Gray Market Medical Lab

Internal Report

Conor Walsh

Feb 2019

Lodestone
SECURITY

Agenda

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

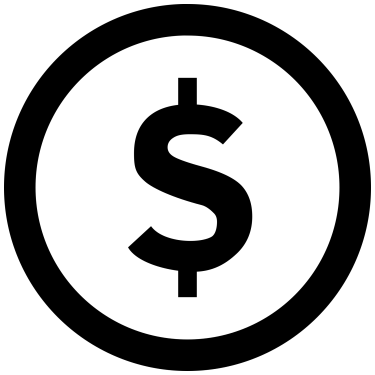
Why We're Here

Lodestone SECURITY

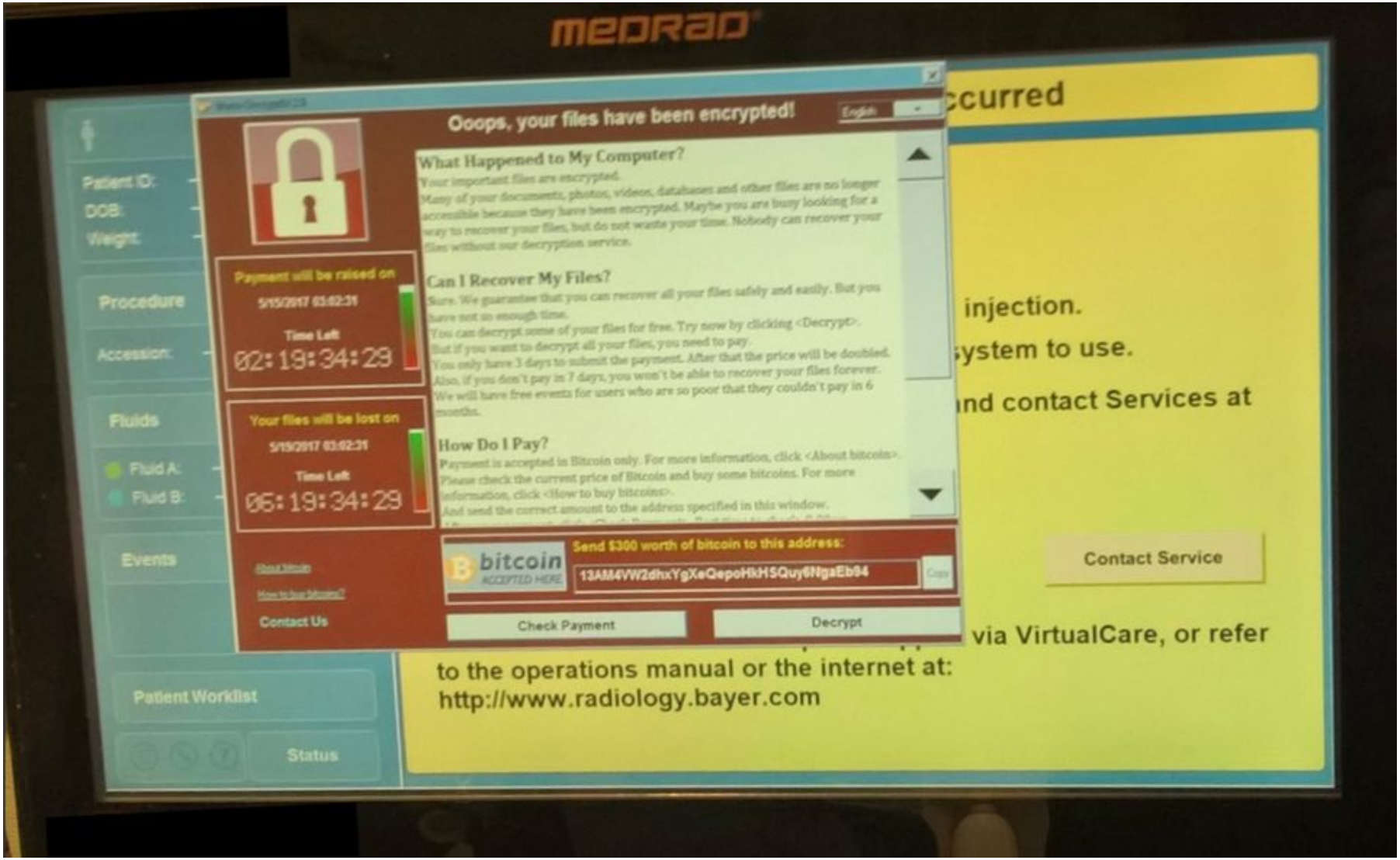
Why Medical Devices?

