

SniffJoke 0.4

“Downgrade multi gigabits sniffers to multi kilobits”
PH-Neutral – may 2011



Agenda – SniffJoke 0.4 May/2011 45min ETA

1. Introduction, target definition
 - 6
2. Theory, implementation issue
 - 4
3. Anatomy of the attacks
 - 8
4. Implementation in SniffJoke framework
 - 14
5. Impact, considerations, TODO
 - 10

Hi! I'm vecna

- Known also as Claudio Agosti
 - s0ftpj, for those who remember what it was
- **Infoblah securblah hackblah**
- Anonymity, cryptography, privacy, paranoid technology, kernel, c++

My english sounds like a google translation, when the network is down, sorry!

Main concepts

- **Target:** vital algorithms present in every network device making passive traffic analysis
- **Thesis:** they haven't enough information to correctly perform flow reassembly
- **Attack:** (ab)using this network capabilities, IP sessions would be (difficult | impossible) to be reassembled
- **Effect:** business and security based on passive traffic analysis could get some troubles :)

Xplico sniffer, capturing pkts without Sj

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











Google™ nature [Ricerca avanzata](#)
[Preferenze](#)

Protezione SafeSearch media attivata

Immagini Mostra: 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](#) Link sponsorizzati
2 Fast Cars
Good Gas Cars
www.mycomputer.com

 <p>in mezzo alla natura 1024 x 768 - 513k - jpg blog.libero.it</p>	 <p>Galleria 1024 x 768 - 176k - jpg www.european-webzine.eu</p>	 <p>Perche' anche la natura ha un suo ... 1600 x 1200 - 1302k - jpg www.enature.it</p>	 <p>... 1024 x 768 - 153k - jpg blog.libero.it</p>	 <p>Nature 1024 x 768 - 369k - jpg www.myspace.com [Altre risultati da photobucket.com]</p>
 <p>1024x768, centro, wallpaper 1024 x 768 - 127k - jpg www.enature.it</p>	 <p>nature-orage-sydney.jpg 800 x 600 - 86k - jpg www.enature.it</p>	 <p>Mother Nature ... 500 x 375 - 36k www.enature.it</p>	 <p>... Earth Nature 500 x 375 - 123k - jpg www.enature.it</p>	 <p>Nature 550 x 400 - 36k - jpg www.enature.it</p>

Done

FoxyProxy: Disabled 127.0.0.1

Xplico sniffer, same search, with Sj

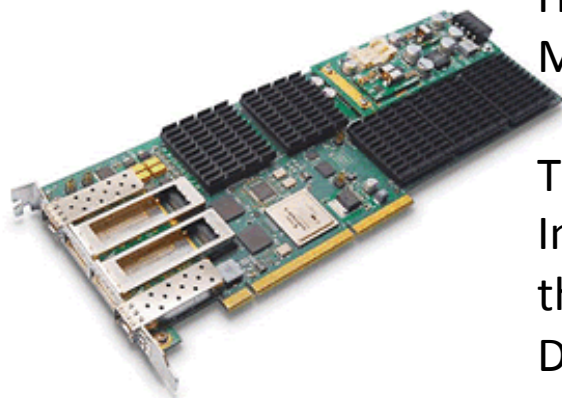
 <http://images.google.it/images?gbv=2&hl=it&q=nature&sa=N&start=20&ndsp=20>

[Web](#) **Immagini** [Maps](#) [News](#) [Video](#) [Gmail](#) [altre](#) 

Done

  FoxyProxy: Xplico    74.125.77.147 +3 

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 – coming soon

- Mass surveillance will sound like control inside national border
- But data, packet, travel for much more nations than source/dest!
- **The mass surveillance technology some years ago hasn't enough computational power: now has it**

Around the world, telcos, financial institutions, federal agencies and large digital service delivery organisations are actively deploying 40Gb/s and 100Gb/s networks in metro, long-haul and short-hop data centre / cloud environments. **The market for ultra-high speed networking is gathering momentum.** [...] These systems are expected to be available for deployment later in 2011.

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

SniffJoke Project goals

- **A new tool against mass surveillance**
- Remember that control doesn't necessarily bring security
- **Fun!!**
- Remember that an organization based on the network is efficient and rapid in evolving
- Exploit the deepest shadow cone in the TCP/IP 😊

a research back in the 1998

- First time I read about, was in phrack #58
- First time I tried to implement, was back in 1999
- A research that seem to be forgotten by vendors
 - until StoneSoft's marketing kick out AET !
- We're talking about a technique that's either *difficult to be implemeted* and *difficult to be tested* too.

Thesis: information is not enough

- In the middle elements will not know what happen to the remote peers
- Hypothetically, a recorded packets will never have reached the remote
- Will have more than one meanings, and the IP/TCP stack choose based in configuration, Operating System, or release number
- In short: **Internet was engineered for 2 peers, not for the third passive analyzer.**

Attack: injecting is not so simple

- You need to not broke the session
- You need to fool the sniffer writing only plausible packets in the flow
- You need to guess how a sniffer works, because a lot of them are not open source
- You need to cover your injection pattern, to avoid be filtered out
- **Sj require one side only**

