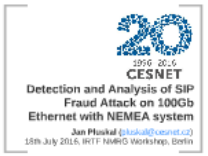
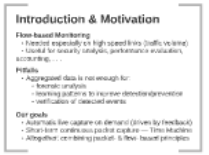
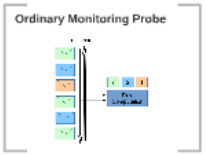
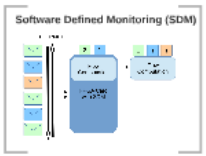
Introduction 1

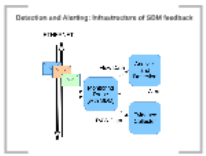




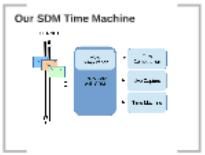


SDM Feedback 2

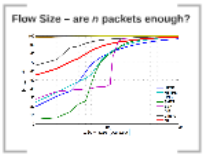


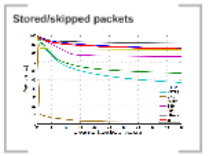


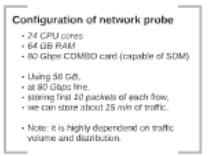
SDM Timemachine 3

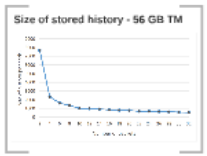


Measurements 4

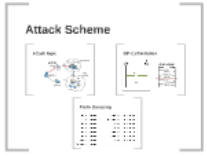


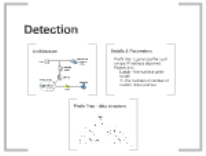






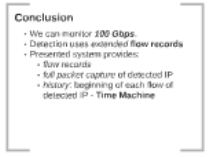
SIP Fraud Attack 5





Visualization 6

Conclusion 7

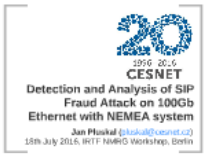


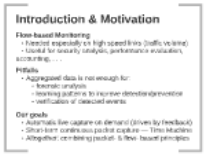
Detection and Analysis of SIP Fraud Attack on 100Gb Ethernet with NEMEA system

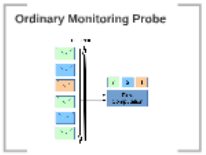
Jan Pluskal (pluskal@cesnet.cz)

18th July 2016, IRTF NMRG Workshop, Berlin

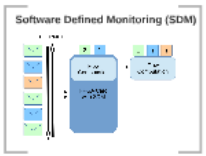
Introduction 1

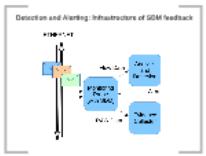




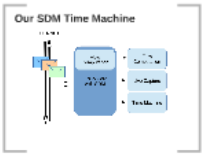


SDM Feedback 2

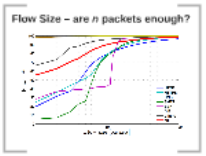


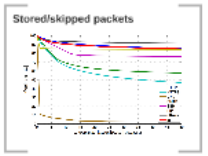


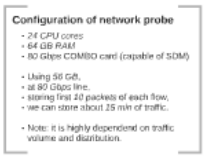
SDM Timemachine 3

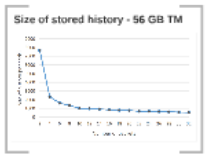


Measurements 4

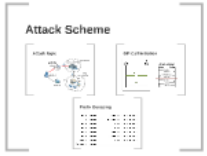


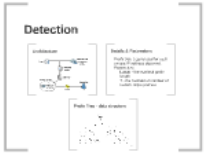






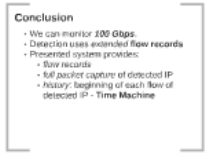
SIP Fraud Attack 5



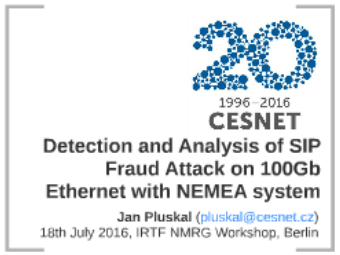


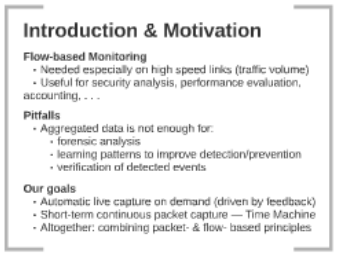
Visualization 6

Conclusion 7



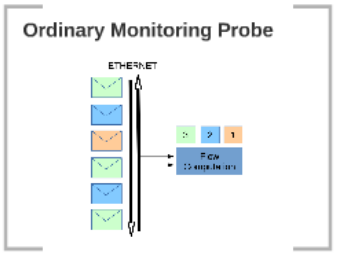
Introduction 1


1996 - 2016
CESNET
Detection and Analysis of SIP Fraud Attack on 100Gb Ethernet with NEMEA system
Jan Pluskal (pluskal@cesnet.cz)
18th July 2016, IRTF NMRG Workshop, Berlin

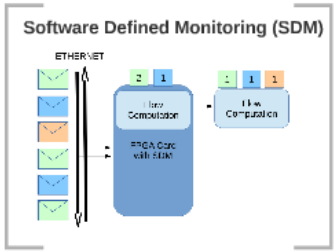

Introduction & Motivation
Flow-based Monitoring
- Needed especially on high speed links (traffic volume)
- Useful for security analysis, performance evaluation, accounting, . . .

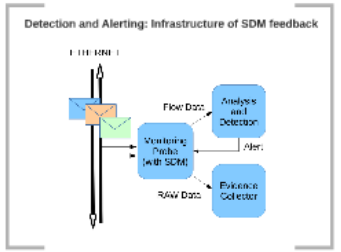
Pitfalls
- Aggregated data is not enough for:
  - forensic analysis
  - learning patterns to improve detection/prevention
  - verification of detected events

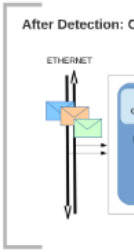
Our goals
- Automatic live capture on demand (driven by feedback)
- Short-term continuous packet capture — Time Machine
- Altogether: combining packet- & flow- based principles


Ordinary Monitoring Probe
ETHERNET

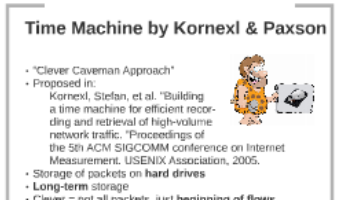
SDM Feedback 2

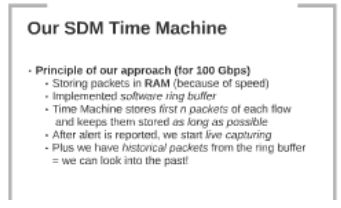

Software Defined Monitoring (SDM)
ETHERNET
Flow Computation
FPGA Core with SDM
Flow Computation

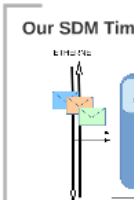

Detection and Alerting: Infrastructure of SDM feedback
Flow Data
Analysis and Detection
Alert
Monitoring Probe with SDM
RAW Data
Evidence Collector


After Detection:
ETHERNET

Timemachine 3


Time Machine by Kornexl & Paxson
- "Clever Caveman Approach"
- Proposed in:
  Kornexl, Stefan, et al. "Building a time machine for efficient recording and retrieval of high-volume network traffic. "Proceedings of the 5th ACM SIGCOMM conference on Internet Measurement. USENIX Association, 2005.
- Storage of packets on **hard drives**
- **Long-term** storage


Our SDM Time Machine
- **Principle of our approach (for 100 Gbps)**
  - Storing packets in **RAM** (because of speed)
  - Implemented *software ring buffer*
  - Time Machine stores *first n packets* of each flow and keeps them stored *as long as possible*
  - After alert is reported, we start *live capturing*
  - Plus we have *historical packets* from the ring buffer = we can look into the past!


Our SDM Tim

Introduction & Motivation

Flow-based Monitoring

- Needed especially on high speed links (traffic volume)
- Useful for security analysis, performance evaluation, accounting, . . .

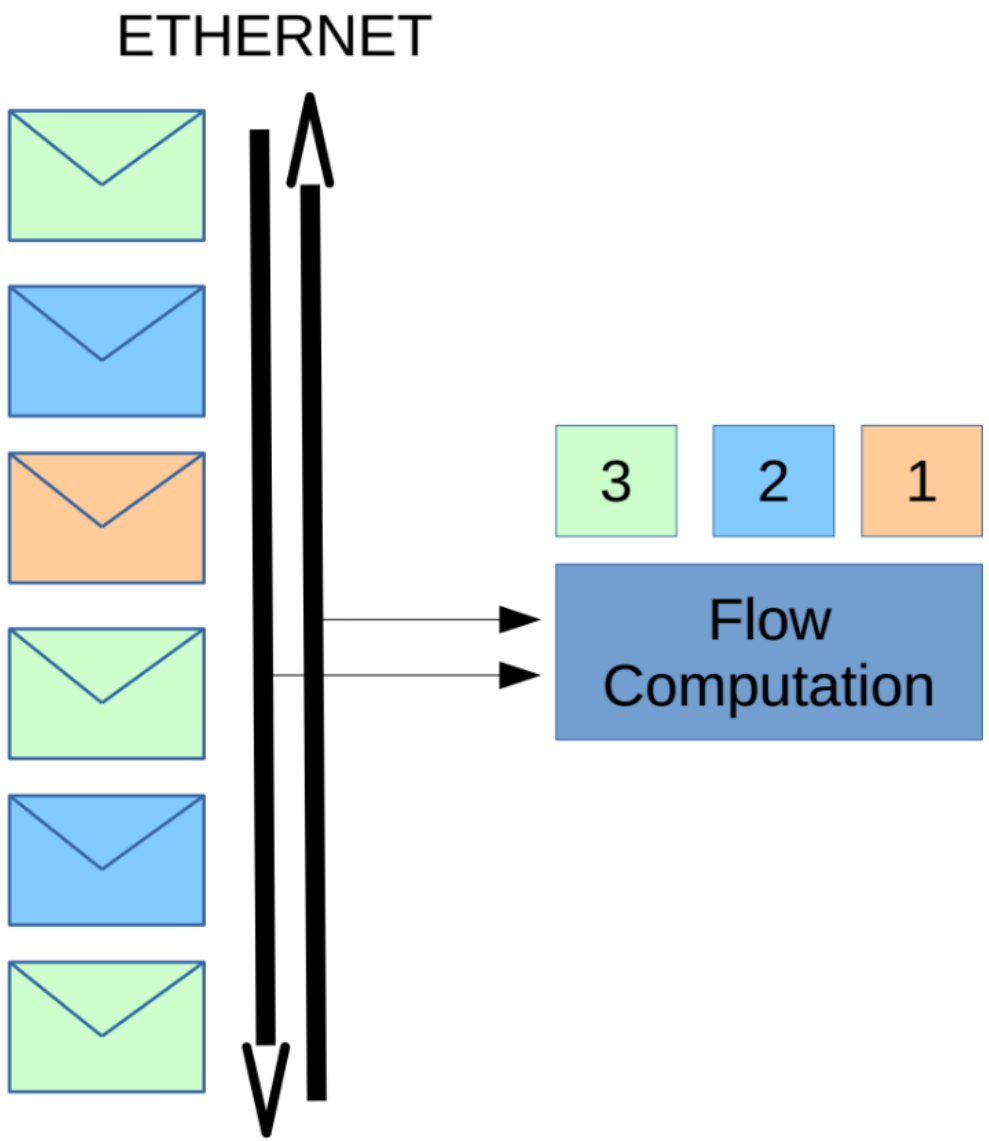
Pitfalls

- Aggregated data is not enough for:
  - forensic analysis
  - learning patterns to improve detection/prevention
  - verification of detected events

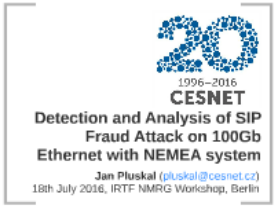
Our goals

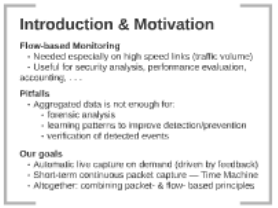
- Automatic live capture on demand (driven by feedback)
- Short-term continuous packet capture — Time Machine
- Altogether: combining packet- & flow- based principles

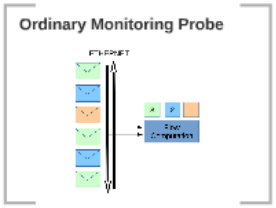
Ordinary Monitoring Probe



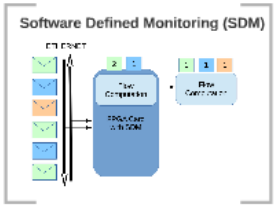
Introduction 1

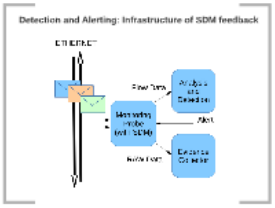

1996–2016
CESNET
Detection and Analysis of SIP Fraud Attack on 100Gb Ethernet with NEMEA system
Jan Pluskal (pluskal@cesnet.cz)
18th July 2016, IRTF NMRG Workshop, Berlin

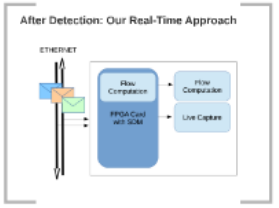

Introduction & Motivation
Flow-based Monitoring
- Needed especially on high speed links (traffic volume)
- Useful for security analysis, performance evaluation, accounting, . . .
Pitfalls
- Aggregated data is not enough for:
  - forensic analysis
  - learning patterns to improve detection/prevention
  - verification of detected events
Our goals
- Automatic live capture on demand (driven by feedback)
- Short-term continuous packet capture — Time Machine
- Altogether: combining packet- & flow- based principles


Ordinary Monitoring Probe

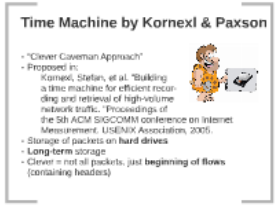
SDM Feedback 2

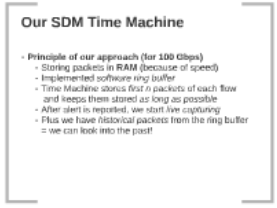

Software Defined Monitoring (SDM)

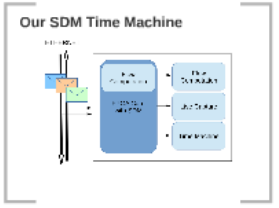

Detection and Alerting: Infrastructure of SDM feedback


After Detection: Our Real-Time Approach

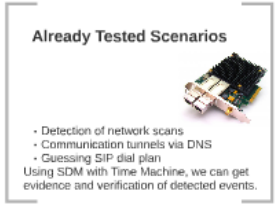
SDM Timemachine 3


Time Machine by Kornexl & Paxson
- "Clever Caveman Approach"
- Proposed in:
  Kornexl, Stefan, et al. "Building a time machine for efficient recording and retrieval of high-volume network traffic." Proceedings of the 5th ACM SIGCOMM conference on Internet Measurement. USENIX Association, 2005.
- Storage of packets on **hard drives**
- **Long-term** storage
- Clever = not all packets, just **beginning of flows** (containing headers)

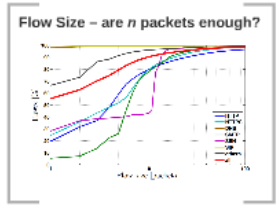

Our SDM Time Machine
- **Principle of our approach (for 100 Gbps)**
  - Storing packets in **RAM** (because of speed)
  - Implemented software *ring buffer*
  - Time Machine stores *first n* packets of each flow and keeps them stored *as long as possible*
  - After alert is reported, we start *live capturing*
  - Plus we have *historical* packets from the ring buffer = we can look into the past!

