

Uso di nDPI per l'Analisi di Traffico Criptato/Malware

Luca Deri <deri@ntop.org>

Chi Sono

- Fondatore del progetto ntop
<http://www.ntop.org>.
- Docente presso il Dipartimento di Informatica dell'Università di Pisa
- Intel Innovator

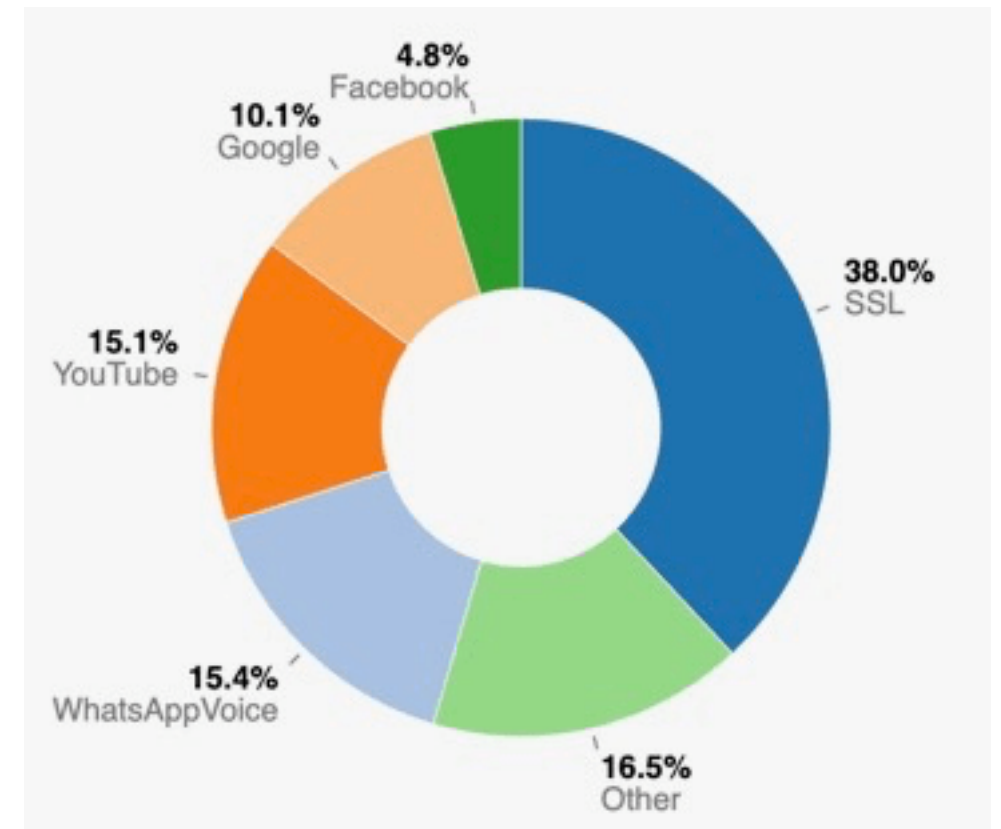


Intel®
Software
Innovator

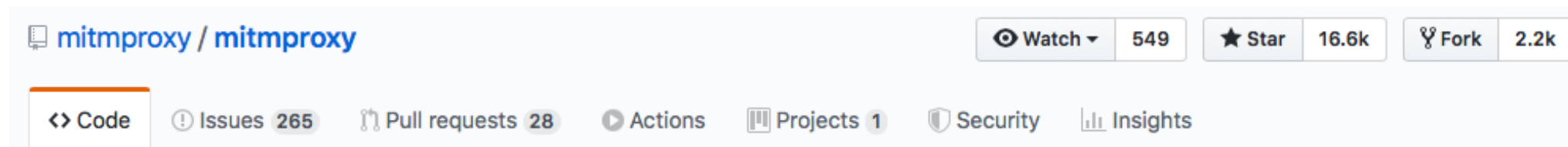


Motivazione

- La maggioranza del traffico Internet è criptato e lo sarà sempre di più.
- Analisi per IP e porta non è più sufficiente.
- I malware stanno “migrando” a TLS e quindi l’analisi di sicurezza basata sull’analisi del payload dei pacchetti non è più una buona idea.



MITM (Man in The Middle)? No Grazie



An interactive TLS-capable intercepting HTTP proxy for penetration testers and software developers. <https://mitmproxy.org/>

Il MITM è la risposta sbagliata ad una domanda lecita. A parte problemi legali o di GDPR:

- Non posso decodificare tutto il traffico TLS se non iniettando una certification authority a tutti i miei client.
- Non tutto il traffico criptato è TLS (es. SSH o VPN) e quindi è una battaglia persa in partenza.
- Alto costo computazionale e soprattutto “etico”: se il traffico è criptato ci sarà pure una ragione?

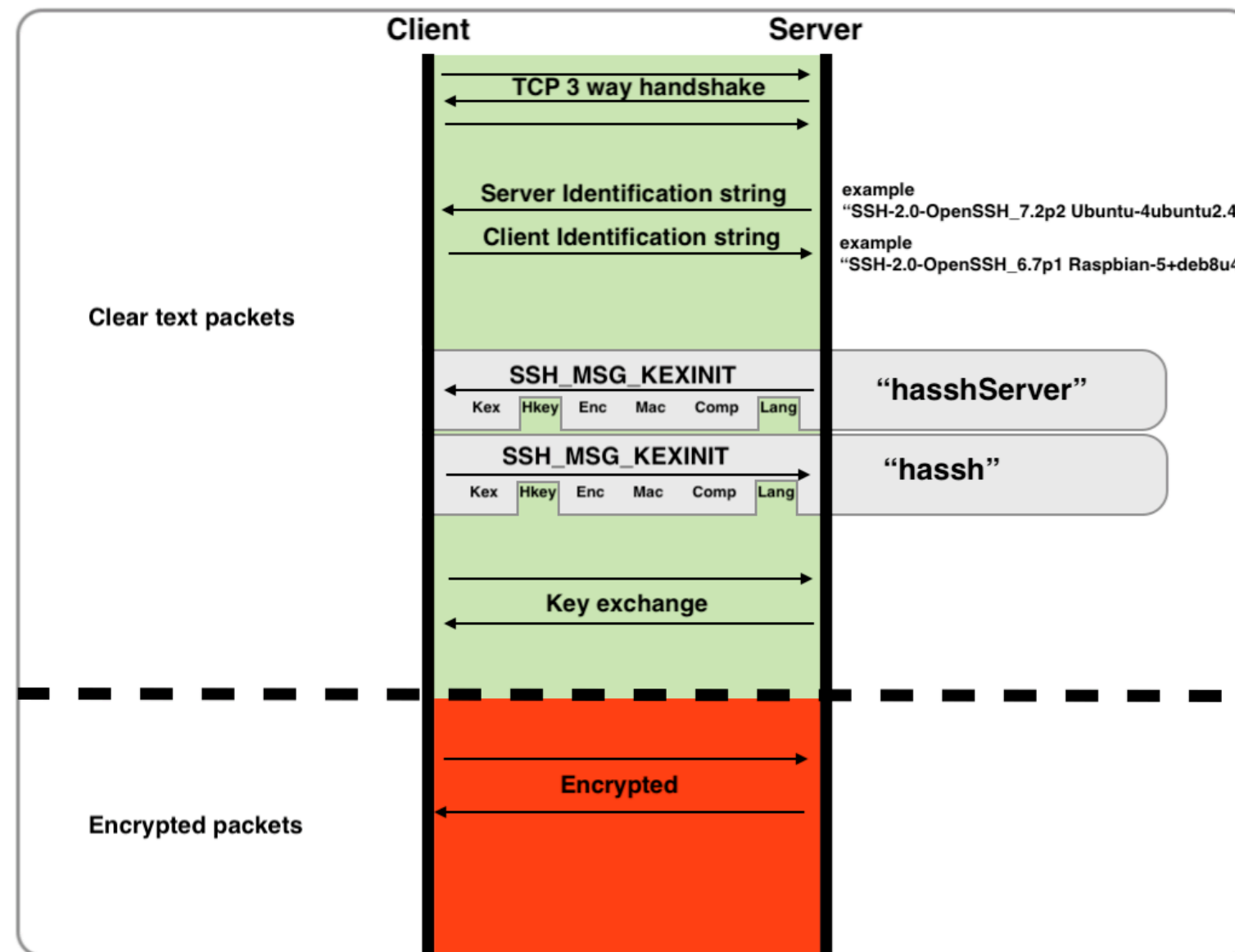
Requisiti [1/2]

