

## Lab Notebook 2

Submitted By: Shrikrishna Bhat

### Contents

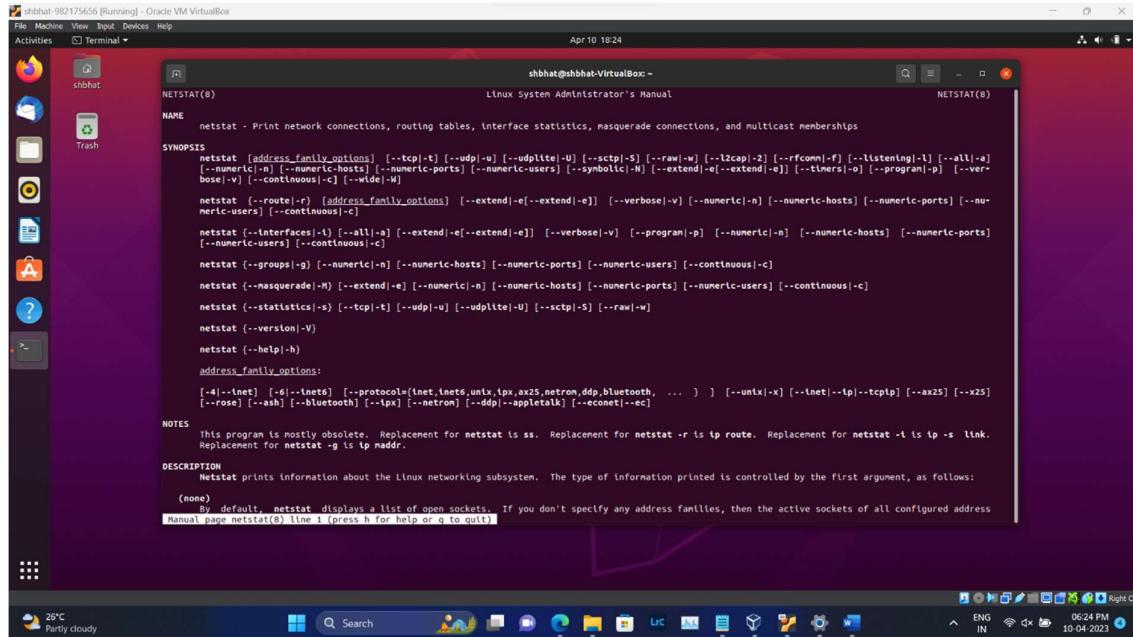
|                                      |    |
|--------------------------------------|----|
| Section 1.....                       | 2  |
| TCP #1 .....                         | 2  |
| 1.1 netstat.....                     | 2  |
| 1.2 lsof.....                        | 4  |
| 1.3 nc.....                          | 5  |
| TCP #2 .....                         | 6  |
| 2.1 iperf.....                       | 6  |
| HTTP # 3.....                        | 8  |
| 3.1 HTTP developer tools Part 1..... | 8  |
| 3.2 HTTP developer tools Part 2..... | 8  |
| 3.3 HTTP developer tools Part 3..... | 10 |
| 3.4 Asynchronous HTTP requests.....  | 12 |
| Section 2.....                       | 14 |
| DNS #1.....                          | 14 |
| 1.1 dig .....                        | 14 |
| 1.2 DNS iterative lookup .....       | 18 |
| 1.3 Reverse DNS Lookup .....         | 20 |
| 1.4 Hosts Enumeration .....          | 21 |
| DNS #2.....                          | 22 |
| 2.1 Geographic DNS.....              | 22 |
| Network Recap Lab #3 .....           | 27 |
| 3.1 REVERSE DNS.....                 | 27 |
| 3.2 ARP and Wireshark.....           | 29 |

## Section 1

### TCP #1

#### 1.1 netstat

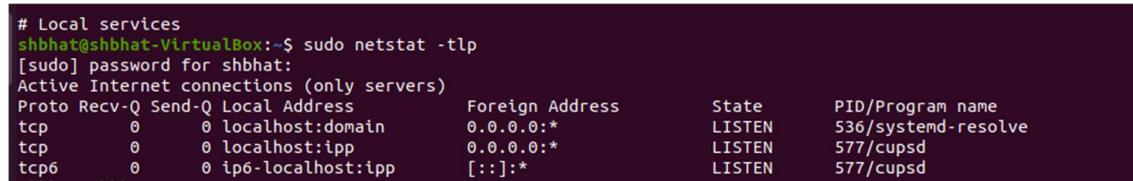
##### 1.1.1 man netstat



```
shbhat@shbhat-VirtualBox:~$ man netstat
shbhat@shbhat-VirtualBox:~$
```

The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "NETSTAT(8)" and it displays the man page for the "netstat" command. The man page covers topics such as NAME, SYNOPSIS, NOTES, and DESCRIPTION. The notes section mentions that the program is mostly obsolete and replaced by "ss". The description section states that netstat prints information about the Linux networking subsystem. The terminal window is part of a desktop interface with a dock at the bottom containing icons for various applications.

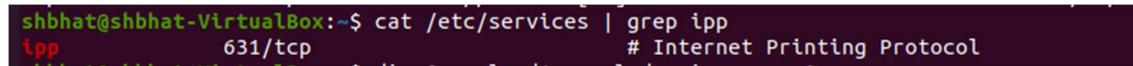
##### 1.1.2 Run the command using sudo and take a screenshot of the output to include in your lab notebook.



```
# Local services
shbhat@shbhat-VirtualBox:~$ sudo netstat -tlp
[sudo] password for shbhat:
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0  localhost:domain        0.0.0.0:*             LISTEN      536/systemd-resolve
tcp        0      0  localhost:ipp          0.0.0.0:*             LISTEN      577/cupsd
tcp6       0      0  ip6-localhost:ipp       [::]:*              LISTEN      577/cupsd
```

##### 1.1.3 For port numbers that are named, examine /etc/services and find the port number that corresponds to it. Include this mapping in your lab notebook.

Answer: I got the port number as 631, which corresponds to ipp.



```
shbhat@shbhat-VirtualBox:~$ cat /etc/services | grep ipp
ipp          631/tcp          # Internet Printing Protocol
```

1.1.4 For ports that only have a number, what service might it be providing based on the name of the program that is being run?

Answer: I did not get any port numbers having only number but on reading about it I found out that it is used to run container services.

1.1.5 Run the netstat command again, but do not use sudo as this is a machine managed by CAT. Include a screenshot of the output.

<img alt="Screenshot of a Linux desktop showing a terminal window running netstat -an. The terminal shows numerous established TCP connections, mostly between the local host and various ports on the network, including ports 22, 23, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 197, 198, 199, 200, 201, 202, 203, 204, 205, 206, 207, 208, 209, 210, 211, 212, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 237, 238, 239, 240, 241, 242, 243, 244, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254, 255, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 267, 268, 269, 270, 271, 272, 273, 274, 275, 276, 277, 278, 279, 280, 281, 282, 283, 284, 285, 286, 287, 288, 289, 290, 291, 292, 293, 294, 295, 296, 297, 298, 299, 299, 300, 301, 302, 303, 304, 305, 306, 307, 308, 309, 310, 311, 312, 313, 314, 315, 316, 317, 318, 319, 320, 321, 322, 323, 324, 325, 326, 327, 328, 329, 330, 331, 332, 333, 334, 335, 336, 337, 338, 339, 340, 341, 342, 343, 344, 345, 346, 347, 348, 349, 350, 351, 352, 353, 354, 355, 356, 357, 358, 359, 360, 361, 362, 363, 364, 365, 366, 367, 368, 369, 370, 371, 372, 373, 374, 375, 376, 377, 378, 379, 380, 381, 382, 383, 384, 385, 386, 387, 388, 389, 390, 391, 392, 393, 394, 395, 396, 397, 398, 399, 399, 400, 401, 402, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 418, 419, 420, 421, 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 432, 433, 434, 435, 436, 437, 438, 439, 440, 441, 442, 443, 444, 445, 446, 447, 448, 449, 450, 451, 452, 453, 454, 455, 456, 457, 458, 459, 459, 460, 461, 462, 463, 464, 465, 466, 467, 468, 469, 469, 470, 471, 472, 473, 474, 475, 476, 477, 478, 479, 479, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 489, 490, 491, 492, 493, 494, 495, 496, 497, 498, 499, 499, 500, 501, 502, 503, 504, 505, 506, 507, 508, 509, 509, 510, 511, 512, 513, 514, 515, 516, 517, 518, 519, 519, 520, 521, 522, 523, 524, 525, 526, 527, 528, 529, 529, 530, 531, 532, 533, 534, 535, 536, 537, 538, 539, 539, 540, 541, 542, 543, 544, 545, 546, 547, 548, 549, 549, 550, 551, 552, 553, 554, 555, 556, 557, 558, 559, 559, 560, 561, 562, 563, 564, 565, 566, 567, 568, 569, 569, 570, 571, 572, 573, 574, 575, 576, 577, 578, 579, 579, 580, 581, 582, 583, 584, 585, 586, 587, 588, 589, 589, 590, 591, 592, 593, 594, 595, 596, 597, 598, 599, 599, 600, 601, 602, 603, 604, 605, 606, 607, 608, 609, 609, 610, 611, 612, 613, 614, 615, 616, 617, 618, 619, 619, 620, 621, 622, 623, 624, 625, 626, 627, 628, 629, 629, 630, 631, 632, 633, 634, 635, 636, 637, 638, 639, 639, 640, 641, 642, 643, 644, 645, 646, 647, 648, 649, 649, 650, 651, 652, 653, 654, 655, 656, 657, 658, 659, 659, 660, 661, 662, 663, 664, 665, 666, 667, 668, 669, 669, 670, 671, 672, 673, 674, 675, 676, 677, 678, 679, 679, 680, 681, 682, 683, 684, 685, 686, 687, 688, 689, 689, 690, 691, 692, 693, 694, 695, 696, 697, 698, 699, 699, 700, 701, 702, 703, 704, 705, 706, 707, 708, 709, 709, 710, 711, 712, 713, 714, 715, 715, 716, 717, 718, 719, 719, 720, 721, 722, 723, 724, 725, 726, 727, 728, 729, 729, 730, 731, 732, 733, 734, 735, 735, 736, 737, 738, 739, 739, 740, 741, 742, 743, 744, 745, 746, 747, 748, 749, 749, 750, 751, 752, 753, 754, 755, 756, 757, 758, 759, 759, 760, 761, 762, 763, 764, 765, 766, 767, 768, 769, 769, 770, 771, 772, 773, 774, 775, 776, 777, 778, 779, 779, 780, 781, 782, 783, 784, 785, 786, 787, 788, 789, 789, 790, 791, 792, 793, 794, 795, 796, 797, 798, 799, 799, 800, 801, 802, 803, 804, 805, 806, 807, 808, 809, 809, 810, 811, 812, 813, 814, 815, 815, 816, 817, 818, 819, 819, 820, 821, 822, 823, 824, 825, 826, 827, 828, 829, 829, 830, 831, 832, 833, 834, 835, 836, 837, 838, 839, 839, 840, 841, 842, 843, 844, 845, 846, 847, 848, 849, 849, 850, 851, 852, 853, 854, 855, 856, 857, 858, 859, 859, 860, 861, 862, 863, 864, 865, 866, 867, 868, 869, 869, 870, 871, 872, 873, 874, 875, 876, 877, 878, 879, 879, 880, 881, 882, 883, 884, 885, 886, 887, 888, 889, 889, 890, 891, 892, 893, 894, 895, 896, 897, 898, 899, 899, 900, 901, 902, 903, 904, 905, 906, 907, 908, 909, 909, 910, 911, 912, 913, 914, 915, 915, 916, 917, 918, 919, 919, 920, 921, 922, 923, 924, 925, 926, 927, 928, 929, 929, 930, 931, 932, 933, 934, 935, 936, 937, 938, 939, 939, 940, 941, 942, 943, 944, 945, 946, 947, 948, 949, 949, 950, 951, 952, 953, 954, 955, 956, 957, 958, 959, 959, 960, 961, 962, 963, 964, 965, 966, 967, 968, 969, 969, 970, 971, 972, 973, 974, 975, 976, 977, 978, 979, 979, 980, 981, 982, 983, 984, 985, 986, 987, 988, 989, 989, 990, 991, 992, 993, 994, 995, 996, 997, 998, 999, 999, 1000, 1001, 1002, 1003, 1004, 1005, 1006, 1007, 1008, 1009, 1009, 1010, 1011, 1012, 1013, 1014, 1015, 1015, 1016, 1017, 1018, 1019, 1019, 1020, 1021, 1022, 1023, 1024, 1025, 1026, 1027, 1027, 1028, 1029, 1029, 1030, 1031, 1032, 1033, 1034, 1035, 1036, 1037, 1038, 1039, 1039, 1040, 1041, 1042, 1043, 1044, 1045, 1046, 1047, 1048, 1049, 1049, 1050, 1051, 1052, 1053, 1054, 1055, 1056, 1057, 1058, 1059, 1059, 1060, 1061, 1062, 1063, 1064, 1065, 1066, 1067, 1068, 1069, 1069, 1070, 1071, 1072, 1073, 1074, 1075, 1076, 1077, 1078, 1079, 1079, 1080, 1081, 1082, 1083, 1084, 1085, 1086, 1087, 1088, 1089, 1089, 1090, 1091, 1092, 1093, 1094, 1095, 1096, 1097, 1097, 1098, 1099, 1099, 1100, 1101, 1102, 1103, 1104, 1105, 1106, 1107, 1108, 1109, 1109, 1110, 1111, 1112, 1113, 1114, 1115, 1116, 1117, 1118, 1119, 1119, 1120, 1121, 1122, 1123, 1124, 1125, 1126, 1127, 1128, 1129, 1129, 1130, 1131, 1132, 1133, 1134, 1135, 1136, 1137, 1138, 1139, 1139, 1140, 1141, 1142, 1143, 1144, 1145, 1146, 1147, 1148, 1149, 1149, 1150, 1151, 1152, 1153, 1154, 1155, 1156, 1157, 1158, 1159, 1159, 1160, 1161, 1162, 1163, 1164, 1165, 1166, 1167, 1168, 1169, 1169, 1170, 1171, 1172, 1173, 1174, 1175, 1176, 1177, 1178, 1179, 1179, 1180, 1181, 1182, 1183, 1184, 1185, 1186, 1187, 1188, 1189, 1189, 1190, 1191, 1192, 1193, 1194, 1195, 1195, 1196, 1197, 1197, 1198, 1199, 1199, 1200, 1201, 1202, 1203, 1204, 1205, 1206, 1207, 1208, 1209, 1209, 1210, 1211, 1212, 1213, 1214, 1215, 1216, 1217, 1218, 1219, 1219, 1220, 1221, 1222, 1223, 1224, 1225, 1226, 1227, 1228, 1229, 1229, 1230, 1231, 1232, 1233, 1234, 1235, 1236, 1237, 1238, 1239, 1239, 1240, 1241, 1242, 1243, 1244, 1245, 1246, 1247, 1248, 1249, 1249, 1250, 1251, 1252, 1253, 1254, 1255, 1256, 1257, 1258, 1259, 1259, 1260, 1261, 1262, 1263, 1264, 1265, 1266, 1267, 1268, 1269, 1269, 1270, 1271, 1272, 1273, 1274, 1275, 1276, 1277, 1278, 1279, 1279, 1280, 1281, 1282, 1283, 1284, 1285, 1286, 1287, 1288, 1289, 1289, 1290, 1291, 1292, 1293, 1294, 1295, 1295, 1296, 1297, 1297, 1298, 1299, 1299, 1300, 1301, 1302, 1303, 1304, 1305, 1306, 1307, 1308, 1309, 1309, 1310, 1311, 1312, 1313, 1314, 1315, 1316, 1317, 1318, 1318, 1319, 1320, 1321, 1322, 1323, 1324, 1325, 1326, 1327, 1328, 1329, 1329, 1330, 1331, 1332, 1333, 1334, 1335, 1336, 1337, 1338, 1339, 1339, 1340, 1341, 1342, 1343, 1344, 1345, 1346, 1347, 1348, 1349, 1349, 1350, 1351, 1352, 1353, 1354, 1355, 1356, 1357, 1358, 1359, 1359, 1360, 1361, 1362, 1363, 1364, 1365, 1366, 1367, 1368, 1369, 1369, 1370, 1371, 1372, 1373, 1374, 1375, 1376, 1377, 1378, 1379, 1379, 1380, 1381, 1382, 1383, 1384, 1385, 1386, 1387, 1388, 1389, 1389, 1390, 1391, 1392, 1393, 1394, 1395, 1395, 1396, 1397, 1397, 1398, 1399, 1399, 1400, 1401, 1402, 1403, 1404, 1405, 1406, 1407, 1408, 1409, 1409, 1410, 1411, 1412, 1413, 1414, 1415, 1416, 1417, 1418, 1418, 1419, 1420, 1421, 1422, 1423, 1424, 1425, 1426, 1427, 1428, 1429, 1429, 1430, 1431, 1432, 1433, 1434, 1435, 1436, 1437, 1438, 1439, 1439, 1440, 1441, 1442, 1443, 1444, 1445, 1446, 1447, 1448, 1449, 1449, 1450, 1451, 1452, 1453, 1454, 1455, 1456, 1457, 1458, 1459, 1459, 1460, 1461, 1462, 1463, 1464, 1465, 1466, 1467, 1468, 1469, 1469, 1470, 1471, 1472, 1473, 1474, 1475, 1476, 1477, 1477, 1478, 1479, 1479, 1480, 1481, 1481, 1482, 1483, 1484, 1485, 1486, 1487, 1488, 1489, 1489, 1490, 1491, 1492, 1493, 1494, 1495, 1495, 1496, 1497, 1497, 1498, 1499, 1499, 1500, 1501, 1502, 1503, 1504, 1505, 1506, 1507, 1508, 1509, 1509, 1510, 1511, 1512, 1513, 1514, 1515, 1516, 1517, 1518, 1518, 1519, 1520, 1521, 1522, 1523, 1524, 1525, 1526, 1527, 1528, 1529, 1529, 1530, 1531, 1532, 1533, 1534, 1535, 1536, 1537, 1538, 1539, 1539, 1540, 1541, 1542, 1543, 1544, 1545, 1546, 1547, 1548, 1549, 1549, 1550, 1551, 1552, 1553, 1554, 1555, 1556, 1557, 1558, 1559, 1559, 1560, 1561, 1562, 1563, 1564, 1565, 1566, 1567, 1568, 1569, 1569, 1570, 1571, 1572, 1573, 1574, 1575, 1576, 1577, 1578, 1578, 1579, 1579, 1580, 1581, 1581, 1582, 1583, 1584, 1585, 1586, 1587, 1588, 1589, 1589, 1590, 1591, 1592, 1593, 1594, 1595, 1595, 1596, 1597, 1597, 1598, 1599, 1599, 1600, 1601, 1602, 1603, 1604, 1605, 1606, 1607, 1608, 1609, 1609, 1610, 1611, 1612, 1613, 1614, 1615, 1616, 1617, 1618, 1618, 1619, 1620, 1621, 1622, 1623, 1624, 1625, 1626, 1627, 1628, 1629, 1629, 1630, 1631, 1632, 1633, 1634, 1635, 1636, 1637, 1638, 1639, 1639, 1640, 1641, 1642, 1643, 1644, 1645, 1646, 1647, 1648, 1649, 1649, 1650, 1651, 1652, 1653, 1654, 1655, 1656, 1657, 1658, 1659, 1659, 1660, 1661, 1662, 1663, 1664, 1665, 1666, 1667, 1668, 1669, 1669, 1670, 1671, 1672, 1673, 1674, 1675, 1676, 1677, 1677, 1678, 1679, 1679, 1680, 1681, 1681, 1682, 1683, 1684, 1685, 1686, 1687, 1688, 1689, 1689, 1690, 1691, 1692, 1693, 1694, 1695, 1695, 1696, 1697, 1697, 1698, 1699, 1699, 1700, 1701, 1702, 1703, 1704, 1705, 1706, 1707, 1708, 1709, 1709, 1710, 1711, 1712, 1713, 1714, 1715, 1716, 1717, 1718, 1718, 1719, 1720, 1721, 1722, 1723, 1724, 1725, 1726, 1727, 1728, 1729, 1729, 1730, 1731, 1732, 1733, 1734, 1735, 1736, 1737, 1738, 1739, 1739, 1740, 1741, 1742, 1743, 1744, 1745, 1746, 1747, 1748, 1749, 1749, 1750, 1751, 1752, 1753, 1754, 1755, 1756, 1757, 1758, 1759, 1759, 1760, 1761, 1762, 1763, 1764, 1765, 1766, 1767, 1768, 1769, 1769, 1770, 1771, 1772, 1773, 1774, 1775, 1776, 1777, 1778, 1778, 1779, 1779, 1780, 1781, 1781, 1782, 1783, 1784, 1785, 1786, 1787, 1788, 1789, 1789, 1790, 1791, 1792, 1793, 1794, 1795, 1795, 1796, 1797, 1797, 1798, 1799, 1799, 1800, 1801, 1802, 1803, 1804, 1805, 1806, 1807, 1808, 1809, 1809, 1810, 1811, 1812, 1813, 1814, 1815, 1816, 1817, 1818, 1818, 1819, 1820, 1821, 1822, 1823, 1824, 1825, 1826, 1827, 1828, 1829, 1829, 1830, 1831, 1832, 1833, 1834, 1835, 1836, 1837, 1838, 1839, 1839, 1840, 1841, 1842, 1843, 1844, 1845, 1846, 1847, 1848, 1849, 1849, 1850, 1851, 1852, 1853, 1854, 1855, 1856, 1857, 1858, 1859, 1859, 1860, 1861, 1862, 1863, 1864, 1865, 1866, 1867, 1868, 1869, 1869, 1870, 1871, 1872, 1873, 1874, 1875, 1876, 1877, 1877, 1878, 1879, 1879, 1880, 1881, 1881, 1882, 1883, 1884, 1885, 1886, 1887, 1888, 1889, 1889, 1890, 1891, 1892, 1893, 1894, 1895, 1895, 1896, 1897, 1897, 1898, 1899, 1899, 1900, 1901, 1902, 1903,

