Afeefah Manzoor

ITN261

Exam hands on

Part 2 A:

IP address of the Windows computer that was infected.

172.16.174.93



MAC address of the Windows computer that was infected.

5c:26:0a:83:b1:d5



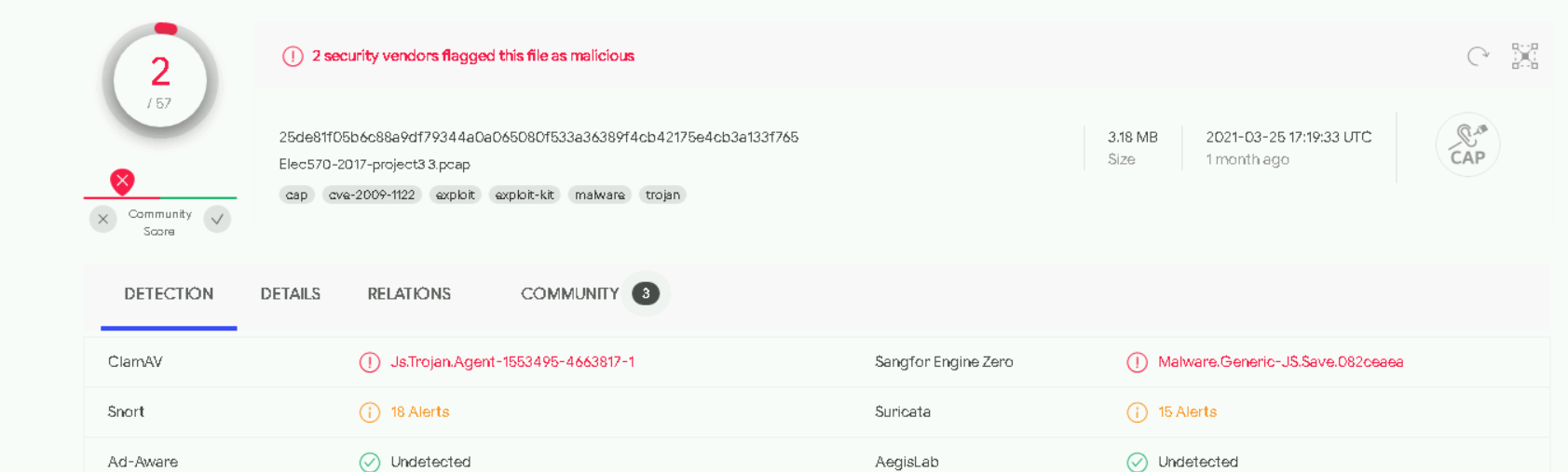
Host name of the Windows computer that was infected.

