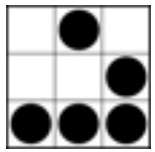
Basta Hacker in TV!

Come la percezione distorta della realtà influenza negativamente la nostra capacità di giudizio



http://www.alba.st/
Verona, Milano, Roma
Phone/Fax +39 045 8271202

Alessio L.R. Pennasilico
a.pennasilico@alba.st

$whois -=mayhem=-

Security Evangelist @ Alba st

Committed:

AIP Associazione Informatici Professionisti, CLUSIT

AIPSI Associazione Italiana Professionisti Sicurezza Informatica

Italian Linux Society, Sikurezza.org, Spippolatori, AIP/OPSI, IISFA

Hacker's Profiling Project, CrISTAL

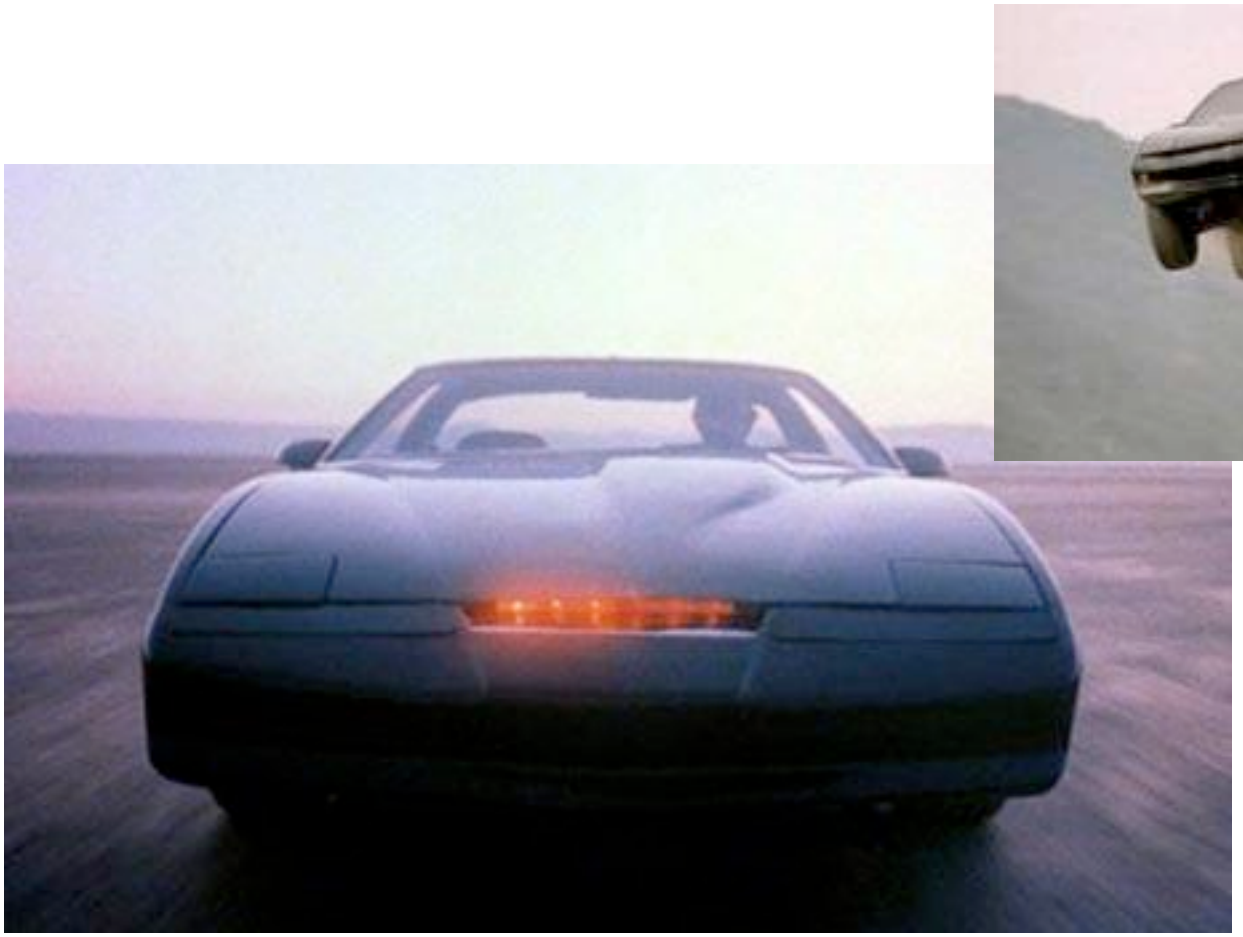
Clusit Associazione Italiana per la Sicurezza Informatica

AIP Associazione Informatici Professionisti ITCS Italian Computer Society

International Information Systems Forensics Association iisfa

Mia nonna diceva...

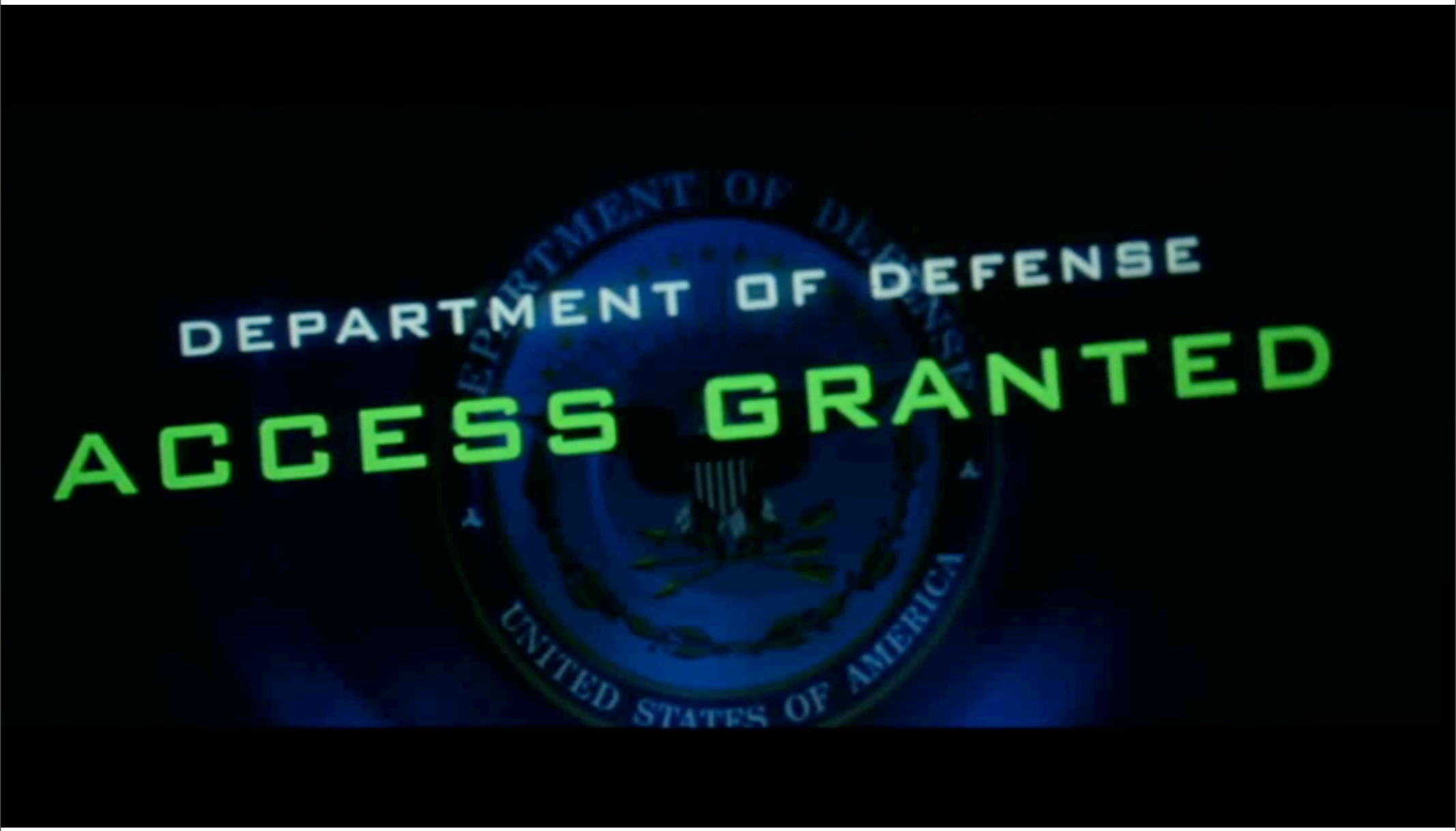
Non credere a tutto quel che vedi in televisione...



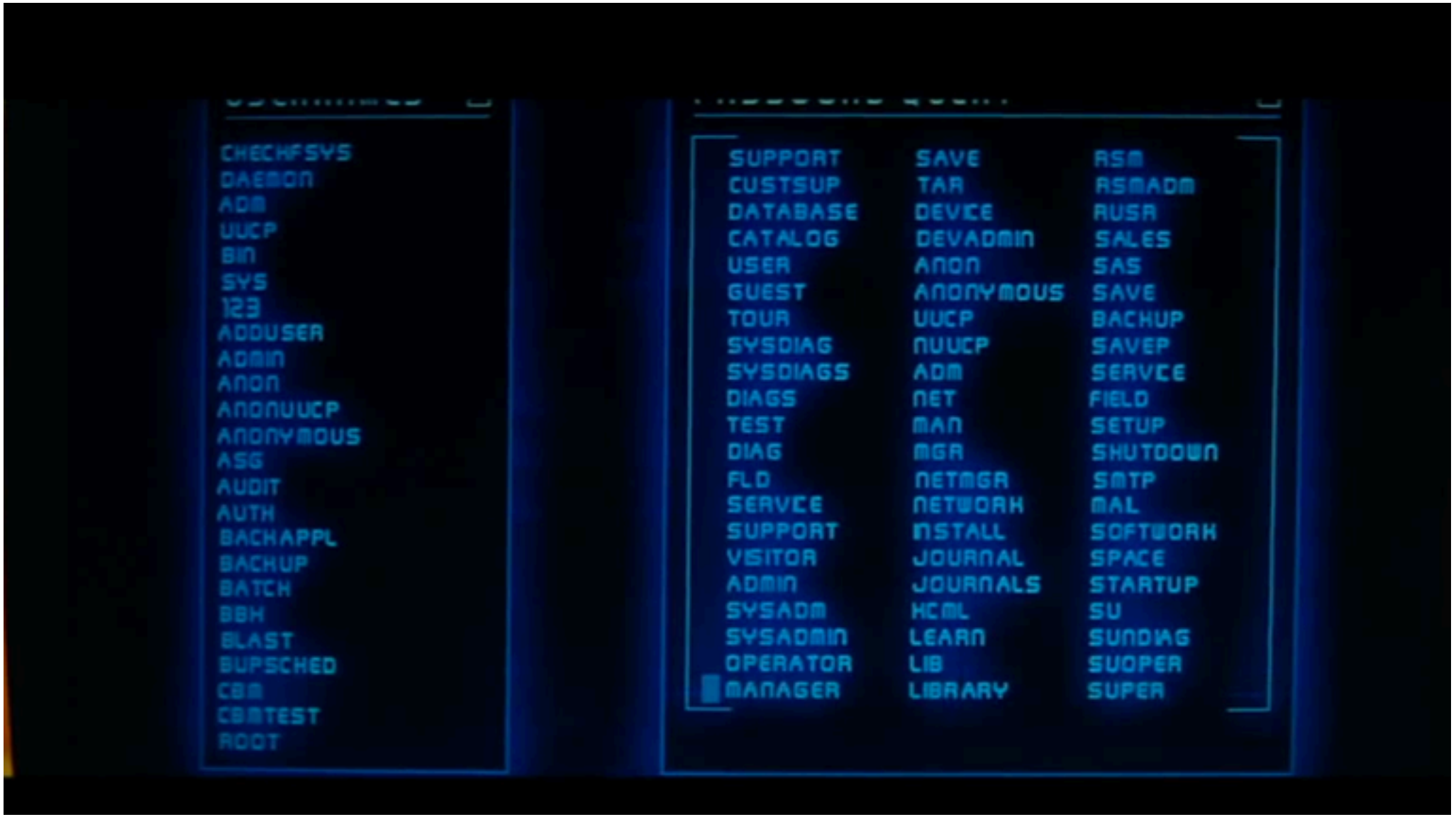
La tecnologia dei desideri...