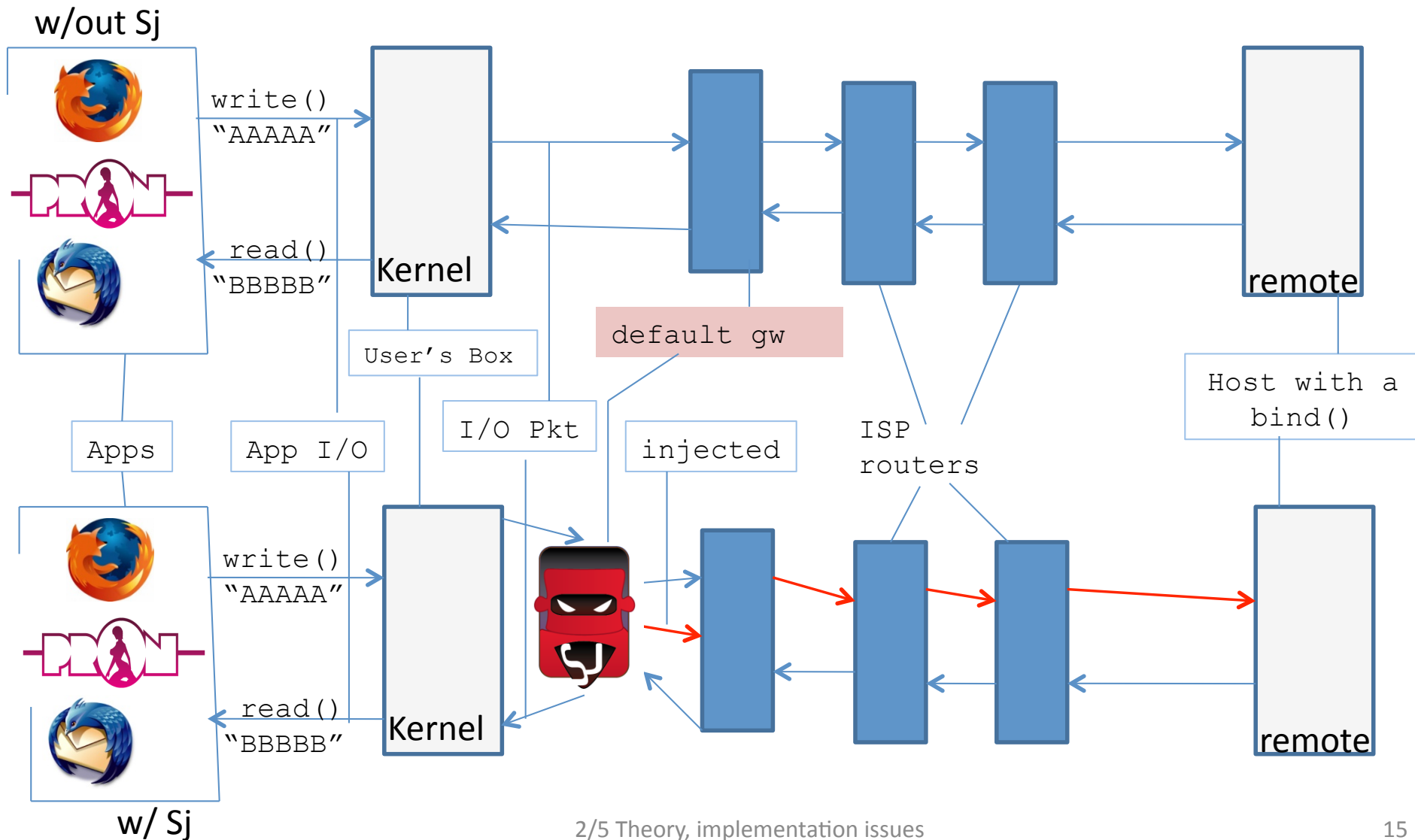
Implementation issue, 1/2

- The first software testing this vulns, was a CASL script
 - CASL is a language for packet forging
 - A TCP session was established “by hand”
- A daily usage will require a transparent layer
- Only in kernel space is possible ?
 - In the past, YES, with a lot of troubles
 - Firsts research goal was to make in userland

Implementation issue, 2/2

- How to intercept outgoing packets ?
 - SniffJoke use a /dev/tun interface, setting himself as default gateway
 - Receive all packets since IP header
 - Forward to the default gw ether address
- How to intercept incoming packets ?
 - Filtering rule to drop packet coming from the gw
 - Reading in datalink layer and resending as raw

SniffJoke network injection



Anatomy of the attack

- Thought packet reassembly as “black box”
 - We could deduce that a realtime sniffer/IDS will try to be faster than ever, in order to optimize the hardware following the bandwidth growing
 - WireShark is the best reference: the top community driven, non realtime, best reassembly available
- The attacks will be planned versus a specific target (a specific sniffer sw).
 - It is easyest, not an 0.4 goal