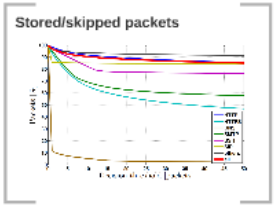

Our SDM Time Machine

Measurements 4


Already Tested Scenarios
- Detection of network scans
- Communication tunnels via DNS
- Guessing SIP dial plan

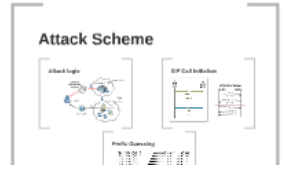
Using SDM with Time Machine, we can get evidence and verification of detected events.

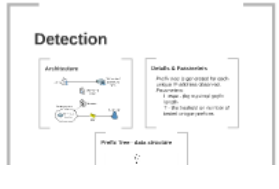

Flow Size – are *n* packets enough?


Stored/skipped packets

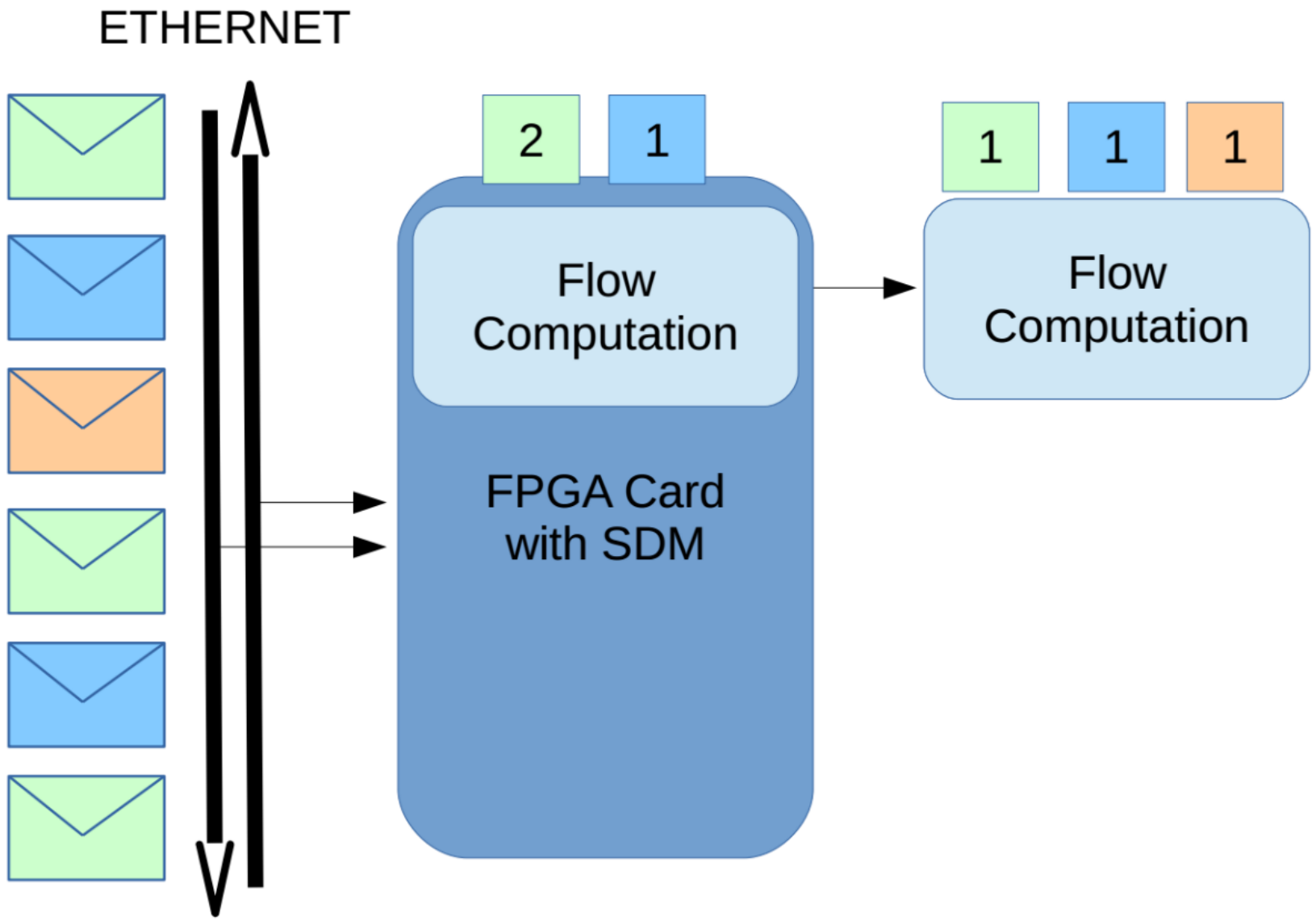
SIP Fraud Attack 5


SIP Fraud Attack
- Gateway should not allow forwarding calls to PSTN without proper authentication.
- Many gateways have very poor security measures (if any at all)
  - A call to PSTN via the gateway require to guess a correct prefix.

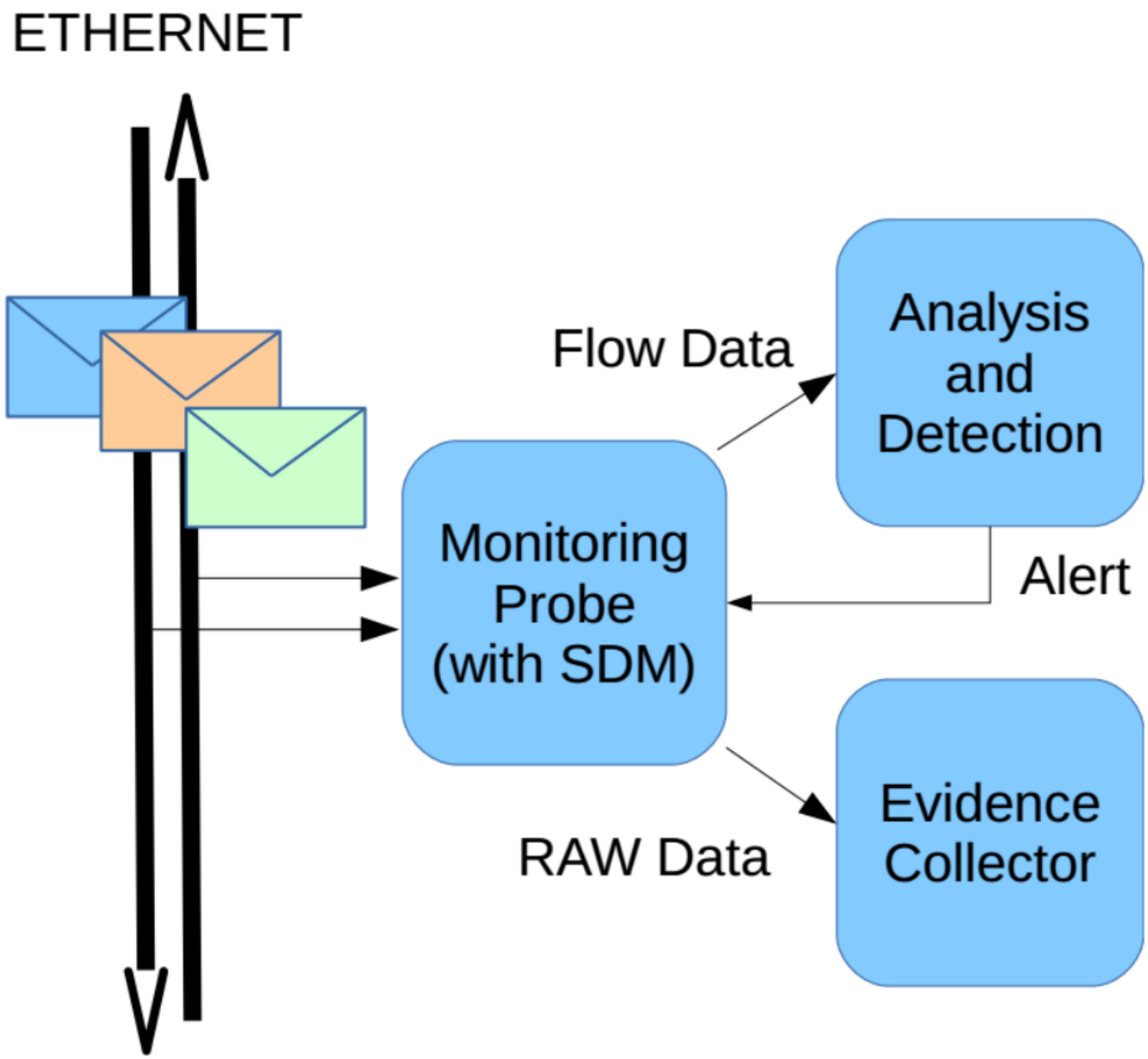

Attack Scheme


Detection

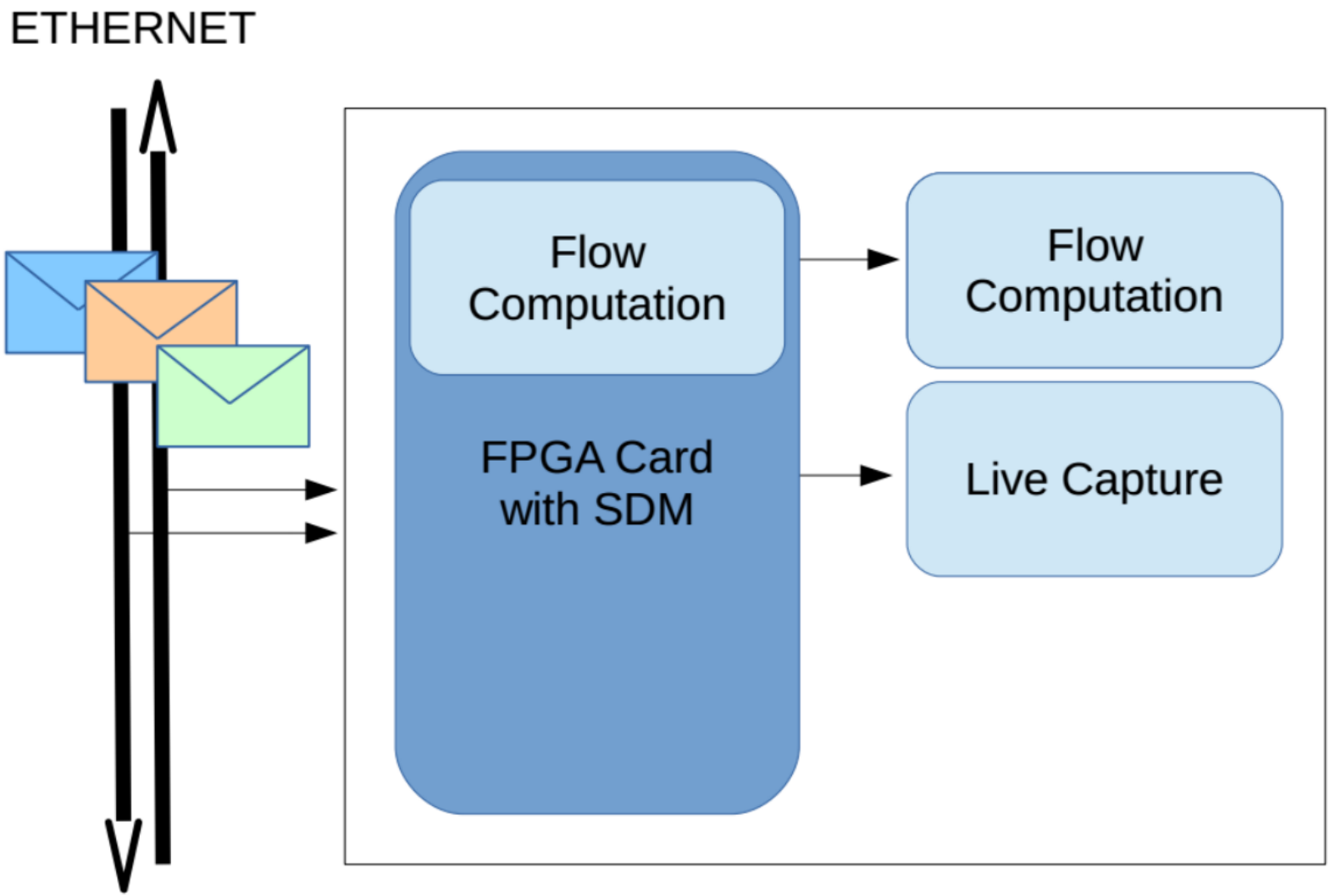
Software Defined Monitoring (SDM)



