SniffJoke 0.5

growing process in Sniffer/NIDS evasion technology

The speaker

- Claudio Agosti, *vecna* in Internet.
- 12+ years of hacking and not in prison :)
- idealistic contributor in various “projects” without a full time job.
- http://www.delirandom.net vecna@delirandom.net

Agenda

- what's sniffer evasion
- which kind of vulnerabilities exist
- patches, improvement and workaround
  - target selection: *sniffers vs NIDS*.
- Sniffjoke goal for 0.5 release: defeat everything that passively eavesdrops traffic from the network.

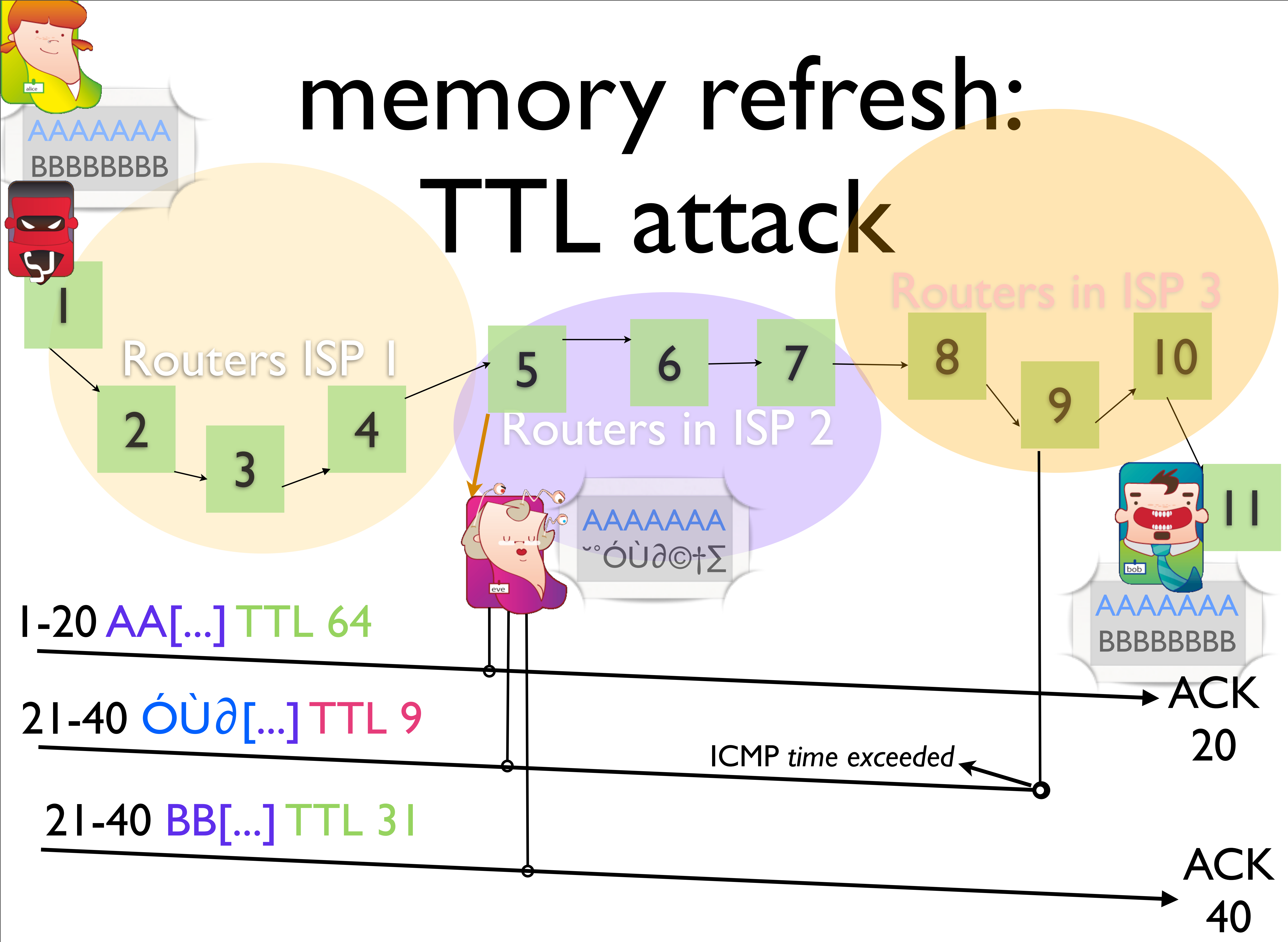
NIDS evasion, A forgotten lore ?

