Network Traffic Analysis Report

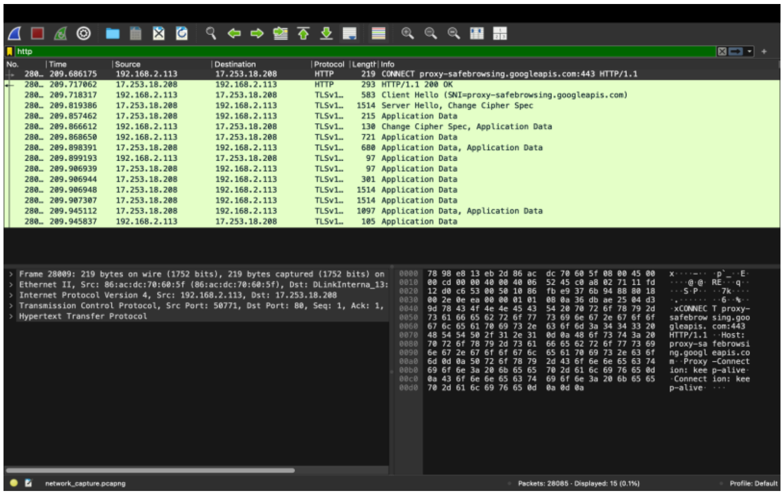
1. Overview

This report summarizes the analysis of captured network traffic, focusing on HTTP, DNS, and TLS protocols to assess security risks and activity patterns.

2. Key Findings

- HTTP Traffic

  Observed a CONNECT request to proxy-safebrowsing.googleapis.com:443.



```
http
No.   Time        Source          Destination     Protocol  Length Info
280… 209.686175  192.168.2.113   17.253.18.208   HTTP       219 CONNECT proxy-safebrowsing.googleapis.com:443 HTTP/1.1
280… 209.717062  17.253.18.208   192.168.2.113   HTTP       293 HTTP/1.1 200 OK
280… 209.718317  192.168.2.113   17.253.18.208   TLSv1…     583 Client Hello (SNI=proxy-safebrowsing.googleapis.com)
280… 209.819386  17.253.18.208   192.168.2.113   TLSv1…    1514 Server Hello, Change Cipher Spec
280… 209.857462  17.253.18.208   192.168.2.113   TLSv1…     215 Application Data
280… 209.866612  192.168.2.113   17.253.18.208   TLSv1…     130 Change Cipher Spec, Application Data
280… 209.868650  192.168.2.113   17.253.18.208   TLSv1…     721 Application Data
280… 209.898391  17.253.18.208   192.168.2.113   TLSv1…     680 Application Data, Application Data
280… 209.899193  192.168.2.113   17.253.18.208   TLSv1…      97 Application Data
280… 209.906939  17.253.18.208   192.168.2.113   TLSv1…      97 Application Data
280… 209.906944  17.253.18.208   192.168.2.113   TLSv1…     301 Application Data
280… 209.906948  17.253.18.208   192.168.2.113   TLSv1…    1514 Application Data
280… 209.907307  17.253.18.208   192.168.2.113   TLSv1…    1514 Application Data
280… 209.945112  17.253.18.208   192.168.2.113   TLSv1…    1097 Application Data, Application Data
280… 209.945837  192.168.2.113   17.253.18.208   TLSv1…     105 Application Data
```

```
> Frame 28009: 219 bytes on wire (1752 bits), 219 bytes captured (1752 bits) on
> Ethernet II, Src: 86:ac:dc:70:60:5f (86:ac:dc:70:60:5f), Dst: DLinkInterna_13:
> Internet Protocol Version 4, Src: 192.168.2.113, Dst: 17.253.18.208
> Transmission Control Protocol, Src Port: 50771, Dst Port: 80, Seq: 1, Ack: 1,
> Hypertext Transfer Protocol
```

```
0000  78 98 e8 13 eb 2d 86 ac  dc 70 60 5f 08 00 45 00   x····-·· ·p`_··E·
0010  00 cd 00 00 40 00 40 06  52 45 c0 a8 02 71 11 fd   ····@·@· RE···q··
0020  12 d0 c6 53 00 50 10 86  fb e9 37 6b 94 88 80 18   ···S·P·· ··7k····
0030  00 2e 0e ea 00 00 01 01  08 0a 36 db ae 25 04 d3   ·.······ ··6··%··
0040  9d 78 43 4f 4e 4e 45 43  54 20 70 72 6f 78 79 2d   ·xCONNEC T proxy-
0050  73 61 66 65 62 72 6f 77  73 69 6e 67 2e 67 6f 6f   safebrow sing.goo
0060  67 6c 65 61 70 69 73 2e  63 6f 6d 3a 34 34 33 20   gleapis. com:443 
0070  48 54 54 50 2f 31 2e 31  0d 0a 48 6f 73 74 3a 20   HTTP/1.1 ··Host: 
0080  70 72 6f 78 79 2d 73 61  66 65 62 72 6f 77 73 69   proxy-sa febrowsi
0090  6e 67 2e 67 6f 6f 67 6c  65 61 70 69 73 2e 63 6f   ng.googl eapis.co
00a0  6d 0d 0a 50 72 6f 78 79  2d 43 6f 6e 6e 65 63 74   m··Proxy -Connect
00b0  69 6f 6e 3a 20 6b 65 65  70 2d 61 6c 69 76 65 0d   ion: kee p-alive·
00c0  0a 43 6f 6e 6e 65 63 74  69 6f 6e 3a 20 6b 65 65   ·Connect ion: kee
00d0  70 2d 61 6c 69 76 65 0d  0a 0d 0a                  p-alive· ···
```

```
network_capture.pcapng          Packets: 28085 · Displayed: 15 (0.1%)          Profile: Default
```

