User-Centered Visual Analysis of PCAP Data

Dr. Alex Ulmer

Introduction

Dr. Alex Ulmer

Research: User-Centered Data Science and Progressive Visual Analytics

Application Area: Cybersecurity

Visual Analysis of PCAP Data

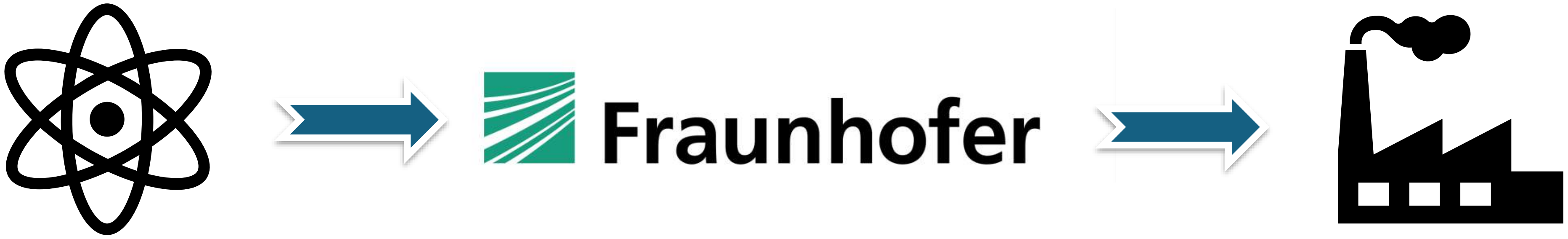
Agenda

1.	Introduction & Agenda	1 min	
2.	Fraunhofer – Applied Research	2 min	<10
3.	Data Science and Visual Analytics	6 min	
4.	Visual Analysis of PCAP Data - Live	15 min	
5.	Application Classification of Packets	7 min	
6.	Explainable AI	9 min	
7.	Visualization Plugin for Wireshark	$_3$5 min	

45 ✓

2. Fraunhofer – Applied Research

Fraunhofer Mission



Explore research ideas and get them market ready

Collaborate with businesses

Create an advantage in the market

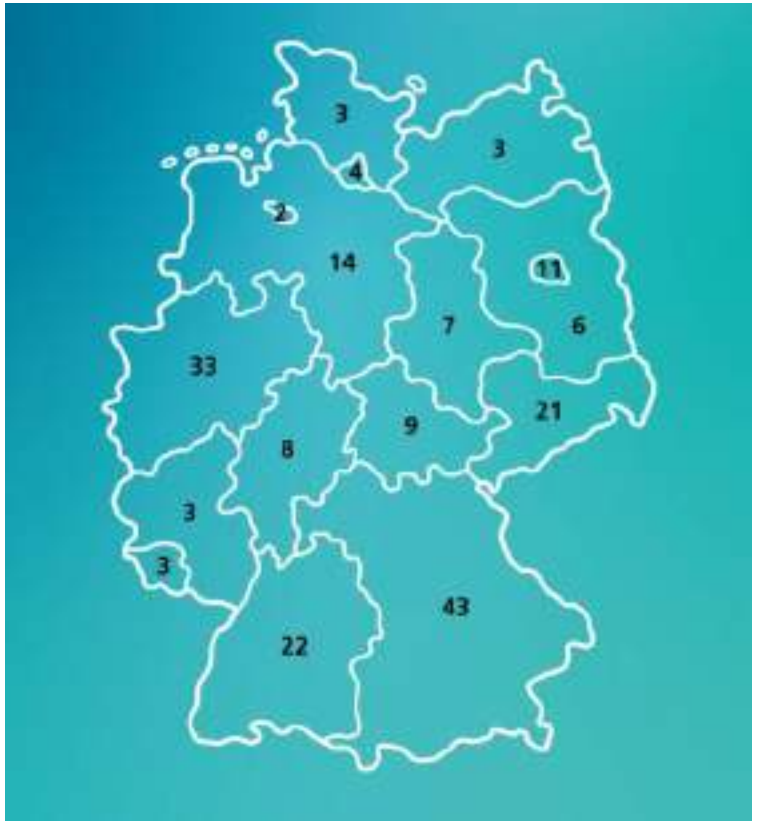
Fraunhofer Institute

76 Institutes
@ 192 locations in Germany

Topics:

- Digitalization
- Energy
- Health and Medicine
- Mobility and Transport
- Work and Management
- Mechanics and Production
- Society and Security

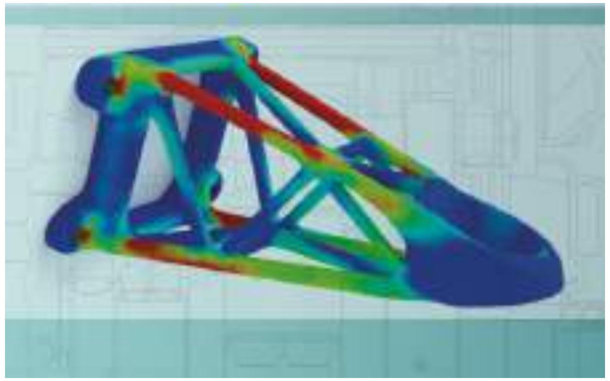
Fraunhofer



Fraunhofer Institute for Computer Graphics Research

40 Years of Computer Graphics Research

Computer Vision, Simulation, 3D Printing,



User Centered Data Science and Visual Analytics

3. Data Science and Visual Analytics

Why Visualization?

