

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



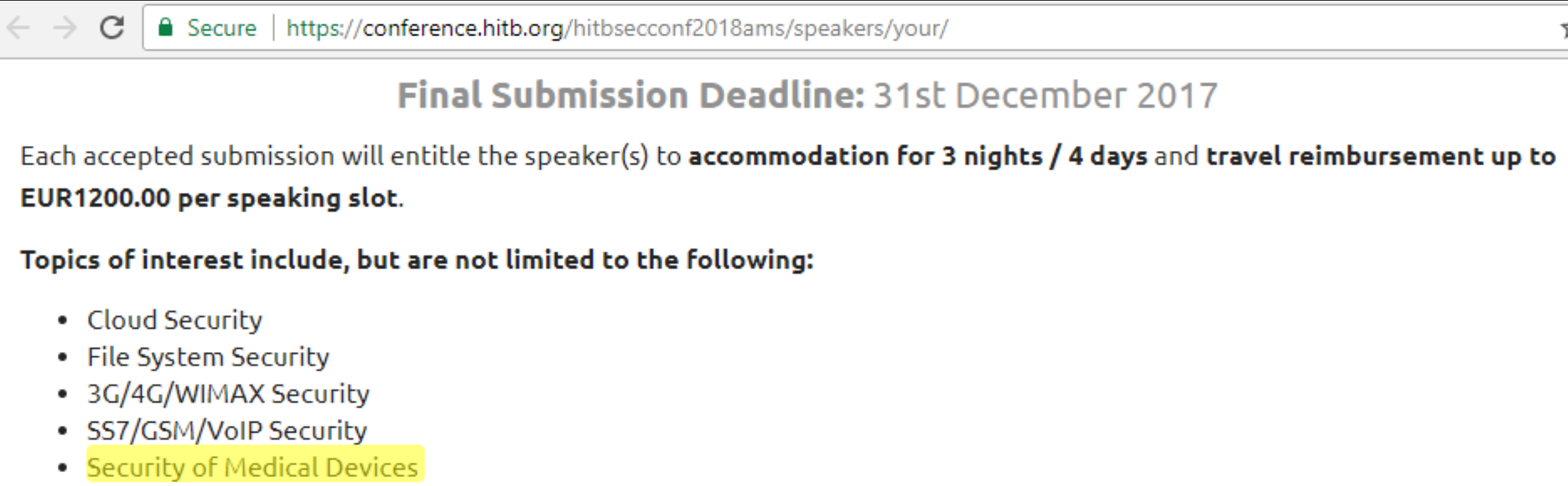
/home/ofir.kamil/



@ofir_kamil

- Security Researcher
- IoT enthusiast
- 10 years of experience

WHY, OH WHY?



The screenshot shows a web browser window with the address bar containing the URL <https://conference.hitb.org/hitbsecconf2018ams/speakers/your/>. The page content includes a bold heading for the final submission deadline, a paragraph detailing the benefits for accepted speakers, and a list of topics of interest. The item 'Security of Medical Devices' is highlighted in yellow.

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

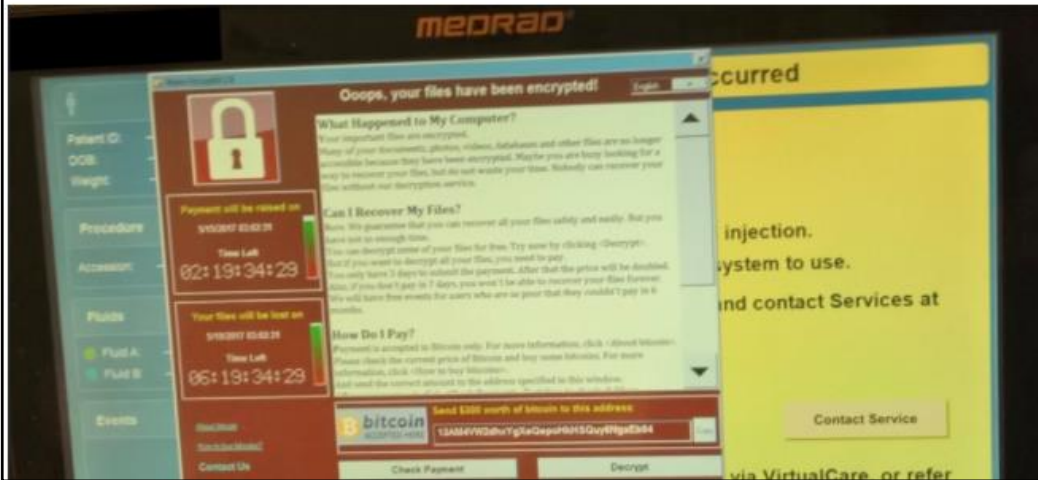


Thomas Fox-Brewster, FORBES STAFF
I cover crime, privacy and security in digital and physical forms. FULL BIO

