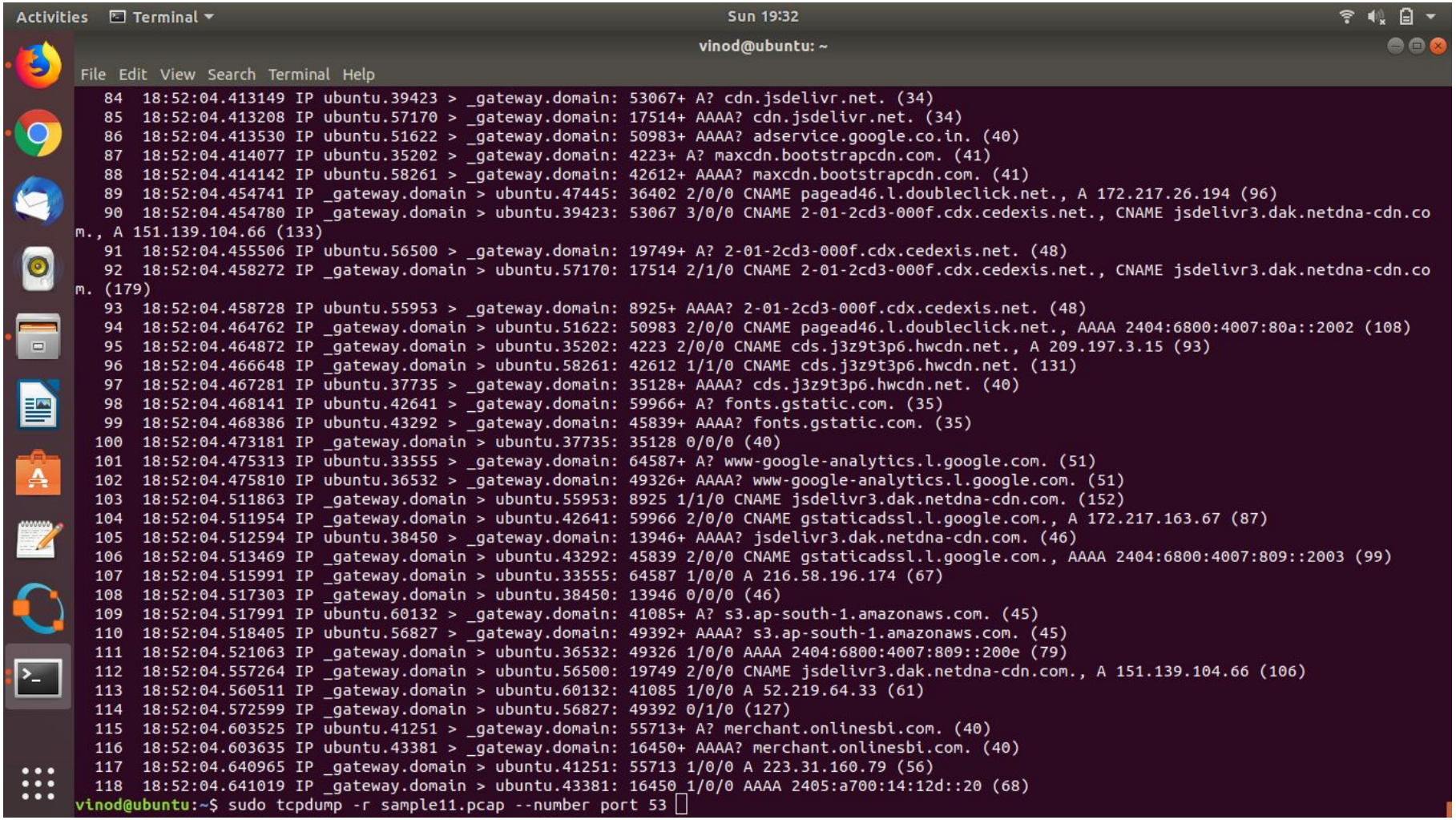
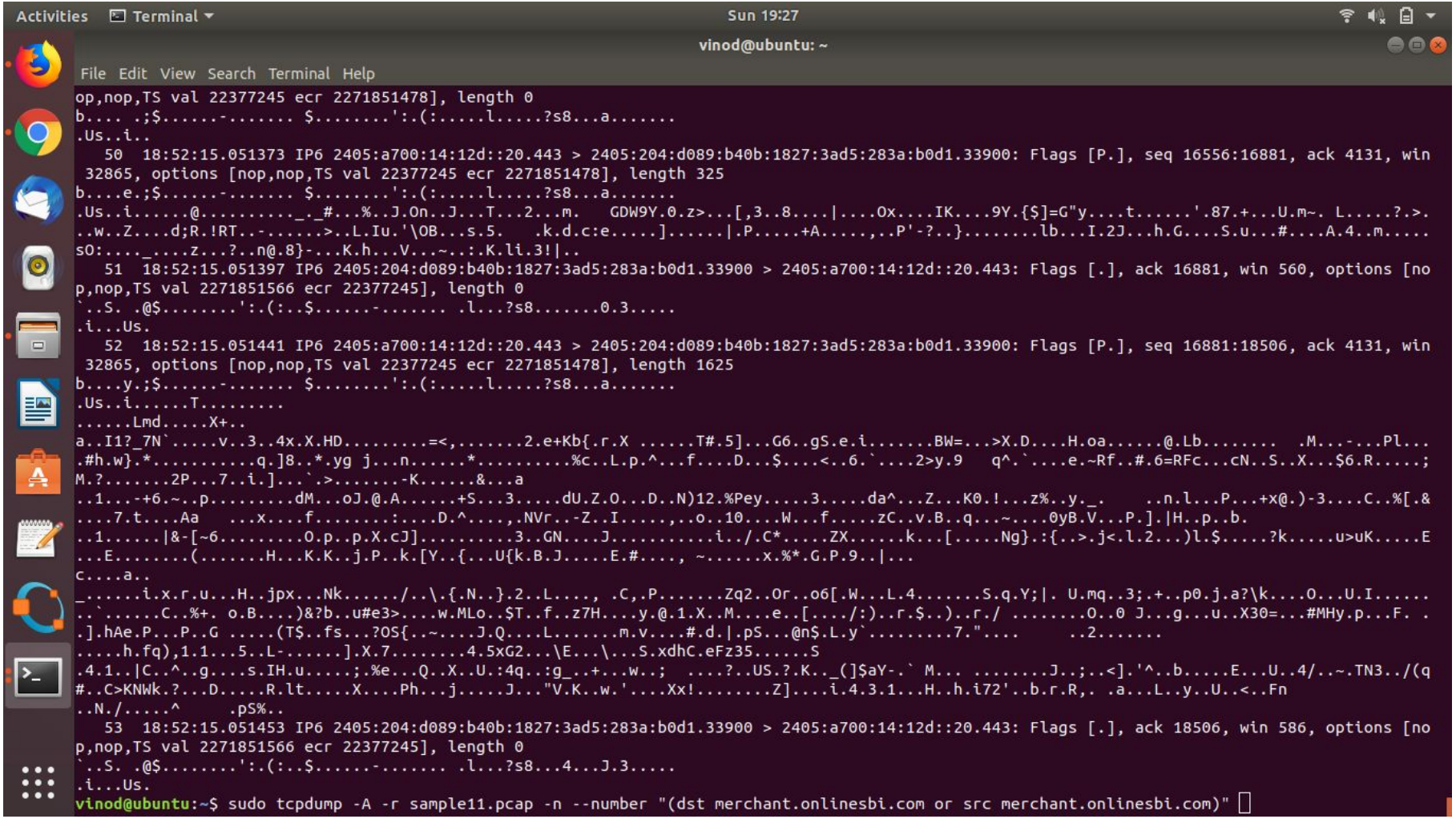
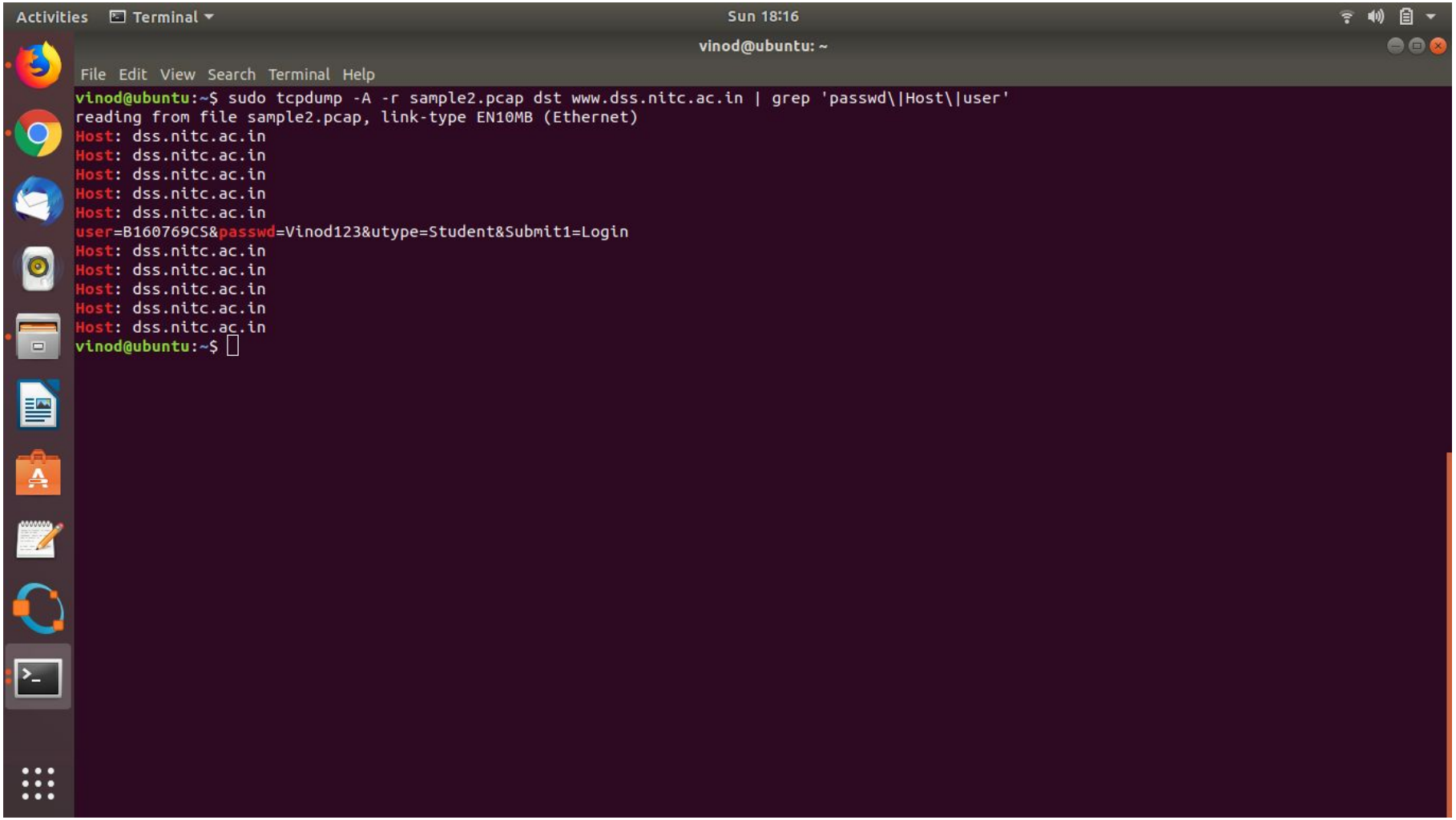

Activities
Terminal
Sun 19:32
vinod@ubuntu: ~
File Edit View Search Terminal Help
84 18:52:04.413149 IP ubuntu.39423 > _gateway.domain: 53067+ A? cdn.jsdelivr.net. (34)
85 18:52:04.413208 IP ubuntu.57170 > _gateway.domain: 17514+ AAAA? cdn.jsdelivr.net. (34)
86 18:52:04.413530 IP ubuntu.51622 > _gateway.domain: 50983+ AAAA? adservice.google.co.in. (40)
87 18:52:04.414077 IP ubuntu.35202 > _gateway.domain: 4223+ A? maxcdn.bootstrapcdn.com. (41)
88 18:52:04.414142 IP ubuntu.58261 > _gateway.domain: 42612+ AAAA? maxcdn.bootstrapcdn.com. (41)
89 18:52:04.454741 IP _gateway.domain > ubuntu.47445: 36402 2/0/0 CNAME pagead46.l.doubleclick.net., A 172.217.26.194 (96)
90 18:52:04.454780 IP _gateway.domain > ubuntu.39423: 53067 3/0/0 CNAME 2-01-2cd3-000f.cdx.cedexis.net., CNAME jsdelivr3.dak.netdna-cdn.com., A 151.139.104.66 (133)
91 18:52:04.455506 IP ubuntu.56500 > _gateway.domain: 19749+ A? 2-01-2cd3-000f.cdx.cedexis.net. (48)
