SOMEBODY CALL A DOCTOR

Asaf Cohen & Ofir Kamil

/home/asaf.cohen/

@_asaf_cohen

- Red Team Lead
- Ex8200
- 14 years of experience
- B.Sc. CS @BGU

Accenture Security

MAGLAN
Cyber Defense & Intelligence

/home/ofir.kamil/

@ofir_kamil

- Security Researcher
- IoT enthusiast
- 10 years of experience

WHY, OH WHY?

Secure | https://conference.hitb.org/hitbsecconf2018ams/speakers/your/

Final Submission Deadline: 31st December 2017

Each accepted submission will entitle the speaker(s) to **accommodation for 3 nights / 4 days** and **travel reimbursement up to EUR1200.00 per speaking slot**.

Topics of interest include, but are not limited to the following:

- Cloud Security
- File System Security
- 3G/4G/WIMAX Security
- SS7/GSM/VoIP Security
- Security of Medical Devices

WHY, OH WHY?

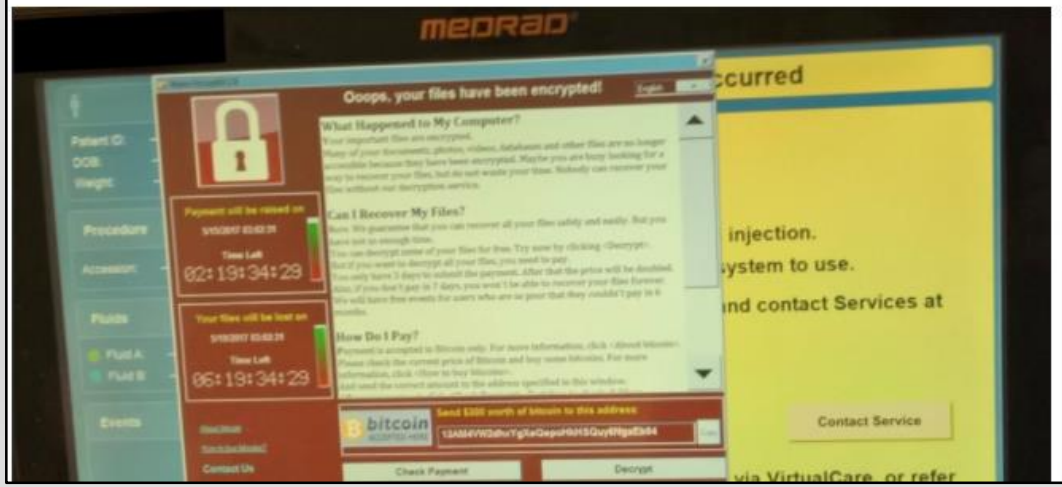
Medical Devices Hit By Ransomware For The First Time In US Hospitals

Thomas Fox-Brewster, FORBES STAFF
I cover crime, privacy and security in digital and physical forms. FULL BIO

Is it possible that North Korea used a stolen National Security Agency hacking tool to infect medical devices at U.S. hospitals? Turns out, in today's topsy-turvy world, it is.

When the NSA cyber weapon-powered WannaCry ransomware spread across the world this past weekend, it infected as many as 200,000 Windows systems, including those at 48 hospital trusts in the U.K. and so-far unnamed medical facilities in the U.S. too. It wasn't just administrative PCs that were hacked, though. Medical devices themselves were affected too, *Forbes* has learned.

A source in the healthcare industry passed *Forbes* an image of an infected Bayer Medrad device in a U.S. hospital. The source did not say which specific hospital was affected, nor could they confirm what Bayer model was hacked. But it appears to be radiology equipment designed to help improve imaging. More specifically, it's a device used for monitoring what's known in the industry as a "power injector," which helps deliver a "contrast agent" to a patient. Such agents consist of chemicals that improve the quality of magnetic resonance imaging (MRI) scans.



https://www.forbes.com

Security

UK hospital meltdown after ransomware worm uses NSA vuln to raid IT

Docs use pen and paper after computers scrambled amid global outbreak

By Kat Hall 12 May 2017 at 14:22 339 SHARE ▼

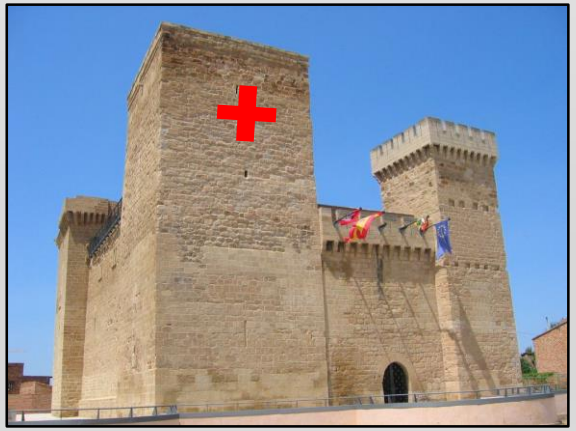
Final update UK hospitals have effectively shut down and are turning away non-emergency patients after ransomware ransacked its networks.