- Gli amministratori di rete devono garantire che il traffico rispetti le politiche stabilite quindi:
 - Limitare banda ad alcuni protocolli (es. BitTorrent).
 - Bloccare comunicazioni criptate che possono nascondere un malware.
 - Dare priorità a traffici importanti come ad esempio cloud o protocolli multimediali (es. WhatsApp o Skype).
- Gli utenti devono:
 - Essere liberi nell'uso di Internet senza sospettare che ci sia un “grande fratello” che li osserva.

Requisiti [2/2]

- Creazione di fingerprint per riconoscere se il mio traffico criptato è “cambiato”.
- Impedire che traffici con problemi di TLS (es. vecchie versioni del protocollo) siano possibili.
- Fornire metriche per decidere circa la natura del traffico (es. SSH vs SCP).
- Identificazione di malware “nascosti” in TLS.

SSH Fingerprinting [1/2]



```
$ ssh 210.172.195.202
```

```
The authenticity of host '210.172.195.202 (210.172.195.202)' can't be established.  
RSA key fingerprint is SHA256:oM1N0BCQLu1paUX3MY8lqgicbMsHEof04F6XsHQVNMU.  
Are you sure you want to continue connecting (yes/no)?
```

SSH Fingerprinting [2/2]

ssh.kex.h_sig

Packet list: Narrow & Wide Case sensitive Hex value EC73

No.	Time	Source	Destination	Protocol	Info
17	0.172860	jake.unipi.it	192.168.1.37	SSHv2	Server: Diffie-Hellman Group Exchange Reply, New Keys

Frame 17: 1042 bytes on wire (8336 bits), 1042 bytes captured (8336 bits)

Ethernet II, Src: Technico_f1:39:76 (10:13:31:f1:39:76), Dst: Apple_06:49:fe (c4:2c:03:06:49:fe)

Internet Protocol Version 4, Src: jake.unipi.it (131.114.18.19), Dst: 192.168.1.37 (192.168.1.37)

Transmission Control Protocol, Src Port: EtherNet-IP-1 (2222), Dst Port: 51388 (51388), Seq: 4061018342, Ack: 2678031444, Len: 976

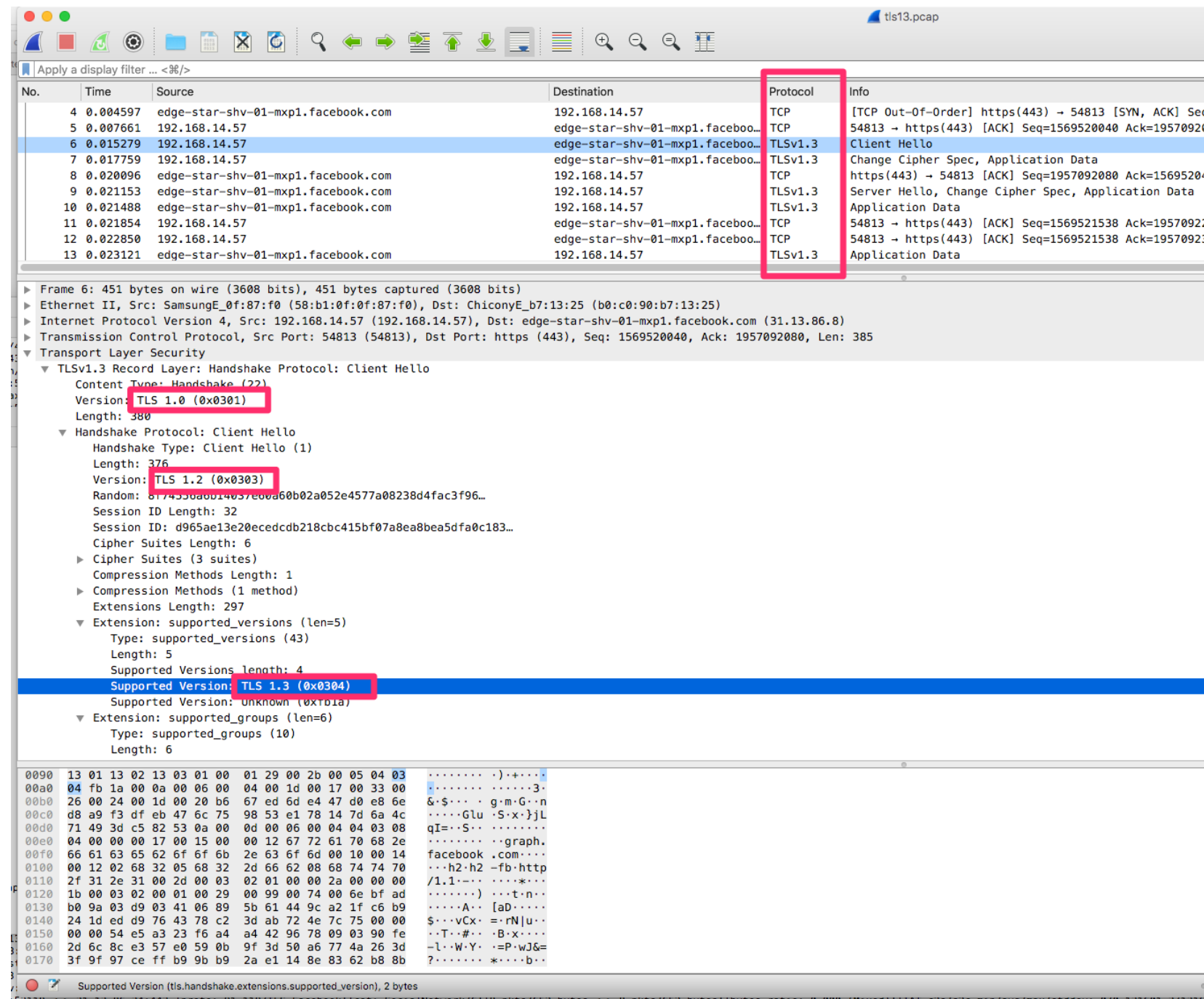
SSH Protocol

- SSH Version 2 (encryption:aes128-ctr mac:umac-64@openssh.com compression:none)
 - Packet Length: 956
 - Padding Length: 7
 - Key Exchange
 - Message Code: Diffie-Hellman Group Exchange Reply (33)
 - KEX host key (type: ssh-rsa)
 - Host key length: 279
 - Host key type length: 7
 - Host key type: ssh-rsa
 - Multi Precision Integer Length: 3
 - RSA public exponent (e): 010001
 - Multi Precision Integer Length: 257
 - RSA modulus (N): 00d0e38720f8a7baa1a278a1e70d41679b909badb2b53ae5...
 - Multi Precision Integer Length: 385
 - DH server f: 009103a639f79e3a614a4a65f38387e39b6de0a5d9c1d926...
 - KEX H signature length: 271
 - KEX H signature: 00000007737382d727361000001001546b4d3161d50b6fb...
 - Padding String: 00

ECDSA key fingerprint is SHA256 of ssh.kex.h_sig

<https://engineering.salesforce.com/open-sourcing-hassh-abed3ae5044c>

Welcome to TLS



The image shows a Wireshark packet capture of a TLS handshake. The top pane displays a list of packets, with packet 6 (a TLSv1.3 Client Hello) selected. The bottom pane shows the detailed view of this packet, highlighting the 'Version' field as 'TLS 1.0 (0x0301)' and the 'Supported Version' field as 'TLS 1.3 (0x0304)'. The packet details include the handshake type, random, session ID, cipher suites, compression methods, and extensions.