92 18:52:04.458272 IP _gateway.domain > ubuntu.57170: 17514 2/1/0 CNAME 2-01-2cd3-000f.cdx.cedexis.net., CNAME jsdelivr3.dak.netdna-cdn.com. (179)
93 18:52:04.458728 IP ubuntu.55953 > _gateway.domain: 8925+ AAAA? 2-01-2cd3-000f.cdx.cedexis.net. (48)
94 18:52:04.464762 IP _gateway.domain > ubuntu.51622: 50983 2/0/0 CNAME pagead46.l.doubleclick.net., AAAA 2404:6800:4007:80a::2002 (108)
95 18:52:04.464872 IP _gateway.domain > ubuntu.35202: 4223 2/0/0 CNAME cds.j3z9t3p6.hwcdn.net., A 209.197.3.15 (93)
96 18:52:04.466648 IP _gateway.domain > ubuntu.58261: 42612 1/1/0 CNAME cds.j3z9t3p6.hwcdn.net. (131)
97 18:52:04.467281 IP ubuntu.37735 > _gateway.domain: 35128+ AAAA? cds.j3z9t3p6.hwcdn.net. (40)
98 18:52:04.468141 IP ubuntu.42641 > _gateway.domain: 59966+ A? fonts.gstatic.com. (35)
99 18:52:04.468386 IP ubuntu.43292 > _gateway.domain: 45839+ AAAA? fonts.gstatic.com. (35)
100 18:52:04.473181 IP _gateway.domain > ubuntu.37735: 35128 0/0/0 (40)
101 18:52:04.475313 IP ubuntu.33555 > _gateway.domain: 64587+ A? www-google-analytics.l.google.com. (51)
