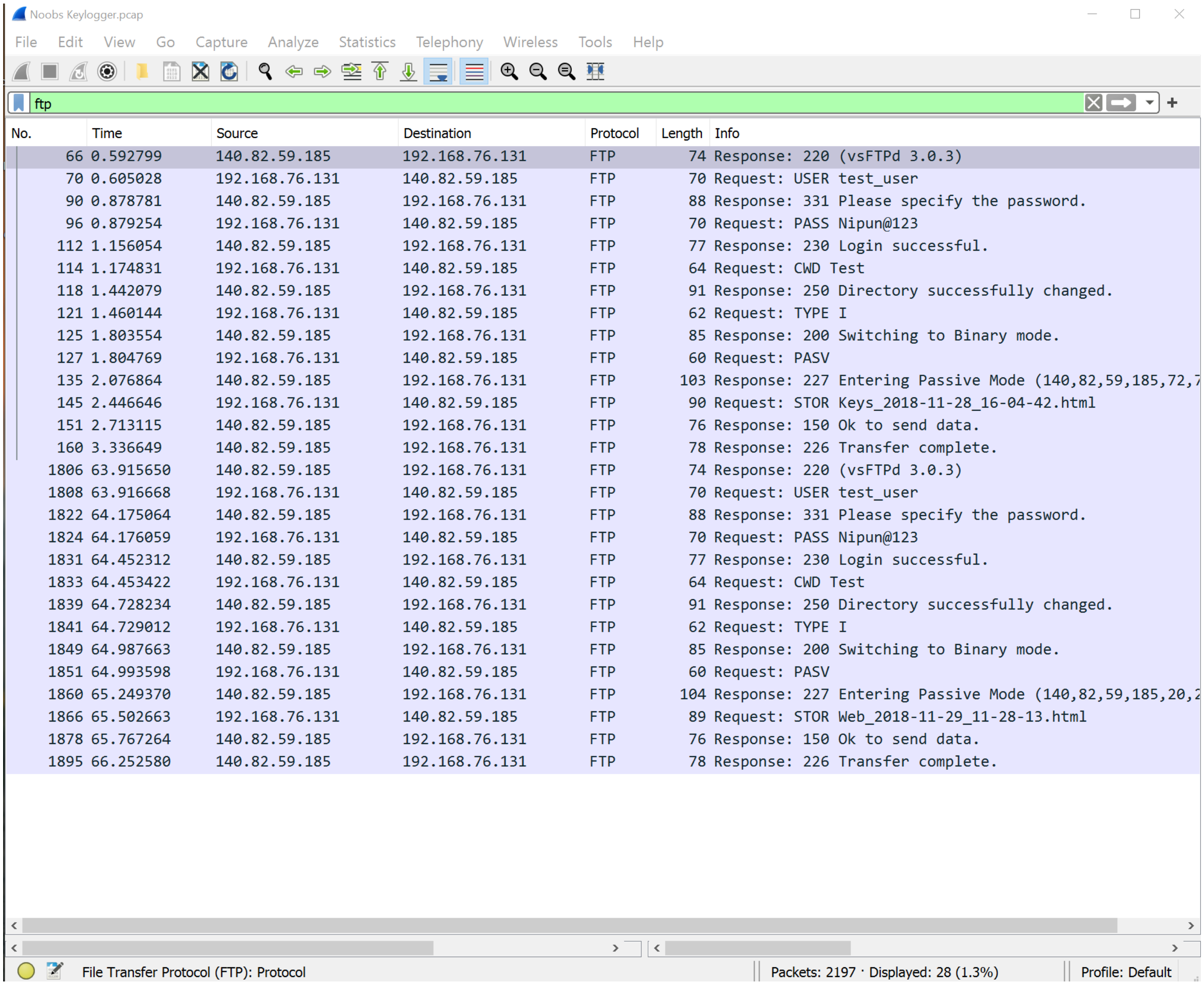
## Exercise 1 – a noobs keylogger

- Used SMTP and POP filters to check if there was something unusual. Nothing unusual
- Filtered using FTP packets The following contained user and PASS commands. This signifies that there was login activity on the server.

