



<Write-ups>

**Kenji**

**Ringzer0ctf.com**

Category: Forensics

Challenge: [9] 44

"Hey Chuck where is the flag?"

<https://ringzer0ctf.com/challenges/44>

## Contents

<b>1. Challenge .....</b>	<b>3</b>
<b>2. Hint I Bought .....</b>	<b>3</b>
<b>3. Tools &amp; References.....</b>	<b>3</b>
<b>4. CTF .....</b>	<b>3</b>

Hey Chuck where is the flag?

Download pcap file

Submit flag

Challenge flag

Flag

Submit »

Last user who solved this challenge kenji

View users write up for this challenge

Submit a write up »

Need help with this challenge?

Buy hint »

Hint for "Hey Chuck where is the flag?" HTTP uses gzip compression sometime.

- Wireshark
- cat

> Let's check the pcap first:

No.	Time	Source	Destination	Protocol	Source Port	Dest Port	Info
187	18.106662	10.0.75.102	10.0.85.10	HTTP	3280	00	GET /askidjlls1234.php HTTP/1.1
13	0.422260	10.0.75.102	100.178.19.195	HTTP	3263	00	GET /image_cache/w.familio.com/73caal47baa2e4e01d2547610071b6f_thumb_jessica-Alba-5-620x400.jpg HTTP/1.1
14	0.431570	10.0.75.102	100.178.19.195	HTTP	3264	00	GET /image_cache/w.familio.com/75a1f51dee2f12f46ef40051163d7f_thumb_ryan-rez40x400.jpg HTTP/1.1
15	0.432110	10.0.75.102	100.178.19.195	HTTP	3265	00	GET /image_cache/membershealth.com/1ab635f1074699f1_thumb_momandadad-200x200.jpg HTTP/1.1
16	0.442172	10.0.75.102	100.178.19.195	HTTP	3266	00	GET /image_cache/recommended-sportsbooks.com/87b00945408440381631440F567879_thumb_Sportsbetting.jpg HTTP/1.1
407	0.230699	10.0.75.102	173.194.46.18	HTTP	3217	00	GET /url?url=srcr-jk4&src=sourcewebdc&lkved=0CCqfJAAJurl=http%3A%2F%2Fwww.chucknorrisfacts.fr&2f&el=X3U1113jg&dw9&g&gusagw/QjCMUdL531ShovgrAIG0B2t&K5G74aig2Dp-
407	0.415979	10.0.75.102	199.16.131.120	HTTP	3269	00	GET / HTTP/1.1
45	0.752574	10.0.75.102	199.16.131.120	HTTP	3270	00	GET /css/csstyle.css HTTP/1.1
467	0.525476	10.0.75.102	199.16.131.120	HTTP	3272	00	GET /css/lightbox.css HTTP/1.1
467	0.525974	10.0.75.102	199.16.131.120	HTTP	3271	00	GET /js/jquery-1.8.1.min.js HTTP/1.1
467	0.529916	10.0.75.102	199.16.131.120	HTTP	3274	00	GET /js/lightbox/jquery-ui-1.8.18.custom.min.js HTTP/1.1
407	0.529916	10.0.75.102	199.16.131.120	HTTP	3273	00	GET /js/lightbox/jquery.smooth-scroll.min.js HTTP/1.1
507	0.535331	10.0.75.102	199.16.131.120	HTTP	3275	00	GET /js/lightbox/lightbox.js HTTP/1.1
393	0.667714	10.0.75.102	199.16.131.120	HTTP	3270	00	GET /img/upload/04eb0e455485f.jpg HTTP/1.1
1427	0.787802	10.0.75.102	199.16.131.120	HTTP	3272	00	GET /img/upload/04eb0e455485f.jpg HTTP/1.1
1427	0.787802	10.0.75.102	199.16.131.120	HTTP	3270	00	GET /img/header.png HTTP/1.1
1437	0.787802	10.0.75.102	199.16.131.120	HTTP	3272	00	GET /img/q.png HTTP/1.1
1447	0.915055	10.0.75.102	199.16.131.120	HTTP	3276	00	GET /img/lightbox/loading.gif HTTP/1.1
1457	0.915055	10.0.75.102	199.16.131.120	HTTP	3277	00	GET /img/lightbox/close.png HTTP/1.1
1467	0.916474	10.0.75.102	199.16.131.120	HTTP	3278	00	GET /img/lightbox/close.png HTTP/1.1
189	0.920851	10.0.75.102	199.16.131.120	HTTP	3281	00	GET /facts HTTP/1.1
194	0.1373309	10.0.75.102	199.16.131.120	HTTP	3282	00	GET /js/vote.js HTTP/1.1
195	0.1740479	10.0.75.102	199.16.131.120	HTTP	3283	00	GET /js/raty/jquery.raty.js HTTP/1.1
