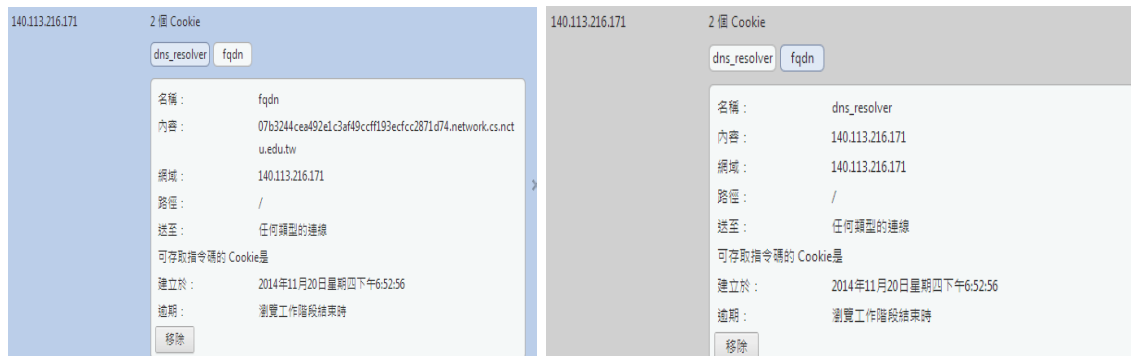


Project2 report

Basically, this project is all about cookie stored in Google (resolver and fqdn).



(a)

(b)

