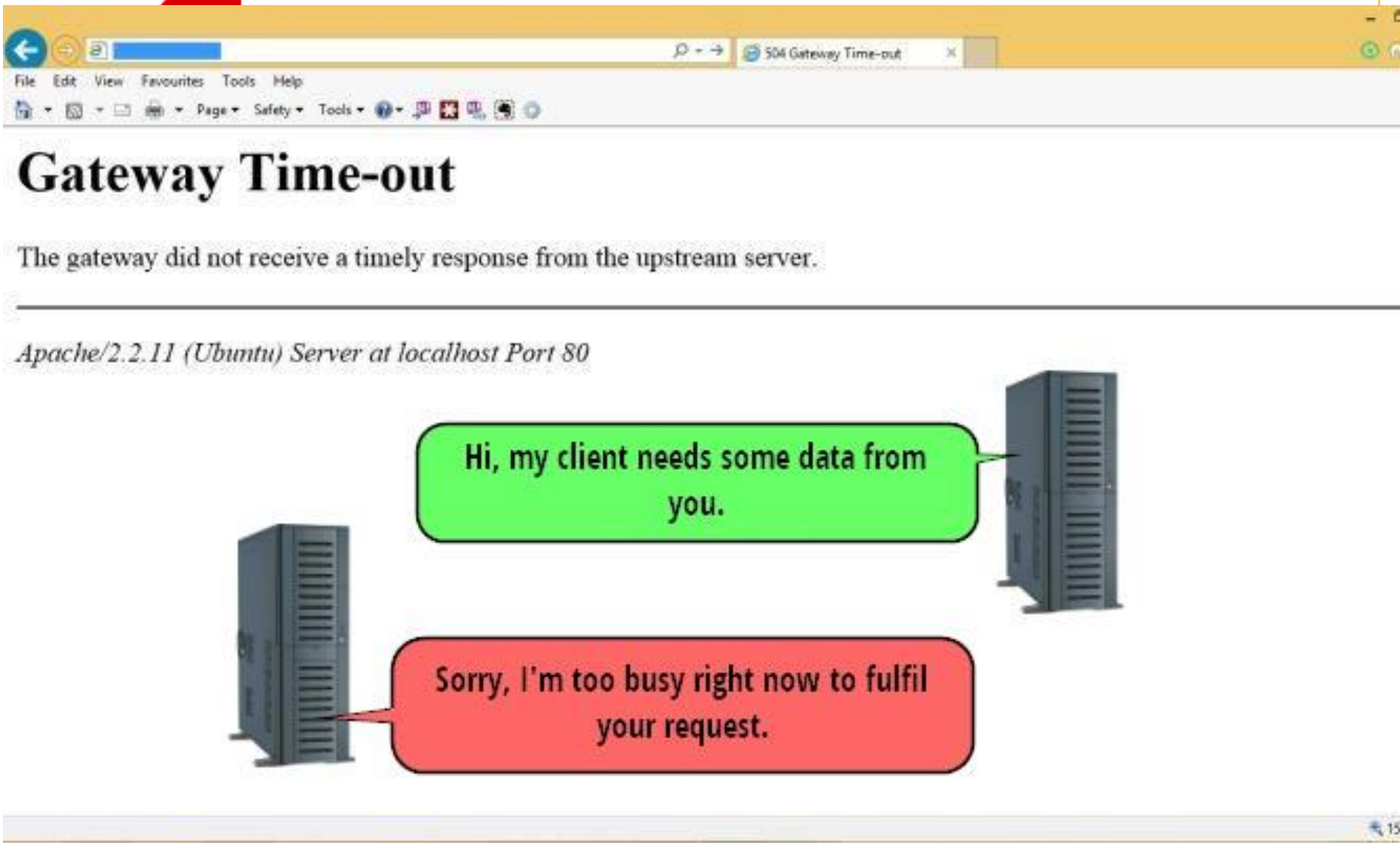
Auto-Sig-Gen

ייצור חתימות בזמן אמת: קו הגנה נוסף לסינון התקפות מניעת שרות

http://www.autosigen.com

Yehuda Afek
Shir Landau Feibish
Michal Shagam
Tel Aviv University

Anat Bremler-Barr
Golan Parashi
IDC Herzliya

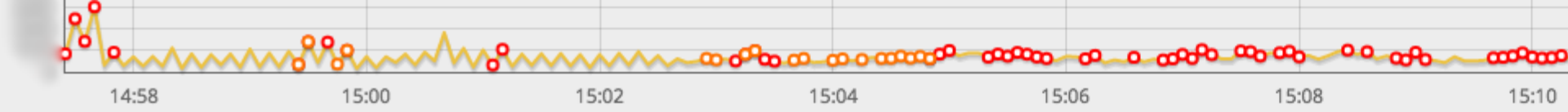

504 Gateway Time-out
File Edit View Favourites Tools Help
Page Safety Tools
Gateway Time-out
The gateway did not receive a timely response from the upstream server.
Apache/2.2.11 (Ubuntu) Server at localhost Port 80
Hi, my client needs some data from you.
Sorry, I'm too busy right now to fulfil your request.

Service Temporarily Unavailable

The server is temporarily unable to service your request due to maintenance downtime or capacity problems. Please try again later.

Apache Server at www.moha.gov.af Port 80

```
176.31.124.142 linuxthefish.net - [07/Aug/2014:19:08:49 +0200] "GET / HTTP/1.0" 200 27785 "-" "WordPress/3.9.2; http://actualites.
.49.20"
144.76.218.4 linuxthefish.net - [07/Aug/2014:19:08:49 +0200] "GET / HTTP/1.0" 200 27785 "-" "-"
195.191.24.29 linuxthefish.net - [07/Aug/2014:19:08:49 +0200] "GET / HTTP/1.0" 200 27785 "-" "WordPress/3.6.1; http://agroanimal.c
46.105.107.96 linuxthefish.net - [07/Aug/2014:19:08:49 +0200] "GET / HTTP/1.0" 200 27785 "-" "WordPress/3.5.2; http://alexthorn.xx
85.214.150.81 linuxthefish.net - [07/Aug/2014:19:08:49 +0200] "GET / HTTP/1.0" 200 27785 "-" "WordPress/3.9.1; http://avedo.net; v
184.72.231.47 linuxthefish.net - [07/Aug/2014:19:08:49 +0200] "GET / HTTP/1.0" 200 27785 "-" "WordPress/3.8.1; http://blog.decalsf
184.72.231.47 linuxthefish.net - [07/Aug/2014:19:08:49 +0200] "GET / HTTP/1.0" 200 27785 "-" "WordPress/3.8.1; http://blog.decalsf
184.72.231.47 linuxthefish.net - [07/Aug/2014:19:08:49 +0200] "GET / HTTP/1.0" 200 27785 "-" "WordPress/3.8.1; http://blog.decalsf
95.211.178.162 linuxthefish.net - [07/Aug/2014:19:08:49 +0200] "GET / HTTP/1.0" 200 27785 "-" "WordPress/3.5.1; http://anime-excee
54.255.149.123 linuxthefish.net - [07/Aug/2014:19:08:49 +0200] "GET / HTTP/1.0" 200 27785 "-" "WordPress/3.9.1; http://10000startu
20"
69.56.173.168 linuxthefish.net - [07/Aug/2014:19:08:49 +0200] "GET / HTTP/1.0" 200 27785 "-" "WordPress/3.8.2; http://damnsexychic
98"
113.192.41.4 linuxthefish.net - [07/Aug/2014:19:08:49 +0200] "GET / HTTP/1.0" 200 27785 "-" "WordPress/3.9.2; http://b2cloud.com.a
176.31.124.142 linuxthefish.net - [07/Aug/2014:19:08:49 +0200] "GET / HTTP/1.0" 200 27785 "-" "WordPress/3.9.2; http://actualites.
.49.20"
208.52.182.204 linuxthefish.net - [07/Aug/2014:19:08:49 +0200] "GET / HTTP/1.0" 200 27785 "-" "WordPress/3.9.2; http://colormemont
198"
85.214.150.81 linuxthefish.net - [07/Aug/2014:19:08:49 +0200] "GET / HTTP/1.0" 200 27785 "-" "WordPress/3.9.1; http://avedo.net; v
69.56.173.168 linuxthefish.net - [07/Aug/2014:19:08:49 +0200] "GET / HTTP/1.0" 200 27785 "-" "WordPress/3.8.2; http://damnsexychic
20"
176.58.98.229 linuxthefish.net - [07/Aug/2014:19:08:49 +0200] "GET / HTTP/1.0" 200 27785 "-" "WordPress/3.5.2; http://crayondata.c
81.169.243.196 linuxthefish.net - [07/Aug/2014:19:08:49 +0200] "GET / HTTP/1.0" 200 27785 "-" "WordPress/2.9.2; http://apetitgalle
83.138.243.108 forum.hostinganl.net - [07/Aug/2014:19:08:49 +0200] "GET /index.php?action=portal;sa=shoutbox;shoutbox_id=1;time=14
rum.hostinganl.net/index.php" "Mozilla/5.0 (Windows NT 5.1; rv:31.0) Gecko/20100101 Firefox/31.0"
144.76.39.151 linuxthefish.net - [07/Aug/2014:19:08:49 +0200] "GET / HTTP/1.0" 200 27785 "-" "WordPress/3.8.4; http://actionshop.m
.59.96.198"
184.72.231.47 linuxthefish.net - [07/Aug/2014:19:08:49 +0200] "GET / HTTP/1.0" 200 27785 "-" "WordPress/3.8.1; http://blog.decalsf
83.168.248.239 linuxthefish.net - [07/Aug/2014:19:08:49 +0200] "GET / HTTP/1.0" 200 27785 "-" "WordPress/3.9.2; http://blogozine.s
69.56.173.168 linuxthefish.net - [07/Aug/2014:19:08:49 +0200] "GET / HTTP/1.0" 200 27785 "-" "WordPress/3.8.2; http://damnsexychic
20"
184.72.231.47 linuxthefish.net - [07/Aug/2014:19:08:49 +0200] "GET / HTTP/1.0" 200 27785 "-" "WordPress/3.8.1; http://blog.decalsf
184.72.231.47 linuxthefish.net - [07/Aug/2014:19:08:49 +0200] "GET / HTTP/1.0" 200 27785 "-" "WordPress/3.8.1; http://blog.decalsf
37.59.65.87 linuxthefish.net - [07/Aug/2014:19:08:49 +0200] "GET / HTTP/1.0" 200 27785 "-" "WordPress/3.9.2; http://complexogeek.c
54.255.149.123 linuxthefish.net - [07/Aug/2014:19:08:49 +0200] "GET / HTTP/1.0" 200 27785 "-" "WordPress/3.9.1; http://10000startu
98"
46.4.19.76 linuxthefish.net - [07/Aug/2014:19:08:49 +0200] "GET / HTTP/1.0" 200 27785 "-" "WordPress/3.9.1; http://blog.fm-arena.c
69.195.222.132 linuxthefish.net - [07/Aug/2014:19:08:49 +0200] "GET / HTTP/1.0" 200 27785 "-" "WordPress/3.9.2; http://blog.doh.ms
184.72.231.47 linuxthefish.net - [07/Aug/2014:19:08:49 +0200] "GET / HTTP/1.0" 200 27785 "-" "WordPress/3.8.1; http://blog.decalsf
184.72.231.47 linuxthefish.net - [07/Aug/2014:19:08:49 +0200] "GET / HTTP/1.0" 200 27785 "-" "WordPress/3.8.1; http://blog.decalsf
50.56.182.44 linuxthefish.net - [07/Aug/2014:19:08:49 +0200] "GET / HTTP/1.0" 200 27785 "-" "WordPress/3.3; http://archive.reclaim
69.56.173.168 linuxthefish.net - [07/Aug/2014:19:08:49 +0200] "GET / HTTP/1.0" 200 27785 "-" "WordPress/3.8.2; http://damnsexychic
20"
162.220.6.187 linuxthefish.net - [07/Aug/2014:19:08:49 +0200] "GET / HTTP/1.0" 200 27785 "-" "WordPress/3.8.1; http://162.220.6.18
108.174.55.39 linuxthefish.net - [07/Aug/2014:19:08:50 +0200] "GET / HTTP/1.0" 200 27785 "-" "WordPress/3.9.1; http://beatproducti
20"
```

