Digital Forensics Assignment 2:

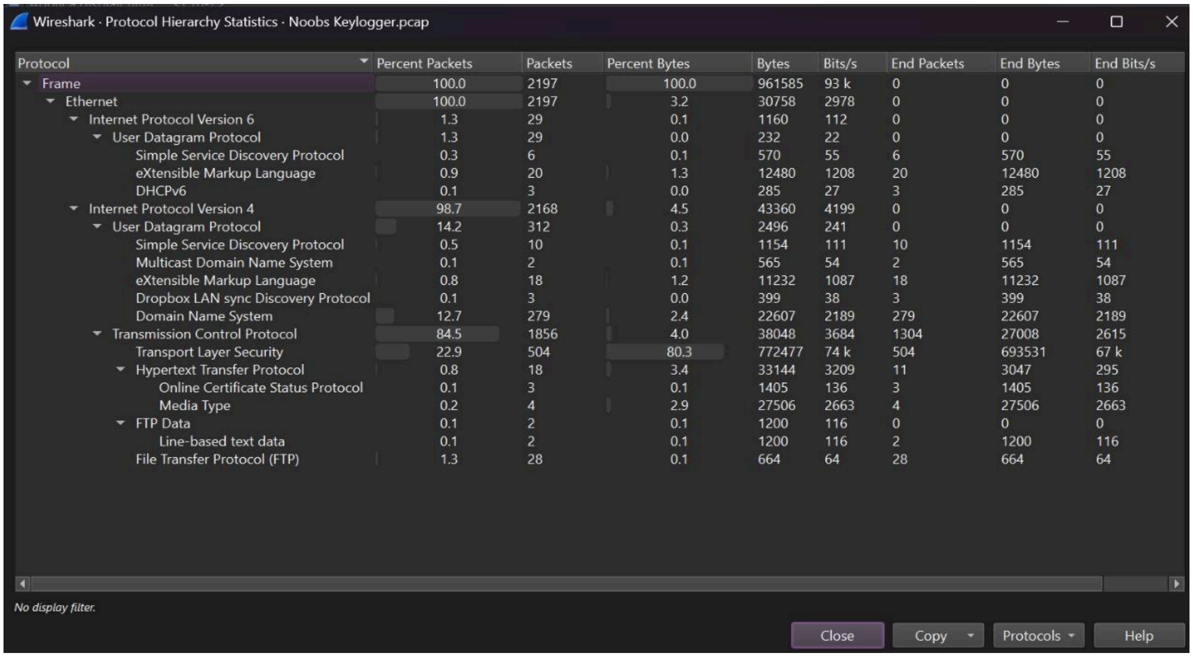
Ammar Hassona (10006003) (T14)

Ahmed Mohamed Hegab (10005393) (T11)

Question 1:

Task 1 –

a,b)



Wireshark · Protocol Hierarchy Statistics · Noobs Keylogger.pcap
Close
Copy
Protocols
Help

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	2197	100.0	961585	93 k	0	0	0
Ethernet	100.0	2197	3.2	30758	2978	0	0	0
Internet Protocol Version 6	1.3	29	0.1	1160	112	0	0	0
User Datagram Protocol	1.3	29	0.0	232	22	0	0	0
Simple Service Discovery Protocol	0.3	6	0.1	570	55	6	570	55
eXtensible Markup Language	0.9	20	1.3	12480	1208	20	12480	1208
DHCPv6	0.1	3	0.0	285	27	3	285	27
Internet Protocol Version 4	98.7	2168	4.5	43360	4199	0	0	0
User Datagram Protocol	14.2	312	0.3	2496	241	0	0	0
Simple Service Discovery Protocol	0.5	10	0.1	1154	111	10	1154	111
Multicast Domain Name System	0.1	2	0.1	565	54	2	565	54
eXtensible Markup Language	0.8	18	1.2	11232	1087	18	11232	1087
Dropbox LAN sync Discovery Protocol	0.1	3	0.0	399	38	3	399	38
Domain Name System	12.7	279	2.4	22607	2189	279	22607	2189
Transmission Control Protocol	84.5	1856	4.0	38048	3684	1304	27008	2615
Transport Layer Security	22.9	504	80.3	772477	74 k	504	693531	67 k
Hypertext Transfer Protocol	0.8	18	3.4	33144	3209	11	3047	295
Online Certificate Status Protocol	0.1	3	0.1	1405	136	3	1405	136
Media Type	0.2	4	2.9	27506	2663	4	27506	2663
FTP Data	0.1	2	0.1	1200	116	0	0	0
Line-based text data	0.1	2	0.1	1200	116	2	1200	116
File Transfer Protocol (FTP)	1.3	28	0.1	664	64	28	664	64

No display filter.

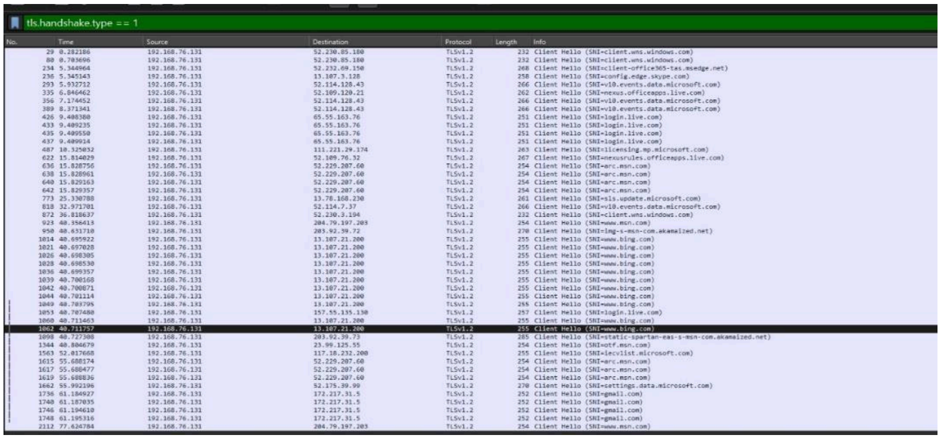
c)

Top 3 protocols by percentage of traffic:

- Transport Layer Security (TLS): 80.3% of bytes (772,477 / 961,585)
- Hypertext Transfer Protocol (HTTP): 3.4% of bytes (33,144 / 961,585)
- Domain Name System (DNS): 2.4% of bytes (22,607 / 961,585)

d)

- Domain Names:

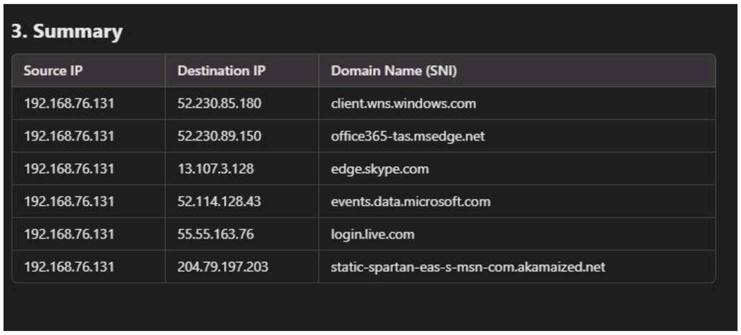


tls.handshake.type == 1

No.	Time	Source	Destination	Protocol	Length	Info
29	0.282186	192.168.76.131	52.230.85.180	TLSv1.2	232	Client Hello (SNI=client.wns.windows.com)
80	0.703696	192.168.76.131	52.230.85.180	TLSv1.2	232	Client Hello (SNI=client.wns.windows.com)
234	5.344964	192.168.76.131	52.232.69.150	TLSv1.2	268	Client Hello (SNI=client-office365-tas.msedge.net)
236	5.345143	192.168.76.131	13.107.3.128	TLSv1.2	258	Client Hello (SNI=config.edge.skype.com)
293	5.932712	192.168.76.131	52.114.128.43	TLSv1.2	266	Client Hello (SNI=v10.events.data.microsoft.com)
335	6.846462	192.168.76.131	52.109.120.21	TLSv1.2	262	Client Hello (SNI=nexus.officeapps.live.com)
356	7.174452	192.168.76.131	52.114.128.43	TLSv1.2	266	Client Hello (SNI=v10.events.data.microsoft.com)
389	8.371341	192.168.76.131	52.114.128.43	TLSv1.2	266	Client Hello (SNI=v10.events.data.microsoft.com)
426	9.408380	192.168.76.131	65.55.163.76	TLSv1.2	251	Client Hello (SNI=login.live.com)
433	9.409235	192.168.76.131	65.55.163.76	TLSv1.2	251	Client Hello (SNI=login.live.com)
435	9.409550	192.168.76.131	65.55.163.76	TLSv1.2	251	Client Hello (SNI=login.live.com)
437	9.409914	192.168.76.131	65.55.163.76	TLSv1.2	251	Client Hello (SNI=login.live.com)
487	10.325032	192.168.76.131	111.221.29.174	TLSv1.2	263	Client Hello (SNI=licensing.mp.microsoft.com)
622	15.814029	192.168.76.131	52.109.76.32	TLSv1.2	267	Client Hello (SNI=nexusrules.officeapps.live.com)
636	15.828756	192.168.76.131	52.229.207.60	TLSv1.2	254	Client Hello (SNI=arc.msn.com)
638	15.828961	192.168.76.131	52.229.207.60	TLSv1.2	254	Client Hello (SNI=arc.msn.com)
640	15.829163	192.168.76.131	52.229.207.60	TLSv1.2	254	Client Hello (SNI=arc.msn.com)
642	15.829357	192.168.76.131	52.229.207.60	TLSv1.2	254	Client Hello (SNI=arc.msn.com)
773	25.330788	192.168.76.131	13.78.168.230	TLSv1.2	261	Client Hello (SNI=sls.update.microsoft.com)
818	32.971701	192.168.76.131	52.114.7.37	TLSv1.2	266	Client Hello (SNI=v10.events.data.microsoft.com)
872	36.818637	192.168.76.131	52.230.3.194	TLSv1.2	232	Client Hello (SNI=client.wns.windows.com)
923	40.356413	192.168.76.131	204.79.197.203	TLSv1.2	254	Client Hello (SNI=www.msn.com)
950	40.631710	192.168.76.131	203.92.39.72	TLSv1.2	270	Client Hello (SNI=img-s-msn-com.akamaized.net)
1014	40.695922	192.168.76.131	13.107.21.200	TLSv1.2	255	Client Hello (SNI=www.bing.com)
1021	40.697028	192.168.76.131	13.107.21.200	TLSv1.2	255	Client Hello (SNI=www.bing.com)
1026	40.698305	192.168.76.131	13.107.21.200	TLSv1.2	255	Client Hello (SNI=www.bing.com)
1028	40.698530	192.168.76.131	13.107.21.200	TLSv1.2	255	Client Hello (SNI=www.bing.com)
1036	40.699357	192.168.76.131	13.107.21.200	TLSv1.2	255	Client Hello (SNI=www.bing.com)
1039	40.700168	192.168.76.131	13.107.21.200	TLSv1.2	255	Client Hello (SNI=www.bing.com)
1042	40.700871	192.168.76.131	13.107.21.200	TLSv1.2	255	Client Hello (SNI=www.bing.com)
1044	40.701114	192.168.76.131	13.107.21.200	TLSv1.2	255	Client Hello (SNI=www.bing.com)
1049	40.703795	192.168.76.131	13.107.21.200	TLSv1.2	255	Client Hello (SNI=www.bing.com)
1053	40.707480	192.168.76.131	157.55.135.130	TLSv1.2	257	Client Hello (SNI=login.live.com)
1060	40.711463	192.168.76.131	13.107.21.200	TLSv1.2	255	Client Hello (SNI=www.bing.com)
1062	40.711757	192.168.76.131	13.107.21.200	TLSv1.2	255	Client Hello (SNI=www.bing.com)
1098	40.727308	192.168.76.131	203.92.39.73	TLSv1.2	285	Client Hello (SNI=static-spartan-eas-s-msn-com.akamaized.net)
1344	40.804679	192.168.76.131	23.99.125.55	TLSv1.2	254	Client Hello (SNI=otf.msn.com)
1563	52.017668	192.168.76.131	117.18.232.200	TLSv1.2	255	Client Hello (SNI=iecvlist.microsoft.com)
1615	55.688174	192.168.76.131	52.229.207.60	TLSv1.2	254	Client Hello (SNI=arc.msn.com)
1617	55.688477	192.168.76.131	52.229.207.60	TLSv1.2	254	Client Hello (SNI=arc.msn.com)
1619	55.688836	192.168.76.131	52.229.207.60	TLSv1.2	254	Client Hello (SNI=arc.msn.com)
1662	55.992196	192.168.76.131	52.175.39.99	TLSv1.2	270	Client Hello (SNI=settings.data.microsoft.com)
1736	61.184927	192.168.76.131	172.217.31.5	TLSv1.2	252	Client Hello (SNI=gmail.com)
1740	61.187035	192.168.76.131	172.217.31.5	TLSv1.2	252	Client Hello (SNI=gmail.com)
1746	61.194610	192.168.76.131	172.217.31.5	TLSv1.2	252	Client Hello (SNI=gmail.com)
1748	61.195316	192.168.76.131	172.217.31.5	TLSv1.2	252	Client Hello (SNI=gmail.com)
2112	77.624784	192.168.76.131	204.79.197.203	TLSv1.2	254	Client Hello (SNI=www.msn.com)