Goal of the research

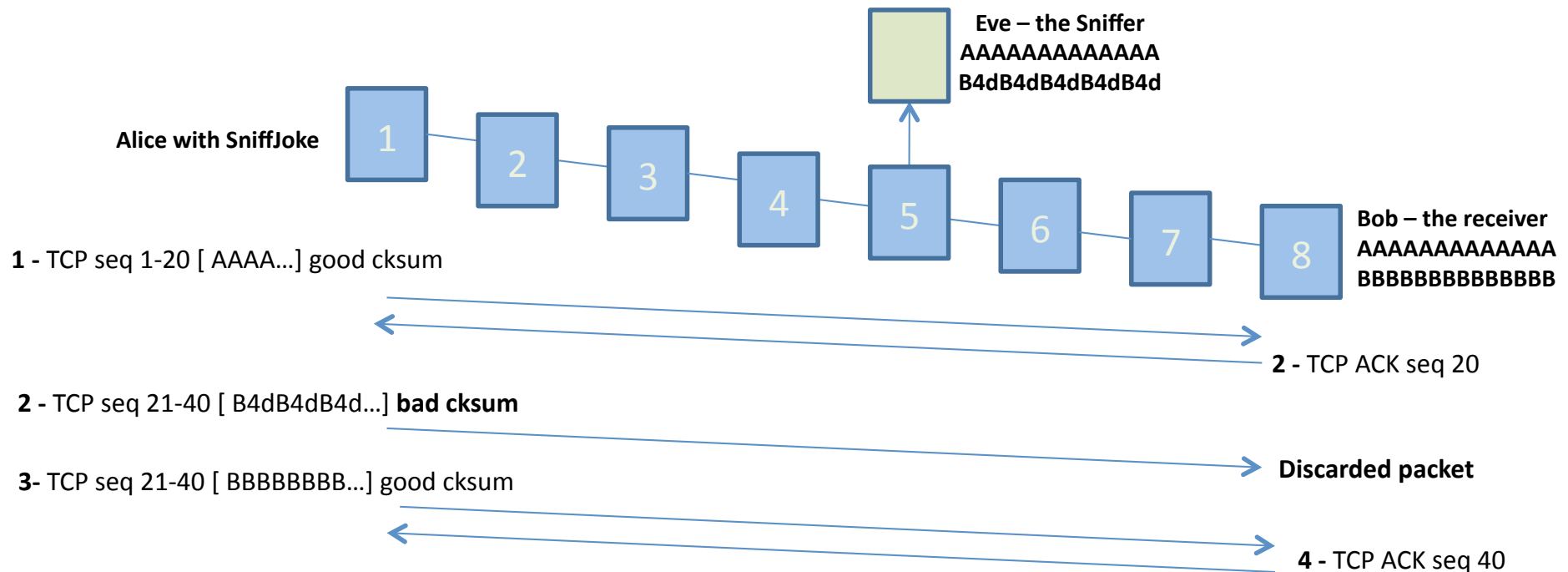
- Found some RFC/stack good way to generate some packets that will:
 - Never reach the destination host
 - Be discarded by the destination host
- AND be accepted by the sniffer, or:
 - Be accepted by the destination host, but only because has been abused of some weird status
- AND discarded by the sniffer
- These way will: **cause desynchronization.**
- These are called **Scramble.**

And.. when the desync is obtained

- Insert fake payload
 - Will cause the sniffer to parse/dump fake data
- Give fake sequencing flow
 - Will cause huge dumps, deleting of previous segm
- Inject fake signaling (FIN, RST, SYN)
 - Close, restart, interrupt an active flow
- These are called **Hack**, and are implemented in the **Plugins**

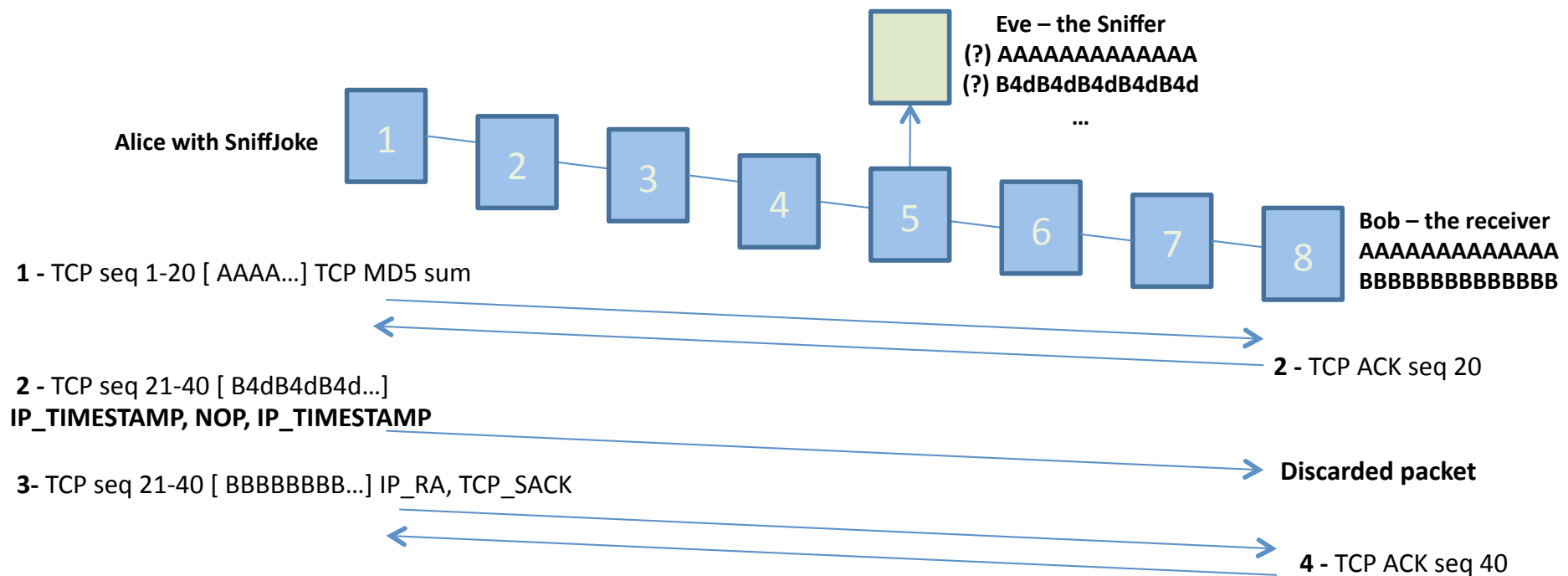
Simple scramble: checksum

- A packet is send with a bad TCP checksum
- the remote service drop it: what the sniffer do ?



New scramble: IP/TCP options

- A packet get an uncommon* IP/TCP option
- The kernel is able to handle it, the sniffer does ?