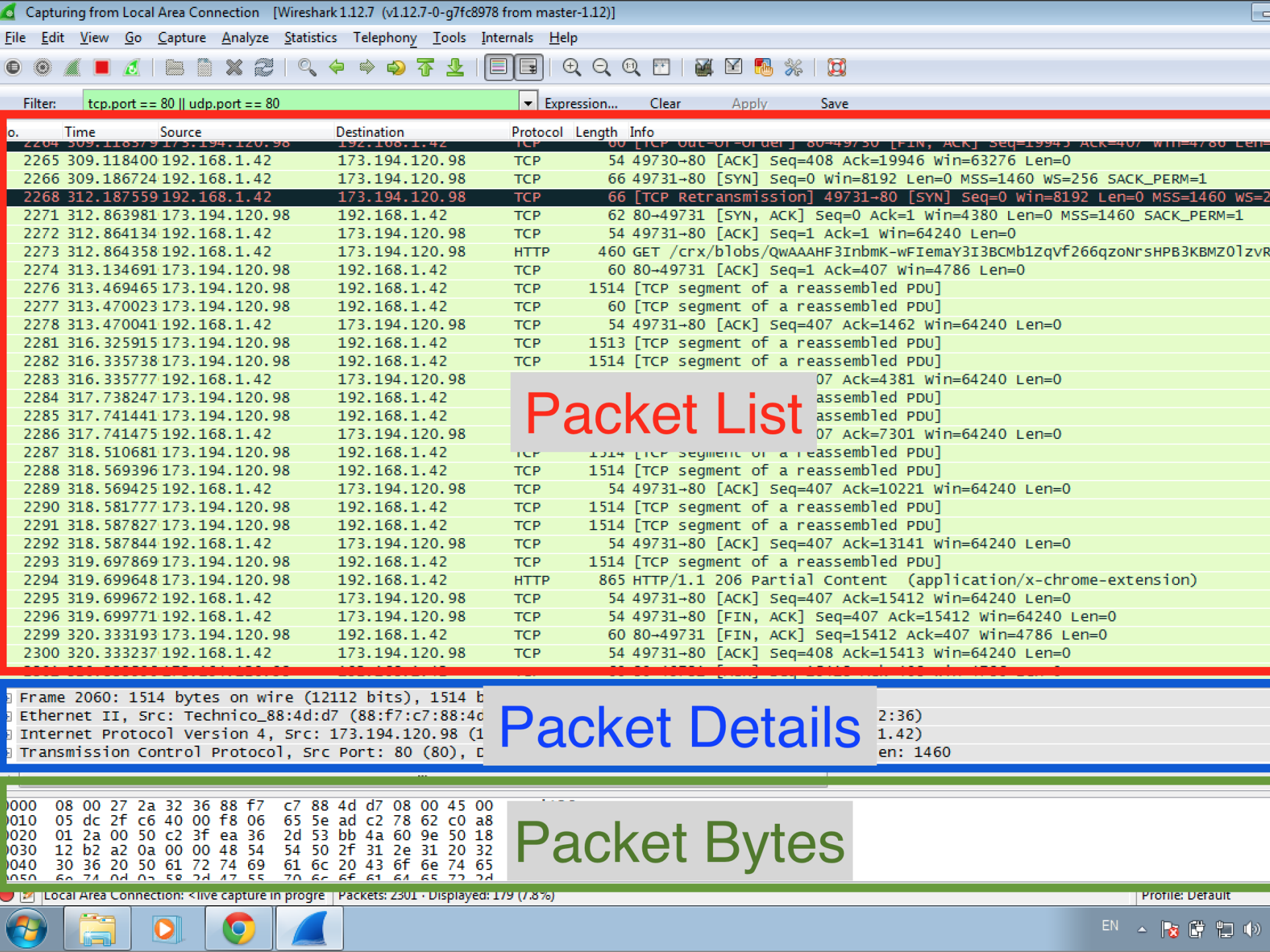


All

» 30 Nov 2015 14:57:28.043 <14>1 2015-11-30T14:57:27.961057Z - - - hostname= appname= [INFO] [2015-11-30 1
{"type":"HystrixCommand","name":"","group":"leserver","currentTime":1448895447725,"isCircuitBreake
gCountCollapsedRequests":0,"rollingCountExceptionsThrown":0,"rollingCountFailure":0,"rollingCountFallbackFailure":0,"rollingCount
esFromCache":0,"rollingCountSemaphoreRejected":0,"rollingCountShortCircuited":0,"rollingCountSuccess":0,"rollingCountThreadPoolRe
tencyExecute_mean":0,"latencyExecute":{"0":0,"25":0,"50":0,"75":0,"90":0,"95":0,"99":0,"99.5":0,"100":0},"latencyTotal_mean":0,"la
{"0":0,"25":0,"50":0,"75":0,"90":0,"95":0,"99":0,"99.5":0,"100":0},"propertyValue_circuitBreakerRequestVolumeThreshold":10,"prope
cuitBreakerErrorThresholdPercentage":50,"propertyValue_circuitBreakerForceOpen":false,"propertyValue_circuitBreakerForceClosed":fa
solationStrategy":"THREAD","propertyValue_executionIsolationThreadTimeoutInMilliseconds":5000,"propertyValue_executionIsolationTh
eyOverride":null,"propertyValue_executionIsolationSemaphoreMaxConcurrentRequests":10,"propertyValue_fallbackIsolationSemaphoreMax
lliseconds":10000,"propertyValue_requestCacheEnabled":true,"propertyValue_requestLogEnabled":true,"reportingHosts":1} /rest

