KNOW THE UNKNOWN®

The Art of Cybersecurity (on a 5G canvas)

Darryle Merlette, CISSP
Executive Director – Security Solutions, NIKSUN Inc.

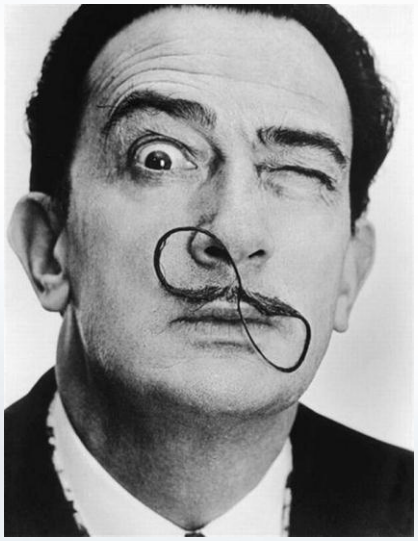
IEEE 5G Summit

May 26, 2015

Hackers and Painters

What hackers and painters have in common is that they're both makers. Along with composers, architects, and writers, what hackers and painters are trying to do is make ***good*** things.

-- Paul Graham (Hackers and Painters)



Evolution

Eavesdropping, Cloning, Spoofing…and IP

- 1G (analog)
  - All band radio receiver to eavesdrop
  - Clone phones to steal airtime
- 2G/3G
  - GSM hack using IMSI catcher to impersonate tower (2G)
  - Noise generator and amplifier to knock 3G network offline, then downgrade to 2G.
- 3G/4G/5G
  - All the vulnerabilities of IP networks…
  - 85% of all internet traffic is WWW
    - Promise of WWWW will likely cause increase

More Mobile Phones than people on Earth

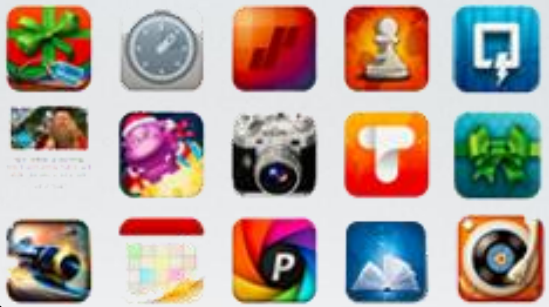
- Monthly global mobile data traffic will surpass *15 Exabytes* by 2018.
- The number of mobile-connected devices exceeds the world's population.
- The average mobile connection speed will surpass 2 Mbps by 2016.
- Due to increased usage on smartphones, smartphones will reach 66 percent of mobile data traffic by 2018.
- Monthly mobile tablet traffic will surpass *2.5 Exabytes per month* by 2018.
- 4G traffic will be more than half of the total mobile traffic by 2018.