Scrambles, strengths and weakness

- TTL expire seem the strongest one (network)
 - Instable in asymmetric link dynamic route
- Checksum
 - Is the worst one, easily trapped
- IP/TCP options
 - Exploit the slow update of the sniffer software
 - Exploit the ambiguity of the protocols
 - Need (!) to be tested for each destination
 - Useful for mystification of “good” packets

Descyn abuse: the plugins

- The Plugins (or, the hack) **implement the damage caused** to the desync session
 - Plugins has ben planned to be flexible at most
 - Internal cache, internal logging
 - Conditional check
 - Verify, mangle, modify packet either outgoing and ingoing too.
- I hope/wish/dream ... **external contrib!**

Example of fake close, 1/4

```
virtual bool condition(const Packet &origpkt, uint8_t availableScrambles)
{
    if (origpkt.chainflag == FINALHACK)
        return false;

    bool ret = origpkt.fragment == false &&
               origpkt.proto == TCP &&
               !origpkt.tcp->syn &&
               !origpkt.tcp->rst &&
               !origpkt.tcp->fin;

    /* cache checking */
    [...]
```

Example of fake close, 2/4

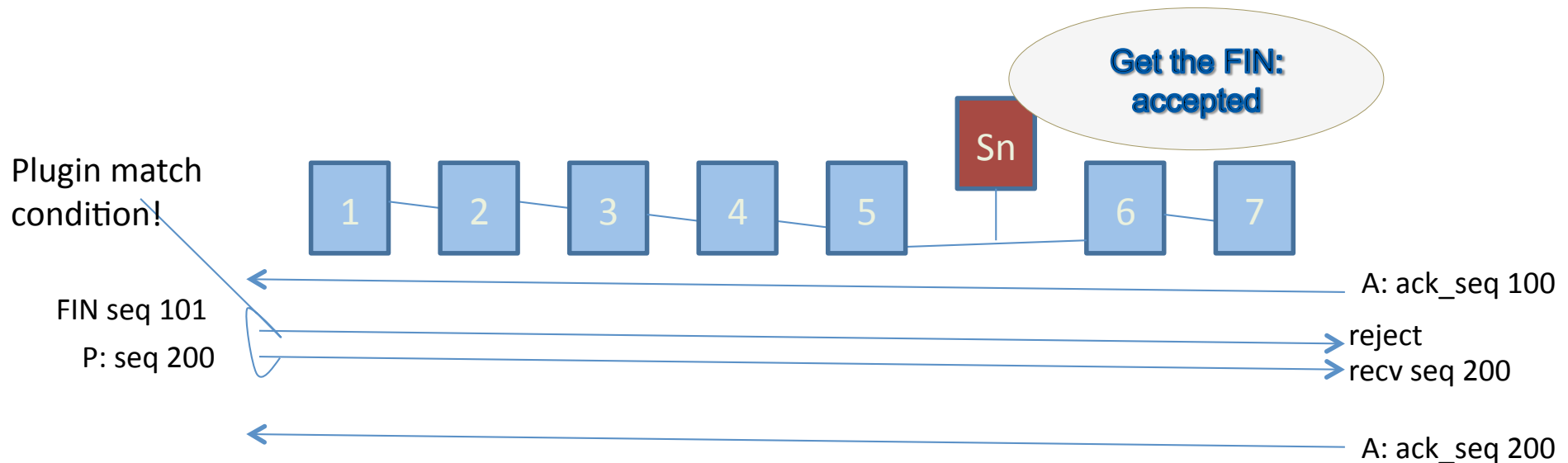
```
virtual void apply(const Packet &origpkt, uint8_t availableScrambles)
{
    Packet * const pkt = new Packet(origpkt);

    pkt->tcp->seq = htonl(ntohl(pkt->tcp->seq) - pkt->tcppayloadlen + 1);

    pkt->tcp->psh = 0;
    pkt->tcp->fin = 1;
    pkt->tcppayloadResize(0);
    pkt->position = ANTICIPATION;
    pkt->wtf = pktRandomDamage(availableScrambles, supportedScrambles);
    pkt->chainflag = FINALHACK;
    pktVector.push_back(pkt);
}
```

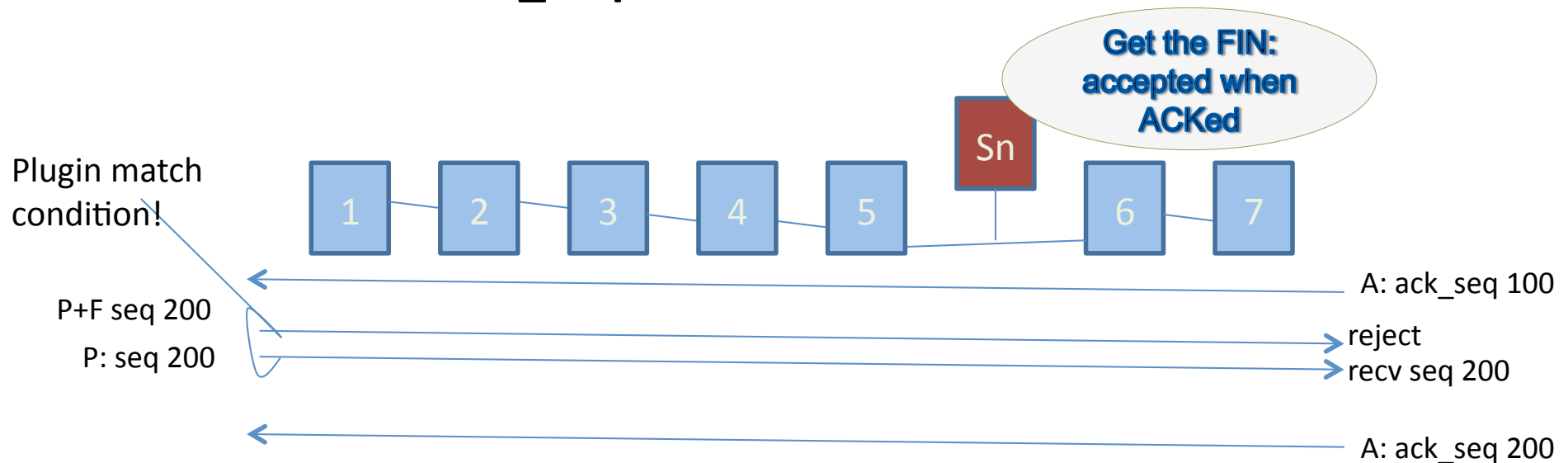
Explain of fake close, 3/4

- **Fact:** our Packet has some payload (`pkt->tcppayloadlen > 0`) is not a fragment and has not FIN, RST, SYN flag
- the sniffer trust the FIN because has the last sequence number + 1
 - `pkt->tcp->seq = htonl(ntohl(pkt->tcp->seq) - pkt->tcppayloadlen + 1);`



