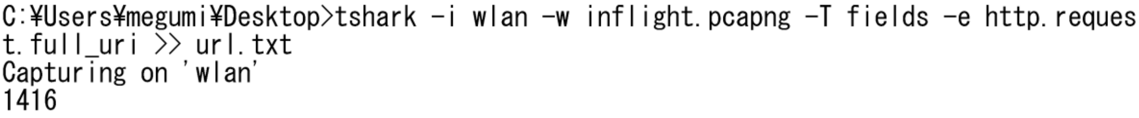
Christmas Wireshark exercise by Megumi Takeshita, ikeriri (@ikeriri)

I am at the aircraft and the flight gives us inflight Wi-Fi service, I have no idea where to go, so let's start fun Christmas Wireshark exercise in the air

1: Start capturing using tshark, and output request URLs to url.txt

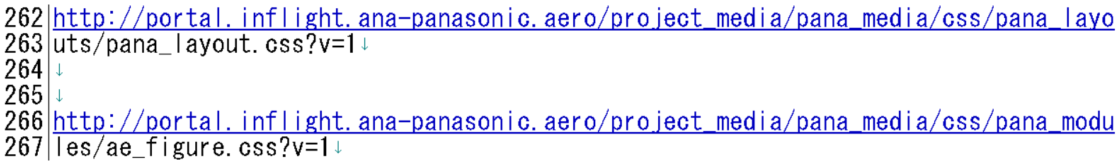
tshark -i wlan -w Desktop¥inflight.pcapng -T fields -e http.request.full_uri >> url.txt



```
C:¥Users¥megumi¥Desktop>tshark -i wlan -w inflight.pcapng -T fields -e http.reques
t.full_uri >> url.txt
Capturing on 'wlan'
1416
```

2: Connect inflight Wi-Fi SSID and (automatically) open captive portal page.

3: Ctrl+C to stop capturing and open url.txt, it contains some parameters.

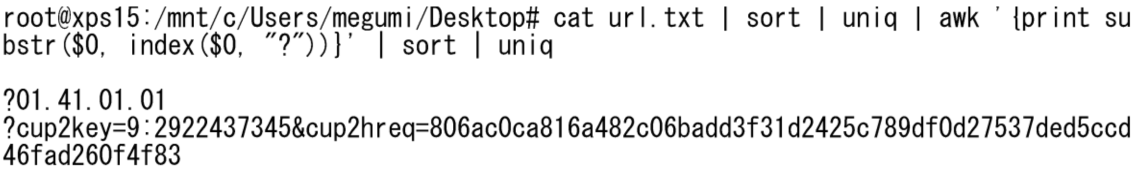


```
http://portal.inflight.ana-panasonic.aero/project_media/pana_media/css/pana_layo
uts/pana_layout.css?v=1↓
↓
↓
http://portal.inflight.ana-panasonic.aero/project_media/pana_media/css/pana_modu
les/ae_figure.css?v=1↓
```

4: start bash, sort and uniq to filter the same sentence, use awk to exclude the words before '?' character and sort, uniq again.

bash cat url.txt | sort | uniq | awk '{print substr($0, index($0, "?"))}' | sort | uniq

we get the parameters lists of http request packet like this

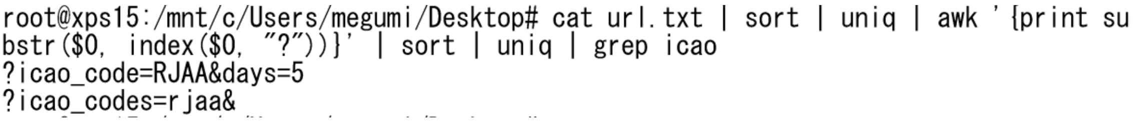


```
root@xps15:/mnt/c/Users/megumi/Desktop# cat url.txt | sort | uniq | awk '{print su
bstr($0, index($0, "?"))}' | sort | uniq

?01.41.01.01
?cup2key=9:2922437345&cup2hreq=806ac0ca816a482c06badd3f31d2425c789df0d27537ded5ccd
46fad260f4f83
```

5: let's find airport, check ICAO (International Civil Aviation Organization) airport code, dd grep icao to the same command, do it again.

cat url.txt | sort | uniq | awk '{print substr($0, index($0, "?"))}' | sort | uniq | grep icao



```
root@xps15:/mnt/c/Users/megumi/Desktop# cat url.txt | sort | uniq | awk '{print su
bstr($0, index($0, "?"))}' | sort | uniq | grep icao
?icao_code=RJAA&days=5
?icao_codes=rjaa&
```

Finally we can find our destination, Narita International Airport (IATA code NRT and ICAO code : RJAA), welcome to Tokyo !!