



De niño a perito informático

JORGE CORONADO
XAngelucho



DISCLAIMER

Este relato es completamente ficticio y ha sido creado con el único propósito de sensibilizar y concienciar acerca de situaciones imaginarias.



¿Qué es un niñoato?



Tú

¿Qué es un niñoato?



ChatGPT

"Niñoato" es una palabra de uso coloquial en español, generalmente de carácter despectivo. Se utiliza para referirse a una persona joven, especialmente un adolescente o un adulto joven, que se comporta de manera inmadura, irresponsable, caprichosa o arrogante. La palabra puede llevar connotaciones de ser malcriado o de tener un sentido exagerado de autoimportancia. Como con cualquier término coloquial o jerga, el uso y la percepción de "niñoato" pueden variar según el contexto cultural y regional.



¿Qué es un perito informático?



La historia comienza...

“El Niño Güei es un producto made in Sevilla
Pequeño héroe de barrio de pacotilla
La diferencia entre él y ustedes
Es que él nunca te va a pedir los tres euros que le debes”. **SFDK**



La informática su pasión

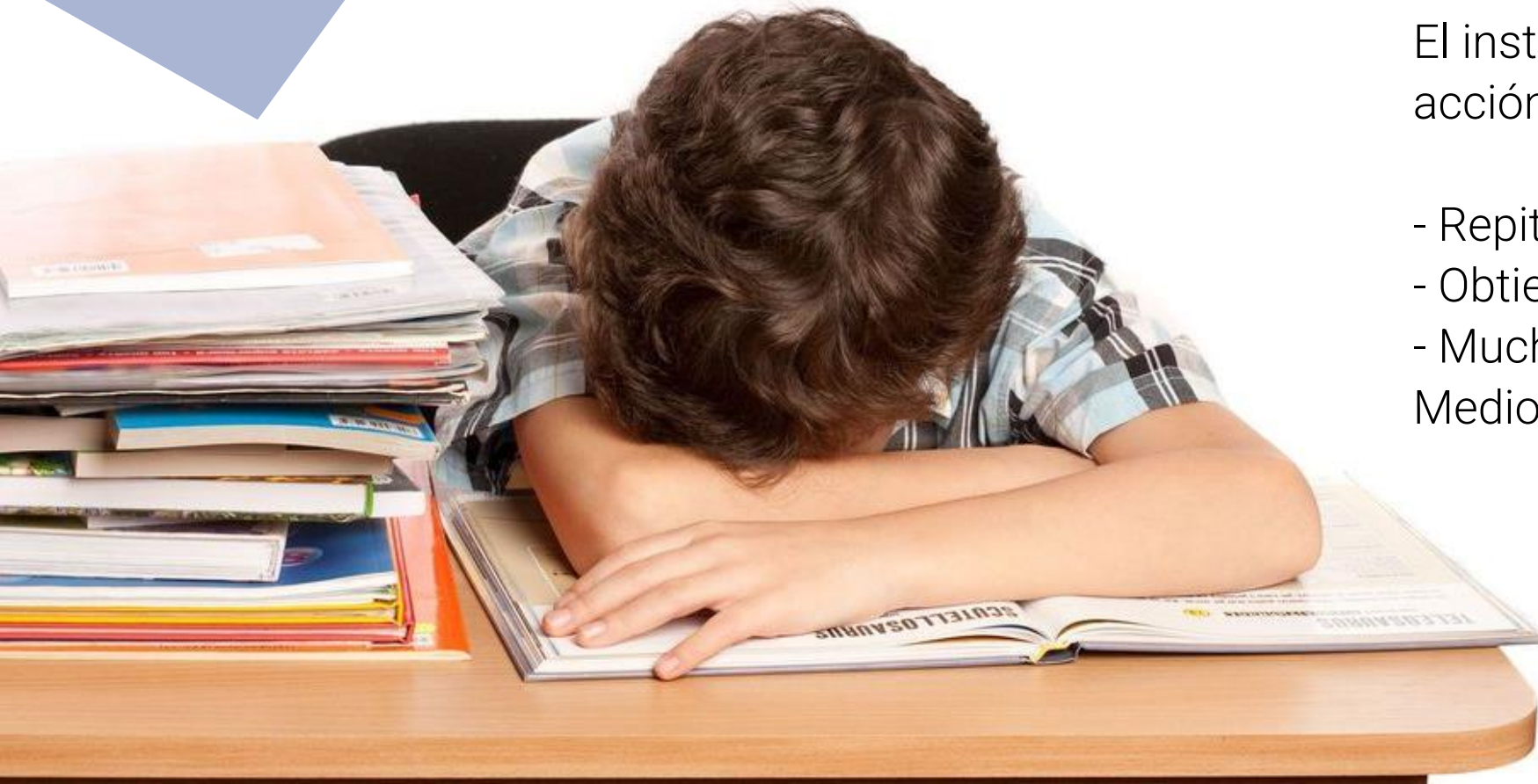
Desde pequeño.