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>

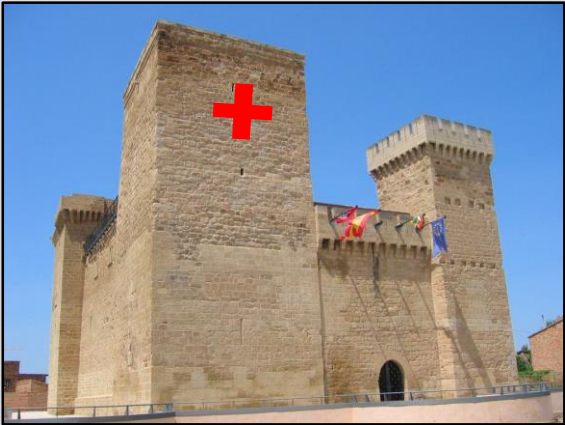
MY HOSPITAL



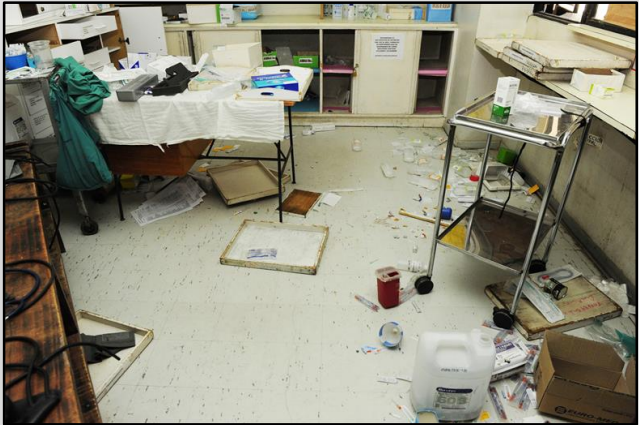
**How management see
hospital network**



**How IT sees
hospital network**



**How patients see
hospital network**



**How we NOW see
hospital network**

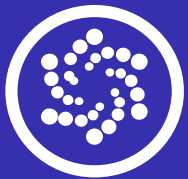
Agenda



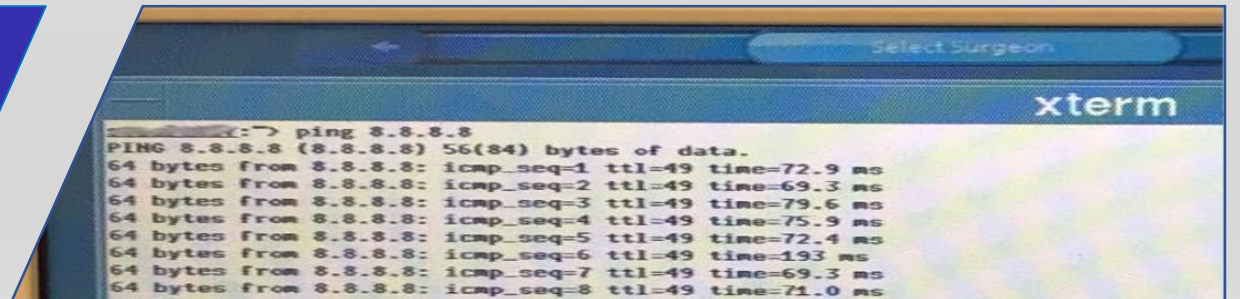
1. Potential attack surface



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



+



=

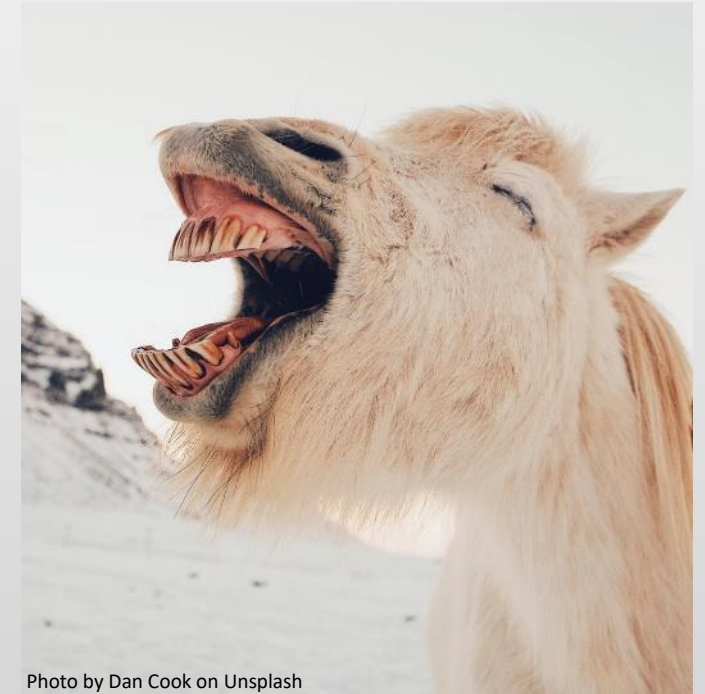
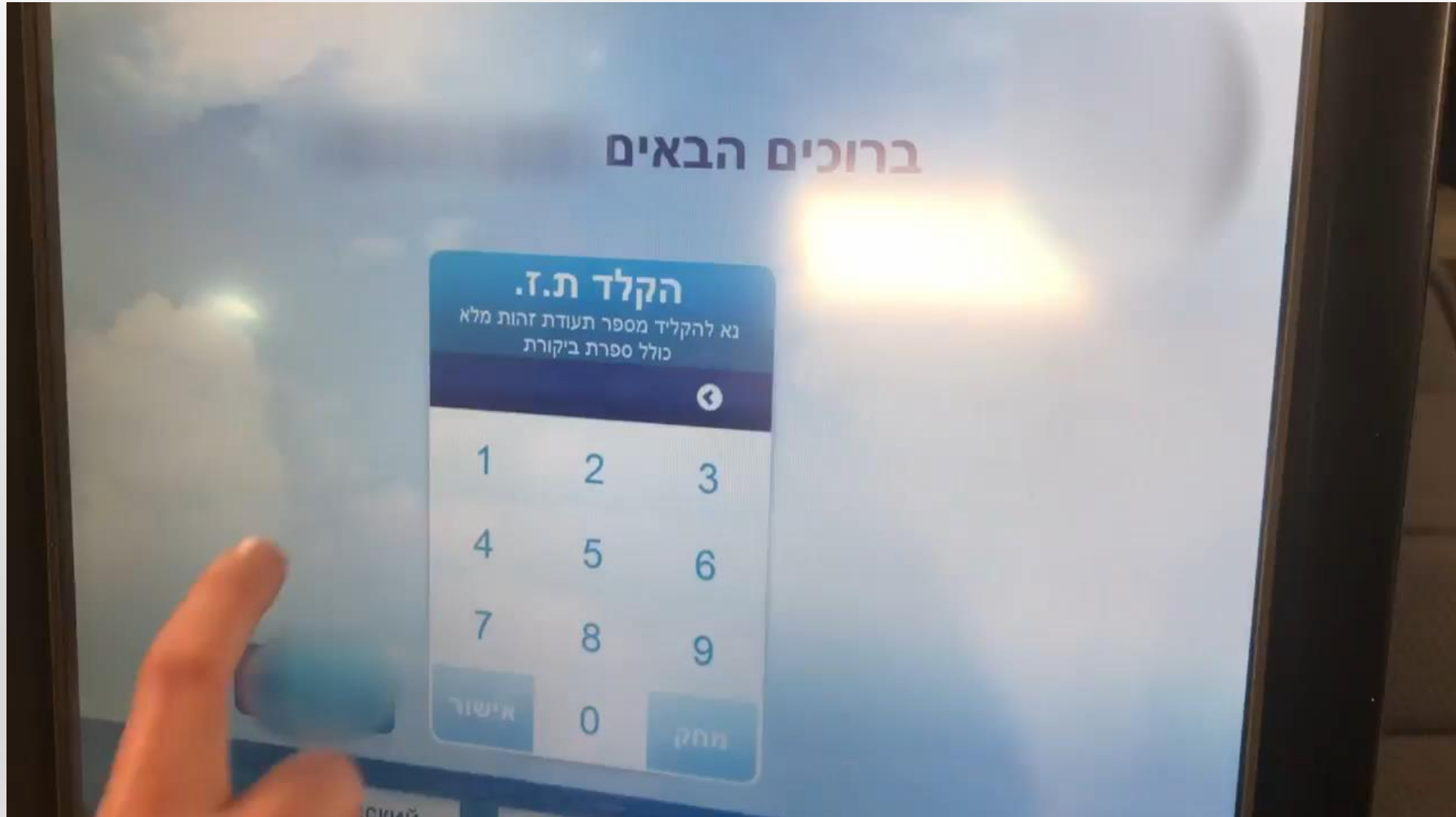


