ALTERNANZA SCUOLA·LAVORO IN ISS

05-15 Febbraio 2019

Percorso formativo:
PS04. Attacchi informatici in sanità? Conoscere per difendersi

Studenti/Liceo:

Antonio DI FOLCO - Liceo Scientifico S. A. Montessori

Geraldine Alison MONTALVO HUAMANI - Liceo Scientifico Louis Pasteur

Marco Antonio SANTIAGO GALLEGOS - Liceo Scientifico V. Volterra

Referenti (Affiliazioni)

Mauro Grigioni (TISP), Francesco Gabbrielli (TETA)

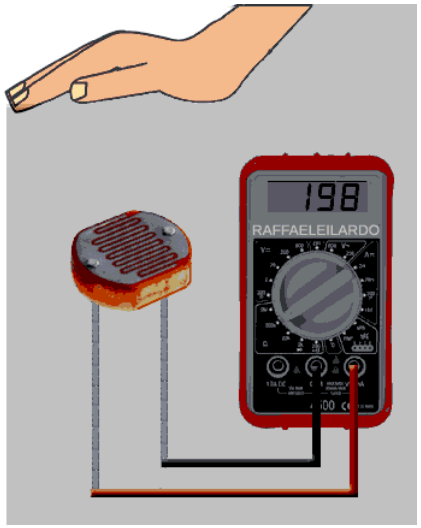
Tutor/Collaboratori (Affiliazioni)

Giuseppe D'Avenio (TISP), Sandra Morelli (TISP), Alessandro Spurio (TISP)

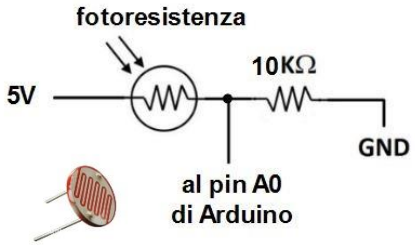
Fausto Giuliani (TISP), Maurizio Lucentini (TISP), Fabio Santavenere (TISP)

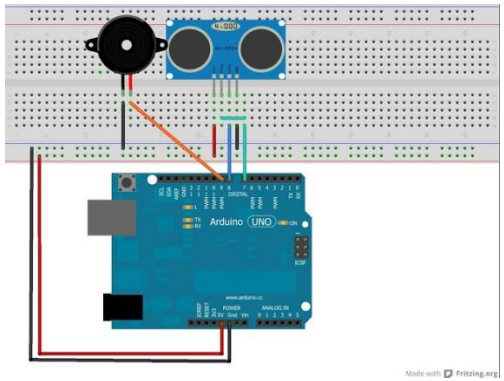
Misura di grandezze fisiche

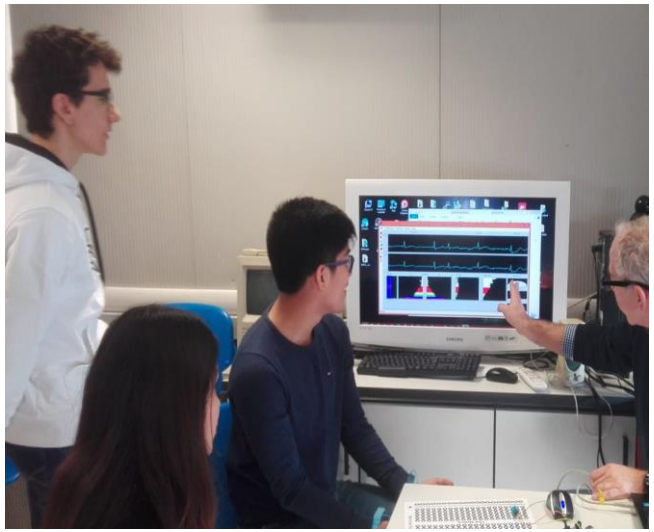
Lettura manuale di grandezze fisiche: tensione, resistenza, intensità luminosa, ….



