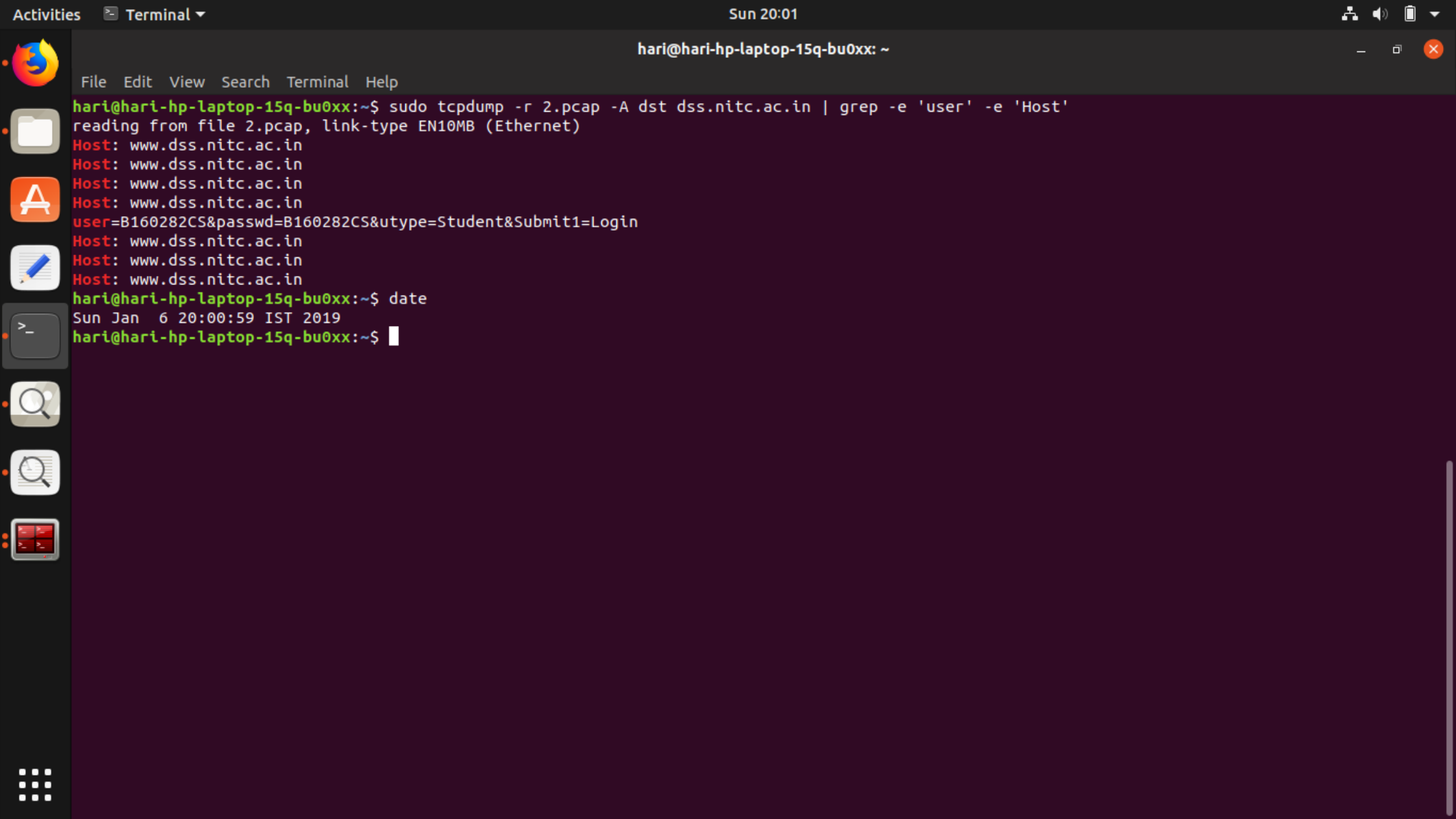
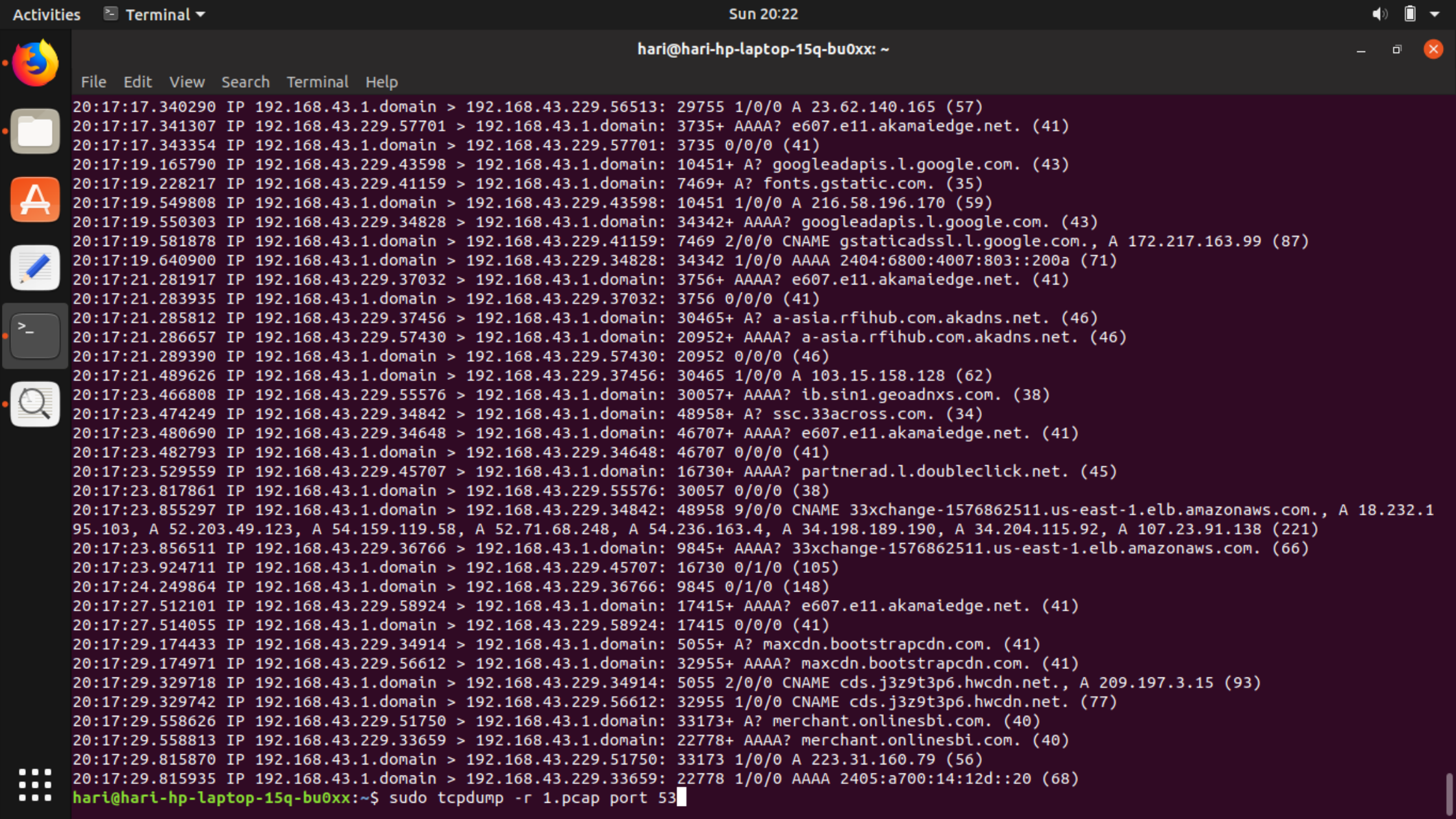
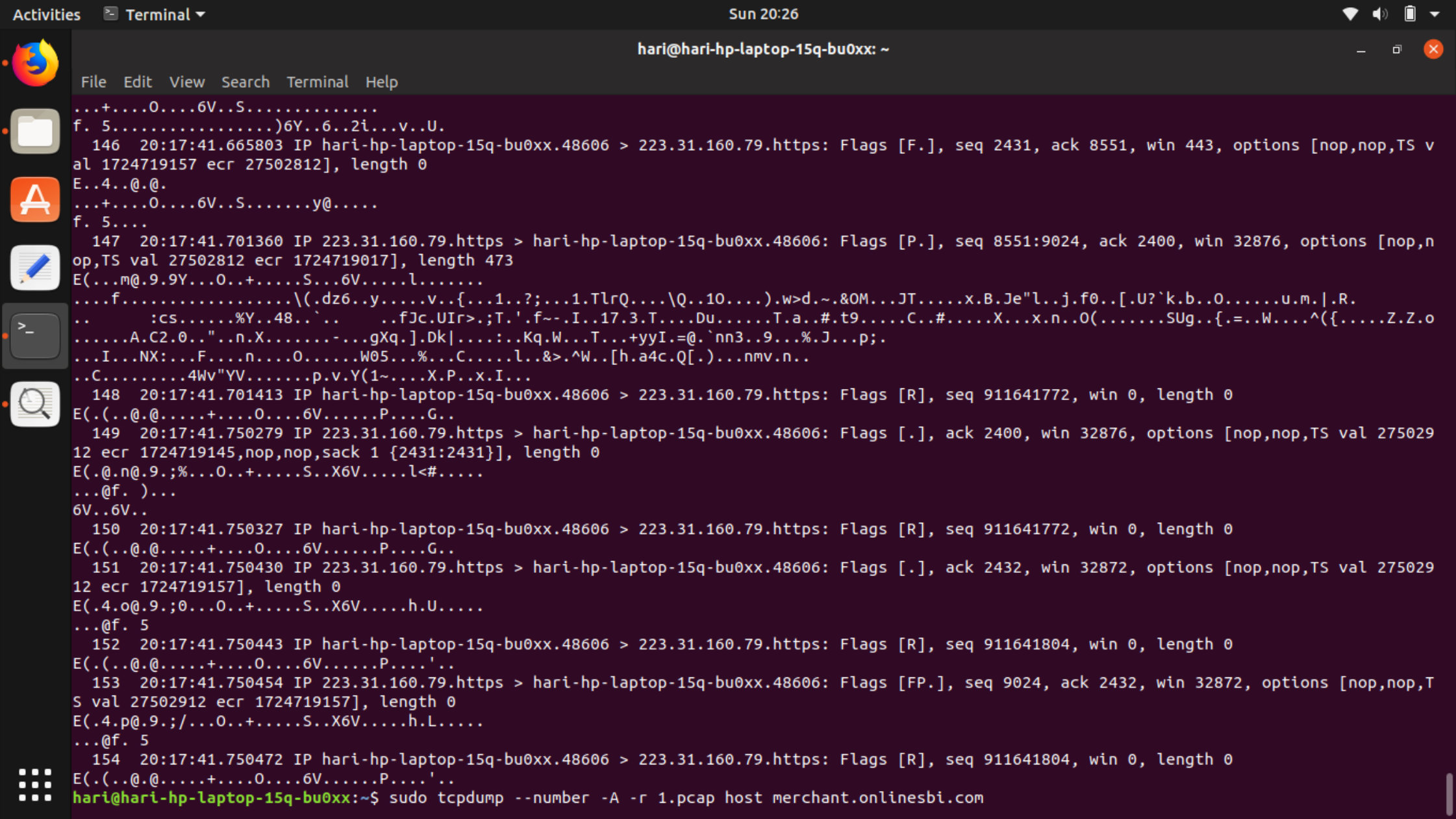

Activities
Terminal
Sun 20:01
hari@hari-hp-laptop-15q-bu0xx: ~
File Edit View Search Terminal Help
hari@hari-hp-laptop-15q-bu0xx:~$ sudo tcpdump -r 2.pcap -A dst dss.nitc.ac.in | grep -e 'user' -e 'Host'
reading from file 2.pcap, link-type EN10MB (Ethernet)
Host: www.dss.nitc.ac.in
Host: www.dss.nitc.ac.in
Host: www.dss.nitc.ac.in
Host: www.dss.nitc.ac.in
user=B160282CS&passwd=B160282CS&utype=Student&Submit1=Login
Host: www.dss.nitc.ac.in
Host: www.dss.nitc.ac.in
Host: www.dss.nitc.ac.in
hari@hari-hp-laptop-15q-bu0xx:~$ date
Sun Jan 6 20:00:59 IST 2019
hari@hari-hp-laptop-15q-bu0xx:~$


Activities
Terminal
Sun 20:22
hari@hari-hp-laptop-15q-bu0xx: ~
File Edit View Search Terminal Help
20:17:17.340290 IP 192.168.43.1.domain > 192.168.43.229.56513: 29755 1/0/0 A 23.62.140.165 (57)
20:17:17.341307 IP 192.168.43.229.57701 > 192.168.43.1.domain: 3735+ AAAA? e607.e11.akamaiedge.net. (41)
20:17:17.343354 IP 192.168.43.1.domain > 192.168.43.229.57701: 3735 0/0/0 (41)
20:17:19.165790 IP 192.168.43.229.43598 > 192.168.43.1.domain: 10451+ A? googleadapis.l.google.com. (43)