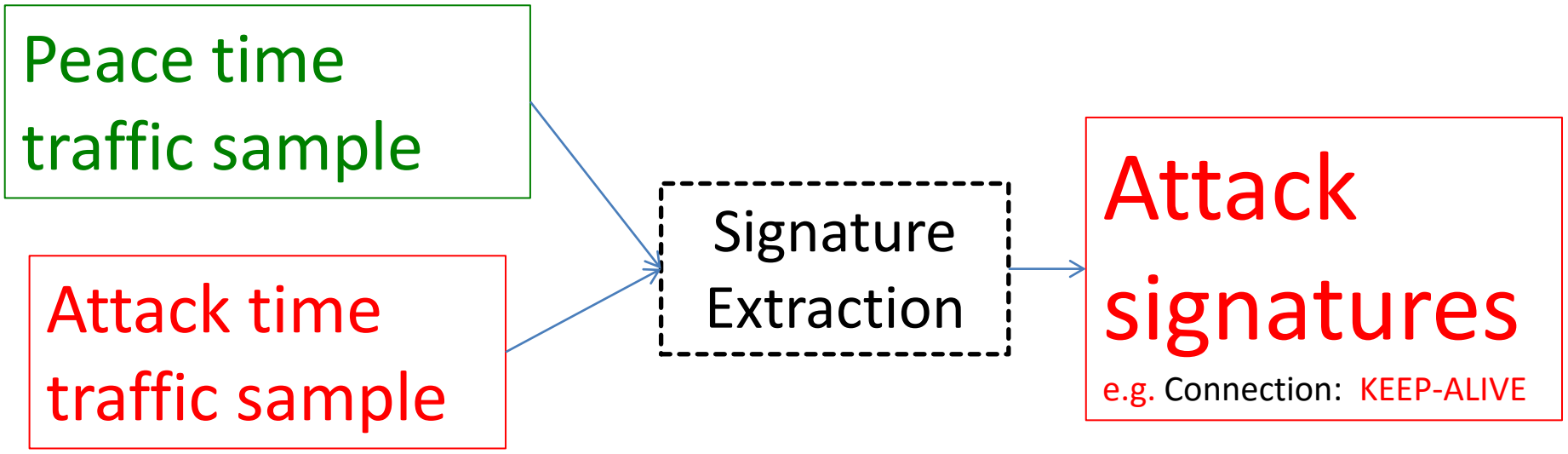
» 30 Nov 2015 14:57:28.043 <14>1 2015-11-30T14:57:27.961097Z - - - hostname= appname= [INFO] [2015-11-30 1
{"type":"HystrixCommand","name":"","group":"leserver","currentTime":1448895447725,"isCircuitBreakerOpen":false,
sedRequests":0,"rollingCountExceptionsThrown":0,"rollingCountFailure":0,"rollingCountFallbackFailure":0,"rollingCountFallbackRejec
:0,"rollingCountSemaphoreRejected":0,"rollingCountShortCircuited":0,"rollingCountSuccess":25,"rollingCountThreadPoolRejected":0,"
e_mean":12,"latencyExecute":{"0":6,"25":8,"50":10,"75":12,"90":17,"95":21,"99":71,"99.5":76,"100":76},"latencyTotal_mean":12,"late
{"0":6,"25":8,"50":10,"75":12,"90":17,"95":21,"99":71,"99.5":76,"100":76},"propertyValue_circuitBreakerRequestVolumeThreshold":10,
lue_circuitBreakerErrorThresholdPercentage":50,"propertyValue_circuitBreakerForceOpen":false,"propertyValue_circuitBreakerForceCl
cutionIsolationStrategy":"THREAD","propertyValue_executionIsolationThreadTimeoutInMilliseconds":15000,"propertyValue_executionIsol
eadPoolKeyOverride":null,"propertyValue_executionIsolationSemaphoreMaxConcurrentRequests":10,"propertyValue_fallbackIsolationSemap
ndowInMilliseconds":10000,"propertyValue_requestCacheEnabled":true,"propertyValue_requestLogEnabled":true,"reportingHosts":1}

» 30 Nov 2015 14:57:28.043 <14>1 2015-11-30T14:57:27.961109Z - - - hostname= appname= [INFO] [2015-11-30 1
{"type":"HystrixCommand","name":"","group":"leserver","currentTime":1448895447725,"isCircuitBreakerOpen":fal
apsedRequests":0,"rollingCountExceptionsThrown":0,"rollingCountFailure":0,"rollingCountFallbackFailure":0,"rollingCountFallbackRe
e":0,"rollingCountSemaphoreRejected":0,"rollingCountShortCircuited":0,"rollingCountSuccess":0,"rollingCountThreadPoolRejected":0,"
te_mean":19,"latencyExecute":{"0":8,"25":11,"50":15,"75":25,"90":53,"95":65,"99":65,"99.5":65,"100":65},"latencyTotal_mean":19,"la
{"0":8,"25":11,"50":15,"75":25,"90":53,"95":65,"99":65,"99.5":65,"100":65},"propertyValue_circuitBreakerRequestVolumeThreshold":10
alue_circuitBreakerErrorThresholdPercentage":50,"propertyValue_circuitBreakerForceOpen":false,"propertyValue_circuitBreakerForceCl
ecutionIsolationStrategy":"THREAD","propertyValue_executionIsolationThreadTimeoutInMilliseconds":5000,"propertyValue_executionIsol
eadPoolKeyOverride":null,"propertyValue_executionIsolationSemaphoreMaxConcurrentRequests":10,"propertyValue_fallbackIsolationSemap


Capturing from Local Area Connection [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: tcp.port == 80 || udp.port == 80
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
2265 309.118400 192.168.1.42 173.194.120.98 TCP 54 49730→80 [ACK] Seq=408 Ack=19946 Win=63276 Len=0
2266 309.186724 192.168.1.42 173.194.120.98 TCP 66 49731→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2268 312.187559 192.168.1.42 173.194.120.98 TCP 66 [TCP Retransmission] 49731→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
2271 312.863981 173.194.120.98 192.168.1.42 TCP 62 80→49731 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 SACK_PERM=1
2272 312.864134 192.168.1.42 173.194.120.98 TCP 54 49731→80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
2273 312.864358 192.168.1.42 173.194.120.98 HTTP 460 GET /crx/blobs/QwAAAHF3InbmK-wFIemaY3I3BCMb1ZqVf266qzoNrsHPB3KBMZOlzvR
2274 313.134691 173.194.120.98 192.168.1.42 TCP 60 80→49731 [ACK] Seq=1 Ack=407 Win=4786 Len=0
2276 313.469465 173.194.120.98 192.168.1.42 TCP 1514 [TCP segment of a reassembled PDU]
2277 313.470023 173.194.120.98 192.168.1.42 TCP 60 [TCP segment of a reassembled PDU]
2278 313.470041 192.168.1.42 173.194.120.98 TCP 54 49731→80 [ACK] Seq=407 Ack=1462 Win=64240 Len=0
2281 316.325915 173.194.120.98 192.168.1.42 TCP 1513 [TCP segment of a reassembled PDU]
2282 316.335738 173.194.120.98 192.168.1.42 TCP 1514 [TCP segment of a reassembled PDU]
2283 316.335777 192.168.1.42 173.194.120.98 07 Ack=4381 Win=64240 Len=0
2284 317.738247 173.194.120.98 192.168.1.42 assembled PDU]
2285 317.741441 173.194.120.98 192.168.1.42 assembled PDU]
2286 317.741475 192.168.1.42 173.194.120.98 07 Ack=7301 Win=64240 Len=0
2287 318.510681 173.194.120.98 192.168.1.42 reassembled PDU]
2288 318.569396 173.194.120.98 192.168.1.42 TCP 1514 [TCP segment of a reassembled PDU]
2289 318.569425 192.168.1.42 173.194.120.98 TCP 54 49731→80 [ACK] Seq=407 Ack=10221 Win=64240 Len=0
2290 318.581777 173.194.120.98 192.168.1.42 TCP 1514 [TCP segment of a reassembled PDU]
2291 318.587827 173.194.120.98 192.168.1.42 TCP 1514 [TCP segment of a reassembled PDU]
2292 318.587844 192.168.1.42 173.194.120.98 TCP 54 49731→80 [ACK] Seq=407 Ack=13141 Win=64240 Len=0
2293 319.697869 173.194.120.98 192.168.1.42 TCP 1514 [TCP segment of a reassembled PDU]
2294 319.699648 173.194.120.98 192.168.1.42 HTTP 865 HTTP/1.1 206 Partial Content (application/x-chrome-extension)
2295 319.699672 192.168.1.42 173.194.120.98 TCP 54 49731→80 [ACK] Seq=407 Ack=15412 Win=64240 Len=0
2296 319.699771 192.168.1.42 173.194.120.98 TCP 54 49731→80 [FIN, ACK] Seq=407 Ack=15412 Win=64240 Len=0
2299 320.333193 173.194.120.98 192.168.1.42 TCP 60 80→49731 [FIN, ACK] Seq=15412 Ack=407 Win=4786 Len=0
2300 320.333237 192.168.1.42 173.194.120.98 TCP 54 49731→80 [ACK] Seq=408 Ack=15413 Win=64240 Len=0
Packet List
Frame 2060: 1514 bytes on wire (12112 bits), 1514 b
Ethernet II, Src: Technico_88:4d:d7 (88:f7:c7:88:4c 2:36)
Internet Protocol Version 4, Src: 173.194.120.98 (1 1.42)
Transmission Control Protocol, Src Port: 80 (80), D en: 1460
Packet Details
0000 08 00 27 2a 32 36 88 f7 c7 88 4d d7 08 00 45 00
0010 05 dc 2f c6 40 00 f8 06 65 5e ad c2 78 62 c0 a8
0020 01 2a 00 50 c2 3f ea 36 2d 53 bb 4a 60 9e 50 18
0030 12 b2 a2 0a 00 00 48 54 54 50 2f 31 2e 31 20 32
0040 30 36 20 50 61 72 74 69 61 6c 20 43 6f 6e 74 65
Packet Bytes
Local Area Connection: <live capture in progre
Packets: 2301 · Displayed: 179 (7.8%)
Profile: Default
EN

Signature Extraction: DDoS attacks

Our Challenge: Automatically find signatures that frequently appear only in attack packets