  No plaintext sensitive data detected.

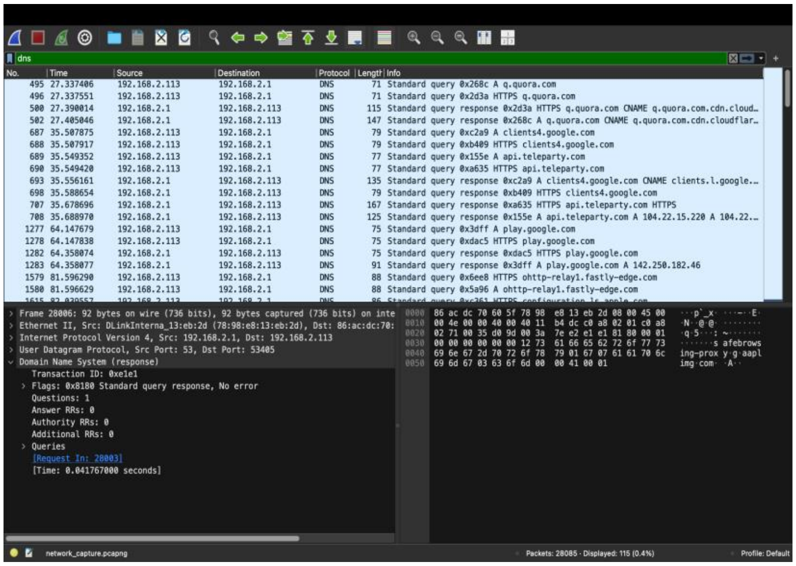
  Risk: Potential credential leakage in unencrypted traffic.

- DNS Traffic

  Notable queries to quora.com, google.com, teleparty.com, and fastly-edge.com.

  No malicious domains identified.

  Risk: High-frequency DNS requests may indicate automated scripts or malware.



