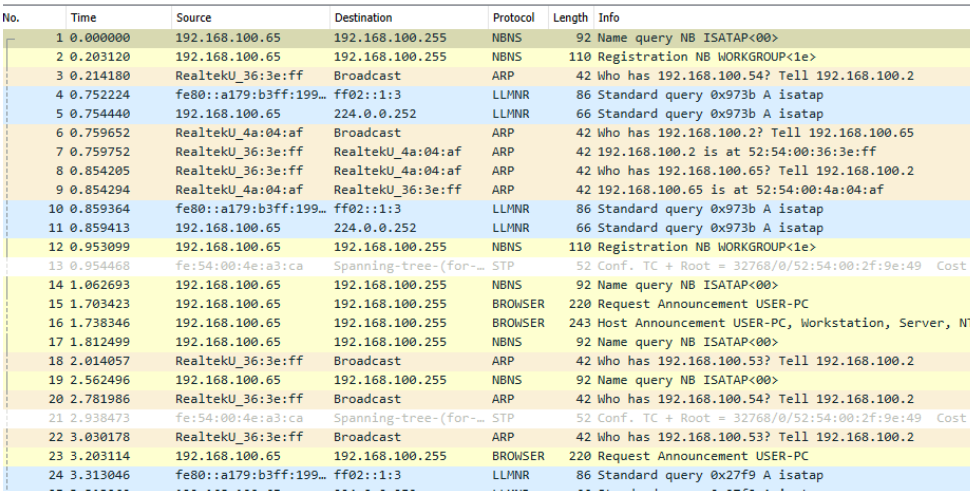
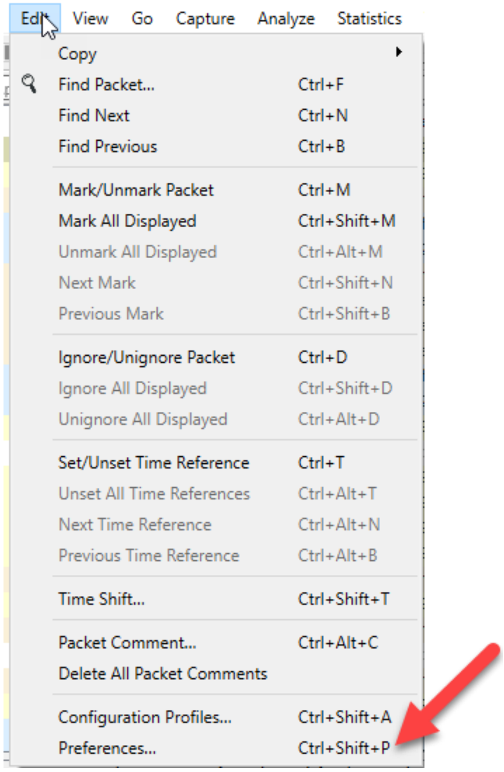
SecDSM October MiniCTF Walkthrough

We’re missing a few columns in within Wireshark. Specifically a Source port and a destination port column. Let’s fix that.