Manca il realismo

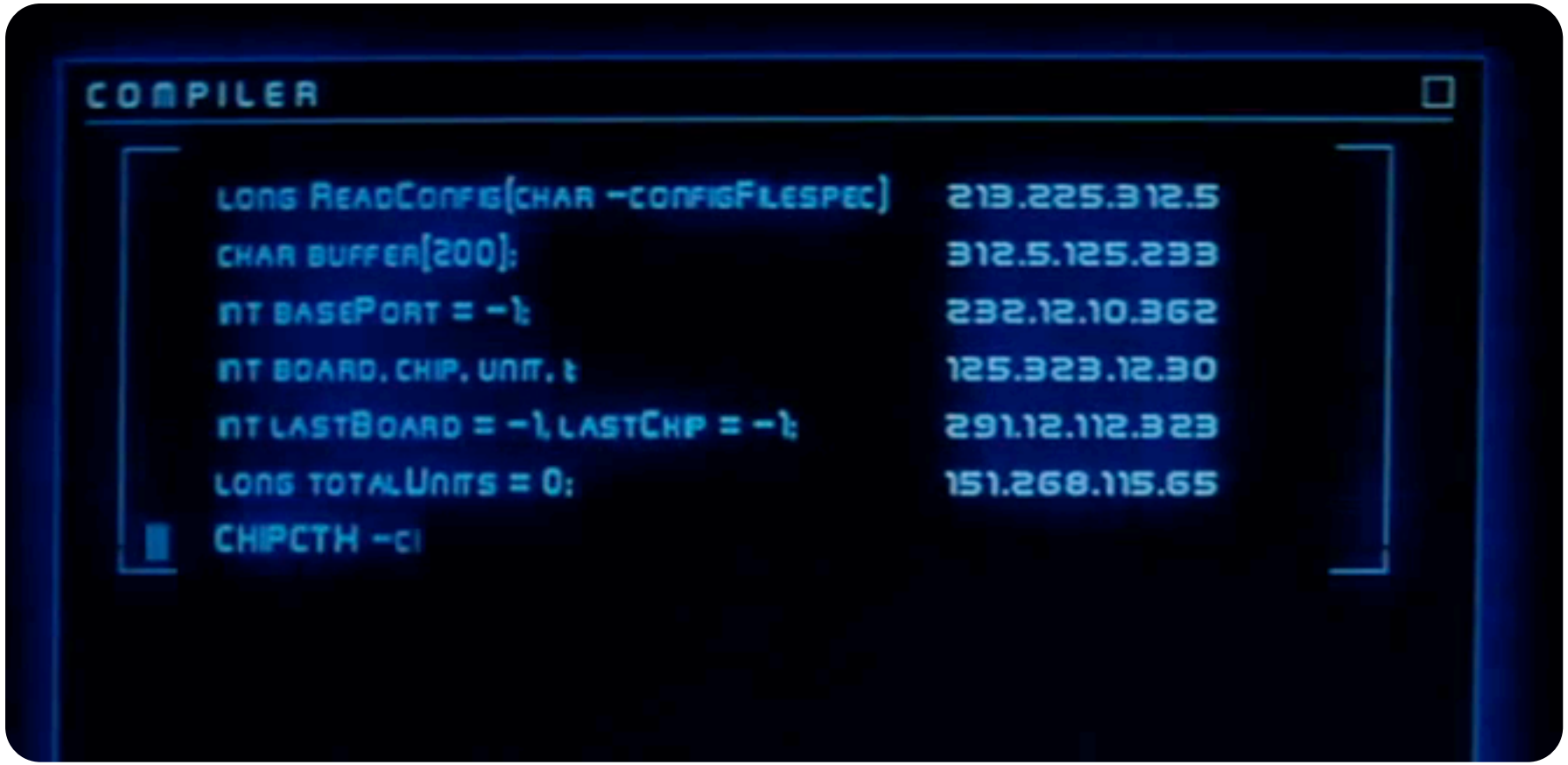
Linguaggio ed immagini



Brute Forcing?