Source: Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2013–2018

Proliferation of Apps and Devices

Convergent & Rich

Games and Apps



Virtual & SAS

Portable & Capable

Rich Multimedia

Chats

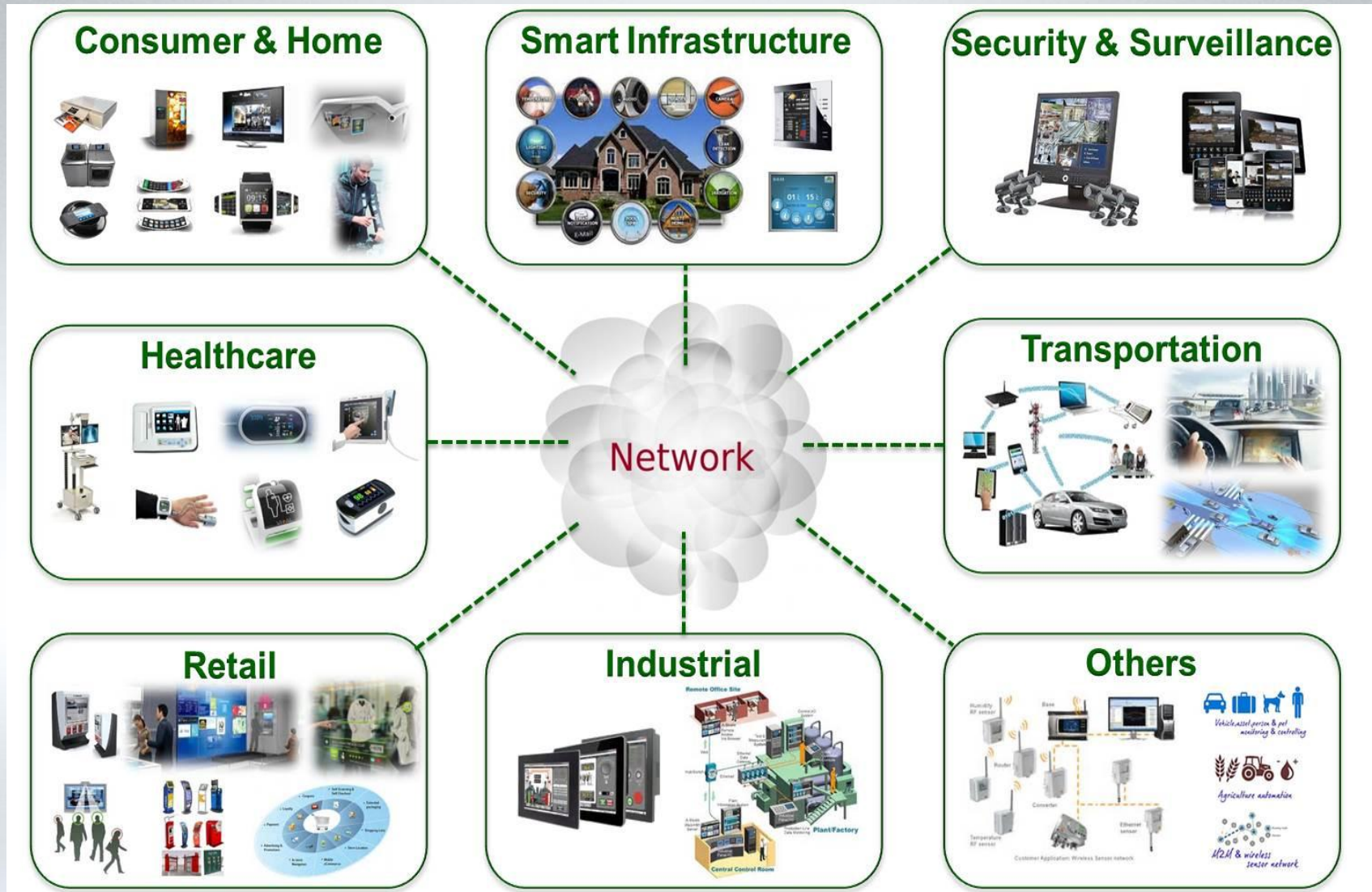
DYNAMIC INTERACTIVE

ANYTIME | **ANYWHERE** | **REAL-TIME**

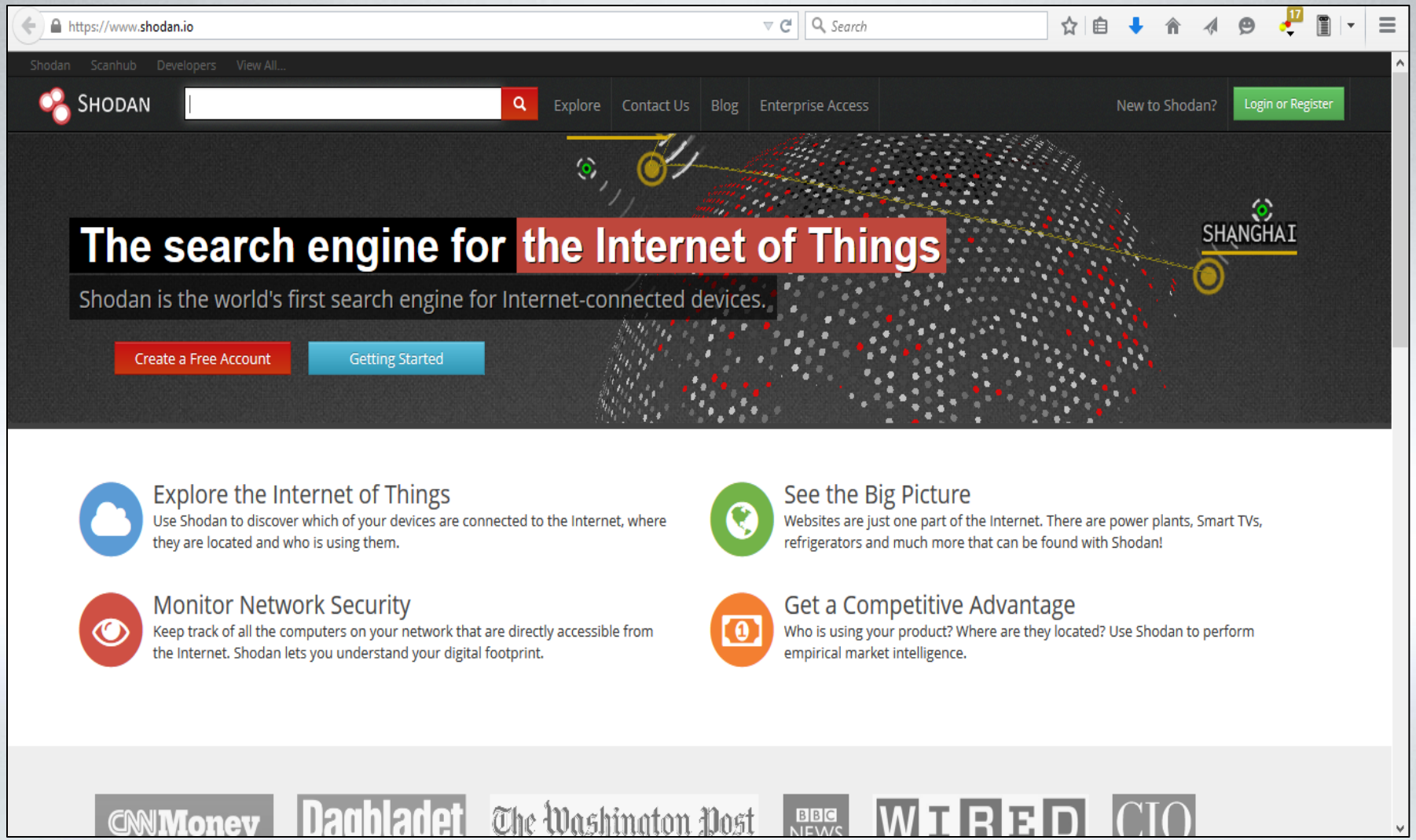
Mobile Malware and Attacks

- Many traditional web-based malware also affect mobile devices
- Wirelurker and Masque (iOS)
  - Creates trojaned versions of apps for binary file replacement
  - If same bundle identifier is used, can replace apps installed through App Store (but not preinstalled apps)
- Roughly 25% of all Google Play apps are clones (Columbia University)

