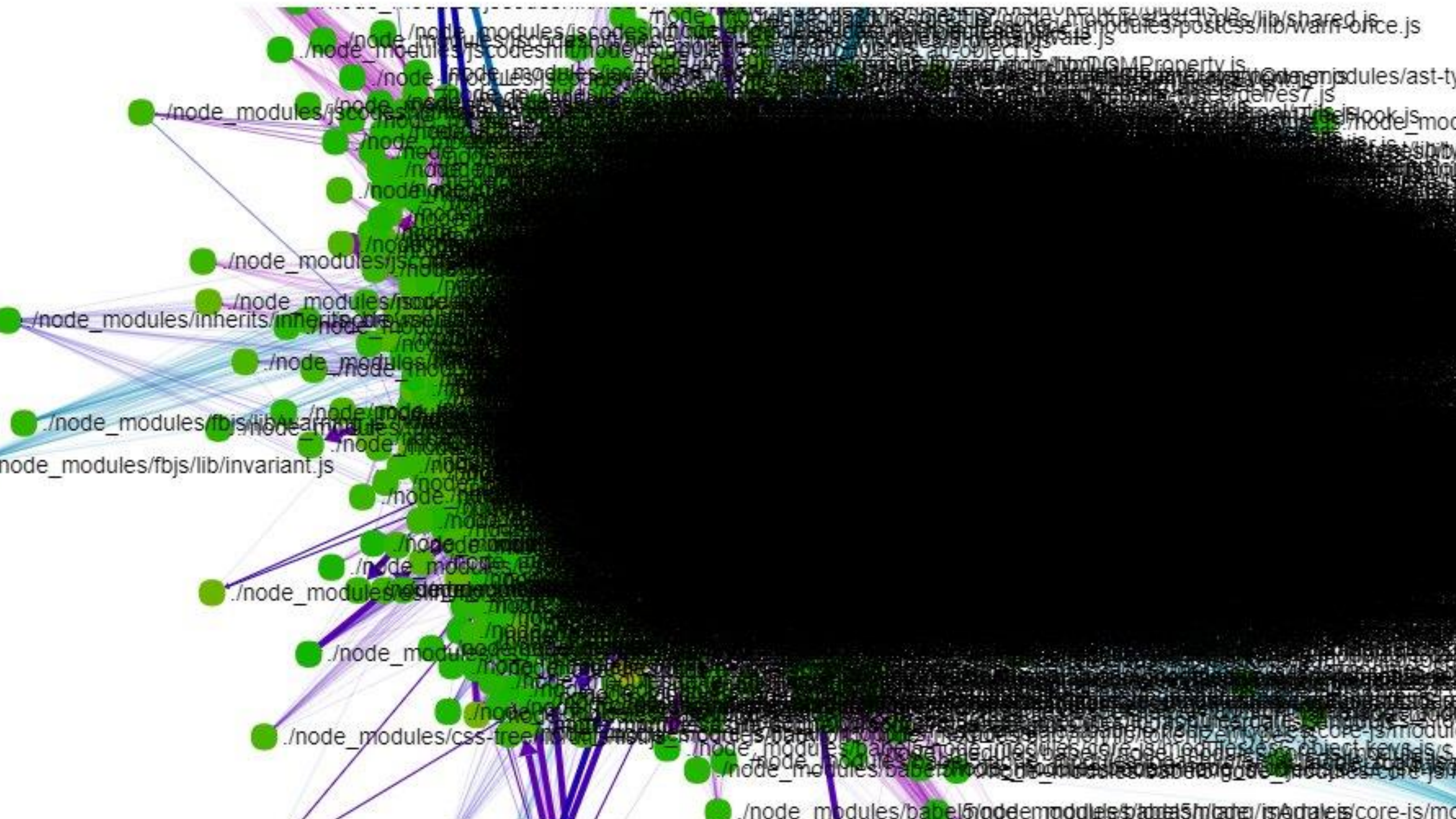
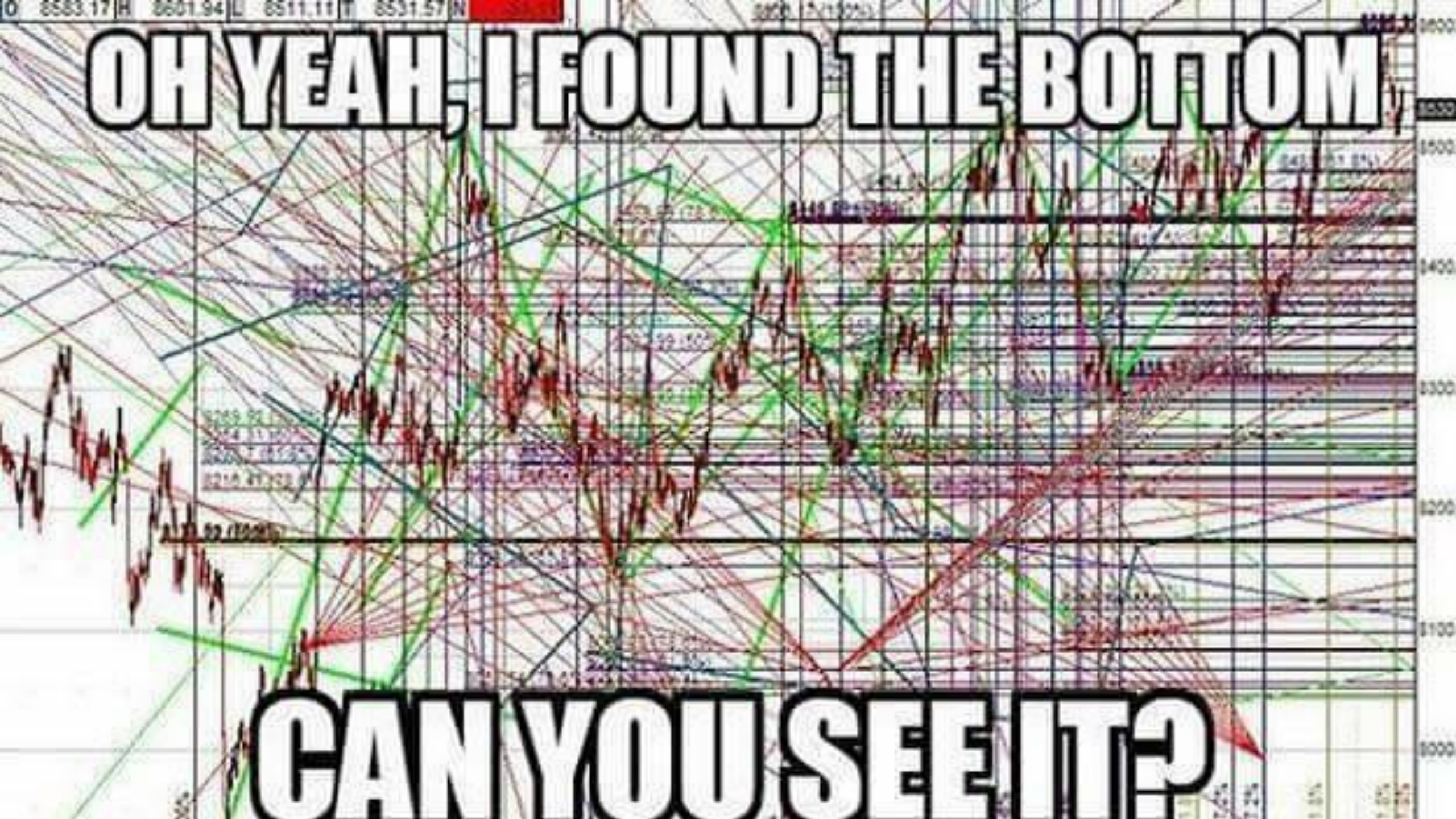
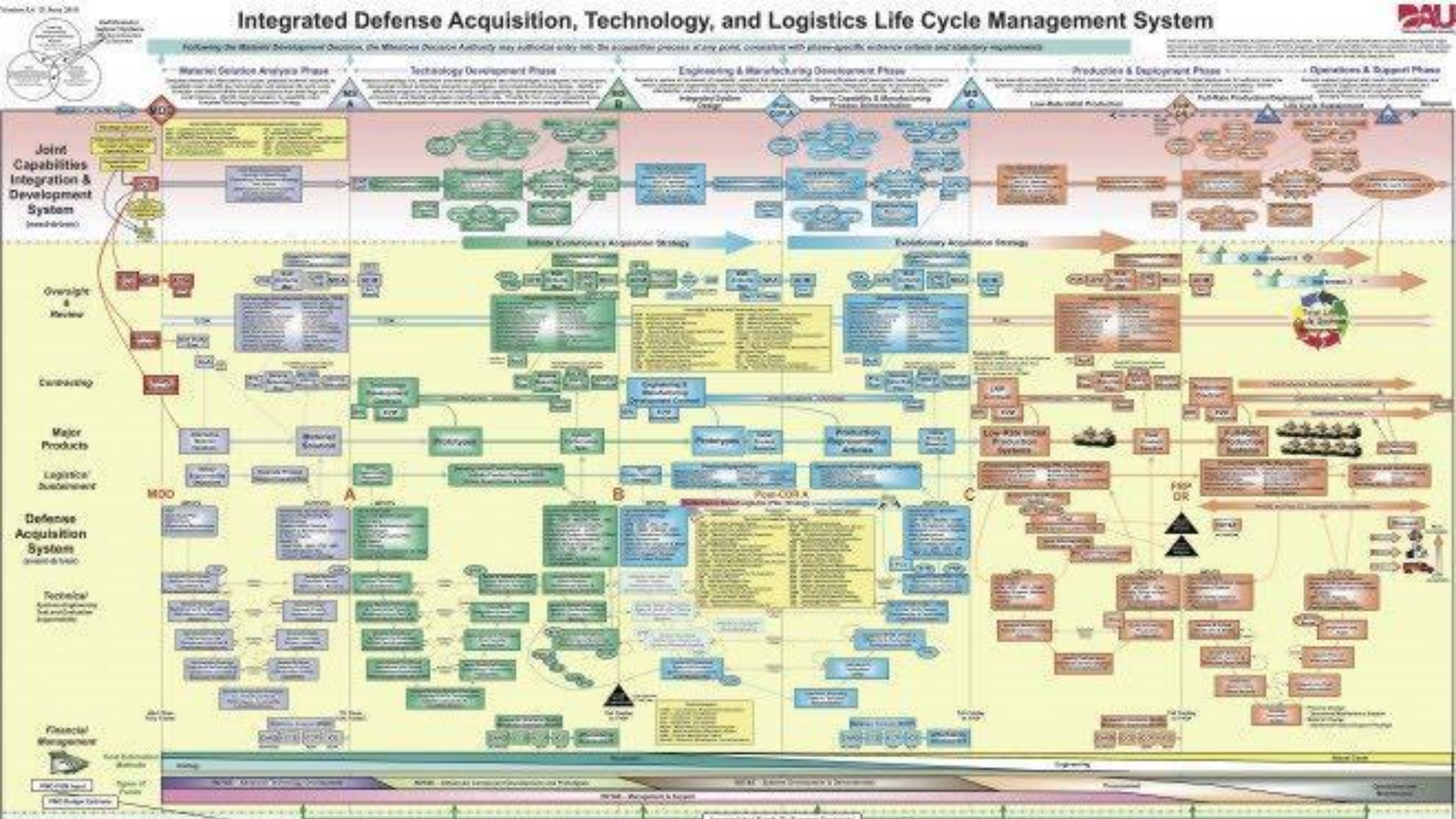
CATS: YOUR PRIVACY IS IMPORTANT
TO US WE WILL NOT SHARE YOUR BASE
WITHOUT YOUR EXPLICIT CONSENT

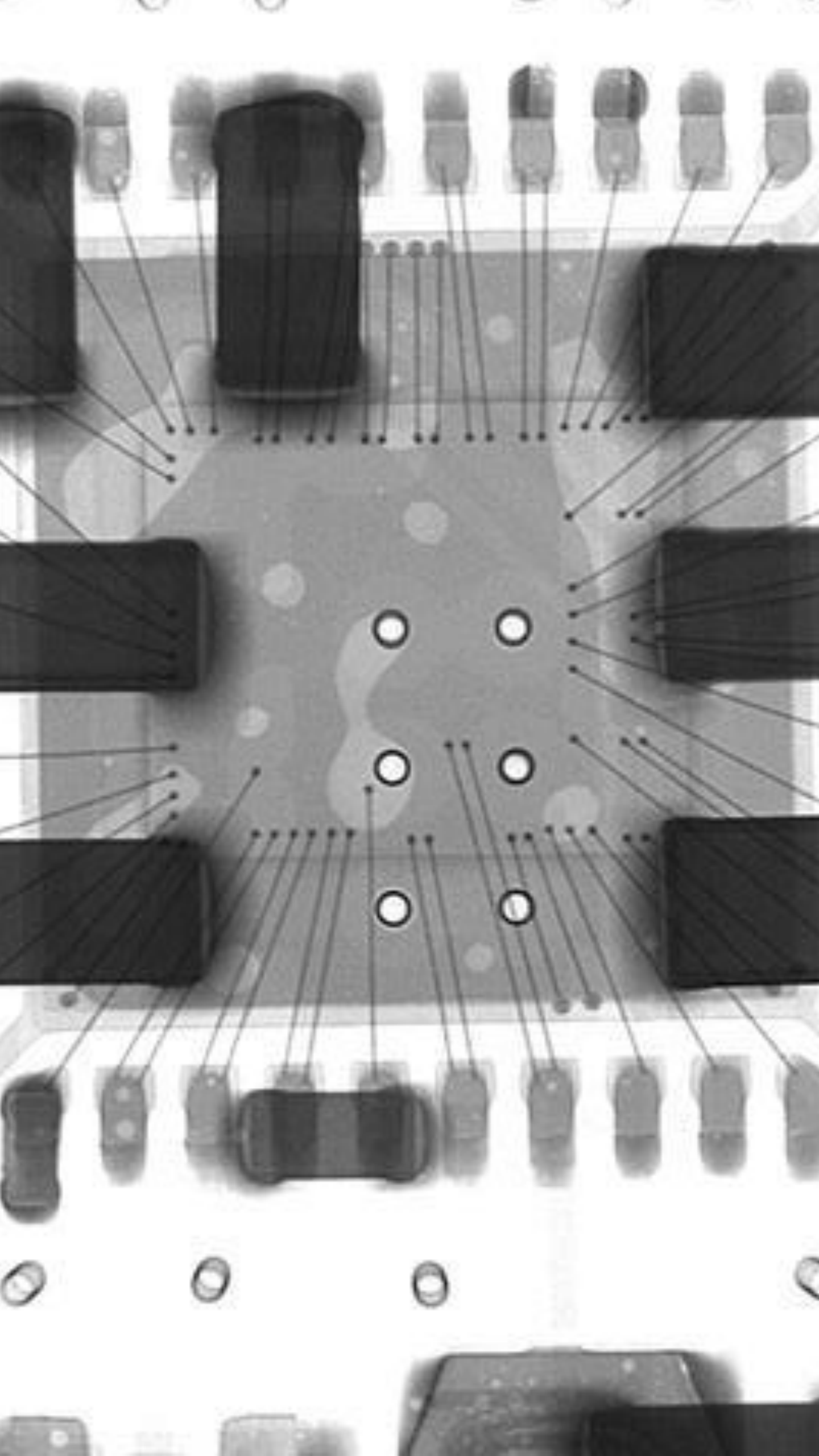

node_modules/fbjs/lib/invariant.js

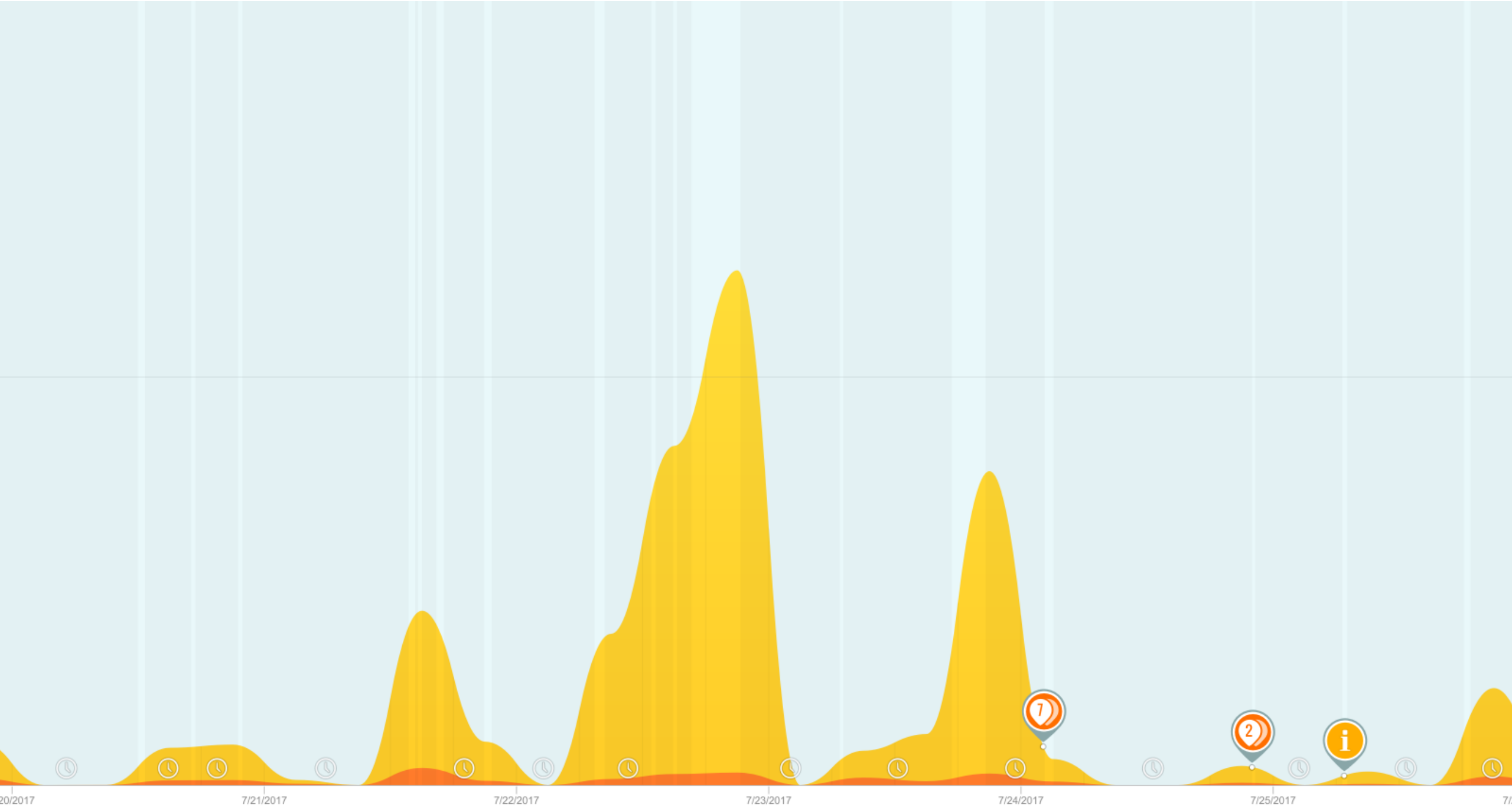

OH YEAH, I FOUND THE BOTTOM
CAN YOU SEE IT?