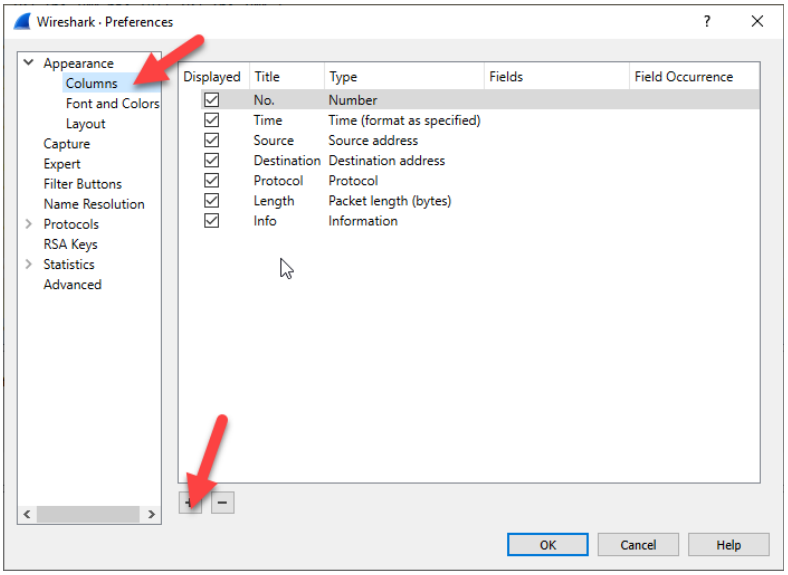


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.100.65	192.168.100.255	NBNS	92	Name query NB ISATAP<00>
2	0.203120	192.168.100.65	192.168.100.255	NBNS	110	Registration NB WORKGROUP<1e>
3	0.214180	RealtekU_36:3e:ff	Broadcast	ARP	42	Who has 192.168.100.54? Tell 192.168.100.2
4	0.752224	fe80::a179:b3ff:199…	ff02::1:3	LLMNR	86	Standard query 0x973b A isatap
5	0.754440	192.168.100.65	224.0.0.252	LLMNR	66	Standard query 0x973b A isatap
6	0.759652	RealtekU_4a:04:af	Broadcast	ARP	42	Who has 192.168.100.2? Tell 192.168.100.65
7	0.759752	RealtekU_36:3e:ff	RealtekU_4a:04:af	ARP	42	192.168.100.2 is at 52:54:00:36:3e:ff
8	0.854205	RealtekU_36:3e:ff	RealtekU_4a:04:af	ARP	42	Who has 192.168.100.65? Tell 192.168.100.2
9	0.854294	RealtekU_4a:04:af	RealtekU_36:3e:ff	ARP	42	192.168.100.65 is at 52:54:00:4a:04:af
10	0.859364	fe80::a179:b3ff:199…	ff02::1:3	LLMNR	86	Standard query 0x973b A isatap
11	0.859413	192.168.100.65	224.0.0.252	LLMNR	66	Standard query 0x973b A isatap
12	0.953099	192.168.100.65	192.168.100.255	NBNS	110	Registration NB WORKGROUP<1e>
13	0.954468	fe:54:00:4e:a3:ca	Spanning-tree-(for-…	STP	52	Conf. TC + Root = 32768/0/52:54:00:2f:9e:49 Cost
14	1.062693	192.168.100.65	192.168.100.255	NBNS	92	Name query NB ISATAP<00>
15	1.703423	192.168.100.65	192.168.100.255	BROWSER	220	Request Announcement USER-PC
16	1.738346	192.168.100.65	192.168.100.255	BROWSER	243	Host Announcement USER-PC, Workstation, Server, NT
17	1.812499	192.168.100.65	192.168.100.255	NBNS	92	Name query NB ISATAP<00>
18	2.014057	RealtekU_36:3e:ff	Broadcast	ARP	42	Who has 192.168.100.53? Tell 192.168.100.2
19	2.562496	192.168.100.65	192.168.100.255	NBNS	92	Name query NB ISATAP<00>
20	2.781986	RealtekU_36:3e:ff	Broadcast	ARP	42	Who has 192.168.100.54? Tell 192.168.100.2
21	2.938473	fe:54:00:4e:a3:ca	Spanning-tree-(for-…	STP	52	Conf. TC + Root = 32768/0/52:54:00:2f:9e:49 Cost
22	3.030178	RealtekU_36:3e:ff	Broadcast	ARP	42	Who has 192.168.100.53? Tell 192.168.100.2
23	3.203114	192.168.100.65	192.168.100.255	BROWSER	220	Request Announcement USER-PC
24	3.313046	fe80::a179:b3ff:199…	ff02::1:3	LLMNR	86	Standard query 0x27f9 A isatap

Go to Edit > Preferences:

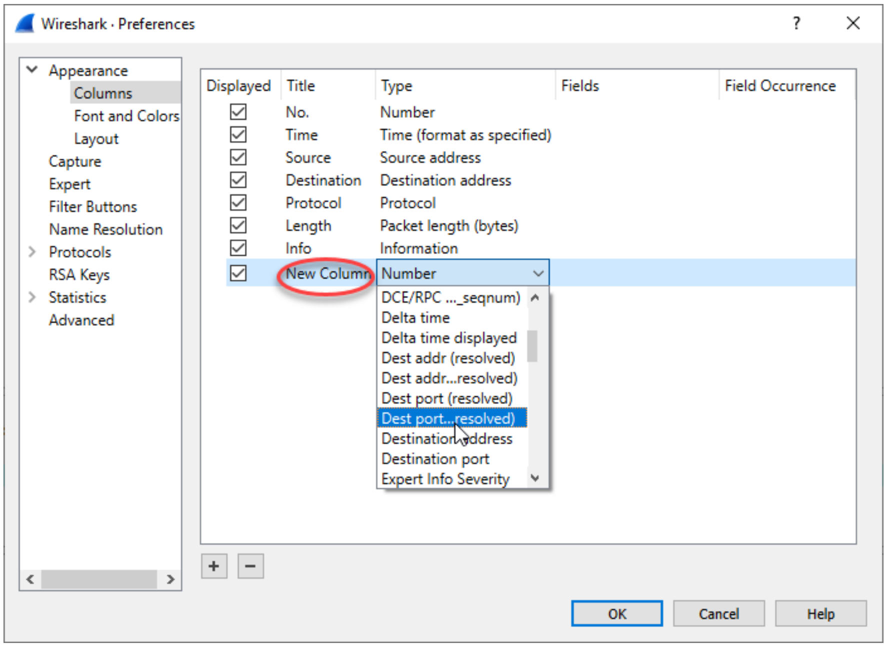

Edit
View
Go
Capture
Analyze
Statistics
Copy
Find Packet... Ctrl+F
Find Next Ctrl+N
Find Previous Ctrl+B
Mark/Unmark Packet Ctrl+M
Mark All Displayed Ctrl+Shift+M
Unmark All Displayed Ctrl+Alt+M
Next Mark Ctrl+Shift+N
Previous Mark Ctrl+Shift+B
Ignore/Unignore Packet Ctrl+D
Ignore All Displayed Ctrl+Shift+D
Unignore All Displayed Ctrl+Alt+D
Set/Unset Time Reference Ctrl+T
Unset All Time References Ctrl+Alt+T
Next Time Reference Ctrl+Alt+N
Previous Time Reference Ctrl+Alt+B
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Delete All Packet Comments
Configuration Profiles... Ctrl+Shift+A
Preferences... Ctrl+Shift+P

Under columns, select the “+” sign:



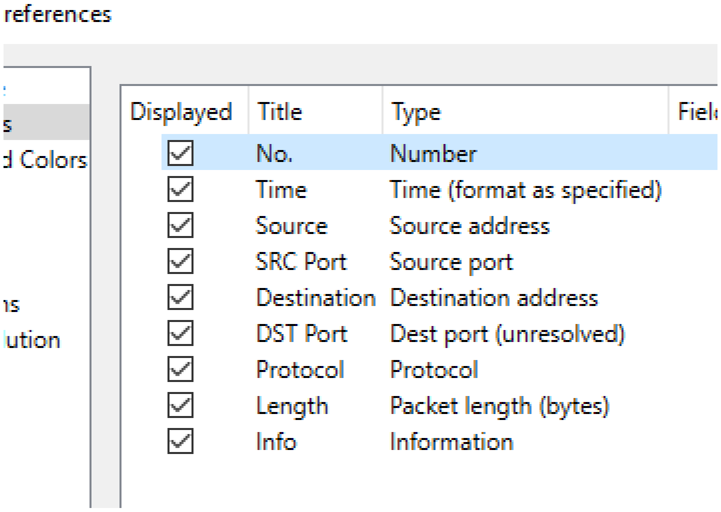
Displayed	Title	Type	Fields	Field Occurrence
☑	No.	Number		
☑	Time	Time (format as specified)		
☑	Source	Source address		
☑	Destination	Destination address		
☑	Protocol	Protocol		
☑	Length	Packet length (bytes)		
☑	Info	Information		

Rename “New column to Whatever you like (mine is set to SRC Port) and set the type dropdown to “Src Port (resolved)”. When setting the destination port the dropdown should be set to “Dest port unresolved” or “Dest port (..resolved)”:



Displayed	Title	Type	Fields	Field Occurrence
☑	No.	Number		
☑	Time	Time (format as specified)		
☑	Source	Source address		
☑	Destination	Destination address		
☑	Protocol	Protocol		
☑	Length	Packet length (bytes)		
☑	Info	Information		
☑	New Column	Number		

You can drag the columns to customize it to your liking. Typically it’s best to have src port display after source address and destination port after destination address. The order should look like this:



references

s

d Colors

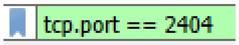
ns

ution

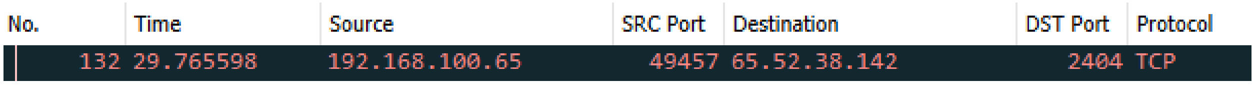
Displayed	Title	Type	Fiel
☑	No.	Number	
☑	Time	Time (format as specified)	
☑	Source	Source address	
☑	SRC Port	Source port	
☑	Destination	Destination address	
☑	DST Port	Dest port (unresolved)	
☑	Protocol	Protocol	
☑	Length	Packet length (bytes)	
☑	Info	Information	

Now that we have that taken care of, let’s take a look at the pcap file.

