# Charles Web Debugging Proxy Exploration for SDK Project

## Set-up

- Instructions for configuring Charles proxy for Mac:
    - https://www.charlesproxy.com/documentation/configuration/browser-and-system-configuration/
    - https://www.youtube.com/watch?v=RwfeH5ahxCg&t=3s (this video is easier to follow when compared to the written instructions)

  Note: I added * to Proxy > SSL Proxying Settings > SSL Proxying > Add as a wildcard to capture all sites
- Instructions for connecting iOS device to Charles:
    - https://www.charlesproxy.com/documentation/faqs/using-charles-from-an-iphone/
    - https://www.youtube.com/watch?v=r7aV39-CKg4 (this video is easier to follow when compared to the written instructions)

## Key Functions

### Viewing Options

There are two viewing options for internet traffic on Charles. Both options provide similar functionality (e.g., can search within both).

- Structure: See requests in the form of a tree (folder structure) where the host is first followed by the folders and directories for the host (Figure 1)
- Sequence: See requests in the order that they happen (Figure 2)

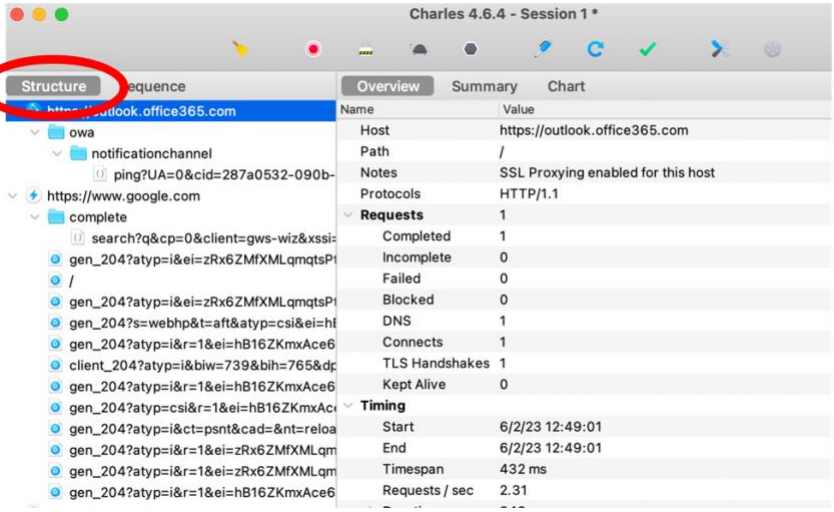


Figure 1. Structure view

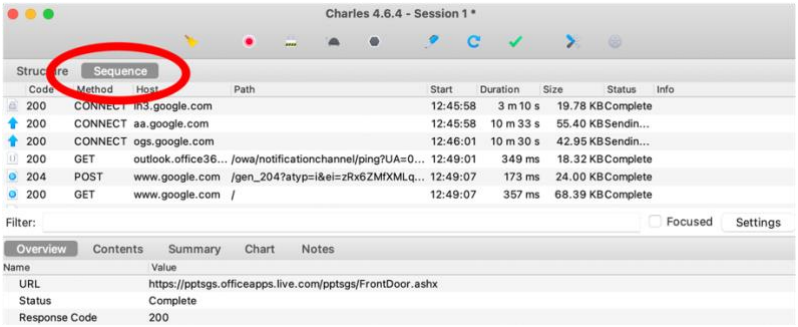


Figure 2. Sequence view

## Filter and Focused

Many hosts will appear (especially as programs and applications run in the background). You can use the filter and focused functionality in both structure and sequence view.

- Filter: Search in text field for specific domains, requests, responses, etc. (Figures 3 and 4)
- Focused: Search for a specific host (Figures 5 and 6)