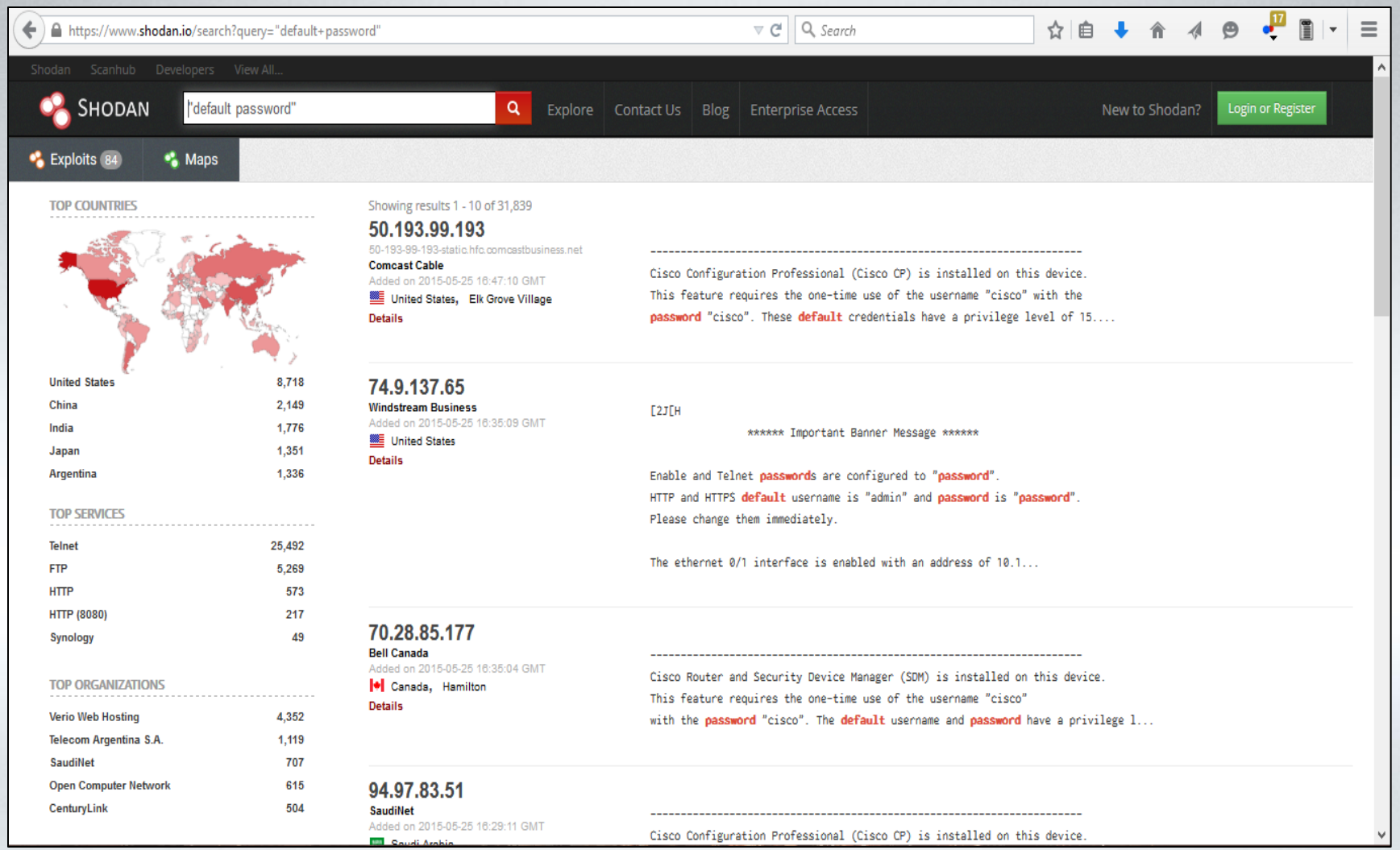
The Internet of Things



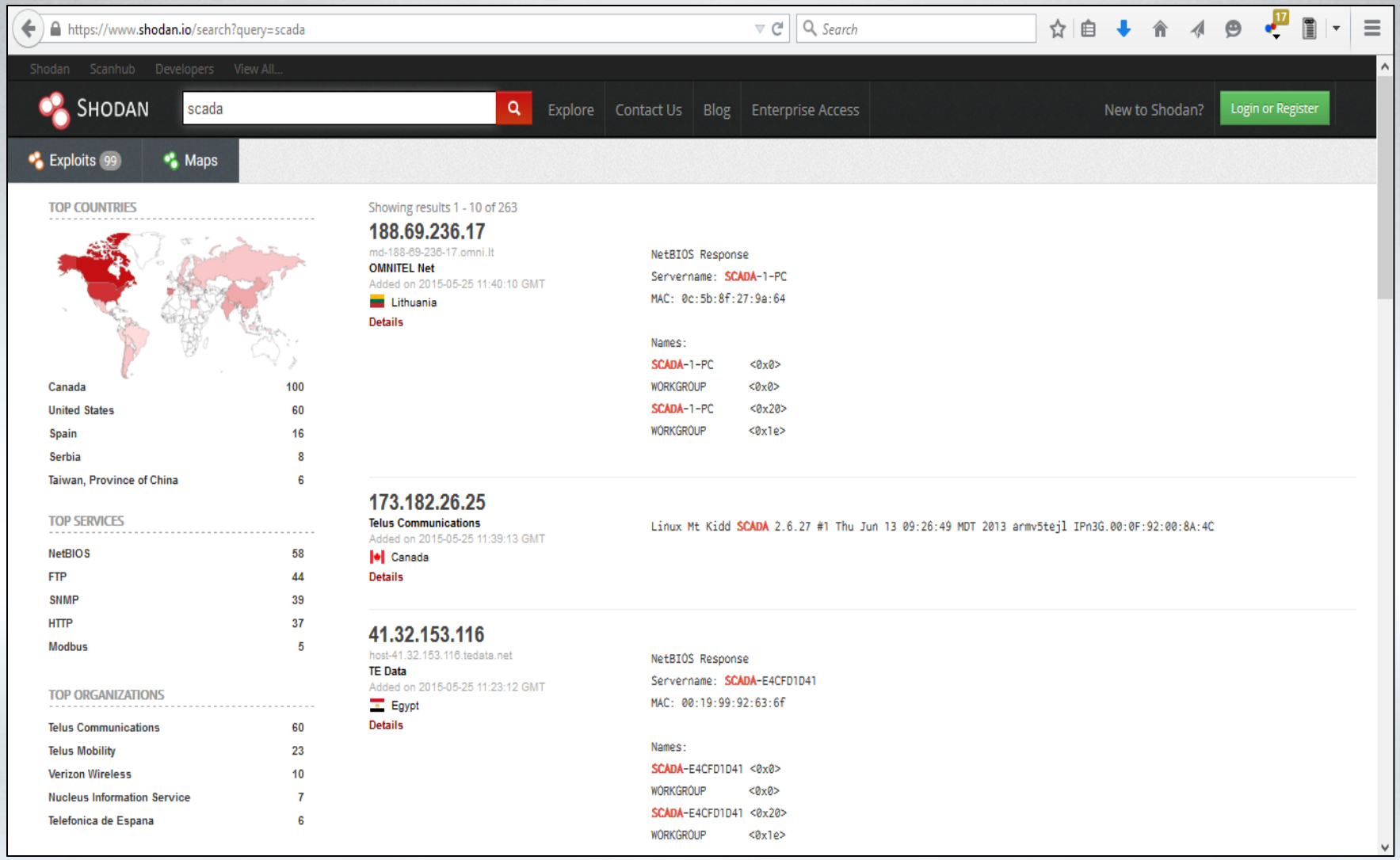
Shodan – Search Engine for IoT



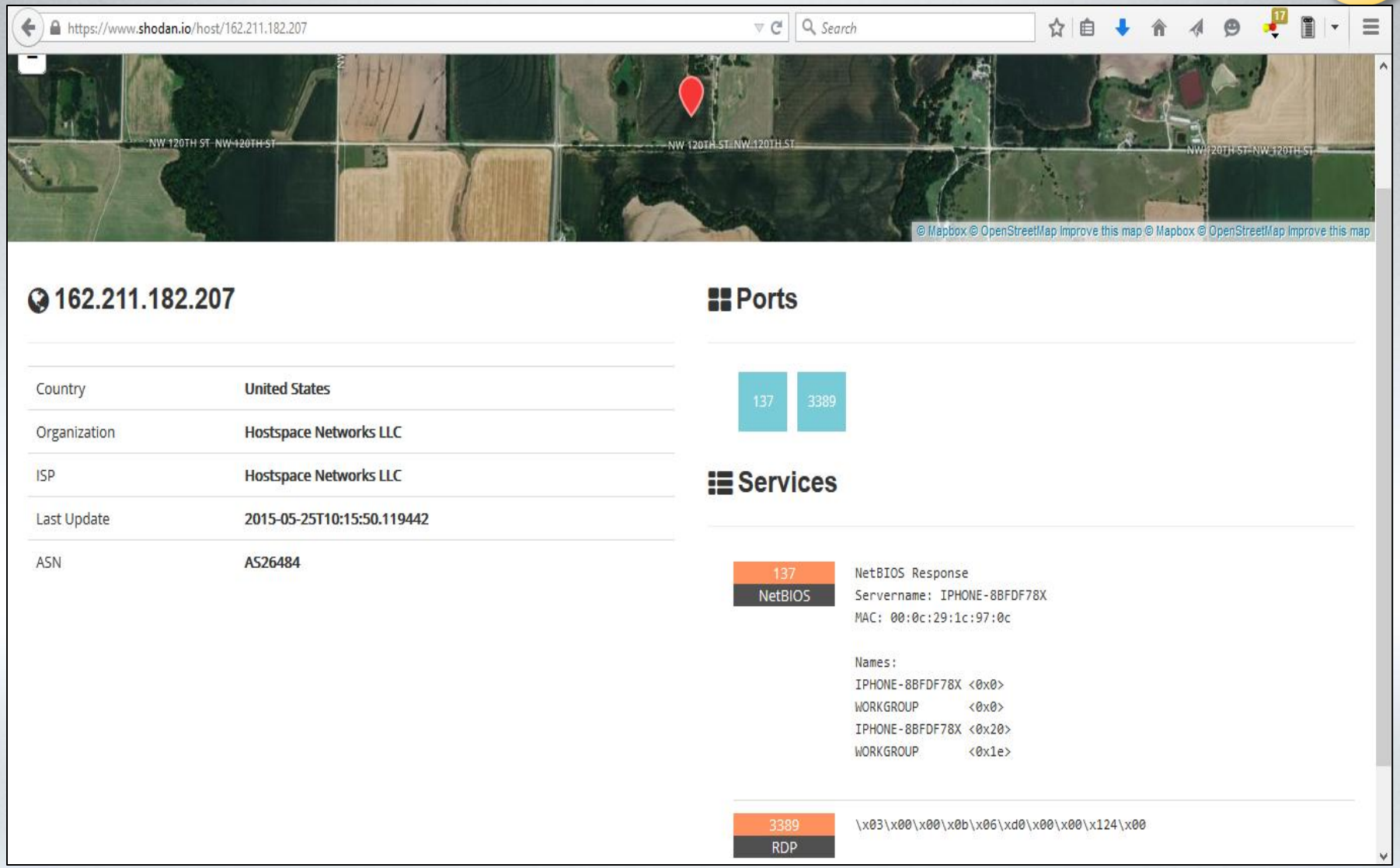
Shodan – Default password device search



Shodan – SCADA search

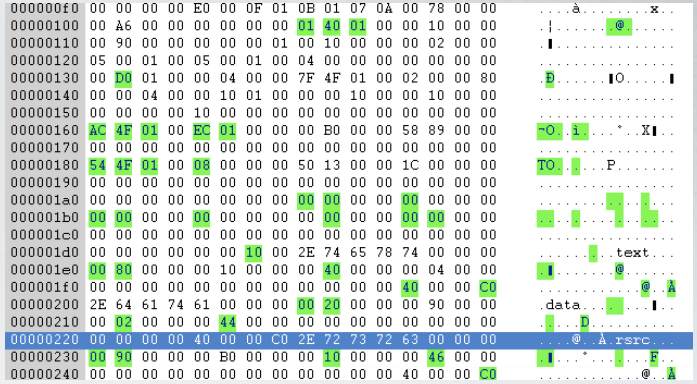


Shodan – IP Address search

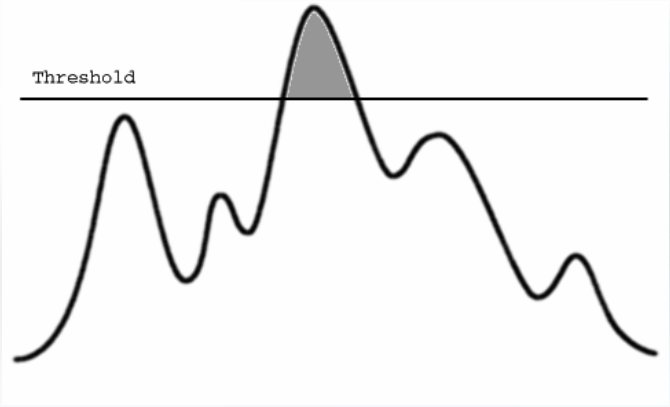


Network Detection

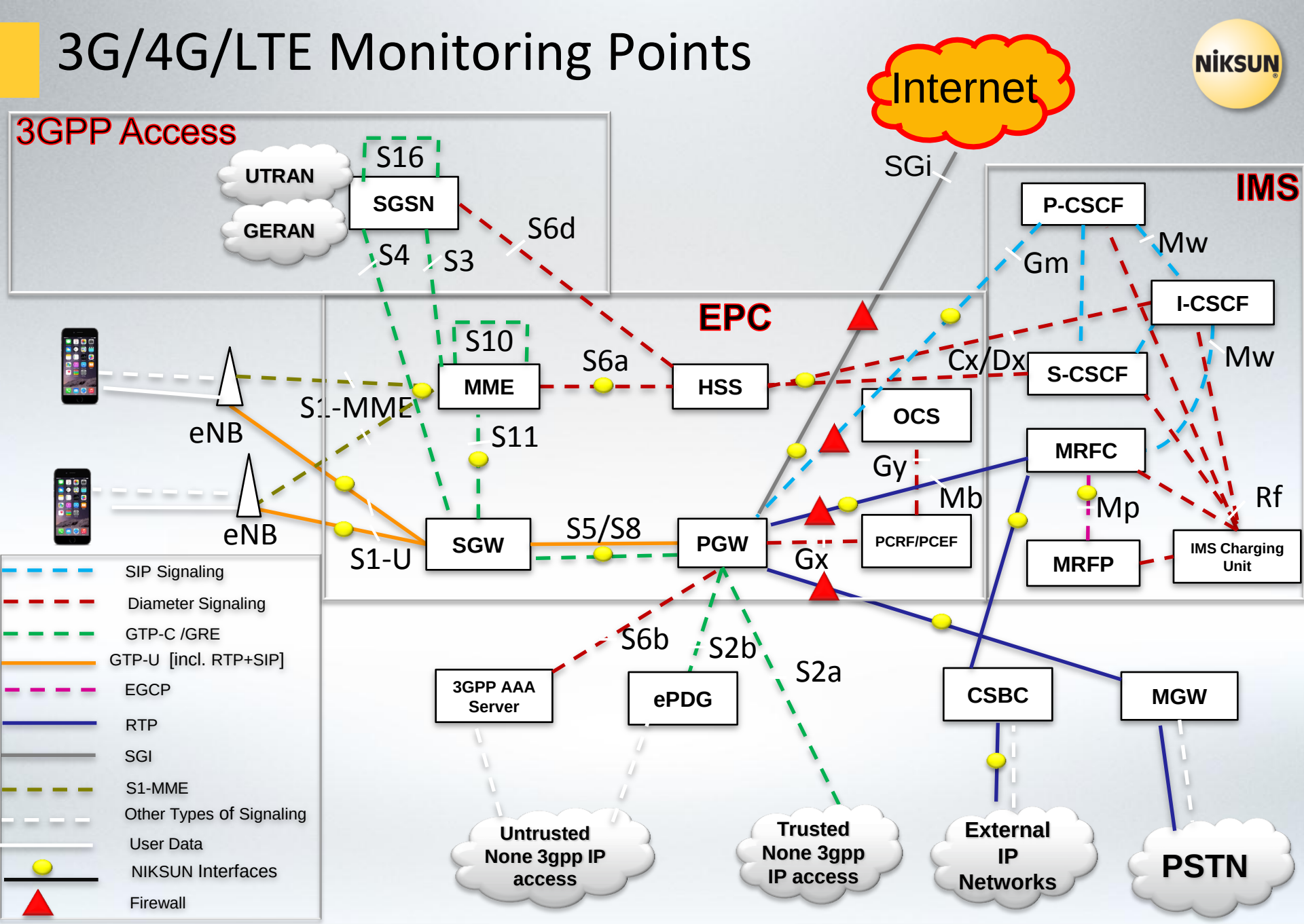
- Two Broad Categories
- Signature Detection
  - Specific patterns in packets
  - Similar to anti-virus paradigm
  - Must be periodically updated
  - Vulnerable to evasion and new attacks