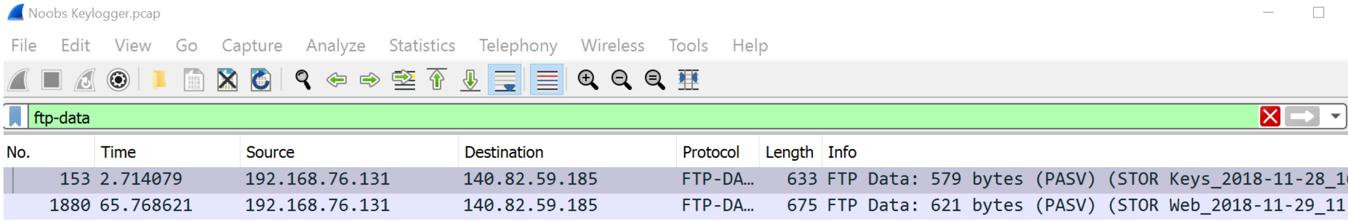


ftp

```
No.    Time        Source          Destination     Protocol Length Info
    66 0.592799    140.82.59.185   192.168.76.131  FTP       74 Response: 220 (vsFTPd 3.0.3)
    70 0.605028    192.168.76.131  140.82.59.185   FTP       70 Request: USER test_user
    90 0.878781    140.82.59.185   192.168.76.131  FTP       88 Response: 331 Please specify the password.
    96 0.879254    192.168.76.131  140.82.59.185   FTP       70 Request: PASS Nipun@123
   112 1.156054    140.82.59.185   192.168.76.131  FTP       77 Response: 230 Login successful.
   114 1.174831    192.168.76.131  140.82.59.185   FTP       64 Request: CWD Test
   118 1.442079    140.82.59.185   192.168.76.131  FTP       91 Response: 250 Directory successfully changed.
   121 1.460144    192.168.76.131  140.82.59.185   FTP       62 Request: TYPE I
   125 1.803554    140.82.59.185   192.168.76.131  FTP       85 Response: 200 Switching to Binary mode.
   127 1.804769    192.168.76.131  140.82.59.185   FTP       60 Request: PASV
   135 2.076864    140.82.59.185   192.168.76.131  FTP      103 Response: 227 Entering Passive Mode (140,82,59,185,72,7
   145 2.446646    192.168.76.131  140.82.59.185   FTP       90 Request: STOR Keys_2018-11-28_16-04-42.html
   151 2.713115    140.82.59.185   192.168.76.131  FTP       76 Response: 150 Ok to send data.
   160 3.336649    140.82.59.185   192.168.76.131  FTP       78 Response: 226 Transfer complete.
  1806 63.915650   140.82.59.185   192.168.76.131  FTP       74 Response: 220 (vsFTPd 3.0.3)
  1808 63.916668   192.168.76.131  140.82.59.185   FTP       70 Request: USER test_user
  1822 64.175064   140.82.59.185   192.168.76.131  FTP       88 Response: 331 Please specify the password.
  1824 64.176059   192.168.76.131  140.82.59.185   FTP       70 Request: PASS Nipun@123
  1831 64.452312   140.82.59.185   192.168.76.131  FTP       77 Response: 230 Login successful.
  1833 64.453422   192.168.76.131  140.82.59.185   FTP       64 Request: CWD Test
  1839 64.728234   140.82.59.185   192.168.76.131  FTP       91 Response: 250 Directory successfully changed.
  1841 64.729012   192.168.76.131  140.82.59.185   FTP       62 Request: TYPE I
  1849 64.987663   140.82.59.185   192.168.76.131  FTP       85 Response: 200 Switching to Binary mode.
  1851 64.993598   192.168.76.131  140.82.59.185   FTP       60 Request: PASV
  1860 65.249370   140.82.59.185   192.168.76.131  FTP      104 Response: 227 Entering Passive Mode (140,82,59,185,20,2
  1866 65.502663   192.168.76.131  140.82.59.185   FTP       89 Request: STOR Web_2018-11-29_11-28-13.html
  1878 65.767264   140.82.59.185   192.168.76.131  FTP       76 Response: 150 Ok to send data.
  1895 66.252580   140.82.59.185   192.168.76.131  FTP       78 Response: 226 Transfer complete.
```

File Transfer Protocol (FTP): Protocol | Packets: 2197 · Displayed: 28 (1.3%) | Profile: Default

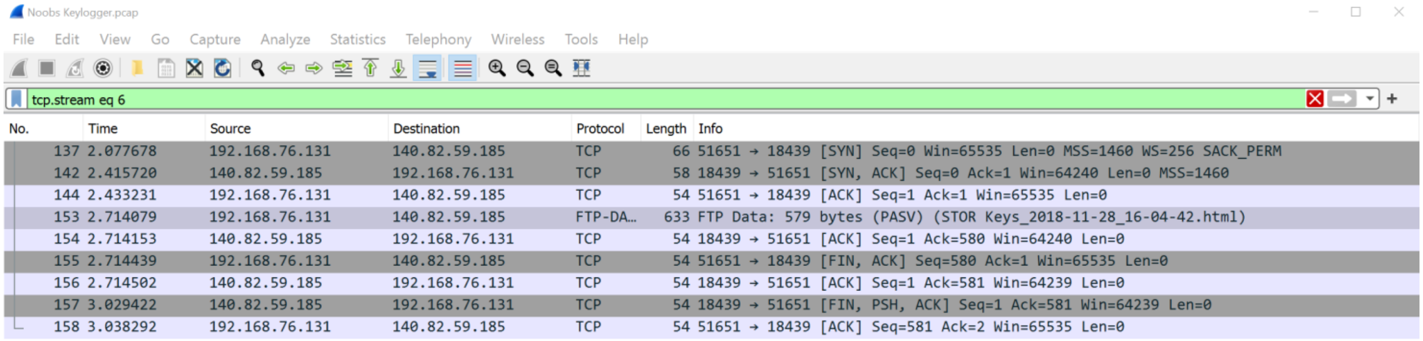
- Filtered using ftp-data. The following results appeared: This filtration only displays files and data transferred.