- first and actual research released in 1998
- difficult to be tested outside a lab
- difficult to be integrated in the daily app.
  - fragrouter (~2002) + libdnet (~2005)
  - innova 2001 - SniffJoke *0.3* 2007, *0.4* 2010
  - StoneSoft 2009-2010
- **but**, the sniffing issue persists, the IDS market stands alive and healthy. Despite this, few tools exist able to perform a wide evasion test.

memory refresh

- An NIDS attack is the injection of forged packets. Those packets are captured by the passive third party.
    - Can be single packet DoS. They are easy to patch.
    - Could be part of the active session, could be based on plausible packets, and *allow the attacker to interfere with the flow reassembly logics*.
        - it is really hard to develop techniques able to interfere with the sniffing activity without disrupting the real session
        - when an evasion is found, maybe really difficult to be patched

memory refresh: TTL attack



alice

AAAAAAA
BBBBBBBB

Routers ISP 1

1 2 3 4

Routers in ISP 2

5 6 7

Routers in ISP 3

8 9 10

11

eve

AAAAAAA
˘°ÓÙ∂©†Σ

bob

AAAAAAA
BBBBBBBB

1-20 AA[...] TTL 64

ACK 20

21-40 ÓÙ∂[...] TTL 9

ICMP *time exceeded*

21-40 BB[...] TTL 31

ACK 40

memory refresh: concepts

- lack of Information on the wire
- An NIDS evasion technique exploits the ambiguous meaning of such packets
  - A NIDS/Sniffer *collects the packets* but has not a mathematical certainty that the packet will be accepted by the remote host
  - By theory, the attacker has no way to know if the attacks has worked or not.

1998 attacks table

	fragroute	Sj 0.4	Sj 0.5 (dev now!)	Patch ?
ip TTL	fixed value	# around, mist	# around, mist	contextual
cksum	Y	Y	Y	normalization
source route	Y	all IP opt	all IP opt	contextual
frag policy	fixed value	dynamic	dynamic	contextual + AM
ip frag overlap	dynamic	dynamic	dynamic	contextual + AM
tcp options	mss|wscale, fixed	some TO, dynamic	lot of TO, adaptive	contextual + AM
PAWS	fixed (anomaly)	N	adaptive	don’t know!
tcp overlap	dynamic	adaptive, chainable	adaptive, chainable	contextual + AM
RST off seq	N	Y	Y	contextual + AM

Attacks concepts

- **Ambiguity methods obtain the desynchronisation** between the reassembled flow and the effective endpoint traffic
- by exploiting this ambiguity, you can decide some kind of disruption to cause to a passive analyzer
  - data you are sending could be hidden from its analysis
  - the established session could appear closed
  - the flow could be broken

Attack targets

- NIDS and sniffers both base their workings on passive traffic collection
  - but NIDS work in a specified network, and could treat traffic with too much anomalies as malicious.
    - work in a contextual security
  - Sniffers cannot map a specific network, cannot drop traffic like an IPS does, and are sold by feature/performance instead of reliability.

patches thru the ages

- Strong TCP check. don’t make any assumption, base the collected data on all the available informations
- Sanitization, restriction policy. keep anomaly counts in sessions and treat evasions.
- Active mapping, know the exploitable details of your network and use them inside the reassembly algorithm.

this about NIDS

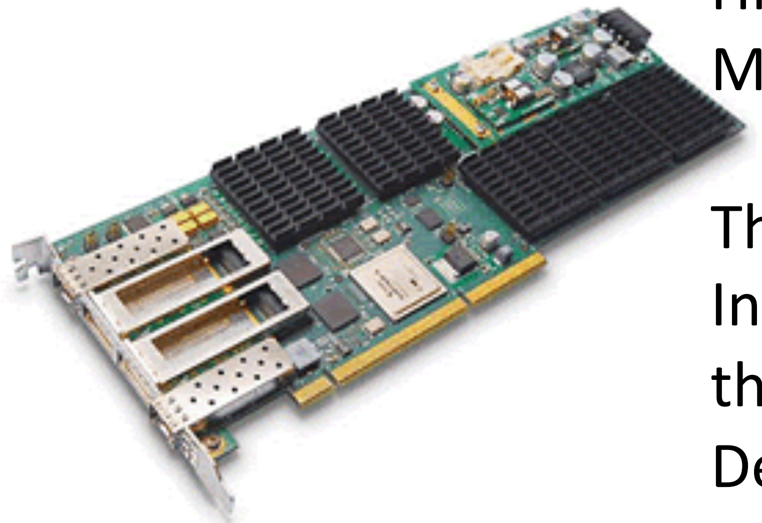
network intrusion detection systems

very different analysis has to be applied at the mass interception tool!

differences

	NIDS	Sniffer
forced sanitization	possibile, but became s.p.f.	impossible: is totally passive
anomaly detection	could apply statistical analysis and trigger alert	could apply analysis but remains unable to reassemble
active mapping	could work in the protected network	a sniffer has not a single network to control

Multi gigabit business



http://www.cybersift.net/hpns.html

High Performance Traffic Inspection, Monitoring and Capture at 10Gbps

The SiftNIC10 is an advanced Network Interface Card combining FPGAs and state of the art support software. The NIC provides full Deep Packet Inspection (Layer 2-7[...] **to operate on 10Gbps backbones** – extending the life of software assets.

