

WIRESHARK ANALYSIS

6669_MachineLearning.pcap											
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help											
Apply a display filter ... <Ctrl-/> Expression... +											
No.	Time	Source	Destination	Protocol	Length	Host	Destination Port	Source Port	Time delta from previous captured frame	Info	
6020	301.601936	172.16.4.193	198.105.121.50	TCP	60				9.294365000	49222 → 80	[FIN, ACK] Seq=
6021	301.602130	172.16.4.193	198.105.121.50	TCP	60				0.000194000	49224 → 80	[FIN, ACK] Seq=
6022	301.602380	172.16.4.193	198.105.121.50	TCP	60				0.000250000	49220 → 80	[FIN, ACK] Seq=
6023	301.602393	172.16.4.193	198.105.121.50	TCP	60				0.000013000	49221 → 80	[FIN, ACK] Seq=
6024	301.770777	198.105.121.50	172.16.4.193	TCP	54				0.168384000	80 → 49222	[ACK] Seq=40333
6025	301.773648	198.105.121.50	172.16.4.193	TCP	54				0.002871000	80 → 49220	[ACK] Seq=30212
6026	301.775716	198.105.121.50	172.16.4.193	TCP	54				0.002068000	80 → 49224	[ACK] Seq=25851
6027	301.776221	198.105.121.50	172.16.4.193	TCP	54				0.000505000	80 → 49221	[ACK] Seq=19296
6028	403.168205	74.125.141.100	172.16.4.193	TCP	54				101.391984000	80 → 49218	[FIN, ACK] Seq=
6029	403.168631	172.16.4.193	74.125.141.100	TCP	60				0.000426000	49218 → 80	[ACK] Seq=1 Ack
6030	403.168934	74.125.141.100	172.16.4.193	TCP	54				0.000303000	80 → 49217	[FIN, ACK] Seq=
6031	403.169078	172.16.4.193	74.125.141.100	TCP	60				0.000144000	49217 → 80	[ACK] Seq=1217
6032	403.429842	74.125.141.100	172.16.4.193	TCP	54				0.260764000	443 → 49219	[FIN, ACK] Seq=
6033	403.430014	172.16.4.193	74.125.141.100	TCP	60				0.000172000	49219 → 443	[ACK] Seq=1538

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help



http.request

Expression...

