

# Seeing the Invisible

Finding Fingerprints on Encrypted Traffic

Adel “0x4D31” Ka.

CHCon’19 / Kawaiicon’19, New Zealand

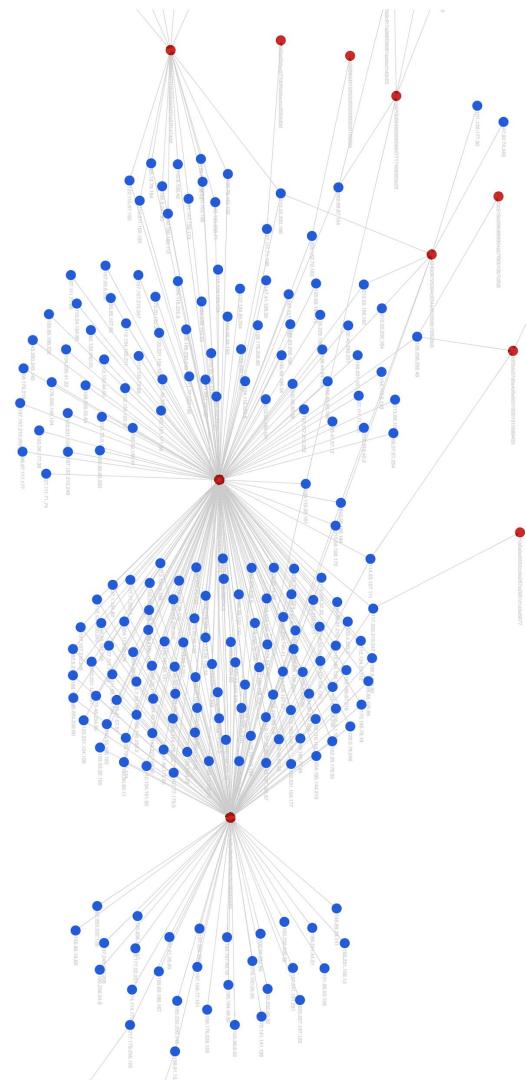
# \$whoami

> 0x4D31



- Honeynet Project
- Detecting badness at \*
- Hobbyist {astro}photographer
- [github.com/0x4D31](https://github.com/0x4D31)

\* Google



# The Problem

# Encrypted Traffic visibility

|    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |      |       |         |        |        |       |       |      |       |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|------|-------|---------|--------|--------|-------|-------|------|-------|
| 3c | 15 | c2 | df | 54 | 9c | 5c | 03 | 39 | cd | 0a | b2 | 08 | 00 | 45 | 00 | <..  | T \.  | 9 ..    | E      |        |       |       |      |       |
| 02 | 68 | 97 | fb | 00 | 00 | 7b | 06 | 43 | 47 | d8 | 3a | c8 | 63 | c0 | a8 | ..   | h ..  | { ..    | CG ..  | c ..   |       |       |      |       |
| 01 | 07 | 01 | bb | e4 | 47 | 62 | 6c | fc | 90 | 6b | e8 | b5 | af | 80 | 18 | ...  | Gbl   | ..      | k ..   |        |       |       |      |       |
| 00 | f0 | c4 | a7 | 00 | 00 | 01 | 01 | 08 | 0a | a5 | 29 | 25 | 03 | 2f | 00 | ...  | ...   | )% ..   | / ..   |        |       |       |      |       |
| 88 | ad | 17 | 03 | 03 | 01 | f1 | fd | 21 | b0 | 64 | fc | fc | de | 2c | 79 | ...  | !     | d ..    | ,y ..  |        |       |       |      |       |
| 25 | ee | ca | f5 | 83 | 92 | f7 | 2c | 36 | c3 | d0 | 9a | 61 | c9 | dd | d8 | % .. | ,     | 6 ..    | a ..   |        |       |       |      |       |
| 45 | b4 | ce | 7d | 46 | 55 | 2e | 6f | ec | 14 | c8 | a7 | a1 | b9 | d8 | 3d | E .. | }FU.o | ..      | = ..   |        |       |       |      |       |
| a6 | 39 | 9e | 00 | 84 | e2 | 00 | 5c | 4d | 6d | f5 | 22 | d7 | 3c | 92 | dd | ..   | 9 ..  | \ Mm .. | " ..   | < ..   |       |       |      |       |
| b2 | be | 5d | ab | e5 | a3 | 08 | 70 | c9 | bb | bc | e6 | 89 | 61 | ad | 45 | ..   | ]     | ..      | p ..   | a ..   | E ..  |       |      |       |
| c5 | 77 | e6 | bf | f0 | 45 | f3 | 56 | a1 | 85 | ae | bb | 9c | ce | 89 | 3e | ..   | w ..  | E ..    | V ..   | > ..   |       |       |      |       |
| 10 | 92 | 7e | c7 | 15 | 35 | ed | ab | d3 | 72 | 3c | 1e | c5 | bd | c4 | 8b | ..   | ~ ..  | 5 ..    | r < .. |        |       |       |      |       |
| 87 | 7c | 02 | 50 | 7e | a5 | fd | 96 | 58 | 60 | a3 | d8 | 80 | b6 | e5 | fe | ..   | ..    | P ..    | ~ ..   | X ..   |       |       |      |       |
| 2b | 17 | 74 | 77 | c0 | 75 | 6e | 19 | d5 | ed | 96 | 39 | 96 | c8 | 97 | dd | ..   | + ..  | tw ..   | un ..  | ..     | 9 ..  |       |      |       |
| 40 | 05 | ac | 28 | ed | 38 | 34 | 41 | ec | 63 | a3 | 0a | b7 | da | 95 | 10 | ..   | @ ..  | ( ..    | 84A .. | c ..   |       |       |      |       |
| 86 | 79 | e1 | 38 | f2 | b8 | 54 | 41 | f9 | d1 | 34 | 04 | 3e | 94 | a3 | d0 | ..   | y ..  | 8 ..    | TA ..  | ..     | 4 ..  | > ..  |      |       |
| b1 | 6f | b8 | 75 | b0 | e5 | 27 | c5 | 17 | 6a | 5d | c8 | f3 | 93 | be | c3 | ..   | o ..  | u ..    | ' ..   | j ..   |       |       |      |       |
| 9a | 5c | 98 | 65 | 6f | af | ec | d7 | 3f | 52 | 89 | b9 | 46 | 90 | 7d | 21 | ..   | \ ..  | eo ..   | ? ..   | R ..   | F ..  | ..    |      |       |
| 35 | 72 | f4 | 63 | 2f | 4d | 35 | 2a | 56 | b3 | e8 | ad | 7f | d8 | 2f | 5b | ..   | 5r .. | c ..    | M5 ..  | *      | V ..  | ..    | / .. |       |
| 6f | b6 | 8d | 34 | 12 | da | e1 | a5 | cd | 66 | 57 | 98 | 8e | ed | 65 | 2e | ..   | o ..  | 4 ..    | ..     | fW ..  | e ..  |       |      |       |
| 71 | 8a | dc | fe | 8f | 44 | 5b | 40 | 70 | ab | d2 | f4 | 94 | 00 | a7 | 36 | ..   | q ..  | ..      | D ..   | [@ ..  | p ..  | ..    | 6 .. |       |
| e3 | a2 | 43 | 3d | d1 | af | 25 | 97 | 98 | 6b | 49 | 3c | 8f | 2b | 40 | 61 | ..   | ..    | C ..    | = ..   | % ..   | kI .. | < ..  | +    | @a .. |
| bf | af | 7d | 89 | 85 | 7a | 05 | c8 | 1d | f0 | d6 | 0c | c9 | 86 | 8d | f4 | ..   | ..    | }       | ..     | z ..   |       |       |      |       |
| 2a | 52 | fd | e4 | 17 | 4b | d5 | cd | 79 | 13 | f5 | 51 | 8d | c4 | 7e | 54 | ..   | *R .. | K ..    | y ..   | Q ..   | ~T .. |       |      |       |
| 54 | ae | e5 | c4 | f6 | 40 | 26 | 02 | cf | 2e | c3 | 81 | fc | 15 | 4e | a6 | ..   | T ..  | @& ..   | .      | .      | N ..  |       |      |       |
| 14 | 73 | b6 | a8 | ea | 93 | d0 | 2c | 6d | a1 | e2 | c5 | 58 | b5 | 63 | e7 | ..   | s ..  | ..      | ,      | m ..   | X ..  | c ..  |      |       |
| e0 | ab | c9 | c9 | 7a | ad | dc | be | 8a | 62 | 44 | 77 | 3c | db | 64 | c0 | ..   | ..    | z ..    | ..     | bDw .. | < ..  | d ..  |      |       |
| 42 | d4 | b9 | 94 | 39 | 56 | 87 | 72 | 60 | eb | 3e | 1c | be | 9f | 98 | a2 | ..   | B ..  | 9V ..   | r ..   | ` ..   | > ..  |       |      |       |
| 8b | e5 | 34 | 62 | 01 | ac | 5a | 5b | d4 | 89 | 6c | 27 | d8 | 41 | f8 | 7c | ..   | ..    | 4b ..   | Z ..   | [ ..   | l ..  | A ..  | ..   |       |
| 7b | 34 | 95 | 81 | 0c | 8f | 32 | 72 | 4b | e3 | ae | 3e | fd | 66 | 53 | a7 | ..   | {4 .. | ..      | 2r ..  | K ..   | > ..  | fS .. |      |       |
| bd | 13 | d9 | 03 | af | d1 | 99 | 17 | 9e | 55 | 95 | 2b | c0 | 07 | 91 | 64 | ..   | ..    | ..      | ..     | U ..   | +     | d ..  |      |       |
| 3b | b9 | 0e | ea | f4 | d6 | ca | a4 | dc | 82 | 04 | bd | b3 | 53 | b6 | 99 | ..   | ;     | ..      | ..     | ..     | S ..  |       |      |       |
| 79 | 88 | c9 | 00 | f4 | ea | f7 | 9b | 40 | 45 | 82 | a0 | 51 | e5 | fc | 91 | ..   | y ..  | ..      | ..     | @E ..  | Q ..  |       |      |       |
| 3b | 74 | 74 | 89 | 2d | c6 | 26 | e8 | b5 | 18 | 46 | b3 | 37 | df | fb | 8a | ..   | ;     | tt ..   | -      | & ..   | F ..  | 7 ..  |      |       |

|    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |        |          |        |        |       |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|--------|----------|--------|--------|-------|
| 3c | 15 | c2 | df | 54 | 9c | 5c | 03 | 39 | cd | 0a | b2 | 08 | 00 | 45 | 00 | <..    | T \      | 9 ..   | E      |       |
| 02 | 68 | 97 | fb | 00 | 00 | 7b | 06 | 43 | 47 | d8 | 3a | c8 | 63 | c0 | a8 | h ..   | { ..     | CG ..  | c ..   |       |
| 01 | 07 | 01 | bb | e4 | 47 | 62 | 6c | fc | 90 | 6b | e8 | b5 | af | 80 | 18 | Gbl .. | k ..     |        |        |       |
| 00 | f0 | c4 | a7 | 00 | 00 | 01 | 01 | 08 | 0a | a5 | 29 | 25 | 03 | 2f | 00 |        |          | )% ..  | / ..   |       |
| 88 | ad | 17 | 03 | 03 | 01 | f1 | fd | 21 | b0 | 64 | fc | fc | de | 2c | 79 | !      | d ..     | ,y ..  |        |       |
| 25 | ee | ca | f5 | 83 | 92 | f7 | 2c | 36 | c3 | d0 | 9a | 61 | c9 | dd | d8 | % ..   | ,        | 6 ..   | a ..   |       |
| 45 | b4 | ce | 7d | 46 | 55 | 2e | 6f | ec | 14 | c8 | a7 | a1 | b9 | d8 | 3d | E ..   | }FU.o .. | = ..   |        |       |
| a6 | 39 | 9e | 00 | 84 | e2 | 00 | 5c | 4d | 6d | f5 | 22 | d7 | 3c | 92 | dd | 9 ..   | \ Mm ..  | " ..   | < ..   |       |
| b2 | be | 5d | ab | e5 | a3 | 08 | 70 | c9 | bb | bc | e6 | 89 | 61 | ad | 45 | ]      | ..       | p ..   | a ..   | E ..  |
| c5 | 77 | e6 | bf | f0 | 45 | f3 | 56 | a1 | 85 | ae | bb | 9c | ce | 89 | 3e | w ..   | E ..     | V ..   | > ..   |       |
| 10 | 92 | 7e | c7 | 15 | 35 | ed | ab | d3 | 72 | 3c | 1e | c5 | bd | c4 | 8b | ..~ .. | 5 ..     | r ..   | < ..   |       |
| 87 | 7c | 02 | 50 | 7e | a5 | fd | 96 | 58 | 60 | a3 | d8 | 80 | b6 | e5 | fe | ..     | P ..     | X ..   |        |       |
| 2b | 17 | 74 | 77 | c0 | 75 | 6e | 19 | d5 | ed | 96 | 39 | 96 | c8 | 97 | dd | + ..   | tw ..    | un ..  | 9 ..   |       |
| 40 | 05 | ac | 28 | ed | 38 | 34 | 41 | ec | 63 | a3 | 0a | b7 | da | 95 | 10 | @ ..   | ( ..     | 84A .. | c ..   |       |
| 86 | 79 | e1 | 38 | f2 | b8 | 54 | 41 | f9 | d1 | 34 | 04 | 3e | 94 | a3 | d0 | y ..   | 8 ..     | TA ..  | 4 ..   | > ..  |
| b1 | 6f | b8 | 75 | b0 | e5 | 27 | c5 | 17 | 6a | 5d | c8 | f3 | 93 | be | c3 | o ..   | u ..     | ' ..   | j ..   |       |
| 9a | 5c | 98 | 65 | 6f | af | ec | d7 | 3f | 52 | 89 | b9 | 46 | 90 | 7d | 21 | \ ..   | eo ..    | ?R ..  | F ..   | }! .. |
| 35 | 72 | f4 | 63 | 2f | 4d | 35 | 2a | 56 | b3 | e8 | ad | 7f | d8 | 2f | 5b | 5r ..  | c/M5*    | V ..   | / ..   | [ ..  |
| 6f | b6 | 8d | 34 | 12 | da | e1 | a5 | cd | 66 | 57 | 98 | 8e | ed | 65 | 2e | o ..   | 4 ..     | fW ..  | e ..   | .     |
| 71 | 8a | dc | fe | 8f | 44 | 5b | 40 | 70 | ab | d2 | f4 | 94 | 00 | a7 | 36 | q ..   | D[@      | p ..   | 6 ..   |       |
| e3 | a2 | 43 | 3d | d1 | af | 25 | 97 | 98 | 6b | 49 | 3c | 8f | 2b | 40 | 61 | C= ..  | % ..     | kI <   | +@a .. |       |
| bf | af | 7d | 89 | 85 | 7a | 05 | c8 | 1d | f0 | d6 | 0c | c9 | 86 | 8d | f4 | }      | ..       | z ..   |        |       |
| 2a | 52 | fd | e4 | 17 | 4b | d5 | cd | 79 | 13 | f5 | 51 | 8d | c4 | 7e | 54 | *R ..  | K ..     | y ..   | Q ..   | ~T .. |
| 54 | ae | e5 | c4 | f6 | 40 | 26 | 02 | cf | 2e | c3 | 81 | fc | 15 | 4e | a6 | T ..   | @& ..    | .      | .      | N ..  |
| 14 | 73 | b6 | a8 | ea | 93 | d0 | 2c | 6d | a1 | e2 | c5 | 58 | b5 | 63 | e7 | s ..   | ,        | m ..   | X ..   | c ..  |
| e0 | ab | c9 | c9 | 7a | ad | dc | be | 8a | 62 | 44 | 77 | 3c | db | 64 | c0 | z ..   | ..       | bDw <  | d ..   |       |
| 42 | d4 | b9 | 94 | 39 | 56 | 87 | 72 | 60 | eb | 3e | 1c | be | 9f | 98 | a2 | B ..   | 9V ..    | r ..   | > ..   |       |
| 8b | e5 | 34 | 62 | 01 | ac | 5a | 5b | d4 | 89 | 6c | 27 | d8 | 41 | f8 | 7c | 4b ..  | Z[ ..    | l' ..  | A ..   | ..    |
| 7b | 34 | 95 | 81 | 0c | 8f | 32 | 72 | 4b | e3 | ae | 3e | fd | 66 | 53 | a7 | {4 ..  | 2r ..    | K ..   | > ..   | fS .. |
| bd | 13 | d9 | 03 | af | d1 | 99 | 17 | 9e | 55 | 95 | 2b | c0 | 07 | 91 | 64 | ..     | ..       | U ..   | +      | d ..  |
| 3b | b9 | 0e | ea | f4 | d6 | ca | a4 | dc | 82 | 04 | bd | b3 | 53 | b6 | 99 | ;      | ..       | ..     | S ..   |       |
| 79 | 88 | c9 | 00 | f4 | ea | f7 | 9b | 40 | 45 | 82 | a0 | 51 | e5 | fc | 91 | y ..   | ..       | @E ..  | Q ..   |       |
| 3b | 74 | 74 | 89 | 2d | c6 | 26 | e8 | b5 | 18 | 46 | b3 | 37 | df | fb | 8a | tt ..  | -& ..    | F ..   | 7 ..   |       |

# Encrypted Traffic



good traffic?

3c 15 c2 df 54 9c 5c 03 39 cd 0a b2 08 00 45 00 <.. T \ . 9 .. E  
02 68 97 fb 00 00 7b 06 43 47 d8 3a c8 63 c0 a8 h .. { . CG : . c ..  
01 07 01 bb e4 47 62 6c fc 90 6b e8 b5 af 80 18 Gbl .. k ..  
00 f0 c4 a7 00 00 01 01 08 0a a5 29 25 03 2f 00 ..... ) % / ..  
88 ad 17 03 ! d .. , y ..  
25 ee ca f5 , 6 .. a ..  
45 b4 ce 7d } FU . o .. = ..\br/>a6 39 9e 00 \ Mm .. " < ..  
b2 be 5d ab .. p .. a E ..  
c5 77 e6 bf .. E V .. > ..  
10 92 7e c7 .. 5 .. r < ..  
87 7c 02 50 P ~ .. X ` ..  
2b 17 74 77 w .. un .. 9 ..  
40 05 ac 28 ( .. 84A .. c ..  
86 79 e1 38 8 .. TA .. 4 .. > ..  
b1 6f b8 75 u .. ' .. j ] ..  
9a 5c 98 65 eo .. ? R .. F .. } ! ..  
35 72 f4 63 c / M5 \* V .. .. / [ ..  
6f b6 8d 34 4 .. f W .. e ..  
71 8a dc fe .. D [ @ p .. .. 6 ..  
e3 a2 43 3d = .. % .. k I < .. + @ a ..  
bf af 7d 89 .. z ..  
2a 52 fd e4 .. K .. y .. Q .. ~ T ..  
54 ae e5 c4 .. @ & .. . .. N ..  
14 73 b6 a8 .. , .. m .. X .. c ..  
e0 ab c9 c9 .. z .. b Dw < .. d ..  
42 d4 b9 94 .. 9 V .. r .. > ..  
8b e5 34 62 b .. Z [ .. l ' .. A .. | ..  
7b 34 95 81 .. 2 r .. K .. > .. f S ..  
  
bd 13 d9 03 af d1 99 17 9e 55 95 2b c0 07 91 64 .. U .. + .. d ..  
3b b9 0e ea f4 d6 ca a4 dc 82 04 bd b3 53 b6 99 ; .. S ..  
79 88 c9 00 f4 ea f7 9b 40 45 82 a0 51 e5 fc 91 y .. @ E .. Q ..  
3b 74 74 89 2d c6 26 e8 b5 18 46 b3 37 df fb 8a ; tt .. - .. & .. F .. 7 ..



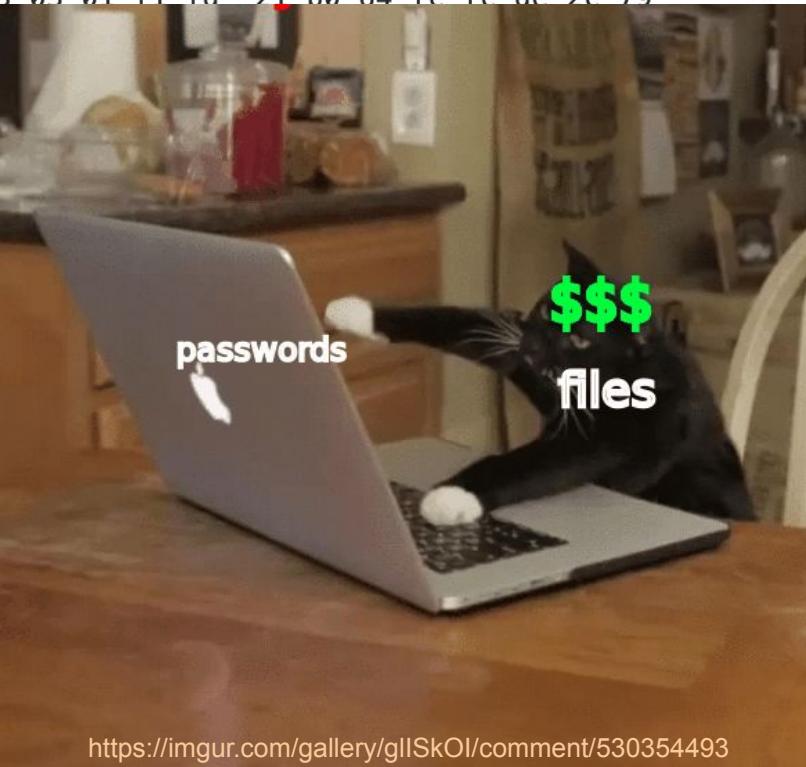
imgflip.com

## Encrypted Traffic

('o\_o')

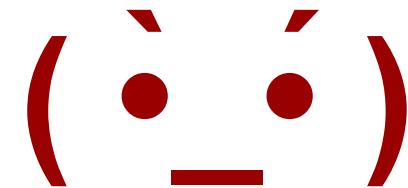
good traffic?

```
3c 15 c2 df 54 9c 5c 03 39 cd 0a b2 08 00 45 00 <...T\ 9...E  
02 68 97 fb 00 00 7b 06 43 47 d8 3a c8 63 c0 a8 h...{ CG::c  
01 07 01 bb e4 47 62 6c fc 90 6b e8 b5 af 80 18 Gbl ..k  
00 f0 c4 a7 00 00 01 01 08 0a a5 29 25 03 2f 00 .....)%/  
88 ad 17 03 03 01 f1 fd 21 b0 64 fc fc de 2c 79 !d..,y  
25 ee ca f ,6..a  
45 b4 ce 7 o...= =  
a6 39 9e 0 \Mm..<..  
b2 be 5d a p.....a.E  
c5 77 e6 b V....>  
10 92 7e c .r<.  
87 7c 02 5 X`..  
2b 17 74 7 .9...  
40 05 ac 2 A..c  
86 79 e1 3 A..4>..  
b1 6f b8 7 ..j]  
9a 5c 98 6 ?R..F..}!  
35 72 f4 6 *V.../[  
6f b6 8d 3 ..fW..e.  
71 8a dc f @p.....6  
e3 a2 43 3 ..kI<.+@a  
bf af 7d 8 ..  
2a 52 fd e y..Q..~T  
54 ae e5 c ..N..  
14 73 b6 a ,m...X.c  
e0 ab c9 c ..bDw<d  
42 d4 b9 9 r..>..  
8b e5 34 6 [..l'..A.|  
7b 34 95 81 0c 81 32 72 4b e5 ae 3e 1d 66 53 a/ ..zr K..>..fS.  
bd 13 d9 03 af d1 99 17 9e 55 95 2b c0 07 91 64 .....U+..d  
3b b9 0e ea f4 d6 ca a4 dc 82 04 bd b3 53 b6 99 ;.....S..  
79 88 c9 00 f4 ea f7 9b 40 45 82 a0 51 e5 fc 91 y.....@E..Q..  
3b 74 74 89 2d c6 26 e8 b5 18 46 b3 37 df fb 8a ;tt--& ..F..7..
```



<https://imgur.com/gallery/gII SkOI/comment/530354493>

# Encrypted Traffic



bad traffic?

# Encrypted Traffic

Any Clues!? 

|    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |          |          |          |          |       |    |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----------|----------|----------|----------|-------|----|
| 02 | 68 | 97 | fb | 00 | 00 | 7b | 06 | 43 | 47 | d8 | 3a | c8 | 63 | c0 | a8 | <..      | T \.     | 9 ..     | E        |       |    |
| 01 | 07 | 01 | bb | e4 | 47 | 62 | 6c | fc | 90 | 6b | e8 | b5 | af | 80 | 18 | ..h ..   | {..      | CG ..    | c ..     |       |    |
| 00 | f0 | c4 | a7 | 00 | 00 | 01 | 01 | 08 | 0a | a5 | 29 | 25 | 03 | 2f | 00 | ..Gbl .. | k ..     | ..)      | % /      |       |    |
| 88 | ad | 17 | 03 | 03 | 01 | f1 | fd | 21 | b0 | 64 | fc | fc | de | 2c | 79 | ..!      | d ..     | ,y       |          |       |    |
| 25 | ee | ca | f5 | 83 | 92 | f7 | 2c | 36 | c3 | d0 | 9a | 61 | c9 | dd | d8 | % ..     | ,        | 6 ..     | a ..     |       |    |
| 45 | b4 | ce | 7d | 46 | 55 | 2e | 6f | ec | 14 | c8 | a7 | a1 | b9 | d8 | 3d | E ..     | }FU.o .. | =        |          |       |    |
| a6 | 39 | 9e | 00 | 84 | e2 | 00 | 5c | 4d | 6d | f5 | 22 | d7 | 3c | 92 | dd | ..9 ..   | \ Mm ..  | " < ..   |          |       |    |
| b2 | be | 5d | ab | e5 | a3 | 08 | 70 | c9 | bb | bc | e6 | 89 | 61 | ad | 45 | ..]      | ..p ..   | a ..     | E ..     |       |    |
| c5 | 77 | e6 | bf | f0 | 45 | f3 | 56 | a1 | 85 | ae | bb | 9c | ce | 89 | 3e | ..w ..   | E ..     | V ..     | >        |       |    |
| 10 | 92 | 7e | c7 | 15 | 35 | ed | ab | d3 | 72 | 3c | 1e | c5 | bd | c4 | 8b | ..~ ..   | 5 ..     | r < ..   |          |       |    |
| 87 | 7c | 02 | 50 | 7e | a5 | fd | 96 | 58 | 60 | a3 | d8 | 80 | b6 | e5 | fe | ..  ..   | P ..     | X ..     |          |       |    |
| 2b | 17 | 74 | 77 | c0 | 75 | 6e | 19 | d5 | ed | 96 | 39 | 96 | c8 | 97 | dd | + ..t    | w ..     | un ..    | 9 ..     |       |    |
| 40 | 05 | ac | 28 | ed | 38 | 34 | 41 | ec | 63 | a3 | 0a | b7 | da | 95 | 10 | @ ..     | ( ..     | 84A ..   | c ..     |       |    |
| 86 | 79 | e1 | 38 | f2 | b8 | 54 | 41 | f9 | d1 | 34 | 04 | 3e | 94 | a3 | d0 | ..y ..   | 8 ..     | TA ..    | 4 ..> .. |       |    |
| b1 | 6f | b8 | 75 | b0 | e5 | 27 | c5 | 17 | 6a | 5d | c8 | f3 | 93 | be | c3 | ..o ..   | u ..     | ' ..     | j ..     |       |    |
| 9a | 5c | 98 | 65 | 6f | af | ec | d7 | 3f | 52 | 89 | b9 | 46 | 90 | 7d | 21 | ..\\ ..  | eo ..    | ?R ..    | F ..     | }! .. |    |
| 35 | 72 | f4 | 63 | 2f | 4d | 35 | 2a | 56 | b3 | e8 | ad | 7f | d8 | 2f | 5b | 5r ..    | c/M5*    | V ..     | /[ ..    |       |    |
| 6f | b6 | 8d | 34 | 12 | da | e1 | a5 | cd | 66 | 57 | 98 | 8e | ed | 65 | 2e | o ..     | 4 ..     | fW ..    | e ..     |       |    |
| 71 | 8a | dc | fe | 8f | 44 | 5b | 40 | 70 | ab | d2 | f4 | 94 | 00 | a7 | 36 | q ..     | D ..     | [@ ..    | p ..     | 6 ..  |    |
| e3 | a2 | 43 | 3d | d1 | af | 25 | 97 | 98 | 6b | 49 | 3c | 8f | 2b | 40 | 61 | ..C ..   | = ..%    | kI < ..  | +@a ..   |       |    |
| bf | af | 7d | 89 | 85 | 7a | 05 | c8 | 1d | f0 | d6 | 0c | c9 | 86 | 8d | f4 | ..}      | ..z ..   |          |          |       |    |
| 2a | 52 | fd | e4 | 17 | 4b | d5 | cd | 79 | 13 | f5 | 51 | 8d | c4 | 7e | 54 | *R ..    | -K ..    | y ..     | Q ..     | ~T .. |    |
| 54 | ae | e5 | c4 | f6 | 40 | 26 | 02 | cf | 2e | c3 | 81 | fc | 15 | 4e | a6 | T ..     | @& ..    | .        | .        | N ..  |    |
| 14 | 73 | b6 | a8 | ea | 93 | d0 | 2c | 6d | a1 | e2 | c5 | 58 | b5 | 63 | e7 | ..s ..   | ,        | m ..     | X ..     | c ..  |    |
| e0 | ab | c9 | c9 | 7a | ad | dc | be | 8a | 62 | 44 | 77 | 3c | db | 64 | c0 | ..z ..   | .        | bDw < .. | d ..     |       |    |
| 42 | d4 | b9 | 94 | 39 | 56 | 87 | 72 | 60 | eb | 3e | 1c | be | 9f | 98 | a2 | B ..     | 9V ..    | r ..     | > ..     |       |    |
| 8b | e5 | 34 | 62 | 01 | ac | 5a | 5b | d4 | 89 | 6c | 27 | d8 | 41 | f8 | 7c | ..4b ..  | Z ..     | [ ..     | l ..     | A ..  | .. |
| 7b | 34 | 95 | 81 | 0c | 8f | 32 | 72 | 4b | e3 | ae | 3e | fd | 66 | 53 | a7 | {4 ..    | 2r ..    | K ..     | > ..     | fS .. |    |
| bd | 13 | d9 | 03 | af | d1 | 99 | 17 | 9e | 55 | 95 | 2b | c0 | 07 | 91 | 64 | ..       | ..       | U ..     | +        | d ..  |    |
| 3b | b9 | 0e | ea | f4 | d6 | ca | a4 | dc | 82 | 04 | bd | b3 | 53 | b6 | 99 | ;        | ..       | ..       | S ..     |       |    |
| 79 | 88 | c9 | 00 | f4 | ea | f7 | 9b | 40 | 45 | 82 | a0 | 51 | e5 | fc | 91 | y ..     | ..       | @E ..    | Q ..     |       |    |
| 3b | 74 | 74 | 89 | 2d | c6 | 26 | e8 | b5 | 18 | 46 | b3 | 37 | df | fb | 8a | ;;tt ..  | -& ..    | F ..     | 7 ..     |       |    |

```
c 15 c2 df 54 9c 5c 03 39 cd 0a b2 08 00 45 00 <...T\ 9...E  
02 68 97 fb 00 00 7b 06 43 47 d8 3a c8 63 c0 a8 h...{CG::c  
01 07 ▼ Transport Layer Security  
00 f0 ▼ TLSv1.3 Record Layer: Handshake Protocol: Client Hello  
88 ad Content Type: Handshake (22)  
25 ee Version: TLS 1.0 (0x0301)  
45 b4 Length: 512  
a6 39 ▼ Handshake Protocol: Client Hello  
b2 be Handshake Type: Client Hello (1)  
c5 77 Length: 508  
10 92 Version: TLS 1.2 (0x0303)  
87 7c Random: 3b6ef74c373ac3d85d4087fa3cf5f4b1ecf128eba4822a8  
2b 17 Session ID Length: 32  
40 05 Session ID: 0c90f77f3b044e135d44fa5191eb87a966fa5cc5bb2  
86 79 Cipher Suites Length: 34  
b1 6f ► Cipher Suites (17 suites)  
9a 5c Compression Methods Length: 1  
35 72 ► Compression Methods (1 method)  
6f b6 Extensions Length: 401  
71 8a ► Extension: Reserved (GREASE) (len=0)  
e3 a2 ► Extension: server_name (len=21)  
bf af ► Extension: extended_master_secret (len=0)  
2a 52 ► Extension: renegotiation_info (len=1)  
54 ae ► Extension: supported_groups (len=10)  
14 73 ► Extension: ec_point_formats (len=2)  
e0 ab ► Extension: session_ticket (len=0)  
42 d4 ► Extension: application_layer_protocol_negotiation (len=0)  
8b e5 ► Extension: status_request (len=5)  
7b 34 ► Extension: signature_algorithms (len=20)  
bd 13 ► Extension: signed_certificate_timestamp (len=0)  
3b b9 ► Extension: key_share (len=43)  
99 88 ► Extension: psk_key_exchange_modes (len=2)  
3b 74 c9 00 f4 ea f7 9b 40 45 82 a0 51 e5 fc 91 y...@E...Q...  
3b 74 74 89 2d c6 26 e8 b5 18 46 b3 37 df fb 8a ;tt--&...F 7...
```

# Encrypted Traffic

Any Clues!? 

# Network Metadata & Fingerprints

Can we use  
Network Metadata & Fingerprints to  
**profile the attackers and tools,**

Can we use  
Network Metadata & Fingerprints to  
**discover hidden connections,**

Can we use  
Network Metadata & Fingerprints to  
possibly **find new evasion methods!?**

# Background

# Fingerprinting

OS Fingerprinting

httpprint

JA3

Browser Fingerprinting

SSL/TLS Fingerprinting

p0f

Application Fingerprinting

fingerprinTLS

HASSH

sslhaf

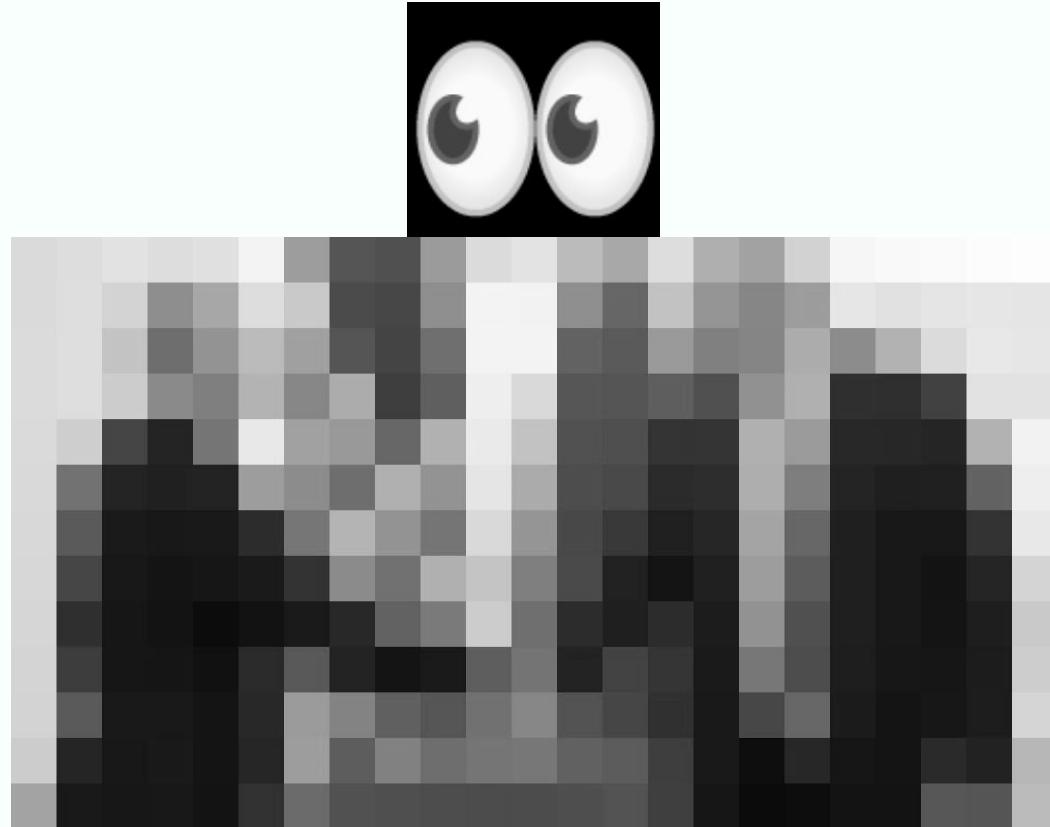


Cryptographic  
protocols need  
to negotiate  
some parameters  
in **clear-text**!