102 18:52:04.475810 IP ubuntu.36532 > _gateway.domain: 49326+ AAAA? www-google-analytics.l.google.com. (51)
103 18:52:04.511863 IP _gateway.domain > ubuntu.55953: 8925 1/1/0 CNAME jsdelivr3.dak.netdna-cdn.com. (152)
104 18:52:04.511954 IP _gateway.domain > ubuntu.42641: 59966 2/0/0 CNAME gstaticadssl.l.google.com., A 172.217.163.67 (87)
105 18:52:04.512594 IP ubuntu.38450 > _gateway.domain: 13946+ AAAA? jsdelivr3.dak.netdna-cdn.com. (46)
106 18:52:04.513469 IP _gateway.domain > ubuntu.43292: 45839 2/0/0 CNAME gstaticadssl.l.google.com., AAAA 2404:6800:4007:809::2003 (99)
107 18:52:04.515991 IP _gateway.domain > ubuntu.33555: 64587 1/0/0 A 216.58.196.174 (67)
108 18:52:04.517303 IP _gateway.domain > ubuntu.38450: 13946 0/0/0 (46)
109 18:52:04.517991 IP ubuntu.60132 > _gateway.domain: 41085+ A? s3.ap-south-1.amazonaws.com. (45)
110 18:52:04.518405 IP ubuntu.56827 > _gateway.domain: 49392+ AAAA? s3.ap-south-1.amazonaws.com. (45)
111 18:52:04.521063 IP _gateway.domain > ubuntu.36532: 49326 1/0/0 AAAA 2404:6800:4007:809::200e (79)