Two use-cases

1. Forensic analysis after the attack

2. In real time to stop the attack

** In tests on a VM.

** 200Mbps – 1Gbps MacBook pro with a small memory footprint (<100M).

Signature Extraction: DDoS attacks

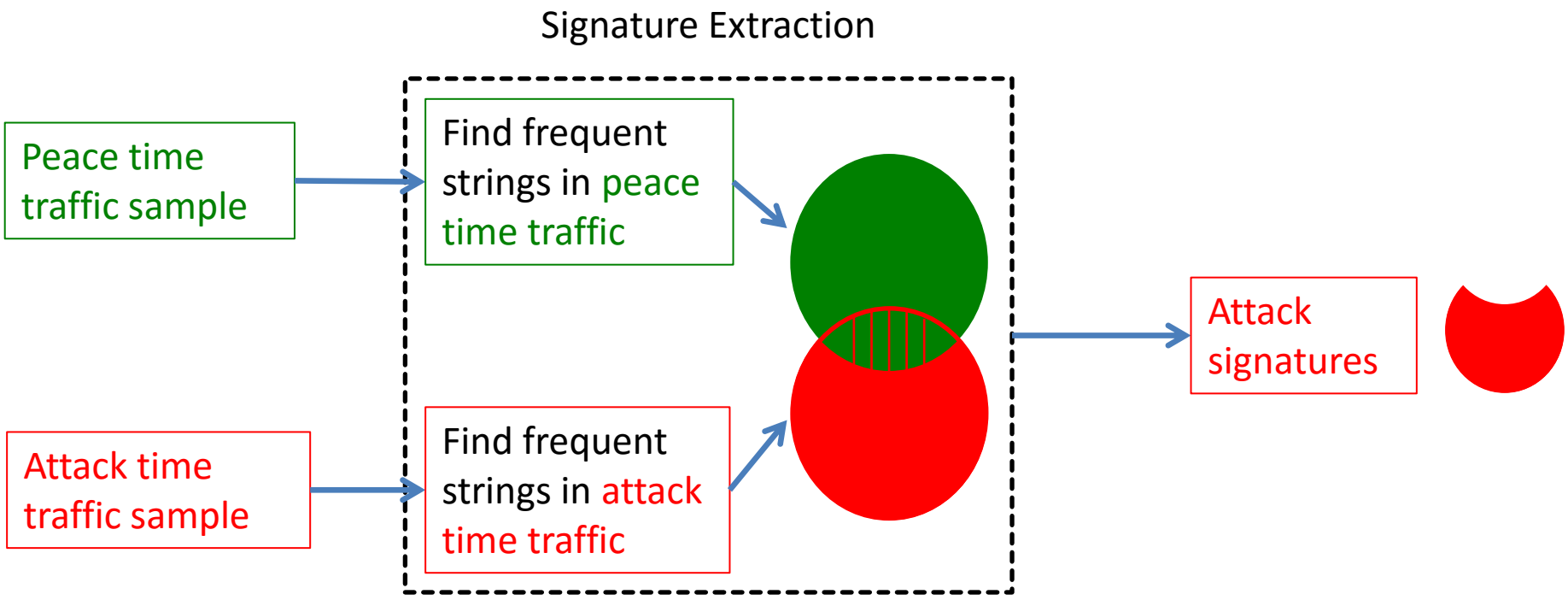
Requirements

1. Allow signatures of varying lengths
2. Don't include signatures found in legitimate traffic
   - Minimum false positives
3. Find minimal set of signatures
   - Some filtering devices have limited capacity
4. Streaming solution:
   - Minimize space requirements
   - Wire speed

Demo

http://www.autosigen.com

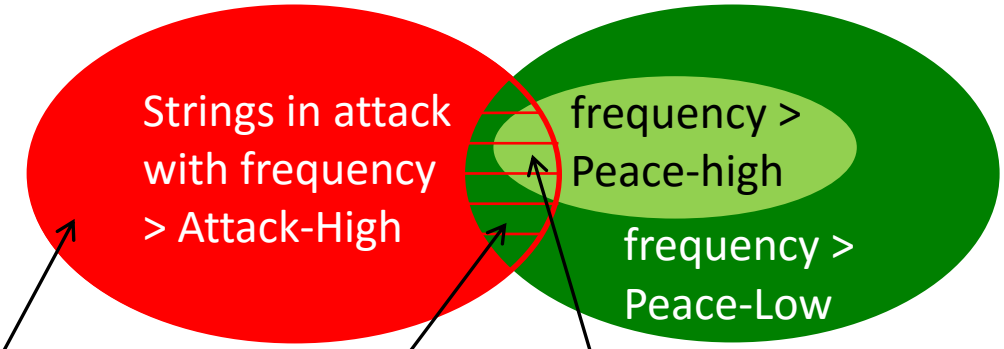
Signature Extraction - High Level



Choosing Signatures

Create signatures that may appear in legitimate traffic, but appear in attack traffic much more