No.	Time	Source	Destination	Protocol	Length	Host	Destination Port	Source Port	Time delta from previous captured frame	Info
2688	94.390289	172.16.4.193	104.28.18.74	HTTP	499	www.homeimprovement.com			0.000208000	GET /wp-content/themes/arr
2731	94.395632	172.16.4.193	104.28.18.74	HTTP	538	www.homeimprovement.com			0.000942000	GET /wp-content/themes/arr
2733	94.399381	172.16.4.193	104.28.18.74	HTTP	536	www.homeimprovement.com			0.001589000	GET /wp-content/themes/arr
2734	94.399630	172.16.4.193	104.28.18.74	HTTP	536	www.homeimprovement.com			0.000249000	GET /wp-content/themes/arr
2806	94.535879	172.16.4.193	139.59.160.143	HTTP	419	retrotip.visionurbana.com.ve			0.000249000	GET /engine/classes/js/dle
2812	94.793727	172.16.4.193	104.28.18.74	HTTP	535	www.homeimprovement.com			0.071400000	GET /wp-includes/js/wp-emc
2819	94.842020	172.16.4.193	104.28.18.74	HTTP	503	www.homeimprovement.com			0.023753000	GET /wp-content/themes/arr
2838	94.910186	172.16.4.193	74.125.141.100	HTTP	400	www.google-analytics.com			0.000245000	GET /analytics.js HTTP/1.1
2841	94.911064	172.16.4.193	74.125.141.100	HTTP	393	www.google-analytics.com			0.000341000	GET /ga.js HTTP/1.1
2852	94.997940	172.16.4.193	194.87.234.129	HTTP	605	tyu.benme.com			0.000470000	GET /?ct=Valdi&biw=Val
2896	95.005679	172.16.4.193	194.87.234.129	HTTP	593	tyu.benme.com			0.000798000	GET /?q=zn_QMvXcJwDQoG
2909	95.149378	172.16.4.193	74.125.141.100	HTTP	1294	www.google-analytics.com			0.017491000	GET /r/_utm.gif?utmwv=5.6
2930	95.279780	172.16.4.193	104.28.18.74	HTTP	690	www.homeimprovement.com			0.022766000	GET /wp-content/themes/arr
2936	95.370478	172.16.4.193	194.87.234.129	HTTP	611	tyu.benme.com			0.010705000	POST /?biw=Mozilla.102kd74
2937	95.380031	172.16.4.193	194.87.234.129	HTTP	612	tyu.benme.com			0.009553000	POST /?oq=CEh3h8_svK7pSP1L
3108	116.415349	172.16.4.193	194.87.234.129	HTTP	754	tyu.benme.com			6.685430000	GET /?biw=SeaMonkey.105qj6
3109	116.486279	172.16.4.193	194.87.234.129	HTTP	735	tyu.benme.com			0.070930000	GET /?biw=Amaya.126qv100.4
3174	117.999230	172.16.4.193	66.152.103.73	HTTP	291	fpdownload2.macromedia.com			0.000246000	GET /get/flashplayer/updat
3178	118.125512	172.16.4.193	194.87.234.129	HTTP	524	tyu.benme.com			0.000246000	GET /?ct=Mozilla&tuif=3375
3186	118.688847	172.16.4.193	194.87.234.129	HTTP	530	tyu.benme.com			0.000245000	GET /?yus=SeaMonkey.115uv6
3824	124.793396	172.16.4.193	5.188.223.104	HTTP	595	spotsbill.com			0.000348000	GET /find.php?g=2054955049
5133	139.244923	172.16.4.193	107.23.24.131	HTTP	408	api.blockcypher.com			0.000361000	GET /v1/btc/main/addr/17c
5160	139.452181	172.16.4.193	107.23.24.131	HTTP	436	api.blockcypher.com			0.016565000	GET /v1/btc/main/txs/314ff
5168	139.838813	172.16.4.193	198.105.121.50	HTTP	395	p27dokhpz2n7nvgr.1jw21x.top			0.000245000	GET /EE7E-AD39-7D8C-080C-1
5238	162.648759	172.16.4.193	104.28.18.74	HTTP	946	www.homeimprovement.com			0.000456000	GET /remodeling-your-kitch
5261	163.051445	172.16.4.193	74.125.141.100	HTTP	1270	www.google-analytics.com			0.000247000	GET /_utm.gif?utmwv=5.6.7
5269	163.080771	172.16.4.193	194.87.234.129	HTTP	605	tyu.benme.com			0.000313000	GET /?ct=Valdi&biw=Val
5271	163.081270	172.16.4.193	194.87.234.129	HTTP	593	tyu.benme.com			0.000249000	GET /?q=zn_QMvXcJwDQoG
5297	163.438605	172.16.4.193	194.87.234.129	HTTP	632	tyu.benme.com			0.009512000	POST /?br_fl=3395&tuif=548
5298	163.445102	172.16.4.193	194.87.234.129	HTTP	632	tyu.benme.com			0.006497000	POST /?br_fl=19298oq=2aCm
5451	181.852622	172.16.4.193	198.105.121.50	HTTP	340	p27dokhpz2n7nvgr.1jw21x.top			0.000245000	GET /EE7E-AD39-7D8C-080C-1
5457	182.511511	172.16.4.193	198.105.121.50	HTTP	350	p27dokhpz2n7nvgr.1jw21x.top			0.042495000	GET /EE7E-AD39-7D8C-080C-1
5461	182.981100	172.16.4.193	198.105.121.50	HTTP	441	p27dokhpz2n7nvgr.1jw21x.top			0.037654000	GET /EE7E-AD39-7D8C-080C-1
5467	183.360711	172.16.4.193	198.105.121.50	HTTP	414	p27dokhpz2n7nvgr.1jw21x.top			0.003326000	GET /media/bs3/css/bootstr
5468	183.361049	172.16.4.193	198.105.121.50	HTTP	398	p27dokhpz2n7nvgr.1jw21x.top			0.000338000	GET /media/style.css HTTP/
5474	183.530715	172.16.4.193	198.105.121.50	HTTP	441	p27dokhpz2n7nvgr.1jw21x.top			0.000243000	GET /media/images/logo.png
5517	184.650979	172.16.4.193	198.105.121.50	HTTP	439	p27dokhpz2n7nvgr.1jw21x.top			0.024648000	GET /media/images/bg.jpg H
5518	184.671713	172.16.4.193	198.105.121.50	HTTP	435	p27dokhpz2n7nvgr.1jw21x.top			0.020734000	GET /media/flags.gif HTTP/