https://www.theregister.co.uk

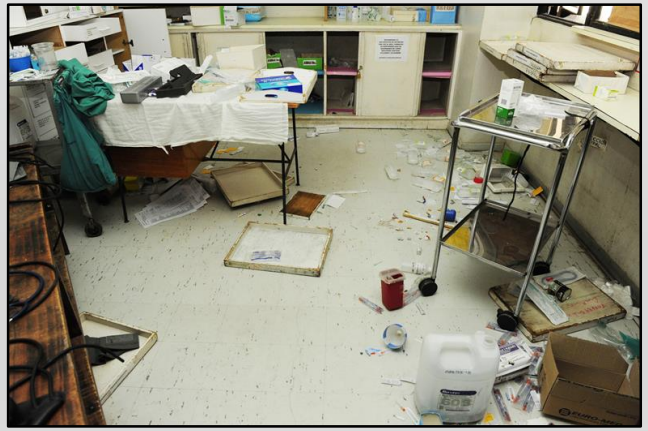
MY HOSPITAL

How management see hospital network

How IT sees hospital network



How patients see hospital network



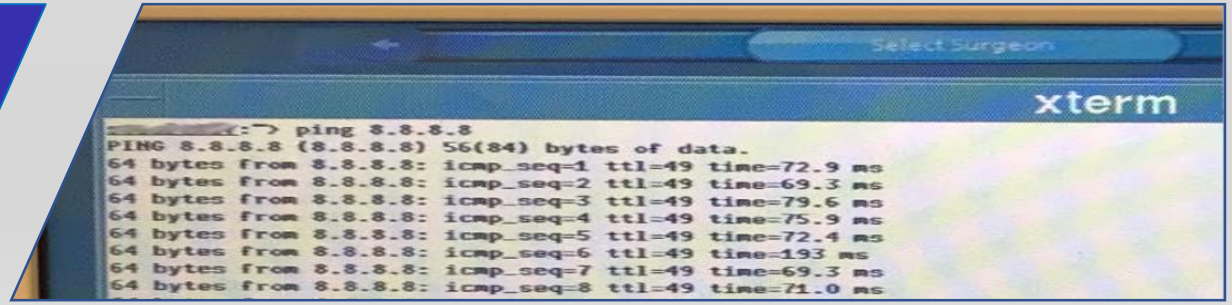
How we NOW see hospital network

Agenda

1. Potential attack surface

2. Security mechanisms

3. Medical devices & PLC's



How to get in?