20:17:19.228217 IP 192.168.43.229.41159 > 192.168.43.1.domain: 7469+ A? fonts.gstatic.com. (35)
20:17:19.549808 IP 192.168.43.1.domain > 192.168.43.229.43598: 10451 1/0/0 A 216.58.196.170 (59)
20:17:19.550303 IP 192.168.43.229.34828 > 192.168.43.1.domain: 34342+ AAAA? googleadapis.l.google.com. (43)
20:17:19.581878 IP 192.168.43.1.domain > 192.168.43.229.41159: 7469 2/0/0 CNAME gstaticadssl.l.google.com., A 172.217.163.99 (87)
20:17:19.640900 IP 192.168.43.1.domain > 192.168.43.229.34828: 34342 1/0/0 AAAA 2404:6800:4007:803::200a (71)
20:17:21.281917 IP 192.168.43.229.37032 > 192.168.43.1.domain: 3756+ AAAA? e607.e11.akamaiedge.net. (41)
20:17:21.283935 IP 192.168.43.1.domain > 192.168.43.229.37032: 3756 0/0/0 (41)
20:17:21.285812 IP 192.168.43.229.37456 > 192.168.43.1.domain: 30465+ A? a-asia.rfihub.com.akadns.net. (46)
20:17:21.286657 IP 192.168.43.229.57430 > 192.168.43.1.domain: 20952+ AAAA? a-asia.rfihub.com.akadns.net. (46)
20:17:21.289390 IP 192.168.43.1.domain > 192.168.43.229.57430: 20952 0/0/0 (46)
20:17:21.489626 IP 192.168.43.1.domain > 192.168.43.229.37456: 30465 1/0/0 A 103.15.158.128 (62)