Noobs Keylogger.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ftp-data

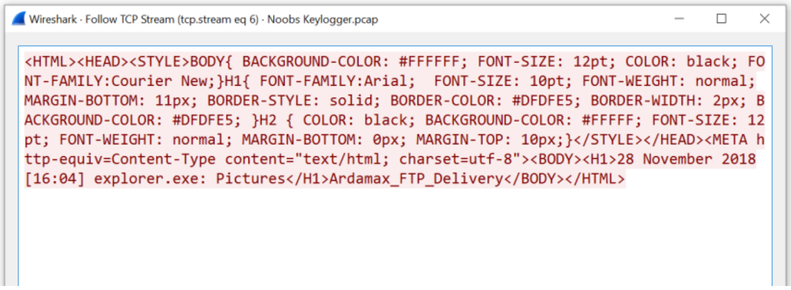
| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 153 | 2.714079 | 192.168.76.131 | 140.82.59.185 | FTP-DA… | 633 | FTP Data: 579 bytes (PASV) (STOR Keys_2018-11-28_1 |
| 1880 | 65.768621 | 192.168.76.131 | 140.82.59.185 | FTP-DA… | 675 | FTP Data: 621 bytes (PASV) (STOR Web_2018-11-29_11 |

- I opened the TCP stream of the packet and was shown the following data: From here, the data is transferred to Network Miner.