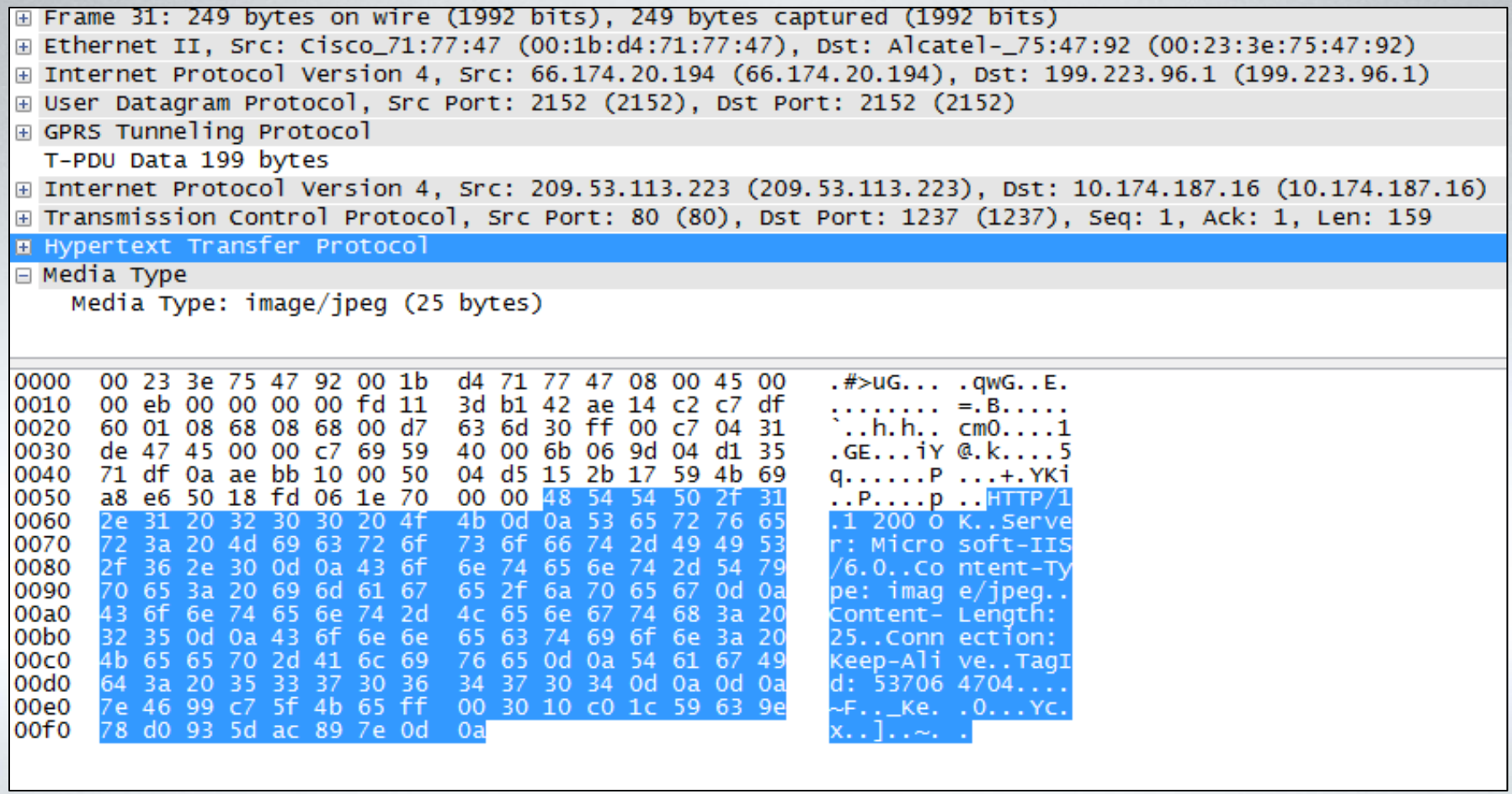
- Anomaly Detection
  - Deviations from statistical/behavioral norms
  - Can either “learn” or “be told” what is “normal”
  - Can often detect new attacks