..e poi acquisizione di grandezze fisiche con strumenti elettronici: sensori analogici e digitali

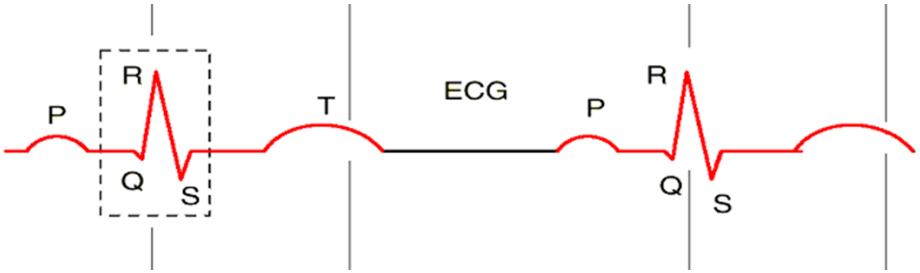


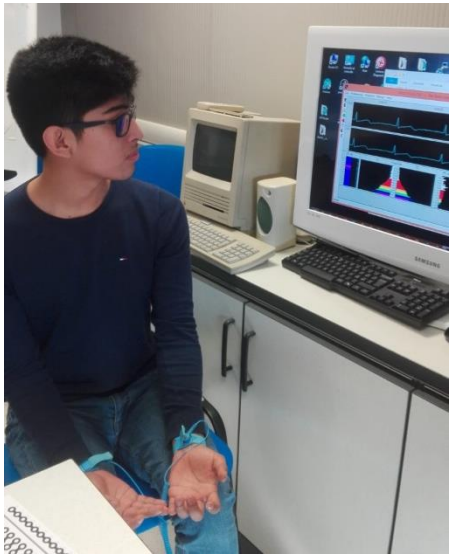




I dati biomedici

***Segnali bioelettrici**, come ad esempio l'**ECG**, che si manifestano come variazioni di campo elettrico, che avvengono nel corpo.*





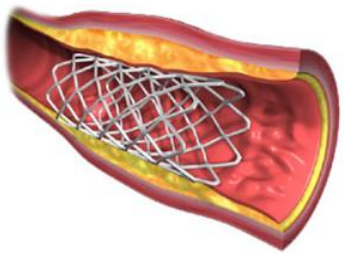
ECG – Elettrocardiogramma

Abbiamo acquisito e registrato su file il nostro ECG e abbiamo calcolato da esso il nostro battito cardiaco.

I parametri fisiologici diventano dati digitali e possono essere trasmessi in rete …….