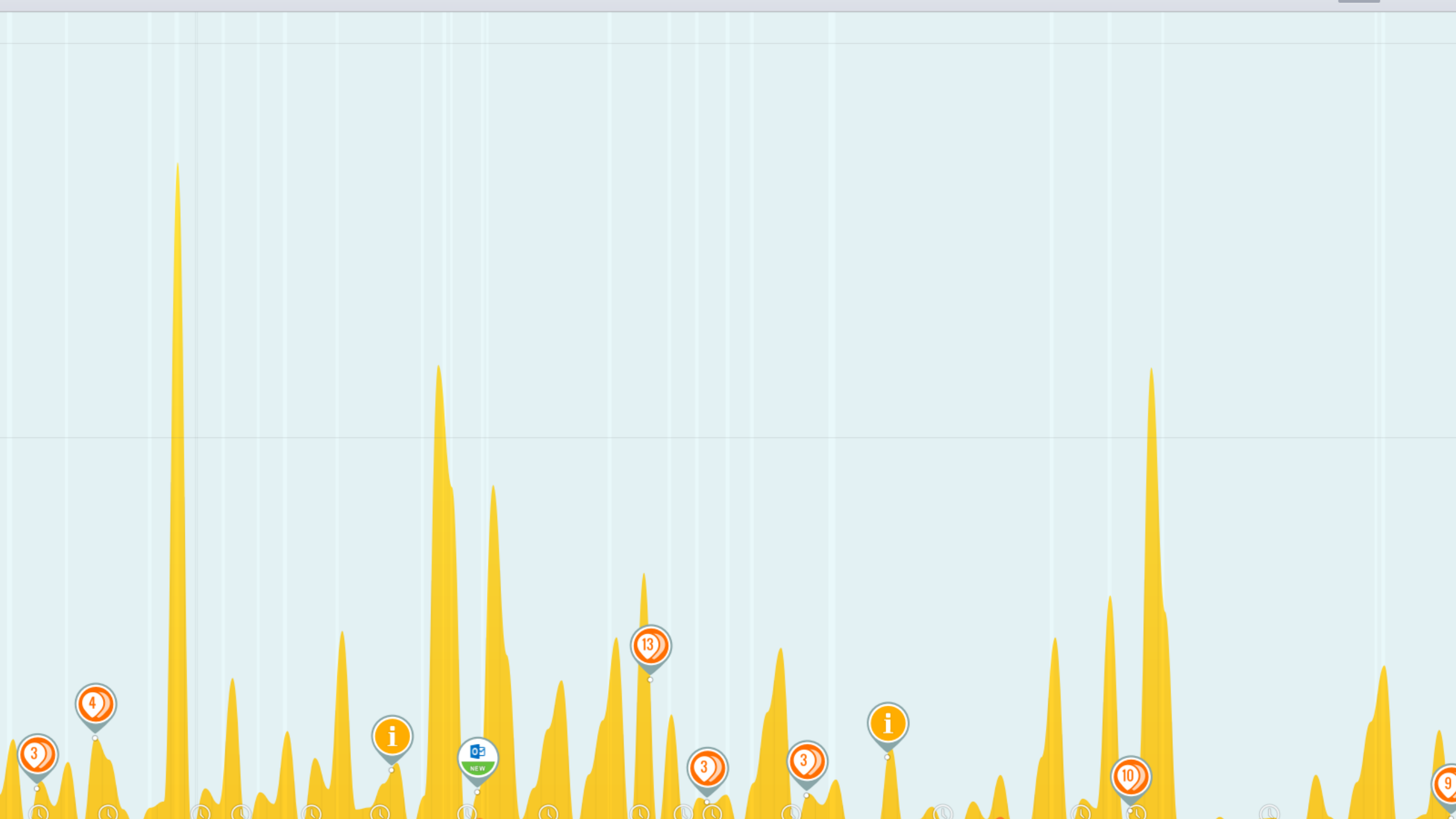
1430953220014.jpg

Integrated Defense Acquisition, Technology, and Logistics Life Cycle Management System

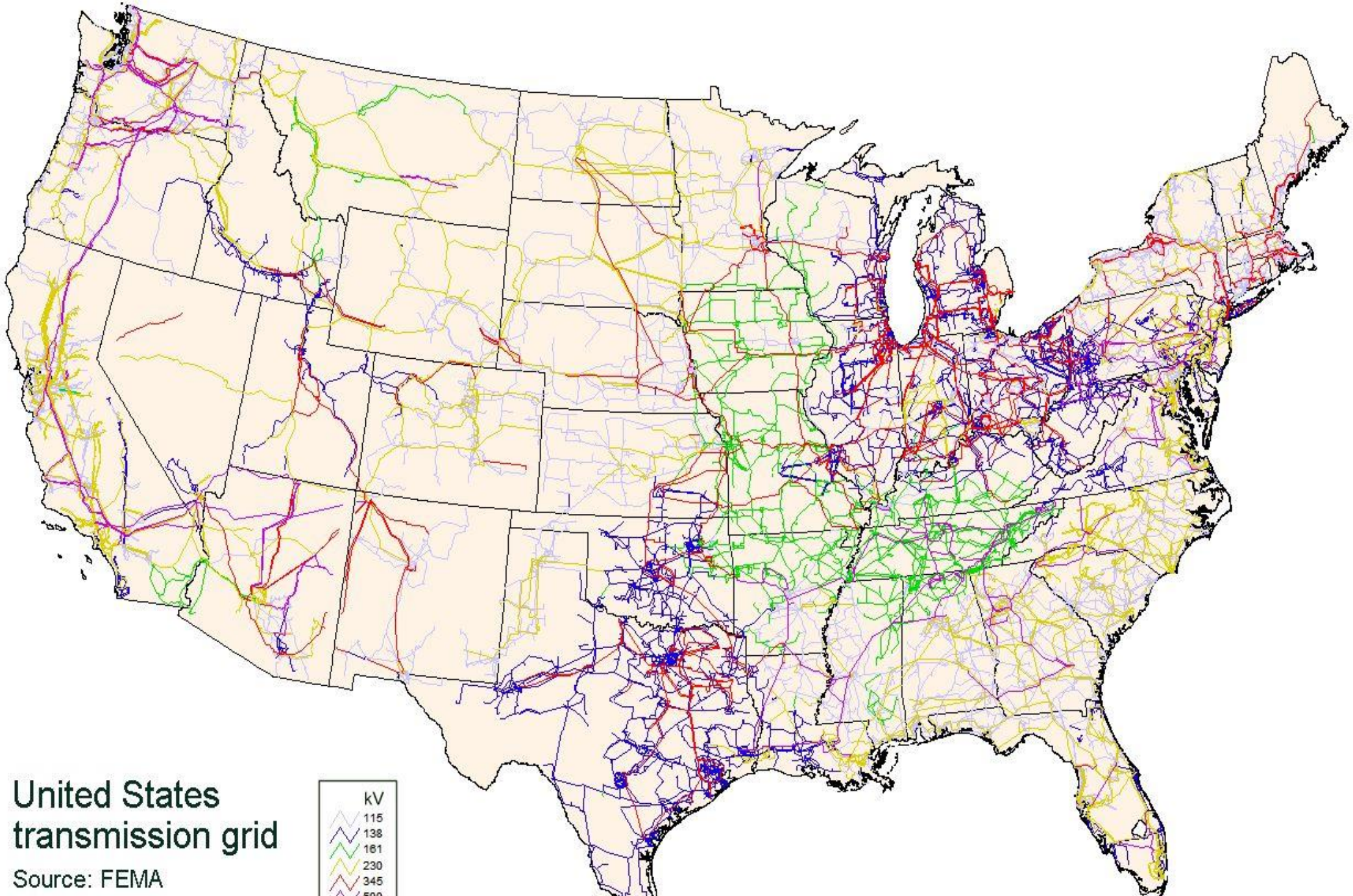





7
2
i
20/2017
7/21/2017
7/22/2017
7/23/2017
7/24/2017
7/25/2017

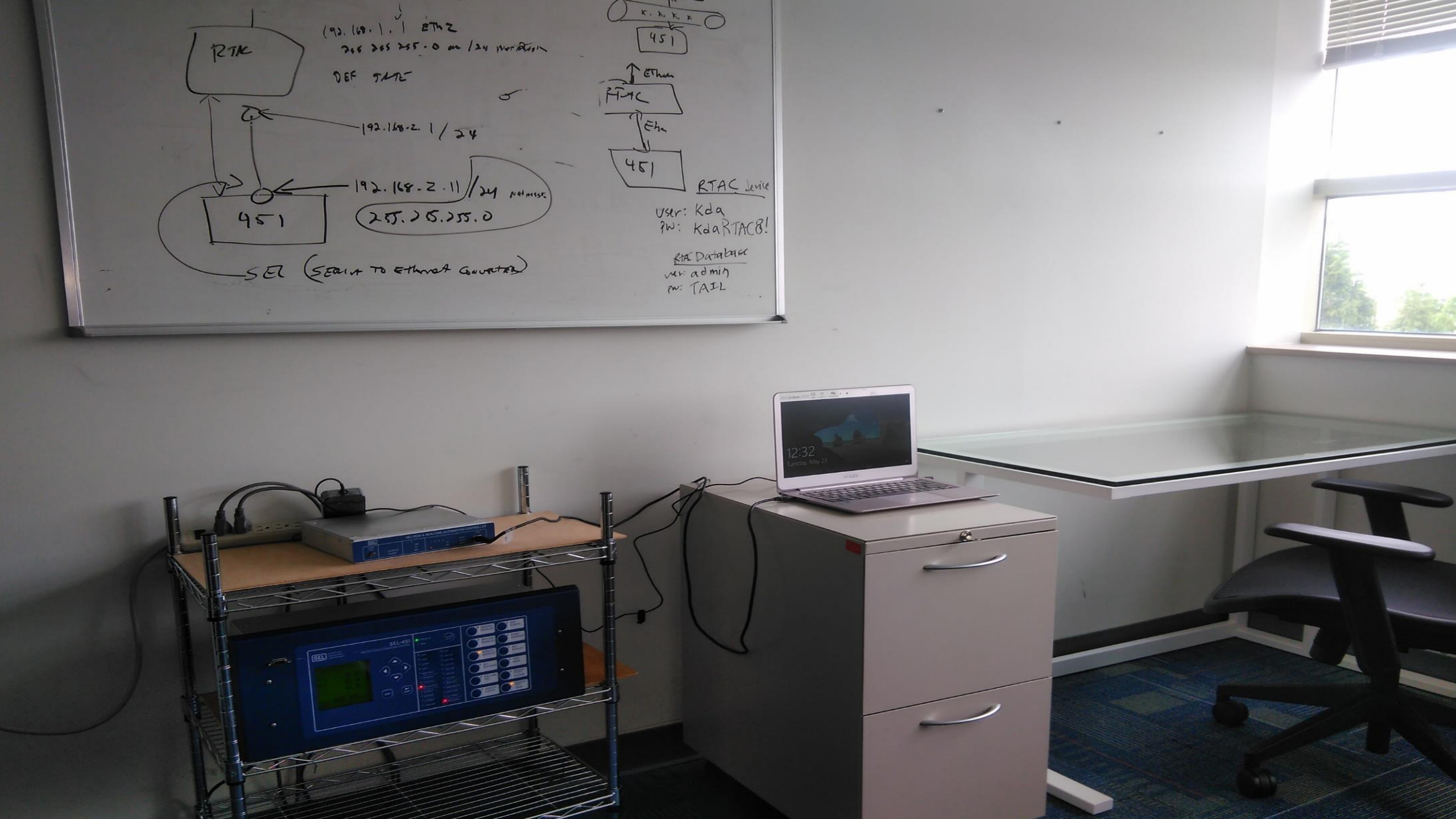

3
4
NEW
13
3
3
10
9

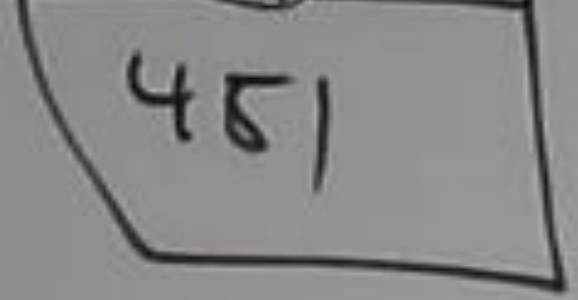

POSEABLE
Mr. Bill
Ohh Nooo!!!


United States
transmission grid
Source: FEMA
kV
115
138
161
230
345


RTAC
(92.168.1.1 ETH2
255 255 255.0 or /24
DEF GATE
192.168.2.1 / 24
451
192.168.2.11 // 24
255.255.255.0
SEL (SERIAL TO ETHERNET CONVERTER)
RTAC
Ethernet
RTAC
Ethernet
451
RTAC device
User: kda
PW: kdaRTAC8!
RTAC Database
user: admin
pw: TAIL
12:32
Tuesday, May 23


DEF CON 1
Alias
Affiliation
Email
Data: 1


RTAC
(192.168.1.1 ETH2
255.255.255.0 or /24 Network
DEF GATE
192.168.2.1/24
451
192.168.2.11/24 Network
255.255.255.0
SEL (SERIAL TO Ethernet CONVERTER)
Ethernet
RTAC
Eth
451
RTAC Device
User: Kda
PW: KdaRTAC8!
RTAC Database
user: admin
pw: TAIL
12:32



RTAC device

User: Kda
PW: KdaRTAC8!

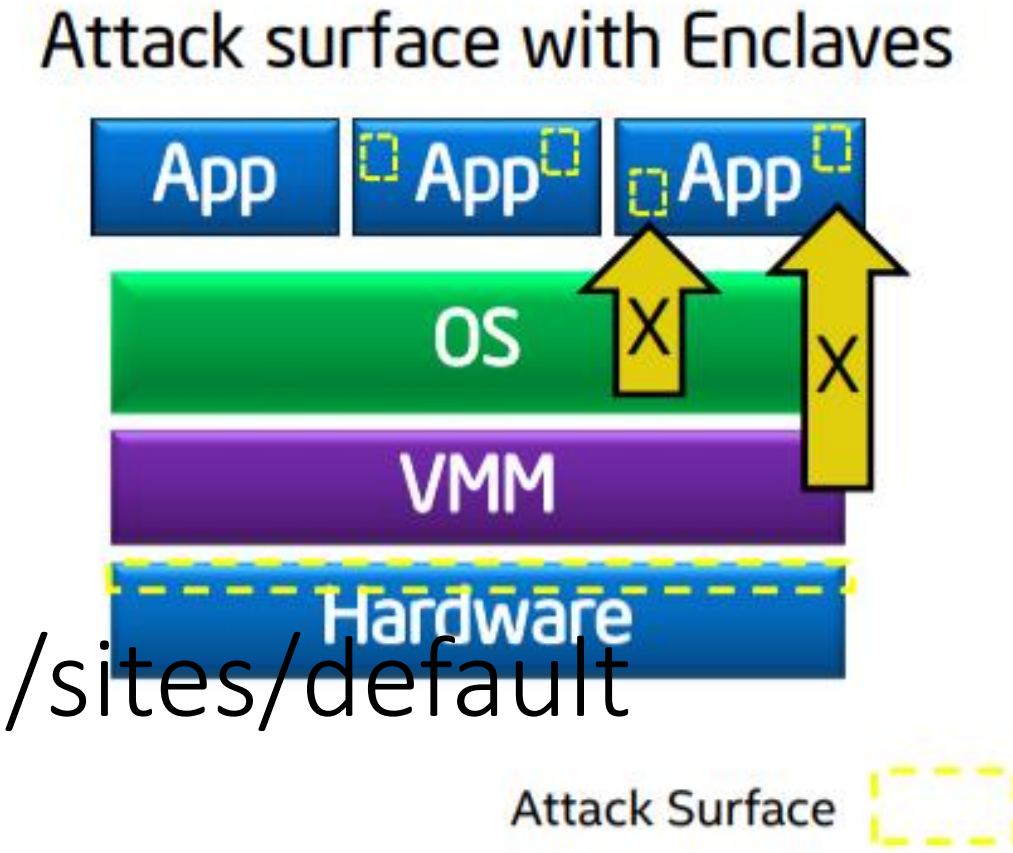
RTAC Database

user: admin
pw: TAIL

Reduced attack surface with SGX

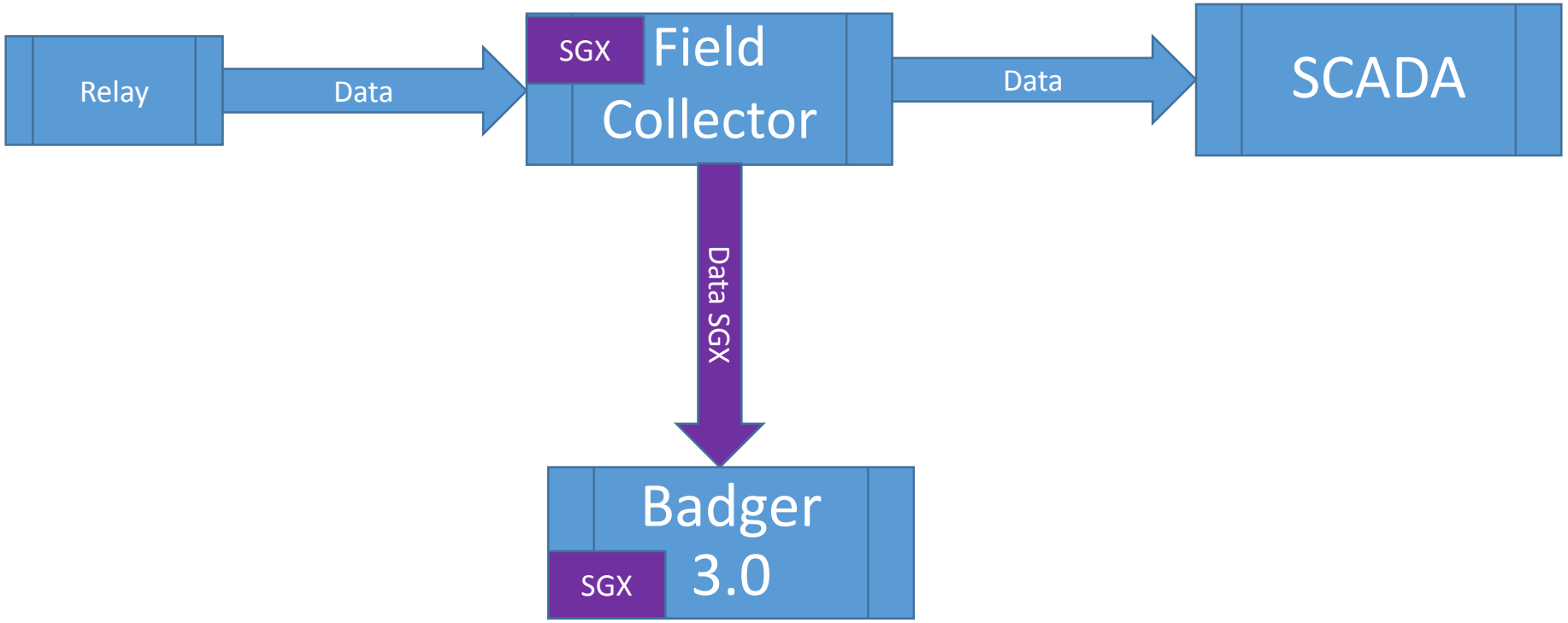
Application gains ability to defend its own secrets

- Smallest attack surface (App + processor)
- Malware that subverts OS/VMM, BIOS, Drivers etc. cannot steal app secrets