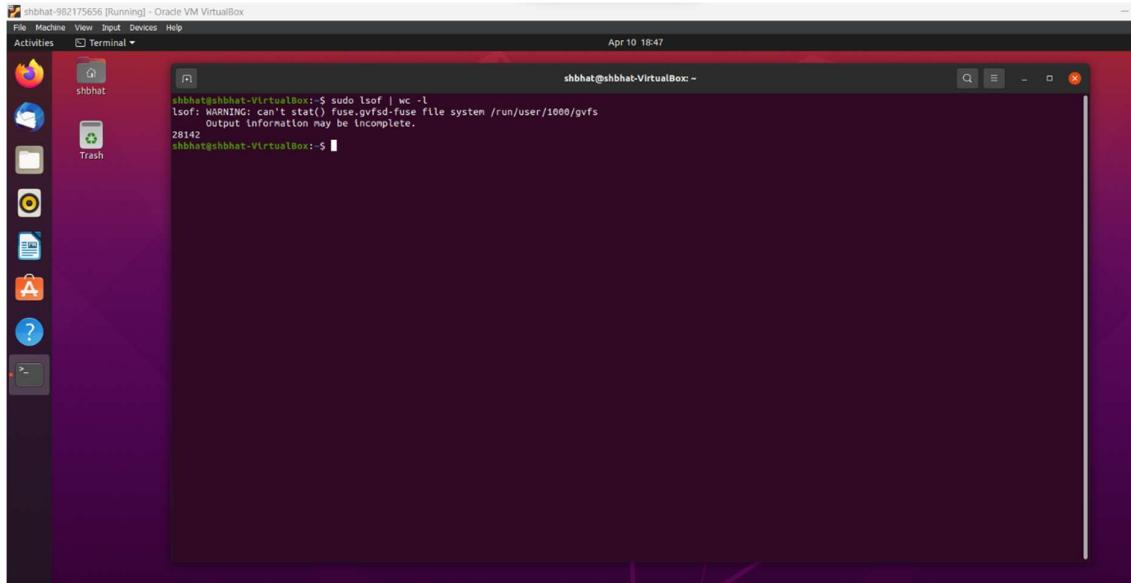
### 1.1.6 What services does this machine provide for external access?

Answer:

It depends on which port the services are being run, some may provide container service. Some may provide IPP service etc.

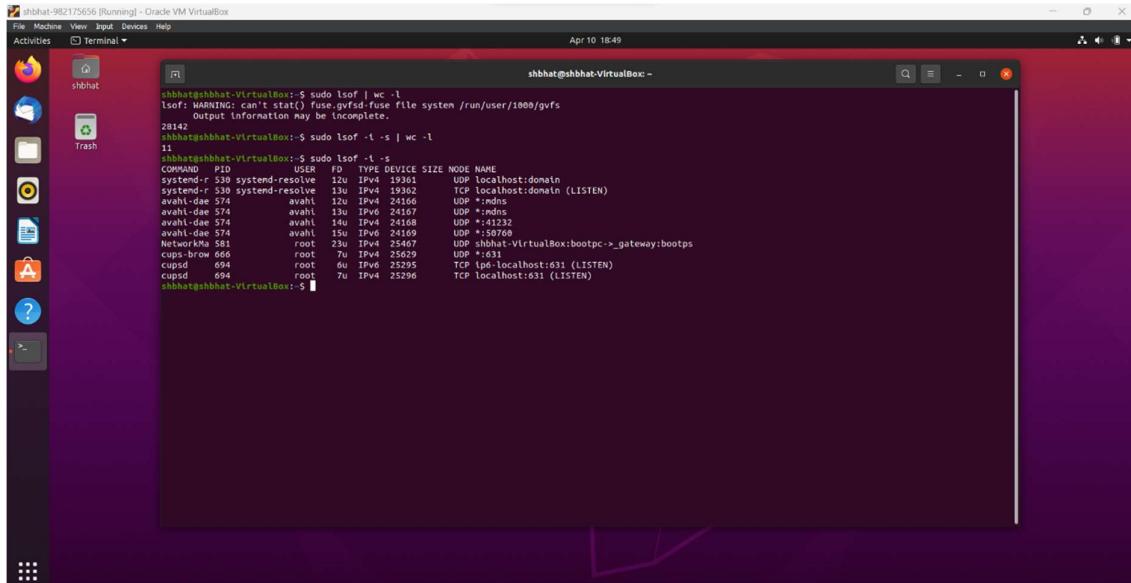
### 1.2 lsof

#### 1.2.1 sudo lsof | wc -l



```
shbhat@shbhat-VirtualBox:~$ sudo lsof | wc -l
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs
          Output information may be incomplete.
28142
shbhat@shbhat-VirtualBox:~$
```

#### 1.2.2 Use the -i and the -s flag of lsof to generate a listing that is equivalent to the one generated with netstat previously and include it in your lab notebook



```
shbhat@shbhat-VirtualBox:~$ sudo lsof | wc -l
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs
          Output information may be incomplete.
28142
shbhat@shbhat-VirtualBox:~$ sudo lsof -i -s | wc -l
11
shbhat@shbhat-VirtualBox:~$ sudo lsof -i -s
COMMAND PID   USER   FD   TYPE DEVICE SIZE NODE NAME
CupsAndP  520   root    1u  IPv4  19361      UDP localhost:domain
systemd-resolve  12u  IPv4  19361      UDP localhost:domain (LISTEN)
systemd-resolve  13u  IPv4  19362      TCP localhost:domain (LISTEN)
avahi-dae  574   avahi   12u  IPv4  24166      UDP *:mdns
avahi-dae  574   avahi   13u  IPv4  24167      UDP *:5353
avahi-dae  574   avahi   14u  IPv4  24168      UDP *:41232
avahi-dae  574   avahi   15u  IPv6  24169      UDP *:50769
NetworkM  581   root    23u  IPv4  25467      UDP shbhat-VirtualBox:bootpc->_gateway:bootps
cups-brow  666   root    7u  IPv4  25629      UDP *:631
CupsAndP  694   root    6u  IPv6  52359      TCP [::1]:631 (LISTEN)
cupsd    694   root    7u  IPv4  52296      TCP localhost:631 (LISTEN)
shbhat@shbhat-VirtualBox:~$
```

1.3 nc

1.3.1 Include for your lab notebook, the version of ssh that is being used. (Type Ctrl+c to exit)

**Answer:**

Port 22 is being used.

SSh version - SSH-2.0-OpenSSH\_8.9p1 is found.

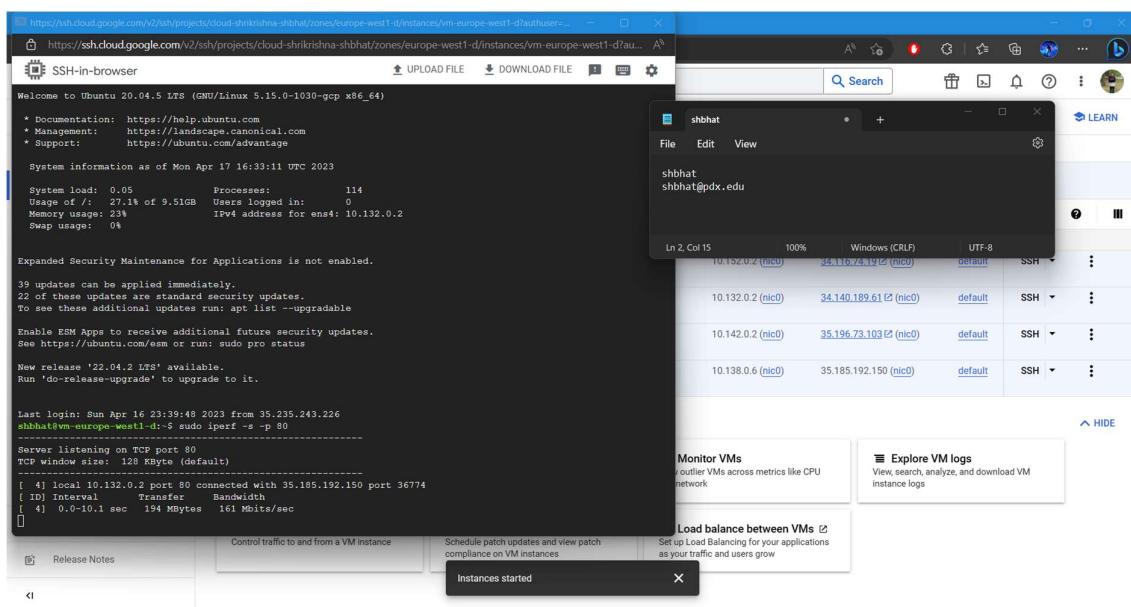
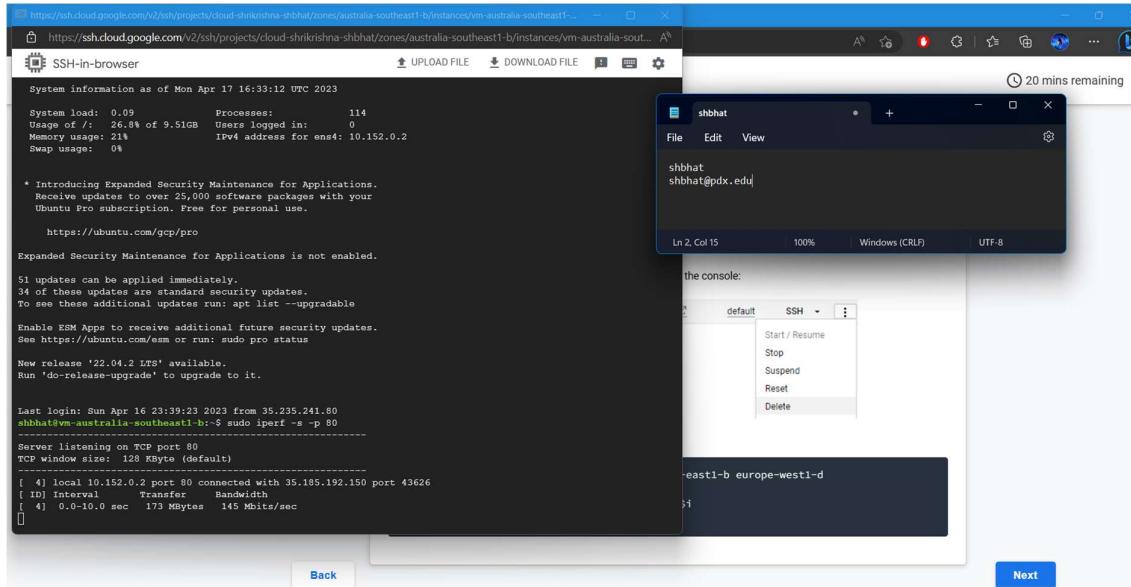
## TCP #2

### 2.1 iperf

#### 2.1.1 – Install iperf in all cloud instances.

Answer: Installed and checked it.