II Fracasado escolar

El instituto no era su sitio y quería acción.

- Repite cuarto de la ESO
- Obtiene la ESA
- Muchos amigos ya en Grado Medio de Informática



Programación

- BACH y BAT (si se puede...)
- C
- C#
- PHP
- Visual Basic 6.0 (saludos EnEIPC)
- VB .NET
- Python
- Ahora, chatGPT



```
ensure no other block  
  
def row_available(block, row):  
    # Determine which of the main  
20 boardRow = int(block / 3);  
21 good = True  
22 for b in range(boardRow * 3, (block + 3) * 3):  
23     if b != block:  
24         if num in board[b][row]:  
25             good = False  
26             break  
    return good
```





QUANTIKA¹⁴
INTELLIGENCE FOR CRIMINAL INVESTIGATIONS

Ciclo medio y trabajo

- Contrato reparando ordenadores
y programando webs

Hacking y defacing

- Master hacker
- Indetectables
- Undercode
- Hackxcrack



Los famosos cuadernos

Fue fundada en 2002 con el nombre de *Los Cuadernos de Hack x Crack* y rebautizada meses más tarde, con el objetivo de obtener un enfoque más comercial, con el nombre *PC Paso a Paso*.² La mayor parte de los contenidos consistía en tutoriales prácticos sobre [hacking](#), pudiendo practicar contra unos servidores que la misma revista proporcionaba. La revista poseía unos [foros](#) oficiales³ donde, gracias a la participación de los lectores, se creó una comunidad y unos contenidos que rivalizaban a la propia publicación. Además, aparecieron canales de comunicación no oficiales, como canales de [IRC](#) en la red *Freenode* frecuentados por lectores de la revista.

Wikipedia

https://es.wikipedia.org/wiki/Los_Cuadernos_de_Hack_x_Crack



Webshells

- ISQL
- UPLOADS
- LFI

!C99madShell v. 2.1 madnet edition ADVANCED!

Software: Apache/2.2.3 (CentOS). PHP/5.1.6
uname -a: Linux localhost.localdomain 2.6.18-194.el5 #1 SMP Fri Apr 2 14:58:35 EDT 2010 i686
uid=48(apache) gid=48(apache) groups=48(apache) context=user_u:system_r:htpd_t:s0
Safe-mode: Off
/var/www/html/ drwxr-xr-x
Free 836.96 MB of 3.78 GB (21.64%)

HOME <=> UPDIR Search Buffer Tools Proc. FTP brute Sec. SQL PHP-code Self remove Logout

Listing folder (4 files and 3 folders):