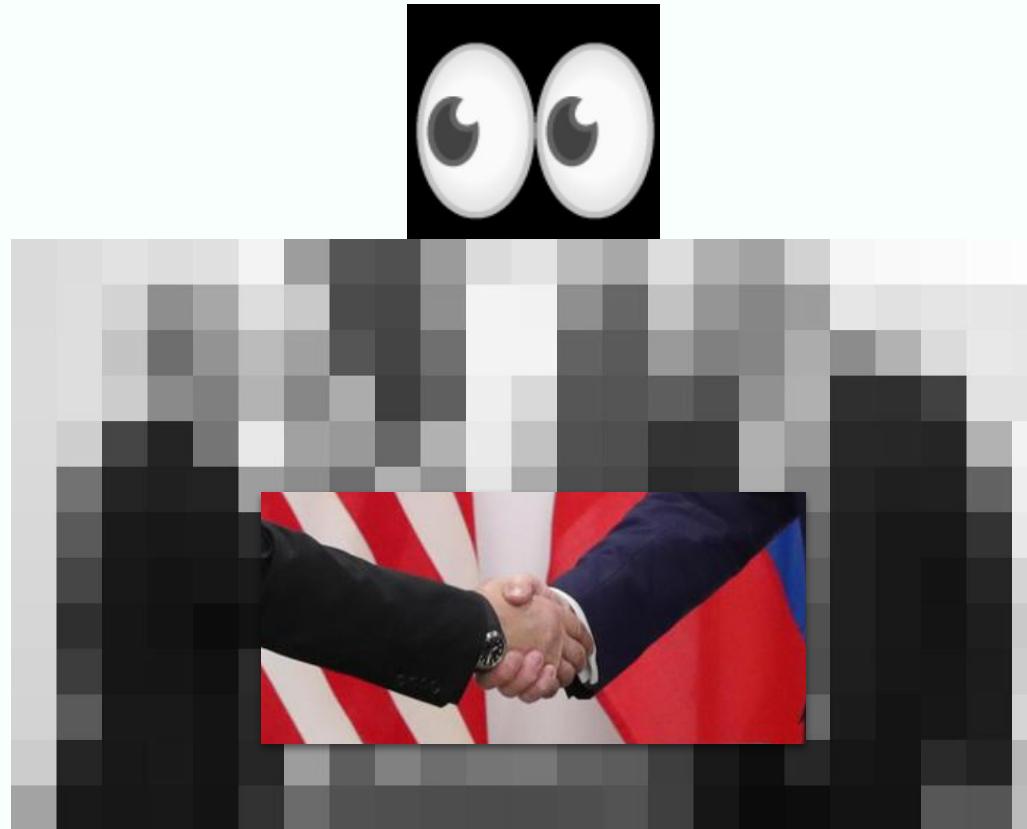
Cryptographic  
protocols need  
to **negotiate**  
some parameters  
in **clear-text!**



Cryptographic  
protocols need  
to **negotiate**  
some parameters  
in **clear-text!**



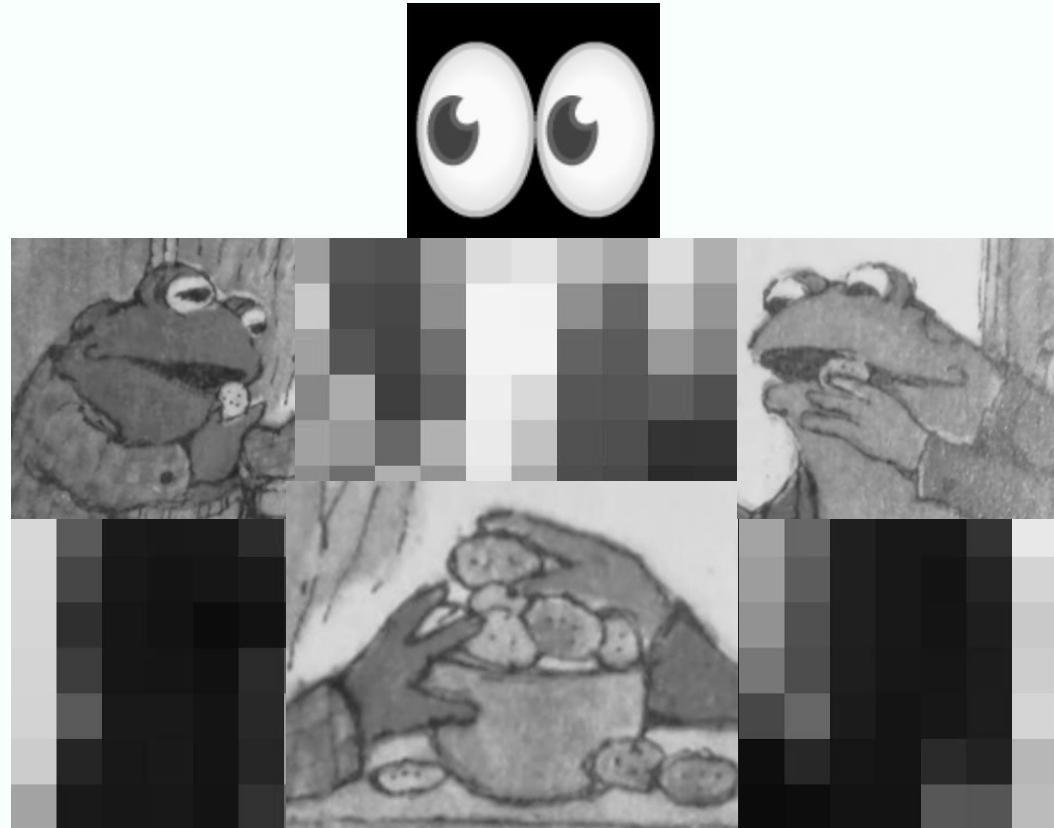
Cryptographic  
protocols need  
to **negotiate**  
some parameters  
in **clear-text**!



Cryptographic  
protocols need  
to **negotiate**  
some parameters  
in **clear-text**!



Cryptographic  
protocols need  
to **negotiate**  
some parameters  
in **clear-text!**



*Frog and Toad* is illustrated by Arnold Lobel

# TLS Client/Server Fingerprinting

using client/server Hello messages

▼ Transport Layer Security  
  ▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello  
    Content Type: Handshake (22)  
    Version: TLS 1.0 (0x0301)  
    Length: 329  
  ▼ Handshake Protocol: Client Hello  
    Handshake Type: Client Hello (1)  
    Length: 325  
    Version: TLS 1.2 (0x0303)  
    ► Random: 8bd177cdf0d6c9ed5e3186125abd35f5a023e3ce8a1fa512...  
    Session ID Length: 0  
    Cipher Suites Length: 148  
  ▼ Cipher Suites (74 suites)  
    Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_CHACHA20\_POLY1305\_SHA256 (0xcc14)  
    Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_CHACHA20\_POLY1305\_SHA256 (0xcc13)  
    Cipher Suite: TLS\_DHE\_RSA\_WITH\_CHACHA20\_POLY1305\_SHA256 (0xcc15)  
    Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (0xc030)  
    Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384 (0xc02c)  
    Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384 (0xc028)  
    Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384 (0xc024)  
    Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA (0xc014)  
    Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA (0xc00a)  
    Cipher Suite: TLS\_DH\_DSS\_WITH\_AES\_256\_GCM\_SHA384 (0x00a5)  
    Cipher Suite: TLS\_DHE\_DSS\_WITH\_AES\_256\_GCM\_SHA384 (0x00a3)  
    Cipher Suite: TLS\_DH\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (0x00a1)  
    Cipher Suite: TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (0x009f)  
    Cipher Suite: TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA256 (0x006b)

|      |                         |                         |                      |
|------|-------------------------|-------------------------|----------------------|
| 0000 | 86 51 a4 84 a5 e5 cc e1 | 7f a8 17 f0 08 00 45 00 | ·Q..... . . . . E    |
| 0010 | 01 82 a4 92 40 00 35 06 | c0 4e d9 b6 8f 61 45 37 | .....@·5· N · aE7    |
| 0020 | 31 46 a0 4b 01 bb 81 39 | 32 e7 b8 64 f6 46 80 18 | 1F·K· · 9 2· d·F· .. |
| 0030 | 00 e5 62 e6 00 00 01 01 | 08 0a 04 4c 96 88 25 f6 | ·b..... ·L·%· ..     |
| 0040 | 13 c3 16 03 01 01 49 01 | 00 01 45 03 03 8b d1 77 | .....I· . E· .. w    |
| 0050 | cd f0 d6 c9 ed 5e 31 86 | 12 5a bd 35 f5 a0 23 e3 | .....^1· . Z·5·#· .. |
| 0060 | ce 8a 1f a5 12 6c 18 8f | fa ff 4a 8f c7 00 00 94 | .....l· . J· .. ..   |
| 0070 | cc 14 cc 13 cc 15 c0 30 | c0 2c c0 28 c0 24 c0 14 | .....0· ,·(·\$.. ..  |
| 0080 | c0 0a 00 a5 00 a3 00 a1 | 00 9f 00 6b 00 6a 00 69 | ..... . . k·j·i ..   |
| 0090 | 00 68 00 39 00 38 00 37 | 00 36 c0 32 c0 2e c0 2a | ·h·9·8·7· .6·2·..*   |
| 00a0 | c0 26 c0 0f c0 05 00 9d | 00 3d 00 35 00 95 c0 2f | &..... =·5·/ ..      |
| 00b0 | c0 2b c0 27 c0 23 c0 13 | c0 09 00 a4 00 a2 00 a0 | ++·'·#.. .. ..       |
| 00c0 | 00 9e 00 67 00 40 00 3f | 00 3e 00 33 00 32 00 31 | ..g·@·?· .>·3·2·1 .. |
| 00d0 | 00 30 c0 31 c0 2d c0 29 | c0 25 c0 0e c0 04 00 9c | ·0·1·..) .%.. ..     |
| 00e0 | 00 3c 00 2f 00 94 00 9a | 00 99 00 98 00 97 00 96 | ..</· .. .. ..       |
| 00f0 | 00 07 c0 11 c0 07 00 66 | c0 0c c0 02 00 05 00 04 | .....f .. .. ..      |

# TLS

<client Hello>

# SSL/TLS Handshake

- Message Flow for a SSL/TLS Handshake



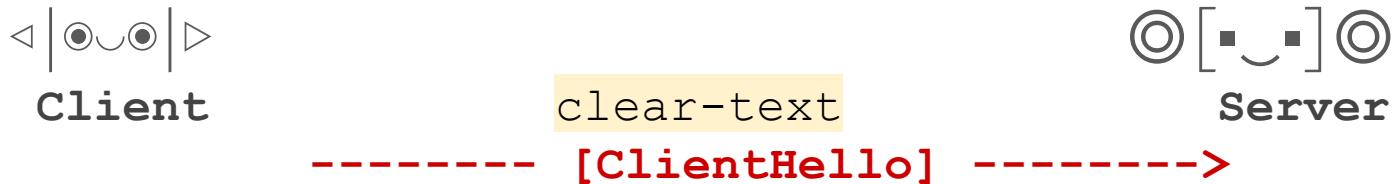
**Client**



**Server**

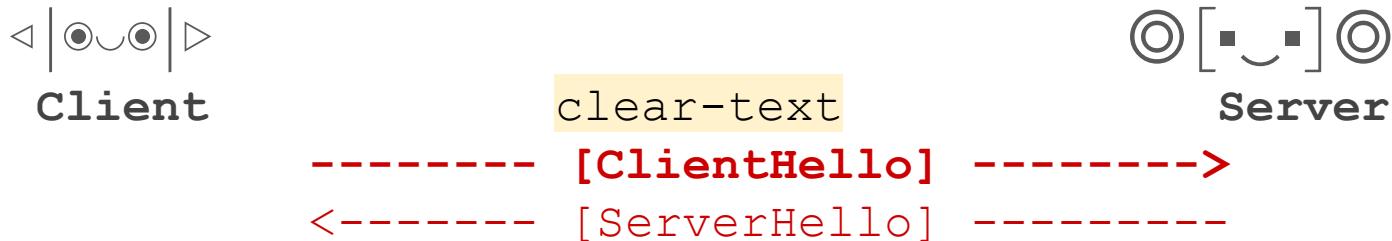
# SSL/TLS Handshake

- Message Flow for a SSL/TLS Handshake



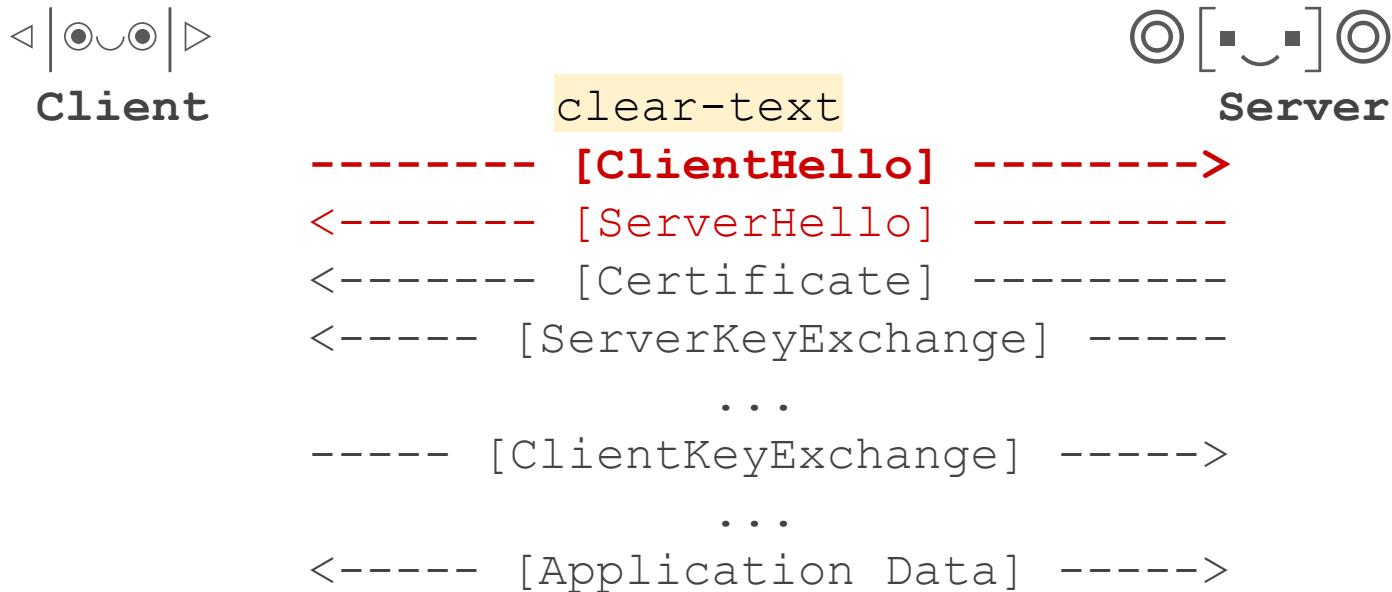
# SSL/TLS Handshake

- Message Flow for a SSL/TLS Handshake



# SSL/TLS Handshake

- Message Flow for a SSL/TLS Handshake



# SSL/TLS ClientHello

```
struct {
    ProtocolVersion client_version;
    Random random;
    SessionID session_id;
    CipherSuite cipher_suites<2..2^16-2>;
    Compression Method compression_methods<1..2^8-1>;
    select (extensions_present) {
        case false:
            struct {};
        case true:
            Extension extensions<0..2^16-1>;
    };
} ClientHello;
```

Reference: <https://tools.ietf.org/html/rfc5246>

# SSL/TLS ClientHello

```
struct {
    ProtocolVersion client_version;
    Random random;
    SessionID session_id;
    CipherSuite cipher_suites<2>;
    Compression Method compression;
    select (extensions_present)
        case false:
            struct {};
        case true:
            Extension extension;
    };
} ClientHello;
```

▼ Transport Layer Security  
▼ TLSv1.3 Record Layer: Handshake Protocol: Client Hello  
    Content Type: Handshake (22)  
    Version: TLS 1.0 (0x0301)  
    Length: 512  
▼ Handshake Protocol: Client Hello  
    Handshake Type: Client Hello (1)  
        Length: 508  
        Version: TLS 1.2 (0x0303)  
        Random: 3b6ef74c373ac3d85d4087fa3cf5f4b1ecf128eba4822a8  
        Session ID Length: 32  
        Session ID: 0c90f77f3b044e135d44fa5191eb87a966fa5cc5bb2  
        Cipher Suites Length: 34  
        ► Cipher Suites (17 suites)  
            Compression Methods Length: 1  
        ► Compression Methods (1 method)  
            Extensions Length: 401  
        ► Extension: Reserved (GREASE) (len=0)  
        ► Extension: server\_name (len=21)  
        ► Extension: extended\_master\_secret (len=0)  
        ► Extension: renegotiation\_info (len=1)  
        ► Extension: supported\_groups (len=10)  
        ► Extension: ec\_point\_formats (len=2)  
        ► Extension: session\_ticket (len=0)  
        ► Extension: application\_layer\_protocol\_negotiation (len=

Reference: <https://tools.ietf.org/html/rfc5246>

# SSL/TLS ClientHello

```
struct {
    ProtocolVersion client_version;
    Random random;
    SessionID session_id;
    CipherSuite cipher_suites<2..2^16>;
    Compression Method compression;
    select (extensions_present) {
        case false:
            struct {};
        case true:
            Extension extensions<0..2^16>;
    };
} ClientHello;
```

▼ Transport Layer Security

▼ TLSv1.3 Record Layer: Handshake Protocol: Client Hello

    Content Type: Handshake (22)

    Version: TLS 1.0 (0x0301)

    Length: 512

▼ Handshake Protocol: Client Hello

    Handshake Type: Client Hello (1)

    Length: 508

**Version: TLS 1.2 (0x0303)**

Session ID: 0c90f77f3b044e135d44fa5191eb87a966fa5cc5bb2

Cipher Suites Length: 34

► Cipher Suites (17 suites)

► Compression Methods Length: 1

► Compression Methods (1 method)

Extensions Length: 401

► Extension: Reserved (GREASE) (len=0)

► Extension: server\_name (len=21)

► Extension: extended\_master\_secret (len=0)

► Extension: renegotiation\_info (len=1)

► Extension: supported\_groups (len=10)

► Extension: ec\_point\_formats (len=2)

► Extension: session\_ticket (len=0)

► Extension: application\_layer\_protocol\_negotiation (len=

Reference: <https://tools.ietf.org/html/rfc5246>

# SSL/TLS ClientHello

```
struct {
    ProtocolVersion client_version;
    Random random;
    SessionID session_id;
    CipherSuite cipher_suites<2>;
    Compression Method compression;
    select (extensions_present) {
        case false:
            struct {};
        case true:
            Extension extensions<0..2016>;
    };
} ClientHello;
```

▼ Transport Layer Security

▼ TLSv1.3 Record Layer: Handshake Protocol: Client Hello

    Content Type: Handshake (22)

    Version: TLS 1.0 (0x0301)

    Length: 512

▼ Handshake Protocol: Client Hello

    Handshake Type: Client Hello (1)

    Length: 508

Cipher Suites Length: 34

Cipher Suites (17 suites)

    cipher\_suites (17 suites)

    Compression Methods Length: 1

- Compression Methods (1 method)
- Extensions Length: 401
- Extension: Reserved (GREASE) (len=0)
- Extension: server\_name (len=21)
- Extension: extended\_master\_secret (len=0)
- Extension: renegotiation\_info (len=1)
- Extension: supported\_groups (len=10)
- Extension: ec\_point\_formats (len=2)
- Extension: session\_ticket (len=0)
- Extension: application\_layer\_protocol\_negotiation (len=

Reference: <https://tools.ietf.org/html/rfc5246>

The cipher suite list is in order of  
the **client's preference** !

# SSL/TLS ClientHello

```
struct {
    ProtocolVersion client_version;
    Random random;
    SessionID session_id;
    CipherSuite cipher_suites<2>;
    Compression Method compression;
    select (extensions_present)
        case false:
            struct {};
        case true:
            Extension extensions;
    };
} ClientHello;
```

▼ Transport Layer Security

▼ TLSv1.3 Record Layer: Handshake Protocol: Client Hello

    Content Type: Handshake (22)

    Version: TLS 1.0 (0x0301)

    Length: 512

▼ Handshake Protocol: Client Hello

    Handshake Type: Client Hello (1)

    Length: 508

Extensions Length: 401

Extension: Reserved (GREASE)

Extension: server\_name (len=2)

Extension: extended\_master\_se

Extension: renegotiation\_info

Extension: supported\_groups (

Extension: ec\_point\_formats (

► Extension: session\_ticket (len=0)

► Extension: application\_layer\_protocol\_negotiation (len=

Reference: <https://tools.ietf.org/html/rfc5246>

# TLS Fingerprinting

sslhaf [1]

FingerprinTLS [2]

JA3 [3]

[1] **sslhaf**: Ivan Ristic, <https://blog.ivanristic.com/2009/06/http-client-fingerprinting-using-ssl-handshake-analysis.html>, 2009

[2] **fingerprinTLS**: Lee Brotherton, <https://blog.squarelemon.com/tls-fingerprinting/>, 2015

[3] **JA3**: John Althouse, Jeff Atkinson, Josh Atkins, <https://engineering.salesforce.com/open-sourcing-ja3-92c9e53c3c41>, 2017

# TLS Fingerprinting

sslhaf [1]

fingerprinTLS [2]

JA3 [3]

[1] **sslhaf**: Ivan Ristic, <https://blog.ivanristic.com/2009/06/http-client-fingerprinting-using-ssl-handshake-analysis.html>, 2009

[2] **fingerprinTLS**: Lee Brotherton, <https://blog.squarelemon.com/tls-fingerprinting/>, 2015

[3] **JA3**: John Althouse, Jeff Atkinson, Josh Atkins, <https://engineering.salesforce.com/open-sourcing-ja3-92c9e53c3c41>, 2017

# TLS Fingerprinting

sslhaf [1]

FingerprintTLS [2]

JA3 [3]

Easy to produce!  
Can be easily shared!

[1] **sslhaf**: Ivan Ristic, <https://blog.ivanristic.com/2009/06/http-client-fingerprinting-using-ssl-handshake-analysis.html>, 2009

[2] **fingerprintTLS**: Lee Brotherston, <https://blog.squarelemon.com/tls-fingerprinting/>, 2015

[3] **JA3**: John Althouse, Jeff Atkinson, Josh Atkins, <https://engineering.salesforce.com/open-sourcing-ja3-92c9e53c3c41>, 2017

# Fingerprinting TLS client/servers with JA3 \*

Concatenate the decimal value of

SSL Version

771,

\* JA3: John Althouse, Jeff Atkinson, Josh Atkins, <https://engineering.salesforce.com/open-sourcing-ja3-92c9e53c3c41>, 2017

# Fingerprinting TLS client/servers with JA3 \*

Concatenate the decimal value of

Cipher Suites

771,4865-4866-4867-49195-49199-49196-49200-5239  
3-52392-49171-49172-156-157-47-53-10,

\* JA3: John Althouse, Jeff Atkinson, Josh Atkins, <https://engineering.salesforce.com/open-sourcing-ja3-92c9e53c3c41>, 2017

# Fingerprinting TLS client/servers with JA3 \*

Concatenate the decimal value of

## Extensions

771,4865-4866-4867-49195-49199-49196-49200-5239  
3-52392-49171-49172-156-157-47-53-10,0-23-65281-1  
0-11-35-16-5-13-18-51-45-43-27-21,

\* JA3: John Althouse, Jeff Atkinson, Josh Atkins, <https://engineering.salesforce.com/open-sourcing-ja3-92c9e53c3c41>, 2017

# Fingerprinting TLS client/servers with JA3 \*

Concatenate the decimal value of

**Elliptic Curves / Supported Groups**

771,4865-4866-4867-49195-49199-49196-49200-5239  
3-52392-49171-49172-156-157-47-53-10,0-23-65281-1  
0-11-35-16-5-13-18-51-45-43-27-21,29-23-24,

\* JA3: John Althouse, Jeff Atkinson, Josh Atkins, <https://engineering.salesforce.com/open-sourcing-ja3-92c9e53c3c41>, 2017

# Fingerprinting TLS client/servers with JA3 \*

Concatenate the decimal value of

## EC Point Formats

771,4865-4866-4867-49195-49199-49196-49200-5239  
3-52392-49171-49172-156-157-47-53-10,0-23-65281-1  
0-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0

\* JA3: John Althouse, Jeff Atkinson, Josh Atkins, <https://engineering.salesforce.com/open-sourcing-ja3-92c9e53c3c41>, 2017

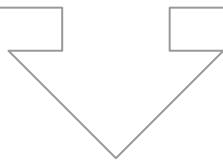
# Fingerprinting TLS client/servers with JA3 \*

771,4865-4866-4867-49195-49199-49196-49200-523  
93-52392-49171-49172-156-157-47-53-10,0-23-6528  
1-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0

\* JA3: John Althouse, Jeff Atkinson, Josh Atkins, <https://engineering.salesforce.com/open-sourcing-ja3-92c9e53c3c41>, 2017

# Fingerprinting TLS client/servers with JA3 \*

771,4865-4866-4867-49195-49199-49196-49200-523  
93-52392-49171-49172-**MD5**157-47-53-10,0-23-6528  
1-10-11-35-16-5-13-18-51-45-43-27-21,29-23-24,0



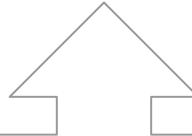
SSL Client Fingerprint (JA3):

66918128f1b9b03303d77c6f2eefd128

\* JA3: John Althouse, Jeff Atkinson, Josh Atkins, <https://engineering.salesforce.com/open-sourcing-ja3-92c9e53c3c41>, 2017

# Fingerprinting TLS client/servers with JA3 \*

the TLS Client is probably  
Chrome!



SSL Client Fingerprint (JA3):

66918128f1b9b03303d77c6f2eefd128

\* JA3: John Althouse, Jeff Atkinson, Josh Atkins, <https://engineering.salesforce.com/open-sourcing-ja3-92c9e53c3c41>, 2017

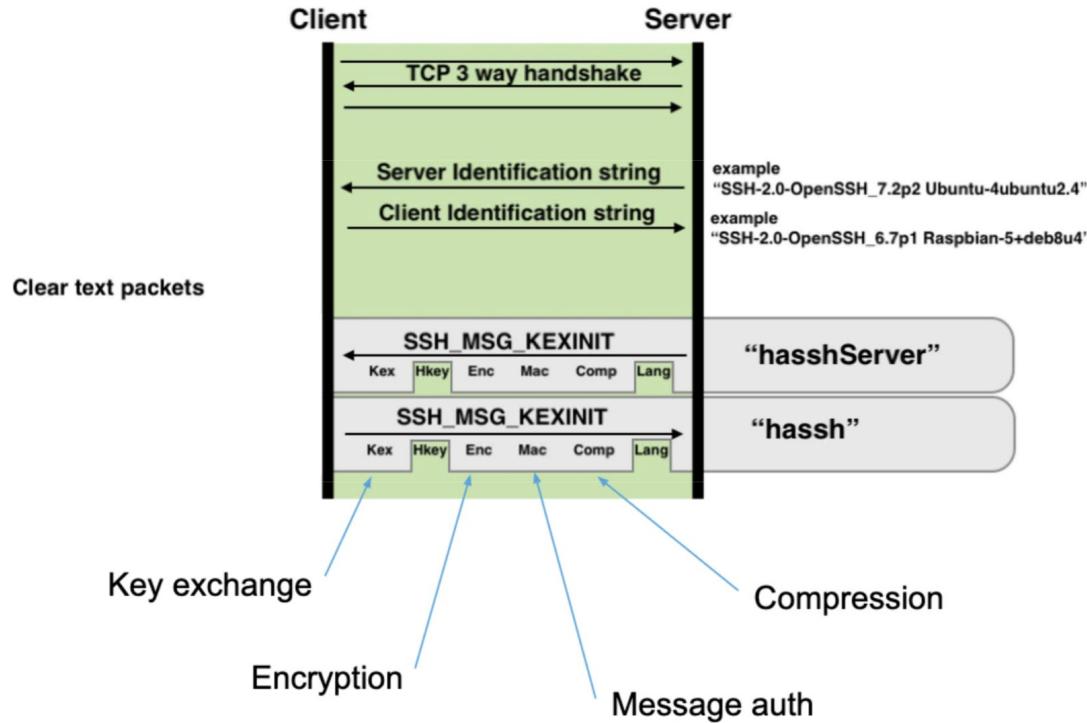
# SSH Client/Server Fingerprinting

using `SSH_MSG_KEXINIT` messages

SSH Protocol  
  ▼ SSH Version 2  
    Packet Length: 1388  
    Padding Length: 4  
  ▼ Key Exchange  
    Message Code: Key Exchange Init (20)  
    ▼ Algorithms  
      Cookie: 493c1ff88f5c28692341c15022837f1b  
      kex\_algorithms length: 269  
      kex\_algorithms string [truncated]: curve25519-sha256,curve25519-sha256-ecdh-sha256-sha256  
      server\_host\_key\_algorithms length: 358  
      server\_host\_key\_algorithms string [truncated]: ecdsa-sha2-nistp256-cert-v02@openssh.com,ecdh-sha2-nistp256-cert-v02@openssh.com,ecdh-sha2-nistp256,ecdsa-sha2-nistp384-cert-v02@openssh.com,ecdsa-sha2-nistp384,ecdh-sha2-nistp384,rsa-sha2-512-cert-v02@openssh.com,rsa-sha2-512,ecdsa-sha2-512-cert-v02@openssh.com,ecdsa-sha2-512  
      encryption\_algorithms\_client\_to\_server length: 108  
      encryption\_algorithms\_client\_to\_server string: chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes192-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr@openssh.com,aes192-ctr@openssh.com,aes128-ctr@openssh.com  
      encryption\_algorithms\_server\_to\_client length: 108  
      encryption\_algorithms\_server\_to\_client string: chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes192-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr@openssh.com,aes192-ctr@openssh.com,aes128-ctr@openssh.com  
      mac\_algorithms\_client\_to\_server length: 213  
      mac\_algorithms\_client\_to\_server string [truncated]: umac-64-etm@openssh.com,umac-128-etm@openssh.com  
      mac\_algorithms\_server\_to\_client length: 213  
      mac\_algorithms\_server\_to\_client string [truncated]: umac-64-etm@openssh.com,umac-128-etm@openssh.com  
      compression\_algorithms\_client\_to\_server length: 26  
      compression\_algorithms\_client\_to\_server string: none,zlib@openssh.com  
      compression\_algorithms\_server\_to\_client length: 26  
      compression\_algorithms\_server\_to\_client string: none,zlib@openssh.com  
      languages\_client\_to\_server length: 0  
      languages\_client\_to\_server string: [Empty]  
      languages\_server\_to\_client length: 0  
      languages\_server\_to\_client string: [Empty]  
      First KEX Packet Follows: 0  
      Reserved: 00000000  
      Padding String: 00000000

```
0000 00 00 05 6c 04 14 49 3c 1f f8 8f 5c 28 69 23 41 ···l.I< ···\(\i#A
0010 c1 50 22 83 7f 1b 00 00 01 0d 63 75 72 76 65 32 .P"..... ··curve2
0020 35 35 31 39 2d 73 68 61 32 35 36 2c 63 75 72 76 5519-sha 256,curv
0030 65 32 35 35 31 39 2d 73 68 61 32 35 36 40 6c 69 e25519-s ha256@li
0040 62 73 73 68 2e 6f 72 67 2c 65 63 64 68 2d 73 68 bssh.org ,ecdh-sh
0050 61 32 2d 6e 69 73 74 70 32 35 36 2c 65 63 64 68 a2-nistp 256,ecdh
0060 2d 73 68 61 32 2d 6e 69 73 74 70 33 38 34 2c 65 -sha2-ni stp384,e
0070 63 64 68 2d 73 68 61 32 2d 6e 69 73 74 70 35 32 cdh-sha2 -nistp52
0080 31 2c 64 69 66 66 69 65 2d 68 65 6c 6c 6d 61 6e 1,diffie -hellman
0090 2d 67 72 6f 75 70 2d 65 78 63 68 61 6e 67 65 2d -group-e xchange-
```

# HASSH Profiling Method



# HASSH - examples

hassh(**Ncrack**) =  
55a77ae9728654f1d4240a29287dc296

hassh(**CobaltStrike\_SSH-client**) =  
a7a87fbe86774c2e40cc4a7ea2ab1b3c

# HASSH - nmap script

```
% nmap --script ssh-hassh.nse -p 22 192.168.10.136

Starting Nmap 7.60 ( https://nmap.org ) at 2019-09-30 20:45 PDT
Nmap scan report for mikrotik.planethacker.net (192.168.10.136)
Host is up (0.0063s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
| ssh-hassh:
|   Server Identification String: SSH-2.0-ROSSH
|   hasshServer: 592ac2fb1645c3dc26ede0a59cd46957
|_  hasshServer Guess: SSH-2.0-ROSSH (100%)
```

<https://github.com/0x4D31/hassh-utils>

# Detecting SSH Honeypots



# Cowrie - bad news

|                       |        |   |
|-----------------------|--------|---|
| hasshServer           | string | 06046964c022c6407d15a27b12a6a4fb  |
| hasshServerAlgorithms | string | curve25519-sha256@rfc5114.com,ecdh-sha384-sha1@openssh.com,ecdh-sha256-sha1@openssh.com,rsa-sha2-512,rsa-sha1,diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha256,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1,poly1305@openssh.com,gcm@openssh.com,256-etm@openssh.com,etm@openssh.com,sha2-512,hmac-sha2-512-etm,hmac-sha2-512,hmac-sha1-96,hmac-sha1,hmac-md5-96,hmac-md5,hmac-ripemd160,hmac-sha2-256,hmac-sha2-256-etm,hmac-sha2-256,hmac-sha1-96-etm,hmac-sha1-96,hmac-sha1,hmac-md5-96-etm,hmac-md5-96,hmac-md5,hmac-ripemd160,hmac-sha2-512,hmac-sha2-512-etm,hmac-sha2-512,hmac-sha1-96-etm,hmac-sha1-96,hmac-sha1,hmac-md5-96-etm,hmac-md5-96,hmac-md5,hmac-ripemd160,t.supportedCiphers = [b'aes128-ctr', b'aes192-ctr', b'aes256-ctr', b'aes128-cbc', b'3des-cbc', b'blowfish-cbc', b'cast128-cbc', b'aes192-cbc', b'aes256-cbc']t.supportedPublicKeys = [b'ssh-rsa', b'ssh-dss']t.supportedMACs = [b'hmac-md5', b'hmac-sha1']t.supportedCompressions = [b'zlib@openssh.com', b'zlib', b'none'] |

# Cowrie - bad news

|             |        |                                  |
|-------------|--------|----------------------------------|
| hasshServer | string | 06046964c022c6407d15a27b12a6a4fb |
|-------------|--------|----------------------------------|

|                       |        |  |
|-----------------------|--------|--|
| hasshServerAlgorithms | string | curve25519-<br>nistp384,ecd<br>sha512,diffie |
|-----------------------|--------|--|

```
t.supportedCiphers = [  
    b'aes128-ctr',  
    b'aes192-ctr',
```

hassh(Cowrie) = a0fd4bc0e72b4b21232a486825b6742

|                             |
|-----------------------------|
| etm@openssl:<br>sha2-512,hm |
|-----------------------------|

```
b'aes192-cbc',  
b'aes256-cbc'  
]  
t.supportedPublicKeys = [b'ssh-rsa', b'ssh-dss']  
t.supportedMACs = [b'hmac-md5', b'hmac-sha1']  
t.supportedCompressions = [b'zlib@openssh.com', b'zlib', b'none']
```

# Cowrie - good news

```
52 src/cowrie/ssh/factory.py 📄
@@ -107,21 +107,45 @@ def buildProtocol(self,
                    log.msg("No moduli, no diffi-
sha256")
                    t.supportedKeyExchanges = ske
```

## Expose SSH key exchange parameters in config file (#1051)

\* Added support for getting encryption, compression, and hash methods from config file