I dispositivi medici

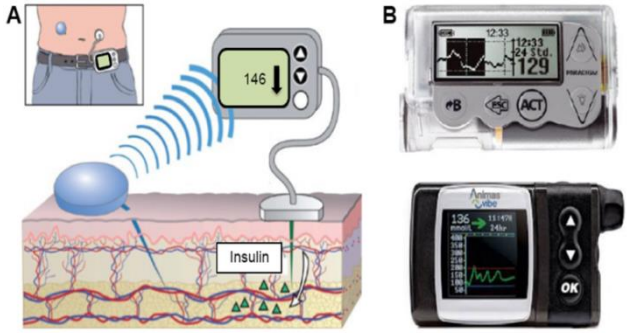
Esempi di DM impiantabili



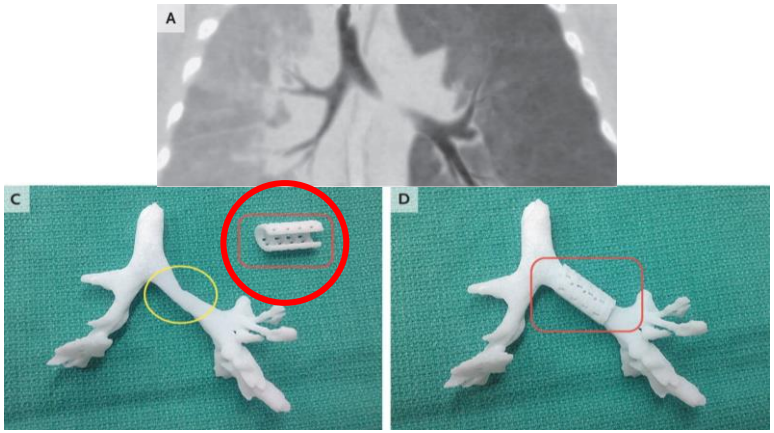
Stent vascolare

Protesi d'anca

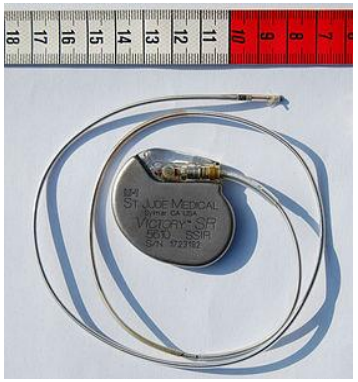
Pompa di insulina



Splint bronchiale



Pacemaker



DM con comunicazione wireless e quindi potenzialmente *vulnerabili*

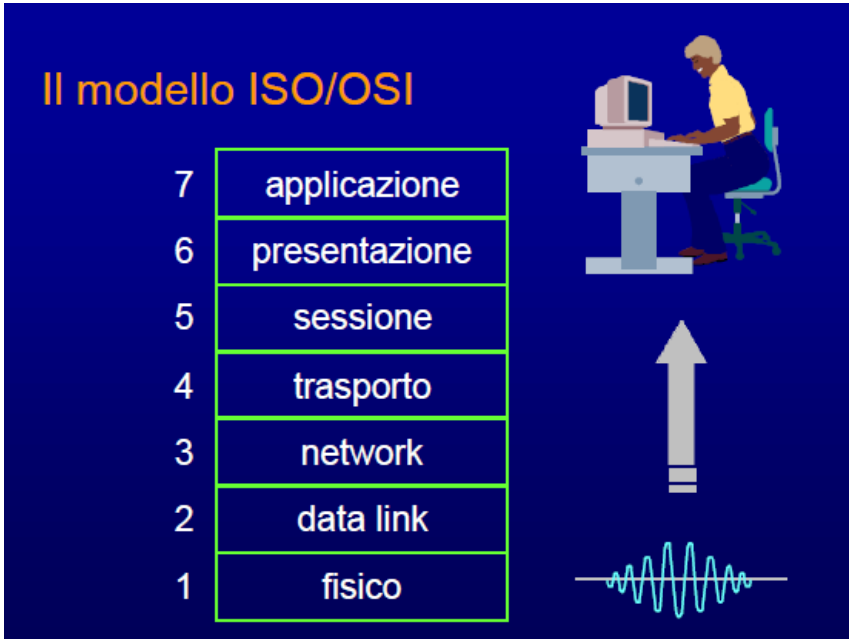
La Banca Dati dei dispositivi medici del Ministero della Salute:
http://www.salute.gov.it/interrogazioneDispositivi/RicercaDispositiviServlet?action=ACTION_MASCHERA

Le reti e Internet

Dalla teoria ……

Ogni computer ha un suo indirizzo IP (*Internet Protocol*) e generalmente è rintracciabile

Il sistema di comunicazione tra macchine è organizzato in 7 livelli, modello **ISO/OSI**: dal livello fisico, il livello più basso, dove a esser regolato è lo scambio di bit tra due nodi della rete fino al livello di applicazione, il livello più alto, dove le comunicazioni avvengono tramite software applicativi tra utenti (ad es. scambio di e-mail; trasferimento di file; collegamento ad un sito web tramite Internet, con un browser).




```
C:\Users\sandra>ipconfig

Configurazione IP di Windows


Scheda LAN wireless Connessione rete wireless:

   Suffisso DNS specifico per connessione: iss.it
   Indirizzo IPv6 locale rispetto al collegamento . : fe80::db4:f616:b377:50f7%1
2
   Indirizzo IPv4. . . . . . . . . . . . : 172.30.0.137
   Subnet mask . . . . . . . . . . . . . : 255.255.0.0
   Gateway predefinito . . . . . . . . . : 172.30.255.254

Scheda Ethernet Connessione alla rete locale (LAN):

   Stato supporto. . . . . . . . . . . . : Supporto disconnesso
   Suffisso DNS specifico per connessione: iss.it

Scheda Tunnel isatap.iss.it:

   Stato supporto. . . . . . . . . . . . : Supporto disconnesso
   Suffisso DNS specifico per connessione: iss.it

Scheda Tunnel Teredo Tunneling Pseudo-Interface:

   Stato supporto. . . . . . . . . . . . : Supporto disconnesso
   Suffisso DNS specifico per connessione:
```