IOT

Partners

Physical Presence

Target Network

Internet Infrastructure

Radio networks

Employees

Potential attack surface – Open AP bridged to LAN

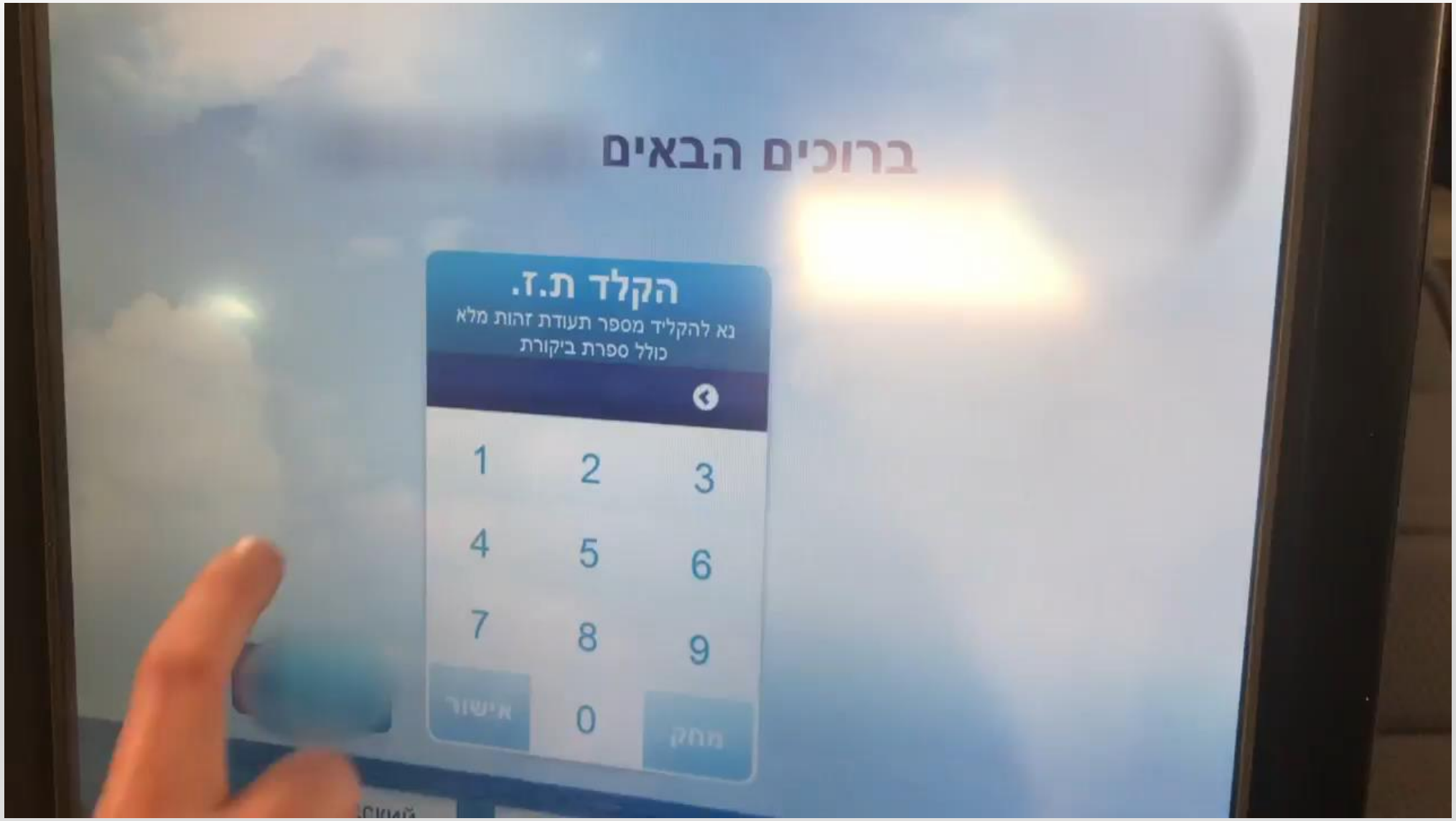
+

=

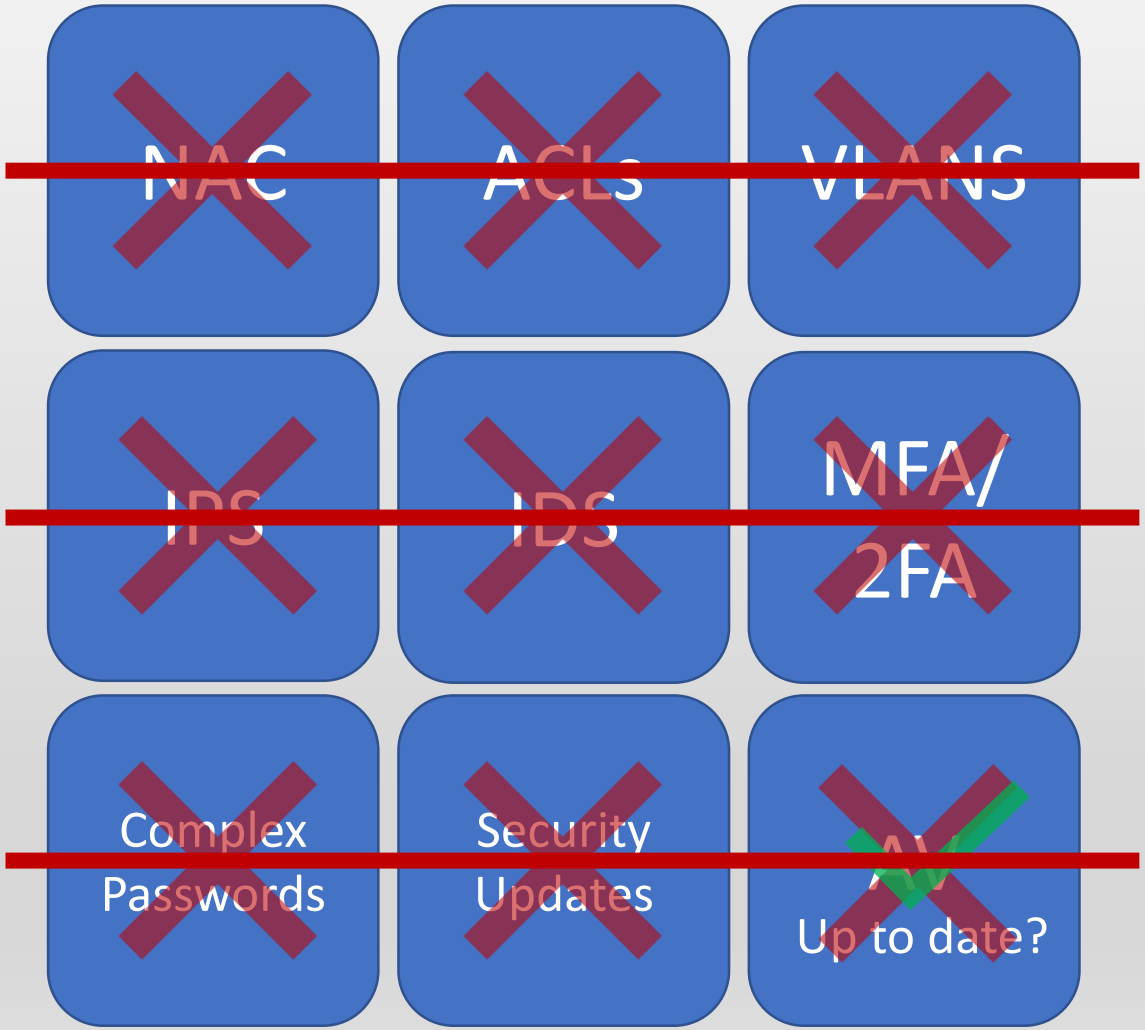