Name	Size	Modify	Owner/Group	Perms	Action
..	LINK	31.01.2011 14:54:34	0/0	drwxr-xr-x	1 <input type="checkbox"/>
.	LINK	29.04.2011 07:09:02	500/0	drwxr-xr-x	1 <input type="checkbox"/>
[drupal-5.23]	DIR	11.08.2010 13:46:30	500/500	drwxr-xr-x	1 <input type="checkbox"/>
[drupal-6.20]	DIR	22.04.2011 03:57:15	500/500	drwxr-xr-x	1 <input type="checkbox"/>
[osticket_1.6.0]	DIR	28.04.2011 10:54:47	500/500	drwxr-xr-x	1 <input type="checkbox"/>
c99.php	137.94 KB	29.04.2011 07:29:39	500/500	-rw-rw-r--	1 E D <input type="checkbox"/>
drupal-5.23.tar.gz	750.26 KB	11.08.2010 13:46:31	500/500	-rw-rw-r--	1 E D <input type="checkbox"/>
drupal-6.20.tar.gz	1.05 MB	15.12.2010 13:16:29	500/500	-rw-rw-r--	1 E D <input type="checkbox"/>
osticket_1.6.0.tar.gz	385.1 KB	07.10.2010 21:22:39	500/500	-rw-rw-r--	1 E D <input type="checkbox"/>

Select all Unselect all With selected: [v] Confirm

:: Command execute ::

Enter: Execute

Select: [v] Execute

:: Search :: - regexp Search

:: Upload :: Browse... Upload
(Read-Only)

:: Make Dir :: Create
(Read-Only)

:: Make File :: Create
(Read-Only)

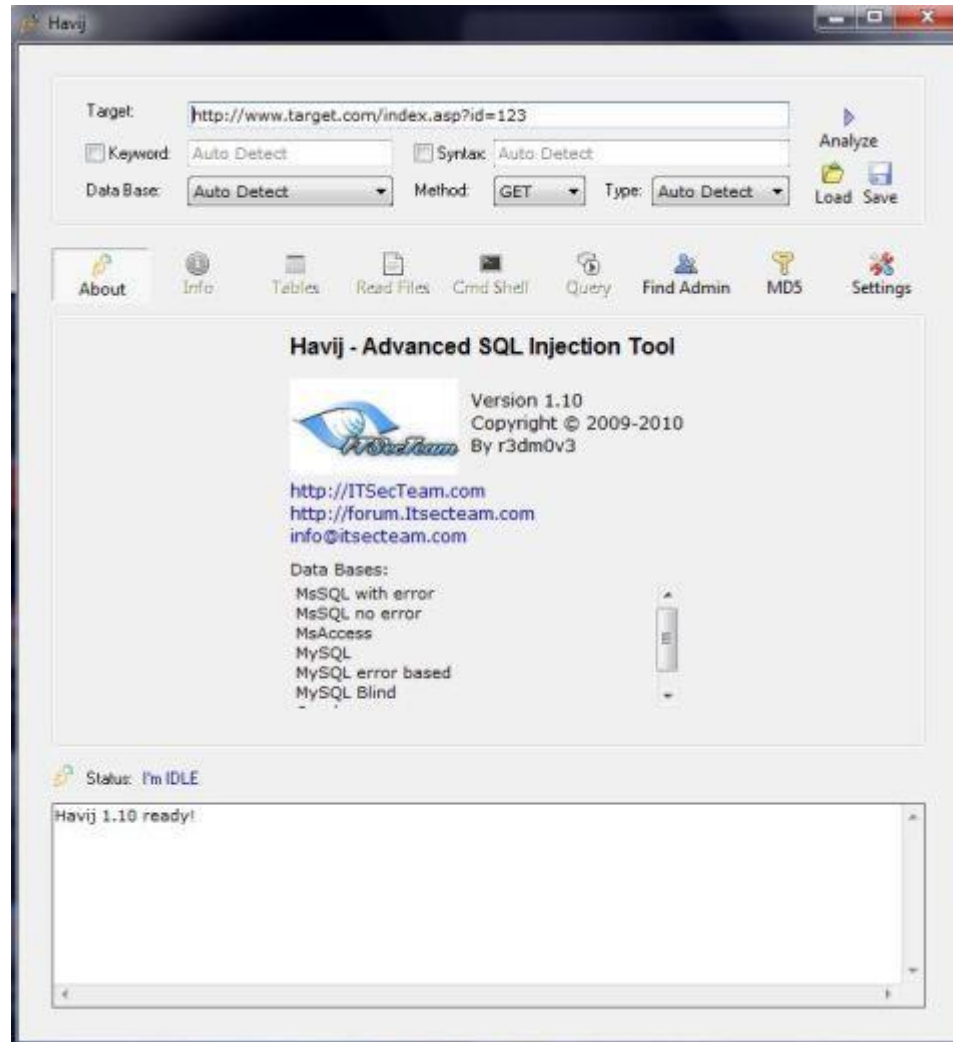
:: Go Dir :: Go

:: Go File :: Go

--[c99madshell v. 2.1 madnet edition ADVANCED EDITED BY MADNET | <http://www.c99madshell.net> | Generation time: 0.0063]--