⌚ master (#1051) 🏷 1.6.0

 **mayanksha** authored and **micheloosterhof** committed on Mar 14

```
-     # Reorder supported ciphers to resemble current openssh more
-     t.supportedCiphers = [
-
-         b'aes128-ctr',
-         b'aes192-ctr',
-         b'aes256-ctr',
-         b'aes128-cbc',
-         b'3des-cbc',
```

```
109
110 +     try:
111 +         t.supportedCiphers = [bytearray(i, 'utf-8') for i in
112 +             CONFIG.get('ssh', 'ciphers').split(',')]
113 +     except NoOptionError:
114 +         # Reorder supported ciphers to resemble current openssh more
115 +         t.supportedCiphers = [
116 +             b'aes128-ctr',
117 +             b'aes192-ctr',
```

```
{  
    "timestamp": "2018-09-29T15:43:09.300627Z",  
    "sensor": "0x4d31-nyc3-01",  
    "src_ip": "10.1.2.3",  
    "eventid": "cowrie.client.kex",  
    "message": "SSH client hassh fingerprint: 68e0ba85e1a818f7c49ea3f4b849bd15",  
    "hassh": "68e0ba85e1a818f7c49ea3f4b849bd15",  
    "hasshAlgorithms": "curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp3  
    diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,ext-info-c;chacha20  
    128-gcm@openssh.com,aes256-gcm@openssh.com,aes128-cbc,aes192-cbc,aes256-cbc,3des-c  
    6-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@  
    c-sha1;none,zlib@openssh.com,zlib",  
    "session": "3fd36ed0e459",  
    "keyAlgs": [⊕],  
    "kexAlgs": [⊕],  
    "macCS": [⊕],  
    "langCS": [⊕],  
    "compCS": [⊕],  
    "encCS": [⊕]  
}
```

HASSH (i.e. SSH Client Fingerprint)

MD5(kexAlgs;encryptionAlgs;macAlgs;compressionAlgs)

# Fingerprinting

# RDP

Remote Desktop Protocol

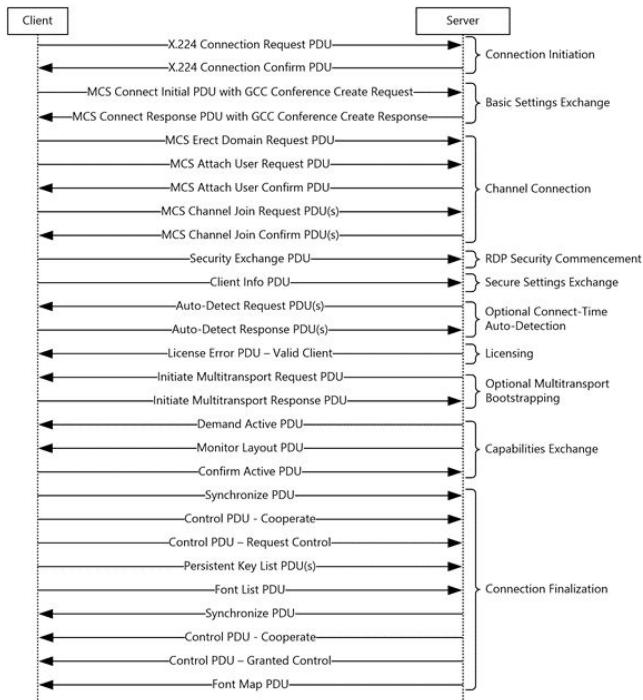
# Fingerprinting

RDP



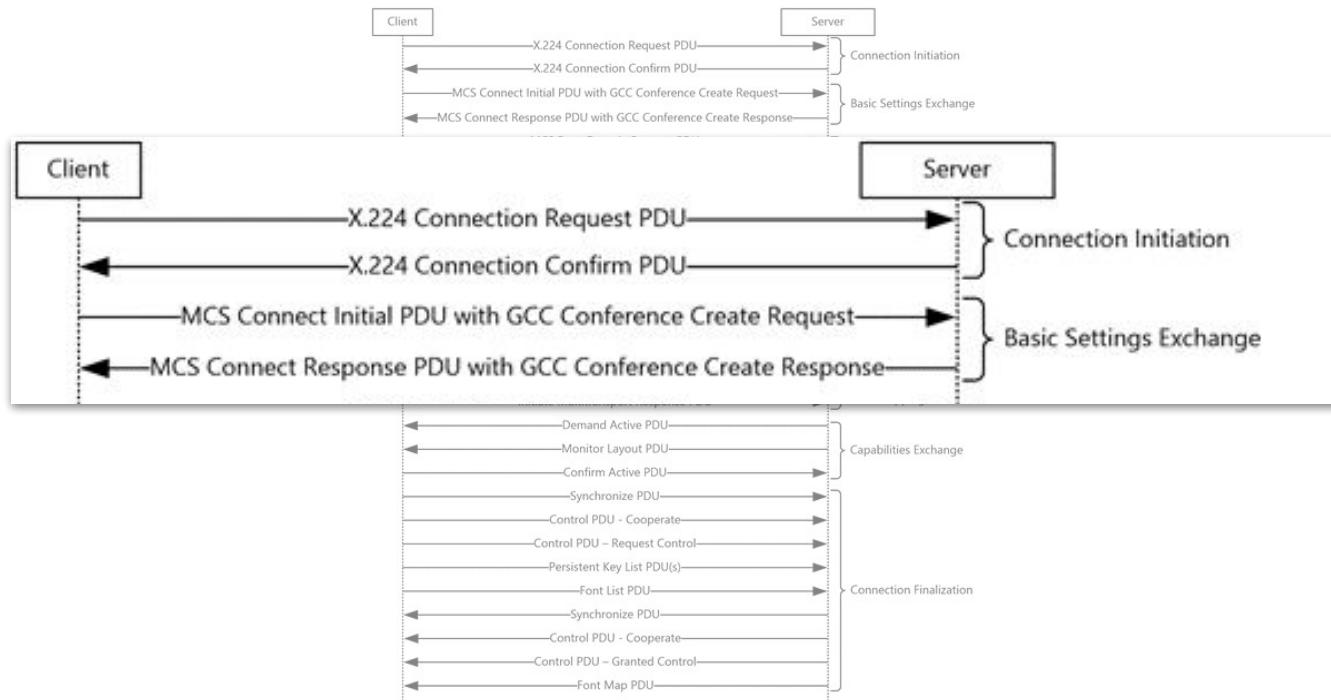
Remote Desktop Protocol

# RDP Connection Sequence



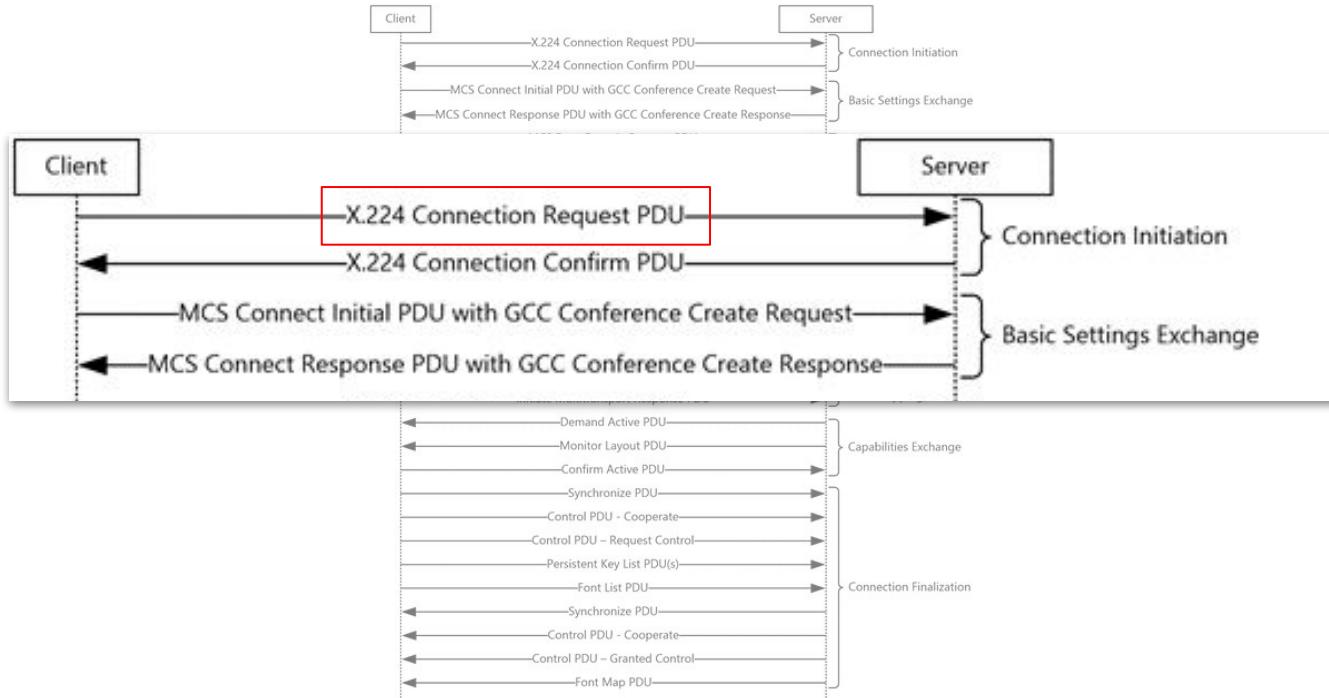
Ref: Microsoft, “[Remote Desktop Protocol: Basic Connectivity and Graphics Remoting](#)”

# RDP Connection Sequence



Ref: Microsoft, “[Remote Desktop Protocol: Basic Connectivity and Graphics Remoting](#)”

# RDP Connection Sequence



Ref: Microsoft, “[Remote Desktop Protocol: Basic Connectivity and Graphics Remoting](#)”

# Client X.224 Connection Request



| No.   | Time                    | Source                  | src port           | Destination    | dst port | Protocol | Info   |
|---|-------------------------|-------------------------|--------------------|----------------|----------|----------|--|
| 4   | 0.000483                | 192.168.56.1            | 54809              | 192.168.56.101 | 3389     | RDP      | Cookie: mstshash=g1ghrsx2, Negotiate Request |
| ▶ Frame 4: 112 bytes on wire (896 bits), 112 bytes captured (896 bits)                                |                         |                         |                    |                |          |          |  |
| ▶ Ethernet II, Src: 0a:00:27:00:00:00 (0a:00:27:00:00:00), Dst: PcsCompu_ed:80:9c (08:00:27:ed:80:9c) |                         |                         |                    |                |          |          |  |
| ▶ Internet Protocol Version 4, Src: 192.168.56.1, Dst: 192.168.56.101                                 |                         |                         |                    |                |          |          |  |
| ▶ Transmission Control Protocol, Src Port: 54809, Dst Port: 3389, Seq: 1, Ack: 1, Len: 46             |                         |                         |                    |                |          |          |  |
| ▶ TPKT, Version: 3, Length: 46  |                         |                         |                    |                |          |          |  |
| ▶ ISO 8073/X.224 COTP Connection-Oriented Transport Protocol  |                         |                         |                    |                |          |          |  |
| ▼ Remote Desktop Protocol   |                         |                         |                    |                |          |          |  |
| Routing Token/Cookie: Cookie: mstshash=g1ghrsx2   |                         |                         |                    |                |          |          |  |
| Type: RDP Negotiation Request (0x01)  |                         |                         |                    |                |          |          |  |
| ▶ Flags: 0x00   |                         |                         |                    |                |          |          |  |
| Length: 8   |                         |                         |                    |                |          |          |  |
| ▼ requestedProtocols: 0x00000001, TLS security supported  |                         |                         |                    |                |          |          |  |
| ..... . .... ..1 = TLS security supported: True   |                         |                         |                    |                |          |          |  |
| ..... . .... ..0. = CredSSP supported: False  |                         |                         |                    |                |          |          |  |
| ..... . .... ..0... = Early User Authorization Result PDU supported: False                            |                         |                         |                    |                |          |          |  |
| 0000  | 08 00 27 ed 80 9c 0a 00 | 27 00 00 00 08 00 45 00 | ..'. .... '.... E. |                |          |          |  |
| 0010  | 00 62 00 00 40 00 40 06 | 48 df c0 a8 38 01 c0 a8 | .b..@ @. H...8...  |                |          |          |  |
| 0020  | 38 65 d6 19 0d 3d 74 62 | 2c b8 47 b8 d1 5c 80 18 | 8e...=tb ,G...\... |                |          |          |  |
| 0030  | 10 15 d8 bb 00 00 01 01 | 08 0a 3e 33 b1 9c 00 00 | .....>3.....       |                |          |          |  |
| 0040  | 00 00 03 00 00 2e 29 e0 | 00 00 00 00 00 43 6f 6f | .....). .... Coo   |                |          |          |  |
| 0050  | 6b 69 65 3a 20 6d 73 74 | 73 68 61 73 68 3d 67 31 | Kie: mst shash=g1  |                |          |          |  |
| 0060  | 67 68 72 73 78 32 0d 0a | 01 00 08 00 01 00 00 00 | ghrsx2.....        |                |          |          |  |

# Client X.224 Connection Request



# Client X.224 Connection Request



| No.   | Time                    | Source                  | src port          | Destination    | dst port | Protocol | Info   |
|---|-------------------------|-------------------------|-------------------|----------------|----------|----------|--|
| 4   | 0.000483                | 192.168.56.1            | 54809             | 192.168.56.101 | 3389     | RDP      | Cookie: mstshash=g1ghrsx2, Negotiate Request |
| ▶ Frame 4: 112 bytes on wire (896 bits), 112 bytes captured (896 bits)                                |                         |                         |                   |                |          |          |  |
| ▶ Ethernet II, Src: 0a:00:27:00:00:00 (0a:00:27:00:00:00), Dst: PcsCompu_ed:80:9c (08:00:27:ed:80:9c) |                         |                         |                   |                |          |          |  |
| ▶ Internet Protocol Version 4, Src: 192.168.56.1, Dst: 192.168.56.101                                 |                         |                         |                   |                |          |          |  |
| ▶ Transmission Control Protocol, Src Port: 54809, Dst Port: 3389, Seq: 1, Ack: 1, Len: 46             |                         |                         |                   |                |          |          |  |
| ▶ TPKT, Version: 3, Length: 46  |                         |                         |                   |                |          |          |  |
| ▶ ISO 8073/X.224 COTP Connection-Oriented Transport Protocol  |                         |                         |                   |                |          |          |  |
| ▼ Remote Desktop Protocol   |                         |                         |                   |                |          |          |  |
| Routing Token/Cookie: Cookie: mstshash=g1ghrsx2   |                         |                         |                   |                |          |          |  |
| Type: RDP Negotiation Request (0x01)  |                         |                         |                   |                |          |          |  |
| ▶ Flags: 0x00   |                         |                         |                   |                |          |          |  |
| Length: 8   |                         |                         |                   |                |          |          |  |
| ▶ requestedProtocols: 0x00000001, TLS security supported  |                         |                         |                   |                |          |          |  |
| .....1 = TLS security supported: True   |                         |                         |                   |                |          |          |  |
| .....0. = CredSSP supported: False  |                         |                         |                   |                |          |          |  |
| .....0... = Early User Authorization Result PDU supported: False                                      |                         |                         |                   |                |          |          |  |
| 0000  | 08 00 27 ed 80 9c 0a 00 | 27 00 00 00 08 00 45 00 | .....             | .....          | E·       |          |  |
| 0010  | 00 62 00 00 40 00 40 06 | 48 df c0 a8 38 01 c0 a8 | b·@·@·            | H··8·          | ··       |          |  |
| 0020  | 38 65 d6 19 0d 3d 74 62 | 2c b8 47 b8 d1 5c 80 18 | 8e··=tb ,G·\`·    | ··             | ··       |          |  |
| 0030  | 10 15 d8 bb 00 00 01 01 | 08 0a 3e 33 b1 9c 00 00 | .....             | ....>3....     | .....    |          |  |
| 0040  | 00 00 03 00 00 2e 29 e0 | 00 00 00 00 00 43 6f 6f | .....) .Coo       | .....          | .....    |          |  |
| 0050  | 6b 69 65 3a 20 6d 73 74 | 73 68 61 73 68 3d 67 31 | Kie: mst shash=g1 | ghrsx2..       | .....    |          |  |
| 0060  | 67 68 72 73 78 32 0d 0a | 01 00 08 00 01 00 00 00 | .....             | .....          | .....    |          |  |

requestedProtocols: 0x00000001

```
0000 08 00 27 ed 80 9c 0a 00 27 00 00 00 08 00 45 00 ..... E·
0010 00 62 00 00 40 00 40 06 48 df c0 a8 38 01 c0 a8 b·@·@· H··8·
0020 38 65 d6 19 0d 3d 74 62 2c b8 47 b8 d1 5c 80 18 8e··=tb ,G·\`·
0030 10 15 d8 bb 00 00 01 01 08 0a 3e 33 b1 9c 00 00 ..... ··
0040 00 00 03 00 00 2e 29 e0 00 00 00 00 43 6f 6f ..... ) .Coo
0050 6b 69 65 3a 20 6d 73 74 73 68 61 73 68 3d 67 31 Kie: mst shash=g1
0060 67 68 72 73 78 32 0d 0a 01 00 08 00 01 00 00 00 ghrsx2 ..
```

There are **two RDP Security** modes

# Standard

There are **two RDP Security modes**

Q(“°~°”)9

# Enhanced

There are **two RDP Security modes**

$\ell(\grave{\text{o}} \underline{\acute{\text{o}}})$

| No. | Time     | Source       | src port | Destination   | dst port | Protocol | Info         |
|-----|----------|--------------|----------|---------------|----------|----------|--------------|
| 8   | 5.257990 | 192.168.15.4 | 49748    | 18.204.197... | 3389     | TLSv1... | Client Hello |

▼ Transport Layer Security  
  ▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello  
    Content Type: Handshake (22)  
    Version: TLS 1.2 (0x0303)  
    Length: 174  
  ▼ Handshake Protocol: Client Hello  
    Handshake Type: Client Hello (1)  
      Length: 170  
      Version: TLS 1.2 (0x0303)  
    ► Random: 5cff631e89e70b94f35aaf834bdd34eccdd8d0fb05272cec...  
    Session ID Length: 0  
    Cipher Suites Length: 42  
    Cipher Suites (21 suites)

# Enhanced

## RDP Security

ε(ò\_ó^)

Supports the following *external security protocols*:

TLS 1.0 / TLS 1.1 / TLS 1.2 / CredSSP / RDSTLS

| No.   | Time     | Source       | src port | Destination   | dst port | Protocol | Info         |
|---|----------|--------------|----------|---------------|----------|----------|--------------|
| 8   | 5.257990 | 192.168.15.4 | 49748    | 18.204.197... | 3389     | TLSv1... | Client Hello |
| ▼ Transport Layer Security                                    |          |              |          |               |          |          |              |
| ▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello      |          |              |          |               |          |          |              |
| Content Type: Handshake (22)                                  |          |              |          |               |          |          |              |
| Version: TLS 1.2 (0x0303)                                     |          |              |          |               |          |          |              |
| Length: 174   |          |              |          |               |          |          |              |
| ▼ Handshake Protocol: Client Hello                            |          |              |          |               |          |          |              |
| Handshake Type: Client Hello (1)                              |          |              |          |               |          |          |              |
| Length: 170   |          |              |          |               |          |          |              |
| Version: TLS 1.2 (0x0303)                                     |          |              |          |               |          |          |              |
| ► Random: 5cff631e89e70b94f35aaf834bdd34eccdd8d0fb05272cec... |          |              |          |               |          |          |              |
| Session ID Length: 0  |          |              |          |               |          |          |              |
| Cipher Suites Length: 42                                      |          |              |          |               |          |          |              |
| ▼ Cipher Suites (21 suites)                                   |          |              |          |               |          |          |              |

Enhanced

RDP Security

ℓ(ò\_ó^)

TLS 1.0 / TLS 1.1 / TLS 1.2 / CredSSP / RDSTLS

| No. | Time     | Source       | src port | Destination   | dst port | Protocol | Info         |
|-----|----------|--------------|----------|---------------|----------|----------|--------------|
| 8   | 5.257990 | 192.168.15.4 | 49748    | 18.204.197... | 3389     | TLSv1... | Client Hello |

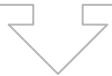
▼ Transport Layer Security  
  ▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello  
    Content Type: Handshake (22)  
    Version: TLS 1.2 (0x0303)  
    Length: 174  
  ▼ Handshake Protocol: Client Hello  
    Handshake Type: Client Hello (1)  
    Length: 170  
    Version: TLS 1.2 (0x0303)  
    ► Random: 5cff631e89e70b94f35aaf834bdd34eccdd8d0fb05272cec...  
    Session ID Length: 0  
    Cipher Suites Length: 42  
    Cipher Suites (21 suites)

# Enhanced

## RDP Security

ℓ(ò\_ó^)

TLS 1.0 / TLS 1.1 / TLS 1.2 / CredSSP / RDSTLS



| No. | Time     | Source       | src port | Destination   | dst port | Protocol | Info         |
|-----|----------|--------------|----------|---------------|----------|----------|--------------|
| 8   | 5.257990 | 192.168.15.4 | 49748    | 18.204.197... | 3389     | TLSv1... | Client Hello |

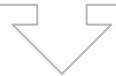
▼ Transport Layer Security  
  ▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello  
    Content Type: Handshake (22)  
    Version: TLS 1.2 (0x0303)  
    Length: 174  
  ▼ Handshake Protocol: Client Hello  
    Handshake Type: Client Hello (1)  
      Length: 170  
      Version: TLS 1.2 (0x0303)  
    ► Random: 5cff631e89e70b94f35aaaf834bdd34eccdd8d0fb05272cec...  
    Session ID Length: 0  
    Cipher Suites Length: 42  
    Cipher Suites (21 suites)

# Enhanced

# RDP Security

ℓ(ò\_ó^)

TLS 1.0 / TLS 1.1 / TLS 1.2 / CredSSP / RDSTLS



# TLS

| No. | Time     | Source       | src port | Destination   | dst port | Protocol | Info         |
|-----|----------|--------------|----------|---------------|----------|----------|--------------|
| 8   | 5.257990 | 192.168.15.4 | 49748    | 18.204.197... | 3389     | TLSv1... | Client Hello |

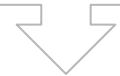
▼ Transport Layer Security  
  ▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello  
    Content Type: Handshake (22)  
    Version: TLS 1.2 (0x0303)  
    Length: 174  
  ▼ Handshake Protocol: Client Hello  
    Handshake Type: Client Hello (1)  
      Length: 170  
      Version: TLS 1.2 (0x0303)  
    ► Random: 5cff631e89e70b94f35aaaf834bdd34eccdd8d0fb05272cec...  
    Session ID Length: 0  
    Cipher Suites Length: 42  
    Cipher Suites (21 suites)

# Enhanced

## RDP Security

ℓ(ò\_ó^)

TLS 1.0 / TLS 1.1 / TLS 1.2 / CredSSP / RDSTLS



**TLS**

→ Can be fingerprinted with JA3

# Enhanced RDP Security

ℓ(ò\_ó^)

|    | os version     | rdp client                | ja3                              | ja3Algorithms              |
|----|----------------|---------------------------|----------------------------------|----------------------------|
| 2  | Windows XP SP3 | RDC 6.1.7600              | c8a0d08d2cbee4bed7cd90e47588ab9b | 769,4-5-10-9-100-98-3-6-19 |
| 3  | Windows 2012   | RDC 6.2.9200              | bc2874f25a8254edb36147c151527cfa | 771,49192-49191-49172-49   |
| 4  | Windows 2008r2 | RDC 6.3.9600              | e6a4e2358d4eee6122403f3cb835bcbd | 771,49192-49191-49172-49   |
| 5  | Windows 2012r2 | RDC 6.3.9600              | 3e686105164b7c9a4cbd59142f18a4e7 | 771,49192-49191-49172-49   |
| 6  | Windows 7      | RDC 6.3.9600              | d54b3eb800cbeccf99fd5d5cdcd7b5b5 | 771,49192-49191-49172-49   |
| 7  | Windows 2016   | RDC 10.0.14393            | 67e3d18fd9ddbbc8eca65f7dedac674  | 771,49196-49195-49200-49   |
| 8  | Windows 2019   | RDC 10.0.17763            | ce5f3254611a8c095a3d821d44539877 | 771,49196-49195-49200-49   |
| 9  | Windows 10     | RDC 10.0.17134            | ce5f3254611a8c095a3d821d44539877 | 771,49196-49195-49200-49   |
| 10 | macOS          | Microsoft Remote Desktop  | e4d448cdfe06dc1243c1eb026c74ac9a | 771,255-49196-49195-4918   |
| 11 | macOS          | FreeRDP                   | 75fb48a465416d66291fb52a733d4787 | 769,49172-49162-57-56-55-  |
| 12 | macOS          | rdpy, rdesktop, python    | e2121ae1544cd5aca048d03505068a6  | 769,49162-49172-57-49161   |
| 13 | macOS          | robertdavidgraham/rdpscan | 0b3e989a2ad13829ab8d65d132480e41 | 769,49172-49162-57-56-65-  |
| 14 | macOS          | pupy's rdp module         | f330c48fc4abc5ffc0720d7f92108e22 | 769,49169-49159-49174-24   |

<https://gist.github.com/0x4D31/>

# Enhanced RDP Security

ℓ(ò\_ó^)

| Search this file... |                |                           |   |                                 |
|---------------------|----------------|---------------------------|---|---------------------------------|
|                     | os version     | rdp client                | ja3                                     | ja3Algorithms                   |
| 1                   | Windows XP SP3 | RDC 6.1.7600              | c8a0d08d2cbee4bed7cd90e47588ab9b        | 769,4-5-10-9-100-98-3-6-19      |
| 2                   | Windows 2012   | RDC 6.2.9200              | bc2874f25a8254edb36147c151527cfa        | 771,49192-49191-49172-49        |
| 3                   | Windows 2008r2 | RDC 6.3.9600              | e6a4e2358d4eee6122403f3cb835bcd         | 771,49192-49191-49172-49        |
| 4                   | Windows 2012r2 | RDC 6.3.9600              | 3e686105164b7c9a4cbd59142f18a4e7        | 771,49192-49191-49172-49        |
| 5                   | Windows 7      | RDC 6.3.9600              | d54b3eb800cbeccff99fd5d5cdcd7b5b5       | 771,49192-49191-49172-49        |
| 6                   | Windows 2016   | RDC 10.0.14302            | 67a2d18f40dddbbc8aca65f7dd0a874         | 771,49192-49191-49172-49        |
| 8                   | Windows 2019   | RDC 10.0.17763            | <b>ce5f3254611a8c095a3d821d44539877</b> | <b>771,49196-49195-49200-49</b> |
| 9                   | Windows 10     | RDC 10.0.17134            | <b>ce5f3254611a8c095a3d821d44539877</b> | <b>771,49196-49195-49200-49</b> |
| 10                  | macOS          | Microsoft Remote Desktop  | e4d448cdfe06dc1243c1eb026c74ac9a        | 771,255-49196-49195-4918        |
| 11                  | macOS          | FreeRDP                   | 75fb48a465416d66291fb52a733d4787        | 769,49172-49162-57-56-55-       |
| 12                  | macOS          | rdpy, rdesktop, python    | e2121ae1544cd5aca048d03505068a6         | 769,49162-49172-57-49161        |
| 13                  | macOS          | robertdavidgraham/rdpscan | 0b3e989a2ad13829ab8d65d132480e41        | 769,49172-49162-57-56-65-       |
| 14                  | macOS          | pupy's rdp module         | f330c48fc4abc5ffc0720d7f92108e22        | 769,49169-49159-49174-24        |

<https://gist.github.com/0x4D31/>

# Enhanced RDP Security

ℓ(ò\_ó^)

## Pupy's RDP module

JA3: f330c48fc4abc5ffc0720d7f92108e22

| Search this file... |                |                           |                                  |                            |
|---------------------|----------------|---------------------------|----------------------------------|----------------------------|
| 1                   | os version     | rdp client                | ja3                              | ja3Algorithms              |
| 2                   | Windows XP SP3 | RDC 6.1.7600              | c8a0d08d2cbee4bed7cd90e47588ab9b | 769,4-5-10-9-100-98-3-6-19 |
| 3                   | Windows 2012   | RDC 6.2.9200              | bc2874f25a8254edb36147c151527cfa | 771,49192-49191-49172-49   |
| 4                   | Windows 2008r2 | RDC 6.3.9600              | e6a4e2358d4eee6122403f3cb835bcbd | 771,49192-49191-49172-49   |
| 5                   | Windows 2012r2 | RDC 6.3.9600              | 3e686105164b7c9a4cbd59142f18a4e7 | 771,49192-49191-49172-49   |
| 6                   | Windows 7      | RDC 6.3.9600              | d54b3eb800cbeccf99fd5d5cdcd7b5b5 | 771,49192-49191-49172-49   |
| 7                   | Windows 2016   | RDC 10.0.14393            | 67e3d18fd9dddbc8eca65f7dedac674  | 771,49196-49195-49200-49   |
| 8                   | Windows 2019   | RDC 10.0.17763            | ce5f3254611a8c095a3d821d44539877 | 771,49196-49195-49200-49   |
| 9                   | Windows 10     | RDC 10.0.17134            | ce5f3254611a8c095a3d821d44539877 | 771,49196-49195-49200-49   |
| 10                  | macOS          | Microsoft Remote Desktop  | e4d448cdfe06dc1243c1eb026c74ac9a | 771,255-49196-49195-4918   |
| 11                  | macOS          | FreeRDP                   | 75fb48a465416d66291fb52a733d4787 | 769,49172-49162-57-56-55-  |
| 12                  | macOS          | rdpy, rdesktop, python    | e2121ae1544cd5acaе048d03505068a6 | 769,49162-49172-57-49161   |
| 13                  | macOS          | robertdavidgraham/rdpscan | 0b3e989a2ad13829ab8d65d132480e41 | 769,49172-49162-57-56-65-  |
| 14                  | macOS          | pupy's rdp module         | f330c48fc4abc5ffc0720d7f92108e22 | 769,49169-49159-49174-24   |

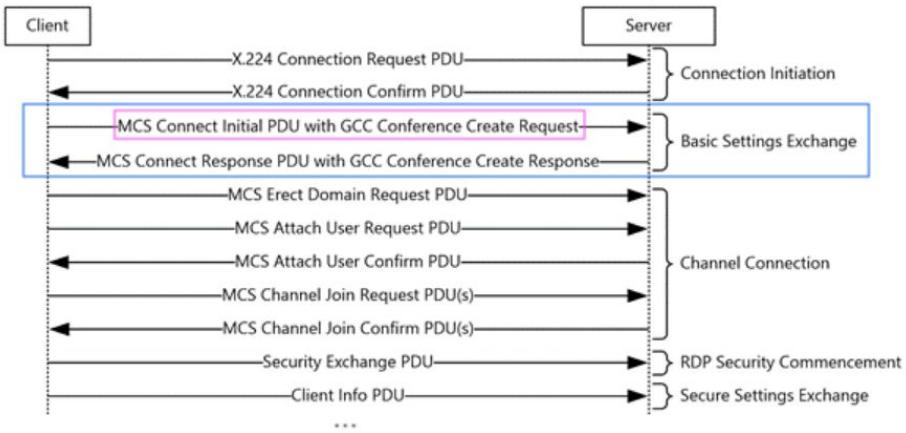
rdpClient-JA3.csv hosted with ❤ by GitHub [view raw](#)

<https://gist.github.com/0x4D31/>

# Standard

## RDP Security

Q(“°~°“)9



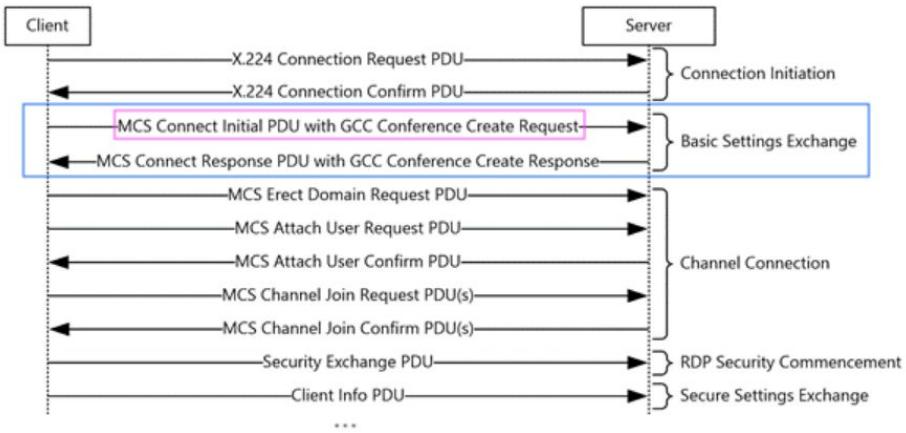
Ref: Microsoft, “[Remote Desktop Protocol: Basic Connectivity and Graphics Remoting](#)”

NO **TLS** in Standard Mode

# Standard

## RDP Security

Q(“°~°“)9



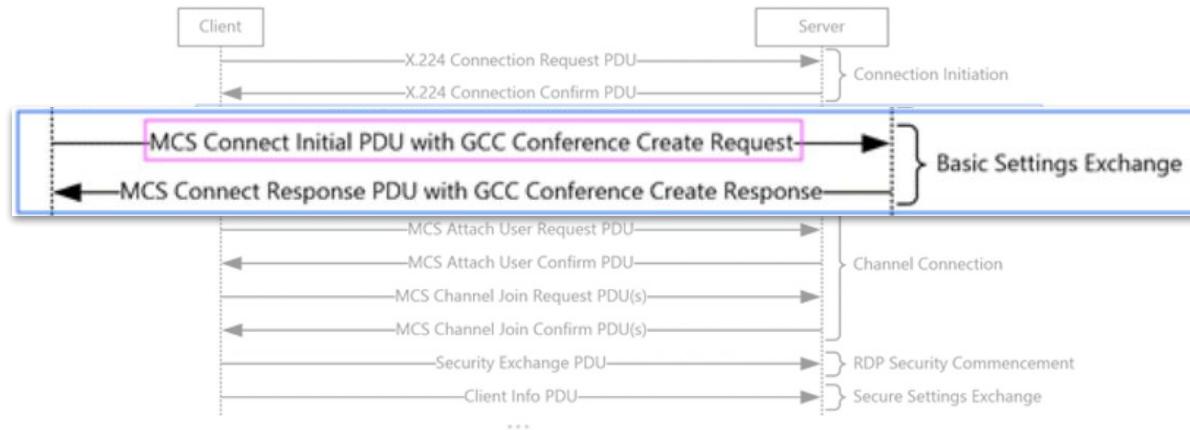
Ref: Microsoft, “[Remote Desktop Protocol: Basic Connectivity and Graphics Remoting](#)”

Uses its own encryption mechanism  
based on RSA and RC4/3DES

# Standard

# RDP Security

Q(“°~°„)9



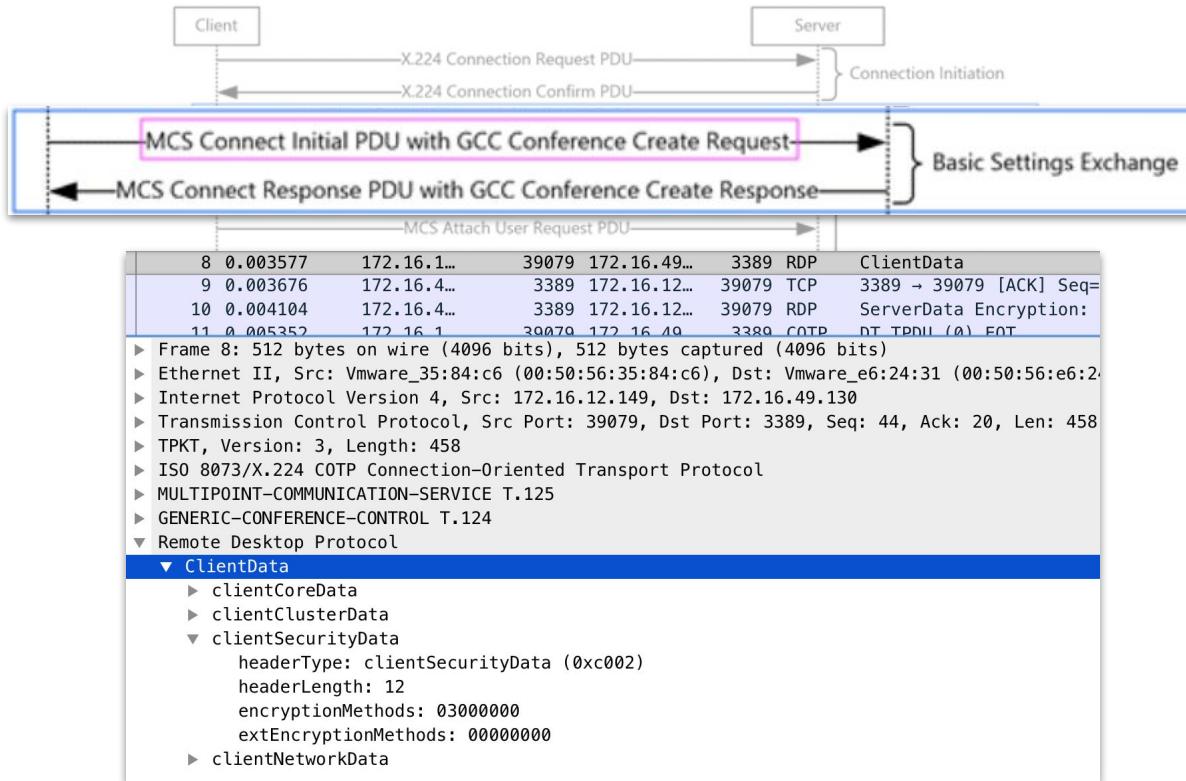
Ref: Microsoft, “[Remote Desktop Protocol: Basic Connectivity and Graphics Remoting](#)”