Alla pratica ……

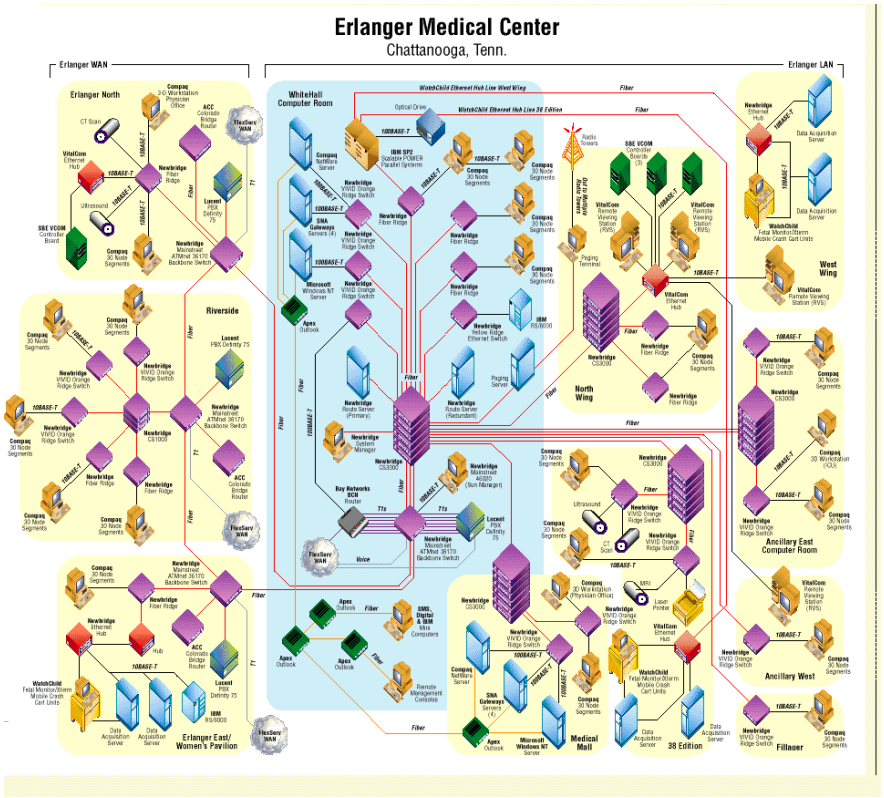
Utilizzo di comandi standard per il controllo delle connessioni:

- «*ipconfig*»
- «*ping*»
- «*tracert*»
- …

Le reti mediche

Dalla teoria……..

Reti mediche: sistemi di complessità crescente



Alla pratica …

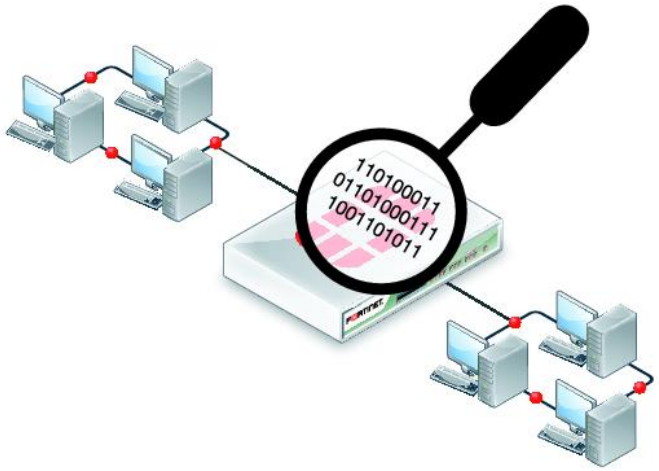
Dalla complessità crescente derivano *vulnerabilità crescenti*. Raccomandazioni e buone pratiche: controllo nella distribuzione di password; aggiornamento regolare delle stesse; aggiornamento e patch dei SO e dei SW.

Ministero del Lavoro, della Salute e delle Politiche Sociali

DIPARTIMENTO DELLA QUALITA'
DIREZIONE GENERALE DELLA PROGRAMMAZIONE SANITARIA E DEI LIVELLI DI ASSISTENZA E DEI PRINCIPI ETICI DI SISTEMA
UFFICIO III
DELL'EX MINISTERO DELLA SALUTE

RACCOMANDAZIONE PER LA PREVENZIONE DEGLI EVENTI AVVERSI CONSEGUENTI AL MALFUNZIONAMENTO DEI DISPOSITIVI MEDICI/APPARECCHI ELETTROMEDICALI