Figure 1 (a)fqdn (b)dns resolver

Next, I use “dig -t CERT fqdn @resolver” to send a query package via my virtual machine and obtain a response. The public key in the response is the target of this project. Figure 2 is the result of dig.

```
network@network-desktop:~$ dig -t CERT 07b3244cea492e1c3af49ccff193ecfcc2871d74.
network.cs.nctu.edu.tw @140.113.216.171
;; Truncated, retrying in TCP mode.

<<>> DiG 9.7.0-P1 <<>> -t CERT 07b3244cea492e1c3af49ccff193ecfcc2871d74.network
.cs.nctu.edu.tw @140.113.216.171
;; global options: +cmd
;; Got answer:
;;->HEADER<-- opcode: QUERY, status: NOERROR, id: 11919
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;07b3244cea492e1c3af49ccff193ecfcc2871d74.network.cs.nctu.edu.tw. IN CERT

;; ANSWER SECTION:
07b3244cea492e1c3af49ccff193ecfcc2871d74.network.cs.nctu.edu.tw. 86400 IN CERT P
GP 0 0 mQENBFQSL/sBCADE2dt/CiIs0o8xNUZyfr8vwzALrhCRMPcEtMe7wGwV Jsmoep680I76xeJ
dSNBuTw24xJctKXbmnmqVRUJ9MI+P/Pfcr+jLMvkt c05L50GwJfSEwF/3hVuyyMRPjUo22a1/FBZhsbw
vrUjWvrdLpIzyc4j X0NDBeik2myMjPqC08pMBiKWzCTg+2JqfwsFshCPVw6EFVgPnBV0dynj 62XmU
NYjupKT/RyOKFphfDzrdxA7MdpIQ3akxly5L9N7F/idNzMrJIIy zWq6V08juPhQRMVlcWTMZeaneTCe
KMIIL9IM2avdp5m8KGTdw/pvIA6 4Z5+AvLwGtGxCHxTWyodABEBAG0025ldHdvcmtMDExMDAYMIK
BOAQT AQIAIGUCVDkv+wIbAwYLCOgHAWIGFQgCCQoLBBYCAwECHgECF4AAcGkQ +964BRNb0fr/wgAv
2520gXZ/14zaHzC1TsZg2KSAJ72kC3IrZvy+nrV uRG/d6Yg6LNL0ikpyrFKIEtgRmUtFSWtb1TERZq
MT+35a4FNfcKwvuz k10ryt3JqVlZBMnHzbKcQBMeeFquQC0CBV+FFsh9rnx55GxJ8zhU0G3Kk/ yphM80
p6vuiHD6RBVuw0Ke1QLBLg6TKq0obLChLcS6t8DbGhRJTQ+cYD IAYfmdQ/M+0Twj5A04CNzRowQWYi
QYr5b53X2hBbQ5dS6EMNhV4Y+BM /0Gst0iLXrU8zwnn5lhhkUFkIbyh+t3rycy34vk35f7gt6rBxG8
WnQs j9JchX4r1g9xDJ9rvrEeLrkB0QRU0S/7A0gaop40fkUag7kVfogu7Y1J +0nLjCIHvKjNj6jCUM
rk9L3DRuSC2c9ixXTeAyyqzrzJvbbvBSJLfPfb +F9Zxqokg9aZmKHSrcrSF21isE6xDK6Aur3Cwf1Z
rVS+3n9/snu207B YPN8AaB4jcwssaMm+SSvvhDCyXHMWQNdwwKZlanGv7ZJWQm/09AFVewx9 /YCFcBc
805mNVTVQ0Iba9hEILN0d4thecouJ28FRnMi3t0vkiSecg6JA L550LHPdlr7b0ZwZD55dwhfJcXXX
991q9JgaRixT1HrPu8Jew78Lf7 x27JrICcHMM2v069xVvPkL/sb4ZqaMYEJ00feyWP9wARAQABiQEFB
BgB AgAJBQJU0S/7AhsMAAoJEPveuAUTW3dH30UH/AhYOCTa0spaBm/kF1V p2gahdpjDvLI6RkKTLj
GGq0GjSzhj+IgYnYeR41kV/P936a2vmPd+ld7 m3Ro/GHqEYigVcHx86xfBNkxvBChyNNUwNigFMMoF
Q2KsVB7eW00b+ cVM45fo60EW050R0IryaSS0i7bMIW/uk2EAngakJdACRMPuGir+SZDC NeM0jJfG
f+zMsGw4x/+QW0h/1pnGZztSKVc5hwR/hMu2aE4Z/yqeyCUL eEzo4CrXyTA8PmLKbBnuCRNm005282b
g0nq+uqsG7j50yRIAwMz5nLX/ 0CjVYPMypk2aHjKzGyJJKTp8oSdLldRdrE8VdDNoec=

;; AUTHORITY SECTION:
network.cs.nctu.edu.tw. 86400 IN NS ns.network.cs.nctu.edu.tw.

;; ADDITIONAL SECTION:
ns.network.cs.nctu.edu.tw. 86400 IN A 140.113.216.171

;; Query time: 6 msec
;; SERVER: 140.113.216.171#53(140.113.216.171)
;; WHEN: Thu Nov 20 18:42:58 2014
;; MSG SIZE rcvd: 1297
```

Figure 2

The green part is the header and the red part is the response. Therefore, I have to create a package identical to the header format.

Filter: ip.addr==140.113.216.171		Expression...	Clear	Apply
72	24.538495	192.168.0.110	140.113.216.171	DNS Standard query CERT 07b3244cea492e1c3af49ccff193ecfcc2871d74.network.cs.nctu.edu.tw
73	24.540783	140.113.216.171	192.168.0.110	DNS Standard query response
74	24.541288	192.168.0.110	140.113.216.171	TCP 50222 > domain [ACK] Seq=84 Win=8448 Len=0 TSV=4294947823 TSER=29039353
75	24.547755	140.113.216.171	192.168.0.110	TCP domain > 50222 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 TSV=29039352 TSER=4294947821 WS=7
76	24.547831	192.168.0.110	140.113.216.171	TCP 50222 > domain [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSV=4294947823 TSER=29039352
77	24.548294	192.168.0.110	140.113.216.171	DNS Standard query CERT 07b3244cea492e1c3af49ccff193ecfcc2871d74.network.cs.nctu.edu.tw
78	24.551875	140.113.216.171	192.168.0.110	TCP domain > 50222 [ACK] Seq=1 Ack=84 Win=29056 Len=0 TSV=29039353 TSER=4294947823
79	24.553567	140.113.216.171	192.168.0.110	DNS Standard query response CERT
80	24.553592	192.168.0.110	140.113.216.171	TCP 50222 > domain [ACK] Seq=84 Ack=1300 Win=8448 Len=0 TSV=4294947824 TSER=29039353
81	24.554653	192.168.0.110	140.113.216.171	TCP 50222 > domain [FIN, ACK] Seq=84 Ack=1300 Win=8448 Len=0 TSV=4294947824 TSER=29039353
82	24.559868	140.113.216.171	192.168.0.110	TCP domain > 50222 [FIN, ACK] Seq=1380 Ack=85 Win=29056 Len=0 TSV=29039354 TSER=4294947824
83	24.559895	192.168.0.110	140.113.216.171	TCP 50222 > domain [ACK] Seq=85 Ack=1301 Win=8448 Len=0 TSV=4294947825 TSER=29039354