112 18:52:04.557264 IP _gateway.domain > ubuntu.56500: 19749 2/0/0 CNAME jsdelivr3.dak.netdna-cdn.com., A 151.139.104.66 (106)
113 18:52:04.560511 IP _gateway.domain > ubuntu.60132: 41085 1/0/0 A 52.219.64.33 (61)
114 18:52:04.572599 IP _gateway.domain > ubuntu.56827: 49392 0/1/0 (127)
115 18:52:04.603525 IP ubuntu.41251 > _gateway.domain: 55713+ A? merchant.onlinesbi.com. (40)
116 18:52:04.603635 IP ubuntu.43381 > _gateway.domain: 16450+ AAAA? merchant.onlinesbi.com. (40)
117 18:52:04.640965 IP _gateway.domain > ubuntu.41251: 55713 1/0/0 A 223.31.160.79 (56)
118 18:52:04.641019 IP _gateway.domain > ubuntu.43381: 16450 1/0/0 AAAA 2405:a700:14:12d::20 (68)
vinod@ubuntu:~$ sudo tcpdump -r sample11.pcap --number port 53


Activities
Terminal
Sun 19:27
vinod@ubuntu: ~
File Edit View Search Terminal Help
op,nop,TS val 22377245 ecr 2271851478], length 0
b.... .;$.....-..... $.......':.(:.....l.....?s8...a.....
.Us..i..
50 18:52:15.051373 IP6 2405:a700:14:12d::20.443 > 2405:204:d089:b40b:1827:3ad5:283a:b0d1.33900: Flags [P.], seq 16556:16881, ack 4131, win
