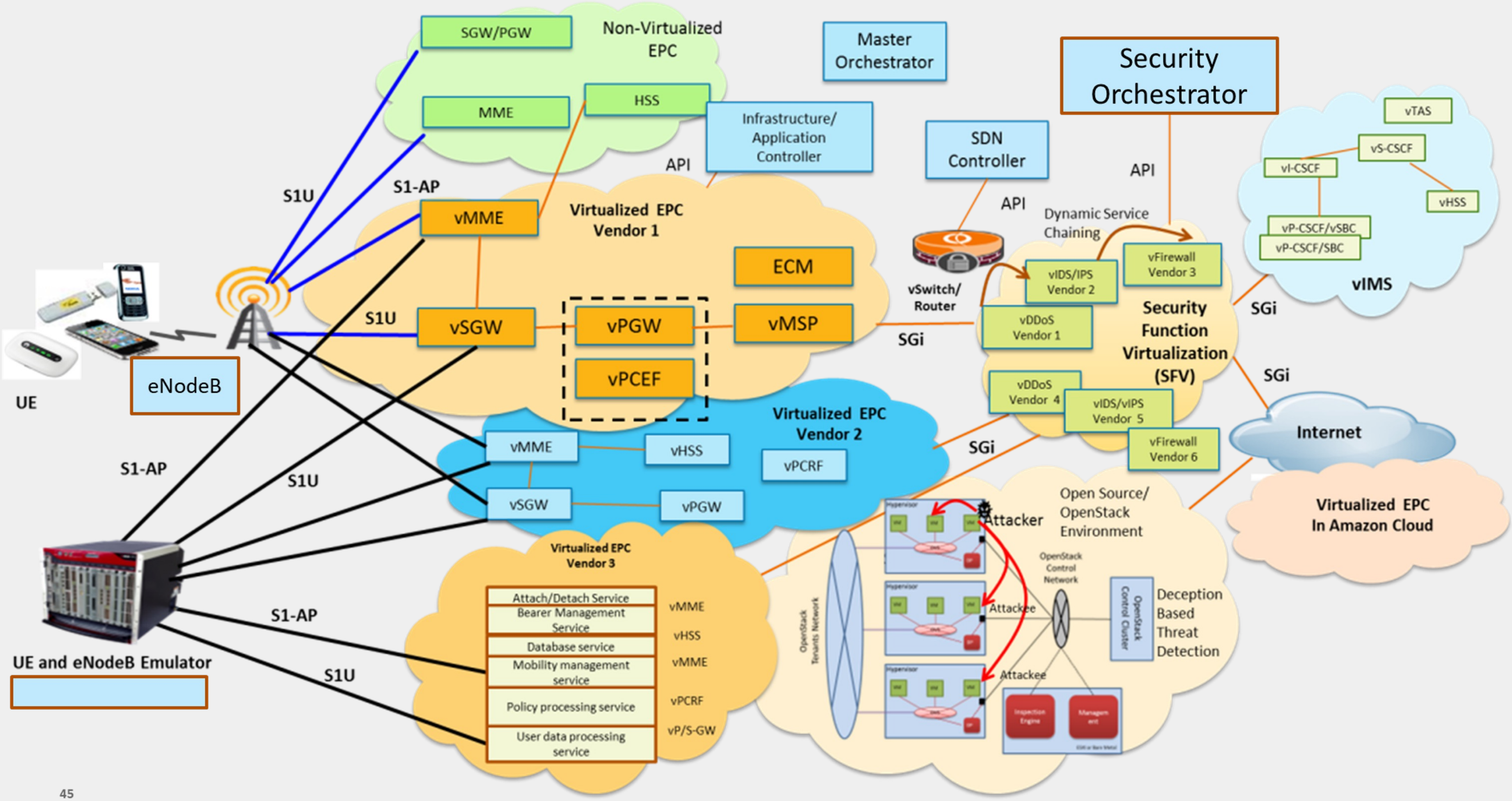