The filter applied to the TLS protocol is the ‘tls.handshake == 1’ which filters the packets where the client and server establish a communication and isolating all the TLS Client Hello packets.

The protocol TLSv1.2 is the dominant protocol as it is the most frequent packet.

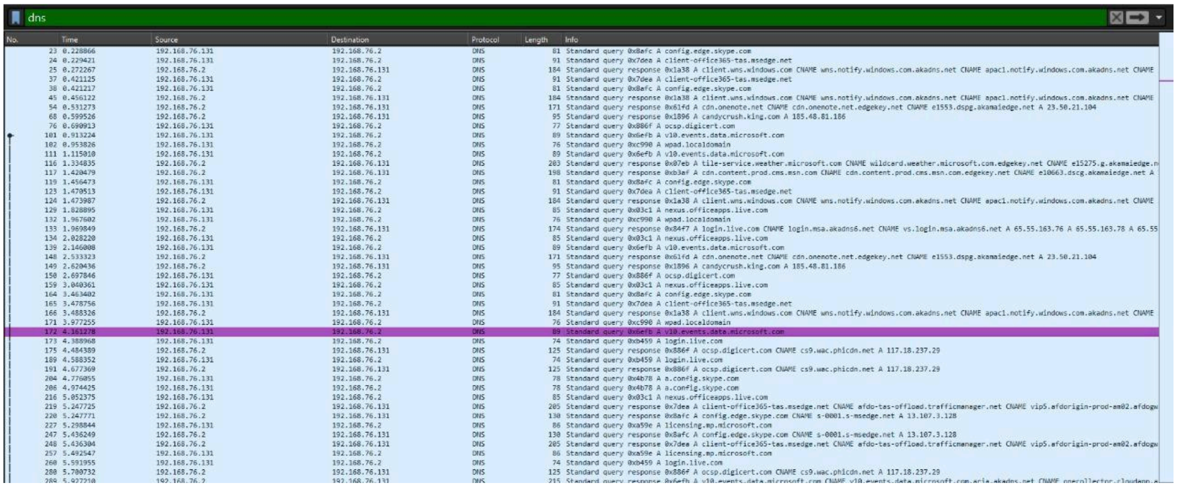


3. Summary

Source IP	Destination IP	Domain Name (SNI)
192.168.76.131	52.230.85.180	client.wns.windows.com
192.168.76.131	52.230.89.150	office365-tas.msedge.net
192.168.76.131	13.107.3.128	edge.skype.com
192.168.76.131	52.114.128.43	events.data.microsoft.com
192.168.76.131	55.55.163.76	login.live.com
192.168.76.131	204.79.197.203	static-spartan-eas-s-msn-com.akamaized.net

TLS domain names

DNS -



```
No.  Time      Source          Destination     Protocol Length Info
 23  0.228866  192.168.76.131  192.168.76.2    DNS       81 Standard query 0x8afc A config.edge.skype.com
 24  0.229421  192.168.76.131  192.168.76.2    DNS       91 Standard query 0x7dea A client-office365-tas.msedge.net
 25  0.272267  192.168.76.2    192.168.76.131  DNS      184 Standard query response 0x1a38 A client.wns.windows.com CNAME wns.notify.windows.com.akadns.net CNAME apac1.notify.windows.com.akadns.net CNAME
 37  0.421125  192.168.76.131  192.168.76.2    DNS       91 Standard query 0x7dea A client-office365-tas.msedge.net
 38  0.421217  192.168.76.131  192.168.76.2    DNS       81 Standard query 0x8afc A config.edge.skype.com
 45  0.456122  192.168.76.2    192.168.76.131  DNS      184 Standard query response 0x1a38 A client.wns.windows.com CNAME wns.notify.windows.com.akadns.net CNAME apac1.notify.windows.com.akadns.net CNAME
 54  0.531273  192.168.76.2    192.168.76.131  DNS      171 Standard query response 0x61fd A cdn.onenote.net CNAME cdn.onenote.net.edgekey.net CNAME e1553.dspg.akamaiedge.net A 23.50.21.104
 68  0.599526  192.168.76.2    192.168.76.131  DNS       95 Standard query response 0x1896 A candycrush.king.com A 185.48.81.186
 76  0.690913  192.168.76.131  192.168.76.2    DNS       77 Standard query 0x886f A ocsp.digicert.com
101  0.913224  192.168.76.131  192.168.76.2    DNS       89 Standard query 0x6efb A v10.events.data.microsoft.com
102  0.953826  192.168.76.131  192.168.76.2    DNS       76 Standard query 0xc990 A wpad.localdomain
111  1.115010  192.168.76.131  192.168.76.2    DNS       89 Standard query 0x6efb A v10.events.data.microsoft.com
116  1.334835  192.168.76.2    192.168.76.131  DNS      203 Standard query response 0x07eb A tile-service.weather.microsoft.com CNAME wildcard.weather.microsoft.com.edgekey.net CNAME e15275.g.akamaiedge.n
117  1.420479  192.168.76.2    192.168.76.131  DNS      198 Standard query response 0xb3af A cdn.content.prod.cms.msn.com CNAME cdn.content.prod.cms.msn.com.edgekey.net CNAME e10663.dscg.akamaiedge.net A
119  1.456473  192.168.76.131  192.168.76.2    DNS       81 Standard query 0x8afc A config.edge.skype.com
123  1.470513  192.168.76.131  192.168.76.2    DNS       91 Standard query 0x7dea A client-office365-tas.msedge.net
124  1.473987  192.168.76.2    192.168.76.131  DNS      184 Standard query response 0x1a38 A client.wns.windows.com CNAME wns.notify.windows.com.akadns.net CNAME apac1.notify.windows.com.akadns.net CNAME
129  1.828895  192.168.76.131  192.168.76.2    DNS       85 Standard query 0x03c1 A nexus.officeapps.live.com
132  1.967602  192.168.76.131  192.168.76.2    DNS       76 Standard query 0xc990 A wpad.localdomain
133  1.969849  192.168.76.2    192.168.76.131  DNS      174 Standard query response 0x84f7 A login.live.com CNAME login.msa.akadns6.net CNAME vs.login.msa.akadns6.net A 65.55.163.76 A 65.55.163.78 A 65.55
134  2.028220  192.168.76.131  192.168.76.2    DNS       85 Standard query 0x03c1 A nexus.officeapps.live.com
139  2.146008  192.168.76.131  192.168.76.2    DNS       89 Standard query 0x6efb A v10.events.data.microsoft.com
148  2.533323  192.168.76.2    192.168.76.131  DNS      171 Standard query response 0x61fd A cdn.onenote.net CNAME cdn.onenote.net.edgekey.net CNAME e1553.dspg.akamaiedge.net A 23.50.21.104
149  2.620436  192.168.76.2    192.168.76.131  DNS       95 Standard query response 0x1896 A candycrush.king.com A 185.48.81.186
150  2.697846  192.168.76.131  192.168.76.2    DNS       77 Standard query 0x886f A ocsp.digicert.com
159  3.040361  192.168.76.131  192.168.76.2    DNS       85 Standard query 0x03c1 A nexus.officeapps.live.com
164  3.463402  192.168.76.131  192.168.76.2    DNS       81 Standard query 0x8afc A config.edge.skype.com
165  3.478756  192.168.76.131  192.168.76.2    DNS       91 Standard query 0x7dea A client-office365-tas.msedge.net
166  3.488326  192.168.76.2    192.168.76.131  DNS      184 Standard query response 0x1a38 A client.wns.windows.com CNAME wns.notify.windows.com.akadns.net CNAME apac1.notify.windows.com.akadns.net CNAME
171  3.977255  192.168.76.131  192.168.76.2    DNS       76 Standard query 0xc990 A wpad.localdomain
172  4.161278  192.168.76.131  192.168.76.2    DNS       89 Standard query 0x6efb A v10.events.data.microsoft.com
173  4.388968  192.168.76.131  192.168.76.2    DNS       74 Standard query 0xb459 A login.live.com
175  4.484389  192.168.76.2    192.168.76.131  DNS      125 Standard query response 0x886f A ocsp.digicert.com CNAME cs9.wac.phicdn.net A 117.18.237.29
189  4.588352  192.168.76.131  192.168.76.2    DNS       74 Standard query 0xb459 A login.live.com
191  4.677369  192.168.76.2    192.168.76.131  DNS      125 Standard query response 0x886f A ocsp.digicert.com CNAME cs9.wac.phicdn.net A 117.18.237.29
204  4.776055  192.168.76.131  192.168.76.2    DNS       78 Standard query 0x4b78 A a.config.skype.com
206  4.974425  192.168.76.131  192.168.76.2    DNS       78 Standard query 0x4b78 A a.config.skype.com
216  5.052375  192.168.76.131  192.168.76.2    DNS       85 Standard query 0x03c1 A nexus.officeapps.live.com
219  5.247725  192.168.76.2    192.168.76.131  DNS      205 Standard query response 0x7dea A client-office365-tas.msedge.net CNAME afdo-tas-offload.trafficmanager.net CNAME vip5.afdorigin-prod-am02.afdogw
220  5.247771  192.168.76.2    192.168.76.131  DNS      130 Standard query response 0x8afc A config.edge.skype.com CNAME s-0001.s-msedge.net A 13.107.3.128
227  5.298844  192.168.76.131  192.168.76.2    DNS       86 Standard query 0xa59e A licensing.mp.microsoft.com
247  5.436249  192.168.76.2    192.168.76.131  DNS      130 Standard query response 0x8afc A config.edge.skype.com CNAME s-0001.s-msedge.net A 13.107.3.128
248  5.436304  192.168.76.2    192.168.76.131  DNS      205 Standard query response 0x7dea A client-office365-tas.msedge.net CNAME afdo-tas-offload.trafficmanager.net CNAME vip5.afdorigin-prod-am02.afdogw
257  5.492547  192.168.76.131  192.168.76.2    DNS       86 Standard query 0xa59e A licensing.mp.microsoft.com
260  5.591955  192.168.76.131  192.168.76.2    DNS       74 Standard query 0xb459 A login.live.com
280  5.700732  192.168.76.2    192.168.76.131  DNS      125 Standard query response 0x886f A ocsp.digicert.com CNAME cs9.wac.phicdn.net A 117.18.237.29
289  5.927210  192.168.76.2    192.168.76.131  DNS      215 Standard query response 0x6efb A v10.events.data.microsoft.com CNAME v10.events.data.microsoft.com.aria.akadns.net CNAME onecollector.cloudapp.a
```