Photo by Dan Cook on Unsplash

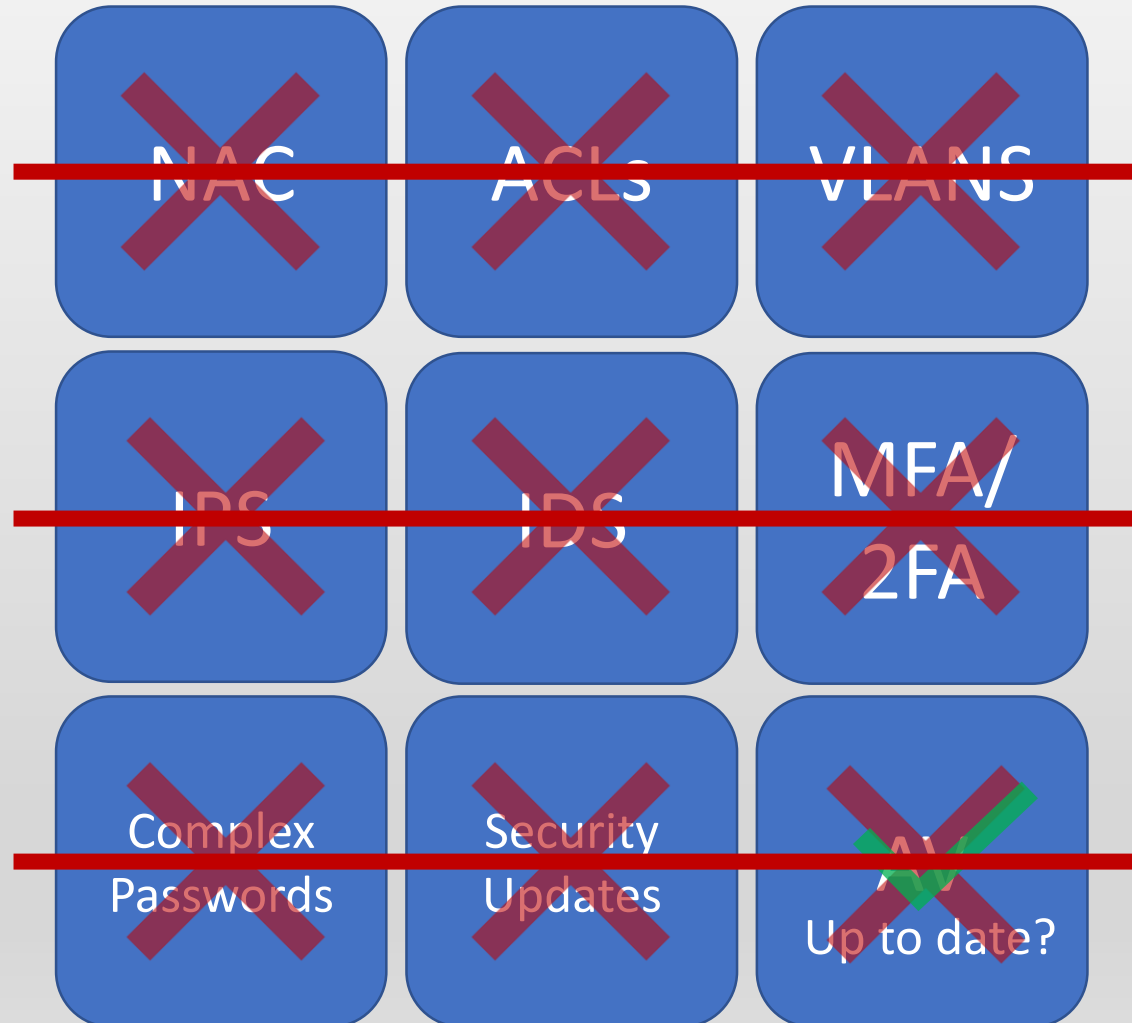
Potential attack surface – “Hot” network jacks bridged to LAN



Potential attack surface – unhardened kiosk connected to LAN



Security Mechanisms



We are in... What's next?



Photo by beastly on Unsplash

Digital Imaging and Communications (DICOM)

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp.stream eq 109 Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
554744	461.472956	192.168.0.209	192.168.65.9	DICOM	7354	P-DATA, PDV Fragment
554745	461.473061	192.168.65.9	192.168.0.209	TCP	60	acc-nema > 56496 [ACK] Seq=190 Ack=20933059 win=...
554746	461.473082	192.168.0.209	192.168.65.9	TCP	60	56496 > acc-nema [ACK] Seq=190 Ack=20933059 win=...
554747	461.473184	192.168.65.9	192.168.0.209	TCP	60	acc-nema > 56496 [ACK] Seq=190 Ack=20933059 win=...
554748	461.473210	192.168.0.209	192.168.65.9	TCP	60	56496 > acc-nema [ACK] Seq=190 Ack=20933059 win=...
554749	461.473307	192.168.65.9	192.168.0.209	TCP	60	acc-nema > 56496 [ACK] Seq=190 Ack=20933059 win=...
554750	461.473352	192.168.0.209	192.168.65.9	TCP	60	56496 > acc-nema [ACK] Seq=190 Ack=20933059 win=...
554751	461.473423	192.168.65.9	192.168.0.209	TCP	60	acc-nema > 56496 [ACK] Seq=190 Ack=20933059 win=...
554752	461.473439	192.168.0.209	192.168.65.9	TCP	60	56496 > acc-nema [ACK] Seq=190 Ack=20933059 win=...
554753	461.473572	192.168.65.9	192.168.0.209	TCP	60	acc-nema > 56496 [ACK] Seq=190 Ack=20933059 win=...
554754	461.473595	192.168.0.209	192.168.65.9	TCP	60	56496 > acc-nema [ACK] Seq=190 Ack=20933059 win=...
554755	461.473635	192.168.65.9	192.168.0.209	TCP	60	acc-nema > 56496 [ACK] Seq=190 Ack=20933059 win=...
554756	461.473664	192.168.0.209	192.168.65.9	TCP	60	56496 > acc-nema [ACK] Seq=190 Ack=20933059 win=...
554757	461.473786	192.168.65.9	192.168.0.209	TCP	60	acc-nema > 56496 [ACK] Seq=190 Ack=20933059 win=...
554758	461.473806	192.168.0.209	192.168.65.9	TCP	60	56496 > acc-nema [ACK] Seq=190 Ack=20933059 win=...
554759	461.473910	192.168.65.9	192.168.0.209	TCP	60	acc-nema > 56496 [ACK] Seq=190 Ack=20933059 win=...
554760	461.473930	192.168.0.209	192.168.65.9	TCP	60	56496 > acc-nema [ACK] Seq=190 Ack=20933059 win=...
554761	461.474035	192.168.65.9	192.168.0.209	TCP	60	acc-nema > 56496 [ACK] Seq=190 Ack=20933059 win=...
554762	461.474070	192.168.0.209	192.168.65.9	TCP	60	56496 > acc-nema [ACK] Seq=190 Ack=20933059 win=...
554763	461.474155	192.168.65.9	192.168.0.209	TCP	60	acc-nema > 56496 [ACK] Seq=190 Ack=20933059 win=...
554764	461.474180	192.168.0.209	192.168.65.9	TCP	60	56496 > acc-nema [ACK] Seq=190 Ack=20933059 win=...
554765	461.474290	192.168.65.9	192.168.0.209	TCP	60	acc-nema > 56496 [ACK] Seq=190 Ack=20933059 win=...
554766	461.474315	192.168.0.209	192.168.65.9	TCP	60	56496 > acc-nema [ACK] Seq=190 Ack=20933059 win=...
554767	461.474413	192.168.65.9	192.168.0.209	TCP	60	acc-nema > 56496 [ACK] Seq=190 Ack=20933059 win=...
554768	461.474456	192.168.0.209	192.168.65.9	TCP	60	56496 > acc-nema [ACK] Seq=190 Ack=20933059 win=...
554769	461.474541	192.168.65.9	192.168.0.209	TCP	60	acc-nema > 56496 [ACK] Seq=190 Ack=20933059 win=...
554770	461.474558	192.168.0.209	192.168.65.9	TCP	60	56496 > acc-nema [ACK] Seq=190 Ack=20933059 win=...
554771	461.474680	192.168.65.9	192.168.0.209	TCP	60	acc-nema > 56496 [ACK] Seq=190 Ack=20933059 win=...
554772	461.474708	192.168.0.209	192.168.65.9	TCP	60	56496 > acc-nema [ACK] Seq=190 Ack=20933059 win=...
554773	461.474806	192.168.65.9	192.168.0.209	TCP	60	acc-nema > 56496 [ACK] Seq=190 Ack=20933059 win=...
554774	461.474848	192.168.0.209	192.168.65.9	TCP	60	56496 > acc-nema [ACK] Seq=190 Ack=20933059 win=...
554775	461.474920	192.168.65.9	192.168.0.209	TCP	60	acc-nema > 56496 [ACK] Seq=190 Ack=20933059 win=...
554776	461.474935	192.168.0.209	192.168.65.9	TCP	60	56496 > acc-nema [ACK] Seq=190 Ack=20933059 win=...
554777	461.475293	192.168.65.9	192.168.0.209	TCP	60	acc-nema > 56496 [ACK] Seq=190 Ack=20933059 win=...
554778	461.475347	192.168.0.209	192.168.65.9	TCP	60	56496 > acc-nema [ACK] Seq=190 Ack=20933059 win=...
554779	461.475958	192.168.65.9	192.168.0.209	TCP	60	acc-nema > 56496 [ACK] Seq=190 Ack=20933059 win=...
554780	461.476011	192.168.0.209	192.168.65.9	TCP	60	56496 > acc-nema [ACK] Seq=190 Ack=20933059 win=...
554781	461.476409	192.168.65.9	192.168.0.209	TCP	60	acc-nema > 56496 [ACK] Seq=190 Ack=20933059 win=...