ISQL

- A mano
- Sqlmap
- HAVIJ



```
SELECT * FROM usuarios WHERE nombre_usuario = 'entrada_usuario';
```

```
' AND (SELECT COUNT(*) FROM usuarios WHERE substring(nombre_usuario, 1, 1) = 'a') > 0 AND '1'='1
```

**¡ANTIGUAMENTE
HACIAMOS LOS
BLIND ISQL A
MANO!**



EI IRC



En 2008...

Por ka0x y Piker
D.O.M TEAM 2008

somos: ka0x, an0de, xarnuz, Piker



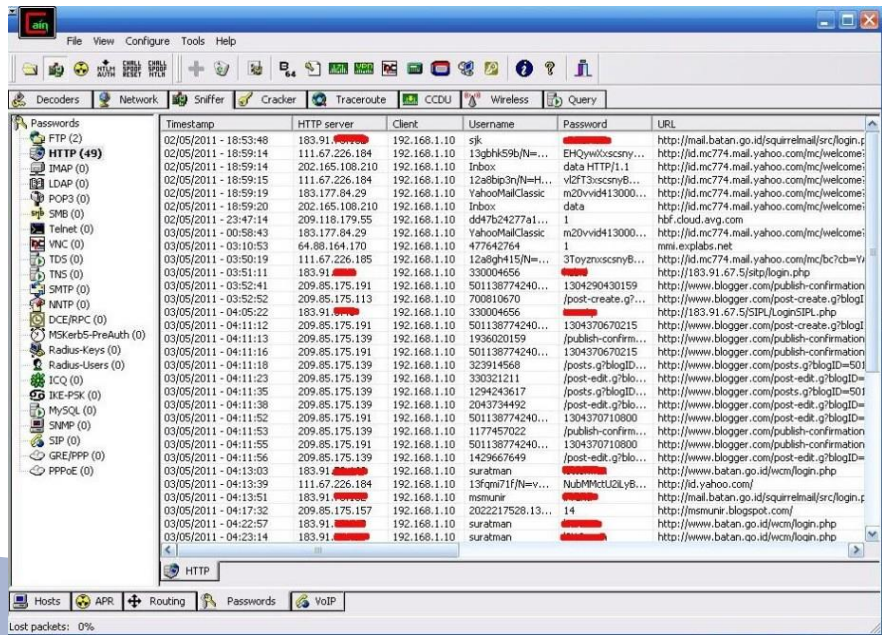
algo en común, le dijo un presidente a un emb

```
poseidon:~ # uname -a;id;whoami;date
2.6.18.2-34-default #1 SMP Mon Nov 27 11
x86_64 x86_64 x86_64 GNU/Linux
uid=0(root) gid=0(root) groups=0(root)
root
Sat Mar 1 21:06:17 CET 2008
poseidon:~ #
```



Los cybercafes, keyloggers y rats

El laboratorio perfecto.



