LaTreil Wimberly

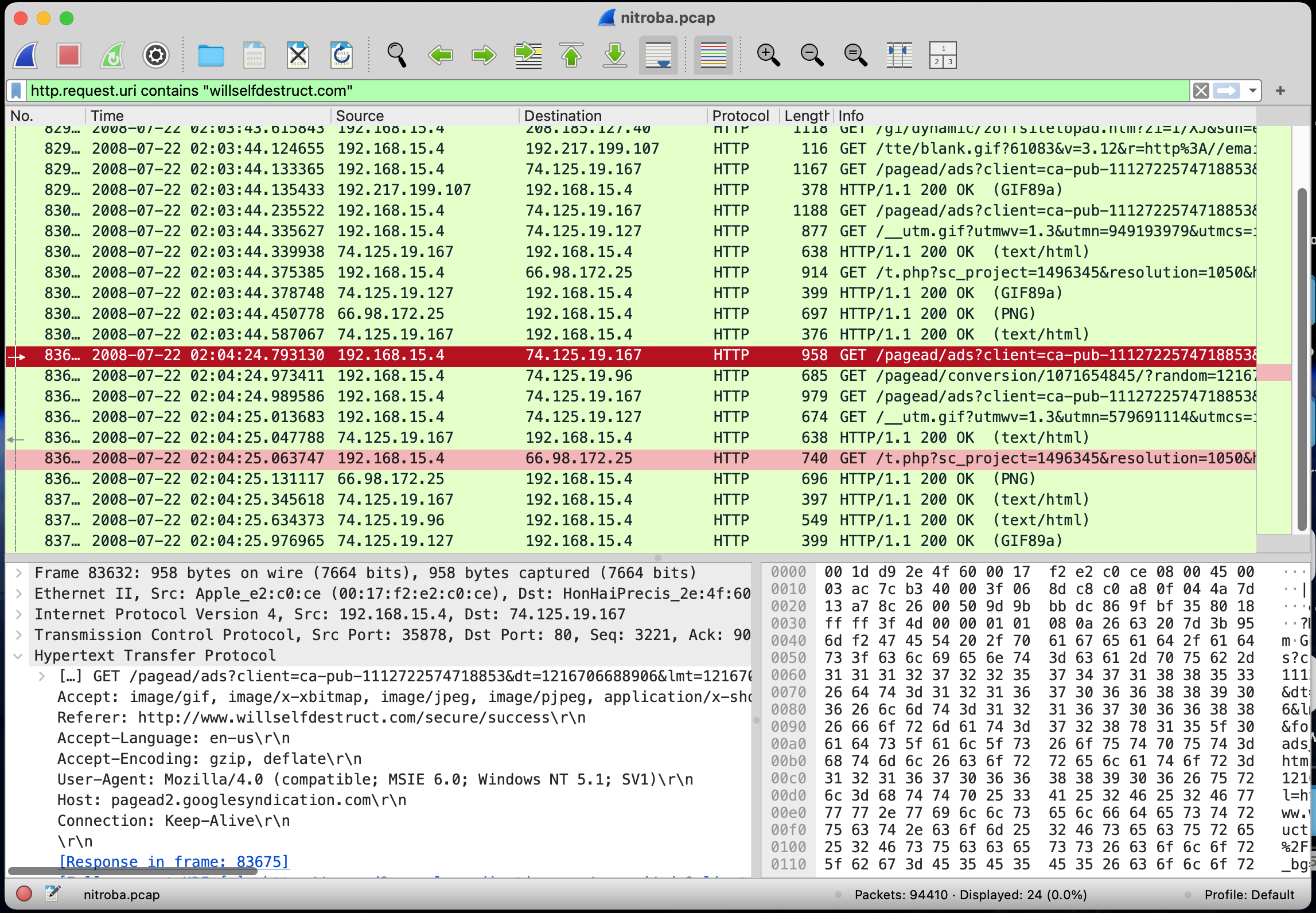
9/10/2025

CTEC 350

Wireshark – Project

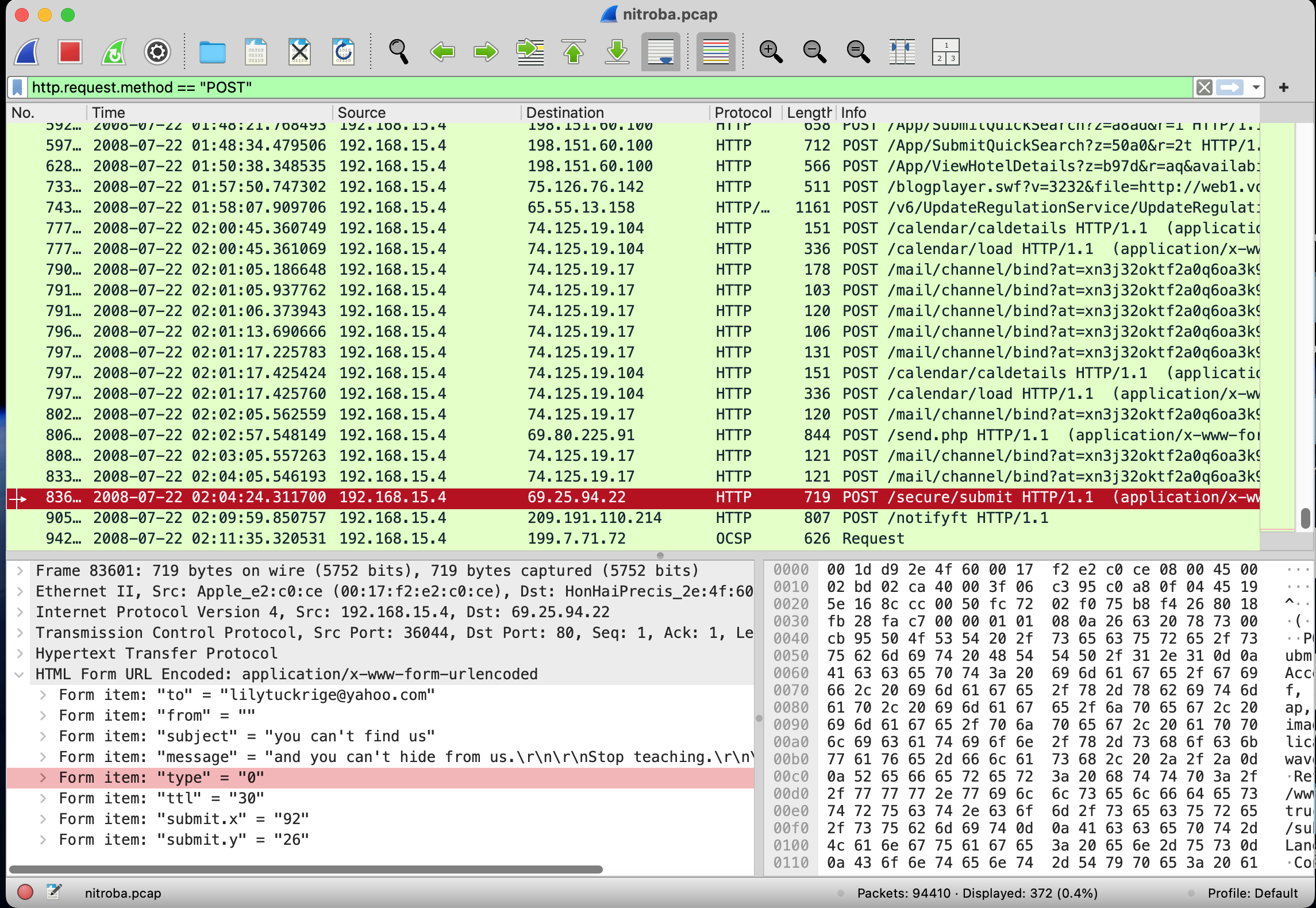
Identify the Suspect IP Address

* Use Wireshark to locate HTTP requests or responses related to [www.willselfdestruct.com](https://www.willselfdestruct.com).
* Find the IP address that appears in those HTTP packets by filtering, for example:
  + http.request.uri contains "willselfdestruct.com"
  + IP address associated with suspect: 74.125.19.96
* Provide a screenshot of the packet list showing the relevant IP.