20:17:23.466808 IP 192.168.43.229.55576 > 192.168.43.1.domain: 30057+ AAAA? ib.sin1.geoadnxs.com. (38)
20:17:23.474249 IP 192.168.43.229.34842 > 192.168.43.1.domain: 48958+ A? ssc.33across.com. (34)
20:17:23.480690 IP 192.168.43.229.34648 > 192.168.43.1.domain: 46707+ AAAA? e607.e11.akamaiedge.net. (41)
20:17:23.482793 IP 192.168.43.1.domain > 192.168.43.229.34648: 46707 0/0/0 (41)
20:17:23.529559 IP 192.168.43.229.45707 > 192.168.43.1.domain: 16730+ AAAA? partnerad.l.doubleclick.net. (45)
20:17:23.817861 IP 192.168.43.1.domain > 192.168.43.229.55576: 30057 0/0/0 (38)
20:17:23.855297 IP 192.168.43.1.domain > 192.168.43.229.34842: 48958 9/0/0 CNAME 33xchange-1576862511.us-east-1.elb.amazonaws.com., A 18.232.1
95.103, A 52.203.49.123, A 54.159.119.58, A 52.71.68.248, A 54.236.163.4, A 34.198.189.190, A 34.204.115.92, A 107.23.91.138 (221)
20:17:23.856511 IP 192.168.43.229.36766 > 192.168.43.1.domain: 9845+ AAAA? 33xchange-1576862511.us-east-1.elb.amazonaws.com. (66)
20:17:23.924711 IP 192.168.43.1.domain > 192.168.43.229.45707: 16730 0/1/0 (105)
20:17:24.249864 IP 192.168.43.1.domain > 192.168.43.229.36766: 9845 0/1/0 (148)
20:17:27.512101 IP 192.168.43.229.58924 > 192.168.43.1.domain: 17415+ AAAA? e607.e11.akamaiedge.net. (41)
