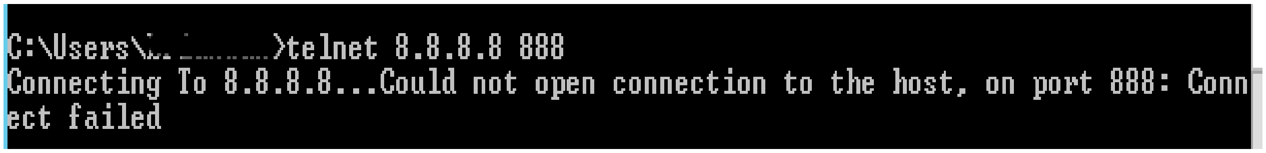
Analyze netmon trace

Last updated by | Jackie Huang | Jan 4, 2022 at 12:24 AM PST

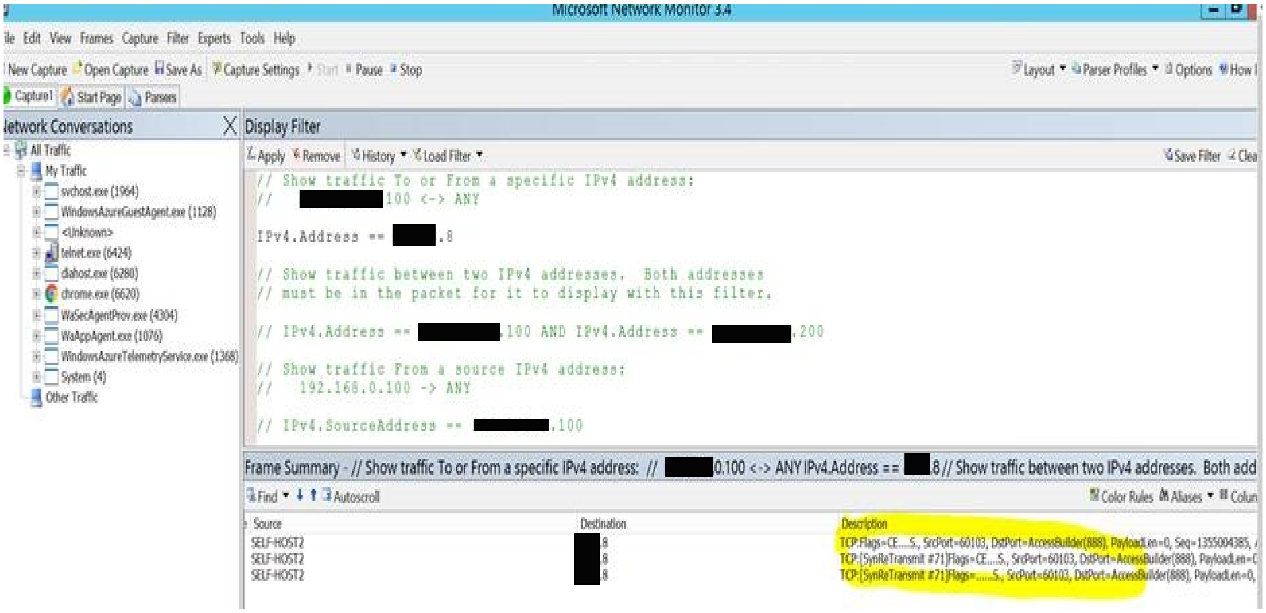
How to analyze netmon trace

Tuesday, March 10, 2020
6:21 PM

When you tried to telnet 8.8.8.8 888 with netmon trace collected, you suppose can see below trace:



```
C:\Users\[redacted]>telnet 8.8.8.8 888
Connecting To 8.8.8.8...Could not open connection to the host, on port 888: Conn
ect failed
```