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


MEDRAD
Ooops, your files have been encrypted!
What Happened to My Computer?
Can I Recover My Files?
How Do I Pay?
Payment will be raised on
5/15/2017 03:02:31
Time Left
02:19:34:29
Your files will be lost on
5/19/2017 03:02:31
Time Left
06:19:34:29
Send $300 worth of bitcoin to this address:
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
bitcoin
ACCEPTED HERE
Contact Us
Check Payment
Decrypt
Patient ID:
DOB:
Weight:
Procedure
Accession:
Fluids
Fluid A:
Fluid B:
Events
Patient Worklist
Status
ccurred
injection.
ystem to use.
nd contact Services at
Contact Service
via VirtualCare, or refer
to the operations manual or the internet at:
http://www.radiology.bayer.com

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

Lodestone SECURITY

Ebay

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]

Lodestone SECURITY

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 PLASTICE 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 syste proven choice for caregivers and clinicians alike. The scalable platform can be initially deployed, a upgraded to include Hospira MedNet™ safety software to meet your evolving patient care needs. innovative PlumSet™ cassette technology and time-saving features simplify medication delivery a 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 containe 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 pati 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) moc
  - 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

Lodestone SECURITY

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.

Lodestone SECURITY

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**

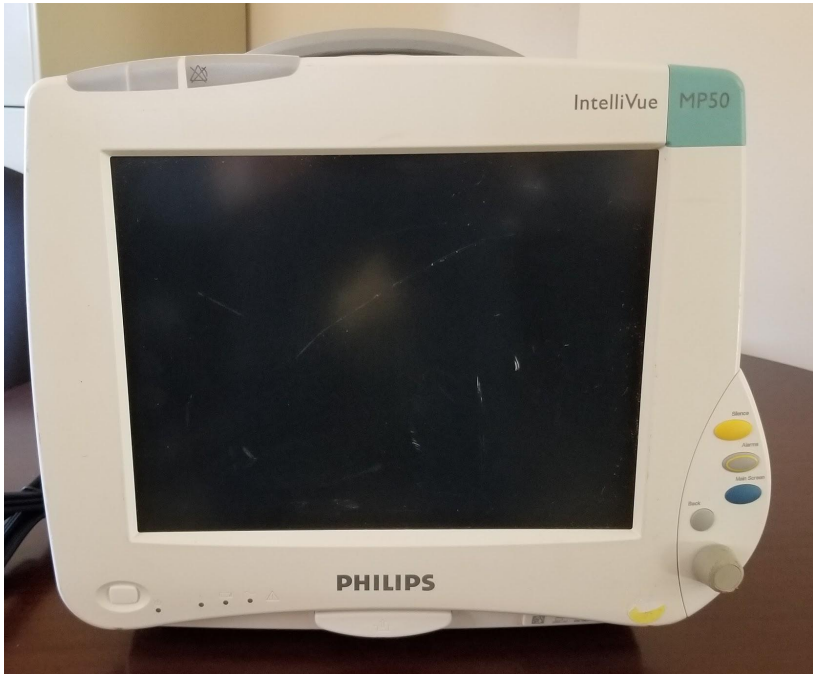
According to discussions with Healthcare Professionals