Photo by Dan Cook on Unsplash

Potential attack surface – “Hot” network jacks bridged to LAN

Potential attack surface – unhardened kiosk connected to LAN



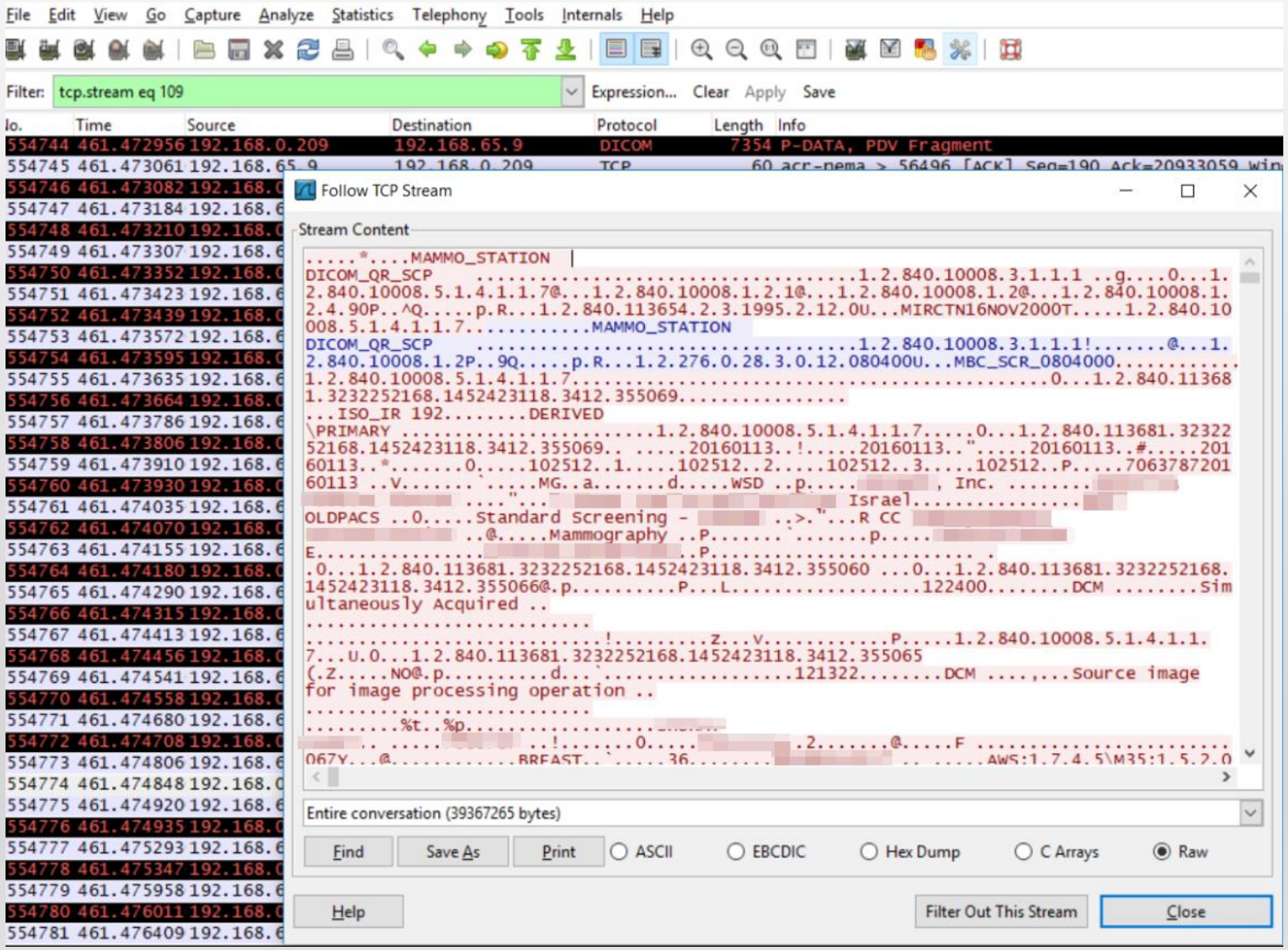
Security Mechanisms



We are in… What’s next?