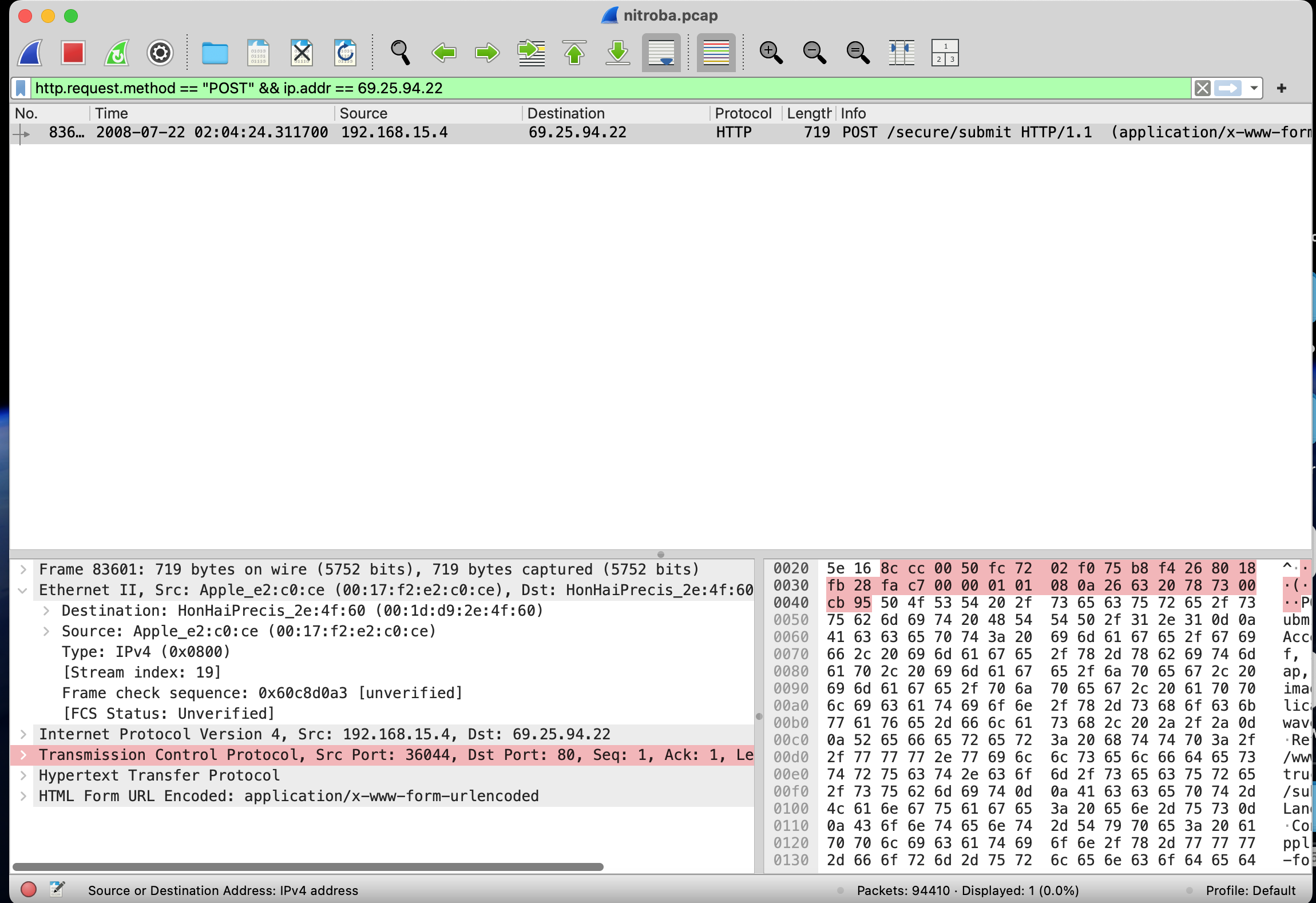
Determine if the IP Posted Harassing Comments

* Search for HTTP POST requests originating from that IP.
* In particular, look for the POST field named data-text-lines (used for line-based text submissions).
* Apply a filter such as
  + Http.request.method == “POST”
* Inspect the POST payload to see if it contains the harassing text.
* IP address: 69.25.94.22