Scrolling through the PCAP, there was a packet that stood out pretty quickly under a strange destination port. Let’s investigate further by filtering the port in wireshark with “Tcp.port == 2404”:

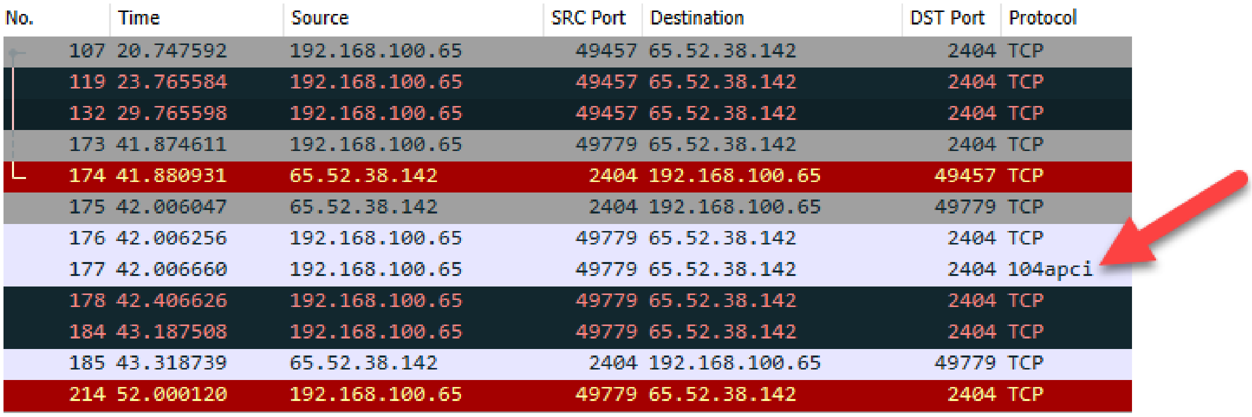


tcp.port == 2404



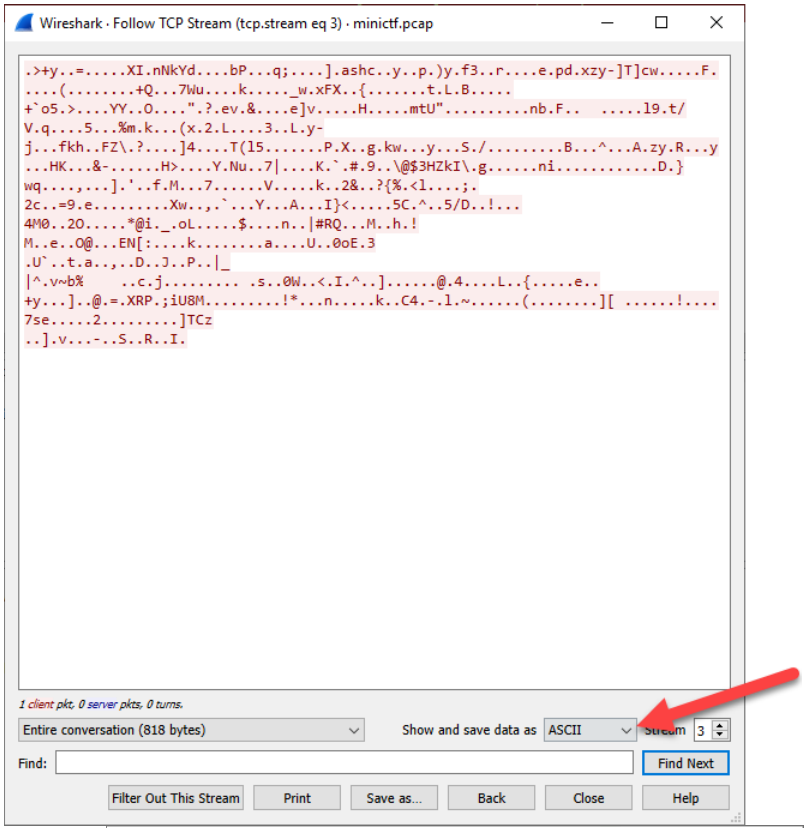
No.	Time	Source	SRC Port	Destination	DST Port	Protocol
132	29.765598	192.168.100.65	49457	65.52.38.142	2404	TCP

Our filtered results (shown below) indicate a strange protocol running on one of the packets. Let’s follow the tcp stream and take a deeper look:



No.	Time	Source	SRC Port	Destination	DST Port	Protocol
107	20.747592	192.168.100.65	49457	65.52.38.142	2404	TCP
119	23.765584	192.168.100.65	49457	65.52.38.142	2404	TCP
132	29.765598	192.168.100.65	49457	65.52.38.142	2404	TCP
173	41.874611	192.168.100.65	49779	65.52.38.142	2404	TCP
174	41.880931	65.52.38.142	2404	192.168.100.65	49457	TCP
175	42.006047	65.52.38.142	2404	192.168.100.65	49779	TCP
176	42.006256	192.168.100.65	49779	65.52.38.142	2404	TCP
177	42.006660	192.168.100.65	49779	65.52.38.142	2404	104apci
178	42.406626	192.168.100.65	49779	65.52.38.142	2404	TCP
184	43.187508	192.168.100.65	49779	65.52.38.142	2404	TCP
185	43.318739	65.52.38.142	2404	192.168.100.65	49779	TCP
214	52.000120	192.168.100.65	49779	65.52.38.142	2404	TCP

By default, packets in wireshark are displayed using ASCII, let's change it to a hex dump and see what we can find:



Wireshark · Follow TCP Stream (tcp.stream eq 3) · minictf.pcap

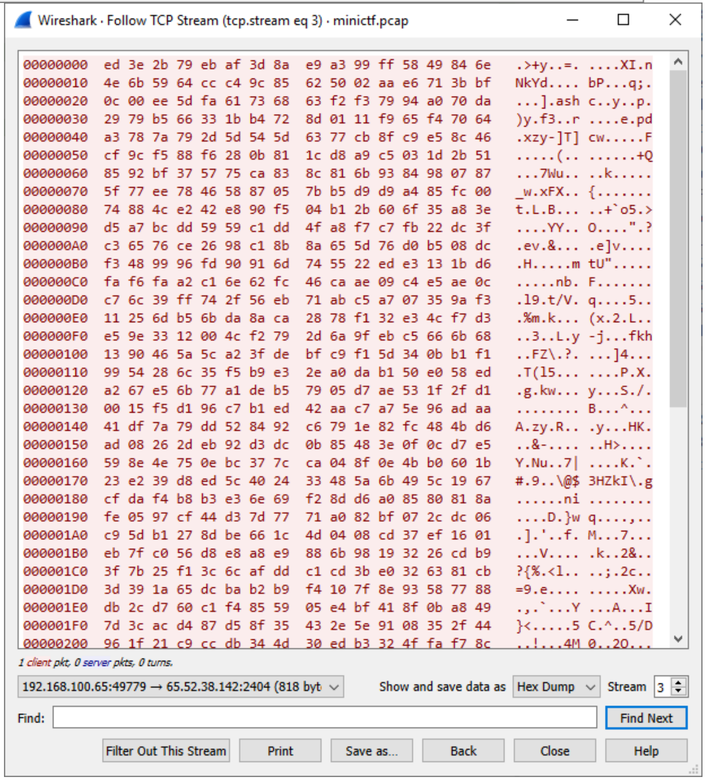
```
.>+y..=.....XI.nNkYd....bP...q;....].ashc..y..p.)y.f3..r....e.pd.xzy-]T]cw.....F.
....(........+Q...7Wu....k....._w.xFX..{.......t.L.B.....
+`o5.>....YY..O....".?.ev.&....e]v.....H.....mtU"..........nb.F..  .....l9.t/
V.q....5...%m.k...(x.2.L....3..L.y-
j...fkh..FZ\.?....]4....T(l5.......P.X..g.kw...y...S./.........B...^...A.zy.R...y
...HK...&-.......H>....Y.Nu..7|....K.`.#.9..\@$3HZkI\.g......ni............D.}
wq....,...].'..f.M...7......V.....k..2&..?{%.<l....;.
2c..=9.e..........Xw..,.`...Y...A...I}<.....5C.^..5/D..!...
4M0..2O.....*@i._.oL.....$....n..|#RQ...M..h.!
M..e..O@...EN[:....k.........a....U..0oE.3
.U`..t.a..,..D..J..P..|_
|^.v~b%    ..c.j......... .s..0W..<.I.^..]......@.4....L..{.....e..
+y...]..@.=.XRP.;iU8M.........!*...n.....k..C4.-.l.~......(........][ ......!....
7se.....2.........]TCz
..].v...-..S..R..I.
```

1 client pkt, 0 server pkts, 0 turns.