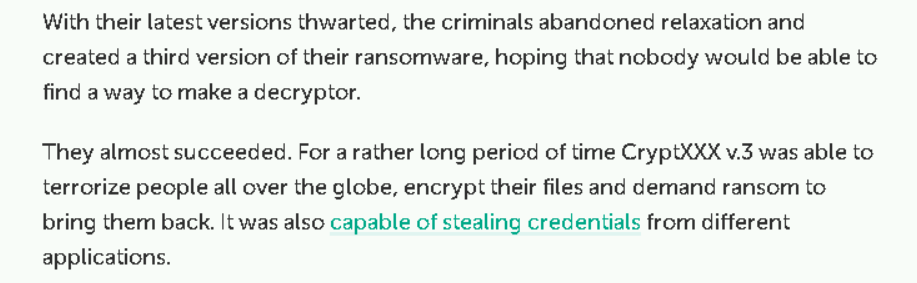
BROCK-PC

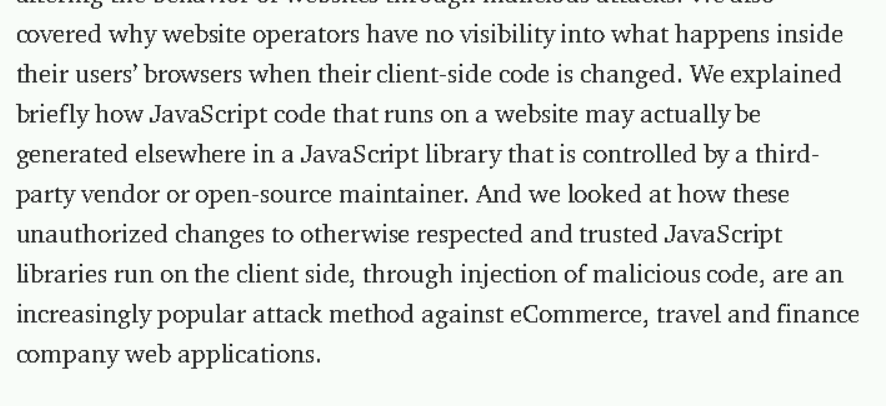


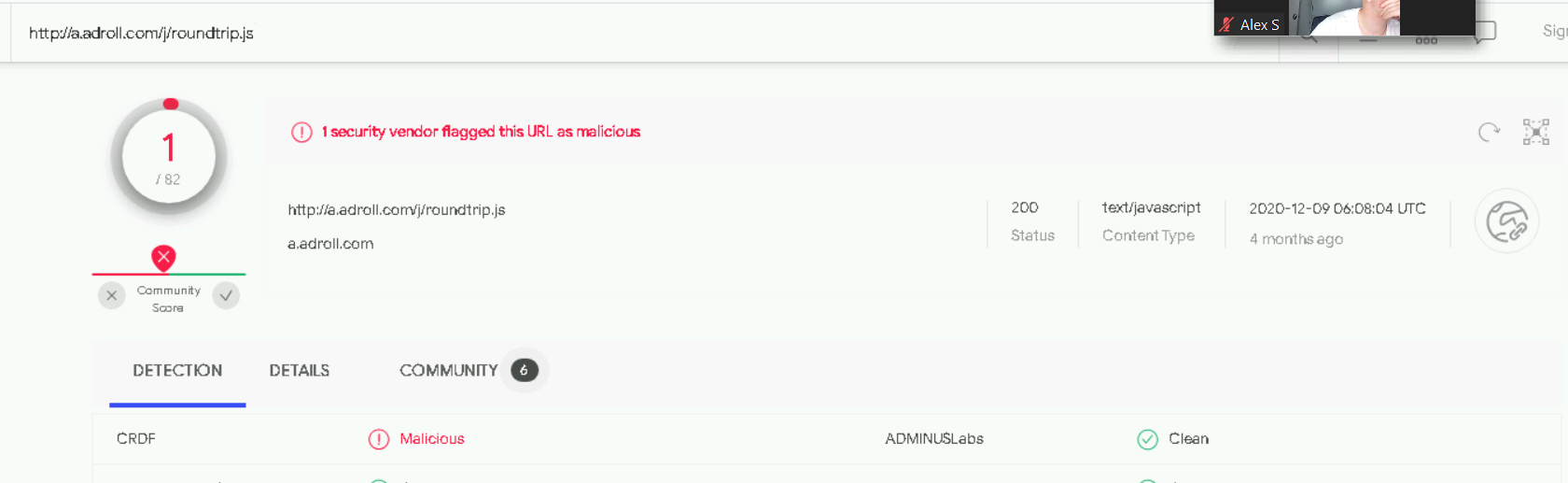
A description of what happened.

Brock-PC has a CryptXXX trojan on his computer that was installed on his machine through a javascript code when he was doing research on his trip to Asia. He got the trojan from a.adroll.com/rountrip.js that installed the javascript file when he visited the site.





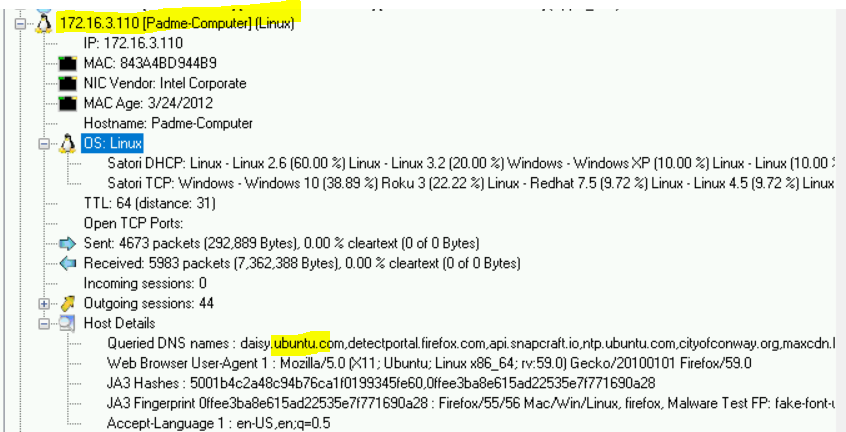




Part 2 B:

Which IP address represents a host running Ubuntu?