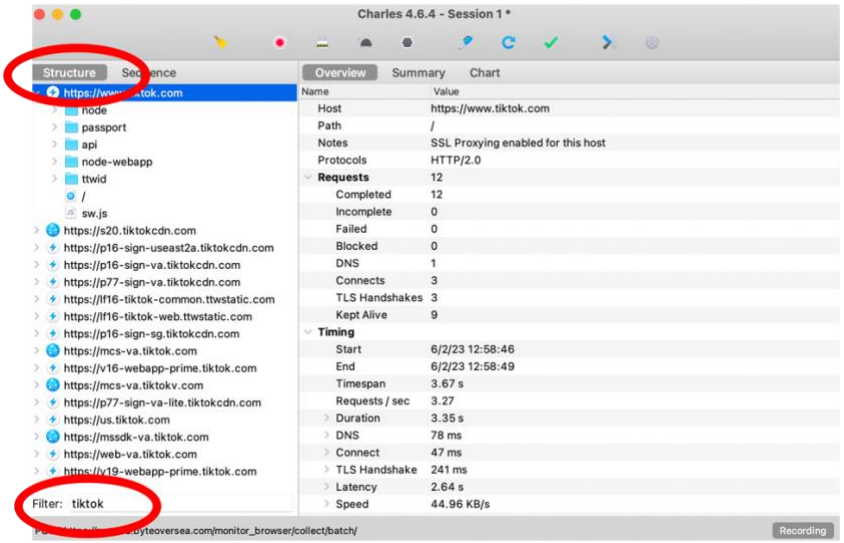


Figure 3. Filtering for TikTok in structure view

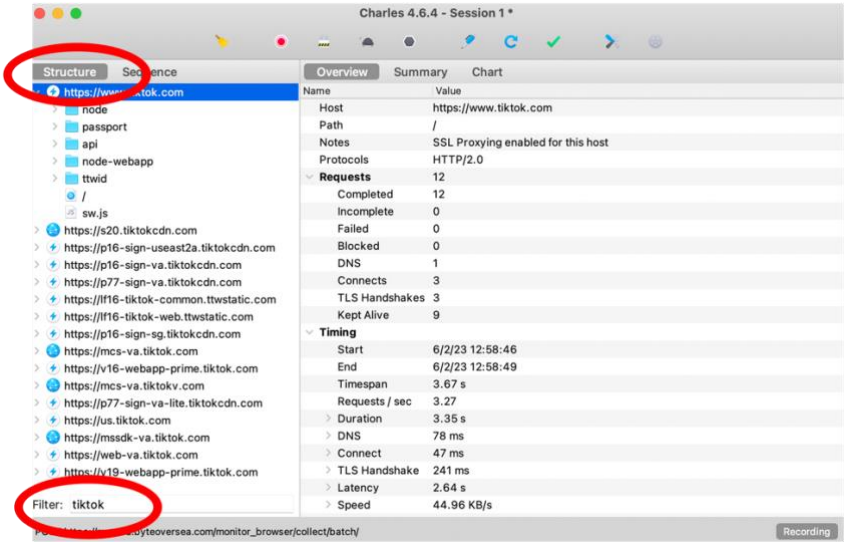


Figure 4. Filtering for TikTok in sequence view

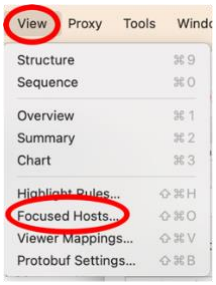


Figure 5. Accessing 'Focused Hosts' option

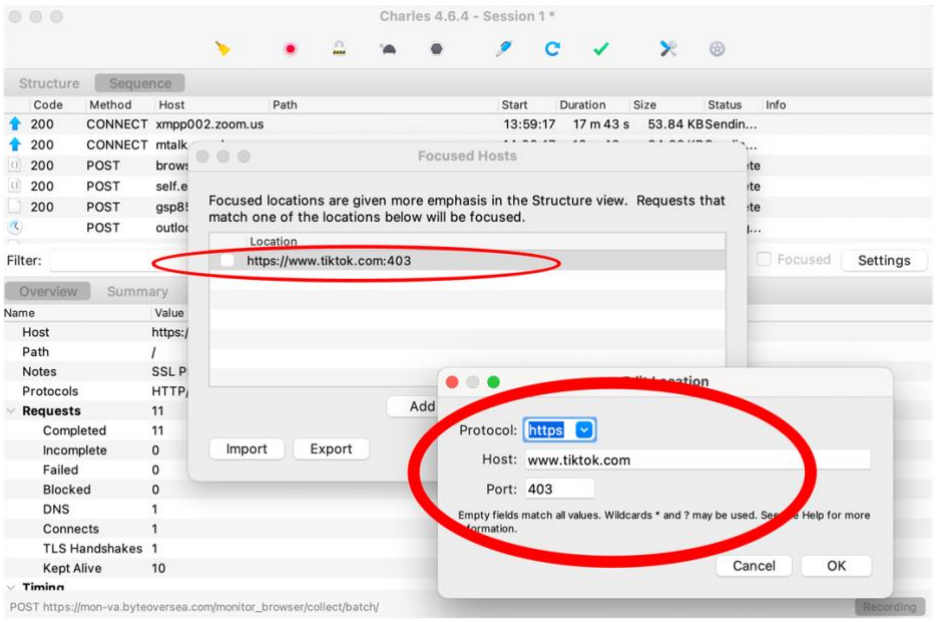


Figure 6. Setting up 'Focused Hosts' option

## Clear

Sometimes Charles proxy becomes too slow or there is generally too much that you don't want being recorded. To clear your session, select the brush tool (Figure 7):