2.1.2 Show a screenshot of the measured bandwidth available between your us-west1-b VM and each of the other Compute Engine VMs. Explain the relative differences (or lack thereof) in your results.



```

https://ssh.cloud.google.com/v2/ssh/projects/cloud-shrkrishna-shbhat/zones/us-east1-b/instances/vm-us-east1-b?authuser=1&... A
https://ssh.cloud.google.com/v2/ssh/projects/cloud-shrkrishna-shbhat/zones/us-east1-b/instances/vm-us-east1-b?authuser=1&...
SSH-in-browser UPLOAD FILE DOWNLOAD FILE
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
System information as of Mon Apr 17 16:33:08 UTC 2023
System load: 0.09 Processes: 116
Usage of /: 26.8% of 9.51GB Users logged in: 0
Memory usage: 21% IPv4 address for ens4: 10.142.0.2
Swap usage: 0%
Expanded Security Maintenance for Applications is not enabled.
51 updates can be applied immediately.
34 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status
New release '22.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sun Apr 16 23:39:30 2023 from 35.235.240.64
shbhat@vm-us-east1-b:~$ sudo iperf -s -p 80
-----
Server listening on TCP port 80
TCP window size: 128 KByte (default)
[ 4] local 10.142.0.2 port 80 connected with 35.185.192.150 port 54118
[ 5] local 10.142.0.2 port 80 connected with 179.43.177.243 port 49866 (peer 14384.3338.21875-rc)
[ ID] Interval Transfer Bandwidth
[ 4] 0.0-10.0 sec 407 MBytes 341 Mbits/sec
[ 5] 0.0-10.0 sec 67.0 Bytes 53.6 bits/sec
[ ] 
shbhat@vm-us-east1-b:~$ 

Control traffic to and from a VM instance
Schedule patch updates and view patch compliance on VM instances
Instances started X

```

```

https://ssh.cloud.google.com/v2/ssh/projects/cloud-shrkrishna-shbhat/zones/us-west1-b/instances/vm-us-west1-b?authuser=1... A
https://ssh.cloud.google.com/v2/ssh/projects/cloud-shrkrishna-shbhat/zones/us-west1-b/instances/vm-us-west1-b?authuser=1...
SSH-in-browser UPLOAD FILE DOWNLOAD FILE
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
System information as of Mon Apr 17 16:33:44.1
shbhat@vm-us-west1-b:~$ sudo iperf -c 34.116.74.19 -p 80
-----
Client connecting to 34.116.74.19, TCP port 80
TCP window size: 85.0 KByte (default)
[ 3] local 10.138.0.6 port 43624 connected with 34.116.74.19 port 80
[ ID] Interval Transfer Bandwidth
[ 3] 0.0-10.0 sec 173 MBytes 145 Mbits/sec
shbhat@vm-us-west1-b:~$ sudo iperf -c 34.140.189.61 -p 80
-----
Client connecting to 34.140.189.61, TCP port 80
TCP window size: 85.0 KByte (default)
[ 3] local 10.138.0.6 port 36774 connected with 34.140.189.61 port 80
[ ID] Interval Transfer Bandwidth
[ 3] 0.0-10.1 sec 194 MBytes 161 Mbits/sec
shbhat@vm-us-west1-b:~$ sudo iperf -c 35.196.73.103 -p 80
-----
Client connecting to 35.196.73.103, TCP port 80
TCP window size: 85.0 KByte (default)
[ 3] local 10.138.0.6 port 54118 connected with 35.196.73.103 port 80
[ ID] Interval Transfer Bandwidth
[ 3] 0.0-10.0 sec 407 MBytes 341 Mbits/sec
shbhat@vm-us-west1-b:~$ 

Control traffic to and from a VM instance
Schedule patch updates and view patch compliance on VM instances
Instances started X

```

Why relative differences?

Answer:

There are various causes for differences in bandwidth, it might be due to distance since it might have to fetch from nearby server or distant server. It might also be due to congestion of packets. It might also be due to the quality of the network connection. Networks with higher latency or packet loss rates can result in reduced bandwidth or less consistent bandwidth measurements. It might also be due to not choosing the optimal routing path which can cause more traffic and there might be reduced bandwidth.

## HTTP # 3

### 3.1 HTTP developer tools Part 1

#### 3.1.1 What is the URL being requested?

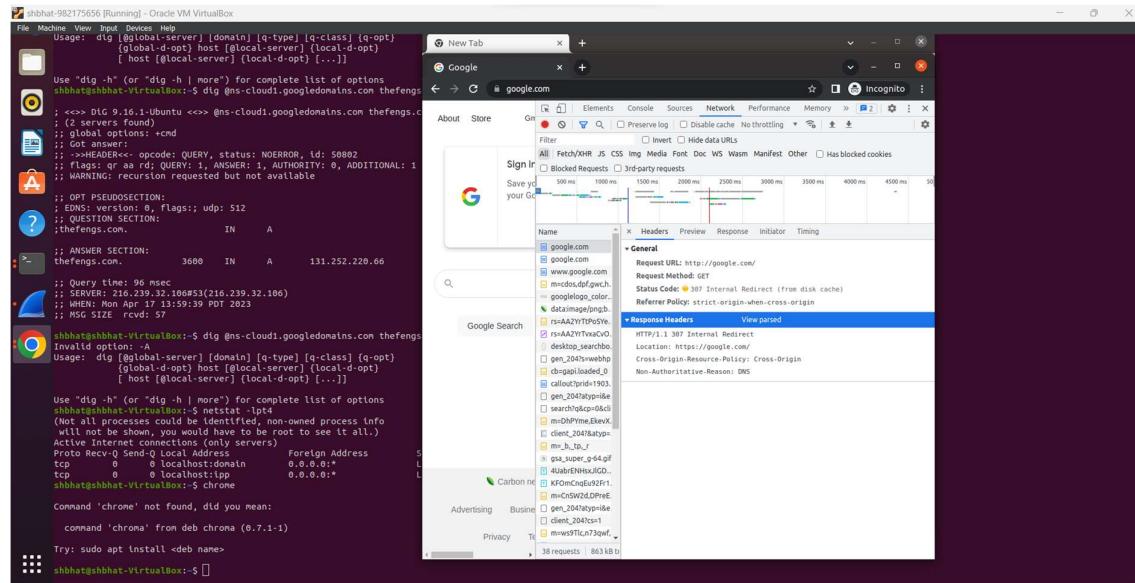
Answer: URL being requested is: <http://google.com/>

#### 3.1.2 What is the HTTP status code in the response and what does it mean?

Answer: Status code 307 Internal Redirect

#### 3.1.3 Look up the status code. Show the associated HTTP response header that is sent in conjunction with this status code for the request.

Answer:



### 3.2 HTTP developer tools Part 2

#### 3.2.1 What is the URL being requested? Is it using HTTP or HTTPS?

Answer: HTTPS

#### 3.2.2 What are the Host: (HTTP 1.1) or: authority: (HTTP 2.0) headers sent by the browser? What is the User-Agent: HTTP header that is sent?

Answer: User agent is mozilla/5.0

Authority: google.com

```

shbhat@shbhat-VirtualBox:~$ dig ns-cloud1.googledomains.com thefengs
...
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 512
; QUESTION SECTION:
;thefengs.com. IN A
...
; ANSWER SECTION:
thefengs.com. 3600 IN A 131.252.220.66
...
shbhat@shbhat-VirtualBox:~$ dig ns-cloud1.googledomains.com thefengs
Invalid option: -A
Usage: dig [[@global-server] | [domain] [q-type] [q-class] [q-opt]
          {[@global-d-opt] host [@local-server] [local-d-opt]
          [ host [@local-server] [local-d-opt] [...]]}
...
shbhat@shbhat-VirtualBox:~$ netstat -lpt4
(Not all processes could be identified, non-owned process info
will not be shown, you may need root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp      0      0 localhost:domain          0.0.0.0:*
tcp      0      0 localhost:tcp            0.0.0.0:*
...
shbhat@shbhat-VirtualBox:~$ chrome
Command 'chrome' not found, did you mean:
  command 'chroma' from deb chroma (0.7.1-1)
Try: sudo apt install <deb name>
shbhat@shbhat-VirtualBox:~$ 

```

The Network tab in the developer tools shows a request to `google.com`. Headers include:

- `Host: google.com`
- `Accept: */*`
- `Accept-Encoding: gzip, deflate, br`
- `Accept-Language: en-US,en;q=0.9`
- `Sec-CH-UA: "Chromium";v="112", "Google Chrome";v="112", "Not:A-Brand";v="99"`
- `Sec-CH-UA-Arch: "x86"`
- `Sec-CH-UA-Bitwidth: "64"`
- `Sec-CH-UA-Full-Version-List: "Chromium";v="112.0.5615.49", "Google Chrome";v="112.0.5615.49", "Not:A-Brand";v="99.0.0.0"`
- `Sec-CH-UA-Mobile: "0"`
- `Sec-CH-UA-Model: "`
- `Sec-CH-UA-Platform: "Linux"`
- `Sec-CH-UA-Platform-Version: "5.15.0"`
- `Sec-CH-UA-Wow64: 70`

```

shbhat@shbhat-VirtualBox:~$ dig ns-cloud1.googledomains.com thefengs
...
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 512
; QUESTION SECTION:
;thefengs.com. IN A
...
; ANSWER SECTION:
thefengs.com. 3600 IN A 131.252.220.66
...
shbhat@shbhat-VirtualBox:~$ dig ns-cloud1.googledomains.com thefengs
Invalid option: -A
Usage: dig [[@global-server] | [domain] [q-type] [q-class] [q-opt]
          {[@global-d-opt] host [@local-server] [local-d-opt]
          [ host [@local-server] [local-d-opt] [...]]}
...
shbhat@shbhat-VirtualBox:~$ netstat -lpt4
(Not all processes could be identified, non-owned process info
will not be shown, you may need root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp      0      0 localhost:domain          0.0.0.0:*
tcp      0      0 localhost:tcp            0.0.0.0:*
...
shbhat@shbhat-VirtualBox:~$ chrome
Command 'chrome' not found, did you mean:
  command 'chroma' from deb chroma (0.7.1-1)
Try: sudo apt install <deb name>
shbhat@shbhat-VirtualBox:~$ 

```

The Network tab in the developer tools shows a request to `google.com`. Headers include:

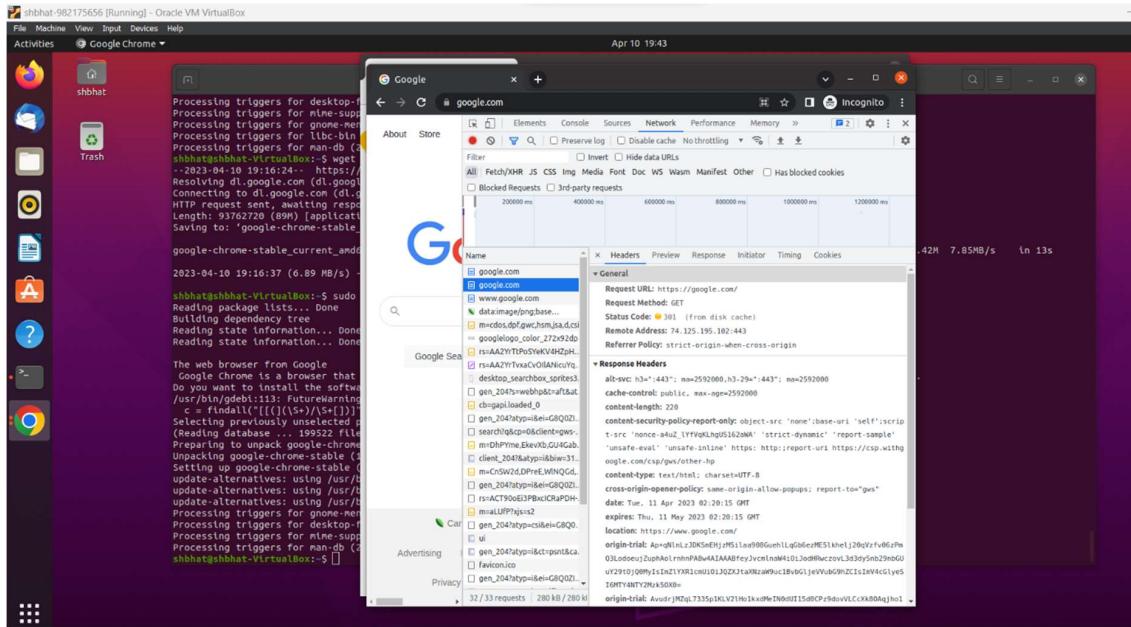
- `Host: google.com`
- `Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8`
- `Accept-Encoding: gzip, deflate, br`
- `Accept-Language: en-US,en;q=0.9`
- `Sec-CH-UA: "Chromium";v="112", "Google Chrome";v="112", "Not:A-Brand";v="99"`
- `Sec-CH-UA-Arch: "x86"`
- `Sec-CH-UA-Bitwidth: "64"`
- `Sec-CH-UA-Full-Version-List: "Chromium";v="112.0.5615.49", "Google Chrome";v="112.0.5615.49", "Not:A-Brand";v="99.0.0.0"`
- `Sec-CH-UA-Mobile: "0"`
- `Sec-CH-UA-Model: "`
- `Sec-CH-UA-Platform: "Linux"`
- `Sec-CH-UA-Platform-Version: "5.15.0"`
- `Sec-CH-UA-Wow64: 70`

3.2.3 What is the HTTP status code in the response and what does it mean? Is it different from the first status code? If so, what is the semantic difference?

Answer: 301, it is different from first status code.

301 redirect is a permanent redirect, while a 307 redirect is a temporary redirect. If you are permanently moving a page to a new location, use a 301 redirect. If you are temporarily moving a page to a new location, use a 307 redirect.