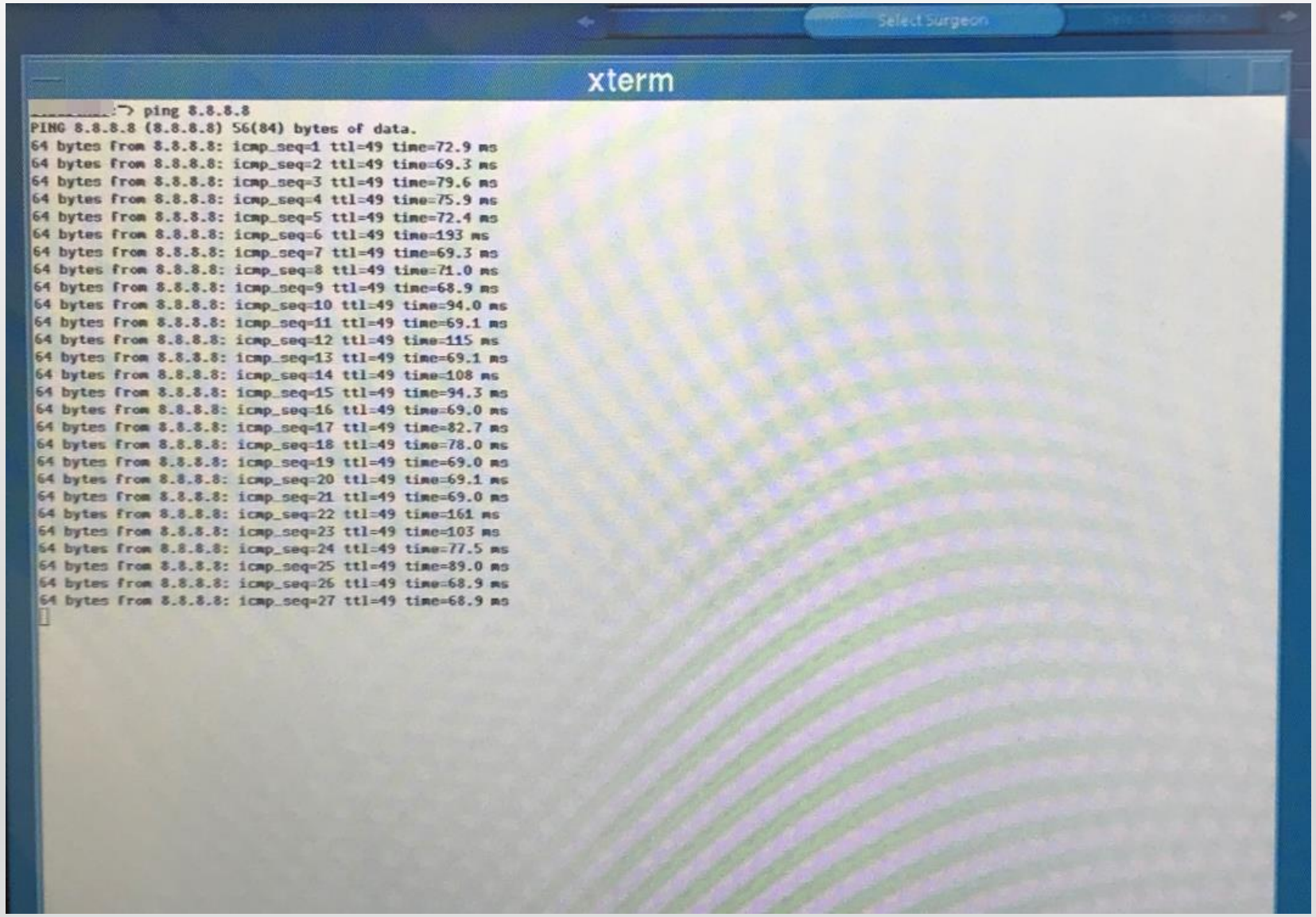

Photo by beasty on Unsplash

Digital Imaging and Communications (DICOM)