A is connected to B

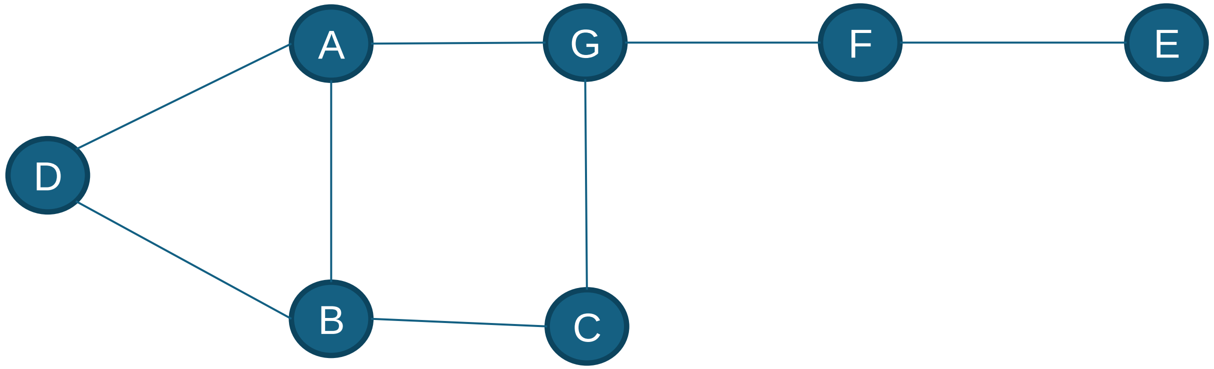
B is connected to C

D is connected to A and B

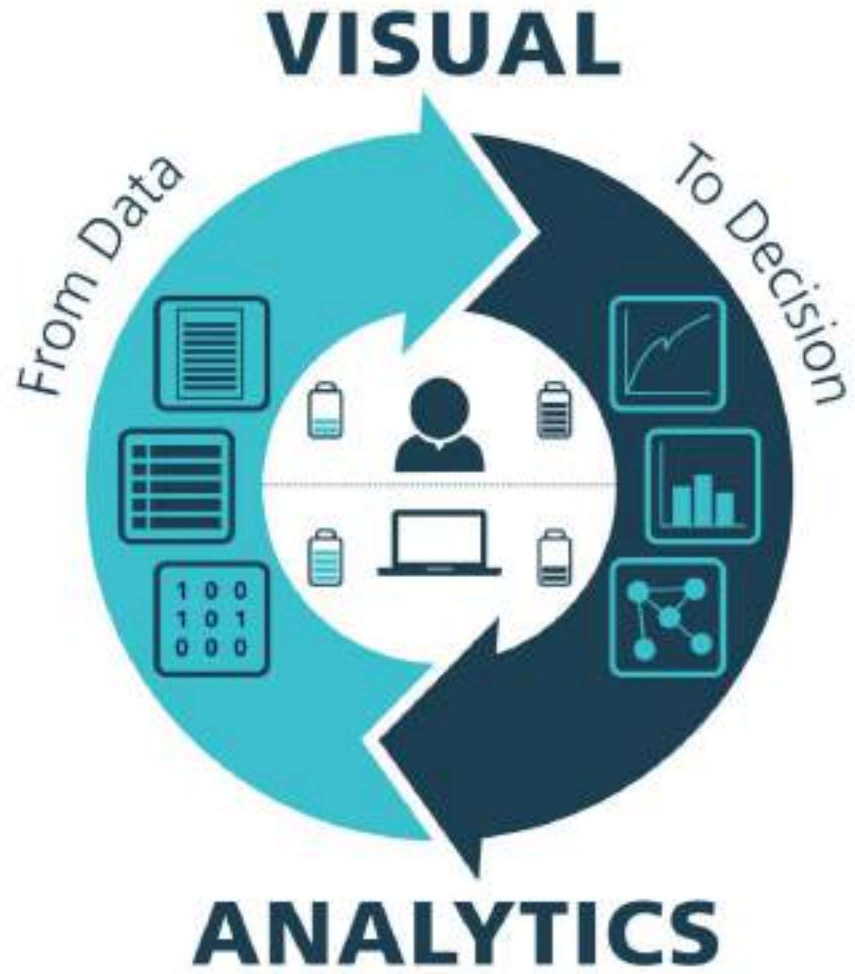
E is connected to F

G is connected to A and C

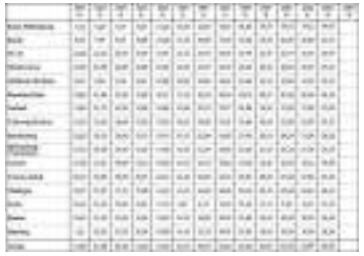
F is connected to G

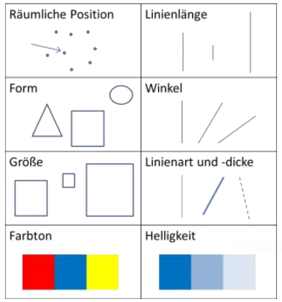


Data Science and Visual Analytics



From Raw Data to Visualizations

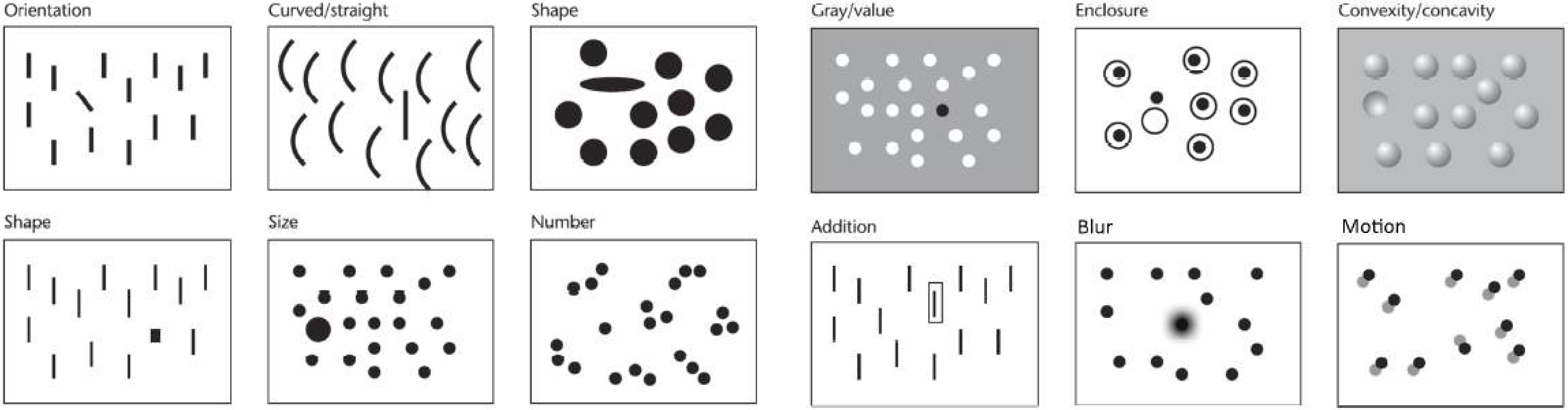




Raw Data → Data Tables → Visual Structures → Views

adapted from Card et al. 1999

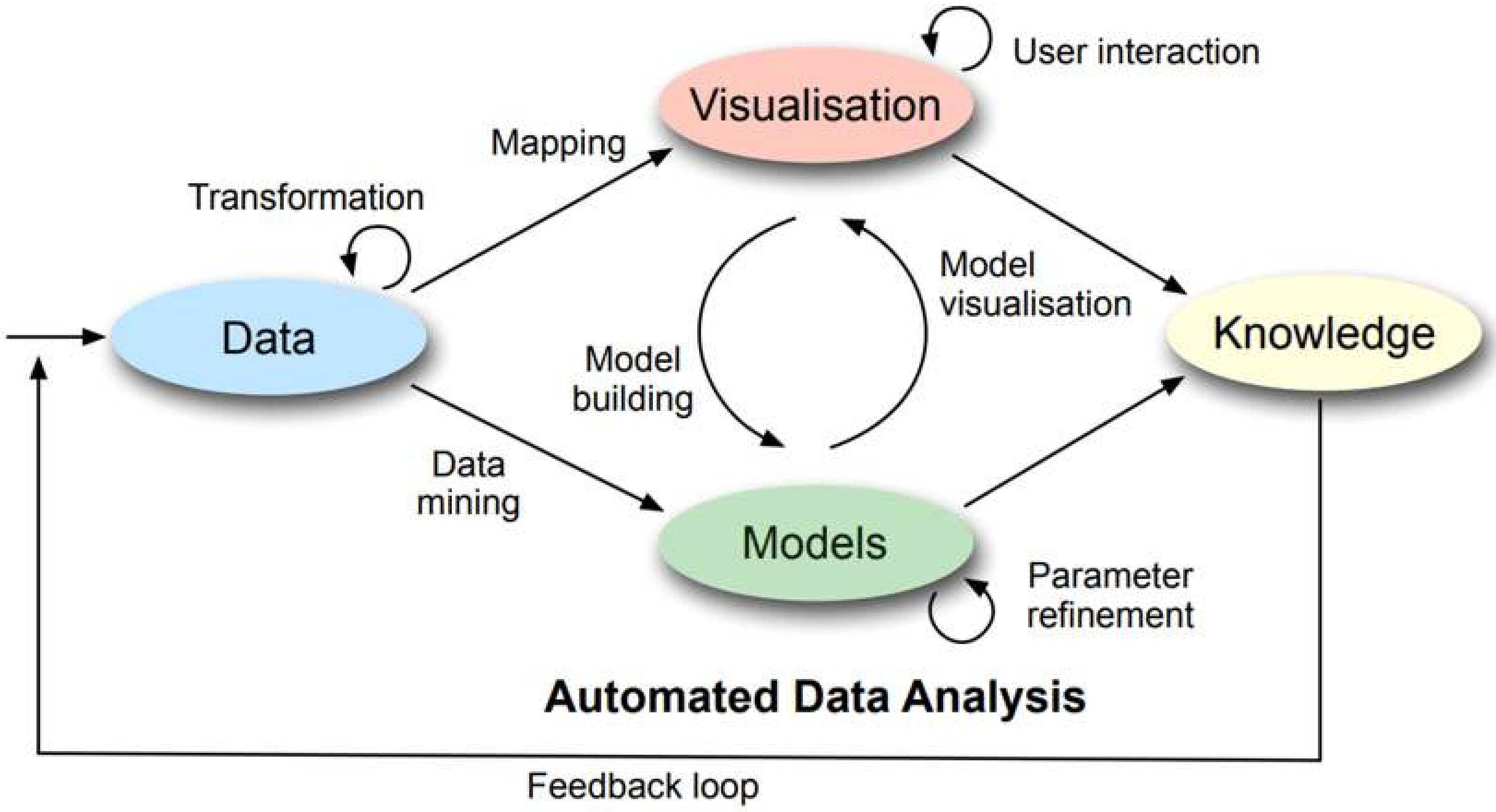
Human Perception for Visualization



Preattentive Attributes for visual perception, adapted from Colin Ware, 2013

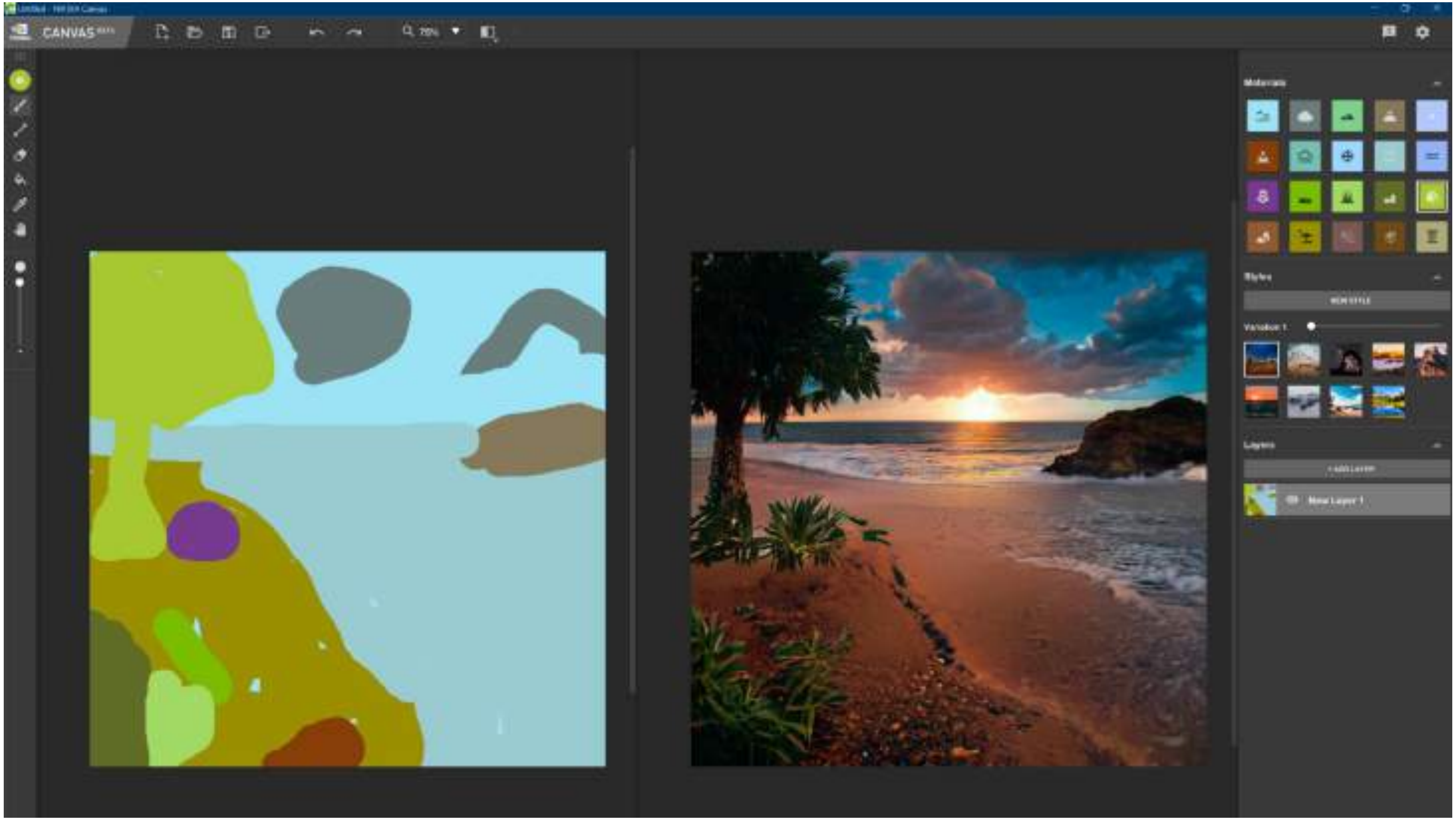
Data Science and Visual Analytics

Bridging Data, Humans, and Artificial Intelligence



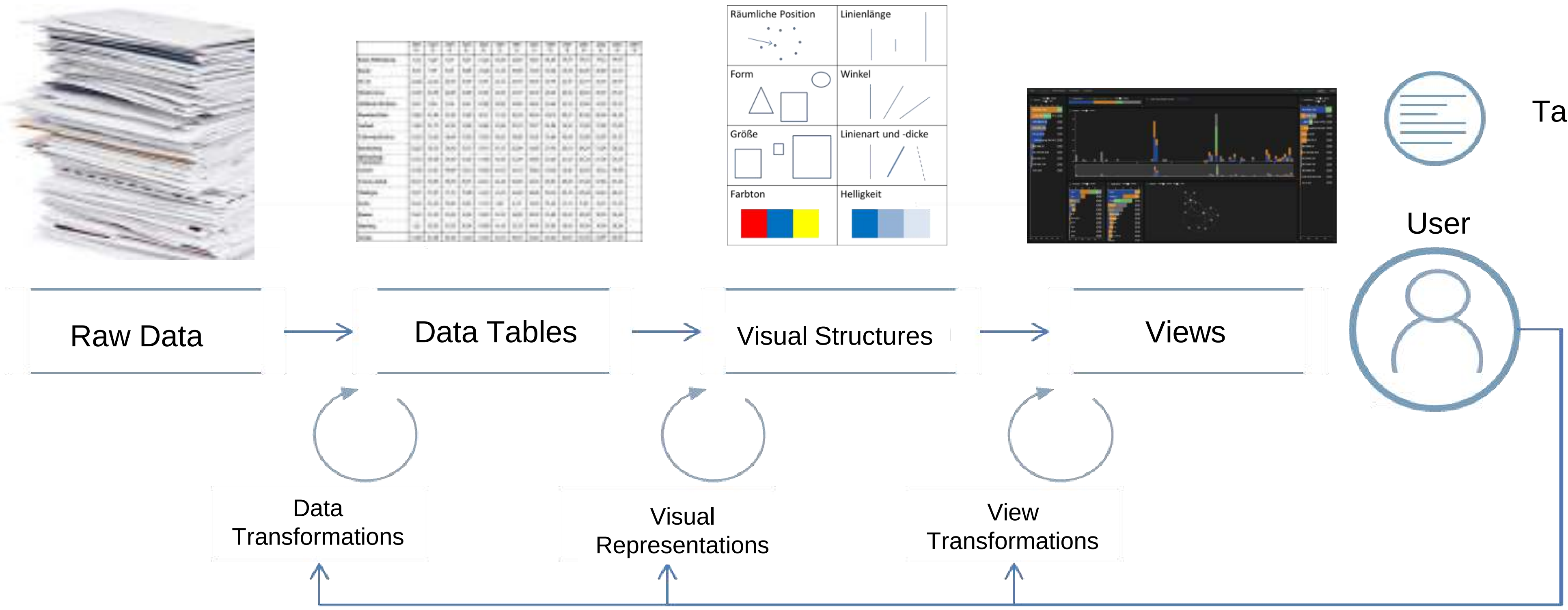
Visual Data Exploration, adapted from Keim et al. 2008

Interactive AI - NVIDIA Canvas



User Centered Design

Change of direction - Which task needs to be completed?



Task

User

Raw Data → Data Tables → Visual Structures → Views

Data Transformations

Visual Representations

View Transformations

adapted from Card et al. 1999

4. Visual Analysis of PCAP Data - Live

NetCapVis

Why did we start NetCapVis?

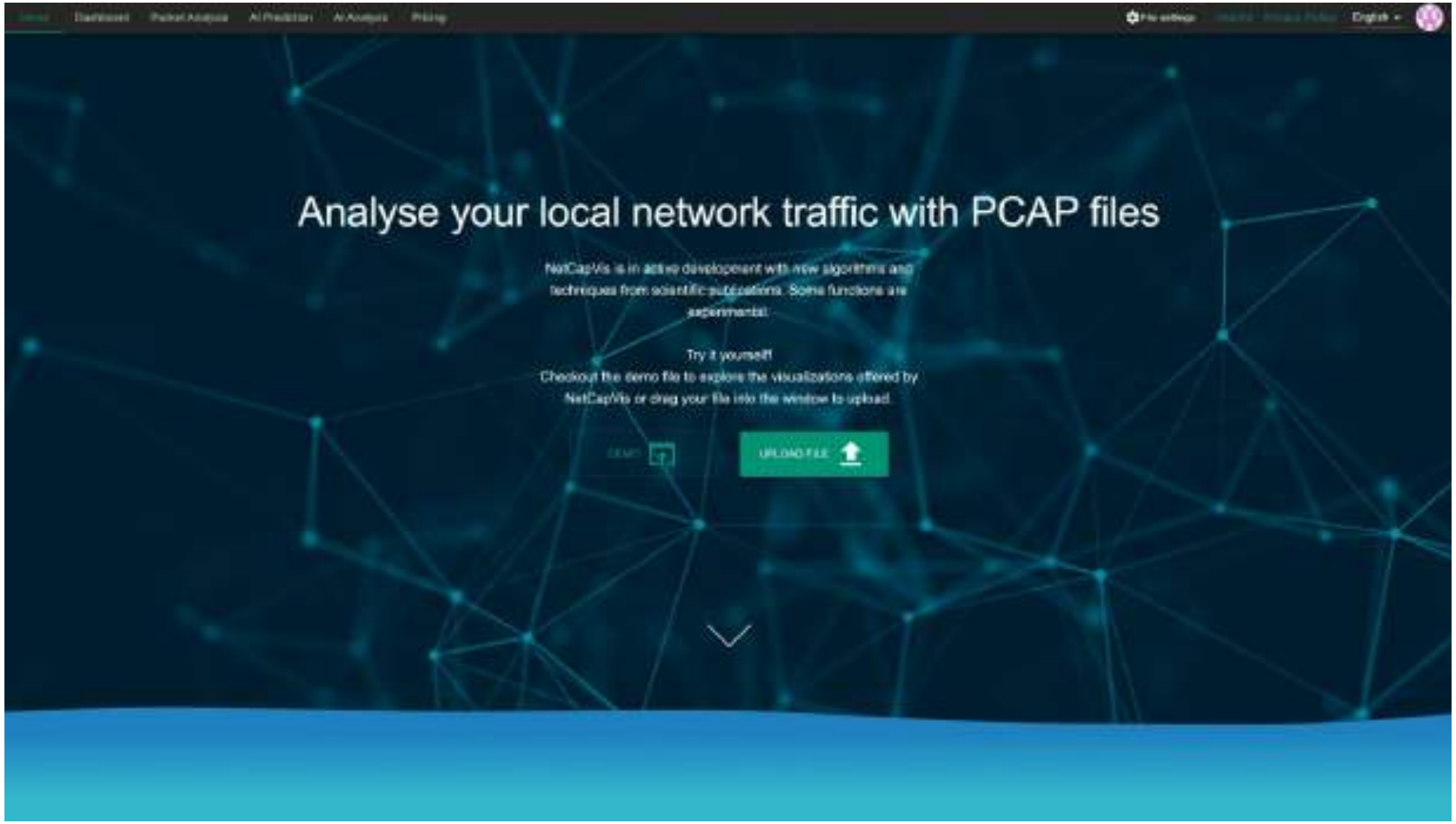
ATHENE
National Research Center
for Applied Cybersecurity

Wireshark is fantastic for experts

But what about beginners?
Can we make it easier to use?