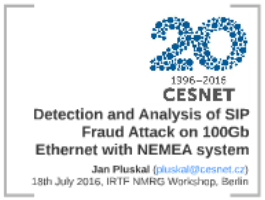
Detection and Alerting: Infrastructure of SDM feedback

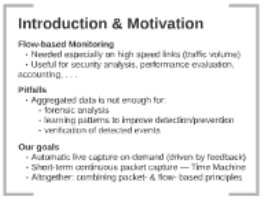


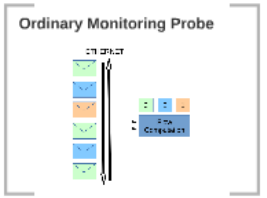
After Detection: Our Real-Time Approach



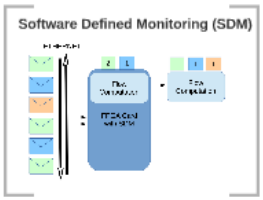
Introduction 1

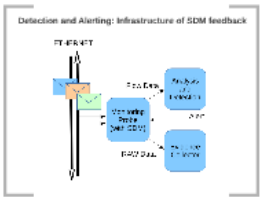


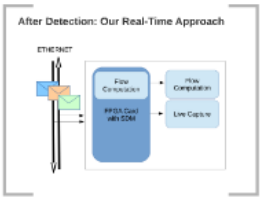




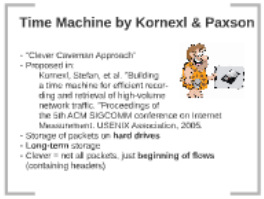
SDM Feedback 2

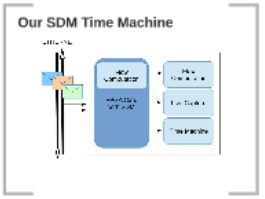




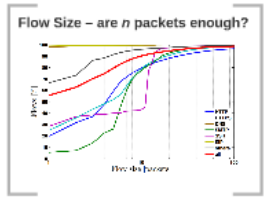


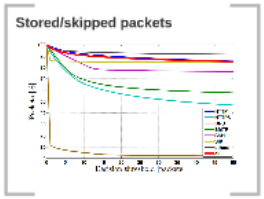
SDM Timemachine 3



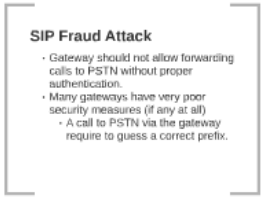


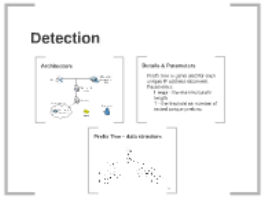
Measurements 4



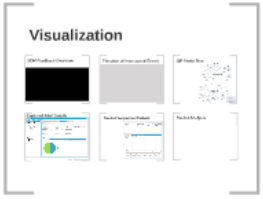


SIP Fraud Attack 5





Visualization 6



Time Machine by Kornexl & Paxson

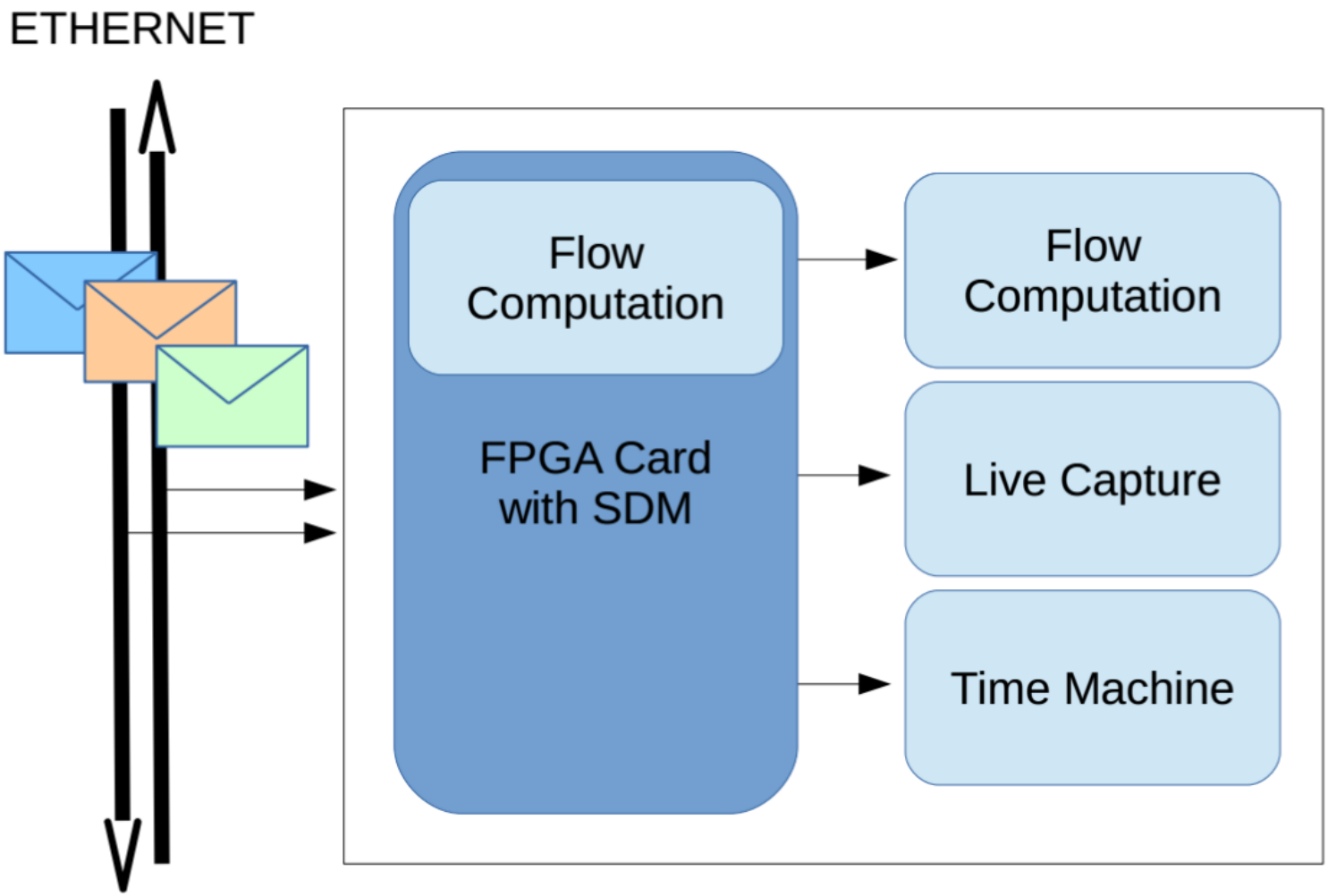
- “Clever Caveman Approach”
- Proposed in:

  Kornexl, Stefan, et al. "Building a time machine for efficient recording and retrieval of high-volume network traffic. "Proceedings of the 5th ACM SIGCOMM conference on Internet Measurement. USENIX Association, 2005.
- Storage of packets on **hard drives**
- **Long-term** storage
- Clever = not all packets, just **beginning of flows** (containing headers)

Our SDM Time Machine

- **Principle of our approach (for 100 Gbps)**
  - Storing packets in **RAM** (because of speed)
  - Implemented *software ring buffer*
  - Time Machine stores *first n packets* of each flow and keeps them stored *as long as possible*
  - After alert is reported, we start *live capturing*
  - Plus we have *historical packets* from the ring buffer = we can look into the past!