The source packet for all Client Hello packets is 192.168.76.131 which indicates a single client machine within the local network.

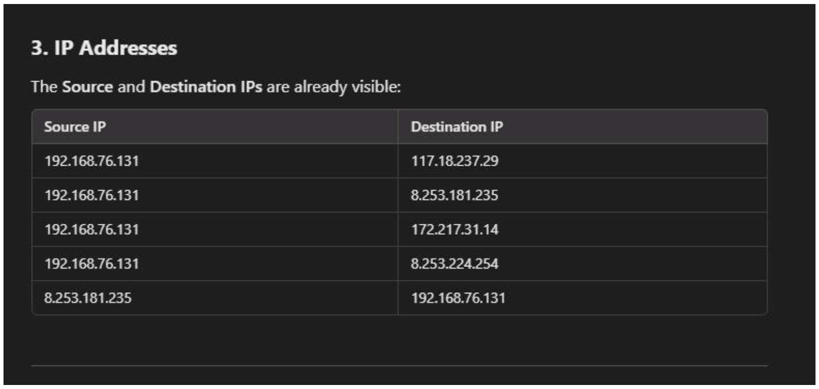
There are multiple external destination IP addresses which are most likely public servers being hosted by various services.

The filter applied to the DNS protocol is the dns filter. The domain names are:

- config.edge.skype.com
  clientoffice365tas.msedge.net
  client.wns.windows.com
  cdn.onenote.net
  candycrush.king.com
  ocsp.digicert.com
  v10.events.data.microsoft.com
  wpad.localdomain
  tileservice.weather.microsoft.com
  cdn.content.prod.cms.msn.com

nexus.officeapps.live.com
login.live.com
arc.msn.com
skypeecs-prod-edge-a.trafficmanager.net
licensing.mp.microsoft.com
static-spartan-eas-s-msn-com.akamaized.net otf.msn.com
ctldl.windowsupdate.com
gmail.com
www.bing.com
www.msn.com
settings.data.microsoft.com
sam.msn.com
ocsp.pki.goog
iecvlist.microsoft.com

HTTP-



3. IP Addresses

The **Source** and **Destination IPs** are already visible:

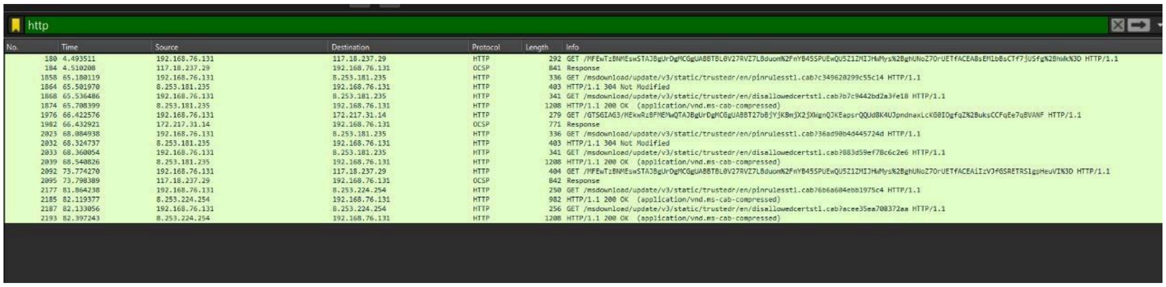
Source IP	Destination IP
192.168.76.131	117.18.237.29
192.168.76.131	8.253.181.235
192.168.76.131	172.217.31.14
192.168.76.131	8.253.224.254
8.253.181.235	192.168.76.131

The domain names from the extracted sample of visible HTTP GET requests are:

- msdownload.update.microsoft.com
- ocsp (OCSP responses – no domain just protocol context)
- v3/static/trusted – part of a subpath for updates (assumed Microsoft-related)

These domains indicate:
Microsoft services (updates and OCSP for certificate validation).

- User Agents



http

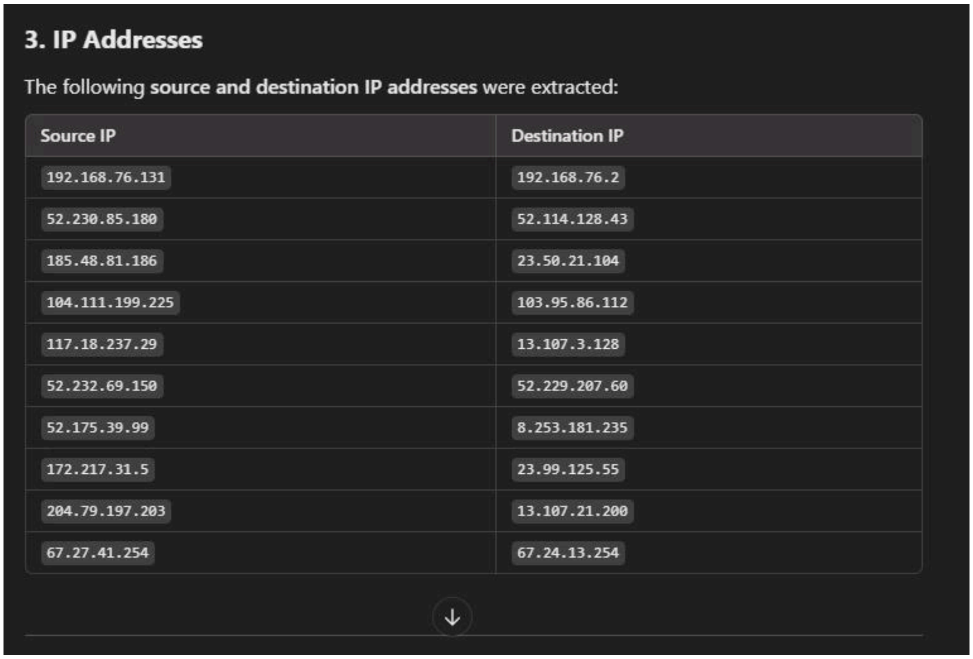
```
No.   Time       Source          Destination     Protocol Length Info
  180 4.493511   192.168.76.131  117.18.237.29   HTTP      292 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMys%2BghUNoZ7OrUETfACEA8sEMlbBsCTf7jUSfg%2BhWk%3D HTTP/1.1
  184 4.510208   117.18.237.29   192.168.76.131  OCSP      841 Response
 1858 65.180119  192.168.76.131  8.253.181.235   HTTP      336 GET /msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?c349620299c55c14 HTTP/1.1
 1864 65.501970  8.253.181.235   192.168.76.131  HTTP      403 HTTP/1.1 304 Not Modified
 1868 65.536486  192.168.76.131  8.253.181.235   HTTP      341 GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?b7c9442bd2a3fe18 HTTP/1.1
 1874 65.708399  8.253.181.235   192.168.76.131  HTTP     1208 HTTP/1.1 200 OK  (application/vnd.ms-cab-compressed)
 1976 66.422576  192.168.76.131  172.217.31.14   HTTP      279 GET /GTSGIAG3/MEkwRzBFMEMwQTAJBgUrDgMCGgUABBT27bBjYjKBmjX2jXWgnQJKEapsrQQUd8K4UJpndnaxLcKG0IOgfqZ%2BuksCCFqEe7qBVANF HTTP/1.1
 1982 66.432921  172.217.31.14   192.168.76.131  OCSP      771 Response
 2023 68.084938  192.168.76.131  8.253.181.235   HTTP      336 GET /msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?36ad90b4d445724d HTTP/1.1
 2032 68.324737  8.253.181.235   192.168.76.131  HTTP      403 HTTP/1.1 304 Not Modified
 2033 68.360054  192.168.76.131  8.253.181.235   HTTP      341 GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?883d59ef78c6c2e6 HTTP/1.1
 2039 68.540826  8.253.181.235   192.168.76.131  HTTP     1208 HTTP/1.1 200 OK  (application/vnd.ms-cab-compressed)
 2092 73.774270  192.168.76.131  117.18.237.29   HTTP      404 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMys%2BghUNoZ7OrUETfACEAiIzVJfGSRETRS1gpHeuVI%3D HTTP/1.1
 2095 73.798389  117.18.237.29   192.168.76.131  OCSP      842 Response
 2177 81.864238  192.168.76.131  8.253.224.254   HTTP      250 GET /msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?6b6a604ebb1975c4 HTTP/1.1
 2185 82.119377  8.253.224.254   192.168.76.131  HTTP      982 HTTP/1.1 200 OK  (application/vnd.ms-cab-compressed)
 2187 82.133056  192.168.76.131  8.253.224.254   HTTP      256 GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?acee35ea708372aa HTTP/1.1
 2193 82.397243  8.253.224.254   192.168.76.131  HTTP     1208 HTTP/1.1 200 OK  (application/vnd.ms-cab-compressed)
```

Filter the packets by http to isolate HTTP packets from other packets. All HTTP requests were made from the user agent: Microsoft-CryptoAPI/10.0\r\n.