No.	Time	Source	Destination	Protocol	Info
4	0.004597	edge-star-shv-01-mxp1.facebook.com	192.168.14.57	TCP	[TCP Out-Of-Order] https(443) → 54813 [SYN, ACK] Seq=1569520040 Ack=1957092080
5	0.007661	192.168.14.57	edge-star-shv-01-mxp1.facebook.com	TCP	54813 → https(443) [ACK] Seq=1569520040 Ack=1957092080
6	0.015279	192.168.14.57	edge-star-shv-01-mxp1.facebook.com	TLSv1.3	Client Hello
7	0.017759	192.168.14.57	edge-star-shv-01-mxp1.facebook.com	TLSv1.3	Change Cipher Spec, Application Data
8	0.020096	edge-star-shv-01-mxp1.facebook.com	192.168.14.57	TCP	https(443) → 54813 [ACK] Seq=1957092080 Ack=1569520040
9	0.021153	edge-star-shv-01-mxp1.facebook.com	192.168.14.57	TLSv1.3	Server Hello, Change Cipher Spec, Application Data
10	0.021488	edge-star-shv-01-mxp1.facebook.com	192.168.14.57	TLSv1.3	Application Data
11	0.021854	192.168.14.57	edge-star-shv-01-mxp1.facebook.com	TCP	54813 → https(443) [ACK] Seq=1569521538 Ack=1957092080
12	0.022850	192.168.14.57	edge-star-shv-01-mxp1.facebook.com	TCP	54813 → https(443) [ACK] Seq=1569521538 Ack=1957092080
13	0.023121	edge-star-shv-01-mxp1.facebook.com	192.168.14.57	TLSv1.3	Application Data

Frame 6: 451 bytes on wire (3608 bits), 451 bytes captured (3608 bits) on interface 0
Ethernet II, Src: SamsungE_0f:87:f0 (58:b1:0f:0f:87:f0), Dst: ChiconyE_b7:13:25 (b0:c0:90:b7:13:25)
Internet Protocol Version 4, Src: 192.168.14.57 (192.168.14.57), Dst: edge-star-shv-01-mxp1.facebook.com (31.13.86.8)
Transmission Control Protocol, Src Port: 54813 (54813), Dst Port: https (443), Seq: 1569520040, Ack: 1957092080, Len: 385
Transport Layer Security
TLSv1.3 Record Layer: Handshake Protocol: Client Hello
Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)
Length: 380
Handshake Protocol: Client Hello
Handshake Type: Client Hello (1)
Length: 376
Version: TLS 1.2 (0x0303)
Random: 8174530a0b14057e00a60b02a052e4577a08238d4fac3f96...
Session ID Length: 32
Session ID: d965ae13e20ecedcd218cbc415bf07a8ea8bea5dfa0c183...
Cipher Suites Length: 6
Cipher Suites (3 suites)
Compression Methods Length: 1
Compression Methods (1 method)
Extensions Length: 297
Extension: supported_versions (len=5)
Type: supported_versions (43)
Length: 5
Supported Versions length: 4
Supported Version: TLS 1.3 (0x0304)
Supported Version: Unknown (0x030a)
Extension: supported_groups (len=6)
Type: supported_groups (10)
Length: 6

0090 13 01 13 02 13 03 01 00 01 29 00 2b 00 05 04 03+...
00a0 04 fb 1a 00 0a 00 06 00 04 00 1d 00 17 00 33 003...
00b0 26 00 24 00 1d 00 20 b6 67 ed 6d e4 47 d0 e8 6e &\$. . . g.m.G..n
00c0 d8 a9 f3 df eb 47 6c 75 98 53 e1 78 14 7d 6a 4cGlu .S.x.}jL
00d0 71 49 3d c5 82 53 0a 00 0d 00 06 00 04 04 03 08 qI=...S...
00e0 04 00 00 00 17 00 15 00 00 12 67 72 61 70 68 2egraph..
00f0 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 00 10 00 14 facebook .com...
0100 00 12 02 68 32 05 68 32 2d 66 62 08 68 74 74 70 ...h2:h2 -fb:http
0110 2f 31 2e 31 00 2d 00 03 02 01 00 00 2a 00 00 00 /1.1... ..*...
0120 1b 00 03 02 00 01 00 29 00 99 00 74 00 6e bf ad) ...t.n...
0130 b0 9a 03 d9 03 41 06 89 5b 61 44 9c a2 1f c6 b9A... [ad...
0140 24 1d ed d9 76 43 78 c2 3d ab 72 4e 7c 75 00 00 \$. .vCx. =rN|u..
0150 00 00 54 e5 a3 23 f6 a4 a4 42 96 78 09 03 90 fe ..T...#...B.x...
0160 2d 6c 8c e3 57 e0 59 0b 9f 3d 50 a6 77 4a 26 3d -l..W.Y. .P.wJ&=
0170 3f 9f 97 ce ff b9 9b b9 2a e1 14 8e 83 62 b8 8b ?.....*...b...

Supported Version (tls.handshake.extensions.supported_version), 2 bytes

TLS Client Fingerprint [1/2]

▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello

Content Type: Handshake (22)

Version: TLS 1.0 (0x0301)

Length: 224

▼ Handshake Protocol: Client Hello

Handshake Type: Client Hello (1)

Length: 220

Version: TLS 1.2 (0x0303) ←

► Random

Session ID Length: 0

Cipher Suites Length: 38

► Cipher Suites (19 suites) ←

Compression Methods Length: 1

► Compression Methods (1 method)

Extensions Length: 141 ←

► Extension: server_name

► Extension: elliptic_curves ←

► Extension: ec_point_formats ←

► Extension: signature_algorithms

► Extension: next_protocol_negotiation

► Extension: Application Layer Protocol Negotiation

► Extension: status_request

► Extension: signed_certificate_timestamp

► Extension: Extended Master Secret

0060	1a e1 15 00 00 26 00 ff c0 2c c0 2b c0 24 c0 23&.. ,.,+.\$.#
0070	c0 0a c0 09 c0 30 c0 2f c0 28 c0 27 c0 14 c0 130./ .(. '....
0080	00 9d 00 9c 00 3d 00 3c 00 35 00 2f 01 00 00 8d=< .5./....
0090	00 00 00 18 00 16 00 00 13 63 6c 69 65 6e 74 73clients
00a0	31 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 00 0a 00 08	1.google .com....
00b0	00 06 00 17 00 18 00 19 00 0b 00 02 01 00 00 0d
00c0	00 12 00 10 04 01 02 01 05 01 06 01 04 03 02 03

TLS Client Fingerprint [2/2]

TLS ClientHello

```
Secure Sockets Layer
  TLSv1 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 214
    Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 210
      Version: TLS 1.0 (0x0301)
      Random
      Session ID Length: 0
      Cipher Suites Length: 120
      Cipher Suites (60 suites)
      Compression Methods Length: 1
      Compression Methods (1 method)
      Extensions Length: 49
      Extension: ec_point_formats
      Extension: elliptic_curves
      Extension: SessionTicket TLS
      Extension: Heartbeat
```