Our SDM Time Machine



Introduction 1

SDM Feedback 2

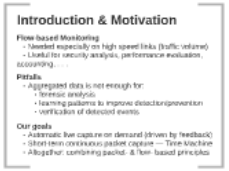
M Timemachine 3

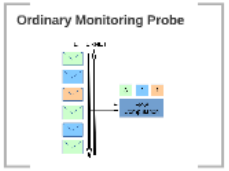
Measurements 4

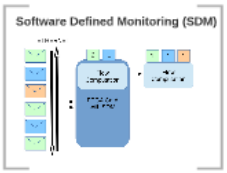
IP Fraud Attack 5

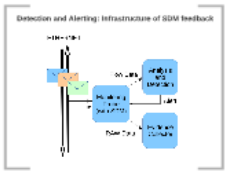
Visualization 6

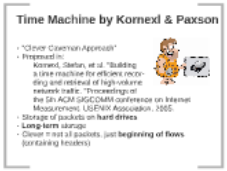
Conclusion 7

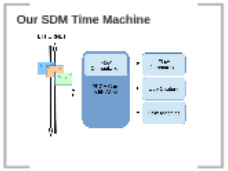


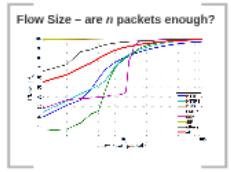


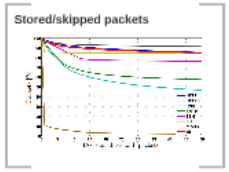


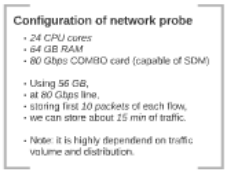


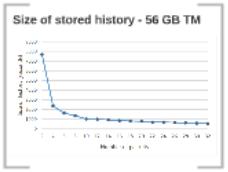


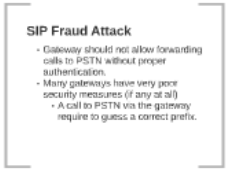


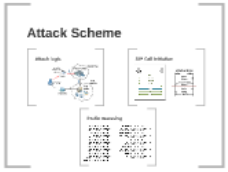


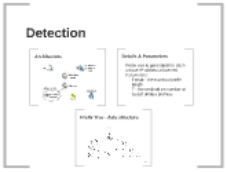


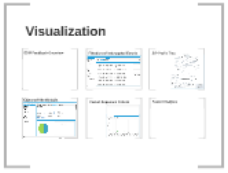


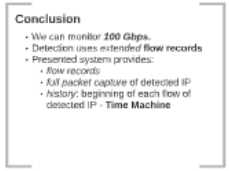










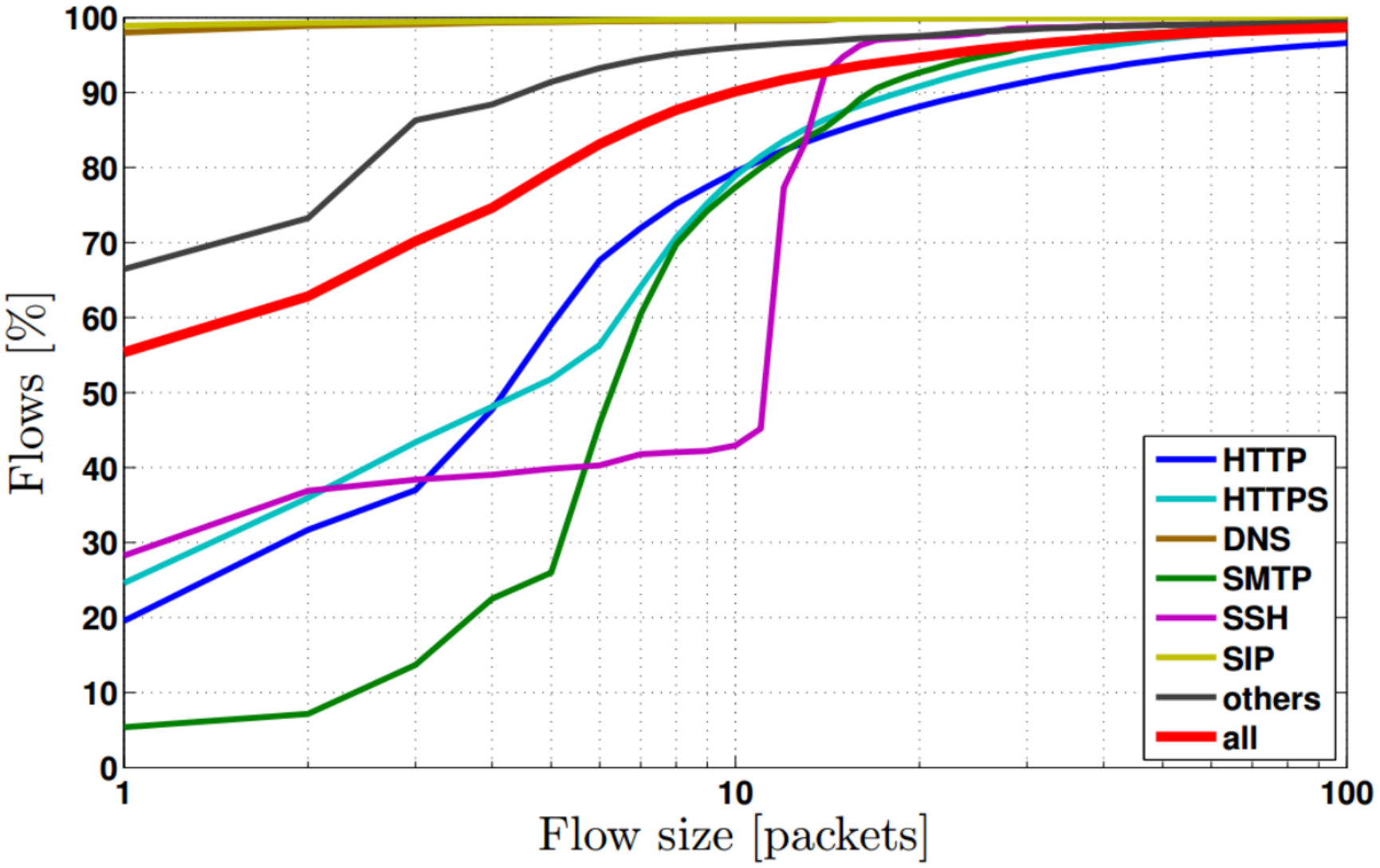


Already Tested Scenarios

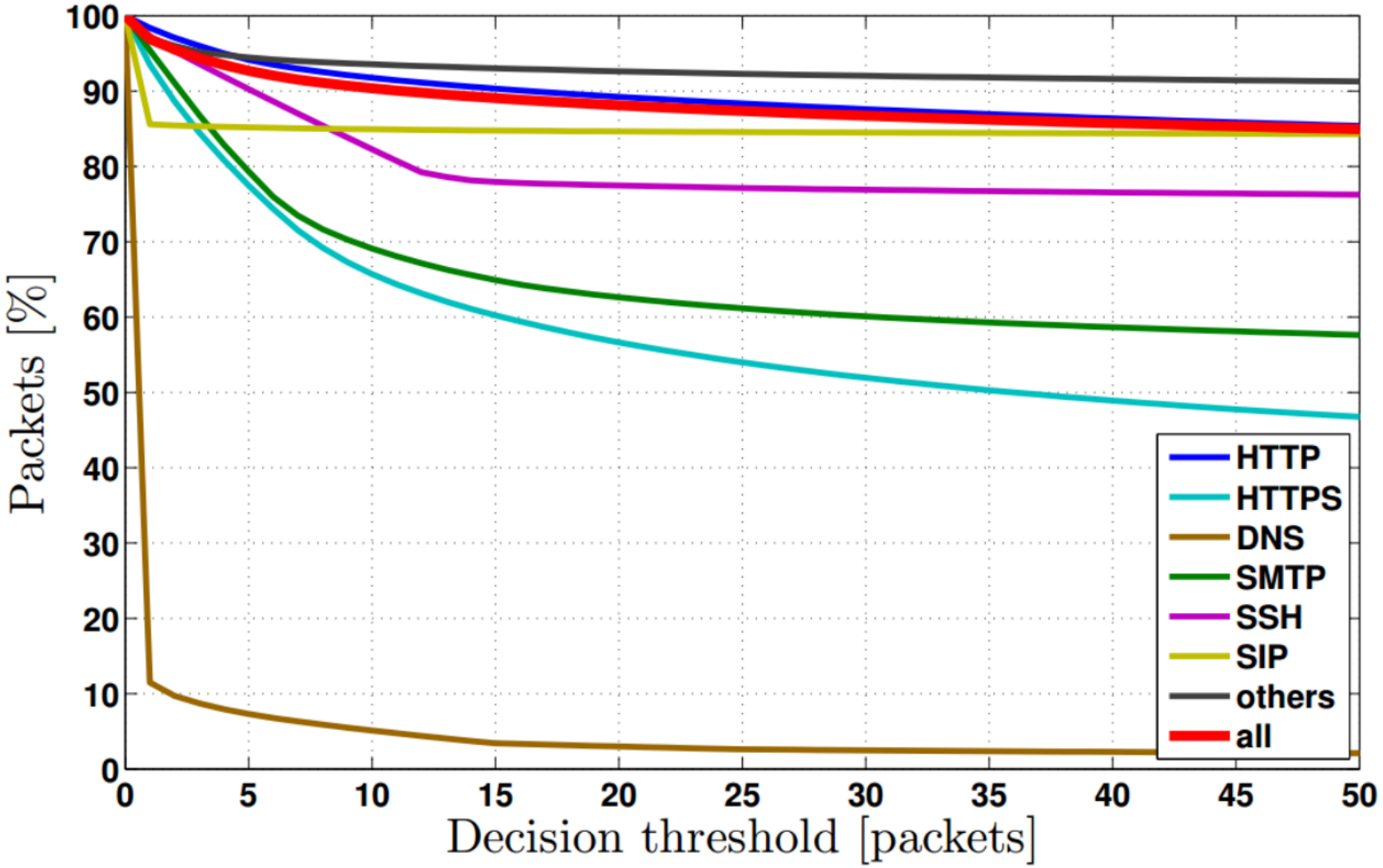
- Detection of network scans
- Communication tunnels via DNS
- Guessing SIP dial plan

Using SDM with Time Machine, we can get evidence and verification of detected events.

Flow Size – are *n* packets enough?



Stored/skipped packets



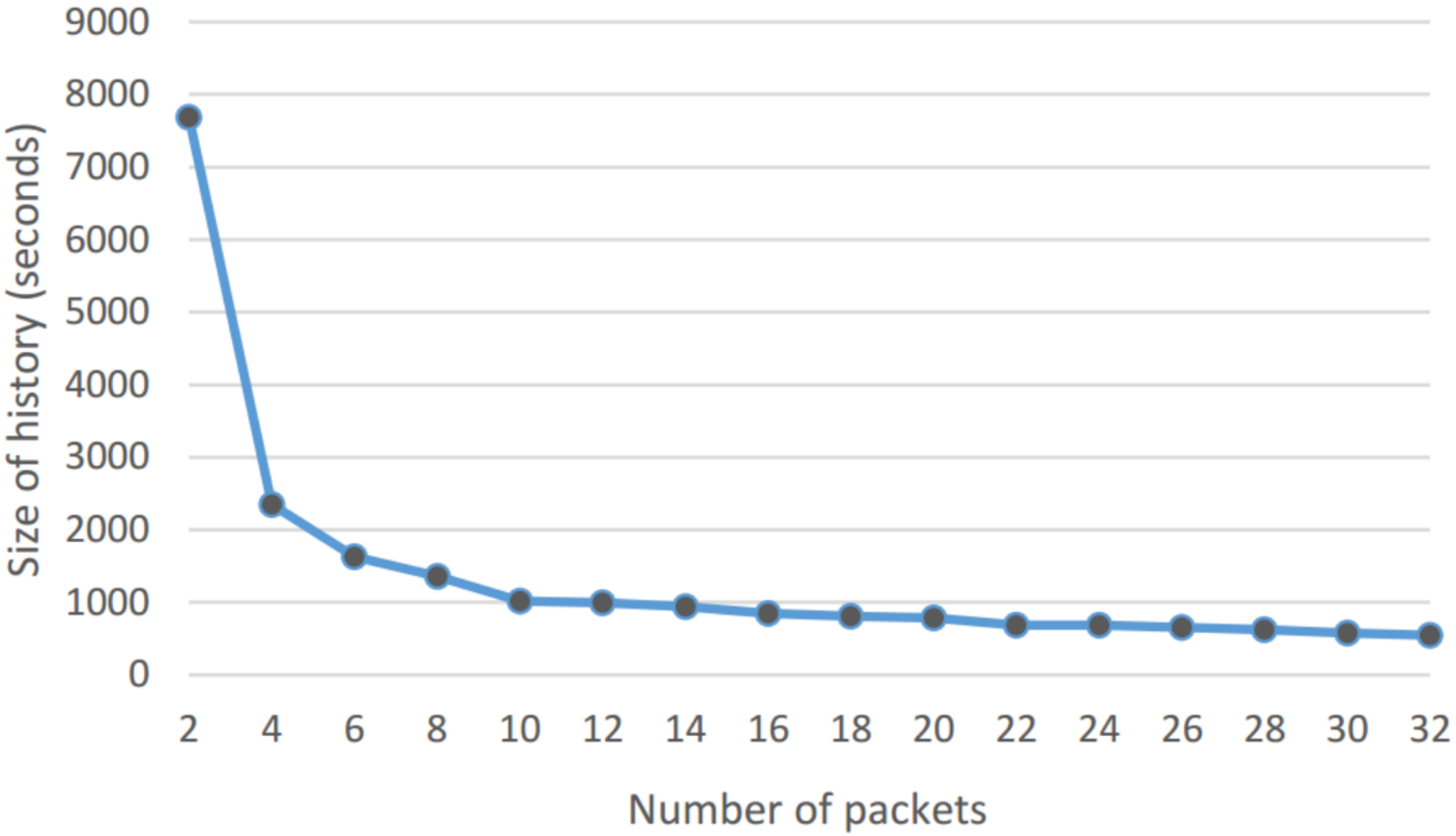
Configuration of network probe

- *24 CPU cores*
- *64 GB RAM*
- *80 Gbps* COMBO card (capable of SDM)

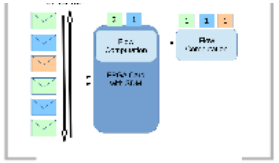
- Using *56 GB*,
- at *80 Gbps* line,
- storing first *10 packets* of each flow,
- we can store about *15 min* of traffic.

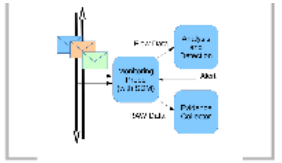
- Note: it is highly dependend on traffic volume and distribution.

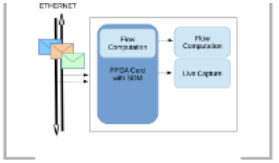
Size of stored history - 56 GB TM



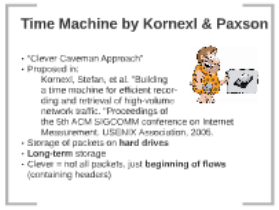
SDM Feedback 2

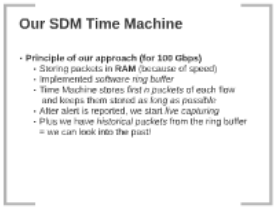


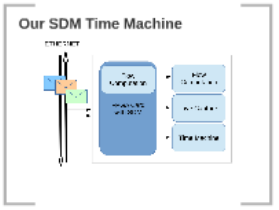




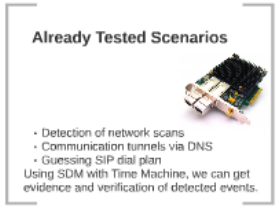
DM Timemachine 3

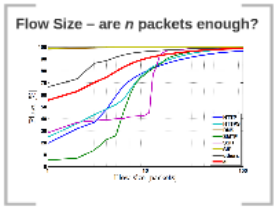


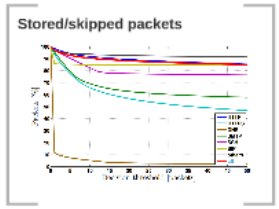




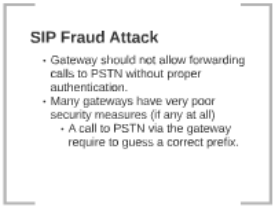
Measurements 4

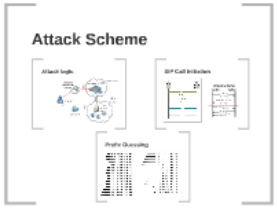


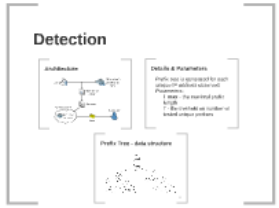




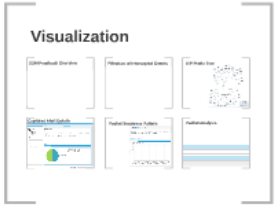
SIP Fraud Attack 5



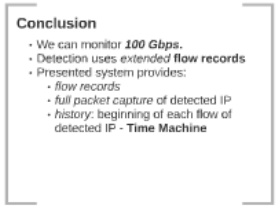




Visualization 6



Conclusion 7

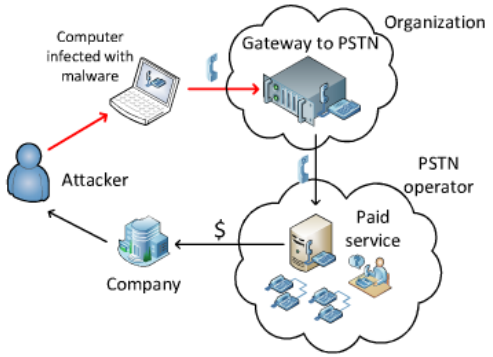


SIP Fraud Attack

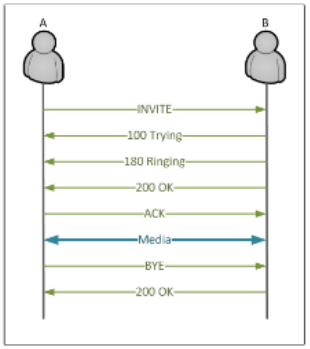
- Gateway should not allow forwarding calls to PSTN without proper authentication.
- Many gateways have very poor security measures (if any at all)
  - A call to PSTN via the gateway require to guess a correct prefix.