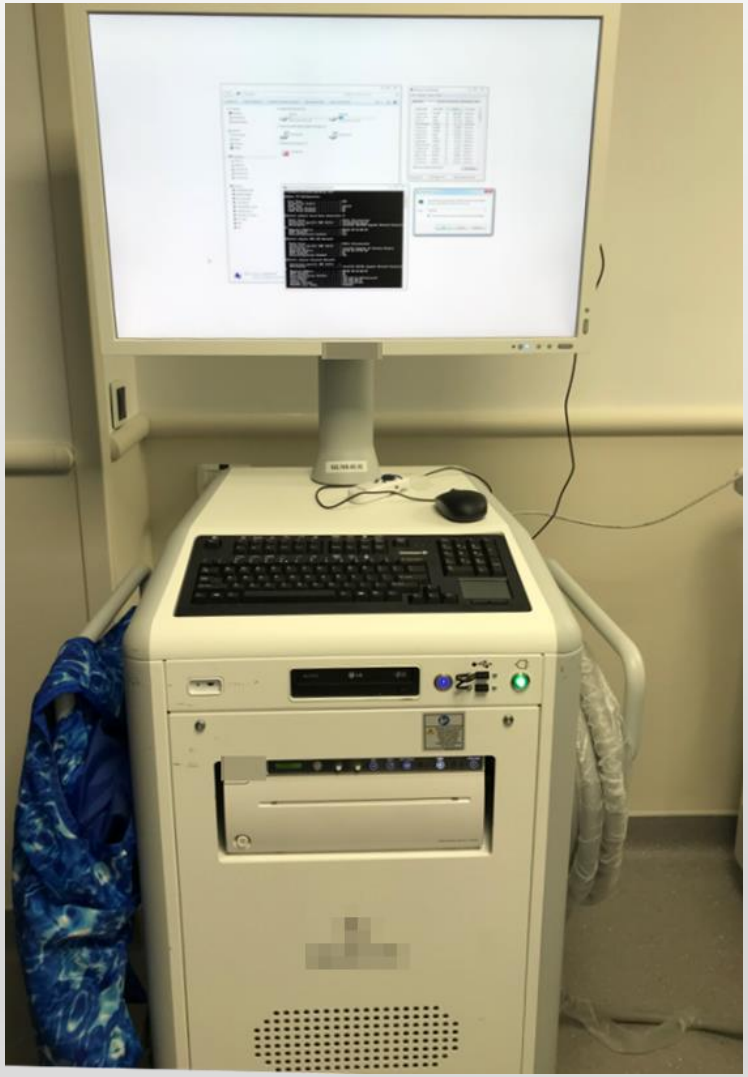


Brain surgical navigation system

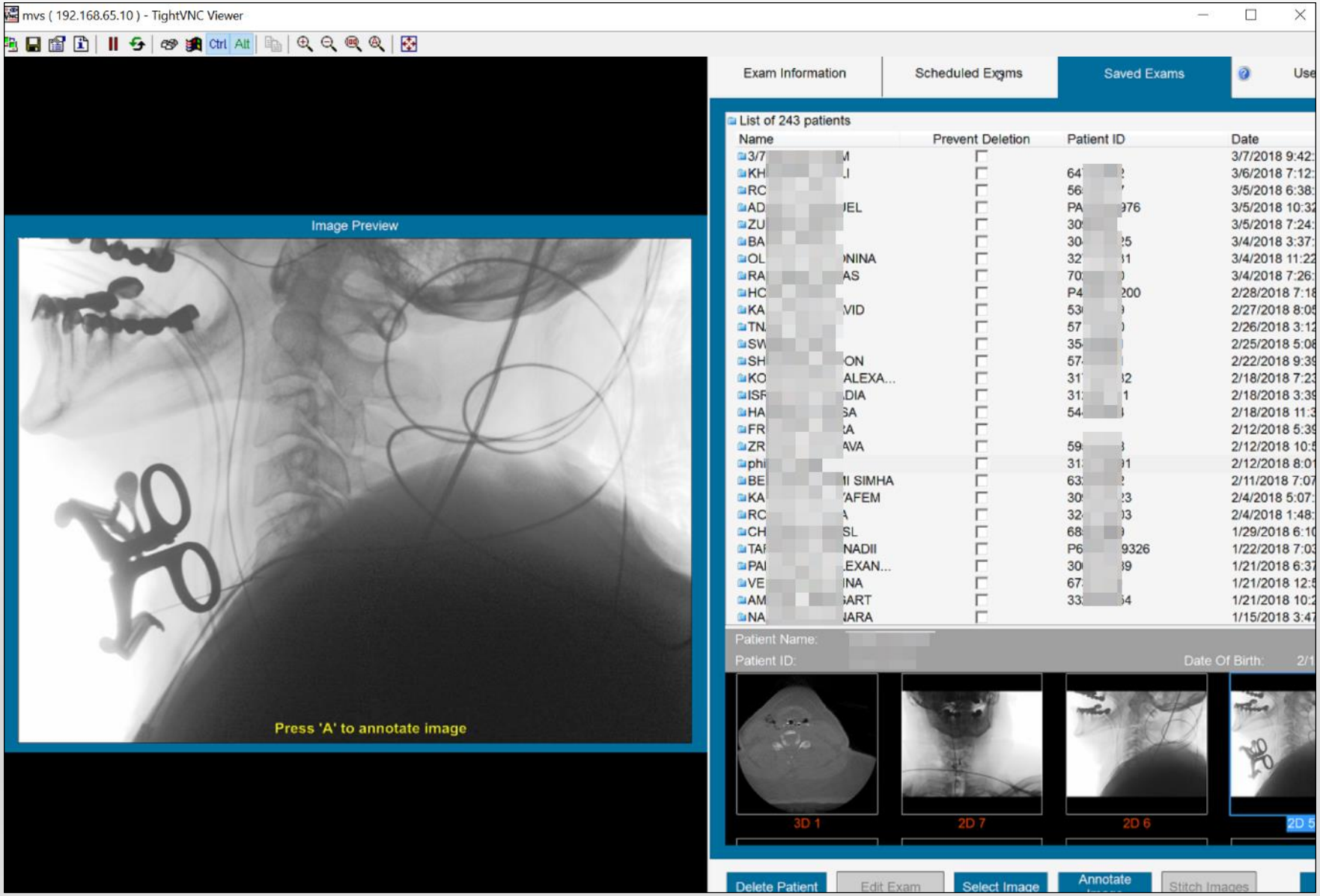
Navigation system – Hello Google ;-)



Portable computed tomography (CT)

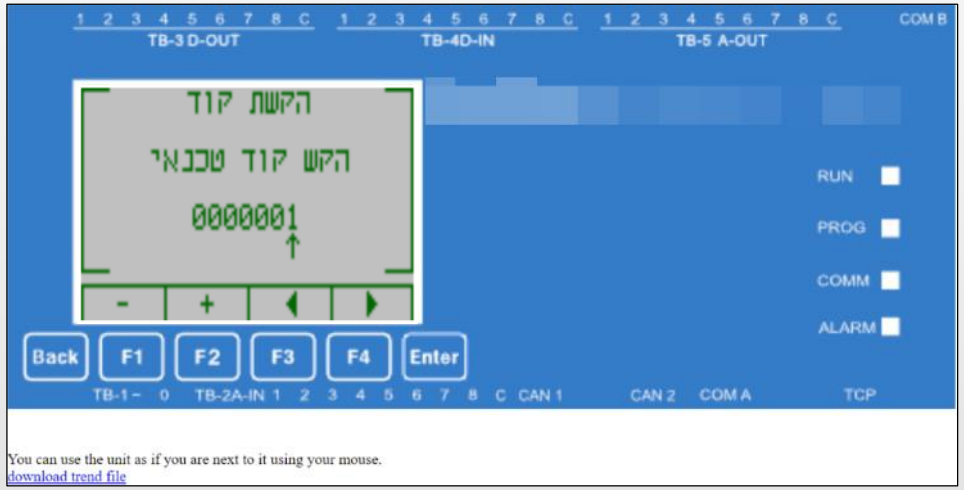


Portable CT – Hello VNC ;-)