20:17:27.514055 IP 192.168.43.1.domain > 192.168.43.229.58924: 17415 0/0/0 (41)
20:17:29.174433 IP 192.168.43.229.34914 > 192.168.43.1.domain: 5055+ A? maxcdn.bootstrapcdn.com. (41)
20:17:29.174971 IP 192.168.43.229.56612 > 192.168.43.1.domain: 32955+ AAAA? maxcdn.bootstrapcdn.com. (41)
20:17:29.329718 IP 192.168.43.1.domain > 192.168.43.229.34914: 5055 2/0/0 CNAME cds.j3z9t3p6.hwcdn.net., A 209.197.3.15 (93)
20:17:29.329742 IP 192.168.43.1.domain > 192.168.43.229.56612: 32955 1/0/0 CNAME cds.j3z9t3p6.hwcdn.net. (77)
20:17:29.558626 IP 192.168.43.229.51750 > 192.168.43.1.domain: 33173+ A? merchant.onlinesbi.com. (40)
20:17:29.558813 IP 192.168.43.229.33659 > 192.168.43.1.domain: 22778+ AAAA? merchant.onlinesbi.com. (40)
20:17:29.815870 IP 192.168.43.1.domain > 192.168.43.229.51750: 33173 1/0/0 A 223.31.160.79 (56)
20:17:29.815935 IP 192.168.43.1.domain > 192.168.43.229.33659: 22778 1/0/0 AAAA 2405:a700:14:12d::20 (68)
hari@hari-hp-laptop-15q-bu0xx:~$ sudo tcpdump -r 1.pcap port 53


Activities
Terminal
Sun 20:26
hari@hari-hp-laptop-15q-bu0xx: ~
File Edit View Search Terminal Help
...+....O....6V..S.............