Microsoft Network Monitor 3.4
File Edit View Frames Capture Filter Experts Tools Help
New Capture Open Capture Save As Capture Settings Start Pause Stop
Layout Parser Profiles Options How I
Capture1 Start Page Parsers
Network Conversations
All Traffic
My Traffic
svchost.exe (1964)
WindowsAzureGuestAgent.exe (1128)
<Unknown>
telnet.exe (6424)
dashost.exe (6280)
chrome.exe (6620)
WaSecAgentProv.exe (4304)
WaAppAgent.exe (1076)
WindowsAzureTelemetryService.exe (1368)
System (4)
Other Traffic
Display Filter
Apply Remove History Load Filter
Save Filter Clea
Find Autoscroll
Color Rules Aliases Colun

```
// Show traffic To or From a specific IPv4 address:
//    [redacted]100 <-> ANY

IPv4.Address == [redacted].8

// Show traffic between two IPv4 addresses.  Both addresses
// must be in the packet for it to display with this filter.

// IPv4.Address == [redacted].100 AND IPv4.Address == [redacted].200

// Show traffic From a source IPv4 address:
//   192.168.0.100 -> ANY

// IPv4.SourceAddress == [redacted].100
```

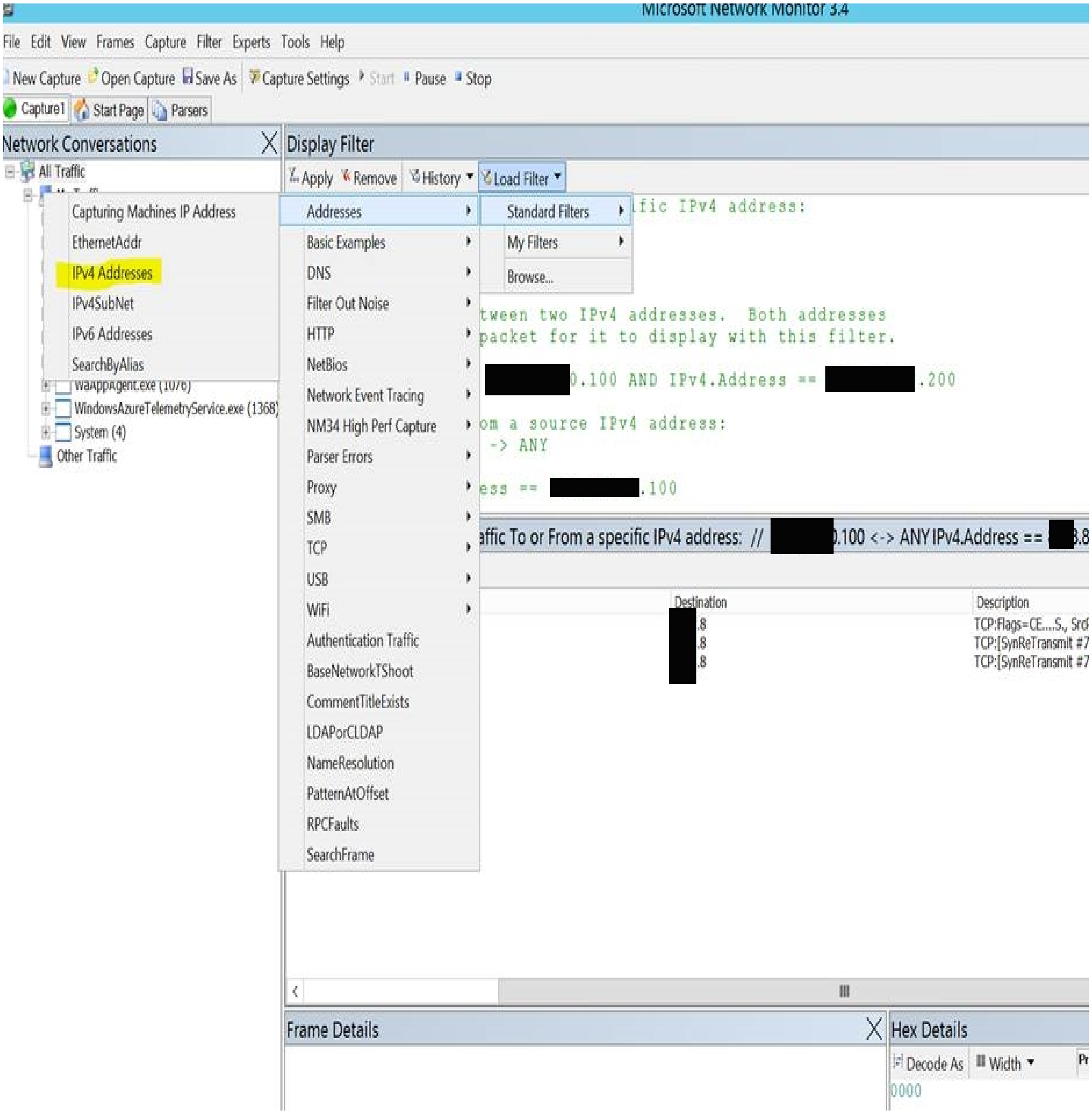
Frame Summary - // Show traffic To or From a specific IPv4 address: // [redacted]0.100 <-> ANY IPv4.Address == [redacted].8 // Show traffic between two IPv4 addresses. Both add

```
Source       Destination     Description
SELF-HOST2   [redacted].8    TCP:Flags=CE....S., SrcPort=60103, DstPort=AccessBuilder(888), PayloadLen=0, Seq=1355004385, /
SELF-HOST2   [redacted].8    TCP:[SynReTransmit #71]Flags=CE....S., SrcPort=60103, DstPort=AccessBuilder(888), PayloadLen=C
SELF-HOST2   [redacted].8    TCP:[SynReTransmit #71]Flags=......S., SrcPort=60103, DstPort=AccessBuilder(888), PayloadLen=0,
```