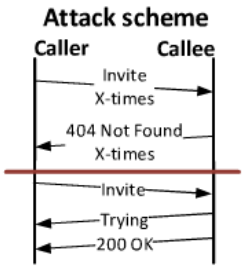
Attack Scheme

Attack logic



SIP Call Initiation



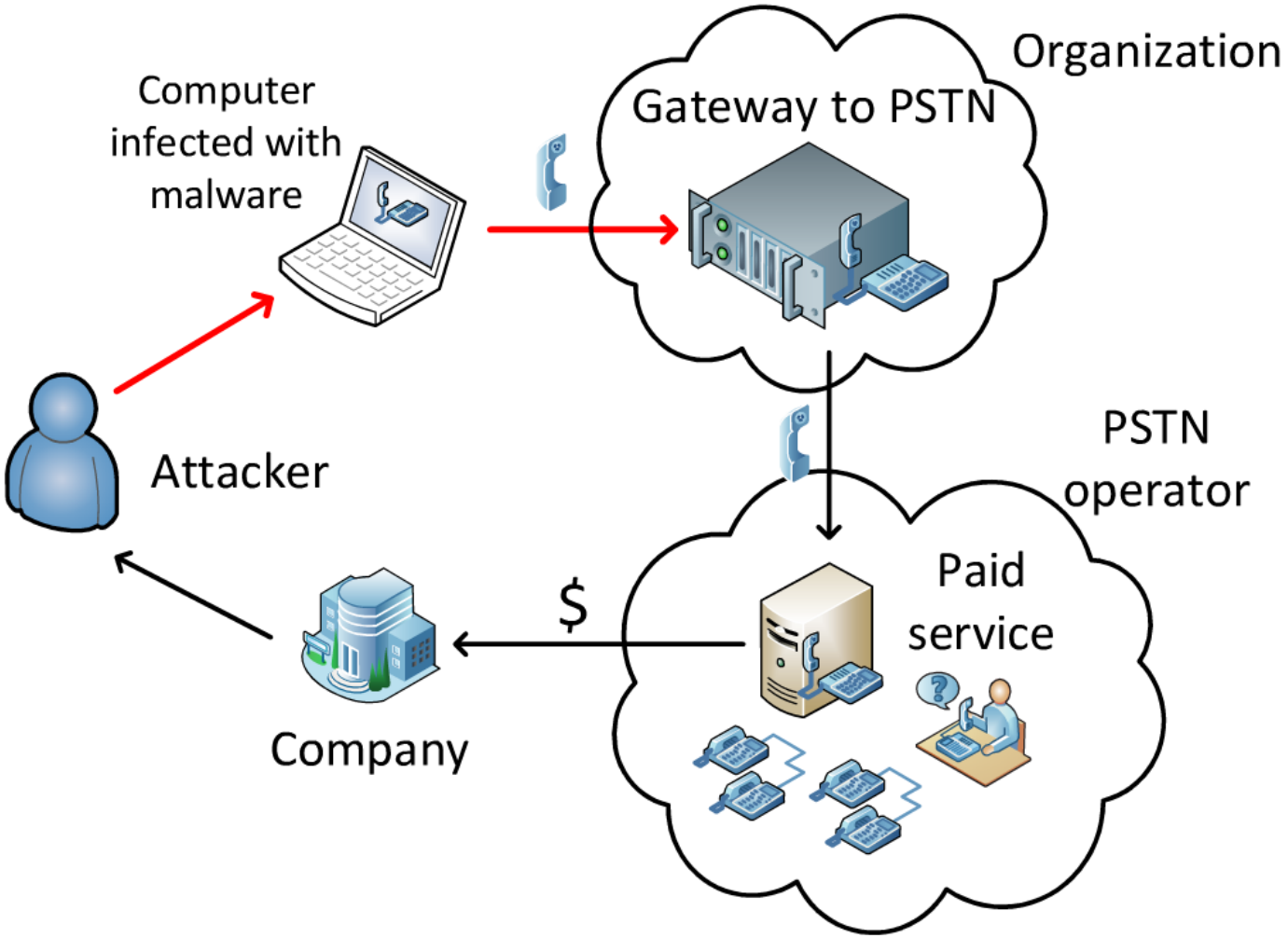


Prefix Guessing

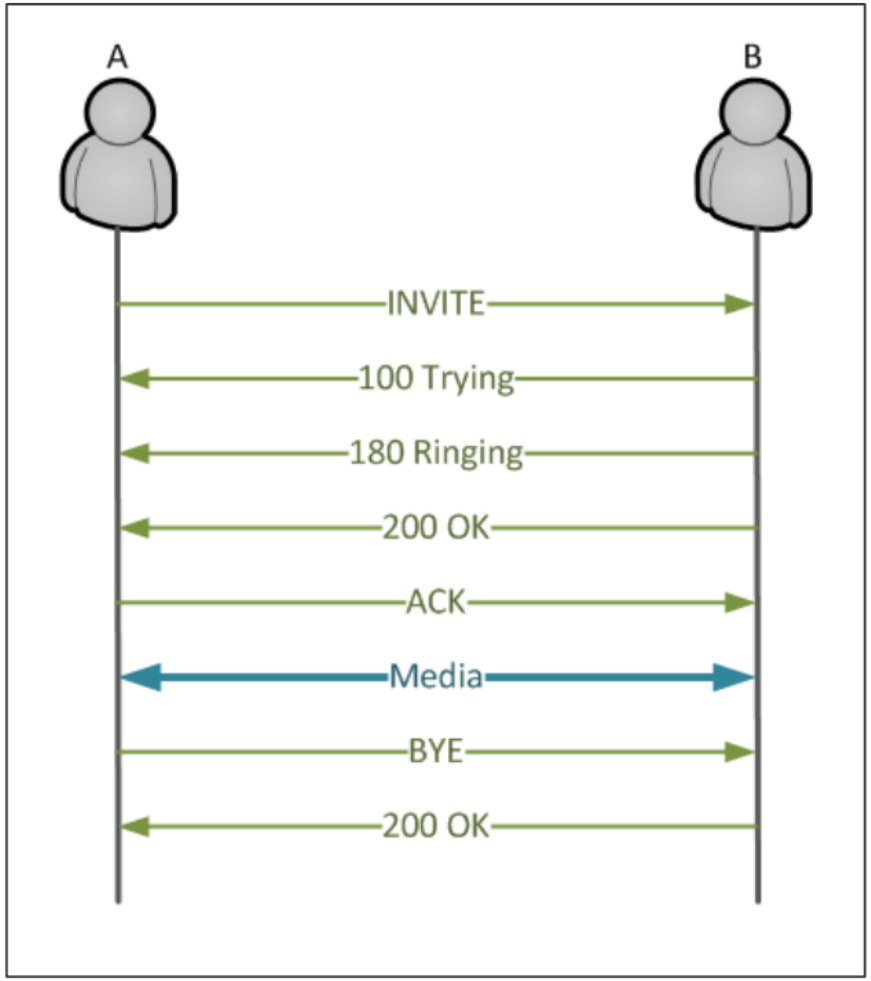
00972592577956@A.B.C.D
000972592577956@A.B.C.D
900972592577956@A.B.C.D
+972592577956@A.B.C.D
972592577956@A.B.C.D
100972592577956@A.B.C.D
800972592577956@A.B.C.D
600972592577956@A.B.C.D
700972592577956@A.B.C.D
400972592577956@A.B.C.D
300972592577956@A.B.C.D
200972592577956@A.B.C.D
500972592577956@A.B.C.D
9990972592577956@A.B.C.D
99990972592577956@A.B.C.D
999990972592577956@A.B.C.D

99999900972592577956@A.B.C.D
999999900972592577956@A.B.C.D
9999999900972592577956@A.B.C.D
99999999900972592577956@A.B.C.D
999999999900972592577956@A.B.C.D
9000972592577956@A.B.C.D
0972592577956@A.B.C.D
0000972592577956@A.B.C.D
00000000972592577956@A.B.C.D
00000000972592577956@A.B.C.D
000000000972592577956@A.B.C.D
0000000000972592577956@A.B.C.D
91000972592577956@A.B.C.D
9900972592577956@A.B.C.D
9100972592577956@A.B.C.D
...

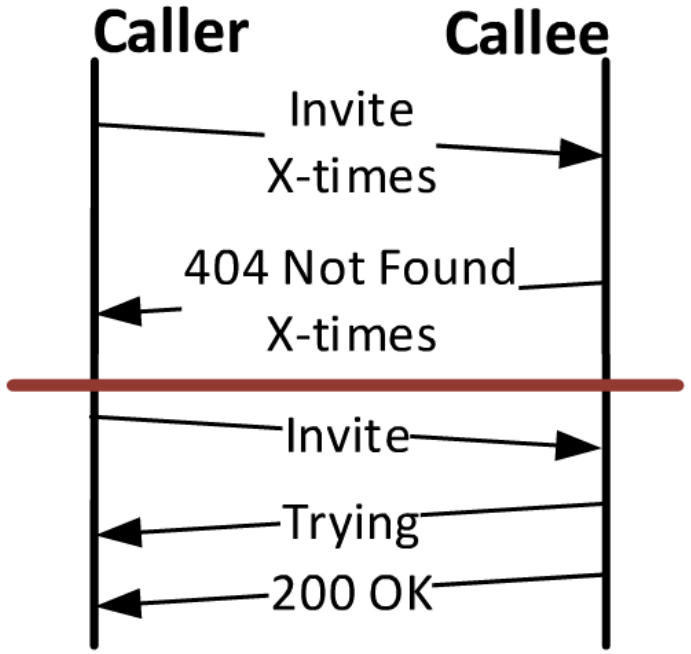
Attack logic



SIP Call Initiation



Attack scheme



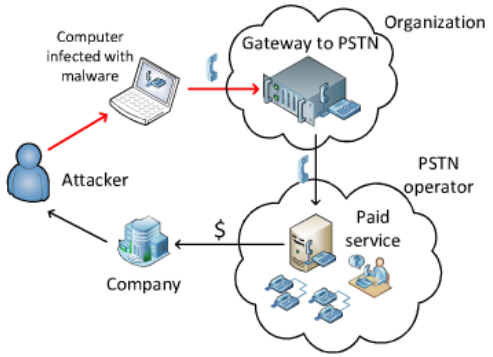
Prefix Guessing

0097259257956@A.B.C.D
00097259257956@A.B.C.D
90097259257956@A.B.C.D
+97259257956@A.B.C.D
97259257956@A.B.C.D
10097259257956@A.B.C.D
80097259257956@A.B.C.D
60097259257956@A.B.C.D
70097259257956@A.B.C.D
40097259257956@A.B.C.D
30097259257956@A.B.C.D
20097259257956@A.B.C.D
50097259257956@A.B.C.D
990097259257956@A.B.C.D
9990097259257956@A.B.C.D
99990097259257956@A.B.C.D

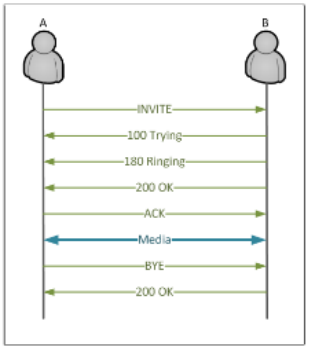
999999097259257956@A.B.C.D
9999999097259257956@A.B.C.D
99999990097259257956@A.B.C.D
999999990097259257956@A.B.C.D
9999999990097259257956@A.B.C.D
900097259257956@A.B.C.D
097259257956@A.B.C.D
00097259257956@A.B.C.D
00000097259257956@A.B.C.D
000000097259257956@A.B.C.D
0000000097259257956@A.B.C.D
00000000097259257956@A.B.C.D
9100097259257956@A.B.C.D
990097259257956@A.B.C.D
910097259257956@A.B.C.D
. . .

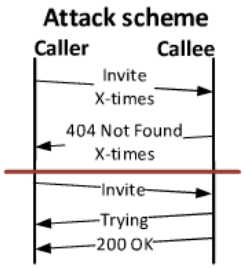
Attack Scheme

Attack logic



SIP Call Initiation





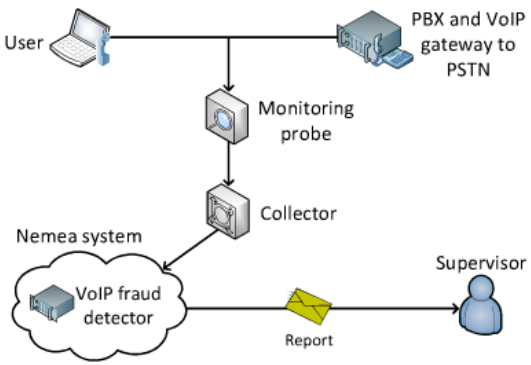
Prefix Guessing

00972592577956@A.B.C.D
000972592577956@A.B.C.D
900972592577956@A.B.C.D
+972592577956@A.B.C.D
972592577956@A.B.C.D
100972592577956@A.B.C.D
800972592577956@A.B.C.D
600972592577956@A.B.C.D
700972592577956@A.B.C.D
400972592577956@A.B.C.D
300972592577956@A.B.C.D
200972592577956@A.B.C.D
500972592577956@A.B.C.D
9990972592577956@A.B.C.D
99990972592577956@A.B.C.D
999990972592577956@A.B.C.D

99999900972592577956@A.B.C.D
999999900972592577956@A.B.C.D
9999999900972592577956@A.B.C.D
99999999900972592577956@A.B.C.D
999999999900972592577956@A.B.C.D
9000972592577956@A.B.C.D
0972592577956@A.B.C.D
0000972592577956@A.B.C.D
00000000972592577956@A.B.C.D
00000000972592577956@A.B.C.D
000000000972592577956@A.B.C.D
0000000000972592577956@A.B.C.D
91000972592577956@A.B.C.D
9900972592577956@A.B.C.D
9100972592577956@A.B.C.D
...

Detection

Architecture

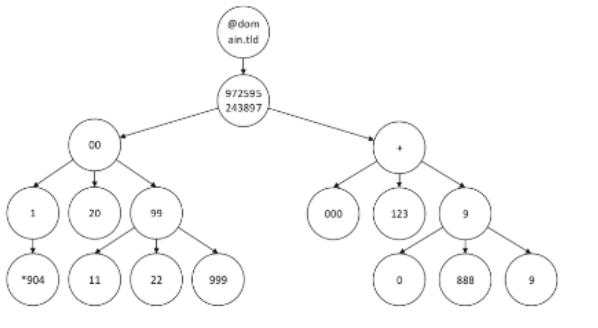


Details & Parameters

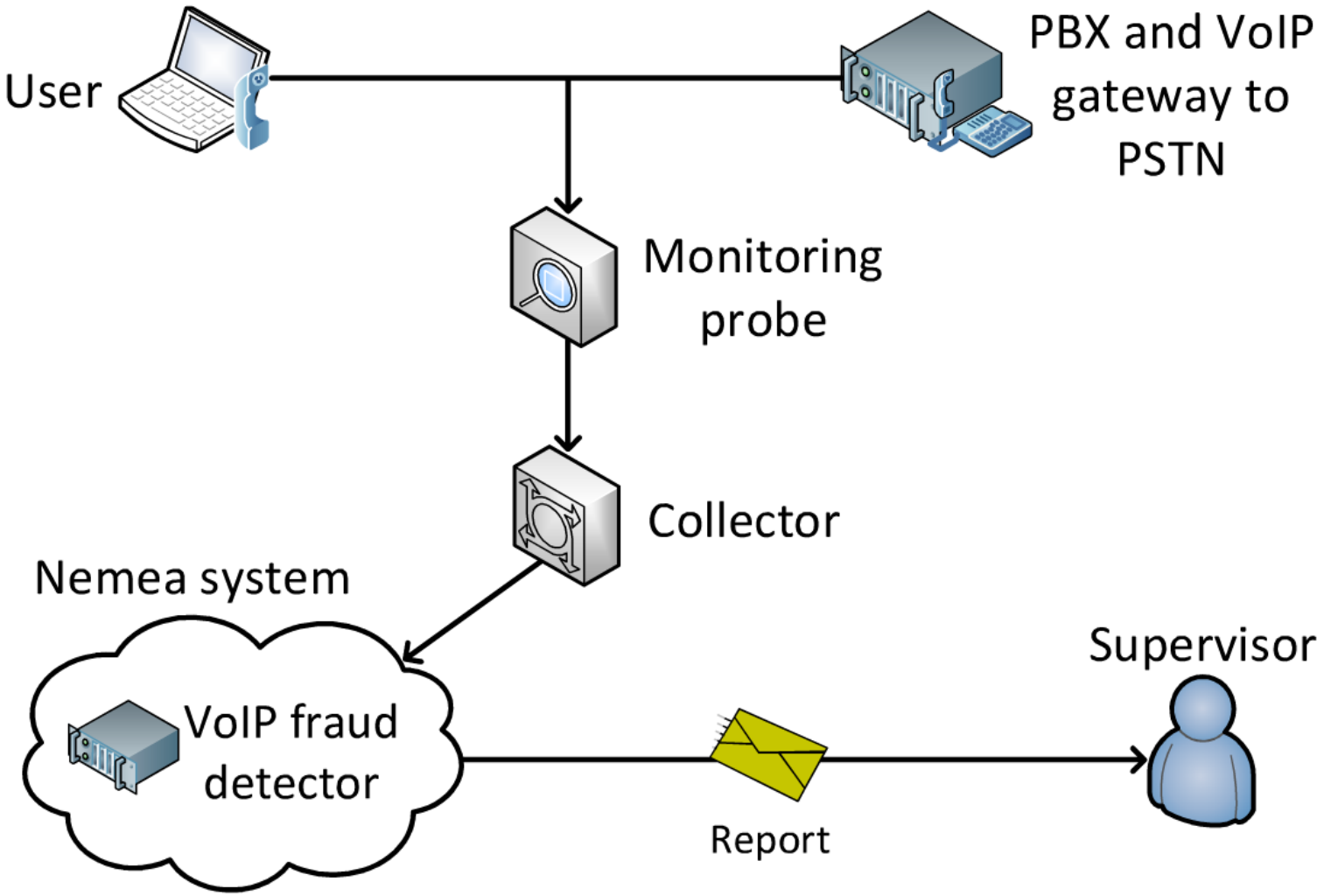
Prefix tree is generated for each unique IP address observed.
Parameters:

l_max - the maximal prefix length
T - the treshold on number of tested unique prefixes