NetCapVis - Live

https://netcapvis.igd.fraunhofer.de



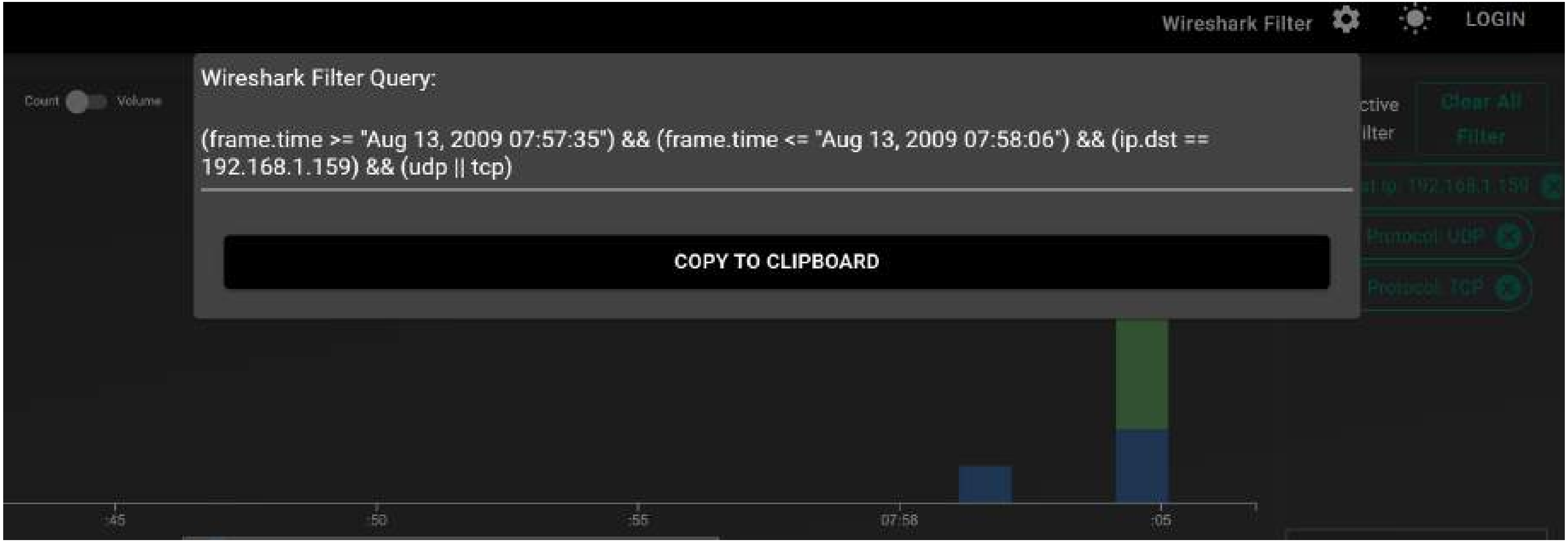
Analyse your local network traffic with PCAP files

NetCapVis is in active development with new algorithms and techniques from scientific publications. Some functions are experimental.

Try it yourself!
Checkout the demo file to explore the visualizations offered by NetCapVis or drag your file into the window to upload.

NetCapVis

Wireshark filter export



(frame.time >= "Aug 13, 2009 07:57:35") && (frame.time <= "Aug 13, 2009 07:58:06") && (ip.dst == 192.168.1.159) && (udp || tcp)

NetCapVis – Parsing and Storage

Parsing

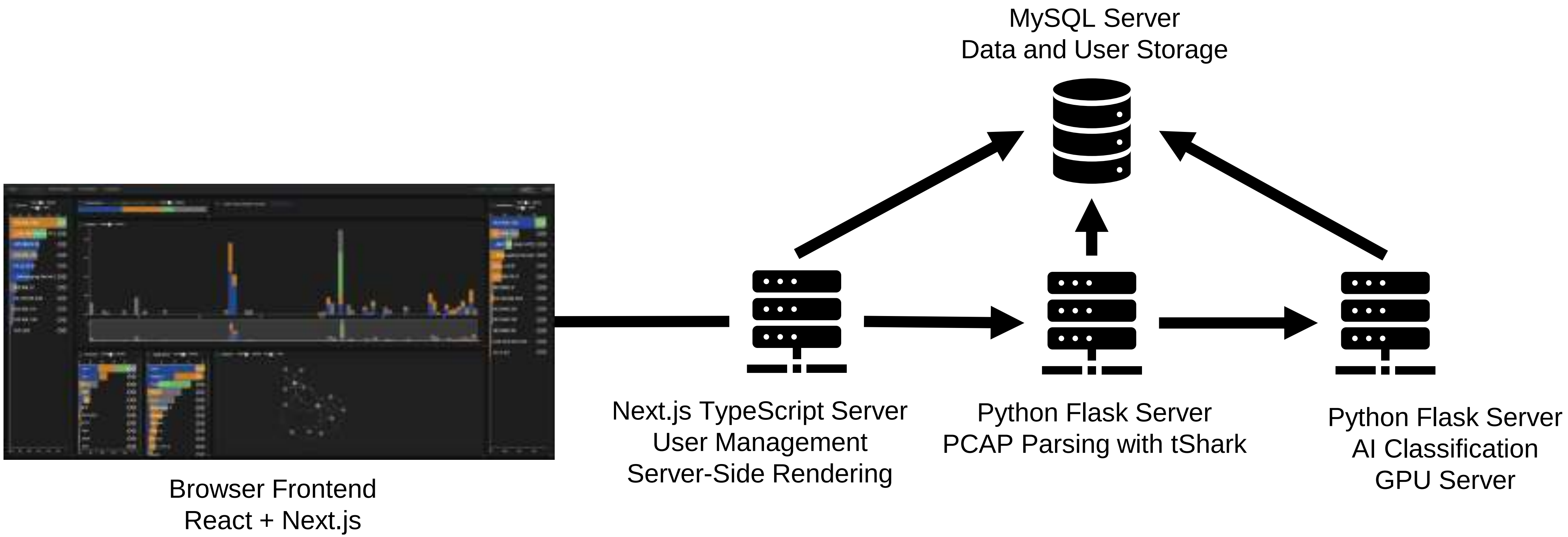
- From Java Backend to Python with tShark

- DNS resolving included
- Working on GeoIP

- tShark optimizations needed

MySQL database to access uploaded data

NetCapVis - Architecture



MySQL Server
Data and User Storage

Browser Frontend
React + Next.js

Next.js TypeScript Server
User Management
Server-Side Rendering

Python Flask Server
PCAP Parsing with tShark

Python Flask Server
AI Classification
GPU Server

NetCapVis – Future Work

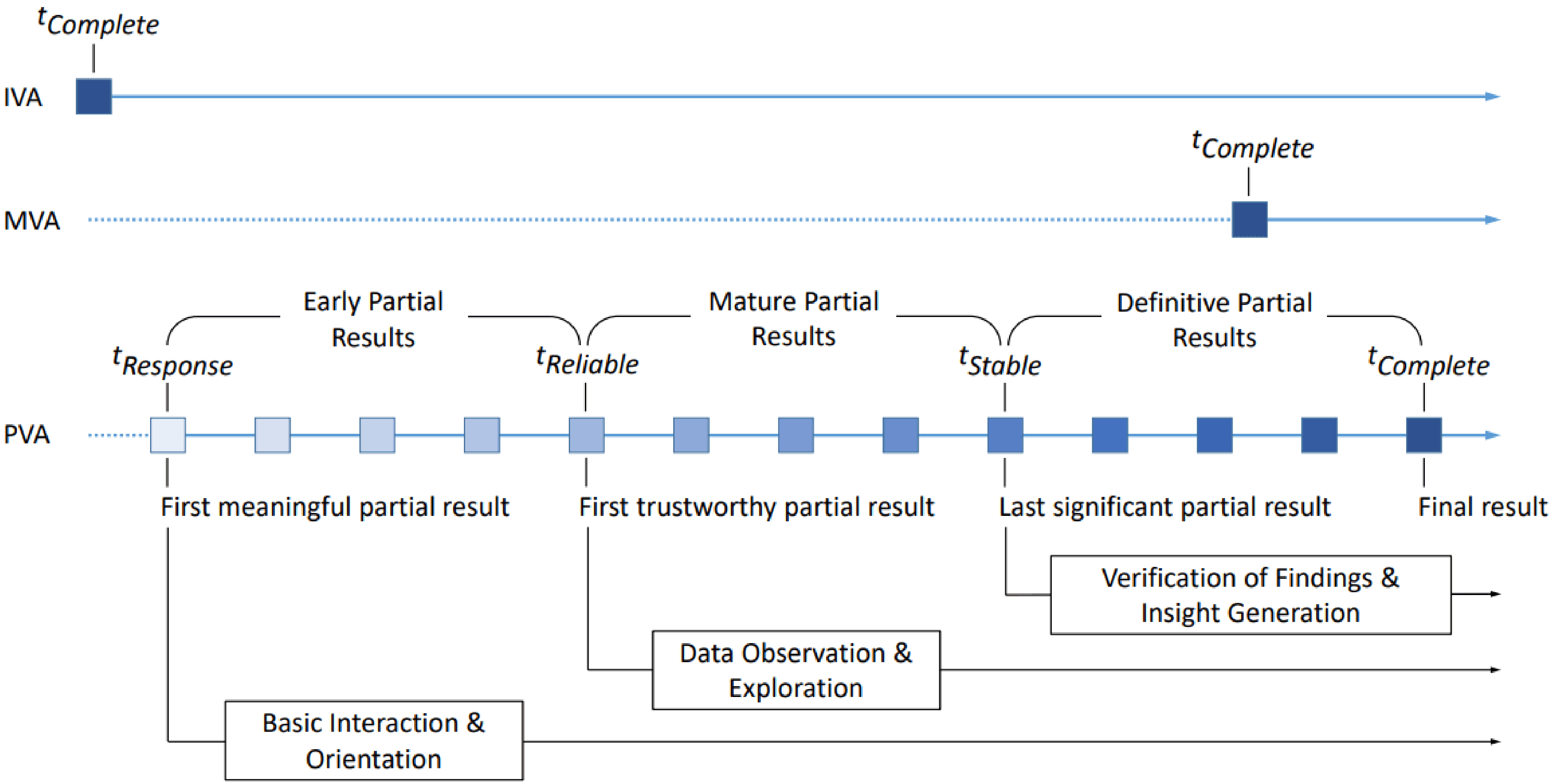
Progressive Data Analysis Approach –

Load large captures

Load streams of data

with interactive visualizations at all times

Progressive Visual Analytics


$t_{Complete}$
IVA
$t_{Complete}$
MVA
Early Partial Results
Mature Partial Results
Definitive Partial Results
$t_{Response}$
$t_{Reliable}$
t_{Stable}
$t_{Complete}$
PVA
First meaningful partial result
First trustworthy partial result
Last significant partial result
Final result
Verification of Findings & Insight Generation
Data Observation & Exploration
Basic Interaction & Orientation

Angelini, Marco, et al. "A review and characterization of progressive visual analytics" 2018.

Progressive Visual Analytics Example

2210 raw data elements left after applying filter - Limited to 1000 entries!

Progressive Visual Analytics Challenges

Chunking a PCAP file is difficult

cutting and merging leads to corrupted data

Priority sampling for the filter that the user is setting

5. Application Classification of Packets

Machine Learning Basics

Machine Learning (ML)

- uncover hidden relationships in multidimensional data

Goals

- extract meaningful patterns from data
- make decisions based on those discoveries
- make predictions with AI systems

Machine Learning Basics

Unsupervised Learning

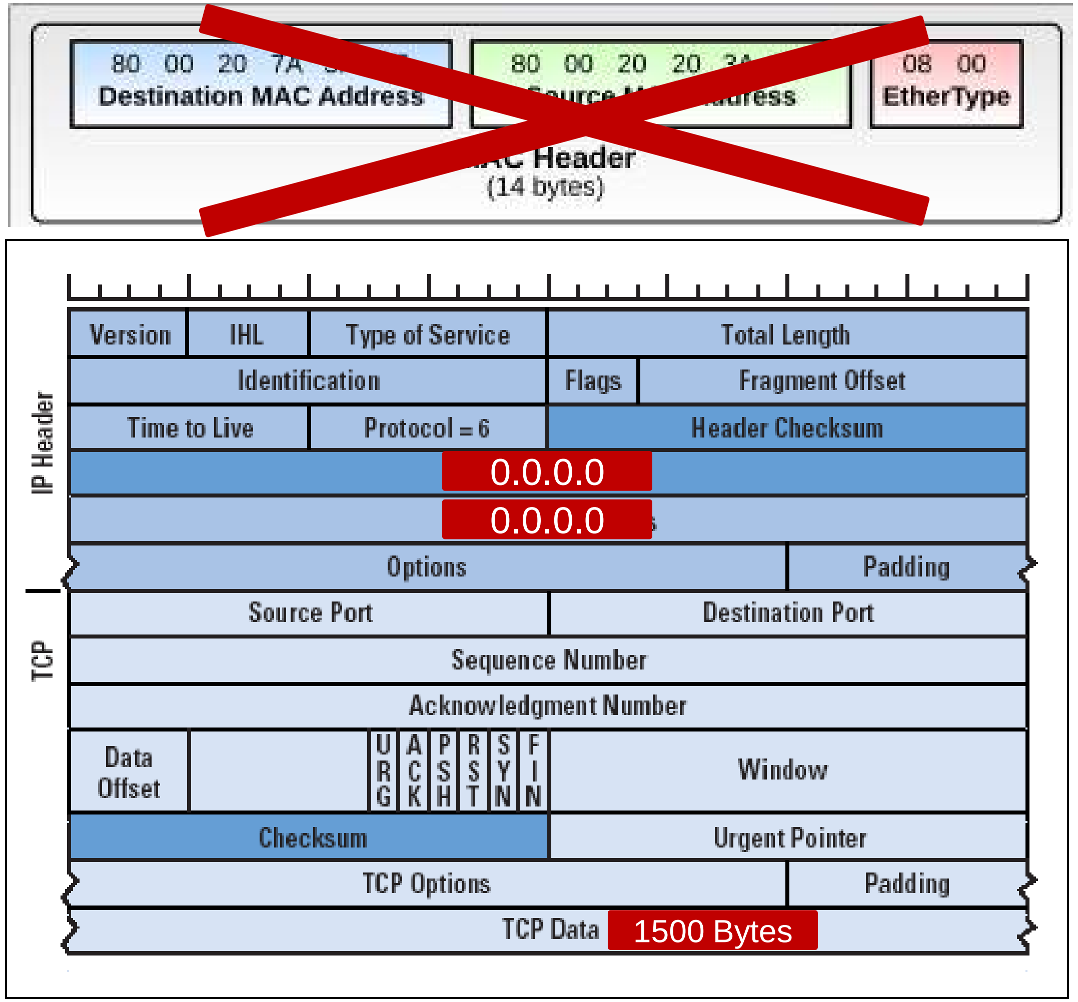
- Find structure in unlabeled data
- For PCAPs:
  Distinguish between normal traffic vs anomaly