172.16.3.110



What type of host is using IP address 172.16.3.188?

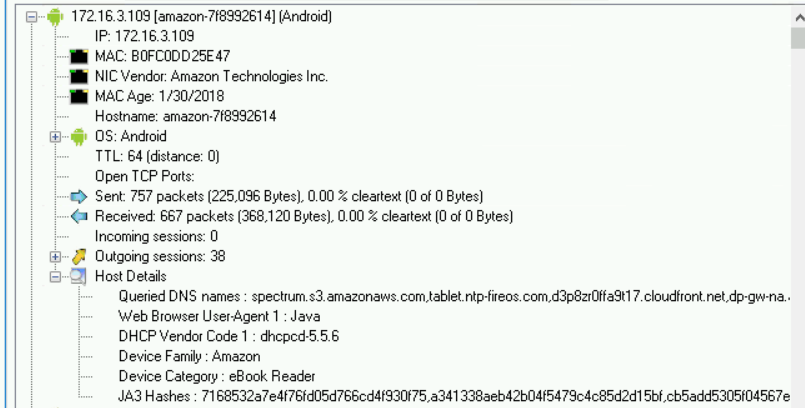
iPhone 8





Which IP address is mostly likely an Amazon Fire tablet?

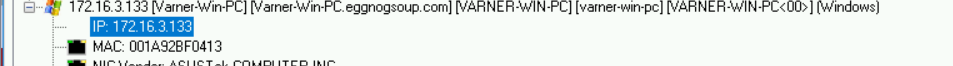
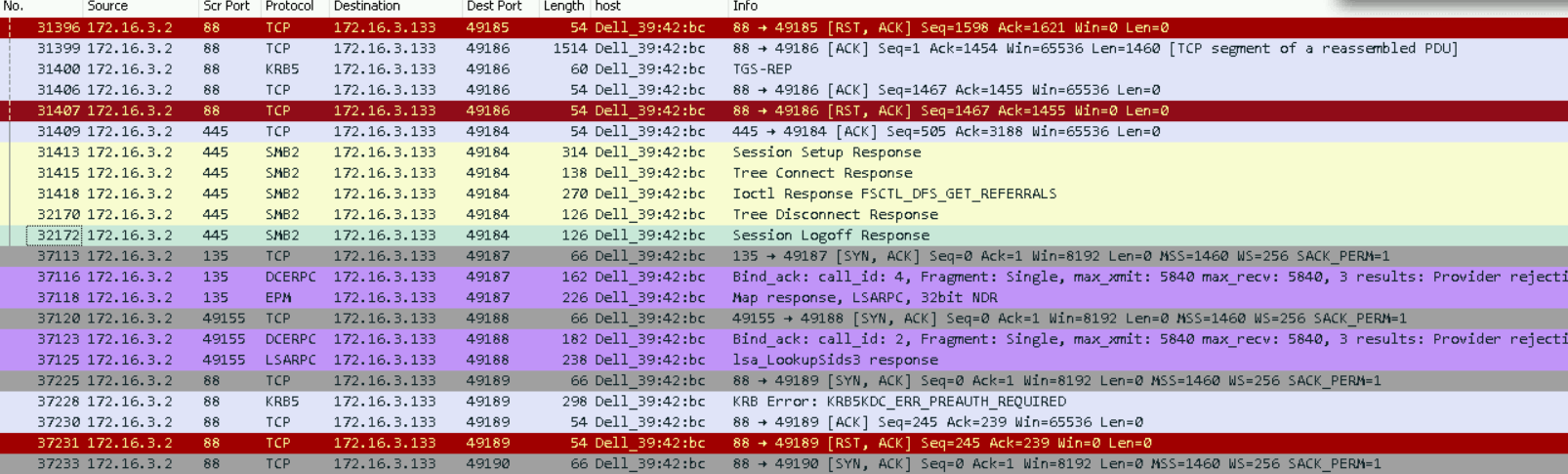
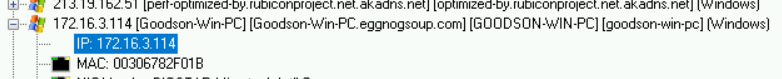
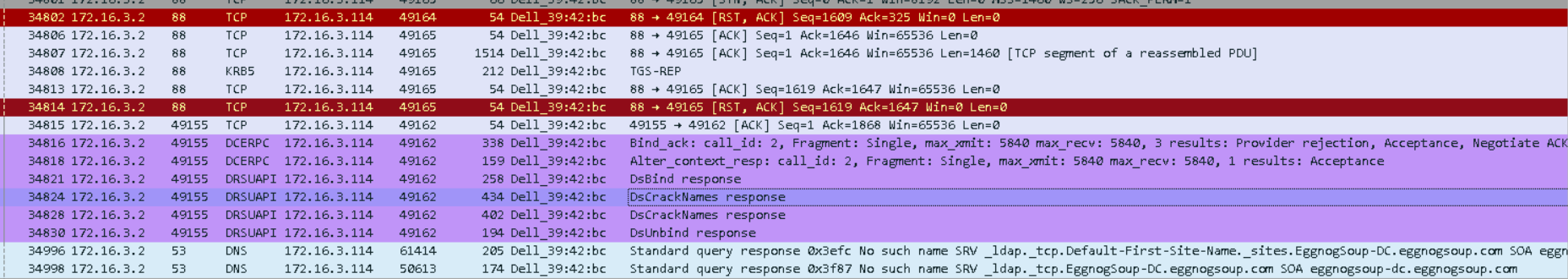