Noobs Keylogger.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

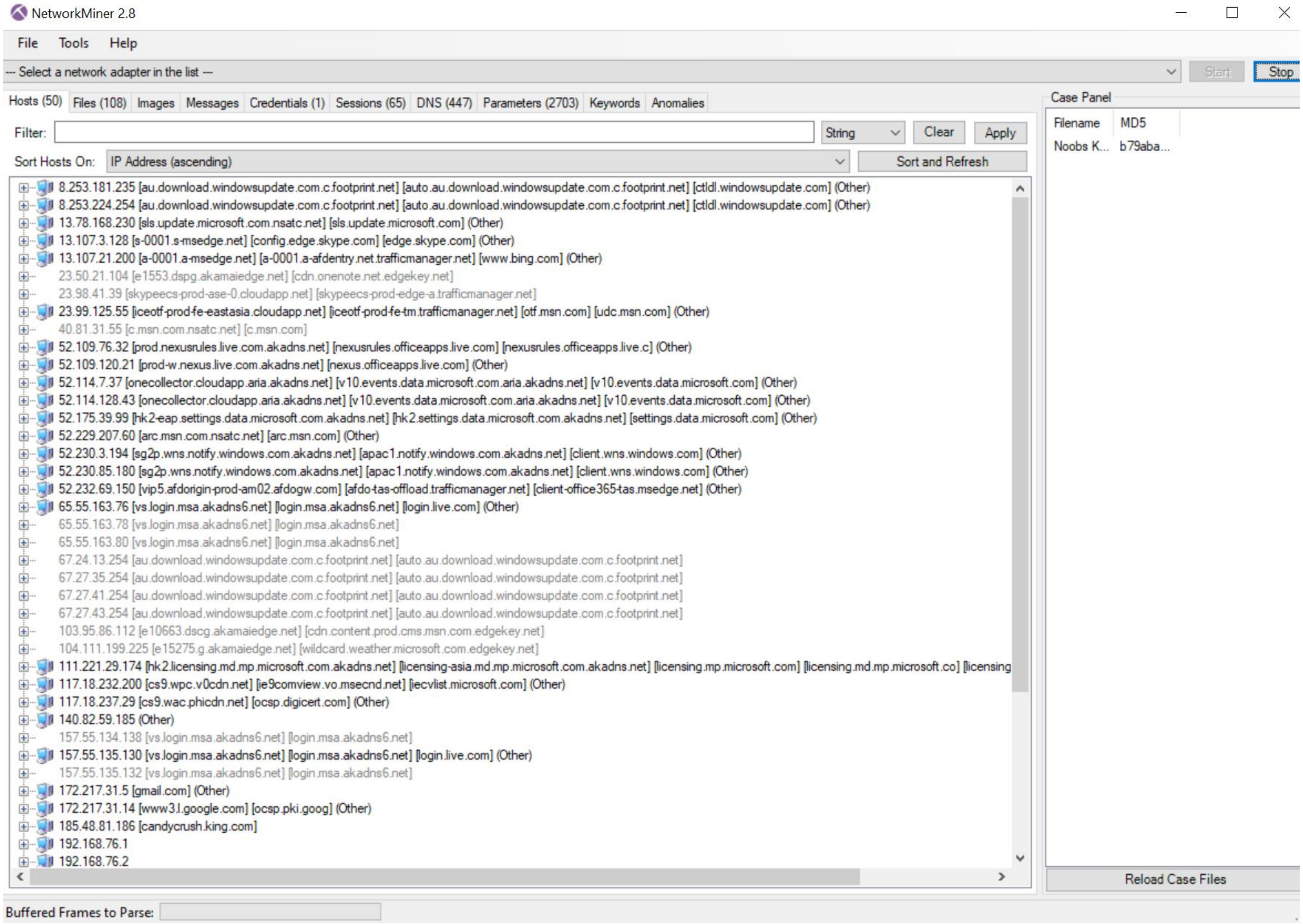
tcp.stream eq 6

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 137 | 2.077678 | 192.168.76.131 | 140.82.59.185 | TCP | 66 | 51651 → 18439 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM |
| 142 | 2.415720 | 140.82.59.185 | 192.168.76.131 | TCP | 58 | 18439 → 51651 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 |
| 144 | 2.433231 | 192.168.76.131 | 140.82.59.185 | TCP | 54 | 51651 → 18439 [ACK] Seq=1 Ack=1 Win=65535 Len=0 |
| 153 | 2.714079 | 192.168.76.131 | 140.82.59.185 | FTP-DA… | 633 | FTP Data: 579 bytes (PASV) (STOR Keys_2018-11-28_16-04-42.html) |
| 154 | 2.714153 | 140.82.59.185 | 192.168.76.131 | TCP | 54 | 18439 → 51651 [ACK] Seq=1 Ack=580 Win=64240 Len=0 |
| 155 | 2.714439 | 192.168.76.131 | 140.82.59.185 | TCP | 54 | 51651 → 18439 [FIN, ACK] Seq=580 Ack=1 Win=65535 Len=0 |
| 156 | 2.714502 | 140.82.59.185 | 192.168.76.131 | TCP | 54 | 18439 → 51651 [ACK] Seq=1 Ack=581 Win=64239 Len=0 |
| 157 | 3.029422 | 140.82.59.185 | 192.168.76.131 | TCP | 54 | 18439 → 51651 [FIN, PSH, ACK] Seq=1 Ack=581 Win=64239 Len=0 |
| 158 | 3.038292 | 192.168.76.131 | 140.82.59.185 | TCP | 54 | 51651 → 18439 [ACK] Seq=581 Ack=2 Win=65535 Len=0 |


Wireshark · Follow TCP Stream (tcp.stream eq 6) · Noobs Keylogger.pcap

```
<HTML><HEAD><STYLE>BODY{ BACKGROUND-COLOR: #FFFFFF; FONT-SIZE: 12pt; COLOR: black; FO
NT-FAMILY:Courier New;}H1{ FONT-FAMILY:Arial;  FONT-SIZE: 10pt; FONT-WEIGHT: normal;
MARGIN-BOTTOM: 11px; BORDER-STYLE: solid; BORDER-COLOR: #DFDFE5; BORDER-WIDTH: 2px; B
ACKGROUND-COLOR: #DFDFE5; }H2 { COLOR: black; BACKGROUND-COLOR: #FFFFFF; FONT-SIZE: 12
pt; FONT-WEIGHT: normal; MARGIN-BOTTOM: 0px; MARGIN-TOP: 10px;}</STYLE></HEAD><META h
ttp-equiv=Content-Type content="text/html; charset=utf-8"><BODY><H1>28 November 2018
[16:04] explorer.exe: Pictures</H1>Ardamax_FTP_Delivery</BODY></HTML>
```

- After opening the pcap file through Network Miner, the results displayed all the hosts within the capture.