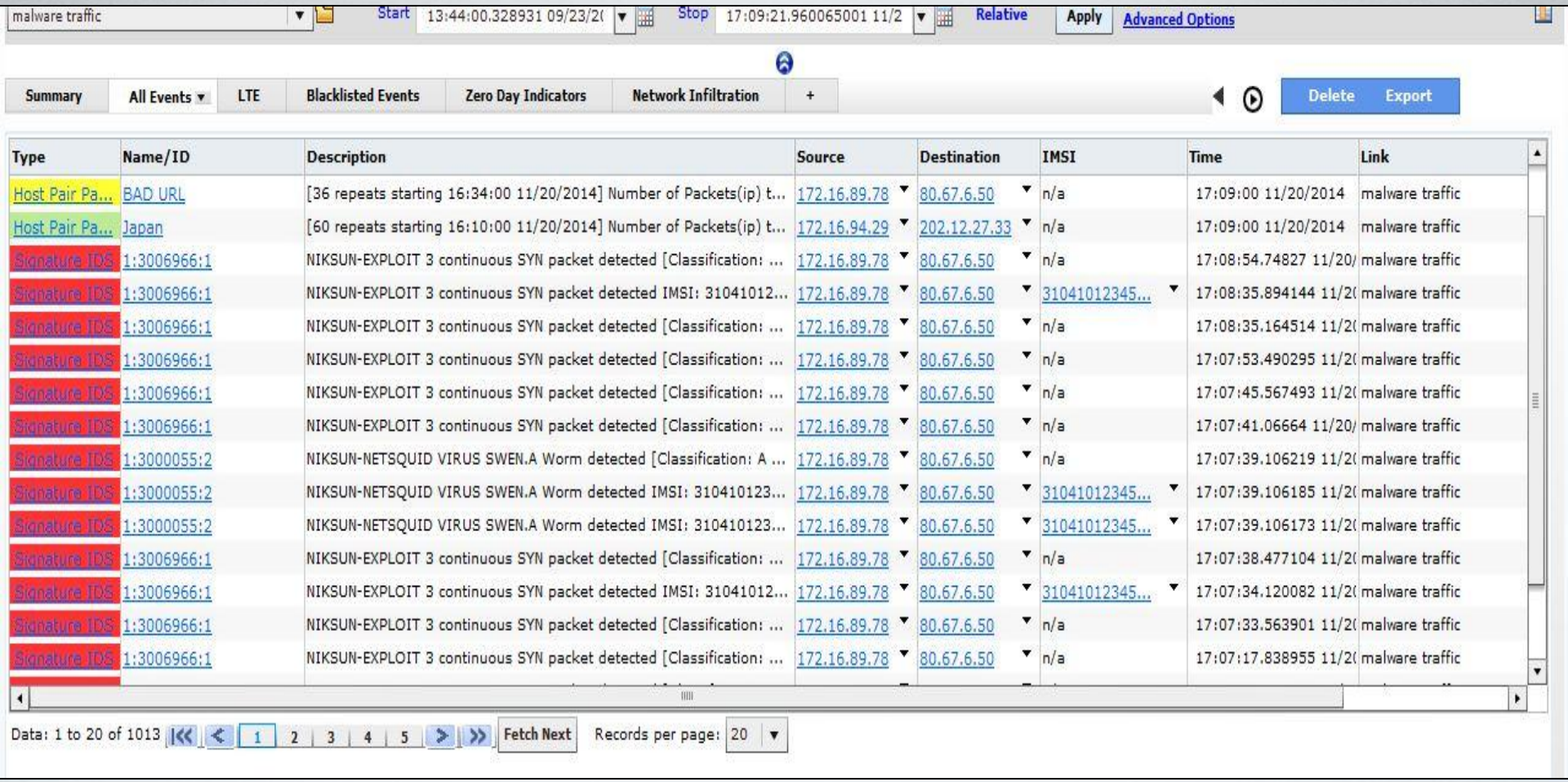
3G/4G/LTE Monitoring Points



Detunneling for detection



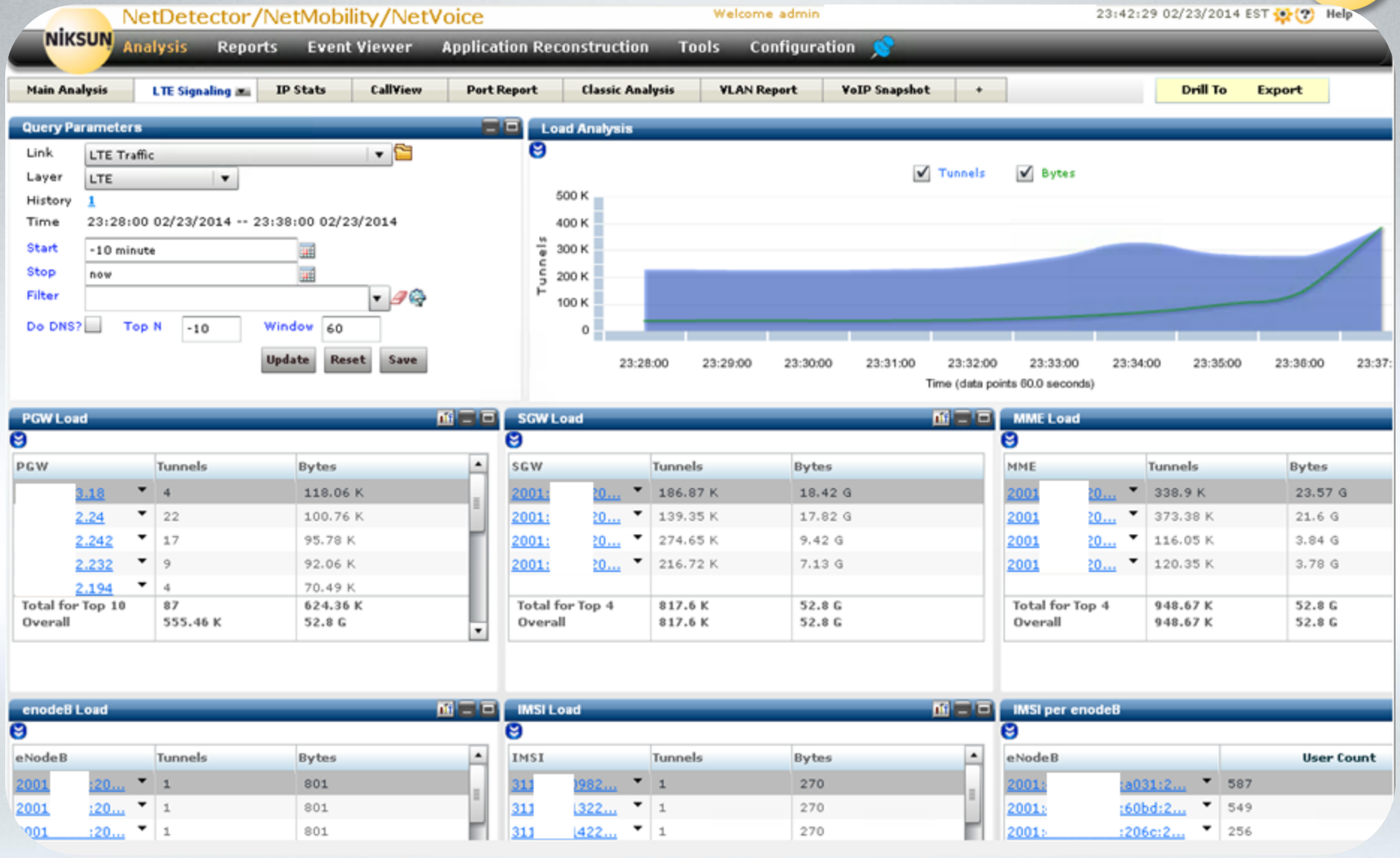
IMSI values as part of alerts



Type	Name/ID	Description	Source	Destination	IMSI	Time	Link
Host Pair Pa...	BAD URL	[36 repeats starting 16:34:00 11/20/2014] Number of Packets(ip) t...	172.16.89.78	80.67.6.50	n/a	17:09:00 11/20/2014	malware traffic
Host Pair Pa...	Japan	[60 repeats starting 16:10:00 11/20/2014] Number of Packets(ip) t...	172.16.94.29	202.12.27.33	n/a	17:09:00 11/20/2014	malware traffic
Signature IDS	1:3006966:1	NIKSUN-EXPLOIT 3 continuous SYN packet detected [Classification: ...	172.16.89.78	80.67.6.50	n/a	17:08:54.74827 11/20/	malware traffic
Signature IDS	1:3006966:1	NIKSUN-EXPLOIT 3 continuous SYN packet detected IMSI: 31041012...	172.16.89.78	80.67.6.50	31041012345...	17:08:35.894144 11/2(	malware traffic
Signature IDS	1:3006966:1	NIKSUN-EXPLOIT 3 continuous SYN packet detected [Classification: ...	172.16.89.78	80.67.6.50	n/a	17:08:35.164514 11/2(	malware traffic
Signature IDS	1:3006966:1	NIKSUN-EXPLOIT 3 continuous SYN packet detected [Classification: ...	172.16.89.78	80.67.6.50	n/a	17:07:53.490295 11/2(	malware traffic
Signature IDS	1:3006966:1	NIKSUN-EXPLOIT 3 continuous SYN packet detected [Classification: ...	172.16.89.78	80.67.6.50	n/a	17:07:45.567493 11/2(	malware traffic
Signature IDS	1:3006966:1	NIKSUN-EXPLOIT 3 continuous SYN packet detected [Classification: ...	172.16.89.78	80.67.6.50	n/a	17:07:41.06664 11/20/	malware traffic
Signature IDS	1:3000055:2	NIKSUN-NETSQUID VIRUS SWEN.A Worm detected [Classification: A ...	172.16.89.78	80.67.6.50	n/a	17:07:39.106219 11/2(	malware traffic
Signature IDS	1:3000055:2	NIKSUN-NETSQUID VIRUS SWEN.A Worm detected IMSI: 310410123...	172.16.89.78	80.67.6.50	31041012345...	17:07:39.106185 11/2(	malware traffic
Signature IDS	1:3000055:2	NIKSUN-NETSQUID VIRUS SWEN.A Worm detected IMSI: 310410123...	172.16.89.78	80.67.6.50	31041012345...	17:07:39.106173 11/2(	malware traffic
Signature IDS	1:3006966:1	NIKSUN-EXPLOIT 3 continuous SYN packet detected [Classification: ...	172.16.89.78	80.67.6.50	n/a	17:07:38.477104 11/2(	malware traffic
Signature IDS	1:3006966:1	NIKSUN-EXPLOIT 3 continuous SYN packet detected IMSI: 31041012...	172.16.89.78	80.67.6.50	31041012345...	17:07:34.120082 11/2(	malware traffic
Signature IDS	1:3006966:1	NIKSUN-EXPLOIT 3 continuous SYN packet detected [Classification: ...	172.16.89.78	80.67.6.50	n/a	17:07:33.563901 11/2(	malware traffic
Signature IDS	1:3006966:1	NIKSUN-EXPLOIT 3 continuous SYN packet detected [Classification: ...	172.16.89.78	80.67.6.50	n/a	17:07:17.838955 11/2(	malware traffic

Data: 1 to 20 of 1013 | 1 | 2 | 3 | 4 | 5 | Fetch Next | Records per page: 20

LTE GTP KPIs


NetDetector/NetMobility/NetVoice
Welcome admin
23:42:29 02/23/2014 EST
Help
Analysis
Reports
Event Viewer
Application Reconstruction
Tools
Configuration
Main Analysis
LTE Signaling
IP Stats
CallView
Port Report
Classic Analysis
VLAN Report
VoIP Snapshot
Drill To
Export
Query Parameters
Link
LTE Traffic
Layer
LTE
History
1
Time
23:28:00 02/23/2014 -- 23:38:00 02/23/2014
Start
-10 minute
Stop
now
Filter
Do DNS?
Top N
-10
Window
60
Update
Reset
Save
Load Analysis
Tunnels
Bytes
500 K
400 K
300 K
200 K
100 K
0
23:28:00
23:29:00
23:30:00
23:31:00
23:32:00
23:33:00
23:34:00
23:35:00
23:36:00
Time (data points 60.0 seconds)
PGW Load
PGW
Tunnels
Bytes
4
118.06 K
22
100.76 K
17
95.78 K
9
92.06 K
4
70.49 K
Total for Top 10
87
624.36 K
Overall
555.46 K
52.8 G
SGW Load
SGW
Tunnels
Bytes
186.87 K
18.42 G
139.35 K
17.82 G
274.65 K
9.42 G
216.72 K
7.13 G
Total for Top 4
817.6 K
52.8 G
Overall
817.6 K
52.8 G
MME Load
MME
Tunnels
Bytes
338.9 K
23.57 G
373.38 K
21.6 G
116.05 K
3.84 G
120.35 K
3.78 G
Total for Top 4
948.67 K
52.8 G
Overall
948.67 K
52.8 G
enodeB Load
eNodeB
Tunnels
Bytes
1
801
IMSI Load
IMSI
Tunnels
Bytes
1
270
IMSI per enodeB
eNodeB
User Count
587
549
256

LTE GTP KPIs

Create Session KPI

Delete Session KPI

Release Access Bearers Sessions KPI

Modify Bearer Sessions KPI

Message Type	Sessions	Cause Code
ModifyBearer	25.91 K(100.00%)	Request_Accepted
ModifyBearer	1(0.00%)	Context_Not_Found
Total for Top 2	25.91 K	N/A
Overall	25.91 K	N/A