- 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



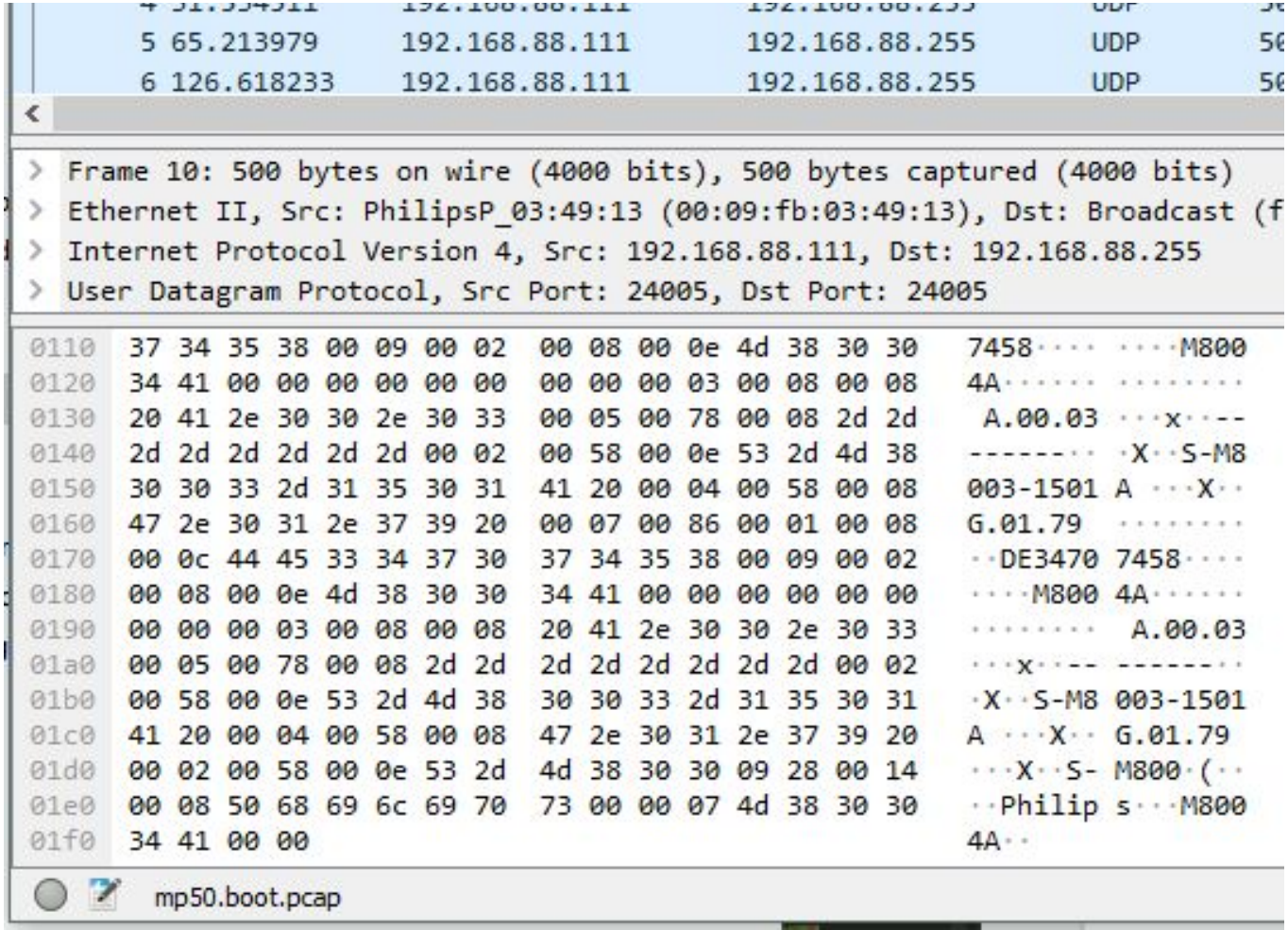
Philips Hall of Honors

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



Data Export Interface Programing Guide

Lodestone SECURITY