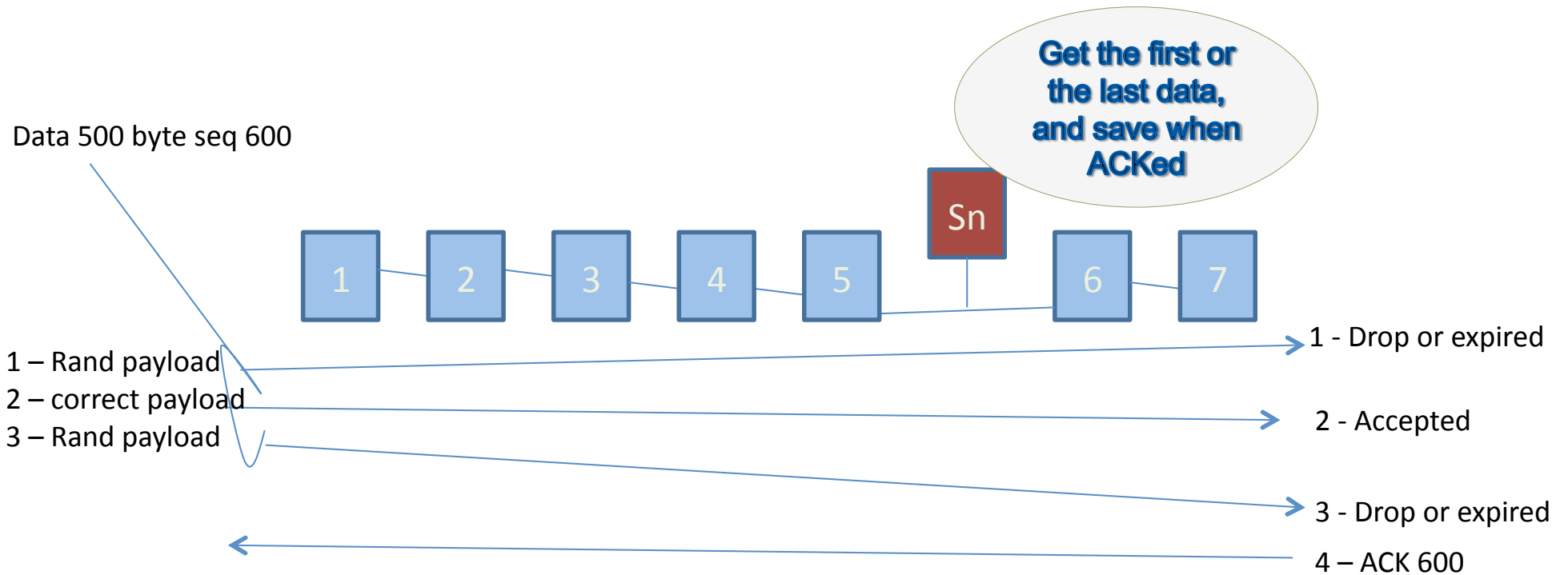
Explain of fake close, 4/4

- **Fact:** our Packet has some payload (`pkt->tcppayloadlen > 0`) is not a fragment and has not FIN, RST, SYN flag
- **CASE 2:** the sniffer trust the FIN because check a coherent `ack_seq` in answer
- **ACK and `TCP.ack_seq` is never touched.**



Fake data injection (TCP/UDP)