Delete Bearer Sessions KPI

Message Type	Sessions	Cause Code
DeleteBearer	290(90.06%)	Request_Accepted
DeleteBearer	32(9.94%)	Request_Unknown_rejected
Total for Top 2	322	N/A
Overall	322	N/A

Update Bearer Sessions KPI

Message Type	Sessions	Cause Code
UpdateBearer	1(100.00%)	Request_Accepted
Total for Top 1	1	N/A
Overall	1	N/A

Downlink Data Sessions KPI

Message Type	Sessions	Cause Code
DownlinkData	4.68 K(94.14%)	Request_Accepted
DownlinkData	289(5.82%)	Unable_to_page_UE
DownlinkData	1(0.02%)	Unable_to_page_UE
DownlinkData	1(0.02%)	Context_Not_Found
Total for Top 4	4.97 K	N/A
Overall	4.97 K	N/A

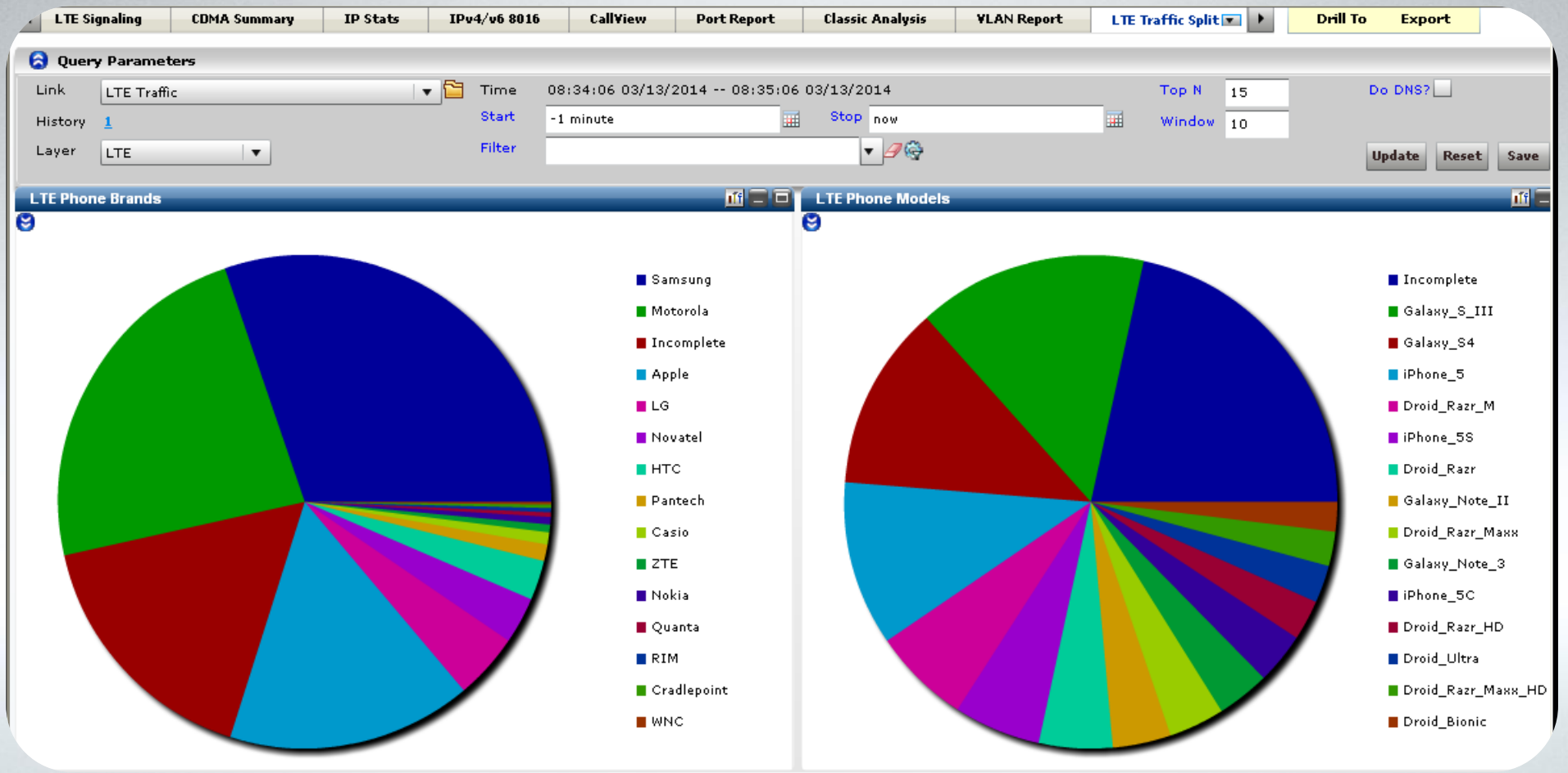
Downlink Data Notification Failure Indication Sessions KPI

Message Type	Sessions	Cause Code
DownlinkDataNotifica...	109(85.16%)	UE_not_respo...
DownlinkDataNotifica...	19(14.84%)	System_failure
Total for Top 2	128	N/A
Overall	128	N/A

Echo Sessions KPI

Message Type	Sessions	Cause Code
Echo	16(100.00%)	TimeOut
Total for Top 1	16	N/A
Overall	16	N/A

LTE GTP KPIs


LTE Signaling
CDMA Summary
IP Stats
IPv4/v6 8016
CallView
Port Report
Classic Analysis
VLAN Report
LTE Traffic Split
Drill To
Export
Query Parameters
Link
LTE Traffic
Time
08:34:06 03/13/2014 -- 08:35:06 03/13/2014
Top N
15
Do DNS?
History
1
Start
-1 minute
Stop
now
Window
10
Layer
LTE
Filter
Update
Reset
Save
LTE Phone Brands
Samsung
Motorola
Incomplete
Apple
LG
Novatel
HTC
Pantech
Casio
ZTE
Nokia
Quanta
RIM
Cradlepoint
WNC
LTE Phone Models
Incomplete
Galaxy_S_III
Galaxy_S4
iPhone_5
Droid_Razr_M
iPhone_5S
Droid_Razr
Galaxy_Note_II
Droid_Razr_Maxx
Galaxy_Note_3
iPhone_5C
Droid_Razr_HD
Droid_Ultra
Droid_Razr_Maxx_HD
Droid_Bionic

LTE Security and Performance Alarms

- Excessive (failed) sessions per UE eNodeB pair/SGW/MME
- Excessive Bytes per IMSI
- Excessive Average Bearer Setup Time
- Tunnels per SGW/MME/UE/eNodeB/PGW
- Alarms available on IMS-GM, S6a, CDMA as well…

Conclusions

- As 4G matures and 5G emerges, the expanding landscape of devices and apps presents an attractive canvas for hackers to paint
- Scalable and holistic monitoring solutions will be needed to help track and mitigate attacks
- As new attack paradigms emerge, innovative solutions must be developed
- Humans are still the weakest link when it comes to security…

Security?

There is no security on this earth. There is only opportunity. -- Gen. Douglas MacArthur

NIKSUN:

Helping You *Know the Unknown*®

For additional information:

Visit us at niksun.com or

email to info@niksun.com

Some Example Detections

- Signatures
  - Shellshock (content "() {“)
  - Known rogue User Agents (eg., content:"User-Agent|3a| ezula“)
  - Known shellcode sequences (eg., 0x90 0x90 0x90…)
  - Stuxnet (content:"/index.php?data=66a96e28“)

- Anomaly Detection (with DAR and GeoIP)
  - Host pair bytes, Host pair packets, Host Flood, Host Scan, Port Scan …
  - Covert IRC: apptype irc and not tcp port (194 or 667 or 6660-6669 or 7000)
  - From China: geo host CN and apptype irc and not tcp port (194 or 667 or 6660-6669 or 7000)
  - Botnet behavior – low bytes over long connection
  - Tunneling: not apptype http and tcp port (80 or 8080 or 8008 or 8081 or 591)

Who Are the Bad Guys?

- No more script kiddies!
- Nation States
  - Espionage
  - Intellectual Property
  - Critical Infrastructure
- Cyber-Criminals
  - Identify Theft
  - Corporate Fraud
  - Financial Infrastructure
- Hacktivists
  - Political Action
  - Corporate Shaming
  - Spear Phishing

Stealth is the New Black

Bad Guys Are Winning…

69 to 158 new malware variants created every minute!