DATA EXPORT INTERFACE
PROGRAMMING GUIDE

IntelliVue Patient Monitor & Avalon Fetal Monitor

X2, MP Series, MX Series, FM Series

Patient Monitoring

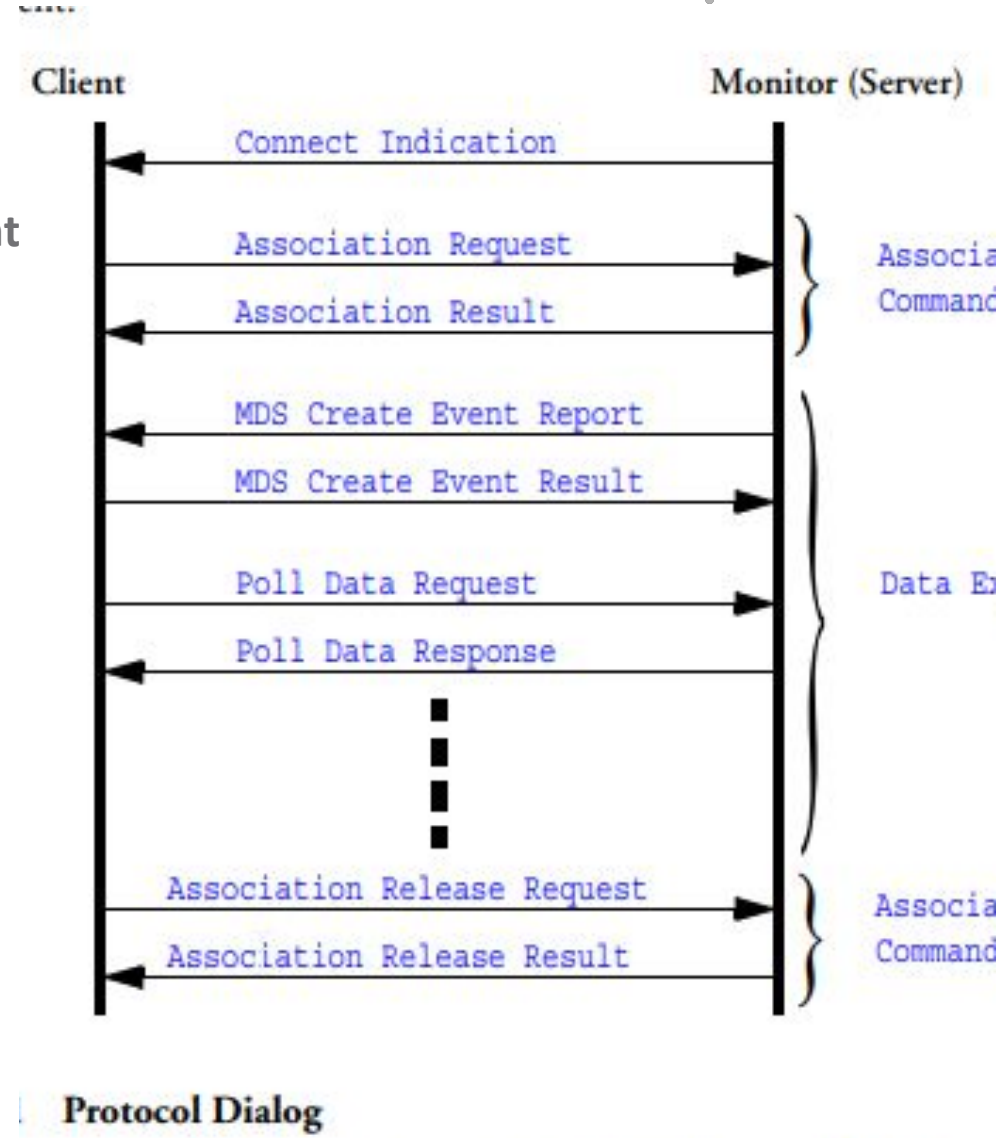
many 08/15

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...