Entire conversation (818 bytes)

Show and save data as ASCII

Stream 3



Wireshark · Follow TCP Stream (tcp.stream eq 3) · minictf.pcap

```
00000000  ed 3e 2b 79 eb af 3d 8a  e9 a3 99 ff 58 49 84 6e   .>+y..=. ....XI.n
00000010  4e 6b 59 64 cc c4 9c 85  62 50 02 aa e6 71 3b bf   NkYd.... bP...q;.
00000020  0c 00 ee 5d fa 61 73 68  63 f2 f3 79 94 a0 70 da   ...].ash c..y..p.
00000030  29 79 b5 66 33 1b b4 72  8d 01 11 f9 65 f4 70 64   )y.f3..r ....e.pd
00000040  a3 78 7a 79 2d 5d 54 5d  63 77 cb 8f c9 e5 8c 46   .xzy-]T] cw.....F
00000050  cf 9c f5 88 f6 28 0b 81  1c d8 a9 c5 03 1d 2b 51   .....(.. ......+Q
00000060  85 92 bf 37 57 75 ca 83  8c 81 6b 93 84 98 07 87   ...7Wu.. ..k.....
00000070  5f 77 ee 78 46 58 87 05  7b b5 d9 d9 a4 85 fc 00   _w.xFX.. {.......
00000080  74 88 4c e2 42 e8 90 f5  04 b1 2b 60 6f 35 a8 3e   t.L.B... ..+`o5.>
00000090  d5 a7 bc dd 59 59 c1 dd  4f a8 f7 c7 fb 22 dc 3f   ....YY.. O....".?
000000A0  c3 65 76 ce 26 98 c1 8b  8a 65 5d 76 d0 b5 08 dc   .ev.&... .e]v....
000000B0  f3 48 99 96 fd 90 91 6d  74 55 22 ed e3 13 1b d6   .H.....m tU".....
000000C0  fa f6 fa a2 c1 6e 62 fc  46 ca ae 09 c4 e5 ae 0c   .....nb. F.......
000000D0  c7 6c 39 ff 74 2f 56 eb  71 ab c5 a7 07 35 9a f3   .l9.t/V. q....5..
000000E0  11 25 6d b5 6b da 8a ca  28 78 f1 32 e3 4c f7 d3   .%m.k... (x.2.L..
000000F0  e5 9e 33 12 00 4c f2 79  2d 6a 9f eb c5 66 6b 68   ..3..L.y -j...fkh
00000100  13 90 46 5a 5c a2 3f de  bf c9 f1 5d 34 0b b1 f1   ..FZ\.?. ...]4...
00000110  99 54 28 6c 35 f5 b9 e3  2e a0 da b1 50 e0 58 ed   .T(l5... ....P.X.
00000120  a2 67 e5 6b 77 a1 de b5  79 05 d7 ae 53 1f 2f d1   .g.kw... y...S./.
00000130  00 15 f5 d1 96 c7 b1 ed  42 aa c7 a7 5e 96 ad aa   ........ B...^...
00000140  41 df 7a 79 dd 52 84 92  c6 79 1e 82 fc 48 4b d6   A.zy.R.. .y...HK.
00000150  ad 08 26 2d eb 92 d3 dc  0b 85 48 3e 0f 0c d7 e5   ..&-.... ..H>....
00000160  59 8e 4e 75 0e bc 37 7c  ca 04 8f 0e 4b b0 60 1b   Y.Nu..7| ....K.`.
00000170  23 e2 39 d8 ed 5c 40 24  33 48 5a 6b 49 5c 19 67   #.9..\@$ 3HZkI\.g
00000180  cf da f4 b8 b3 e3 6e 69  f2 8d d6 a0 85 80 81 8a   ......ni ........
00000190  fe 05 97 cf 44 d3 7d 77  71 a0 82 bf 07 2c dc 06   ....D.}w q....,..
000001A0  c9 5d b1 27 8d be 66 1c  4d 04 08 cd 37 ef 16 01   .].'..f. M...7...
000001B0  eb 7f c0 56 d8 e8 a8 e9  88 6b 98 19 32 26 cd b9   ...V.... .k..2&..
000001C0  3f 7b 25 f1 3c 6c af dd  c1 cd 3b e0 32 63 81 cb   ?{%.<l.. ..;.2c..
000001D0  3d 39 1a 65 dc ba b2 b9  f4 10 7f 8e 93 58 77 88   =9.e.... .....Xw.
000001E0  db 2c d7 60 c1 f4 85 59  05 e4 bf 41 8f 0b a8 49   .,.`...Y ...A...I
000001F0  7d 3c ac d4 87 d5 8f 35  43 2e 5e 91 08 35 2f 44   }<.....5 C.^..5/D
00000200  96 1f 21 c9 cc db 34 4d  30 ed b3 32 4f fa f7 8c   ..!...4M 0..2O...
```