- Another hack that expect the foreign ACK



Lists of plugin combined

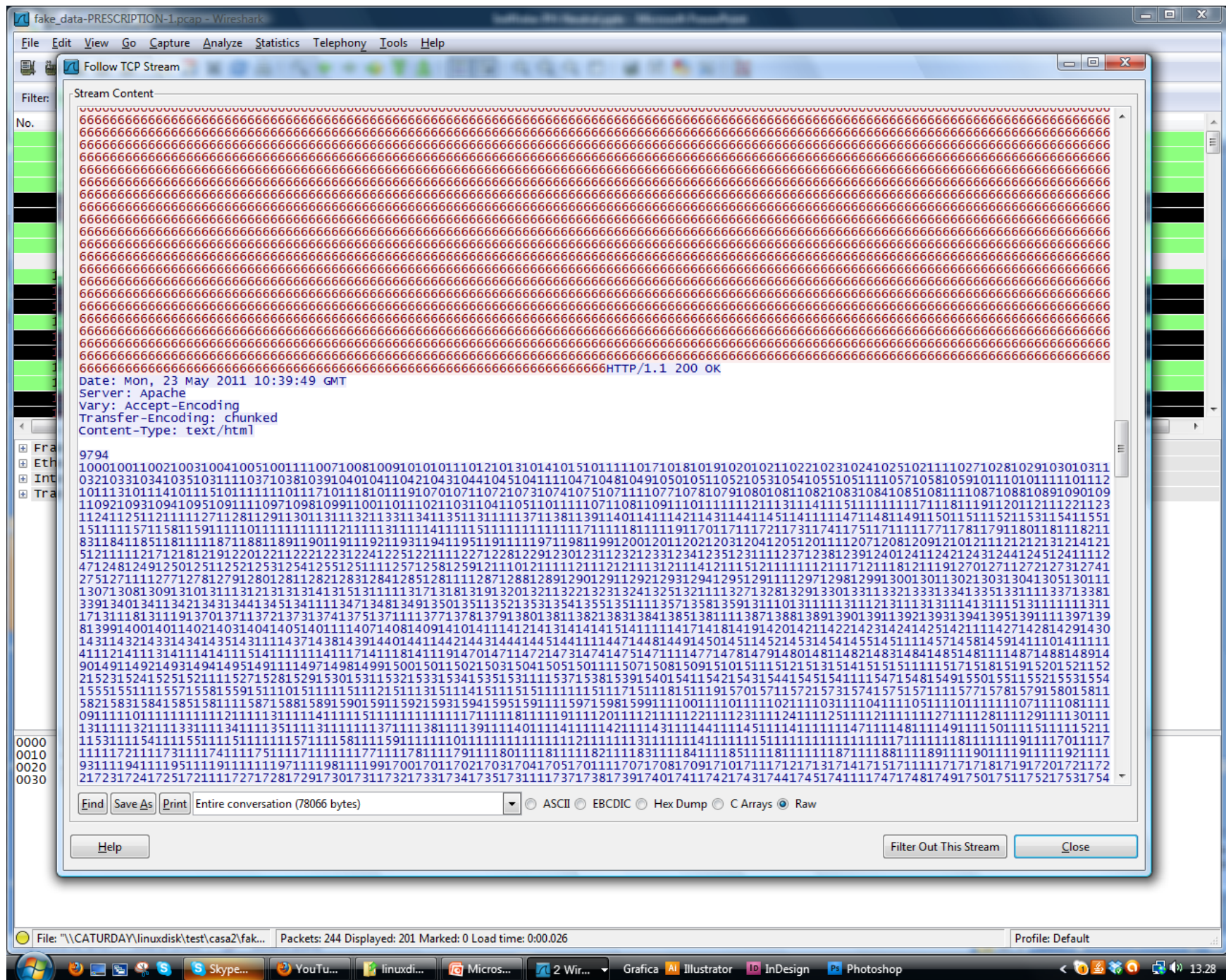
```
# cat plugins-enabled.conf
fake_close_fin,PRESCRIPTION,MALFORMED,GUILTY
fake_close_rst,PRESCRIPTION,MALFORMED,GUILTY
fake_data,PRESCRIPTION,MALFORMED,GUILTY
fake_seq,PRESCRIPTION,MALFORMED,GUILTY
fake_syn,PRESCRIPTION,MALFORMED,GUILTY
fake_zero_window,INNOCENT
fragmentation,INNOCENT
segmentation,INNOCENT
shift_ack,PRESCRIPTION,MALFORMED,GUILTY
valid_rst_fake_seq,INNOCENT
```