What does it mean? It means that you could not make TCP connection to the 8.8.8.8 server side based on the port 888, so you can see two SynReTransmit additional packages there, since Source SELF-HOST2 could not make connection to 8.8.8.8 at the first package, it will keep on making connection.

Tips:

1, You can Click Load Filter->Standard Filter->Addresses->IPv4 Addresses

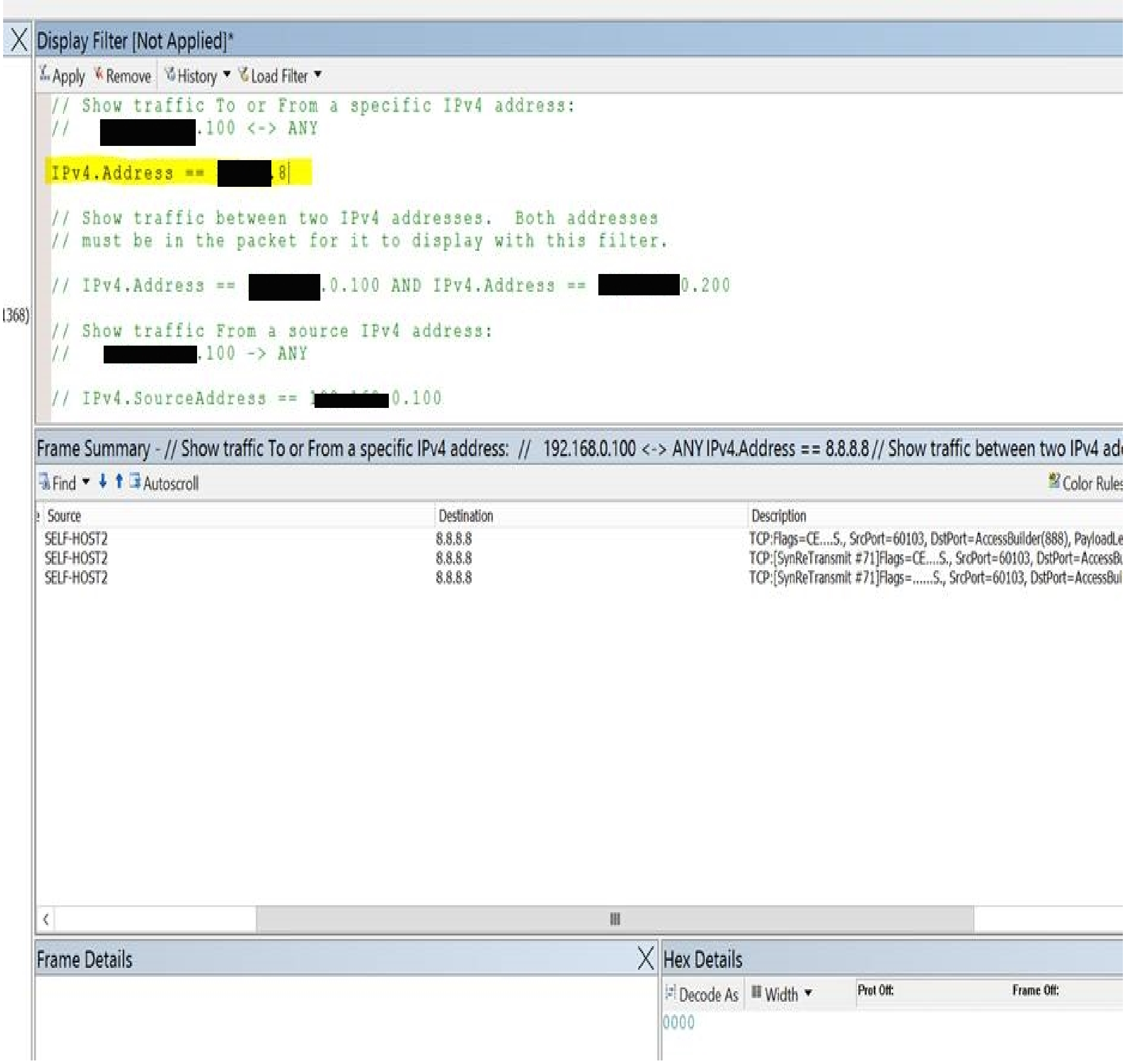


```
ific IPv4 address:

tween two IPv4 addresses.  Both addresses
packet for it to display with this filter.
 [redacted].100 AND IPv4.Address == [redacted].200

om a source IPv4 address:
 -> ANY

ess == [redacted].100
```

