
ATTACK
DEFENSE
by PentesterAcademy

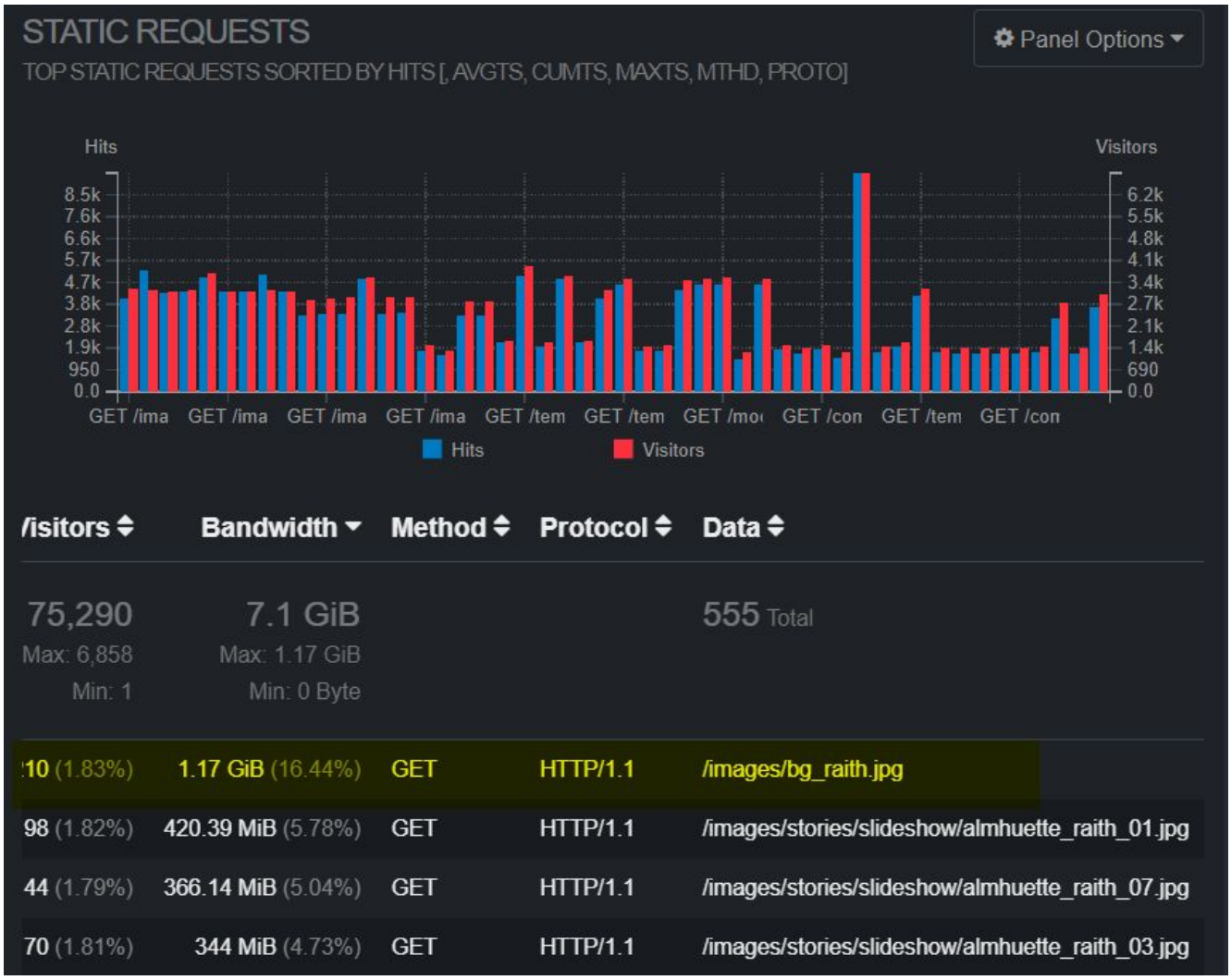
Name	Apache Log Analysis: GoAccess
URL	https://www.attackdefense.com/challengedetails?cid=142
Type	Forensics : Webserver Log Analysis

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic.