Vulnerabilità e attacchi



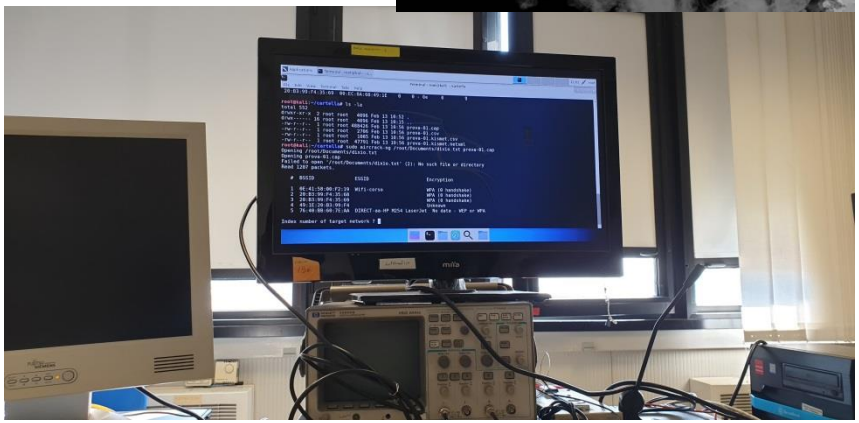
Dalla teoria …

Una delle tecniche usate dagli hacker (*man in the middle*) è lo ***sniffing***

E una possibile tecnica di difesa per testare la vulnerabilità di un sistema (reti, sistemi operativi, applicazioni) è l'utilizzo di strumenti di attacco in difesa!!!

Sniffing di password (WLan)

Con l'utilizzo di Kali Linux dopo aver eseguito una serie di comandi siamo riusciti ad ottenere la password della rete wi-fi alla quale eravamo connessi

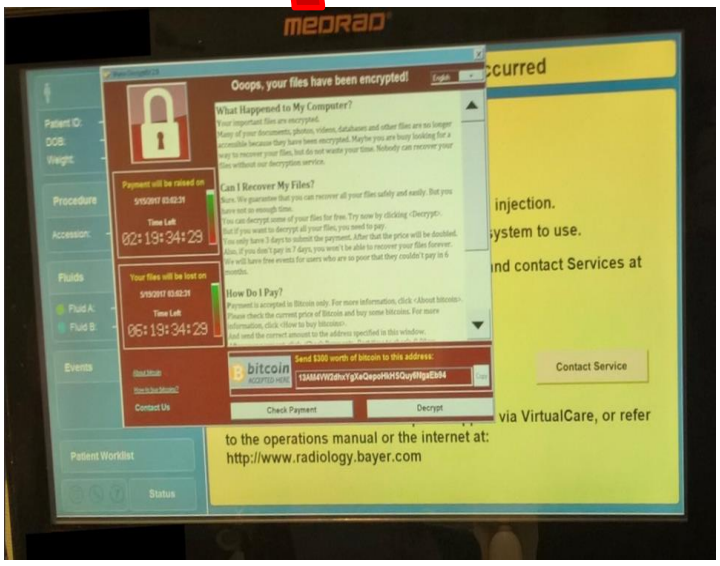


Vulnerabilità e attacchi in sanità

Attacco alla rete ospedaliera (SIS e DM) - Apparecchiatura radiologica

Nel maggio 2017 il *ransomware* WannaCry ha colpito circa 200.000 sistemi informatici basati su Windows in strutture mediche in tutto il mondo e anche DM: "Medical Devices Hit By Ransomware For The First Time in US Hospitals" posting to the website of Forbes Magazine: https://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/#44b2a5a6425c

Colpito anche il DM «Iniettore di potenza" della Bayer Medrad.
L'iniettore è interfacciato con il sistema di imaging radiologico, per verificare la qualità delle immagini ottenute con la minima quantità possibile di mezzo di contrasto, e per poter essere attivato anche da una stanza di controllo esterna a quella in esame.
Monitor di comando dell'iniettore, con display touch-screen, con PC (SO Windows) collegato alla rete ospedaliera (SIS).



Vulnerabilità e attacchi in sanità

Attacco alla rete ospedaliera

Spesso la protezione dai rischi di attacchi informatici in sanità si può implementare con precauzioni di base

NHS could have avoided WannaCry hack with 'basic IT security', says report

National Audit Office says NHS and Department of Health must 'get their act together' or suffer 'far worse' than chaos experienced in May

▲ Five hospitals had to divert ambulances away after the WannaCry hack. Photograph: Andy Rain/EPA

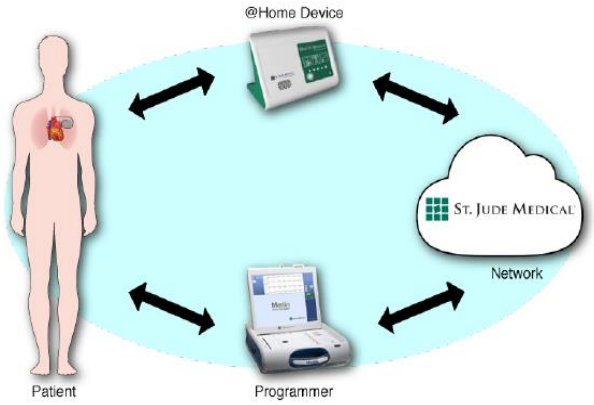
The NHS could have avoided the crippling effects of the "relatively unsophisticated" WannaCry ransomware outbreak in May with "basic IT security", according to an independent investigation into the cyber-attack.