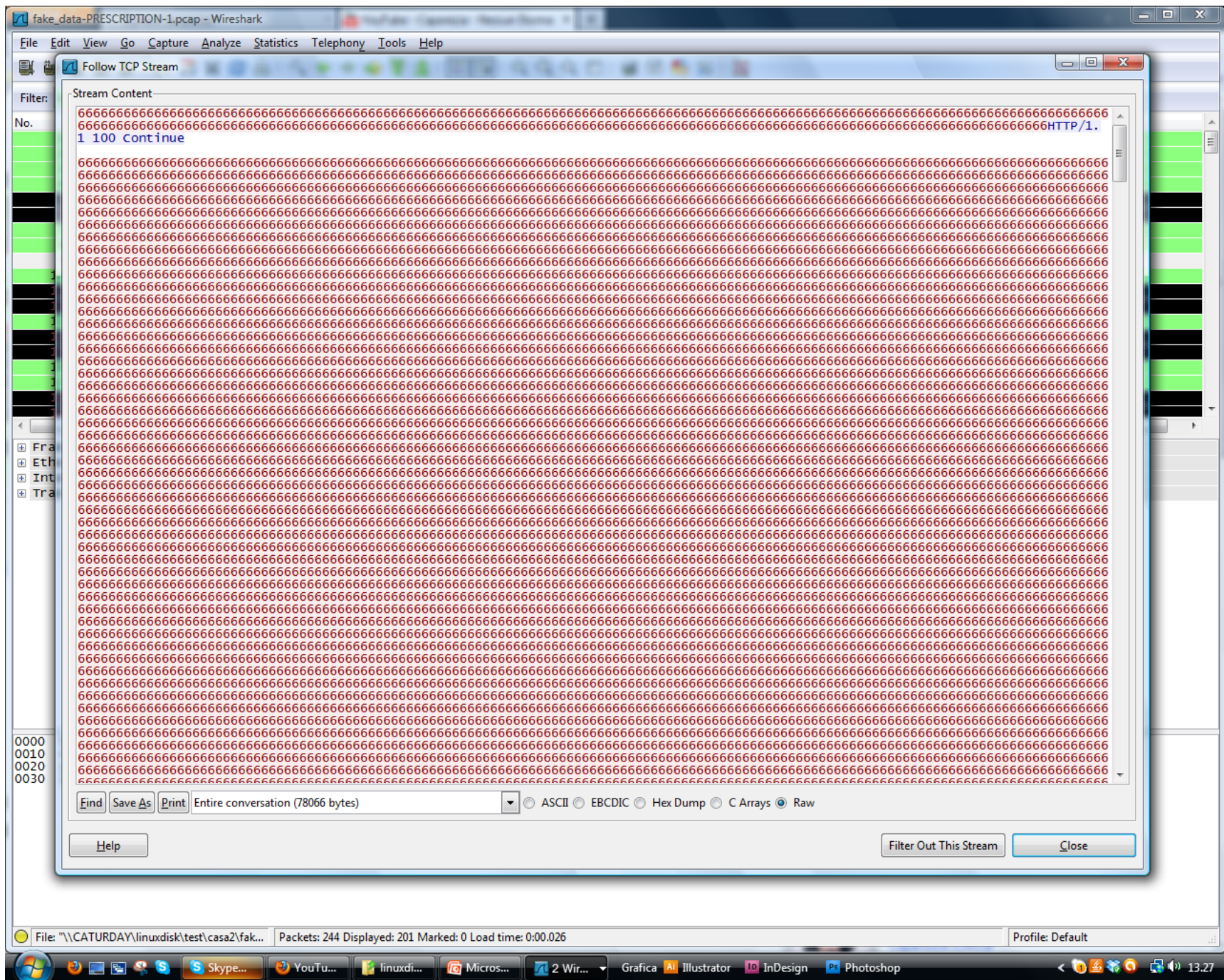
Plugins and options autoprobe

- Each ISP, gateway, firewall, may implement filter of different kinds
 - `sniffjoke-autotest` is a script using every kind of possible available combinations, aiming to select the working combos alone
 - Generate two location dependent configuration file: `iptcp-options.conf` and `plugins-enabled.conf`
 - Every location need an autotest, using the wrong parameters will cause a plethora of faults

Autotest usage

- Goal: generate config files for the location
 - Use a service doing an HTTP ECHO POST
- Retrieve info, message and urls from a remote server (not required, **everyone could setup one**)
 - Offer to submit analysis results
 - I'm expecting useful analyze with IP/TCP options are supported around the world
- `sniffjoke-autotest -l office -d /usr/local/var/sniffjoke -n 1`





Randomization pattern, 1

- Application of the plugins must not be linear, to avoid any kind of pattern recognition by lazy sniffers
 - Every TCP service will be customized in a configuration file
 - Every plugins contains preferred usage
 - Internal selection of protocol, service, status, destination is possible
 - In some plugins less usage is better, other will be pland as permanent usage, depends by the plugins

Randomization pattern, 2

```
$ cat /usr/local/var/sniffjoke/home/port-aggressivity.conf
# this is always on the top of the port definition file, act as
  default
0:65535          RARE
# follow the port rules
22              NONE
# common unencrypted mail
25,110,143      LONGPEEK
# Intensive in the web
80,8080,3128    PEEKATSTART
# Windows service
135:139         PEEK10PKT
# SQL.mysql
156,3306        LONGPEEK
# edonkey
4662           VERYRARE,EVERY20SECONDS
```

Randomization pattern, 3

```
# NONE ..... never used the hack (0% probability)
# VERYRARE ..... 5%
# RARE ..... 15%
# COMMON ..... 40%
# HEAVY ..... 75%
# ALWAYS ..... 100%
# PEEK10PKT ..... packer number 9, 10, 11 = 80%, other 2%
# PEEK30PKT ..... packet number 29, 30, 31, = 90%, other 2%
# EVERY5SECONDS ..... if the number of seconds are divisible by
  5= 90%
#
#           other moments, 2%
# EVERY20SECONDS ..... if the number of seconds are divisible by
  20= 90%
#
#           other moment, 2%
# PEEKATSTART ..... the first 20 packets = 65%, up to the 40th=
  20%, after 2%
# LONGPEEK ..... the first 60 pkts = 65%, up to the 120th=
  20%, after 2%
```

Other features (implemented)

- --chain
 - Every plugin define if an injected/mangled packet will be hacked again (max 2 rounds)
- --no-udp –no-tcp
- ipwhitelist.conf and ipblacklist.conf
- Mystification
 - If supported, inject always IP/TCP options

Lacking feature

- Server side support
 - Will be able to protect a session when the contacted service run in the box with sniffjoke
- Passive OS fingerprint
 - And usage of this information as a scramble selector
- IP/TCP options probe to each single destination

Under study attack, 1

- The plugin `fake_zero_window` in fact don't do anything useful
 - `Tcp.window` analysis and abuse will bring a packet to be discarded by the server
 - But the sniffer will know this
 - SACK abuse, ECN, ICMP source quench, rfc1146 advanced checksum usage

Under study scramble, 2

- PAWS, is a TCP option that will cause a discarding of a packet that bring an internal timestamp too much old
 - But a sniffer will know this timings difference, how to fool it ? How much will go in deep ?

Some SniffJoke effects...

- Dump of +100Mb per sessions! :)
- Decoding of entirely faked data (TX)
 - Mixing, in the worst case
- Cuts and loss of received data (RX)
- *Not so stable*
 - MALFORMED scramble causes seldom session break (non linux target hard to test, weird ISP conf)
 - Remove by hand in plugins-enabled.conf