3.2.4 Show the associated HTTP response header that is sent in conjunction with this status code for the request.



### 3.3 HTTP developer tools Part 3

#### 3.3.1 What is the URL being requested? Is it using HTTP or HTTPS?

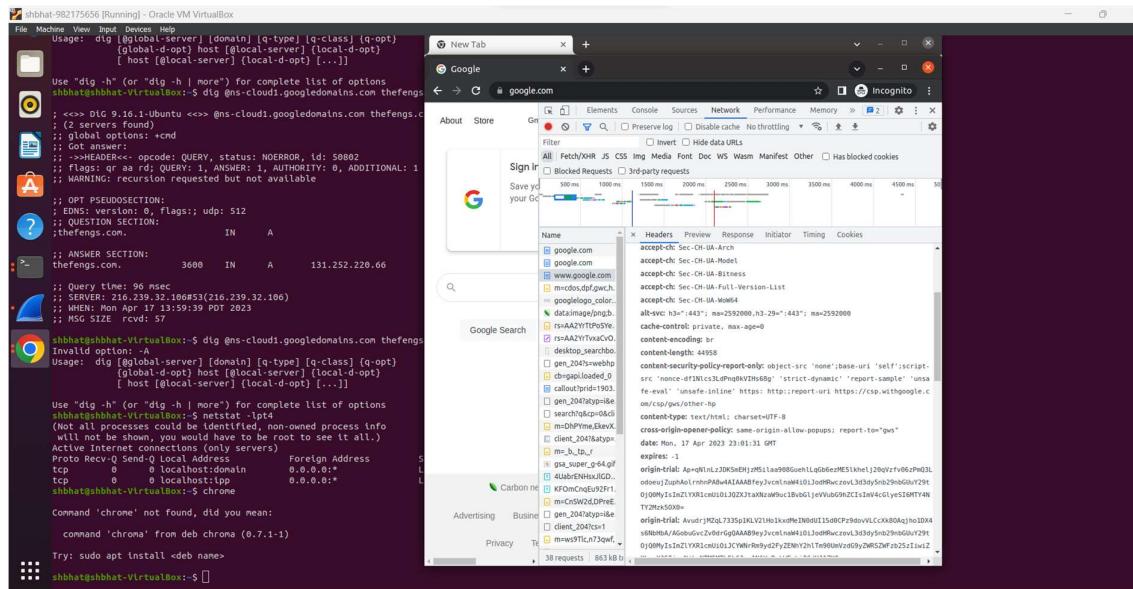
Answer: <https://google.com>, it is using HTTPS.

#### 3.3.2 What is the HTTP status code in the response?

Answer: Status code 200

#### 3.3.3 Look for an alt-svc: HTTP response header. Does the server believe the client can use HTTP3/QUIC?

Answer: On looking at the alt-svc, we can see that server believes that client can use HTTP3 since we can see the value h3 there.



3.3.4 Examine the HTTP response headers for cookies. Show the cookies that are set and which ones specify that no SameSite restrictions are in place. What does the setting indicate about the cookies that are set?

Answer:

On examining the cookies we can see that there are two values ‘lax’ and ‘none’.

Lax - Means that the cookie is not sent on cross-site requests, such as on requests to load images or frames, but is sent when a user is navigating to the origin site from an external site (for example, when following a link). This is the default behaviour if the SameSite attribute is not specified.

None - means that the browser sends the cookie with both cross-site and same-site requests. The Secure attribute must also be set when setting this value, like so SameSite=None; Secure. If Secure is missing an error will be logged.

Source : [Set-Cookie - HTTP | MDN \(mozilla.org\)](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie)

```
shbhat@shbhat-VirtualBox:~$ dig -h
File Machine View Input Devices Help
Usage: dig [-g[lobal]-server] [domain] [-q[type]] [-c[lass]] [-q[opt]]
          [-g[lobal-d-opt]] host [-l[ocal]-server] [-l[ocal-d-opt]] [...]
          [-h[ost] [-l[ocal]-server] [-l[ocal-d-opt]] [...]]]

Use "dig -h" (or "dig -h | more") for complete list of options
shbhat@shbhat-VirtualBox:~$ dig @ns-cloud1.googledomains.com thefengs.C
; <>> DUC 16.1.16.1-Ubuntu <>> @ns-cloud1.googledomains.com thefengs.C
; (2 servers found)
; global options: +cmd
; Got answer:
;挺好的
;   query: thefengs.C type: QUERY, status: NOERROR, id: 50882
;   flags: qr aa rdcl rdv; r: 1, ANSWER: 1, AUTHORITY: 1
;   WARNING: recursion requested but not available

; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: ud; udp: 512
; QUESTION SECTION:
; ;thefengs.C.
; ; ANSWER SECTION:
thefengs.C. 3600 IN A 131.252.220.66
; Query time: 96 msec
; SERVER: 216.239.32.106#53 (216.239.32.106)
; WHEN: Mon Apr 17 13:59:39 PDT 2023
; MSG SIZE rcvd: 57

shbhat@shbhat-VirtualBox:~$ dig @ns-cloud1.googledomains.com thefengs.C
; <>> DUC 16.1.16.1-Ubuntu <>> @ns-cloud1.googledomains.com thefengs.C
; global option: +A
Usage: dig [-g[lobal]-server] [domain] [-q[type]] [-c[lass]] [-q[opt]]
          [-g[lobal-d-opt]] host [-l[ocal]-server] [-l[ocal-d-opt]] [...]
          [-h[ost] [-l[ocal]-server] [-l[ocal-d-opt]] [...]]]

Use "dig -h" (or "dig -h | more") for complete list of options
shbhat@shbhat-VirtualBox:~$ netstat -lptd
(Not all processes could be identified, non-owned process info
will not be shown, you would have to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address
tcp      0      0  localhost:domain        0.0.0.0:*
tcp      0      0  localhost:ipp          0.0.0.0:*
```

### 3.4 Asynchronous HTTP requests

3.4.1 Show the requests and responses in the listing. Click on the last request sent, then click on the response to see that its payload has returned the data that is then rendered on the search page similar to what is shown below for “rabbid”.

```
shbhatashbhat@VirtualBox:~$ dig +dns+cloud1.googledomains.com thefengs.C
;; global options: +cmd
;; Got answer:
;; ->>>HEADER<-- opcode: QUERY, status: NOERROR, id: 50802
;; flags: qr aa rdq; r: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
;; EDNS version: 0, flags: udp: 512
;; SECTION: ANSWER
;; ;thefengs.com.
;; ANSWER SECTION:
thefengs.com. 3600 IN A 131.252.220.66

;; Query time: 96 msec
;; SERVER: 216.239.32.106#53 (216.239.32.106)
;; WHEN: Mon Apr 17 13:59:39 PDT 2023
;; MSG SIZE rcvd: 57

shbhatashbhat@VirtualBox:~$ dig +dns+cloud1.googledomains.com thefengs.C
;; global options: +cmd
;; Got answer:
;; ->>>HEADER<-- opcode: QUERY, status: NOERROR, id: 50802
;; flags: qr aa rdq; r: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
;; EDNS version: 0, flags: udp: 512
;; SECTION: ANSWER
;; ;thefengs.com.
;; ANSWER SECTION:
thefengs.com. 3600 IN A 131.252.220.66

;; Query time: 96 msec
;; SERVER: 216.239.32.106#53 (216.239.32.106)
;; WHEN: Mon Apr 17 13:59:39 PDT 2023
;; MSG SIZE rcvd: 57

shbhatashbhat@VirtualBox:~$ chrome
Optimal invalid.
Usage: dig +global-server| [domain] [+type] [+class] [+opt]
      host [+local-server] [local-dopt]
      [+host [+local-server] [local-dopt] [...]]

Use "dig +h | more" for complete list of options
shbhatashbhat@VirtualBox:~$ netstat -lptd
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:8080             0.0.0.0:*               LISTEN
shbhatashbhat@VirtualBox:~$ chrome

Command 'chrome' not found, did you mean:
  command 'chrome' from deb chrome (0.7.1-1)

Try: sudo apt install deb-name

shbhatashbhat@VirtualBox:~$ 
```

```
phbhhat:987176565$ (Running) - Oracle VM VirtualBox
File Machine View Input Devices Help
Usage: dig [global-server] [domain] [q-type] [q-class] [q-opt]
       [global-d-opt] host [local-server] [local-d-opt]
       [host @local-server] [local-d-opt] [...]

Use "dig -H" or "(dig -H | more)" for complete list of options
shbhhat@shbhhat-VirtualBox:~$ dig ns-cloud.googledomains.com thefengs.co

; <>> DIG V9.16.1-ubuntu <>> @ns-cloud.googledomains.com thefengs.co
;; (2 servers found)
;; global options: +cmd
;; Got answer:
;;挺好的
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: udp: 512
;; QUESTION SECTION:
;thefengs.co. IN A

;; ANSWER SECTION:
thefengs.co. 3600 IN A 131.252.220.66

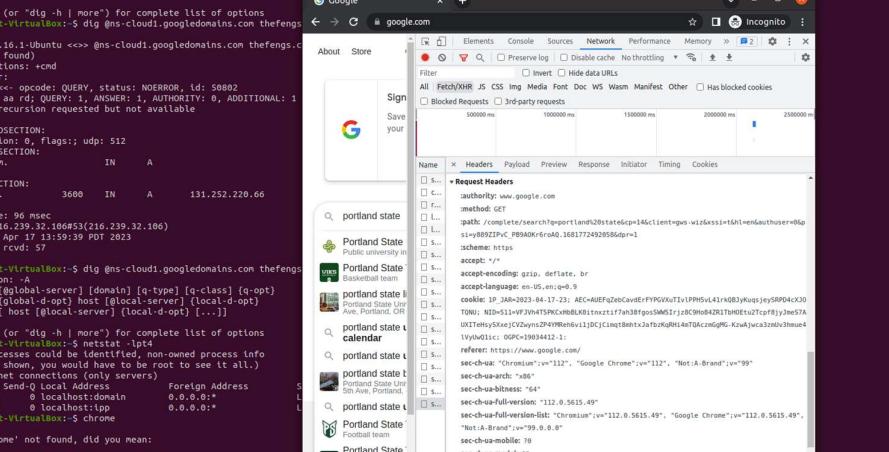
;; Query time: 96 msec
;; SERVER: 216.239.32.106#53 (216.239.32.106)
;; WHEN: Mon Apr 17 13:59:39 PDT 2023
;; MSG SIZE rcvd: 104

shbhhat@shbhhat-VirtualBox:~$ dig ns-cloud.googledomains.com thefengs.co
Invalid option: -A
Usage: dig [global-server] [domain] [q-type] [q-class] [q-opt]
       [global-d-opt] host [local-server] [local-d-opt]
       [host @local-server] [local-d-opt] [...]

Use "dig -H" or "(dig -H | more)" for complete list of options
shbhhat@shbhhat-VirtualBox:~$ dig -A ns-cloud.googledomains.com thefengs.co
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
proto Recv-Q Send-Q Foreign Address          Local Address        PID/Program name
tcp        0      0 localhost:domain          0.0.0.0:          0
tcp        0      0 localhost:ipp            0.0.0.0:          0
shbhhat@shbhhat-VirtualBox:~$ chrome

Command 'chrome' not found, did you mean:
  command 'chroma' from deb chroma (8.7.1-1)

Try: sudo apt install <deb name>
shbhhat@shbhhat-VirtualBox:~$ 
```



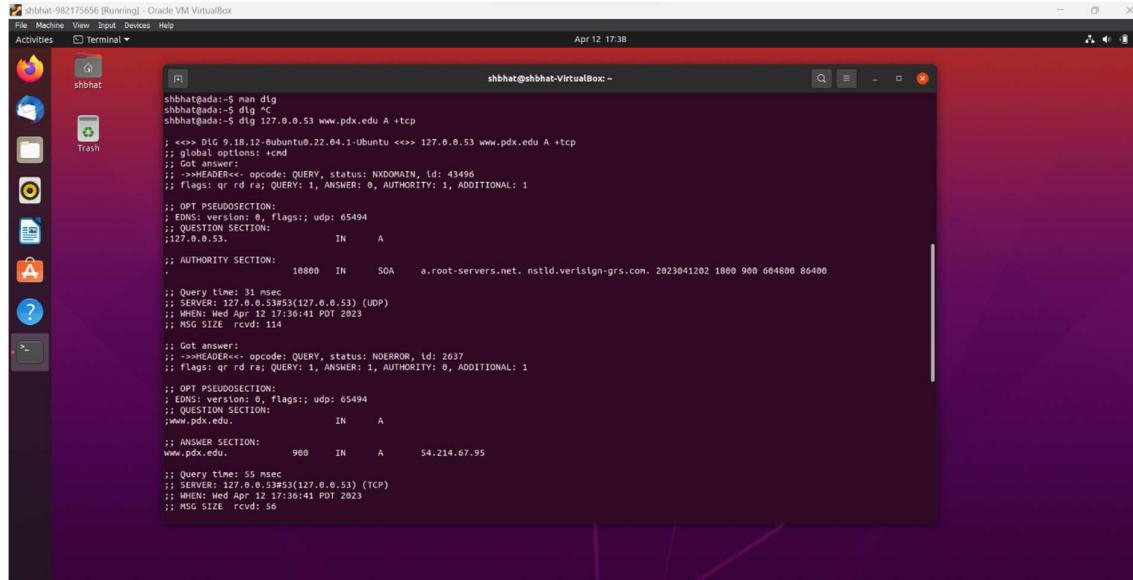
A screenshot of a Linux desktop environment (Ubuntu) running in Oracle VM VirtualBox. The desktop has a purple theme with icons for file manager, terminal, and system tools. A terminal window on the left shows the process of installing Google Chrome from source. A browser window in the center shows the Google homepage. To the right, the developer tools (Elements, Console, Sources, Network, etc.) are open, with the Network tab showing network traffic for the Google search results page.

