

Suricata and the Shark: suriwire

É. Leblond

Stamus Networks

July. 03, 2018



Get the mascot



- Available on Amazon: <https://www.amazon.co.uk/Vivid-Arts-Meerkat-Shark-Onesie/dp/B01MAYA3A1>
- For only 19.99 brexit coins¹

¹Worth 76745.63 Columbian Peso

Get Suricata information in Wireshark

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	SID	Info
3050	12697.058138	192.168.2.7	222.89.52.102	UDP	72		1082 → 47465 Len=30
3051	12697.106154	61.191.61.40	192.168.2.7	TCP	1514	2018959	80 → 1091 [ACK] Seq=29467 Ack=197 Win=65
3052	12697.109988	61.191.61.40	192.168.2.7	TCP	1514		80 → 1091 [ACK] Seq=30927 Ack=197 Win=65
3053	12697.114176	61.191.61.40	192.168.2.7	TCP	1514		80 → 1091 [ACK] Seq=32387 Ack=197 Win=65
3054	12697.118117	61.191.61.40	192.168.2.7	TCP	1514		80 → 1091 [ACK] Seq=33847 Ack=197 Win=65
3055	12697.120301	192.168.2.7	61.191.61.40	TCP	54	2009991, 2019714	1091 → 80 [ACK] Seq=197 Ack=32387 Win=17
3056	12697.122339	61.191.61.40	192.168.2.7	TCP	1514		80 → 1091 [ACK] Seq=35307 Ack=197 Win=65
3057	12697.126260	61.191.61.40	192.168.2.7	TCP	1514		80 → 1091 [ACK] Seq=36767 Ack=197 Win=65
3058	12697.130425	61.191.61.40	192.168.2.7	TCP	1514		80 → 1091 [ACK] Seq=38227 Ack=197 Win=65
3059	12697.134379	61.191.61.40	192.168.2.7	TCP	1514		80 → 1091 [ACK] Seq=39687 Ack=197 Win=65

▶ Frame 3051: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)

▶ Ethernet II, Src: Intel_61:2d:8f (00:d0:b7:61:2d:8f), Dst: 00:54:00:12:34:57 (00:54:00:12:34:57)

▶ Internet Protocol Version 4, Src: 61.191.61.40, Dst: 192.168.2.7

▶ Transmission Control Protocol, Src Port: 80, Dst Port: 1091, Seq: 29467, Ack: 197, Len: 1460

▼ Suricata alert: 2018959 (ET POLICY PE EXE or DLL Windows file download HTTP)

GID: 1

SID: 2018959

Rev: 3

Message: ET POLICY PE EXE or DLL Windows file download HTTP

▶ [Expert Info (Warning/Malformed): ET POLICY PE EXE or DLL Windows file download HTTP]

```
0000  00 54 00 12 34 57 00 d0 b7 61 2d 8f 08 00 45 00  .T..4W..a...E.
0010  05 dc 15 62 40 00 6c 06 b6 23 3d bf 3d 28 c0 a8  ..b@.l. .#.=(..
0020  02 07 00 50 04 43 57 24 5a ee 68 9f 25 55 50 10  ...P.CWS Z.h.%UP.
0030  ff 3b 45 d1 00 00 48 54 54 50 2f 31 2e 31 20 32  ;E...HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 43 6f 6e 74 65 6e 74 2d 4c  00 OK..C ontent-L
```

• SID (suricata.alert.sid) Packets: 1354508 · Displayed: 1354508 (100.0%) · Load time: 0:15.332 Profile: Default

Also get extracted metadata

115	12.920748	10.3.1.1	10.3.1.2	TCP	2962445 → 56746 [ACK] Seq=25185 Ack=3
116	12.920753	10.3.1.1	10.3.1.2	SMB2	363 Read Response
117	12.924091	10.3.1.2	10.3.1.1	TCP	78 [TCP Window Update] 56746 → 445 [
118	12.924096	10.3.1.2	10.3.1.1	TCP	66 56746 → 445 [ACK] Seq=3604 Ack=28
119	12.924743	10.3.1.2	10.3.1.1	SMB2	158 Close Request File: file69.txt
120	12.928852	10.3.1.1	10.3.1.2	SMB2	194 Close Response
121	12.932295	10.3.1.2	10.3.1.1	SMB2	254 Create Request File: file69.txt