32865, options [nop,nop,TS val 22377245 ecr 2271851478], length 325
b....e.;$.....-..... $.......':.(:.....l.....?s8...a.....
.Us..i.....@.........._._#...%..J.On..J...T...2...m. GDW9Y.0.z>...[,3..8....|....Ox....IK....9Y.{$]=G"y....t.....'.87.+...U.m~. L.....?.>.
..w..Z....d;R.!RT..-.....>..L.Iu.'\OB...s.5. .k.d.c:e.....].....|.P.....+A....,..P'-?..}.....lb...I.2J...h.G....S.u...#....A.4..m.....
sO:...._....z...?..n@.8}-...K.h...V...~..:.K.li.3!|..
51 18:52:15.051397 IP6 2405:204:d089:b40b:1827:3ad5:283a:b0d1.33900 > 2405:a700:14:12d::20.443: Flags [.], ack 16881, win 560, options [no
p,nop,TS val 2271851566 ecr 22377245], length 0
`..S. .@$.....':.(:..$.....-..... .l...?s8.....0.3.....
.i...Us.
52 18:52:15.051441 IP6 2405:a700:14:12d::20.443 > 2405:204:d089:b40b:1827:3ad5:283a:b0d1.33900: Flags [P.], seq 16881:18506, ack 4131, win
32865, options [nop,nop,TS val 22377245 ecr 2271851478], length 1625
b....y.;$.....-..... $.......':.(:.....l.....?s8...a.....
.Us..i.....T.....
