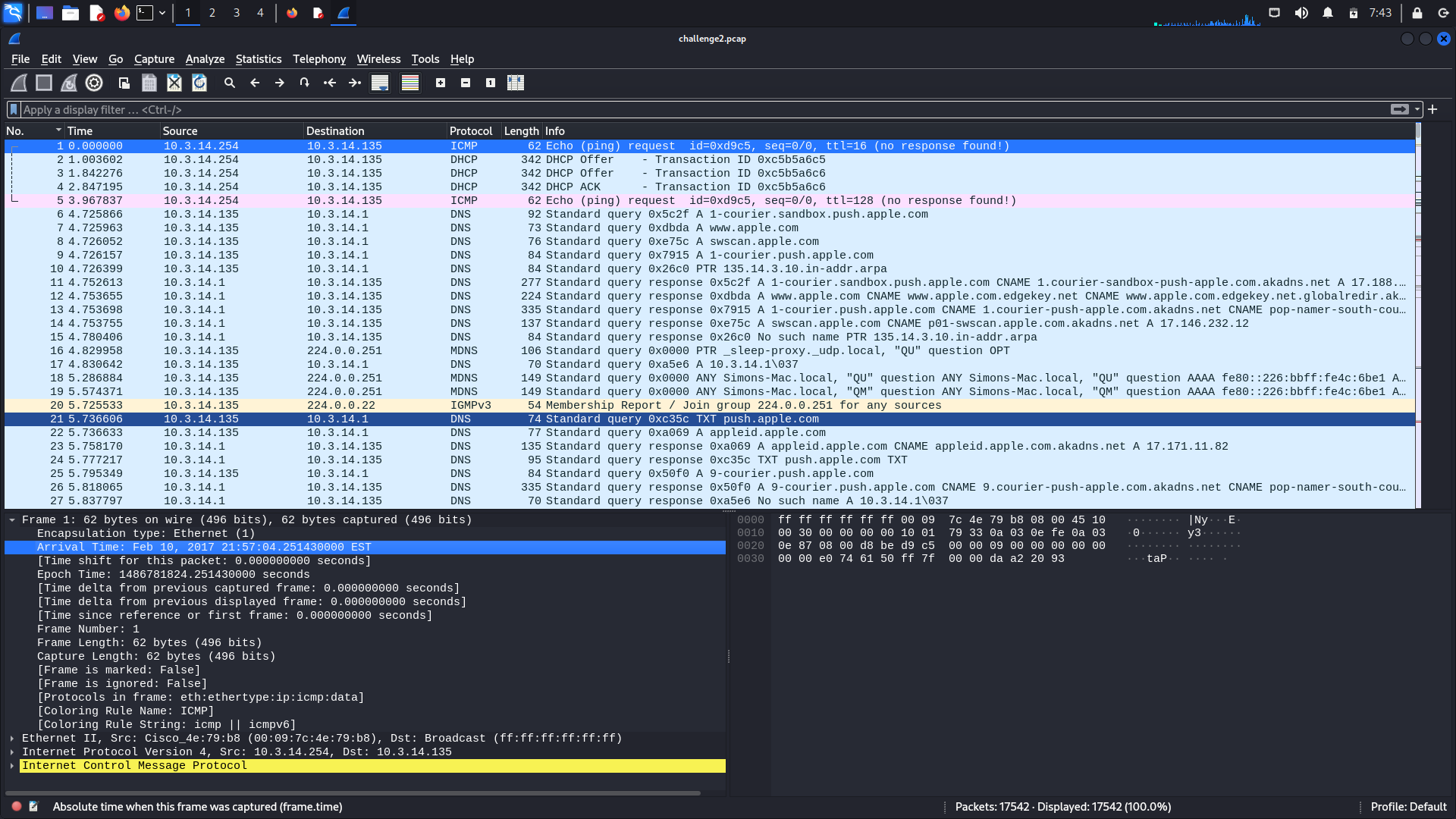
**QUESTIONS BASIC:**

1.Document the date, start time and end time of the pcap in UTC (GMT).

Ans. Select 1st packet expand **Frame Header**. Check arrive time.

**A screenshot of a computer

Description automatically generatedIn GMT Feb 11, 2017 02:57:04.251430000 GMT**.