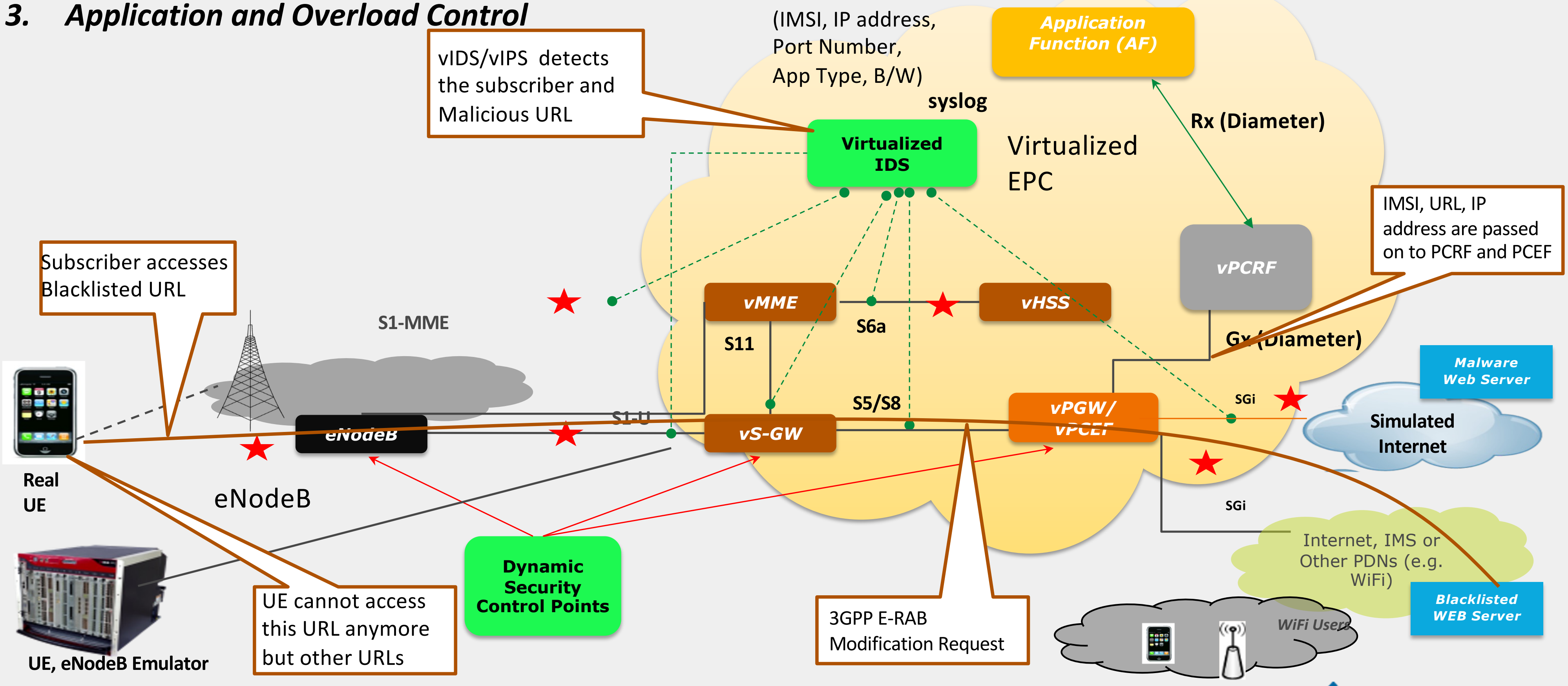
Sample Open Source Testbed