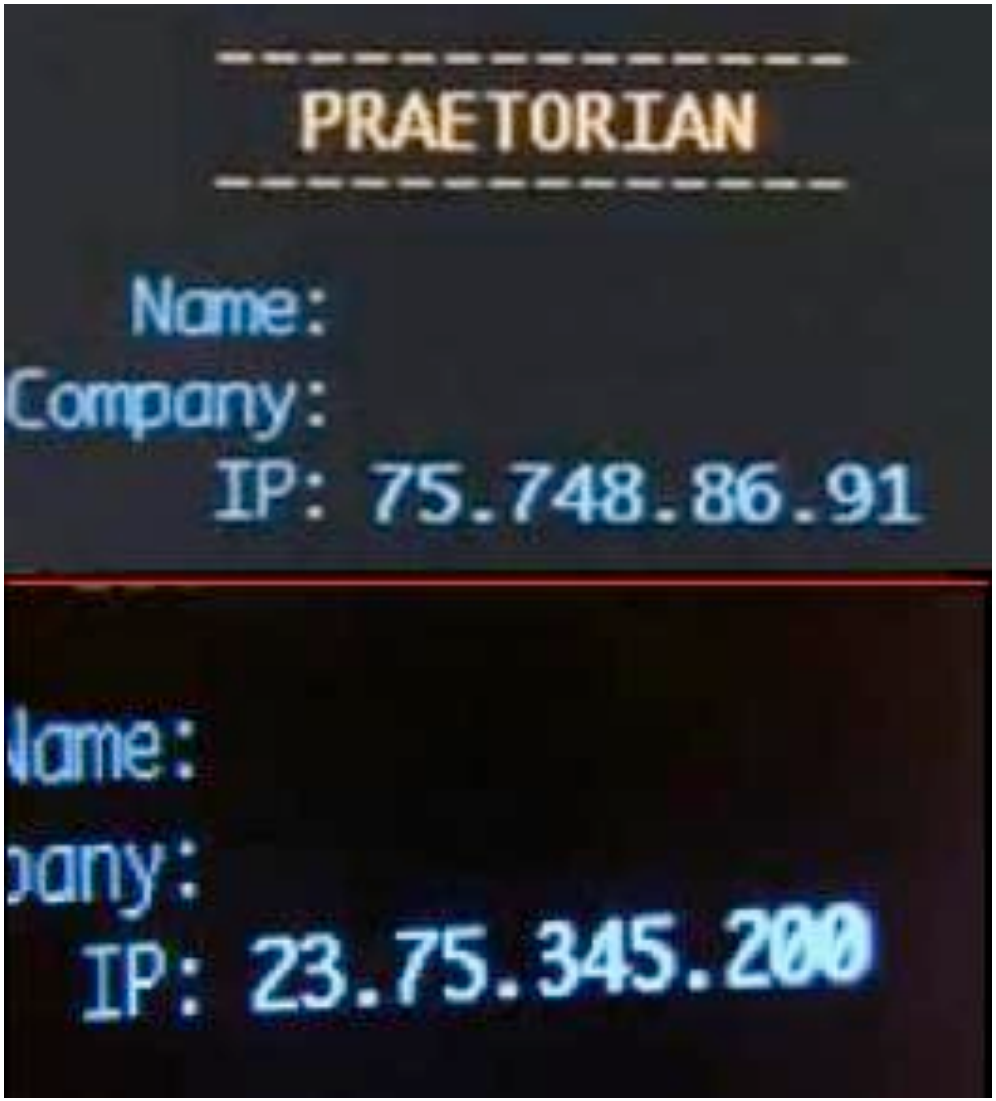


Anonimizzare le informazioni

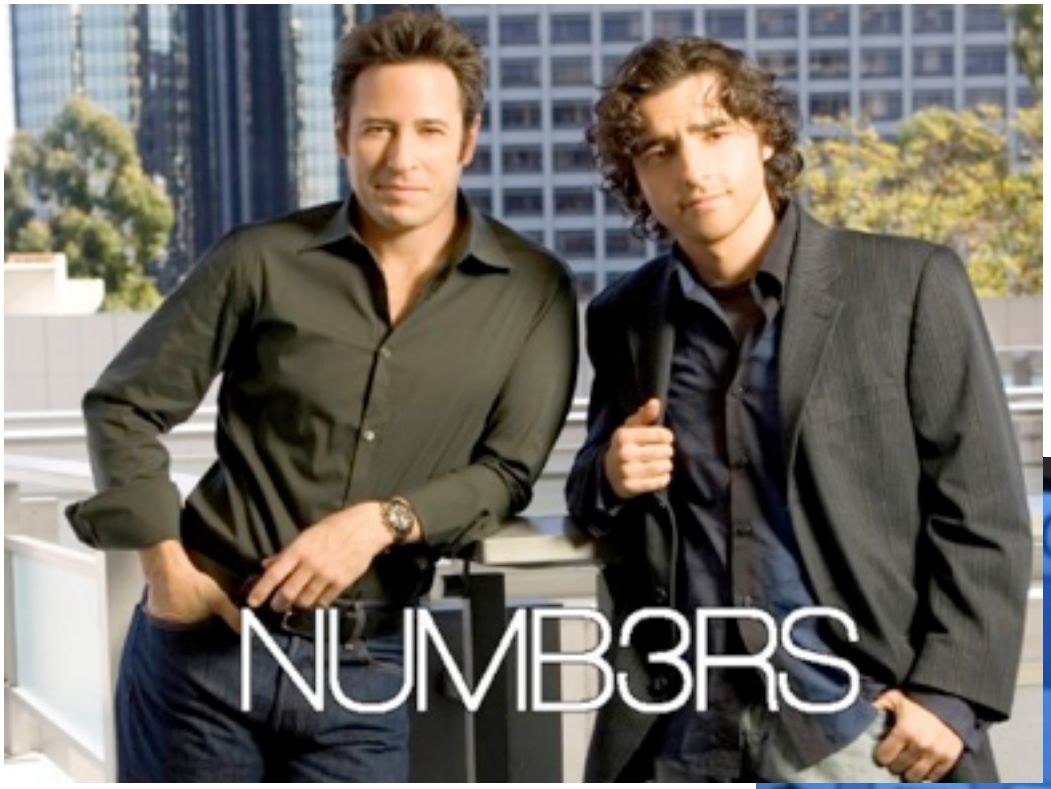


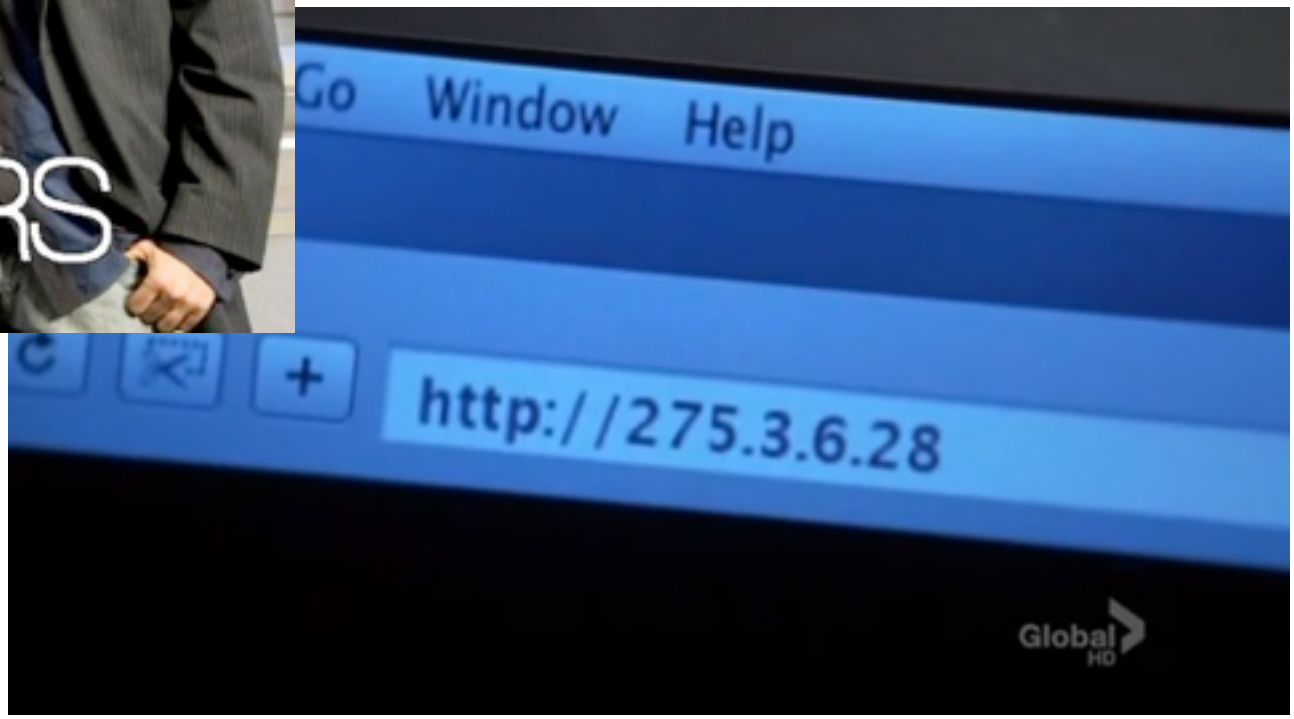
Prassi...


Escape is
impossible
when you're
caught in...
THE
NET
A FILM BY IRWIN WINKLER


PRAETORIAN
Name:
Company:
IP: 75.748.86.91
Name:
pany:
IP: 23.75.345.200

Prassi...



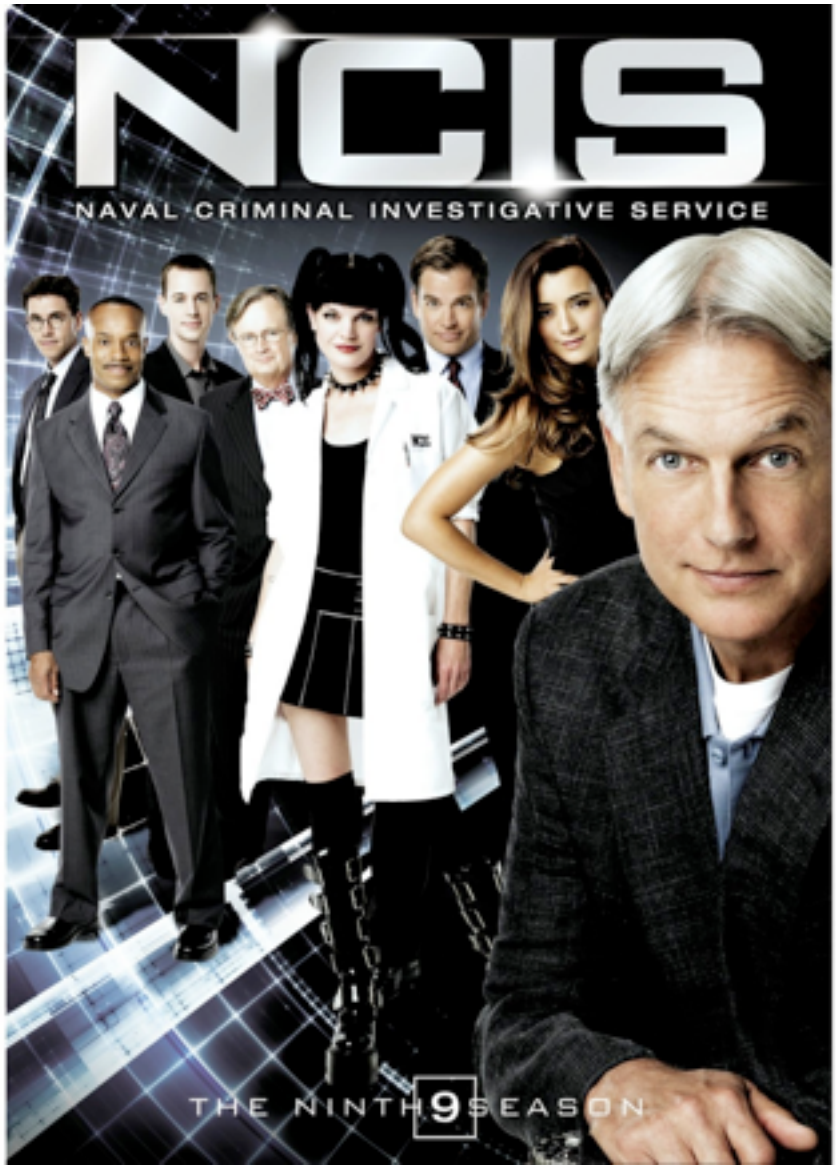


Visualroute?

Chi di voi lo usa per determinare la sorgente di un attacco?

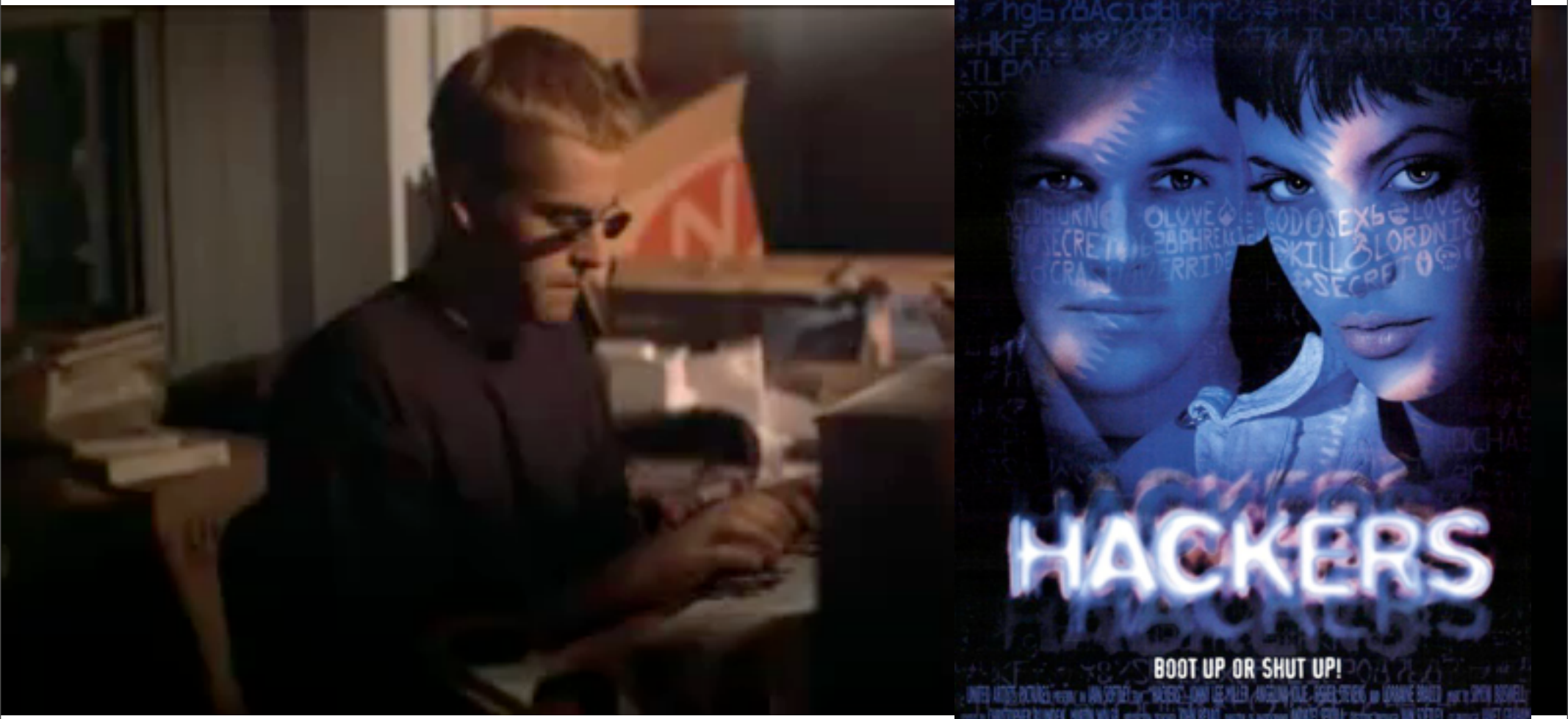
Forenser?