.....Lmd.....X+..
a..I1?_7N`.....v..3..4x.X.HD.....=<,.....2.e+Kb{.r.X .....T#.5]...G6..gS.e.i.....BW=...>X.D....H.oa.....@.Lb..... .M...-...Pl...
.#h.w}.*.....q.]8..*.yg j...n.....*.....%c..L.p.^...f....D...$....<..6.`....2>y.9 q^.`....e.~Rf..#.6=RFc...cN..S..X...$6.R.....;
M.?.....2P...7..i.]...`.>.....-K.....&...a
..1...-+6.~..p.....dM...oJ.@.A.....+S...3.....dU.Z.O...D..N)12.%Pey.....3.....da^...Z...K0.!...z%..y._. ..n.l...P...+x@.)-3....C..%[.&
....7.t....Aa ...x....f.....:....D.^....,.NVr..-Z..I.....,..o..10....W...f.....zC..v.B..q...~....0yB.V...P.].|H..p..b.
..1.....|&-[~6.....O.p..p.X.cJ].....3..GN....J.....i../.C*.....ZX.....k...[.....Ng}.:{..>.j<.l.2...)l.$.....?k.....u>uK.....E
...E.....(.....H...K.K..j.P..k.[Y..{...U{k.B.J.....E.#...., ~.....x.%*.G.P.9..|...
c....a..
_.....i.x.r.u...H..jpx...Nk...../..\.{.N..}.2..L...., .C,.P.....Zq2..Or..o6[.W...L.4.....S.q.Y;|. U.mq..3;.+..p0.j.a?\k....O...U.I.....
..`.....C..%+. o.B....)&?b..u#e3>....w.MLo..$T..f..z7H....y.@.1.X..M....e..[..../:)..r.$..)..r./ .....O..0 J...g...u..X30=...#MHy.p...F. .
.].hAe.P...P..G .....(T$..fs...?OS{..~....J.Q....L.....m.v....#.d.|.pS...@n$.L.y`.....7.".... ..2.....
.....h.fq),1.1...5..L-.....].X.7.....4.5xG2...\E...\...S.xdhC.eFz35.....S
.4.1..|C..^..g....s.IH.u.....;.%e...Q..X..U.:4q..:g_..+...w..; ....?..US.?.K.._(]$aY-.` M... .....J..;..<].'^..b.....E...U..4/..~.TN3../(q
#..C>KNWk.?...D.....R.lt.....X....Ph...j.....J..."V.K..w.'....Xx!.....Z]....i.4.3.1...H..h.i72'..b.r.R,. .a...L..y..U..<..Fn
..N./.....^ .pS%..
53 18:52:15.051453 IP6 2405:204:d089:b40b:1827:3ad5:283a:b0d1.33900 > 2405:a700:14:12d::20.443: Flags [.], ack 18506, win 586, options [no
p,nop,TS val 2271851566 ecr 22377245], length 0
`..S. .@$.....':.(:..$.....-..... .l...?s8...4...J.3.....
.i...Us.
vinod@ubuntu:~$ sudo tcpdump -A -r sample11.pcap -n --number "(dst merchant.onlinesbi.com or src merchant.onlinesbi.com)"


Activities
Terminal
Sun 18:16
vinod@ubuntu: ~
File Edit View Search Terminal Help
vinod@ubuntu:~$ sudo tcpdump -A -r sample2.pcap dst www.dss.nitc.ac.in | grep 'passwd\|Host\|user'
reading from file sample2.pcap, link-type EN10MB (Ethernet)
Host: dss.nitc.ac.in
Host: dss.nitc.ac.in
Host: dss.nitc.ac.in
Host: dss.nitc.ac.in
Host: dss.nitc.ac.in
user=B160769CS&passwd=Vinod123&utype=Student&Submit1=Login
Host: dss.nitc.ac.in
Host: dss.nitc.ac.in
Host: dss.nitc.ac.in
Host: dss.nitc.ac.in
Host: dss.nitc.ac.in
vinod@ubuntu:~$