Virtual IDS Prototype for Mobility CORE

1. ***Malicious URL Detection and Mitigation***
2. ***Malware Detection and Mitigation***
3. ***Application and Overload Control***



vIDS/vIPS detects the subscriber and Malicious URL

Subscriber accesses Blacklisted URL

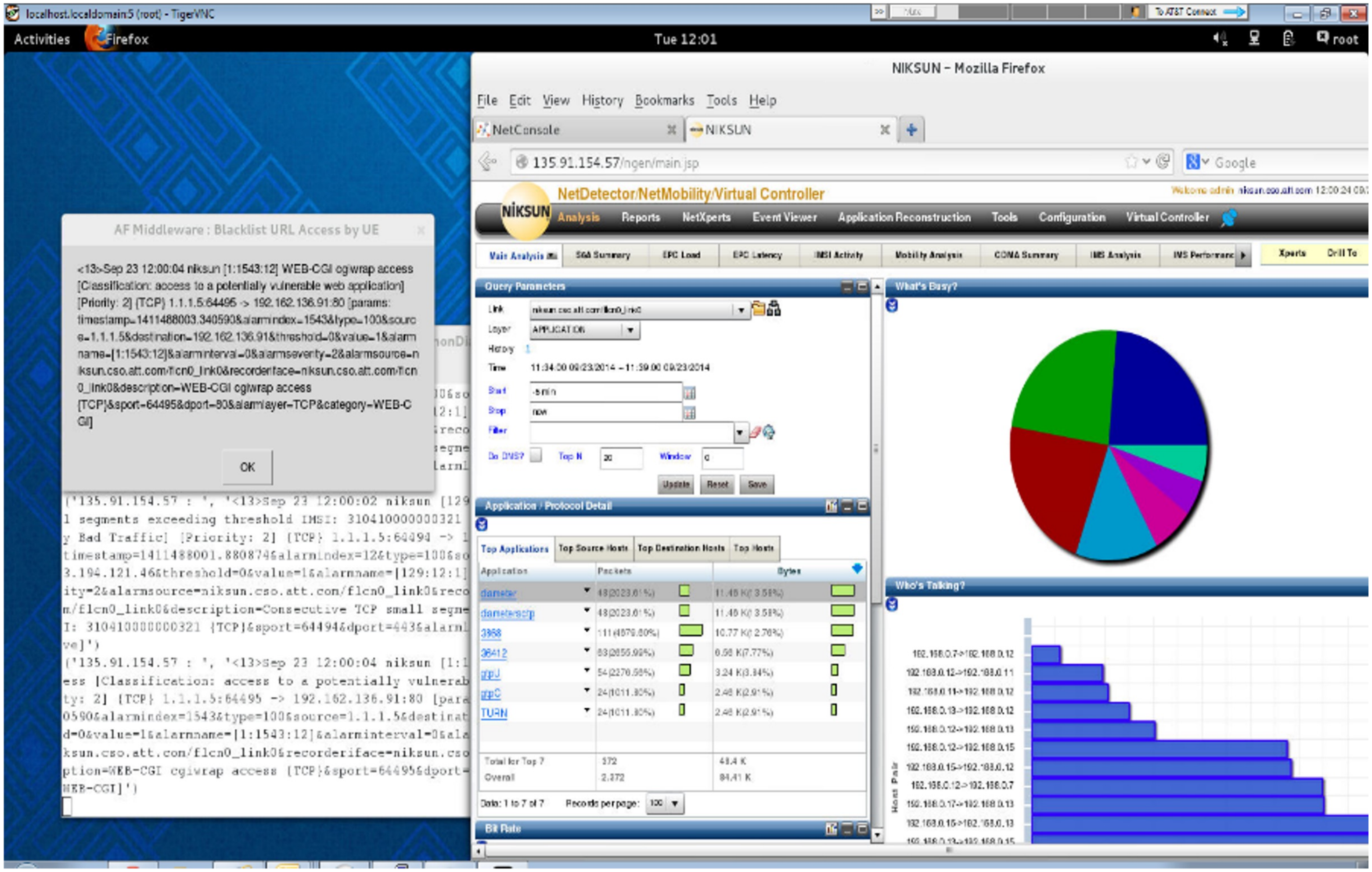
UE cannot access this URL anymore but other URLs