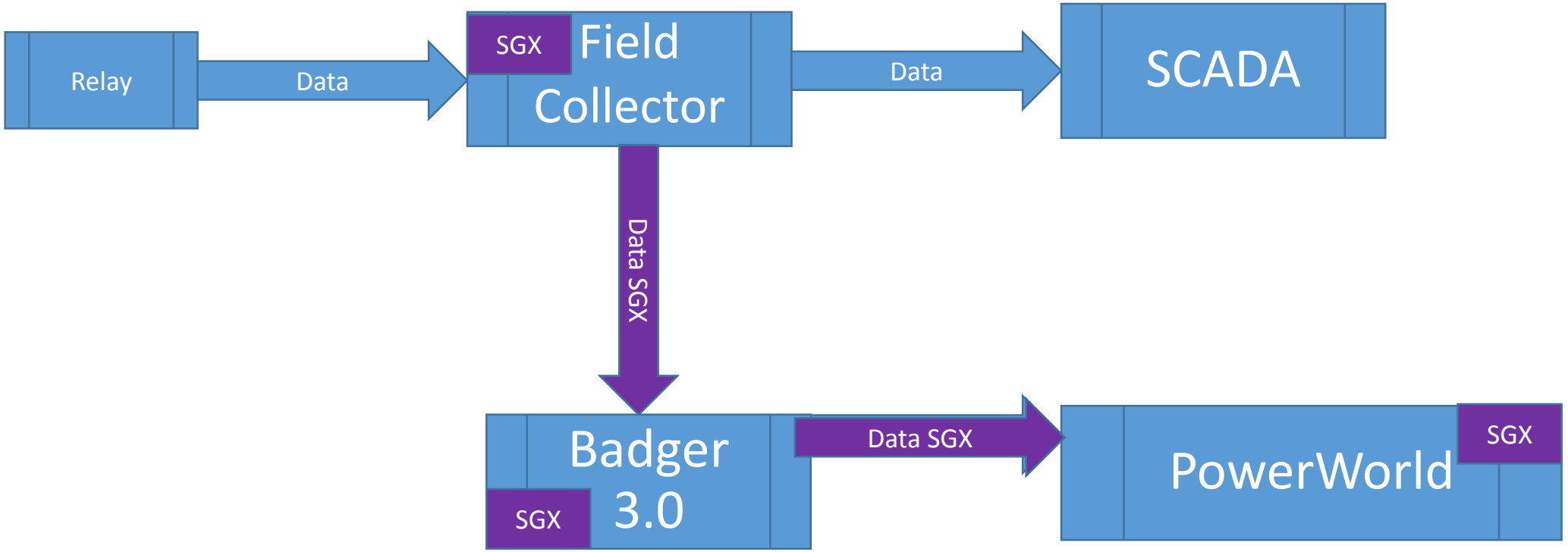


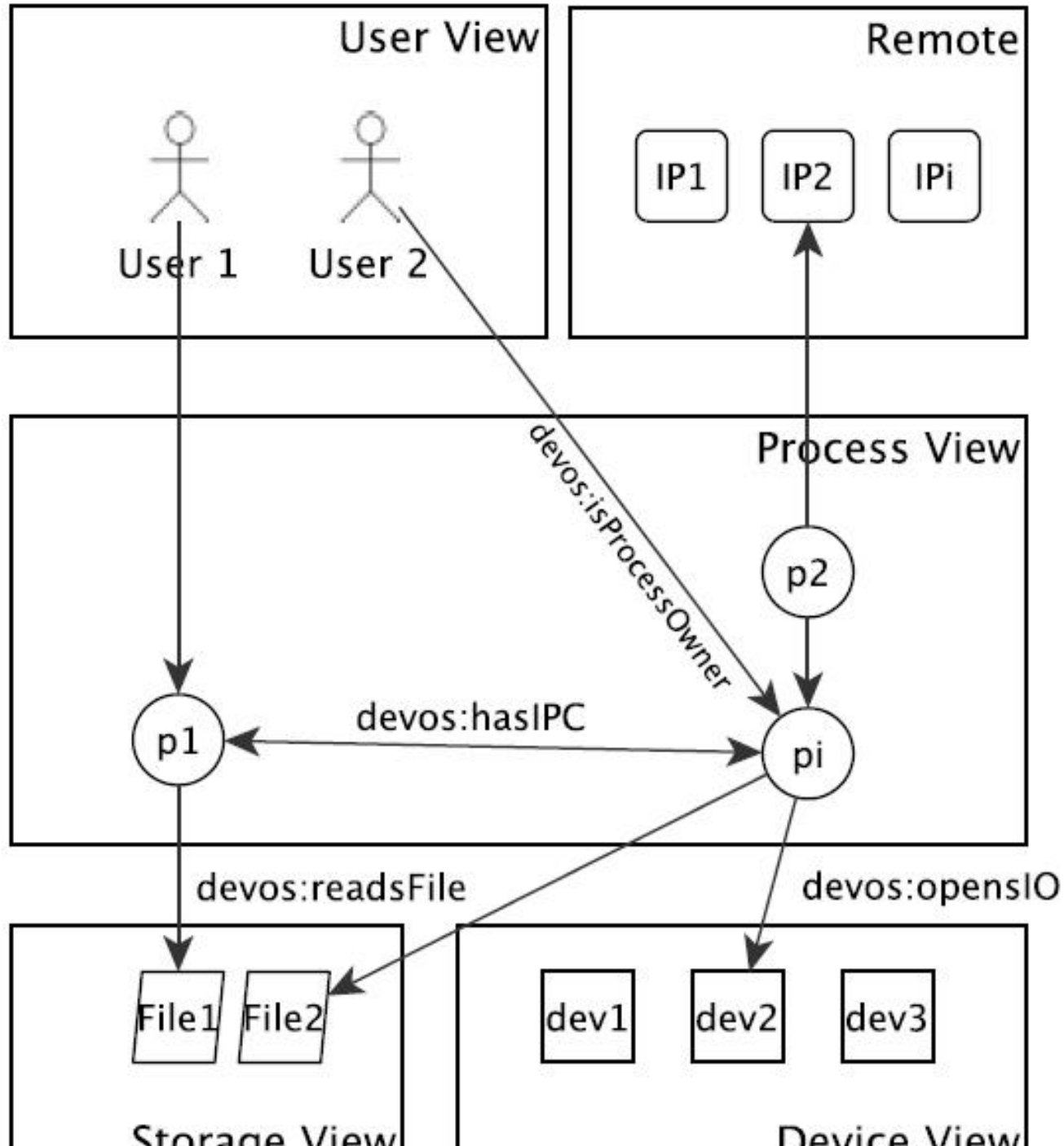
https://software.intel.com/sites/default/files/332680-002.pdf

Data Flows



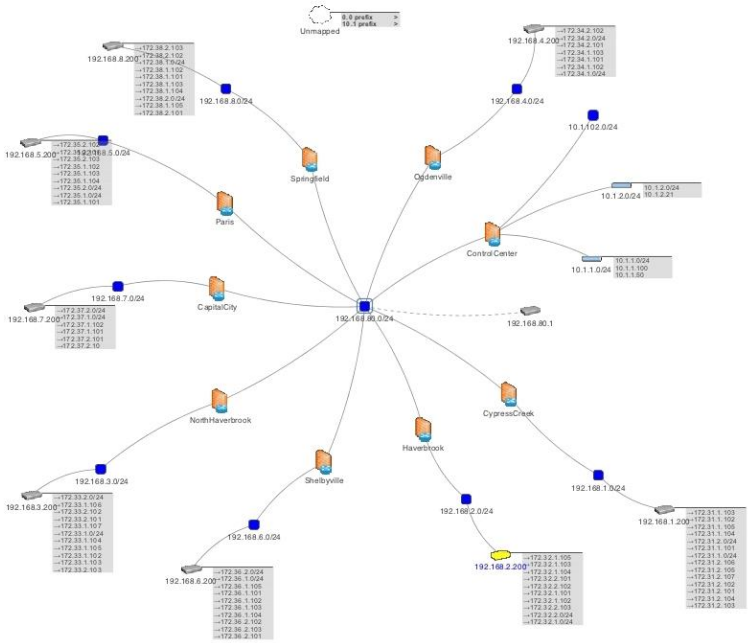
Data Flows

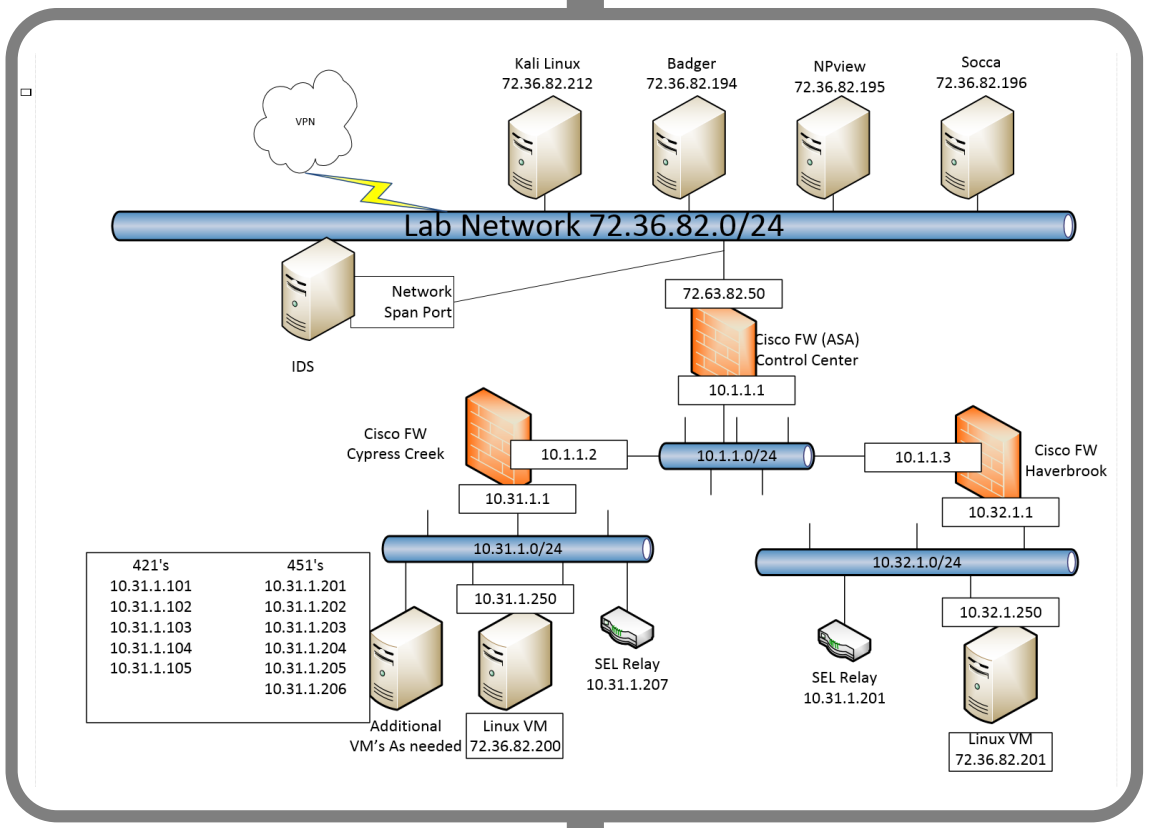



User View
User 1
User 2
Remote
IP1
IP2
IPi
Process View
devos:isProcessOwner
p2
p1
devos:hasIPC
pi
devos:readsFile
devos:opensIO
File1
File2
dev1
dev2
dev3
Storage View
Device View

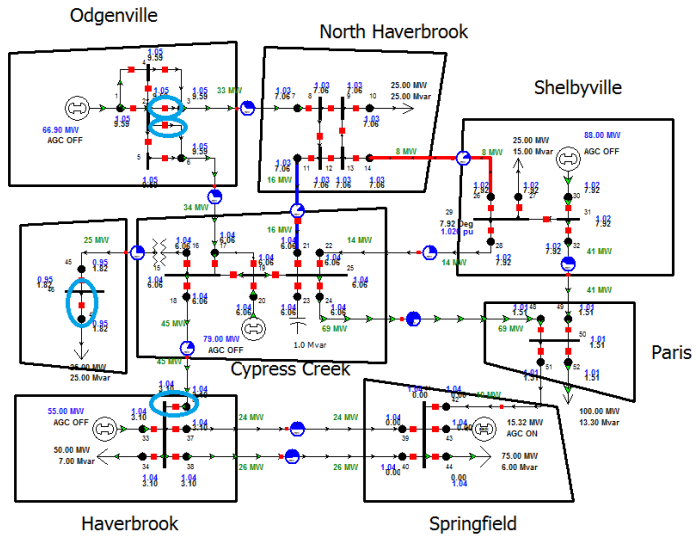
Testbed Setup

Cyber Topology (NP-View)

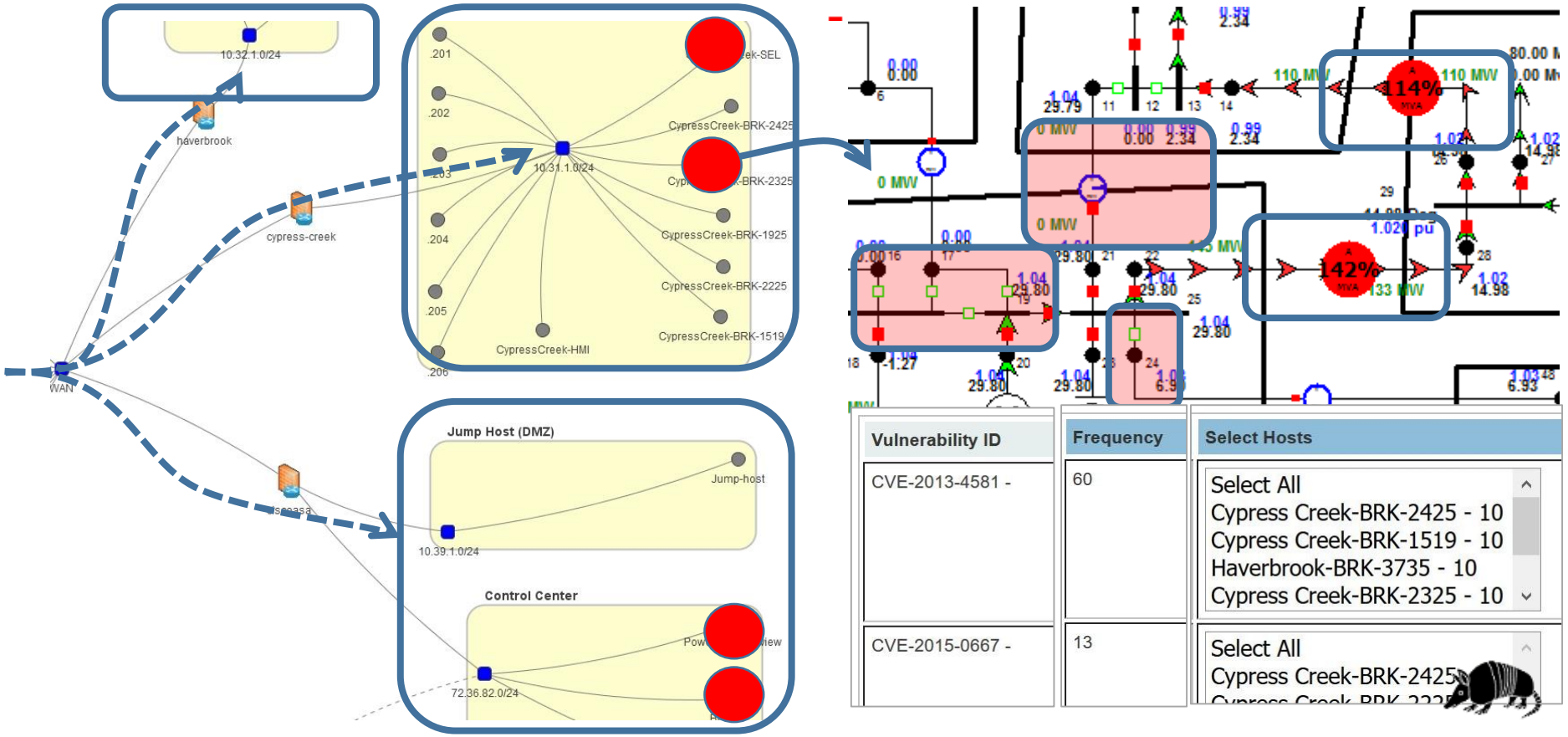




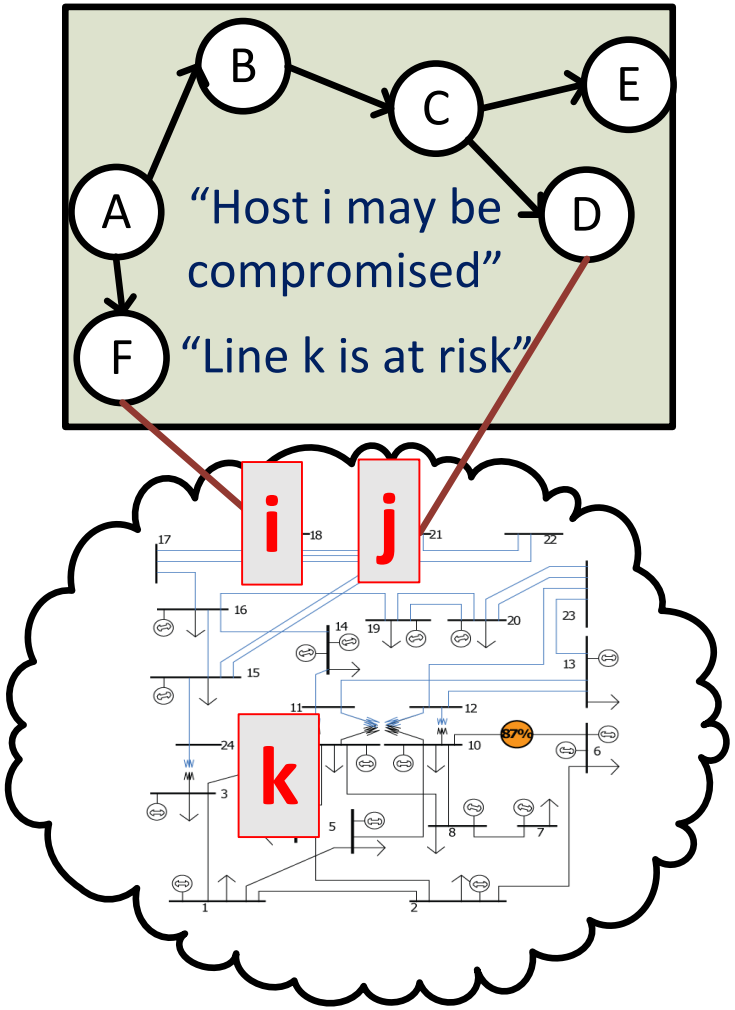
Power Topology (PowerWorld)