Follow TCP Stream

Stream Content

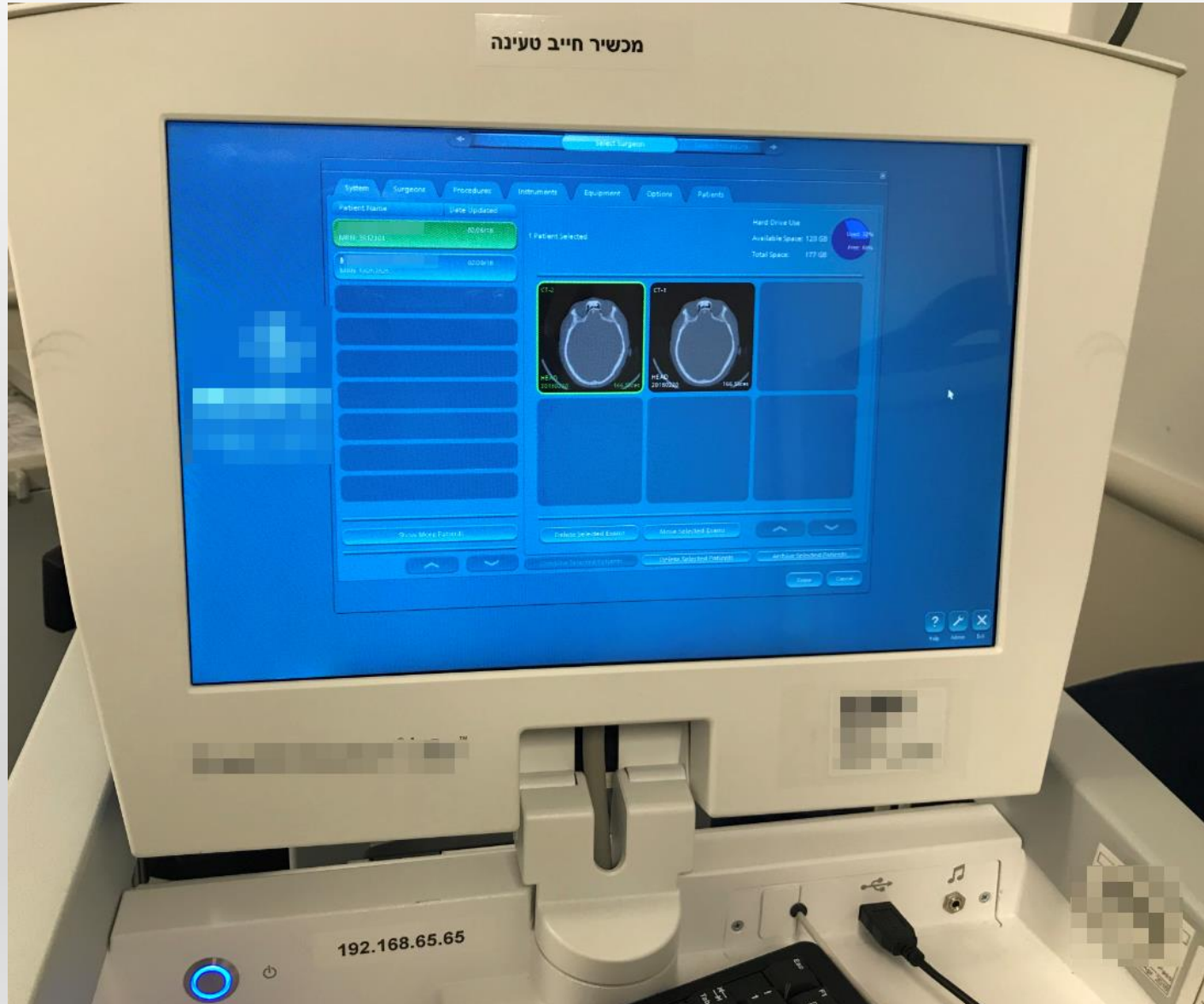
```
.....*...MAMMO_STATION |
DICOM_QR_SCP .....1.2.840.10008.3.1.1.1..g...0...1.
2.840.10008.5.1.4.1.1.7@...1.2.840.10008.1.2.1@...1.2.840.10008.1.2@...1.2.840.10008.1.
2.4.90P..^Q...p.R...1.2.840.113654.2.3.1995.2.12.0U...MIRCTN16NOV2000T.....1.2.840.10
008.5.1.4.1.1.7.....MAMMO_STATION
DICOM_QR_SCP .....1.2.840.10008.3.1.1.1!.....@...1.
2.840.10008.1.2P..9Q....p.R...1.2.276.0.28.3.0.12.080400U...MBC_SCR_0804000.....
1.2.840.10008.5.1.4.1.1.7.....
1.3232252168.1452423118.3412.355069.....
...ISO_IR 192.....DERIVED
\PRIMARY .....1.2.840.10008.5.1.4.1.1.7.....0...1.2.840.113681.32322
52168.1452423118.3412.355069.. ....20160113..!.....20160113..". ....20160113..#.....201
60113..*.....0.....102512..1.....102512..2.....102512..3.....102512..P.....7063787201
60113..V.....MG..a.....d.....WSD..p....., Inc. ....
.....Israel}.....
OLDPACS ..0....Standard Screening - .....>."...R CC .....
.....Mammography ..P.....P.....
E.....P.....
..0...1.2.840.113681.3232252168.1452423118.3412.355060 ...0...1.2.840.113681.3232252168.
1452423118.3412.355066@.p.....P...L.....122400.....DCM .....Sim
ultaneously Acquired ..
.....!.....Z..V.....P.....1.2.840.10008.5.1.4.1.1.
7...U.0...1.2.840.113681.3232252168.1452423118.3412.355065
(.Z....NO@.p.....d.....121322.....DCM .....Source image
for image processing operation ..
.....%t..%p.....
.....0.....2.....@.....F .....
067Y..@.....RRFAST.....36.....AWS:1.7.4.5\M35:1.5.2.0
```