--- Select a network adapter in the list ---

Filter: String

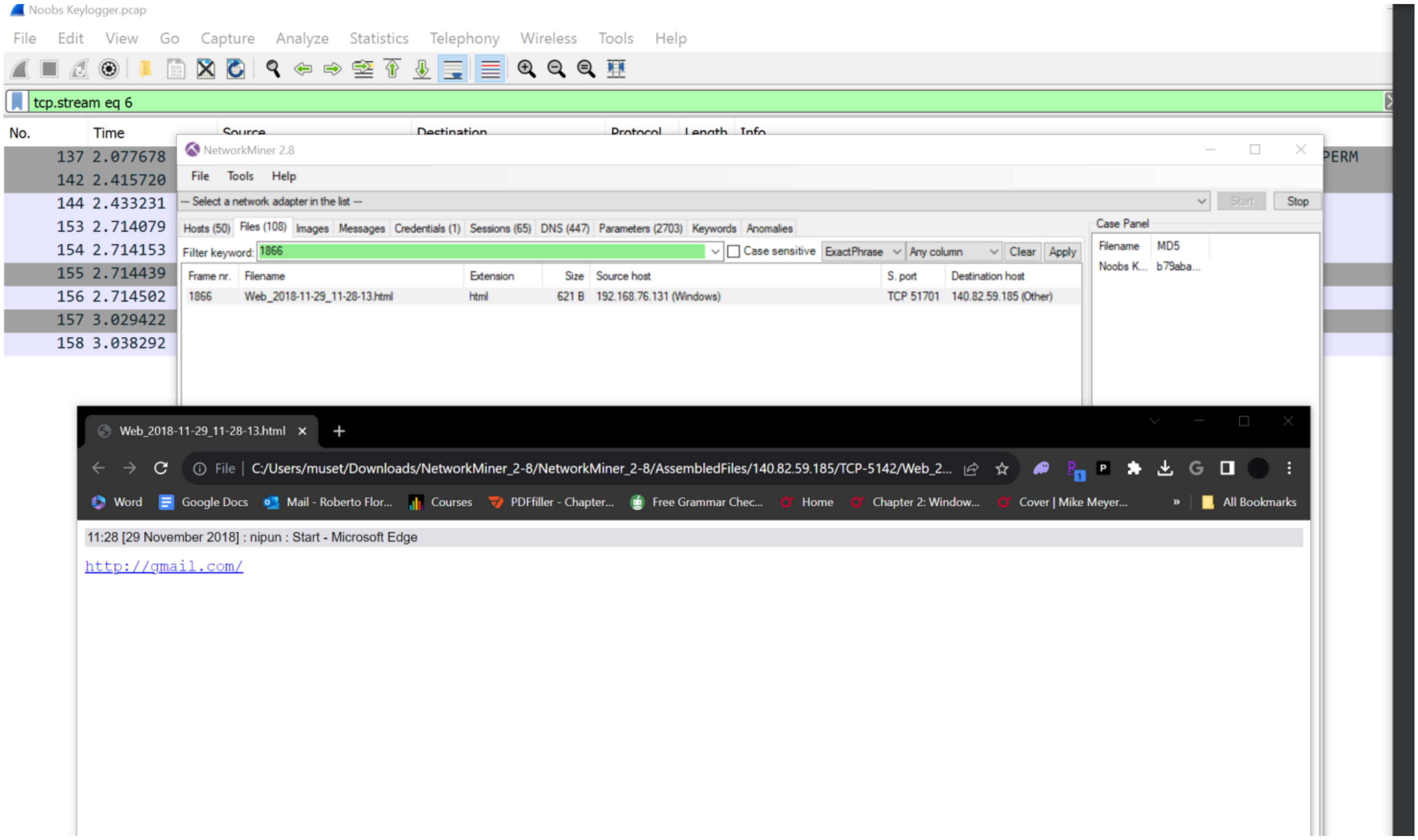
Sort Hosts On: IP Address (ascending)

```
8.253.181.235 [au.download.windowsupdate.com.c.footprint.net] [auto.au.download.windowsupdate.com.c.footprint.net] [ctldl.windowsupdate.com] (Other)
8.253.224.254 [au.download.windowsupdate.com.c.footprint.net] [auto.au.download.windowsupdate.com.c.footprint.net] [ctldl.windowsupdate.com] (Other)
13.78.168.230 [sls.update.microsoft.com.nsatc.net] [sls.update.microsoft.com] (Other)
13.107.3.128 [s-0001.s-msedge.net] [config.edge.skype.com] [edge.skype.com] (Other)
13.107.21.200 [a-0001.a-msedge.net] [a-0001.a-afdentry.net.trafficmanager.net] [www.bing.com] (Other)
23.50.21.104 [e1553.dspg.akamaiedge.net] [cdn.onenote.net.edgekey.net]
23.98.41.39 [skypeecs-prod-ase-0.cloudapp.net] [skypeecs-prod-edge-a.trafficmanager.net]
23.99.125.55 [iceotf-prod-fe-eastasia.cloudapp.net] [iceotf-prod-fe-tm.trafficmanager.net] [otf.msn.com] [udc.msn.com] (Other)
40.81.31.55 [c.msn.com.nsatc.net] [c.msn.com]
52.109.76.32 [prod.nexusrules.live.com.akadns.net] [nexusrules.officeapps.live.com] [nexusrules.officeapps.live.c] (Other)
52.109.120.21 [prod-w.nexus.live.com.akadns.net] [nexus.officeapps.live.com] (Other)
52.114.7.37 [onecollector.cloudapp.aria.akadns.net] [v10.events.data.microsoft.com.aria.akadns.net] [v10.events.data.microsoft.com] (Other)
52.114.128.43 [onecollector.cloudapp.aria.akadns.net] [v10.events.data.microsoft.com.aria.akadns.net] [v10.events.data.microsoft.com] (Other)
52.175.39.99 [hk2-eap.settings.data.microsoft.com.akadns.net] [hk2.settings.data.microsoft.com.akadns.net] [settings.data.microsoft.com] (Other)
52.229.207.60 [arc.msn.com.nsatc.net] [arc.msn.com] (Other)
52.230.3.194 [sg2p.wns.notify.windows.com.akadns.net] [apac1.notify.windows.com.akadns.net] [client.wns.windows.com] (Other)
52.230.85.180 [sg2p.wns.notify.windows.com.akadns.net] [apac1.notify.windows.com.akadns.net] [client.wns.windows.com] (Other)
52.232.69.150 [vip5.afdorigin-prod-am02.afdogw.com] [afdo-tas-offload.trafficmanager.net] [client-office365-tas.msedge.net] (Other)
65.55.163.76 [vs.login.msa.akadns6.net] [login.msa.akadns6.net] [login.live.com] (Other)
65.55.163.78 [vs.login.msa.akadns6.net] [login.msa.akadns6.net]
65.55.163.80 [vs.login.msa.akadns6.net] [login.msa.akadns6.net]
67.24.13.254 [au.download.windowsupdate.com.c.footprint.net] [auto.au.download.windowsupdate.com.c.footprint.net]
67.27.35.254 [au.download.windowsupdate.com.c.footprint.net] [auto.au.download.windowsupdate.com.c.footprint.net]
67.27.41.254 [au.download.windowsupdate.com.c.footprint.net] [auto.au.download.windowsupdate.com.c.footprint.net]
67.27.43.254 [au.download.windowsupdate.com.c.footprint.net] [auto.au.download.windowsupdate.com.c.footprint.net]
103.95.86.112 [e10663.dscg.akamaiedge.net] [cdn.content.prod.cms.msn.com.edgekey.net]
104.111.199.225 [e15275.g.akamaiedge.net] [wildcard.weather.microsoft.com.edgekey.net]
111.221.29.174 [hk2.licensing.md.mp.microsoft.com.akadns.net] [licensing-asia.md.mp.microsoft.com.akadns.net] [licensing.mp.microsoft.com] [licensing.md.mp.microsoft.co] [licensing
117.18.232.200 [cs9.wpc.v0cdn.net] [ie9comview.vo.msecnd.net] [iecvlist.microsoft.com] (Other)
117.18.237.29 [cs9.wac.phicdn.net] [ocsp.digicert.com] (Other)
140.82.59.185 (Other)
157.55.134.138 [vs.login.msa.akadns6.net] [login.msa.akadns6.net]
157.55.135.130 [vs.login.msa.akadns6.net] [login.msa.akadns6.net] [login.live.com] (Other)
157.55.135.132 [vs.login.msa.akadns6.net] [login.msa.akadns6.net]
172.217.31.5 [gmail.com] (Other)
172.217.31.14 [www3.l.google.com] [ocsp.pki.goog] (Other)
185.48.81.186 [candycrush.king.com]
192.168.76.1
192.168.76.2
```

| Filename | MD5 |
|---|---|
| Noobs K... | b79aba... |

Buffered Frames to Parse:

- I filtered all the files and used the STOR command. After completing all the steps, the following information revealed the infected system, server, frequent data, and files that the attacker had sent.
- The last portion of the lab doesn't allow access to the server, but the pdf shows how simple it was to login and expose information regarding the attacker.