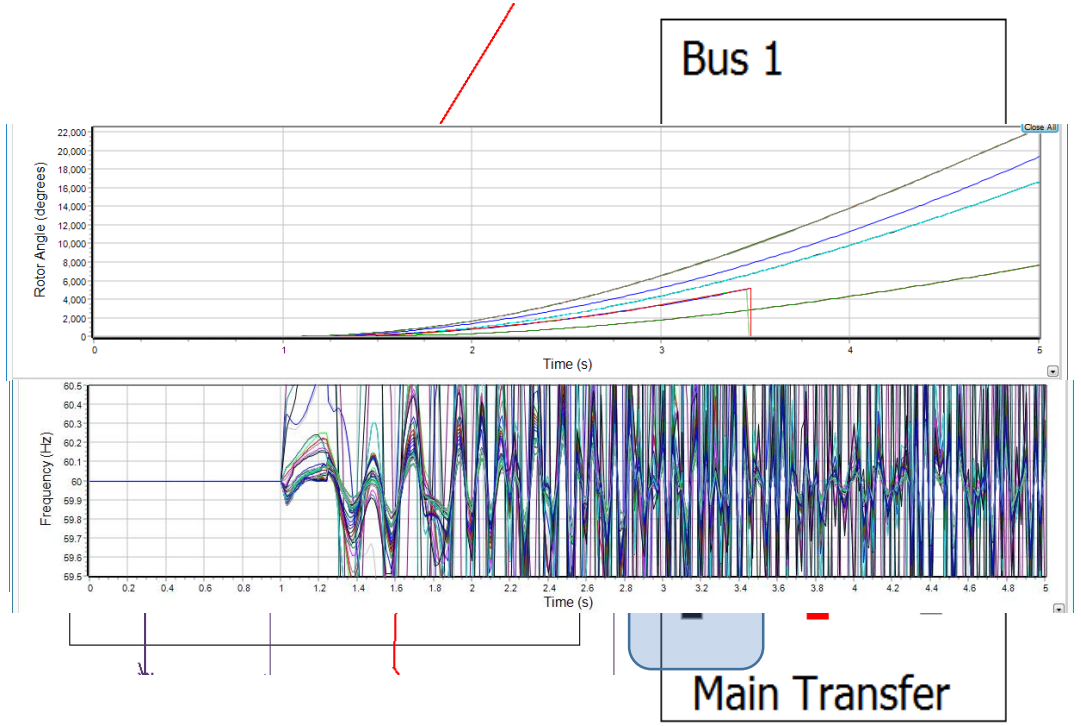


Aggregate information and plan actions

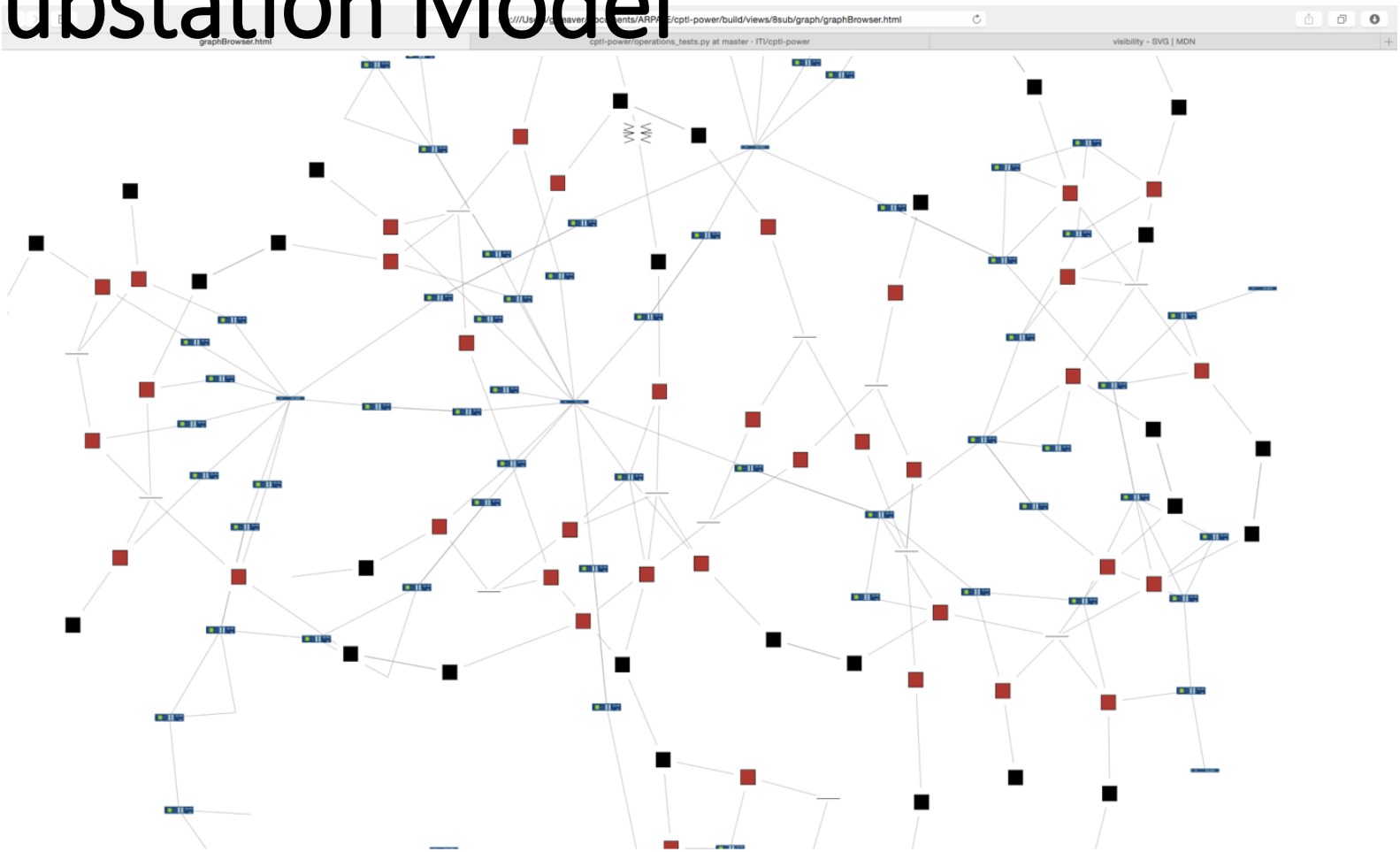


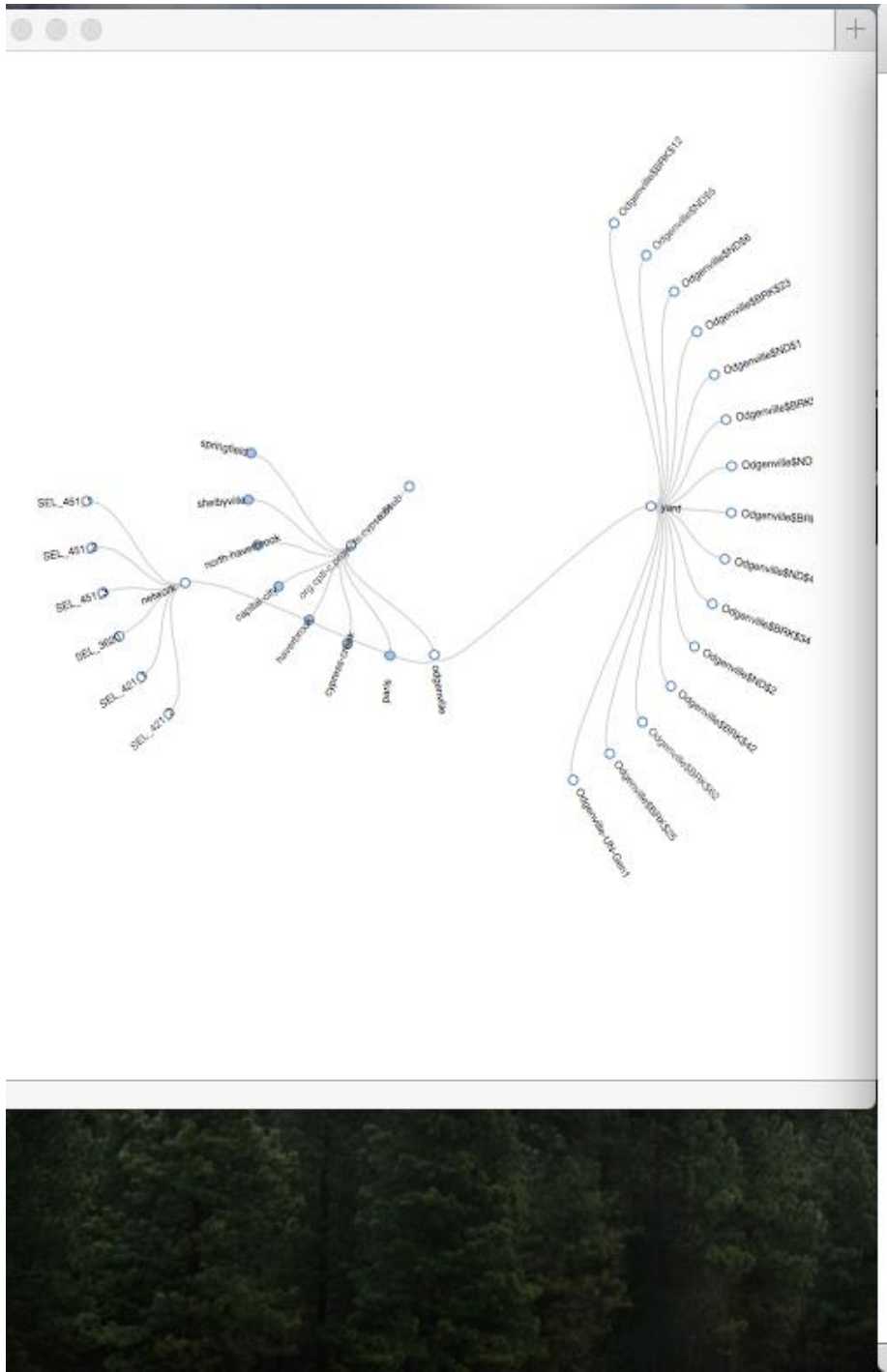
Physical Connections and Impact

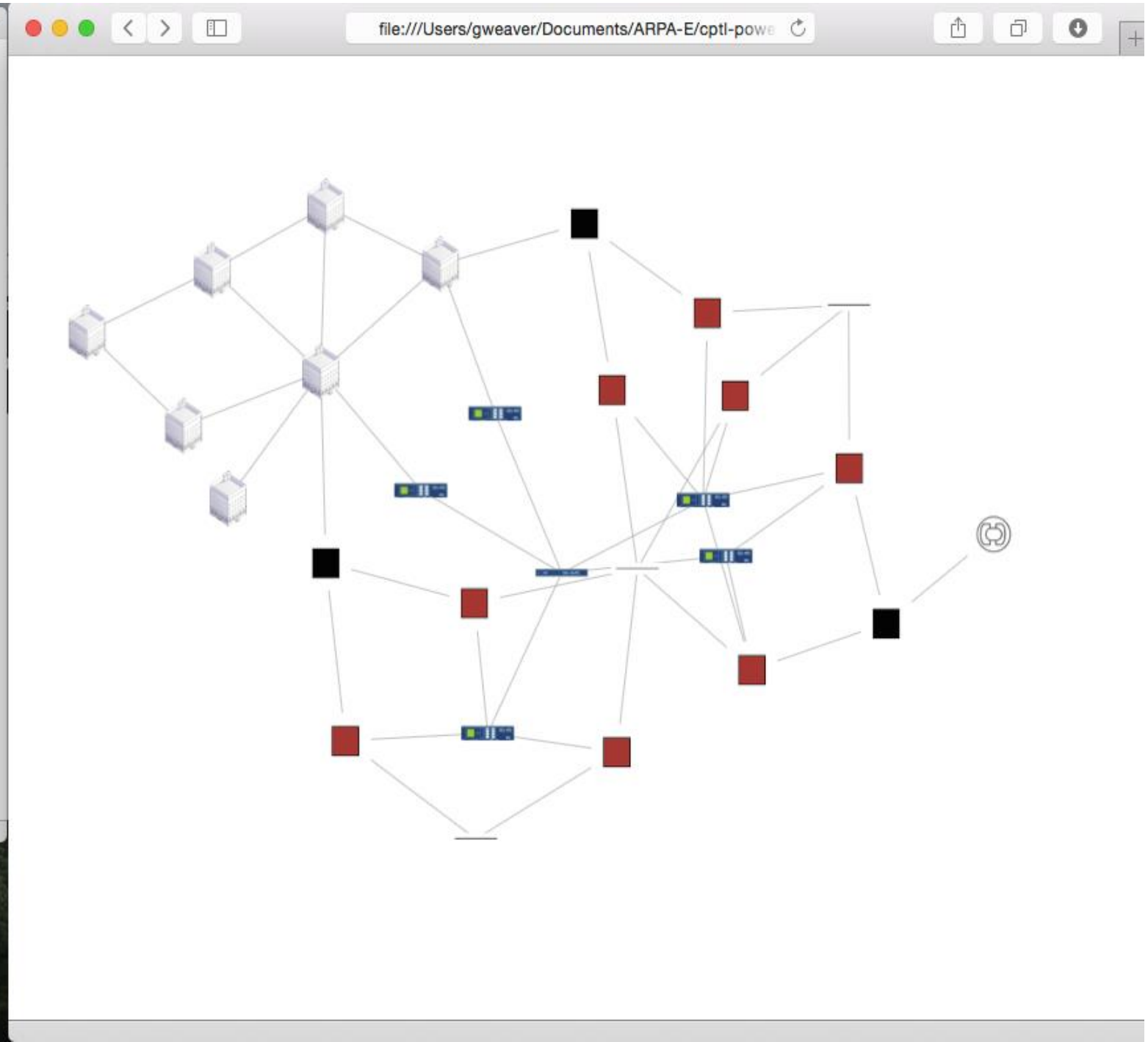


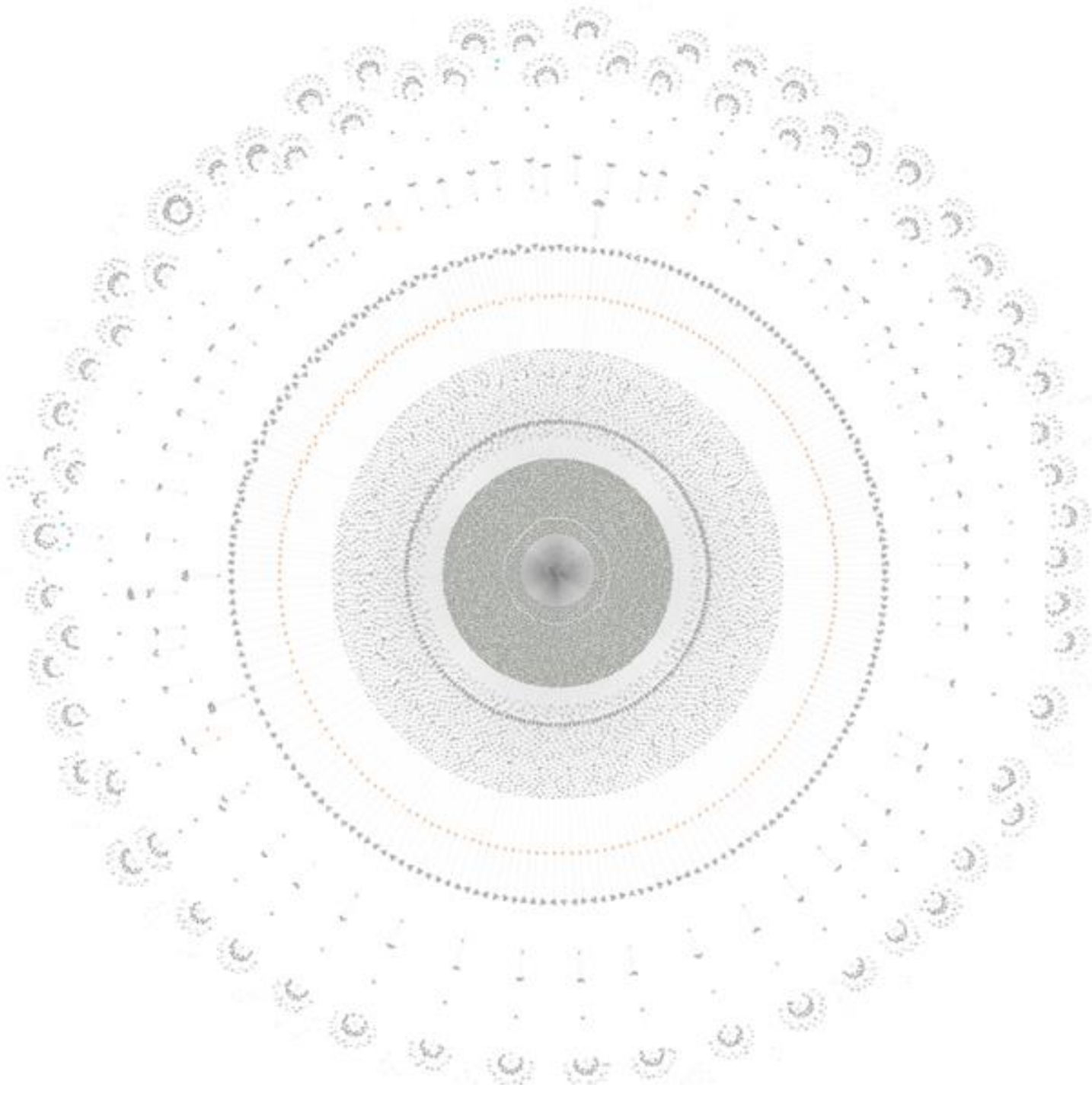


The 8 Substation Model

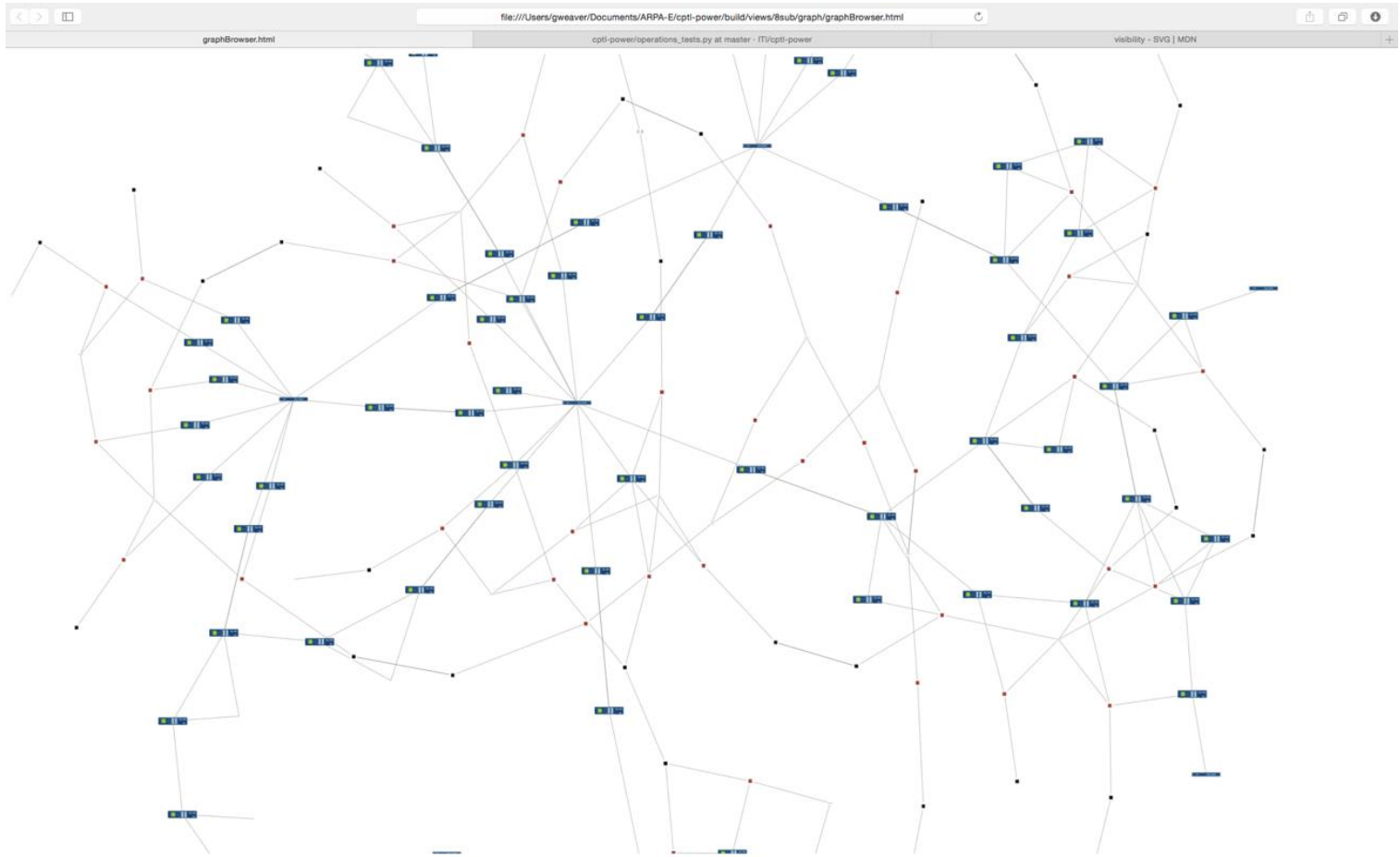



SEL_451
SEL_451
SEL_451
SEL_351
SEL_421
SEL_421
network
springfield
shelbyville
north-haven-rock
capital-city2
hayesfield
cypress-city
davis
odgenville
yard
OdgenvilleSBRK512
OdgenvilleSND35
OdgenvilleSND36
OdgenvilleSBRK323
OdgenvilleSND51
OdgenvilleSBRK
OdgenvilleSND
OdgenvilleSBRK
OdgenvilleSND54
OdgenvilleSBRK534
OdgenvilleSND32
OdgenvilleSBRK342
OdgenvilleSBRK302
OdgenvilleSBRK329
Odgenville-Unit-Distrct