Supervised Learning

- Learn from labeled data (prior knowledge)
- For PCAPs:
  Define specific classes, gather training data and label it

PCAP Data Preparation

1. Remove small packets (SYN/ACK, ...)
2. Remove ethernet header
3. Set src and dst address to 0.0.0.0
4. Cut or pad payload to 1500 Bytes
5. Similar approach for other protocols



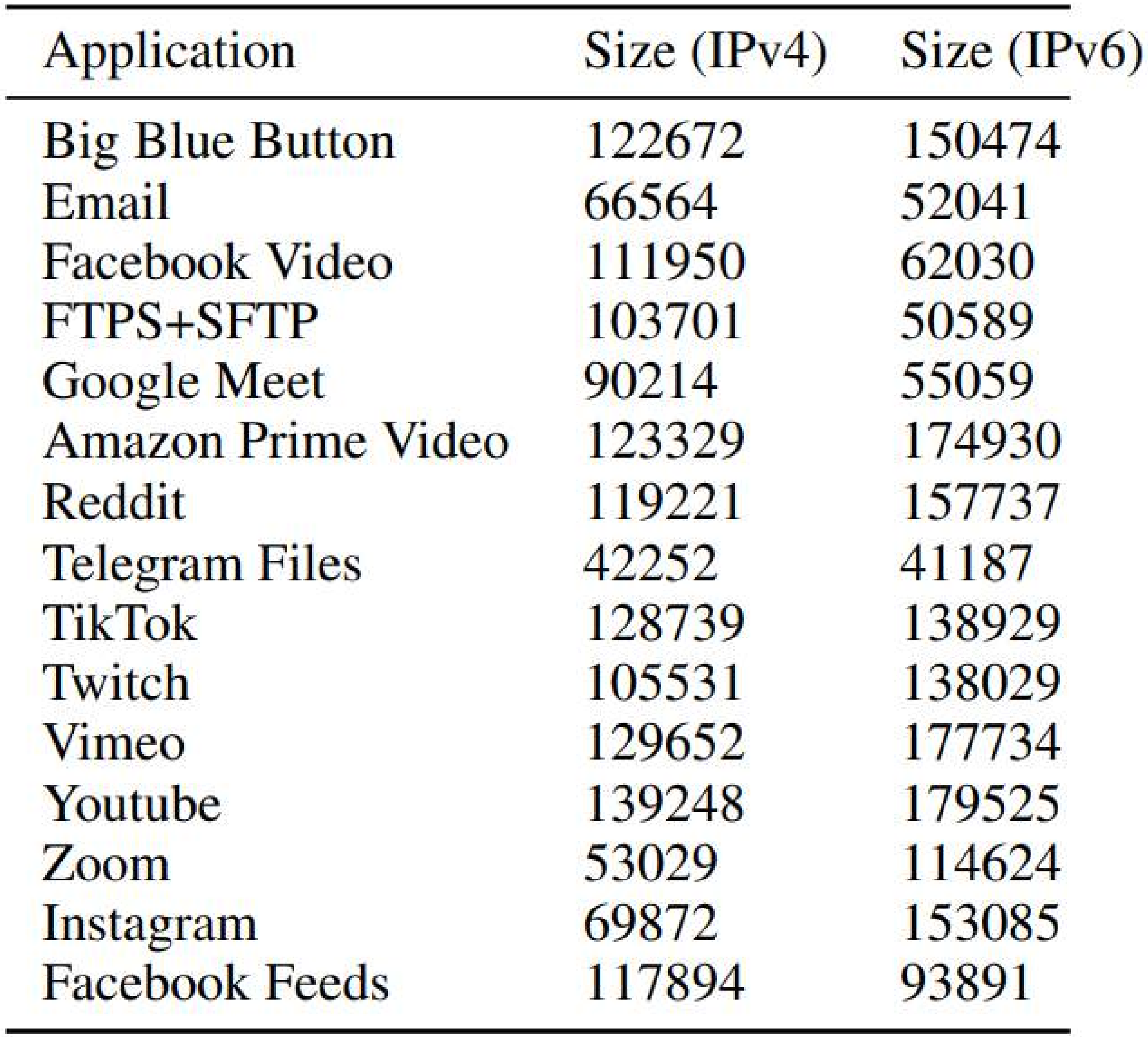
M. Lotfollahi, et al. Deep packet: A novel approach for encrypted traffic classification using deep learning 2017. Dataset : ISCXVPN2016

Training Data and Classes

Goal:

Predict which application caused a packet

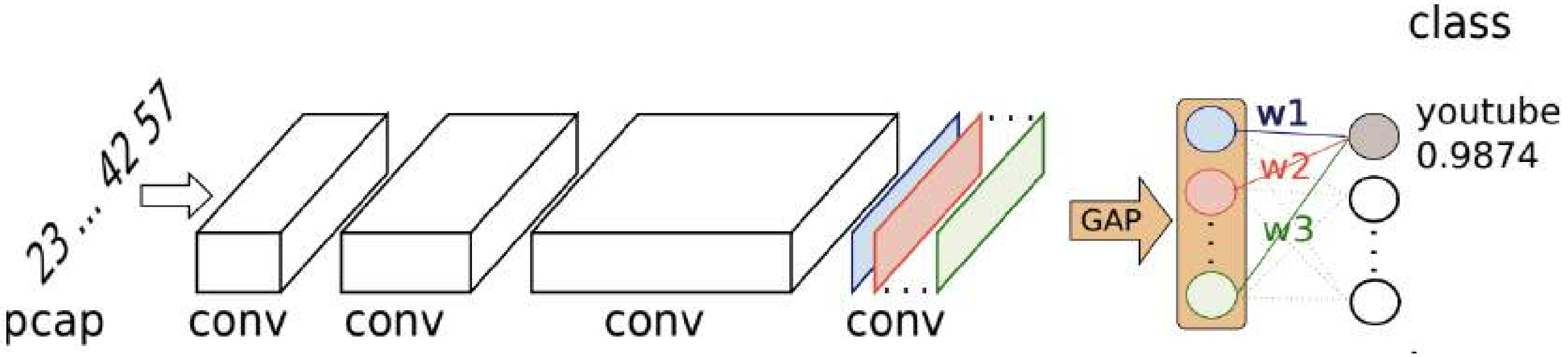
Training data for the AI system



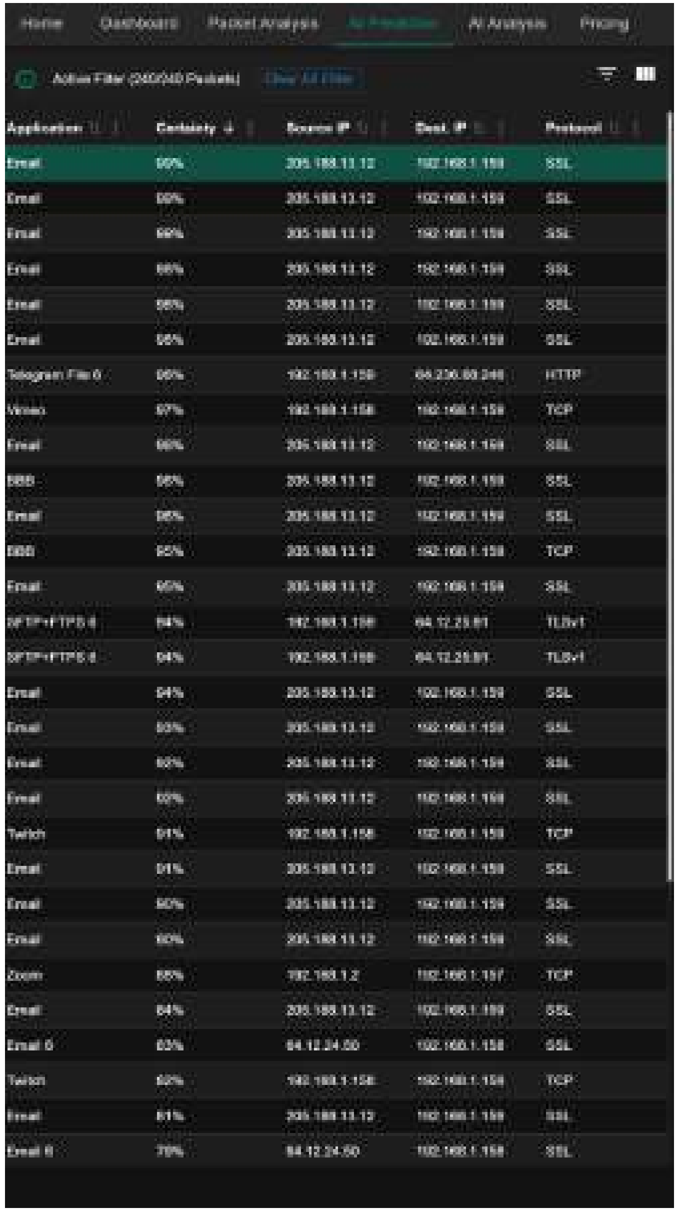
Application	Size (IPv4)	Size (IPv6)
Big Blue Button	122672	150474
Email	66564	52041
Facebook Video	111950	62030
FTPS+SFTP	103701	50589
Google Meet	90214	55059
Amazon Prime Video	123329	174930
Reddit	119221	157737
Telegram Files	42252	41187
TikTok	128739	138929
Twitch	105531	138029
Vimeo	129652	177734
Youtube	139248	179525
Zoom	53029	114624
Instagram	69872	153085
Facebook Feeds	117894	93891

AI Architecture

Convolutional Neural Network (CNN)