Possible Clients

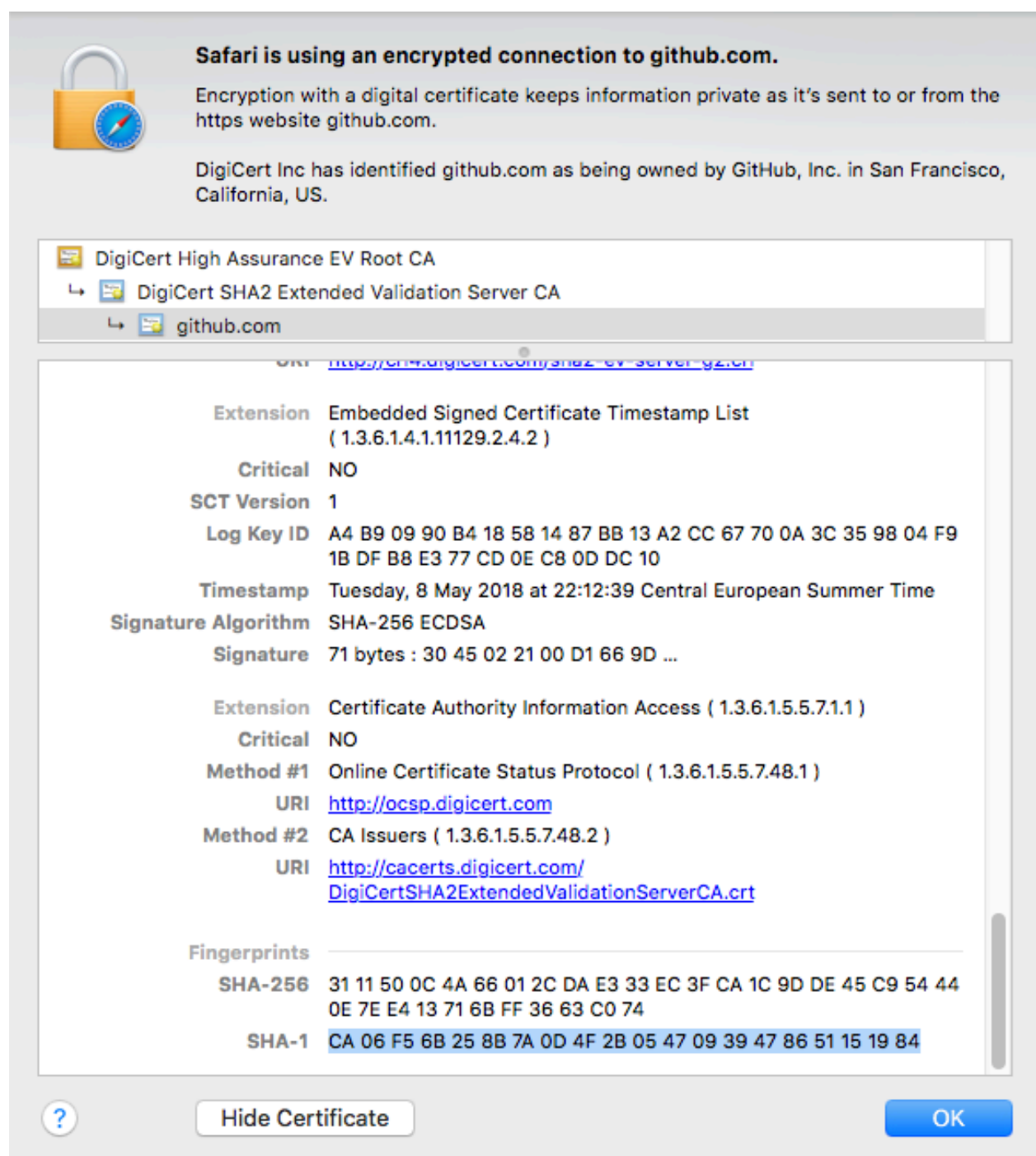


True Client

OpenSSL
Cryptography and SSL/TLS Toolkit
(v: 1.0.1r)

<https://engineering.salesforce.com/tls-fingerprinting-with-ja3-and-ja3s-247362855967>

SSL Certificate Fingerprint [1/3]



SSL Certificate Fingerprint [2/3]

1 0.000000 192.168.1.20 api-drf.smoot.apple.com TLSv1.2 Client Hello

2 0.047526 api-drf.smoot.apple.com 192.168.1.20 TCP https(443) → 54827 [SYN]

3 0.047648 192.168.1.20 api-drf.smoot.apple.com TCP 54827 → https(443) [ACK]

4 0.051407 api-drf.smoot.apple.com 192.168.1.20 TLSv1.2 Server Hello

5 0.052057 api-drf.smoot.apple.com 192.168.1.20 TCP https(443) → 54827 [ACK]

6 0.052127 192.168.1.20 api-drf.smoot.apple.com TCP 54827 → https(443) [ACK]

7 0.053360 api-drf.smoot.apple.com 192.168.1.20 TLSv1.2 Certificate, Server Key Exchange

8 0.053451 192.168.1.20 api-drf.smoot.apple.com TCP 54827 → https(443) [ACK]

9 0.060942 192.168.1.20 api-drf.smoot.apple.com TLSv1.2 Client Key Exchange

10 0.060974 192.168.1.20 api-drf.smoot.apple.com TLSv1.2 Change Cipher Spec

11 0.061030 192.168.1.20 api-drf.smoot.apple.com TLSv1.2 Encrypted Handshake Message

12 0.107078 api-drf.smoot.apple.com 192.168.1.20 TCP https(443) → 54827 [ACK]

13 0.108364 api-drf.smoot.apple.com 192.168.1.20 TLSv1.2 New Session Ticket, Change Cipher Spec

14 0.108432 192.168.1.20 api-drf.smoot.apple.com TCP 54827 → https(443) [ACK]

15 0.109505 192.168.1.20 api-drf.smoot.apple.com TLSv1.2 Application Data

16 0.161736 api-drf.smoot.apple.com 192.168.1.20 TLSv1.2 Application Data

17 0.161793 192.168.1.20 api-drf.smoot.apple.com TCP 54827 → https(443) [ACK]

18 0.214627 192.168.1.20 api-drf.smoot.apple.com TLSv1.2 Application Data

19 0.268418 api-drf.smoot.apple.com 192.168.1.20 TLSv1.2 Application Data

Frame 7: 1465 bytes on wire (11720 bits), 1465 bytes captured (11720 bits) on interface 0

Ethernet II, Src: AvmAudio_75:4e:6a (5c:49:79:75:4e:6a), Dst: Apple_06:49:fe (c4:2c:03:06:49:fe)

Internet Protocol Version 4, Src: 17.252.75.246 (17.252.75.246), Dst: 192.168.1.20 (192.168.1.20)

Transmission Control Protocol, Src Port: https (443), Dst Port: 54827 (54827), Seq: 1735620727, Ack: 4023694595, Len: 1399

[3 Reassembled TCP Segments (3862 bytes): #4(1370), #5(1440), #7(1052)]

Transport Layer Security

TLSv1.2 Record Layer: Handshake Protocol: Certificate

Content Type: Handshake (22)

Version: TLS 1.2 (0x0303)

Length: 3857

Handshake Protocol: Certificate

Handshake Type: Certificate (11)

Length: 3853

Certificates Length: 3850

Certificates (3850 bytes)

Certificate Length: 1265

Certificate: 308204ed308203d5a00302010202101776b0f5475c409c14 (id-at-commonName=*.smoot.apple.com,id-at-organizationalUnitName=Siri S

Certificate Length: 1340

Certificate: 3082053830820420a0030201020210513fb97

Certificate Length: 1236

Certificate: 308204d030820439a0030201020210250ce8e

Transport Layer Security

Frame (1465 bytes) Reassembled TCP (3862 bytes)