User agents for the DNS protocol are the same as the user agents for HTTP protocol

User agents for the TLS protocol cannot be fetched as the connections are encrypted. Therefore, the only way to get the user agent is by getting either the decryption key or to capture the HTTP requests in the traffic (which is not applicable here).

- IP Addresses



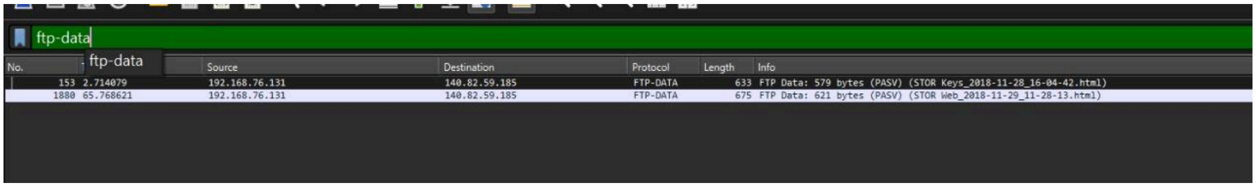
3. IP Addresses

The following **source and destination IP addresses** were extracted:

Source IP	Destination IP
`192.168.76.131`	`192.168.76.2`
`52.230.85.180`	`52.114.128.43`
`185.48.81.186`	`23.50.21.104`
`104.111.199.225`	`103.95.86.112`
`117.18.237.29`	`13.107.3.128`
`52.232.69.150`	`52.229.207.60`
`52.175.39.99`	`8.253.181.235`
`172.217.31.5`	`23.99.125.55`
`204.79.197.203`	`13.107.21.200`
`67.27.41.254`	`67.24.13.254`

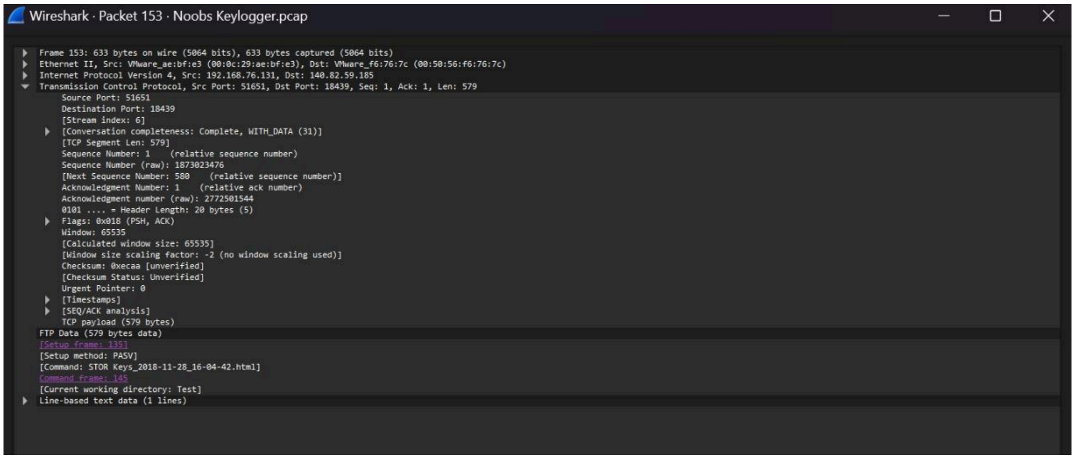
Task 2 –

a)



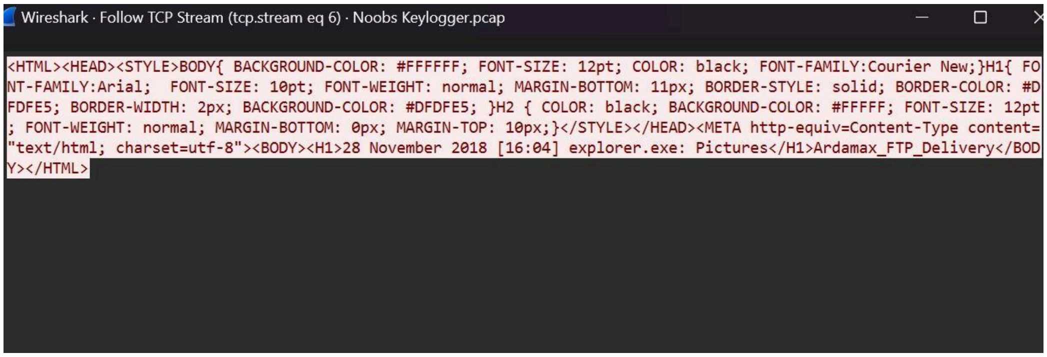
ftp-data

No.	Time	Source	Destination	Protocol	Length	Info
153	2.714079	192.168.76.131	140.82.59.185	FTP-DATA	633	FTP Data: 579 bytes (PASV) (STOR Keys_2018-11-28_16-04-42.html)
1880	65.768621	192.168.76.131	140.82.59.185	FTP-DATA	675	FTP Data: 621 bytes (PASV) (STOR Web_2018-11-29_11-28-13.html)



Wireshark · Packet 153 · Noobs Keylogger.pcap

```
Frame 153: 633 bytes on wire (5064 bits), 633 bytes captured (5064 bits)
Ethernet II, Src: VMware_ae:bf:e3 (00:0c:29:ae:bf:e3), Dst: VMware_f6:76:7c (00:50:56:f6:76:7c)
Internet Protocol Version 4, Src: 192.168.76.131, Dst: 140.82.59.185
Transmission Control Protocol, Src Port: 51651, Dst Port: 18439, Seq: 1, Ack: 1, Len: 579
    Source Port: 51651
    Destination Port: 18439
    [Stream index: 6]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 579]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 1873023476
    [Next Sequence Number: 580    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2772501544
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 65535
    [Calculated window size: 65535]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0xecaa [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (579 bytes)
FTP Data (579 bytes data)
[Setup frame: 135]
[Setup method: PASV]
[Command: STOR Keys_2018-11-28_16-04-42.html]
Command frame: 145
[Current working directory: Test]
Line-based text data (1 lines)
```

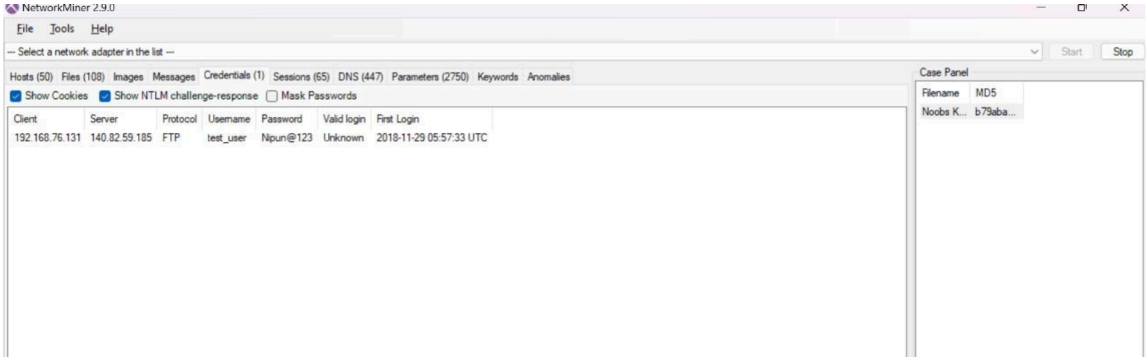


Wireshark · Follow TCP Stream (tcp.stream eq 6) · Noobs Keylogger.pcap

```
<HTML><HEAD><STYLE>BODY{ BACKGROUND-COLOR: #FFFFFF; FONT-SIZE: 12pt; COLOR: black; FONT-FAMILY:Courier New;}H1{ FO
NT-FAMILY:Arial;  FONT-SIZE: 10pt; FONT-WEIGHT: normal; MARGIN-BOTTOM: 11px; BORDER-STYLE: solid; BORDER-COLOR: #D
FDFE5; BORDER-WIDTH: 2px; BACKGROUND-COLOR: #DFDFE5; }H2 { COLOR: black; BACKGROUND-COLOR: #FFFFF; FONT-SIZE: 12pt
; FONT-WEIGHT: normal; MARGIN-BOTTOM: 0px; MARGIN-TOP: 10px;}</STYLE></HEAD><META http-equiv=Content-Type content=
"text/html; charset=utf-8"><BODY><H1>28 November 2018 [16:04] explorer.exe: Pictures</H1>Ardamax_FTP_Delivery</BOD
Y></HTML>
```

By following the TCP Stream for the pcap files we get the following keylogger.

b)

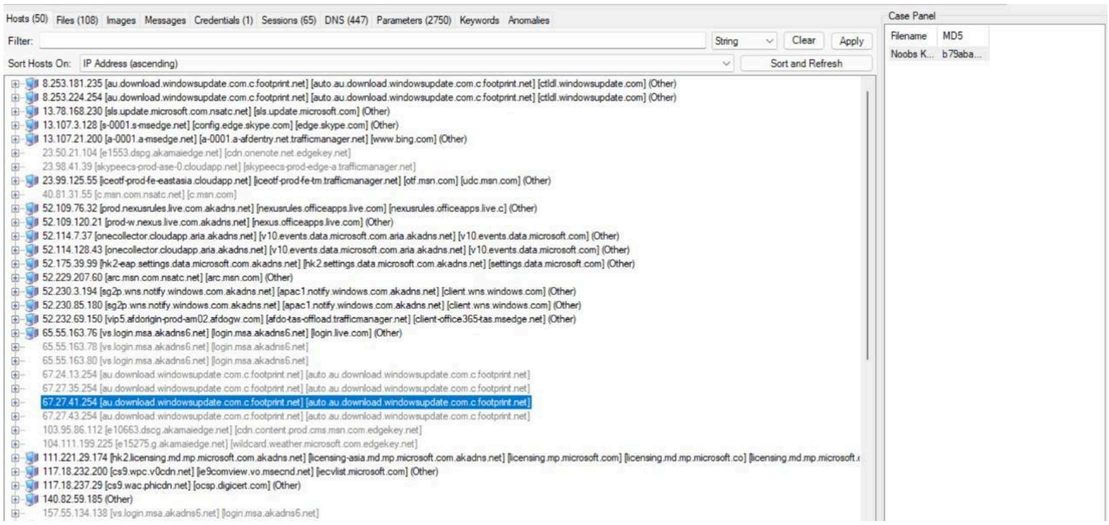


☑ Show Cookies ☑ Show NTLM challenge-response □ Mask Passwords

Client	Server	Protocol	Username	Password	Valid login	First Login
192.168.76.131	140.82.59.185	FTP	test_user	Nipun@123	Unknown	2018-11-29 05:57:33 UTC