CSI:
CSI: CSI:NY CSI:
AXN


NCIS
NAVAL CRIMINAL INVESTIGATIVE SERVICE
THE NINTH 9 SEASON

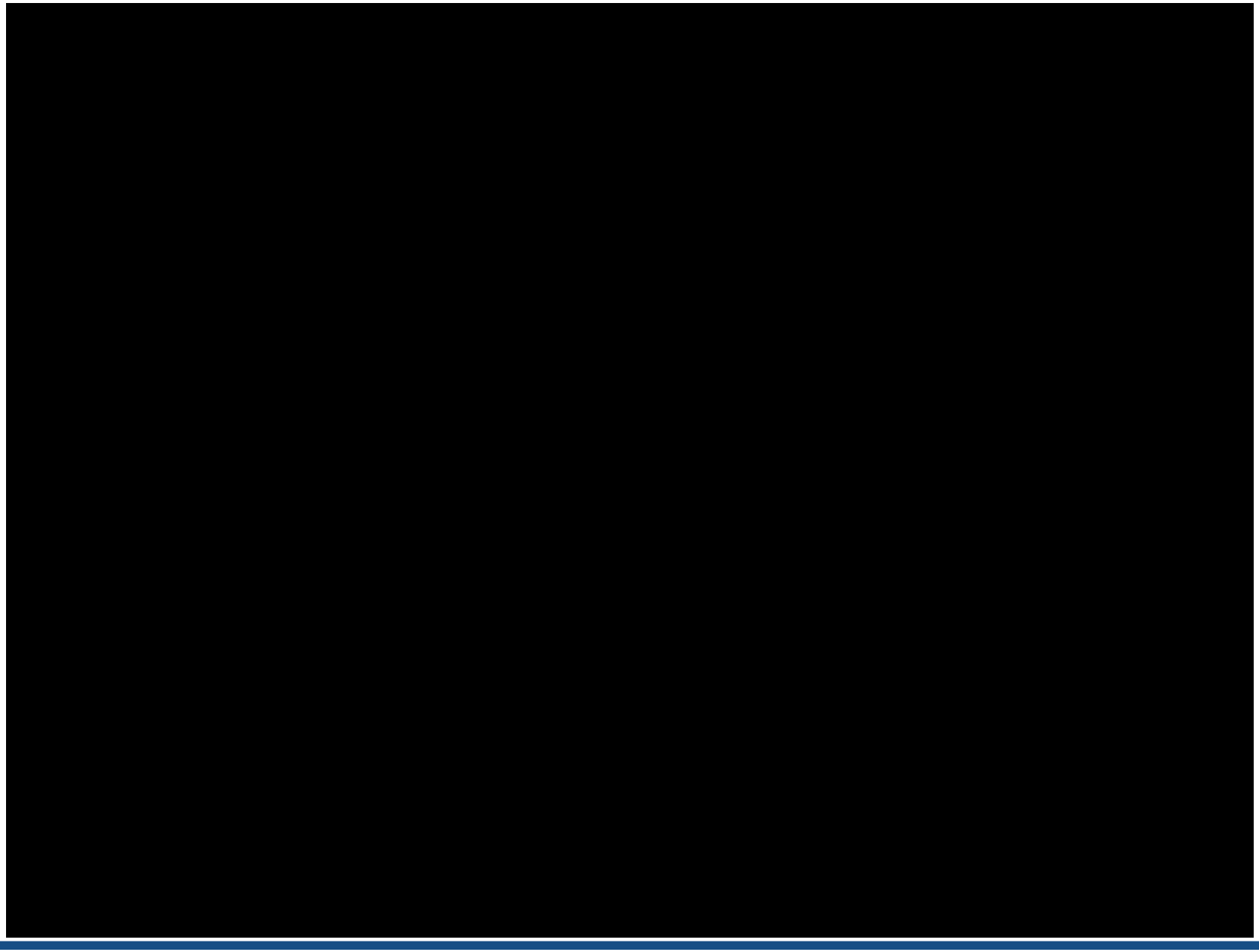
Reagire “velocemente”