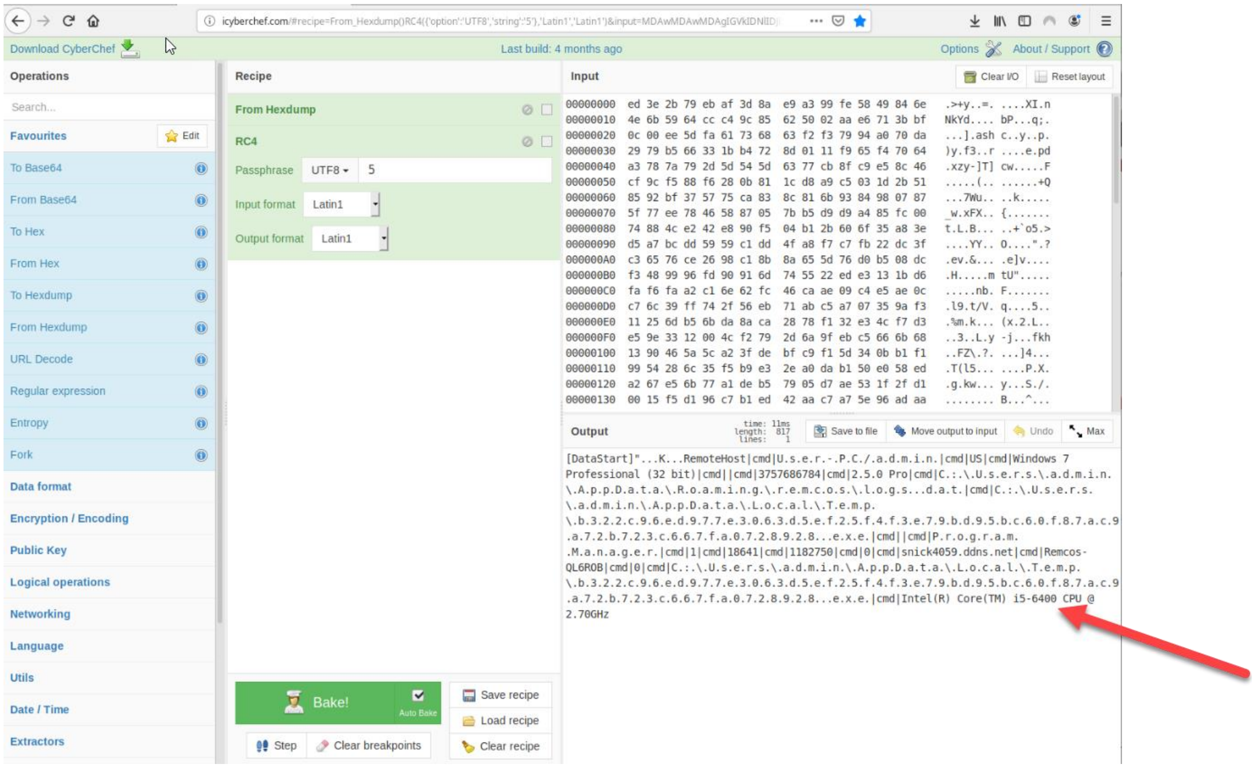
1 client pkt, 0 server pkts, 0 turns.

192.168.100.65:49779 → 65.52.38.142:2404 (818 byt

Show and save data as Hex Dump

Stream 3

Due to one of the hints given during the CTF, I realized that this was created using RC4 and that the passphase was a recurring character. Due to the nature of RC4, if you encrypt something with the passphrase “aaaaa”, when decrypting with the passphase “a”, you will decode the entire file. Cyberchef is a great tool for decrypting the hex code, so I copied the hex into the site, Set the recipe and pretty much brute forced the passphrase (a, b, c, d, etc). Eventually I got to numbers and when I hit “5”, the data in the screenshot below was displayed:



From Hexdump

RC4

Passphrase UTF8 5

Input format Latin1

Output format Latin1

```
00000000  ed 3e 2b 79 eb af 3d 8a  e9 a3 99 fe 58 49 84 6e   .>+y..=. ....XI.n
00000010  4e 6b 59 64 cc c4 9c 85  62 50 02 aa e6 71 3b bf   NkYd.... bP...q;.
00000020  0c 00 ee 5d fa 61 73 68  63 f2 f3 79 94 a0 70 da   ...].ash c..y..p.
00000030  29 79 b5 66 33 1b b4 72  8d 01 11 f9 65 f4 70 64   )y.f3..r ....e.pd
00000040  a3 78 7a 79 2d 5d 54 5d  63 77 cb 8f c9 e5 8c 46   .xzy-]T] cw.....F
00000050  cf 9c f5 88 f6 28 0b 81  1c d8 a9 c5 03 1d 2b 51   .....(.. ......+Q
00000060  85 92 bf 37 57 75 ca 83  8c 81 6b 93 84 98 07 87   ...7Wu.. ..k.....
00000070  5f 77 ee 78 46 58 87 05  7b b5 d9 d9 a4 85 fc 00   _w.xFX.. {.......
00000080  74 88 4c e2 42 e8 90 f5  04 b1 2b 60 6f 35 a8 3e   t.L.B... ..+`o5.>
00000090  d5 a7 bc dd 59 59 c1 dd  4f a8 f7 c7 fb 22 dc 3f   ....YY.. O....".?
000000A0  c3 65 76 ce 26 98 c1 8b  8a 65 5d 76 d0 b5 08 dc   .ev.&... .e]v....
000000B0  f3 48 99 96 fd 90 91 6d  74 55 22 ed e3 13 1b d6   .H.....m tU".....
000000C0  fa f6 fa a2 c1 6e 62 fc  46 ca ae 09 c4 e5 ae 0c   .....nb. F.......
000000D0  c7 6c 39 ff 74 2f 56 eb  71 ab c5 a7 07 35 9a f3   .l9.t/V. q....5..
000000E0  11 25 6d b5 6b da 8a ca  28 78 f1 32 e3 4c f7 d3   .%m.k... (x.2.L..
000000F0  e5 9e 33 12 00 4c f2 79  2d 6a 9f eb c5 66 6b 68   ..3..L.y -j...fkh
00000100  13 90 46 5a 5c a2 3f de  bf c9 f1 5d 34 0b b1 f1   ..FZ\.?. ...]4...
00000110  99 54 28 6c 35 f5 b9 e3  2e a0 da b1 50 e0 58 ed   .T(l5... ....P.X.
00000120  a2 67 e5 6b 77 a1 de b5  79 05 d7 ae 53 1f 2f d1   .g.kw... y...S./.
00000130  00 15 f5 d1 96 c7 b1 ed  42 aa c7 a7 5e 96 ad aa   ........ B...^...
```

```
time:   11ms
length:  817
lines:     1
```

```
[DataStart]"...K...RemoteHost|cmd|U.s.e.r.-.P.C./.a.d.m.i.n.|cmd|US|cmd|Windows 7
Professional (32 bit)|cmd||cmd|3757686784|cmd|2.5.0 Pro|cmd|C.:.\.U.s.e.r.s.\.a.d.m.i.n.
\.A.p.p.D.a.t.a.\.R.o.a.m.i.n.g.\.r.e.m.c.o.s.\.l.o.g.s...d.a.t.|cmd|C.:.\.U.s.e.r.s.
\.a.d.m.i.n.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.T.e.m.p.
\.b.3.2.2.c.9.6.e.d.9.7.7.e.3.0.6.3.d.5.e.f.2.5.f.4.f.3.e.7.9.b.d.9.5.b.c.6.0.f.8.7.a.c.9
.a.7.2.b.7.2.3.c.6.6.7.f.a.0.7.2.8.9.2.8...e.x.e.|cmd||cmd|P.r.o.g.r.a.m.
.M.a.n.a.g.e.r.|cmd|1|cmd|18641|cmd|1182750|cmd|0|cmd|snick4059.ddns.net|cmd|Remcos-
QL6ROB|cmd|0|cmd|C.:.\.U.s.e.r.s.\.a.d.m.i.n.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.T.e.m.p.
\.b.3.2.2.c.9.6.e.d.9.7.7.e.3.0.6.3.d.5.e.f.2.5.f.4.f.3.e.7.9.b.d.9.5.b.c.6.0.f.8.7.a.c.9
.a.7.2.b.7.2.3.c.6.6.7.f.a.0.7.2.8.9.2.8...e.x.e.|cmd|Intel(R) Core(TM) i5-6400 CPU @
2.70GHz
```

Final thoughts:

This CTF was new to me, as I did not have much experience in network forensics. I can say that I learned quite a bit from this one, and I hope to continue learning. I specifically wanted to thank SecDSM for this and developing the Secure Iowa 2019 CTF. Both of which I had an opportunity to take part and learn. I hope this walkthrough helps someone, and any new members who are afraid of entering CTFs, you won’t know what you are capable of until you try!!