f. 5.................)6Y..6..2i...v..U.
  146 20:17:41.665803 IP hari-hp-laptop-15q-bu0xx.48606 > 223.31.160.79.https: Flags [F.], seq 2431, ack 8551, win 443, options [nop,nop,TS v
al 1724719157 ecr 27502812], length 0
E..4..@.@.
...+....O....6V..S.......y@.....
f. 5....
  147 20:17:41.701360 IP 223.31.160.79.https > hari-hp-laptop-15q-bu0xx.48606: Flags [P.], seq 8551:9024, ack 2400, win 32876, options [nop,n
op,TS val 27502812 ecr 1724719017], length 473
E(...m@.9.9Y...O..+.....S...6V.....l.......
....f..................\(.dz6..y.....v..{...1..?;...1.TlrQ....\Q..1O....).w>d.~.&OM...JT.....x.B.Je"l..j.f0..[.U?`k.b..O......u.m.|.R.
..   :cs......%Y..48..`..   ..fJc.UIr>.;T.'.f~-.I..17.3.T....Du......T.a..#.t9.....C..#.....X...x.n..O(.......SUg..{.=..W....^({.....Z.Z.o
......A.C2.0.."..n.X.......-...gXq.].Dk|....:..Kq.W...T...+yyI.=@.`nn3..9...%.J...p;.
...I...NX:...F....n....O......W05...%...C.....l..&>.^W..[h.a4c.Q[.)...nmv.n..
..C.........4Wv"YV.......p.v.Y(1~....X.P..x.I...
  148 20:17:41.701413 IP hari-hp-laptop-15q-bu0xx.48606 > 223.31.160.79.https: Flags [R], seq 911641772, win 0, length 0
E(.(..@.@.....+....O....6V......P....G..
  149 20:17:41.750279 IP 223.31.160.79.https > hari-hp-laptop-15q-bu0xx.48606: Flags [.], ack 2400, win 32876, options [nop,nop,TS val 275029
12 ecr 1724719145,nop,nop,sack 1 {2431:2431}], length 0
E(.@.n@.9.;%...O..+.....S..X6V.....l<#.....
...@f.)...
6V..6V..
  150 20:17:41.750327 IP hari-hp-laptop-15q-bu0xx.48606 > 223.31.160.79.https: Flags [R], seq 911641772, win 0, length 0
E(.(..@.@.....+....O....6V......P....G..
  151 20:17:41.750430 IP 223.31.160.79.https > hari-hp-laptop-15q-bu0xx.48606: Flags [.], ack 2432, win 32872, options [nop,nop,TS val 275029
12 ecr 1724719157], length 0
E(.4.o@.9.;0...O..+.....S..X6V.....h.U.....
...@f. 5
  152 20:17:41.750443 IP hari-hp-laptop-15q-bu0xx.48606 > 223.31.160.79.https: Flags [R], seq 911641804, win 0, length 0
E(.(..@.@.....+....O....6V......P....'..
  153 20:17:41.750454 IP 223.31.160.79.https > hari-hp-laptop-15q-bu0xx.48606: Flags [FP.], seq 9024, ack 2432, win 32872, options [nop,nop,T
S val 27502912 ecr 1724719157], length 0
E(.4.p@.9.;/...O..+.....S..X6V.....h.L.....
...@f. 5
  154 20:17:41.750472 IP hari-hp-laptop-15q-bu0xx.48606 > 223.31.160.79.https: Flags [R], seq 911641804, win 0, length 0
E(.(..@.@.....+....O....6V......P....'..
hari@hari-hp-laptop-15q-bu0xx:~$ sudo tcpdump --number -A -r 1.pcap host merchant.onlinesbi.com