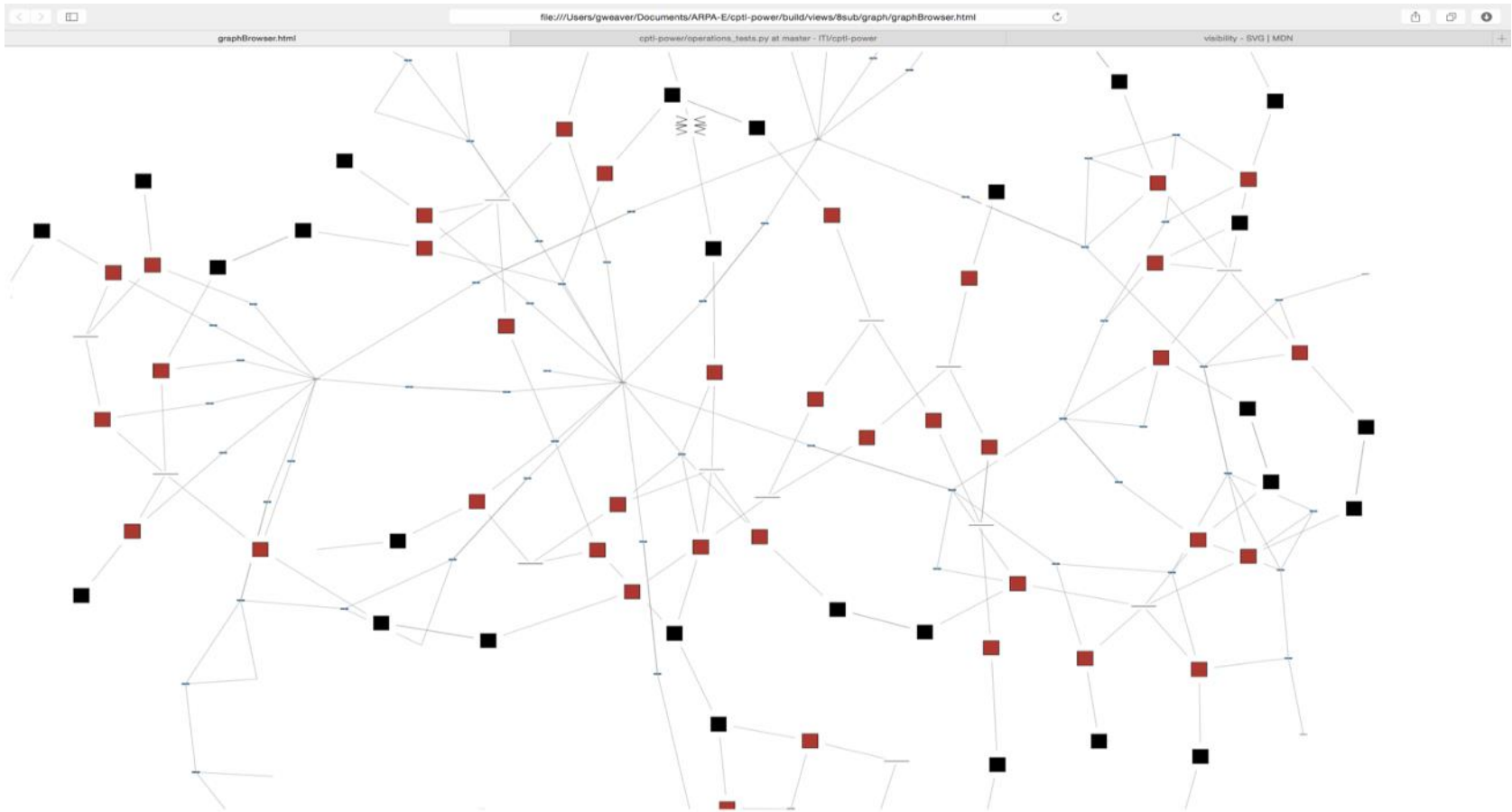

file:///Users/gweaver/Documents/ARPA-E/cptl-powe



Substation Networks

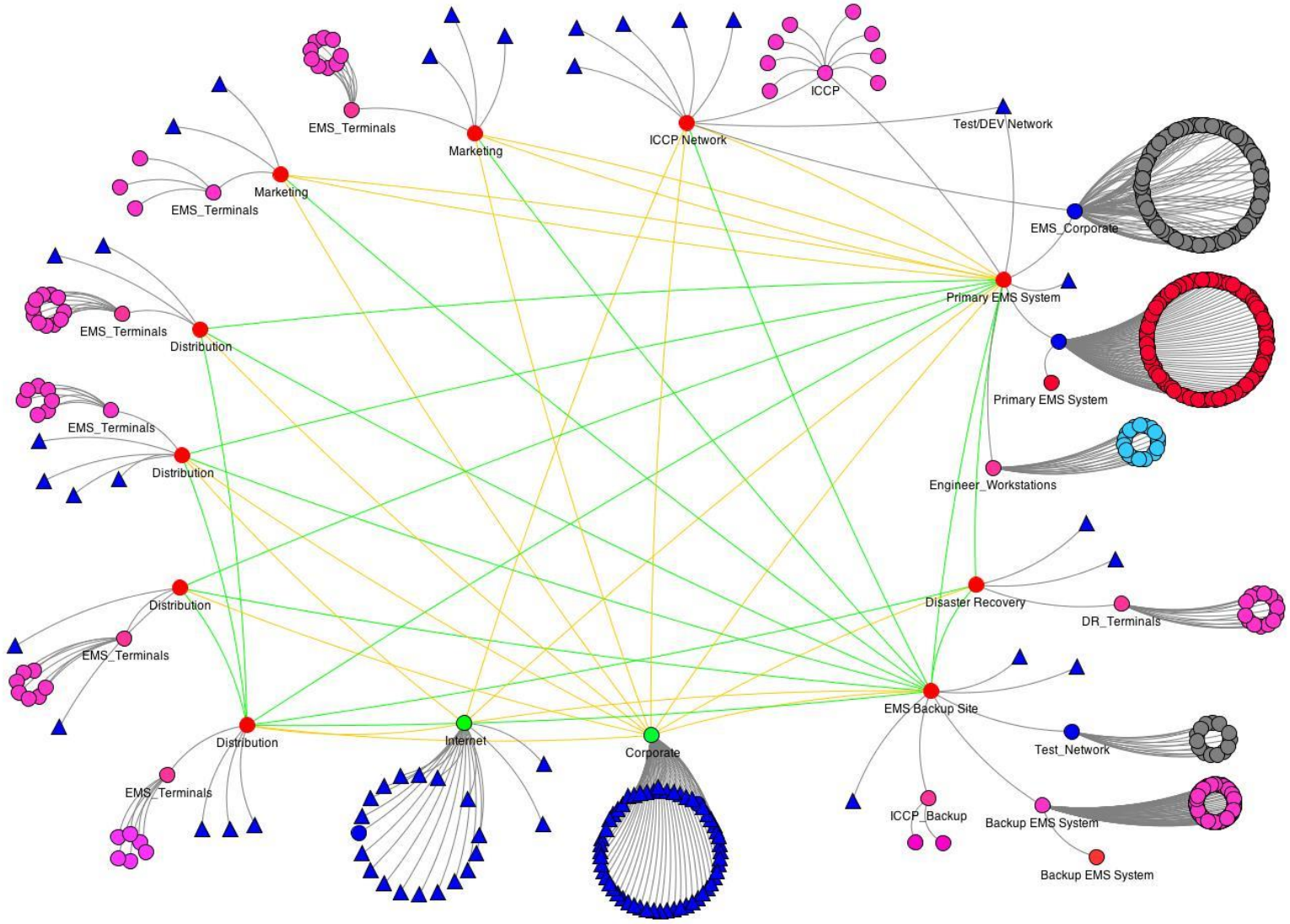


Substation Networks

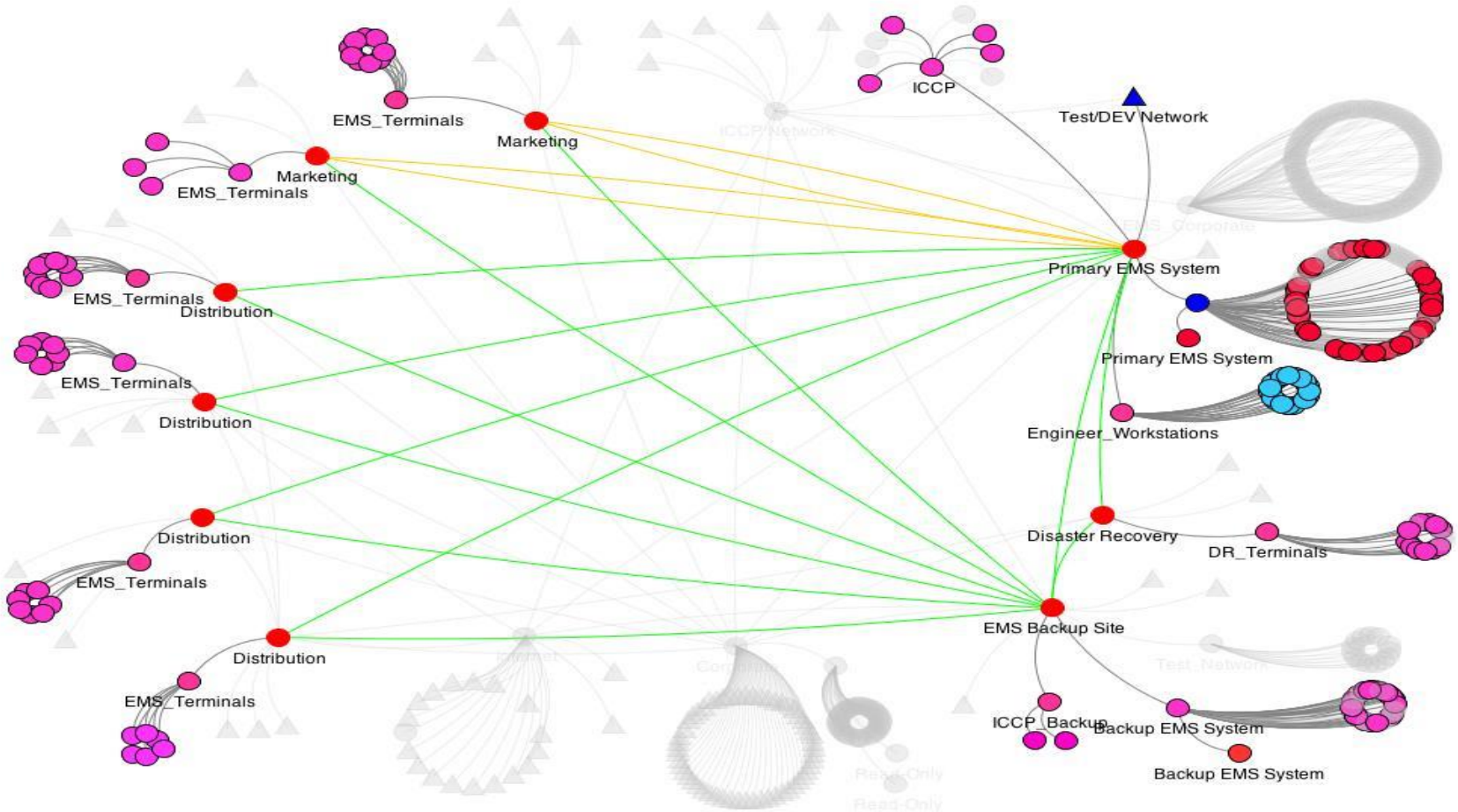



DEF CON 1

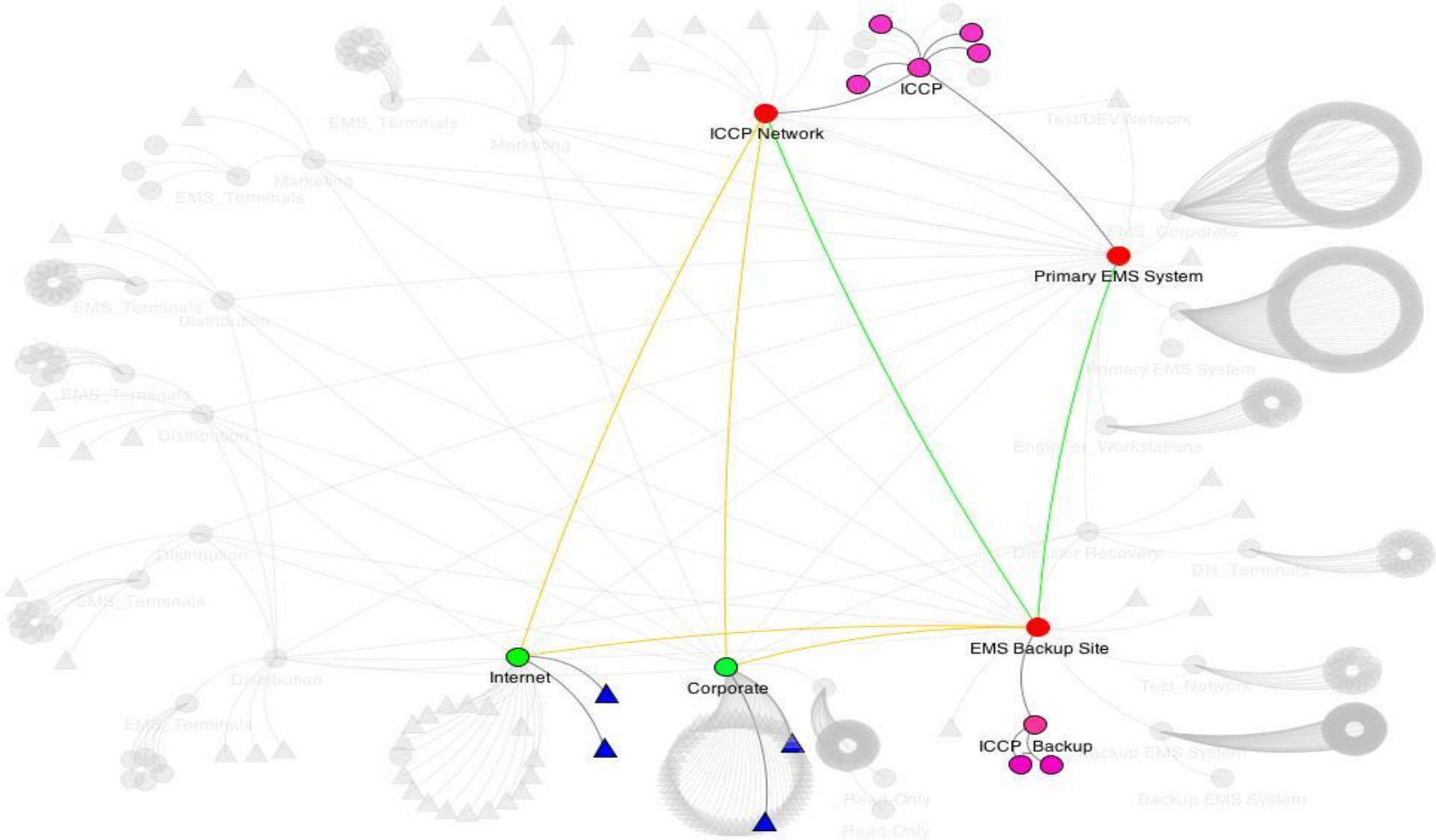
Example of an EMS network



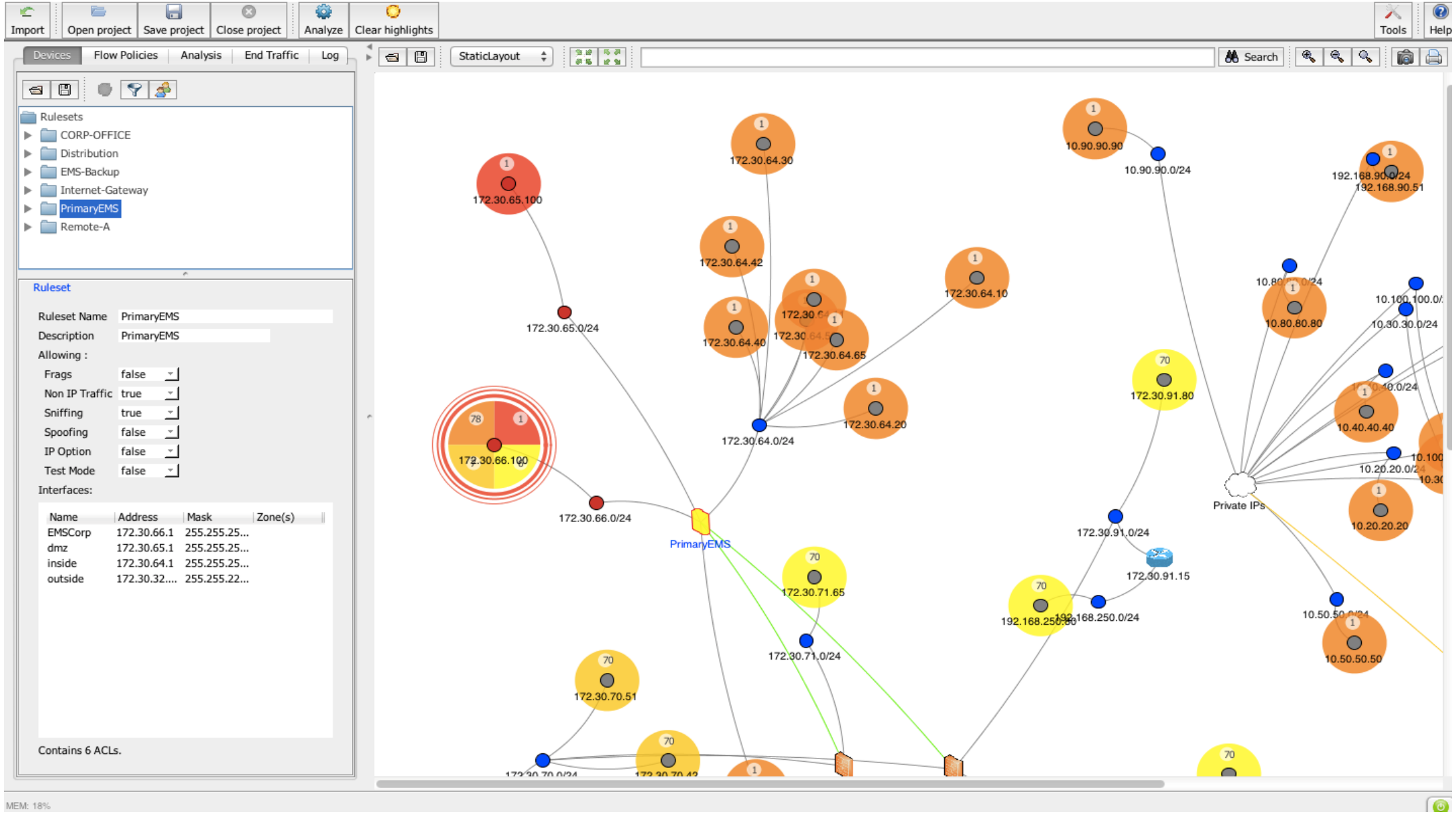
EMS Specific Traffic Highlighted

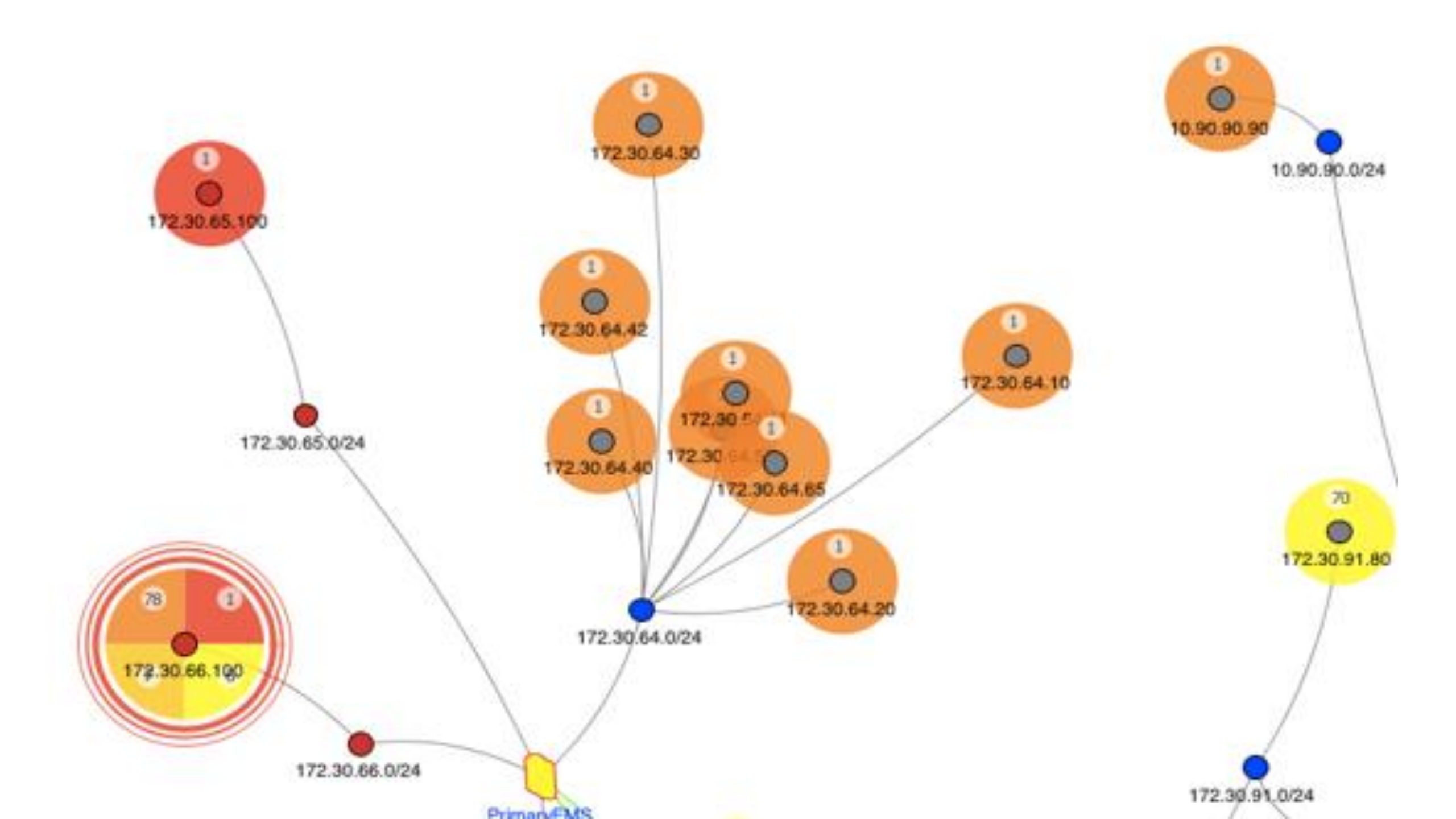


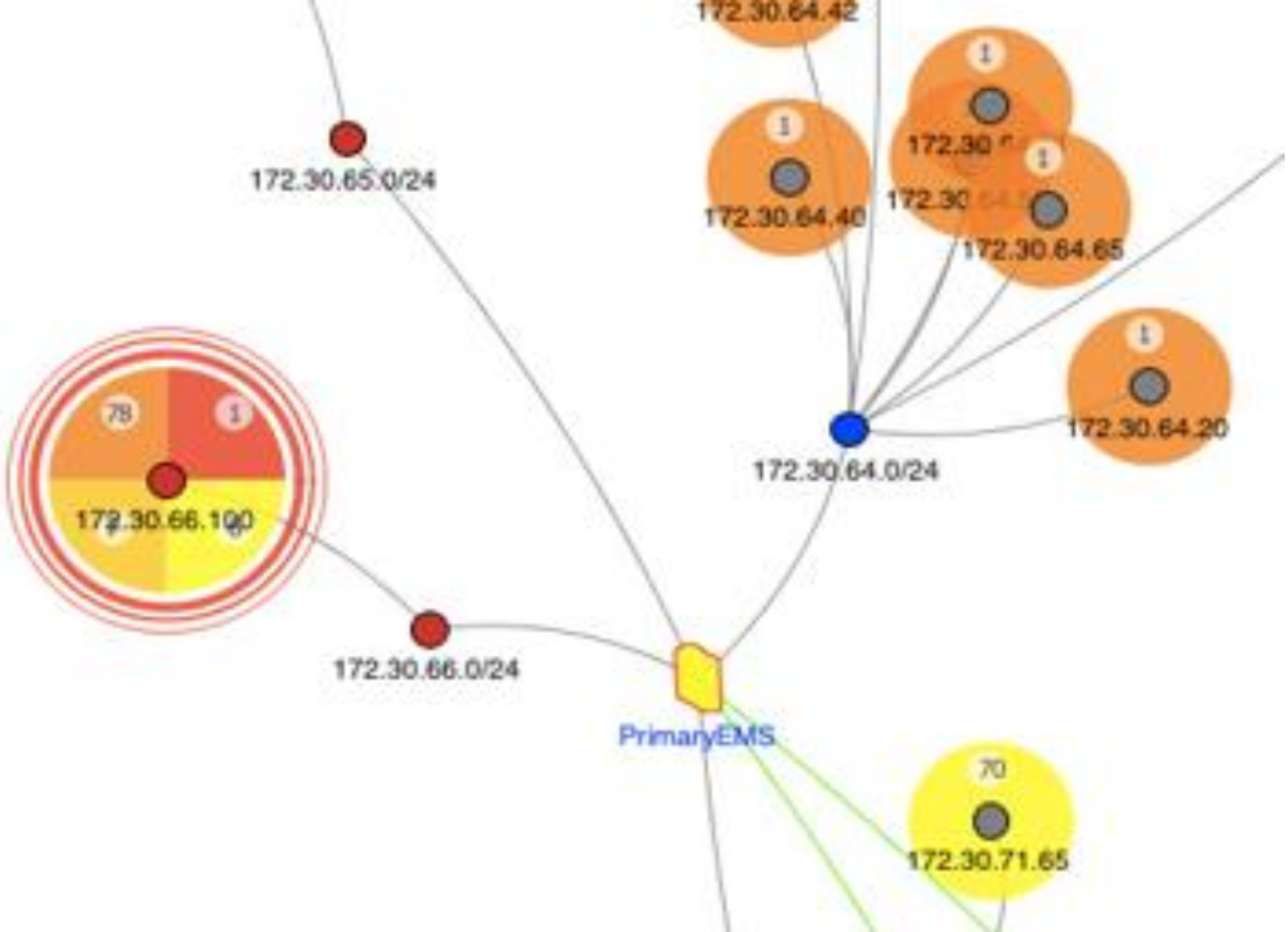