Intelligence Support Systems for Lawful Interception, Criminal Investigations, Intelligence Gathering and Information Sharing Conference and Expo

http://www.telestrategies.com/ISS_WASH/index.htm

VANTAGE is a mass and target interception system that intercepts, filters, and analyzes voice, data, and multimedia for intelligence purposes. Using sophisticated probing technology and Verint's real-time filtering mechanisms, VANTAGE passively collects maximum communications, extracts the most important information, and uses stored data analysis for generating intelligence from data collected over time. http://verint.com/communications_interception/

100 gb/sec sniffers

coming soon on...

http://www.endace.com/endaceextreme.html

- Mass survelliance will sound like control inside national border
  - But data, packets, travel for much more nations than source & destination!
- Some years ago the mass survelliance technology hadn't enough computational power: now it has.

downgrade multi gigabit sniffers to multi kilobits

- This is the official Sniffjoke's payoff
- a multi gigabit probe needs to make assumptions in high speed traffic analysis.
- **could** it check every checksum ? **could** it keep track of every data-ack? **could** it be updated with the most recent header options ? **could** it manage packet loss ? needs to have **strict timeout** inside, because it requires to clean the huge connections table about the tracked packets.
- every assumption is an exploitable vulnerability by Sniffjoke.

checked vulnerability

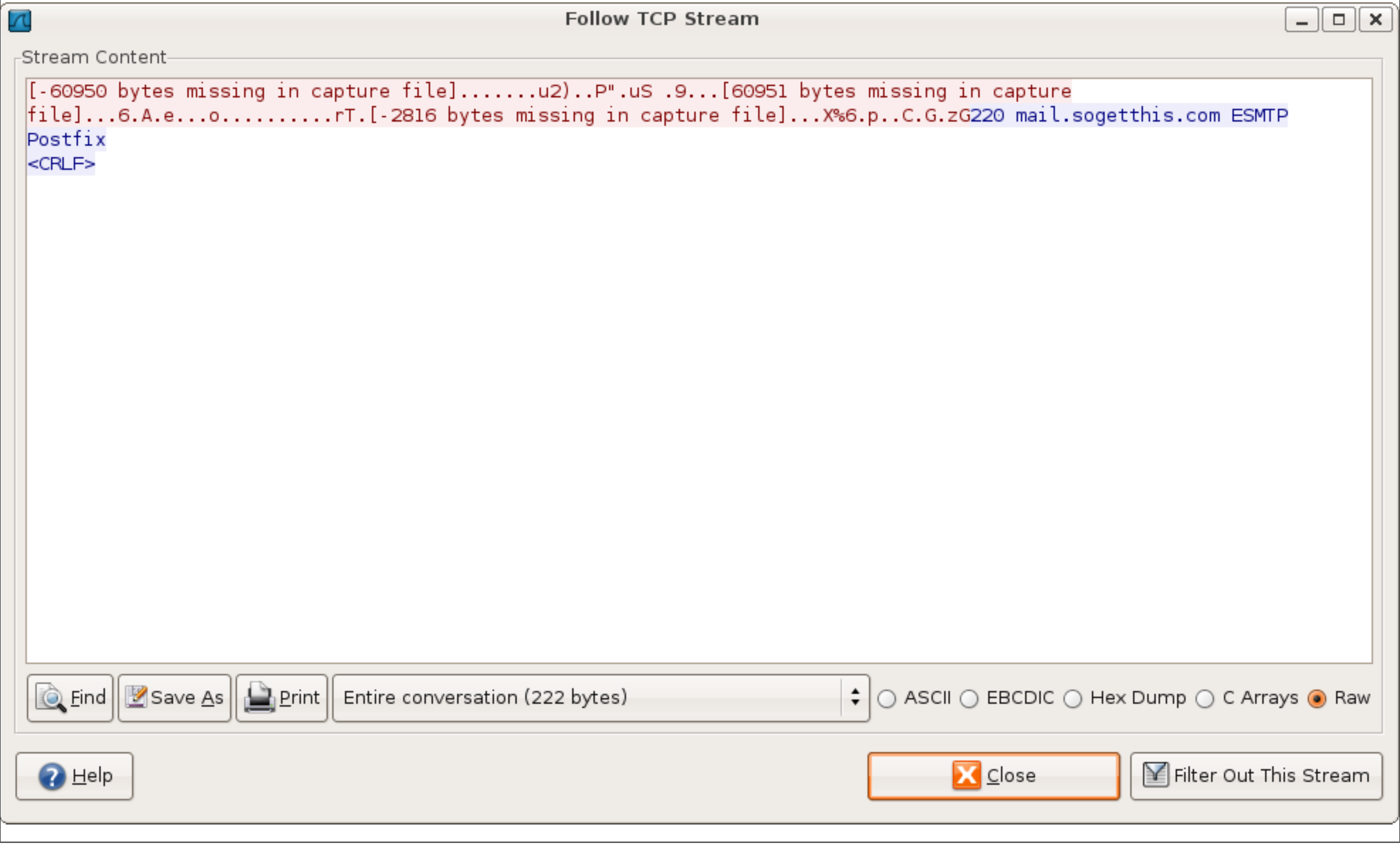
	fragroute	SniffJoke 0.2	SniffJoke 0.3	SniffJoke 0.4
dsniff	N (?)	N	N	Y
xplico	N/A (Y ?)	evasion detection	Y	Y
snort	old releases	N	N	Y (lab only)
wireshark	N/A (Y ?)	N	Y	Y
ethereal (*)	Y	Y	Y	Y