Entire conversation (39367265 bytes)

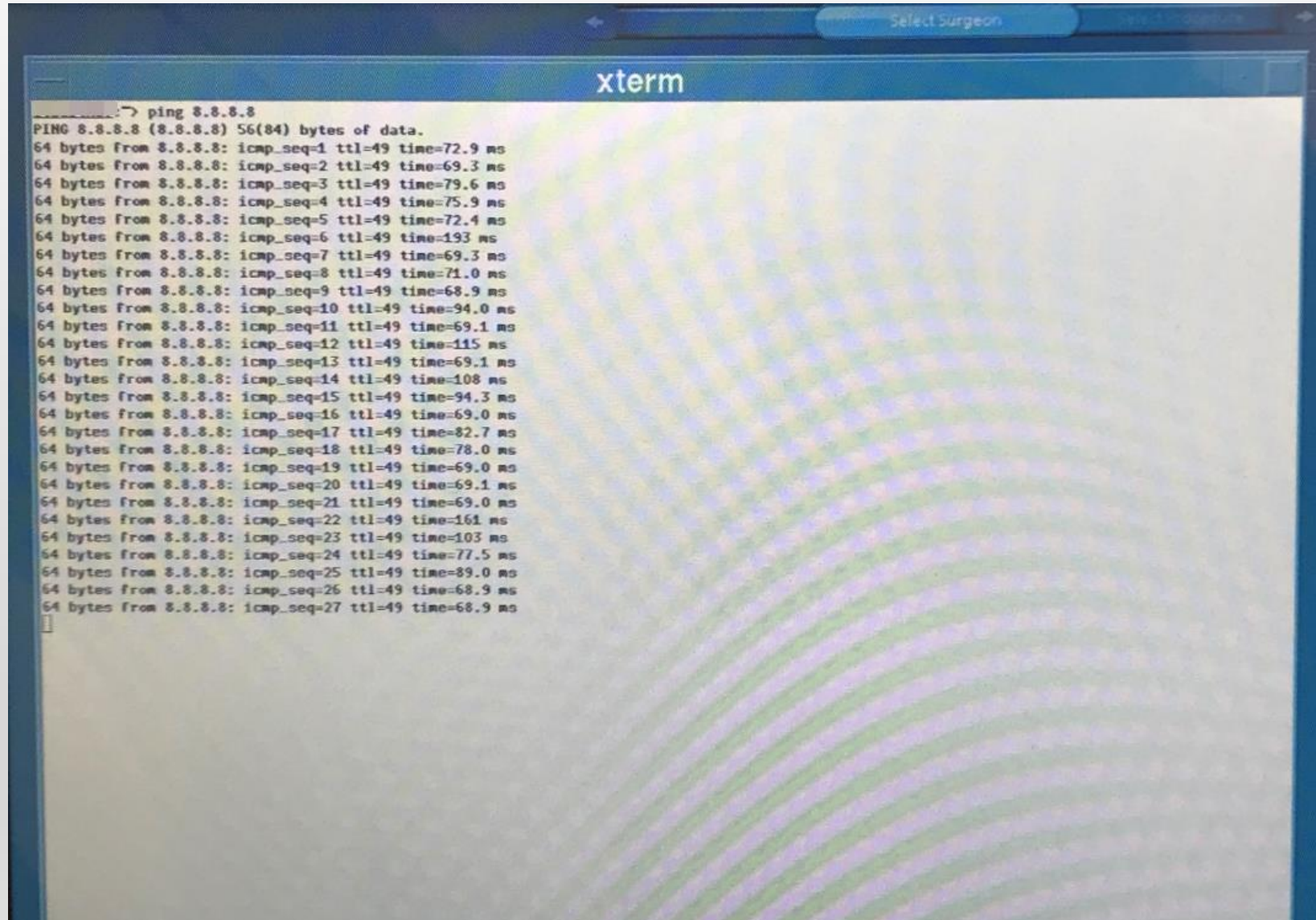
Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw

Help Filter Out This Stream Close

Brain surgical navigation system



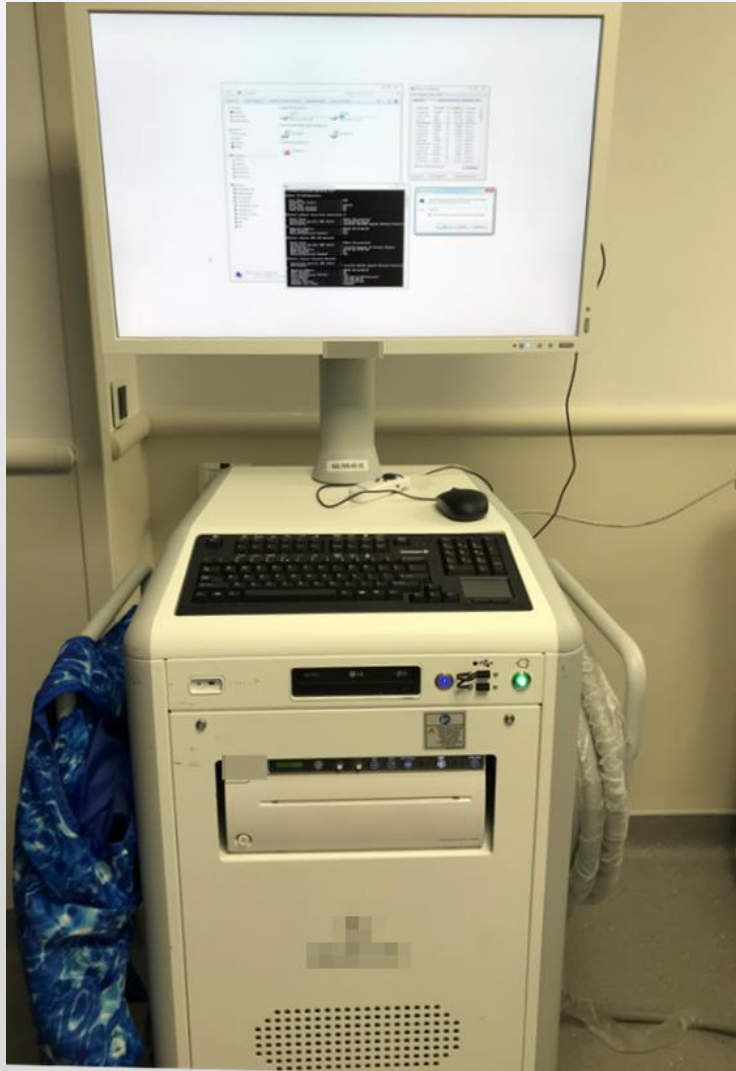
Navigation system – Hello Google ;-)