	Host	
1e46ba9c0151d4d34a7939daabd778ad.clo.footprintdns.com	2.0	
2.bing.com	1.0	
3a0849dbc3c36a673eb2ddd2fcf0494a.clo.footprintdns.com	2.0	
40bbdaf00bf29a6114a5019e397a2a15.clo.footprintdns.com	2.0	
6b8960d1b061131b015f93f32d0a56f4.clo.footprintdns.com	2.0	
a4.bing.com	1.0	
apl.blockcypher.com	2.0	
da6ab9a9cf82c8f939081a82c7d90031.clo.footprintdns.com	2.0	
e623e8223493b6793a476840214720b1.clo.footprintdns.com	2.0	
fdownload2.macromedia.com	1.0	
p27dokhpz2n7nvgr.1jw2lx.top	24.0	
report.footprintdns.com	2.0	
retrotip.visionurbana.com.ve	1.0	
spotsbill.com	2.0	
tse1.mm.bing.net	4.0	
tyu.benme.com	15.0	
www.bing.com	78.0	
www.google-analytics.com	4.0	
www.homeimprovement.com	17.0	
www.msftncsi.com	1.0	



p27dokhpz2n7nvgr.1jw2lx.top



Todos

Imágenes

Maps

Videos

Noticias

Más

Preferencias

Herramientas

Cerca de 191 resultados (0.51 segundos)

Cerber Payment Site: p27dokhpz2n7nvgr.1jw2lx.top

<https://ransomwaretracker.abuse.ch/.../p27dokhpz2n7nvgr.1jw2lx...> ▼ Traducir esta página

27 ene. 2017 - Cerber Payment Site: p27dokhpz2n7nvgr.1jw2lx.top. Threat: Payment Site.

Malware: Cerber. URL: http://p27dokhpz2n7nvgr.1jw2lx.top.

Src IP	SPort	Dst IP	DPort	Pr	Event Message
104.211.160.15	80	172.16.4.193	49190	6	GPL WEB_CLIENT web bug 0x0 gif attempt
138.91.83.37	80	172.16.4.193	49184	6	GPL WEB_CLIENT web bug 0x0 gif attempt
104.28.18.74	80	172.16.4.193	49195	6	ET CURRENT_EVENTS Evil Redirector Leading to EK Jul 12 2016
104.28.18.74	80	172.16.4.193	49195	6	ETPRO CURRENT_EVENTS Evil Redirect to RIG-v EK Oct 24 2016
172.16.4.193	49202	194.87.234.129	80	6	ET CURRENT_EVENTS RIG EK URI struct Oct 24 2016 (RIG-v)
194.87.234.129	80	172.16.4.193	49202	6	ETPRO CURRENT_EVENTS RIG EK Landing Pre-filter (Rig-v)
194.87.234.129	80	172.16.4.193	49202	6	ET CURRENT_EVENTS RIG EK Landing Sep 12 2016 T2
194.87.234.129	80	172.16.4.193	49202	6	ETPRO CURRENT_EVENTS RIG EK Landing Nov 30 2016 (RIG-v)
194.87.234.129	80	172.16.4.193	49209	6	ETPRO CURRENT_EVENTS RIG/Sundown/Xer EK Payload Jul 06 2...

3 of 10

6669_MachineLearning.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request and ip.addr == 194.87.234.129