Filename	MD5
Noobs K...	b79aba...

c)



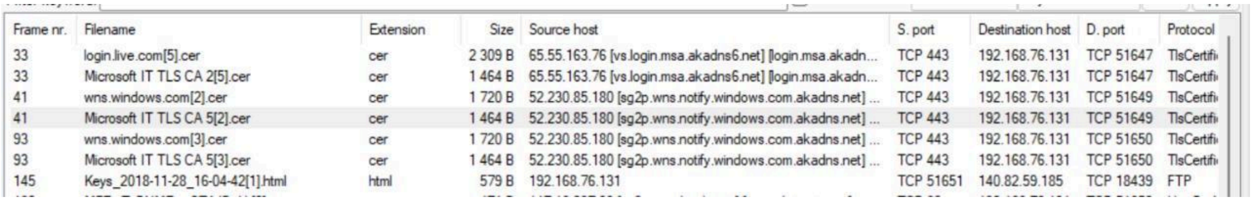
Filename	MD5
Noobs K...	b79aba...

```
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.md.mp.microsoft.c
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]
```

After we opened pcap file using Network Miner we find that we have 50 hosts and 1 credential. The credentials are displayed in b) are:

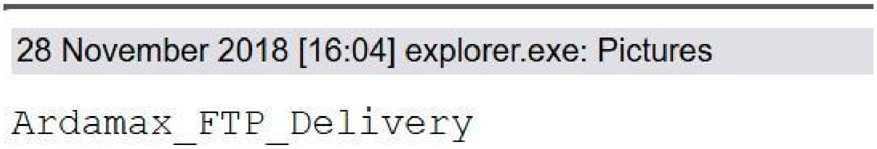
- Client IP: 192.168.76.131
- Server IP: 140.82.59.185
- Protocol: FTP
- Username: test_user
- Password: Nipun@123
- Valid Login: unknown
- First Login: 2018-11-29 5:57:33 UTC

d) The files needed are the ones that have their protocol as FTP as this is the protocol that the attacker is using to receive the data from the keylogger.



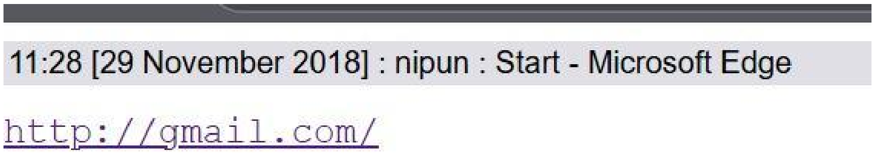
Frame nr.	Filename	Extension	Size	Source host	S. port	Destination host	D. port	Protocol
33	login.live.com[5].cer	cer	2 309 B	65.55.163.76 [vs.login.msa.akadns6.net] [login.msa.akadn...	TCP 443	192.168.76.131	TCP 51647	TlsCerti
33	Microsoft IT TLS CA 2[5].cer	cer	1 464 B	65.55.163.76 [vs.login.msa.akadns6.net] [login.msa.akadn...	TCP 443	192.168.76.131	TCP 51647	TlsCerti
41	wns.windows.com[2].cer	cer	1 720 B	52.230.85.180 [sg2p.wns.notify.windows.com.akadns.net] ...	TCP 443	192.168.76.131	TCP 51649	TlsCerti
41	Microsoft IT TLS CA 5[2].cer	cer	1 464 B	52.230.85.180 [sg2p.wns.notify.windows.com.akadns.net] ...	TCP 443	192.168.76.131	TCP 51649	TlsCerti
93	wns.windows.com[3].cer	cer	1 720 B	52.230.85.180 [sg2p.wns.notify.windows.com.akadns.net] ...	TCP 443	192.168.76.131	TCP 51650	TlsCerti
93	Microsoft IT TLS CA 5[3].cer	cer	1 464 B	52.230.85.180 [sg2p.wns.notify.windows.com.akadns.net] ...	TCP 443	192.168.76.131	TCP 51650	TlsCerti
145	Keys_2018-11-28_16-04-42[1].html	html	579 B	192.168.76.131	TCP 51651	140.82.59.185	TCP 18439	FTP

1) The infected system is the system with IP 192.168.76.131 as we can see that the first few requests the destination host is the same but the it changed.
2) As soon as the protocol changed to FTP in which the system became the source and the destination host changed to the attacker's destination host of 140.82.59.185.
3) These were the files that were sent to the attacker



28 November 2018 [16:04] explorer.exe: Pictures

Ardamax_FTP_Delivery



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

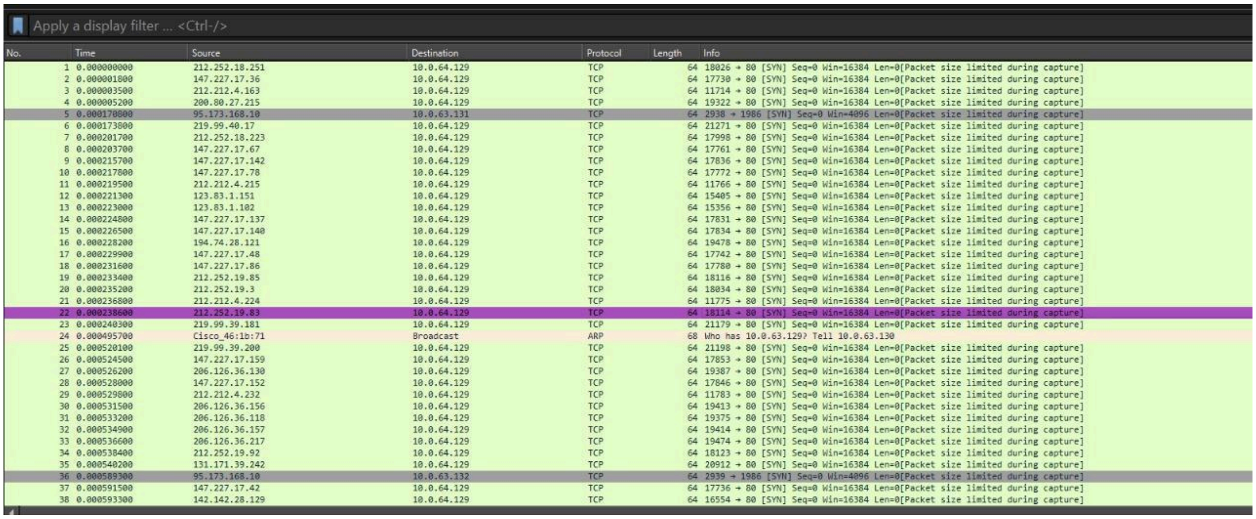
http://gmail.com/

4) In addition to the keystrokes, we found the time the file was created and uploaded.

1. Timestamps of file creation and upload:

- Keys_2018-11-28_16-04-42[1].html:
    - Timestamp: 28 November 2018 [16:04].
- Web_2018-11-29_11-28-13[1].html:
    - Timestamp: 29 November 2018 [11:28].
- Both timestamps indicate when the files were likely generated by the keylogger and uploaded to the FTP server.

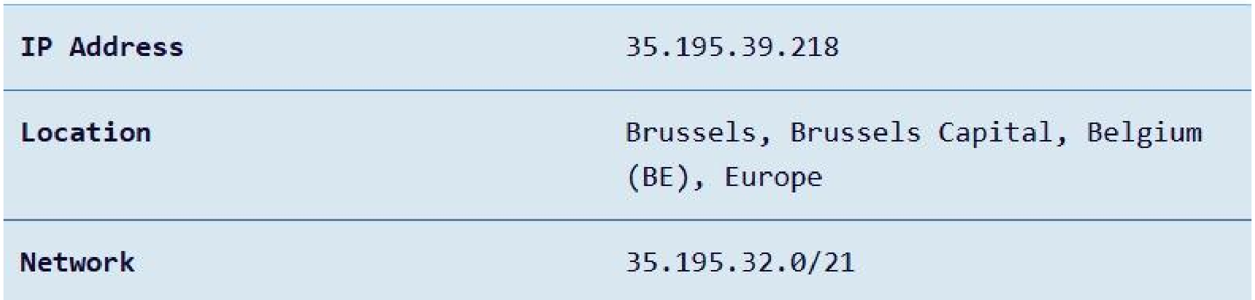
Question 2:



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	212.252.18.251	10.0.64.129	TCP	64	18026 → 80 [SYN] Seq=0 Win=16384 Len=0[Packet size limited during capture]
2	0.000001800	147.227.17.36	10.0.64.129	TCP	64	17730 → 80 [SYN] Seq=0 Win=16384 Len=0[Packet size limited during capture]
3	0.000003500	212.212.4.163	10.0.64.129	TCP	64	11714 → 80 [SYN] Seq=0 Win=16384 Len=0[Packet size limited during capture]
4	0.000005200	200.80.27.215	10.0.64.129	TCP	64	19322 → 80 [SYN] Seq=0 Win=16384 Len=0[Packet size limited during capture]
5	0.000170800	95.173.168.10	10.0.63.131	TCP	64	2938 → 1986 [SYN] Seq=0 Win=4096 Len=0[Packet size limited during capture]
6	0.000173800	219.99.40.17	10.0.64.129	TCP	64	21271 → 80 [SYN] Seq=0 Win=16384 Len=0[Packet size limited during capture]
7	0.000201700	212.252.18.223	10.0.64.129	TCP	64	17998 → 80 [SYN] Seq=0 Win=16384 Len=0[Packet size limited during capture]
8	0.000203700	147.227.17.67	10.0.64.129	TCP	64	17761 → 80 [SYN] Seq=0 Win=16384 Len=0[Packet size limited during capture]
9	0.000215700	147.227.17.142	10.0.64.129	TCP	64	17836 → 80 [SYN] Seq=0 Win=16384 Len=0[Packet size limited during capture]
10	0.000217800	147.227.17.78	10.0.64.129	TCP	64	17772 → 80 [SYN] Seq=0 Win=16384 Len=0[Packet size limited during capture]
11	0.000219500	212.212.4.215	10.0.64.129	TCP	64	11766 → 80 [SYN] Seq=0 Win=16384 Len=0[Packet size limited during capture]
12	0.000221300	123.83.1.151	10.0.64.129	TCP	64	15405 → 80 [SYN] Seq=0 Win=16384 Len=0[Packet size limited during capture]
13	0.000223000	123.83.1.102	10.0.64.129	TCP	64	15356 → 80 [SYN] Seq=0 Win=16384 Len=0[Packet size limited during capture]
14	0.000224800	147.227.17.137	10.0.64.129	TCP	64	17831 → 80 [SYN] Seq=0 Win=16384 Len=0[Packet size limited during capture]
15	0.000226500	147.227.17.140	10.0.64.129	TCP	64	17834 → 80 [SYN] Seq=0 Win=16384 Len=0[Packet size limited during capture]
16	0.000228200	194.74.28.121	10.0.64.129	TCP	64	19478 → 80 [SYN] Seq=0 Win=16384 Len=0[Packet size limited during capture]
17	0.000229900	147.227.17.48	10.0.64.129	TCP	64	17742 → 80 [SYN] Seq=0 Win=16384 Len=0[Packet size limited during capture]
18	0.000231600	147.227.17.86	10.0.64.129	TCP	64	17780 → 80 [SYN] Seq=0 Win=16384 Len=0[Packet size limited during capture]
19	0.000233400	212.252.19.85	10.0.64.129	TCP	64	18116 → 80 [SYN] Seq=0 Win=16384 Len=0[Packet size limited during capture]
20	0.000235200	212.252.19.3	10.0.64.129	TCP	64	18034 → 80 [SYN] Seq=0 Win=16384 Len=0[Packet size limited during capture]
21	0.000236800	212.212.4.224	10.0.64.129	TCP	64	11775 → 80 [SYN] Seq=0 Win=16384 Len=0[Packet size limited during capture]
22	0.000238600	212.252.19.83	10.0.64.129	TCP	64	18114 → 80 [SYN] Seq=0 Win=16384 Len=0[Packet size limited during capture]
23	0.000240300	219.99.39.181	10.0.64.129	TCP	64	21179 → 80 [SYN] Seq=0 Win=16384 Len=0[Packet size limited during capture]
24	0.000495700	Cisco_46:1b:71	Broadcast	ARP	68	Who has 10.0.63.129? Tell 10.0.63.130
25	0.000520100	219.99.39.200	10.0.64.129	TCP	64	21198 → 80 [SYN] Seq=0 Win=16384 Len=0[Packet size limited during capture]
26	0.000524500	147.227.17.159	10.0.64.129	TCP	64	17853 → 80 [SYN] Seq=0 Win=16384 Len=0[Packet size limited during capture]
27	0.000526200	206.126.36.130	10.0.64.129	TCP	64	19387 → 80 [SYN] Seq=0 Win=16384 Len=0[Packet size limited during capture]
28	0.000528000	147.227.17.152	10.0.64.129	TCP	64	17846 → 80 [SYN] Seq=0 Win=16384 Len=0[Packet size limited during capture]
29	0.000529800	212.212.4.232	10.0.64.129	TCP	64	11783 → 80 [SYN] Seq=0 Win=16384 Len=0[Packet size limited during capture]
30	0.000531500	206.126.36.156	10.0.64.129	TCP	64	19413 → 80 [SYN] Seq=0 Win=16384 Len=0[Packet size limited during capture]
31	0.000533200	206.126.36.118	10.0.64.129	TCP	64	19375 → 80 [SYN] Seq=0 Win=16384 Len=0[Packet size limited during capture]
32	0.000534900	206.126.36.157	10.0.64.129	TCP	64	19414 → 80 [SYN] Seq=0 Win=16384 Len=0[Packet size limited during capture]
33	0.000536600	206.126.36.217	10.0.64.129	TCP	64	19474 → 80 [SYN] Seq=0 Win=16384 Len=0[Packet size limited during capture]
34	0.000538400	212.252.19.92	10.0.64.129	TCP	64	18123 → 80 [SYN] Seq=0 Win=16384 Len=0[Packet size limited during capture]
35	0.000540200	131.171.39.242	10.0.64.129	TCP	64	20912 → 80 [SYN] Seq=0 Win=16384 Len=0[Packet size limited during capture]
36	0.000589300	95.173.168.10	10.0.63.132	TCP	64	2939 → 1986 [SYN] Seq=0 Win=4096 Len=0[Packet size limited during capture]
37	0.000591500	147.227.17.42	10.0.64.129	TCP	64	17736 → 80 [SYN] Seq=0 Win=16384 Len=0[Packet size limited during capture]
38	0.000593300	142.142.28.129	10.0.64.129	TCP	64	16554 → 80 [SYN] Seq=0 Win=16384 Len=0[Packet size limited during capture]

1) As we can see this is a SYN Flood Attack (or a DDOS Attack) in order to crash the server service and prevent the real users from being able to access the server. The attack overwhelms the server with TCP Requests without waiting to listen to the server response (ACK or NACK). We can tell this is a SYN Flood Attack as the attacker is using different IPs to ping the same server port in very short periods of time (milliseconds).

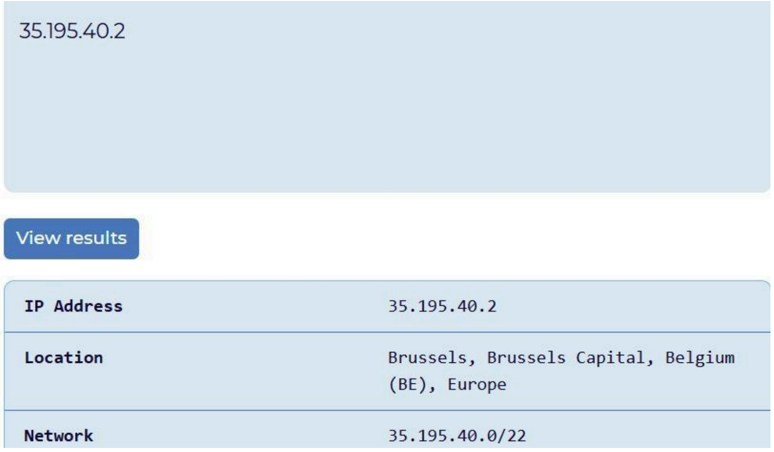
2)



IP Address	35.195.39.218
Location	Brussels, Brussels Capital, Belgium (BE), Europe
Network	35.195.32.0/21

This range covers 2048 IP addresses which all likely belong to the same geographical location (Brussels, Belgium, Europe).

- First IP: 35.195.32.0 (Network Address)
- Last IP: 35.195.32.0 (Broadcast Address)
- Network: 35.195.32.0/21
- Range: 35.195.32.0 to 35.195.39.255

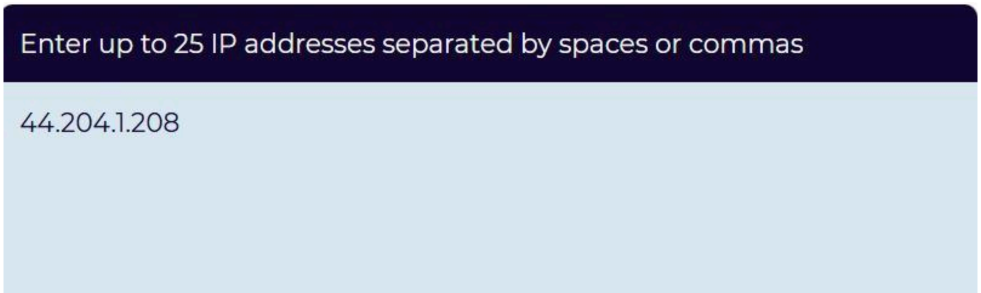


35.195.40.2

IP Address	35.195.40.2
Location	Brussels, Brussels Capital, Belgium (BE), Europe
Network	35.195.40.0/22

This range covers 1024 IP addresses which all likely belong to the same geographical location (Brussels, Belgium, Europe).

- First IP: 35.195.40.0 (Network Address)
- Last IP: 35.195.43.255 (Broadcast Address)
- Network: 35.195.40.0/22
- Range: 35.195.40.0 to 35.195.43.255

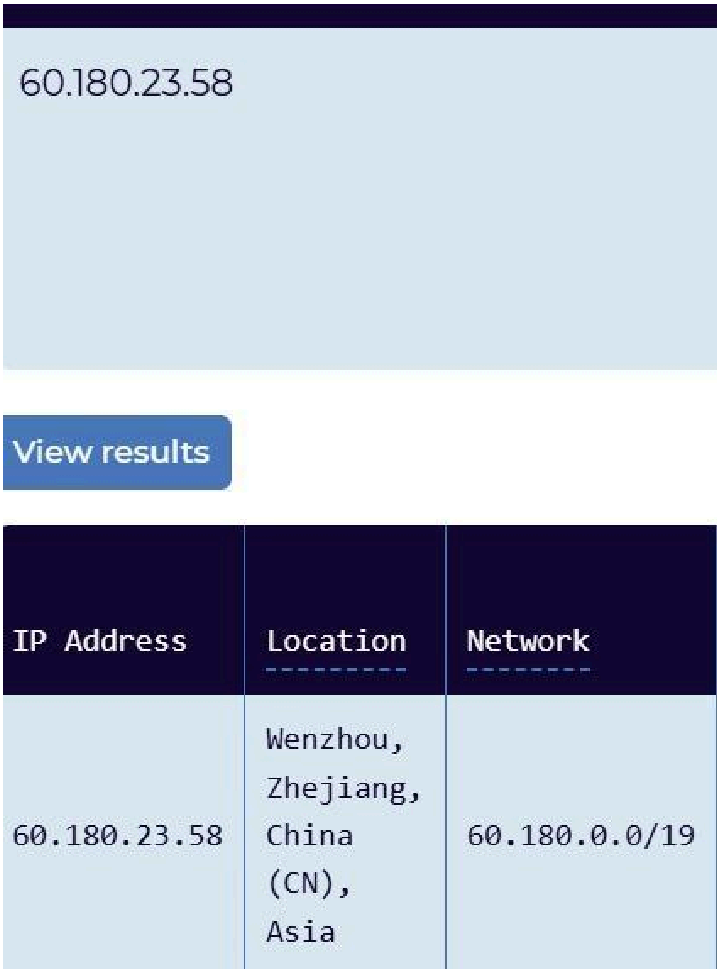


Enter up to 25 IP addresses separated by spaces or commas

44.204.1.208

This range covers 65,536 IP addresses which all likely belong to the same geographical location (Ashburn, Virginia, United States, North America).