Interesting fields in the **Basic Settings Exchange** phase

# Standard

## RDP Security

Q(“°~°„)9



Interesting fields in the **Basic Settings Exchange** phase

# Standard

## RDP Security

Q(„°~°„)9

```
▼ Remote Desktop Protocol
  ▼ ClientData
    ▼ clientCoreData
      headerType: clientCoreData (0xc001)
      headerLength: 216
      versionMajor: 4
      versionMinor: 8
      desktopWidth: 800
      desktopHeight: 600
      colorDepth: 8 bits-per-pixel (bpp) (0xca01)
      SASSequence: 43523
      keyboardLayout: 1033
      clientBuild: 2600
      clientName: rdpscan
      keyboardType: IBM enhanced (101-key or 102-key) keyboard (4)
      keyboardSubType: 0
      keyboardFunctionKey: 12
      imeFileName: 0000000000000000000000000000000000000000000000000000000000...
      postBeta2ColorDepth: 8 bits-per-pixel (bpp) (0xca01)
      clientProductId: 1
      serialNumber: 0
      highColorDepth: Unknown (0x00ff)
      supportedColorDepths: 0x0007
      earlyCapabilityFlags: 1
      clientDigProductId:
      connectionType: Unknown (0)
      pad1octet: 0x00
      serverSelectedProtocol: 0
    ► clientClusterData
    ► clientSecurityData
    ► clientNetworkData
```

# Standard

## RDP Security

Q(„°~°„)9

```
▼ Remote Desktop Protocol
  ▼ ClientCoreData
    headerType: clientCoreData (0xc001)
    headerLength: 216
    versionMajor: 4
    versionMinor: 8
      ▼ DESKTOPCOREDATA_000
        desktopHeight: 600
        colorDepth: 8 bits-per-pixel (bpp) (0xca01)
        SASSequence: 43523
        keyboardLayout: 1033
        clientBuild: 2600
        clientName: rdpscan
        keyboardType: IBM enhanced (101-key or 102-key) keyboard (4)
        keyboardSubType: 0
        keyboardFunctionKey: 12
        imeFileName: 0000000000000000000000000000000000000000000000000000000000...
        postBeta2ColorDepth: 8 bits-per-pixel (bpp) (0xca01)
        clientProductId: 1
        serialNumber: 0
        highColorDepth: Unknown (0x00ff)
        supportedColorDepths: 0x0007
        earlyCapabilityFlags: 1
        clientDigProductId:
        connectionType: Unknown (0)
        pad1octet: 0x00
        serverSelectedProtocol: 0
    ► clientClusterData
    ► clientSecurityData
    ► clientNetworkData
```

# Standard

## RDP Security

Q(“°~°„)9

```
▼ Remote Desktop Protocol
  ▼ ClientData
    ► clientCoreData
    ▼ clientClusterData
      headerType: clientClusterData (0xc004)
      headerLength: 12
      clusterFlags: 0x00000015
      redirectedSessionId: 0x00000000
    ▼ clientSecurityData
      headerType: clientSecurityData (0xc002)
      headerLength: 12
      encryptionMethods: 1b000000
      extEncryptionMethods: 00000000
    ▼ clientNetworkData
      headerType: clientNetworkData (0xc003)
      headerLength: 56
      channelCount: 4
    ▼ channelDefArray
      ▼ channelDef
        name: rdpdr
        ► options: 0x80800000
      ▼ channelDef
        name: rdpsnd
        ► options: 0xc0000000
      ▼ channelDef
        name: cliprdr
        ► options: 0xc0a00000
      ▼ channelDef
        name: drdynvc
        ► options: 0xc0800000
```

# Standard

## RDP Security

Q(“°~°„)9

```
▼ Remote Desktop Protocol
  ▼ ClientData
    ▶ clientClusterData
      ▼ clientClusterData
        headerType: clientClusterData (0xc004)
        headerLength: 12
        clusterFlags: 0x00000015

      ▼ clientSecurityData
        headerType: clientSecurityData (0xc002)
        headerLength: 12
        encryptionMethods: 1b000000
        extEncryptionMethods: 00000000

      ▼ clientNetworkData
        headerType: clientNetworkData (0xc003)
        headerLength: 56
        channelCount: 4
        ▼ channelDefArray
          ▼ channelDef
            name: rdpdr
            ▶ options: 0x80800000
          ▼ channelDef
            name: rdpsnd
            ▶ options: 0xc0000000
          ▼ channelDef
            name: cliprdr
            ▶ options: 0xc0a00000
          ▼ channelDef
            name: drdynvc
            ▶ options: 0xc0800000
```

# Standard

## RDP Security

Q(“°~°„)9

```
▼ Remote Desktop Protocol
  ▼ ClientData
    ► clientCoreData
    ▼ clientClusterData
      headerType: clientClusterData (0xc004)
      headerLength: 12
      clusterFlags: 0x00000015
      redirectedSessionId: 0x00000000
    ▼ clientSecurityData
      headerType: clientSecurityData (0xc002)
      headerLength: 12
      encryptionMethods: 1b000000
      extEncryptionMethods: 00000000
      headerLength: 56
      channelCount: 4
    ▼ channelDefArray
      ▼ channelDef
        name: rdpdr
        ► options: 0x80800000
      ▼ channelDef
        name: rdpsnd
        ► options: 0xc0000000
      ▼ channelDef
        name: cliprdr
        ► options: 0xc0a00000
      ▼ channelDef
        name: drdynvc
        ► options: 0xc0800000
```

# Standard

## RDP Security

Q(“°~°„)9

```
▼ Remote Desktop Protocol
  ▼ ClientData
    ► clientCoreData
    ▼ clientClusterData
      headerType: clientClusterData (0xc004)
      headerLength: 12
      clusterFlags: 0x00000015
      redirectedSessionId: 0x00000000
    ▼ clientSecurityData
      headerType: clientSecurityData (0xc002)
      headerLength: 12
  ▼ clientNetworkData
    headerType: clientNetworkData (0xc003)
    headerLength: 56
    channelCount: 4
  ▼ channelDefArray
    ▼ channelDef
      name: rdpdr
      ► options: 0x80800000
    ▼ channelDef
      name: rdpsnd
      ► options: 0xc0000000
    ▼ channelDef
      name: cliprdr
      ► options: 0xc0a00000
    ▼ channelDef
      name: drdynvc
      ► options: 0xc0800000
```

# Introducing RD<sup>P</sup>; profiling RDP clients in standard mode

Concatenate the value of

**Major Version**

10,

# Introducing RD<sup>P</sup>; profiling RDP clients in standard mode

Concatenate the value of

**Minor Version**

10,8,

# Introducing RDFFP; profiling RDP clients in standard mode

Concatenate the value of

Cluster Flags

10,8,00000015,

# Introducing RDFP; profiling RDP clients in standard mode

Concatenate the value of

## Encryption Methods

10,8,00000015,0000001b,

# Introducing RDFP; profiling RDP clients in standard mode

Concatenate the value of

Ext Encryption Methods

10,8,00000015,0000001b,00000000,

# Introducing RDFP; profiling RDP clients in standard mode

Concatenate the value of

Channel Defs

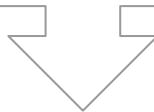
10,8,00000015,0000001b,00000000,rdpdr:80800000-rdp  
snd:c0000000-cliprdr:coa00000-drdynvc:c0800000

# Introducing RDFFP; profiling RDP clients in standard mode

10,8,00000015,0000001b,00000000,rdpdr:80800000-rdp  
snd:c0000000-cliprdr:coa00000-drdynvc:c0800000

# Introducing RDFP; profiling RDP clients in standard mode

```
10,8,00000015,0000001b,c0000000,rdpdr:80800000-rdp  
snd:c0000000-cliprdr:c0a0c0c0-drdynvc:c0800000
```



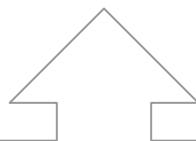
**MD5**

RDP Client Fingerprint (RDFP):

b7ab0ffd49f5700c138a08e2cdd5a948

# Introducing RDFP; profiling RDP clients in standard mode

Windows 10, RDC 10.0.17134



RDP Client Fingerprint (RDFP):

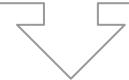
b7ab0ffd49f5700c138a08e2cdd5a948

# Introducing RD<sup>P</sup>; profiling RDP clients in standard mode

4,8,0000009,0000003,00000000,MS\_T120:00008080

# Introducing RDFP; profiling RDP clients in standard mode

4,8,0000009,00000003,MD50000,MS\_T120:00008080



RDPSCAN, bluekeep vuln scanner

daeb0f3467798401324445d3721aa887

# RDP Fingerprinting

## blog post



[medium.com/@0x4d31](https://medium.com/@0x4d31)

► Remote Desktop Protocol

▼ ClientData

- ▶ clientCoreData
  - headerType: clientCoreData (0xc001)
  - headerLength: 212
  - versionMajor: 4
  - versionMinor: 8
  - desktopWidth: 1280
  - desktopHeight: 800
  - colorDepth: 8 bits-per-pixel (bpp) (0xca01)
  - SASSequence: 43523
  - keyboardLayout: 2057
  - clientBuild: 2600
  - clientName: EMP-LAP-0014
  - keyboardType: IBM enhanced (101-key or 102-key) keyboard (4)
  - keyboardSubType: 0
  - keyboardFunctionKey: 12
  - imeFileName: 000...
  - postBeta2ColorDepth: 8 bits-per-pixel (bpp) (0xca01)
  - clientProductId: 1
  - serialNumber: 0
  - highColorDepth: 16-bit 565 RGB mask (0x0010)
  - supportedColorDepths: 0x0007
  - earlyCapabilityFlags: 1
  - clientDigProductId: 76487-OEM-0011903-00107
  - connectionType: Unknown (0)
  - pad1octet: 0x00
- ▶ clientClusterData
- ▶ clientSecurityData
  - headerType: clientSecurityData (0xc002)
  - headerLength: 12
  - encryptionMethods: 01000000
  - extEncryptionMethods: 00000000
- ▶ clientNetworkData

# QUICK

<https://github.com/0x4D31/quick>

a go library based on gopacket for analyzing  
QUIC CHLO messages

2019/05/11 05:42:10 192.168.1.9:56149 -> 172.217.167.74:443(  
Public Flags: d  
CID: b8142bd8c89f0e6e  
Version: Q043  
Packet Number: 1  
Message Authentication Hash: 924c2de3a9be804519ffa6e3  
Frame Type: a0  
Stream ID: 1  
Data Length: 1024  
Tag: CHLO  
Tag Number: 25  
SNI: "fonts.googleapis.com"  
UAID: "Chrome/74.0.3729.131 Intel Mac OS X 10\_14\_4"  
Tags in Order: ["PAD" "SNI" "STK" "VER" "CCS" "NONC" "AEAD" "UA"  
Tag Values: map[AEAD:AESEG CCRT:86c30bf78fd9372c67f8adc58015e3ff]

2019/05/11 05:42:10 192.168.1.9:58556 -> 172.217.25.174:443(  
Public Flags: d  
CID: e4fc1c8ad38dc14  
Version: Q043  
Packet Number: 1  
Message Authentication Hash: 478ed5740d47dccc07b86b43  
Frame Type: a0  
Stream ID: 1  
Data Length: 1024  
Tag: CHLO  
Tag Number: 25  
SNI: "[www.youtube.com](http://www.youtube.com)"  
UAID: "Chrome/74.0.3729.131 Intel Mac OS X 10\_14\_4"  
Tags in Order: ["PAD" "SNI" "STK" "VER" "CCS" "NONC" "AEAD" "UA"  
Tag Values: map[AEAD:AESEG CCRT:2237aaad1bebaa6c67f8adc58015e3ff]

# Clustering and Profiling Internet-Wide Scans

# The Problem

- Honeypots: Limited network logging
  - General connection info and application-level data
  - No network metadata and handshake logging!

# Network Metadata

- Bro/Zeek
- Suricata
  - HTTP, DNS, TLS
- Netcap
- Tshark

## ssl.log | SSL handshakes

| FIELD                                | TYPE                         | DESCRIPTION   |
|--------------------------------------|------------------------------|---|
| ts                                   | time                         | Timestamp when SSL connection was established   |
| uid & id                             |                              | Underlying connection info > See https://www.wireshark.org/docs/man-pages/ssl.html#uid_and_id |
| version                              | string                       | SSL version that the server offered   |
| cipher                               | string                       | SSL cipher suite that the server chose  |
| curve                                | string                       | Elliptic curve server chose if using ECDHE  |
| server_name                          | string                       | Value of Server Name Indicator SSL extension  |
| session_id                           | string                       | Session ID offered by client for session resumption   |
| resumed                              | bool                         | Flag that indicates the session was resumed   |
| last_alert                           | string                       | Last alert that was seen during the connection  |
| next_protocol                        | string                       | Next protocol server chose using application layer next protocol extension, if seen           |
| established                          | bool                         | Was this connection established successfully?   |
| cert_chain <sup>1</sup>              | vector                       | Chain of certificates offered by server   |
| cert_chain_fuids <sup>1</sup>        | vector                       | File UIDs for certs in cert_chain   |
| client_cert_chain <sup>1</sup>       | vector                       | Chain of certificates offered by client   |
| client_cert_chain_fuids <sup>1</sup> | vector                       | File UIDs for certs in client_cert_chain  |
| subject <sup>1</sup>                 | string                       | Subject of the X.509 cert offered by server   |
| issuer <sup>1</sup>                  | string                       | Subject of the signer of the server cert  |
| client_subject <sup>1</sup>          | string                       | Subject of the X.509 cert offered by client   |
| client_issuer <sup>1</sup>           | string                       | Subject of the signer of the client cert  |
| validation_status <sup>2</sup>       | string                       | Certificate validation result for this handshake  |
| ocsp_status <sup>2</sup>             | string                       | OCSP validation result for this handshake   |
| ocsp_response <sup>2</sup>           | string                       | OCSP response as a string   |
| notary <sup>3</sup>                  | Cert<br>Notary::<br>Response | A response from the ICSI certificate notary   |



fatt.

fingerprint all the things!





66 61 74 74 2e

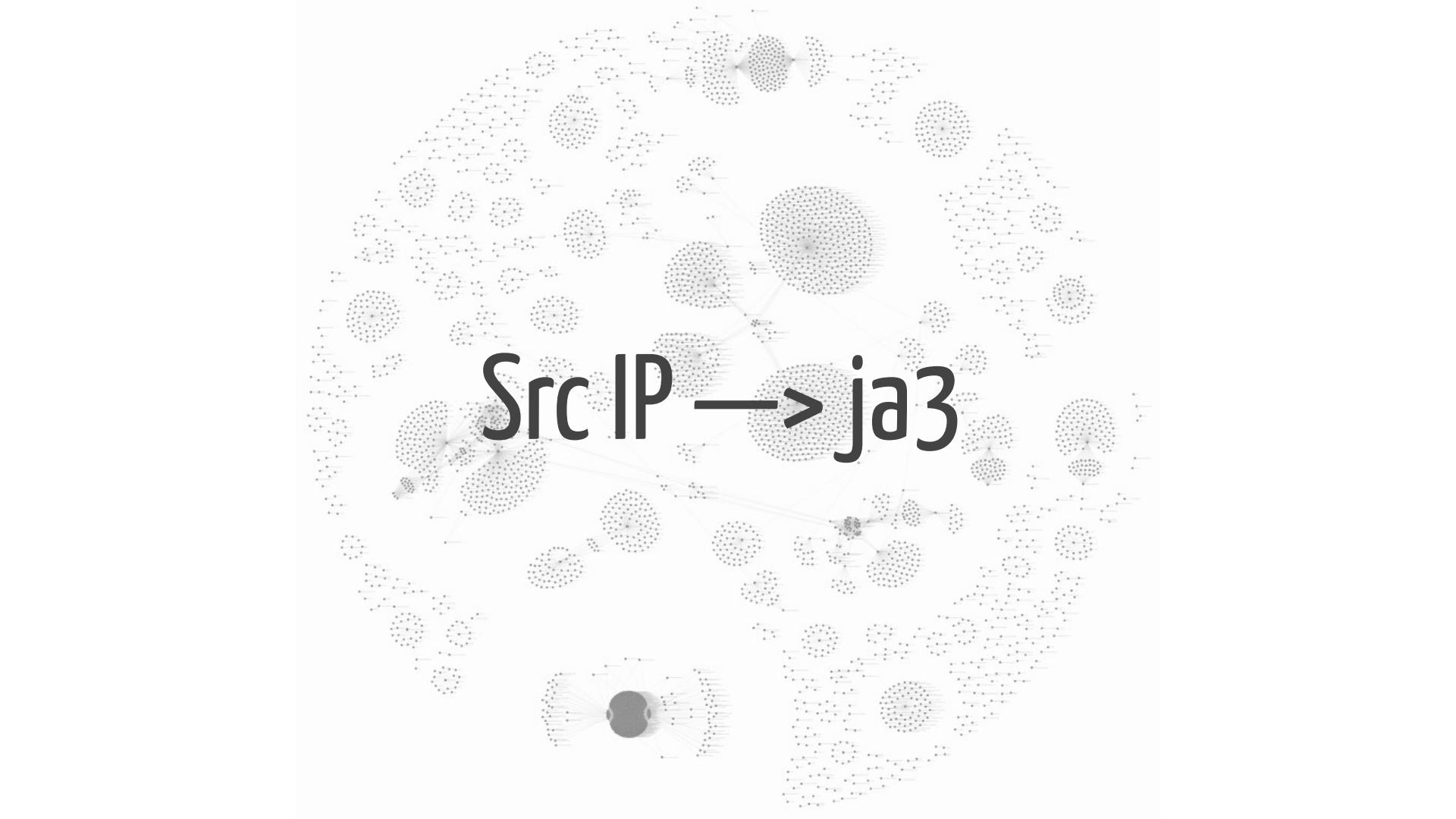
fingerprint all the things!

[github.com/0x4D31/fatt](https://github.com/0x4D31/fatt)

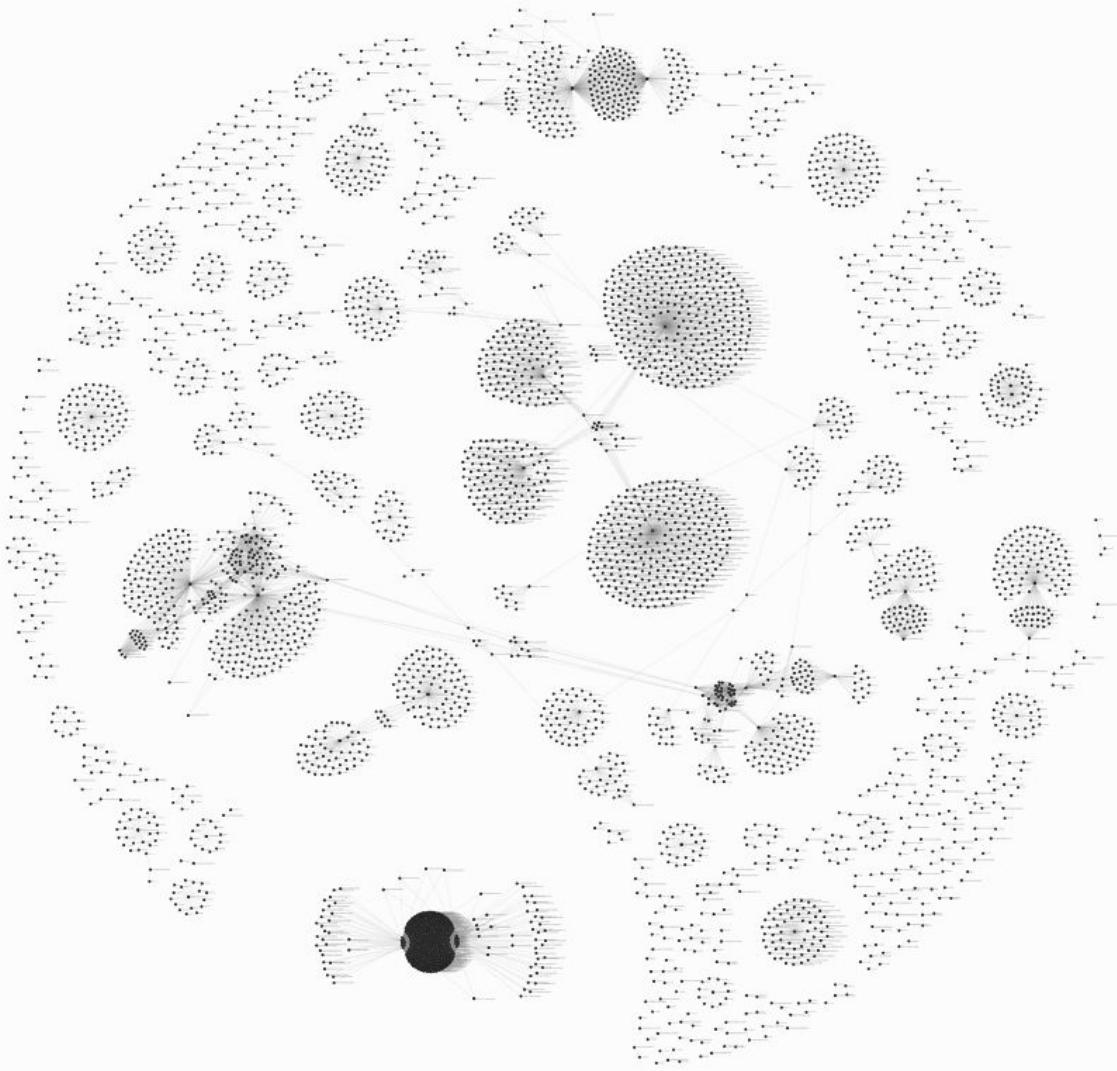
- a pyshark based script for extracting **network metadata** and **fingerprints** from pcap files and live network traffic
- Supported protocols: TLS, SSH, RDP, HTTP, gQUIC
- Main use-case: monitoring honeypots, network forensics
- Json output
- Downside: Performance

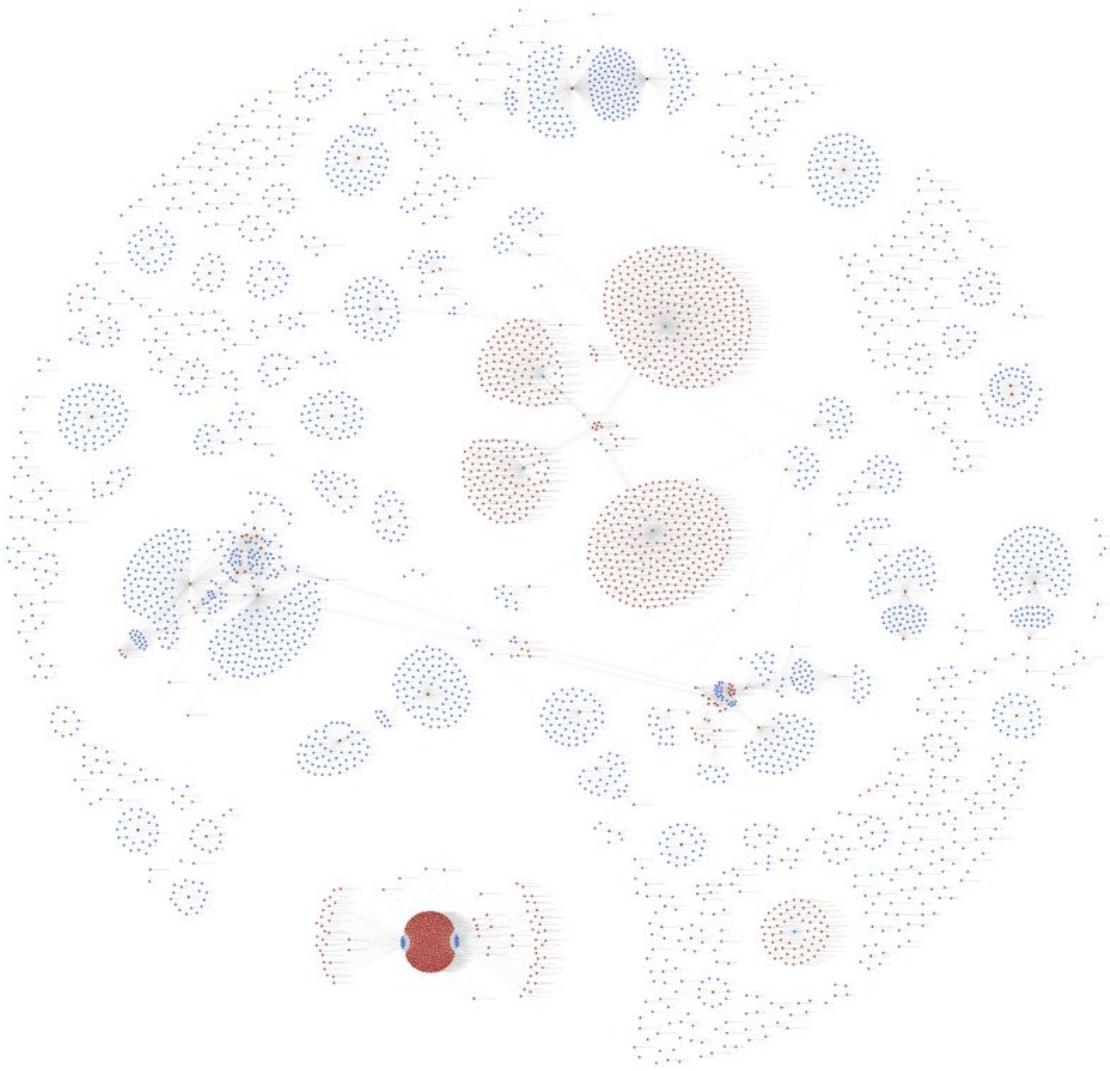
# Observations

[TLS]