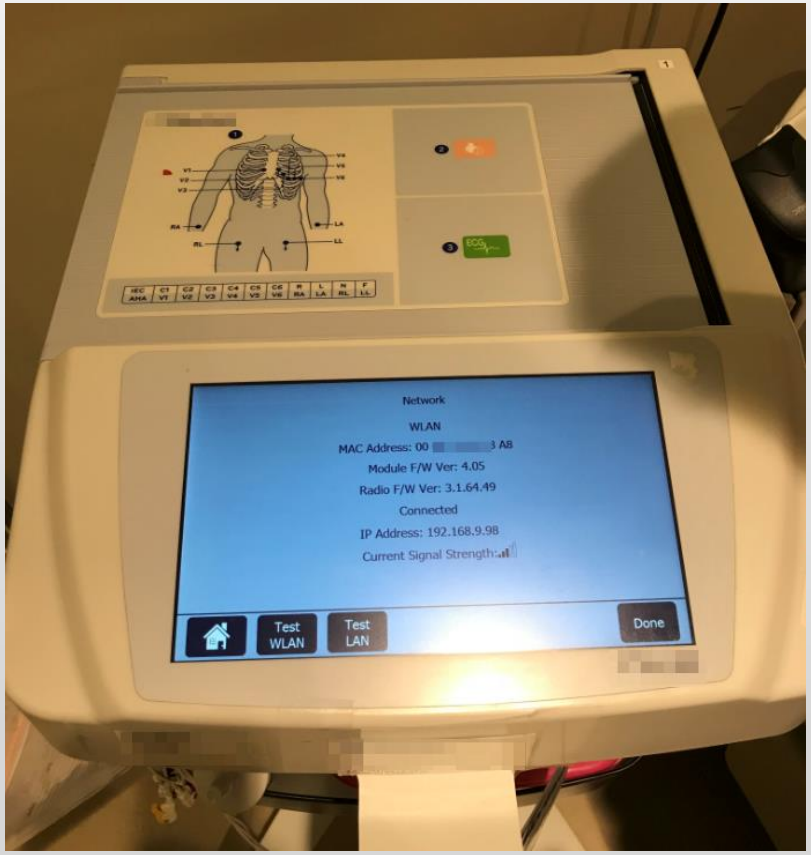


Programmable logic controllers (PLC’s)

Programmable logic controllers (PLC’s)



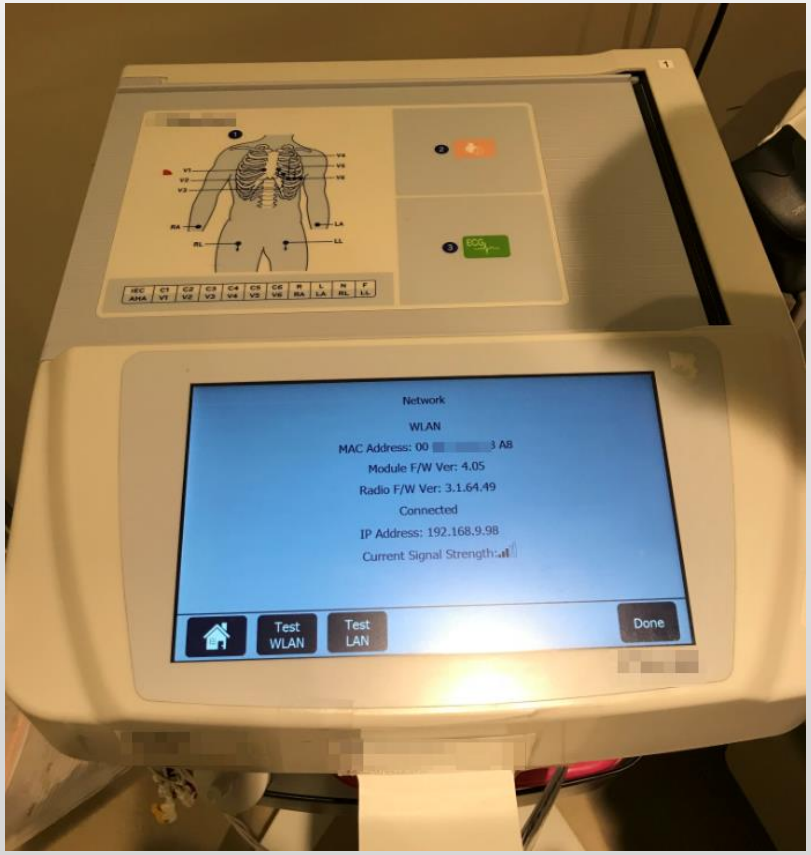
Electrocardiography (ECG/EKG) – default passwords