## Section 2

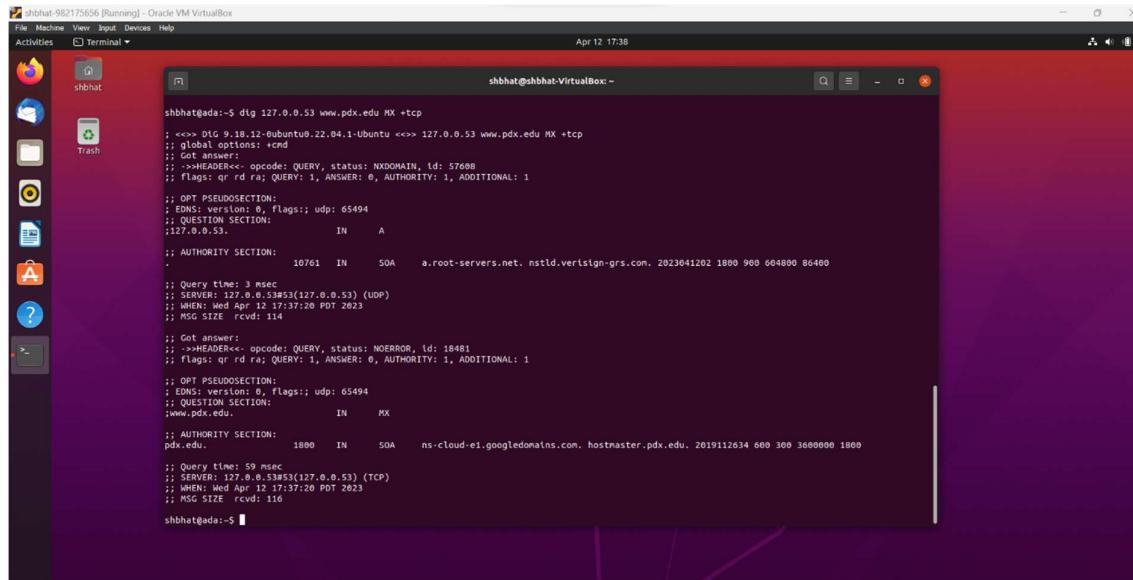
### DNS #1

#### 1.1 dig

1.1.1 Use dig to query the PSU's local DNS server at 131.252.208.53 for the A record of www.pdx.edu using TCP. Then, use dig to do the same for the MX record of pdx.edu. What do the ANSWER sections explain about where PSU's web/mail services are run from?



```
shbhat@ada:~$ man dig
shbhat@ada:~$ dig
shbhat@ada:~$ dig 127.0.0.53 www.pdx.edu A +tcp
; <>> DLG 9.18.12-0ubuntu22.04.1-Ubuntu <>> 127.0.0.53 www.pdx.edu A +tcp
; global options: +cd
; Got answer:
; >>>HEADER<< opcode: QUERY, status: NXDOMAIN, id: 43496
; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 65494
; QUESTION SECTION:
;www.pdx.edu.           IN      A
;
; AUTHORITY SECTION:
;ns.          10800   IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2023041202 1800 900 664800 86400
;
; Got answer:
; >>>HEADER<< opcode: QUERY, status: NOERROR, id: 2637
; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 65494
; QUESTION SECTION:
;www.pdx.edu.           IN      A
;
; ANSWER SECTION:
;www.pdx.edu.         900    IN      A       54.214.67.95
;
; Query time: 55 msec
; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
; WHEN: Wed Apr 12 17:36:41 PDT 2023
; MSG SIZE rcvd: 56
```



```
shbhat@ada:~$ dig 127.0.0.53 www.pdx.edu MX +tcp
; <>> DLG 9.18.12-0ubuntu22.04.1-Ubuntu <>> 127.0.0.53 www.pdx.edu MX +tcp
; global options: +cd
; Got answer:
; >>>HEADER<< opcode: QUERY, status: NXDOMAIN, id: 57608
; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 65494
; QUESTION SECTION:
;www.pdx.edu.           IN      MX
;
; AUTHORITY SECTION:
;ns.          10761   IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2023041202 1800 900 664800 86400
;
; Got answer:
; >>>HEADER<< opcode: QUERY, status: NOERROR, id: 18481
; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 65494
; QUESTION SECTION:
;www.pdx.edu.           IN      MX
;
; AUTHORITY SECTION:
;pdx.edu.            1800    IN      SOA     ns-cloud-e1.googledomains.com. hostmaster.pdx.edu. 2019112634 600 300 3600000 1800
;
; Query time: 55 msec
; SERVER: 127.0.0.53#53(127.0.0.53) (TCP)
; WHEN: Wed Apr 12 17:37:20 PDT 2023
; MSG SIZE rcvd: 116
shbhat@ada:~$
```

The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "shbhat@shbhat-VirtualBox: ~". The content of the terminal shows the output of a DNS query, specifically a recursive query for the domain pdx.edu. The output includes the following details:

- QUESTION SECTION:** pdx.edu. IN A
- ANSWER SECTION:**
  - pdx.edu. 178 IN HX 1 aspmx.l.google.com.
  - pdx.edu. 178 IN HX 5 alt2.aspmx.l.google.com.
  - pdx.edu. 178 IN HX 5 alt1.aspmx.l.google.com.
  - pdx.edu. 178 IN HX 10 alt4.aspmx.l.google.com.
  - pdx.edu. 178 IN HX 10 alt3.aspmx.l.google.com.
- OPT PSEUDOSECTION:**
  - aspx.l.google.com. 178 IN A 74.125.195.27
  - aspx.l.google.com. 178 IN AAAA 2607:f8b0:400e:c02::1a
- Query time:** 3 msec
- SERVER:** 127.0.0.53#53 (127.0.0.53) (UDP)
- WHEN:** Wed Apr 12 17:40:38 PDT 2023
- MSG SIZE rcvd:** 114

The ANSWER section of the first query should provide an IP address, which is where the web server for www.pdx.edu is hosted. The ANSWER section of the second query should provide one or more mail server names, along with their priority values, which are used for handling email traffic for pdx.edu.

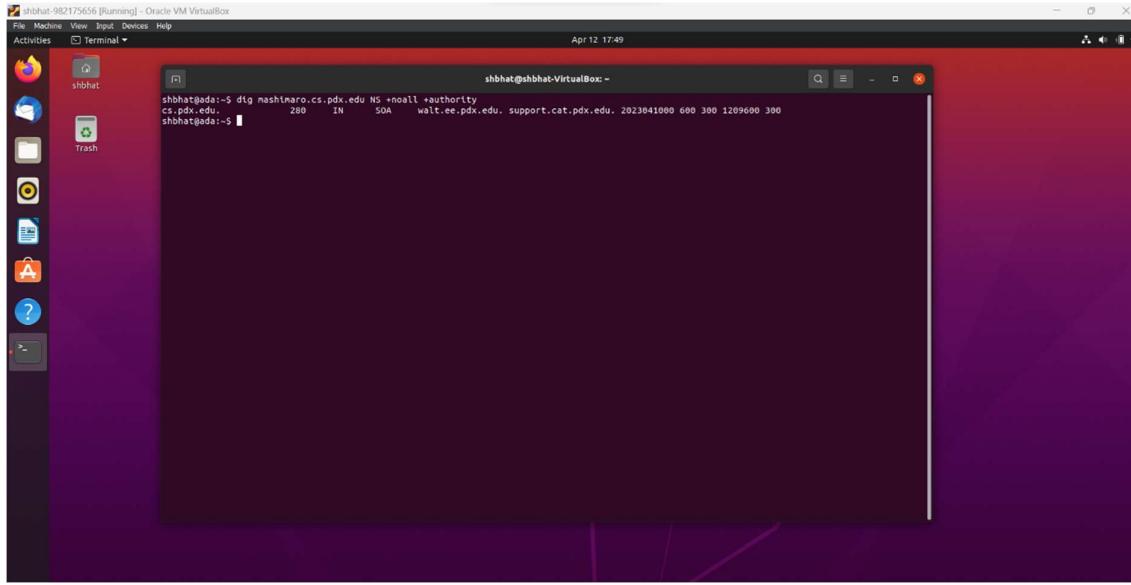
#### 54.214.67.95 – Web services are hosted

**;; ANSWER SECTION:**

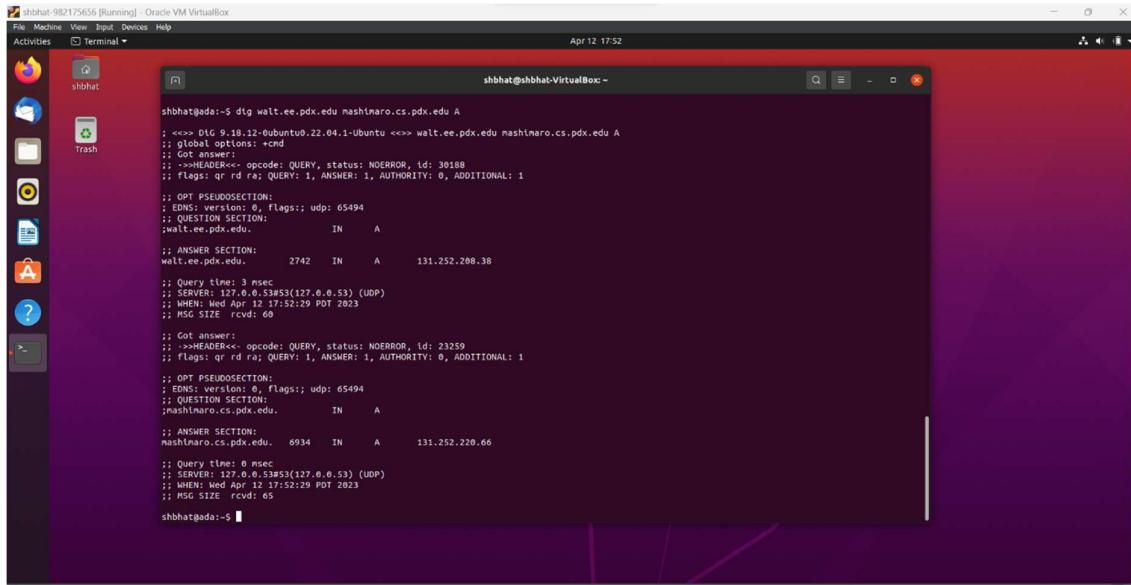
|          |     |    |    |                             |
|----------|-----|----|----|-----------------------------|
| pdx.edu. | 178 | IN | MX | 1 aspmx.l.google.com.       |
| pdx.edu. | 178 | IN | MX | 5 alt2.aspmx.l.google.com.  |
| pdx.edu. | 178 | IN | MX | 5 alt1.aspmx.l.google.com.  |
| pdx.edu. | 178 | IN | MX | 10 alt4.aspmx.l.google.com. |
| pdx.edu. | 178 | IN | MX | 10 alt3.aspmx.l.google.com. |

Mail services are hosted

1.1.2 Find the authoritative server (NS record type, AUTHORITY section response) for mashimaro.cs.pdx.edu and then query that server for the A record of mashimaro.cs.pdx.edu. Show both.

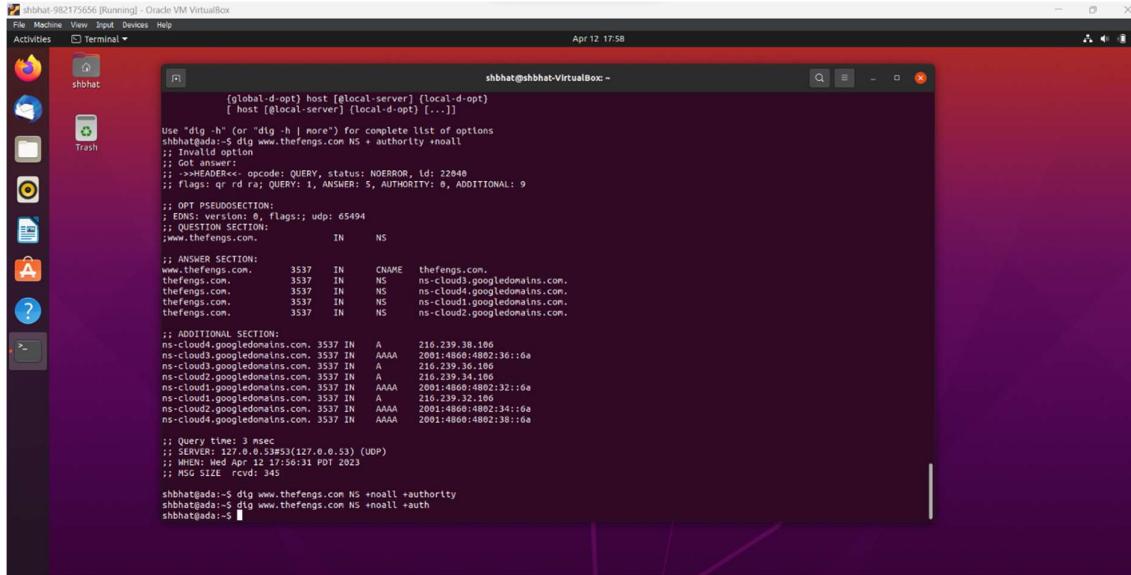


```
shbhat@shbhat-VirtualBox:~$ dig mashimaro.cs.pdx.edu NS +noall +authority
; <>> OIG 9.18.12-ubuntu0.22.04.1-Ubuntu <>> walt.ee.pdx.edu mashimaro.cs.pdx.edu A
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 30188
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 65494
; QUESTION SECTION:
;mashimaro.cs.pdx.edu.           IN      A
;
;; ANSWER SECTION:
walt.ee.pdx.edu.    2742   IN      A      131.252.208.38
;
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 23259
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 65494
; QUESTION SECTION:
;mashimaro.cs.pdx.edu.           IN      A
;
;; ANSWER SECTION:
mashimaro.cs.pdx.edu. 6934   IN      A      131.252.220.66
;
;; Query time: 3 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Apr 12 17:52:29 PDT 2023
;; MSG SIZE rcvd: 63
```

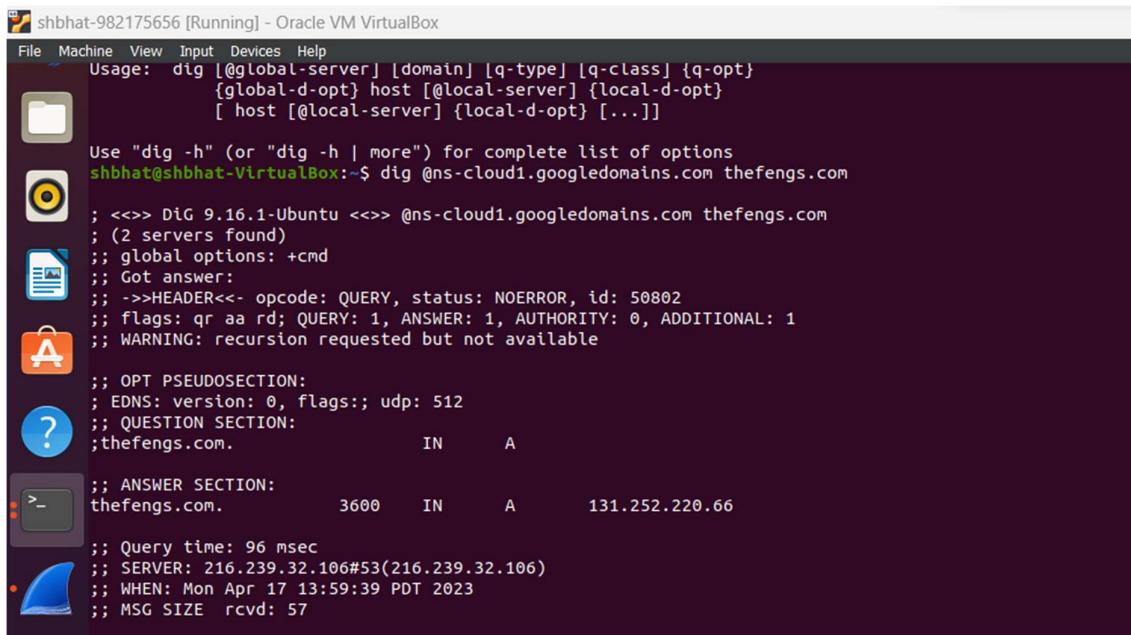


```
shbhat@shbhat-VirtualBox:~$ dig walt.ee.pdx.edu mashimaro.cs.pdx.edu A
; <>> OIG 9.18.12-ubuntu0.22.04.1-Ubuntu <>> walt.ee.pdx.edu mashimaro.cs.pdx.edu A
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 30188
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 65494
; QUESTION SECTION:
;mashimaro.cs.pdx.edu.           IN      A
;
;; ANSWER SECTION:
walt.ee.pdx.edu.    2742   IN      A      131.252.208.38
;
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 23259
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 65494
; QUESTION SECTION:
;mashimaro.cs.pdx.edu.           IN      A
;
;; ANSWER SECTION:
mashimaro.cs.pdx.edu. 6934   IN      A      131.252.220.66
;
;; Query time: 3 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Apr 12 17:52:29 PDT 2023
;; MSG SIZE rcvd: 63
```