- ▶ Frame 120: 194 bytes on wire (1552 bits), 194 bytes captured (1552 bits)
- ▶ Ethernet II, Src: 6e:a8:a8:d3:75:ec (6e:a8:a8:d3:75:ec), Dst: a6:96:79:5e:31:ba (a6:96:79:5e:31:ba)
- ▶ Internet Protocol Version 4, Src: 10.3.1.1, Dst: 10.3.1.2
- ▶ Transmission Control Protocol, Src Port: 445, Dst Port: 56746, Seq: 28378, Ack: 3696, Len: 128
- ▶ NetBIOS Session Service
- ▶ SMB2 (Server Message Block Protocol version 2)
- ▼ Suricata SMB Info
 - SMB Command: SMB2_COMMAND_READ
 - SMB Filename: file69.txt
 - SMB Share: \\10.3.1.1\public
 - SMB Status: STATUS_SUCCESS
- ▼ Suricata File Info
 - Fileinfo filename: file69.txt
 - Fileinfo magic: ASCII text, with very long lines
 - Fileinfo sha1: a3b69227c4a176882144ffd0daf60bd8d57375d
 - Fileinfo size: 3109
 - Fileinfo stored: false

Filter is working

suricata.fileinfo.sha1 == "510dbcb0d481c60a7432e71b29b0a17cf08fb14f" Expression...

No.	Time	Source	Destination	Protocol	Length	SID	Info
4059	12705.193248	192.168.2.7	61.191.61.40	TCP	54		1091 → 80 [ACK] Seq=295 Ack=81856 Win=17520 Len=

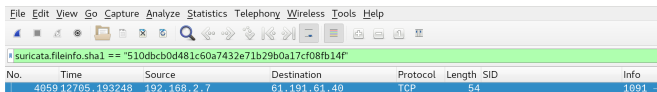
Internet Protocol Version 4, Src: 192.168.2.7, Dst: 61.191.61.40
Transmission Control Protocol, Src Port: 1091, Dst Port: 80, Seq: 295, Ack: 81856, Len: 0
Suricata HTTP Info
HTTP URL: /ww/aa3.exe
HTTP hostname: vcrvcr.3322.org
HTTP user agent: MyIE/1.0
HTTP Content Type: application/octet-stream
HTTP Method: GET
HTTP Protocol: HTTP/1.1
HTTP Status: 200
HTTP Length: 25616
Suricata File Info
Fileinfo filename: /ww/aa3.exe
Fileinfo magic: PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
Fileinfo sha1: 510dbcb0d481c60a7432e71b29b0a17cf08fb14f
Fileinfo size: 25616
Fileinfo stored: false

```
0000 00 d0 b7 61 2d 8f 00 54 00 12 34 57 08 00 45 00  ...a-.T..4W..E.  
0010 00 28 09 4b 40 00 80 06 b3 ee c0 a8 02 07 3d bf  .(.K@... ..==.  
0020 3d 28 04 43 00 50 68 9f 25 b7 57 25 27 93 50 10  =(.C.Ph. %W%'P.  
0030 44 70 1c 2c 00 00                                Dp,...
```

Fileinfo sha1 (suricata.fileinfo.sha1) Packets: 1354508 · Displayed: 1 (0.0%) · Marked: 1 (0.0%) · Load time: 0:18.357 Profile: Default

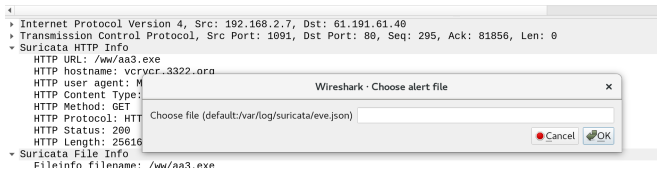
How it works

- Wireshark plugin written in Lua
- Load JSON file generated by Suricata (via Tools->Suricata->Activate)
- Add a new top domain protocol named suricata



The screenshot shows the Wireshark interface with a packet capture table. The table has columns for No., Time, Source, Destination, Protocol, Length, SID, and Info. A row is highlighted in blue, representing a TCP packet.

No.	Time	Source	Destination	Protocol	Length	SID	Info
4059	12705.193248	192.168.2.7	61.191.61.40	TCP	54		1091 →



The screenshot shows the packet details pane in Wireshark. The selected packet is an Internet Protocol Version 4, Src: 192.168.2.7, Dst: 61.191.61.40. The details pane shows the following information:

- Internet Protocol Version 4, Src: 192.168.2.7, Dst: 61.191.61.40
- Transmission Control Protocol, Src Port: 1091, Dst Port: 80, Seq: 295, Ack: 81856, Len: 0
- Suricata HTTP Info
 - HTTP URL: /wm/aa3.exe
 - HTTP hostname: vcrvr.3322.org
 - HTTP user agent: M
 - HTTP Content Type:
 - HTTP Method: GET
 - HTTP Protocol: HTTP
 - HTTP Status: 200
 - HTTP Length: 25616
- Suricata File Info
 - Fileinfo filename: /wm/aa3.exe

A dialog box titled "Wireshark - Choose alert file" is open over the details pane. It contains a text field with the text "Choose file (default:/var/log/suricata/eve.json)" and "Cancel" and "OK" buttons.

Questions ?



Thanks to

- anonymous NSA agent
- Wireshark team
- OISF and Suricata team

Contact me

- el@stamus-networks.com
- Twitter: @regiteric

Get it, use it

- <https://github.com/regit/suriwire>