Certificate (tls.handshake.certificate), 1265 bytes

Packets: 68 · Displayed: 68

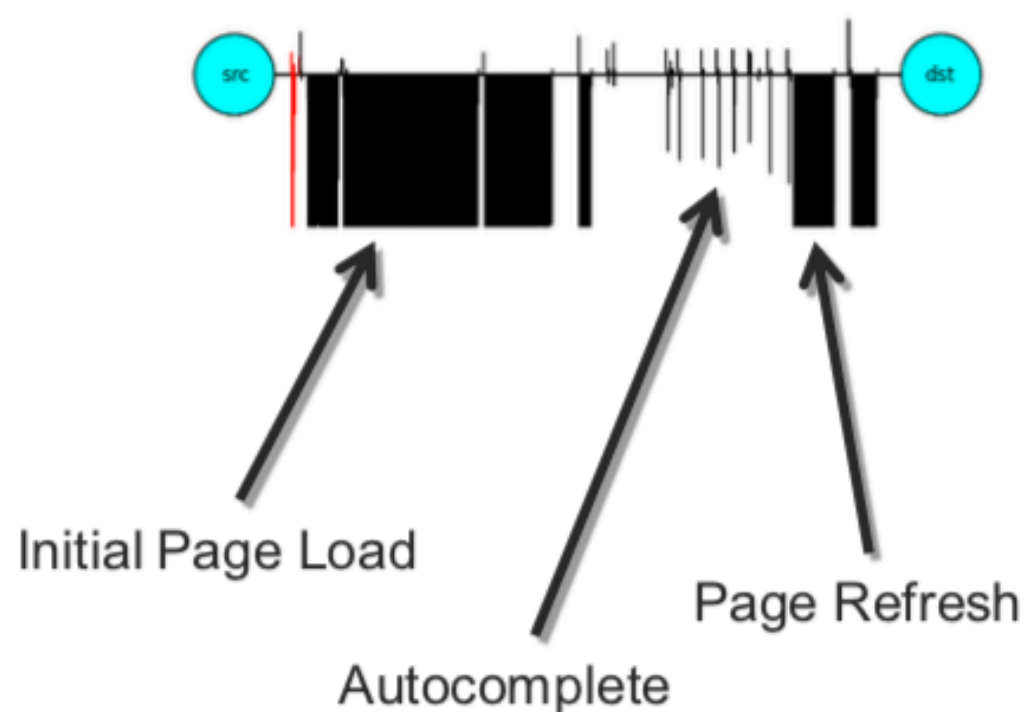
SSL Certificate Fingerprint [3/3]

- Save export bytes as ssl.bin
- `openssl x509 -inform der -in ssl.bin -text > ssl.der`
- `openssl x509 -noout -fingerprint -sha1 -inform pem -in ssl.der`
SHA1 Fingerprint=C8:9C:6E:98:35:E2:44:02:2E:
69:0B:D0:43:2B:E6:75:8C:12:7F:44

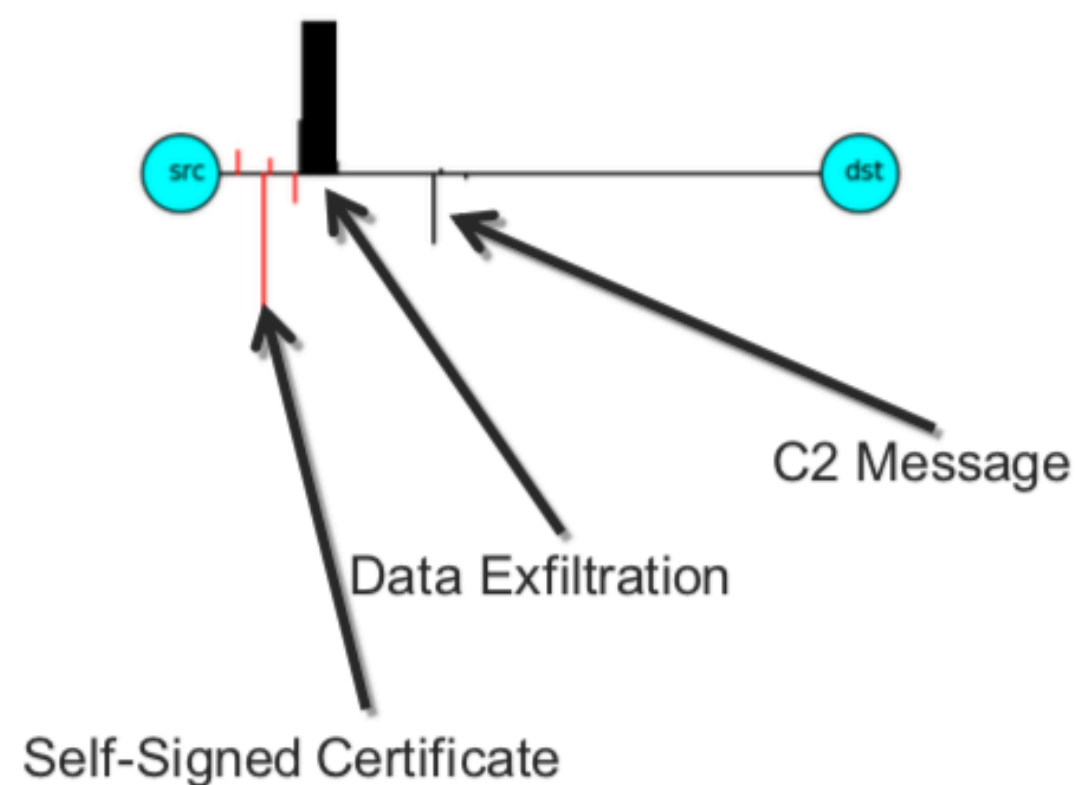
<https://knowledge.digicert.com/solution/SO28771.html>

Analisi Malware su TLS [1/7]

Google Search

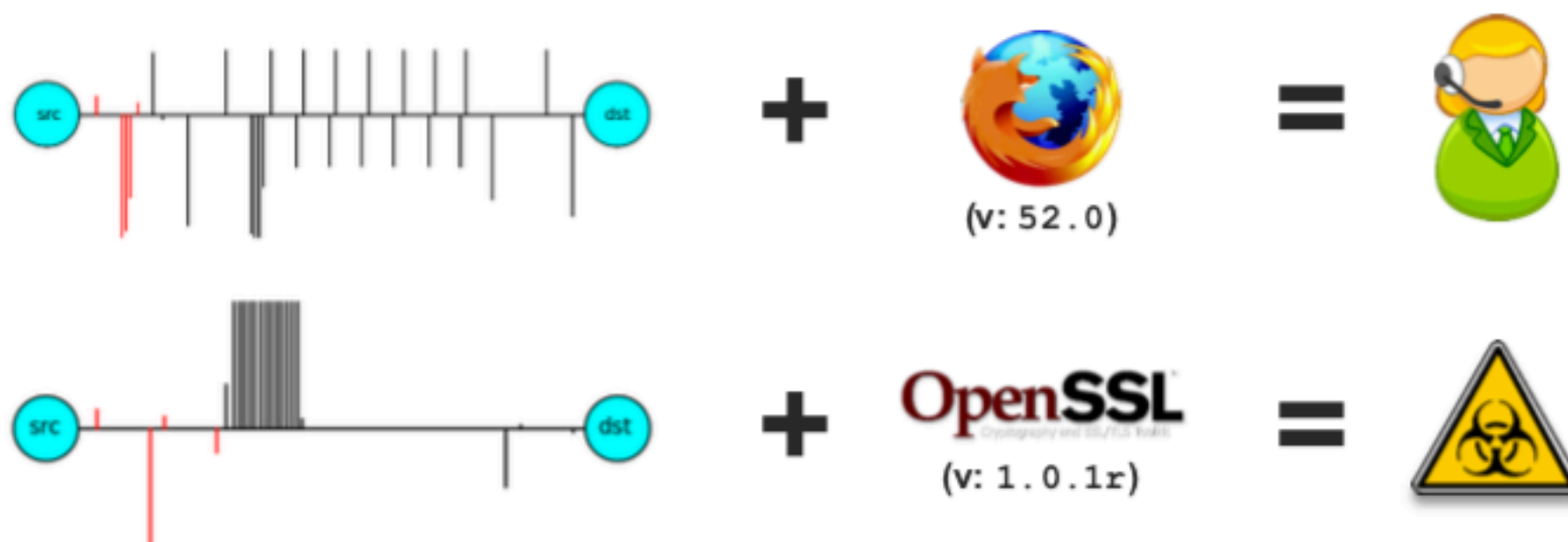


Bestafera



Bestafera: <https://www.fortiguard.com/encyclopedia/virus/7893011>

Analisi Malware su TLS [2/7]