### 1.1.3 Find the authoritative server for thefengs.com and then query that server for the A record of thefengs.com.



```
shbhat@shbhat-VirtualBox:~$ dig www.thefengs.com NS +authority +nall
; <>> DiG 9.16.1-Ubuntu <>> @ns-cloud1.googledomains.com thefengs.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22040
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 0
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.thefengs.com.      IN      NS
;; ANSWER SECTION:
www.thefengs.com.  3537    IN      CNAME   thefengs.com.
thefengs.com.        3537    IN      NS      ns-cloud3.googledomains.com.
thefengs.com.        3537    IN      NS      ns-cloud1.googledomains.com.
thefengs.com.        3537    IN      NS      ns-cloud1.googledomains.com.
thefengs.com.        3537    IN      NS      ns-cloud2.googledomains.com.
ns-cloud3.googledomains.com. 3537 IN  A 216.239.38.106
ns-cloud3.googledomains.com. 3537 IN  AAAA 2001:4800:4802:36::6a
ns-cloud3.googledomains.com. 3537 IN  A 216.239.36.106
ns-cloud3.googledomains.com. 3537 IN  AAAA 2001:4800:4802:36::6a
ns-cloud1.googledomains.com. 3537 IN  A 216.239.32.106
ns-cloud1.googledomains.com. 3537 IN  AAAA 2001:4800:4802:32::6a
ns-cloud2.googledomains.com. 3537 IN  A 216.239.32.106
ns-cloud2.googledomains.com. 3537 IN  AAAA 2001:4800:4802:34::6a
ns-cloud1.googledomains.com. 3537 IN  AAAA 2001:4800:4802:38::6a
;; ADDITIONAL SECTION:
ns-cloud1.googledomains.com. 3537 IN  A 216.239.38.106
ns-cloud1.googledomains.com. 3537 IN  AAAA 2001:4800:4802:36::6a
ns-cloud1.googledomains.com. 3537 IN  A 216.239.36.106
ns-cloud1.googledomains.com. 3537 IN  AAAA 2001:4800:4802:36::6a
ns-cloud2.googledomains.com. 3537 IN  A 216.239.32.106
ns-cloud2.googledomains.com. 3537 IN  AAAA 2001:4800:4802:32::6a
ns-cloud1.googledomains.com. 3537 IN  A 216.239.32.106
ns-cloud1.googledomains.com. 3537 IN  AAAA 2001:4800:4802:34::6a
ns-cloud2.googledomains.com. 3537 IN  A 216.239.32.106
ns-cloud2.googledomains.com. 3537 IN  AAAA 2001:4800:4802:38::6a
;; Query time: 3 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Apr 12 17:56:31 PDT 2023
;; MSG SIZE rcvd: 345
shbhat@shbhat:~$ dig www.thefengs.com NS +noall +authority
shbhat@shbhat:~$ dig www.thefengs.com NS +noall +auth
shbhat@shbhat:~$
```



```
shbhat@shbhat-982175656 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Usage: dig {@global-server} {domain} [{q-type}] [{q-class}] [{q-opt}]
{@global-d-opt} host {@local-server} {local-d-opt}
[ host {@local-server} {local-d-opt} [...]]]

Use "dig -h" (or "dig -h | more") for complete list of options
shbhat@shbhat-VirtualBox:~$ dig @ns-cloud1.googledomains.com thefengs.com
; <>> DiG 9.16.1-Ubuntu <>> @ns-cloud1.googledomains.com thefengs.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50802
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;thefengs.com.          IN      A

;; ANSWER SECTION:
thefengs.com.  3600    IN      A      131.252.220.66
;; Query time: 96 msec
;; SERVER: 216.239.32.106#53(216.239.32.106)
;; WHEN: Mon Apr 17 13:59:39 PDT 2023
;; MSG SIZE rcvd: 57
```

### 1.1.4 When a web request hits port 80 of 131.252.220.66, how does the server know which site to serve from? (i.e. what protocol header)

Answer:

When a web request hits port 80 of an IP address, the server relies on the HTTP protocol header to determine which site to serve from. The HTTP protocol header is a part of the HTTP request that a client sends to a server when making an HTTP request. This header

contains several fields, including the "Host" field, which specifies the domain name of the website being requested.

For example, if a client sends an HTTP request to 131.252.220.66 with the following header:

## GET / HTTP/1.1

Host: example.com

The server at 131.252.220.66 will check the "Host" field in the HTTP header to determine which site the request is intended for. In this case, the server will recognize that the request is intended for the "example.com" website and will serve the appropriate content.

If the "Host" field is missing or contains an unrecognized domain name, the server will typically serve a default website or return an error message.

## 1.2 DNS iterative lookup

1.2.1 Include the results of each query for your lab notebook.

```
shbhat@shbhat-VirtualBox:~$ dig @192.5.5.241 www.amazon.co.uk NS +norecurse +tcp A
;; Warning, extra type option
;: SERVER: 192.5.5.241#53(192.5.5.241) (TCP)
;: WHEN: Wed Apr 12 18:26:53 PDT 2023
;: MSG SIZE rcvd: 549
shbhat@shbhat:~$ dig @nsa.nic.uk www.amazon.co.uk NS +norecurse +tcp A
;; Warning, extra type option
;: SERVER: 192.5.5.22.04.1-Ubuntu <>> @192.5.5.241 www.amazon.co.uk NS +norecurse +tcp A
;: (1 server found)
;: global options: +cd
;: Got answer:
;: -->HEADER<-- opcode: QUERY, status: NOERROR, id: 27176
;: flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 8, ADDITIONAL: 17
;: OPT PSEUDOSECTION:
;: EDNS: version: 0, flags: udp: 65535
;: QUESTION SECTION:
;:www.amazon.co.uk.           IN      A
;: AUTHORITY SECTION:
uk.                           172800  IN      NS      nsa.nic.uk.
uk.                           172800  IN      NS      nsb.nic.uk.
uk.                           172800  IN      NS      nsc.nic.uk.
uk.                           172800  IN      NS      nsd.nic.uk.
uk.                           172800  IN      NS      dns1.nic.uk.
uk.                           172800  IN      NS      dns2.nic.uk.
uk.                           172800  IN      NS      dns3.nic.uk.
uk.                           172800  IN      NS      dns4.nic.uk.
;: ADDITIONAL SECTION:
nsa.nic.uk.                   172800  IN      A       156.154.100.3
nsa.nic.uk.                   172800  IN      AAAA     2610:a1:100:1::3
nsb.nic.uk.                   172800  IN      A       156.154.101.3
nsb.nic.uk.                   172800  IN      AAAA     2601:502:2ed9::3
nsc.nic.uk.                   172800  IN      A       156.154.102.3
nsc.nic.uk.                   172800  IN      AAAA     2610:a1:100:2::3
nsd.nic.uk.                   172800  IN      A       156.154.103.3
nsd.nic.uk.                   172800  IN      AAAA     2610:a1:1010:1::3
dns1.nic.uk.                  172800  IN      A       213.248.216.1
dns1.nic.uk.                  172800  IN      AAAA     2801:600:1001:1
dns2.nic.uk.                  172800  IN      A       103.49.86.1
dns2.nic.uk.                  172800  IN      AAAA     2491:f6b8:490::1
dns3.nic.uk.                  172800  IN      A       213.248.226.1
dns3.nic.uk.                  172800  IN      AAAA     2491:f6b8:490::1
shbhat@shbhat:~$
```

```
shbhat@shbhat-VirtualBox:~$ dig @nsa.nic.uk www.amazon.co.uk NS +norecurse +tcp A
;; Warning, extra type option
;: SERVER: 192.5.5.241#53(192.5.5.241) (TCP)
;: WHEN: Wed Apr 12 18:26:53 PDT 2023
;: MSG SIZE rcvd: 549
shbhat@shbhat:~$ dig @nsa.nic.uk www.amazon.co.uk NS +norecurse +tcp A
;; Query time: 3 msec
;; SERVER: 192.5.5.241#53(192.5.5.241) (TCP)
;; WHEN: Wed Apr 12 18:26:53 PDT 2023
;; MSG SIZE rcvd: 549
shbhat@shbhat:~$ dig @nsa.nic.uk www.amazon.co.uk NS +norecurse +tcp A
;; Warning, extra type option
;: SERVER: 192.5.5.22.04.1-Ubuntu <>> @nsa.nic.uk www.amazon.co.uk NS +norecurse +tcp A
;: (1 server found)
;: global options: +cd
;: Got answer:
;: -->HEADER<-- opcode: QUERY, status: NOERROR, id: 23452
;: flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 10, ADDITIONAL: 1
;: OPT PSEUDOSECTION:
;: EDNS: version: 0, flags: udp: 1232
;: COOKIE: 505984cfd106906064375ab269ea47d227565093 (good)
;: QUESTION SECTION:
;:www.amazon.co.uk.           IN      A
;: AUTHORITY SECTION:
amazon.co.uk.                  172800  IN      NS      ns1.p31.dynect.net.
amazon.co.uk.                  172800  IN      NS      pdns3.ultrads.info.
amazon.co.uk.                  172800  IN      NS      pdns3.ultrads.org.
amazon.co.uk.                  172800  IN      NS      pdns1.ultrads.net.
amazon.co.uk.                  172800  IN      NS      pdns4.ultrads.org.
amazon.co.uk.                  172800  IN      NS      ns1.p31.dynect.net.
amazon.co.uk.                  172800  IN      NS      ns4.p31.dynect.net.
amazon.co.uk.                  172800  IN      NS      pdns2.ultrads.net.
amazon.co.uk.                  172800  IN      NS      pdns0.ultrads.co.uk.
;: Query time: 19 msec
;; SERVER: 156.154.100.3#53(nsa.nic.uk) (TCP)
;; WHEN: Wed Apr 12 18:28:18 PDT 2023
;; MSG SIZE rcvd: 336
shbhat@shbhat:~$
```

```

shbhat@shbhat-VirtualBox: ~
dig @ns1.p31.dynect.net www.amazon.co.uk NS +noredirect +tcp A
; Query time: 19 msec
; SERVER: 156.154.106.3#53(ns1.p31.dynect.net) (TCP)
; WHEN: Wed Apr 12 18:28:18 PDT 2023
; MSG SIZE rcvd: 338
shbhat@ada:~$ dig @ns1.p31.dynect.net www.amazon.co.uk NS +noredirect +tcp A
; Warning, extra type option
; <>> DLG 9.18.12.0ubuntu0.22.04.1-Ubuntu <>> @ns1.p31.dynect.net www.amazon.co.uk NS +noredirect +tcp A
; (1 server found)
; global options: +cmd
; Got answer:
; flags: qr aa; opcode: QUERY, status: NOERROR, id: 19957
; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 1
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: ud; cookie: 2abed04ad3af5cisc96d9364375b068e1a44f0b27f6fd5 (good)
; QUESTION SECTION:
;www.amazon.co.uk. IN A
; ANSWER SECTION:
www.amazon.co.uk. 1800 IN CNAME tp.bfdc3ca1-frontier.amazon.co.uk.
; AUTHORITY SECTION:
bfdc3ca1-frontier.amazon.co.uk. 900 IN NS ns-248.awsdns-31.com.
bfdc3ca1-frontier.amazon.co.uk. 900 IN NS ns-1624.awsdns-11.co.uk.
bfdc3ca1-frontier.amazon.co.uk. 900 IN NS ns-1078.awsdns-06.org.
bfdc3ca1-frontier.amazon.co.uk. 900 IN NS ns-853.awsdns-42.net.

; Query time: 19 msec
; SERVER: 108.59.163.31#53(ns1.p31.dynect.net) (TCP)
; WHEN: Wed Apr 12 18:29:42 PDT 2023
; MSG SIZE rcvd: 261
shbhat@ada:~$
```

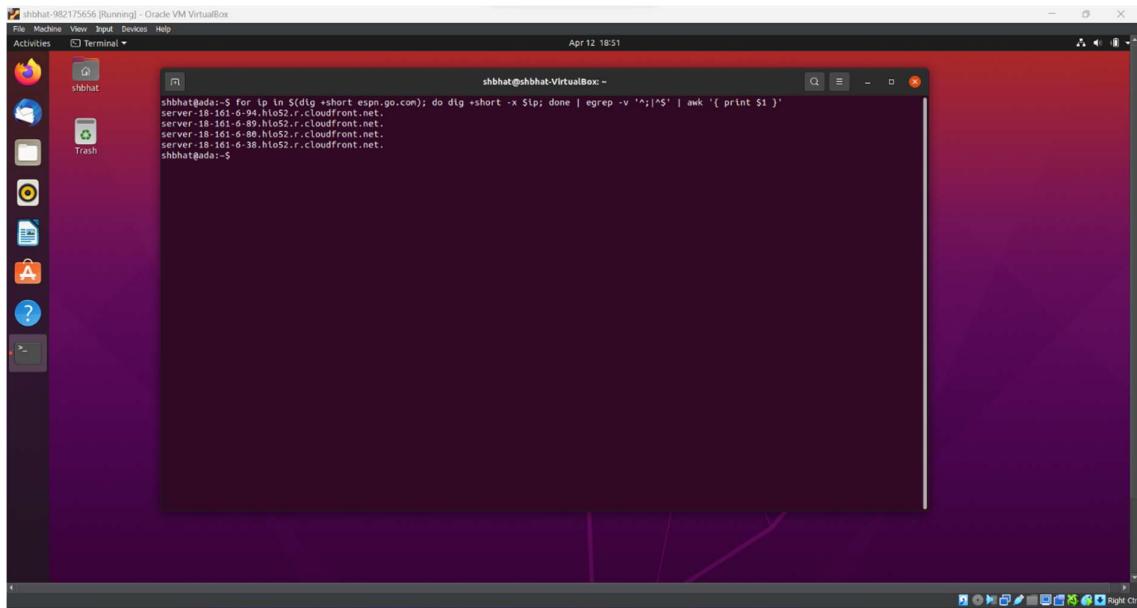
### 1.3 Reverse DNS Lookup

1.3.1 Use a single command line with commands dig, egrep, and awk, to list all IPv4 addresses that espn.go.com points to.

```

shbhat@shbhat-VirtualBox: ~
dig +short espn.go.com | egrep '^([0-9]+\.(0-9)+\.(0-9)+\.(0-9)+$' | awk '{ print $1 }'
18.161.6.34
18.161.6.38
18.161.6.80
18.161.6.89
shbhat@ada:~$
```

1.3.2 Take that list and create a single for loop in the shell that iterates over the list and performs a reverse lookup of each IP address to find each address's associated DNS name. As with the previous step, pipe the output of the for loop to egrep and awk so that the output consists only of the DNS names.

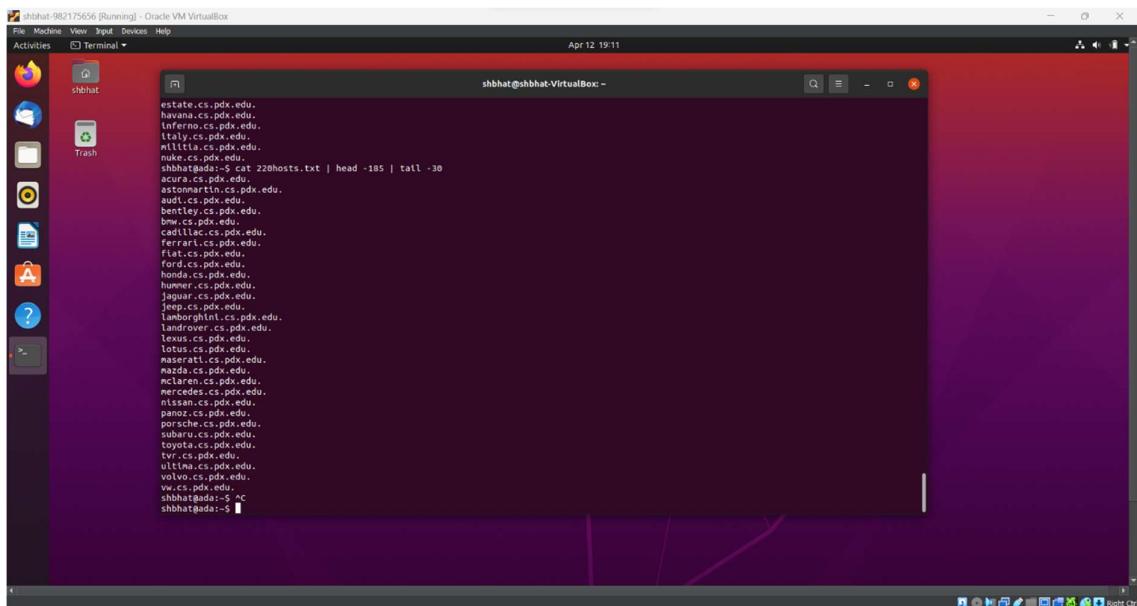


## 1.4 Hosts Enumeration

### 1.4.1 Show the results in your lab notebook.

Answer:

```
cat 220hosts.txt | head -185 | tail -30
```



## DNS #2

### 2.1 Geographic DNS

#### 2.1.1 What geographic locations do ipinfo.io and DB-IP return?

The screenshot shows two separate sessions of a web browser, each displaying four geolocation results from different sources. The top session is for IP address 131.252.208.53 and the bottom session is for 198.82.247.66. Each session contains four cards: IP2Location, ipinfo.io, DB-IP, and iPregistry.co. The results are identical for both IP addresses.