The image shows a screenshot of a terminal window titled "xterm". The terminal displays the output of a ping command to the IP address 8.8.8.8. The output shows 27 successful ping requests, each returning 64 bytes of data with a TTL of 49 and various response times ranging from approximately 68.9 ms to 161 ms. The terminal window is part of a larger application interface, with a "Select Surgeon" button visible at the top.

```
 Select Surgeon
xterm
-> ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data:
64 bytes from 8.8.8.8: icmp_seq=1 ttl=49 time=72.9 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=49 time=69.3 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=49 time=79.6 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=49 time=75.9 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=49 time=72.4 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=49 time=193 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=49 time=69.3 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=49 time=71.0 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=49 time=68.9 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=49 time=94.0 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=49 time=69.1 ms
64 bytes from 8.8.8.8: icmp_seq=12 ttl=49 time=115 ms
64 bytes from 8.8.8.8: icmp_seq=13 ttl=49 time=69.1 ms
64 bytes from 8.8.8.8: icmp_seq=14 ttl=49 time=108 ms
64 bytes from 8.8.8.8: icmp_seq=15 ttl=49 time=94.3 ms
64 bytes from 8.8.8.8: icmp_seq=16 ttl=49 time=69.0 ms
64 bytes from 8.8.8.8: icmp_seq=17 ttl=49 time=82.7 ms
64 bytes from 8.8.8.8: icmp_seq=18 ttl=49 time=78.0 ms
64 bytes from 8.8.8.8: icmp_seq=19 ttl=49 time=69.0 ms
64 bytes from 8.8.8.8: icmp_seq=20 ttl=49 time=69.1 ms
64 bytes from 8.8.8.8: icmp_seq=21 ttl=49 time=69.0 ms
64 bytes from 8.8.8.8: icmp_seq=22 ttl=49 time=161 ms
64 bytes from 8.8.8.8: icmp_seq=23 ttl=49 time=103 ms
64 bytes from 8.8.8.8: icmp_seq=24 ttl=49 time=77.5 ms
64 bytes from 8.8.8.8: icmp_seq=25 ttl=49 time=89.0 ms
64 bytes from 8.8.8.8: icmp_seq=26 ttl=49 time=68.9 ms
64 bytes from 8.8.8.8: icmp_seq=27 ttl=49 time=68.9 ms
```

Portable computed tomography (CT)



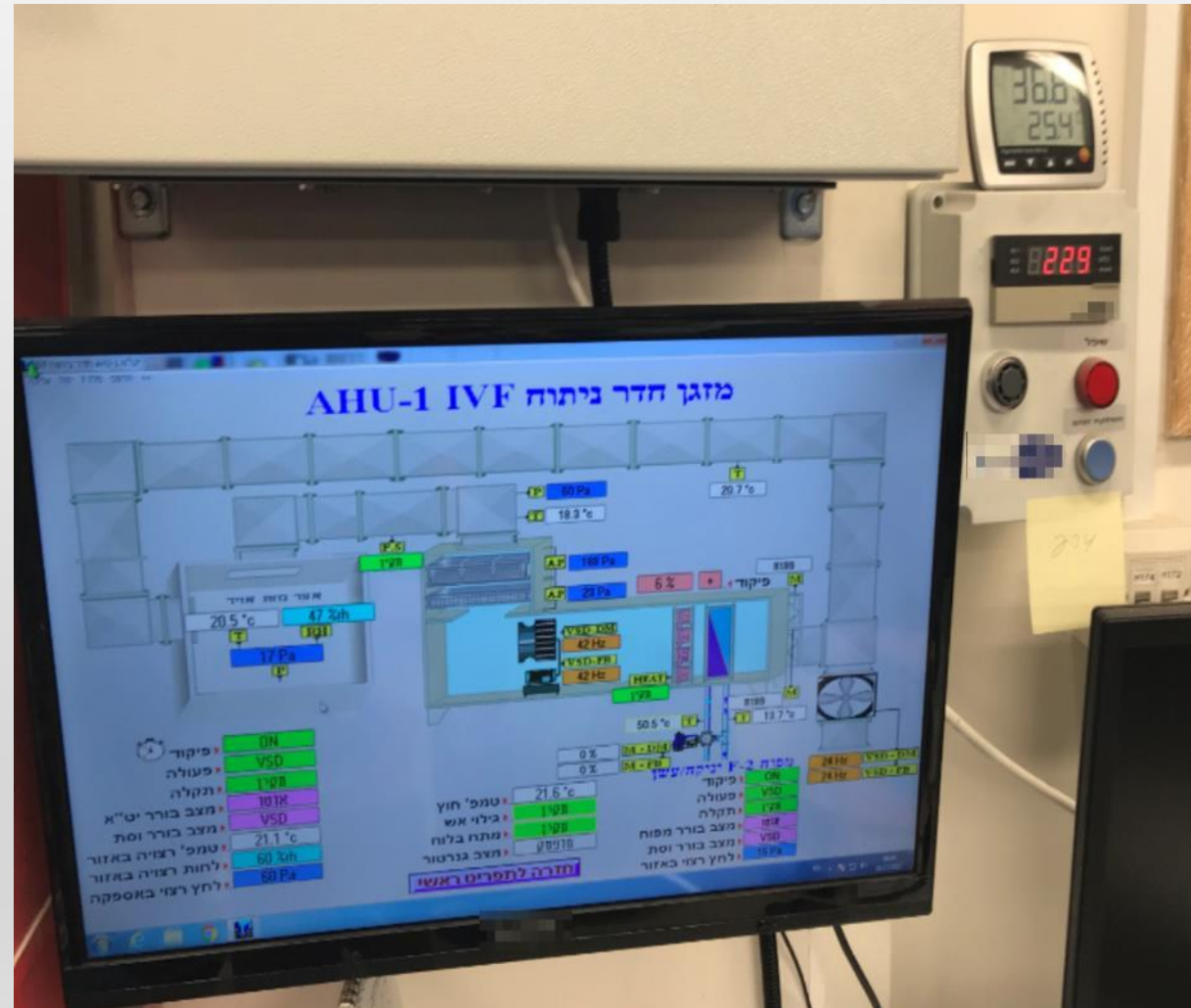
Portable CT – Hello VNC ;-)