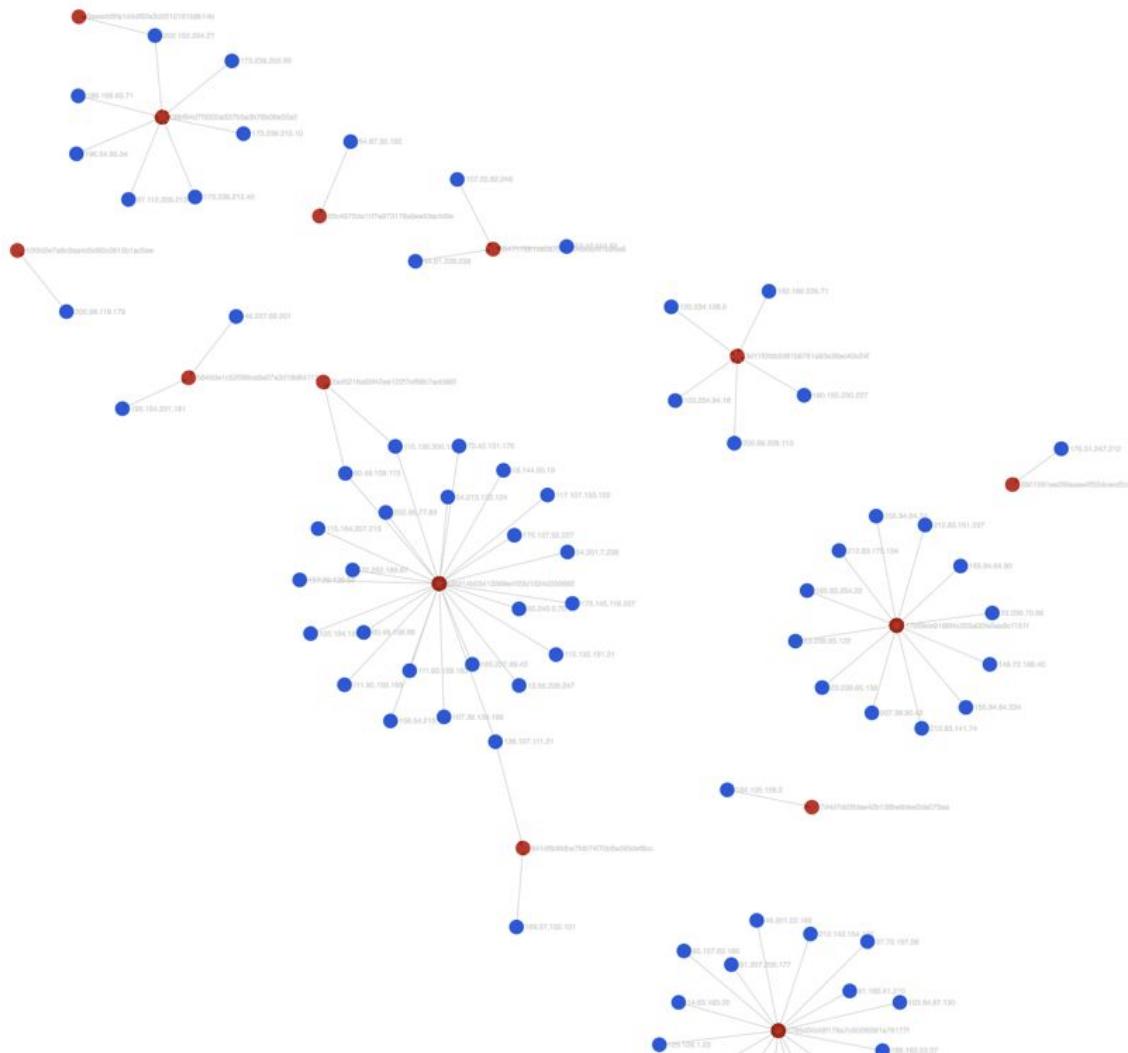
Src IP → ja3

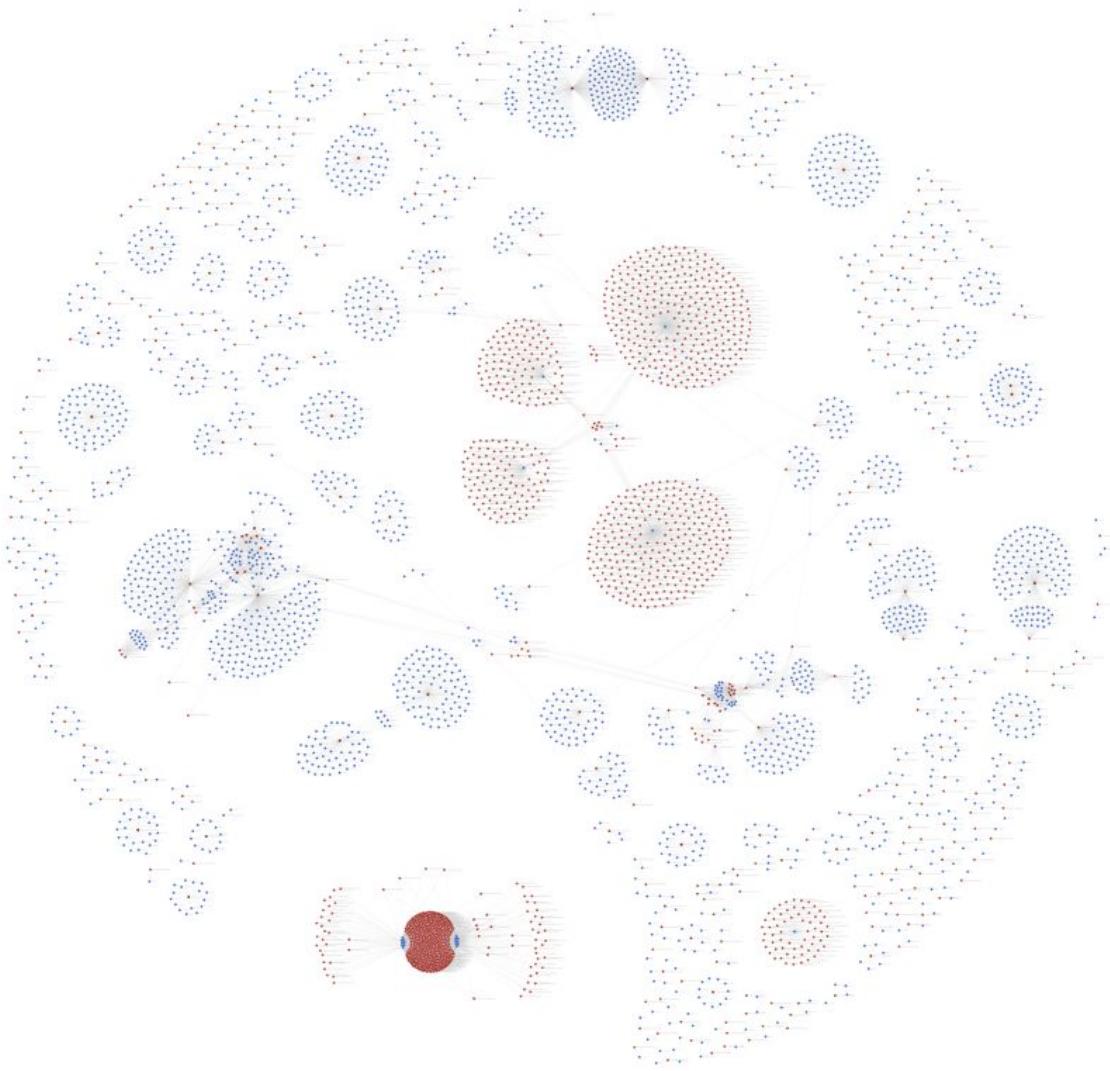




Src IP → ja3

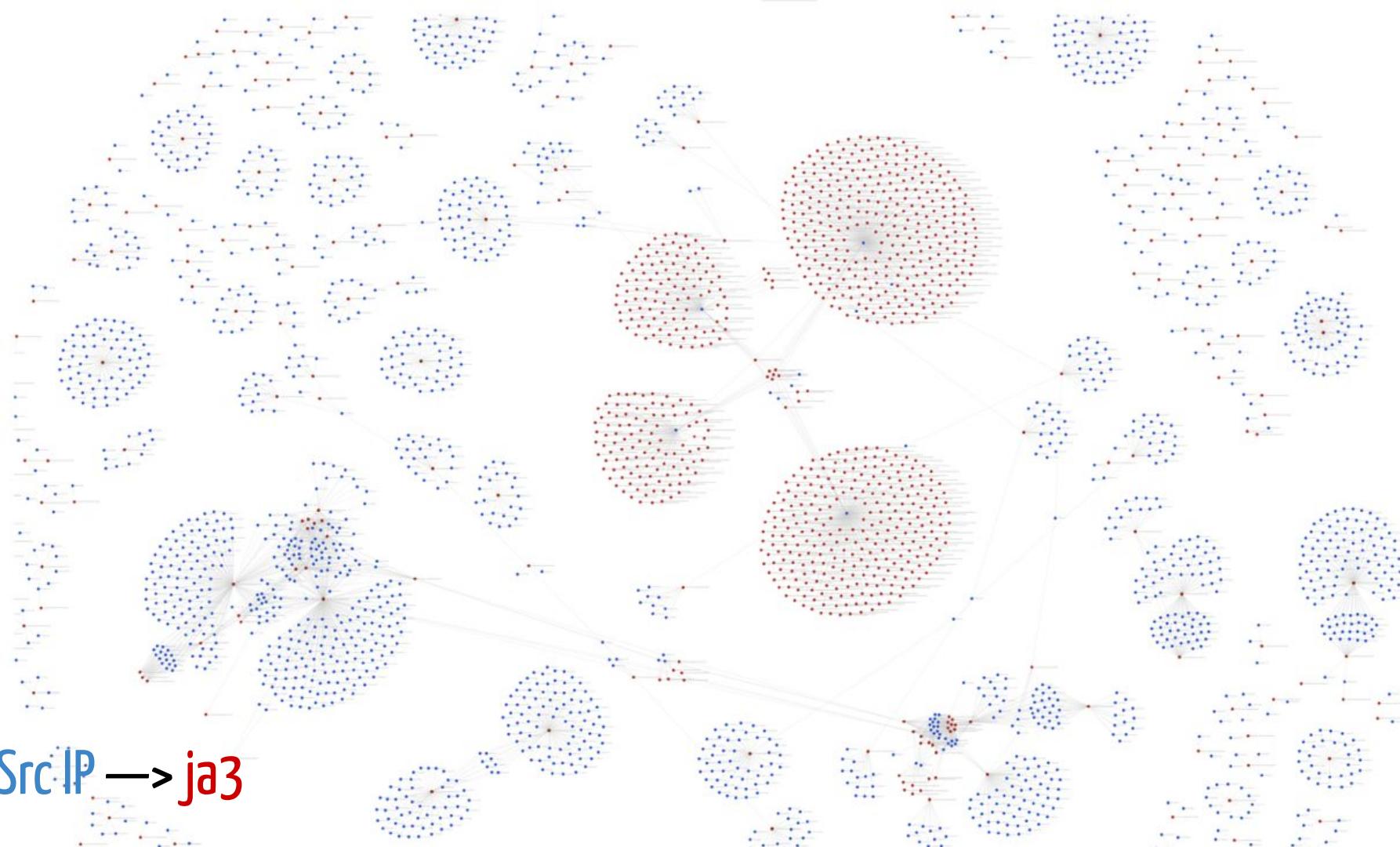
Src IP → ja3



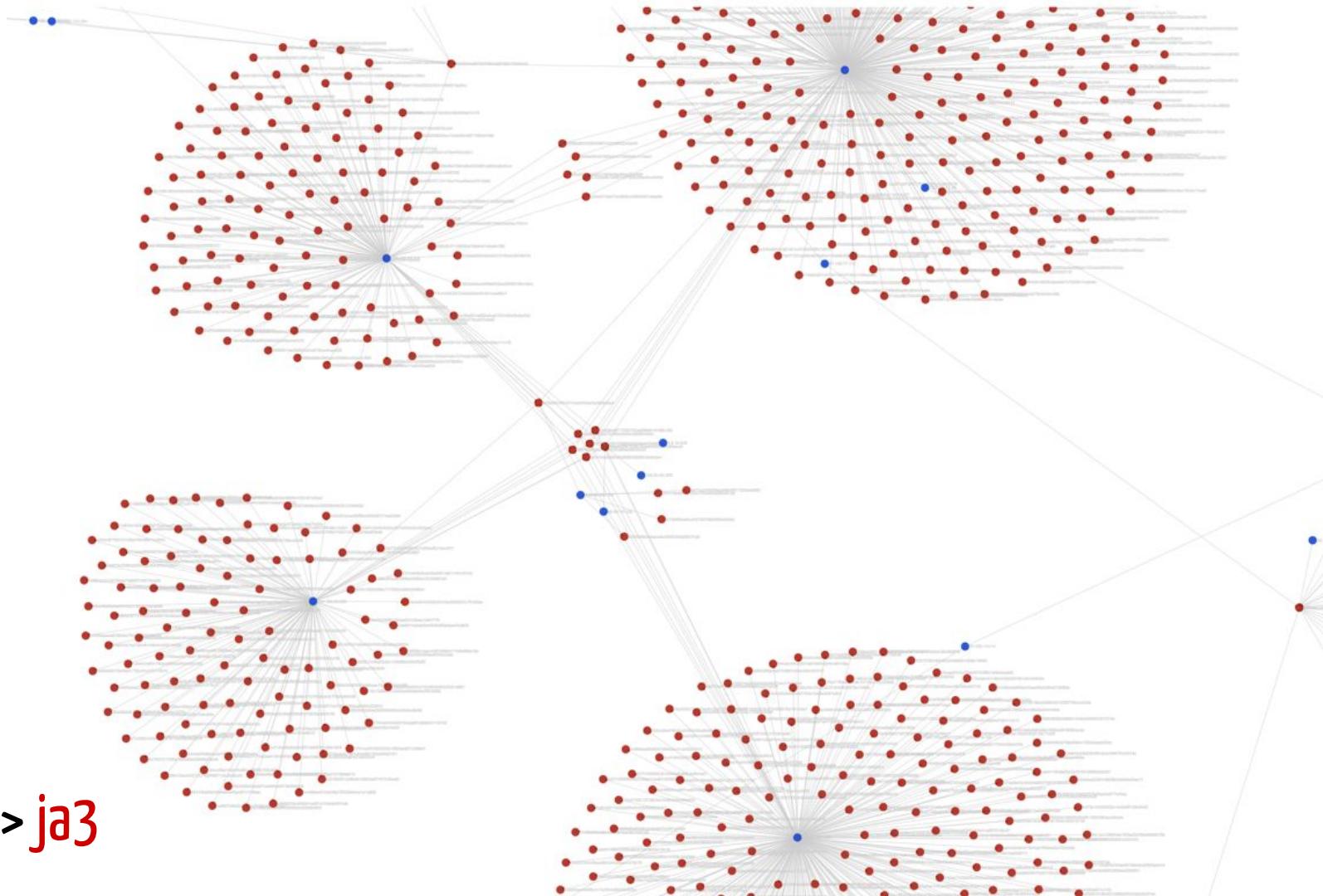


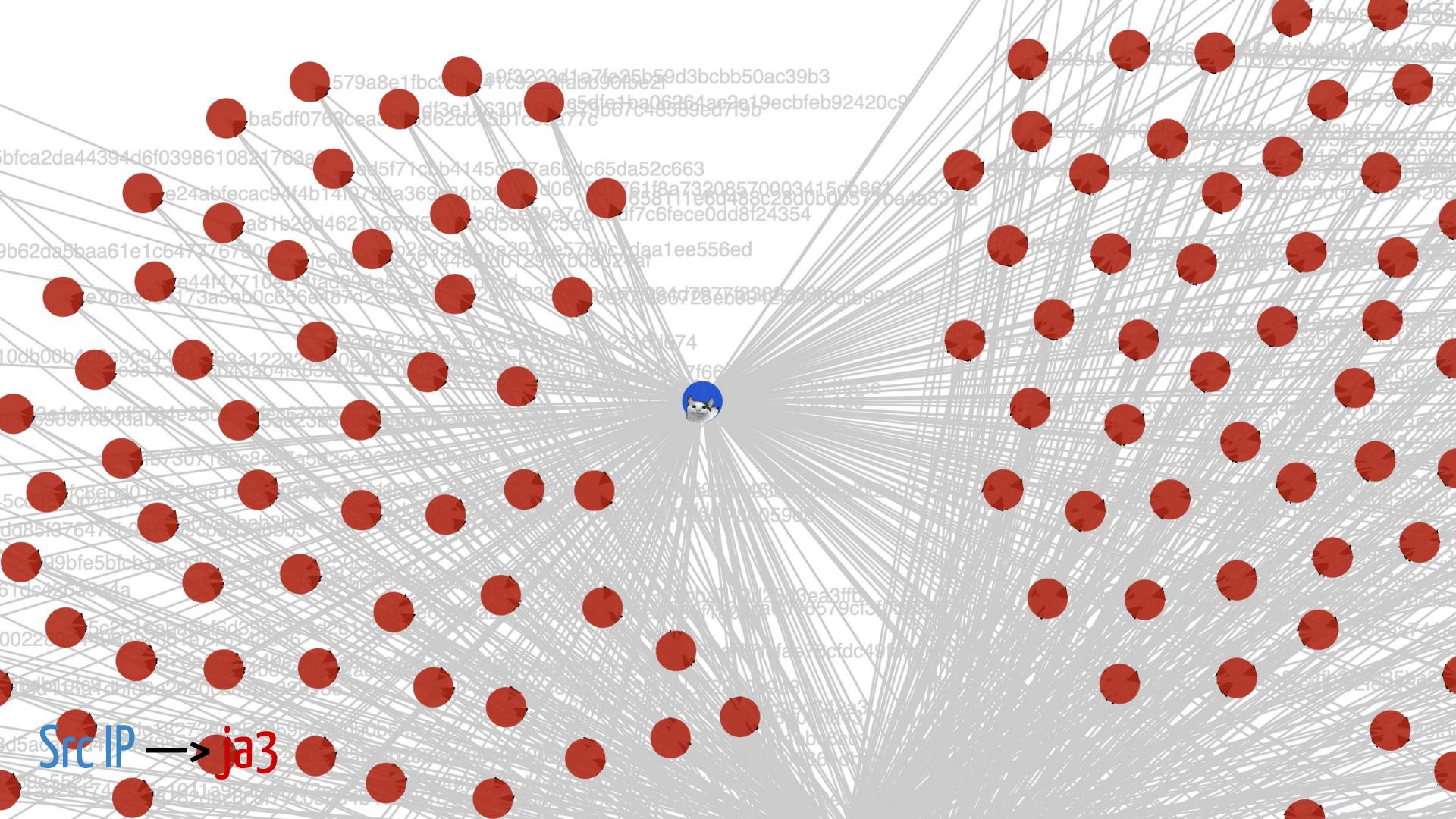
Src IP → ja3

Src IP → ja3



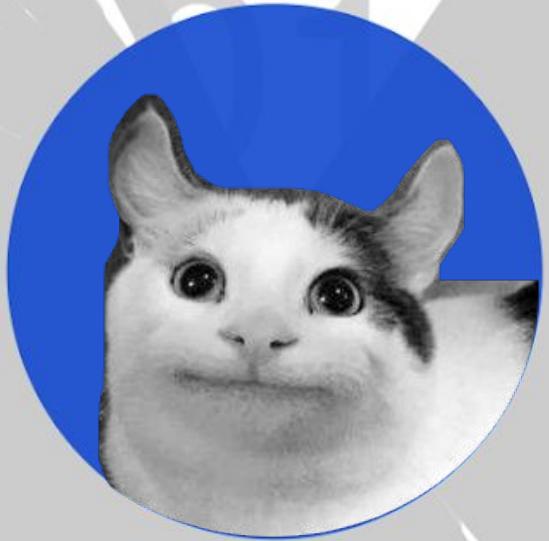
Src IP → ja3





Src IP → ja3





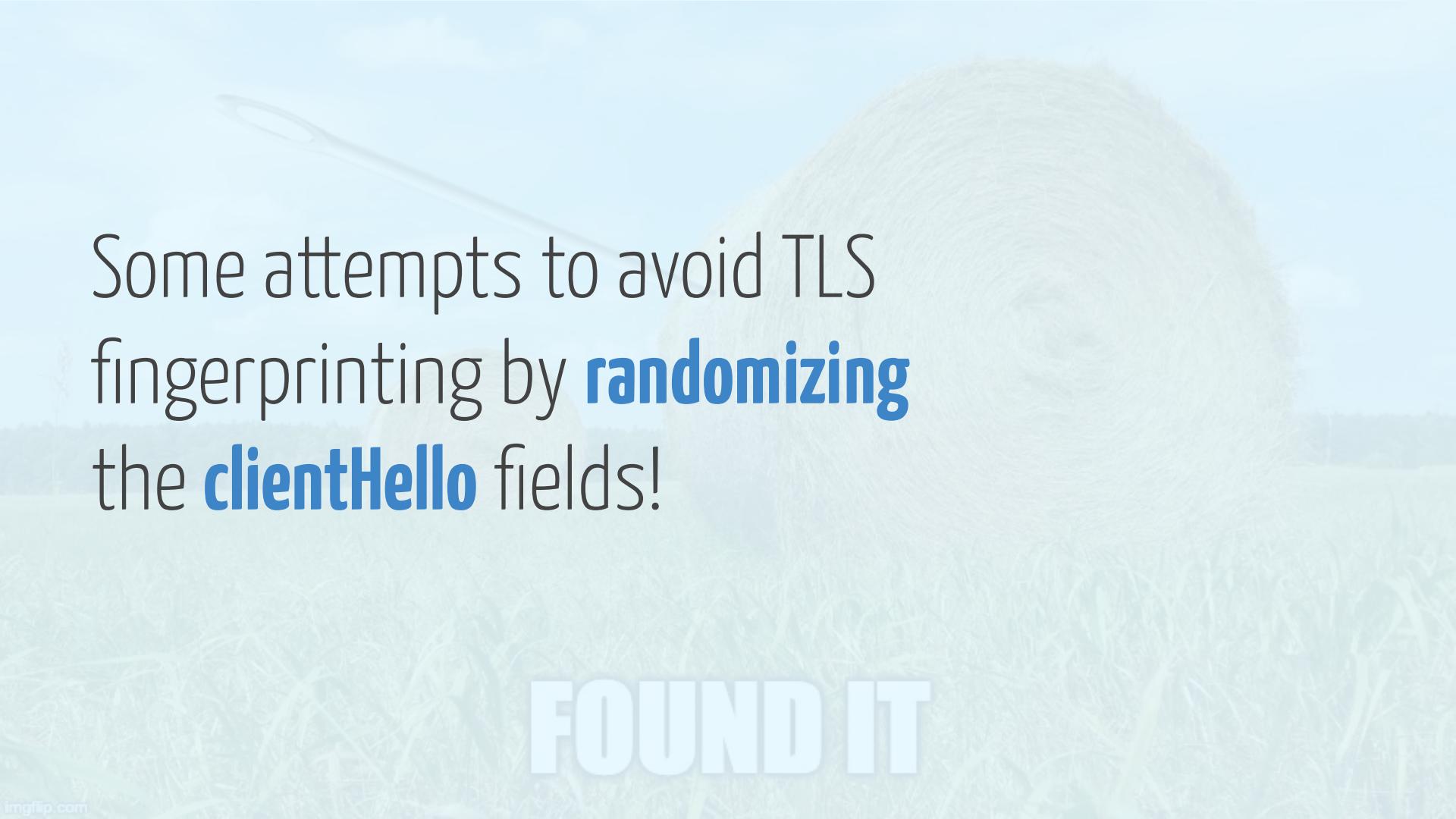
Src IP → ja3



Src IP → ja3



**FOUND IT**



Some attempts to avoid TLS  
fingerprinting by **randomizing**  
the **clientHello** fields!

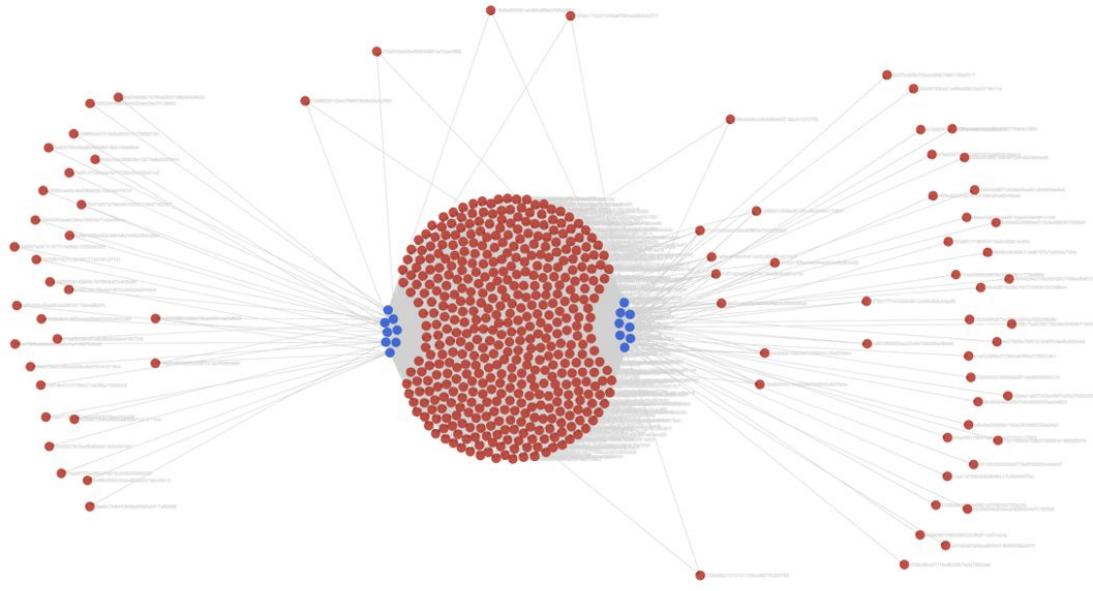
**FOUND IT**

A large, light-colored, textured pom-pom or ball of string serves as the background for the slide. It has a soft, fuzzy appearance with visible loops and strands.

Some attempts to avoid TLS  
fingerprinting by **randomizing**  
the **clientHello** fields!

They make themselves **easier** to detect by attempting to avoid fingerprinting !

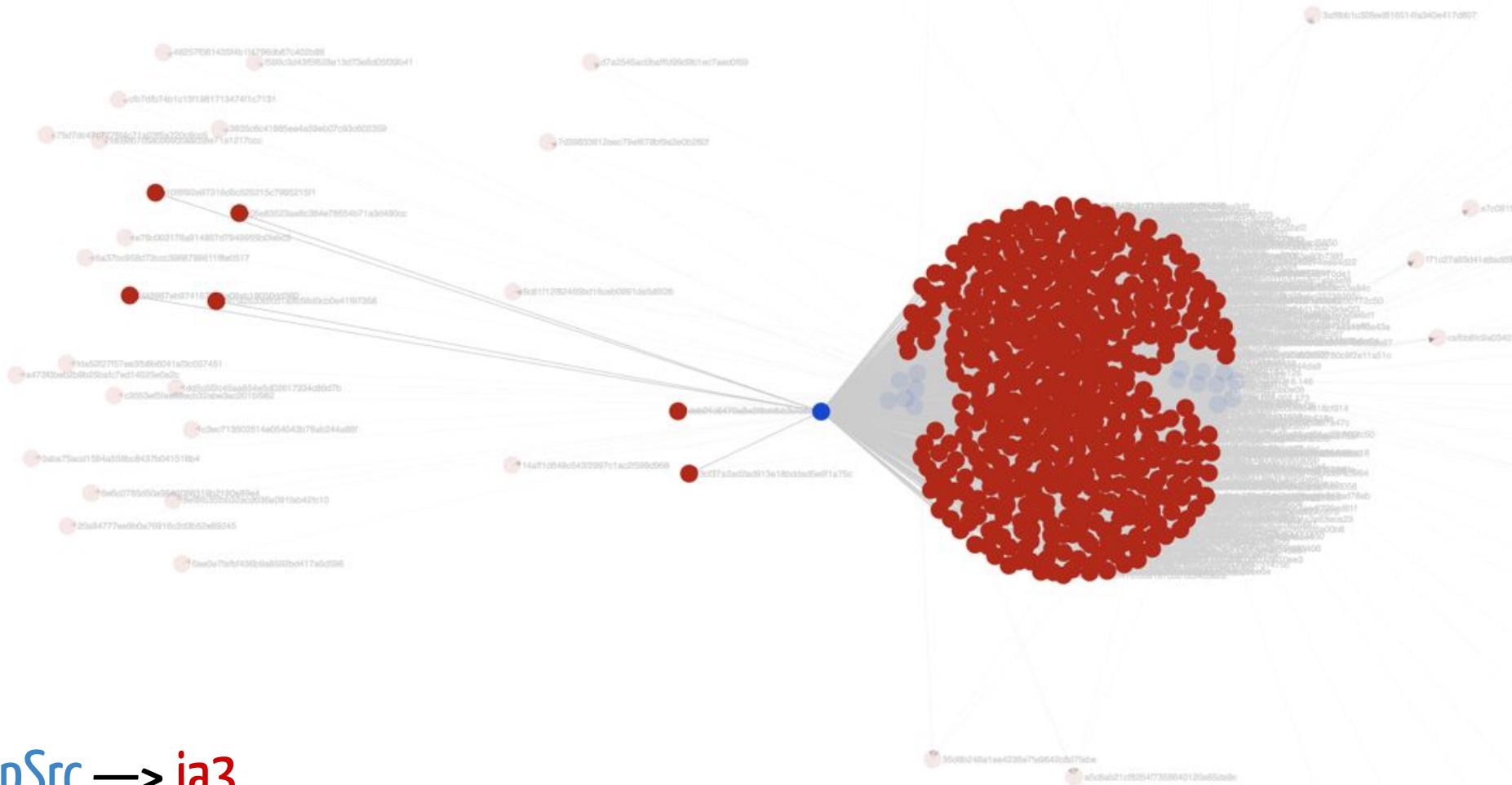
**FOUND IT**



one IP address → many JA3 values

3 different actors, 3 unique patterns

ipSrc → ja3



# Fingerprint Modification /evasion - I

| srcip   | dstport | ja3_hash                         | ja3_fields | ja3_str_length | request                      | tool        | org         | asn     | os          |
|---------|---------|----------------------------------|------------|----------------|------------------------------|-------------|-------------|---------|-------------|
| 184.185 | 443     | c044e9bc139d7e54aa9ed62568470de1 | 2,0,,,     | 6              |                              |             | Linode, LLC | AS63949 | Linux 3.11+ |
| 28.185  | 443     | c044e9bc139d7e54aa9ed62568470de1 | 2,0,,,     | 6              |                              |             | Linode, LLC | AS63949 | Linux 3.11+ |
| 181.53  | 443     | c044e9bc139d7e54aa9ed62568470de1 | 2,0,,,     | 6              |                              |             | Linode, LLC | AS63949 | Linux 3.11+ |
| 216.146 | 443     | c044e9bc139d7e54aa9ed62568470de1 | 2,0,,,     | 6              |                              |             | Linode, LLC | AS63949 | Linux 3.11+ |
| 176.220 | 443     | c044e9bc139d7e54aa9ed62568470de1 | 2,0,,,     | 6              |                              |             | Linode, LLC | AS63949 | Linux 3.11+ |
| 207.173 | 443     | c044e9bc139d7e54aa9ed62568470de1 | 2,0,,,     | 6              |                              |             | Linode, LLC | AS63949 | Linux 3.11+ |
| 45.103  | 443     | c044e9bc139d7e54aa9ed62568470de1 | 2,0,,,     | 6              |                              |             | Linode, LLC | AS63949 | Linux 3.11+ |
| 216.146 | 443     | c044e9bc139d7e54aa9ed62568470de1 | 2,0,,,     | 6              |                              |             | Linode, LLC | AS63949 | Linux 3.11+ |
| 153.71  | 443     | c044e9bc139d7e54aa9ed62568470de1 | 2,0,,,     | 6              |                              |             | Linode      | AS63949 |             |
| 154.126 | 443     | c044e9bc139d7e54aa9ed62568470de1 | 2,0,,,     | 6              |                              |             | Linode      | AS63949 |             |
| 180.112 | 443     | c044e9bc139d7e54aa9ed62568470de1 | 2,0,,,     | 6              |                              |             | Linode, LLC | AS63949 | Linux 3.11+ |
| 172.241 | 443     | c044e9bc139d7e54aa9ed62568470de1 | 2,0,,,     | 6              |                              |             | Linode, LLC | AS63949 | Linux 3.11+ |
| 132.213 | 443     | c044e9bc139d7e54aa9ed62568470de1 | 2,0,,,     | 6              |                              |             | Linode      | AS63949 |             |
| .57     | 443     | c044e9bc139d7e54aa9ed62568470de1 | 2,0,,,     | 6              |                              |             | Linode, LLC | AS63949 | Linux 3.11+ |
| 237.43  | 443     | c044e9bc139d7e54aa9ed62568470de1 | 2,0,,,     | 6              | \x15\x03\x03\x00\x02\x01\x00 | ZMAP_CLIENT | Linode, LLC | AS63949 | Linux 3.11+ |
| 253.76  | 443     | c044e9bc139d7e54aa9ed62568470de1 | 2,0,,,     | 6              |                              |             | Linode, LLC | AS63949 | Linux 3.11+ |
| 184.185 | 443     | c044e9bc139d7e54aa9ed62568470de1 | 2,0,,,     | 6              |                              |             | Linode, LLC | AS63949 | Linux 3.11+ |
| 198.123 | 443     | c044e9bc139d7e54aa9ed62568470de1 | 2,0,,,     | 6              | \x15\x03\x03\x00\x02\x01\x00 |             | Linode, LLC | AS63949 | Linux 3.11+ |
| 237.43  | 443     | c044e9bc139d7e54aa9ed62568470de1 | 2,0,,,     | 6              | \x15\x03\x03\x00\x02\x01\x00 |             | Linode, LLC | AS63949 | Linux 3.11+ |

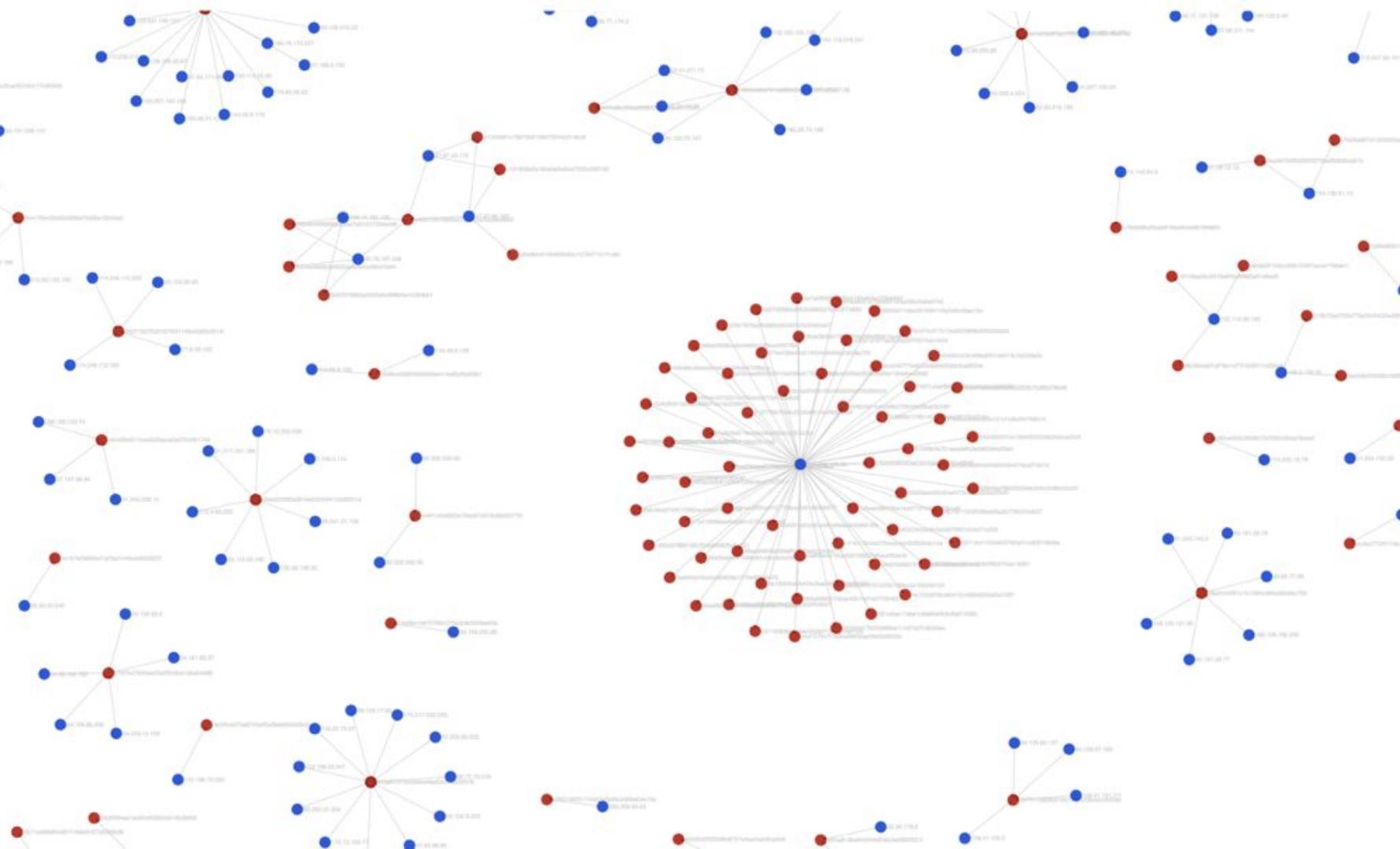
# Fingerprint Modification /evasion - I

|                 |         | ja3_fields                       | ja3_str_length | request | tool                         | org         | asn         | os          |             |
|-----------------|---------|----------------------------------|----------------|---------|------------------------------|-------------|-------------|-------------|-------------|
| srcip           | dstport | ja3_hash                         |                |         |                              |             |             |             |             |
| 139.162.184.185 | 443     | dbeecf711df2f2311b34ea8c1afa4ef8 | 2,131200,,,    | 11      |                              | Linode, LLC | AS63949     | Linux 3.11+ |             |
| 178.79.128.185  | 443     | dbeecf711df2f2311b34ea8c1afa4ef8 | 2,131200,,,    | 11      |                              | Linode, LLC | AS63949     | Linux 3.11+ |             |
| 139.162.181.53  | 443     | dbeecf711df2f2311b34ea8c1afa4ef8 | 2,131200,,,    | 11      |                              | Linode, LLC | AS63949     | Linux 3.11+ |             |
| 151.236.216.146 | 443     | dbeecf711df2f2311b34ea8c1afa4ef8 | 2,131200,,,    | 11      |                              | Linode, LLC | AS63949     | Linux 3.11+ |             |
| 139.162.176.220 | 443     | dbeecf711df2f2311b34ea8c1afa4ef8 | 2,131200,,,    | 11      |                              | Linode, LLC | AS63949     | Linux 3.11+ |             |
| 139.162.207.173 | 443     | dbeecf711df2f2311b34ea8c1afa4ef8 | 2,131200,,,    | 11      |                              | Linode, LLC | AS63949     | Linux 3.11+ |             |
| 212.71.245.103  | 443     | dbeecf711df2f2311b34ea8c1afa4ef8 | 2,131200,,,    | 11      |                              | Linode, LLC | AS63949     | Linux 3.11+ |             |
| 151.236.216.146 | 443     | dbeecf711df2f2311b34ea8c1afa4ef8 | 2,131200,,,    | 11      |                              | Linode, LLC | AS63949     | Linux 3.11+ |             |
| 172.104.153.71  | 443     | dbeecf711df2f2311b34ea8c1afa4ef8 | 2,131200,,,    | 11      |                              | Linode      | AS63949     |             |             |
| 172.104.154.126 | 443     | dbeecf711df2f2311b34ea8c1afa4ef8 | 2,131200,,,    | 11      |                              | Linode      | AS63949     |             |             |
| 139.162.180.112 | 443     | dbeecf711df2f2311b34ea8c1afa4ef8 | 2,131200,,,    | 11      |                              | Linode, LLC | AS63949     | Linux 3.11+ |             |
| 139.162.172.241 | 443     | dbeecf711df2f2311b34ea8c1afa4ef8 | 2,131200,,,    | 11      |                              | Linode, LLC | AS63949     | Linux 3.11+ |             |
| 172.104.132.213 | 443     | dbeecf711df2f2311b34ea8c1afa4ef8 | 2,131200,,,    | 11      |                              | Linode      | AS63949     |             |             |
| 185.3.94.57     | 443     | dbeecf711df2f2311b34ea8c1afa4ef8 | 2,131200,,,    | 11      |                              | Linode, LLC | AS63949     | Linux 3.11+ |             |
| 139.162.237.43  | 443     | dbeecf711df2f2311b34ea8c1afa4ef8 | 2,131200,,,    | 11      | \x15\x03\x03\x00\x02\x01\x00 | Linode, LLC | AS63949     | Linux 3.11+ |             |
| 139.162.253.76  | 443     | dbeecf711df2f2311b34ea8c1afa4ef8 | 2,131200,,,    | 11      |                              | ZMAP_CLIENT | Linode, LLC | AS63949     | Linux 3.11+ |
| 139.162.184.185 | 443     | dbeecf711df2f2311b34ea8c1afa4ef8 | 2,131200,,,    | 11      |                              | Linode, LLC | AS63949     | Linux 3.11+ |             |
| 139.162.198.123 | 443     | dbeecf711df2f2311b34ea8c1afa4ef8 | 2,131200,,,    | 11      | \x15\x03\x03\x00\x02\x01\x00 | Linode, LLC | AS63949     | Linux 3.11+ |             |
| 139.162.237.43  | 443     | dbeecf711df2f2311b34ea8c1afa4ef8 | 2,131200,,,    | 11      | \x15\x03\x03\x00\x02\x01\x00 | Linode, LLC | AS63949     | Linux 3.11+ |             |
| 139.162.184.185 | 443     | d6fb7815e88dd0d8b15528b78c04b223 | 2,131200,,,    | 11      |                              | Linode, LLC | AS63949     | Linux 3.11+ |             |
| 178.79.128.185  | 443     | d6fb7815e88dd0d8b15528b78c04b223 | 2,131200,,,    | 11      |                              | Linode, LLC | AS63949     | Linux 3.11+ |             |

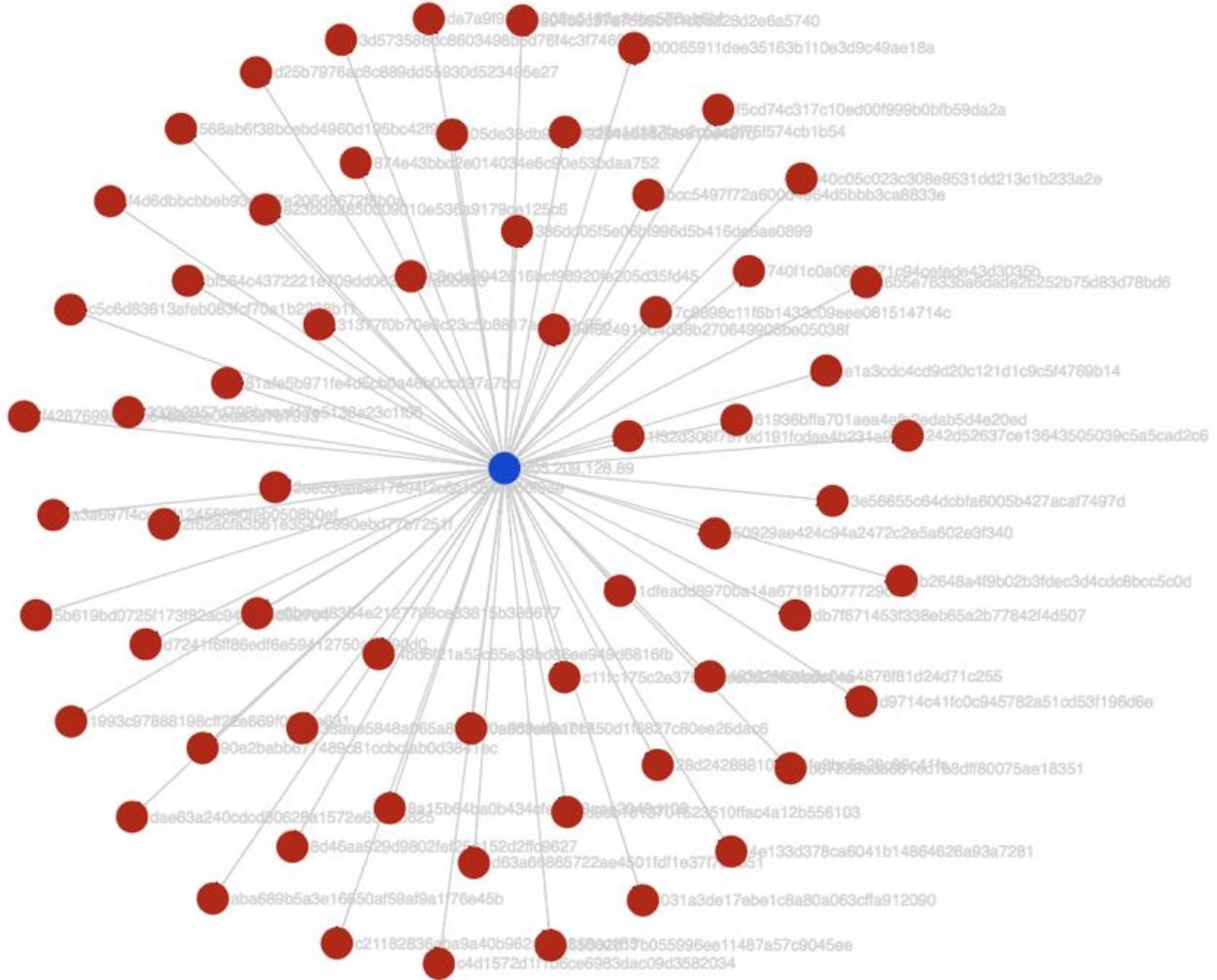
# Fingerprint Modification /evasion - I

| ja3_fields       |
|------------------|
| 768,21-255,,,    |
| 768,27-255,,,    |
| 768,49175-255,,, |
| 768,99-255,,,    |
| 768,12-255,,,    |
| 768,26-255,,,    |
| 768,9-255,,,     |
| 768,98-255,,,    |
| 768,100-255,,,   |
| 768,96-255,,,    |
| 768,97-255,,,    |
| 768,101-255,,,   |
| 768,14-255,,,    |
| 768,17-255,,,    |
| 768,20-255,,,    |
| 768,25-255,,,    |
| 768,8-255,,,     |
| 768,11-255,,,    |
| 768,23-255,,,    |
| 768,49158-255,,, |

| _time                        | srcip           | ja3_hash                          |
|------------------------------|-----------------|-----------------------------------|
| 2018-04-10T20:18:00.119+0000 | 139.162.184.185 | df092ef5e7a32dabcd42442c0037912e  |
| 2018-04-10T20:18:00.119+0000 | 139.162.184.185 | 10df32b3dcc46f4a7e481a370840519f  |
| 2018-04-10T20:18:00.119+0000 | 139.162.184.185 | faab34f1247b30b9f615903c4220076e  |
| 2018-04-10T20:18:00.119+0000 | 139.162.184.185 | 05fcf8b1aa9016b275cf79d47358771e  |
| 2018-04-10T20:18:00.123+0000 | 139.162.184.185 | e7968c3b72ecd03a7184ea034d4fec62  |
| 2018-04-10T20:18:00.123+0000 | 139.162.184.185 | f0294f0f8850c715eeadd675b7747b79  |
| 2018-04-10T20:18:00.123+0000 | 139.162.184.185 | 4283e21040c4417a3232fd4782918c16  |
| 2018-04-10T20:18:00.123+0000 | 139.162.184.185 | fee19778297abf56e541914ff74f6226  |
| 2018-04-10T20:18:00.126+0000 | 139.162.184.185 | 29bd6b9bf3f407b70f557eb2057896d8  |
| 2018-04-10T20:18:00.126+0000 | 139.162.184.185 | 5c89f4ec38319d55b7f885b7622c3a03  |
| 2018-04-10T20:18:00.126+0000 | 139.162.184.185 | 83386cbe78ad6346c0f91632747217a5  |
| 2018-04-10T20:18:00.131+0000 | 139.162.184.185 | acf5ddb3359966e4e5abc95aff84fa8   |
| 2018-04-10T20:18:00.131+0000 | 139.162.184.185 | 6846665f62c94d752775700ad8eb48ad  |
| 2018-04-10T20:18:00.131+0000 | 139.162.184.185 | 840d5724fbcd39003ecf99064d21c95e  |
| 2018-04-10T20:18:00.131+0000 | 139.162.184.185 | 965d9c52af5efc63b3fc1c78fede00f8  |
| 2018-04-10T20:18:00.131+0000 | 139.162.184.185 | 3cd877cf75cccd1b90046cb01e99c0619 |
| 2018-04-10T20:18:00.131+0000 | 139.162.184.185 | 7172b4bf900f5b30f5b24214691bfc56  |
| 2018-04-10T20:18:00.135+0000 | 139.162.184.185 | c2cc4e4ac0df30d5964b622df86c52d1  |
| 2018-04-10T20:18:00.135+0000 | 139.162.184.185 | 7063171f81740a7339d37570d3d6db84  |
| 2018-04-10T20:18:00.135+0000 | 139.162.184.185 | 618e3c499018e55d62fe52fe7a059b57  |
| 2018-04-10T20:18:00.135+0000 | 139.162.184.185 | 4ef3bbebfaefe790c233ca98d49ccb48  |



ipSrc → ja3



# Fingerprint Modification /evasion - II

# ja3\_fields

|                              |        |  |
|------------------------------|--------|--|
|                              |        | 103-51-159-107-57-136-158-69-49200-49192-49172-49199-49191-49171-61          |
| 2018-01-30T20:59:26.669+0000 | 128.89 | 29-28-65279-65278-99-101-17-114-19-115-50-64-162-116-56-106-163-49218-49238- |
| 2018-01-30T20:59:27.121+0000 | 128.89 | 103-51-159-107-57-136-158-69-49192-49172-49199-49191-49171-61                |
| 2018-01-30T20:59:27.177+0000 | 128.89 | 103-51-159-107-57-136-158-69-49172-49199-49191-49171-61                      |
| 2018-01-30T20:59:27.712+0000 | 128.89 | 103-51-159-107-57-136-158-69-49172-49199-49191-49171-61                      |
| 2018-01-30T20:59:30.305+0000 | 128.89 | 49311-49315-159-49220-49234-49221-49235-69-190-49276-136-196-49277-52394-5   |
| 2018-01-30T20:59:30.661+0000 | 128.89 | 103-51-159-107-57-136-158-69-49199-49191-49171-61                            |
| 2018-01-30T20:59:31.085+0000 | 128.89 | 103-51-107-57-136-158-69-49199-49191-49171-61                                |
| 2018-01-30T20:59:31.629+0000 | 128.89 | 103-51-57-136-158-69-49199-49191-49171-61                                    |
| 2018-01-30T20:59:32.185+0000 | 128.89 | 103-51-136-158-69-49199-49191-49171-61                                       |
| 2018-01-30T20:59:35.053+0000 | 128.89 | 103-51-158-69-49199-49191-49171-61   |