3GPP E-RAB Modification Request

IMSI, URL, IP address are passed on to PCRF and PCEF

(IMSI, IP address, Port Number, App Type, B/W)

Blacklisted URL Detection and Mitigation



AF Middleware : Blacklist URL Access by UE

```
<13>Sep 23 12:00:04 niksun [1:1543:12] WEB-CGI cgiwrap access
[Classification: access to a potentially vulnerable web application]
[Priority: 2] {TCP} 1.1.1.5:64495 -> 192.162.136.91:80 [params:
timestamp=1411488003.340590&alarmindex=1543&type=100&sourc
e=1.1.1.5&destination=192.162.136.91&threshold=0&value=1&alarm
name=[1:1543:12]&alarminterval=0&alarmseverity=2&alarmsource=n
iksun.cso.att.com/flcn0_link0&recorderiface=niksun.cso.att.com/flcn
0_link0&description=WEB-CGI cgiwrap access
{TCP}&sport=64495&dport=80&alarmlayer=TCP&category=WEB-C
GI]
```

OK

```
('135.91.154.57 : ', '<13>Sep 23 12:00:02 niksun [129
l segments exceeding threshold IMSI: 310410000000321
y Bad Traffic] [Priority: 2] {TCP} 1.1.1.5:64494 -> 1
timestamp=1411488001.880874&alarmindex=12&type=100&so
3.194.121.46&threshold=0&value=1&alarmname=[129:12:1]
ity=2&alarmsource=niksun.cso.att.com/flcn0_link0&reco
m/flcn0_link0&description=Consecutive TCP small segme
I: 310410000000321 {TCP}&sport=64494&dport=443&alarml
ve]')
('135.91.154.57 : ', '<13>Sep 23 12:00:04 niksun [1:1
ess [Classification: access to a potentially vulnerab
ty: 2] {TCP} 1.1.1.5:64495 -> 192.162.136.91:80 [para
0590&alarmindex=1543&type=100&source=1.1.1.5&destinat
d=0&value=1&alarmname=[1:1543:12]&alarminterval=0&ala
ksun.cso.att.com/flcn0_link0&recorderiface=niksun.cso
ption=WEB-CGI cgiwrap access {TCP}&sport=64495&dport=
WEB-CGI]')
```

Query Parameters

Link: niksun.cso.att.com/flcn0_link0
Layer: APPLICATION
History: 1
Time: 11:34:00 09/23/2014 – 11:39:00 09/23/2014
Start: -5min
Stop: now
Filter:
Do DNS? □ Top N: 20 Window: 0