Analisi Malware su TLS [3/7]

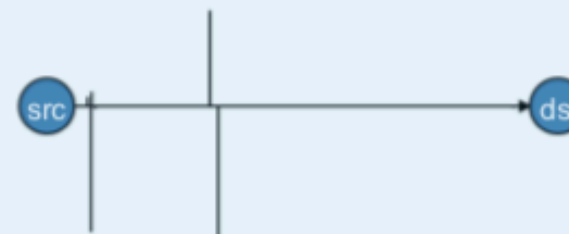


Contextual Flows	Client		Session	Server
	TCP/IP	Source Address Source Port	# Bytes # Packets	Destination Address Destination Port
	Intraflow	Packet Lengths Packet Arrival Times		
	TLS	Ciphersuite Offer Vector Extensions Offer Supported Elliptic Curves SNI	Record Length Record Times Record Types	Certificate Chain Selected Ciphersuite
	DNS	Name		Response Code TTL
	HTTP	Headers	Headers File Magic	Headers

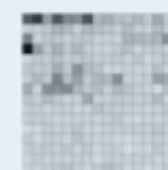
<https://github.com/cisco/joy>

Analisi Malware su TLS [4/7]

- SPLT – Sequence of Packet Lengths and Arrival Times



- Byte Distribution
- Byte Entropy



- TLS unencrypted header data
 - Certificates, SNI, Ciphersuites, Extensions

TLS
metadata

- DNS linked flows

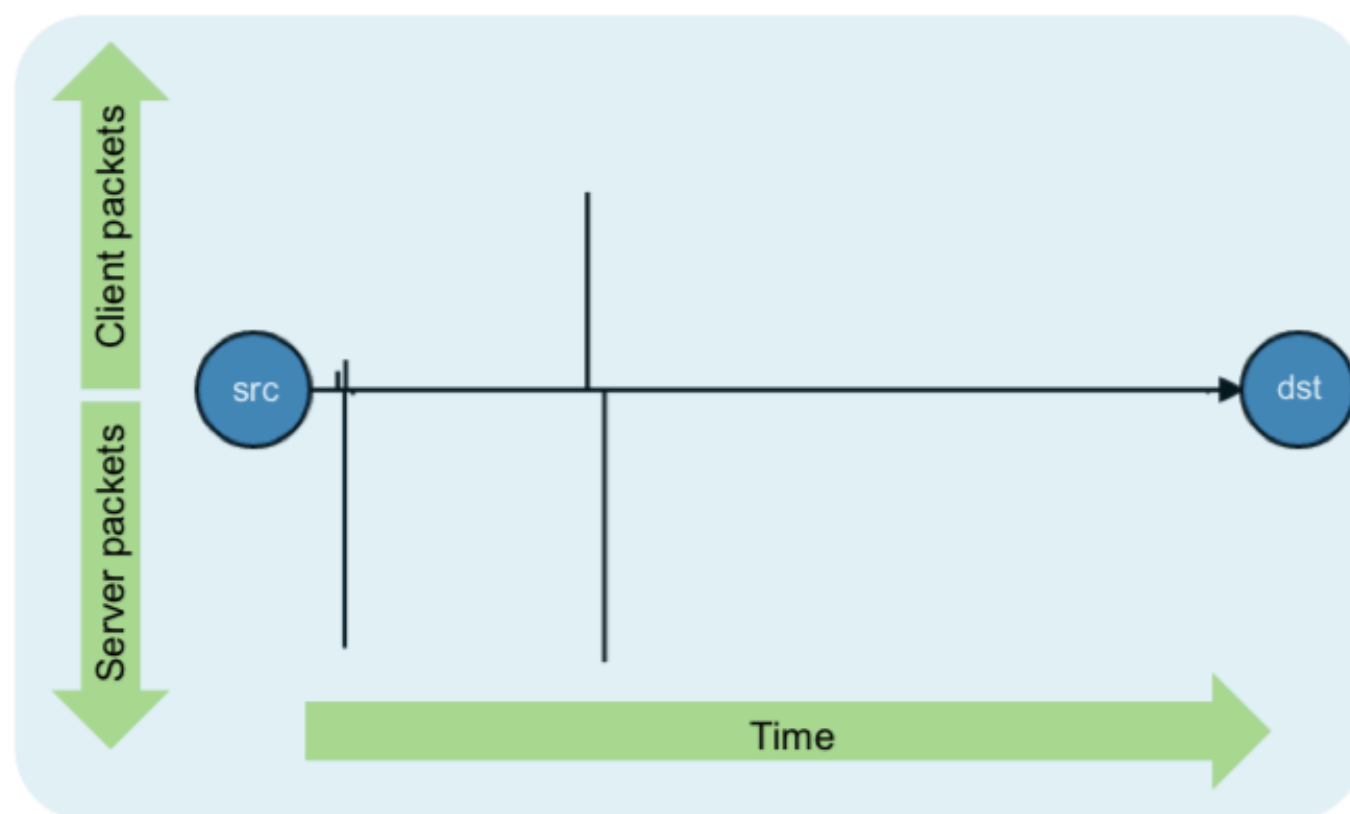
DNS

- HTTP linked flows

HTTP

Analisi Malware su TLS [5/7]

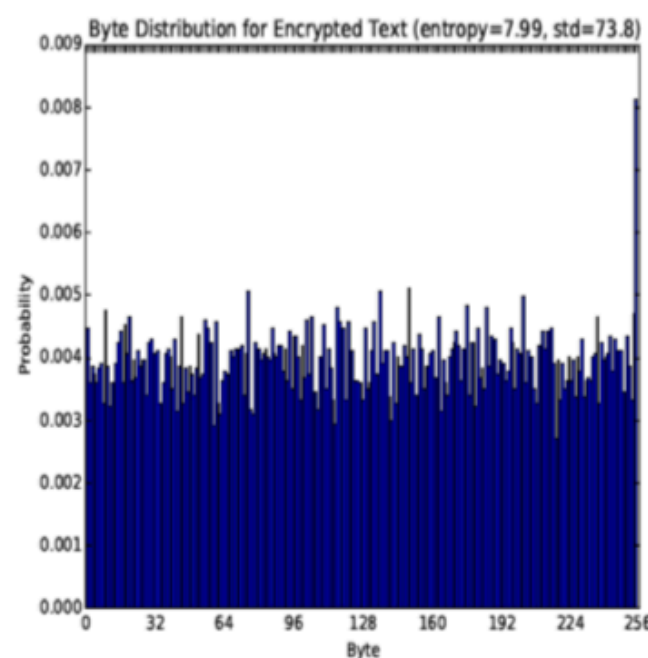
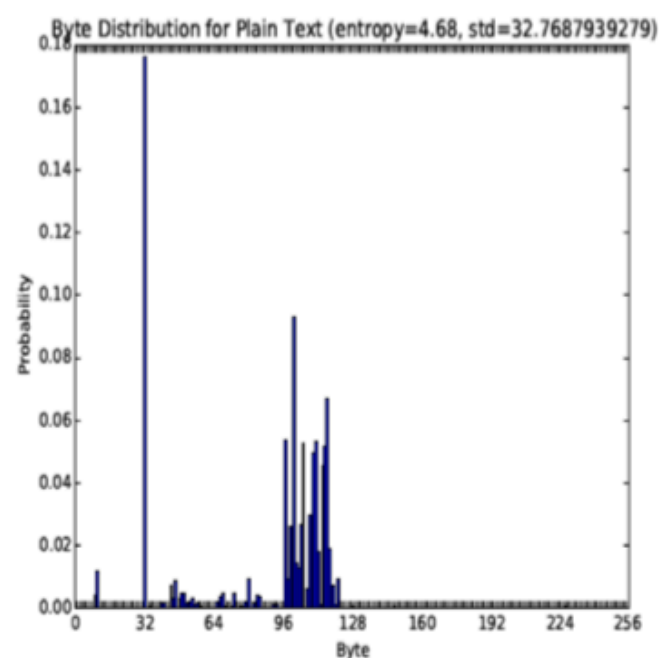
Sequence of Packet Lengths and Times



```
"packets": [  
  { "b": 22, "ipt": 33, "dir": ">" },  
  { "b": 1432, "ipt": 4, "dir": "<" },  
  { "b": 30, "ipt": 1, "dir": ">" },  
  { "b": 4, "ipt": 145, "dir": "<" },  
  ...  
]
```