No.	Time	Source	Destination	Protocol	Length	Host	Destination Port	Source Port	Time delta from previous captured frame	Info
2852	94.997940	172.16.4.193	194.87.234.129	HTTP	695	tyu.benme.com			0.000470000	GET /?ct=Vivaldi&biw=Vivaldi
2896	95.005679	172.16.4.193	194.87.234.129	HTTP	593	tyu.benme.com			0.000798000	GET /?q=zn_QMvXcJwDQDofGMv
2936	95.370478	172.16.4.193	194.87.234.129	HTTP	611	tyu.benme.com			0.010705000	POST /?biw=Mozilla.102kd74
2937	95.380031	172.16.4.193	194.87.234.129	HTTP	612	tyu.benme.com			0.009553000	POST /?oq=CEh3h8_svk7pSP1l
3108	116.415349	172.16.4.193	194.87.234.129	HTTP	754	tyu.benme.com			6.685430000	GET /?biw=SeaMonkey.105qj6
3109	116.486279	172.16.4.193	194.87.234.129	HTTP	735	tyu.benme.com			0.070930000	GET /?biw=Amaya.126qv100.4
3178	118.125512	172.16.4.193	194.87.234.129	HTTP	524	tyu.benme.com			0.000246000	GET /?ct=Mozilla&tuif=3375
3186	118.688847	172.16.4.193	194.87.234.129	HTTP	530	tyu.benme.com			0.000245000	GET /?yus=SeaMonkey.115uv8
5269	163.080771	172.16.4.193	194.87.234.129	HTTP	695	tyu.benme.com			0.000313000	GET /?ct=Vivaldi&biw=Vivaldi
5271	163.081270	172.16.4.193	194.87.234.129	HTTP	593	tyu.benme.com			0.000249000	GET /?q=zn_QMvXcJwDQDofGMv
5297	163.438065	172.16.4.193	194.87.234.129	HTTP	632	tyu.benme.com			0.009512000	POST /?br_fl=3395&tuif=548
5298	163.445102	172.16.4.193	194.87.234.129	HTTP	632	tyu.benme.com			0.006497000	POST /?br_fl=1929&oq=2aCm3
5520	184.817181	172.16.4.193	194.87.234.129	HTTP	765	tyu.benme.com			0.002059000	GET /?tuif=2138&br_fl=1788
5521	184.857556	172.16.4.193	194.87.234.129	HTTP	768	tyu.benme.com			0.040375000	GET /?oq=pLLYG0AS3jxbTfgNp
5613	187.251521	172.16.4.193	194.87.234.129	HTTP	533	tyu.benme.com			0.000245000	GET /?br_fl=5844&tuif=5862

Identification: 0x05f5 (1525)

- Flags: 0x4000, Don't fragment
- Time to live: 128
- Protocol: TCP (6)
- Header checksum: 0x9509 [validation disabled]
- [Header checksum status: Unverified]
- Source: 172.16.4.193
- Destination: 194.87.234.129

Transmission Control Protocol, Src Port: 49202, Dst Port: 80, Seq: 1, Ack: 1, Len: 551

Hypertext Transfer Protocol

- [Truncated]GET /?ct=Vivaldi&biw=Vivaldi.95ec76.406i7c5k7&oq=h8fItKeRvawGyjRaFcw1nyYdeAwgQ8_qtiEKBzBKfgz6D-hyMAZih16LRVvQ42w&tuif=2320&q=wH7QMvXcJwDNFYbGMvrER6NbNknQA0KxpH2_drZdZqxK6ni20b5UUSk6FqCEh
- Accept: text/html, application/xhtml+xml, */*\r\n
- Referer: http://www.homeimprovement.com/remodeling-your-kitchen-cabinets.html\r\n
- Accept-Language: en-US\r\n
- User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko\r\n
- Accept-Encoding: gzip, deflate\r\n