affic To or From a specific IPv4 address: // [redacted].100 <-> ANY IPv4.Address == [redacted].8

Destination	Description
[redacted].8	TCP:Flags=CE....S., Src
[redacted].8	TCP:[SynReTransmit #7
[redacted].8	TCP:[SynReTransmit #7

2, Input IPv4.Address == 8.8.8.8 as filter, and click Apply. After that, you will see only the communication from local machine to the destination 8.8.8.8.



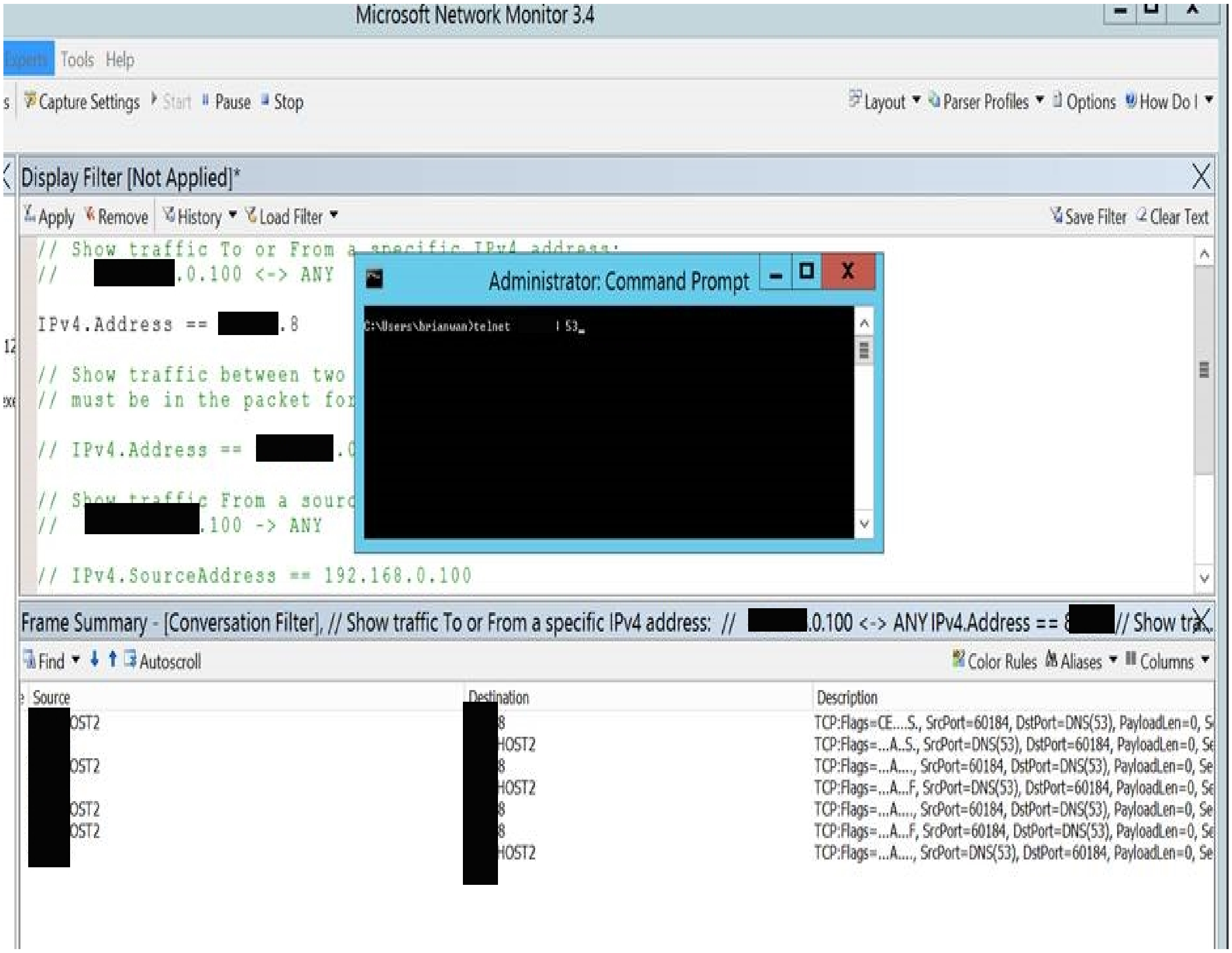
```
// Show traffic To or From a specific IPv4 address:
//    [redacted].100 <-> ANY

IPv4.Address == [redacted].8

// Show traffic between two IPv4 addresses.  Both addresses
// must be in the packet for it to display with this filter.

// IPv4.Address == [redacted].0.100 AND IPv4.Address == [redacted]0.200

// Show traffic From a source IPv4 address:
//    [redacted].100 -> ANY

// IPv4.SourceAddress == [redacted]0.100
```

Frame Summary - // Show traffic To or From a specific IPv4 address: // 192.168.0.100 <-> ANY IPv4.Address == 8.8.8.8 // Show traffic between two IPv4 ad

Source	Destination	Description
SELF-HOST2	8.8.8.8	TCP:Flags=CE....S., SrcPort=60103, DstPort=AccessBuilder(888), PayloadLe
SELF-HOST2	8.8.8.8	TCP:[SynReTransmit #71]Flags=CE....S., SrcPort=60103, DstPort=AccessBu
SELF-HOST2	8.8.8.8	TCP:[SynReTransmit #71]Flags=......S., SrcPort=60103, DstPort=AccessBui

How about below good scenario?

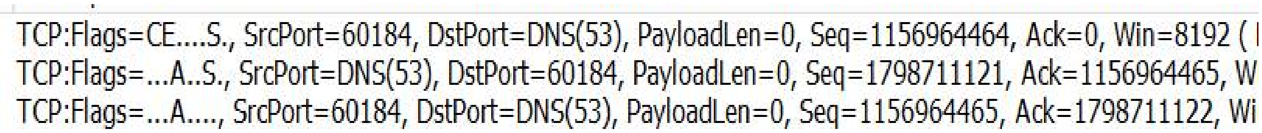
telnet 8.8.8.8 53 and working fine without any issue, you can see TCP three handshake happening, and then finished the session with 4 way handshake.