- First IP: 44.204.1.208 (Network Address)
- Last IP: 44.204.255.255 (Broadcast Address)
- Network: 44.204.0.0/16
- Range: 44.204.0.0 to 44.204.255.255

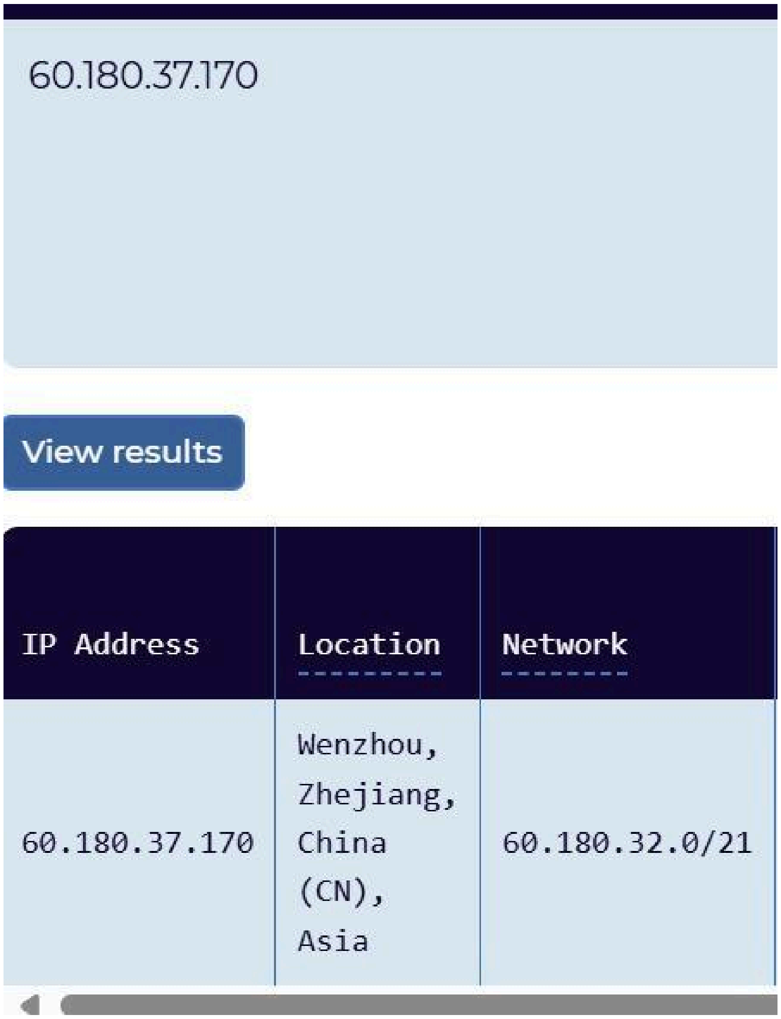


60.180.23.58

IP Address	Location	Network
60.180.23.58	Wenzhou, Zhejiang, China (CN), Asia	60.180.0.0/19

This range covers 8192 IP addresses which all likely belong to the same geographical location (Wenzhou, Zhejiang, China, Asia).

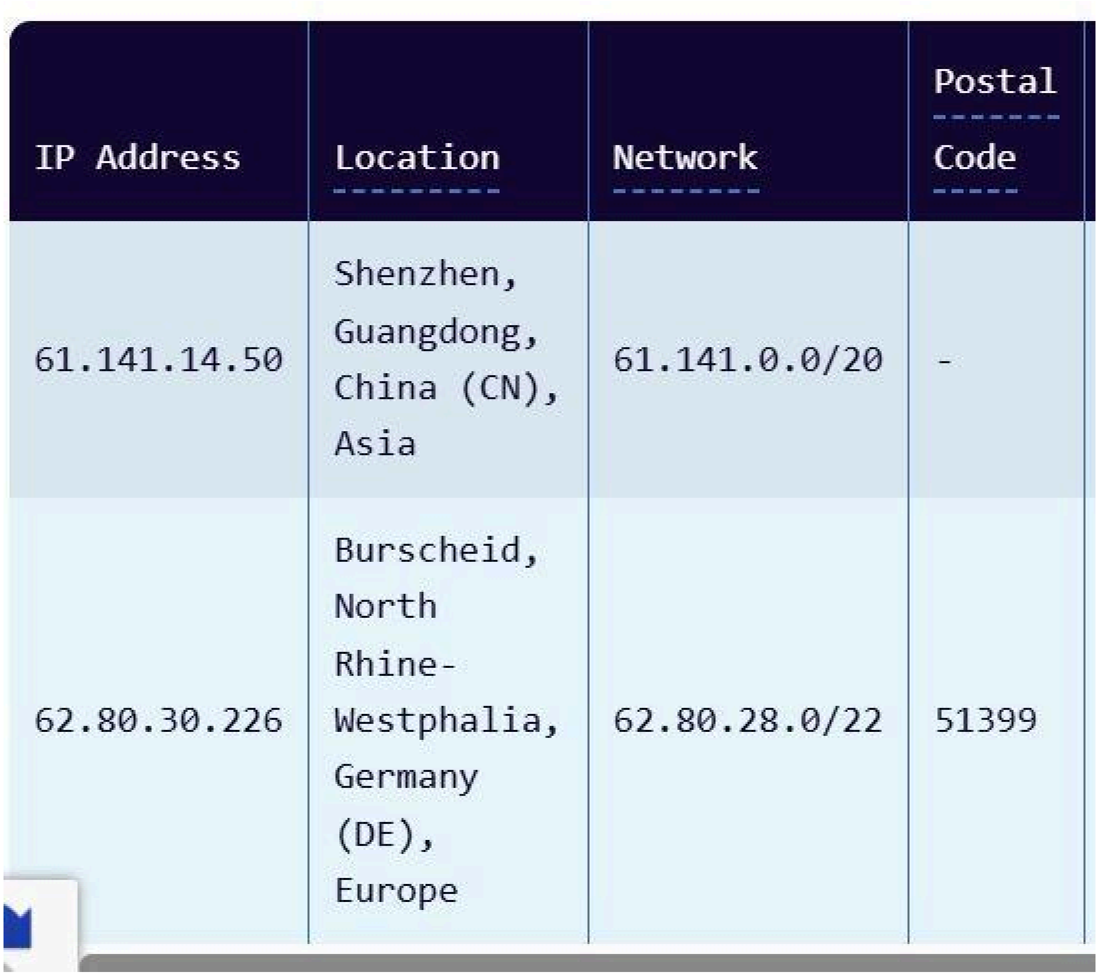
- First IP: 60.180.0.0 (Network Address)
- Last IP: 60.180.31.255 (Broadcast Address)
- Network: 60.180.0.0/19
- Range: 60.180.0.0 to 60.180.31.255


60.180.37.170

IP Address	Location	Network
60.180.37.170	Wenzhou, Zhejiang, China (CN), Asia	60.180.32.0/21

This range covers 2048 IP addresses which all likely belong to the same geographical location (Wenzhou, Zhejiang, China, Asia).

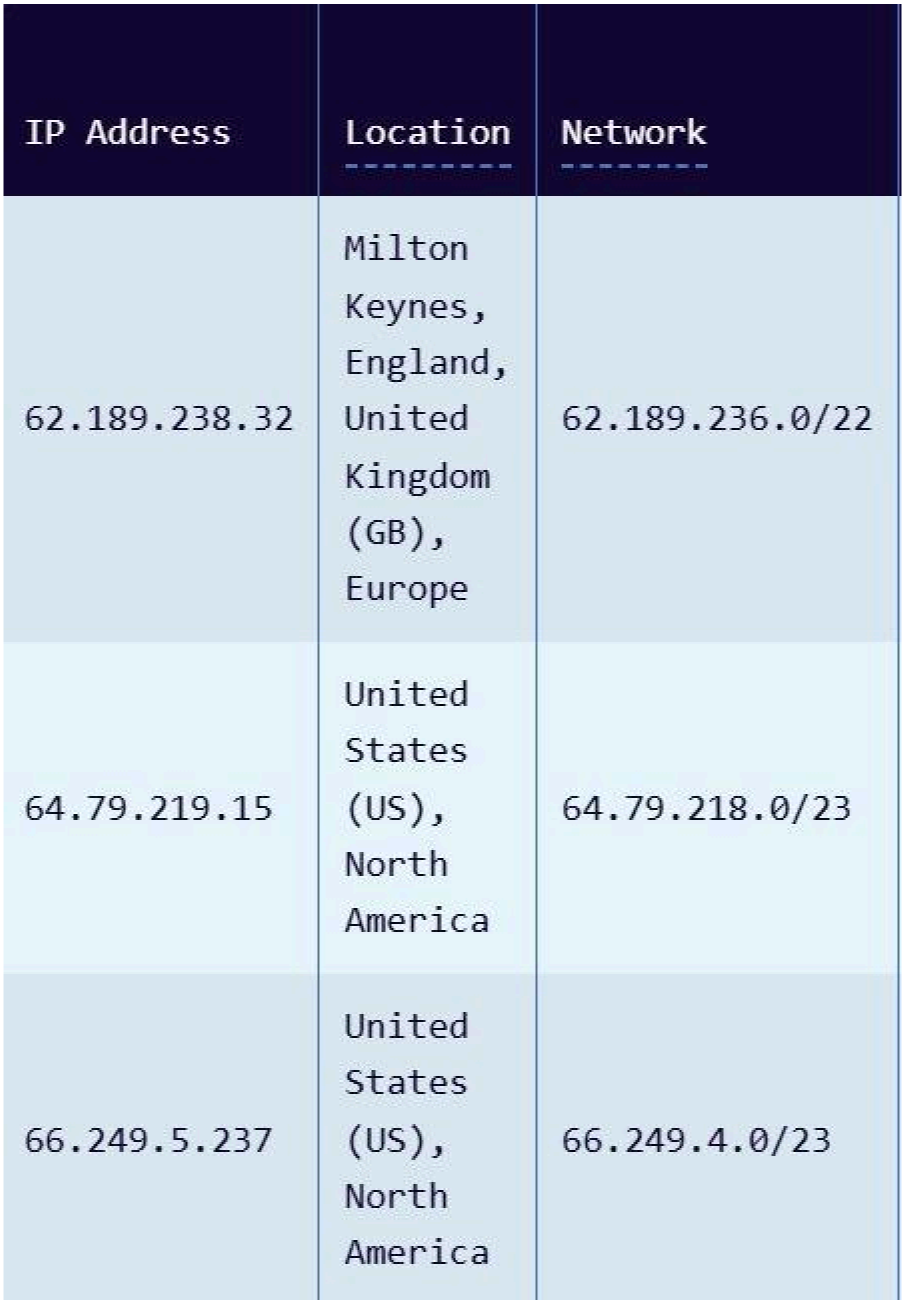
- First IP: 60.180.32.0 (Network Address)
- Last IP: 60.180.39.255 (Broadcast Address)
- Network: 60.180.32.0/21
- Range: 60.180.32.0 to 60.180.39.255



IP Address	Location	Network	Postal Code
61.141.14.50	Shenzhen, Guangdong, China (CN), Asia	61.141.0.0/20	-
62.80.30.226	Burscheid, North Rhine-Westphalia, Germany (DE), Europe	62.80.28.0/22	51399

61.141.0.0/20 → 61.141.0.0 to 61.141.15.255 (Shenzhen, China).