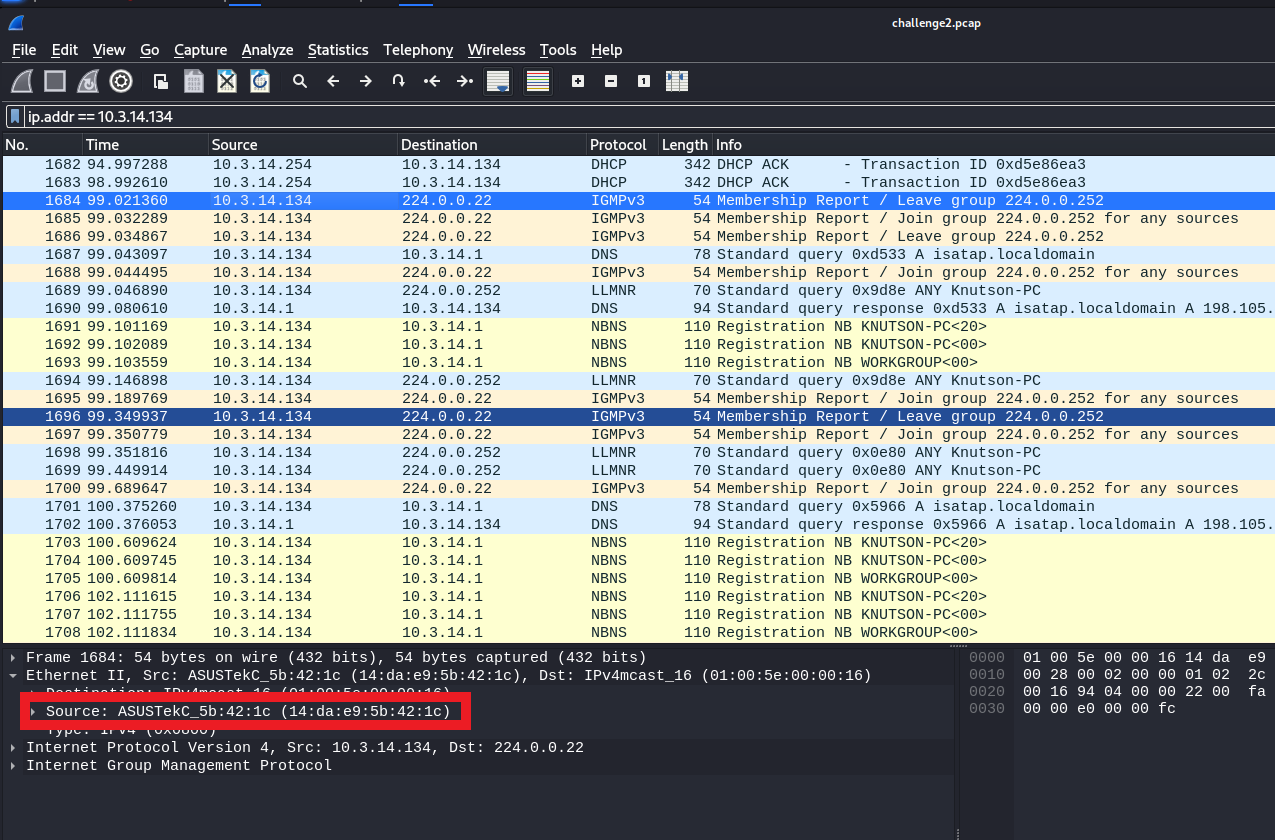
2.Document the IP address of the three hosts in the pcap.