Figure 3

Domain Name System (query)

[Response In: 79]

Length: 81 ← Length of query

Transaction ID: 0x2e8f

Flags: 0x0100 (Standard query)

- 0... .. = Response: Message is a query
- .000 0... .. = Opcode: Standard query (0)
-0... .. = Truncated: Message is not truncated ← Some flags
-1... .. = Recursion desired: Do query recursively
-0... .. = Z: reserved (0)
-0... .. = Non-authenticated data OK: Non-authenticated data is unacceptable

Questions: 1

Answer RRs: 0 ← A question without answer

Authority RRs: 0

Additional RRs: 0

Queries

- 07b3244cea492e1c3af49ccff193ecfcc2871d74.network.cs.nctu.edu.tw: type CERT, class IN
 - Name: 07b3244cea492e1c3af49ccff193ecfcc2871d74.network.cs.nctu.edu.tw
 - Type: CERT (Certificate) ← CERT = 37
 - Class: IN (0x0001)

Figure 4

Figure 3 and 4 are the content of the query package analyzed using Wireshark. From the figure 3 (red part), since the response will be truncated if dig is sent using UDP, TCP is considered as the final version. TCP will further send the information of query length. The final result is identical to the results observed on Wireshark.

<p>Questions: 1</p> <p>Answer RRs: 1</p> <p>Authority RRs: 1</p> <p>Additional RRs: 1</p> <p>Queries</p>	<p>Answers</p> <ul style="list-style-type: none"> 07b3244cea492e1c3af49ccff193ecfcc2871d74.network.cs.nctu.edu.tw: type CERT, class IN <ul style="list-style-type: none"> Name: 07b3244cea492e1c3af49ccff193ecfcc2871d74.network.cs.nctu.edu.tw Type: CERT (Certificate) Class: IN (0x0001) Time to live: 1 day Data length: 1171 Type: SPKI Key footprint: 0x0000 Algorithm: Unknown (0x00) Public key <p>Authoritative nameservers</p> <ul style="list-style-type: none"> network.cs.nctu.edu.tw: type NS, class IN, ns ns.network.cs.nctu.edu.tw <ul style="list-style-type: none"> Name: network.cs.nctu.edu.tw Type: NS (Authoritative name server) Class: IN (0x0001) Time to live: 1 day Data length: 5 Name server: ns.network.cs.nctu.edu.tw <p>Additional records</p> <ul style="list-style-type: none"> ns.network.cs.nctu.edu.tw: type A, class IN, addr 140.113.216.171 <ul style="list-style-type: none"> Name: ns.network.cs.nctu.edu.tw Type: A (Host address) Class: IN (0x0001) Time to live: 1 day Data length: 4 Addr: 140.113.216.171
---	--

The final is to analyze the response, which contains a question (query), an answer, an authority RR, an additional RR. The common parts in answer, authority RR, additional

RR are the name, type, class, ttl, data length. Public key also appears in the answer section.