Timestamp	HTTP server	Client	Username	Password	URL
02/05/2011 - 18:53:48	183.91.175.139	192.168.1.10	sjk		http://mail.batan.go.id/squirrelmail/src/login.f...
02/05/2011 - 18:59:14	111.67.226.184	192.168.1.10	13ghhh59b(N=...	EHQywwoscsny...	http://ld.mc774.mail.yahoo.com/mc/welcome!
02/05/2011 - 18:59:14	202.165.108.210	192.168.1.10	Inbox	data HTTP/1.1	http://ld.mc774.mail.yahoo.com/mc/welcome!
02/05/2011 - 18:59:15	111.67.226.184	192.168.1.10	12a88b3n(N=H...	v1Z73iscsnyB...	http://ld.mc774.mail.yahoo.com/mc/welcome!
02/05/2011 - 18:59:19	183.177.84.29	192.168.1.10	YahooMailClassi...	m20vvi4H13000...	http://ld.mc774.mail.yahoo.com/mc/welcome!
02/05/2011 - 18:59:20	202.165.108.210	192.168.1.10	Inbox	data	http://ld.mc774.mail.yahoo.com/mc/welcome!
02/05/2011 - 23:47:14	209.118.179.55	192.168.1.10	dd47b24277a1...	1	hbf.cloud.avg.com
03/05/2011 - 00:58:43	183.177.84.29	192.168.1.10	YahooMailClassi...	m20vvi4H13000...	http://ld.mc774.mail.yahoo.com/mc/welcome!
03/05/2011 - 03:10:53	64.88.164.170	192.168.1.10	477642764	1	nini.explabs.net
03/05/2011 - 03:50:19	111.67.226.185	192.168.1.10	12a88b3n(N=H...	3TeyzrvscsnyB...	http://ld.mc774.mail.yahoo.com/mc/bc?cb=V...
03/05/2011 - 03:51:11	183.91.175.139	192.168.1.10	330004656		http://183.91.67.5/step/login.php
03/05/2011 - 03:52:41	209.85.175.191	192.168.1.10	501138774240...	1304290430159	http://www.blogger.com/publish-confirmation
03/05/2011 - 03:52:52	209.85.175.113	192.168.1.10	700810670	/post-create.g?...	http://www.blogger.com/post-create.g?blogID=...
03/05/2011 - 04:05:22	183.91.175.139	192.168.1.10	330004656		http://183.91.67.5/SIPL/LoginSIPL.php
03/05/2011 - 04:11:42	209.85.175.191	192.168.1.10	501138774240...	1304370670215	http://www.blogger.com/post-create.g?blogID=...
03/05/2011 - 04:11:43	209.85.175.139	192.168.1.10	1936020159	/publish-confir...	http://www.blogger.com/publish-confirmation
03/05/2011 - 04:11:16	209.85.175.191	192.168.1.10	501138774240...	1304370670215	http://www.blogger.com/publish-confirmation
03/05/2011 - 04:11:18	209.85.175.139	192.168.1.10	323914568	/posts.g?blogID=...	http://www.blogger.com/posts.g?blogID=501...
03/05/2011 - 04:11:23	209.85.175.139	192.168.1.10	330321211	/post-edit.g?blo...	http://www.blogger.com/post-edit.g?blogID=...
03/05/2011 - 04:11:35	209.85.175.139	192.168.1.10	1294243617	/posts.g?blogID=...	http://www.blogger.com/posts.g?blogID=501...
03/05/2011 - 04:11:38	209.85.175.139	192.168.1.10	2043734492	/post-edit.g?blo...	http://www.blogger.com/post-edit.g?blogID=...
03/05/2011 - 04:11:52	209.85.175.191	192.168.1.10	501138774240...	1304370710800	http://www.blogger.com/post-edit.g?blogID=...
03/05/2011 - 04:11:53	209.85.175.139	192.168.1.10	1177457022	/publish-confir...	http://www.blogger.com/publish-confirmation
03/05/2011 - 04:11:55	209.85.175.191	192.168.1.10	501138774240...	1304370710800	http://www.blogger.com/publish-confirmation
03/05/2011 - 04:11:56	209.85.175.139	192.168.1.10	1429667649	/post-edit.g?blo...	http://www.blogger.com/post-edit.g?blogID=...
03/05/2011 - 04:13:03	183.91.175.139	192.168.1.10	suratman		http://www.batan.go.id/wcm/login.php
03/05/2011 - 04:13:39	111.67.226.184	192.168.1.10	13famt71f(N=ev...	NUMMfctU2LYb...	http://ld.yahoo.com/
03/05/2011 - 04:13:51	183.91.175.139	192.168.1.10	msmunir		http://mail.batan.go.id/squirrelmail/src/login.f...
03/05/2011 - 04:17:32	209.85.175.157	192.168.1.10	2022217528.13...	14	http://msmunir.blogspot.com/
03/05/2011 - 04:22:57	183.91.175.139	192.168.1.10	suratman		http://www.batan.go.id/wcm/login.php
03/05/2011 - 04:23:14	183.91.175.139	192.168.1.10	suratman		http://www.batan.go.id/wcm/login.php




Los congresos

“Voy a ir a todos”.