Prefix Tree - data structure



Architecture



Details & Parameters

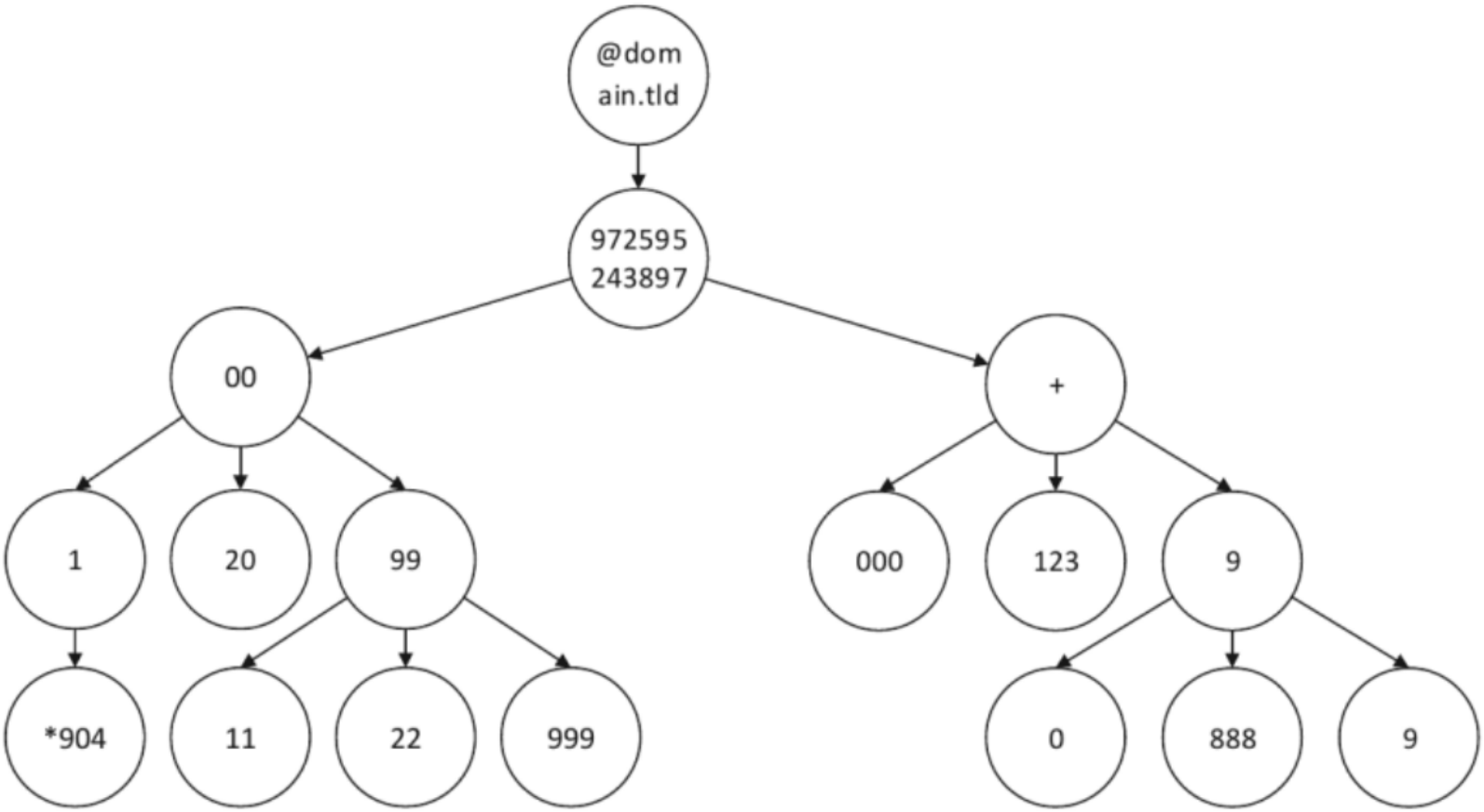
Prefix tree is generated for each unique IP address observed.

Parameters:

l_max - the maximal prefix length

T - the treshold on number of tested unique prefixes

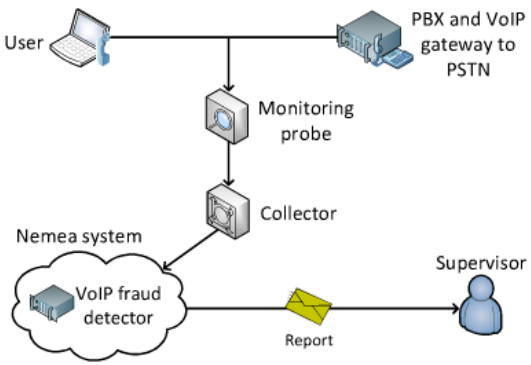
Prefix Tree - data structure



baf

Detection

Architecture

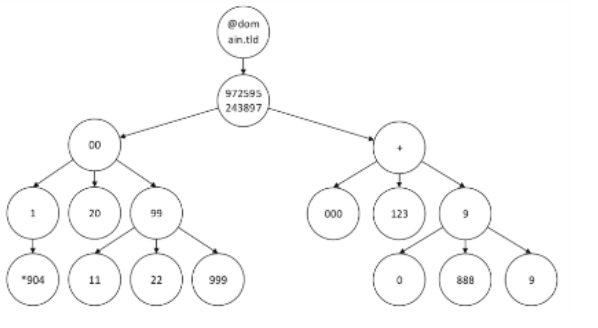


Details & Parameters

Prefix tree is generated for each unique IP address observed.
Parameters:

l_max - the maximal prefix length
T - the treshold on number of tested unique prefixes

Prefix Tree - data structure



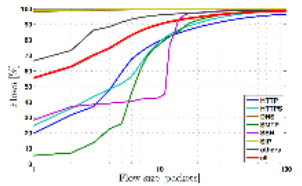
Measurements 4

Already Tested Scenarios

- Detection of network scans
- Communication tunnels via DNS
- Guessing SIP dial plan

Using SDM with Time Machine, we can get evidence and verification of detected events.

Flow Size – are *n* packets enough?

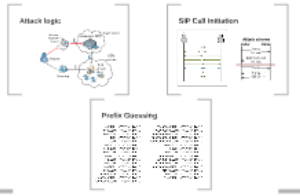


P Fraud Attack 5

SIP Fraud Attack

- Gateway should not allow forwarding calls to PSTN without proper authentication.
- Many gateways have very poor security measures (if any at all)
  - A call to PSTN via the gateway require to guess a correct prefix.

Attack Scheme



Visualization 6

Netfox Detective

Visualization

Conclusion 7

Conclusion

- We can monitor ***100 Gbps***.
- Detection uses *extended* **flow records**
- Presented system provides:
  - *flow records*
  - *full packet capture* of detected IP
  - *history*: beginning of each flow of detected IP - **Time Machine**

1996–2016 CESNET

Thank you!
Any questions?

@liberouter

https://www.liberouter.org

This presentation

My contact

Acknowledgment
- Tomas Cejka
- Zdenek Rosa
- Tomas Jansky
- Viktor Pus

Jan Pluskal

Netfox Detective

WEB

HTTP
SSL/TLS

IM

XMPP
YMSG
OSCAR

Emails

IMAP
POP3
SMTP

Webmail

Gmail
Seznam.cz
Yahoo
Email.cz
MS Live
Centrum.cz
Atlas.cz
Mujmail.cz
Roundcube
Horde
Etc...