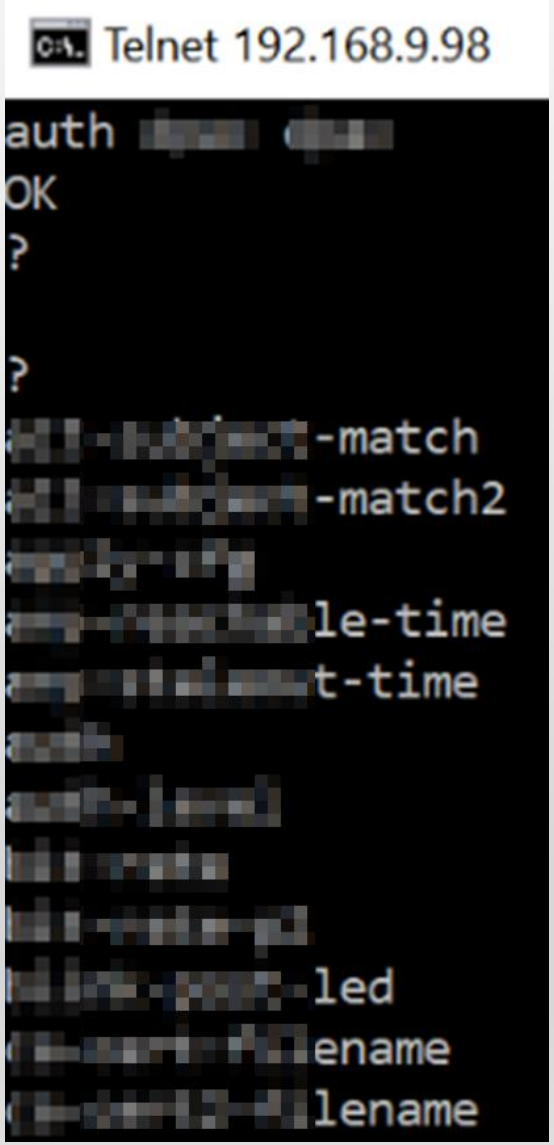


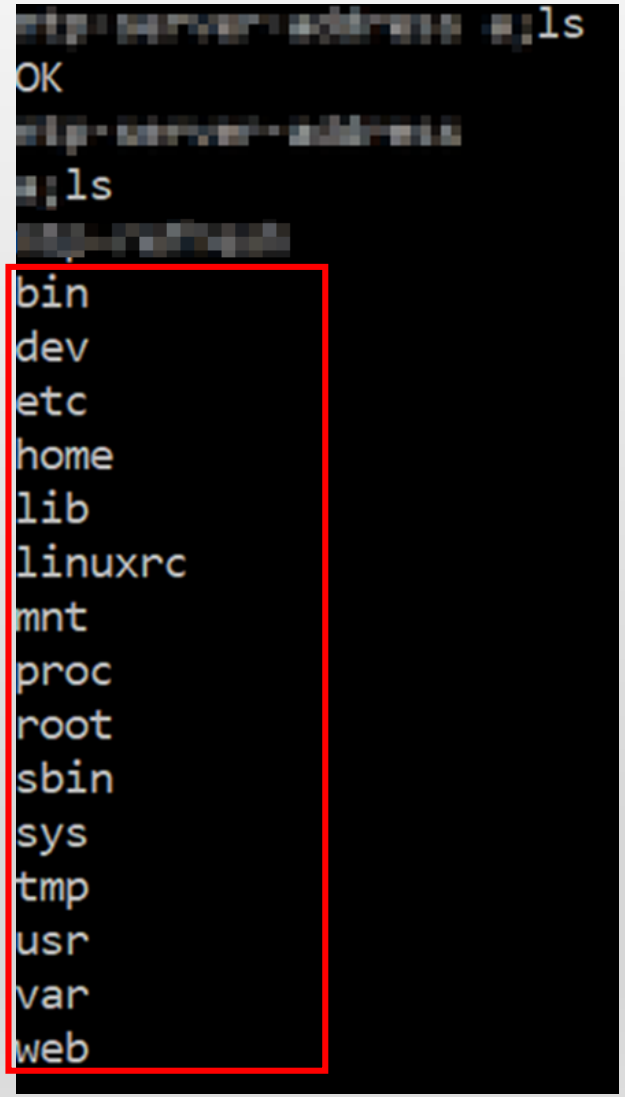
Command Prompt - ftp 192.168.9.98

```
C:\>ftp 192.168.9.98
Connected to 192.168.9.98.
220 [redacted] FTP server (GNU inetutils 1.4.1) ready.
500 'OPTS UTF8 ON': command not understood.
User (192.168.9.98:(none)): [redacted]
331 Password required for [redacted].
Password:
230 User [redacted] logged in.
```

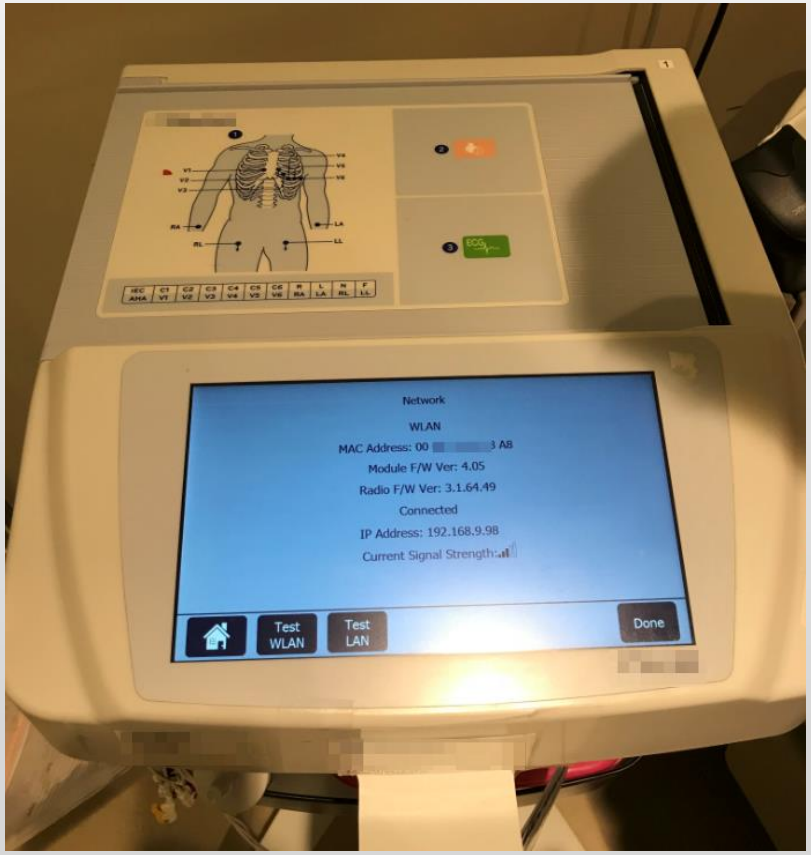
Electrocardiography (ECG/EKG)







Electrocardiography (ECG/EKG)



Full control on device

```
cat /proc/cpuinfo
OK

Processor       : ARM926EJ-S rev 5 (v5l)
BogoMIPS        : 197.83
Features        : swp half thumb fastmult edsp java
CPU implementer : 0x41
CPU architecture: 5TEJ
CPU variant     : 0x0
CPU part        : 0x926
CPU revision    : 5

Hardware        :  Processor
Revision        : 0000
Serial          : 0000000000000000
```

One month checkpoint, but what have we learn so far?