Noobs Keylogger.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 6

```
No.   Time
  137 2.077678
  142 2.415720
  144 2.433231
  153 2.714079
  154 2.714153
  155 2.714439
  156 2.714502
  157 3.029422
  158 3.038292
```

NetworkMiner 2.8
File Tools Help
-- Select a network adapter in the list --
Start
Stop
Hosts (50) Files (108) Images Messages Credentials (1) Sessions (65) DNS (447) Parameters (2703) Keywords Anomalies

Filter keyword: 1866 ☐ Case sensitive ExactPhrase Any column Clear Apply

| Frame nr. | Filename | Extension | Size | Source host | S. port | Destination host |
|---|---|---|---|---|---|---|
| 1866 | Web_2018-11-29_11-28-13.html | html | 621 B | 192.168.76.131 (Windows) | TCP 51701 | 140.82.59.185 (Other) |

Case Panel

| Filename | MD5 |
|---|---|
| Noobs K... | b79aba... |

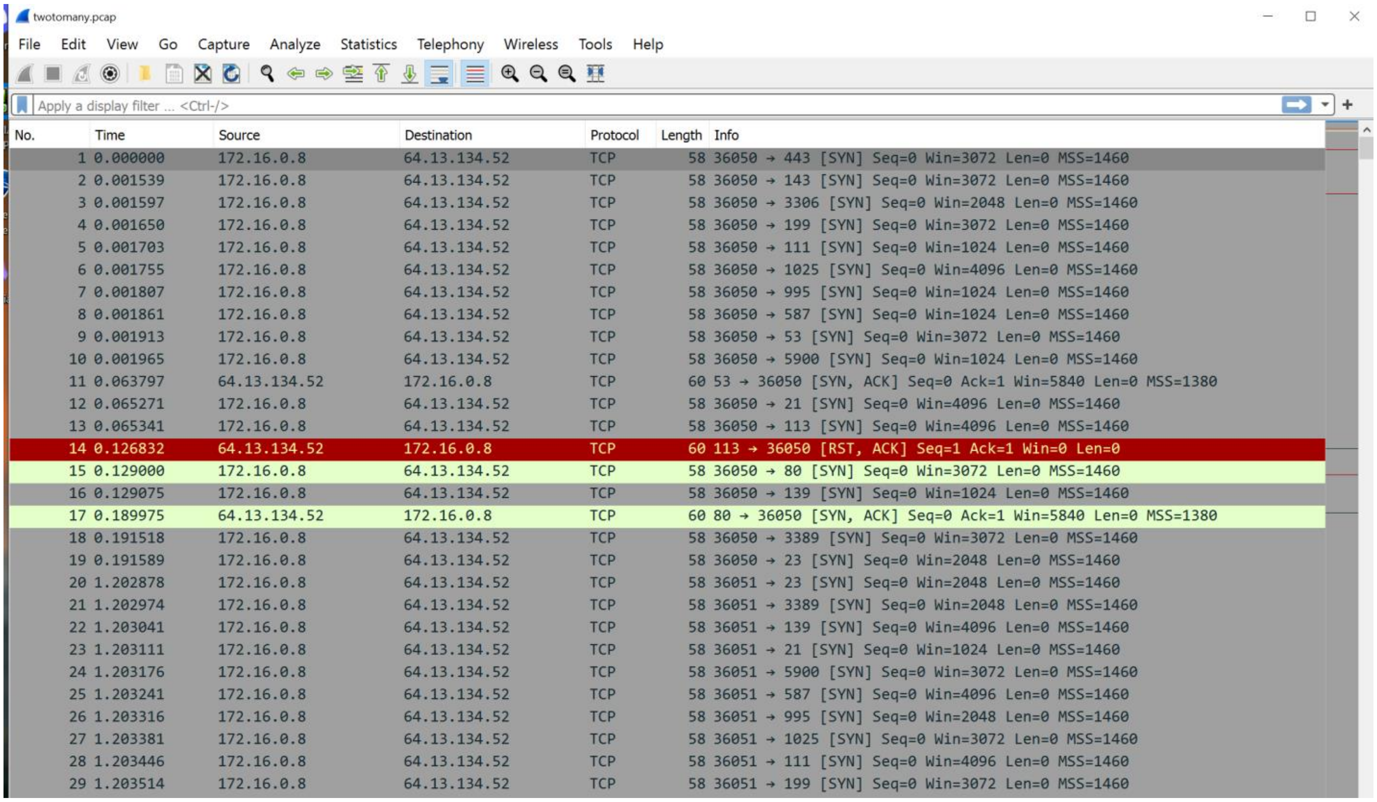
C:/Users/muset/Downloads/NetworkMiner_2-8/NetworkMiner_2-8/AssembledFiles/140.82.59.185/TCP-5142/Web_2...