ph-neutral3.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: tcp.stream eq 2 Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
3	0.000020	172.16.1.3	82.165.106.109	TCP	[TCP Port numbers reused] 53014 > http [SYN] Seq=0 win=5520 Len=0 MSS=1380 SACK_PERM=1 TSV=1
4	0.121083	82.165.106.109	172.16.1.3	TCP	http > 53014 [SYN, ACK] Seq=0 Ack=4294898334 win=5840 Len=0 MSS=1460 wS=7
5	0.124607	172.16.1.3	82.165.106.109	TCP	82.165.106.109:80 > 172.16.1.3:53014 [ACK] Seq=8212 Ack=4771147 Len=0
6	0.124618	172.16.1.3	82.165.106.109	TCP	82.165.106.109:80 > 172.16.1.3:53014 [ACK] Seq=8212 Ack=4771147 Len=0
7	0.124626	172.16.1.3	82.165.106.109	TCP	82.165.106.109:80 > 172.16.1.3:53014 [ACK] Seq=8212 Ack=4771147 Len=0
8	0.124633	172.16.1.3	82.165.106.109	TCP	82.165.106.109:80 > 172.16.1.3:53014 [ACK] Seq=8212 Ack=4771147 Len=0
9	0.124638	172.16.1.3	82.165.106.109	TCP	82.165.106.109:80 > 172.16.1.3:53014 [ACK] Seq=8212 Ack=4771147 Len=0
10	0.124645	172.16.1.3	82.165.106.109	TCP	82.165.106.109:80 > 172.16.1.3:53014 [ACK] Seq=8212 Ack=4771147 Len=0
11	0.124651	172.16.1.3	82.165.106.109	TCP	82.165.106.109:80 > 172.16.1.3:53014 [ACK] Seq=8212 Ack=4771147 Len=0
12	0.124658	172.16.1.3	82.165.106.109	TCP	82.165.106.109:80 > 172.16.1.3:53014 [ACK] Seq=8212 Ack=4771147 Len=0
13	0.124664	172.16.1.3	82.165.106.109	TCP	82.165.106.109:80 > 172.16.1.3:53014 [ACK] Seq=8212 Ack=4771147 Len=0
14	0.124668	172.16.1.3	82.165.106.109	TCP	82.165.106.109:80 > 172.16.1.3:53014 [ACK] Seq=8212 Ack=4771147 Len=0
15	0.124675	172.16.1.3	82.165.106.109	TCP	82.165.106.109:80 > 172.16.1.3:53014 [ACK] Seq=8212 Ack=4771147 Len=0
16	0.124679	172.16.1.3	82.165.106.109	TCP	82.165.106.109:80 > 172.16.1.3:53014 [ACK] Seq=8212 Ack=4771147 Len=0
17	0.124686	172.16.1.3	82.165.106.109	TCP	82.165.106.109:80 > 172.16.1.3:53014 [ACK] Seq=8212 Ack=4771147 Len=0
18	0.124693	172.16.1.3	82.165.106.109	TCP	82.165.106.109:80 > 172.16.1.3:53014 [ACK] Seq=8212 Ack=4771147 Len=0
19	0.124700	172.16.1.3	82.165.106.109	TCP	82.165.106.109:80 > 172.16.1.3:53014 [ACK] Seq=8212 Ack=4771147 Len=0
20	0.266234	172.16.1.3	82.165.106.109	TCP	82.165.106.109:80 > 172.16.1.3:53014 [ACK] Seq=8212 Ack=4771147 Len=0
21	0.288843	172.16.1.3	82.165.106.109	TCP	82.165.106.109:80 > 172.16.1.3:53014 [ACK] Seq=8212 Ack=4771147 Len=0

Follow TCP Stream

Stream Content

```

HTTP/1.1 200 OK
Date: Mon, 23 May 2011 11:23:42 GMT
Server: Apache
Connection: close
Content-Type: text/html

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Frameset//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-frameset.dtd">

<html>
<head>
<title>ph-neutral.darklab.org</title>
<meta name="keywords" content="" />
<meta name="description" content="" />
</head>
<frameset rows="100%">
<frame src="http://ph-neutral.darklab.org" title="ph-neutral.darklab.org" frameborder="0"
noresize="noresize"/>
</frameset>
<body>
<h1>ph-neutral.darklab.org</h1>
<p><a href="http://ph-neutral.darklab.org">http://ph-neutral.org</a></p>
</body>
</noframes>
</frameset>
</html>

```

Find Save As Print Entire conversation (665 bytes) Filter Out This Stream Close

Entire conversation (665 bytes)
172.16.1.3:53014 --> 82.165.106.109:http (0 bytes)
82.165.106.109:http --> 172.16.1.3:53014 (665 bytes)

0000 00 1e e5 92 69 0a 00 1e 8c 6d e5 19 08 00 45 00 ...i...m...E.
0010 00 28 79 6b 40 00 09 06 8e 3f ac 10 01 03 52 a5 .(yk@...?....R.
0020 6a 6d cf 16 00 50 74 37 96 88 57 c8 92 52 50 11 jm...Pt7 ..W..RP.
0030 00 2c 81 40 00 00 ...@..

File: "\\CATURDAY\linuxdisk\ph-neutral3.p... Packets: 622 Displayed: 31 Marked: 0 Load time: 0:00.055 Profile: Default

Follow TCP Stream

Stream Content

```
[-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 ESMT  
Postfix  
<CRLF>
```

Find Save As Print Entire conversation (222 bytes) ASCII EBCDIC Hex Dump C Arrays Raw

Help

Effects (hypothesis, wishes, etc...)

- Massive passive sniffing will face an escalation of complexity, like cryptography/cryptanalysis does ?
 - A skilled analyst will understand the meaning of the packets, anyway
- Transparent proxy, relayed traffic and non passive data collector, are untouched by Sj
- Pervasive use of sniffjoke, with all feature completed, will vanify every data retention strategy: how much is hard to communicate ?
 - In raw data collection, almost

Project goals for 0.5

- Collect evidence of defeated sniffers
 - IDS may or may not be present
- Found some \$/€
- Became multiplatform in unix based
 - Windows client + openwrt package
- Be stable in IP/TCP options scramble
- Support server side connections!

Links

- <http://www.delirandom.net/sniffjoke>
 - <http://www.delirandom.net/sniffjoke/0.3-release>
 - Insertion, Evasion and Denial of Service: Eluding Network Intrusion Detections (Secure Network INC, 1998)
- <http://github.com/vecna/sniffjoke>
- <http://github.com/evilaliv3/sniffjoke>
- <http://www.mail-archive.com/wireshark-dev@wireshark.org/msg13474.html>
- <http://en.roolz.org/trafscrambler.html>
- <https://twitter.com/sniffjoke>