Thresholds:
Attack-high
Peace-low
Peace-high
Delta



Signatures

Signatures only if attack frequency at least delta more than peace frequency

False positives

Signatures

Signature frequency:
71% 65% 45% 35%

Packet types

Packet type 1: … bad…guy…

Packet type 2: …really… bad…guy…

Packet type 3: … mean…guy…

Packet type 4: … really…bad…

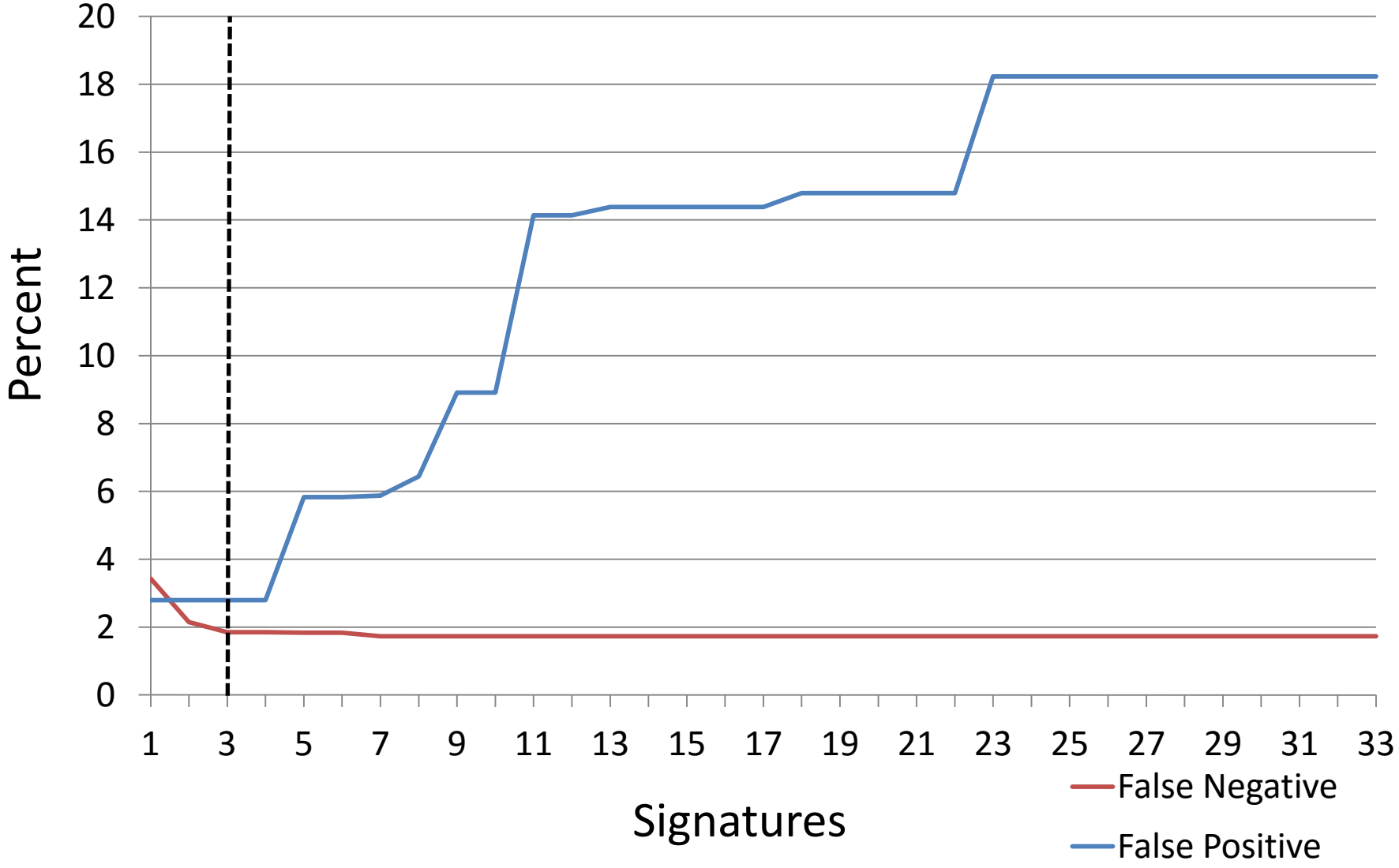
Packet type 5: bad…mean… guy…

Packet type 6: … bad…

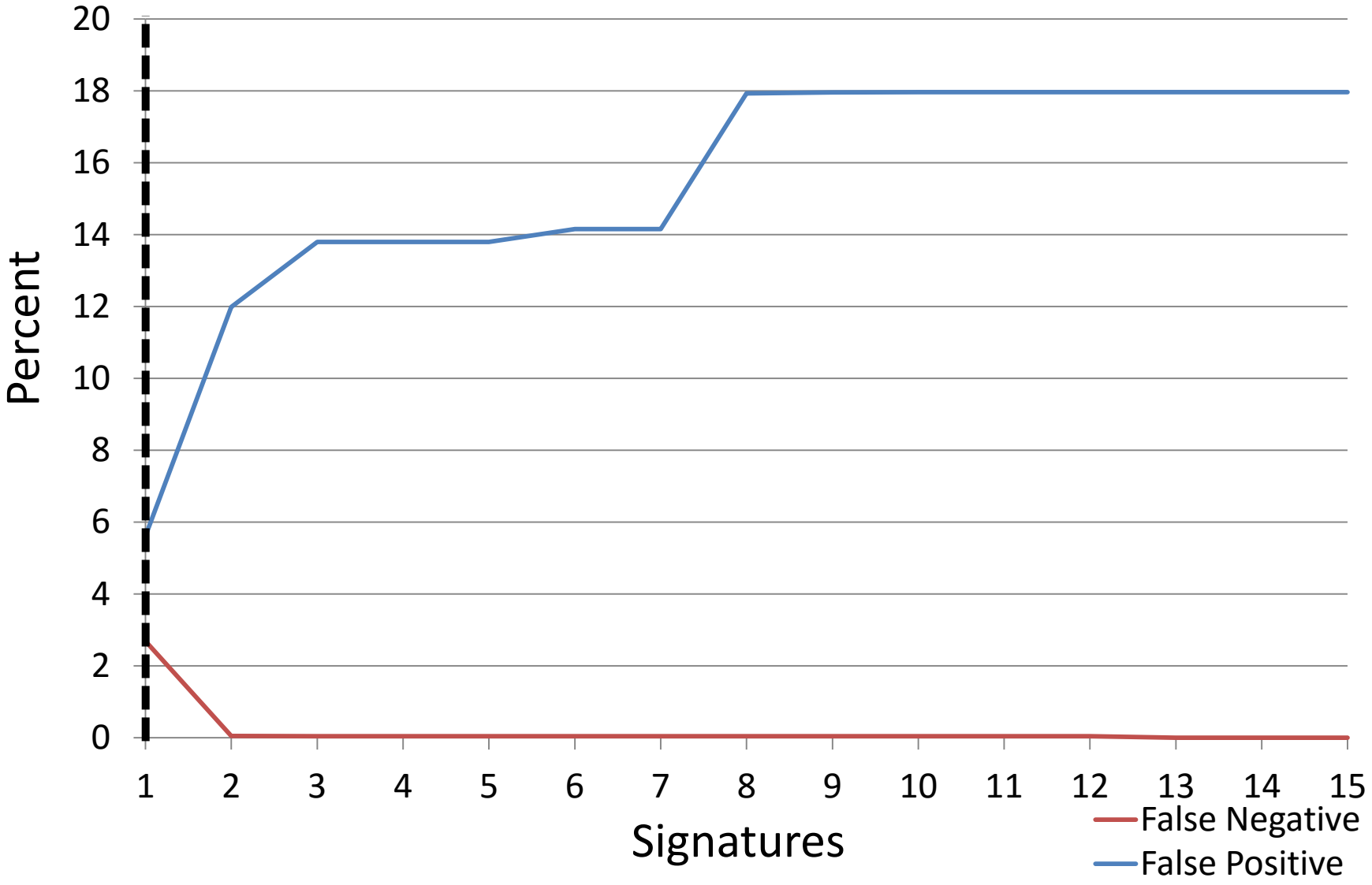
Packet type frequency:	bad	guy	really	mean
10%	✓	✓		
20%	✓	✓	✓	
20%		✓		✓
25%	✓		✓	
15%	✓	✓		✓
1%	✓			