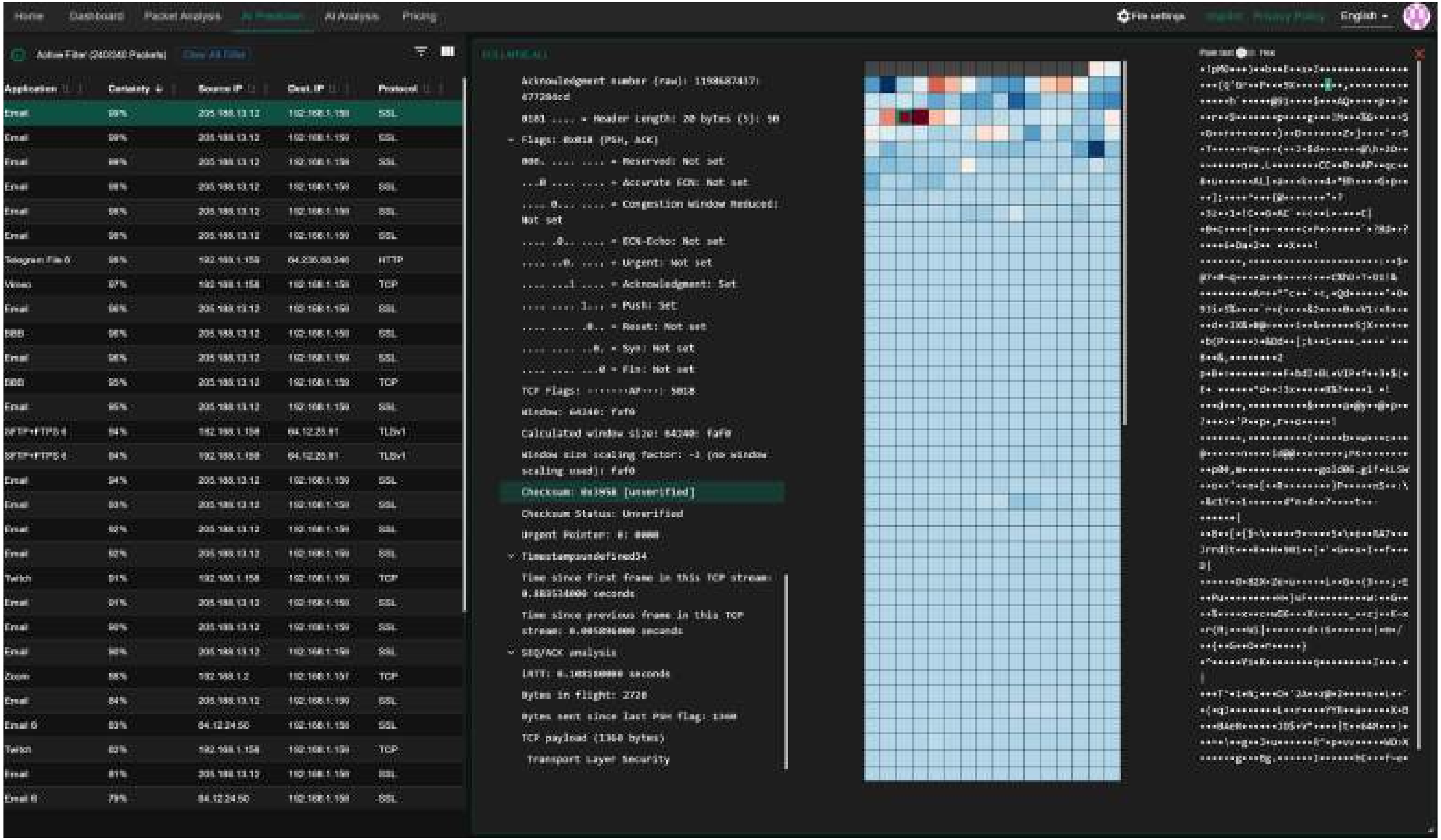


NetCapVis AI Predictions



Application	Certainty ↓	Source IP	Dest. IP	Protocol
Email	99%	205.188.13.12	192.168.1.159	SSL
Email	99%	205.188.13.12	192.168.1.159	SSL
Email	99%	205.188.13.12	192.168.1.159	SSL
Email	98%	205.188.13.12	192.168.1.159	SSL
Email	98%	205.188.13.12	192.168.1.159	SSL
Email	98%	205.188.13.12	192.168.1.159	SSL
Telegram File 0	98%	192.168.1.158	64.236.89.246	HTTP
Vimeo	97%	192.168.1.158	192.168.1.159	TCP
Email	96%	205.188.13.12	192.168.1.159	SSL
BBB	96%	205.188.13.12	192.168.1.159	SSL
Email	96%	205.188.13.12	192.168.1.159	SSL
BBB	95%	205.188.13.12	192.168.1.159	TCP
Email	95%	205.188.13.12	192.168.1.159	SSL
SFTP+FTPS 0	94%	192.168.1.159	64.12.23.81	TLSv1
SFTP+FTPS 0	94%	192.168.1.159	64.12.23.81	TLSv1
Email	94%	205.188.13.12	192.168.1.159	SSL
Email	93%	205.188.13.12	192.168.1.159	SSL
Email	93%	205.188.13.12	192.168.1.159	SSL
Email	92%	205.188.13.12	192.168.1.159	SSL
Twitch	91%	192.168.1.158	192.168.1.159	TCP
Email	91%	205.188.13.12	192.168.1.159	SSL
Email	90%	205.188.13.12	192.168.1.159	SSL
Email	90%	205.188.13.12	192.168.1.159	SSL
Zoom	88%	192.168.1.2	192.168.1.157	TCP
Email	84%	205.188.13.12	192.168.1.159	SSL
Email 0	83%	64.12.24.50	192.168.1.158	SSL
Twitch	82%	192.168.1.158	192.168.1.159	TCP
Email	81%	205.188.13.12	192.168.1.159	SSL
Email 0	79%	64.12.24.50	192.168.1.158	SSL

NetCapVis AI Predictions

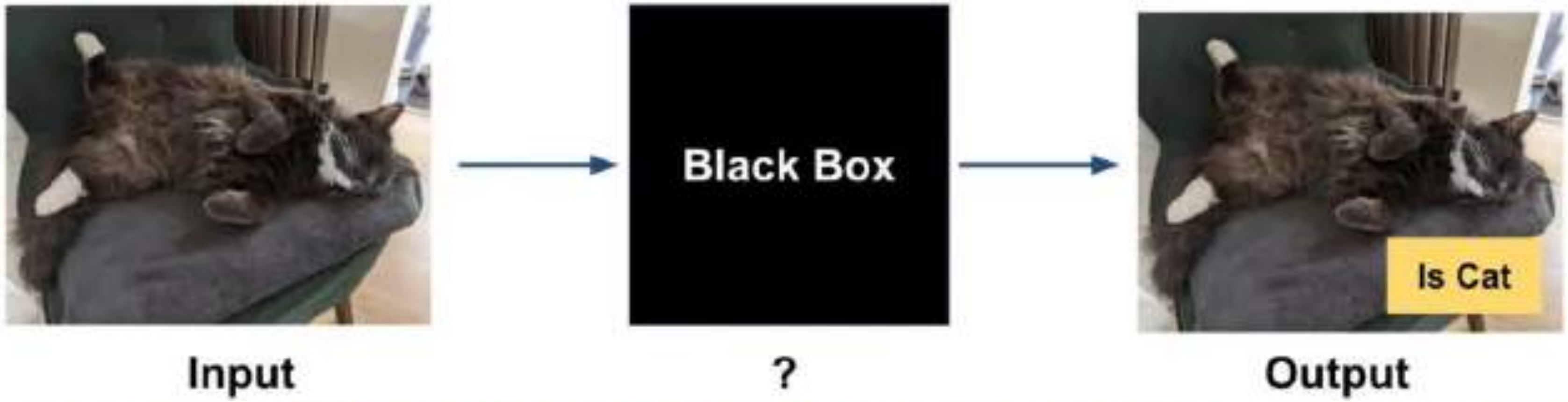


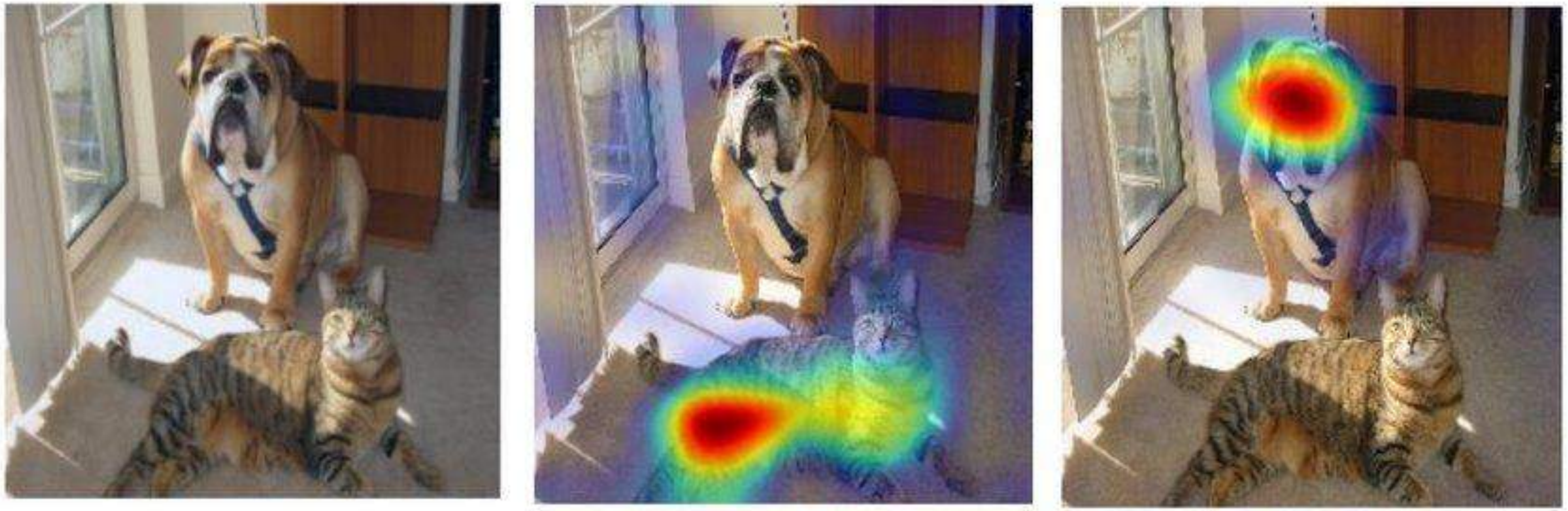
Application	Certainty ↓	Source IP	Dest. IP	Protocol
Email	99%	205.188.13.12	192.168.1.159	SSL
Email	99%	205.188.13.12	192.168.1.159	SSL
Email	99%	205.188.13.12	192.168.1.159	SSL
Email	98%	205.188.13.12	192.168.1.159	SSL
Email	98%	205.188.13.12	192.168.1.159	SSL
Email	98%	205.188.13.12	192.168.1.159	SSL
Telegram File 0	98%	192.168.1.158	64.236.60.240	HTTP
Video	97%	192.168.1.158	192.168.1.159	TCP
Email	96%	205.188.13.12	192.168.1.159	SSL
BBB	96%	205.188.13.12	192.168.1.159	SSL
Email	96%	205.188.13.12	192.168.1.159	SSL
BBB	95%	205.188.13.12	192.168.1.159	TCP
Email	95%	205.188.13.12	192.168.1.159	SSL
SFTP+FTPS 0	94%	192.168.1.158	64.12.25.91	TLSv1
SFTP+FTPS 0	94%	192.168.1.158	64.12.25.91	TLSv1
Email	94%	205.188.13.12	192.168.1.159	SSL
Email	93%	205.188.13.12	192.168.1.159	SSL
Email	92%	205.188.13.12	192.168.1.159	SSL
Email	92%	205.188.13.12	192.168.1.159	SSL
Twitch	91%	192.168.1.158	192.168.1.159	TCP
Email	91%	205.188.13.12	192.168.1.159	SSL
Email	90%	205.188.13.12	192.168.1.159	SSL
Email	90%	205.188.13.12	192.168.1.159	SSL
Zoom	88%	192.168.1.2	192.168.1.107	TCP
Email	84%	205.188.13.12	192.168.1.159	SSL
Email 0	83%	64.12.24.50	192.168.1.159	SSL
Twitch	82%	192.168.1.158	192.168.1.159	TCP
Email	81%	205.188.13.12	192.168.1.159	SSL
Email 0	79%	64.12.24.50	192.168.1.159	SSL

```
  Acknowledgment number (raw): 1198687437:
  4772Bdcd
  0101 .... = Header Length: 20 bytes (5): 50
v Flags: 0x018 (PSH, ACK)
  000. .... .... = Reserved: Not set
  ...0 .... .... = Accurate ECN: Not set
  .... 0... .... = Congestion Window Reduced:
  Not set
  .... .0.. .... = ECN-Echo: Not set
  .... ..0. .... = Urgent: Not set
  .... ...1 .... = Acknowledgment: Set
  .... .... 1... = Push: Set
  .... .... .0.. = Reset: Not set
  .... .... ..0. = Syn: Not set
  .... .... ...0 = Fin: Not set
  TCP Flags: ·······AP···: 5018
  Window: 64240: faf0
  Calculated window size: 64240: fafo
  Window size scaling factor: -1 (no window
  scaling used): fafo
  Checksum: 0x1958 [unverified]
  Checksum Status: Unverified
  Urgent Pointer: 0: 0000
v Timestampundefined34
  Time since first frame in this TCP stream:
  0.882524000 seconds
  Time since previous frame in this TCP
  stream: 0.005896000 seconds
v SEQ/ACK analysis
  iRTT: 0.188180000 seconds
  Bytes in flight: 2720
  Bytes sent since last PSH flag: 1360
  TCP payload (1360 bytes)
   Transport Layer Security
```

6. Explainable AI

What is XAI?

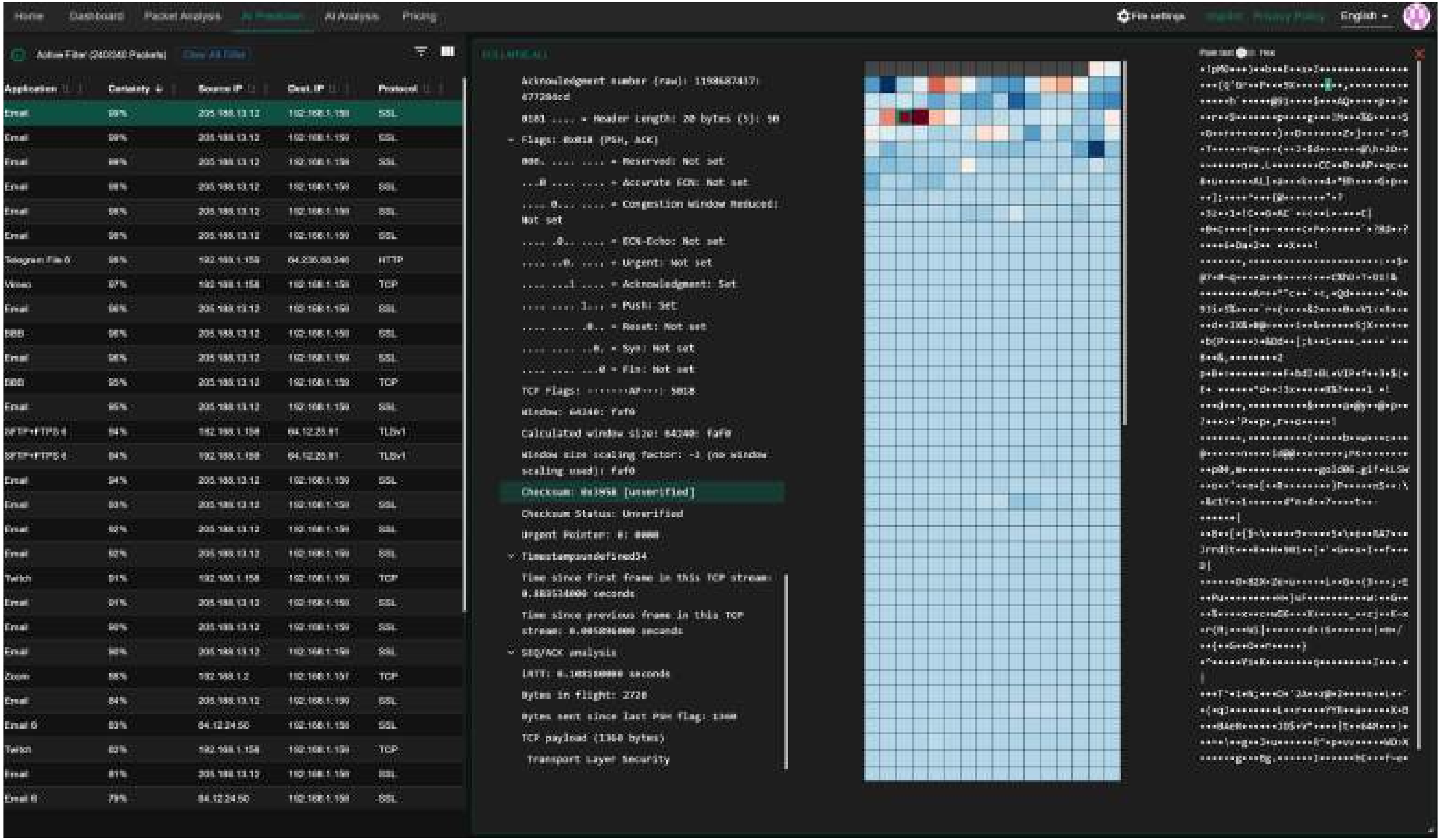




(a) Original Image (b) Grad-CAM 'Cat' (c) Grad-CAM 'Dog'