sniffjoke 0.5 is not aiming to exploit new sniffers/IDS, but be stable in a real case scenario against professional products.

various kind of damage

- Denial of service: huge file dump
  (sequence number shifting)
- Invalid data recorded instead of the real one
  (fake payload)
- Incoming connection desync and override
  (invalid ack-ing)
- premature closing of currently running session
  (fin, rst and syn flags acceptance)
- creating hole of data inside the session
  (drop packets, fragment or sections of payload)

wireshark try to reassembly an e-mail captured

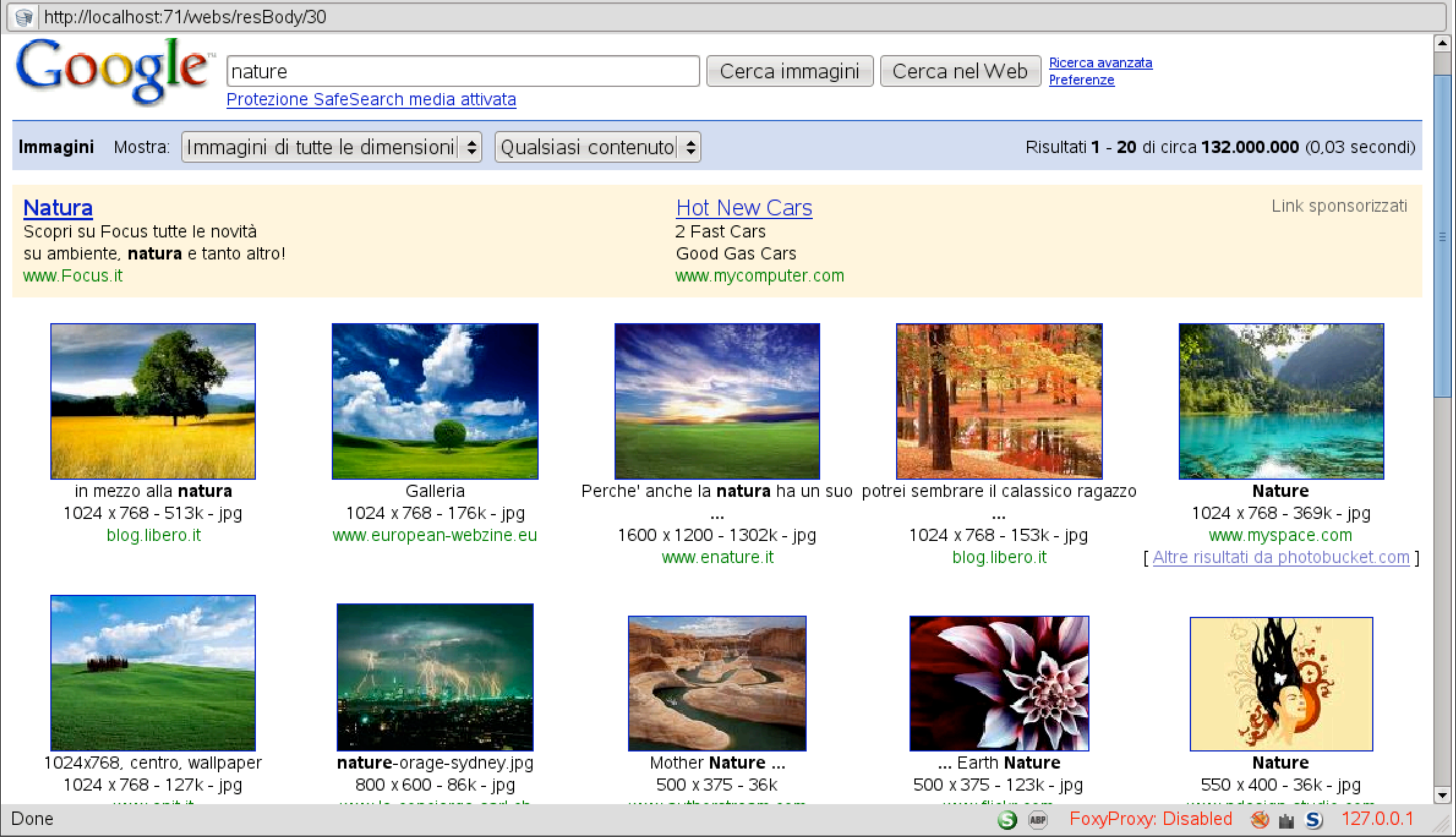


```
[-60950 bytes missing in capture file].......u2)..P".uS .9...[60951 bytes missing in capture
file]...6.A.e...o.........rT.[-2816 bytes missing in capture file]...X%6.p..C.G.zG220 mail.sogetthis.com ESMTP
Postfix
<CRLF>
```