VoIP

RTP
SIP

Games

Minecraft
Warcraft

Social Networks

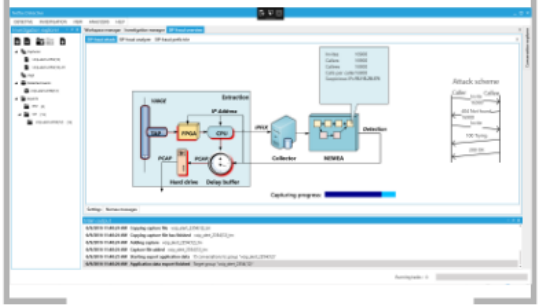
Facebook

Crypto currencies

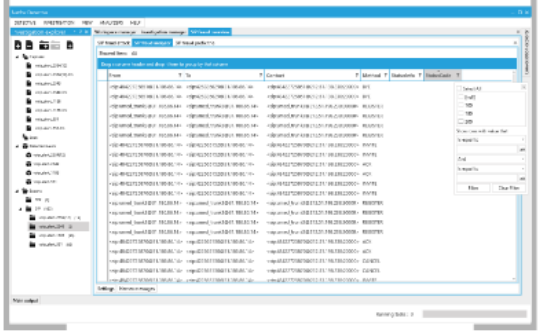
BitCoin

Visualization

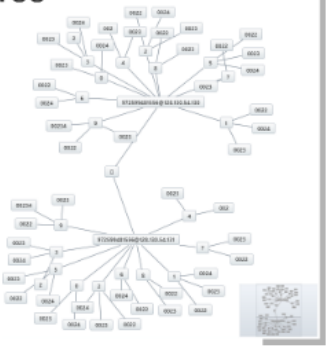
SDM Feedback Overview



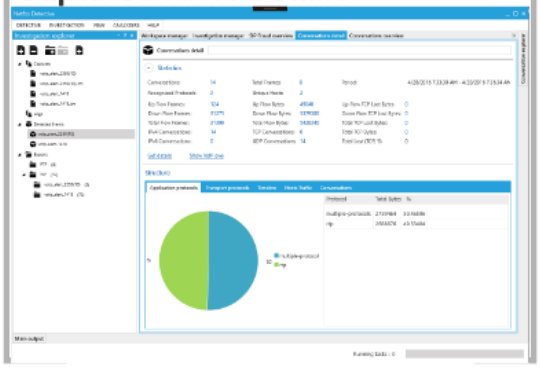
Filtration of Intercepted Events



SIP Prefix Tree

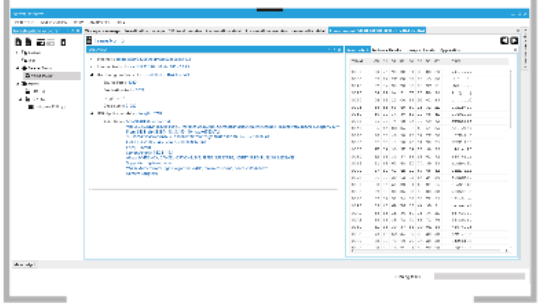


Captured Alert Details

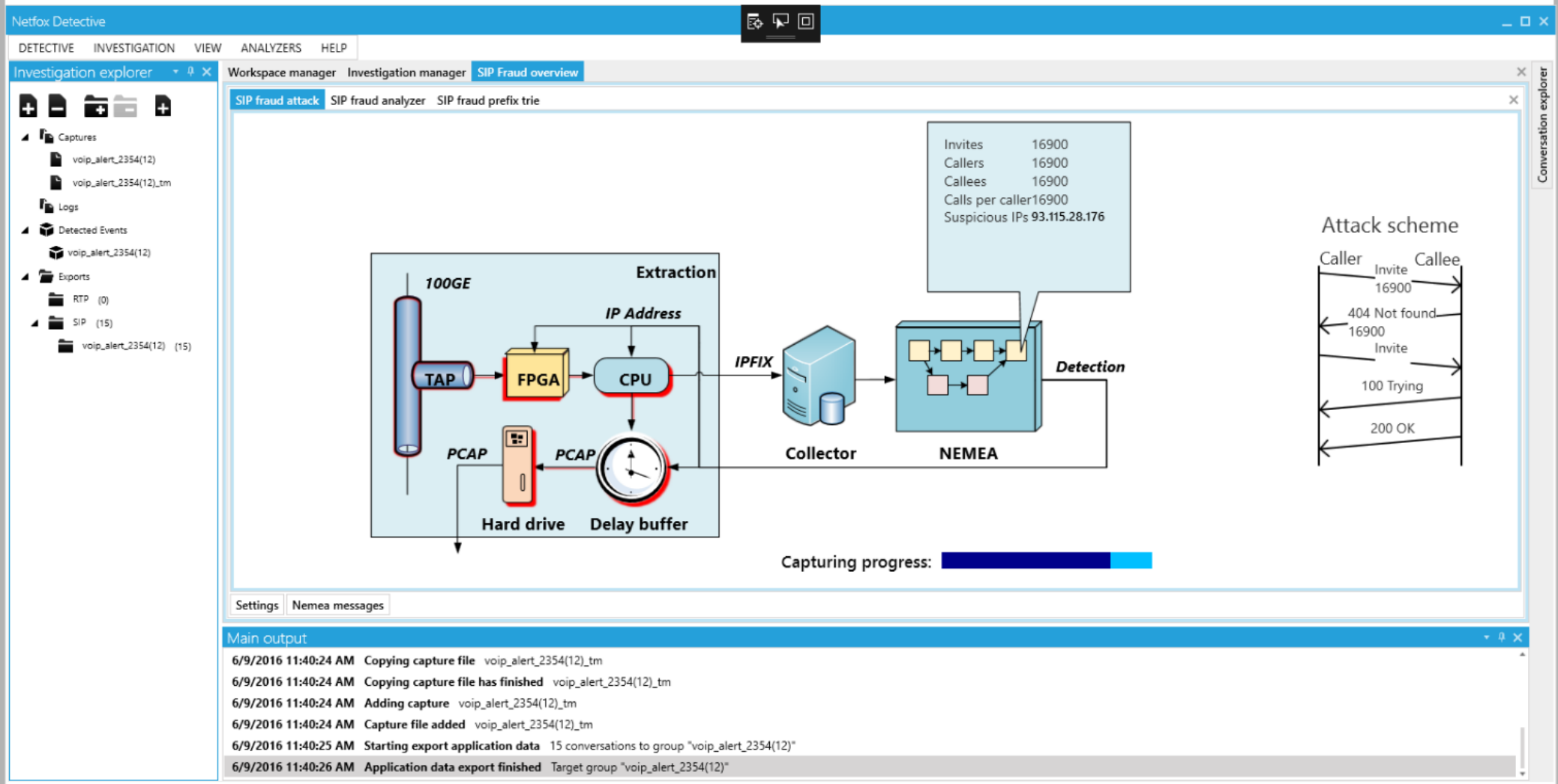


Packet Sequence Pattern

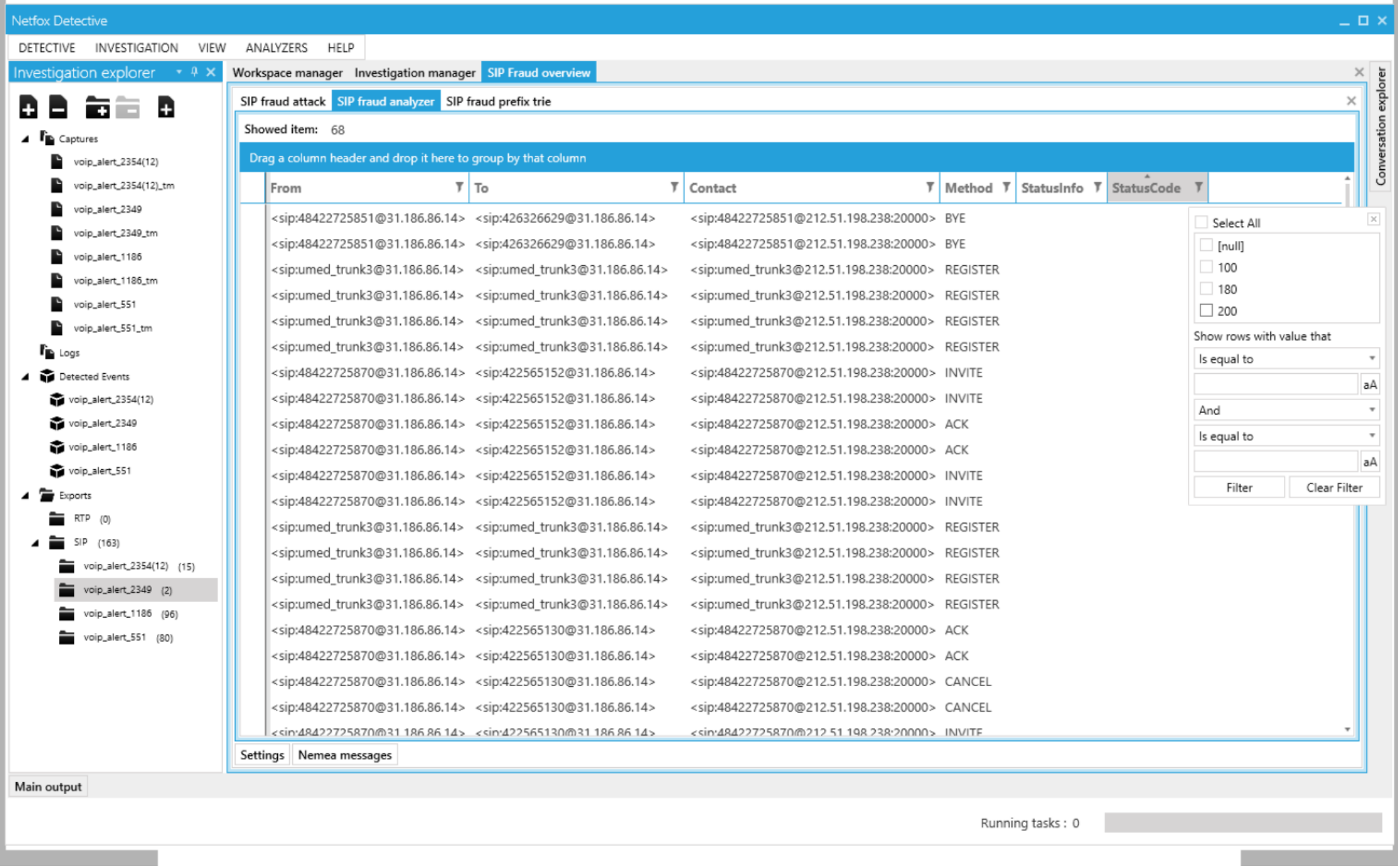
Packet Analysis



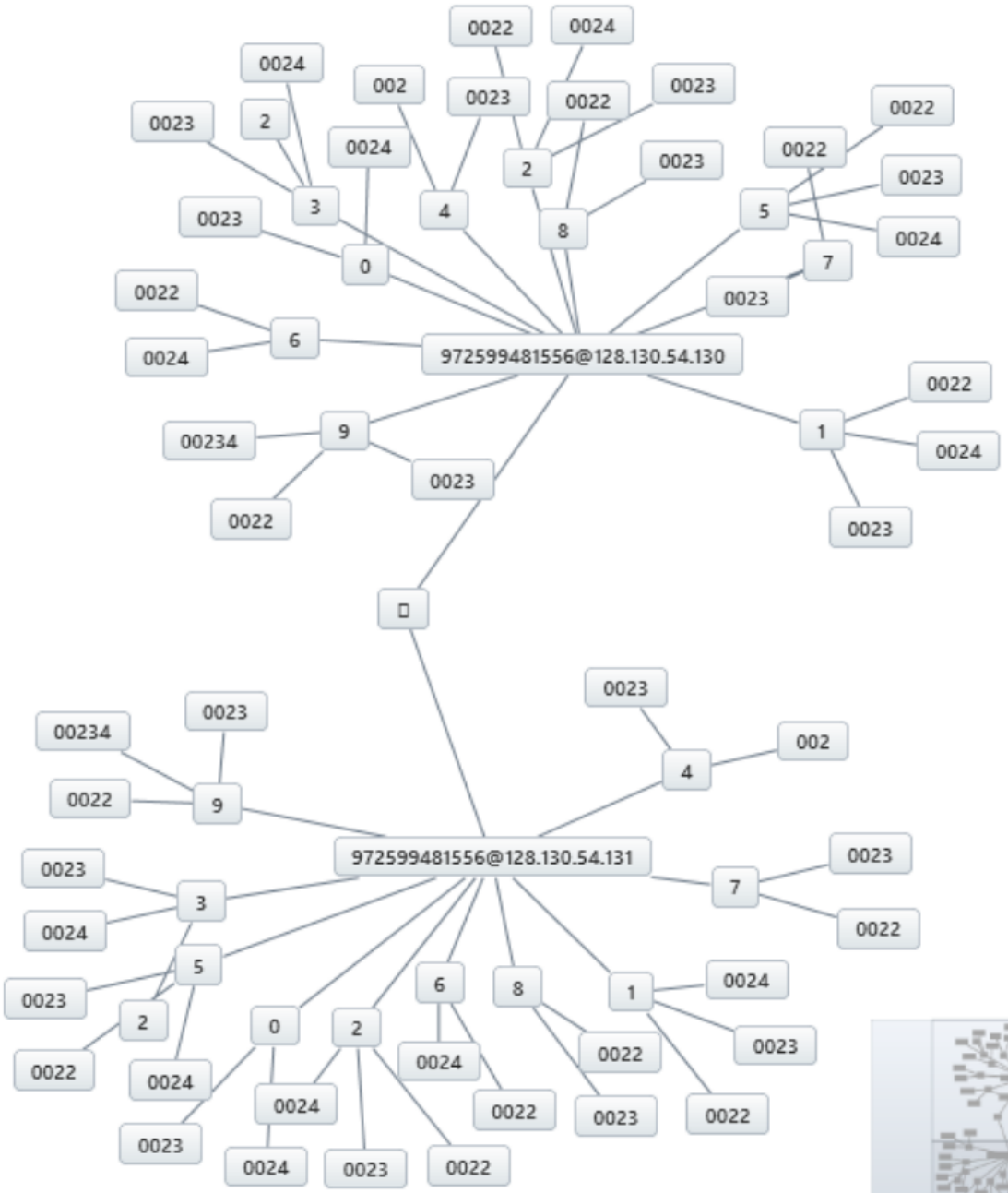
SDM Feedback Overview



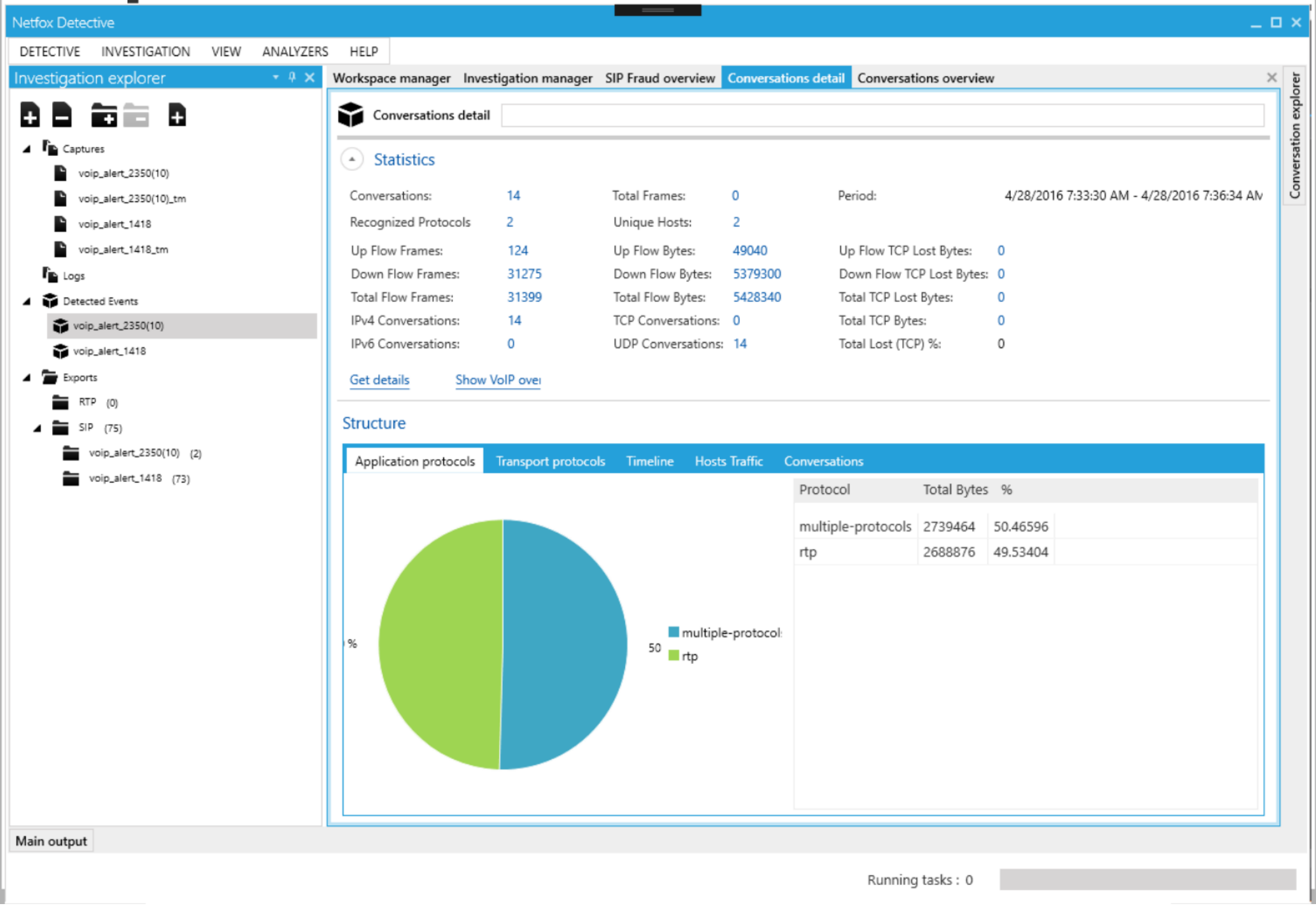
Filtration of Intercepted Events



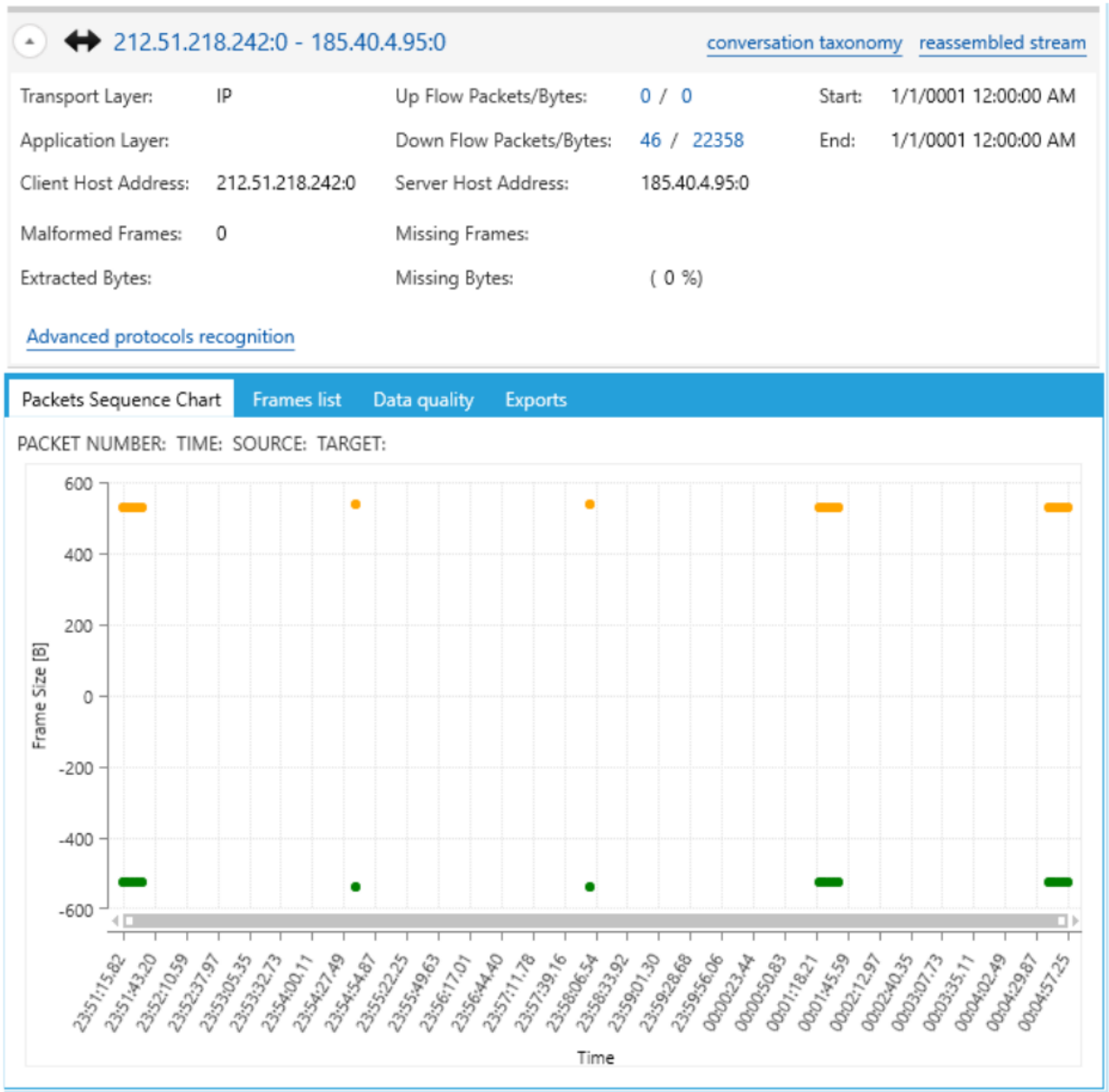
SIP Prefix Tree



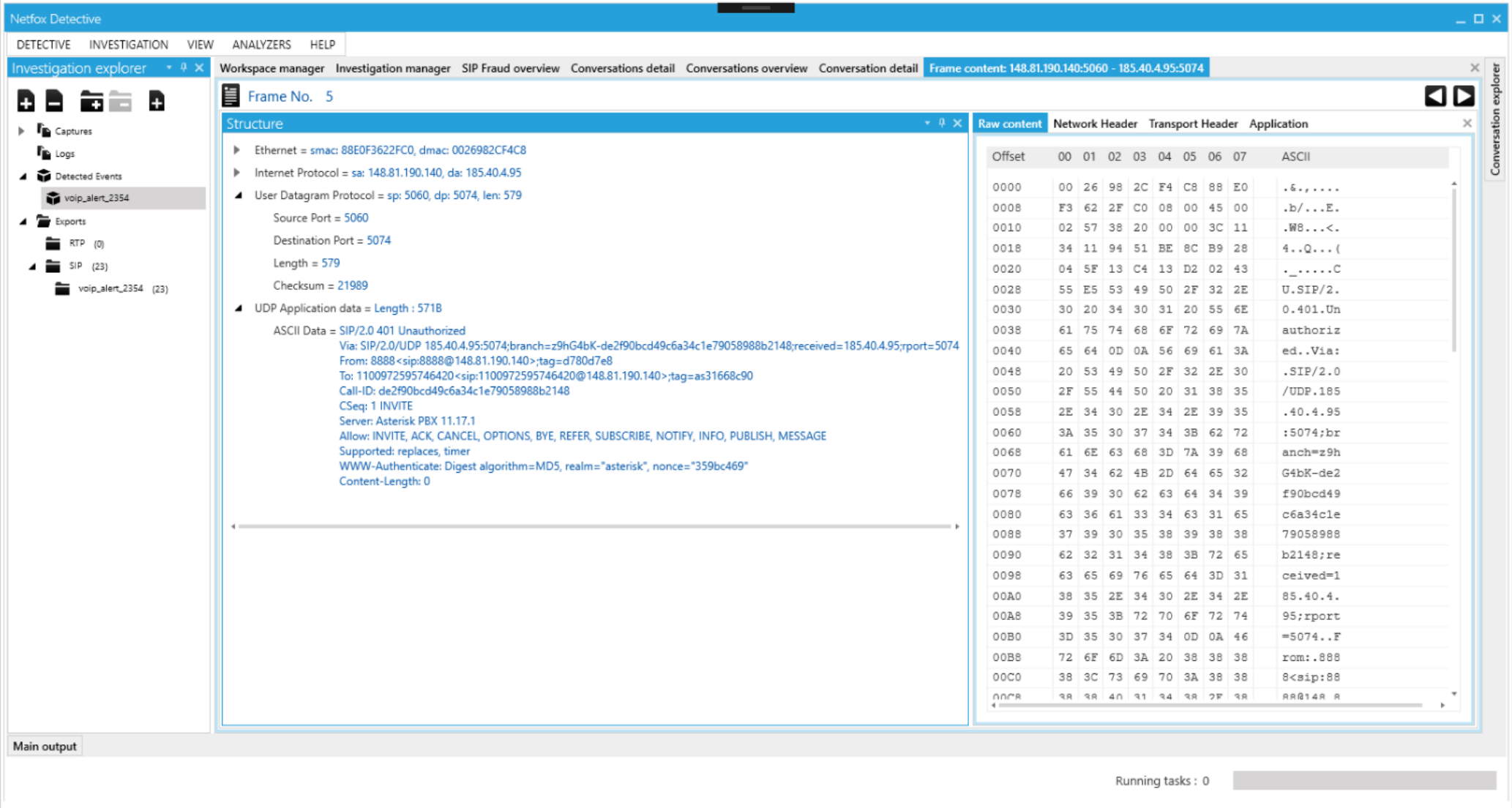
Captured Alert Details



Packet Sequence Pattern

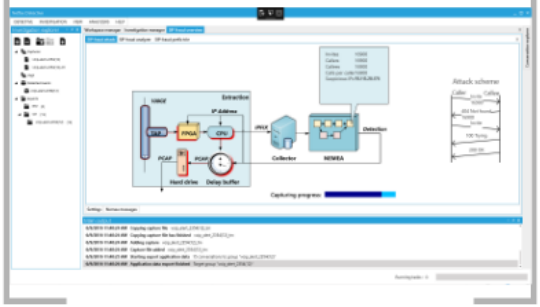


Packet Analysis

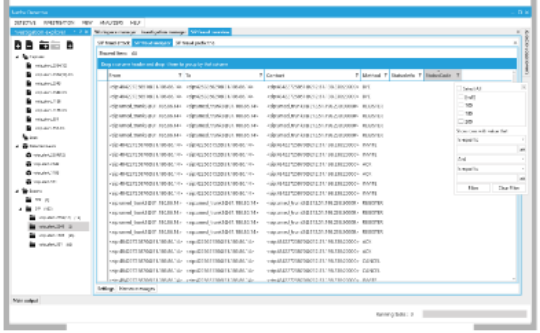


Visualization

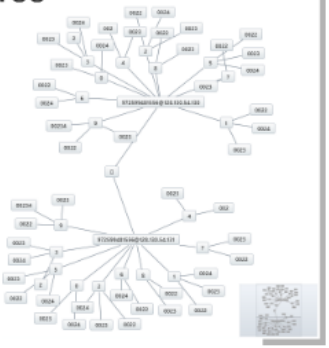
SDM Feedback Overview



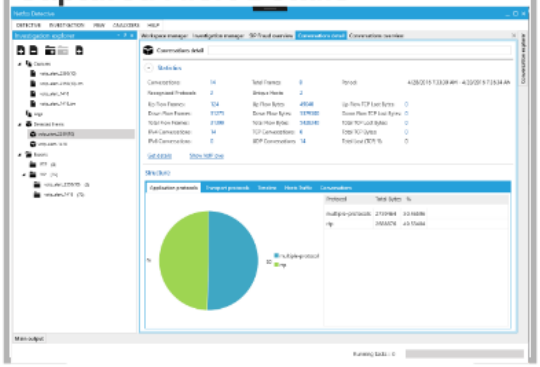
Filtration of Intercepted Events



SIP Prefix Tree

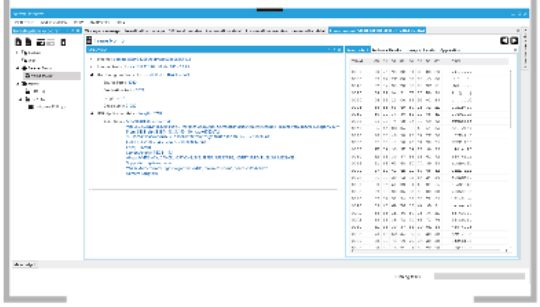


Captured Alert Details



Packet Sequence Pattern

Packet Analysis



Fraud Attack 5

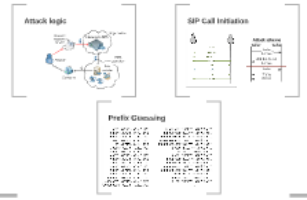
Visualization 6

Conclusion 7

SIP Fraud Attack

- Gateway should not allow forwarding calls to PSTN without proper authentication.
- Many gateways have very poor security measures (if any at all)
  - A call to PSTN via the gateway require to guess a correct prefix.

Attack Scheme



Netfox Detective

Visualization

Conclusion

- We can monitor ***100 Gbps***.
- Detection uses *extended* **flow records**
- Presented system provides:
  - *flow records*
  - *full packet capture* of detected IP
  - *history*: beginning of each flow of detected IP - **Time Machine**

Thank you! Any questions?

1996–2016
CESNET

@liberouter

https://www.liberouter.org

This presentation

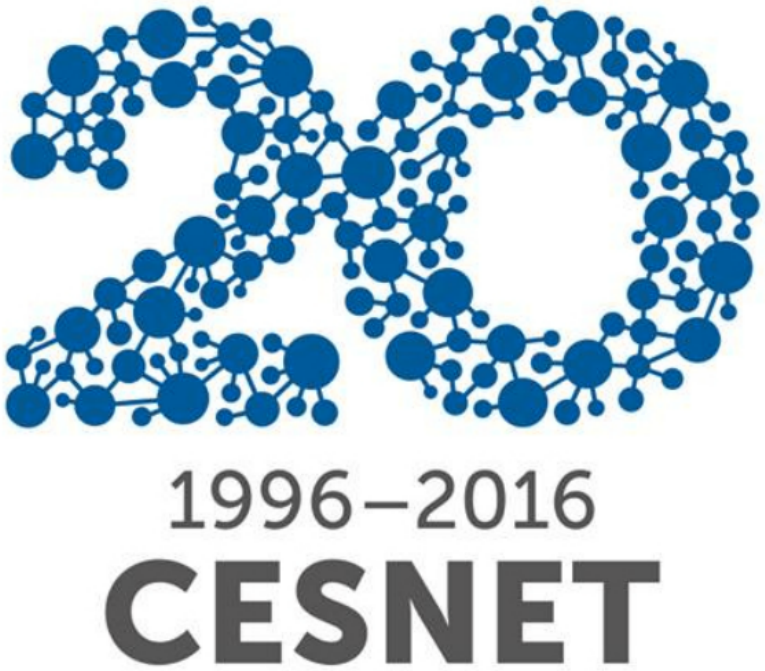
My contact

Acknowledgment
- Tomas Cejka
- Zdenek Rosa
- Tomas Jansky
- Viktor Puš

Jan Pluskal

Conclusion

- We can monitor ***100 Gbps*.**
- Detection uses *extended* **flow records**
- Presented system provides:
  - *flow records*
  - *full packet capture* of detected IP
  - *history*: beginning of each flow of detected IP - **Time Machine**



Thank you!
Any questions?

@liberouter

https://www.liberouter.org

This presentation

https://prezi.com/rbwm_9todtb7

Acknowledgment

- Tomas Cejka
- Zdenek Rosa
- Tomas Jansky
- Viktor Pus

My contact

Jan Pluskal

Bibliography

- **Benáček, P., Blažek, R.B., Čejka, T., Kubátová, H.**: "*Change-Point Detection Method on 100 Gb/s Ethernet Interface*", ACM/IEEE Symposium on Architectures for Networking and Communications Systems 2014 (ANCS2014), Marina del Rey, CA, USA, 2014
- **Čejka, T., Kekely, L., Benáček, P., Blažek, R.B., Kubátová, H.**: "*FPGA Accelerated Change-Point Detection Method for 100 Gb/s Networks*", Doctoral Workshop on Mathematical and Engineering Methods in Computer Science (MEMICS), 2014 (will be published in Oct. 2014)
- **Čejka, T., Rosa, Z., Kubátová, H.**: "*Stream-wise Detection of Surreptitious Traffic over DNS*", 19th IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (IEEE CAMAD 2014), Athens, Greece, 2014 (will be published in Dec. 2014)

- Lots of Google indexed images has been used for this presentation...credit goes to their creators!