ICCP Traffic Highlighted

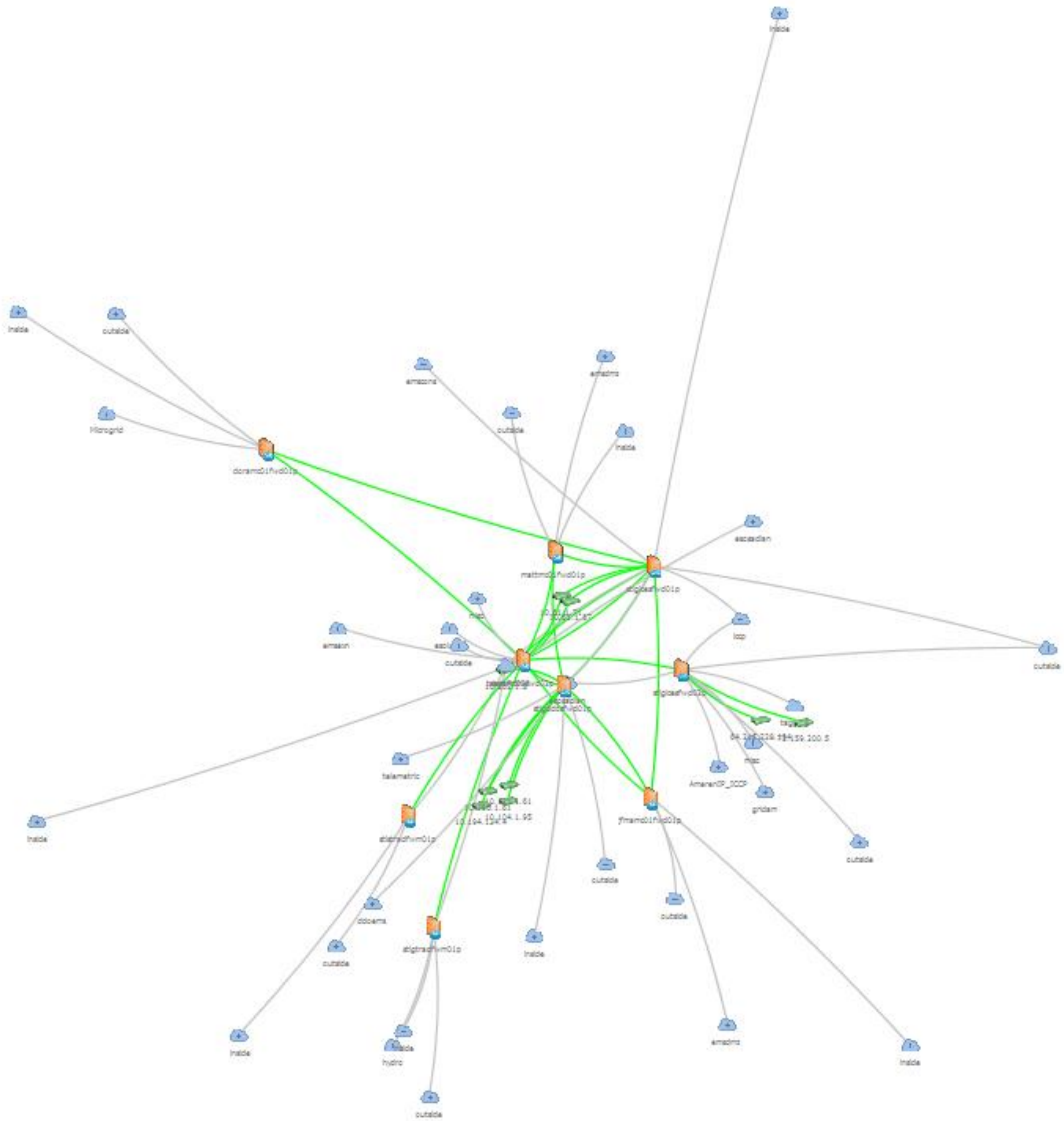


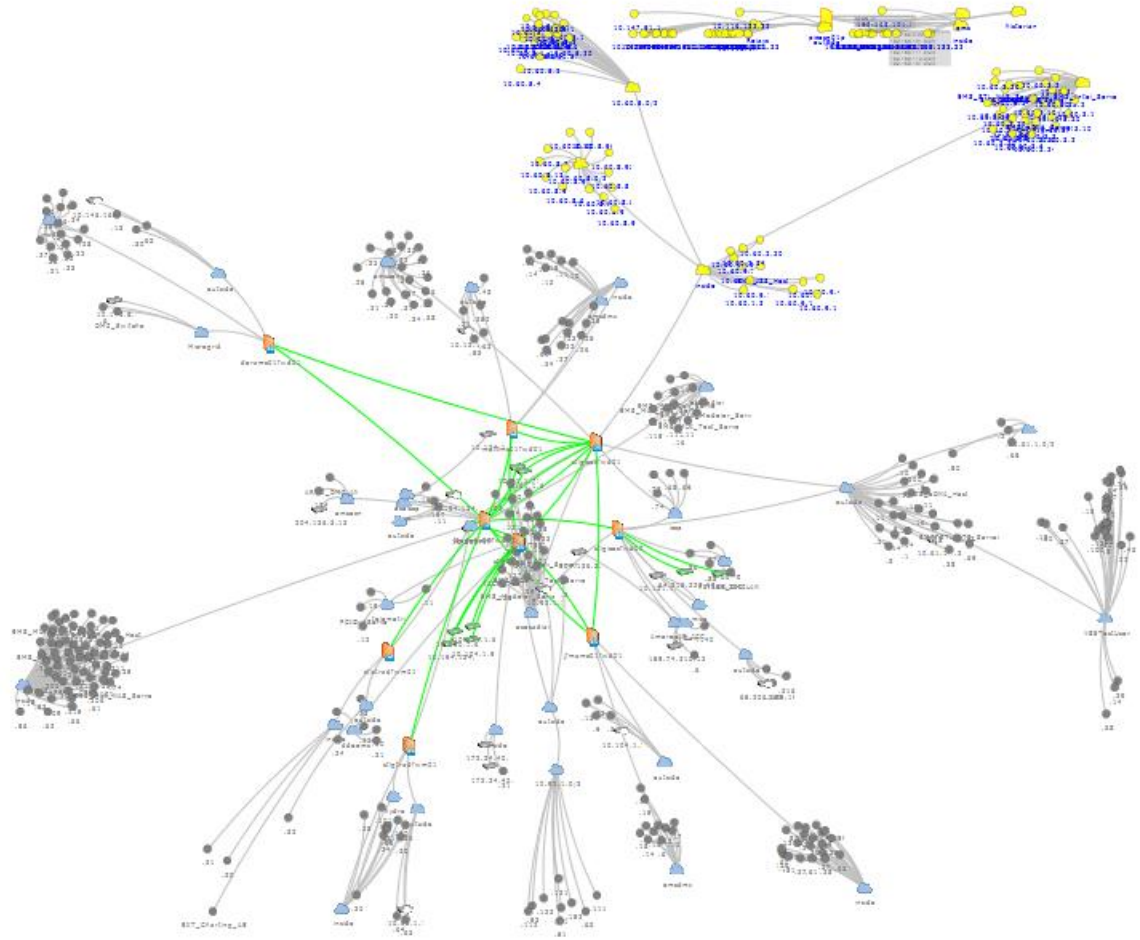
Review Attack Surface from Vulnerability Information

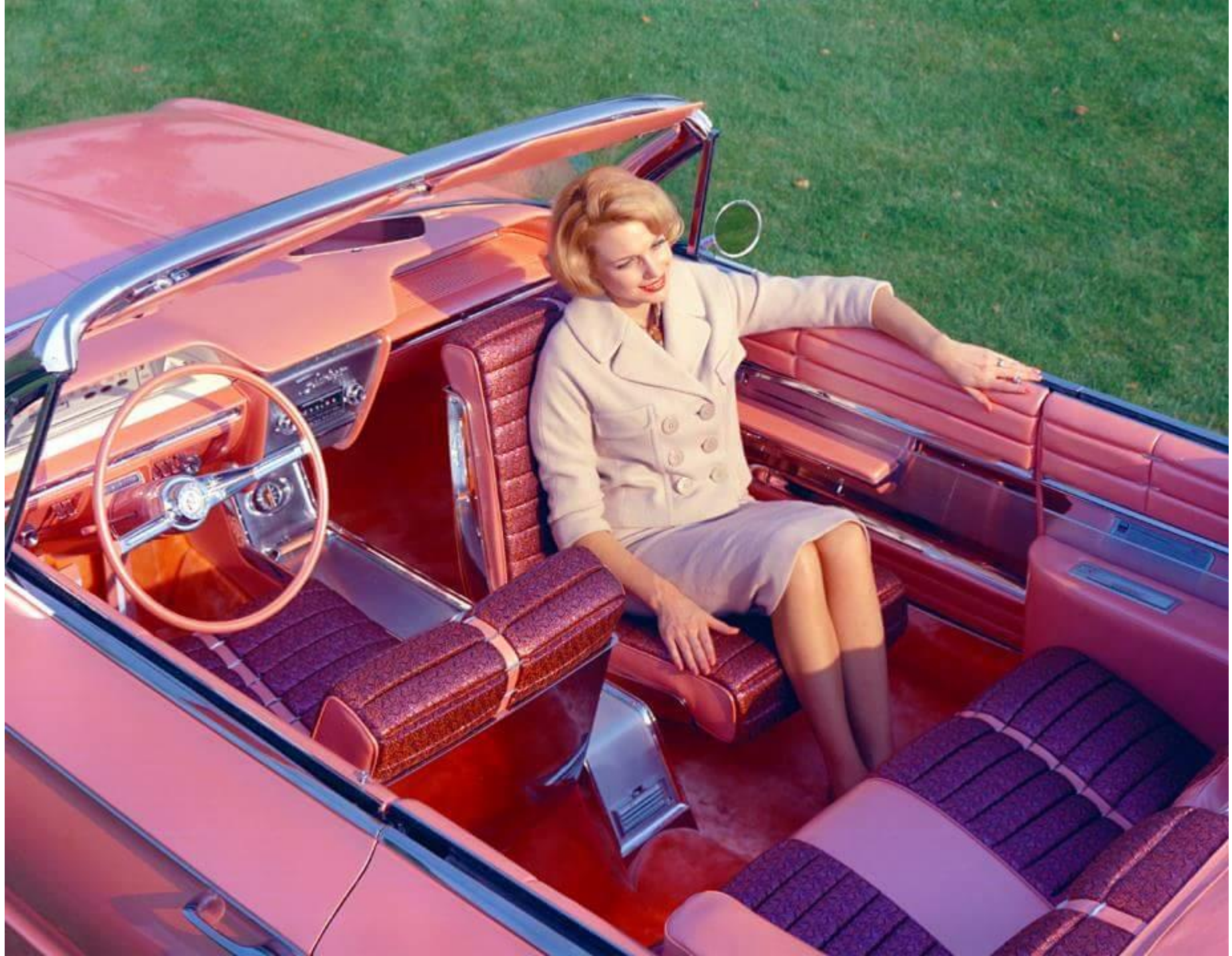


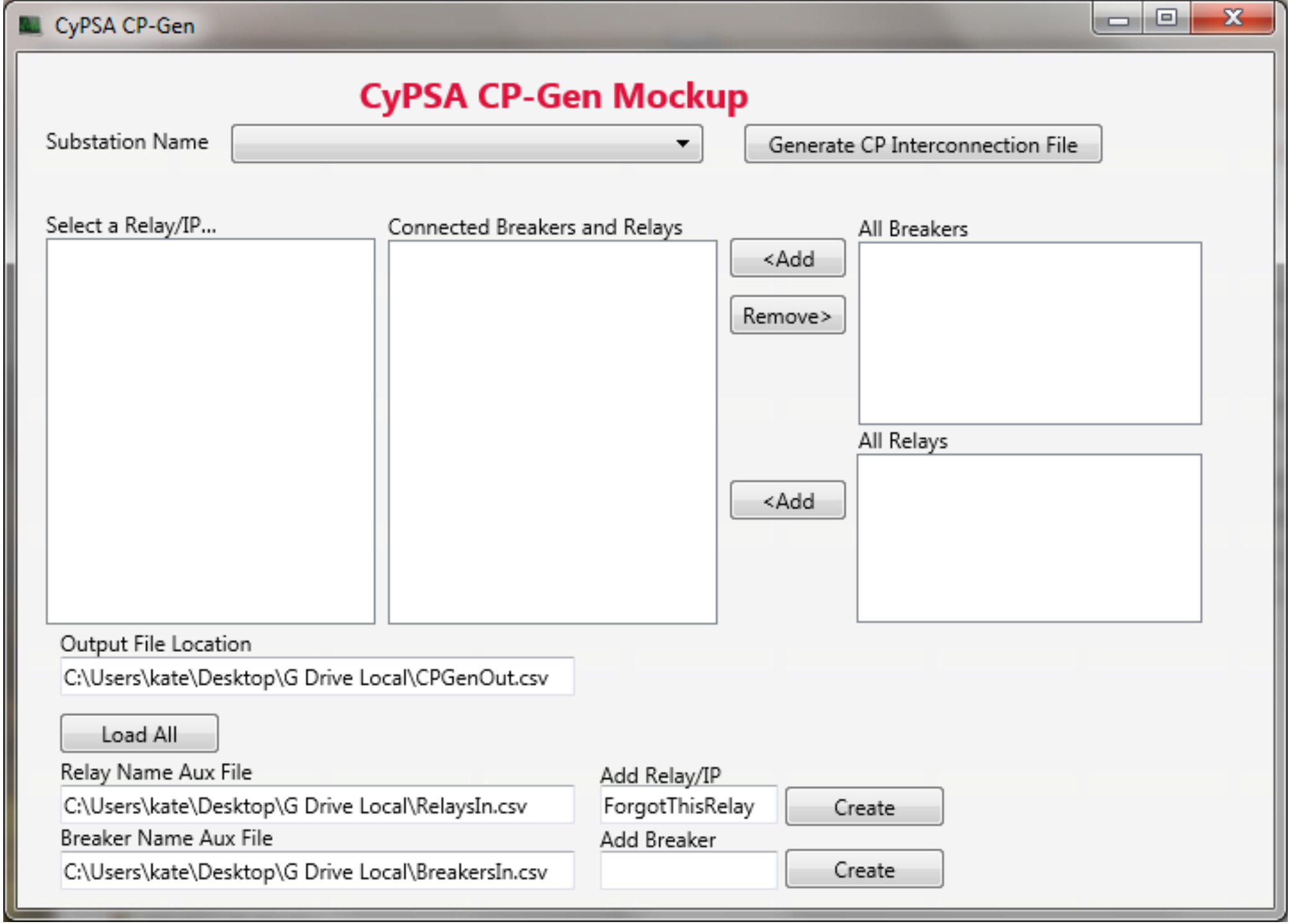

1
172.30.64.30
1
172.30.65.100
1
172.30.64.42
1
172.30.64.40
1
172.30.64.65
1
172.30.64.10
172.30.65.0/24
172.30.64.0/24
78
1
172.30.66.100
1
172.30.64.20
172.30.66.0/24
1
10.90.90.90
10.90.90.0/24
70
172.30.91.80
172.30.91.0/24