Entire conversation (222 bytes)

○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

x-plico, capturing traffic **without** sniffjoke protection



http://localhost:71/webs/resBody/30

Google

nature

Cerca immagini | Cerca nel Web

Ricerca avanzata
Preferenze

Protezione SafeSearch media attivata

Immagini Mostra: Immagini di tutte le dimensioni | Qualsiasi contenuto

Risultati **1** - **20** di circa **132.000.000** (0,03 secondi)

Natura
Scopri su Focus tutte le novità
su ambiente, **natura** e tanto altro!
www.Focus.it

Hot New Cars
2 Fast Cars
Good Gas Cars
www.mycomputer.com

Link sponsorizzati

in mezzo alla **natura**
1024 x 768 - 513k - jpg
blog.libero.it

Galleria
1024 x 768 - 176k - jpg
www.european-webzine.eu

Perche' anche la **natura** ha un suo ...
1600 x 1200 - 1302k - jpg
www.enature.it

potrei sembrare il calassico ragazzo ...
1024 x 768 - 153k - jpg
blog.libero.it

Nature
1024 x 768 - 369k - jpg
www.myspace.com
[Altre risultati da photobucket.com]

1024x768, centro, wallpaper
1024 x 768 - 127k - jpg

nature-orage-sydney.jpg
800 x 600 - 86k - jpg

Mother **Nature** ...
500 x 375 - 36k

... Earth **Nature**
500 x 375 - 123k - jpg

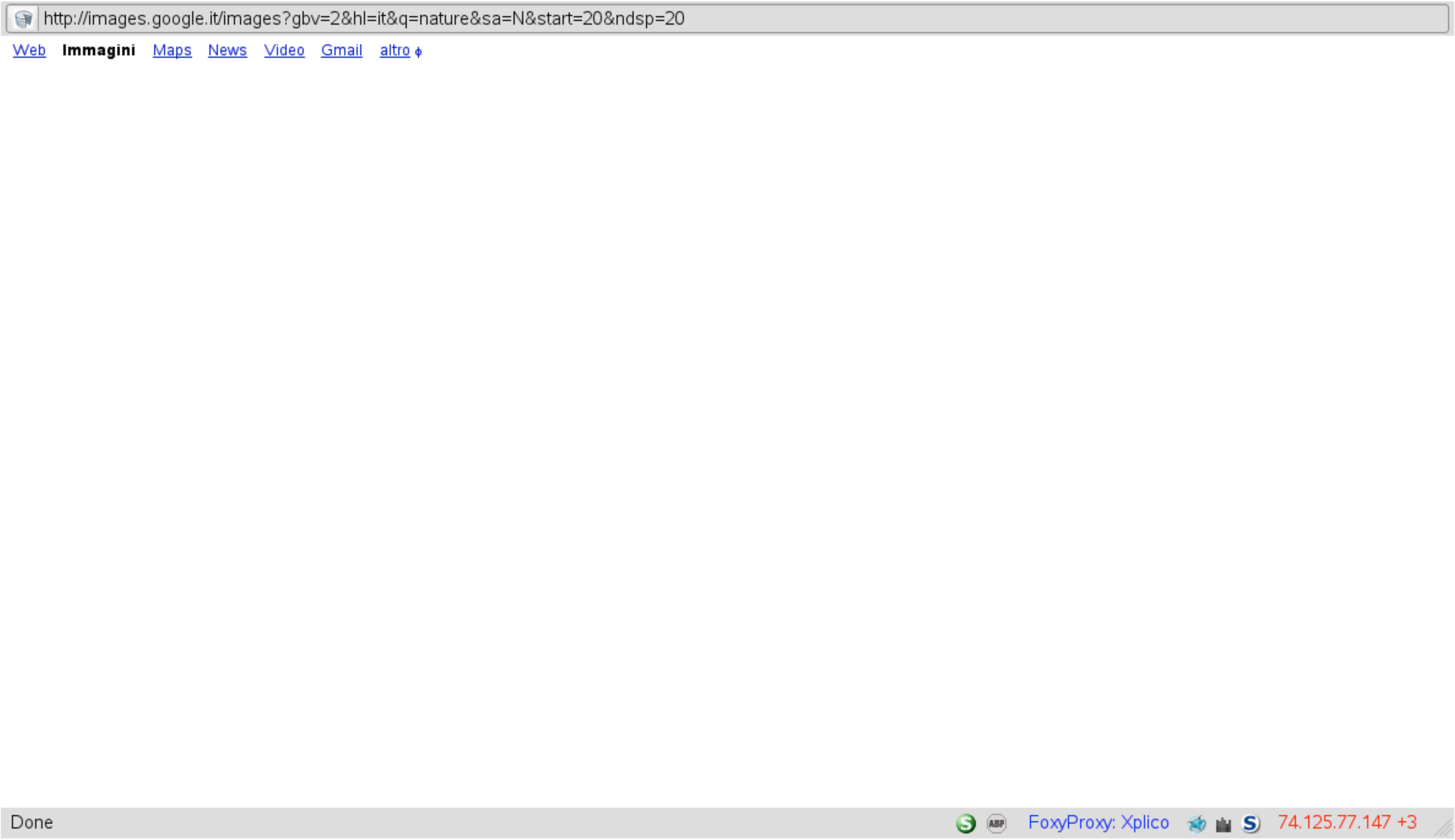
Nature
550 x 400 - 36k - jpg

Done

FoxyProxy: Disabled

127.0.0.1

x-plico, same request, traffic protected by sniffjoke



http://images.google.it/images?gbv=2&hl=it&q=nature&sa=N&start=20&ndsp=20

SniffJoke base research