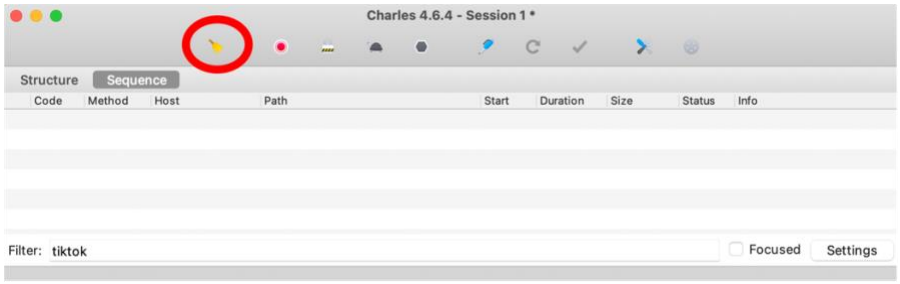


Figure 7. Brush button to clear session

## Start and Pause

The default seems to be that Charles will begin recording your internet traffic when you open the application. You can pause the recording by selecting the button circled in Figure 8.

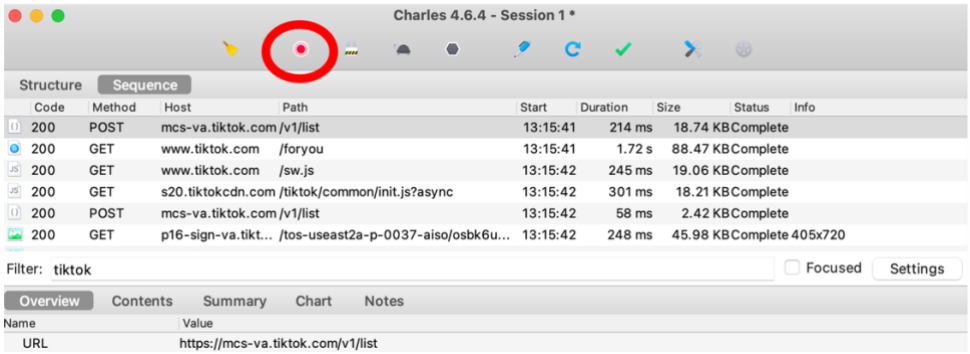


Figure 8. Pause button

## Examining Internet Traffic

As mentioned in the email, not all apps can be accessed to the same extent (e.g., cannot access traffic for TikTok app—see Figure 9). I think this is due to something called SSL pinning or certificate pinning. To check issues with certificates, you can use the O-Saft tool. There are also workarounds that are possible with a jailbroken iPhone, including TrustMe and SSL Kill Switch. Everything below describes the analysis that can be done without workarounds, i.e., traffic with just the Charles proxy tool.