Microsoft Network Monitor 3.4
Experts Tools Help
Capture Settings Start Pause Stop
Layout ▾ Parser Profiles ▾ Options How Do I ▾
Display Filter [Not Applied]*
Apply Remove History ▾ Load Filter ▾
Save Filter Clear Text
Administrator: Command Prompt
Frame Summary - [Conversation Filter], // Show traffic To or From a specific IPv4 address: // [redacted].0.100 <-> ANY IPv4.Address == 8[redacted]// Show tra
Find ▾ Autoscroll
Color Rules Aliases ▾ Columns ▾

```
// Show traffic To or From a specific IPv4 address:
//   [redacted].0.100 <-> ANY

IPv4.Address == [redacted].8

// Show traffic between two
// must be in the packet for

// IPv4.Address == [redacted].0

// Show traffic From a sourc
//   [redacted].100 -> ANY

// IPv4.SourceAddress == 192.168.0.100
```

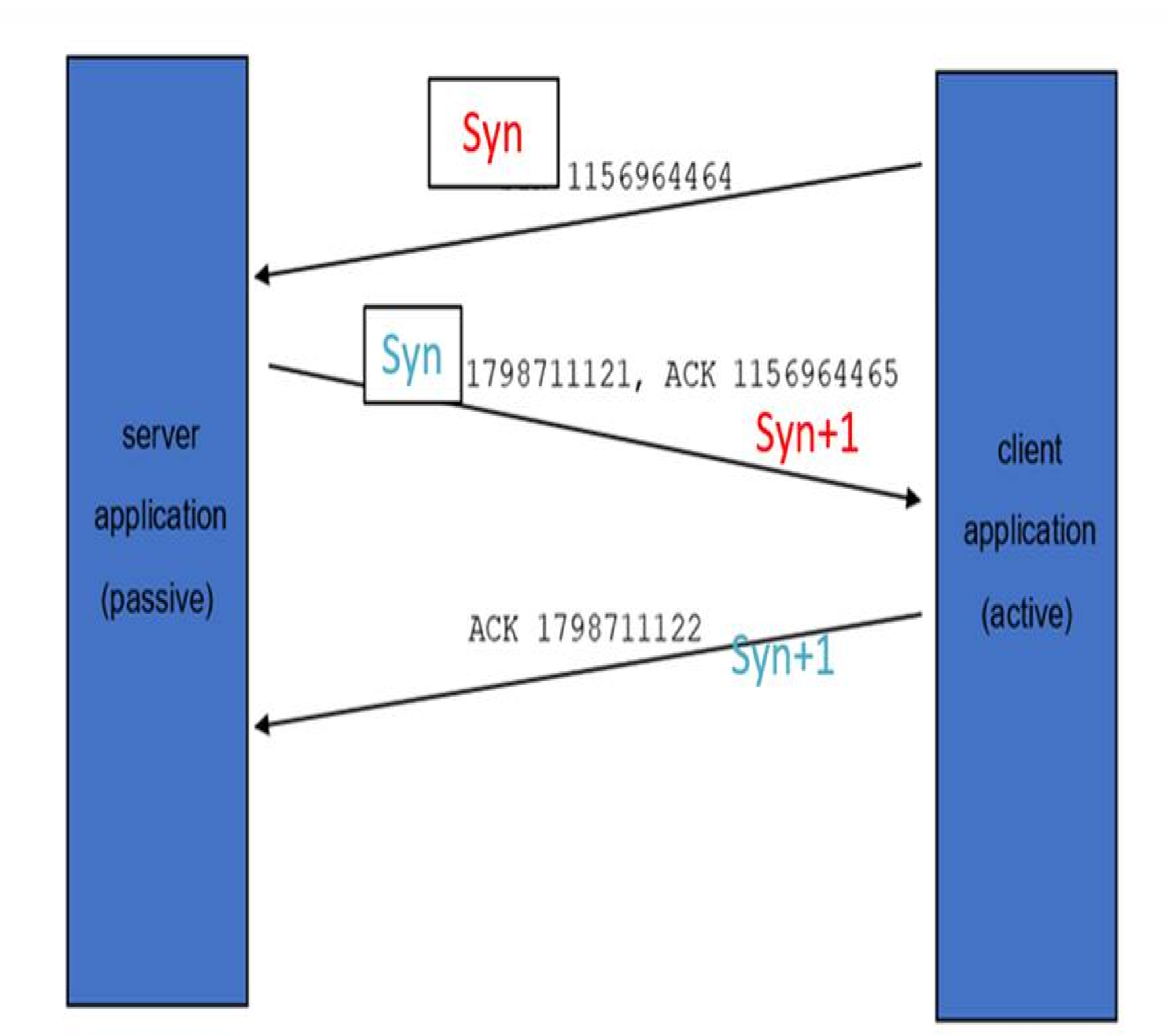
```
C:\Users\brianwan>telnet       | 53_
```