11:28 [29 November 2018] : nipun : Start - Microsoft Edge

http://gmail.com/

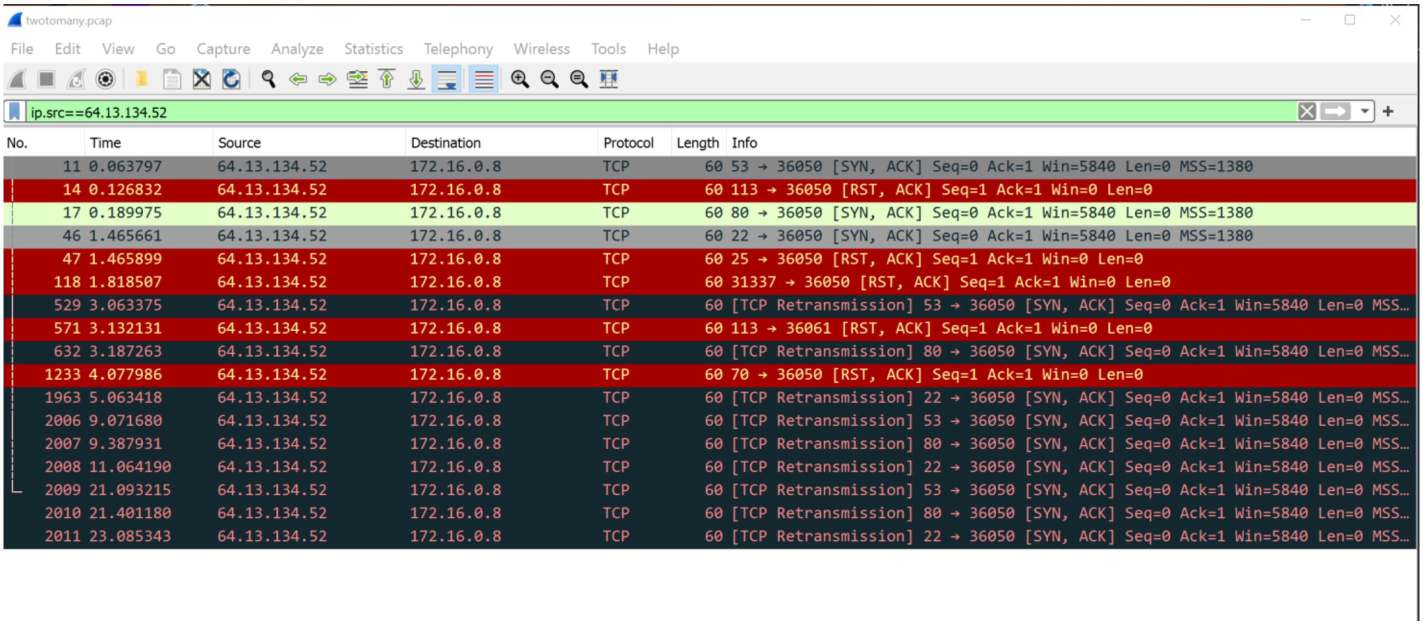
## Exercise 2 – Two too many

- I opened another pcap file using Wireshark.
- The following file displays SYN packets being sent out from the following IP address (64.13.134.52).



| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000 | 172.16.0.8 | 64.13.134.52 | TCP | 58 | 36050 → 443 [SYN] Seq=0 Win=3072 Len=0 MSS=1460 |
| 2 | 0.001539 | 172.16.0.8 | 64.13.134.52 | TCP | 58 | 36050 → 143 [SYN] Seq=0 Win=3072 Len=0 MSS=1460 |
| 3 | 0.001597 | 172.16.0.8 | 64.13.134.52 | TCP | 58 | 36050 → 3306 [SYN] Seq=0 Win=2048 Len=0 MSS=1460 |
| 4 | 0.001650 | 172.16.0.8 | 64.13.134.52 | TCP | 58 | 36050 → 199 [SYN] Seq=0 Win=3072 Len=0 MSS=1460 |
| 5 | 0.001703 | 172.16.0.8 | 64.13.134.52 | TCP | 58 | 36050 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460 |
| 6 | 0.001755 | 172.16.0.8 | 64.13.134.52 | TCP | 58 | 36050 → 1025 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 |
| 7 | 0.001807 | 172.16.0.8 | 64.13.134.52 | TCP | 58 | 36050 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460 |
| 8 | 0.001861 | 172.16.0.8 | 64.13.134.52 | TCP | 58 | 36050 → 587 [SYN] Seq=0 Win=1024 Len=0 MSS=1460 |
| 9 | 0.001913 | 172.16.0.8 | 64.13.134.52 | TCP | 58 | 36050 → 53 [SYN] Seq=0 Win=3072 Len=0 MSS=1460 |
| 10 | 0.001965 | 172.16.0.8 | 64.13.134.52 | TCP | 58 | 36050 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460 |
| 11 | 0.063797 | 64.13.134.52 | 172.16.0.8 | TCP | 60 | 53 → 36050 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 |
| 12 | 0.065271 | 172.16.0.8 | 64.13.134.52 | TCP | 58 | 36050 → 21 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 |
| 13 | 0.065341 | 172.16.0.8 | 64.13.134.52 | TCP | 58 | 36050 → 113 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 |
| 14 | 0.126832 | 64.13.134.52 | 172.16.0.8 | TCP | 60 | 113 → 36050 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 15 | 0.129000 | 172.16.0.8 | 64.13.134.52 | TCP | 58 | 36050 → 80 [SYN] Seq=0 Win=3072 Len=0 MSS=1460 |
| 16 | 0.129075 | 172.16.0.8 | 64.13.134.52 | TCP | 58 | 36050 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460 |
| 17 | 0.189975 | 64.13.134.52 | 172.16.0.8 | TCP | 60 | 80 → 36050 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 |
| 18 | 0.191518 | 172.16.0.8 | 64.13.134.52 | TCP | 58 | 36050 → 3389 [SYN] Seq=0 Win=3072 Len=0 MSS=1460 |
| 19 | 0.191589 | 172.16.0.8 | 64.13.134.52 | TCP | 58 | 36050 → 23 [SYN] Seq=0 Win=2048 Len=0 MSS=1460 |
| 20 | 1.202878 | 172.16.0.8 | 64.13.134.52 | TCP | 58 | 36050 → 23 [SYN] Seq=0 Win=2048 Len=0 MSS=1460 |
| 21 | 1.202974 | 172.16.0.8 | 64.13.134.52 | TCP | 58 | 36051 → 3389 [SYN] Seq=0 Win=2048 Len=0 MSS=1460 |
| 22 | 1.203041 | 172.16.0.8 | 64.13.134.52 | TCP | 58 | 36051 → 139 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 |
| 23 | 1.203111 | 172.16.0.8 | 64.13.134.52 | TCP | 58 | 36051 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460 |
| 24 | 1.203176 | 172.16.0.8 | 64.13.134.52 | TCP | 58 | 36051 → 5900 [SYN] Seq=0 Win=3072 Len=0 MSS=1460 |
| 25 | 1.203241 | 172.16.0.8 | 64.13.134.52 | TCP | 58 | 36051 → 587 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 |
| 26 | 1.203316 | 172.16.0.8 | 64.13.134.52 | TCP | 58 | 36051 → 995 [SYN] Seq=0 Win=2048 Len=0 MSS=1460 |
| 27 | 1.203381 | 172.16.0.8 | 64.13.134.52 | TCP | 58 | 36051 → 1025 [SYN] Seq=0 Win=3072 Len=0 MSS=1460 |
| 28 | 1.203446 | 172.16.0.8 | 64.13.134.52 | TCP | 58 | 36051 → 111 [SYN] Seq=0 Win=4096 Len=0 MSS=1460 |
| 29 | 1.203514 | 172.16.0.8 | 64.13.134.52 | TCP | 58 | 36051 → 199 [SYN] Seq=0 Win=3072 Len=0 MSS=1460 |

- In order to find the last section of the three-way handshake, applying the following filter will display the responses sent from the suspected IP address (64.13.134.52).
- The results display the SYN/ACK information from ports 53, 80, and 22, which are open ports. Additionally, I can also see the cases in which there has been a network loss, and the sender has retried to send the following packets.



ip.src==64.13.134.52

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 11 | 0.063797 | 64.13.134.52 | 172.16.0.8 | TCP | 60 | 53 → 36050 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 |
| 14 | 0.126832 | 64.13.134.52 | 172.16.0.8 | TCP | 60 | 113 → 36050 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 17 | 0.189975 | 64.13.134.52 | 172.16.0.8 | TCP | 60 | 80 → 36050 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 |
| 46 | 1.465661 | 64.13.134.52 | 172.16.0.8 | TCP | 60 | 22 → 36050 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 |
| 47 | 1.465899 | 64.13.134.52 | 172.16.0.8 | TCP | 60 | 25 → 36050 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 118 | 1.818507 | 64.13.134.52 | 172.16.0.8 | TCP | 60 | 31337 → 36050 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 529 | 3.063375 | 64.13.134.52 | 172.16.0.8 | TCP | 60 | [TCP Retransmission] 53 → 36050 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS… |
| 571 | 3.132131 | 64.13.134.52 | 172.16.0.8 | TCP | 60 | 113 → 36061 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 632 | 3.187263 | 64.13.134.52 | 172.16.0.8 | TCP | 60 | [TCP Retransmission] 80 → 36050 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS… |
| 1233 | 4.077986 | 64.13.134.52 | 172.16.0.8 | TCP | 60 | 70 → 36050 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 1963 | 5.063418 | 64.13.134.52 | 172.16.0.8 | TCP | 60 | [TCP Retransmission] 22 → 36050 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS… |
| 2006 | 9.071680 | 64.13.134.52 | 172.16.0.8 | TCP | 60 | [TCP Retransmission] 53 → 36050 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS… |
| 2007 | 9.387931 | 64.13.134.52 | 172.16.0.8 | TCP | 60 | [TCP Retransmission] 80 → 36050 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS… |
| 2008 | 11.064190 | 64.13.134.52 | 172.16.0.8 | TCP | 60 | [TCP Retransmission] 22 → 36050 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS… |
| 2009 | 21.093215 | 64.13.134.52 | 172.16.0.8 | TCP | 60 | [TCP Retransmission] 53 → 36050 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS… |
| 2010 | 21.401180 | 64.13.134.52 | 172.16.0.8 | TCP | 60 | [TCP Retransmission] 80 → 36050 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS… |
| 2011 | 23.085343 | 64.13.134.52 | 172.16.0.8 | TCP | 60 | [TCP Retransmission] 22 → 36050 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS… |