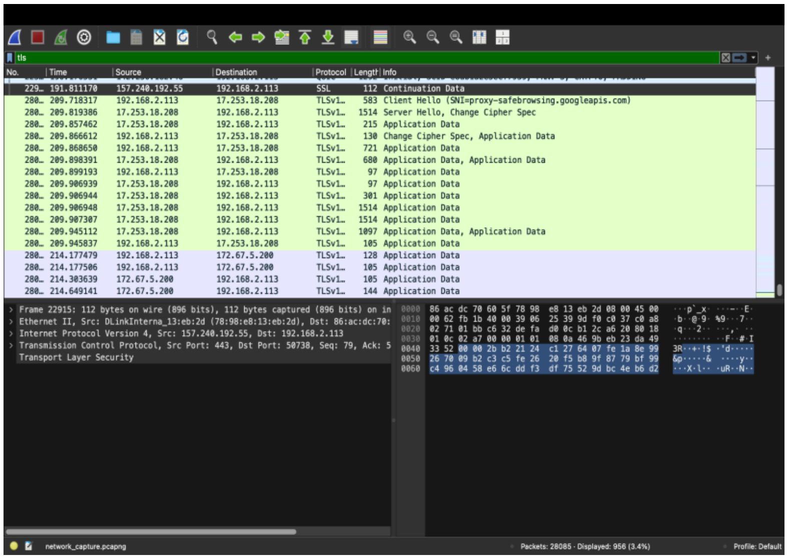
```
No.   Time       Source          Destination     Protocol Length Info
  495 27.337406  192.168.2.113   192.168.2.1     DNS       71 Standard query 0x268c A q.quora.com
  496 27.337551  192.168.2.113   192.168.2.1     DNS       71 Standard query 0x2d3a HTTPS q.quora.com
  500 27.390014  192.168.2.1     192.168.2.113   DNS      115 Standard query response 0x2d3a HTTPS q.quora.com CNAME q.quora.com.cdn.cloud…
  502 27.405046  192.168.2.1     192.168.2.113   DNS      147 Standard query response 0x268c A q.quora.com CNAME q.quora.com.cdn.cloudflar…
  687 35.507875  192.168.2.113   192.168.2.1     DNS       79 Standard query 0xc2a9 A clients4.google.com
  688 35.507917  192.168.2.113   192.168.2.1     DNS       79 Standard query 0xb409 HTTPS clients4.google.com
  689 35.549352  192.168.2.113   192.168.2.1     DNS       77 Standard query 0x155e A api.teleparty.com
  690 35.549420  192.168.2.113   192.168.2.1     DNS       77 Standard query 0xa635 HTTPS api.teleparty.com
  693 35.556161  192.168.2.1     192.168.2.113   DNS      135 Standard query response 0xc2a9 A clients4.google.com CNAME clients.l.google.…
  698 35.588654  192.168.2.1     192.168.2.113   DNS       79 Standard query response 0xb409 HTTPS clients4.google.com
  707 35.678696  192.168.2.1     192.168.2.113   DNS      167 Standard query response 0xa635 HTTPS api.teleparty.com HTTPS
  708 35.688970  192.168.2.1     192.168.2.113   DNS      125 Standard query response 0x155e A api.teleparty.com A 104.22.15.220 A 104.22.…
 1277 64.147679  192.168.2.113   192.168.2.1     DNS       75 Standard query 0x3dff A play.google.com
 1278 64.147838  192.168.2.113   192.168.2.1     DNS       75 Standard query 0xdac5 HTTPS play.google.com
 1282 64.358074  192.168.2.1     192.168.2.113   DNS       75 Standard query response 0xdac5 HTTPS play.google.com
 1283 64.358077  192.168.2.1     192.168.2.113   DNS       91 Standard query response 0x3dff A play.google.com A 142.250.182.46
 1579 81.596290  192.168.2.113   192.168.2.1     DNS       88 Standard query 0x6ee8 HTTPS ohttp-relay1.fastly-edge.com
 1580 81.596629  192.168.2.113   192.168.2.1     DNS       88 Standard query 0x5a96 A ohttp-relay1.fastly-edge.com
```

```
> Frame 28006: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on inte
> Ethernet II, Src: DLinkInterna_13:eb:2d (78:98:e8:13:eb:2d), Dst: 86:ac:dc:70:
> Internet Protocol Version 4, Src: 192.168.2.1, Dst: 192.168.2.113
> User Datagram Protocol, Src Port: 53, Dst Port: 53405
v Domain Name System (response)
    Transaction ID: 0xe1e1
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    [Request In: 28003]
    [Time: 0.041767000 seconds]
```

```
0000  86 ac dc 70 60 5f 78 98  e8 13 eb 2d 08 00 45 00   ···p`_x· ···-··E·
0010  00 4e 00 00 40 00 40 11  b4 dc c0 a8 02 01 c0 a8   ·N··@·@· ········
0020  02 71 00 35 d0 9d 00 3a  7e e2 e1 e1 81 80 00 01   ·q·5···: ~·······
0030  00 00 00 00 00 00 12 73  61 66 65 62 72 6f 77 73   ·······s afebrows
0040  69 6e 67 2d 70 72 6f 78  79 01 67 07 61 61 70 6c   ing-prox y·g·aapl
0050  69 6d 67 03 63 6f 6d 00  00 41 00 01               img·com· ·A··
```