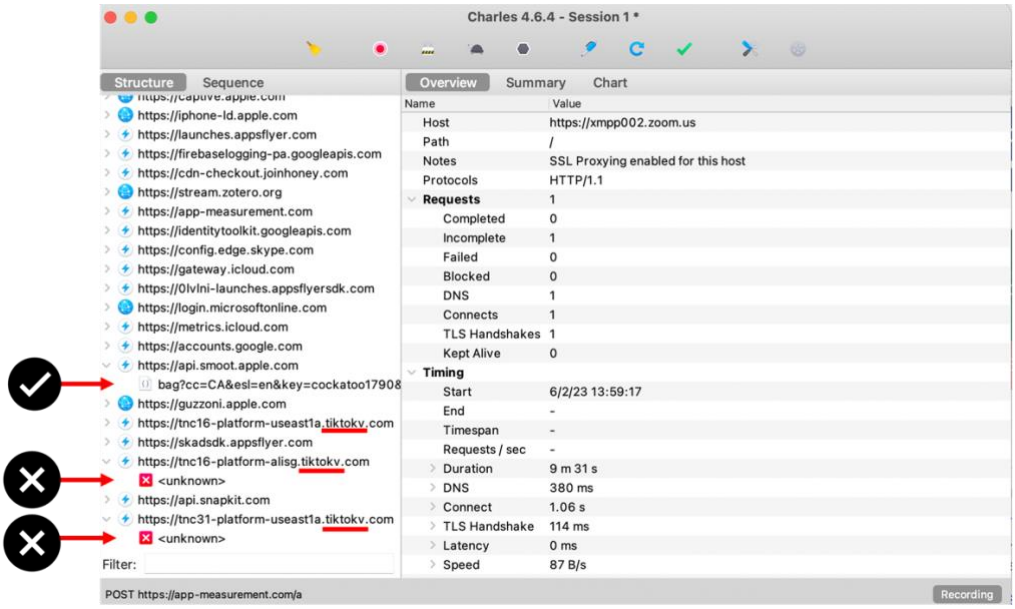


Figure 9. <unknown> error when using TikTok app

## Traffic: Headers, Requests, and Responses

You can identify a list of hosts when opening an application. For example, Figure 10 lists hosts with requests when opening TikTok on an iPhone. You can see that AppsFlyer launches when opening TikTok. Note that the <unknown> error occurs when accessing TikTok as an app. More detailed information on hosts, requests, responses, and data can be found when opening TikTok from an internet browser (regardless of device)—see Figure 11.