**Geolocation data from IP2Location (Product: DB6, 2023-4-1)**

|                            |                                |
|----------------------------|--------------------------------|
| IP ADDRESS: 131.252.208.53 | ISP: Portland State University |
| COUNTRY: United States     | ORGANIZATION: Not available    |
| REGION: Oregon             | LATITUDE: 45.5213              |
| CITY: Portland             | LONGITUDE: -122.6859           |

**Geolocation data from ipinfo.io (Product: API, real-time)**

|                            |   |
|----------------------------|---|
| IP ADDRESS: 131.252.208.53 | ISP: Portland State University                    |
| COUNTRY: United States     | ORGANIZATION: Portland State University (pdx.edu) |
| REGION: Oregon             | LATITUDE: 45.5234                                 |
| CITY: Portland             | LONGITUDE: -122.6762                              |

**Geolocation data from DB-IP (Product: API, real-time)**

|                                 |   |
|---------------------------------|---|
| IP ADDRESS: 131.252.208.53      | ISP: Portland State University          |
| COUNTRY: United States          | ORGANIZATION: Portland State University |
| REGION: Oregon                  | LATITUDE: 45.584                        |
| CITY: Portland (North Portland) | LONGITUDE: -122.728                     |

**Geolocation data from iPregistry.co (Product: API, real-time)**

|                                 |   |
|---------------------------------|---|
| IP ADDRESS: 131.252.208.53      | ISP: Portland State University          |
| COUNTRY: United States          | ORGANIZATION: Portland State University |
| REGION: Oregon                  | LATITUDE: 45.584                        |
| CITY: Portland (North Portland) | LONGITUDE: -122.728                     |

**Geolocation data from IP2Location (Product: DB6, 2023-4-1)**

|                           |   |
|---------------------------|---|
| IP ADDRESS: 198.82.247.66 | ISP: Virginia Polytechnic Institute and State Univ. |
| COUNTRY: United States    | ORGANIZATION: Not available                         |
| REGION: Virginia          | LATITUDE: 37.2557                                   |
| CITY: Blacksburg          | LONGITUDE: -80.4315                                 |

**Geolocation data from ipinfo.io (Product: API, real-time)**

|                           |   |
|---------------------------|---|
| IP ADDRESS: 198.82.247.66 | ISP: Virginia Polytechnic Institute and State Univ.                   |
| COUNTRY: United States    | ORGANIZATION: Virginia Polytechnic Institute and State Univ. (vt.edu) |
| REGION: Virginia          | LATITUDE: 37.2296   |
| CITY: Blacksburg          | LONGITUDE: -80.4139   |

**Geolocation data from DB-IP (Product: API, real-time)**

|                                      |  |
|--------------------------------------|--|
| IP ADDRESS: 198.82.247.66            | ISP: Virginia Polytechnic Institute and State Univ.          |
| COUNTRY: United States               | ORGANIZATION: Virginia Polytechnic Institute and State Univ. |
| REGION: Virginia                     | LATITUDE: 37.2037  |
| CITY: Blacksburg (Farmview - Ramble) | LONGITUDE: -80.4143  |

#### 2.1.2 Record one address for www.google.com from each result for your lab notebook.

Answer:

Web server: 142.251.33.100

The image shows two side-by-side terminal windows running on an Ubuntu 22.04 desktop environment within Oracle VM VirtualBox. Both windows have a red header bar with the title "shbhat@shbhat-VirtualBox:~".

**Terminal Window 1 (Left):**

```
shbhat@ada:~$ dig www.google.com @131.252.208.53
; <>> DIG 9.18.12-0ubuntu0.22.04.1-Ubuntu <>> www.google.com @131.252.208.53
; global options: +cmd
; Got answer:
; >>>HEADER<- opcode: QUERY, status: NOERROR, id: 5258
; Flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 4096
; COOKIE: 0027bd95c257aa90100000643767ad551039b3e41cebfff (good)
; QUESTION SECTION:
;www.google.com.           IN      A
;
;ANSWER SECTION:
www.google.com.      218     IN      A      142.251.33.100
;
; Query time: 0 msec
; SERVER: 131.252.208.53#(131.252.208.53) (UDP)
; WHEN: Wed Apr 12 19:23:34 PDT 2023
; MSG SIZE rcvd: 87
shbhat@ada:~$
```

**Terminal Window 2 (Right):**

```
shbhat@shbhat-VirtualBox:~$ dig www.google.com @198.82.247.66
; <>> DIG 9.18.12-0ubuntu0.22.04.1-Ubuntu <>> www.google.com @198.82.247.66
; global options: +cmd
; Got answer:
; >>>HEADER<- opcode: QUERY, status: NOERROR, id: 2241
; Flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1
;
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 1232
; COOKIE: c441978698fb3a35035755a643767d24be37b3ec8f4cc09 (good)
; QUESTION SECTION:
;www.google.com.           IN      A
;
;ANSWER SECTION:
www.google.com.      34     IN      A      172.253.62.99
www.google.com.      34     IN      A      172.253.62.147
www.google.com.      34     IN      A      172.253.62.103
www.google.com.      34     IN      A      172.253.62.105
www.google.com.      34     IN      A      172.253.62.164
www.google.com.      34     IN      A      172.253.62.106
;
; Query time: 67 msec
; SERVER: 198.82.247.66#53(198.82.247.66) (UDP)
; WHEN: Wed Apr 12 19:24:18 PDT 2023
; MSG SIZE rcvd: 107
shbhat@shbhat:~$
```

The desktop environment includes a dock with icons for various applications like a browser, file manager, and system tools. The bottom right corner shows system status including weather (27°C, mostly sunny), battery level (ENG IN), and network information (07:24 PM, 12-04-2023).

2.1.3 What is the geographic distance between each DNS server and the IP address it resolves for [www.google.com](http://www.google.com)?

Answer:

DNS Servers:

- 172.253.62.105 -> 2016 n mi, 3734 km
- 172.253.62.103 -> 2016 n mi, 3734 km
- 172.253.62.147 -> 611 n mi, 1132 km
- 172.253.62.104 -> 2016 n mi, 3734 km
- 172.253.62.106 -> 2016 n mi, 3734 km
- 172.253.62.99 -> 2016 n mi, 3734 km

The screenshot shows a Windows desktop environment. In the foreground, a command prompt window is open with the following text:  
shbhat  
shbhat@pdx.edu

In the background, a web browser is displaying the "Latitude/Longitude Distance Calculator" from the National Hurricane Center. The calculator interface includes fields for inputting coordinates and selecting distance units (nautical miles or statute miles). The calculated distance is shown as 2016 n mi.

02.2: DNS, Recap | IP Address Lookup | Geolocation | IP Address Lookup | Geolocation | Latitude/Longitude Distance | dig: server, flag, options | WhatsApp

ANALYSES & FORECASTS • DATA & TOOLS • EDUCATIONAL RESOURCES • ARCHIVES • ABOUT • SEARCH •

## Latitude/Longitude Distance Calculator

Enter latitude and longitude of two points, select the desired units: nautical miles (in mi), statute miles (in miles), kilometers (in km) or meters (in m). Latitudes and longitudes may be entered in any of three different formats: decimal degrees (DD.DD), degrees and decimal minutes (DD MM.MM), or degrees, minutes and decimal seconds (DD MM.SS.SS).

**Important Note:** The distance calculator on this page is provided for informational purposes only. The calculations are approximate in nature and may differ a little from the distances as given in the official forecasts and advisories.

[Click here to find your latitude/longitude](#)

**Input Location Points**

| Latitude 1 | Longitude 1 |          |   |
|------------|-------------|----------|---|
| 47.6062    | N           | 122.3321 | W |

| Latitude 2 | Longitude 2 |         |   |
|------------|-------------|---------|---|
| 38.8951    | N           | 77.0364 | W |

**Distance**  
(rounded to the nearest whole unit)

|      |    |
|------|----|
| 3734 | km |
|------|----|

**Compute** **Reset**

adapted from the Great Circle Calculator  
written by Ed Williams  
(used with permission)

More information on Great Circle navigation can be found [here](#).

**Quick Links and Additional Resources**

**TROPICAL CYCLONE FORECASTS**  
Tropical Cyclone Advisories  
Tropical Cyclone Outlook

**SOCIAL MEDIA**  
NHC on Facebook  
Twitter

**RESEARCH AND DEVELOPMENT**  
NOAA Hurricane Research Division  
Hurricane Forecast Model

**NWS FORECAST OFFICES**  
Weather Prediction Center  
Storm Prediction Center  
Ocean Prediction Center

Ln 2, Col 15      100%      Windows (CRLF)      UTF-8

02.2: DNS, Recap | IP Address Lookup | Geolocation | IP Address Lookup | Geolocation | Latitude/Longitude Distance | dig: server, flag, options | WhatsApp

Home Mobile Site Text Version RSS Local Forecast Enter City, State or ZIP code

## NATIONAL HURRICANE CENTER and CENTRAL PACIFIC HURRICANE CENTER

NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION

ANALYSES & FORECASTS • DATA & TOOLS • EDUCATIONAL RESOURCES •

## Latitude/Longitude Distance Calculator

Enter latitude and longitude of two points, select the desired units: nautical miles (in mi), statute miles (in miles), kilometers (in km) or meters (in m). Latitudes and longitudes may be entered in any of three different formats: decimal degrees (DD.DD), degrees and decimal minutes (DD MM.MM), or degrees, minutes and decimal seconds (DD MM.SS.SS).

**Important Note:** The distance calculator on this page is provided for informational purposes only. The calculations are approximate in nature and may differ a little from the distances as given in the official forecasts and advisories.

[Click here to find your latitude/longitude](#)

**Input Location Points**

| Latitude 1 | Longitude 1 |          |   |
|------------|-------------|----------|---|
| 47.6062    | N           | 122.3321 | W |

| Latitude 2 | Longitude 2 |         |   |
|------------|-------------|---------|---|
| 37.422     | N           | 122.084 | W |

**Distance**  
(rounded to the nearest whole unit)

|      |    |
|------|----|
| 1132 | km |
|------|----|

**Compute** **Reset**

adapted from the Great Circle Calculator  
written by Ed Williams  
(used with permission)

More information on Great Circle navigation can be found [here](#).

Ln 2, Col 15      100%      Windows (CRLF)      UTF-8

## 2.1.4 Traceroute - Do the routes reveal any information on the accuracy of the geographic locations given? (Answer might be no)

```

Windows PowerShell
shbhat@ada:~$ traceroute 131.252.288.53
traceroute to 131.252.288.53 (131.252.288.53), 30 hops max, 60 byte packets
1 r0ns.cat.pdx.edu (131.252.288.53) 1.165 ms 1.051 ms 0.997 ms
shbhat@ada:~$ traceroute 198.82.247.66
traceroute to 198.82.247.66 (198.82.247.66), 30 hops max, 60 byte packets
1 radiant.seas.pdx.edu (131.252.288.212) 2.258 ms 2.224 ms 2.305 ms
2 CORE1.net.pdx.edu (131.252.5.142) 0.994 ms 0.874 ms 0.822 ms
3 131.252.5.213 (131.252.5.213) 1.048 ms 0.997 ms 0.893 ms
4 port-psu-pe-01.net.linkoregon.org (199.126.135) 16.334 ms 10.173 ms 10.125 ms
5 eugn-oh-vpn-01.net.linkoregon.org (207.98.126.3) 10.362 ms 10.295 ms 10.287 ms
6 bois-gtwy-pe-01.net.linkoregon.org (207.98.126.135) 16.059 ms 9.993 ms 9.993 ms
7 bois-gtwy-pe-01-loren.net.linkoregon.org (163.253.5.65) 11.195 ms 11.085 ms 11.016 ms
8 hundredrudge-0-0-0-22.4079.core1.salt.net.internet2.edu (163.253.5.64) 65.928 ms 65.699 ms 65.524 ms
9 fourhundredrudge-0-0-0-22.4079.core1.salt.net.internet2.edu (163.253.1.249) 64.413 ms fourhundredrudge-0-0-0-23.4079.core1.salt.net.internet2.edu (163.253.1.3)
10 fourhundredrudge-0-0-0-22.4079.core1.salt.net.internet2.edu (163.253.1.30) 65.437 ms fourhundredrudge-0-0-0-23.4079.core1.salt.net.internet2.edu (163.253.1.3)
11 fourhundredrudge-0-0-0-22.4079.core1.salt.net.internet2.edu (163.253.1.170) 65.874 ms 65.856 ms fourhundredrudge-0-0-0-23.4079.core1.salt.net.internet2.edu (163.253.1.251)
12 fourhundredrudge-0-0-0-22.4079.core1.salt.net.internet2.edu (163.253.1.243) 64.349 ms 64.358 ms 64.288 ms
13 fourhundredrudge-0-0-0-22.4079.core1.salt.net.internet2.edu (163.253.1.244) 66.514 ms 66.505 ms fourhundredrudge-0-0-0-22.4079.core1.salt.net.internet2.edu (163.253.1.97) 66.416 ms
14 fourhundredrudge-0-0-0-3.4079.core2.eqch.net.internet2.edu (163.253.2.19) 65.010 ms 65.036 ms 64.932 ms
15 fourhundredrudge-0-0-0-3.4079.core2.eqch.net.internet2.edu (163.253.2.16) 66.487 ms 66.414 ms 64.777 ms
16 fourhundredrudge-0-0-0-3.4079.core2.eqch.net.internet2.edu (163.253.1.138) 65.437 ms 65.379 ms 65.313 ms
17 192.175.14 (192.175.14) 63.457 ms 63.340 ms
18 vtacs-1.msap.cns.vt.edu (192.78.187.18) 114.241 ms 114.266 ms 114.204 ms
19 hill-border.xe-5-0-2.0.cns.vt.edu (128.173.0.194) 112.822 ms 112.757 ms 112.614 ms
20 128.173.0.210 (128.173.0.210) 114.096 ms 114.041 ms 113.971 ms
21 * cas-core1.lo6.2000.cns.vt.edu (198.82.1.143) 115.274 ms 115.189 ms
22 jeru.cns.vt.edu (198.82.247.66) 68.950 ms 68.886 ms 68.881 ms
shbhat@ada:~$
```

Yes they do reveal the location details, For first 2 IP addresses, we got the traceroute and it describes the accuracy of location.