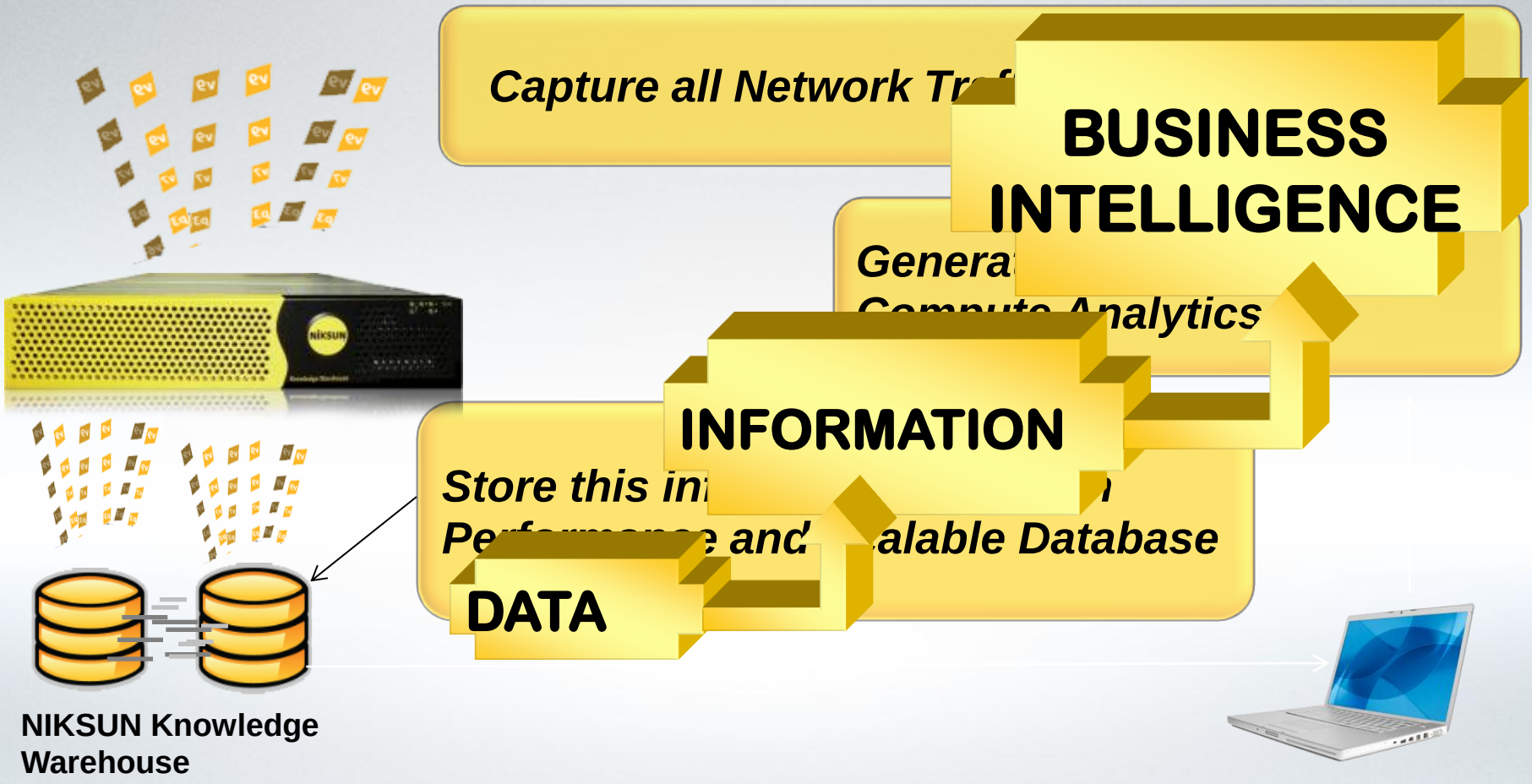
-- McAfee/PandaLabs

Traditional Tools: Log Analysis -- Great… But

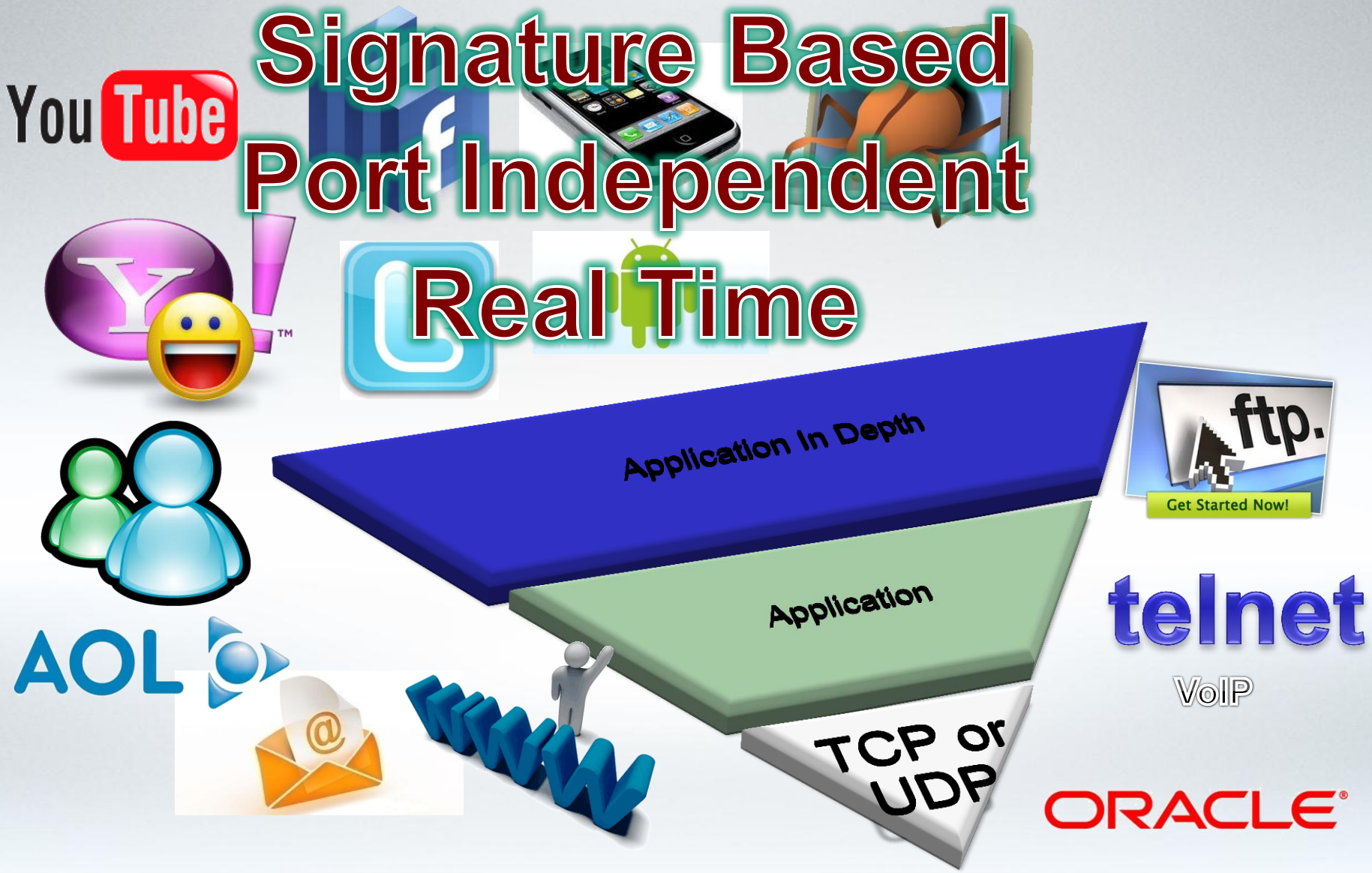
- **Consider the physical analog…**
  - **Bank robbery: identify and catch the robber from transaction records**
  - **Convenience store: identify and catch a thief from sales transaction receipts**
  - **Office visitor theft: identify and catch perpetrator based on sign-in/sign-out logs**

- **Why rely on logs in the network world?**

NIKSUN's Solution Architecture



Dynamic Application Recognition



Detection Made Easy!