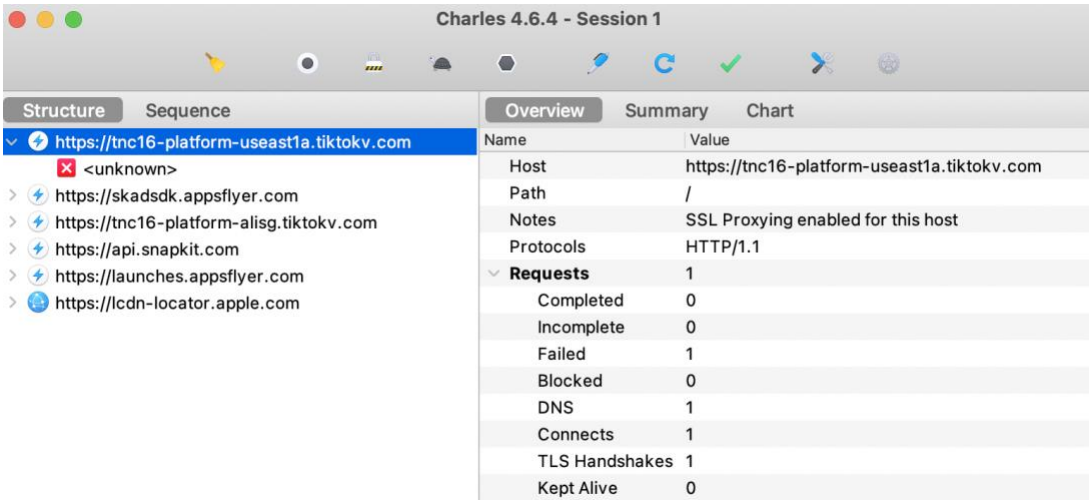


Figure 10. Opening the TikTok app on an iPhone

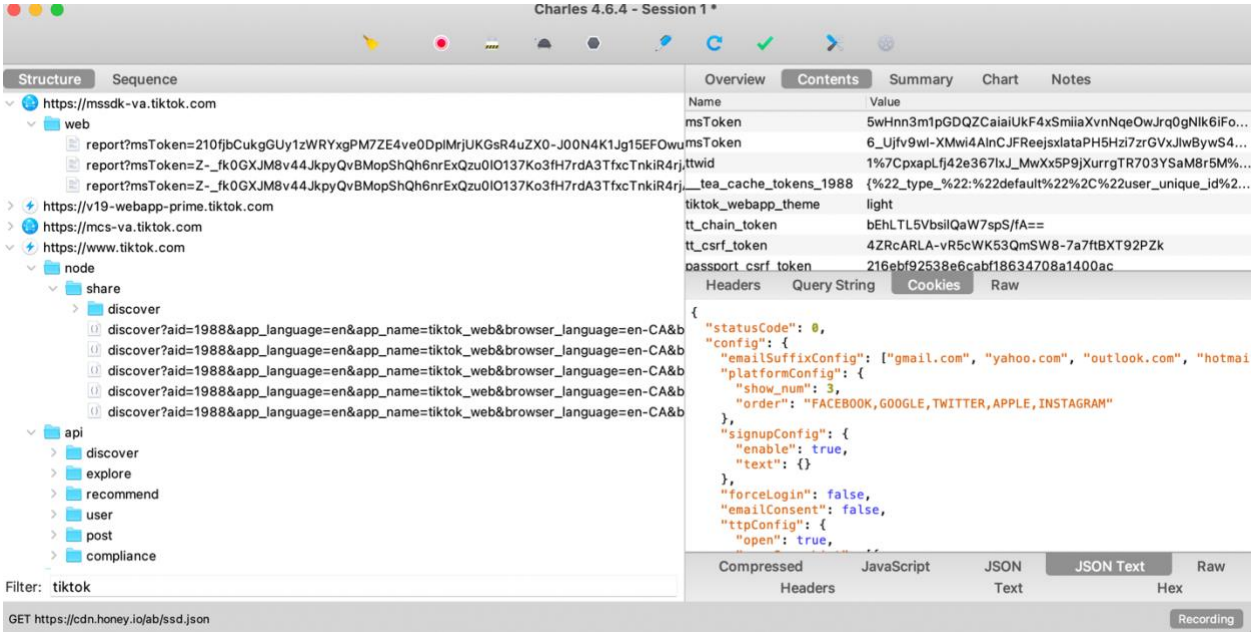


Figure 11. Opening the TikTok website on an iPhone from Safari

## Request Types

It seems it's easier to see codes in sequence mode (see Figure 12 to locate request types). Change to sequence mode to see a list of request types. The most common seem to be: GET, POST, PUT, DELETE, and CONNECT. These requests send or receive data from servers. For more details on each of these, please see the following guide: https://www.w3schools.com/tags/ref_httpmethods.asp.

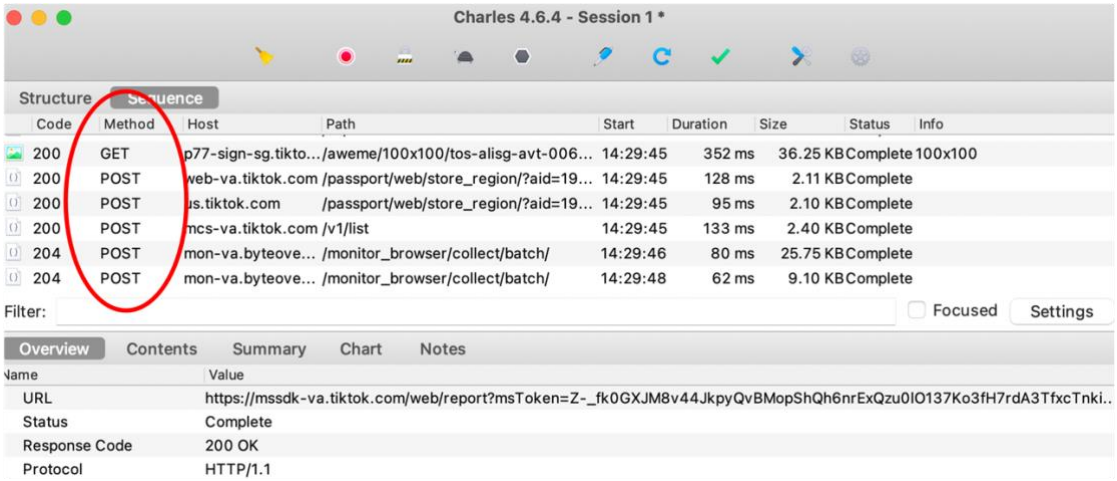


Figure 12. Request methods

## Status Codes

You can check whether a response has been sent correctly by looking at the status code (Figure 13). The status codes have been grouped into certain classes. You can find more about specific status codes at the following link: https://developer.mozilla.org/en-US/docs/Web/HTTP/Status.