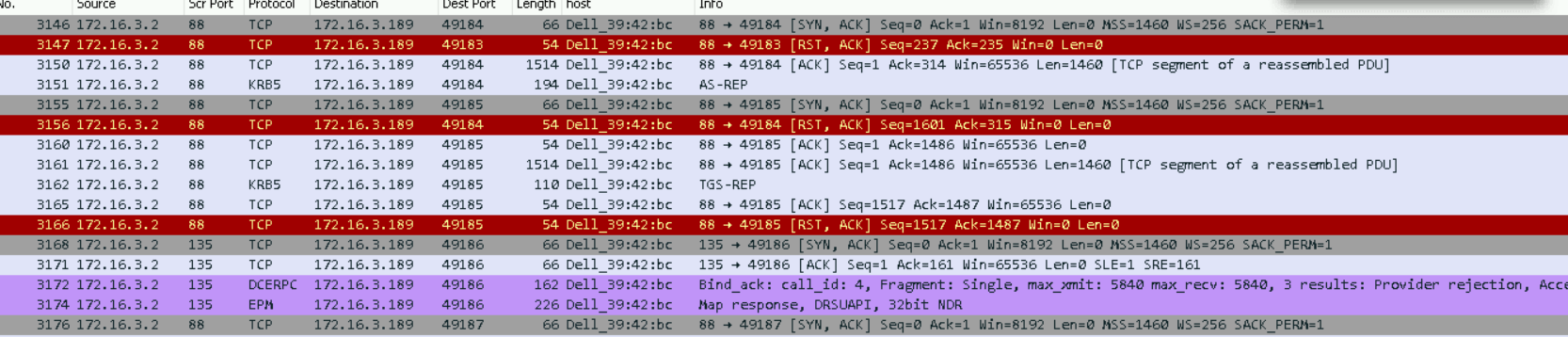
172.16.3.109





Which of the three Windows hosts shows indications of an infection with Emotet and IcedID banking Trojan (Bokbot)?

1. 172.16.3.189 (Palumbo-Win-PC)
2. 172.16.3.114 (Goodson-Win-PC)
3. 172.16.3.133 (Varner-Win-PC)

What is the brand and type of device on 172.16.3.112?

Samsung

Some sort of Tablet or eBook