Vulnerabilità: punto debole del sistema a fronte di una certa minaccia
Minaccia: insieme di circostanze che può potenzialmente creare danni
Rischio: esprime la probabilità che un evento accada e l'entità del danno che arreca al sistema, se questo accade

Attacco: qualsiasi azione che usa una vulnerabilità per concretizzare una minaccia
Diverse sono le aree di vulnerabilità di un Sistema Informativo, rete aziendale o rete privata, e diverse sono le minacce informatiche.
Contromisura: azione, dispositivo, procedura o tecnica che consente di rimuovere o di ridurre una vulnerabilità

Vulnerabilità e attacchi in sanità

Pacemaker - DM impiantabile: rischio di attacco wireless



Gli avvisi di sicurezza

FDA. "Cybersecurity Vulnerabilities Identified in **St. Jude** Medical's Implantable Cardiac Devices and ***Merlin@Home Transmitter***: FDA Safety Communication", **09 January 2017**: http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843.htm

Archivio degli avvisi di sicurezza del **Ministero della Salute** (http://www.salute.gov.it/portale/news/p3_2_1_3_1.jsp?lingua=italiano&menu=notizie&p=avvisi&tipo=dispo&dataa=2019/12/31&datada=2017/01/01): avviso del **3 aprile 2017**

Abbiamo cercato *notizie di vulnerabilità dei DM* sui siti degli Enti governativi:

FDA (Food and Drug Administration, USA): www.fda.gov

Ministero della Salute, IT: www.salute.gov.it

Gruppo Cybersecurity

Gruppo di studio nazionale per la sicurezza in Sanità

https://ufficiostampa.iss.it/?p=224

CS N°5/2018 – Sicurezza informatica in sanità, nasce il primo gruppo di studio nazionale

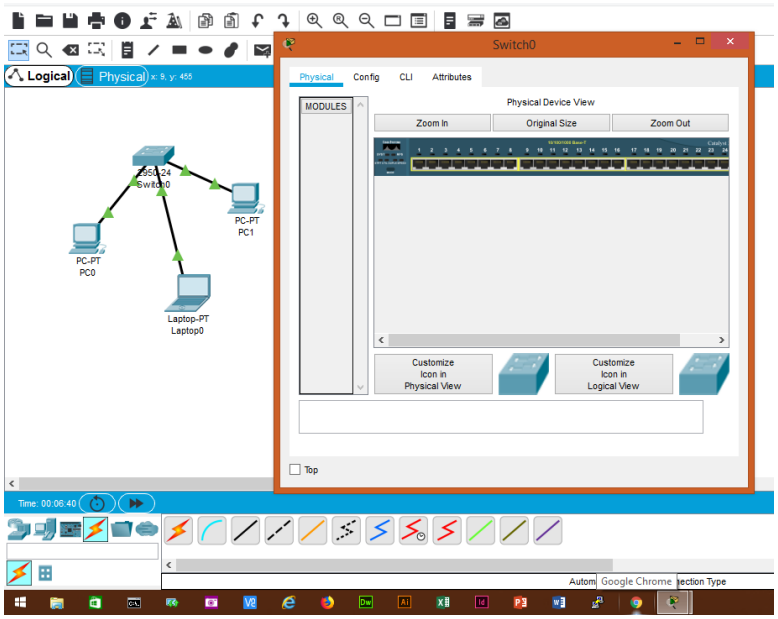
Coordinato dall'ISS

Centri referenti ISS:

- Centro Nazionale per la Telemedicina e le Nuove Tecnologie Assistenziali (**TETA**) – **Francesco Gabbrielli**
- Centro Nazionale di Tecnologie Innovative in Sanità Pubblica (**TISP**) – **Mauro Grigioni**

I laboratori …

Dal laboratorio reale …..
Schede Arduino, Raspberry e vari componenti elettronici



… al laboratorio virtuale …
che utilizza SW specifici free capaci di simulare il funzionamento di una rete al fine di poter individuare le vulnerabilità HW e SW


Hacker non mi fai paura!
So come difendermi…..
Al di là del mondo reale… vi è uno virtuale e vale la pena conoscerlo!!!
GRAZIE!