Trustworthy versus Explainable AI in Autonomous Vessels, Glomsrud et al. (2019)

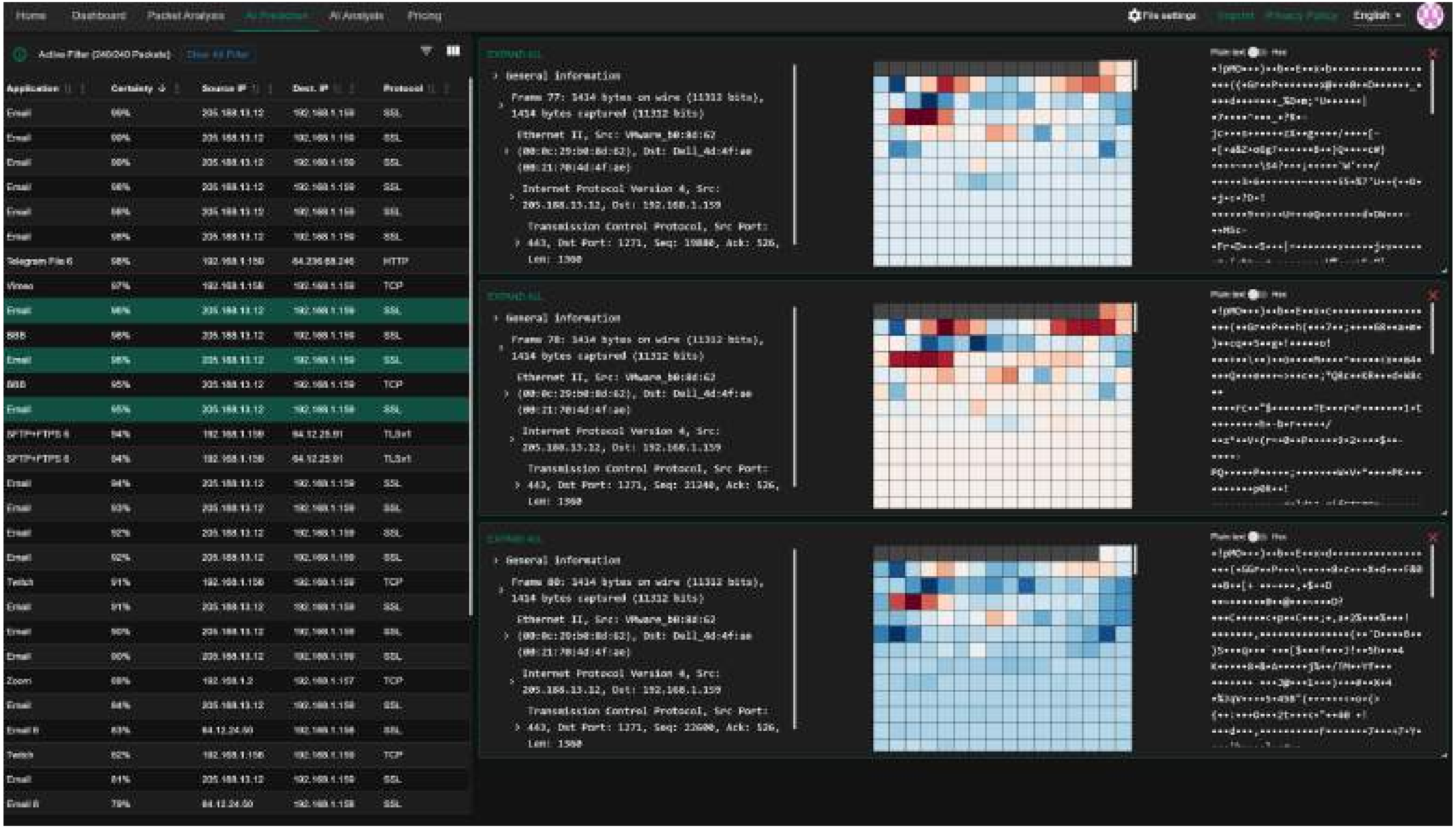
Local Class Activation Maps (CAMs)



Application	Certainty ↓	Source IP	Dest. IP	Protocol
Email	99%	205.188.13.12	192.168.1.159	SSL
Email	99%	205.188.13.12	192.168.1.159	SSL
Email	99%	205.188.13.12	192.168.1.159	SSL
Email	98%	205.188.13.12	192.168.1.159	SSL
Email	98%	205.188.13.12	192.168.1.159	SSL
Email	98%	205.188.13.12	192.168.1.159	SSL
Telegram File 0	98%	192.168.1.158	64.236.68.240	HTTP
Vimeo	97%	192.168.1.158	192.168.1.159	TCP
Email	96%	205.188.13.12	192.168.1.159	SSL
BBB	96%	205.188.13.12	192.168.1.159	SSL
Email	96%	205.188.13.12	192.168.1.159	SSL
BBB	95%	205.188.13.12	192.168.1.159	TCP
Email	95%	205.188.13.12	192.168.1.159	SSL
SFTP+FTPS 0	94%	192.168.1.158	64.12.25.91	TLSv1
SFTP+FTPS 0	94%	192.168.1.158	64.12.25.91	TLSv1
Email	94%	205.188.13.12	192.168.1.159	SSL
Email	93%	205.188.13.12	192.168.1.159	SSL
Email	92%	205.188.13.12	192.168.1.159	SSL
Email	92%	205.188.13.12	192.168.1.159	SSL
Twitch	91%	192.168.1.158	192.168.1.159	TCP
Email	91%	205.188.13.12	192.168.1.159	SSL
Email	90%	205.188.13.12	192.168.1.159	SSL
Email	90%	205.188.13.12	192.168.1.159	SSL
Zoom	88%	192.168.1.2	192.168.1.157	TCP
Email	84%	205.188.13.12	192.168.1.159	SSL
Email 0	83%	64.12.24.50	192.168.1.159	SSL
Twitch	82%	192.168.1.158	192.168.1.159	TCP
Email	81%	205.188.13.12	192.168.1.159	SSL
Email 0	79%	64.12.24.50	192.168.1.159	SSL

```
   Acknowledgment number (raw): 1198687437:
   477208cd
   0101 .... = Header Length: 20 bytes (5): 50
 ⌄ Flags: 0x018 (PSH, ACK)
   000. .... .... = Reserved: Not set
   ...0 .... .... = Accurate ECN: Not set
   .... 0... .... = Congestion Window Reduced:
   Not set
   .... .0.. .... = ECN-Echo: Not set
   .... ..0. .... = Urgent: Not set
   .... ...1 .... = Acknowledgment: Set
   .... .... 1... = Push: Set
   .... .... .0.. = Reset: Not set
   .... .... ..0. = Syn: Not set
   .... .... ...0 = Fin: Not set
   TCP Flags: ·······AP···: 5018
   Window: 64240: faf0
   Calculated window size: 64240: faf0
   Window size scaling factor: -1 (no window
   scaling used): faf0
   Checksum: 0x1958 [unverified]
   Checksum Status: Unverified
   Urgent Pointer: 0: 0000
 ⌄ TimestampsundefinedJ4
   Time since first frame in this TCP stream:
   0.883524000 seconds
   Time since previous frame in this TCP
   stream: 0.005896000 seconds
 ⌄ SEQ/ACK analysis
   iRTT: 0.100100000 seconds
   Bytes in flight: 2720
   Bytes sent since last PSH flag: 1360
   TCP payload (1360 bytes)
    Transport Layer Security
```

Local Class Activation Maps (CAMs)



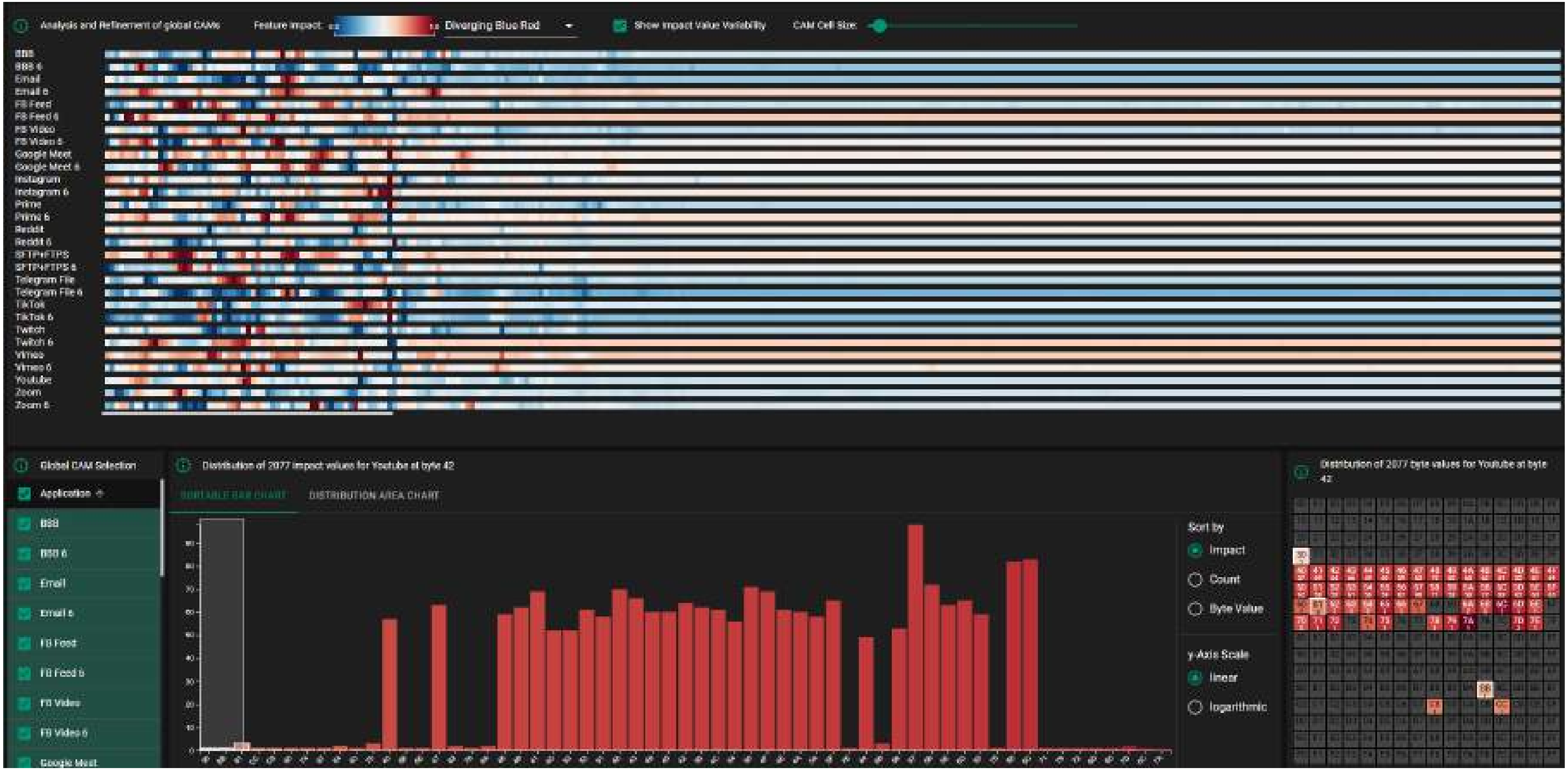
Application	Certainty	Source IP	Dest. IP	Protocol
Email	99%	205.188.13.12	192.168.1.159	SSL
Email	99%	205.188.13.12	192.168.1.159	SSL
Email	99%	205.188.13.12	192.168.1.159	SSL
Email	98%	205.188.13.12	192.168.1.159	SSL
Email	98%	205.188.13.12	192.168.1.159	SSL
Email	98%	205.188.13.12	192.168.1.159	SSL
Telegram File 6	98%	192.168.1.159	84.236.68.246	HTTP
Vimeo	97%	192.168.1.156	192.168.1.159	TCP
Email	96%	205.188.13.12	192.168.1.159	SSL
BBB	96%	205.188.13.12	192.168.1.159	SSL
Email	96%	205.188.13.12	192.168.1.159	SSL
BBB	95%	205.188.13.12	192.168.1.159	TCP
Email	95%	205.188.13.12	192.168.1.159	SSL
SFTP+FTPS 6	94%	192.168.1.159	84.12.25.81	TLSv1
SFTP+FTPS 6	94%	192.168.1.159	84.12.25.81	TLSv1
Email	94%	205.188.13.12	192.168.1.159	SSL
Email	93%	205.188.13.12	192.168.1.159	SSL
Email	92%	205.188.13.12	192.168.1.159	SSL
Email	92%	205.188.13.12	192.168.1.159	SSL
Twitch	91%	192.168.1.156	192.168.1.159	TCP
Email	91%	205.188.13.12	192.168.1.159	SSL
Email	90%	205.188.13.12	192.168.1.159	SSL
Email	90%	205.188.13.12	192.168.1.159	SSL
Zoom	88%	192.168.1.2	192.168.1.157	TCP
Email	84%	205.188.13.12	192.168.1.159	SSL
Email 6	83%	84.12.24.50	192.168.1.159	SSL
Twitch	82%	192.168.1.156	192.168.1.159	TCP
Email	81%	205.188.13.12	192.168.1.159	SSL
Email 6	79%	84.12.24.50	192.168.1.159	SSL

```
> General information
> Frame 77: 1434 bytes on wire (11312 bits), 1434 bytes captured (11312 bits)
> Ethernet II, Src: VMware_b0:8d:62 (00:0c:29:b0:8d:62), Dst: Dell_4d:4f:ae (00:21:70:4d:4f:ae)
> Internet Protocol Version 4, Src: 205.188.13.12, Dst: 192.168.1.159
> Transmission Control Protocol, Src Port: 443, Dst Port: 1271, Seq: 10880, Ack: 526, Len: 1380
```

```
> General information
> Frame 78: 1434 bytes on wire (11312 bits), 1434 bytes captured (11312 bits)
> Ethernet II, Src: VMware_b0:8d:62 (00:0c:29:b0:8d:62), Dst: Dell_4d:4f:ae (00:21:70:4d:4f:ae)
> Internet Protocol Version 4, Src: 205.188.13.12, Dst: 192.168.1.159
> Transmission Control Protocol, Src Port: 443, Dst Port: 1271, Seq: 21240, Ack: 526, Len: 1380
```

```
> General information
> Frame 80: 1434 bytes on wire (11312 bits), 1434 bytes captured (11312 bits)
> Ethernet II, Src: VMware_b0:8d:62 (00:0c:29:b0:8d:62), Dst: Dell_4d:4f:ae (00:21:70:4d:4f:ae)
> Internet Protocol Version 4, Src: 205.188.13.12, Dst: 192.168.1.159
> Transmission Control Protocol, Src Port: 443, Dst Port: 1271, Seq: 22600, Ack: 526, Len: 1380
```