172.30.64.42
1
172.30.64.40
1
172.30.64.65
1
172.30.64.20
1
172.30.64.0/24
172.30.65.0/24
78
1
172.30.66.100
172.30.66.0/24
PrimaryEMS
70
172.30.71.65

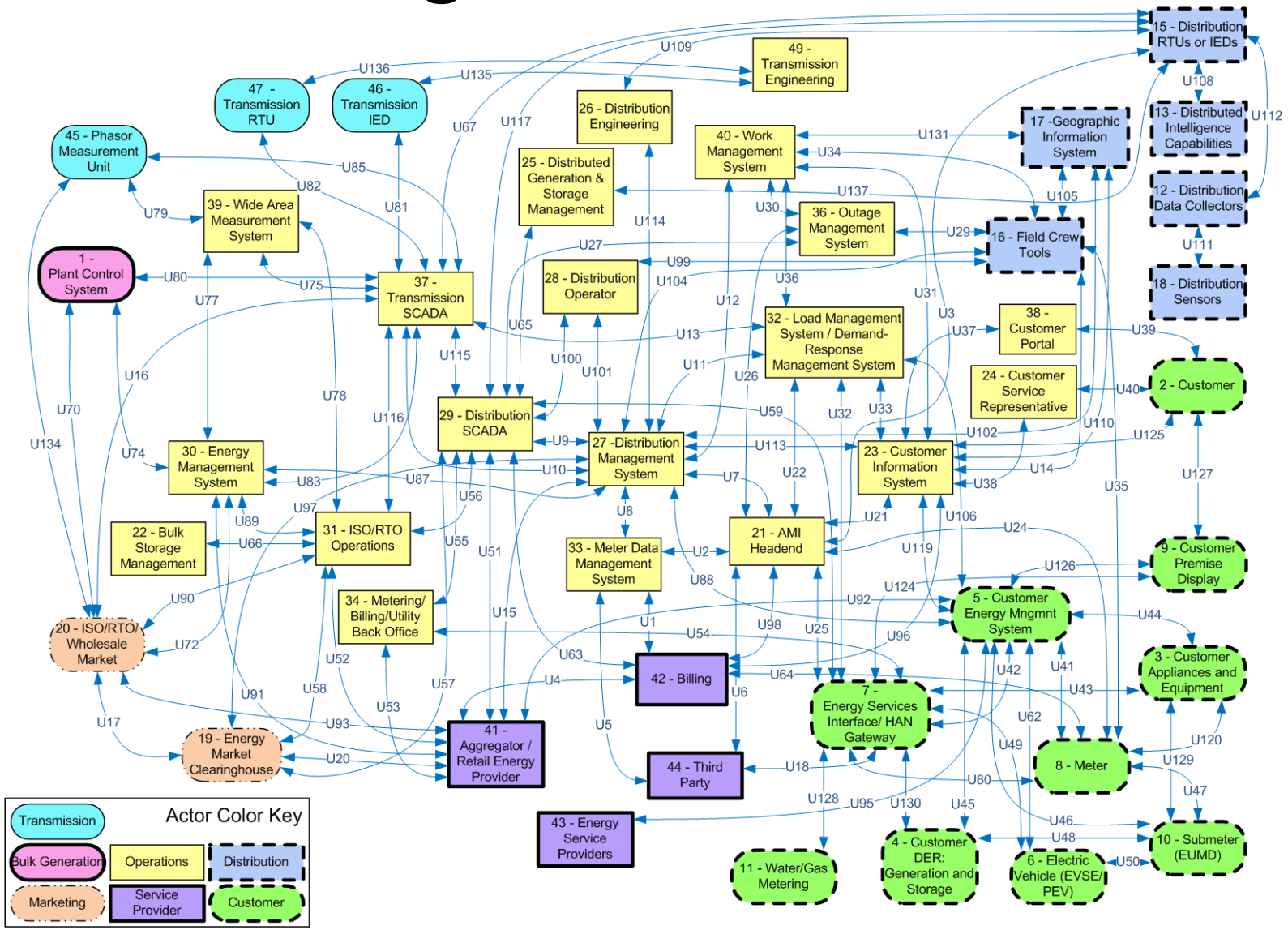




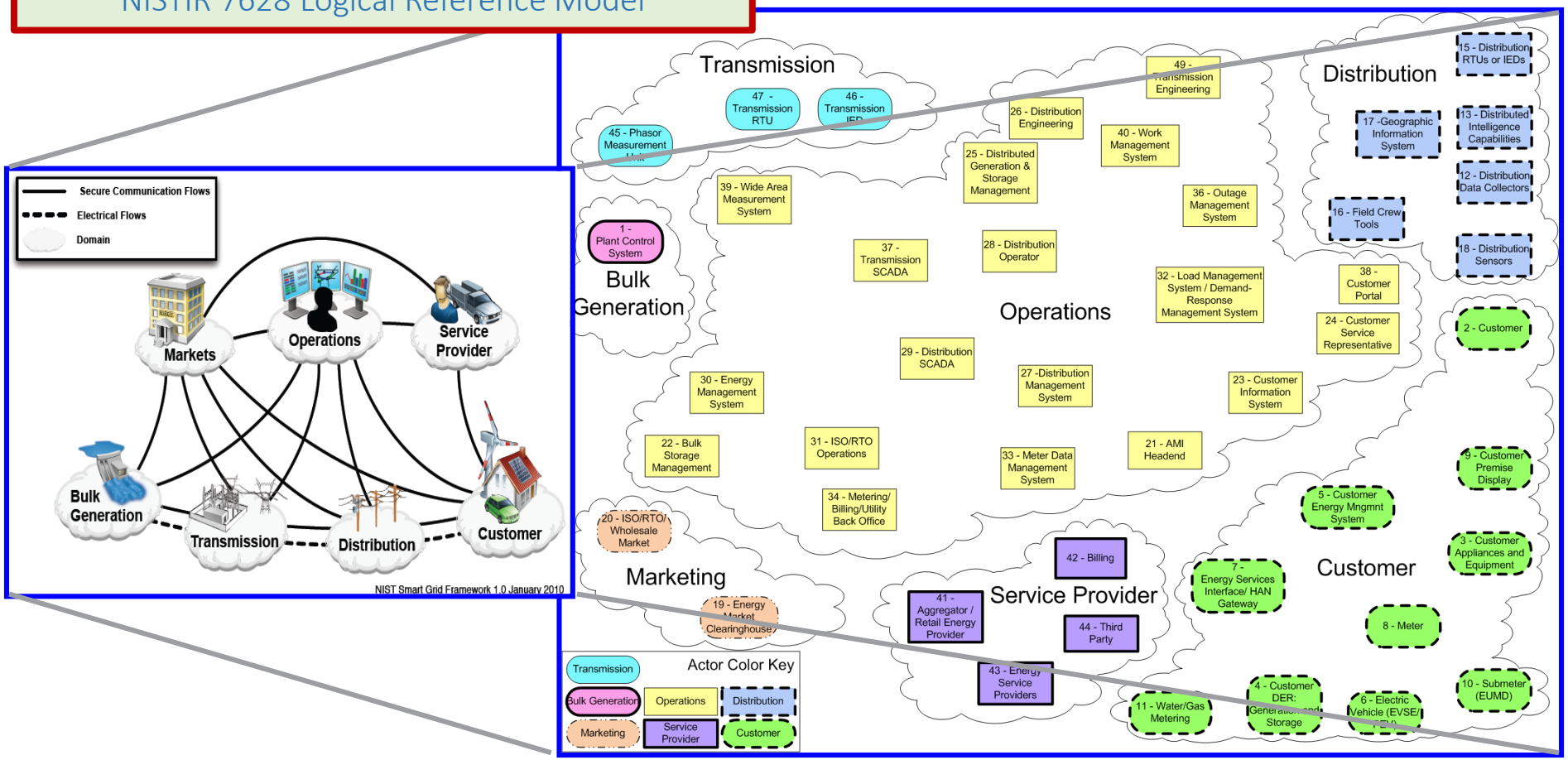



CyPSA CP-Gen
CyPSA CP-Gen Mockup
Substation Name
Generate CP Interconnection File
Select a Relay/IP...
Connected Breakers and Relays
<Add
Remove>
All Breakers
All Relays
<Add
Output File Location
C:\Users\kate\Desktop\G Drive Local\CPGenOut.csv
Load All
Relay Name Aux File
C:\Users\kate\Desktop\G Drive Local\RelaysIn.csv
Breaker Name Aux File
C:\Users\kate\Desktop\G Drive Local\BreakersIn.csv
Add Relay/IP
ForgotThisRelay
Create
Add Breaker
Create

NISTIR Logical reference Model



NISTIR 7628 Logical Reference Model

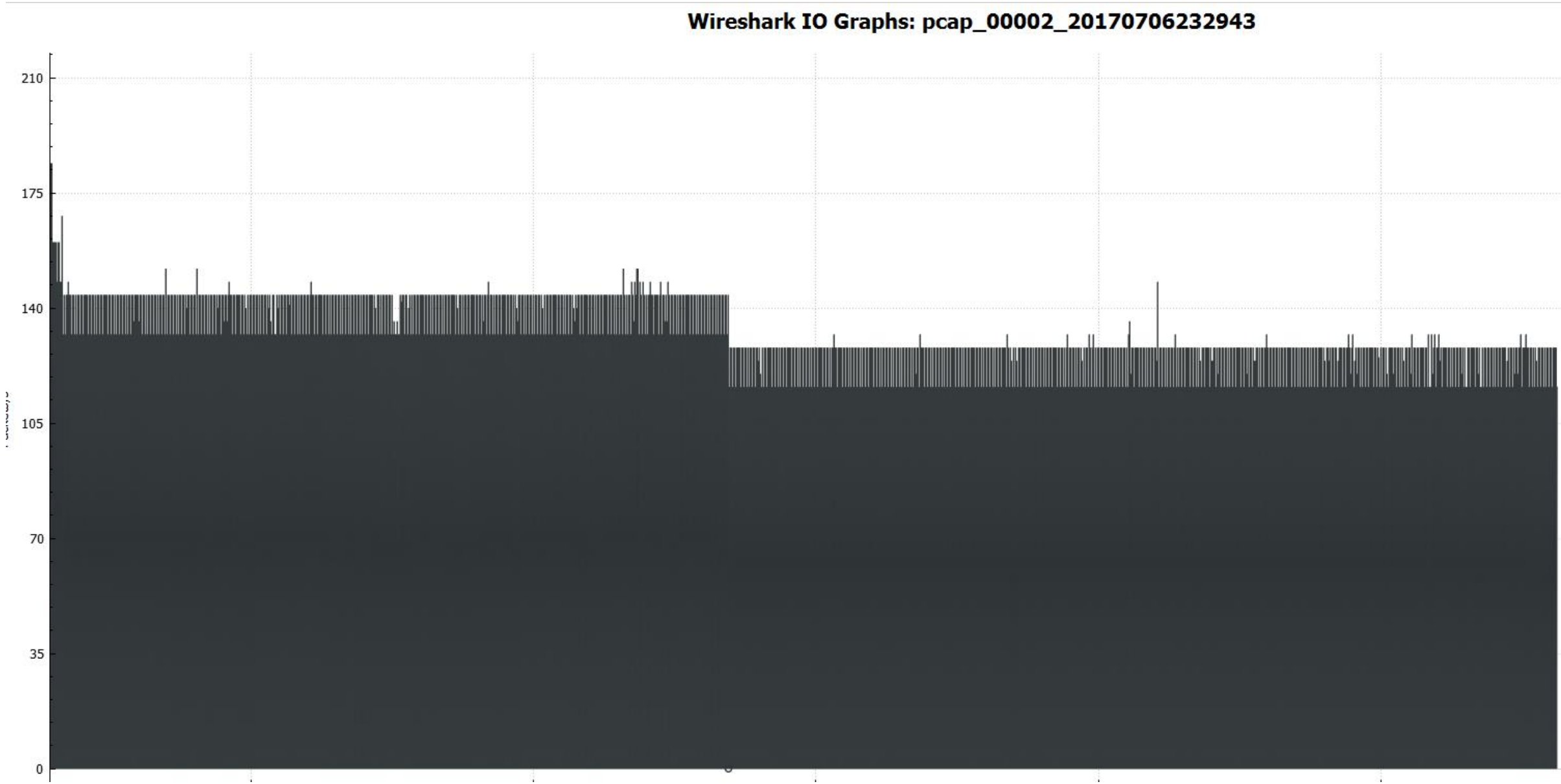


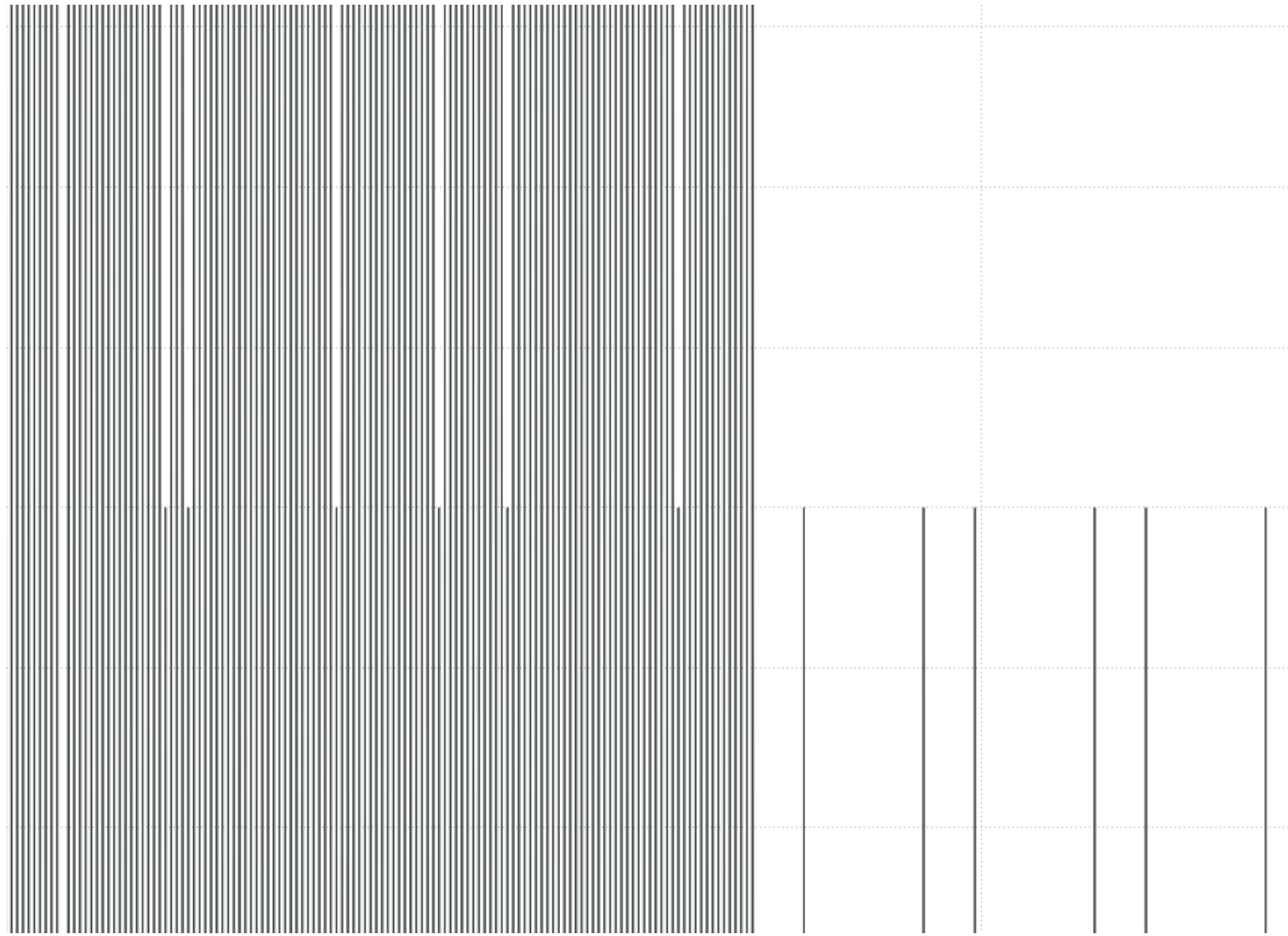
PURPOSE: "NISTIR 7628 presents an analytical framework to aid developing effective cyber security strategies tailored to organizationally unique combinations of Smart Grid-related characteristics, risks, and vulnerabilities."


