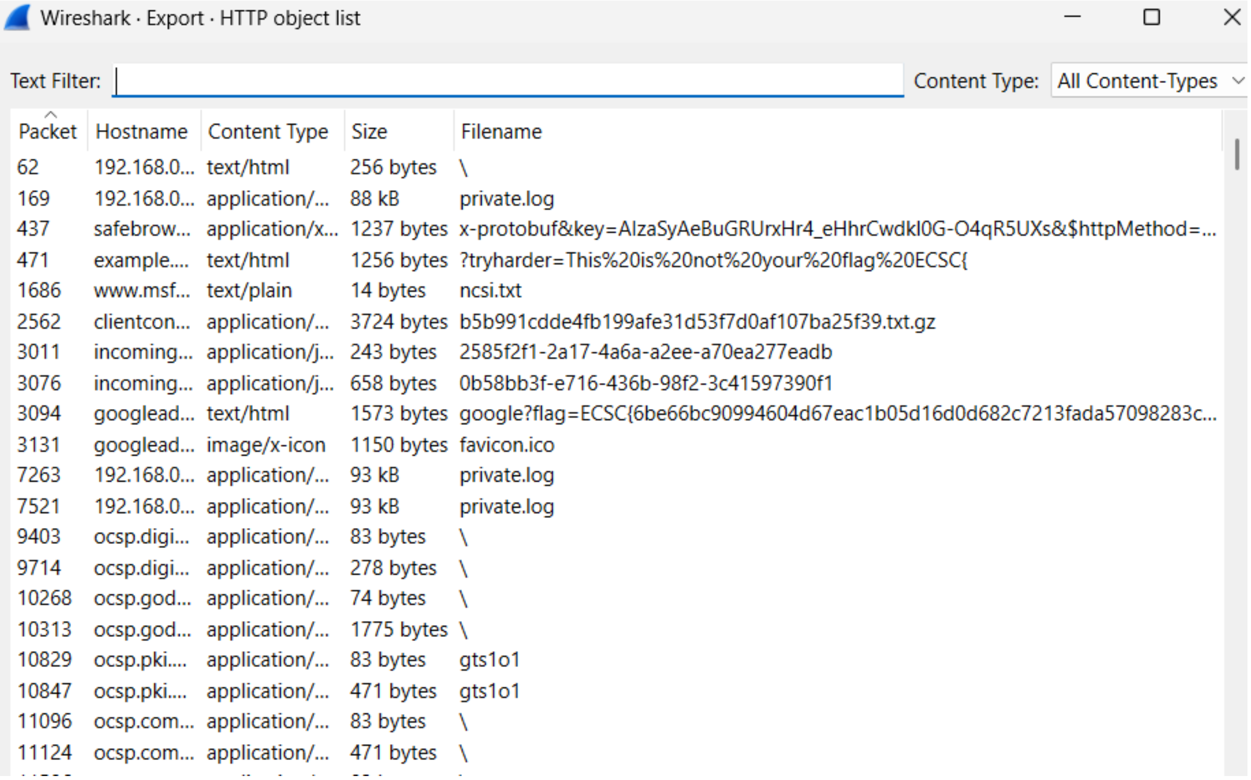
After opening the pcapng and looking through the http objects, we notice 2 different private.log files, with 88KB and 93KB respectively. These files can be used to decrypt TLS traffic (In wireshark, Edit > Preferences> TLS > log file). Using the first one doesn't help, but using the second one and looking through the HTTP objects again:



Text Filter:

Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
62	192.168.0...	text/html	256 bytes	\
169	192.168.0...	application/...	88 kB	private.log
437	safebrow...	application/x...	1237 bytes	x-protobuf&key=AIzaSyAeBuGRUrxHr4_eHhrCwdkI0G-O4qR5UXs&$httpMethod=...
471	example....	text/html	1256 bytes	?tryharder=This%20is%20not%20your%20flag%20ECSC{
1686	www.msf...	text/plain	14 bytes	ncsi.txt
2562	clientcon...	application/...	3724 bytes	b5b991cdde4fb199afe31d53f7d0af107ba25f39.txt.gz
3011	incoming...	application/j...	243 bytes	2585f2f1-2a17-4a6a-a2ee-a70ea277eadb
3076	incoming...	application/j...	658 bytes	0b58bb3f-e716-436b-98f2-3c41597390f1
3094	googlead...	text/html	1573 bytes	google?flag=ECSC{6be66bc90994604d67eac1b05d16d0d682c7213fada57098283c...
3131	googlead...	image/x-icon	1150 bytes	favicon.ico
7263	192.168.0...	application/...	93 kB	private.log
7521	192.168.0...	application/...	93 kB	private.log
9403	ocsp.digi...	application/...	83 bytes	\
9714	ocsp.digi...	application/...	278 bytes	\
10268	ocsp.god...	application/...	74 bytes	\
10313	ocsp.god...	application/...	1775 bytes	\
10829	ocsp.pki....	application/...	83 bytes	gts1o1
10847	ocsp.pki....	application/...	471 bytes	gts1o1
11096	ocsp.com...	application/...	83 bytes	\
11124	ocsp.com...	application/...	471 bytes	\

And the flag can be seen by either saving the file or opening it in a stream.

Made with love by: AndreiCat