Analisi Malware su TLS [6/7]

Byte Distribution and entropy



"entropy": 7.165,

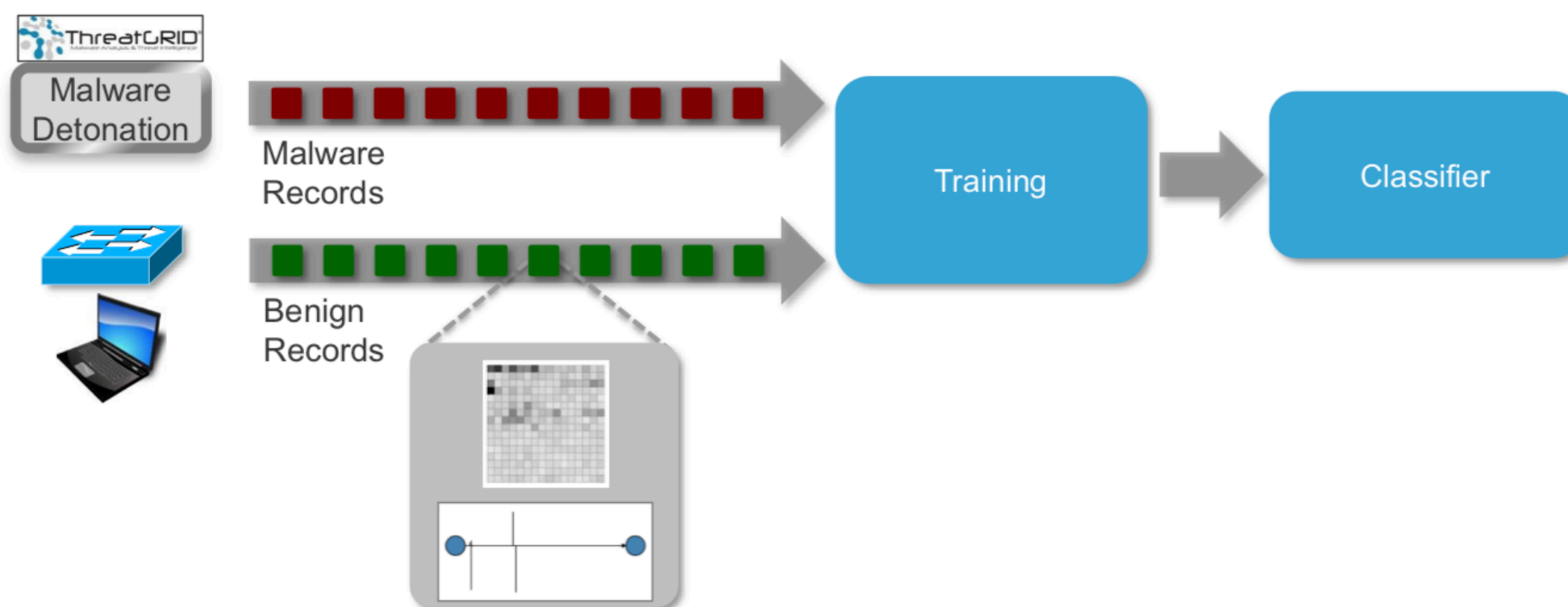
"bd": [

23, 7, 4, 8, 4, 12, 7, 4,
12, 5, 98, 6, 5, 101, 14, 8,
9, 9, 6, 8, 10, 6, 10, 6,
16, 8, 3, 16, 7, 7, 3, 11,
189, 6, 24, 9, 10, 10, 5, 7,
19, 8, 16, 8, 34, 79, 61, 90,
102, 91, 56, 47, 35, 47, 30, 25,

...

]

Analisi Malware su TLS [7/7]



nDPI

nDPI

Open Source Deep Packet Inspection Software Toolkit

traffic-analysis

dpi

ndpi

deep-packet-inspection



C



LGPL-3.0



522



1,873



82 (1 issue needs help)



3

Updated 37 minutes ago



- Libreria open source per il DPI (Deep Packet Inspection): <https://github.com/ntop/nDPI>
- Oltre 240 protocolli supportati.
- Estensibile a runtime via file di configurazione.
- Disponibile su MacOS, Linux, Windows....
- Usata da molti progetti liberi per analisi e blocco traffico di rete.

nDPI: SSH

```
$ ./example/ndpiReader -i ./tests/pcap/ssh.pcap -v 2
```

...

Detected protocols:

SSH	packets: 258	bytes: 35546	flows: 1
-----	--------------	--------------	----------

Protocol statistics:

Acceptable	35546 bytes
------------	-------------

```
1 TCP 172.16.238.1:58395 <=> 172.16.238.168:22 [proto: 92/SSH][cat: RemoteAccess/12][159 pkts/15615 bytes <=> 99 pkts/19931 bytes][bytes ratio: -0.121 (Mixed)][IAT c2s/s2c min/avg/max/stddev: 0/0 1845.8/2933.8 166223/166224 14794.2/19692.2][Pkt Len c2s/s2c min/avg/max/stddev: 66/66 98.2/201.3 970/1346 83.1/283.2][Client: SSH-2.0-OpenSSH_5.3][HASSH-C: 21B457A327CE7A2D4FCE5EF2C42400BD][Server: SSH-2.0-OpenSSH_5.6][HASSH-S: B1C6C0D56317555B85C7005A3DE29325]
```

Sessione Interattiva (no SCP)