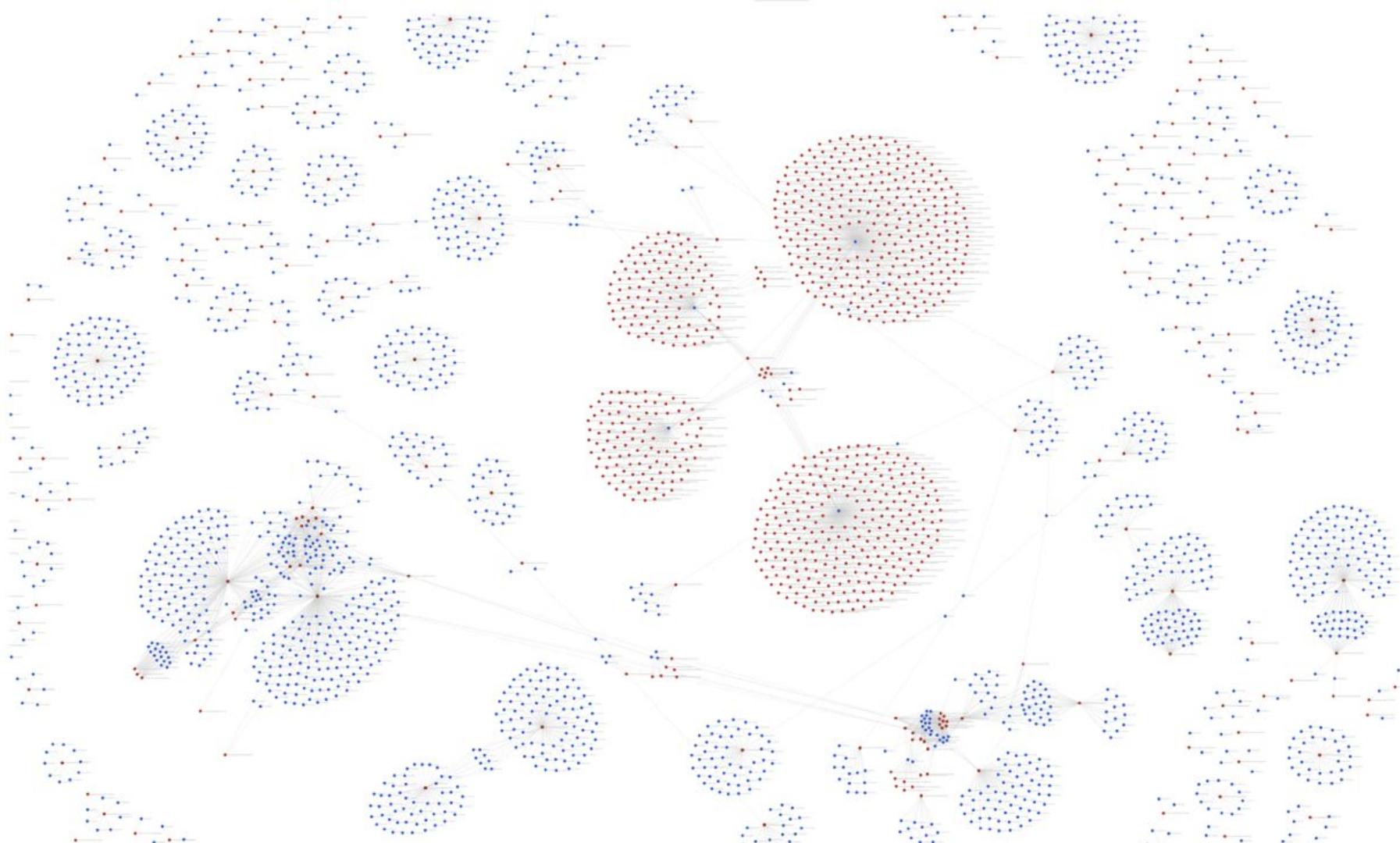
# Fingerprint Modification /evasion - II

|                              |        |  |
|------------------------------|--------|--|
|                              |        | 172-149-183-173-49256-49262-49257-49263-49304-49298-49305-49299-52398-46-184 |
| 2018-01-30T20:59:08.401+0000 | 128.89 | 185-146-124-10-125-47-60-49308-49312-156-126-53-61-49309-49313               |
| 2018-01-30T20:59:09.489+0000 | 128.89 | 185-146-124-10-125-47-60-49308-49312-156-126-53-49309-49313                  |
| 2018-01-30T20:59:10.593+0000 | 128.89 | 185-146-124-10-125-47-60-49308-49312-156-126-49309-49313                     |
| 2018-01-30T20:59:11.657+0000 | 128.89 | 185-146-124-10-125-47-60-49308-49312-126-49309-49313                         |
| 2018-01-30T20:59:12.857+0000 | 128.89 | 185-146-124-10-125-47-60-49308-49312-126-49309-49313                         |
| 2018-01-30T20:59:14.973+0000 | 128.89 | 185-146-124-10-125-47-49308-49312-126-49309-49313                            |
| 2018-01-30T20:59:16.445+0000 | 128.89 | 185-146-124-10-125-47-49308-49312-126-49309-49313                            |
| 2018-01-30T20:59:17.497+0000 | 128.89 | 185-146-124-10-125-49308-49312-126-49309-49313                               |
| 2018-01-30T20:59:18.793+0000 | 128.89 | 157-49212-49232-49213-49233-65-186-49274-132-192-49275-9-7-1-2               |
| 2018-01-30T20:59:19.849+0000 | 128.89 | 49212-49232-49213-49233-65-186-49274-132-192-49275-9-7-1-2                   |
| 2018-01-30T20:59:20.817+0000 | 128.89 | 49212-49232-49213-49233-65-186-49274-192-49275-9-7-1-2                       |
| 2018-01-30T20:59:21.613+0000 | 128.89 | 49212-49232-49213-49233-65-186-49274-192-49275-9-7-1-2                       |
| 2018-01-30T20:59:22.343+0000 | 128.89 | 49212-49232-49213-49233-186-49274-192-49275-9-7-1-2                          |
| 2018-01-30T20:59:25.547+0000 | 128.89 | 49212-49232-49213-49233-186-49274-192-49275-9-7-1-2                          |
| 2018-01-30T20:59:26.163+0000 | 128.89 | 59-4-5-150-49180-49183-49186-49179-49182-49185-49178-49181-49184             |
|                              |        | 103-51-159-107-57-136-158-69-49200-49192-49172-49199-49191-49171             |
|                              |        | 103-51   |
|                              |        | 51-103   |

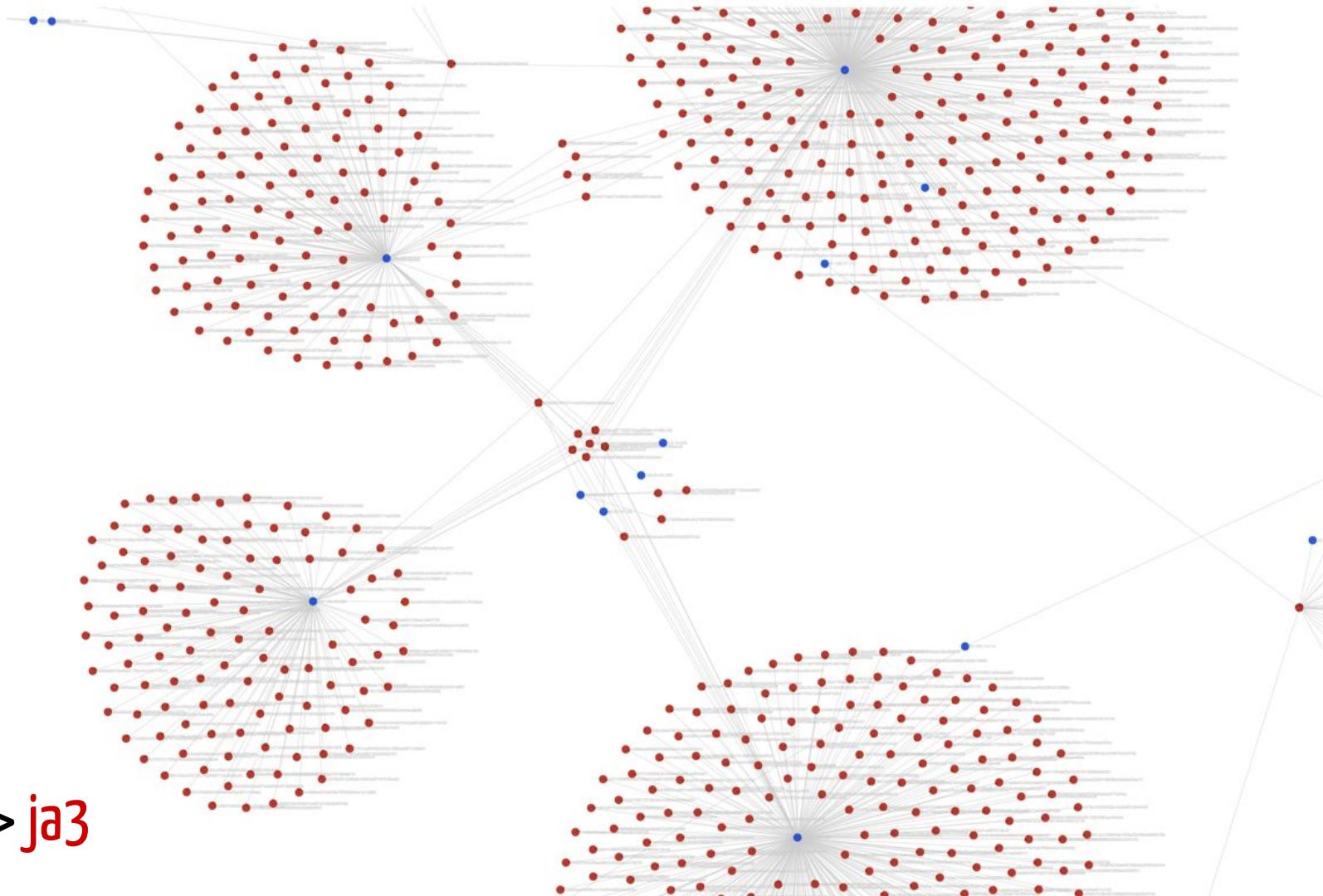
# Fingerprint Modification /evasion - II

|   |
|---|
| 49188-49325-49327-49196-49224-49244-49225-49245-49266-49286-49267-49287-52393-52244-49158 |
| 49159-49204-49205-49207-49206-49208-49264-49265-49306-49307-52396-49209-49210-49211-49203 |
| 49170-49171-49191-49199-49172-49192-49200-49228-49248-49229-49249-49270-49290-49271-49291 |
| 49170-49171-49191-49199-49172-49192-49228-49248-49229-49249-49270-49290-49271-49291       |
| 49170-49171-49191-49199-49172-49228-49248-49229-49249-49270-49290-49271-49291             |
| 49170-49171-49191-49199-49228-49248-49229-49249-49270-49290-49271-49291                   |
| 49170-49171-49191-49228-49248-49229-49249-49270-49290-49271-49291                         |
| 49170-49171-49228-49248-49229-49249-49270-49290-49271-49291                               |
| 49170-49228-49248-49229-49249-49270-49290-49271-49291                                     |

|   |
|---|
| 49303-49297-52397-45-180-181-142-20-119-22-120-51-103-49310-49314       |
| 49303-49297-52397-45-180-181-142-20-119-22-120-51-49310-49314           |
| 49303-49297-52397-45-180-181-142-20-119-22-120-49310-49314              |
| 158-121-57-107-49311-49315-159-49220-49234-49221-49235-69-190-49276-136 |
| 158-121-57-107-49311-49315-49220-49234-49221-49235-69-190-49276-136     |
| 158-121-57-49311-49315-49220-49234-49221-49235-69-190-49276-136         |
| 158-121-49311-49315-49220-49234-49221-49235-69-190-49276-136            |
| 158-121-49311-49315-49220-49234-49221-49235-69-190-49276                |
| 121-49311-49315-49220-49234-49221-49235-69-190-49276                    |
| 121-49311-49315-49220-49234-49221-49235-190-49276                       |



ipSrc → ja3



# Fingerprint Modification /evasion - III

| ja3_ciphers                  |         |  |
|------------------------------|---------|--|
| _time                        | srcip   | ja3  |
| 2018-01-12T08:09:11.794+0000 | .26.237 | 27a33d6c1e581cf2783  |
|                              |         | 458944-327808-196736-65664-524416-393280-262272-131200   |
| 2018-01-12T08:09:11.842+0000 | .26.237 | e76a0619f4cf744ab2b!   |
|                              |         | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10                               |
| 2018-01-12T08:09:11.842+0000 | .26.237 | 6b2355cd870327854d   |
|                              |         | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10                               |
| 2018-01-12T08:09:11.842+0000 | .26.237 | 8d9e064b97093a2c47!  |
|                              |         | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10                               |
| 2018-01-12T08:09:11.842+0000 | .26.237 | 27a33d6c1e581cf2783  |
|                              |         | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10                               |
| 2018-01-12T08:09:11.886+0000 | .26.237 | a22efd10e07be383b4c  |
|                              |         | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10                               |
| 2018-01-12T08:09:11.934+0000 | .26.237 | 99f66d824338b066f1b  |
|                              |         | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10                               |
| 2018-01-12T08:09:11.978+0000 | .26.237 | 27a33d6c1e581cf2783  |
|                              |         | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10                               |
| 2018-01-12T08:09:12.026+0000 | .26.237 | d5ad1a88d4c511586af  |
|                              |         | 0-22016  |
| 2018-01-12T08:09:12.072+0000 | .26.237 | a7674bf7508673e9d0e  |
|                              |         | 148-49283-28-157-49236-49308-12-171-177-5-40-49215-49239-156-49207-69-36-11-54-82-183-27-90-49237-32 |
| 2018-01-12T08:09:12.072+0000 | .26.237 | 0443db5df8b9dcc91ae  |
|                              |         | 49176-49214-177-49234-62-67-82-59-49179-50-49158-171-146-65-134-189-143-49252-49194-46-49319-49202-  |
| 2018-01-12T08:09:12.072+0000 | .26.237 | 17c9534bfc2a8edeb78  |
|                              |         | 64-49194-75-175-76-187-49293-49296-48-39-181-38-134-49315-159-9-92-170-81-49227-126-55-137-52245-128 |
| 2018-01-12T08:09:12.072+0000 | .26.237 | cff64173dc5b1e96141c   |
|                              |         | 49269-183-49316-49202-44-49248-49236-49163-82-49159-49229-144-49257-49185-11-54-12-186-157-67-49290  |
| 2018-01-12T08:09:12.072+0000 | .26.237 | 5f68c6edaa625acbb8b  |
|                              |         | 49269-183-49316-49202-44-49248-49236-49163-82-49159-49229-144-49257-49185-11-54-12-186-157-67-49290  |
| 2018-01-12T08:09:12.072+0000 | .26.237 | 63fa392b1105a8c4318  |
|                              |         | 55-191-49209-33-170-48-49203-176-49321-49169-190-49314-49182-153-49220-18-195-187-92-137-96-39-4930  |
| 2018-01-12T08:09:12.072+0000 | .26.237 | 5933eab69b3db48087   |
|                              |         | 189-49205-126-167-49306-49320-49160-37-90-22-49188-134-49223-115-175-49168-63-184-88-49156-49221-49  |
| 2018-01-12T08:09:12.072+0000 | .26.237 | c6343c3579d2e0ea07   |
|                              |         | 180-49306-84-49181-49254-49313-49320-49289-89-49261-184-49284-107-49269-49302-22-103-49249-49305-49  |
| 2018-01-12T08:09:12.072+0000 | .26.237 | dd6a913257a568cff93  |
|                              |         | 137-96-49259-170-163-116-49199-54-49248-49200-49230-172-48-64-49269-75-145-193-70-49163-49290-53-49  |
| 2018-01-12T08:09:12.072+0000 | .26.237 | 9a1b3fc416b0b64e228  |
|                              |         | 65279-24-49186-57-161-49218-49162-34-165-140-49-51-49295-49233-56-150-179-98-65278-49208-49179-4915  |
| 2018-01-12T08:09:12.073+0000 | .26.237 | 1482d0297ccdfdd83c   |
|                              |         | 49178-49216-49208-49279-49164-43-49265-92-49266-51-138-52245-19-49270-49307-154-160-49195-121-4919   |
| 2018-01-12T08:09:12.118+0000 | .26.237 | 681843facb648b3494c  |
|                              |         | 63-30-65278-49153-147-40-49196-49171-61-29-196-79-49242-16-38-49227-49160-57-49315-52-99-49299-1-49  |
|                              |         | 49173-49317-174-49272-49190-47-42-141-49161-168-108-71-17-49240-75-175-76-187-49293-49296-64-49194-  |

# Fingerprint Modification /evasion - III

| _time                        | srcip   | ja3                  | ja3_ciphers  |
|------------------------------|---------|----------------------|--|
| 2018-01-12T08:09:11.794+0000 | .26.237 | 27a33d6c1e581cf2783  | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10                               |
| 2018-01-12T08:09:11.842+0000 | .26.237 | e76a0619f4cf744ab2b! | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10                               |
| 2018-01-12T08:09:11.842+0000 | .26.237 | 6b2355cd870327854d   | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10                               |
| 2018-01-12T08:09:11.842+0000 | .26.237 | 8d9e064b97093a2c47!  | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10                               |
| 2018-01-12T08:09:11.842+0000 | .26.237 | 27a33d6c1e581cf2783  | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10                               |
| 2018-01-12T08:09:11.886+0000 | .26.237 | a22efd10e07be383b4c  | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10                               |
| 2018-01-12T08:09:11.934+0000 | .26.237 | 99f66d824338b066f1b  | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10                               |
| 2018-01-12T08:09:11.978+0000 | .26.237 | 27a33d6c1e581cf2783  | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10                               |
| 2018-01-12T08:09:12.026+0000 | .26.237 | d5ad1a88d4c511586af  | 0-22016  |
| 2018-01-12T08:09:12.072+0000 | .26.237 | a7674bf7508673e9d0e  | 148-49283-28-157-49236-49308-12-171-177-5-40-49215-49239-156-49207-69-36-11-54-82-183-27-90-49237-32 |
| 2018-01-12T08:09:12.072+0000 | .26.237 | 0443db5df8b9dcc91ae  | 49176-49214-177-49234-62-67-82-59-49179-50-49158-171-146-65-134-189-143-49252-49194-46-49319-49202-  |
| 2018-01-12T08:09:12.072+0000 | .26.237 | 17c9534bfc2a8edeb78  | 64-49194-75-175-76-187-49293-49296-48-39-181-38-134-49315-159-9-92-170-81-49227-126-55-137-52245-128 |
| 2018-01-12T08:09:12.072+0000 | .26.237 | cff64173dc5b1e96141c | 49269-183-49316-49202-44-49248-49236-49163-82-49159-49229-144-49257-49185-11-54-12-186-157-67-49290  |
| 2018-01-12T08:09:12.072+0000 | .26.237 | 5f68c6edaa625acbb8b  | 49162-156-157-47-53-49170-10   |
| 2018-01-12T08:09:12.072+0000 | .26.237 | 63fa392b1105a8c4318  | 55-191-49209-33-170-48-49203-176-49321-49169-190-49314-49182-153-49220-18-195-187-92-137-96-39-4930  |
| 2018-01-12T08:09:12.072+0000 | .26.237 | 5933eab69b3db48087   | 189-49205-126-167-49306-49320-49160-37-90-22-49188-134-49223-115-175-49168-63-184-88-49156-49221-49  |
| 2018-01-12T08:09:12.072+0000 | .26.237 | c6343c3579d2e0ea07   | 180-49306-84-49181-49254-49313-49320-49289-89-49261-184-49284-107-49269-49302-22-103-49249-49305-49  |
| 2018-01-12T08:09:12.072+0000 | .26.237 | dd6a913257a568cff93  | 137-96-49259-170-163-116-49199-54-49248-49200-49230-172-48-64-49269-75-145-193-70-49163-49290-53-49  |
| 2018-01-12T08:09:12.072+0000 | .26.237 | 9a1b3fc416b0b64e228  | 65279-24-49186-57-161-49218-49162-34-165-140-49-51-49295-49233-56-150-179-98-65278-49208-49179-4915  |
| 2018-01-12T08:09:12.073+0000 | .26.237 | 1482d0297ccdfdd83c   | 49178-49216-49208-49279-49164-43-49265-92-49266-51-138-52245-19-49270-49307-154-160-49195-121-4919   |
| 2018-01-12T08:09:12.118+0000 | .26.237 | 681843facb648b3494c  | 63-30-65278-49153-147-40-49196-49171-61-29-196-79-49242-16-38-49227-49160-57-49315-52-99-49299-1-49  |

# Fingerprint Modification /evasion - III

| _time                        | srcip   | ja3                  | ja3_ciphers  |
|------------------------------|---------|----------------------|--|
| 2018-01-12T08:09:11.794+0000 | .26.237 | 27a33d6c1e581cf2783  | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10<br>458944-327808-196736-65664-524416-393280-262272-131200 |
| 2018-01-12T08:09:11.842+0000 | .26.237 | e76a0619f4cf744ab2b! | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10   |
| 2018-01-12T08:09:11.842+0000 | .26.237 | 6b2355cd870327854d   | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10   |
| 2018-01-12T08:09:11.842+0000 | .26.237 | 8d9e064b97093a2c47   | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10   |
| 2018-01-12T08:09:11.842+0000 | .26.237 | 27a33d6c1e581cf2783  | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10   |
| 2018-01-12T08:09:11.886+0000 | .26.237 | a22efd10e07be383b4c  | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10   |
| 2018-01-12T08:09:11.934+0000 | .26.237 | 99f66d824338b066f1b  | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10   |
| 2018-01-12T08:09:11.978+0000 | .26.237 | 27a33d6c1e581cf2783  | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10   |
| 2018-01-12T08:09:12.026+0000 | .26.237 | d5ad1a88d4c511586af  | 0-22016  |
| 2018-01-12T08:09:12.072+0000 | .26.237 | a7674bf7508673e9d0e  | 148-49283-28-157-49236-49308-12-171-177-5-40-49215-49239-156-49207-69-36-11-54-82-183-27-90-49237-32                             |
| 2018-01-12T08:09:12.072+0000 | .26.237 | 0443db5df8b9dcc91ae  | 49176-49214-177-49234-62-67-82-59-49179-50-49158-171-146-65-134-189-143-49252-49194-46-49319-49202-                              |
| 2018-01-12T08:09:12.072+0000 | .26.237 | 17c9534bfc2a8edeb78  | 64-49194-75-175-76-187-49293-49296-48-39-181-38-134-49315-159-9-92-170-81-49227-126-55-137-52245-128                             |
| 2018-01-12T08:09:12.072+0000 | .26.237 | cff64173dc5b1e96141c | 49269-183-49316-49202-44-49248-49236-49163-82-49159-49229-144-49257-49185-11-54-12-186-157-67-49290                              |
| 2018-01-12T08:09:12.072+0000 | .26.237 | 5f68c6edaa625acbb8b  | 49269-183-49316-49202-44-49248-49236-49163-82-49159-49229-144-49257-49185-11-54-12-186-157-67-49290                              |
| 2018-01-12T08:09:12.072+0000 | .26.237 | 63fa392b1105a8c4318  | 55-191-49209-33-170-48-49203-176-49321-49169-190-49314-49182-153-49220-18-195-187-92-137-96-39-4930                              |
| 2018-01-12T08:09:12.072+0000 | .26.237 | 5933eab69b3db48087   | 189-49205-126-167-49306-49320-49160-37-90-22-49188-134-49223-115-175-49168-63-184-88-49156-49221-49                              |
| 2018-01-12T08:09:12.072+0000 | .26.237 | c6343c3579d2e0ea07   | 180-49306-84-49181-49254-49313-49320-49289-89-49261-184-49284-107-49269-49302-22-103-49249-49305-49                              |
| 2018-01-12T08:09:12.072+0000 | .26.237 | dd6a913257a568cff93  | 137-96-49259-170-163-116-49199-54-49248-49200-49230-172-48-64-49269-75-145-193-70-49163-49290-53-49                              |
| 2018-01-12T08:09:12.072+0000 | .26.237 | 9a1b3fc416b0b64e228  | 65279-24-49186-57-161-49218-49162-34-165-140-49-51-49295-49233-56-150-179-98-65278-49208-49179-4915                              |
| 2018-01-12T08:09:12.073+0000 | .26.237 | 1482d0297ccdfdd83c   | 49178-49216-49208-49279-49164-43-49265-92-49266-51-138-52245-19-49270-49307-154-160-49195-121-4919                               |
| 2018-01-12T08:09:12.118+0000 | .26.237 | 681843facb648b3494c  | 63-30-65278-49153-147-40-49196-49171-61-29-196-79-49242-16-38-49227-49160-57-49315-52-99-49299-1-493                             |

# Fingerprint Modification /evasion - III

| _time                        | srcip   | ja3                  | ja3_ciphers  |
|------------------------------|---------|----------------------|--|
| 2018-01-12T08:09:11.794+0000 | .26.237 | 27a33d6c1e581cf2783  | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10<br>458944-327808-196736-65664-524416-393280-262272-131200 |
| 2018-01-12T08:09:11.842+0000 | .26.237 | e76a0619f4cf744ab2b  | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10   |
| 2018-01-12T08:09:11.842+0000 | .26.237 | 6b2355cd870327854d   | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10   |
| 2018-01-12T08:09:11.842+0000 | .26.237 | 8d9e064b97093a2c47   | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10   |
| 2018-01-12T08:09:11.842+0000 | .26.237 | 27a33d6c1e581cf2783  | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10   |
| 2018-01-12T08:09:11.886+0000 | .26.237 | a22efd10e07be383b4c  | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10   |
| 2018-01-12T08:09:11.934+0000 | .26.237 | 99f66d824338b066f1b  | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10   |
| 2018-01-12T08:09:11.978+0000 | .26.237 | 27a33d6c1e581cf2783  | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10   |
| 2018-01-12T08:09:12.026+0000 | .26.237 | d5ad1a88d4c511586af  | 0-22016  |
| 2018-01-12T08:09:12.072+0000 | .26.237 | a7674bf7508673e9d0e  | 148-49283-28-157-49236-49308-12-171-177-5-40-49215-49239-156-49207-69-36-11-54-82-183-27-90-49237-32                             |
| 2018-01-12T08:09:12.072+0000 | .26.237 | 0443db5df8b9dcc91ae  | 49176-49214-177-49234-62-67-82-59-49179-50-49158-171-146-65-134-189-143-49252-49194-46-49319-49202-                              |
| 2018-01-12T08:09:12.072+0000 | .26.237 | 17c9534bfc2a8edeb78  | 64-49194-75-175-76-187-49293-49296-48-39-181-38-134-49315-159-9-92-170-81-49227-126-55-137-52245-128                             |
| 2018-01-12T08:09:12.072+0000 | .26.237 | cff64173dc5b1e96141c | 49269-183-49316-49202-44-49248-49236-49163-82-49159-49229-144-49257-49185-11-54-12-186-157-67-49290                              |
| 2018-01-12T08:09:12.072+0000 | .26.237 | 5f68c6edaa625acbb8b  | 55-191-49209-33-170-48-49203-176-49321-49169-190-49314-49182-153-49220-18-195-187-92-137-96-39-4930                              |
| 2018-01-12T08:09:12.072+0000 | .26.237 | 63fa392b1105a8c4318  | 189-49205-126-167-49306-49320-49160-37-90-22-49188-134-49223-115-175-49168-63-184-88-49156-49221-49                              |
| 2018-01-12T08:09:12.072+0000 | .26.237 | 5933eab69b3db48087   | 180-49306-84-49181-49254-49313-49320-49289-89-49261-184-49284-107-49269-49302-22-103-49249-49305-49                              |
| 2018-01-12T08:09:12.072+0000 | .26.237 | c6343c3579d2e0ea07   | 137-96-49259-170-163-116-49199-54-49248-49200-49230-172-48-64-49269-75-145-193-70-49163-49290-53-49                              |
| 2018-01-12T08:09:12.072+0000 | .26.237 | dd6a913257a568cff93  | 65279-24-49186-57-161-49218-49162-34-165-140-49-51-49295-49233-56-150-179-98-65278-49208-49179-4915                              |
| 2018-01-12T08:09:12.073+0000 | .26.237 | 9a1b3fc416b0b64e228  | 49178-49216-49208-49279-49164-43-49265-92-49266-51-138-52245-19-49270-49307-154-160-49195-121-4919                               |
| 2018-01-12T08:09:12.118+0000 | .26.237 | 1482d0297ccdfdd83c   | 63-30-65278-49153-147-40-49196-49171-61-29-196-79-49242-16-38-49227-49160-57-49315-52-99-49299-1-49                              |
|                              |         | 681843facb648b3494c  | 49173-49317-174-49272-49190-47-42-141-49161-168-108-71-17-49240-75-175-76-187-49293-49296-64-49194-                              |

# Fingerprint Modification /evasion - III

| _time                        | srcip   | ja3                  | ja3_ciphers  |
|------------------------------|---------|----------------------|--|
| 2018-01-12T08:09:11.794+0000 | .26.237 | 27a33d6c1e581cf2783  | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10<br>458944-327808-196736-65664-524416-393280-262272-131200 |
| 2018-01-12T08:09:11.842+0000 | .26.237 | e76a0619f4cf744ab2b  | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10   |
| 2018-01-12T08:09:11.842+0000 | .26.237 | 6b2355cd870327854d   | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10   |
| 2018-01-12T08:09:11.842+0000 | .26.237 | 8d9e064b97093a2c47   | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10   |
| 2018-01-12T08:09:11.842+0000 | .26.237 | 27a33d6c1e581cf2783  | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10   |
| 2018-01-12T08:09:11.886+0000 | .26.237 | a22efd10e07be383b4c  | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10   |
| 2018-01-12T08:09:11.934+0000 | .26.237 | 99f66d824338b066f1b  | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10   |
| 2018-01-12T08:09:11.978+0000 | .26.237 | 27a33d6c1e581cf2783  | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10   |
| 2018-01-12T08:09:12.026+0000 | .26.237 | d5ad1a88d4c511586af  | 0-22016  |
| 2018-01-12T08:09:12.072+0000 | .26.237 | a7674bf7508673e9d0e  | 148-49283-28-157-49236-49308-12-171-177-5-40-49215-49239-156-49207-69-36-11-54-82-183-27-90-49237-32                             |
| 2018-01-12T08:09:12.072+0000 | .26.237 | 0443db5df8b9dcc91ae  | 49176-49214-177-49234-62-67-82-59-49179-50-49158-171-146-65-134-189-143-49252-49194-46-49319-49202-                              |
| 2018-01-12T08:09:12.072+0000 | .26.237 | 17c9534bfc2a8edeb78  | 64-49194-75-175-76-187-49293-49296-48-39-181-38-134-49315-159-9-92-170-81-49227-126-55-137-52245-128                             |
| 2018-01-12T08:09:12.072+0000 | .26.237 | cff64173dc5b1e96141c | 49269-183-49316-49202-44-49248-49236-49163-82-49159-49229-144-49257-49185-11-54-12-186-157-67-49290                              |
| 2018-01-12T08:09:12.072+0000 | .26.237 | 5f68c6edaa625acbb8b  | 55-191-49209-33-170-48-49203-176-49321-49169-190-49314-49182-153-49220-18-195-187-92-137-96-39-4930                              |
| 2018-01-12T08:09:12.072+0000 | .26.237 | 63fa392b1105a8c4318  | 189-49205-126-167-49306-49320-49160-37-90-22-49188-134-49223-115-175-49168-63-184-88-49156-49221-49                              |
| 2018-01-12T08:09:12.072+0000 | .26.237 | 5933eab69b3db48087   | 180-49306-84-49181-49254-49313-49320-49289-89-49261-184-49284-107-49269-49302-22-103-49249-49305-49                              |
| 2018-01-12T08:09:12.072+0000 | .26.237 | c6343c3579d2e0ea07   | 137-96-49259-170-163-116-49199-54-49248-49200-49230-172-48-64-49269-75-145-193-70-49163-49290-53-49                              |
| 2018-01-12T08:09:12.072+0000 | .26.237 | dd6a913257a568cff93  | 65279-24-49186-57-161-49218-49162-34-165-140-49-51-49295-49233-56-150-179-98-65278-49208-49179-4915                              |
| 2018-01-12T08:09:12.073+0000 | .26.237 | 9a1b3fc416b0b64e228  | 49178-49216-49208-49279-49164-43-49265-92-49266-51-138-52245-19-49270-49307-154-160-49195-121-4919                               |
| 2018-01-12T08:09:12.118+0000 | .26.237 | 1482d0297ccdfddd83c  | 63-30-65278-49153-147-40-49196-49171-61-29-196-79-49242-16-38-49227-49160-57-49315-52-99-49299-1-49                              |
|                              |         | 681843facb648b3494c  | 49173-49317-174-49272-49190-47-42-141-49161-168-108-71-17-49240-75-175-76-187-49293-49296-64-49194-                              |

