Encryption de requêtes

DNS est un protocole UDP opérant au port 53. Ceci implique que la requête est en texte clair, sans encryption et que n'importe qui interceptant la requête peut identifier l'ensemble des services auxquels vous accédez. On peut penser ici à l'administration informatique du cégep, d'un café internet ou encore d'un aéroport. Une requête a généralement la structure suivante :

```
Domain Name System (query)
    Questions: 1
    Queries
        tiktok.com: type A, class IN
            Name: tiktok.com
            Type: A (1) (Host Address)
            Class: IN (0x0001)
```

Dans cette requête, un serveur DNS est interrogé pour l'entrée de type A (correspondant à l'adresse IPv4 du domaine) pour tiktok.com. On peut observer avec la section "Questions: 1" que je demande ici uniquement une information (l'entrée de type A).

La réponse à cette demande serait la suivante :

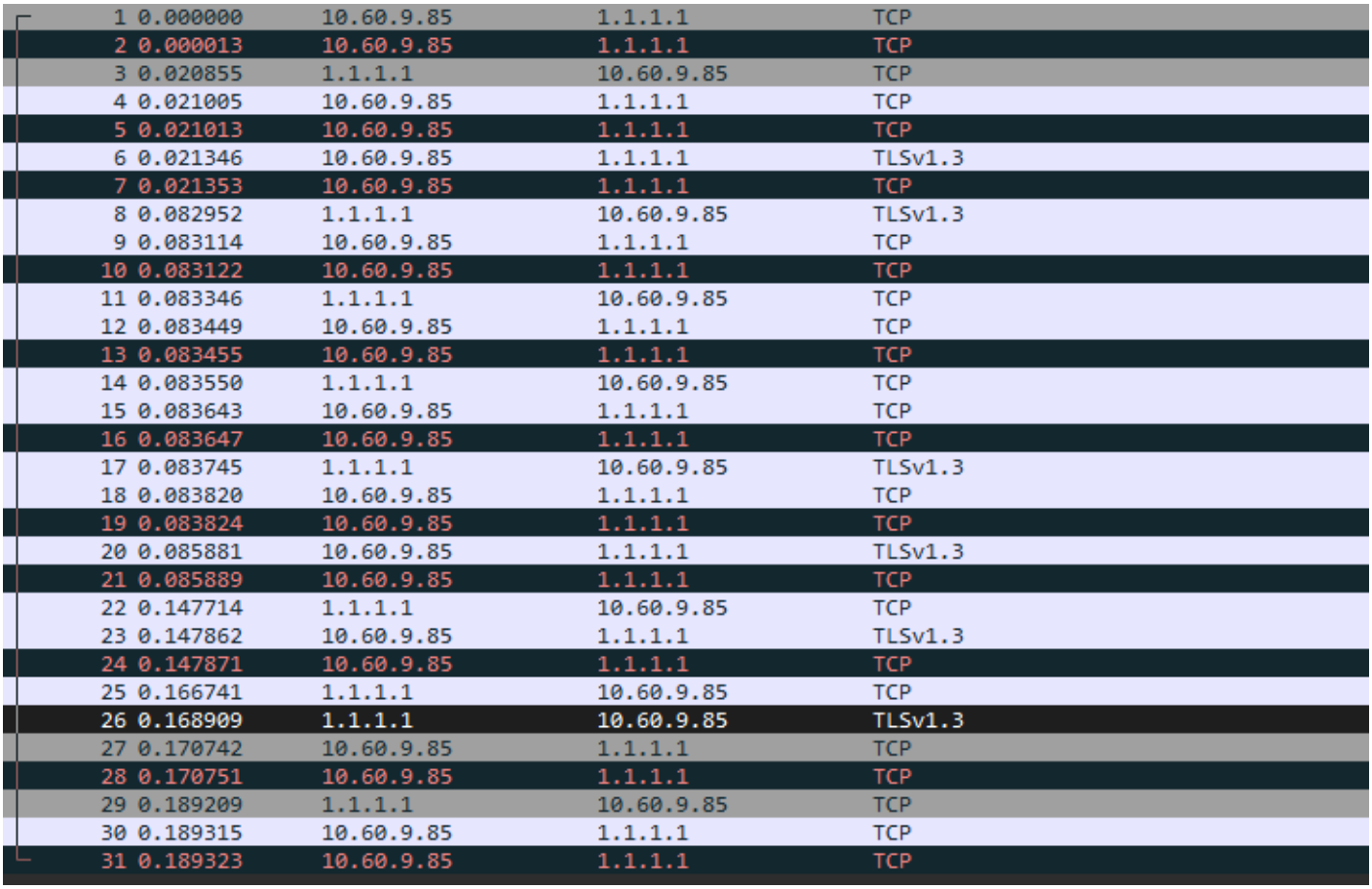
```
Domain Name System (response)
    Questions: 1
    Queries
        tiktok.com: type A, class IN
            Name: tiktok.com
            Type: A (1) (Host Address)
            Class: IN (0x0001)
    Answers
        tiktok.com: type A, class IN, addr 23.222.17.15
            Name: tiktok.com
            Type: A (1) (Host Address)
            Class: IN (0x0001)
            Address: 23.222.17.15
        tiktok.com: type A, class IN, addr 23.222.17.8
            Name: tiktok.com
            Type: A (1) (Host Address)
            Class: IN (0x0001)
            Address: 23.222.17.8
```

On observe ici que la réponse à l'entrée "tiktok.com" est 23.222.17.8. On peut donc assumer que l'appareil ayant effectué la requête a contacté TikTok.