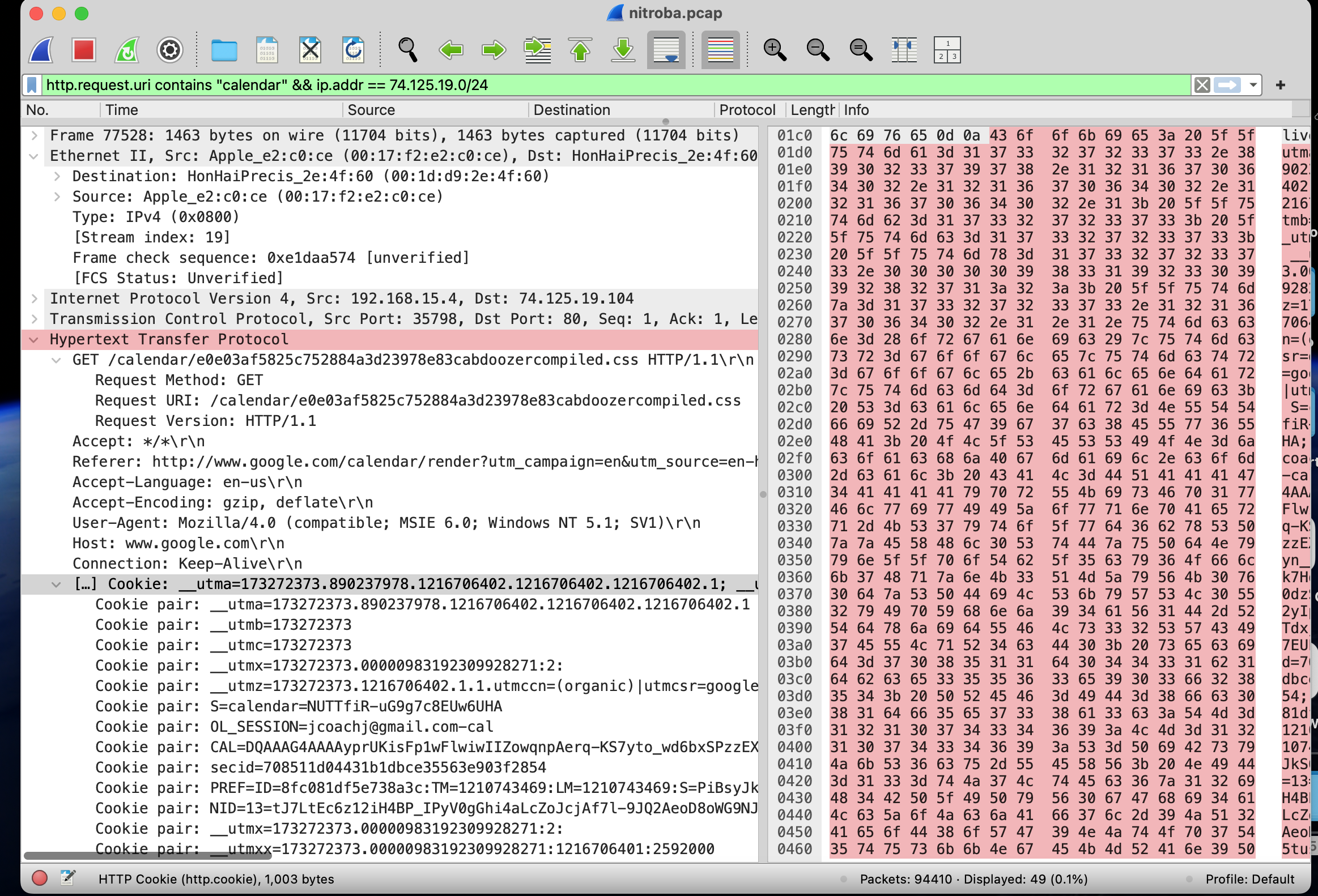


Correlate IP to a MAC Address

* Once you have the suspect IP, find the corresponding MAC address in the same HTTP transactions.
* Use a filter like:
  + Ip.addr == <suspect\_IP>
  + And observe the Ethernet frames for the source MAC
  + Mac address: 00:17:f2:e2:c0:ce