When traceroute is done to 2 of the google servers it times out after reaching some point, but when we do traceroute to main webserver of google it points to a location in Seattle.

```

Windows PowerShell
shbhat@ada:~$ traceroute 172.253.62.105
traceroute to 172.253.62.105 (172.253.62.105), 30 hops max, 60 byte packets
1 r0ns.cat.pdx.edu (131.252.288.212) 1.143 ms 1.235 ms 1.340 ms
2 CORE1.net.pdx.edu (131.252.5.142) 0.986 ms 0.968 ms 0.959 ms
3 131.252.5.213 (131.252.5.213) 0.892 ms 0.879 ms 0.900 ms
4 google.maxx.net (198.32.195.34) 24.202 ms 24.142 ms 24.099 ms
5 188.170.248.139 (188.170.248.139) 11.386 ms 11.325 ms 11.301 ms
6 172.253.76.192 (172.253.76.192) 13.770 ms 13.720 ms 13.688 ms
7 142.256.213.71 (142.256.213.71) 54.326 ms 142.251.226.159 (142.251.226.159) 55.733 ms 142.251.226.163 (142.251.226.163) 52.342 ms
8 142.251.64.248 (142.251.64.248) 66.249 ms * 142.251.64.252 (142.251.64.252) 64.468 ms
9 142.251.64.252 (142.251.64.252) 64.468 ms *
10 142.256.230.219 (142.256.230.219) 67.265 ms 172.253.65.78 (172.253.65.78) 65.848 ms 142.256.218.226 (142.256.218.226) 66.911 ms
11 142.251.285.105 (142.251.285.105) 66.351 ms 172.253.68.75 (172.253.68.75) 66.988 ms 172.253.68.73 (172.253.68.73) 64.934 ms
12 * *
13 * *
14 * *
15 * *
16 * *
17 * *
18 * *
19 * *
20 * *
21 bc-in-f105.le100.net (172.253.62.105) 65.305 ms 65.263 ms *
shbhat@ada:~$ traceroute 172.253.62.105
traceroute to 172.253.62.105 (172.253.62.105), 30 hops max, 60 byte packets
1 radiant.seas.pdx.edu (131.252.288.212) 1.109 ms 4.155 ms 4.111 ms
2 CORE1.net.pdx.edu (131.252.5.142) 0.998 ms 0.816 ms 0.761 ms
3 131.252.5.213 (131.252.5.213) 0.892 ms 0.879 ms 0.891 ms
4 google.maxx.net (198.32.195.34) 42.023 ms 41.958 ms 42.893 ms
5 74.125.243.179 (74.125.243.179) 6.120 ms 108.178.245.188 (108.178.245.188) 5.135 ms 108.178.245.118 (108.178.245.118) 4.814 ms
6 172.253.76.192 (172.253.76.192) 13.770 ms 13.720 ms 13.688 ms
7 142.256.213.61 (142.256.213.61) 51.926 ms 142.256.213.61 (142.256.213.61) 51.926 ms
8 * 142.251.65.2 (142.251.65.2) 64.901 ms *
9 142.250.209.206 (142.250.209.206) 66.642 ms 142.251.284.161 (142.251.284.161) 66.280 ms 142.251.284.199 (142.251.284.199) 65.390 ms
10 142.250.209.206 (142.250.209.206) 66.642 ms 142.251.284.161 (142.251.284.161) 66.280 ms 142.251.284.199 (142.251.284.199) 65.390 ms
11 70.125.37.153 (70.125.37.153) 65.392 ms 172.253.68.81 (172.253.68.81) 66.373 ms 142.251.285.105 (142.251.285.105) 66.455 ms
12 * *
13 * *
14 * *
15 * *
16 * *
17 * *
18 * *
19 * *
20 * *
21 bc-in-f103.le100.net (172.253.62.105) 65.607 ms 65.599 ms 65.153 ms
shbhat@ada:~$ traceroute 142.251.33.100
traceroute to 142.251.33.100 (142.251.33.100), 30 hops max, 60 byte packets
1 radiant.seas.pdx.edu (131.252.288.212) 1.109 ms 4.155 ms 4.111 ms
2 CORE1.net.pdx.edu (131.252.5.142) 0.998 ms 0.874 ms 0.733 ms
3 131.252.5.213 (131.252.5.213) 1.058 ms 1.009 ms 0.939 ms
4 google.maxx.net (198.32.195.34) 30.131 ms 34.066 ms 34.087 ms
5 74.125.243.179 (74.125.243.179) 5.015 ms 108.178.245.188 (108.178.245.188) 4.815 ms 108.178.245.118 (108.178.245.118) 4.536 ms
6 142.251.50.177 (142.251.50.177) 4.224 ms 3.985 ms 142.251.50.175 (142.251.50.175) 4.536 ms
7 sea3910-in-f11.le100.net (142.251.33.100) 0.966 ms 4.799 ms 4.734 ms
shbhat@ada:~$
```

## Network Recap Lab #3

### 3.1 REVERSE DNS

3.1.1 Perform a reverse DNS lookup on the DNS server to find its name.

Include it in your lab notebook.

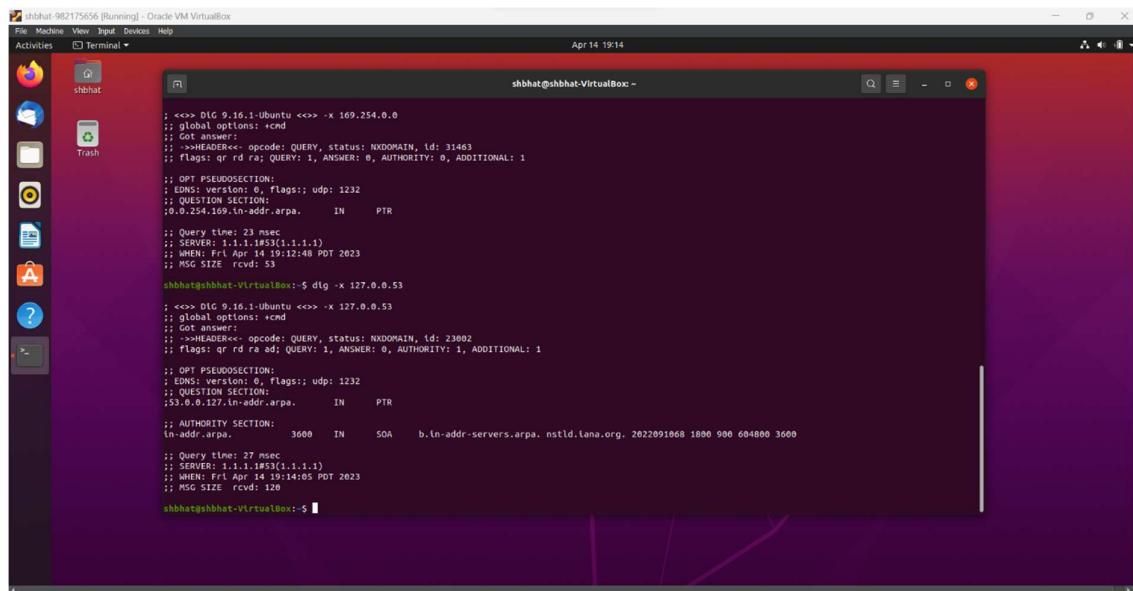
## Answer:

shbhat@shbhat-VirtualBox: ~

```
shbhat@shbhat-VirtualBox: ~$ ifconfig
ens3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 10.0.2.15 brd 255.255.255.0 broadcast 10.0.2.255
                netmask 255.255.255.0 scopeid 0x20<link>
                ether fe80::fe0:2fffe%ens3 brd ff:ff:ff:ff:ff:ff link-layer
                txqueuelen 1000  (Ethernet)
                  RX packets 0 bytes 0 (0.0 B)
                  RX errors 0 dropped 0 overruns 0 frame 0
                  TX packets 172 bytes 22692 (22.6 KB)
                  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 brd 255.255.255.0
                netmask 255.255.255.0 scopeid 0x0<host>
                link-layer 0000:00:00:00:00:00
                txqueuelen 1000  (Local loopback)
                  RX packets 156 bytes 13278 (13.2 kB)
                  RX errors 0 dropped 0 overruns 0 frame 0
                  TX packets 156 bytes 13278 (13.2 kB)
                  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

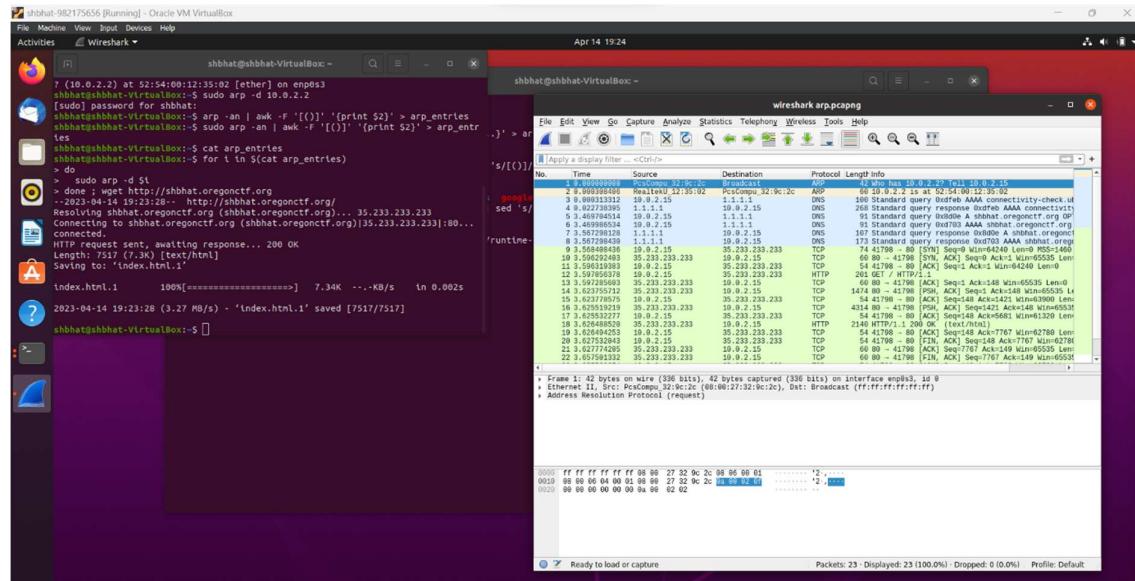
shbhat@shbhat-VirtualBox: ~$ netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask        Flags   MSS Window irtt Iface
0.0.0.0         10.0.2.2      0.0.0.0       U      0        0        0 enp0s3
10.0.2.0        0.0.0.0       255.255.255.0 U      0        0        0 enp0s3
109.254.0.0     0.0.0.0       255.255.0.0   U      0        0        0 enp0s3
shbhat@shbhat-VirtualBox: ~$
```



```
; <>>. DLG 9.16.1-Ubuntu <>> -x 169.254.0.0
; global options: +cmd
; Got answer:
; >>>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 31463
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 1232
; QUESTION SECTION:
;_0.0.254.169.in-addr.arpa. IN PTR
; Query time: 23 msec
; SERVER: 1.1.1.1#53(1.1.1.1)
; WHEN: Fri Apr 14 19:12:48 PDT 2023
; MSG SIZE rcvd: 53
shbhat@shbhat-VirtualBox:~$ dig -x 127.0.0.53
; <>>. DLG 9.16.1-Ubuntu <>> -x 127.0.0.53
; global options: +cmd
; Got answer:
; >>>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 23002
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 1232
; QUESTION SECTION:
;_53.0.0.127.in-addr.arpa. IN PTR
; AUTHORITY SECTION:
;_in-addr.arpa. 3600 IN SOA b.in-addr-servers.arpa. ns.tld.lana.org. 2022091068 1800 900 604800 3600
; Query time: 27 msec
; SERVER: 1.1.1.1#53(1.1.1.1)
; WHEN: Fri Apr 14 19:14:05 PDT 2023
; MSG SIZE rcvd: 328
shbhat@shbhat-VirtualBox:~$
```

### 3.2 ARP and Wireshark

3.2.1 Take a screenshot of the trace within Wireshark and include an annotation of the packets in the trace to explain the purpose of each of the packets being exchanged.



Brief annotation of packets and explanation.

- 1) ARP The client sends an ARP request first to determine the MAC address of the DNS server and sends appropriate response.
- 2) DNS is then initiated to DNS server to get specific IP address of specific domain name and we get DNS response with IP address.
- 3) Next is TCP connection and connection is initiated via 3-way handshake and we get SYN and ACK.
- 4) Finally, HTTP request is sent which is mainly GET in our case and we get HTTP response with status code usually 200 that connection is successfully established.

### 3.2.2 How many DNS requests are made?

Answer:

3 DNS requests are made and 3 DNS responses.

### 3.2.3 How many TCP connections does the browser initiate simultaneously to the site?

Answer:

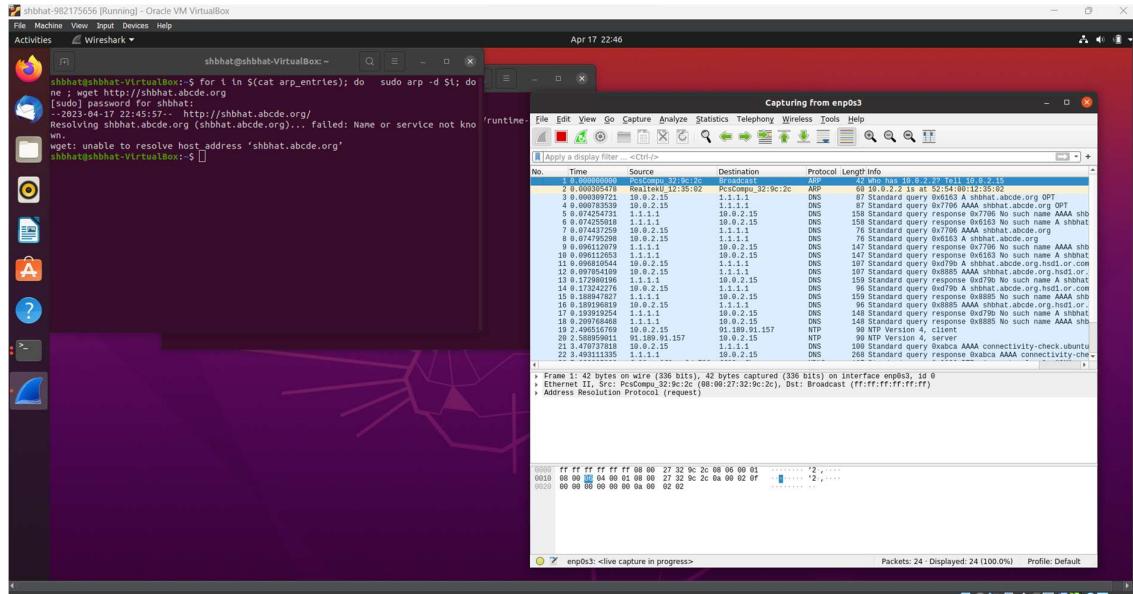
Total 14 TCP requests and if we divide it by 2 we will get 7 which is the request initiated simultaneously to the site.

### 3.2.4 How many HTTP GET requests are there for embedded objects?

Answer:

#### 1 HTTP Get

### 3.2.5 Run the lab again using random characters after the <OdinID> in the DNS name you are fetching.



### 3.2.6 How many DNS requests are made?

Answer:

Total of 16 DNS requests, 8 requests and 8 responses.

### 3.2.7 How many TCP connections does the browser initiate simultaneously to the site?

Answer:

0 TCP since the site is invalid.

### 3.2.8 How many HTTP GET requests are there for embedded objects?

Answer:

0 HTTP requests because this site does not exist.