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help



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

Expression... +

No.	Time	Source	Destination	Protocol	Length	Host	Destination Port	Source Port	Time delta from previous captured frame	Info
3991	129.352477	172.16.4.193	90.2.1.17	UDP	67		6892	58978	0.000012000	58978 → 6892 Len=25
3992	129.352488	172.16.4.193	90.2.1.18	UDP	67		6892	58978	0.000011000	58978 → 6892 Len=25
3993	129.352499	172.16.4.193	90.2.1.19	UDP	67		6892	58978	0.000011000	58978 → 6892 Len=25
3994	129.352510	172.16.4.193	90.2.1.20	UDP	67		6892	58978	0.000011000	58978 → 6892 Len=25
3995	129.352521	172.16.4.193	90.2.1.21	UDP	67		6892	58978	0.000011000	58978 → 6892 Len=25
3996	129.352532	172.16.4.193	90.2.1.22	UDP	67		6892	58978	0.000011000	58978 → 6892 Len=25
3997	129.352543	172.16.4.193	90.2.1.23	UDP	67		6892	58978	0.000011000	58978 → 6892 Len=25
3998	129.352554	172.16.4.193	90.2.1.24	UDP	67		6892	58978	0.000011000	58978 → 6892 Len=25
3999	129.352565	172.16.4.193	90.2.1.25	UDP	67		6892	58978	0.000011000	58978 → 6892 Len=25
4000	129.352576	172.16.4.193	90.2.1.26	UDP	67		6892	58978	0.000011000	58978 → 6892 Len=25
4001	129.352587	172.16.4.193	90.2.1.27	UDP	67		6892	58978	0.000011000	58978 → 6892 Len=25
4002	129.352597	172.16.4.193	90.2.1.28	UDP	67		6892	58978	0.000010000	58978 → 6892 Len=25
4003	129.352608	172.16.4.193	90.2.1.29	UDP	67		6892	58978	0.000011000	58978 → 6892 Len=25
4004	129.352619	172.16.4.193	90.2.1.30	UDP	67		6892	58978	0.000011000	58978 → 6892 Len=25
4005	129.352631	172.16.4.193	90.2.1.31	UDP	67		6892	58978	0.000012000	58978 → 6892 Len=25
4006	129.352643	172.16.4.193	90.3.1.0	UDP	67		6892	58978	0.000012000	58978 → 6892 Len=25
4007	129.352655	172.16.4.193	90.3.1.1	UDP	67		6892	58978	0.000012000	58978 → 6892 Len=25
4008	129.352665	172.16.4.193	90.3.1.2	UDP	67		6892	58978	0.000010000	58978 → 6892 Len=25
4009	129.352676	172.16.4.193	90.3.1.3	UDP	67		6892	58978	0.000011000	58978 → 6892 Len=25
4010	129.352687	172.16.4.193	90.3.1.4	UDP	67		6892	58978	0.000011000	58978 → 6892 Len=25
4011	129.352698	172.16.4.193	90.3.1.5	UDP	67		6892	58978	0.000011000	58978 → 6892 Len=25
4012	129.352709	172.16.4.193	90.3.1.6	UDP	67		6892	58978	0.000011000	58978 → 6892 Len=25
4013	129.352720	172.16.4.193	90.3.1.7	UDP	67		6892	58978	0.000011000	58978 → 6892 Len=25
4014	129.352731	172.16.4.193	90.3.1.8	UDP	67		6892	58978	0.000011000	58978 → 6892 Len=25
4015	129.352742	172.16.4.193	90.3.1.9	UDP	67		6892	58978	0.000011000	58978 → 6892 Len=25
4016	129.352935	172.16.4.193	90.3.1.10	UDP	67		6892	58978	0.000193000	58978 → 6892 Len=25
4017	129.352950	172.16.4.193	90.3.1.11	UDP	67		6892	58978	0.000015000	58978 → 6892 Len=25
4018	129.352961	172.16.4.193	90.3.1.12	UDP	67		6892	58978	0.000011000	58978 → 6892 Len=25
4019	129.352972	172.16.4.193	90.3.1.13	UDP	67		6892	58978	0.000011000	58978 → 6892 Len=25
4020	129.352983	172.16.4.193	90.3.1.14	UDP	67		6892	58978	0.000011000	58978 → 6892 Len=25
4021	129.352994	172.16.4.193	90.3.1.15	UDP	67		6892	58978	0.000011000	58978 → 6892 Len=25
4022	129.353004	172.16.4.193	90.3.1.16	UDP	67		6892	58978	0.000010000	58978 → 6892 Len=25
4023	129.353016	172.16.4.193	90.3.1.17	UDP	67		6892	58978	0.000012000	58978 → 6892 Len=25
4024	129.353026	172.16.4.193	90.3.1.18	UDP	67		6892	58978	0.000010000	58978 → 6892 Len=25
4025	129.353037	172.16.4.193	90.3.1.19	UDP	67		6892	58978	0.000011000	58978 → 6892 Len=25
4026	129.353047	172.16.4.193	90.3.1.20	UDP	67		6892	58978	0.000010000	58978 → 6892 Len=25
4027	129.353058	172.16.4.193	90.3.1.21	UDP	67		6892	58978	0.000011000	58978 → 6892 Len=25
4028	129.353069	172.16.4.193	90.3.1.22	UDP	67		6892	58978	0.000011000	58978 → 6892 Len=25
4029	129.353080	172.16.4.193	90.3.1.23	UDP	67		6892	58978	0.000011000	58978 → 6892 Len=25
4030	129.353091	172.16.4.193	90.3.1.24	UDP	67		6892	58978	0.000011000	58978 → 6892 Len=25
4031	129.353101	172.16.4.193	90.3.1.25	UDP	67		6892	58978	0.000010000	58978 → 6892 Len=25