

Forum:[Hack Forums](#)

Thread: [search google query in wireshark trace](#)

tulamba - April 27, 2018, 8:02 pm

I am stuck in this question. I tried my best but it seems I am not able to find the google query. It seems for some reason, I was not able to decrypt the trace :(

Here is the question

PHP Code

```
<?php
```

Someone performed a Google search, the evidence of which was recorded in the file "https.pcap". What was the one-word search term?
(Hint: You will also need privkey.pem.)

[google.com/file/d/1ghYh5EDndITB-nUgvZ7TNjUR-XpL5YzO/view?usp=sharing](https://drive.google.com/file/d/1ghYh5EDndITB-nUgvZ7TNjUR-XpL5YzO/view?usp=sharing)https.pcap
[google.com/file/d/141Mdr6Y0y2NMO07Fz_DeJm184FOp_BI-/view?usp=sharing](https://drive.google.com/file/d/141Mdr6Y0y2NMO07Fz_DeJm184FOp_BI-/view?usp=sharing)privkey.pem

Any hints or help will be deeply appreciated.

CyberStrike - April 27, 2018, 8:18 pm

Well after you have the ssl cert you need a session key.

<https://jimshaver.net/2015/02/11/decrypting-tls-browser-traffic-with-wireshark-the-easy-way/>

(it's a local variable pretty much give the article a read)

tulamba - April 28, 2018, 6:50 am

(Apr 27, 2018 08:18 PM)sirru5h Wrote: [\[CITE\]](#) Well after you have the ssl cert you need a session key.

<https://jimshaver.net/2015/02/11/decrypting-tls-browser-traffic-with-wireshark-the-easy-way/>

(it's a local variable pretty much give the article a read)

Thanks for your reply. I did go through this article but it didn't help :(

pandass - May 1, 2018, 7:23 pm

I put it in wireshark, added the pem file as a SSH key and one of the decoded files was titled (bunch of text)"toomanysecrets", so I used that