Update Reset Save

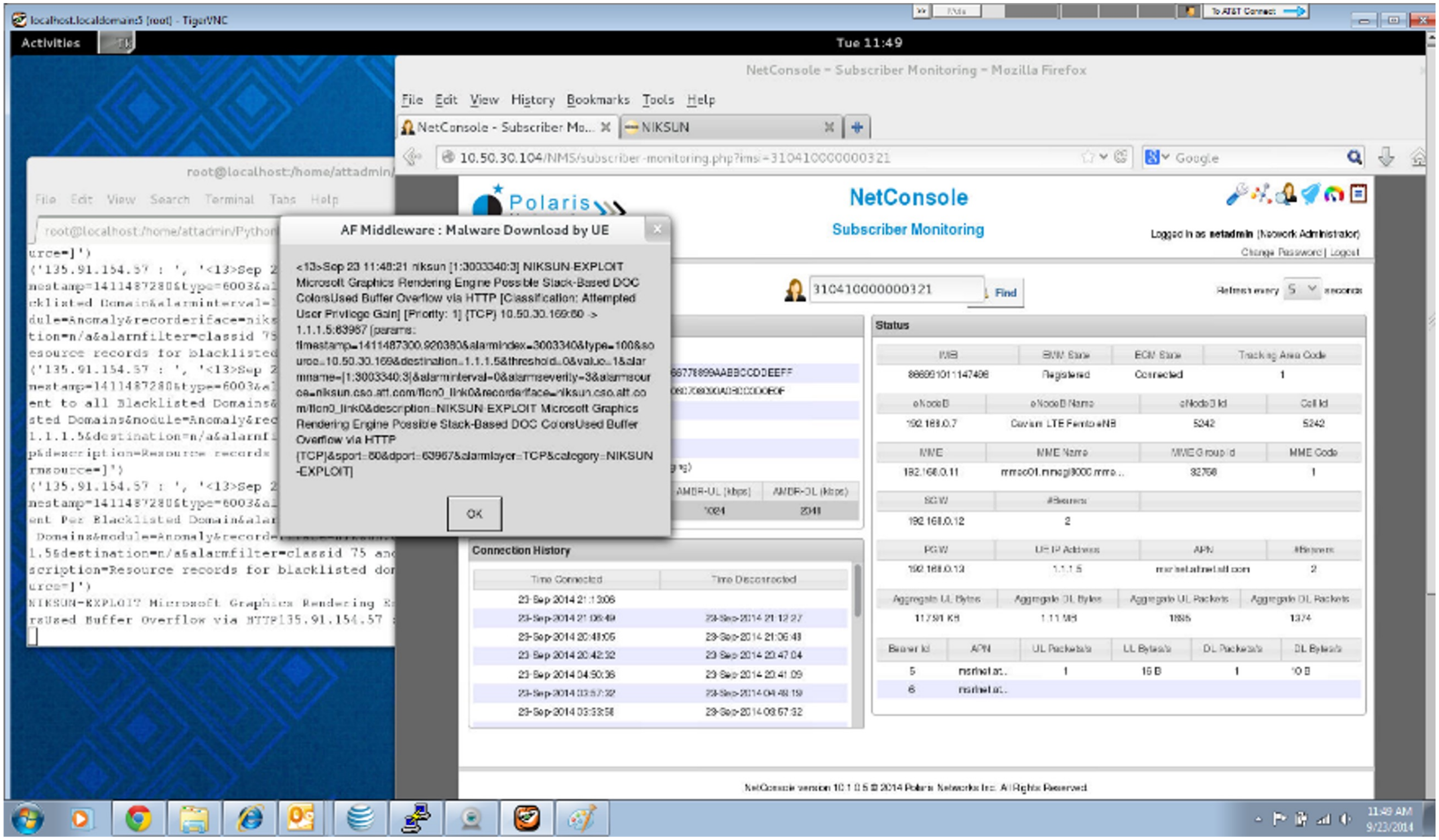
Application / Protocol Detail

Top Applications | Top Source Hosts | Top Destination Hosts | Top Hosts

Application	Packets		Bytes	
diameter	48(2023.61%)	🟩	11.48 K(3.58%)	🟩
diametersctp	48(2023.61%)	🟩	11.48 K(3.58%)	🟩
3868	111(4679.60%)	🟩	10.77 K(2.78%)	🟩
36412	63(2655.99%)	🟩	6.56 K(7.77%)	🟩
gtpU	54(2276.58%)	🟩	3.24 K(3.84%)	🟩
gtpC	24(1011.80%)	🟩	2.46 K(2.91%)	🟩
TURN	24(1011.80%)	🟩	2.46 K(2.91%)	🟩
Total for Top 7	372		48.4 K	
Overall	2,372		84.41 K	