- An attack is composed by two factor
  - the Scramble: is the technique used to obtain desyncronization
  - the Injection: is the packet assumes as real, accepted in the reassembled flow, and source of the damage

Scrambles in SniffJoke

	0.4 status	0.5 goal
TCP opt	few	exploit every possible abuse :)
TCP md5	working, but need remote app	working, but need remote app
OS dependent trick	only RST+FIN P.o.C.	integrate passive OS fingerprint
IP opt policy	silent drop	check them at the last hop
Congestion based attacks	not implemented	under research
IP timestamp expire	not implemented	under research

Injection

each implemented in a different loadable plugin

bad syncronization	fake seq	invalid window	invalid ack	
payload breaking	fake payload	overlap segments	fragmentation	segmentation
forced closing	fake syn	fake fin	fake rst	valid rst off window

IP/TCP options scramble

- when an host receives a packet with a unsupported IP-option, drop the packet (and the sniffer could not know)
- when a new IP option is implemented, the reassembly device is not updated
- some TCP-option, need to be interpreted because interfere strongly with the packets acceptance or dropping

TCP options examples

- TCP MD5 signature check has been developed to avoid BPG spoofing (now TTL auth based is used)
    - a multi gigabit sniffer could not perform MD5 checks for performance reason, but avoiding this check, is victim of packets ambiguity!