Network Working Group
Request for Comments: 3514
Category: Informational

S. Bellovin
AT&T Labs Research
1 April 2003

The Security Flag in the IPv4 Header

Status of this Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

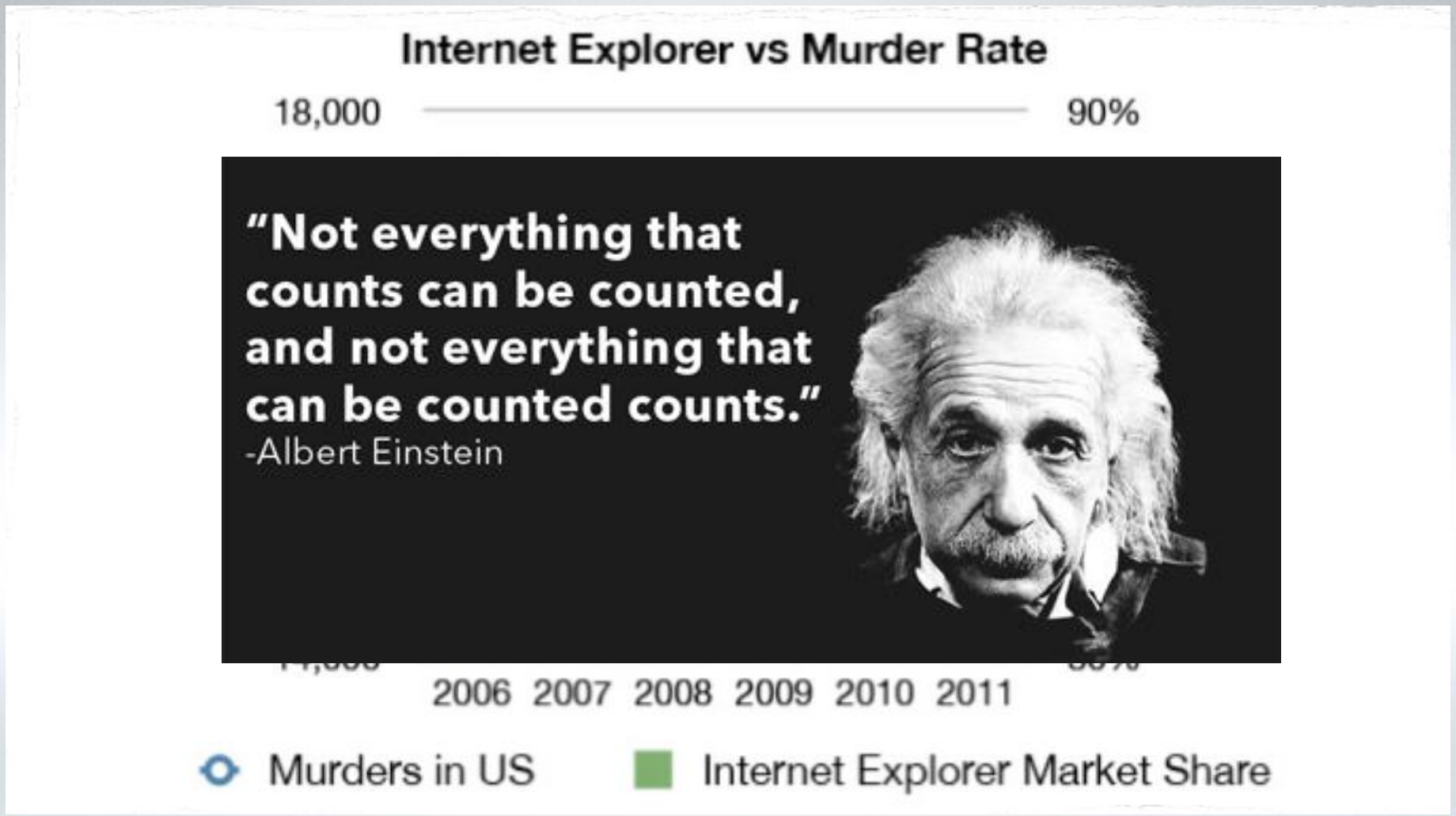
Abstract

Firewalls, packet filters, intrusion detection systems, and the like often have difficulty distinguishing between packets that have malicious intent and those that are merely unusual. We define a security flag in the IPv4 header as a means of distinguishing the two cases.

1. Introduction

Firewalls [CBR03], packet filters, intrusion detection systems, and the like often have difficulty distinguishing between packets that have malicious intent and those that are merely unusual. The problem is that making such determinations is hard. To solve this problem, we define a security flag, known as the "evil" bit, in the IPv4 [RFC791] header. Benign packets have this bit set to 0; those that are used for an attack will have the bit set to 1.

Be Careful With Your Data!



NIKSUN Solutions

Cyber Security

Surveillance, Detection and Forensics

Network Performance

Proactive Network, Service and Application Monitoring

Mobility

Performance and Security Monitoring for Cellular Networks

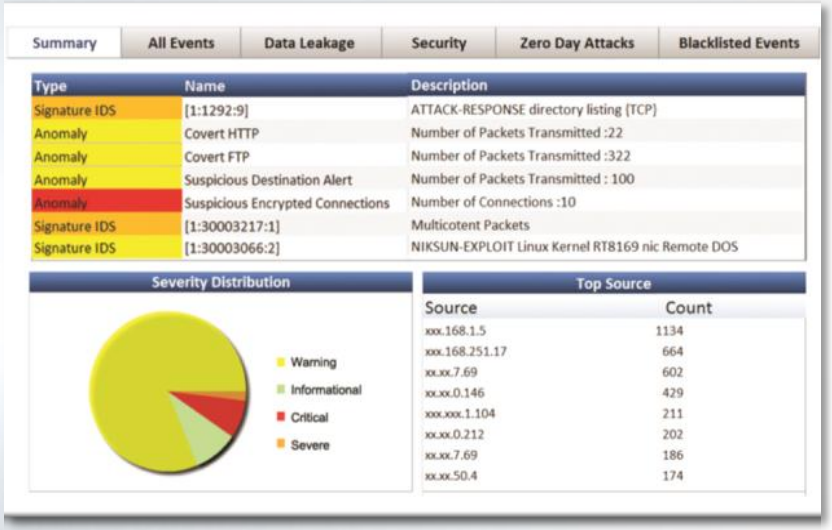
NIKSUN Product Portfolio

NetDetector® NetDetectorLive™	Security Monitoring Detection & Alerting Forensics
NetMobility® NetVoice®	3G & 4G Analysis VoIP Performance
NetVCR® FlowAggregator™ NetBlackBox Pro®	Performance Monitoring Flow Monitoring Troubleshooting
NetRTX™ NetSLM™ NetMulticast™ NetPoller™	SLA/QoS Alerting Advanced Analysis
NetOmni™ NetX™ Central Manager™ NetTrident™	Scalable Monitoring Reports Alerts Forensics
NetReporter™ NetXperts™	Reporting Expert Analysis

NIKSUN Security Solutions

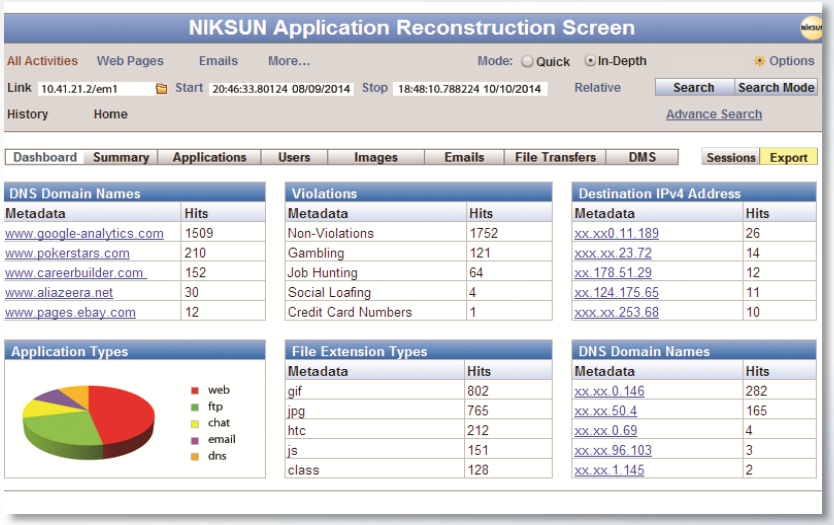
NetDetector®

Comprehensive and actionable solution for network security



NetDetectorLive™

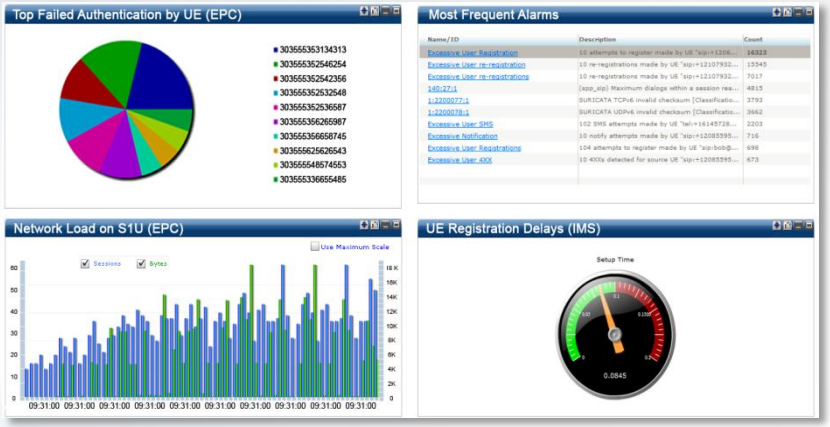
Lightning fast search & application reconstruction for real-time network security forensics



NIKSUN Mobility Solutions

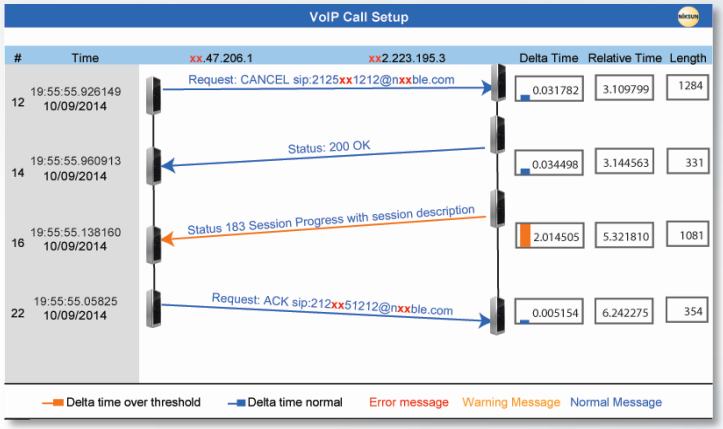
NetMobility®

Performance and Security Analysis for 3G and 4G Networks



NetVoice®

VoIP Monitoring & Troubleshooting Solution



NIKSUN Enterprise Solution

NetOmni™

Single Unifying Information Portal For All Network Data