Le origini

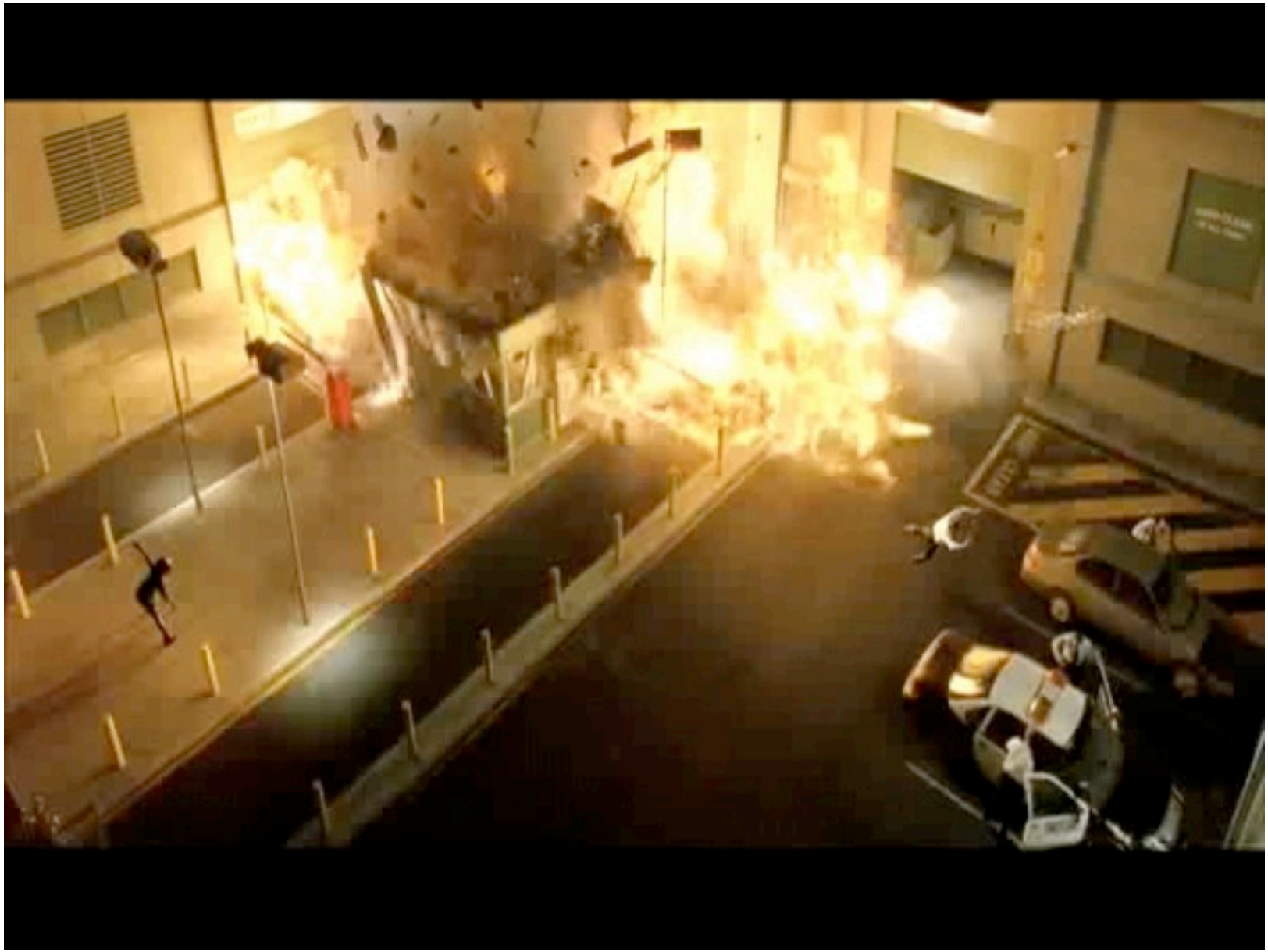


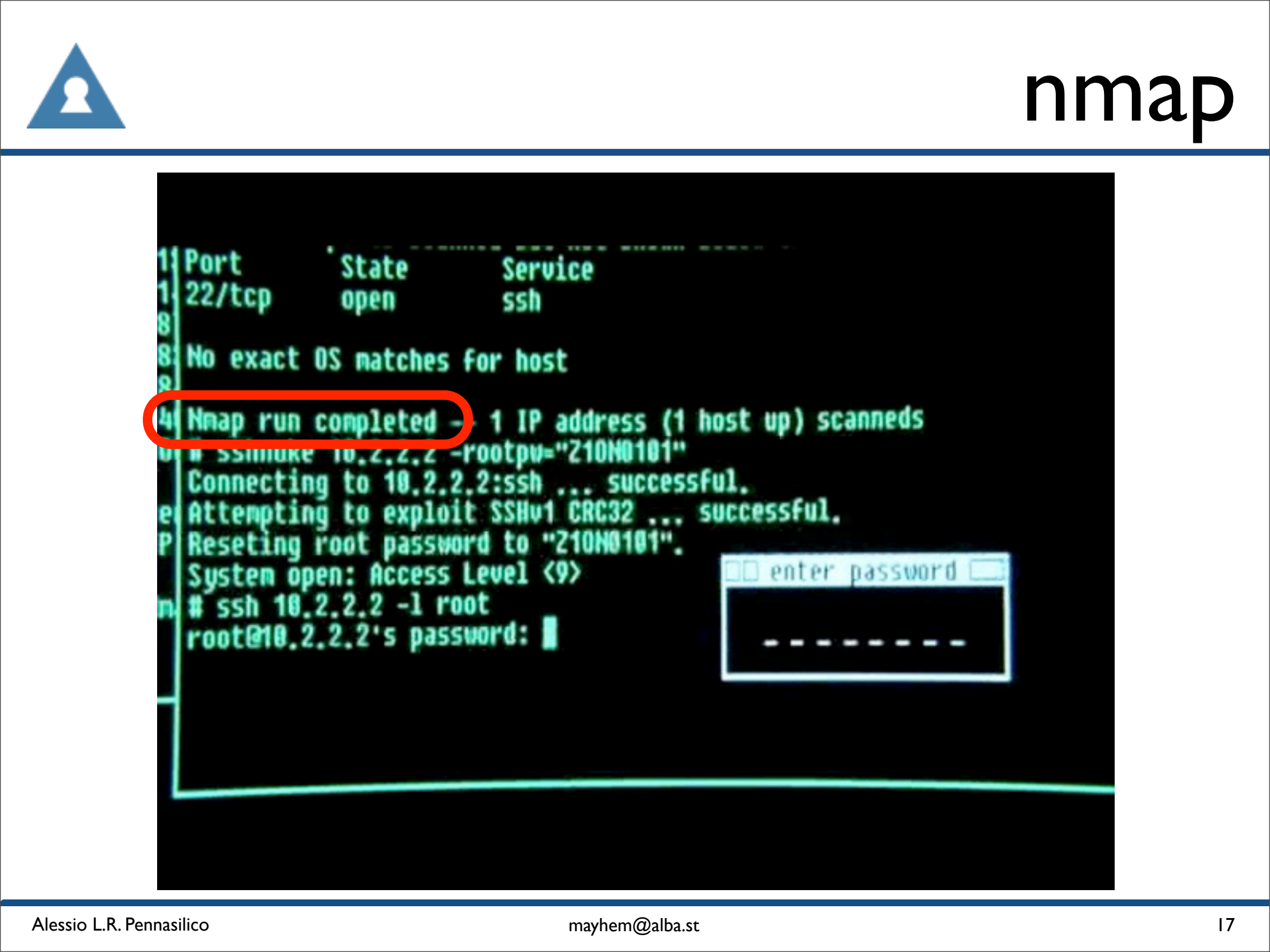
THEIR CRIME IS CURIOSITY
HACKERS
BOOT UP OR SHUT UP!
ON LINE - THIS FALL

Matrix Reloaded



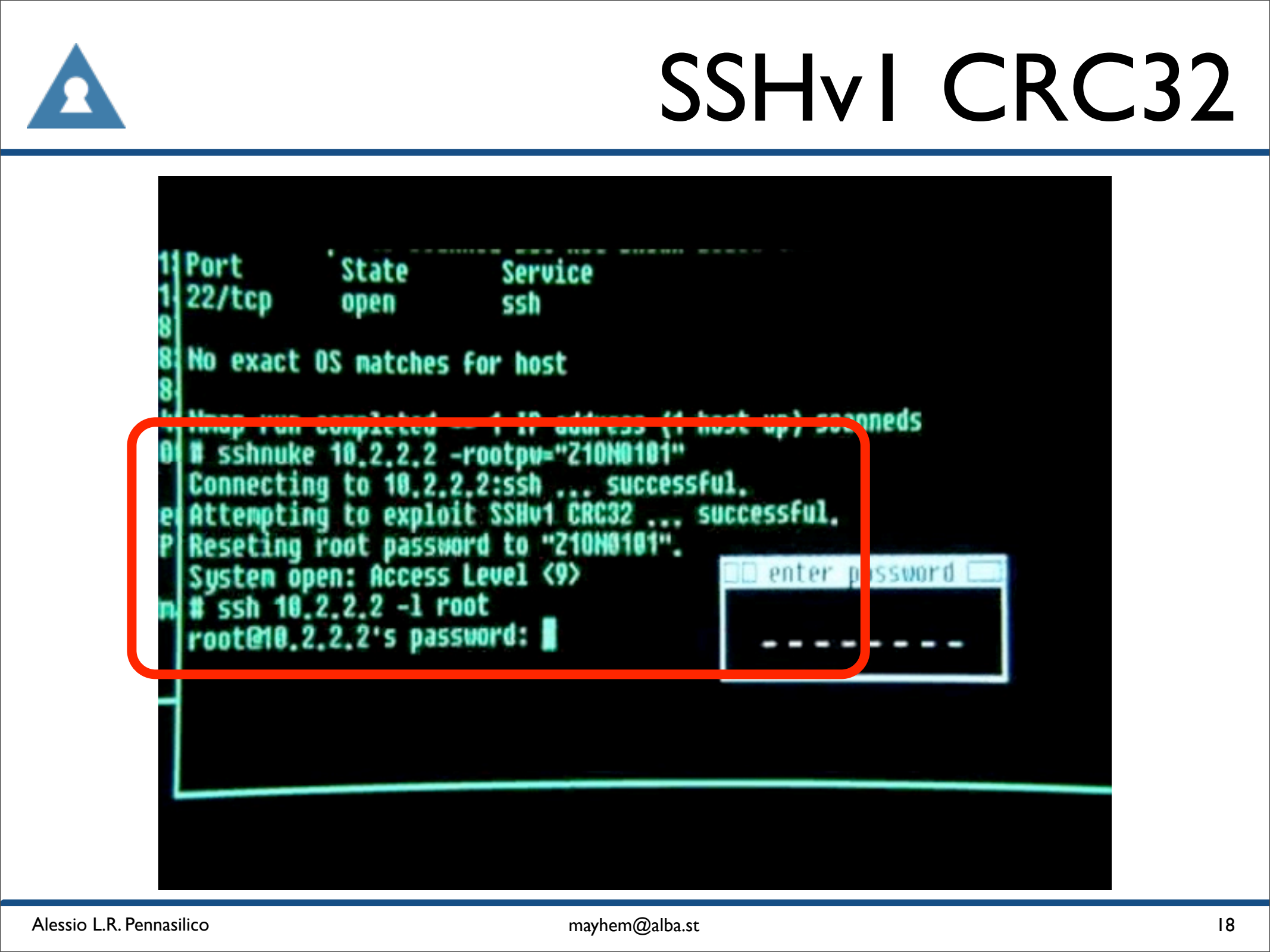
Phisical Security





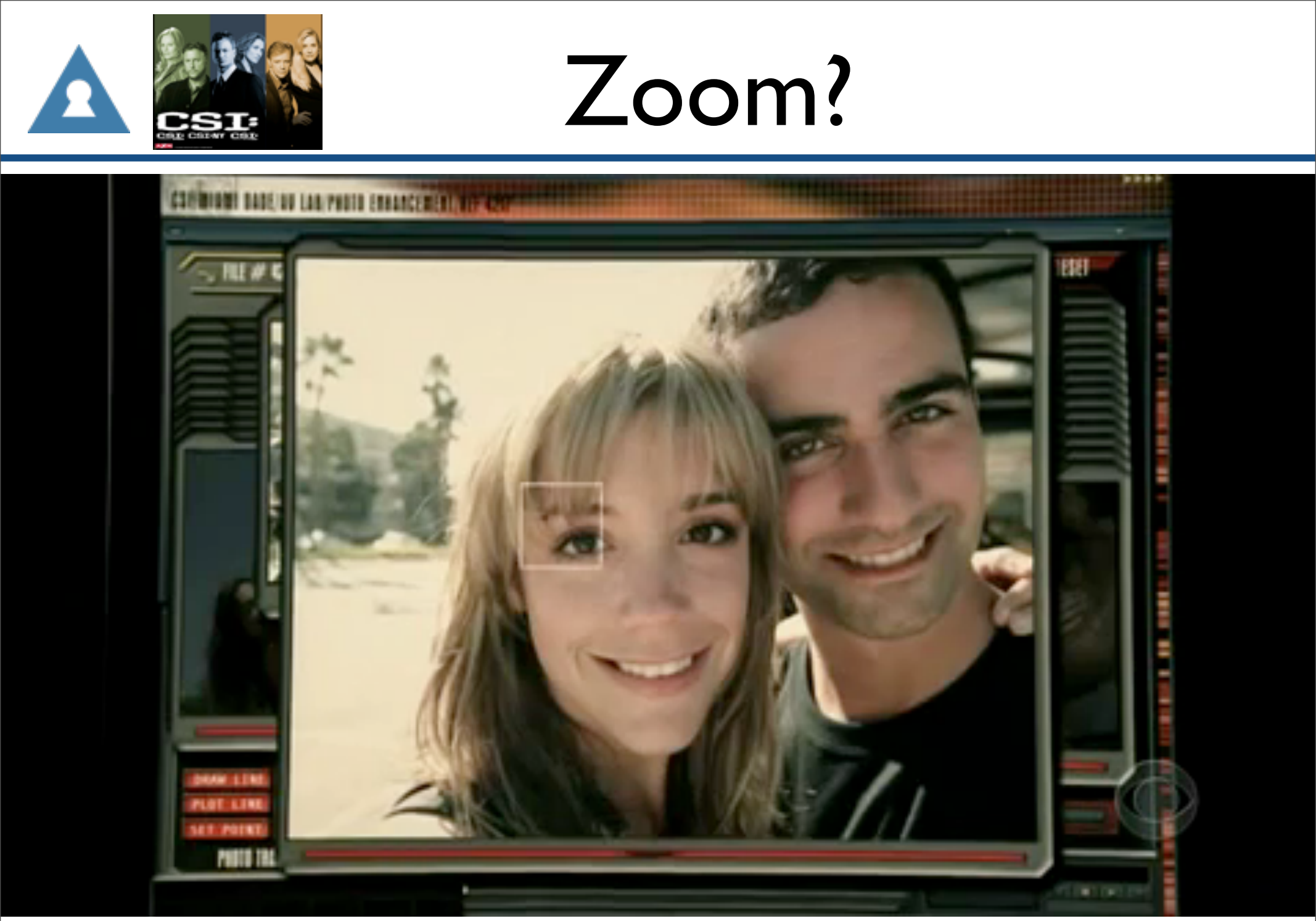
nmap

Port State Service
22/tcp open ssh
No exact OS matches for host
Nmap run completed - 1 IP address (1 host up) scanneds
Connecting to 10.2.2.2:ssh ... successful.
Attempting to exploit SSHv1 CRC32 ... successful.
Reseting root password to "21ON0101".
System open: Access Level <9>
ssh 10.2.2.2 -l root
root@10.2.2.2's password:
enter password