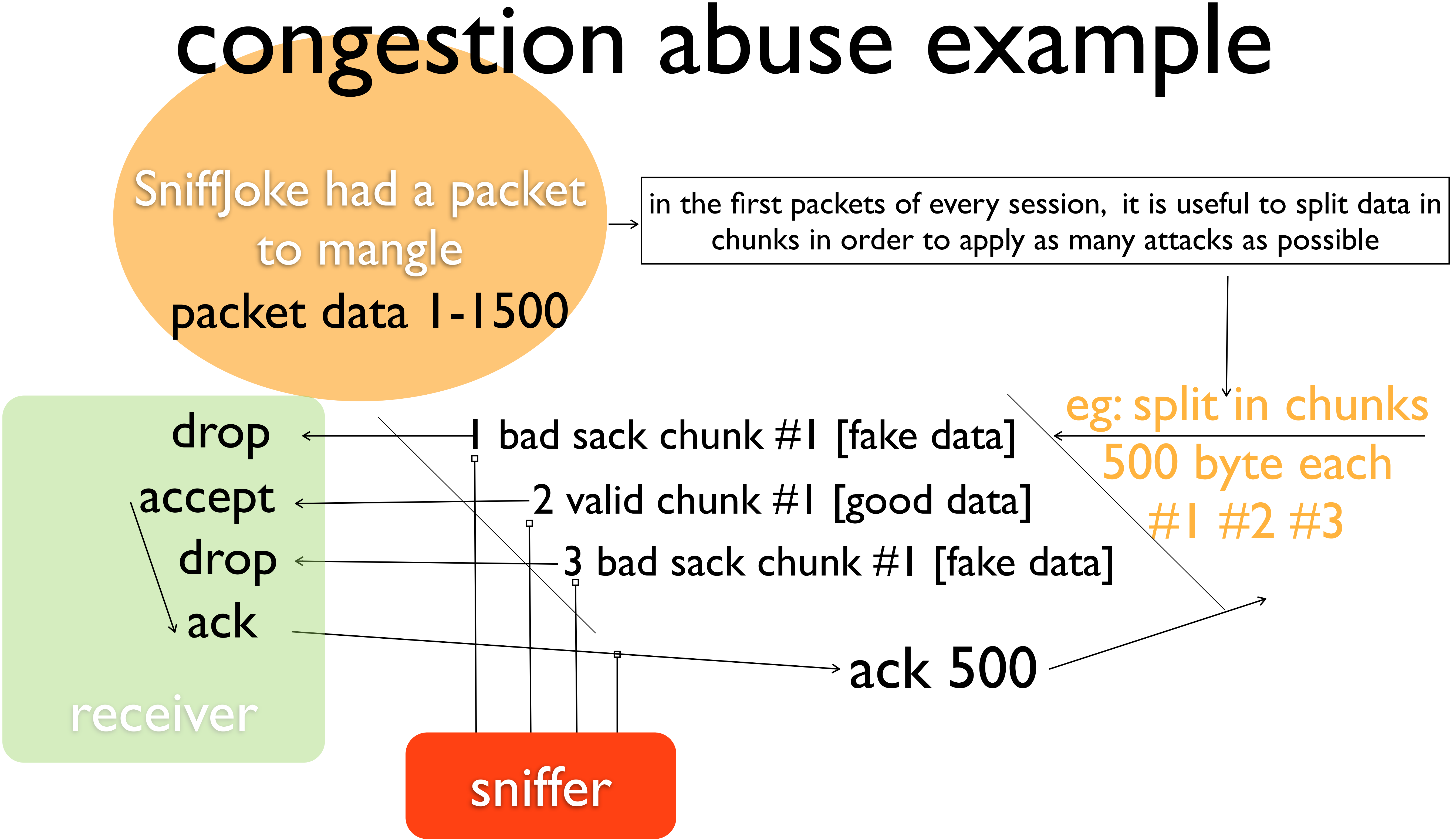
Congestion based attacks

- TCP plain is ACK dependent (sessions with high packet loss and high bandwidth have bad performances)
- SACK has been developed to detect packet loss and perform selective packet retransmissions.
  - RFCs: SACK 1996, NewReno 2003, D-SACK 2000, ECN... these extensions produce a lot of congestion avoidance algorithms.

Congestion algorithm injection logic

- The *sender* doesn't know how many algorithms are supported by the *receiver*
- Different OSes have different boundaries (eg: Windows CTCP): **the ambiguity**!
    - SACK-block validation is based on internal value of the stack (OS dependent vars, session max-window, timings) unknown by the sniffer.

congestion abuse example



SniffJoke had a packet to mangle

packet data 1-1500

in the first packets of every session, it is useful to split data in chunks in order to apply as many attacks as possible

eg: split in chunks

500 byte each

#1 #2 #3

1 bad sack chunk #1 [fake data]

2 valid chunk #1 [good data]

3 bad sack chunk #1 [fake data]

drop

accept

drop

ack

receiver

ack 500

sniffer

sniffer will not understand which chunk is accepted by the receiver, and by the queue design, will keep the first or the last packet only.