Question 1: Which static resource received most requests in terms of bandwidth?

Answer: images/bg_raith.jpg

Solution:

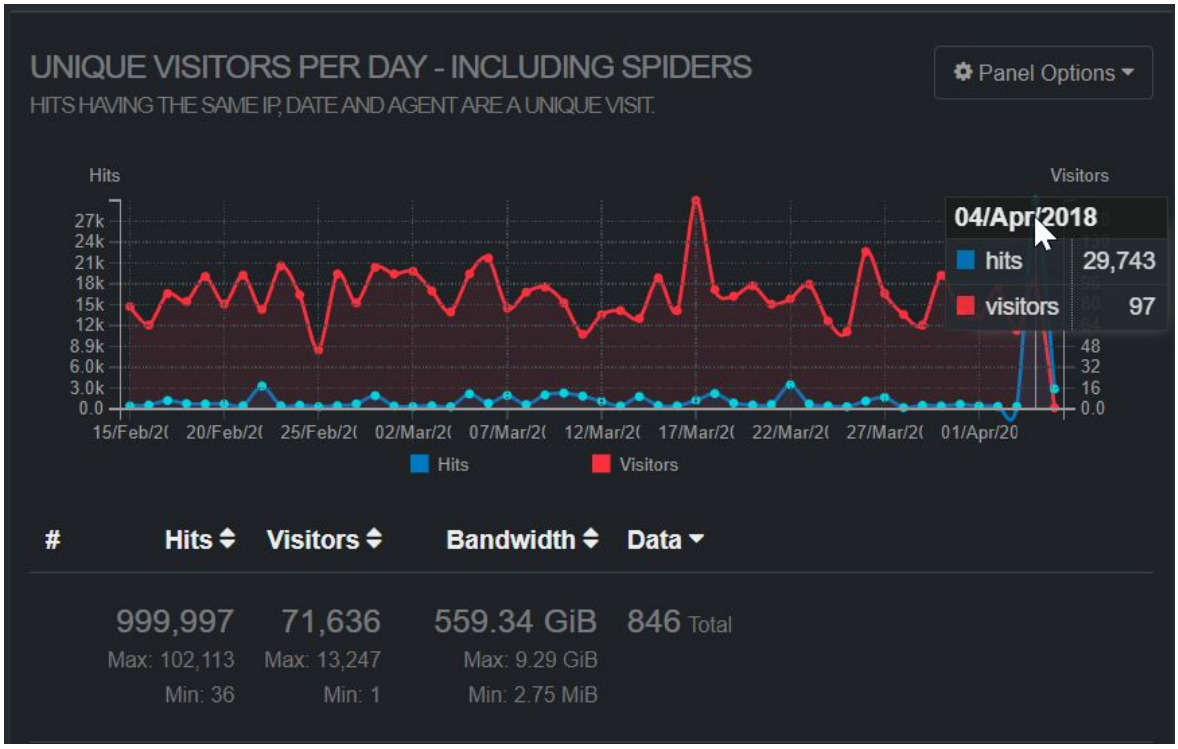


Question 2: The website was targeted with a DoS attack some day ago. Can you pinpoint the date?

Answer: 4th April 2018

Solution:

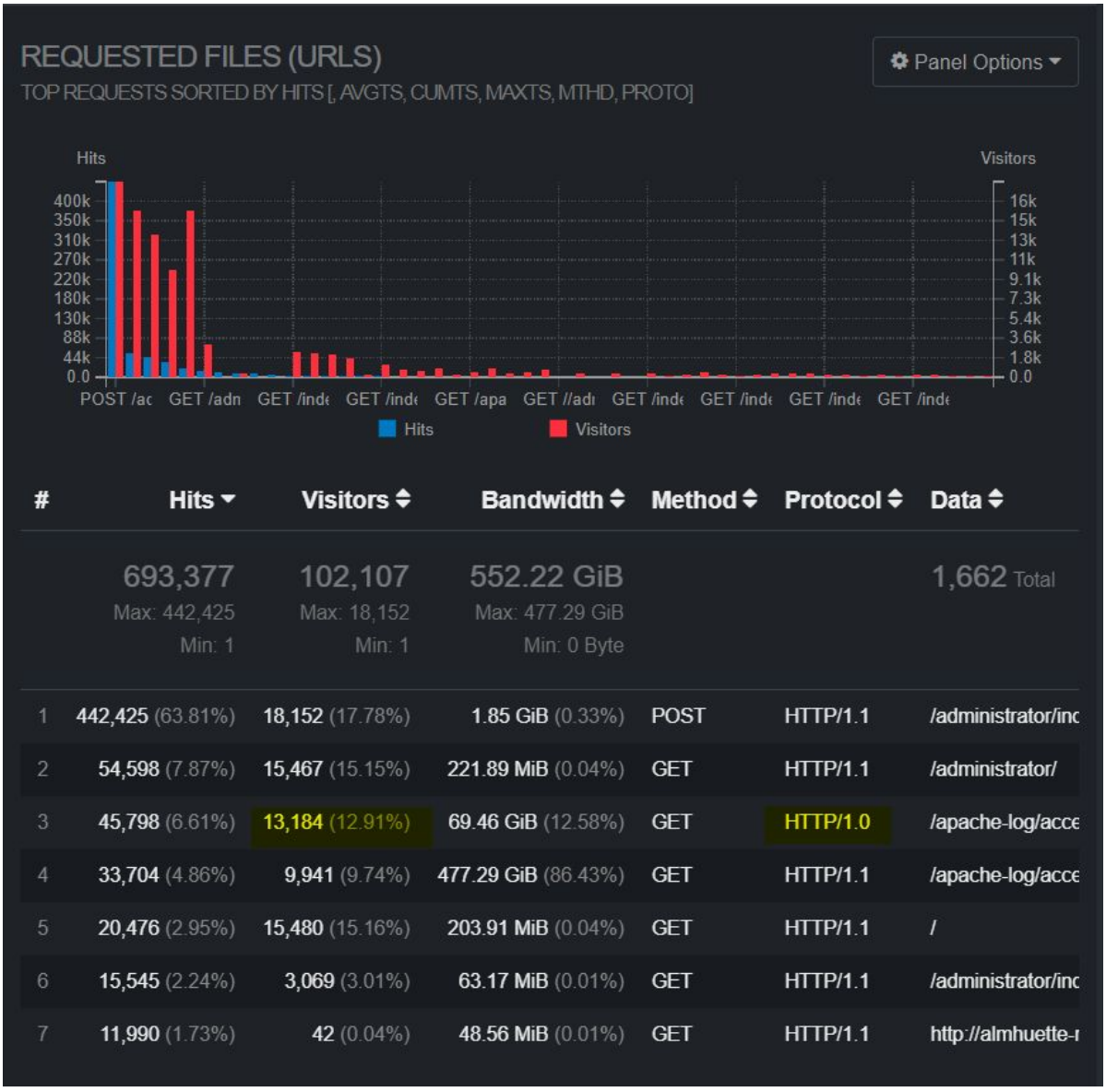
There is a spike in unique visitors per day on 4th April 2018.



Question 3:. What percentage of the visitors accessed the website using HTTP/1.0 protocol?

Answer: 12.91%

Solution:



#	Hits	Visitors	Bandwidth	Method	Protocol	Data
	693,377 Max: 442,425 Min: 1	102,107 Max: 18,152 Min: 1	552.22 GiB Max: 477.29 GiB Min: 0 Byte			1,662 Total
1	442,425 (63.81%)	18,152 (17.78%)	1.85 GiB (0.33%)	POST	HTTP/1.1	/administrator/inc
2	54,598 (7.87%)	15,467 (15.15%)	221.89 MiB (0.04%)	GET	HTTP/1.1	/administrator/
3	45,798 (6.61%)	13,184 (12.91%)	69.46 GiB (12.58%)	GET	HTTP/1.0	/apache-log/acce
4	33,704 (4.86%)	9,941 (9.74%)	477.29 GiB (86.43%)	GET	HTTP/1.1	/apache-log/acce
5	20,476 (2.95%)	15,480 (15.16%)	203.91 MiB (0.04%)	GET	HTTP/1.1	/
6	15,545 (2.24%)	3,069 (3.01%)	63.17 MiB (0.01%)	GET	HTTP/1.1	/administrator/inc
7	11,990 (1.73%)	42 (0.04%)	48.56 MiB (0.01%)	GET	HTTP/1.1	http://almhuette-r

Question 4: Some requests were made to the web server to check if it is hosting a popular CMS. Which CMS the sequesters were looking for?

Answer: WordPress (we can see not found logs for wp-login.php)

Solution:

Question 5: What percentage of hits were originated from Azerbaijan country?

Answer: 0.21%

Solution:

Question 6: Which flavor of the Android OS was used by most of the visitors?