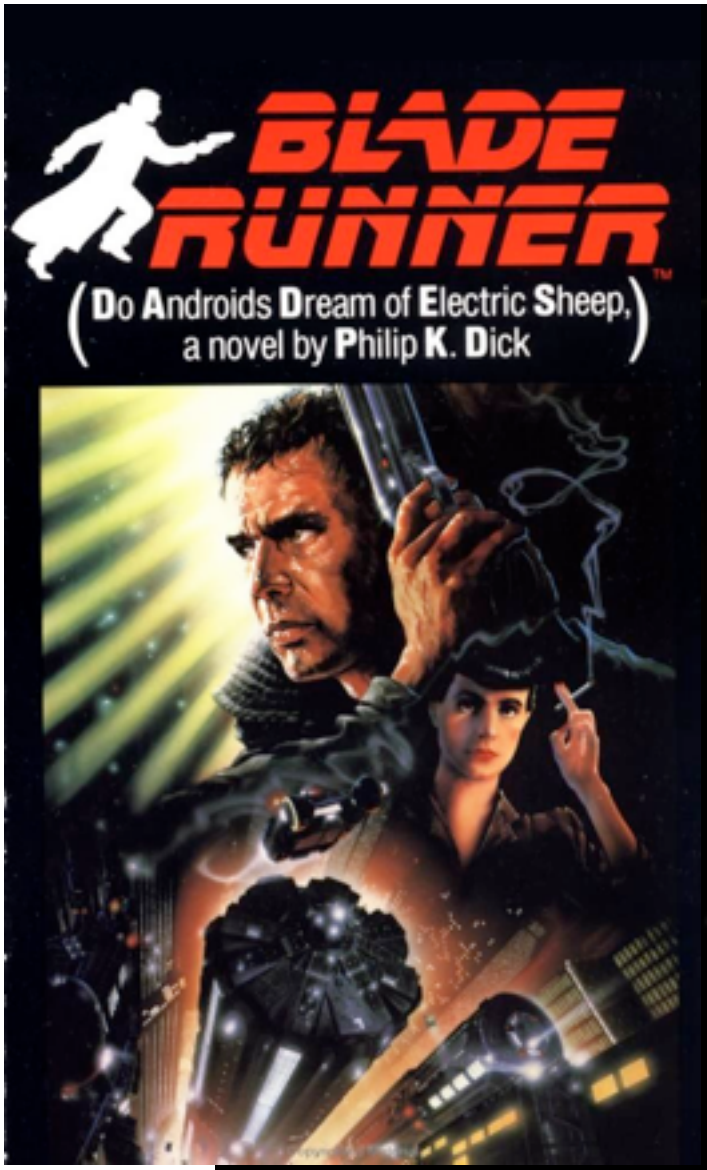
SSHv1 CRC32

Port State Service
22/tcp open ssh
No exact OS matches for host
sshnuke 10.2.2.2 -rootpw="Z10N0101"
Connecting to 10.2.2.2:ssh ... successful.
Attempting to exploit SSHv1 CRC32 ... successful.
Reseting root password to "Z10N0101".
System open: Access Level <9>
ssh 10.2.2.2 -l root
root@10.2.2.2's password:
enter password


Zoom?
CSI:
DRAW LINE
PLOT LINE
SET POINT
PHOTO TOOL

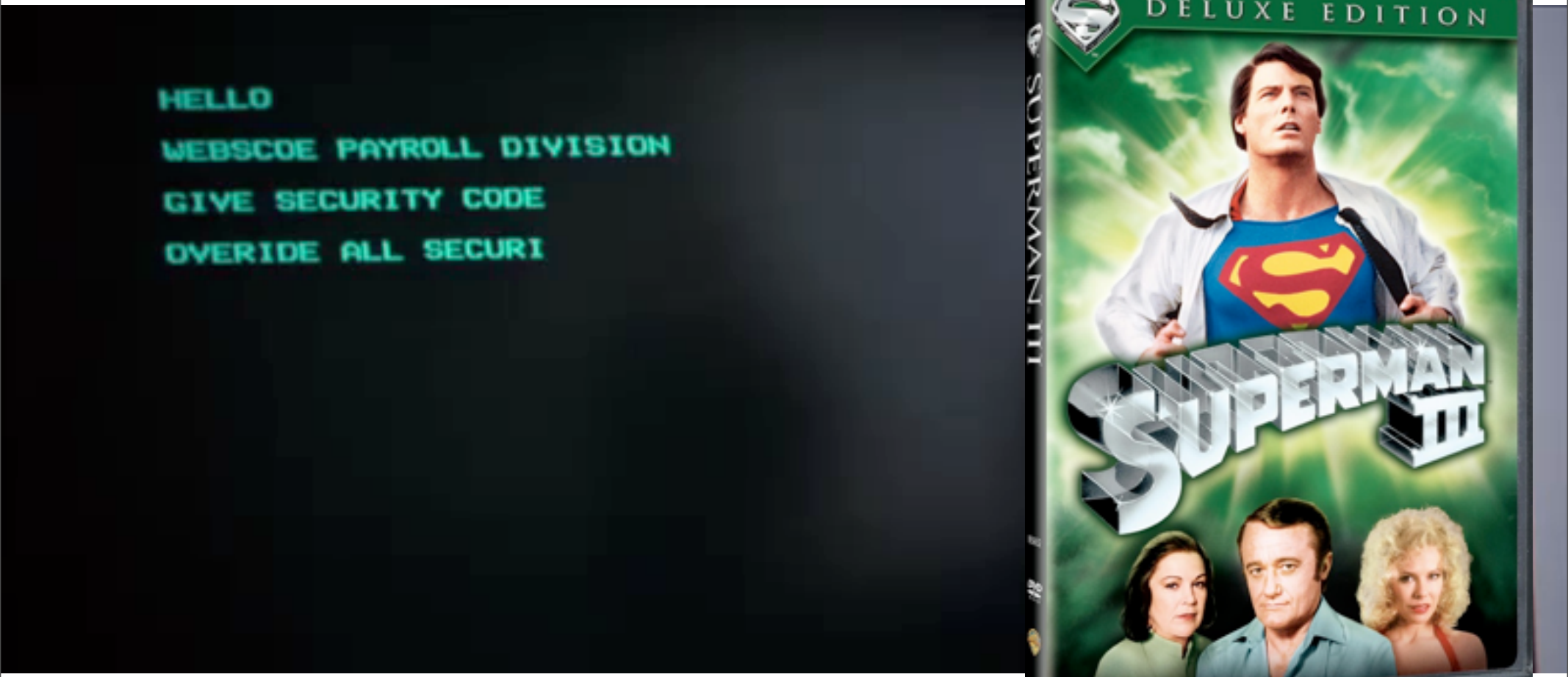
Zoomare con iPhone...

Le origini

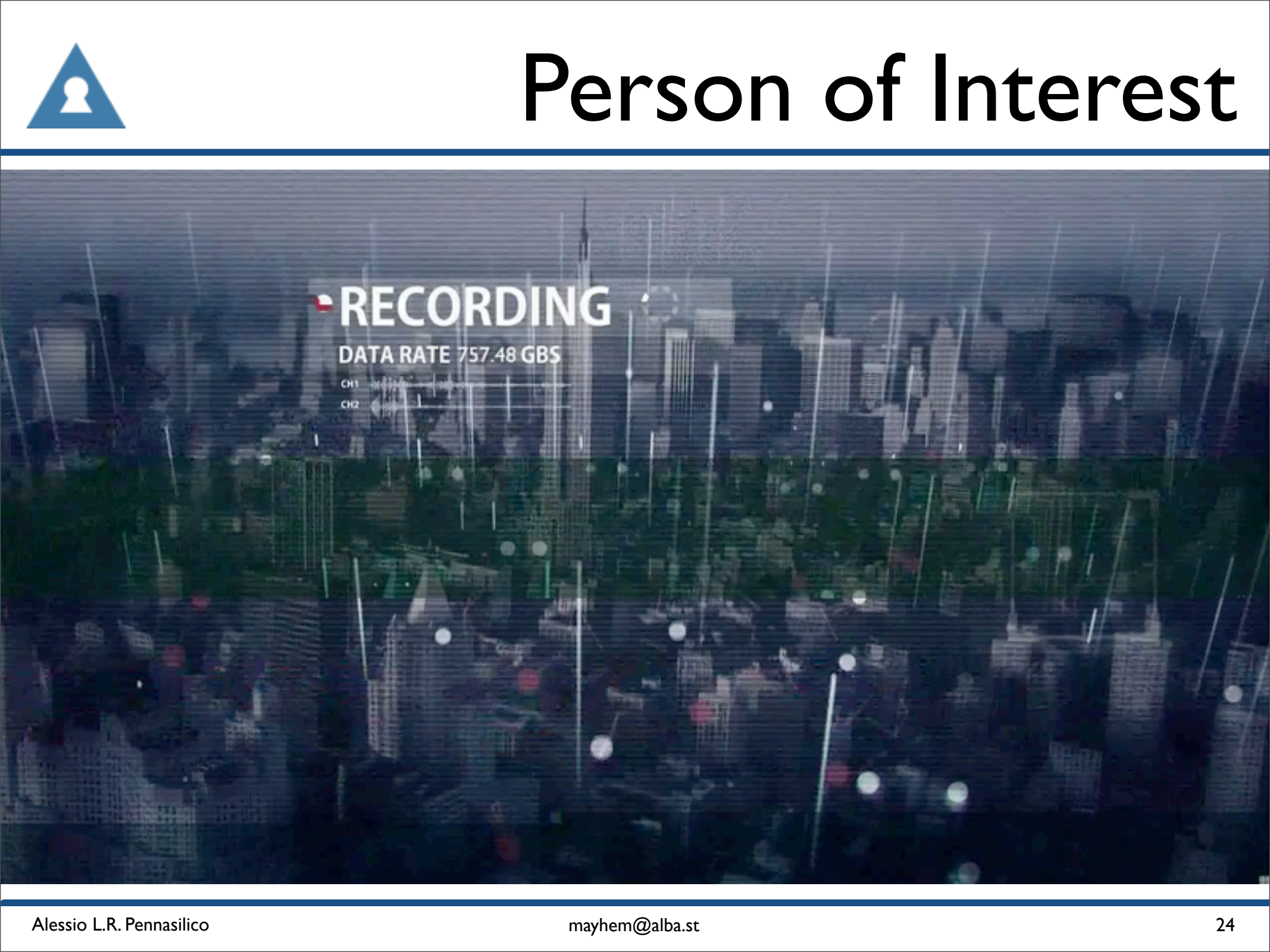

BLADE RUNNER
(Do Androids Dream of Electric Sheep,
a novel by Philip K. Dick)