SniffJoke 0.4.x feat

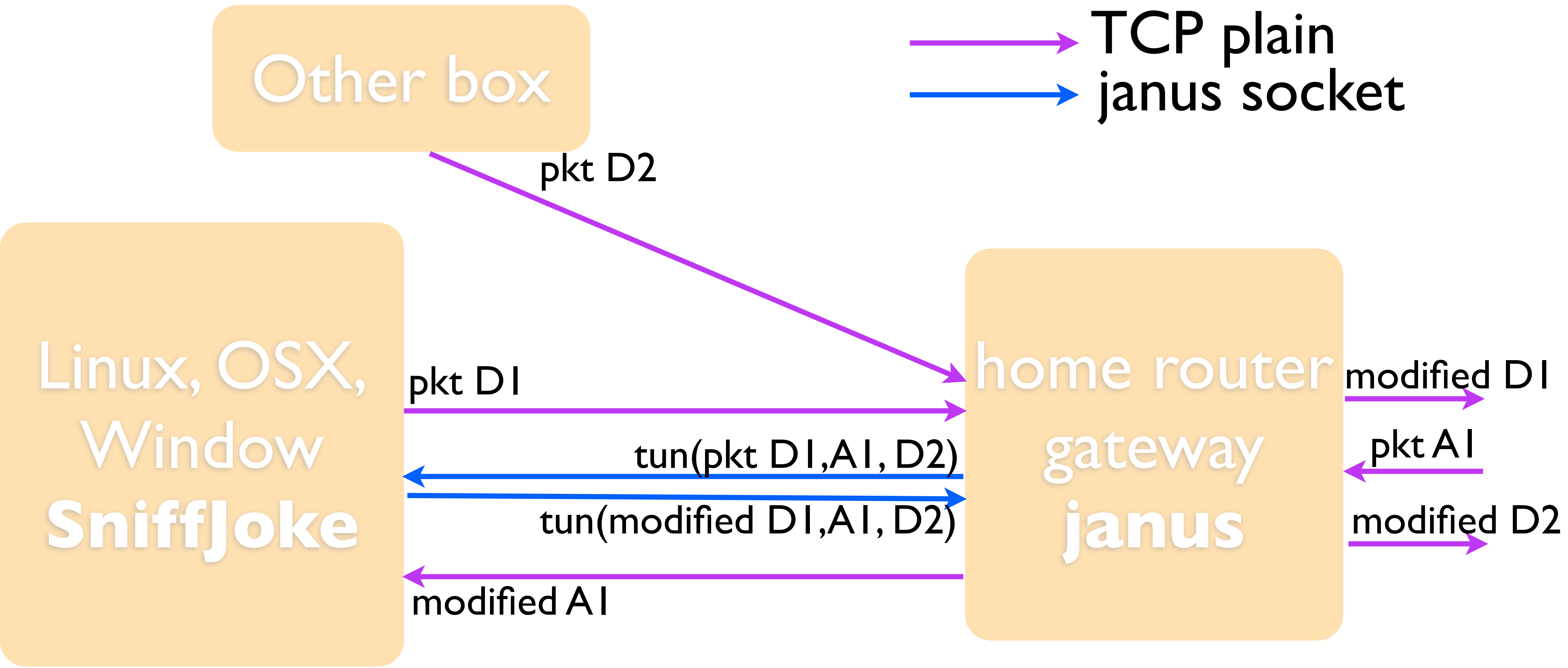
- Location based adaptive combinations
  - `sniffjoke-autotest` has been revealed to be the limitation in real case scenarios.
- Configurable ports aggressiveness
- Avoid signature based detection

SniffJoke 0.4 issues

- it was a single monolithic software
- it included OS dependent commands, operations and calls, reducing the portability

SniffJoke 0.5 portability solution

janus



Janus could run in the same box of Sniffjoke or in the gateway.

janus portability achievements

- Past implementation of divert was painful
- janus is written in plain C, and required SOCK_PACKET datalink access
- janus portability is based on a configuration file containing commands usable in almost every operating system

janus logic

- set a static arp overriding the default gateway
- sniff your traffic, forward to a TCP port *if attached*
- drop the traffic directed to the default gateway
- read at interface layer the outgoing traffic and forward to another TCP port, *if attached*
- reinject the traffic received to the proper destination.

this allows to have a portable application able to run on OpenWRT, lafonera, Linux, MacOSX, *BSD...

SniffJoke 0.5 feat
continuos probe

- in 0.4 release, the attacks set was defined by a configuration file different for each location (`plugin-enabled.conf`)
    - it's required, because your own nat device could be fooled by injected packet and close the session.
- in 0.5, a continuos check of usable combinations is performed and results are cached. To every destination host is assigned a complete map of IP/TCP options reaching the destination, Operating System detected, hop distance, overlapping behaviour.

release status

- in github two branches are present: **master** (the not-really-“*stable*” 0.4.2) and **devel**, 0.5 under development.
- gentoo, backtrack, .deb and .rpm packages of 0.4.2 has been done
- 0.5 aim to work in iPhone, Android, *BSD, windows.
- `sniffjokectl` was the client name, we’re planning to use a JSON library to manage sniffjoke and janus administration.

next goals

- found a laboratory and test professional IDS and Sniffer (we have only *theoretical hints*!)
- write report, advisory: push the security market to face with the possibility that a security device could be bypassed.
- and in those two points: **I couldn't do without a partnership.** I'm looking for security companies that want to focus on evasion research and countermeasures.

Thanks! Questions ?

https://twitter.com/#!/sniffjoke

vecna@delirandom.net

```
pub   1024D/C6765430 2009-08-25 [expires: 2012-10-03]
      Key fingerprint = 341F 1A8C E2B4 F4F4 174D  7C21 B842 093D C676 5430
```

sniffjoke@sikurezza.org
mailing list
https://www.sikurezza.org/lists/listinfo/sniffjoke

http://www.delirandom.net/sniffjoke
http://github.com/vecna/sniffjoke
http://github.com/evilaliv3/janus

out of band slide: some useful documents

The one:

http://insecure.org/stf/secnet_ids/secnet_ids.html

revisited:
http://www.symantec.com/connect/articles/evading-nids-revisited

https://tools.ietf.org/html/rfc4614

A Roadmap for Transmission Control Protocol (TCP) Specification Documents

https://www.ietf.org/html/rfc6274

Security Assessment of the Internet Protocol Version 4

http://www.cnsr.info/Download/PDF/a4b.pdf

Verifying TCP Implementation