Il est donc facile de déterminer avec ces informations facilement capturables à quels services un appareils se réfère que ce soit par une attaque de type "Man In The Middle" (MITM) ou en étant tout simplement l'administrateur d'un réseau.

Pour améliorer la sécurité de ce mécanisme, il est dorénavant possible d'effectuer des requêtes par "HTTPS" ou "Hypertext Protocol Secure" ou encore par "TLS" ou "Transport Layer Security" permettant l'encryption de ces requêtes entre un client et un serveur DNS. Ce faisant, les requêtes DNS sont encryptées et acheminées en TCP par le port 443 (DoH) ou 853 (DoT) au serveur DNS.

On peut observer ici qu'une requête DNS pour tiktok.com est beaucoup plus complexe et encryptée en TLS.



1	0.000000	10.60.9.85	1.1.1.1	TCP
2	0.000013	10.60.9.85	1.1.1.1	TCP
3	0.020855	1.1.1.1	10.60.9.85	TCP
4	0.021005	10.60.9.85	1.1.1.1	TCP
5	0.021013	10.60.9.85	1.1.1.1	TCP
6	0.021346	10.60.9.85	1.1.1.1	TLSv1.3
7	0.021353	10.60.9.85	1.1.1.1	TCP
8	0.082952	1.1.1.1	10.60.9.85	TLSv1.3
9	0.083114	10.60.9.85	1.1.1.1	TCP
10	0.083122	10.60.9.85	1.1.1.1	TCP
11	0.083346	1.1.1.1	10.60.9.85	TCP
12	0.083449	10.60.9.85	1.1.1.1	TCP
13	0.083455	10.60.9.85	1.1.1.1	TCP
14	0.083550	1.1.1.1	10.60.9.85	TCP
15	0.083643	10.60.9.85	1.1.1.1	TCP
16	0.083647	10.60.9.85	1.1.1.1	TCP
17	0.083745	1.1.1.1	10.60.9.85	TLSv1.3
18	0.083820	10.60.9.85	1.1.1.1	TCP
19	0.083824	10.60.9.85	1.1.1.1	TCP
20	0.085881	10.60.9.85	1.1.1.1	TLSv1.3
21	0.085889	10.60.9.85	1.1.1.1	TCP
22	0.147714	1.1.1.1	10.60.9.85	TCP
23	0.147862	10.60.9.85	1.1.1.1	TLSv1.3
24	0.147871	10.60.9.85	1.1.1.1	TCP
25	0.166741	1.1.1.1	10.60.9.85	TCP
26	0.168909	1.1.1.1	10.60.9.85	TLSv1.3
27	0.170742	10.60.9.85	1.1.1.1	TCP
28	0.170751	10.60.9.85	1.1.1.1	TCP
29	0.189209	1.1.1.1	10.60.9.85	TCP
30	0.189315	10.60.9.85	1.1.1.1	TCP
31	0.189323	10.60.9.85	1.1.1.1	TCP

Ceci est le trafic qu'un administrateur réseau ou un une personne au milieu pourrait observer pour une telle requête/réponse :

```
Transport Layer Security
    [Stream index: 0]
    TLSv1.3 Record Layer: Application Data Protocol: Domain Name System
        Opaque Type: Application Data (23)
        Version: TLS 1.2 (0x0303)
```

```
        Length: 445
        Encrypted Application Data […]:
45b4de58ddc0edd64aeea19a460b8c70dbff0494487d7f653a30c69b88cafd0301991a8b516080abf3997d8543d6cf
a129759689dece0caf937e7e43b0b7ca3b32cee01d283ad6167f22d6d0e7c7d62b1207bd79d4ed343b0051ae5bff72
9e2cae97e83fced64
        [Application Data Protocol: Domain Name System]
    TLSv1.3 Record Layer: Application Data Protocol: Domain Name System
        Opaque Type: Application Data (23)
        Version: TLS 1.2 (0x0303)
        Length: 487
        Encrypted Application Data […]:
3e4547e09af20c69527369f8f2dd96da903012c63afad1295cac5263e51d1e0c829d3b3ff4d5bc5b108f364581231f
9b76518c414fb4a0c977896866c9aeb01aab9b80cdbcac5e29721e997fbdcce4f9c443de6683632b6937eb14d341ec
84bb67ad2a7d8ce12
        [Application Data Protocol: Domain Name System]
```

Revision #4
Created 2025-10-19 22:14:11 UTC by Alexandre Arsenault-Jetté
Updated 2025-10-20 00:08:52 UTC by Alexandre Arsenault-Jetté