197	0.179069	10.0.75.102	199.16.131.120	HTTP	3287	00	GET /js/effects.js HTTP/1.1
204	0.124046	10.0.75.102	199.16.131.120	HTTP	3285	00	GET /img/social/logo-twitter.png HTTP/1.1
205	0.124046	10.0.75.102	199.16.131.120	HTTP	3284	00	GET /img/social/logo-facebook.png HTTP/1.1
206	0.1242197	10.0.75.102	199.16.131.120	HTTP	3286	00	GET /img/social/google-plus.png HTTP/1.1
216	0.1758250	10.0.75.102	199.16.131.120	HTTP	3286	00	GET /js/raty/img/star-off.png HTTP/1.1
217	0.1758250	10.0.75.102	199.16.131.120	HTTP	3284	00	GET /js/raty/img/star-on.png HTTP/1.1
218	0.1758257	10.0.75.102	199.16.131.120	HTTP	3285	00	GET /js/raty/img/star-half.png HTTP/1.1
219	0.1759084	10.0.75.102	199.16.131.120	HTTP	3288	00	GET /img/lightbox/cancel-off.png HTTP/1.1
1	0.000000	10.0.75.102	204.230.199.68	HTTP	3230	00	GET /p/c1c1-28c2-063645867-http%3A%2F%2Fpfp2eabou2k2comf2Kz2f1fshedsdp12f2f2fencolqpf3k2ntsk&2-10X20u1K207img3K20f200K2u61k220P9C&v=htp3k3K2f2k6w2kegqo1e2-
3	0.161553	10.0.75.102	204.230.199.68	HTTP	3230	00	GET /p/c1c1-28c2-063645867-http%3A%2F%2Fpfp2eabou2k2comf2Kz2f1fshedsdp12f2f2fencolqpf3k2ntsk&2-10X20u1K207img3K20f200K2u61k220P9C&v=htp3k3K2f2k6w2kegqo1e2-
4	0.164444	10.0.75.102	204.230.199.68	HTTP	3230	00	GET /p/c1c1-28c2-063645867-http%3A%2F%2Fpfp2eabou2k2comf2Kz2f1fshedsdp12f2f2fencolqpf3k2ntsk&2-10X20u1K207img3K20f200K2u61k220P9C&v=htp3k3K2f2k6w2kegqo1e2-
7	0.345593	10.0.75.102	74.125.226.233	HTTP	3231	00	GET /collect/v=16jw645512609228&pageview=&1&id=http%3A%2F%2Fpfp2eabou2k2comf2Kz2f1fshedsdp12f2f2fencolqpf3k2ntsk&2-10X20u1K207img3K20f200K2u61k220P9C&v=htp3k3K2f2k6w2kegqo1e2-
10	0.382372	10.0.75.102	74.125.226.233	HTTP	3260	00	GET /collect/v=16jw645512609228&pageview=&1&id=http%3A%2F%2Fpfp2eabou2k2comf2Kz2f1fshedsdp12f2f2fencolqpf3k2ntsk&2-10X20u1K207img3K20f200K2u61k220P9C&v=htp3k3K2f2k6w2kegqo1e2-
214	0.531822	10.0.75.102	74.125.226.233	HTTP	3231	00	GET /p/c1c1-28c2-063645867-http%3A%2F%2Fpfp2eabou2k2comf2Kz2f1fshedsdp12f2f2fencolqpf3k2ntsk&2-10X20u1K207img3K20f200K2u61k220P9C&v=htp3k3K2f2k6w2kegqo1e2-
214	0.531822	10.0.75.102	74.125.226.233	HTTP	3231	00	GET /p/c1c1-28c2-063645867-http%3A%2F%2Fpfp2eabou2k2comf2Kz2f1fshedsdp12f2f2fencolqpf3k2ntsk&2-10X20u1K207img3K20f200K2u61k220P9C&v=htp3k3K2f2k6w2kegqo1e2-

> There's lots of requests coming from multiple sources. After checking the website:

<http://www.chucknorrisfacts.fr/>

⇒ No interest.

(I have check all the image uploaded inside the website. Even those 2 jpg files uploaded shown on pcap:

<http://www.chucknorrisfacts.fr/img/upload/q50abe8d54658f.jpg>

<http://www.chucknorrisfacts.fr/img/upload/q50f9c04804440.jpg>

Because the image is no longer exist, but i can still find it on archive.org:



> Turn out: It's nothing inside and have no flag related.

So...

> After bought the Hint. I find out that I can extract some content/request i cannot see directly on Wireshark by "save" them as gzip and use "cat" command to check them there.

> Right on first try, i have succeeded read the flag with the packet from: 10.0.85.10

```
root@SIFT -> ~/Downloads
# cat askldj3lkj234.gzip
Hey this is a flag FLAG-GehFMsqCeNvof5szVpB2Dmjxroot@SIFT -> ~/Downloads
#
```

> YES! The Flag!

**FLAG-GehFMsqCeNvof5szVpB2Dmjx**

</Thank you>