guy & really

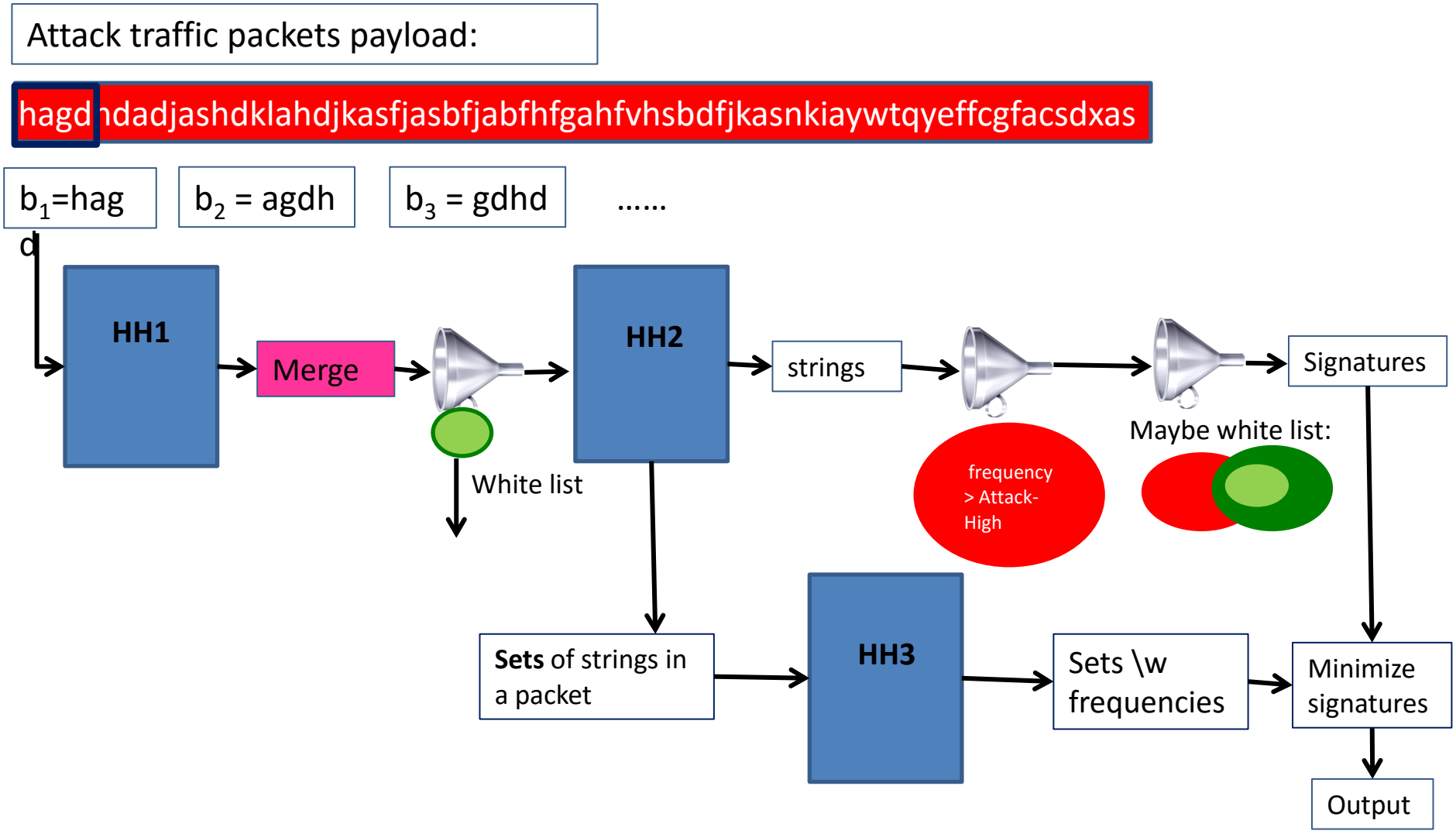
Minimizing the number of signatures

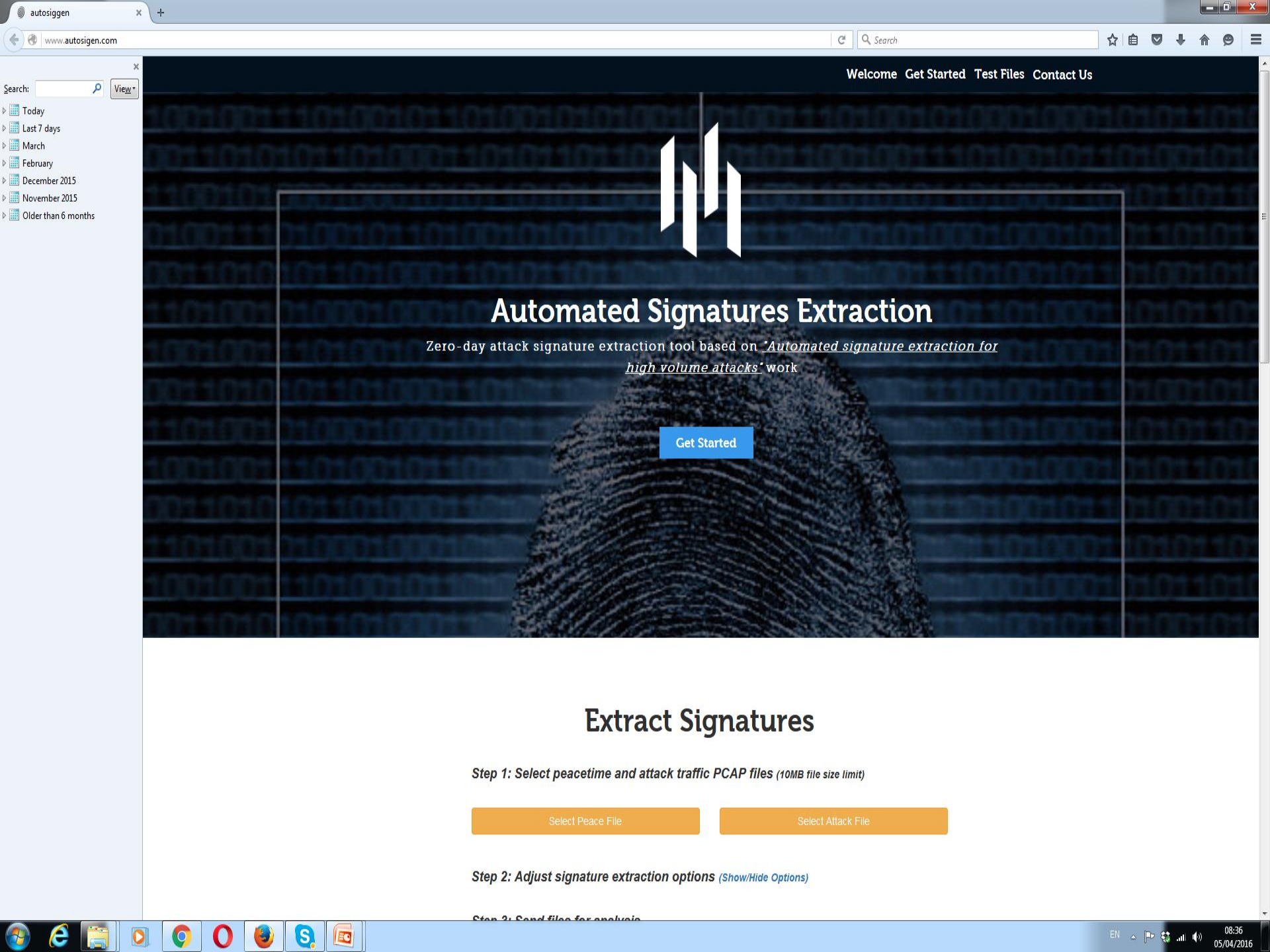


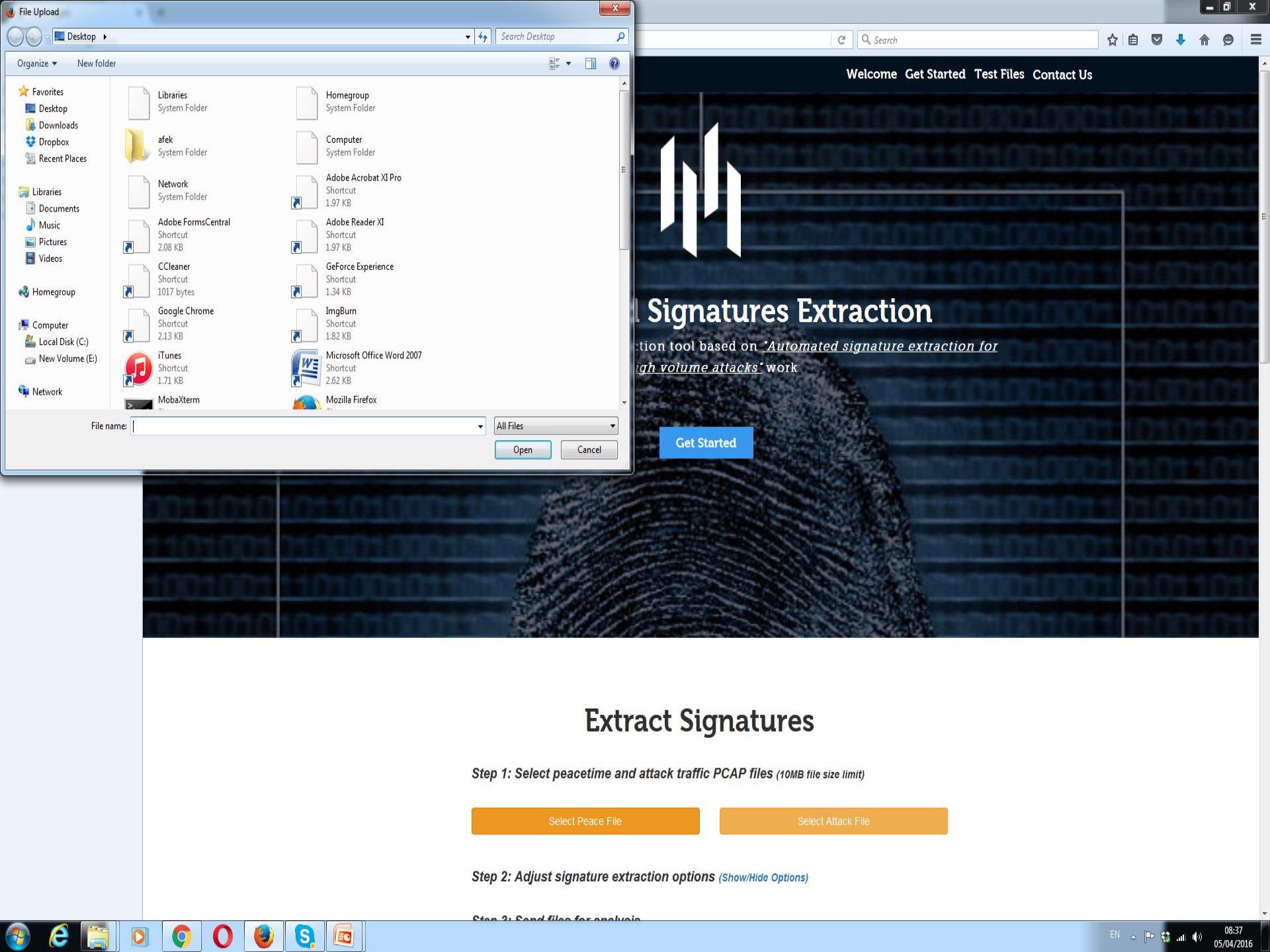
Minimizing the number of signatures

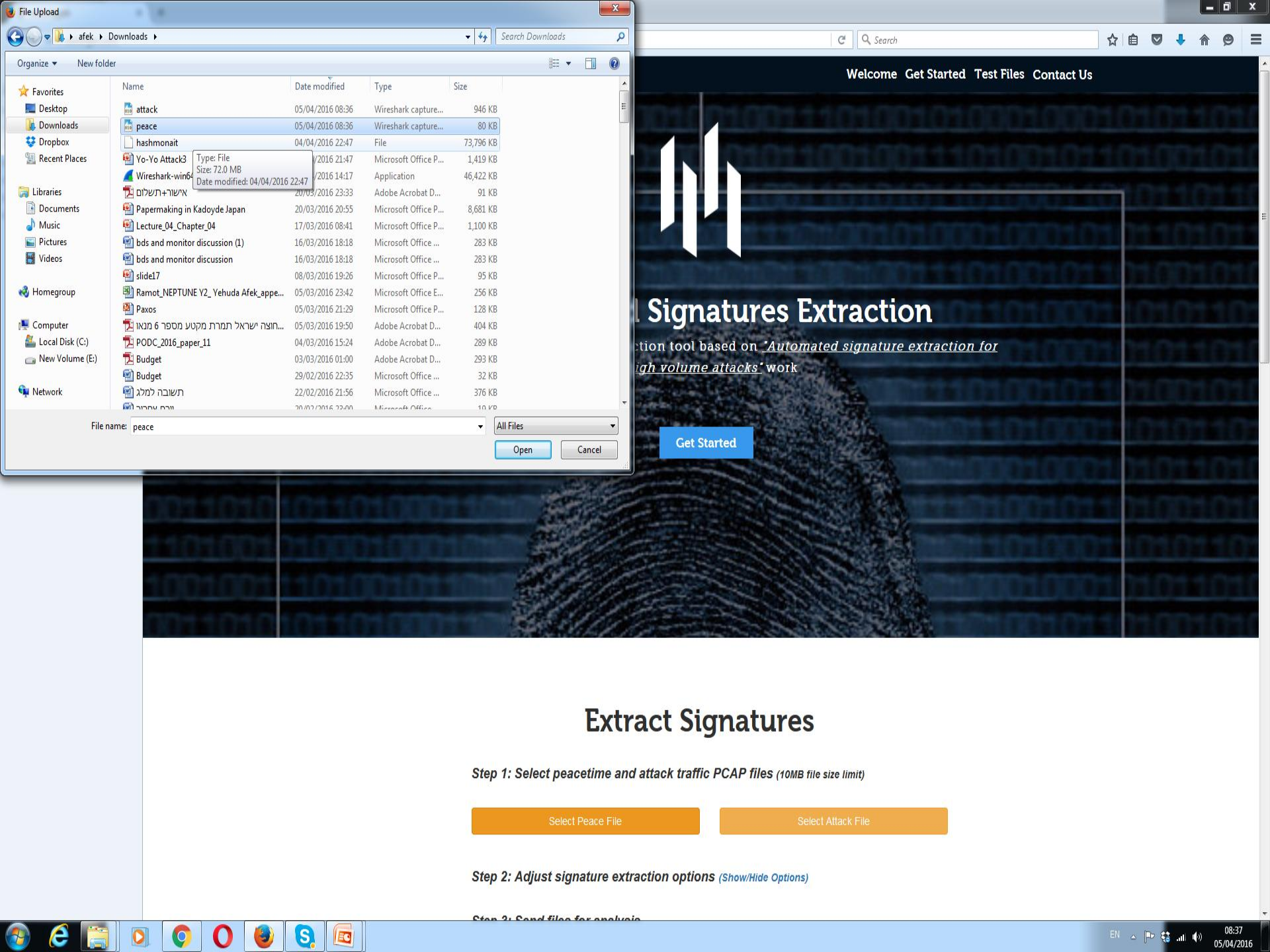


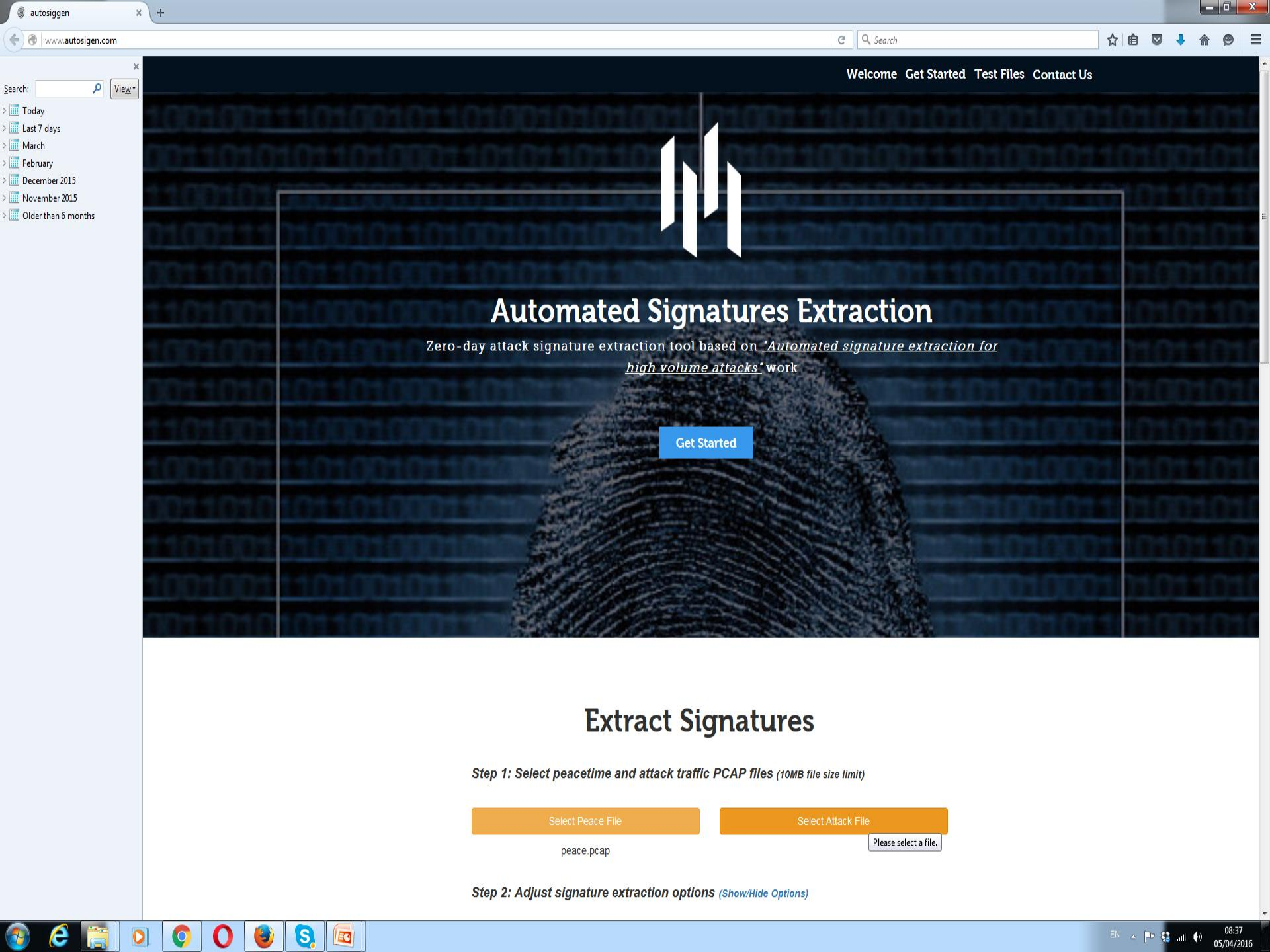
Signature Extraction - Architecture

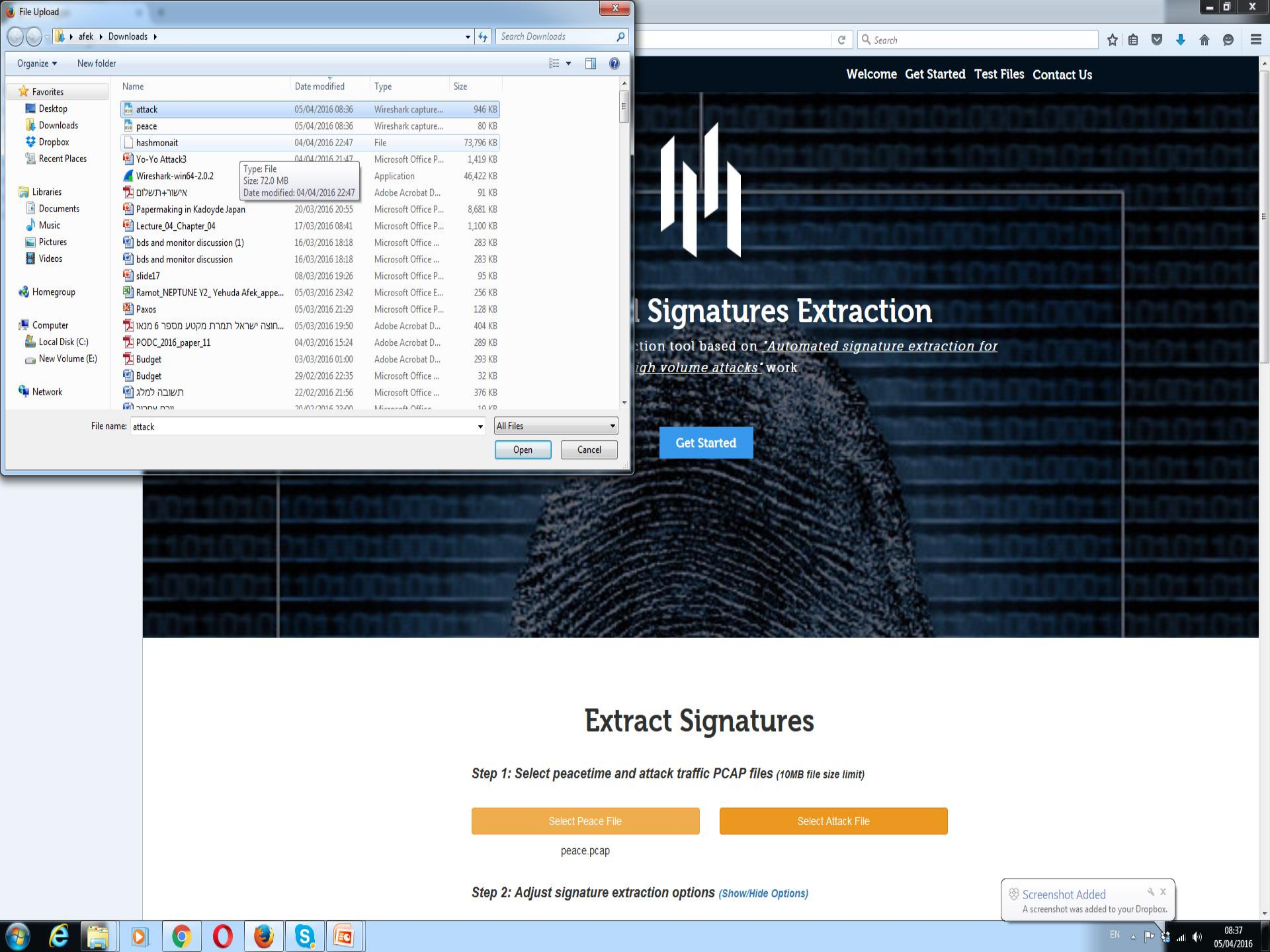



autosiggen
www.autosigen.com
Search
Search:
View
Today
Last 7 days
March
February
December 2015
November 2015
Older than 6 months
Welcome
Get Started
Test Files
Contact Us
Automated Signatures Extraction
Zero-day attack signature extraction tool based on "Automated signature extraction for high volume attacks" work
Get Started
Extract Signatures
Step 1: Select peacetime and attack traffic PCAP files (10MB file size limit)
Select Peace File
Select Attack File
Step 2: Adjust signature extraction options (Show/Hide Options)
EN
08:36
05/04/2016


File Upload
Desktop
Search Desktop
Organize
New folder
Favorites
Desktop
Downloads
Dropbox
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
Computer
Local Disk (C:)
New Volume (E:)
Network
Libraries
System Folder
Homegroup
System Folder
afek
System Folder
Computer
System Folder
Network
System Folder
Adobe Acrobat XI Pro
Shortcut
1.97 KB
Adobe FormsCentral
Shortcut
2.08 KB
Adobe Reader XI
Shortcut
1.97 KB
CCleaner
Shortcut
1017 bytes
GeForce Experience
Shortcut
1.34 KB
Google Chrome
Shortcut
2.13 KB
ImgBurn
Shortcut
1.82 KB
iTunes
Shortcut
1.71 KB
Microsoft Office Word 2007
Shortcut
2.62 KB
MobaXterm
Mozilla Firefox
File name:
All Files
Open
Cancel
Search
Welcome
Get Started
Test Files
Contact Us
Signatures Extraction
tion tool based on "Automated signature extraction for
igh volume attacks" work
Get Started
Extract Signatures
Step 1: Select peacetime and attack traffic PCAP files (10MB file size limit)
Select Peace File
Select Attack File
Step 2: Adjust signature extraction options (Show/Hide Options)
EN
08:37
05/04/2016