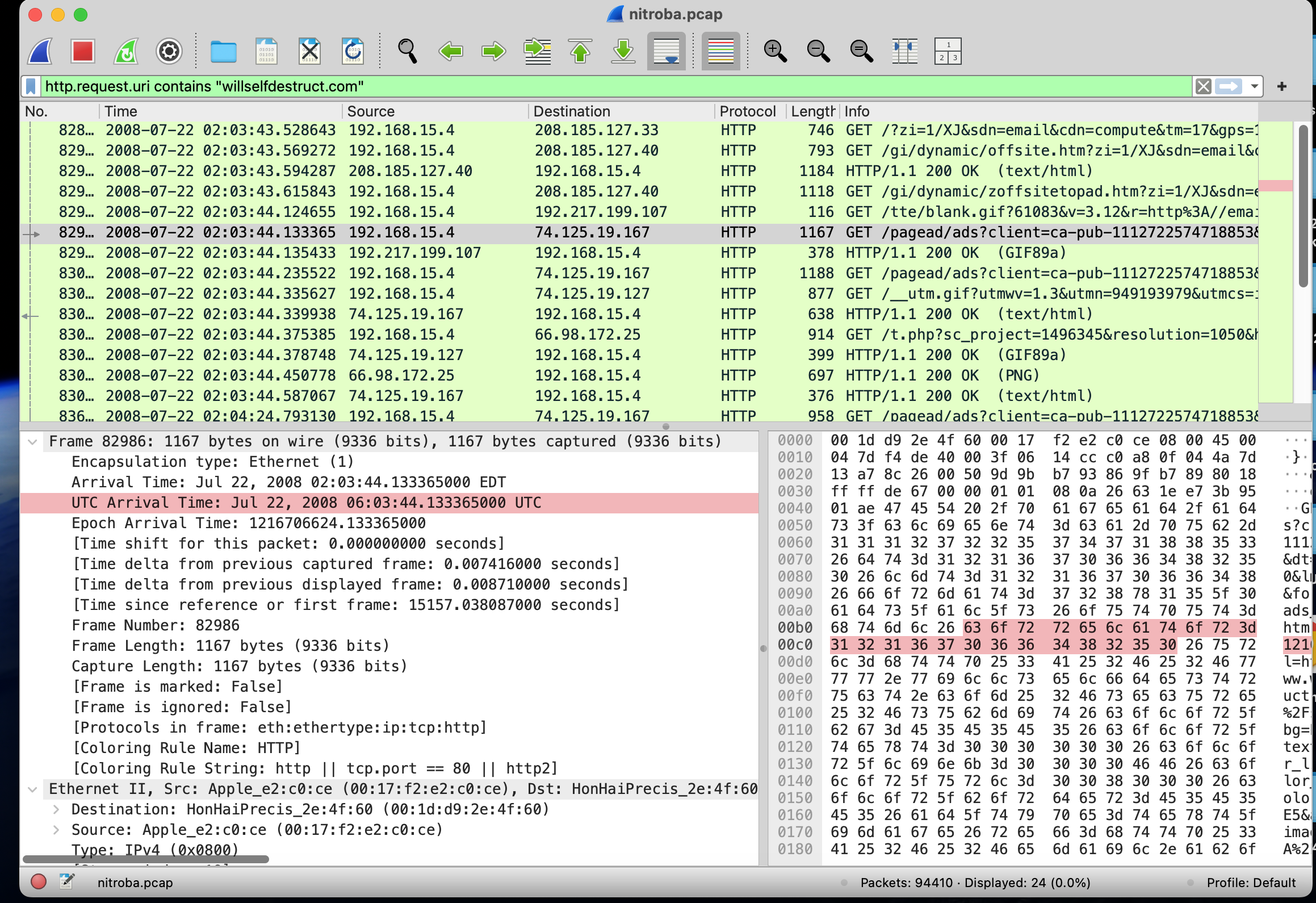


Match the MAC Address to a suspect



* Mac address matches with IP address of suspect.
* The suspect’s email was found in the cookies filter.

Determine the Timing of Access



* The suspect’s machine accessed willselfdestruct.com on July, 22, 2008 at 6:03.

Answer the Following Questions

Which IP accessed [www.willselfdestruct.com](https://www.willselfdestruct.com)?

* 74.125.19.96

Does that IP post harassing comments to the website?

* No, 69.25.94.22 posted harassing comments to the website.

Does the HTTP POST contain the harassment message?

* Yes, the HTTP Post contained the message.

Is that IP associated with any suspect on the class roster?

* Yes, it is Johnny Coach.

Is the suspect in the faculty’s class?

* Yes, it is Johnny Coach.

When did the suspect use [www.willselfdestruct.com](https://www.willselfdestruct.com)?

* July, 22, 2008 at 6:03.