Global Class Activation Maps (CAMs)



Analysis and Refinement of global CAMs

Feature impact: Diverging Blue Red

☑ Show Impact Value Variability

CAM Cell Size:

Global CAM Selection

Distribution of 2077 impact values for Youtube at byte 42

SORTABLE BAR CHART | DISTRIBUTION AREA CHART

Sort by

● Impact

○ Count

○ Byte Value

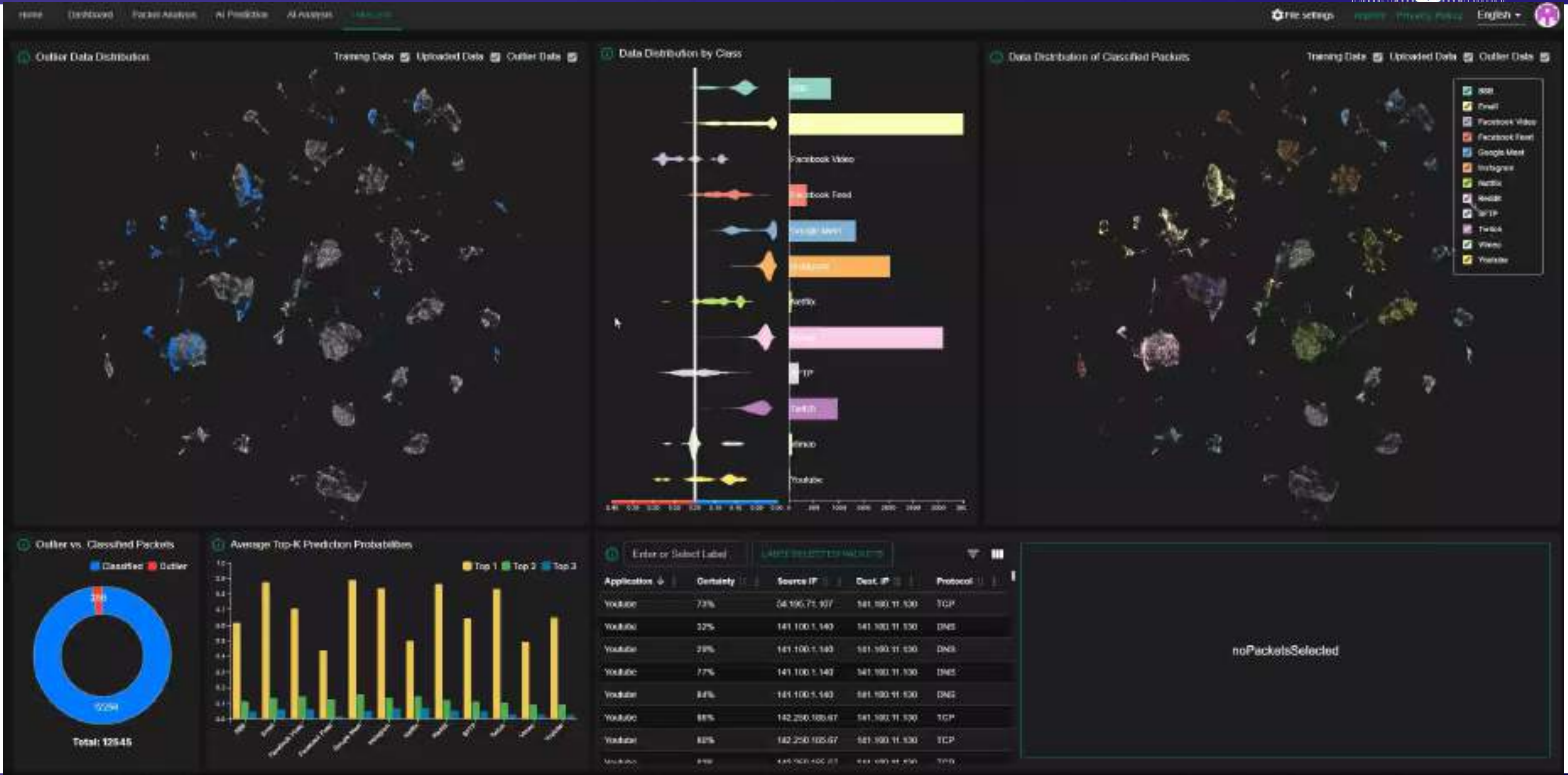
y-Axis Scale

● linear

○ logarithmic

Distribution of 2077 byte values for Youtube at byte 42

Data Drift and Active Learning



Application	Certainty	Source IP	Dest. IP	Protocol
Youtube	73%	34.106.71.107	141.100.11.130	TCP
Youtube	32%	141.100.1.140	141.100.11.130	DNS
Youtube	29%	141.100.1.140	141.100.11.130	DNS
Youtube	77%	141.100.1.140	141.100.11.130	DNS
Youtube	84%	141.100.1.140	141.100.11.130	DNS
Youtube	88%	142.250.185.67	141.100.11.130	TCP
Youtube	80%	142.250.185.67	141.100.11.130	TCP
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Insights and Future Work

Insights

- Enrcypted payload has almost no contribution to classification
- Training data preparation requires more expertise
- Sequence and ack number need to be cut
- Variable length of TCP options

Future Work

- Feedback system: network expert corrects the AI system
- Aggregate bytes to acutal fields of the protocol
- Active Learning: split or combine application classes

Bridging Expertise between Communities

Bringing visualization, machine learning and network experts together

Come talk to us!