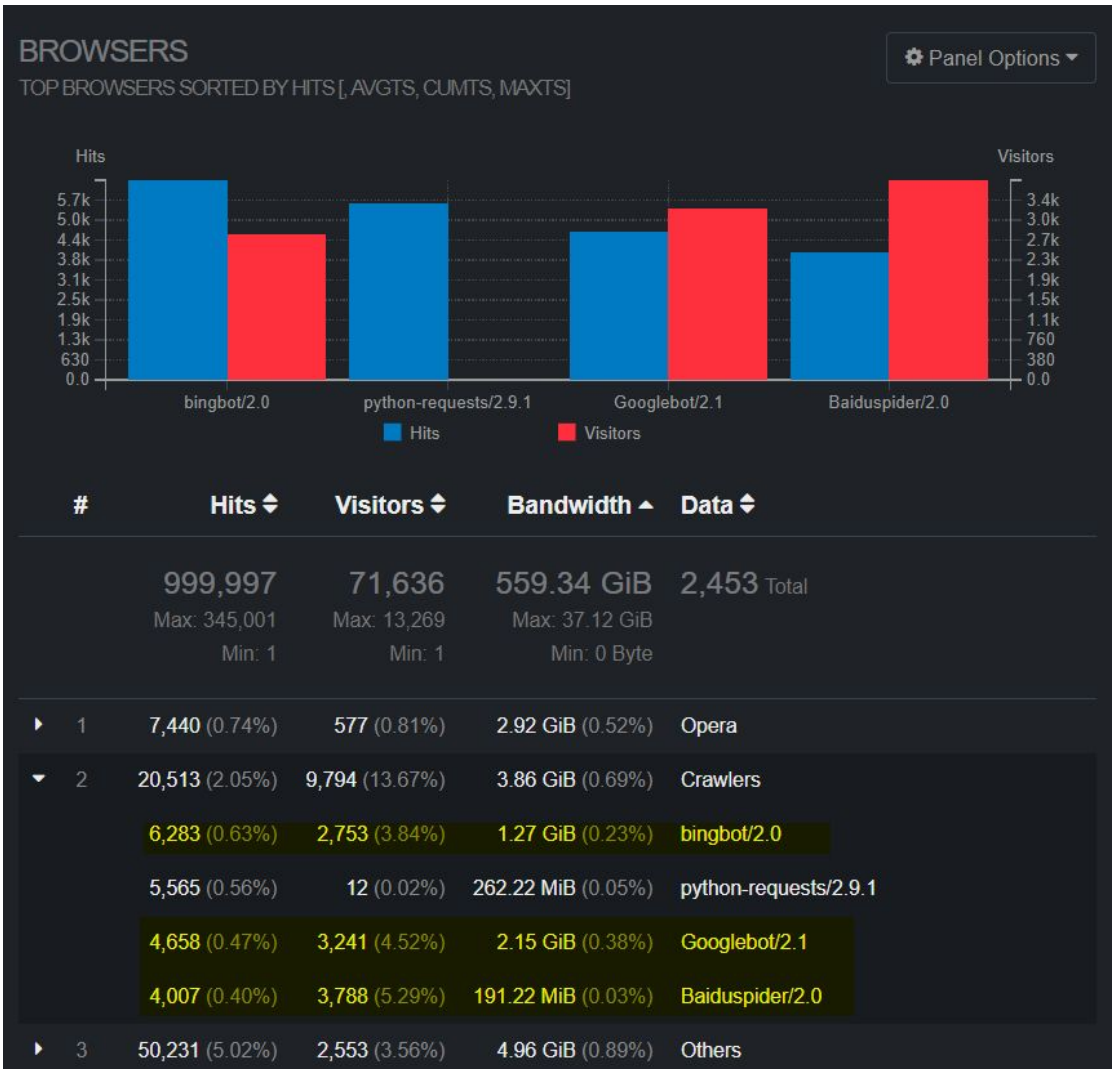
Answer: Marshmallow 6.0.1

Solution:

Question 7: Crawlers of three search engines crawled the website. Can you name the search engines?

Answer: Google, Bing and Baidu

Solution:

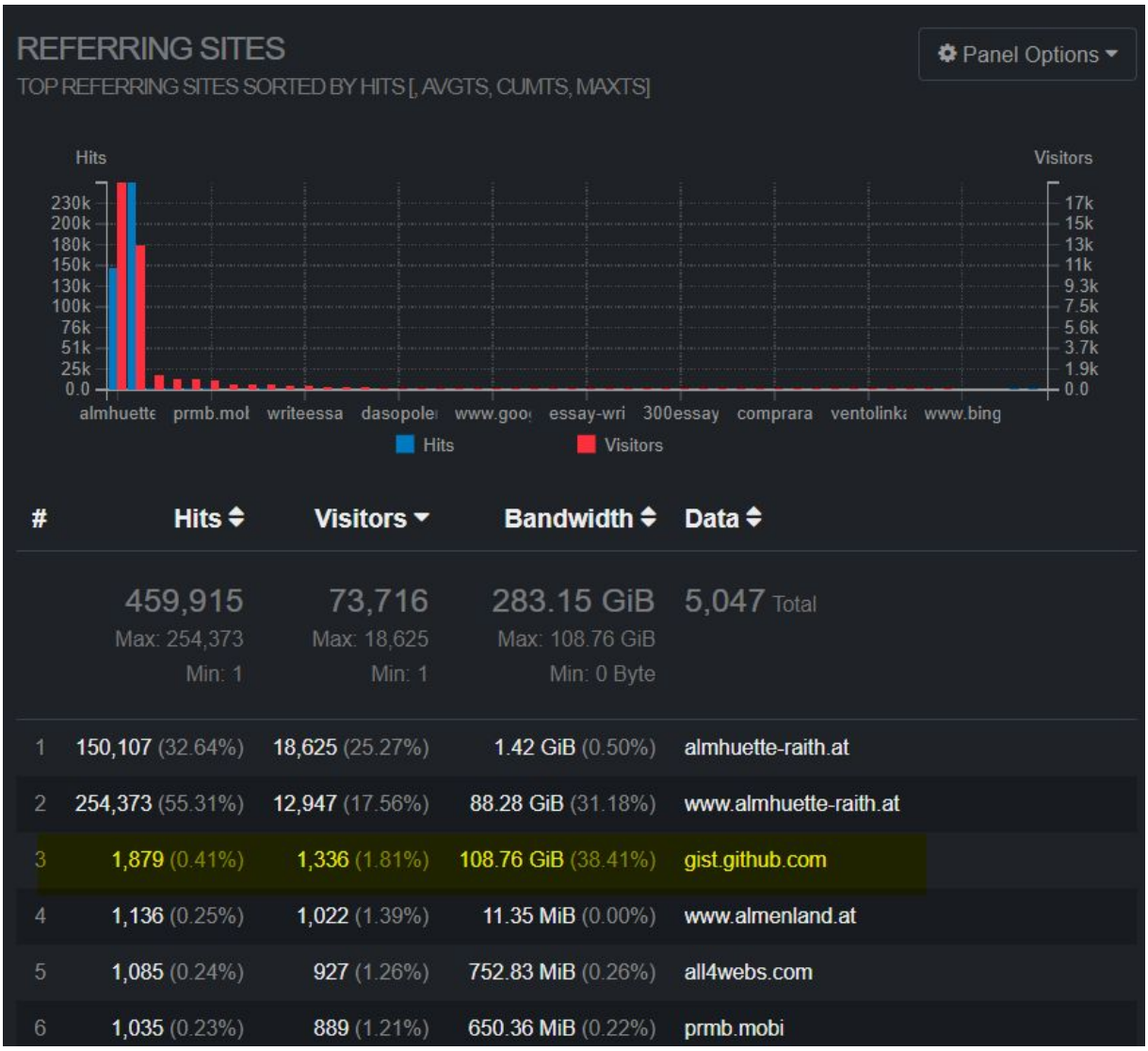


#	Hits	Visitors	Bandwidth	Data
	999,997 Max: 345,001 Min: 1	71,636 Max: 13,269 Min: 1	559.34 GiB Max: 37.12 GiB Min: 0 Byte	2,453 Total
1	7,440 (0.74%)	577 (0.81%)	2.92 GiB (0.52%)	Opera
2	20,513 (2.05%)	9,794 (13.67%)	3.86 GiB (0.69%)	Crawlers
	6,283 (0.63%)	2,753 (3.84%)	1.27 GiB (0.23%)	bingbot/2.0
	5,565 (0.56%)	12 (0.02%)	262.22 MiB (0.05%)	python-requests/2.9.1
	4,658 (0.47%)	3,241 (4.52%)	2.15 GiB (0.38%)	Googlebot/2.1
	4,007 (0.40%)	3,788 (5.29%)	191.22 MiB (0.03%)	Baiduspider/2.0
3	50,231 (5.02%)	2,553 (3.56%)	4.96 GiB (0.89%)	Others

Question 8: Which external website is responsible for sending in most visitors?

Answer: GitHub

Solution:

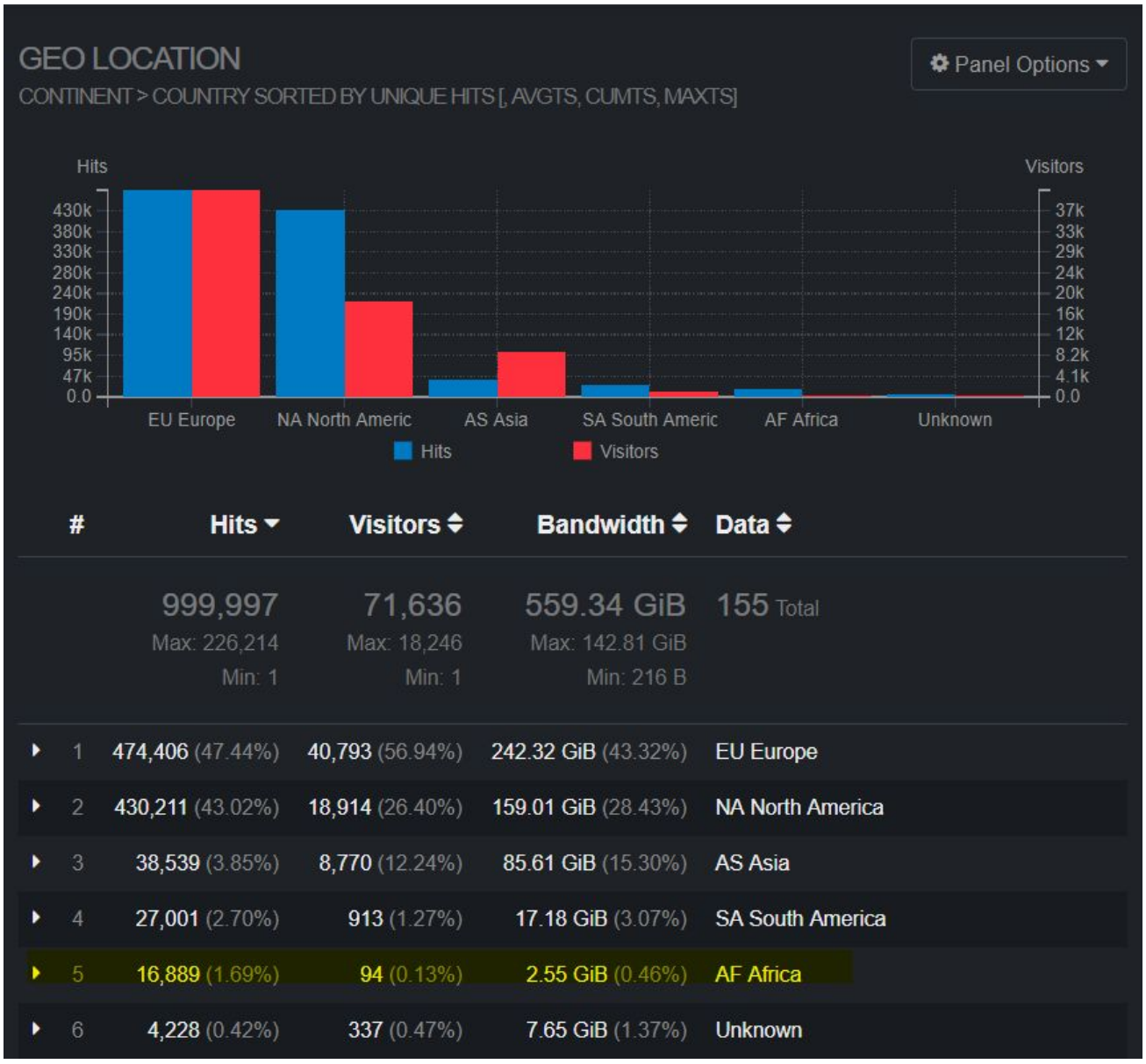


#	Hits	Visitors	Bandwidth	Data
	459,915 Max: 254,373 Min: 1	73,716 Max: 18,625 Min: 1	283.15 GiB Max: 108.76 GiB Min: 0 Byte	5,047 Total
1	150,107 (32.64%)	18,625 (25.27%)	1.42 GiB (0.50%)	almhuette-raith.at
2	254,373 (55.31%)	12,947 (17.56%)	88.28 GiB (31.18%)	www.almhuette-raith.at
3	1,879 (0.41%)	1,336 (1.81%)	108.76 GiB (38.41%)	gist.github.com
4	1,136 (0.25%)	1,022 (1.39%)	11.35 MiB (0.00%)	www.almenland.at
5	1,085 (0.24%)	927 (1.26%)	752.83 MiB (0.26%)	all4webs.com
6	1,035 (0.23%)	889 (1.21%)	650.36 MiB (0.22%)	prmb.mobi

Question 9: What percentage of hits were originated from Africa continent?

Answer: 1.69%

Solution:



#	Hits	Visitors	Bandwidth	Data
	999,997 Max: 226,214 Min: 1	71,636 Max: 18,246 Min: 1	559.34 GiB Max: 142.81 GiB Min: 216 B	155 Total
1	474,406 (47.44%)	40,793 (56.94%)	242.32 GiB (43.32%)	EU Europe
2	430,211 (43.02%)	18,914 (26.40%)	159.01 GiB (28.43%)	NA North America
3	38,539 (3.85%)	8,770 (12.24%)	85.61 GiB (15.30%)	AS Asia
4	27,001 (2.70%)	913 (1.27%)	17.18 GiB (3.07%)	SA South America
5	16,889 (1.69%)	94 (0.13%)	2.55 GiB (0.46%)	AF Africa
6	4,228 (0.42%)	337 (0.47%)	7.65 GiB (1.37%)	Unknown