Source	Destination	Description
[redacted]OST2	[redacted]8	TCP:Flags=CE....S., SrcPort=60184, DstPort=DNS(53), PayloadLen=0, S
[redacted]	[redacted]HOST2	TCP:Flags=...A..S., SrcPort=DNS(53), DstPort=60184, PayloadLen=0, Se
[redacted]OST2	[redacted]8	TCP:Flags=...A...., SrcPort=60184, DstPort=DNS(53), PayloadLen=0, Se
[redacted]	[redacted]HOST2	TCP:Flags=...A...F, SrcPort=DNS(53), DstPort=60184, PayloadLen=0, Se
[redacted]OST2	[redacted]8	TCP:Flags=...A...., SrcPort=60184, DstPort=DNS(53), PayloadLen=0, Se
[redacted]OST2	[redacted]8	TCP:Flags=...A...F, SrcPort=60184, DstPort=DNS(53), PayloadLen=0, Se
[redacted]	[redacted]HOST2	TCP:Flags=...A...., SrcPort=DNS(53), DstPort=60184, PayloadLen=0, Se

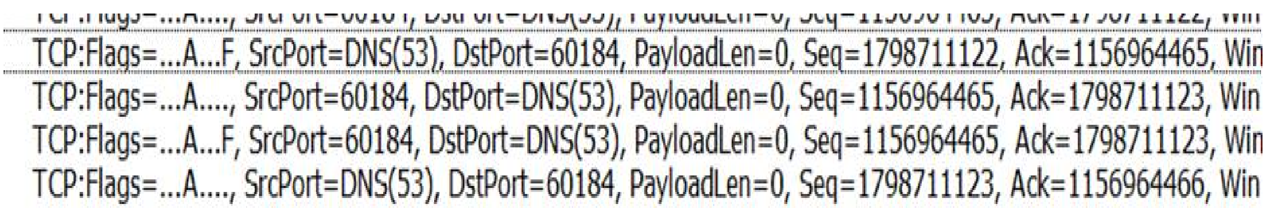


```
TCP:Flags=CE....S., SrcPort=60184, DstPort=DNS(53), PayloadLen=0, Seq=1156964464, Ack=0, Win=8192 ( I
TCP:Flags=...A..S., SrcPort=DNS(53), DstPort=60184, PayloadLen=0, Seq=1798711121, Ack=1156964465, W
TCP:Flags=...A...., SrcPort=60184, DstPort=DNS(53), PayloadLen=0, Seq=1156964465, Ack=1798711122, Wi
```