Data: 1 to 7 of 7 Records per page: 100

Malware Detection and Mitigation


localhost.localdomain5 [root] - TigerVNC
Activities
Tue 11:49
NetConsole - Subscriber Monitoring - Mozilla Firefox
File Edit View History Bookmarks Tools Help
NetConsole - Subscriber Mo...
NIKSUN
10.50.30.104/NMS/subscriber-monitoring.php?imsi=310410000000321
Google
Polaris
NetConsole
Subscriber Monitoring
Logged in as netadmin (Network Administrator)
Change Password | Logout
310410000000321
Find
Refresh every 5 seconds
root@localhost:/home/attadmin/
File Edit View Search Terminal Tabs Help
root@localhost:/home/attadmin/Python
OK
11:49 AM
9/23/2014

```
urce=]')
('135.91.154.57 : ', '<13>Sep 2
mestamp=1411487280&type=6003&a
cklisted Domain&alarminterval=1
dule=Anomaly&recorderiface=niks
tion=n/a&alarmfilter=classid 75
esource records for blacklisted
('135.91.154.57 : ', '<13>Sep 2
mestamp=1411487280&type=6003&a
ent to all Blacklisted Domains&
sted Domains&module=Anomaly&rec
1.1.1.5&destination=n/a&alarmfi
p&description=Resource records
rmsource=]')
('135.91.154.57 : ', '<13>Sep 2
mestamp=1411487280&type=6003&a
ent Per Blacklisted Domain&alar
 Domains&module=Anomaly&recorde
1.5&destination=n/a&alarmfilter=classid 75 and
scription=Resource records for blacklisted dom
urce=]')
NIKSUN-EXPLOIT Microsoft Graphics Rendering E
rsUsed Buffer Overflow via HTTP135.91.154.57 :
```

AF Middleware : Malware Download by UE

```
<13>Sep 23 11:48:21 niksun [1:3003340:3] NIKSUN-EXPLOIT
Microsoft Graphics Rendering Engine Possible Stack-Based DOC
ColorsUsed Buffer Overflow via HTTP [Classification: Attempted
User Privilege Gain] [Priority: 1] {TCP} 10.50.30.169:80 ->
1.1.1.5:63967 [params:
timestamp=1411487300.920380&alarmindex=3003340&type=100&so
urce=10.50.30.169&destination=1.1.1.5&threshold=0&value=1&alar
mname=[1:3003340:3]&alarminterval=0&alarmseverity=3&alarmsour
ce=niksun.cso.att.com/flon0_link0&recorderiface=niksun.cso.att.co
m/flon0_link0&description=NIKSUN-EXPLOIT Microsoft Graphics
Rendering Engine Possible Stack-Based DOC ColorsUsed Buffer
Overflow via HTTP
[TCP]&sport=80&dport=63967&alarmlayer=TCP&category=NIKSUN
-EXPLOIT]
```

AMBR-UL (kbps)	AMBR-DL (kbps)
1024	2048

Connection History

Time Connected	Time Disconnected
23-Sep-2014 21:13:06	
23-Sep-2014 21:08:49	23-Sep-2014 21:12:27
23-Sep-2014 20:48:05	23-Sep-2014 21:06:48
23-Sep-2014 20:42:32	23-Sep-2014 20:47:04
23-Sep-2014 04:50:36	23-Sep-2014 20:41:09
23-Sep-2014 03:57:32	23-Sep-2014 04:48:19
23-Sep-2014 03:33:58	23-Sep-2014 03:57:32

Status

IMEI	EMM State	ECM State	Tracking Area Code
866691011147408	Registered	Connected	1

