808b0d98'}}]]}}]]}}]]}}}

```


Shout Down From My Mountain



I must tell the world of my discovery!

To the Google



intellivue programming guide



All

Shopping

Images

Videos

News

More

Settings

Tools

About 26,000 results (0.40 seconds)

[PDF] **IntelliVue Patient Monitor & Avalon Fetal Monitor ... - Philips InCenter**
incenter.medical.philips.com/doclib/GetDoc.aspx?func=ll&objId=11407611...

Connecting to the **Intellivue** MP5 Monitor MIB/RS232 Interface or the This **Programming Guide** is for use with the Philips **IntelliVue** X2, MP Series and MX ...

.....

GitHub - somno/einstein: Einstein provides a communication interface ...

<https://github.com/somno/einstein> ▼

Much of this work was built based on the Philips **IntelliVue** Patient Monitor DATA EXPORT INTERFACE **PROGRAMMING GUIDE** for the X2, MP Series, MX ...

Einstein... Damn You!

somno / **einstein**

<> Code

! Issues 0

🔗 Pull requests 6

📁 Projects 0

📖 Wiki

📊 Insights

Einstein provides a communication interface for Philips IntelliVue Patient Monitors.

📦 245 commits

🌿 9 branches

🏷️ 0 releases

Branch: master ▼

New pull request

Create new branch

 doismellburning Merge pull request #55 from somno/feature/no-tuple-unpacking ...

📁 **einstein** Remove tuple parameter unpacking

📄 .coveragerc Ignore NotImplementedError raises for coverage purposes

📄 api.raml Send observation state as list of enum strings

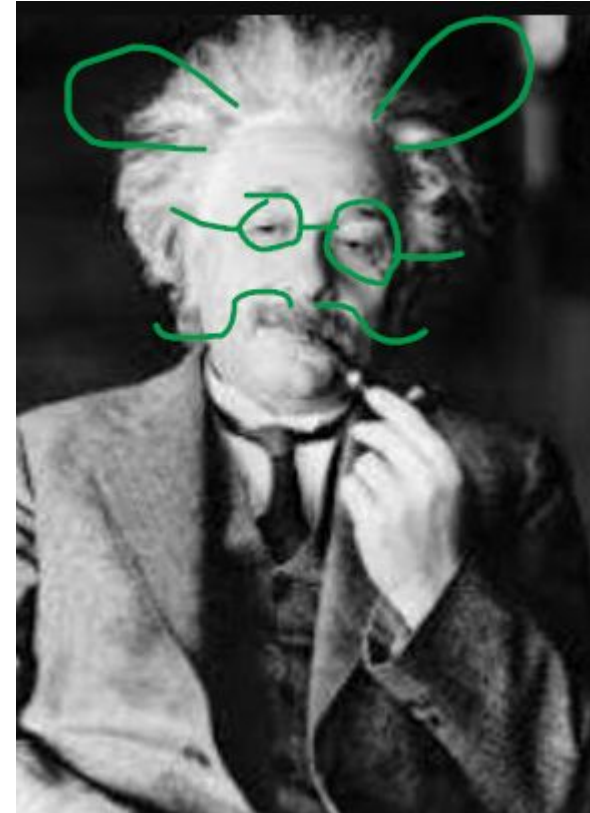
📖 README.md

einstein

Einstein provides a communication interface for Philips IntelliVue Patient Monitors.

Einstein

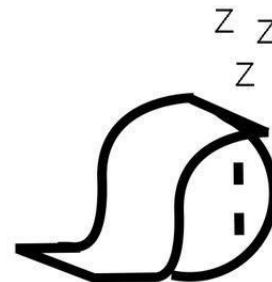
- **Intellivue Data Export client**
- **Python2.7**
 - **DEPRECATED...DEPRECATED...DEPRECATED**
 - Yeah, yeah, we get it
- **Built on Scapy library**
- **Follows Data Export Protocol**
 - Listens for Connect Indication broadcast
 - Associates, then polls
 - POST's observed data to user-specified URL
- **No Patient Demographic data though...**



Somno

An agile, 21st century, digital Anaesthetic record that's built for the people that use them.

- <https://somno.github.io/Hello-World/>
- Result of NHS Hack Day London
- Based on Opal
 - *"A web framework for building highly usable healthcare applications."*
 - Run by Open Health Care UK
 - London based group, works with the NHS
 - *"We work with clients in the NHS to help build a health system fit for the digital age."*
 - Runs the NHS Hack Day





Frankenstein

So, what do we do from here?

- **Teach it to speak patient data**
- **Stop waiting for broadcast**
- **Endpoint for adding monitor IP's**
 - From nmap, for instance...
- **Testing from different subnets, firewalls, etc.**
- **Running in a client environment?**
 - I have one in mind
- **Working with Open Health Care UK?**
 - Maybe when we break into the international market...