# Fingerprint Modification /evasion - III

| _time                        | srcip   | ja3                  | ja3_ciphers  |
|------------------------------|---------|----------------------|--|
| 2018-01-12T08:09:11.794+0000 | .26.237 | 27a33d6c1e581cf2783  | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10<br>458944-327808-196736-65664-524416-393280-262272-131200 |
| 2018-01-12T08:09:11.842+0000 | .26.237 | e76a0619f4cf744ab2b  | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10   |
| 2018-01-12T08:09:11.842+0000 | .26.237 | 6b2355cd870327854d   | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10   |
| 2018-01-12T08:09:11.842+0000 | .26.237 | 8d9e064b97093a2c47   | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10   |
| 2018-01-12T08:09:11.842+0000 | .26.237 | 27a33d6c1e581cf2783  | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10   |
| 2018-01-12T08:09:11.886+0000 | .26.237 | a22efd10e07be383b4c  | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10   |
| 2018-01-12T08:09:11.934+0000 | .26.237 | 99f66d824338b066f1b  | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10   |
| 2018-01-12T08:09:11.978+0000 | .26.237 | 27a33d6c1e581cf2783  | 49199-49195-49200-49196-49171-49161-49172-49162-156-157-47-53-49170-10   |
| 2018-01-12T08:09:12.026+0000 | .26.237 | d5ad1a88d4c511586af  | 0-22016  |
| 2018-01-12T08:09:12.072+0000 | .26.237 | a7674bf7508673e9d0e  | 148-49283-28-157-49236-49308-12-171-177-5-40-49215-49239-156-49207-69-36-11-54-82-183-27-90-49237-32                             |
| 2018-01-12T08:09:12.072+0000 | .26.237 | 0443db5df8b9dcc91ae  | 49176-49214-177-49234-62-67-82-59-49179-50-49158-171-146-65-134-189-143-49252-49194-46-49319-49202-                              |
| 2018-01-12T08:09:12.072+0000 | .26.237 | 17c9534bfc2a8edeb78  | 64-49194-75-175-76-187-49293-49296-48-39-181-38-134-49315-159-9-92-170-81-49227-126-55-137-52245-128                             |
| 2018-01-12T08:09:12.072+0000 | .26.237 | cff64173dc5b1e96141c | 49269-183-49316-49202-44-49248-49236-49163-82-49159-49229-144-49257-49185-11-54-12-186-157-67-4929                               |
| 2018-01-12T08:09:12.072+0000 | .26.237 | 5f68c6edaa625acbb8b  | 55-191-49209-33-170-48-49203-176-49321-49169-190-49314-49182-153-49220-18-195-187-92-137-96-39-4930                              |
| 2018-01-12T08:09:12.072+0000 | .26.237 | 63fa392b1105a8c4318  | 189-49205-126-167-49306-49320-49160-37-90-22-49188-134-49223-115-175-49168-63-184-88-49156-49221-49                              |
| 2018-01-12T08:09:12.072+0000 | .26.237 | 5933eab69b3db48087   | 180-49306-84-49181-49254-49313-49320-49289-89-49261-184-49284-107-49269-49302-22-103-49249-49305-4                               |
| 2018-01-12T08:09:12.072+0000 | .26.237 | c6343c3579d2e0da07   | 137-96-49259-170-163-116-49199-54-49248-49200-49230-172-48-64-49269-75-145-193-70-49163-49290-53-49                              |
| 2018-01-12T08:09:12.072+0000 | .26.237 | dd6a913257a568cff93  | 65279-24-49186-57-161-49218-49162-34-165-140-49-51-49295-49233-56-150-179-98-65278-49208-49179-4919                              |
| 2018-01-12T08:09:12.073+0000 | .26.237 | 9a1b3fc416b0b64e228  | 49178-49216-49208-49279-49164-43-49265-92-49266-51-138-52245-19-49270-49307-154-160-49195-121-4919                               |
| 2018-01-12T08:09:12.118+0000 | .26.237 | 1482d0297ccdfdd83c   | 63-30-65278-49153-147-40-49196-49171-61-29-196-79-49242-16-38-49227-49160-57-49315-52-99-49299-1-49                              |
|                              |         |                      | 49173-49317-174-49272-49190-47-42-141-49161-168-108-71-17-49240-75-175-76-187-49293-49296-64-49194-                              |

# Fingerprint Modification /evasion - III

(~26 days later)

| _time                        | srcip   | ja3                 | ja3_ciphers   |
|------------------------------|---------|---------------------|---|
| 2018-01-15T12:19:20.688+0000 | .26.232 | 23558e64d3f12b140t  | 5-4-2-1-22-51-57-58-24-53-10-27-47-52-49168-49158-49173-49163-49153-59-49200-49196-49192-49188-49172- |
| 2018-01-15T12:19:22.898+0000 | .26.232 | 23558e64d3f12b140t  | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10                    |
| 2018-02-09T09:13:30.102+0000 | .26.235 | 6231f3e090902b283t  | 458944-327808-196736-65664-524416-393280-262272-131200  |
| 2018-02-09T09:13:30.146+0000 | .26.235 | e76a0619f4cf744ab2  | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10                    |
| 2018-02-09T09:13:30.146+0000 | .26.235 | b8aee29e75d6428de   | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10                    |
| 2018-02-09T09:13:30.146+0000 | .26.235 | 02c79708912f09605t  | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10                    |
| 2018-02-09T09:13:30.146+0000 | .26.235 | 6231f3e090902b283t  | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10                    |
| 2018-02-09T09:13:30.186+0000 | .26.235 | 225febcb6a5c122e4c2 | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10                    |
| 2018-02-09T09:13:30.230+0000 | .26.235 | d4cfea6a0a57b3f8ed  | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10                    |
| 2018-02-09T09:13:30.274+0000 | .26.235 | 6231f3e090902b283t  | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10                    |
| 2018-02-09T09:13:30.318+0000 | .26.235 | 33d99dd27735072ba   | 0-22016   |
| 2018-02-09T09:13:30.357+0000 | .26.235 | 744d459ee33c957b4   | 49227-49201-33-183-96-19-49232-80-49175-156-3-49273-179-49199-49264-49304-49215-149-65279-182-57-53-  |
| 2018-02-09T09:13:30.357+0000 | .26.235 | e2d87fde34d1ff1f434 | 40-80-49266-157-49213-49275-81-49200-62-7-49276-124-71-126-165-49183-49185-87-24-49261-147-25-49267-  |
| 2018-02-09T09:13:30.357+0000 | .26.235 | df5779b4f188abc958  | 79-171-16-92-49277-49168-11-187-49179-99-52243-49292-49290-49192-59-143-37-160-49284-86-24-49181-132  |
| 2018-02-09T09:13:30.357+0000 | .26.235 | a2083923440174e78   | 72-49160-170-11-49229-197-129-49158-65278-49322-49296-46-49292-49304-114-43-49263-96-125-91-9-49166-  |
| 2018-02-09T09:13:30.357+0000 | .26.235 | aa70fd98d19f6dda13  | 49310-49251-17-171-49234-49161-71-170-107-49231-49261-49270-49216-74-49269-173-49287-87-49188-49226   |
| 2018-02-09T09:13:30.357+0000 | .26.235 | b162bbf7959a7623a0  | 49247-78-49193-52-49256-139-49164-55-135-81-49301-49205-133-49154-190-49244-49294-49170-49278-56-88   |
| 2018-02-09T09:13:30.357+0000 | .26.235 | 9c5b4f9c58e53b744t  | 49172-10-83-14-15-158-154-49178-84-49322-49257-49261-49234-144-77-49213-49250-49291-49208-49270-180   |
| 2018-02-09T09:13:30.358+0000 | .26.235 | 0fadcc51d6aeda5042t | 49286-21-184-96-44-49249-49214-49274-49189-42-49306-102-49303-39-66-49263-13-49215-194-49271-49164-   |
| 2018-02-09T09:13:30.358+0000 | .26.235 | 0c8df396426c3d053t  | 49174-49226-49268-78-162-140-22-49225-79-49250-161-38-49206-49214-66-49257-6-4-17-88-49251-180-49155  |
| 2018-02-09T09:13:30.358+0000 | .26.235 | 542085678730261d9   | 168-49200-26-106-49323-49176-49212-49307-100-120-49182-49301-49240-49289-49201-78-49218-148-49302-    |

# Fingerprint Modification /evasion - III

(~26 days later)

| _time                        | srcip   | ja3                 | ja3_ciphers   |
|------------------------------|---------|---------------------|---|
| 2018-01-15T12:19:20.688+0000 | .26.232 | 23558e64d3f12b140t  | 5-4-2-1-22-51-57-58-24-53-10-27-47-52-49168-49158-49173-49163-49153-59-49200-49196-49192-49188-49172- |
| 2018-01-15T12:19:22.898+0000 | .26.232 | 23558e64d3f12b140t  | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10                    |
| 2018-02-09T09:13:30.102+0000 | .26.235 | 6231f3e090902b283t  | 458944-327808-196736-65664-524416-393280-262272-131200  |
| 2018-02-09T09:13:30.146+0000 | .26.235 | e76a0619f4cf744ab2  | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10                    |
| 2018-02-09T09:13:30.146+0000 | .26.235 | b8aee29e75d6428de   | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10                    |
| 2018-02-09T09:13:30.146+0000 | .26.235 | 02c79708912f09605t  | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10                    |
| 2018-02-09T09:13:30.146+0000 | .26.235 | 6231f3e090902b283t  | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10                    |
| 2018-02-09T09:13:30.186+0000 | .26.235 | 225febcb6a5c122e4c2 | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10                    |
| 2018-02-09T09:13:30.230+0000 | .26.235 | d4cfea6a0a57b3f8ed  | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10                    |
| 2018-02-09T09:13:30.274+0000 | .26.235 | 6231f3e090902b283t  | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10                    |
| 2018-02-09T09:13:30.318+0000 | .26.235 | 33d99dd27735072ba   | 0-22016   |
| 2018-02-09T09:13:30.357+0000 | .26.235 | 744d459ee33c957b4   | 49227-49201-33-183-96-19-49232-80-49175-156-3-49273-179-49199-49264-49304-49215-149-65279-182-57-53-  |
| 2018-02-09T09:13:30.357+0000 | .26.235 | e2d87fde34d1ff1f434 | 40-80-49266-157-49213-49275-81-49200-62-7-49276-124-71-126-165-49183-49185-87-24-49261-147-25-49267-  |
| 2018-02-09T09:13:30.357+0000 | .26.235 | df5779b4f188abc958  | 79-171-16-92-49277-49168-11-187-49179-99-52243-49292-49290-49192-59-143-37-160-49284-86-24-49181-132  |
| 2018-02-09T09:13:30.357+0000 | .26.235 | a2083923440174e78   | 72-49160-170-11-49229-197-129-49158-65278-49322-49296-46-49292-49304-114-43-49263-96-125-91-9-49166-  |
| 2018-02-09T09:13:30.357+0000 | .26.235 | aa70fd98d19f6dda13  | 49310-49251-17-171-49234-49161-71-170-107-49231-49261-49270-49216-74-49269-173-49287-87-49188-49226   |
| 2018-02-09T09:13:30.357+0000 | .26.235 | b162bbf7959a7623a0  | 49247-78-49193-52-49256-139-49164-55-135-81-49301-49205-133-49154-190-49244-49294-49170-49278-56-88   |
| 2018-02-09T09:13:30.357+0000 | .26.235 | 9c5b4f9c58e53b744t  | 49172-10-83-14-15-158-154-49178-84-49322-49257-49261-49234-144-77-49213-49250-49291-49208-49270-180   |
| 2018-02-09T09:13:30.358+0000 | .26.235 | 0fadcc51d6aeda5042t | 49286-21-184-96-44-49249-49214-49274-49189-42-49306-102-49303-39-66-49263-13-49215-194-49271-49164-   |
| 2018-02-09T09:13:30.358+0000 | .26.235 | 0c8df396426c3d053t  | 49174-49226-49268-78-162-140-22-49225-79-49250-161-38-49206-49214-66-49257-6-4-17-88-49251-180-49155  |
| 2018-02-09T09:13:30.358+0000 | .26.235 | 542085678730261d9   | 168-49200-26-106-49323-49176-49212-49307-100-120-49182-49301-49240-49289-49201-78-49218-148-49302-    |

# Fingerprint Modification /evasion - III

(~26 days later)

| _time                        | srcip   | ja3                 | ja3_ciphers   |
|------------------------------|---------|---------------------|---|
| 2018-01-15T12:19:20.688+0000 | .26.232 | 23558e64d3f12b140t  | 5-4-2-1-22-51-57-58-24-53-10-27-47-52-49168-49158-49173-49163-49153-59-49200-49196-49192-49188-49172- |
| 2018-01-15T12:19:22.898+0000 | .26.232 | 23558e64d3f12b140t  | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10                    |
| 2018-02-09T09:13:30.102+0000 | .26.235 | 6231f3e090902b283t  | 458944-327808-196736-65664-524416-393280-262272-131200  |
| 2018-02-09T09:13:30.146+0000 | .26.235 | e76a0619f4cf744ab2  | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10                    |
| 2018-02-09T09:13:30.146+0000 | .26.235 | b8aee29e75d6428de   | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10                    |
| 2018-02-09T09:13:30.146+0000 | .26.235 | 02c79708912f09605t  | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10                    |
| 2018-02-09T09:13:30.146+0000 | .26.235 | 6231f3e090902b283t  | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10                    |
| 2018-02-09T09:13:30.186+0000 | .26.235 | 225febcb6a5c122e4c2 | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10                    |
| 2018-02-09T09:13:30.230+0000 | .26.235 | d4cfea6a0a57b3f8ed  | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10                    |
| 2018-02-09T09:13:30.274+0000 | .26.235 | 6231f3e090902b283t  | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10                    |
| 2018-02-09T09:13:30.318+0000 | .26.235 | 33d99dd27735072ba   | 0-22016   |
| 2018-02-09T09:13:30.357+0000 | .26.235 | 744d459ee33c957b4   | 49227-49201-33-183-96-19-49232-80-49175-156-3-49273-179-49199-49264-49304-49215-149-65279-182-57-53-  |
| 2018-02-09T09:13:30.357+0000 | .26.235 | e2d87fde34d1ff1f434 | 40-80-49266-157-49213-49275-81-49200-62-7-49276-124-71-126-165-49183-49185-87-24-49261-147-25-49267-  |
| 2018-02-09T09:13:30.357+0000 | .26.235 | df5779b4f188abc958  | 79-171-16-92-49277-49168-11-187-49179-99-52243-49292-49290-49192-59-143-37-160-49284-86-24-49181-132  |
| 2018-02-09T09:13:30.357+0000 | .26.235 | a2083923440174e78   | 72-49160-170-11-49229-197-129-49158-65278-49322-49296-46-49292-49304-114-43-49263-96-125-91-9-49166-  |
| 2018-02-09T09:13:30.357+0000 | .26.235 | aa70fd98d19f6dda13  | 49310-49251-17-171-49234-49161-71-170-107-49231-49261-49270-49216-74-49269-173-49287-87-49188-49226   |
| 2018-02-09T09:13:30.357+0000 | .26.235 | b162bbf7959a7623a0  | 49247-78-49193-52-49256-139-49164-55-135-81-49301-49205-133-49154-190-49244-49294-49170-49278-56-88   |
| 2018-02-09T09:13:30.357+0000 | .26.235 | 9c5b4f9c58e53b744t  | 49172-10-83-14-15-158-154-49178-84-49322-49257-49261-49234-144-77-49213-49250-49291-49208-49270-180   |
| 2018-02-09T09:13:30.358+0000 | .26.235 | 0fadcc51d6aeda5042t | 49286-21-184-96-44-49249-49214-49274-49189-42-49306-102-49303-39-66-49263-13-49215-194-49271-49164-   |
| 2018-02-09T09:13:30.358+0000 | .26.235 | 0c8df396426c3d053t  | 49174-49226-49268-78-162-140-22-49225-79-49250-161-38-49206-49214-66-49257-6-4-17-88-49251-180-49155  |
| 2018-02-09T09:13:30.358+0000 | .26.235 | 542085678730261d9   | 168-49200-26-106-49323-49176-49212-49307-100-120-49182-49301-49240-49289-49201-78-49218-148-49302-    |

# Fingerprint Modification /evasion - III

(~26 days later)

| _time                        | srcip   | ja3                  |
|------------------------------|---------|----------------------|
| 2018-01-15T12:19:20.688+0000 | .26.232 | 23558e64d3f12b140t   |
| 2018-01-15T12:19:22.898+0000 | .26.232 | 23558e64d3f12b140t   |
| 2018-02-09T09:13:30.102+0000 | .26.235 | 6231f3e090902b283t   |
| 2018-02-09T09:13:30.146+0000 | .26.235 | e76a0619f4cf744ab2t  |
| 2018-02-09T09:13:30.146+0000 | .26.235 | b8aee29e75d6428de    |
| 2018-02-09T09:13:30.146+0000 | .26.235 | 02c79708912f09605t   |
| 2018-02-09T09:13:30.146+0000 | .26.235 | 6231f3e090902b283t   |
| 2018-02-09T09:13:30.186+0000 | .26.235 | 225febcb6a5c122e4c2t |
| 2018-02-09T09:13:30.230+0000 | .26.235 | d4cfea6a0a57b3f8edt  |
| 2018-02-09T09:13:30.274+0000 | .26.235 | 6231f3e090902b283t   |
| 2018-02-09T09:13:30.318+0000 | .26.235 | 33d99dd27735072ba    |
| 2018-02-09T09:13:30.357+0000 | .26.235 | 744d459ee33c957b4    |
| 2018-02-09T09:13:30.357+0000 | .26.235 | e2d87fde34d1ff1f434  |
| 2018-02-09T09:13:30.357+0000 | .26.235 | df5779b4f188abc958   |
| 2018-02-09T09:13:30.357+0000 | .26.235 | a2083923440174e78    |
| 2018-02-09T09:13:30.357+0000 | .26.235 | aa70fd98d19f6dda13   |
| 2018-02-09T09:13:30.357+0000 | .26.235 | b162bbf7959a7623a0   |
| 2018-02-09T09:13:30.357+0000 | .26.235 | 9c5b4f9c58e53b744t   |
| 2018-02-09T09:13:30.358+0000 | .26.235 | 0fadcc51d6aeda5042t  |
| 2018-02-09T09:13:30.358+0000 | .26.235 | 0c8df396426c3d053t   |
| 2018-02-09T09:13:30.358+0000 | .26.235 | 542085678730261d9    |

# Fingerprint Modification /evasion - III

(~26 days later)

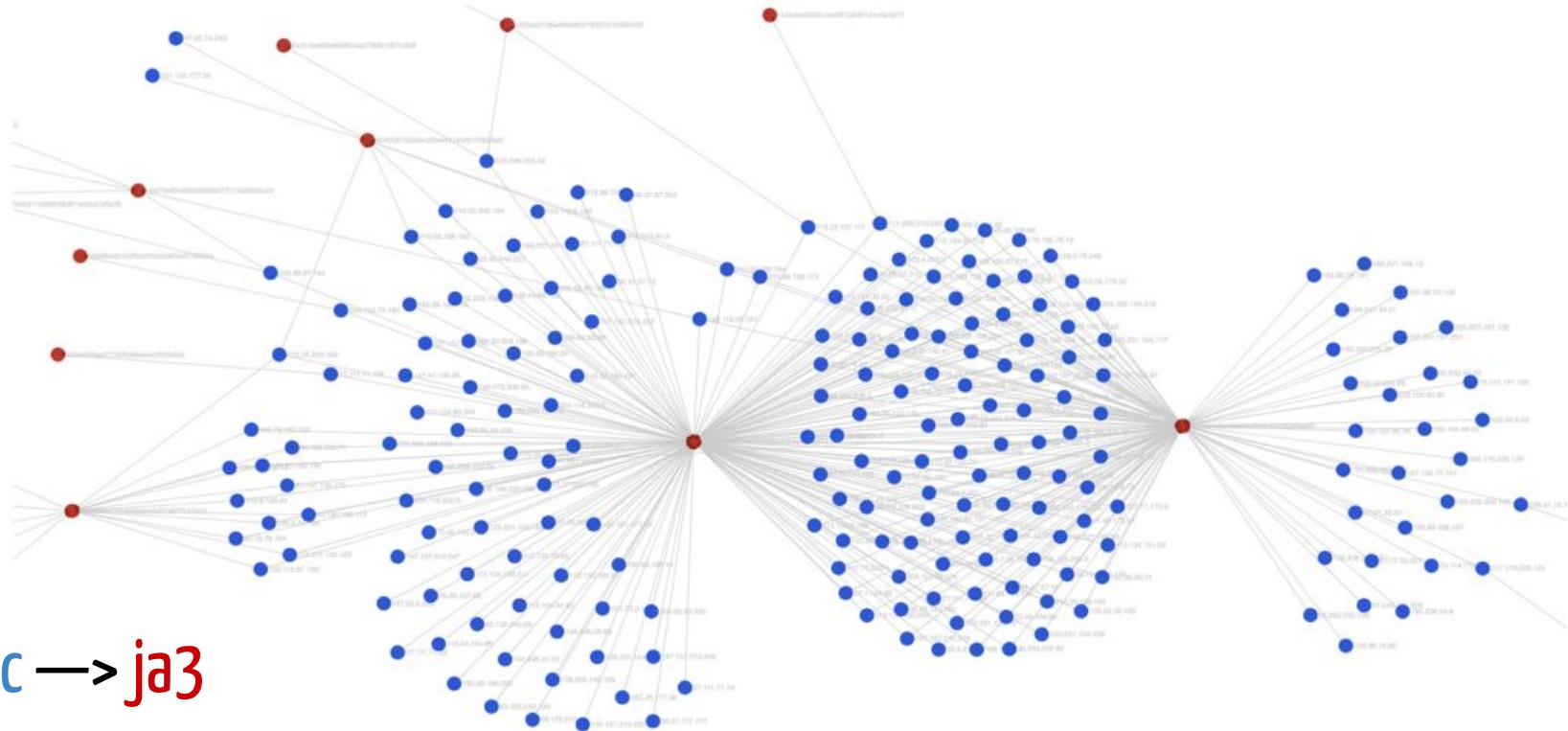
| _time                        | srcip   | ja3                  | ja3_ciphers  |
|------------------------------|---------|----------------------|--|
| 2018-01-15T12:19:20.688+0000 | .26.232 | 23558e64d3f12b140t   | 5-4-2-1-22-51-57-58-24-53-10-27-47-52-49168-49158-49173-49163-49153-59-49200-49196-49192-49188-49172-52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10  |
| 2018-01-15T12:19:22.898+0000 | .26.232 | 23558e64d3f12b140t   | 458944-327808-196736-65664-524416-393280-262272-131200   |
| 2018-02-09T09:13:30.102+0000 | .26.235 | 6231f3e090902b283t   | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10   |
| 2018-02-09T09:13:30.146+0000 | .26.235 | e76a0619f4cf744ab2t  | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10   |
| 2018-02-09T09:13:30.146+0000 | .26.235 | b8aee29e75d6428de    | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10   |
| 2018-02-09T09:13:30.146+0000 | .26.235 | 02c79708912f096059t  | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10   |
| 2018-02-09T09:13:30.146+0000 | .26.235 | 6231f3e090902b283t   | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10   |
| 2018-02-09T09:13:30.186+0000 | .26.235 | 225febcb6a5c122e4c2t | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10   |
| 2018-02-09T09:13:30.230+0000 | .26.235 | d4cfea6a0a57b3f8edt  | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10   |
| 2018-02-09T09:13:30.274+0000 | .26.235 | 6231f3e090902b283t   | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10   |
| 2018-02-09T09:13:30.318+0000 | .26.235 | 33d99dd27735072ba    | 0-22016  |
| 2018-02-09T09:13:30.357+0000 | .26.235 | 744d459ee33c957b4t   | 49227-49201-33-183-96-19-49232-80-49175-156-3-49273-179-49199-49264-49304-49215-149-65279-182-57-53-40-80-49266-157-49213-49275-81-49200-62-7-49276-124-71-126-165-49183-49185-87-24-49261-147-25-49267-79-171-16-92-49277-49168-11-187-49179-99-52243-49292-49290-49192-59-143-37-160-49284-86-24-49181-132-72-49160-170-11-49229-197-129-49158-65278-49322-49296-46-49292-49304-114-43-49263-96-125-91-9-49166-49310-49251-17-171-49234-49161-71-170-107-49231-49261-49270-49216-74-49269-173-49287-87-49188-49226-49247-78-49193-52-49256-139-49164-55-135-81-49301-49205-133-49154-190-49244-49294-49170-49278-56-88-49172-10-83-14-15-158-154-49178-84-49322-49257-49261-49234-144-77-49213-49250-49291-49208-49270-180-49286-21-184-96-44-49249-49214-49274-49189-42-49306-102-49303-39-66-49263-13-49215-194-49271-49164-49174-49226-49268-78-162-140-22-49225-79-49250-161-38-49206-49214-66-49257-6-4-17-88-49251-180-49155-168-49200-26-106-49323-49176-49212-49307-100-120-49182-49301-49240-49289-49201-78-49218-148-49302-1 |
| 2018-02-09T09:13:30.358+0000 | .26.235 | 0fadcc51d6aeda5042t  |  |
| 2018-02-09T09:13:30.358+0000 | .26.235 | 0c8df396426c3d0539t  |  |
| 2018-02-09T09:13:30.358+0000 | .26.235 | 542085678730261d9t   |  |

# Fingerprint Modification /evasion - III

(~26 days later)

| _time                        | srcip   | ja3                  | ja3_ciphers   |
|------------------------------|---------|----------------------|---|
| 2018-01-15T12:19:20.688+0000 | .26.232 | 23558e64d3f12b140t   | 5-4-2-1-22-51-57-58-24-53-10-27-47-52-49168-49158-49173-49163-49153-59-49200-49196-49192-49188-49172-52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10 |
| 2018-01-15T12:19:22.898+0000 | .26.232 | 23558e64d3f12b140t   | 458944-327808-196736-65664-524416-393280-262272-131200  |
| 2018-02-09T09:13:30.102+0000 | .26.235 | 6231f3e090902b283t   | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10  |
| 2018-02-09T09:13:30.146+0000 | .26.235 | e76a0619f4cf744ab2t  | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10  |
| 2018-02-09T09:13:30.146+0000 | .26.235 | b8aee29e75d6428de    | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10  |
| 2018-02-09T09:13:30.146+0000 | .26.235 | 02c79708912f096059t  | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10  |
| 2018-02-09T09:13:30.146+0000 | .26.235 | 6231f3e090902b283t   | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10  |
| 2018-02-09T09:13:30.186+0000 | .26.235 | 225febcb6a5c122e4c2t | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10  |
| 2018-02-09T09:13:30.230+0000 | .26.235 | d4cfea6a0a57b3f8edt  | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10  |
| 2018-02-09T09:13:30.274+0000 | .26.235 | 6231f3e090902b283t   | 52392-52393-49199-49200-49195-49196-49171-49161-49172-49162-156-157-47-53-49170-10  |
| 2018-02-09T09:13:30.318+0000 | .26.235 | 33d99dd27735072ba    | 0-22016   |
| 2018-02-09T09:13:30.357+0000 | .26.235 | 744d459ee33c957b4t   | 49227-49201-33-183-96-19-49232-80-49175-156-3-49273-179-49199-49264-49304-49215-149-65279-182-57-53   |
| 2018-02-09T09:13:30.357+0000 | .26.235 | e2d87fde34d1ff1f434t | 40-80-49266-157-49213-49275-81-49200-62-7-49276-124-71-126-165-49183-49185-87-24-49261-147-25-49267   |
| 2018-02-09T09:13:30.357+0000 | .26.235 | df5779b4f188abc958t  | 79-171-16-92-49277-49168-11-187-49179-99-52243-49292-49290-49192-59-143-37-160-49284-86-24-49181-132  |
| 2018-02-09T09:13:30.357+0000 | .26.235 | a2083923440174e78t   | 72-49160-170-11-49229-197-129-49158-65278-49322-49296-46-49292-49304-114-43-49263-96-125-91-9-49166   |
| 2018-02-09T09:13:30.357+0000 | .26.235 | aa70fd98d19f6dda13t  | 49310-49251-17-171-49234-49161-71-170-107-49231-49261-49270-49216-74-49269-173-49287-87-49188-49222   |
| 2018-02-09T09:13:30.357+0000 | .26.235 | b162bbf7959a7623at   | 49247-78-49193-52-49256-139-49164-55-135-81-49301-49205-133-49154-190-49244-49294-49170-49278-56-88   |
| 2018-02-09T09:13:30.358+0000 | .26.235 | 9c5b4f9c58e53b744t   | 49172-10-83-14-15-158-154-49178-84-49322-49257-49261-49234-144-77-49213-49250-49291-49208-49270-180   |
| 2018-02-09T09:13:30.358+0000 | .26.235 | 0fadcd51d6aeda5042t  | 49286-21-184-96-44-49249-49214-49274-49189-42-49306-102-49303-39-66-49263-13-49215-194-49271-49164  |
| 2018-02-09T09:13:30.358+0000 | .26.235 | 0c8df396426c3d0539t  | 49174-49226-49268-78-162-140-22-49225-79-49250-161-38-49206-49214-66-49257-6-4-17-88-49251-180-49156  |
| 2018-02-09T09:13:30.358+0000 | .26.235 | 542085678730261dt    | 168-49200-26-106-49323-49176-49212-49307-100-120-49182-49301-49240-49289-49201-78-49218-148-49302-1   |

# Profiling the tools and actors



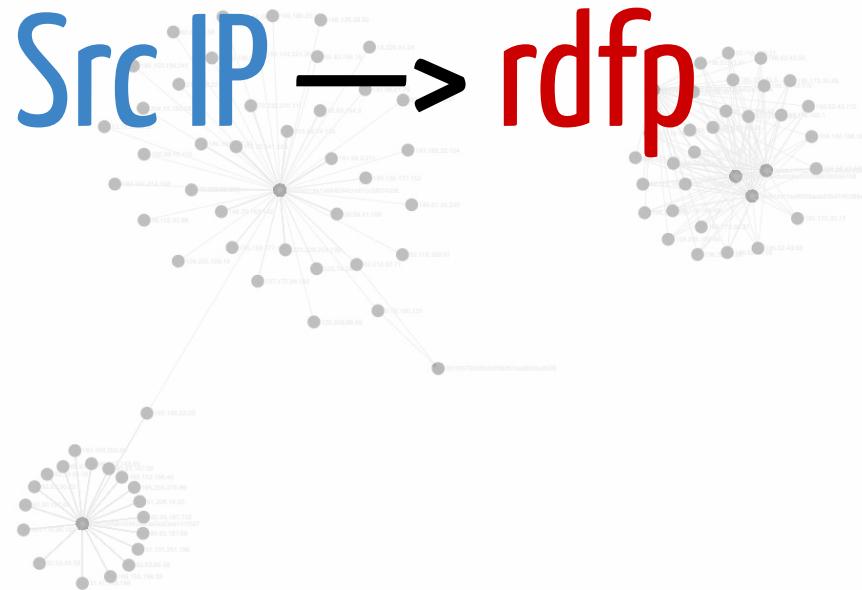
# Profiling the tools and actors

| _time                        | srcip    | dstport | ja3_hash                         | ja3_fields                  | server_name                    |
|------------------------------|----------|---------|----------------------------------|-----------------------------|--------------------------------|
| 2018-02-24T07:40:06.369+0000 | 1159.53  | 443     | eae050f0cb6163c28dd34324c1e28d74 | 771,255-49196-49195-49188-4 | <a href="#">www.bing.com</a>   |
| 2018-02-24T09:21:42.033+0000 | 1167.122 | 443     | 5001b4c2a48c94b76ca1f0199345fe60 | 771,52392-52393-49199-4920  | <a href="#">5njk.com</a>       |
| 2018-02-24T09:26:08.037+0000 | 1167.122 | 443     | 5001b4c2a48c94b76ca1f0199345fe60 | 771,52392-52393-49199-4920  | <a href="#">5njk.com</a>       |
| 2018-02-24T09:35:11.436+0000 | 1167.122 | 443     | 5001b4c2a48c94b76ca1f0199345fe60 | 771,52392-52393-49199-4920  | <a href="#">5njk.com</a>       |
| 2018-02-24T10:19:56.461+0000 | 23.69    | 443     | 5001b4c2a48c94b76ca1f0199345fe60 | 771,52392-52393-49199-4920  | <a href="#">ec22r.com</a>      |
| 2018-02-24T10:20:03.276+0000 | 23.69    | 443     | eae050f0cb6163c28dd34324c1e28d74 | 771,255-49196-49195-49188-4 | <a href="#">www.yandex.com</a> |
| 2018-02-24T10:20:04.117+0000 | 23.69    | 443     | eae050f0cb6163c28dd34324c1e28d74 | 771,255-49196-49195-49188-4 | <a href="#">www.google.com</a> |
| 2018-02-24T10:20:04.521+0000 | 23.69    | 443     | eae050f0cb6163c28dd34324c1e28d74 | 771,255-49196-49195-49188-4 | <a href="#">www.bing.com</a>   |
| 2018-02-24T10:26:20.373+0000 | 23.69    | 443     | 5001b4c2a48c94b76ca1f0199345fe60 | 771,52392-52393-49199-4920  | <a href="#">5njk.com</a>       |
| 2018-02-24T10:26:27.401+0000 | 23.69    | 443     | eae050f0cb6163c28dd34324c1e28d74 | 771,255-49196-49195-49188-4 | <a href="#">www.google.com</a> |
| 2018-02-24T10:26:27.409+0000 | 23.69    | 443     | eae050f0cb6163c28dd34324c1e28d74 | 771,255-49196-49195-49188-4 | <a href="#">www.yandex.com</a> |
| 2018-02-24T10:26:28.537+0000 | 23.69    | 443     | eae050f0cb6163c28dd34324c1e28d74 | 771,255-49196-49195-49188-4 | <a href="#">www.bing.com</a>   |
| 2018-02-24T11:53:40.309+0000 | 1167.122 | 443     | 5001b4c2a48c94b76ca1f0199345fe60 | 771,52392-52393-49199-4920  | <a href="#">mwg6aj.com</a>     |
| 2018-02-26T15:29:02.032+0000 | 248.215  | 443     | 38d1c1933f0062c7c9046659faf08872 | 771,49200-49196-49192-4918  | <a href="#">www.bing.com</a>   |
| 2018-02-26T16:34:40.229+0000 | 0.95.90  | 443     | 5001b4c2a48c94b76ca1f0199345fe60 | 771,52392-52393-49199-4920  | <a href="#">ec22r.com</a>      |
| 2018-02-26T17:07:14.321+0000 | 248.215  | 443     | 38d1c1933f0062c7c9046659faf08872 | 771,49200-49196-49192-4918  | <a href="#">5d4w7c3w.com</a>   |
| 2018-02-26T17:07:15.601+0000 | 248.215  | 443     | 38d1c1933f0062c7c9046659faf08872 | 771,49200-49196-49192-4918  | <a href="#">www.google.com</a> |
| 2018-02-26T17:07:15.940+0000 | 248.215  | 443     | 38d1c1933f0062c7c9046659faf08872 | 771,49200-49196-49192-4918  | <a href="#">www.yandex.com</a> |
| 2018-02-26T17:07:16.085+0000 | 248.215  | 443     | 38d1c1933f0062c7c9046659faf08872 | 771,49200-49196-49192-4918  | <a href="#">www.bing.com</a>   |
| 2018-02-26T17:38:10.496+0000 | 192.248  | 443     | 5001b4c2a48c94b76ca1f0199345fe60 | 771,52392-52393-49199-4920  | <a href="#">u8sj3.com</a>      |