eNodeB	eNodeB Name	eNodeB Id	Cell Id
192.168.0.7	Cavium LTE Femto eNB	5242	5242

MME	MME Name	MME Group Id	MME Code
192.168.0.11	mmec01.mmegi8000.mme...	32768	1

SGW	#Bearers	
192.168.0.12	2	

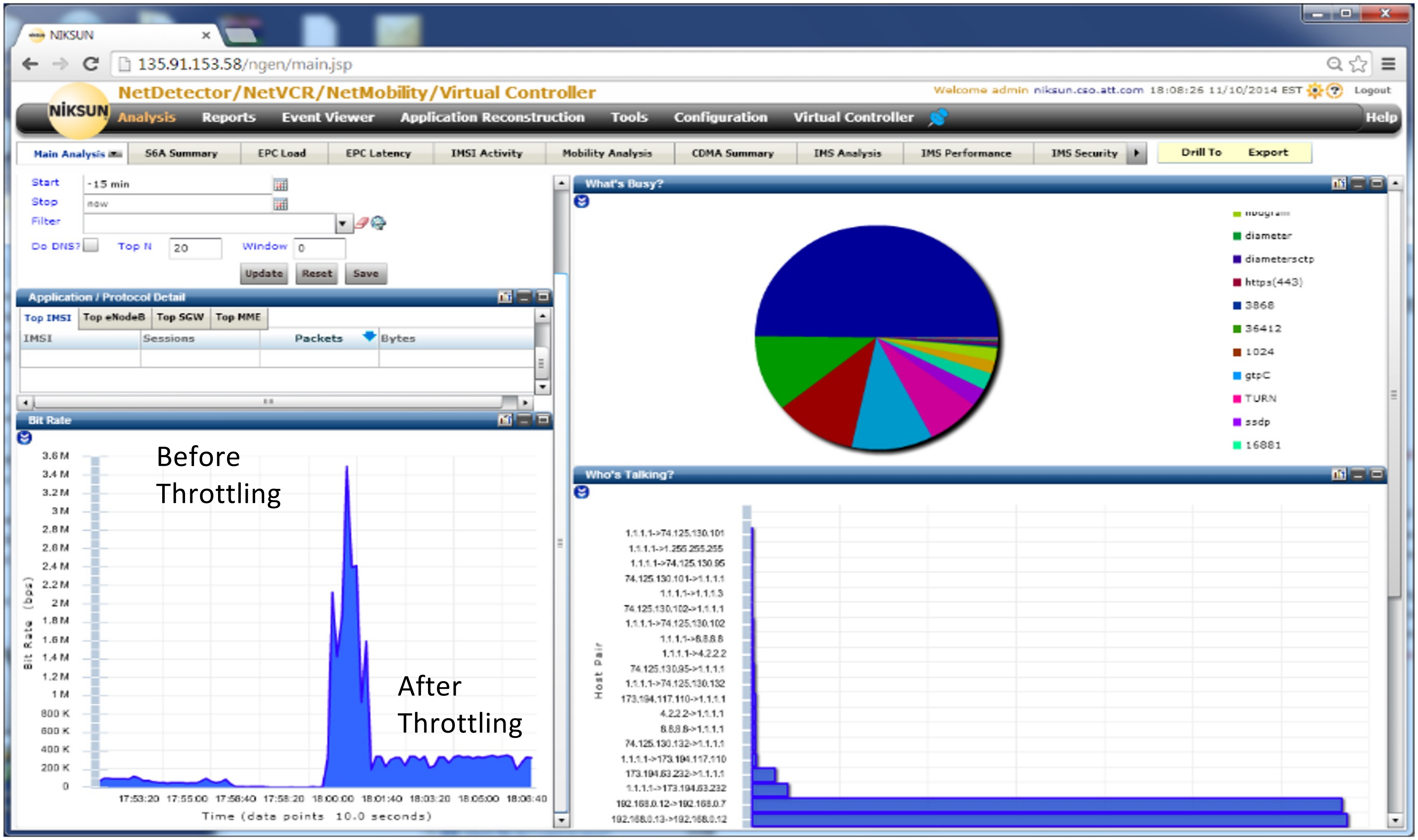
PGW	UE IP Address	APN	#Bearers
192.168.0.13	1.1.1.5	marketatnet.att.com	2

Aggregate UL Bytes	Aggregate DL Bytes	Aggregate UL Packets	Aggregate DL Packets
117.91 KB	1.11 MB	1885	1374

Bearer Id	APN	UL Packets/s	UL Bytes/s	DL Packets/s	DL Bytes/s
5	nsrhet.at...	1	16 B	1	10 B
6	nsrhet.at...				

NetConsole version 10.1.0.5 © 2014 Polaris Networks Inc. All Rights Reserved.

Bandwidth Overload Detection and Mitigation



Start: -15 min

Stop: now

Filter:

Do DNS? □ Top N: 20 Window: 0

IMSI	Sessions	Packets	Bytes

Before Throttling

After Throttling