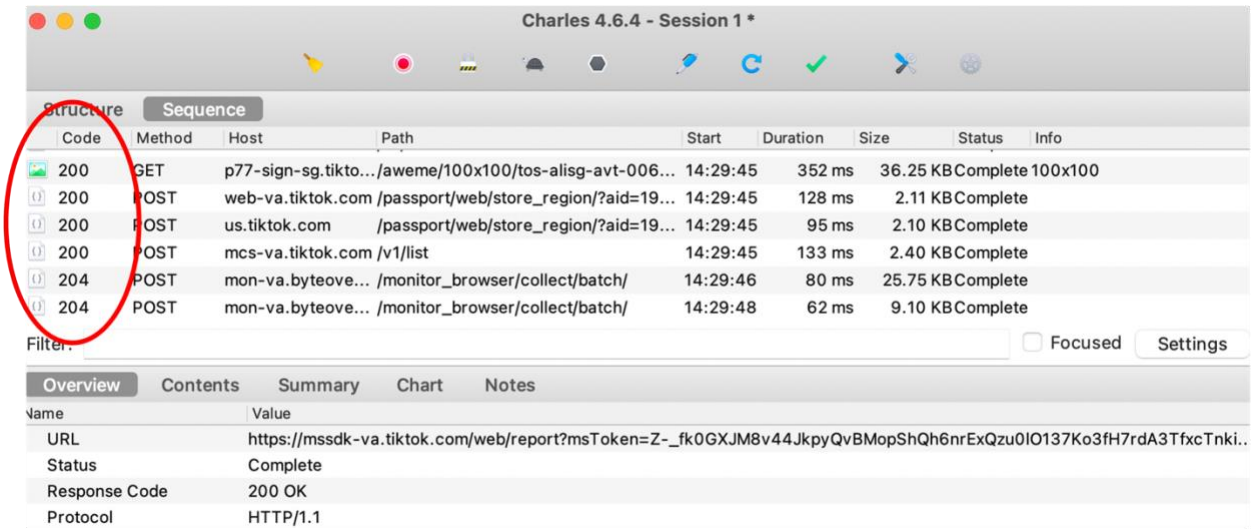


Figure 13. Status codes

## Cookies

To obtain a list of cookies associated with a particular host (e.g., us.tiktok.com in Figure 14), click on Contents > Cookies in sequence mode.

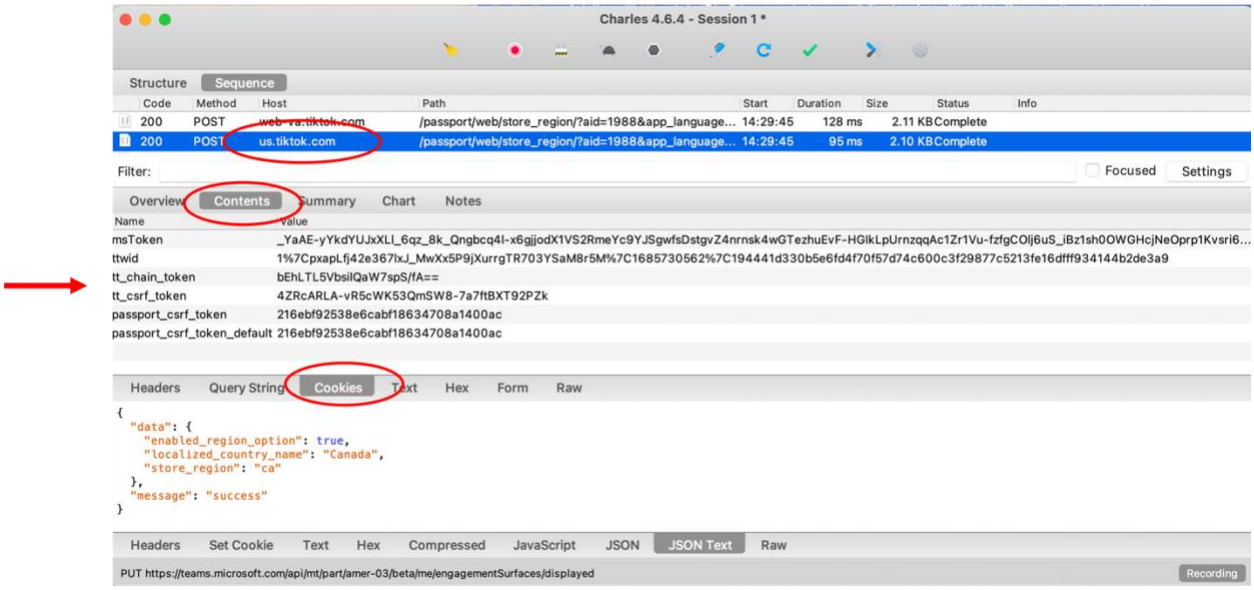


Figure 14. Identifying cookies associated with a host