Alex

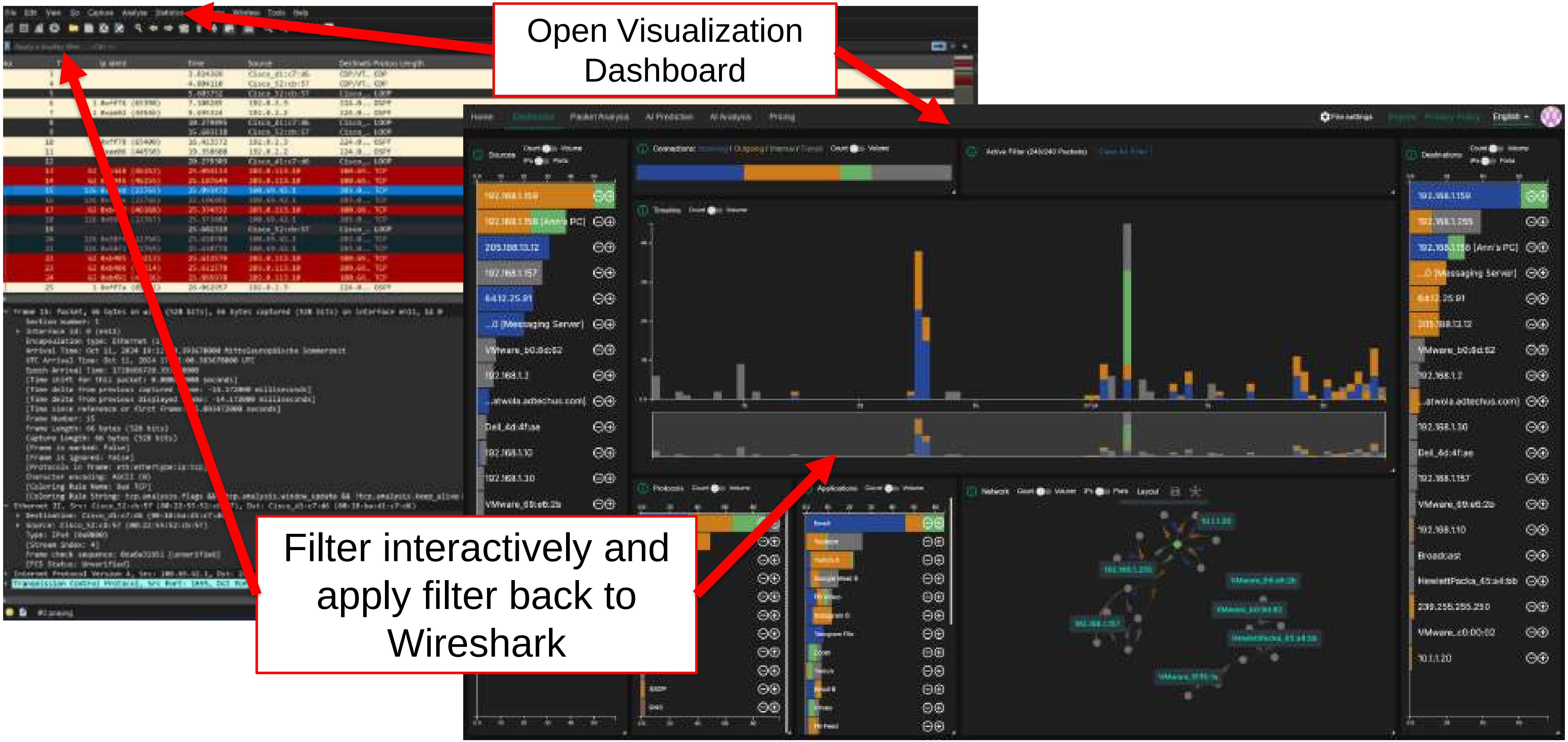
Igor

David

Felix

7. Visualization Plugin for Wireshark

Idea: Vizualization Dashboard



Open Visualization Dashboard

Filter interactively and apply filter back to Wireshark

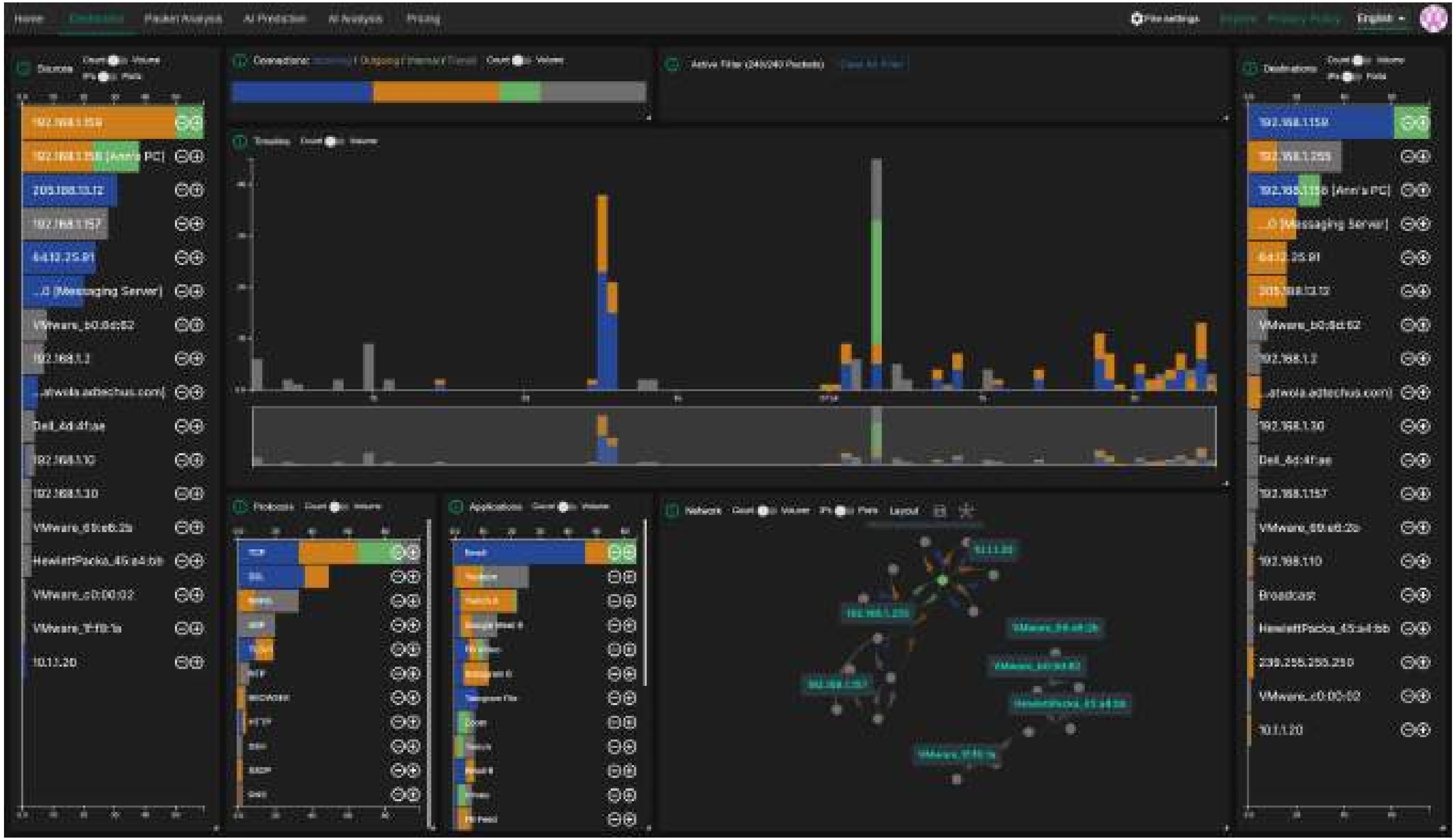
Idea: Vizualization Dashboard

Interacitve Dashboard only

No Packet Table

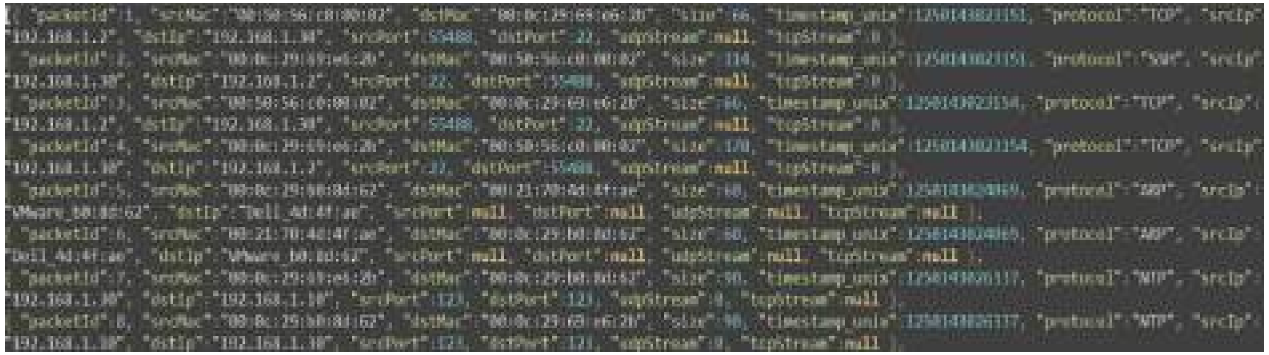
No AI Functions

For free



Option A: Cloud-hosted Dashboard

Reduced Packet Header Data

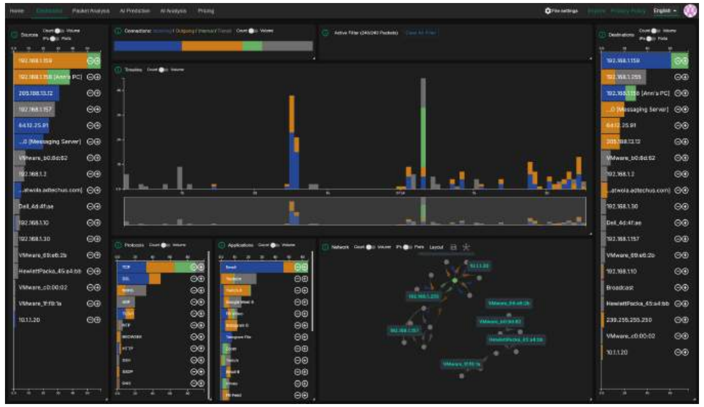


```
[{"packetId":1, "srcMac":"00:50:56:c0:00:02", "dstMac":"00:0c:29:69:e6:2b", "size":66, "timestamp_unix":1250143822151, "protocol":"TCP", "srcIp":
"192.168.1.2", "dstIp":"192.168.1.30", "srcPort":55488, "dstPort":22, "udpStream":null, "tcpStream":0 },
 {"packetId":2, "srcMac":"00:0c:29:69:e6:2b", "dstMac":"00:50:56:c0:00:02", "size":114, "timestamp_unix":1250143822151, "protocol":"SSH", "srcIp":
"192.168.1.30", "dstIp":"192.168.1.2", "srcPort":22, "dstPort":55488, "udpStream":null, "tcpStream":0 },
 {"packetId":3, "srcMac":"00:50:56:c0:00:02", "dstMac":"00:0c:29:69:e6:2b", "size":66, "timestamp_unix":1250143822154, "protocol":"TCP", "srcIp":
"192.168.1.2", "dstIp":"192.168.1.30", "srcPort":55488, "dstPort":22, "udpStream":null, "tcpStream":0 },
 {"packetId":4, "srcMac":"00:0c:29:69:e6:2b", "dstMac":"00:50:56:c0:00:02", "size":170, "timestamp_unix":1250143822154, "protocol":"TCP", "srcIp":
"192.168.1.30", "dstIp":"192.168.1.2", "srcPort":22, "dstPort":55488, "udpStream":null, "tcpStream":0 },
 {"packetId":5, "srcMac":"00:0c:29:b0:8d:62", "dstMac":"00:21:70:4d:4f:ae", "size":60, "timestamp_unix":1250143824069, "protocol":"ARP", "srcIp":
"VMware_b0:8d:62", "dstIp":"Dell_4d:4f:ae", "srcPort":null, "dstPort":null, "udpStream":null, "tcpStream":null },
 {"packetId":6, "srcMac":"00:21:70:4d:4f:ae", "dstMac":"00:0c:29:b0:8d:62", "size":60, "timestamp_unix":1250143824069, "protocol":"ARP", "srcIp":
"Dell_4d:4f:ae", "dstIp":"VMware_b0:8d:62", "srcPort":null, "dstPort":null, "udpStream":null, "tcpStream":null },
 {"packetId":7, "srcMac":"00:0c:29:69:e6:2b", "dstMac":"00:0c:29:b0:8d:62", "size":90, "timestamp_unix":1250143826117, "protocol":"NTP", "srcIp":
"192.168.1.30", "dstIp":"192.168.1.10", "srcPort":123, "dstPort":123, "udpStream":0, "tcpStream":null },
 {"packetId":8, "srcMac":"00:0c:29:b0:8d:62", "dstMac":"00:0c:29:69:e6:2b", "size":90, "timestamp_unix":1250143826117, "protocol":"NTP", "srcIp":
"192.168.1.30", "dstIp":"192.168.1.10", "srcPort":123, "dstPort":123, "udpStream":0, "tcpStream":null },
```

json

https://...../dashboard

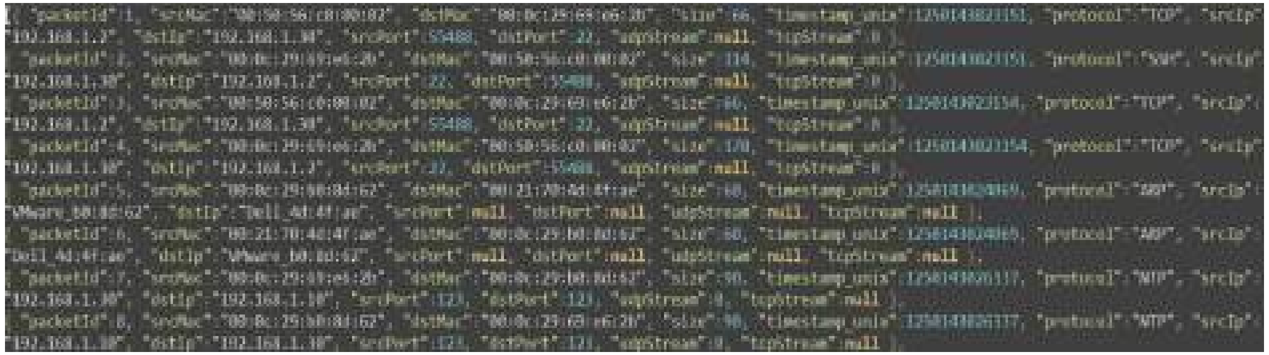
filter query



(frame.time >= "Aug 13, 2009 07:57:35") && (frame.time <= "Aug 13, 2009 07:58:06") && (ip.dst == 192.168.1.159) && (tcp || udp)

Option B: Local Dashboard

Reduced Packet Header Data

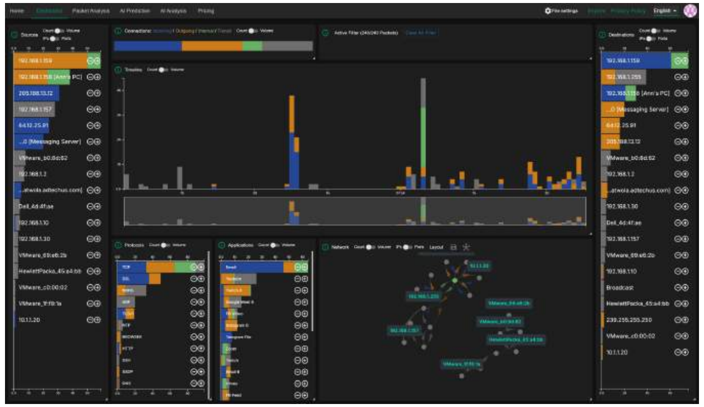


```
[{"packetId":1, "srcMac":"00:50:56:c0:00:02", "dstMac":"00:0c:29:69:e6:2b", "size":66, "timestamp_unix":1250143823151, "protocol":"TCP", "srcIp":
"192.168.1.2", "dstIp":"192.168.1.30", "srcPort":55488, "dstPort":22, "udpStream":null, "tcpStream":0},
{"packetId":2, "srcMac":"00:0c:29:69:e6:2b", "dstMac":"00:50:56:c0:00:02", "size":114, "timestamp_unix":1250143823151, "protocol":"SSH", "srcIp":
"192.168.1.30", "dstIp":"192.168.1.2", "srcPort":22, "dstPort":55488, "udpStream":null, "tcpStream":0},
{"packetId":3, "srcMac":"00:50:56:c0:00:02", "dstMac":"00:0c:29:69:e6:2b", "size":66, "timestamp_unix":1250143823154, "protocol":"TCP", "srcIp":
"192.168.1.2", "dstIp":"192.168.1.30", "srcPort":55488, "dstPort":22, "udpStream":null, "tcpStream":0},
{"packetId":4, "srcMac":"00:0c:29:69:e6:2b", "dstMac":"00:50:56:c0:00:02", "size":170, "timestamp_unix":1250143823154, "protocol":"TCP", "srcIp":
"192.168.1.30", "dstIp":"192.168.1.2", "srcPort":22, "dstPort":55488, "udpStream":null, "tcpStream":0},
{"packetId":5, "srcMac":"00:0c:29:b0:8d:62", "dstMac":"00:21:70:4d:4f:ae", "size":60, "timestamp_unix":1250143824069, "protocol":"ARP", "srcIp":
"VMware_b0:8d:62", "dstIp":"Dell_4d:4f:ae", "srcPort":null, "dstPort":null, "udpStream":null, "tcpStream":null},
{"packetId":6, "srcMac":"00:21:70:4d:4f:ae", "dstMac":"00:0c:29:b0:8d:62", "size":60, "timestamp_unix":1250143824069, "protocol":"ARP", "srcIp":
"Dell_4d:4f:ae", "dstIp":"VMware_b0:8d:62", "srcPort":null, "dstPort":null, "udpStream":null, "tcpStream":null},
{"packetId":7, "srcMac":"00:0c:29:69:e6:2b", "dstMac":"00:0c:29:b0:8d:62", "size":90, "timestamp_unix":1250143826117, "protocol":"NTP", "srcIp":
"192.168.1.30", "dstIp":"192.168.1.10", "srcPort":123, "dstPort":123, "udpStream":0, "tcpStream":null},
{"packetId":8, "srcMac":"00:0c:29:b0:8d:62", "dstMac":"00:0c:29:69:e6:2b", "size":90, "timestamp_unix":1250143826117, "protocol":"NTP", "srcIp":
"192.168.1.10", "dstIp":"192.168.1.30", "srcPort":123, "dstPort":123, "udpStream":0, "tcpStream":null
```

json

localhost:3000/dashboard

filter query



(frame.time >= "Aug 13, 2009 07:57:35") && (frame.time <= "Aug 13, 2009 07:58:06") && (ip.dst == 192.168.1.159) && (tcp || udp)

Options: Vizualization Dashboard

Option A: Cloud-hosted Dashboard

- ⊕ easier integration
- ⊕ no extra install
- ⊖ internet connection required
- ⊖ data upload

Option B: Local Dashboard

- ⊕ data stays on the device
- ⊕ no service dependency
- ⊖ more install requirements
- ⊖ start own localhost service

What do you think?

Would you use this plugin?

Which option would you perfer?

Are there more options?

Contact and Feedback

Dr. Alex Ulmer

User Centered Data Science, Visual Analytics
Fraunhofer IGD
Darmstadt, Germany

alex.ulmer@igd.fraunhofer.de

LinkedIn:

Thank you!

SharkFest Feedback Form