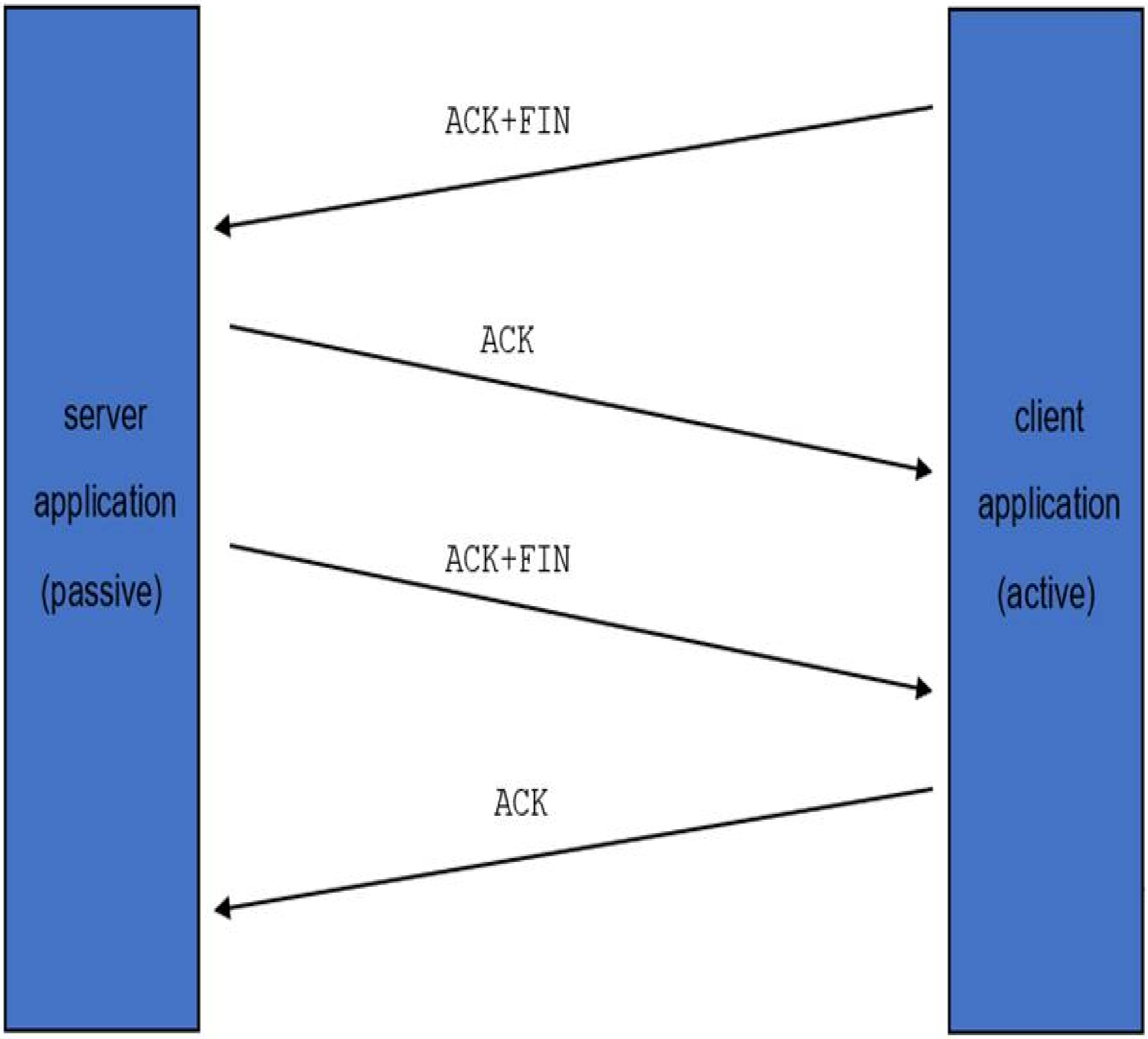
Based on the above tcp 3 handshake, you can see below pic.



4 handshake to finish the session would be following chart:



```
TCP:Flags=...A...., SrcPort=60184, DstPort=DNS(53), PayloadLen=0, Seq=1156964465, Ack=1798711122, Win
TCP:Flags=...A...F, SrcPort=DNS(53), DstPort=60184, PayloadLen=0, Seq=1798711122, Ack=1156964465, Win
TCP:Flags=...A...., SrcPort=60184, DstPort=DNS(53), PayloadLen=0, Seq=1156964465, Ack=1798711123, Win
TCP:Flags=...A...F, SrcPort=60184, DstPort=DNS(53), PayloadLen=0, Seq=1156964465, Ack=1798711123, Win
TCP:Flags=...A...., SrcPort=DNS(53), DstPort=60184, PayloadLen=0, Seq=1798711123, Ack=1156964466, Win
```



Created with Microsoft OneNote 2016.

How good have you found this content?

🙂 🙁