Help Papa
Play
Back
demo
Hello Kitty
HAPPY HAPPY Family

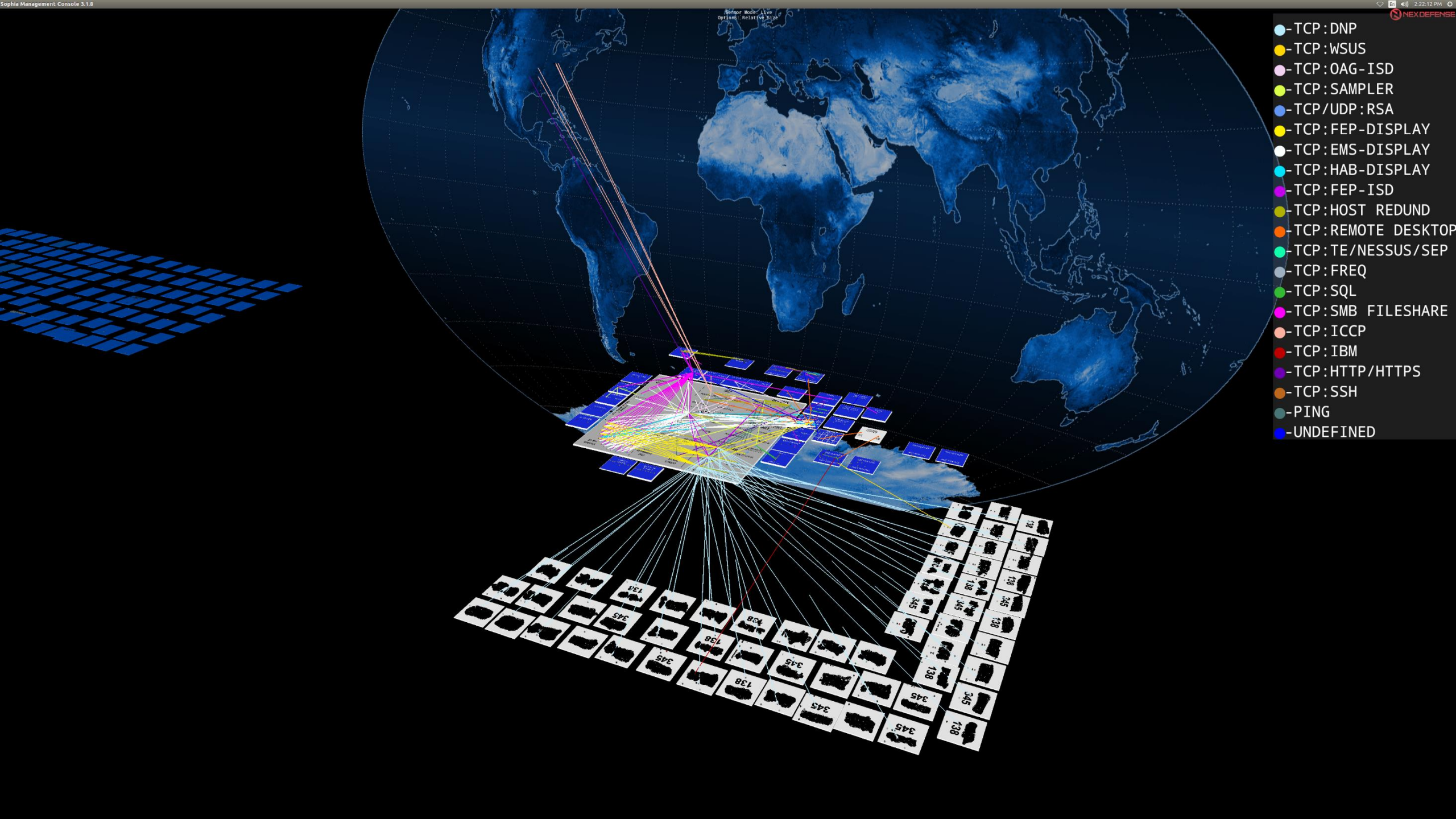
IPv4 · 14 | IPv6 | TCP · 29 | UDP

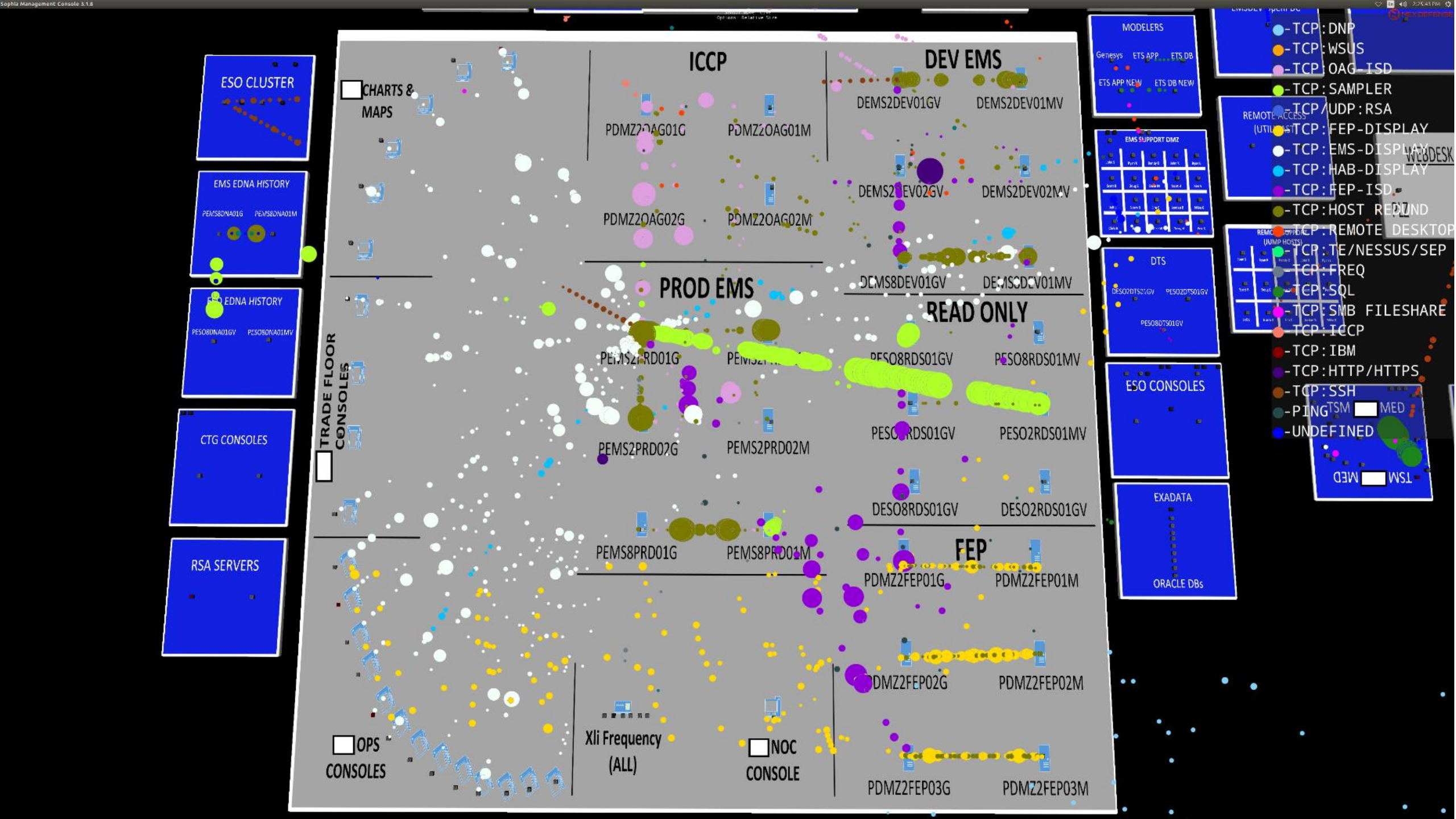
ort	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Co
64388	13,824	1228 k	6896	459 k	6928	769 k	-
55172	299,934	26 M	134914	9247 k	165020	17 M	-
63054	270,031	20 M	135003	8984 k	135028	11 M	-
51443	269,674	21 M	134944	8984 k	134730	12 M	-
61675	303,221	29 M	134865	8973 k	168356	20 M	-
50182	269,829	20 M	134788	8969 k	135041	11 M	-
55173	269,835	25 M	134893	8979 k	134942	16 M	-
65362	16,184	1308 k	8096	539 k	8088	768 k	-
51444	13,762	1224 k	6892	458 k	6870	765 k	-
61680	142,140	10 M	69820	4651 k	72320	5534 k	-
50422	141,646	11 M	69758	4690 k	71888	7297 k	-
51951	28	1696	16	968	12	728	-
51952	4	248	4	248	0	0	-
51954	116	8132	56	3724	60	4408	-
51959	114,909	10 M	57422	3824 k	57487	6388 k	-
54054	4	248	4	248	0	0	-
20000	16,184	1308 k	8088	768 k	8096	539 k	-
20000	13,762	1224 k	6870	765 k	6892	458 k	-
20000	141,646	11 M	71888	7297 k	69758	4690 k	-
20000	269,674	21 M	134730	12 M	134944	8984 k	-
20000	142,140	10 M	72320	5534 k	69820	4651 k	-
20000	4	248	0	0	4	248	-
20000	303,221	29 M	168356	20 M	134865	8973 k	-
20000	128,761	11 M	64427	7157 k	64334	4284 k	-
20000	269,829	20 M	135041	11 M	134788	8969 k	-
20000	120	8380	60	4408	60	3972	-
20000	270,031	20 M	135028	11 M	135003	8984 k	-
20000	269,835	25 M	134942	16 M	134893	8979 k	-
20000	299,934	26 M	165020	17 M	134914	9247 k	-

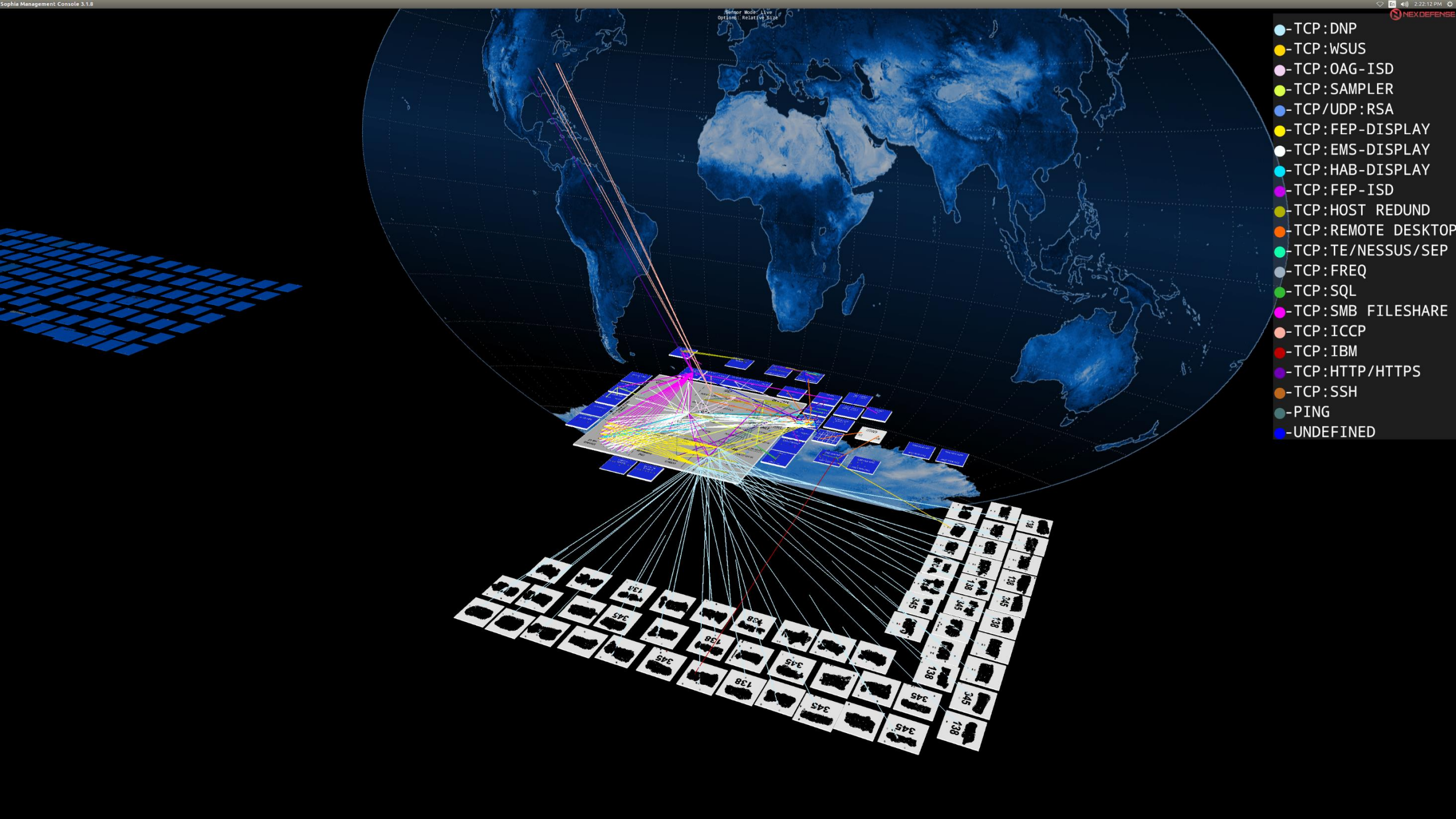

Wireshark IO Graphs: pcap_00002_20170706232943
210
175
140
105
70
35
0

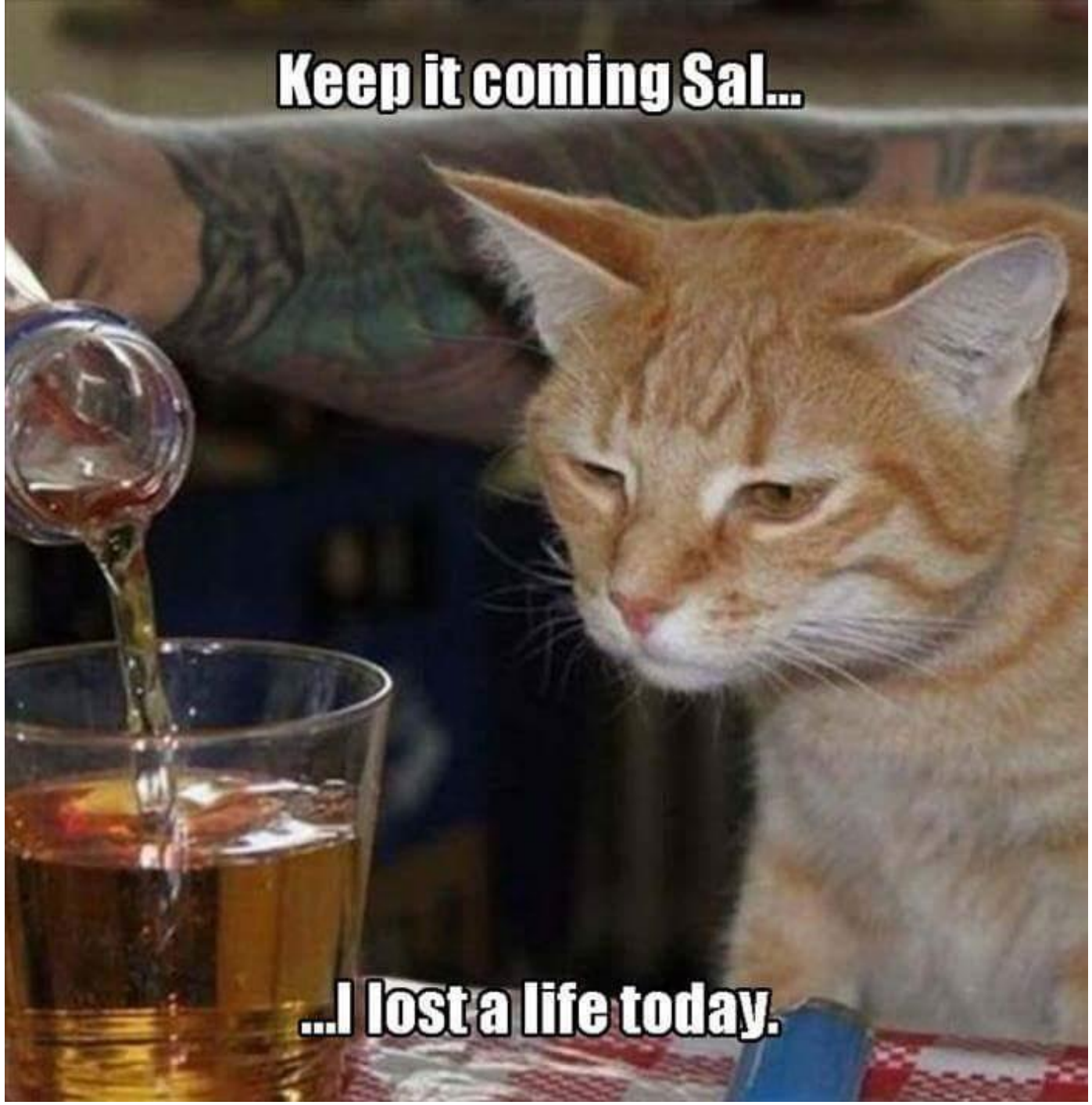



ENOUGH TALK
SHOW ME A
DEMO!!!


Sensor Mode: Live
Options: Relative Size
NEXDEFENSE
-TCP:DNP
-TCP:WSUS
-TCP:OAG-ISD
-TCP:SAMPLER
-TCP/UDP:RSA
-TCP:FEP-DISPLAY
-TCP:EMS-DISPLAY
-TCP:HAB-DISPLAY
-TCP:FEP-ISD
-TCP:HOST REDUND
-TCP:REMOTE DESKTOP
-TCP:TE/NESSUS/SEP
-TCP:FREQ
-TCP:SQL
-TCP:SMB FILESHARE
-TCP:ICCP
-TCP:IBM
-TCP:HTTP/HTTPS
-TCP:SSH
-PING
-UNDEFINED


ESO CLUSTER
EMS EDNA HISTORY
PEMS8DNA01G
PEMS8DNA01M
EDNA HISTORY
PESO8DNA01GV
PESO8DNA01MV
CTG CONSOLES
RSA SERVERS
CHARTS & MAPS
ICCP
PDMZ2OAG01G
PDMZ2OAG01M
PDMZ2OAG02G
PDMZ2OAG02M
DEV EMS
DEMS2DEV01GV
DEMS2DEV01MV
DEMS2DEV02GV
DEMS2DEV02MV
DEMS8DEV01GV
DEMS8DEV01MV
PROD EMS
READ ONLY
PEMS2PRD01G
PEMS2PRD02G
PEMS2PRD02M
PESO8RDS01GV
PESO8RDS01MV
PESO2RDS01GV
PESO2RDS01MV
DESO8RDS01GV
DESO2RDS01GV
TRADE FLOOR CONSOLES
PEMS8PRD01G
PEMS8PRD01M
FEP
PDMZ2FEP01G
PDMZ2FEP01M
PDMZ2FEP02G
PDMZ2FEP02M
PDMZ2FEP03G
PDMZ2FEP03M
OPS CONSOLES
Xli Frequency (ALL)
NOC CONSOLE
MODELERS
Genesys
ETS APP
ETS DB
ETS APP NEW
ETS DB NEW
EMS SUPPORT DMZ
DTS
DESO2DTS01GV
PESO2DTS01GV
PESO8DTS01GV
ESO CONSOLES
EXADATA
ORACLE DBs
REMOTE ACCESS (UTILITY)
REMOTE SUPPORT (JUMP HOSTS)
TSM
MED
-TCP:DNP
-TCP:WSUS
-TCP:OAG-ISD
-TCP:SAMPLER
-TCP/UDP:RSA
-TCP:FEP-DISPLAY
-TCP:EMS-DISPLAY
-TCP:HAB-DISPLAY
-TCP:FEP-ISD
-TCP:HOST REDUND
-TCP:REMOTE DESKTOP
-TCP:TE/NESSUS/SEP
-TCP:FREQ
-TCP:SQL
-TCP:SMB FILESHARE
-TCP:ICCP
-TCP:IBM
-TCP:HTTP/HTTPS
-TCP:SSH
-PING
-UNDEFINED


Sensor Mode: Live
Options: Relative Size
NEXDEFENSE
-TCP:DNP
-TCP:WSUS
-TCP:OAG-ISD
-TCP:SAMPLER
-TCP/UDP:RSA
-TCP:FEP-DISPLAY
-TCP:EMS-DISPLAY
-TCP:HAB-DISPLAY
-TCP:FEP-ISD
-TCP:HOST REDUND
-TCP:REMOTE DESKTOP
-TCP:TE/NESSUS/SEP
-TCP:FREQ
-TCP:SQL
-TCP:SMB FILESHARE
-TCP:ICCP
-TCP:IBM
-TCP:HTTP/HTTPS
-TCP:SSH
-PING
-UNDEFINED


Keep it coming Sal...
...I lost a life today.