- TLS Traffic

Multiple TLS handshakes captured, ensuring encrypted communication.



```
No.   Time        Source          Destination     Protocol Length Info
229…  191.811170  157.240.192.55  192.168.2.113   SSL       112 Continuation Data
280…  209.718317  192.168.2.113   17.253.18.208   TLSv1…    583 Client Hello (SNI=proxy-safebrowsing.googleapis.com)
280…  209.819386  17.253.18.208   192.168.2.113   TLSv1…   1514 Server Hello, Change Cipher Spec
280…  209.857462  17.253.18.208   192.168.2.113   TLSv1…    215 Application Data
280…  209.866612  192.168.2.113   17.253.18.208   TLSv1…    130 Change Cipher Spec, Application Data
280…  209.868650  192.168.2.113   17.253.18.208   TLSv1…    721 Application Data
280…  209.898391  17.253.18.208   192.168.2.113   TLSv1…    680 Application Data, Application Data
280…  209.899193  192.168.2.113   17.253.18.208   TLSv1…     97 Application Data
280…  209.906939  17.253.18.208   192.168.2.113   TLSv1…     97 Application Data
280…  209.906944  17.253.18.208   192.168.2.113   TLSv1…    301 Application Data
280…  209.906948  17.253.18.208   192.168.2.113   TLSv1…   1514 Application Data
280…  209.907307  17.253.18.208   192.168.2.113   TLSv1…   1514 Application Data
280…  209.945112  17.253.18.208   192.168.2.113   TLSv1…   1097 Application Data, Application Data
280…  209.945837  192.168.2.113   17.253.18.208   TLSv1…    105 Application Data
280…  214.177479  192.168.2.113   172.67.5.200    TLSv1…    128 Application Data
280…  214.177506  192.168.2.113   172.67.5.200    TLSv1…    105 Application Data
280…  214.303639  172.67.5.200    192.168.2.113   TLSv1…    105 Application Data
280…  214.649141  172.67.5.200    192.168.2.113   TLSv1…    144 Application Data
```

```
> Frame 22915: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on in
> Ethernet II, Src: DLinkInterna_13:eb:2d (78:98:e8:13:eb:2d), Dst: 86:ac:dc:70:
> Internet Protocol Version 4, Src: 157.240.192.55, Dst: 192.168.2.113
> Transmission Control Protocol, Src Port: 443, Dst Port: 50738, Seq: 79, Ack: 5
  Transport Layer Security
```

```
0000  86 ac dc 70 60 5f 78 98  e8 13 eb 2d 08 00 45 00   ···p`_x· ···-··E·
0010  00 62 fb 1b 40 00 39 06  25 39 9d f0 c0 37 c0 a8   ·b··@·9· %9···7··
0020  02 71 01 bb c6 32 de fa  d0 0c b1 2c a6 20 80 18   ·q···2·· ···,· ··
0030  01 0c 02 a7 00 00 01 01  08 0a 46 9b eb 23 da 49   ········ ··F··#·I
0040  33 52 00 00 2b b2 21 24  c1 27 64 07 fe 1a 8e 99   3R··+·!$ ·'d·····
0050  26 70 09 b2 c3 c5 fe 26  20 f5 b8 9f 87 79 bf 99   &p·····&  ····y··
0060  c4 96 04 58 e6 6c dd f3  df 75 52 9d bc 4e b6 d2   ···X·l·· ·uR··N··
```

Risk: Unverified TLS connections to unknown IPs may pose security threats.

3. Conclusion

Traffic analysis indicates normal activity with no immediate threats. Further monitoring of DNS and proxy requests is advised.