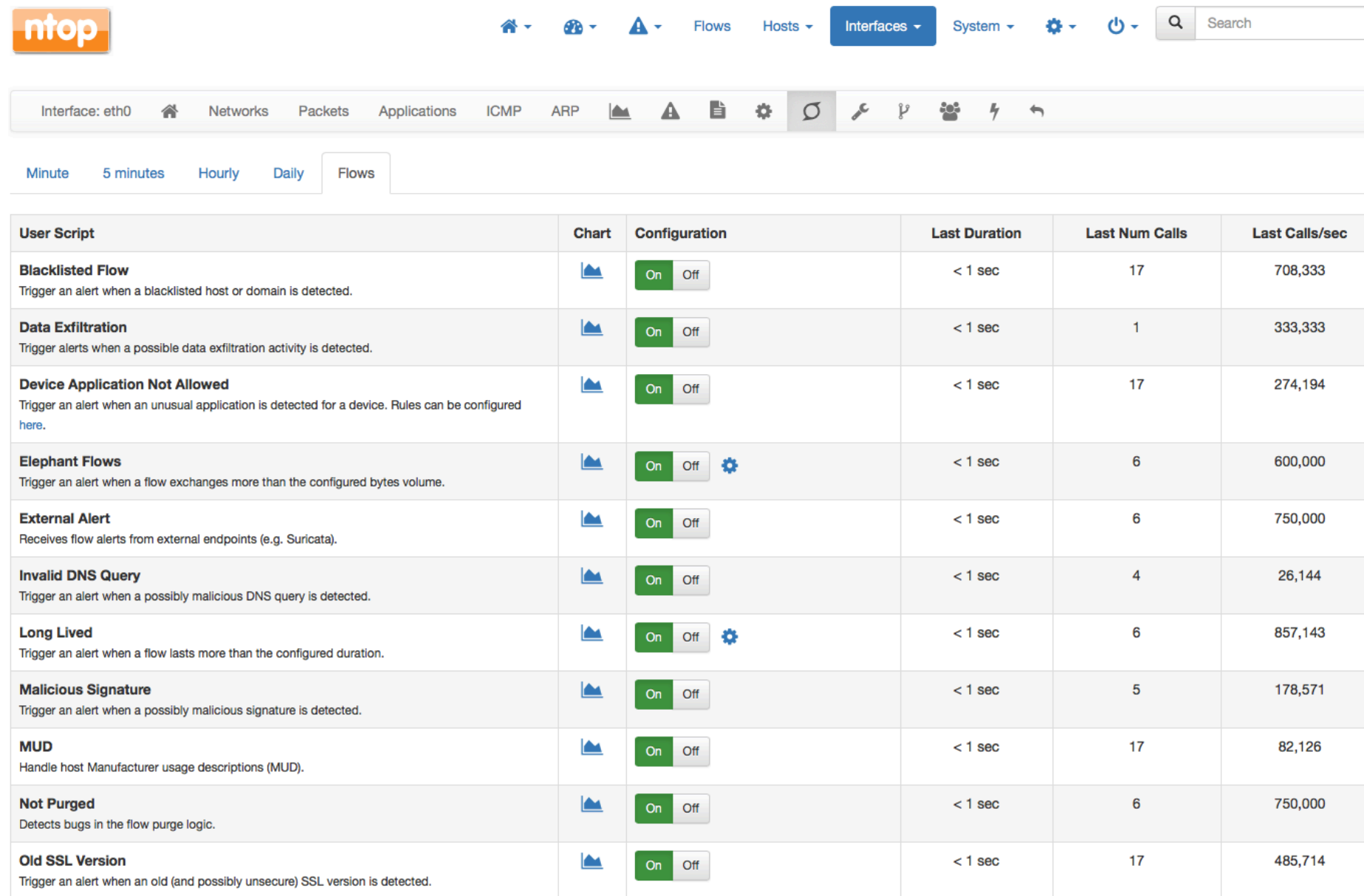
nDPI:TLS














```
$ ./example/ndpiReader -v 2 -J -i ./tests/pcap/instagram.pcap |grep TLS
```

```
..
  11 TCP 192.168.0.103:44558 <=> 46.33.70.174:443 [byte_dist:
62,10,7,8,4,6,1,2,3,3,6,4,3,3,3,4,4,3,3,6,4,3,3,3,3,2,2,1,0,1,2,3,4,3,2,1,1,1,0,1,0,0,2,0,1,3,2,2,1,0,3,1,2,1,1,1,
2,3,0,1,1,2,2,1,0,0,0,0,0,1,1,4,0,0,1,3,1,1,3,1,0,0,1,0,1,1,1,0,1,0,1,0,1,2,2,0,1,4,2,2,4,2,3,1,4,3,0,1,1,3,4,2,1,
2,1,1,4,0,1,3,4,0,2,0,1,0,1,2,2,0,1,0,0,2,0,2,0,3,3,2,1,1,1,2,1,0,0,0,1,3,1,0,2,0,0,1,1,2,1,2,1,0,1,2,0,0,0,2,1,0,
2,0,0,0,0,0,1,2,1,0,2,2,0,0,0,1,2,2,1,1,1,1,17,1,1,0,1,1,0,3,3,1,2,1,0,3,2,1,0,0,1,0,1,0,0,0,2,1,1,3,2,0,1,1,3,1,0,
,2,2,0,1,0,1,1,1,1,2,1,2,1,1,2,0,0,0,1,0,3,1,1,1,2,1,1,0,2]] [byte_dist_mean: 89.834140] [byte_dist_std: 62.276198]
[entropy: 0.977652] [total_entropy: 4577.368959] [score: 0.0166] [proto: 91.211/TLS.Instagram] [cat: SocialNetwork/6]
[10 pkts/1545 bytes <=> 7 pkts/4824 bytes] [bytes ratio: -0.515 (Download)] [IAT c2s/s2c min/avg/max/stddev: 0/0
21.1/29.2 79/103 25.5/38.4] [Pkt Len c2s/s2c min/avg/max/stddev: 66/66 154.5/689.1 516/1484 151.0/647.4] [TLSv1]
[Client: igcdn-photos-h-a.akamaihd.net] [JA3C: 54ae5fcb0159e2ddf6a50e149221c7c7] [Server: a248.e.akamai.net] [JA3S:
7df57c06f869fc3ce509521cae2f75ce] [Organization: Akamai Technologies Inc.] [Certificate SHA-1: EA:5A:
20:95:78:D7:09:60:5C:A1:E4:CA:A5:2B:BD:C1:78:FB:23:27] [Validity: 2015-06-19 16:52:07 - 2016-06-19 16:52:05]
[Cipher: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA]
..
```

| = malware

nDPI in ntopng



User Script	Chart	Configuration	Last Duration	Last Num Calls	Last Calls/sec
Blacklisted Flow Trigger an alert when a blacklisted host or domain is detected.		<input checked="" type="checkbox"/> On <input type="checkbox"/> Off	< 1 sec	17	708,333
Data Exfiltration Trigger alerts when a possible data exfiltration activity is detected.		<input checked="" type="checkbox"/> On <input type="checkbox"/> Off	< 1 sec	1	333,333
Device Application Not Allowed Trigger an alert when an unusual application is detected for a device. Rules can be configured here .		<input checked="" type="checkbox"/> On <input type="checkbox"/> Off	< 1 sec	17	274,194
Elephant Flows Trigger an alert when a flow exchanges more than the configured bytes volume.		<input checked="" type="checkbox"/> On <input type="checkbox"/> Off 	< 1 sec	6	600,000
External Alert Receives flow alerts from external endpoints (e.g. Suricata).		<input checked="" type="checkbox"/> On <input type="checkbox"/> Off	< 1 sec	6	750,000
Invalid DNS Query Trigger an alert when a possibly malicious DNS query is detected.		<input checked="" type="checkbox"/> On <input type="checkbox"/> Off	< 1 sec	4	26,144
Long Lived Trigger an alert when a flow lasts more than the configured duration.		<input checked="" type="checkbox"/> On <input type="checkbox"/> Off 	< 1 sec	6	857,143
Malicious Signature Trigger an alert when a possibly malicious signature is detected.		<input checked="" type="checkbox"/> On <input type="checkbox"/> Off	< 1 sec	5	178,571
MUD Handle host Manufacturer usage descriptions (MUD).		<input checked="" type="checkbox"/> On <input type="checkbox"/> Off	< 1 sec	17	82,126
Not Purged Detects bugs in the flow purge logic.		<input checked="" type="checkbox"/> On <input type="checkbox"/> Off	< 1 sec	6	750,000
Old SSL Version Trigger an alert when an old (and possibly insecure) SSL version is detected.		<input checked="" type="checkbox"/> On <input type="checkbox"/> Off	< 1 sec	17	485,714

<https://github.com/ntop/ntopng>

Grazie



jobs@ntop.org