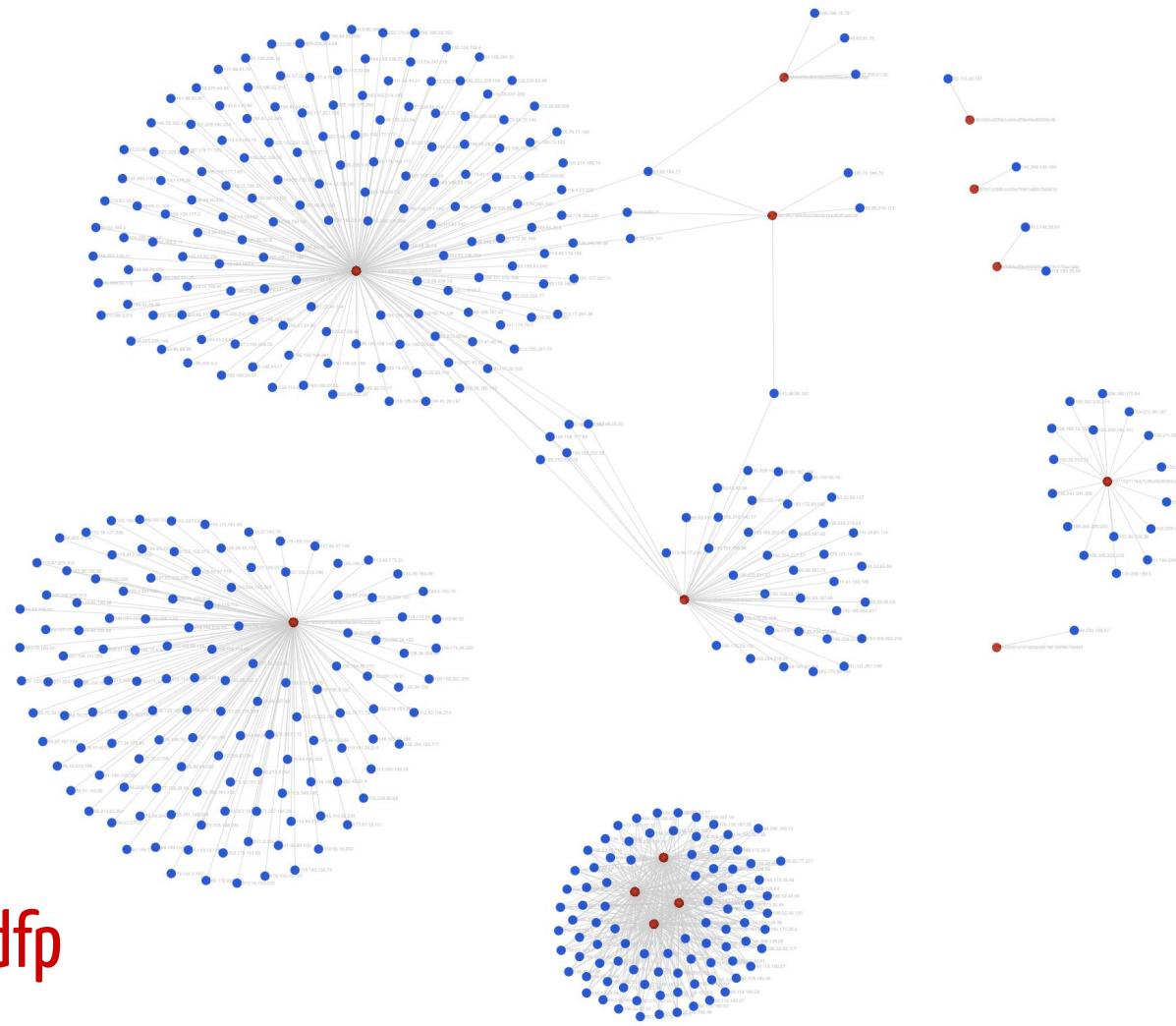
# Observations

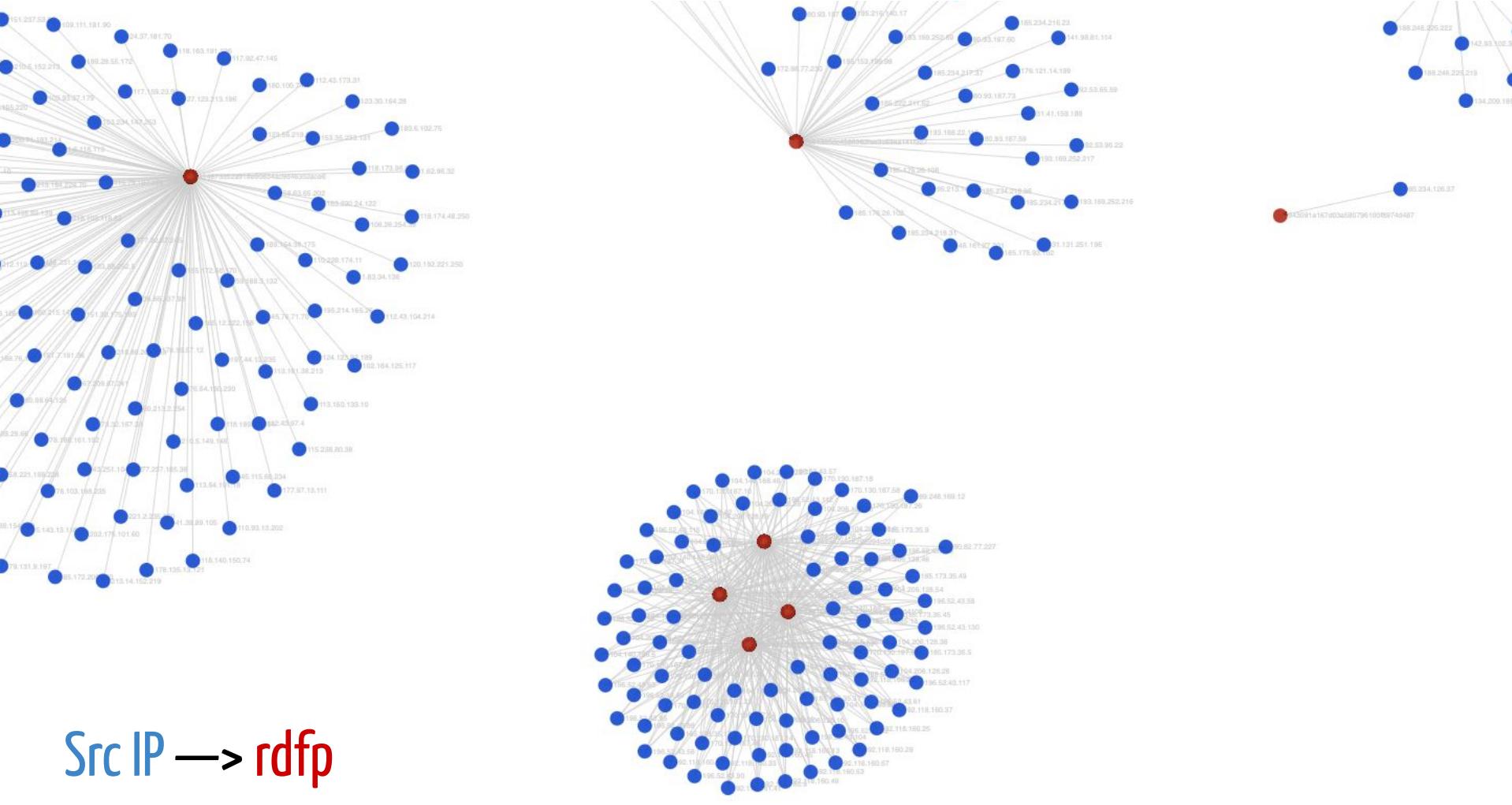
[RDP]

Src IP → rdfp

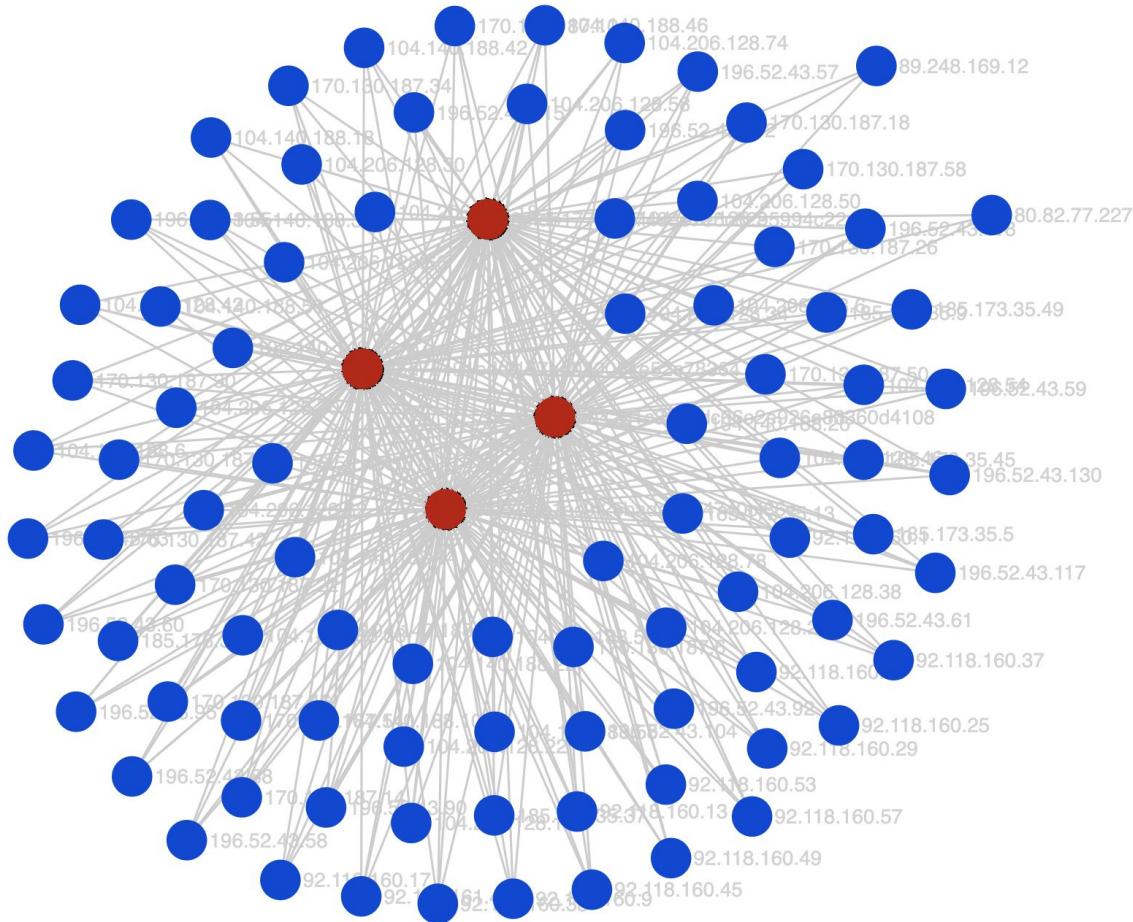


# Src IP → rdfp





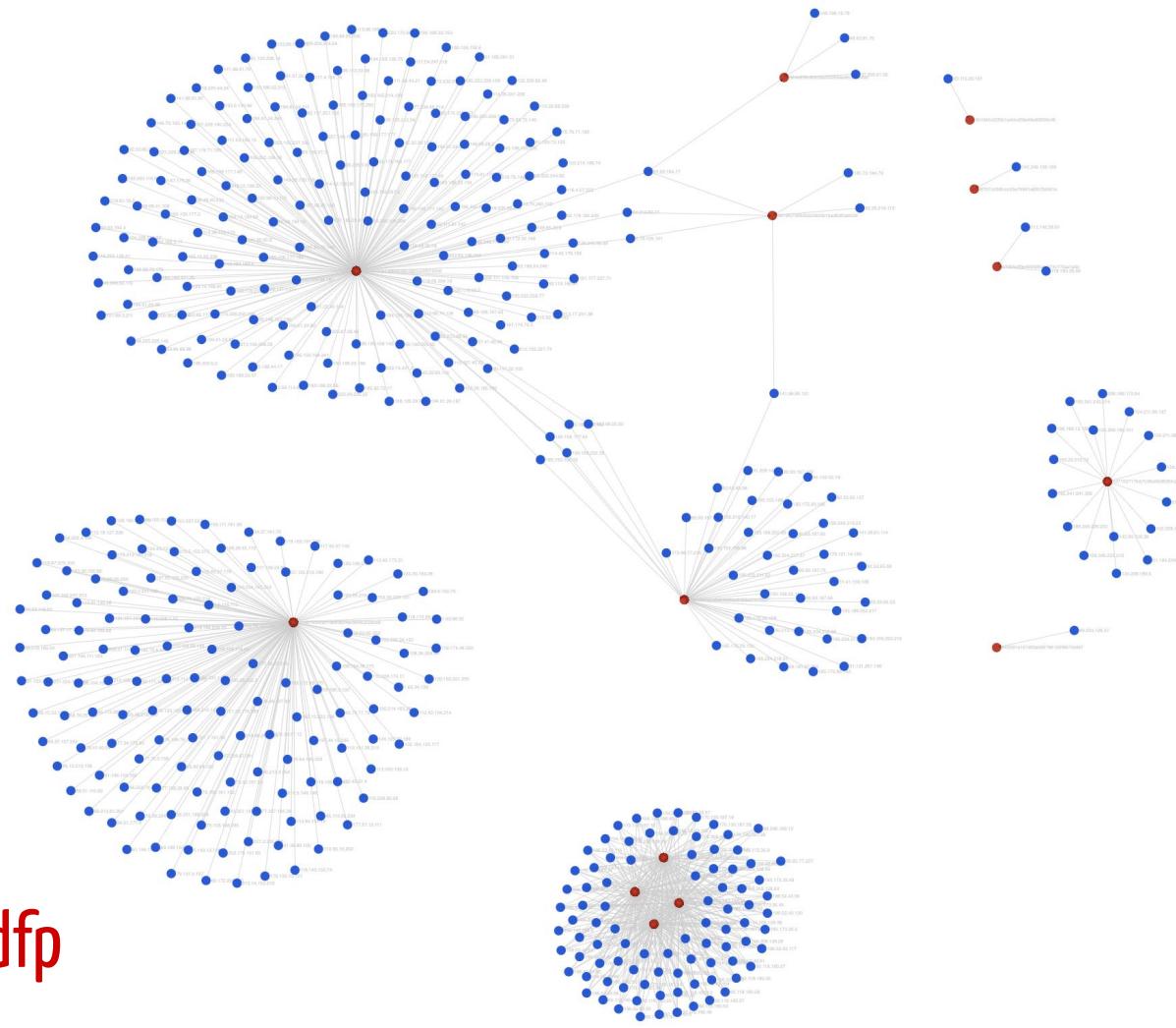
Src IP → rdfp



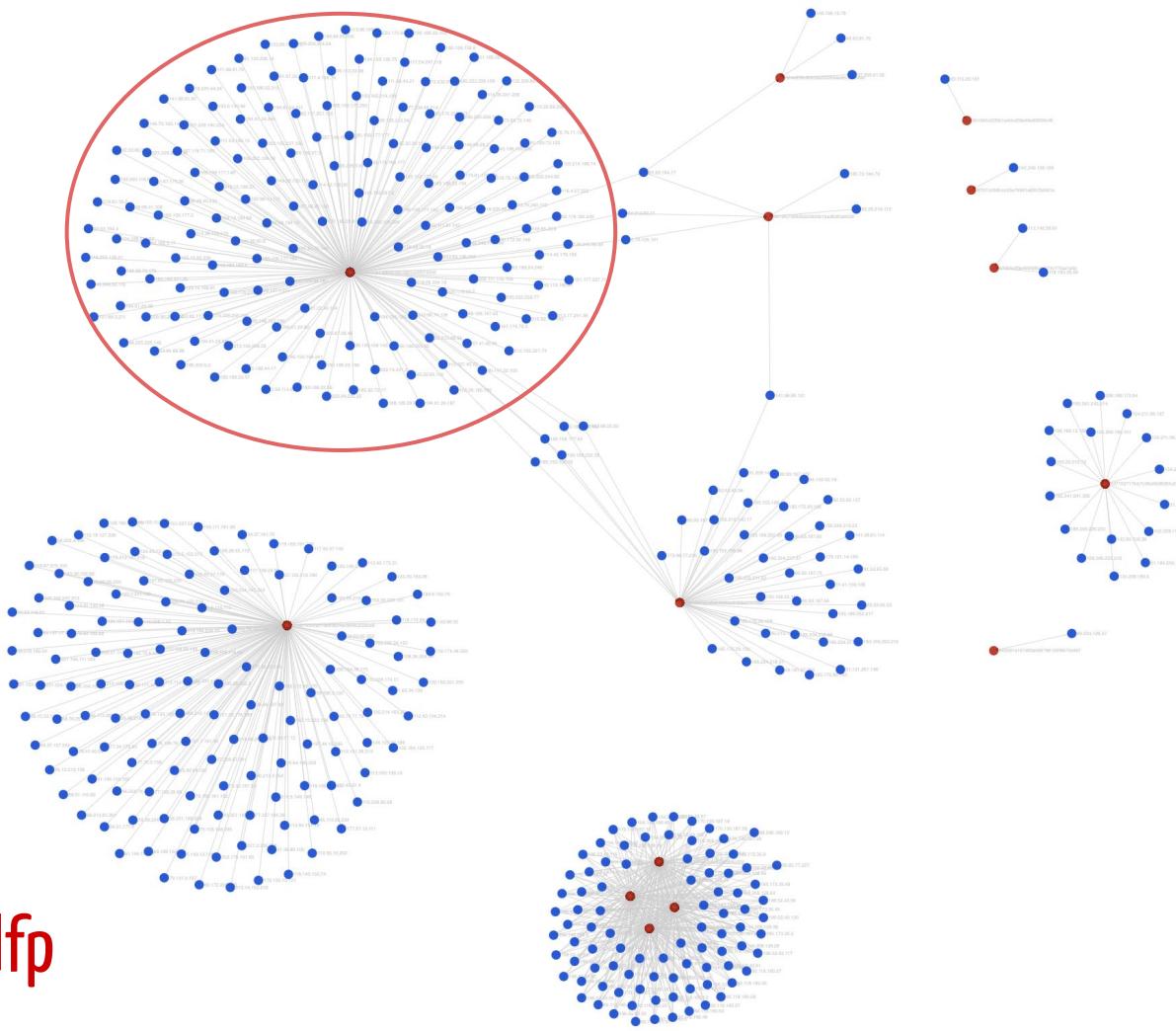
# Randomized RDP Cookie

| sourcelp | values(rdp.cookie)   | values(rdp.rdfp)   |
|----------|--|--|
| 80.82.7  | mstshash=nmap  | 0efdb177fd787489e7e6c8295994c22d<br>46d75491eddf157ad030051e52e78364<br>cb42d1c3edbdc06e2e926e83360d4108                                     |
| 89.248.  | mstshash=nmap  | 0efdb177fd787489e7e6c8295994c22d<br>46d75491eddf157ad030051e52e78364<br>cb42d1c3edbdc06e2e926e83360d4108                                     |
| 185.173  | mstshash=gHYfbjEMP<br>mstshash=gYrIgsrnZ<br>mstshash=mQWBWuurb<br>mstshash=qoXLLFizq | 0efdb177fd787489e7e6c8295994c22d<br>46d75491eddf157ad030051e52e78364<br>cb42d1c3edbdc06e2e926e83360d4108<br>fefd61bfc1ec9f25bada8354740cf86e |
| 170.130  | mstshash=fwAeNsuD<br>mstshash=oYYvhHFCq<br>mstshash=sOsMtUzuW<br>mstshash=yB1Nbiekh  | 0efdb177fd787489e7e6c8295994c22d<br>46d75491eddf157ad030051e52e78364<br>cb42d1c3edbdc06e2e926e83360d4108<br>fefd61bfc1ec9f25bada8354740cf86e |
| 185.173  | mstshash=dGioJTpEG<br>mstshash=jXCdWwuKY<br>mstshash=rMIRfBldR<br>mstshash=syemUsHMN | 0efdb177fd787489e7e6c8295994c22d<br>46d75491eddf157ad030051e52e78364<br>cb42d1c3edbdc06e2e926e83360d4108<br>fefd61bfc1ec9f25bada8354740cf86e |

Src IP → rdfp



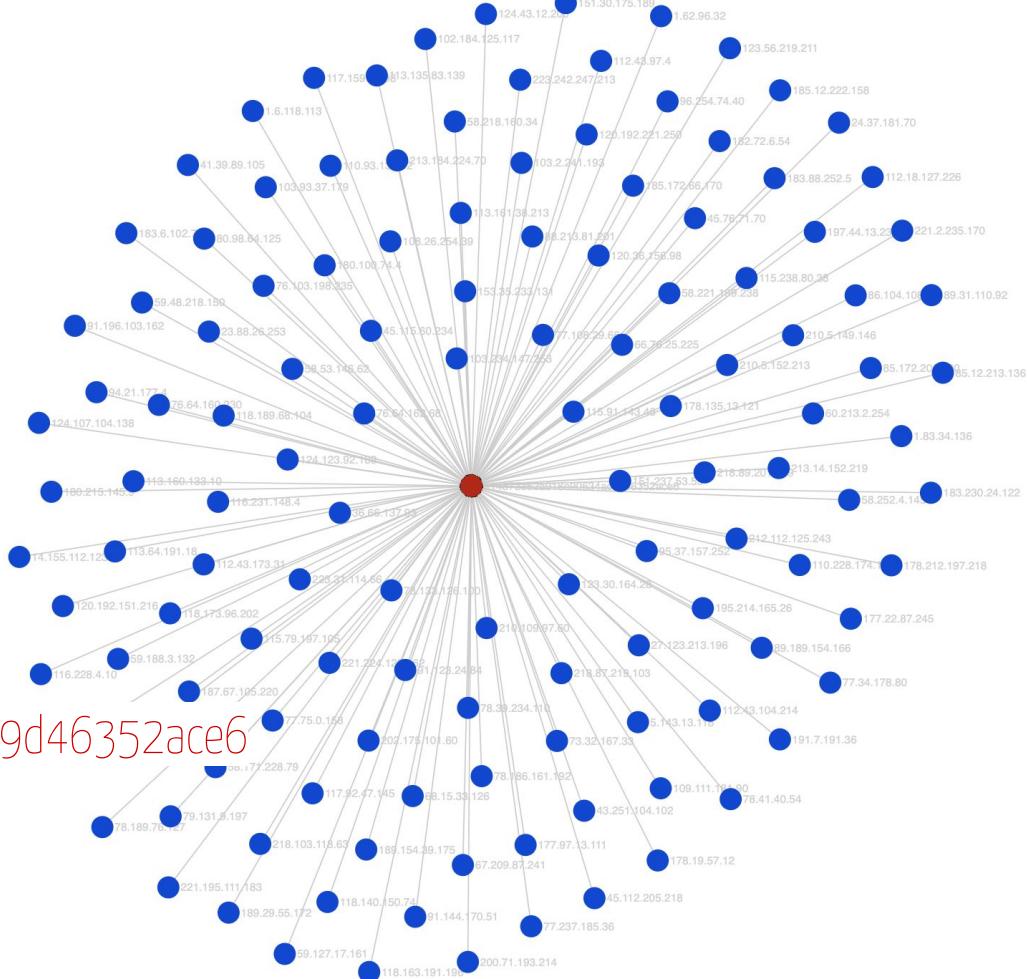
Src IP → rdfs



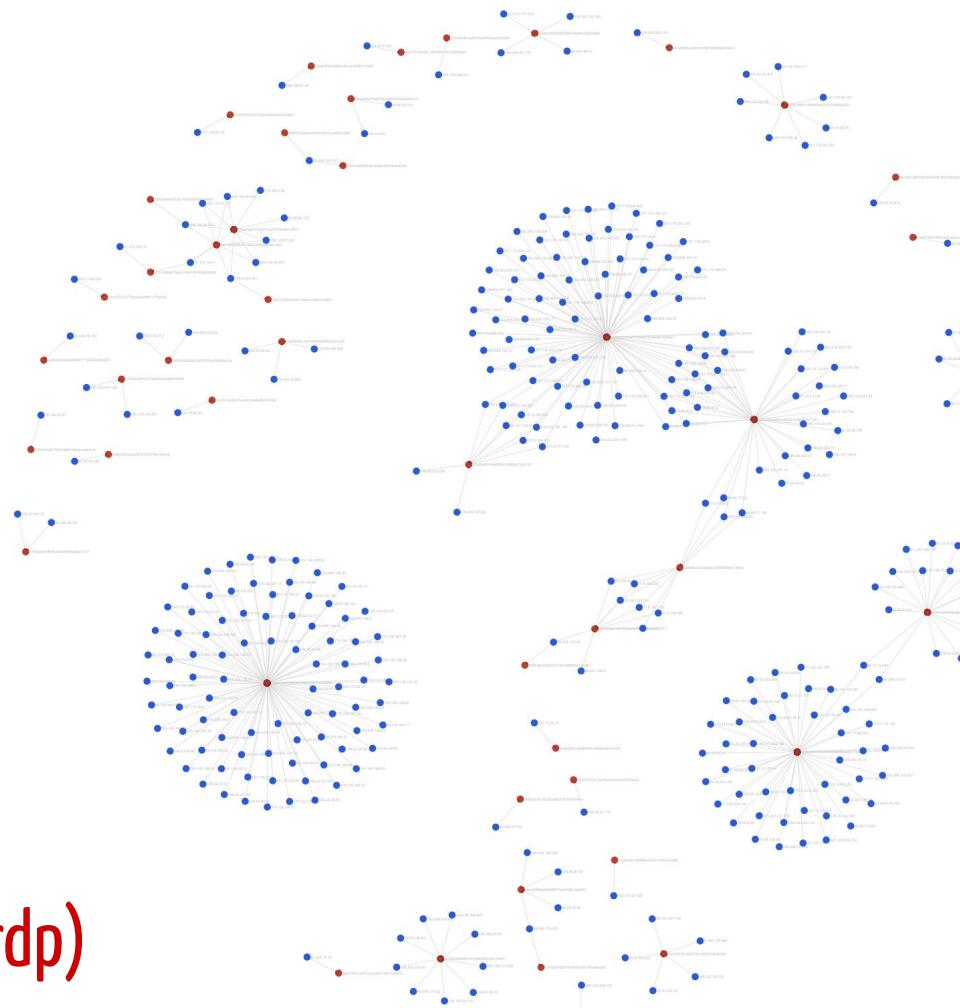
# Morto malware

rdfp: a14873352a918e90634ac9d46352ace6

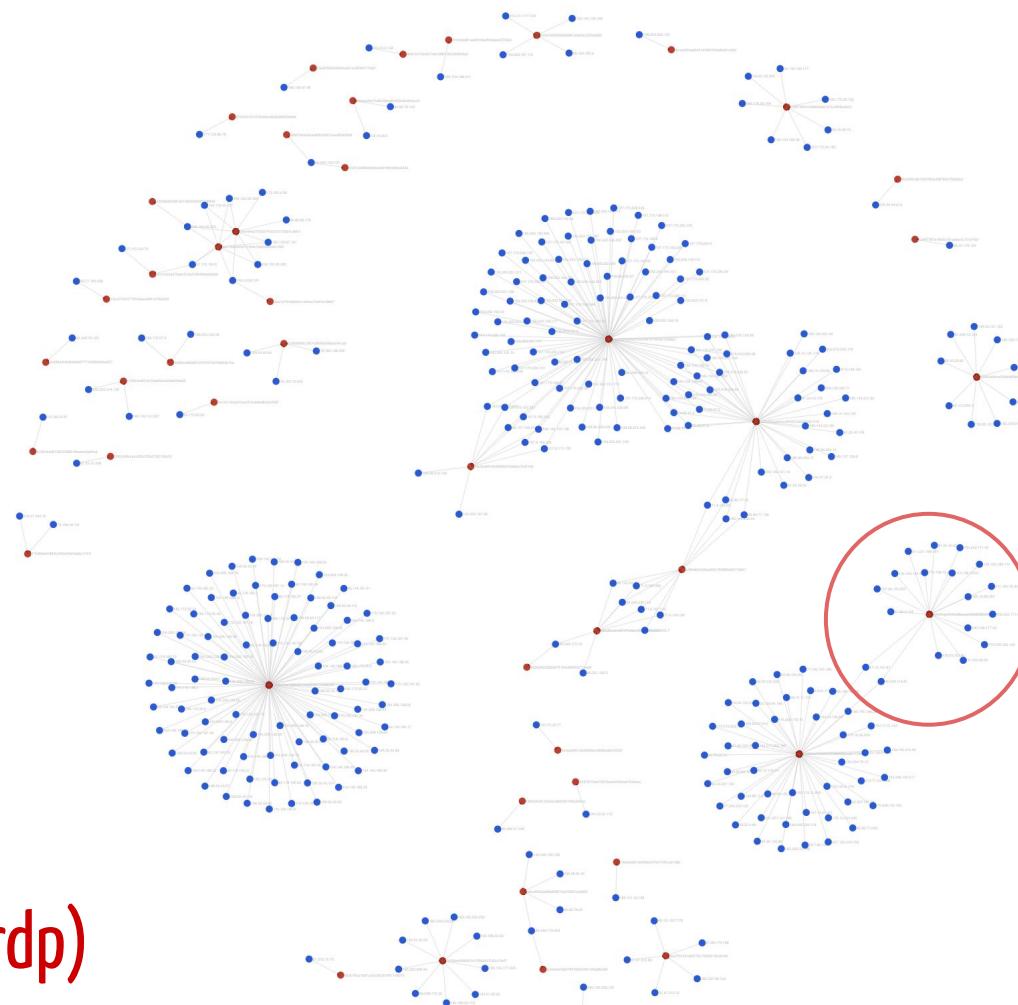
Src IP → rdfp

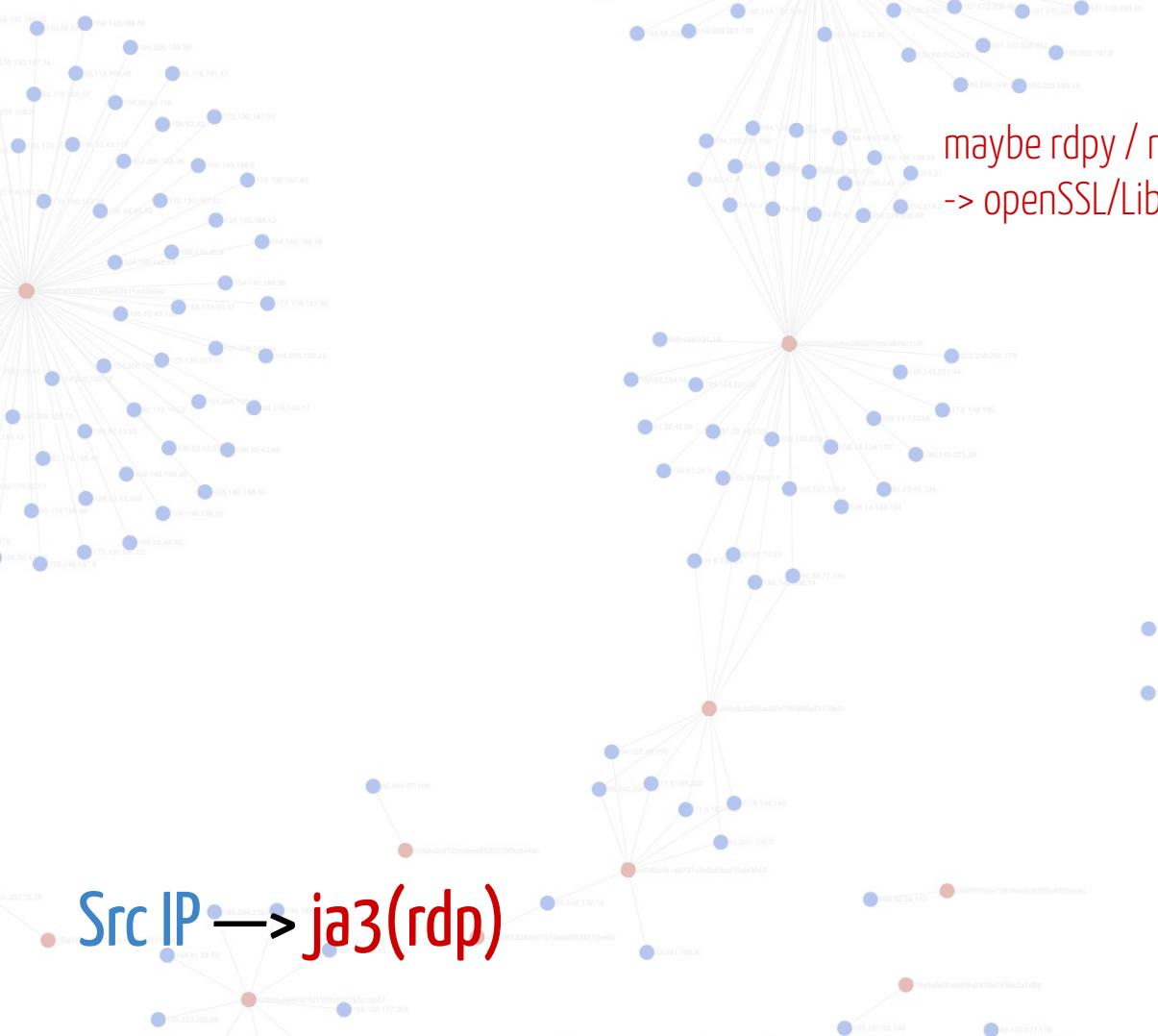


Src IP → ja3(rdp)

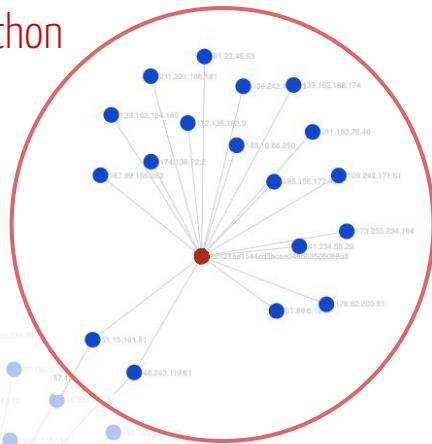


Src IP → ja3(rdp)





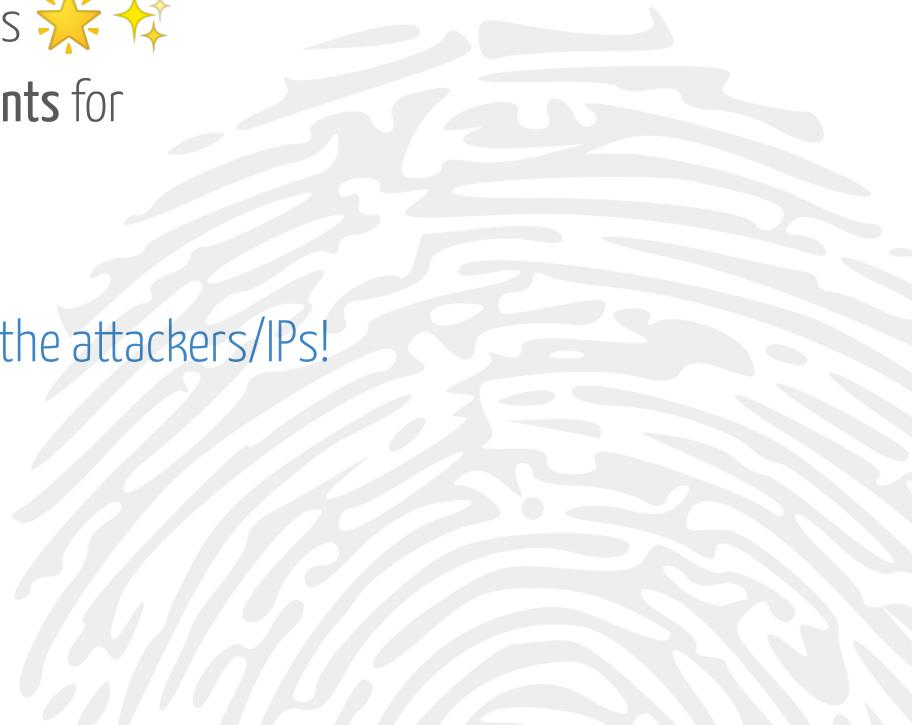
maybe rdp / rdesktop / python  
→ openSSL/LibreSSL-2.2.7!?



Src IP → ja3(rdp)

# Key Takeaways

- NSM is not dead!
- Initial handshake in cryptographic protocols is 
- You can use network metadata and fingerprints for
  - Hunting badness!
  - Profiling attackers and their tools
  - Discovering new connections between the attackers/IPs!
  - Detecting evasion techniques



A wide-angle photograph of a mountainous landscape at night. The sky is filled with stars and the bright, colorful band of the Milky Way. In the foreground, a small orange tent is set up on a grassy slope, its interior glowing with light. The mountains in the background are partially covered in snow and illuminated by a warm, orange glow from the horizon, likely from a nearby town or campsite.

Thank You

@0x4d31