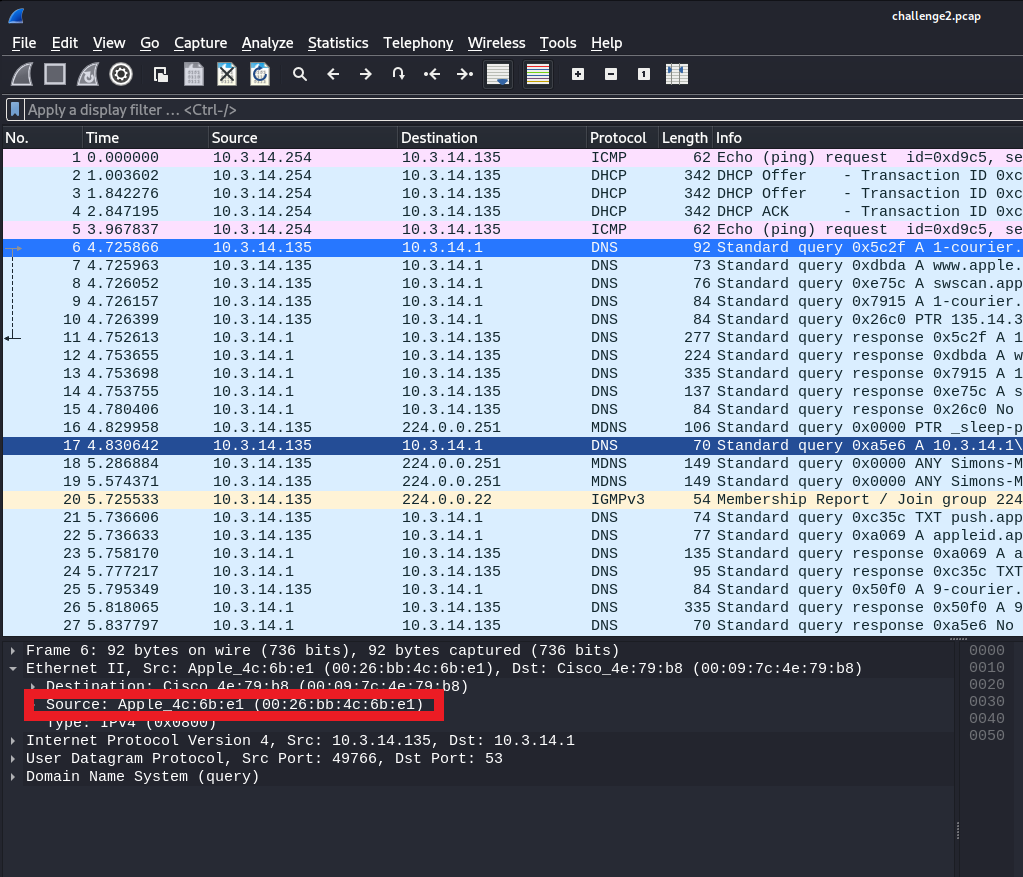
**Ans. IP Address of Hosts 10.3.14.131, 10.3.14.134, 10.3.14.135**

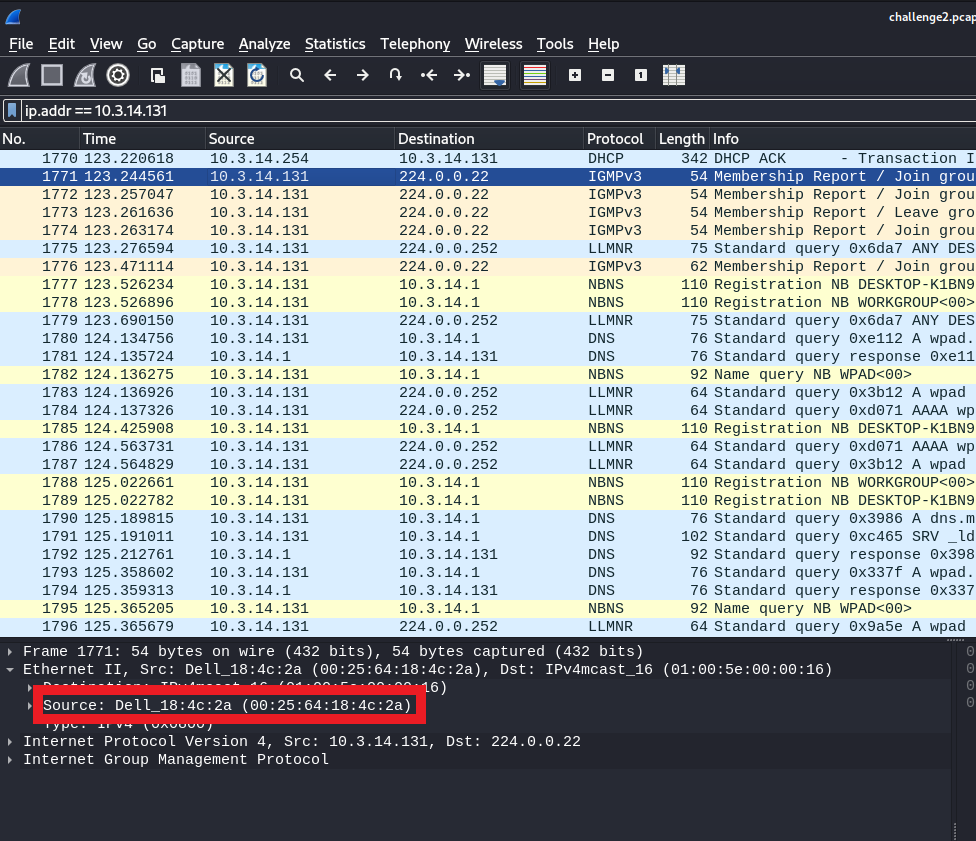
A screenshot of a computer

Description automatically generated

3.Document the mac address of the three hosts in the pcap.