Protocol Dialog

Hacking a Client (together)

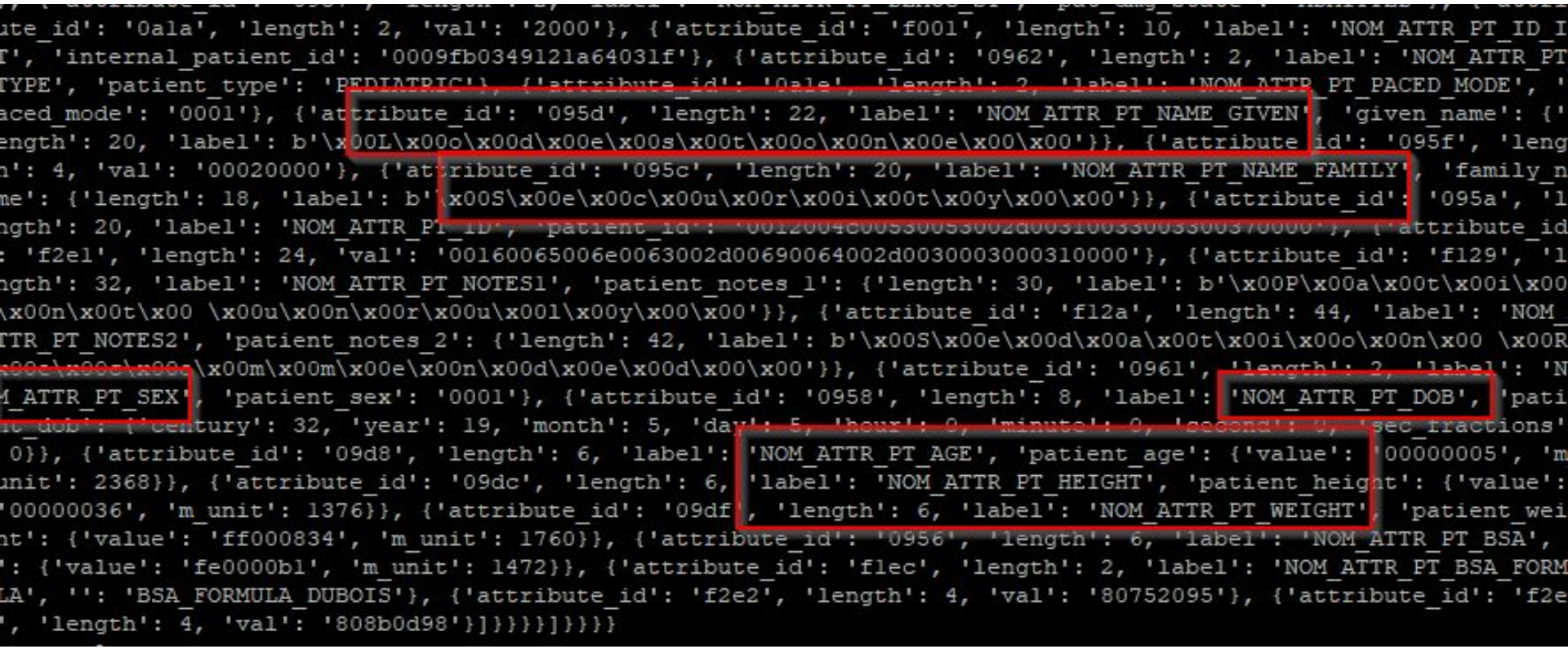
```
    attribute['val'] = parse_protocol_support(val)
elif(attr_id == 'f100'):
    attribute['val'] = parse_network_address(val)
elif(attr_id == '0986'):
    attribute['system_type'] = parse_system_type(va
elif(attr_id == '092d'):
    attribute['val'] = parse_product_specification(
elif(attr_id == '0928'):
    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_asso
elif(attr_id == '0948'):
    attribute['label'] = 'NOM_ATTR_NOM_VERS'
    attribute['nomenclature'] = parse_nomenclature(
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(
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(
```

- **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?