Rubare con NFC

Frodi


HELLO
WEBSCOE PAYROLL DIVISION
GIVE SECURITY CODE
OVERIDE ALL SECURI

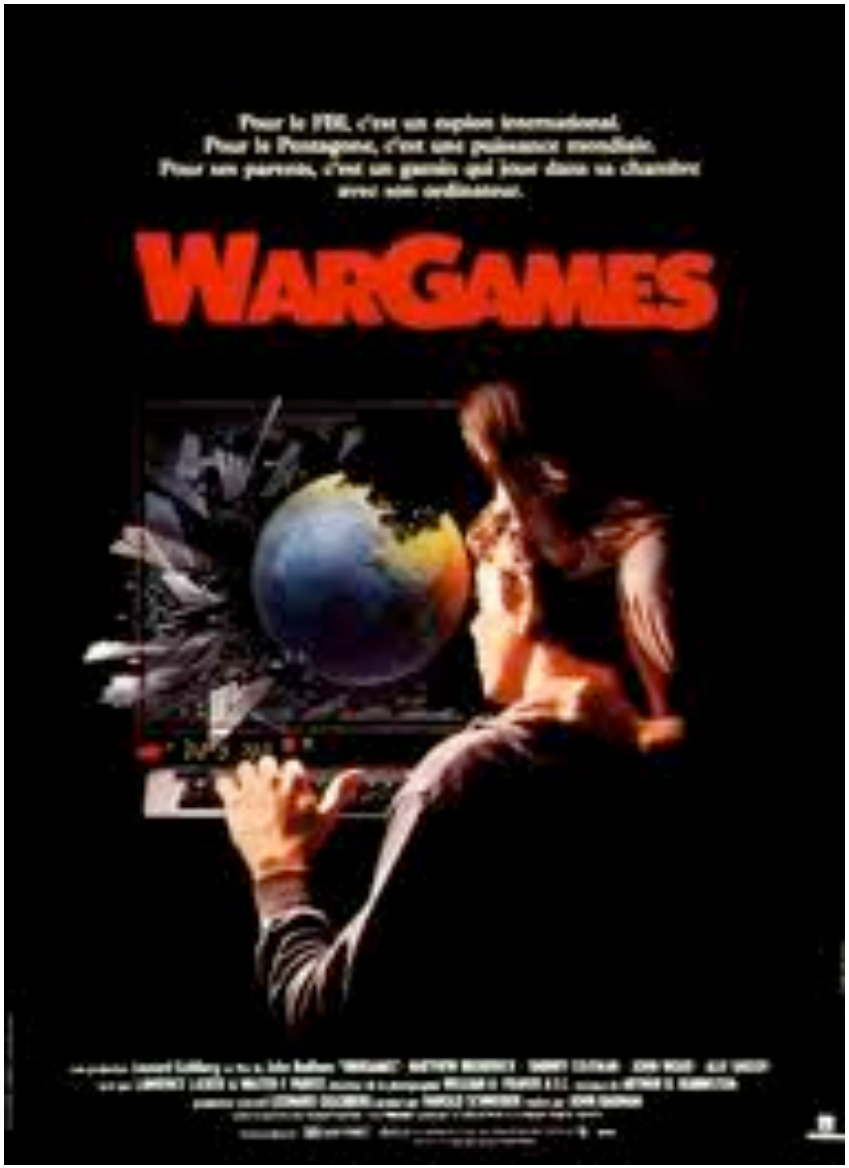
DELUXE EDITION
SUPERMAN III
SUPERMAN III



Person of Interest

I social network

Il più realistico?

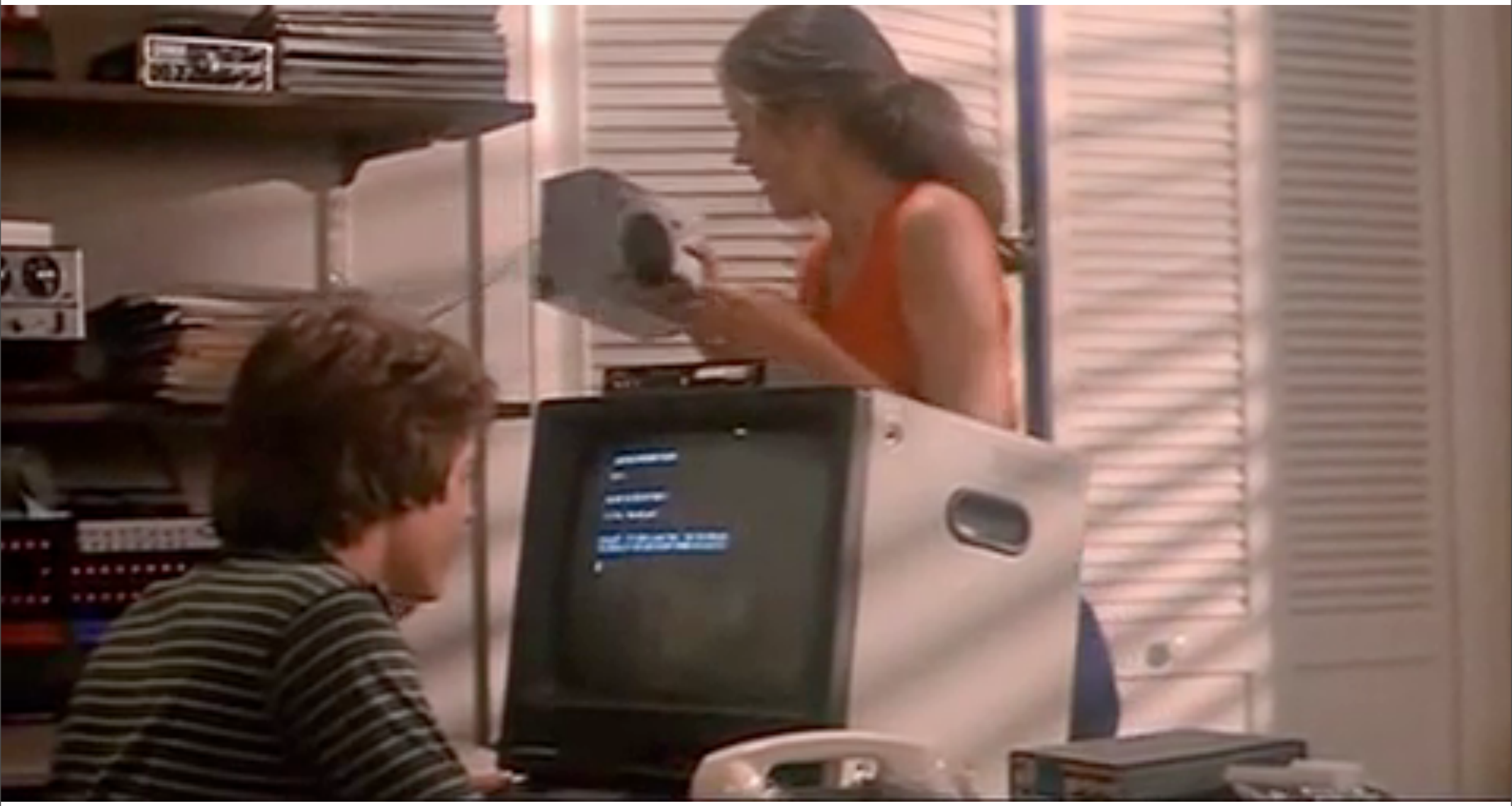


Wardialing

TO SCAN FOR CARRIER TONES, PLEASE LIST
DESIRED AREA CODES AND PREFIXES

A E PRFX NUMBER	AREA CODE PRFX NUMBER	AREA CODE PRFX NUMBER	AREA CODE PRF
1) 399	(311) 437	(311) 767	

Gli hacker sono sexy?

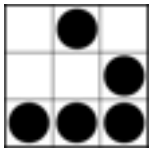


Wardialing

Mai parlare della backdoor!

Economia “digitale”

La realtà?



Economia “reale”

AP The Associated Press @AP

Following

Breaking: Two Explosions in the White House and Barack Obama is injured

Reply Retweet Favorite More

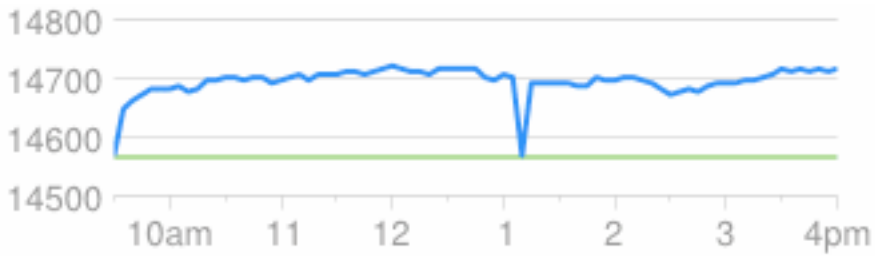
3,146 RETWEETS 149 FAVORITES

1:07 PM - 23 Apr 13

Dow Jones Industrial Average 2 Minute

Dow Jones Indices: .DJI - Apr 23 4:37pm ET

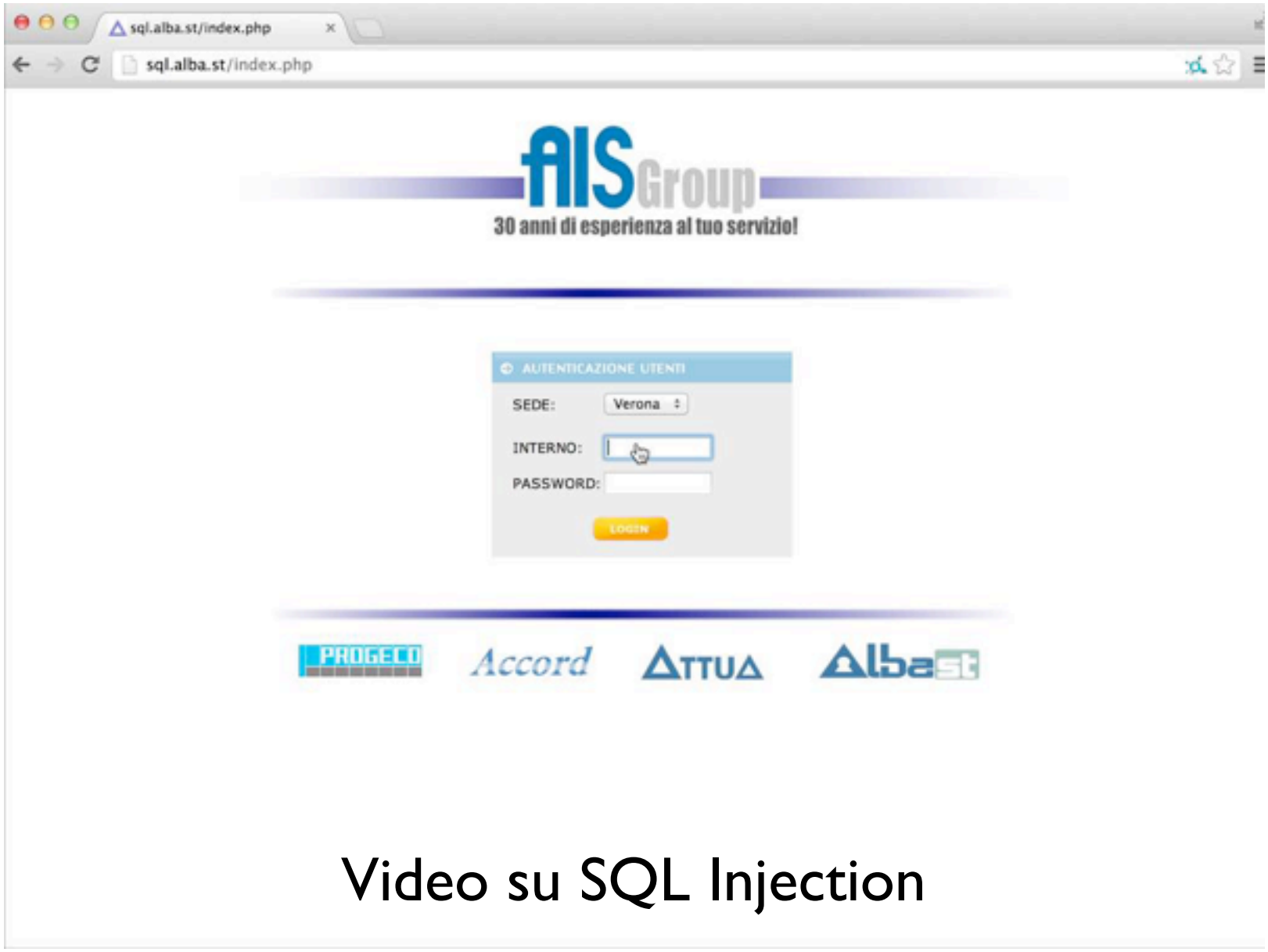
14719.46 +152.29 (1.05%)