Ans. **MAC Address of 10.3.14.134 is 14:da:e9:5b:42:1c**

 **MAC Address of 10.3.14.135 is 00:26:bb:4c:6b:e1**

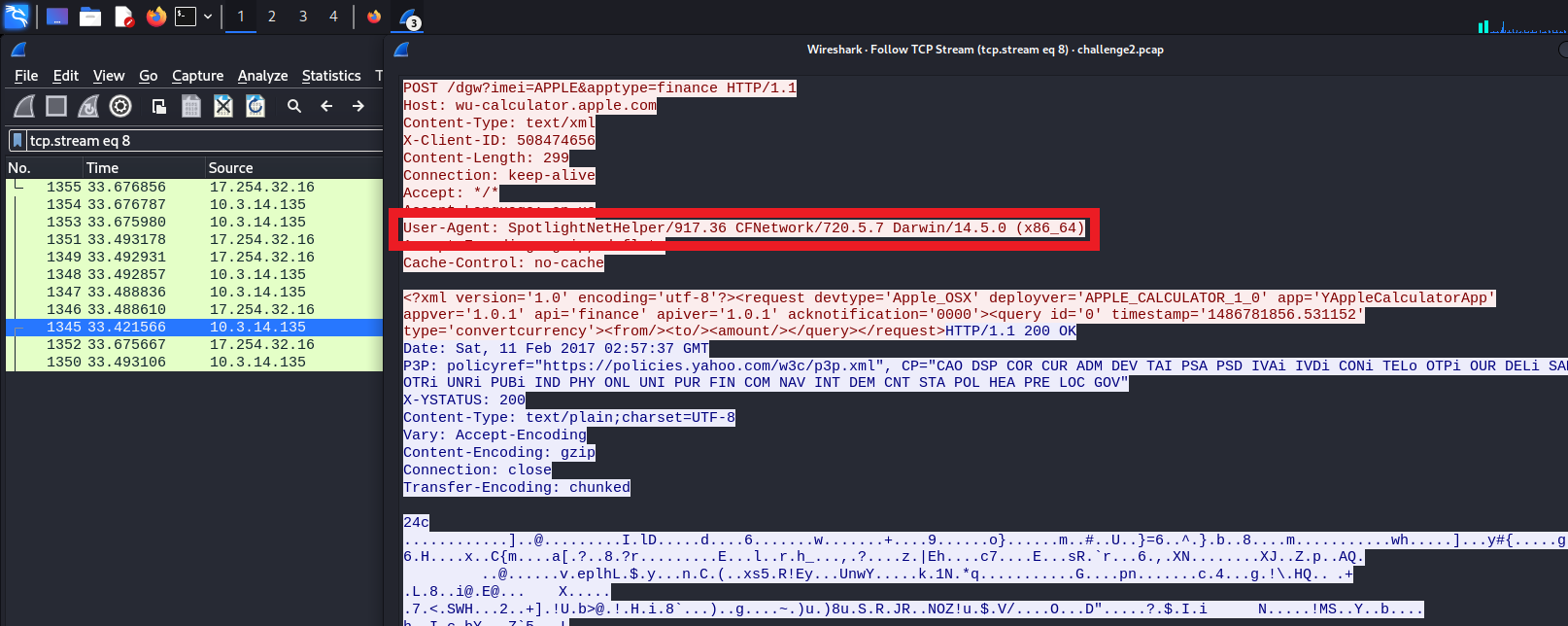
**MAC Address of 10.3.14.131 is 00:25:64:18:4c:2a**

4.Document the type of computer (Windows, Mac, Android, etc) for each of the three hosts in the pcap.

A screen shot of a computer

Description automatically generatedAns. **10.3.14.134 Host is using Windows 7 machine.**

**10.3.14.135 Host is using MacOS.**



**A screenshot of a computer

Description automatically generated10.3.14.131 Host is using Windows 10 OS**

5.Determine which host(s) were infected.

**A screenshot of a computer

Description automatically generatedAns. Inspect all the file in HTTP Object list. Upload file on virustotal.com to see is file is Infected or not. Doing same Two files found Infected load.php & search.php .**

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

MORE ADVANCED:

6.Document the family (or families) of malware based on indicators from the pcap.

**Ans. Family of malware was Trojan Ransomware.**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

7.Document the root cause for any infections noted in the pcap.

**A screenshot of a computer

Description automatically generatedAns. Analysing packet reveals. The MZ…………………………@ is a executable file format used for .EXE files in DOS.**

A screenshot of a computer

Description automatically generated

8. Searched malicious website from this virus got downloaded in system.

**Ans. For Host 10.3.14.131 malware was downloaded from unittogreas.top & For Host 10.3.14.135 malware was downloaded from kuzem2.kku.edu.tr**

A screenshot of a computer

Description automatically generated