File Upload
afek ▸ Downloads ▸
Search Downloads
Organize
New folder
Favorites
Desktop
Downloads
Dropbox
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
Computer
Local Disk (C:)
New Volume (E:)
Network
Name
Date modified
Type
Size
attack 05/04/2016 08:36 Wireshark capture... 946 KB
peace 05/04/2016 08:36 Wireshark capture... 80 KB
hashmonait 04/04/2016 22:47 File 73,796 KB
Yo-Yo Attack3 Microsoft Office P... 1,419 KB
Wireshark-win64 Application 46,422 KB
אישור+תשלום Adobe Acrobat D... 91 KB
Papermaking in Kadoyde Japan 20/03/2016 20:55 Microsoft Office P... 8,681 KB
Lecture_04_Chapter_04 17/03/2016 08:41 Microsoft Office P... 1,100 KB
bds and monitor discussion (1) 16/03/2016 18:18 Microsoft Office ... 283 KB
bds and monitor discussion 16/03/2016 18:18 Microsoft Office ... 283 KB
slide17 08/03/2016 19:26 Microsoft Office P... 95 KB
Ramot_NEPTUNE Y2_ Yehuda Afek_appe... 05/03/2016 23:42 Microsoft Office E... 256 KB
Paxos 05/03/2016 21:29 Microsoft Office P... 128 KB
חוצה ישראל תמרת מקטע מספר 6 מנאו... 05/03/2016 19:50 Adobe Acrobat D... 404 KB
PODC_2016_paper_11 04/03/2016 15:24 Adobe Acrobat D... 289 KB
Budget 03/03/2016 01:00 Adobe Acrobat D... 293 KB
Budget 29/02/2016 22:35 Microsoft Office ... 32 KB
תשובה למלג 22/02/2016 21:56 Microsoft Office ... 376 KB
Type: File
Size: 72.0 MB
Date modified: 04/04/2016 22:47
File name: peace
All Files
Open
Cancel
Search
Welcome
Get Started
Test Files
Contact Us
Signatures Extraction
tion tool based on "Automated signature extraction for
igh volume attacks" work
Get Started
Extract Signatures
Step 1: Select peacetime and attack traffic PCAP files (10MB file size limit)
Select Peace File
Select Attack File
Step 2: Adjust signature extraction options (Show/Hide Options)
EN
08:37
05/04/2016


autosiggen
www.autosigen.com
Search
Search:
View
Today
Last 7 days
March
February
December 2015
November 2015
Older than 6 months
Welcome
Get Started
Test Files
Contact Us
Automated Signatures Extraction
Zero-day attack signature extraction tool based on "Automated signature extraction for high volume attacks" work
Get Started
Extract Signatures
Step 1: Select peacetime and attack traffic PCAP files (10MB file size limit)
Select Peace File
Select Attack File
Please select a file.
peace.pcap
Step 2: Adjust signature extraction options (Show/Hide Options)
EN
08:37
05/04/2016


File Upload
afek ▸ Downloads ▸
Search Downloads
Organize
New folder
Favorites
Desktop
Downloads
Dropbox
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
Computer
Local Disk (C:)
New Volume (E:)
Network
Name
Date modified
Type
Size
attack 05/04/2016 08:36 Wireshark capture... 946 KB
peace 05/04/2016 08:36 Wireshark capture... 80 KB
hashmonait 04/04/2016 22:47 File 73,796 KB
Yo-Yo Attack3 Microsoft Office P... 1,419 KB
Wireshark-win64-2.0.2 Application 46,422 KB
אישור+תשלום Adobe Acrobat D... 91 KB
Papermaking in Kadoyde Japan 20/03/2016 20:55 Microsoft Office P... 8,681 KB
Lecture_04_Chapter_04 17/03/2016 08:41 Microsoft Office P... 1,100 KB
bds and monitor discussion (1) 16/03/2016 18:18 Microsoft Office ... 283 KB
bds and monitor discussion 16/03/2016 18:18 Microsoft Office ... 283 KB
slide17 08/03/2016 19:26 Microsoft Office P... 95 KB
Ramot_NEPTUNE Y2_ Yehuda Afek_appe... 05/03/2016 23:42 Microsoft Office E... 256 KB
Paxos 05/03/2016 21:29 Microsoft Office P... 128 KB
חוצה ישראל תמרת מקטע מספר 6 מנאו... 05/03/2016 19:50 Adobe Acrobat D... 404 KB
PODC_2016_paper_11 04/03/2016 15:24 Adobe Acrobat D... 289 KB
Budget 03/03/2016 01:00 Adobe Acrobat D... 293 KB
Budget 29/02/2016 22:35 Microsoft Office ... 32 KB
תשובה למלג 22/02/2016 21:56 Microsoft Office ... 376 KB
Type: File
Size: 72.0 MB
Date modified: 04/04/2016 22:47
File name: attack
All Files
Open
Cancel
Search
Welcome
Get Started
Test Files
Contact Us
Signatures Extraction
tion tool based on "Automated signature extraction for
gh volume attacks" work
Get Started
Extract Signatures
Step 1: Select peacetime and attack traffic PCAP files (10MB file size limit)
Select Peace File
Select Attack File
peace.pcap
Step 2: Adjust signature extraction options (Show/Hide Options)
Screenshot Added
A screenshot was added to your Dropbox.
EN
08:37
05/04/2016

Extract Signatures

***Step 1: Select peacetime and attack traffic PCAP files** (10MB file size limit)*

Select Peace File

peace.pcap

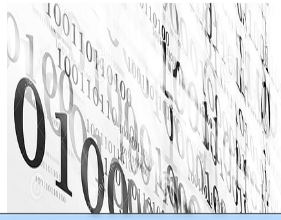
Select Attack File

attack.pcap

***Step 2: Adjust signature extraction options** (Show/Hide Options)*

Step 3: Send files for analysis

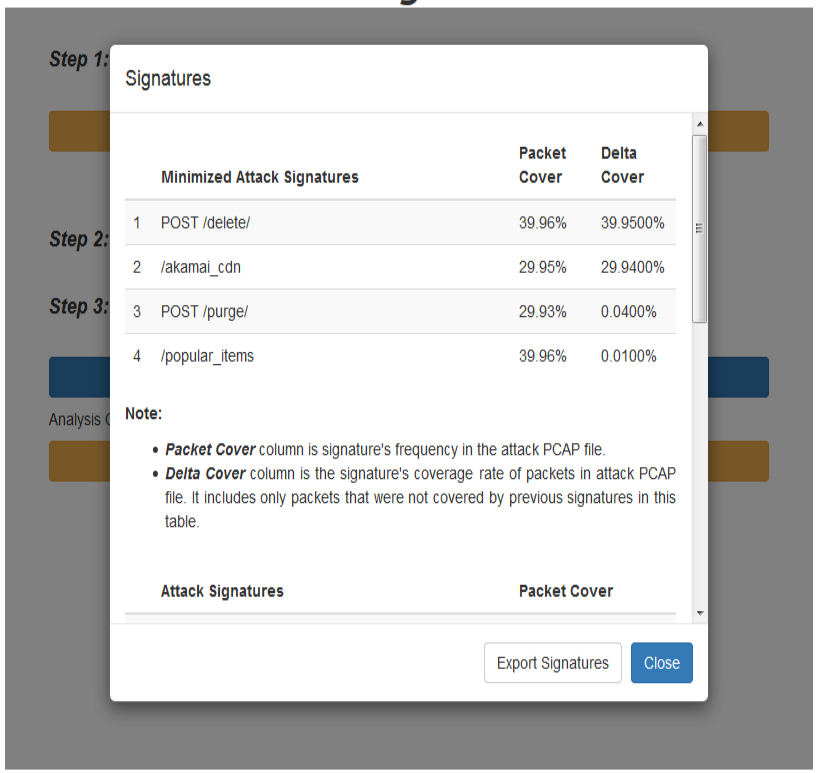
Extract Signatures

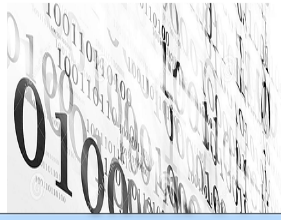


Synthetic Test Files

- Following are sample synthetic HTTP peacetime and attack traffic PCAP file.
- They can be downloaded and used in the above form.
- Peacetime capture contains 1,000 requests to 9 different URLs.

Extract Signatures





Synthetic Test Files

- Following are sample synthetic HTTP peacetime and attack traffic PCAP file.
- They can be downloaded and used in the above form.
- Peacetime capture contains 1,000 requests to 9 different URLs.

Extract Signatures

Step 1:

Step 2:

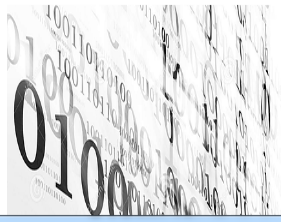
Step 3:

Analysis

Signatures

	Peace Signatures (Top 10)	Packet Cover
1	GET /welcome	11.60%
2	POST /verify	11.60%
3	POST /upload	11.30%
4	POST /logout	11.30%
5	GET /sites	10.90%
6	GET /getpage	10.70%
7	GET /my-account	10.60%
8	POST /signin	10.60%
9	GET /apps	10.50%

Export Signatures Close



Synthetic Test Files

- Following are sample synthetic HTTP peacetime and attack traffic PCAP file.
- They can be downloaded and used in the above form.
- Peacetime capture contains 1,000 requests to 9 different URLs.