62.80.28.0/22 → 62.80.28.0 to 62.80.31.255 (Burscheid, Germany).



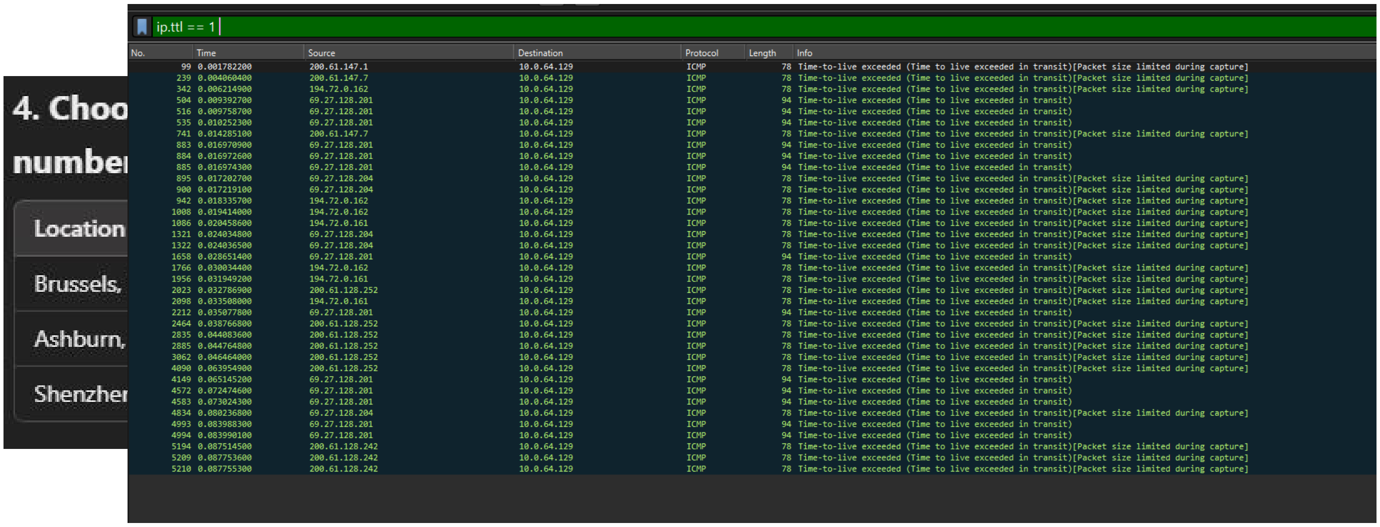
IP Address	Location	Network
62.189.238.32	Milton Keynes, England, United Kingdom (GB), Europe	62.189.236.0/22
64.79.219.15	United States (US), North America	64.79.218.0/23
66.249.5.237	United States (US), North America	66.249.4.0/23

62.189.236.0/22 → 62.189.236.0 to 62.189.239.255 (Milton Keynes, UK).

64.79.218.0/23 → 64.79.218.0 to 64.79.219.255 (US).

66.249.4.0/23 → 66.249.4.0 to 66.249.5.255 (US).

3) We found a total of 9 countries for the IPs we analyzed.
   Belgium, Virginia, China, US, Germany, France ,Russia, Taiwan,Brazil



4. Choo
numbe

Location
Brussels,
Ashburn,
Shenzhe

```
ip.ttl == 1

No.     Time         Source            Destination     Protocol  Length  Info
     99 0.001782200  200.61.147.1      10.0.64.129     ICMP          78  Time-to-live exceeded (Time to live exceeded in transit)[Packet size limited during capture]
    239 0.004060400  200.61.147.7      10.0.64.129     ICMP          78  Time-to-live exceeded (Time to live exceeded in transit)[Packet size limited during capture]
    342 0.006214900  194.72.0.162      10.0.64.129     ICMP          78  Time-to-live exceeded (Time to live exceeded in transit)[Packet size limited during capture]
    504 0.009392700  69.27.128.201     10.0.64.129     ICMP          94  Time-to-live exceeded (Time to live exceeded in transit)
    516 0.009758700  69.27.128.201     10.0.64.129     ICMP          94  Time-to-live exceeded (Time to live exceeded in transit)
    535 0.010252300  69.27.128.201     10.0.64.129     ICMP          94  Time-to-live exceeded (Time to live exceeded in transit)
    741 0.014285100  200.61.147.7      10.0.64.129     ICMP          78  Time-to-live exceeded (Time to live exceeded in transit)[Packet size limited during capture]
    883 0.016970900  69.27.128.201     10.0.64.129     ICMP          94  Time-to-live exceeded (Time to live exceeded in transit)
    884 0.016972600  69.27.128.201     10.0.64.129     ICMP          94  Time-to-live exceeded (Time to live exceeded in transit)
    885 0.016974300  69.27.128.201     10.0.64.129     ICMP          94  Time-to-live exceeded (Time to live exceeded in transit)
    895 0.017202700  69.27.128.204     10.0.64.129     ICMP          78  Time-to-live exceeded (Time to live exceeded in transit)[Packet size limited during capture]
    900 0.017219100  69.27.128.204     10.0.64.129     ICMP          78  Time-to-live exceeded (Time to live exceeded in transit)[Packet size limited during capture]
    942 0.018335700  194.72.0.162      10.0.64.129     ICMP          78  Time-to-live exceeded (Time to live exceeded in transit)[Packet size limited during capture]
   1008 0.019414000  194.72.0.162      10.0.64.129     ICMP          78  Time-to-live exceeded (Time to live exceeded in transit)[Packet size limited during capture]
   1086 0.020458600  194.72.0.161      10.0.64.129     ICMP          78  Time-to-live exceeded (Time to live exceeded in transit)[Packet size limited during capture]
   1321 0.024034800  69.27.128.204     10.0.64.129     ICMP          78  Time-to-live exceeded (Time to live exceeded in transit)[Packet size limited during capture]
   1322 0.024036500  69.27.128.204     10.0.64.129     ICMP          78  Time-to-live exceeded (Time to live exceeded in transit)[Packet size limited during capture]
   1658 0.028651400  69.27.128.201     10.0.64.129     ICMP          94  Time-to-live exceeded (Time to live exceeded in transit)
   1766 0.030034400  194.72.0.162      10.0.64.129     ICMP          78  Time-to-live exceeded (Time to live exceeded in transit)[Packet size limited during capture]
   1956 0.031949200  194.72.0.161      10.0.64.129     ICMP          78  Time-to-live exceeded (Time to live exceeded in transit)[Packet size limited during capture]
   2023 0.032786900  200.61.128.252    10.0.64.129     ICMP          78  Time-to-live exceeded (Time to live exceeded in transit)[Packet size limited during capture]
   2098 0.033508000  194.72.0.161      10.0.64.129     ICMP          78  Time-to-live exceeded (Time to live exceeded in transit)[Packet size limited during capture]
   2212 0.035077800  69.27.128.201     10.0.64.129     ICMP          94  Time-to-live exceeded (Time to live exceeded in transit)
   2464 0.038766800  200.61.128.252    10.0.64.129     ICMP          78  Time-to-live exceeded (Time to live exceeded in transit)[Packet size limited during capture]
   2835 0.044083600  200.61.128.252    10.0.64.129     ICMP          78  Time-to-live exceeded (Time to live exceeded in transit)[Packet size limited during capture]
   2885 0.044764800  200.61.128.252    10.0.64.129     ICMP          78  Time-to-live exceeded (Time to live exceeded in transit)[Packet size limited during capture]
   3062 0.046464000  200.61.128.252    10.0.64.129     ICMP          78  Time-to-live exceeded (Time to live exceeded in transit)[Packet size limited during capture]
   4090 0.063954900  200.61.128.252    10.0.64.129     ICMP          78  Time-to-live exceeded (Time to live exceeded in transit)[Packet size limited during capture]
   4149 0.065145200  69.27.128.201     10.0.64.129     ICMP          94  Time-to-live exceeded (Time to live exceeded in transit)
   4572 0.072474600  69.27.128.201     10.0.64.129     ICMP          94  Time-to-live exceeded (Time to live exceeded in transit)
   4583 0.073024300  69.27.128.201     10.0.64.129     ICMP          94  Time-to-live exceeded (Time to live exceeded in transit)
   4834 0.080236800  69.27.128.204     10.0.64.129     ICMP          78  Time-to-live exceeded (Time to live exceeded in transit)[Packet size limited during capture]
   4993 0.083988300  69.27.128.201     10.0.64.129     ICMP          94  Time-to-live exceeded (Time to live exceeded in transit)
   4994 0.083990100  69.27.128.201     10.0.64.129     ICMP          94  Time-to-live exceeded (Time to live exceeded in transit)
   5194 0.087514500  200.61.128.242    10.0.64.129     ICMP          78  Time-to-live exceeded (Time to live exceeded in transit)[Packet size limited during capture]
   5209 0.087753600  200.61.128.242    10.0.64.129     ICMP          78  Time-to-live exceeded (Time to live exceeded in transit)[Packet size limited during capture]
   5210 0.087755300  200.61.128.242    10.0.64.129     ICMP          78  Time-to-live exceeded (Time to live exceeded in transit)[Packet size limited during capture]
```

4)

- Brussels, Belgium: 64 packets.
- Ashburn, United States: 128 packets.
- Shenzhen, China: 96 packets.

4) These packets are most likely made by bots as the traffic originates from multiple IP addresses across different countries. This behavior is unusual for a normal device and legitimate network and suggests a botnet distributing attack traffic. The packet counts and IP distributions are typical indicators of automated bots rather than human behavior.

5) Normal TTL Range: Devices usually start with TTL values like 64, 128, or 255.

   Abnormal TTL: If the TTL values are unusually low, it may indicate that the packet has passed through many network hops, suggesting traffic is routed through unexpected or malicious paths. Consistent TTLs across many IPs may also indicate spoofed packets. If we had TTL values, we could compare them to standard device behavior to detect anomalies.