- Rootedcon
- Noconname
- Conectacon
- Etc



Evento Angelucho FSI SEGURIDAD

 <http://elblogdeangelucho.com/elblogdeangelucho/blog/2013/09/06/sevilla-jornadas-gratuitas-sobre-seguridad-en-internet-los-dias-27-y-28-de-septiembre/>

 <https://web.archive.org/web/20221206105008/http://elblogdeangelucho.com/elblogdeangelucho/blog/2013/09/06/sevilla-jornadas-gratuitas-sobre-seguridad-en-internet-los-dias-27-y-28-de-septiembre/>



JORNADAS
**SEGURIDAD INFORMATICA
DELITOS INFORMATICOS Y
PROTECCION DE DATOS**

SEVILLA
27 Y 28 DE SEPTIEMBRE

www.quantika14.com
www.fsiseguridad.com
info: 605 93 89 08

FSI
Formación de seguridad informática

Monté una empresa



Primeros peritajes informáticos

1. Metodologías
2. Plantilla de informes
3. Ratificación



Estudios

<https://quantika14.com/estudios-de-investigacion/>



ESCARGAR GRATIS

Leer más



COMPRAR Y AYUDAR

DESCARGA GRATIS

Leer más



Un caso real



La búsqueda de un supuesto violador en busca y captura.

El caso

Situación:

- El investigado tiene varias denuncias por agresión sexual
- El investigado no comparece y se procede a la búsqueda y captura
- Más de 3 meses y no lo encontraban

El perfil de agresor:

- Menor de 30 años
- Cuerpo de gimnasio
- Muy activo en las redes sociales

El modus operandi:

- Cambiaba de forma regular su hospedaje, pero repetía hoteles y casas de amigos
- Hablaba con las menores por Instagram
- Quedaba con ellas con ellas para tatuarlas y allí realizaba la agresión



El equipo

El equipo multidisciplinar:

- Detectives
- Peritos informáticos
- Criminóloga
- Abogados

Colaboración y contacto constante con Guardia Civil y posteriormente con Policía Nacional.

Operativo:

- Anzuelo con Iplogger
- Big data
- Identificación de ubicaciones y lugares con OSINT



RESULTADOS

1. Iniciamos contacto a través de Instagram y lanzamos un anzuelo digital. En tan solo dos días, logramos obtener la dirección IP del sujeto investigado.
2. Utilizando técnicas de OSINT (Open Source Intelligence), identificamos diversos lugares que el sujeto frecuentaba y a los que regresaba con regularidad. Un detective se desplazó a estos lugares para verificar su presencia, empleando fotografías y la red WIFI del cliente como método de confirmación.
3. Se elaboró un listado de tatuadores presentes en Instagram y otro de usuarios que habían compartido recientemente su experiencia obteniendo un tatuaje. El detective estableció contacto con estas usuarias tatuadas para recabar más información.
4. Finalmente, una de las cuentas proporcionó la identificación del sujeto investigado y nos facilitó su ubicación actual.



Conclusiones

- ✓ La programación es importante
- ✓ No hace falta ser ingeniero informático y mucho menos colegiado para actuar como perito de parte en España
- ✓ El análisis de datos te da ventaja.
- ✓ Ve a todos los eventos de ciberseguridad y conoce a personas interesantes.



***NOSOTROS SOMOS NUESTRA MAYOR VULNERABILIDAD,
PERO TAMBIÉN NUESTRO MEJOR ANTIVIRUS.***

Gracias



QUANTIKA¹⁴
● INTELLIGENCE FOR CRIMINAL INVESTIGATIONS