Open	14567.17
High	14721.42
Low	14554.29
Volume	137,301,977
Avg Vol	N/A
Mkt Cap	N/A

1d 5d 1m 6m 1y 5y max

SQL Injection



Video su SQL Injection

Altri rischi?

Posso interrogare il DB e ottenere tutti i dati contenuti:

```
' UNION ALL SELECT NULL,username,password,NULL FROM
utenti WHERE 'x'='x
```

Password in cleartext

Sql Injection

sql.alba.st/ricerca.php

AIS Group

30 anni di esperienza al tuo servizio!

<< Pagina principale

Ricerca di un numero di telefono

Inserire il nome:

Ricerca

Chiamata di un numero di telefono

Inserire il numero/contatto skype:

Chiama

I numeri preceduti da un asterisco (*) appartengono alla rubrica personale.

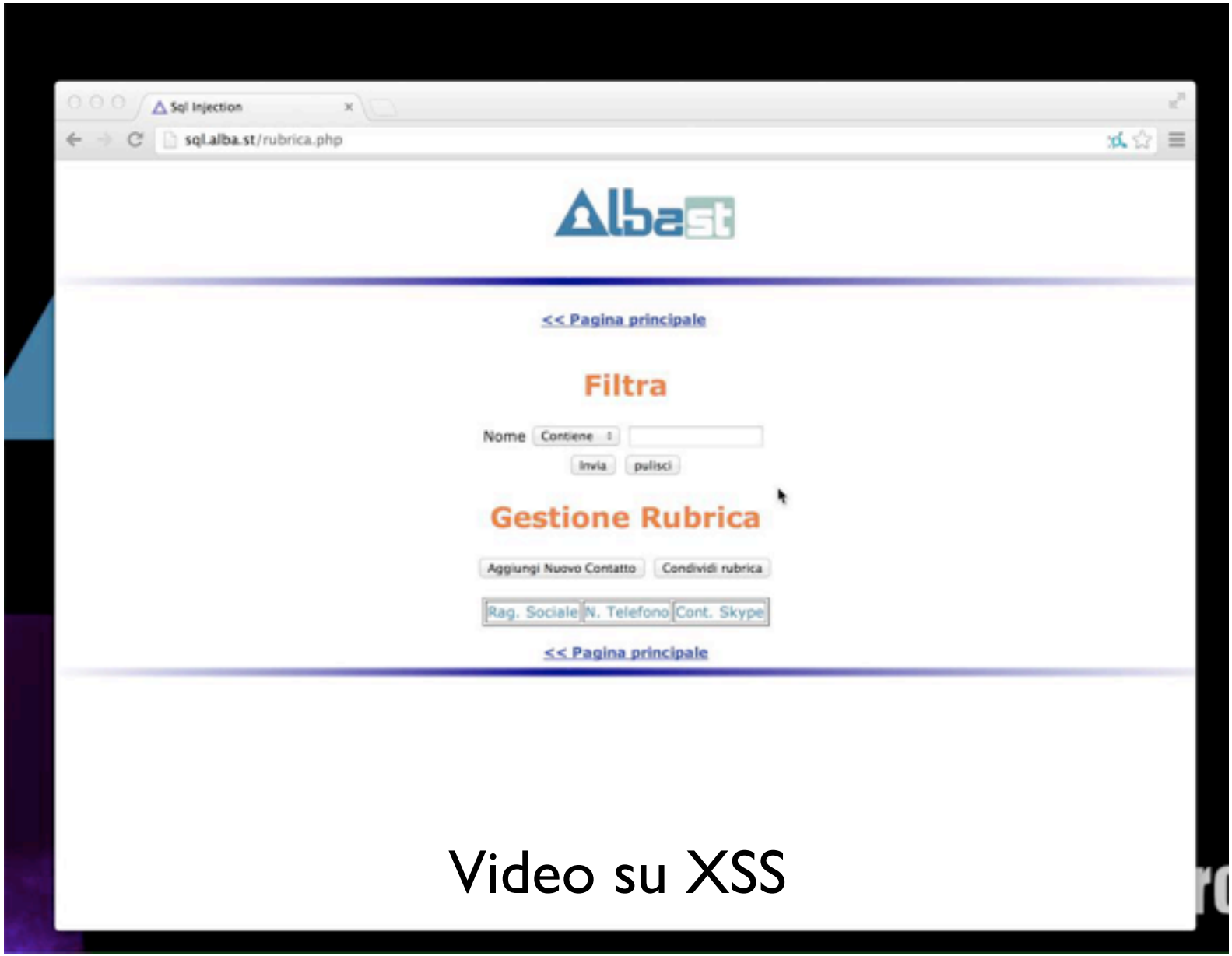
* Mario Rossi	045112233	Ch. Da
* Giuseppe Verdi	098123	Ch. Da
* Paolo Bianchi	01111234	Ch. Da
cyrax	superstrongpassword	Ch. Da
johndoe	cleartextpasswordaresafe	Ch. Da
admin	guest	Ch. Da

Come mi proteggo?

Evito di processare i caratteri speciali come ‘

Prevedo il processo che si chiama “normalizzare l’input”

Cross site scripting



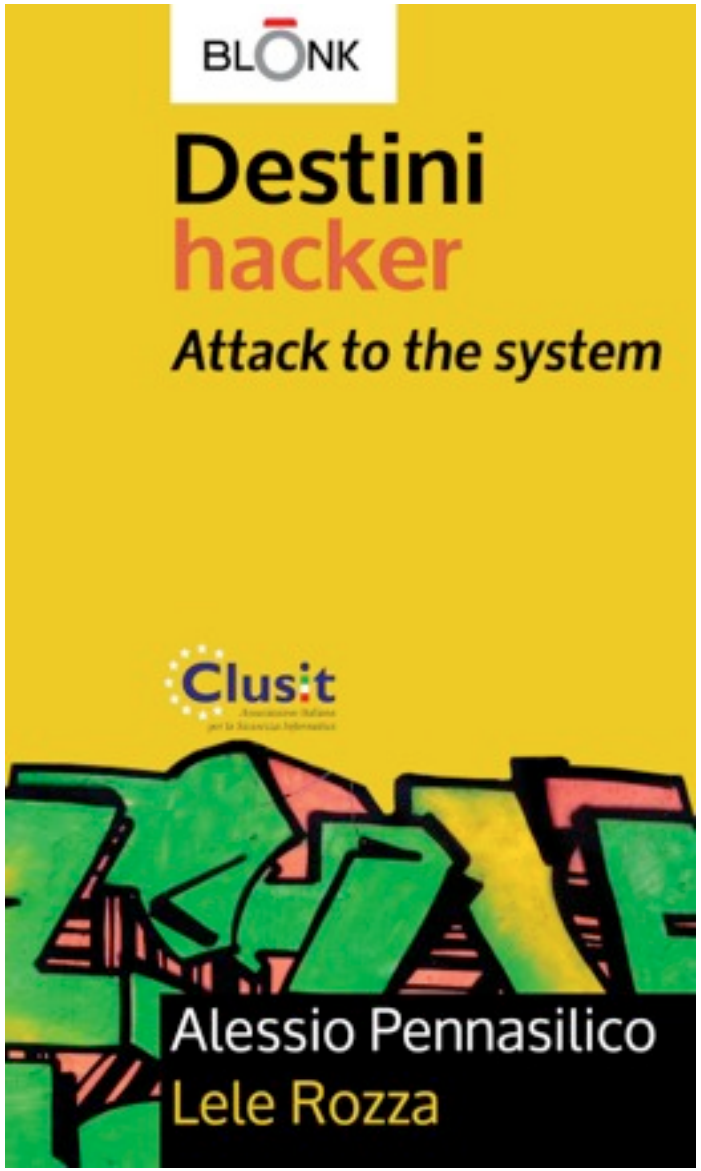
Video su XSS

Le informazioni

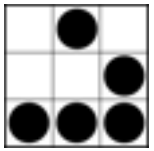
Lieto fine?

Awarness


BLONK
Destini
hacker
Attacco al sistema
Clusit
Alessio Pennasilico
Lele Rozza


BLONK
Destini
hacker
Attack to the system
Clusit
Alessio Pennasilico
Lele Rozza

Conclusioni



Tecnologia aliena?

Cosa dobbiamo affrontare?

Rischi

reali, concreti

semplici da trasformare in incidenti

alta probabilità di conversione in incident

grande impatto sul business

Cosa fare?

Rischi

facili da prevenire

difficili da mitigare a posteriori

Security by Design

Se costruisco una casa

senza progettare

uscite di sicurezza

costruirle a lavori finiti

sarà disastroso

Grazie dell’attenzione!

Domande?

http://www.alba.st/
Verona, Milano, Roma
Phone/Fax +39 045 8271202

Alessio L.R. Pennasilico
a.pennasilico@alba.st