Lodestone SECURITY

Oh my, P.H.I.

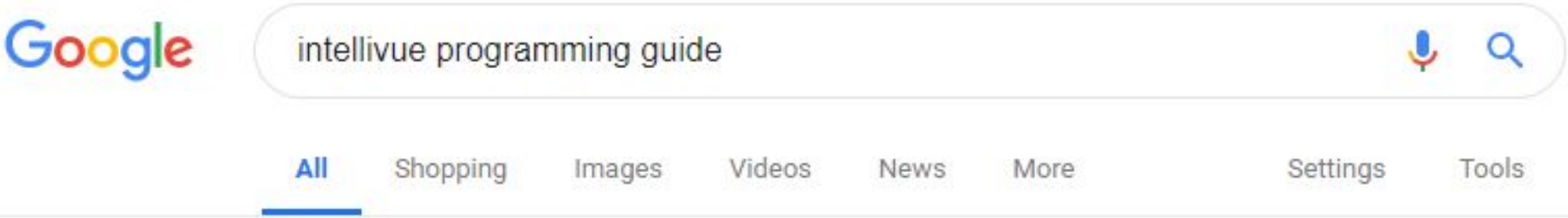


Lodestone SECURITY

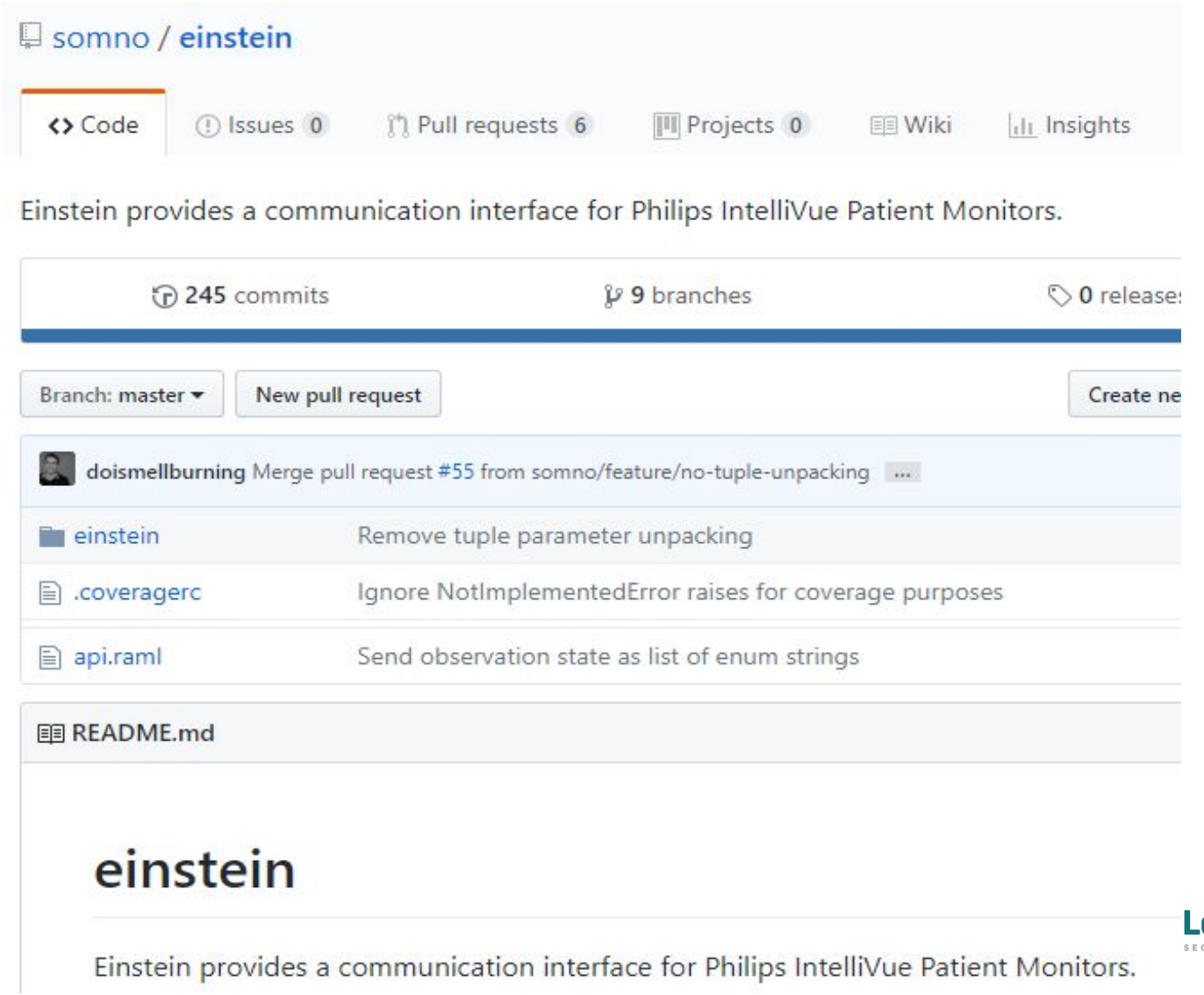
Shout Down From My Mountain

I must tell the world of my discovery!

To the Google

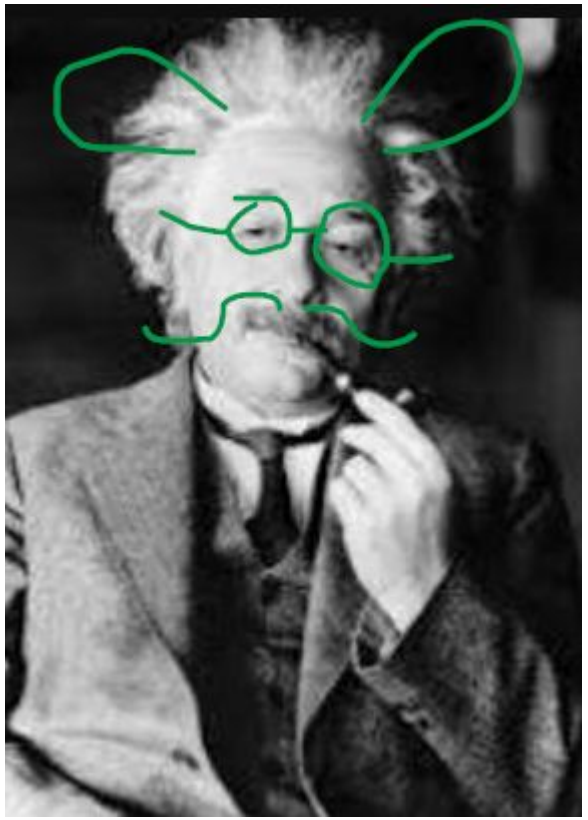


Einstein… Damn You!



Einstein

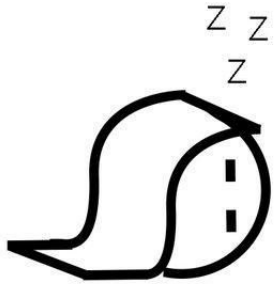
- **Intellivue Data Export client**
- **Python2.7**
  - DEPRECATED...DEPRECATED...DEPRECATED
    - Yeah, yeah, we get it
- **Built on Scapy library**
- **Follows Data Export Protocol**
  - Listens for Connect Indication broadcast
  - Associates, then polls
  - POST's observed data to user-specified URL
- **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



Frankeinstein

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...