The screenshot displays a medical software interface within a TightVNC Viewer window. The window title is "mvs (192.168.65.10) - TightVNC Viewer". The interface is divided into several sections:

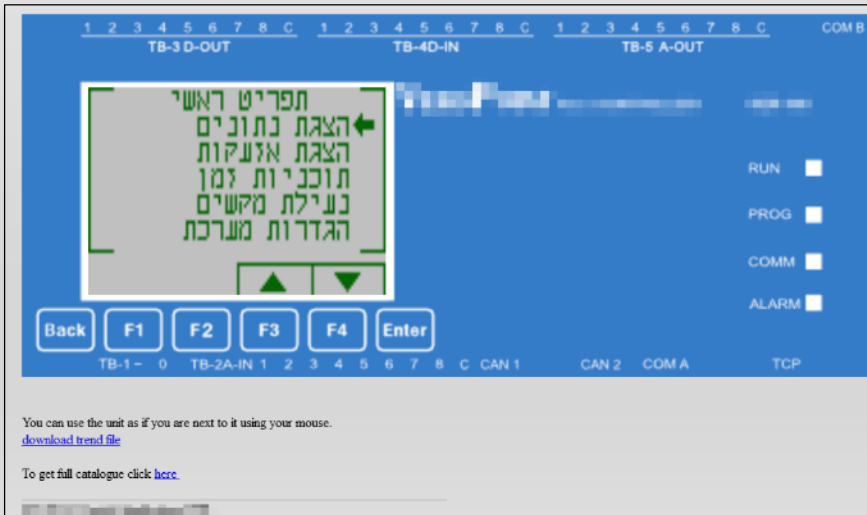
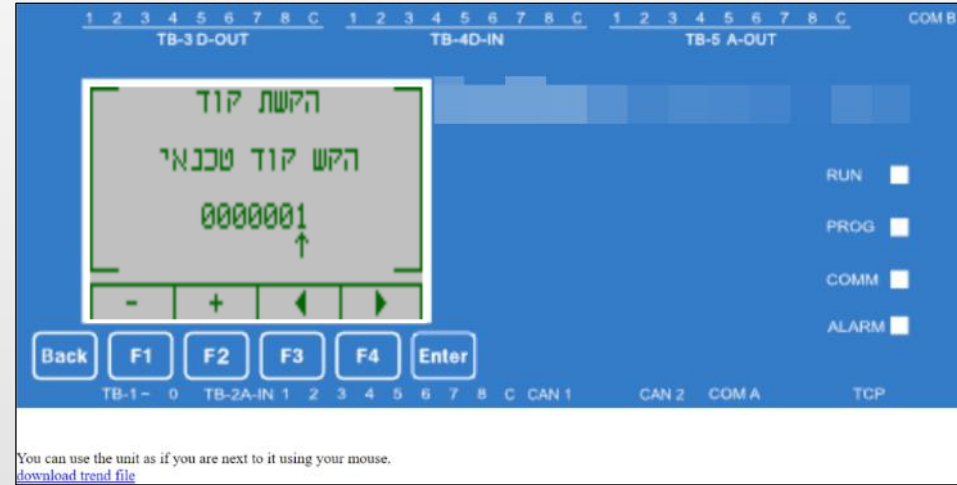
- Image Preview:** A large window showing a CT scan of a patient's head and neck. The scan is annotated with a pair of scissors. Below the image, the text "Press 'A' to annotate image" is visible.
- Exam Information / Scheduled Exgms / Saved Exams:** A navigation bar with tabs for "Exam Information", "Scheduled Exgms", and "Saved Exams".
- List of 243 patients:** A table listing patient information. The table has columns for Name, Prevent Deletion, Patient ID, and Date.
- Patient Details:** Below the list, there are fields for "Patient Name:" and "Patient ID:", and a "Date Of Birth:" field with the value "2/1".
- Image Thumbnails:** A row of four small image thumbnails, each with a label below it: "3D 1", "2D 7", "2D 6", and "2D 5".
- Buttons:** At the bottom, there are buttons for "Delete Patient", "Edit Exam", "Select Image", "Annotate", and "Switch Images".

Name	Prevent Deletion	Patient ID	Date
3/7 M	<input type="checkbox"/>		3/7/2018 9:42:
KH J	<input type="checkbox"/>	64	3/6/2018 7:12:
RC	<input type="checkbox"/>	56	3/5/2018 6:38:
AD JEL	<input type="checkbox"/>	PA 976	3/5/2018 10:32:
ZU	<input type="checkbox"/>	30	3/5/2018 7:24:
BA	<input type="checkbox"/>	30	3/4/2018 3:37:
OL NINA	<input type="checkbox"/>	32	3/4/2018 11:22:
RA AS	<input type="checkbox"/>	70	3/4/2018 7:26:
HC	<input type="checkbox"/>	P4 200	2/28/2018 7:18:
KA VID	<input type="checkbox"/>	53	2/27/2018 8:05:
TN	<input type="checkbox"/>	57	2/26/2018 3:12:
SW	<input type="checkbox"/>	35	2/25/2018 5:06:
SH ON	<input type="checkbox"/>	57	2/22/2018 9:39:
KO ALEXA...	<input type="checkbox"/>	31	2/18/2018 7:23:
ISF DIA	<input type="checkbox"/>	31	2/18/2018 3:39:
HA SA	<input type="checkbox"/>	54	2/18/2018 11:3:
FR A	<input type="checkbox"/>		2/12/2018 5:39:
ZR AVA	<input type="checkbox"/>	59	2/12/2018 10:5:
phi	<input type="checkbox"/>	31	2/12/2018 8:01:
BE II SIMHA	<input type="checkbox"/>	63	2/11/2018 7:07:
KA AFEM	<input type="checkbox"/>	30	2/4/2018 5:07:
RC A	<input type="checkbox"/>	32	2/4/2018 1:48:
CH SL	<input type="checkbox"/>	68	1/29/2018 6:10:
TAI NADII	<input type="checkbox"/>	P6 9326	1/22/2018 7:03:
PAI EXAN...	<input type="checkbox"/>	30	1/21/2018 6:37:
VE INA	<input type="checkbox"/>	67	1/21/2018 12:5:
AM ART	<input type="checkbox"/>	33	1/21/2018 10:2:
NA IARA	<input type="checkbox"/>		1/15/2018 3:47:

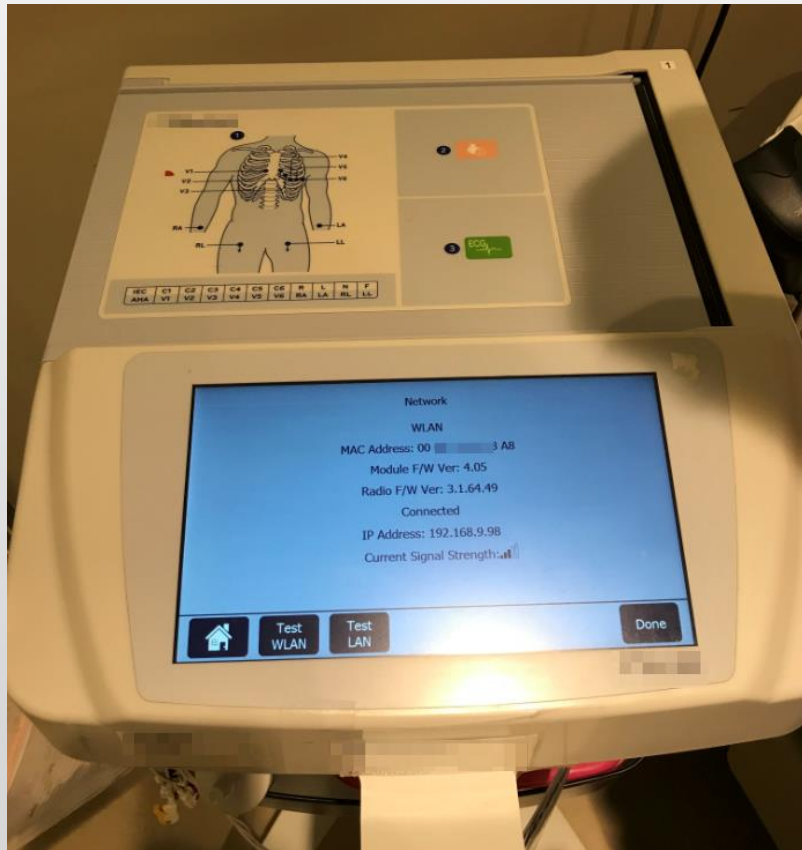
Programmable logic controllers (PLC's)



Programmable logic controllers (PLC's)



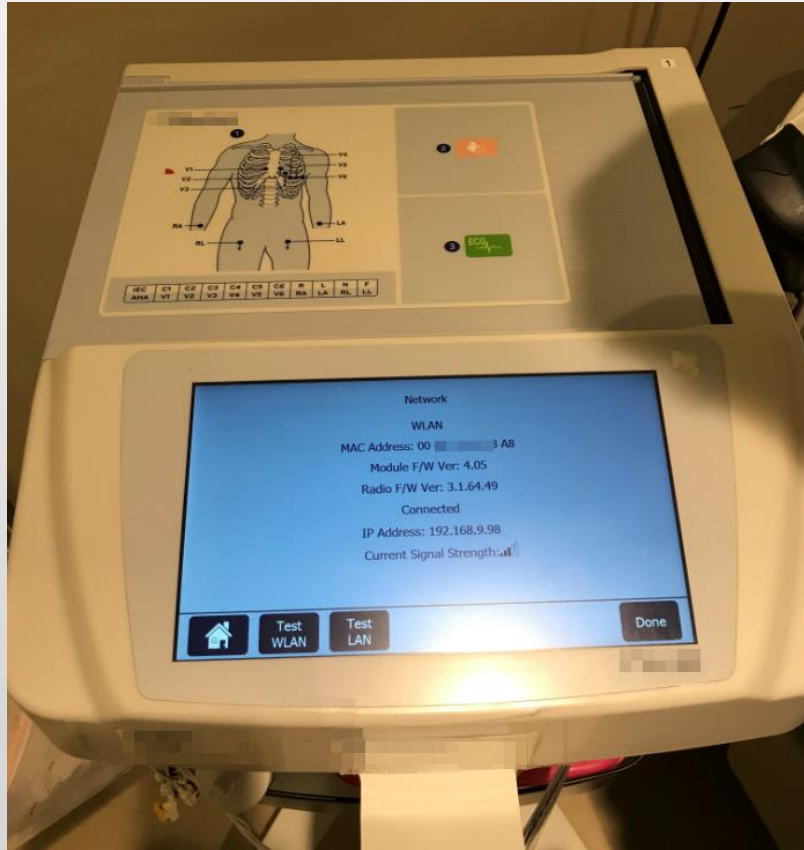
Electrocardiography (ECG/EKG) – default passwords



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.
```

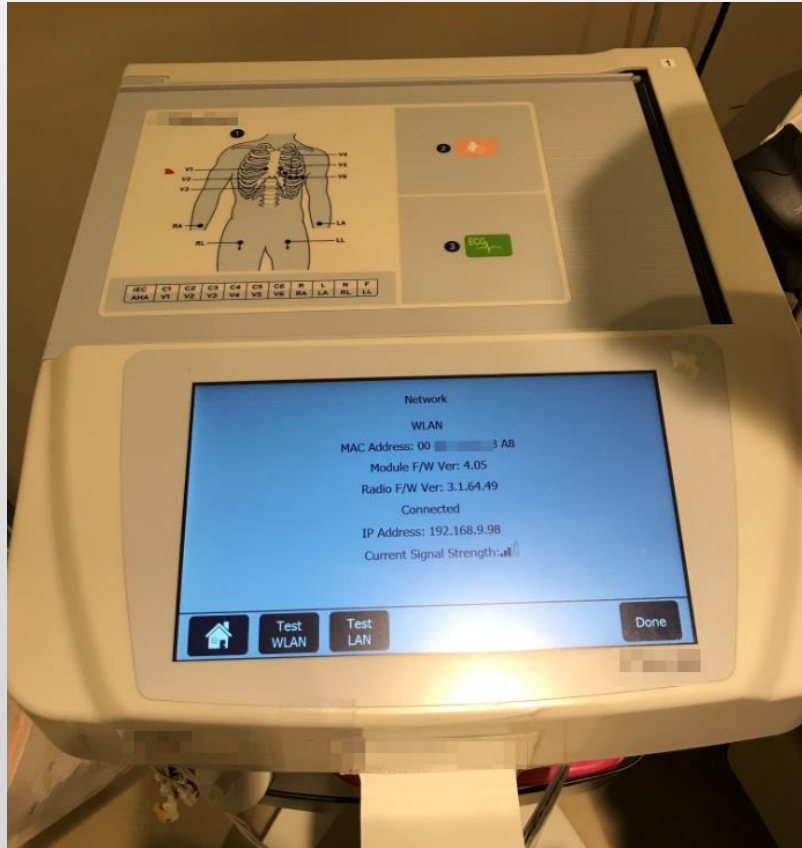
Electrocardiography (ECG/EKG)



```
0x Telnet 192.168.9.98
auth
OK
?
?
-match
-match2
le-time
t-time
led
ename
lename
```

```
server-address |ls
OK
server-address
|ls
bin
dev
etc
home
lib
linuxrc
mnt
proc
root
sbin
sys
tmp
usr
var
web
```

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?



