The DPI Analyzer

A Strategic Approach to Traffic Inspection

Presented by **Kagner Vladi**

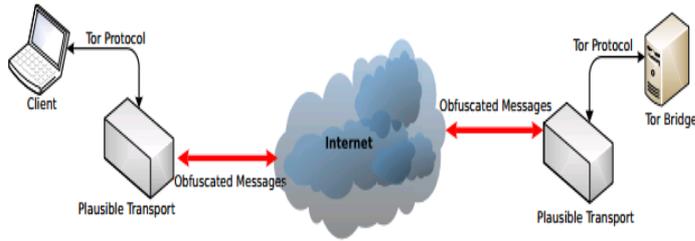Student at Shamoon College of Engineering (SCE)

June 14, 2014

2 Step 1

Research and collecting information

SkypeMorph

Disguise Communication

SkypeMorph
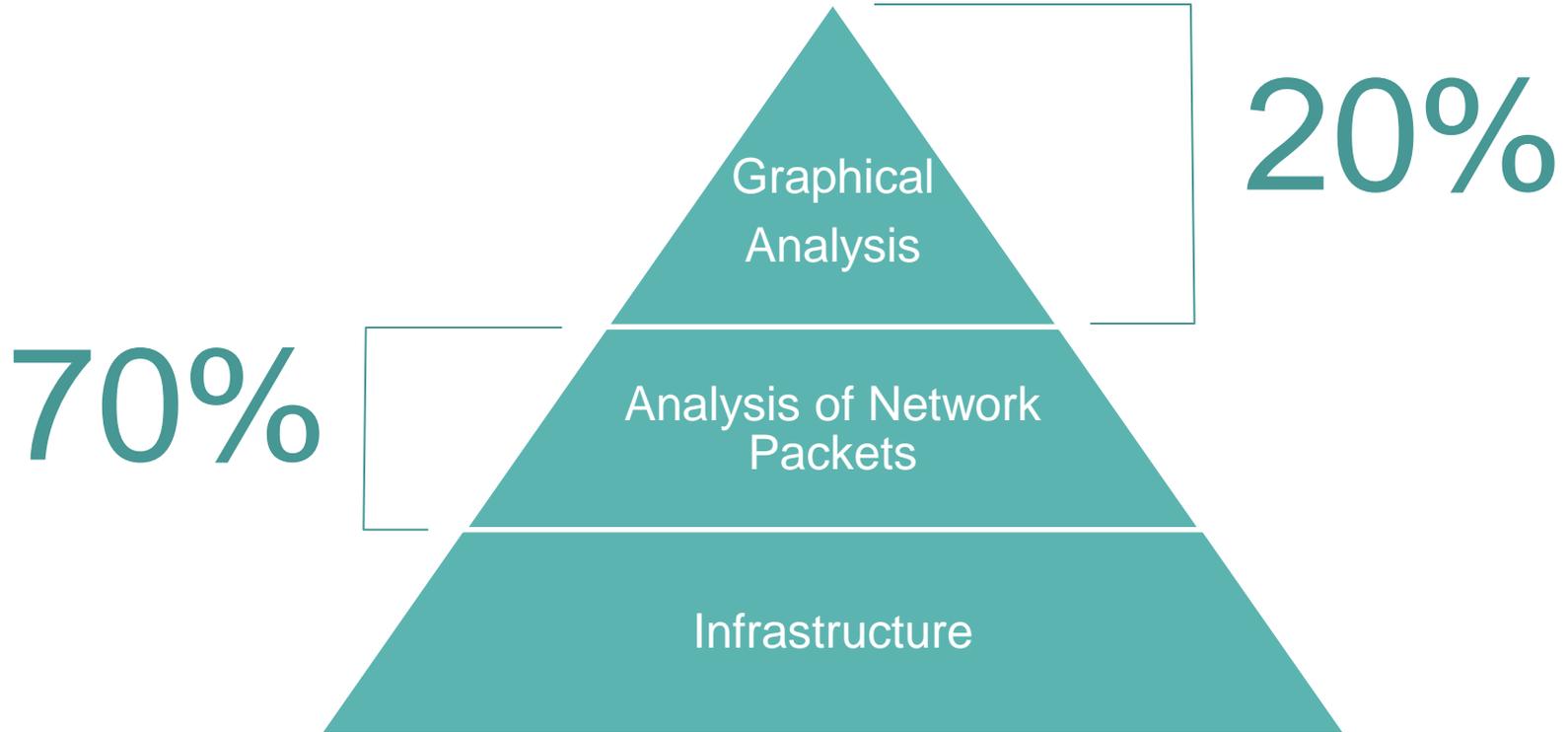## Protocol Obfuscation for Censorship Resistance

Tor traffic obfuscation: SkypeMorph disguises communication between the bridge and the client as a Skype video call, which is our target protocol. Protocol obfuscation is greatly needed when facing large-scale censorship mechanisms, such as deep packet inspection.

4

Step 2
Implementation and Testing

Architecture and Basic Phases

20%

Graphical Analysis

70%

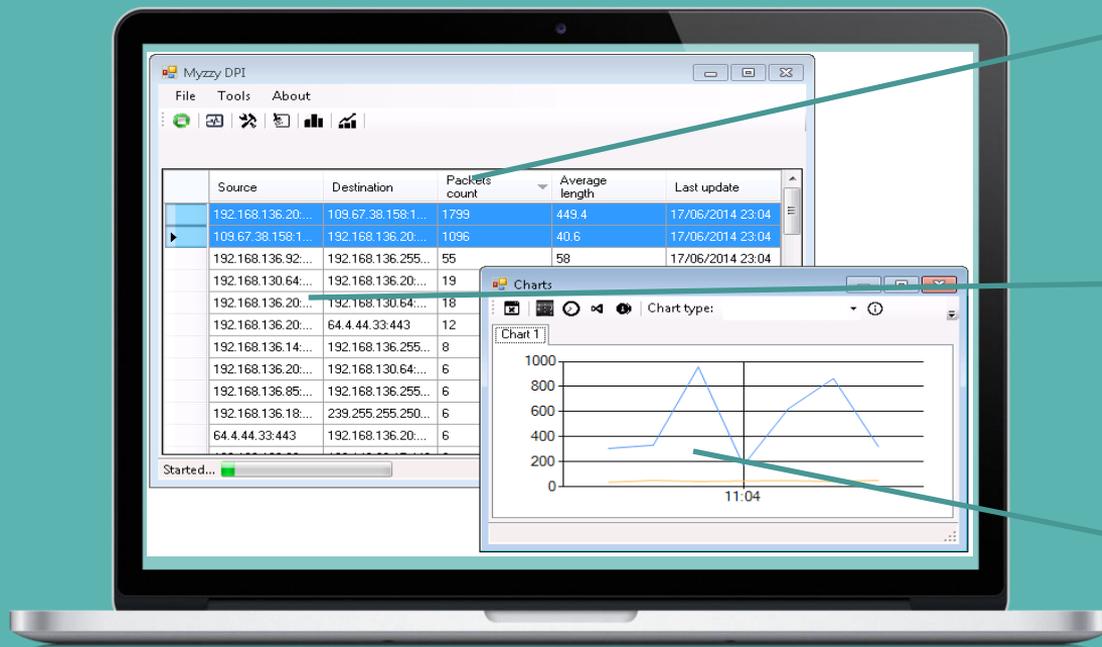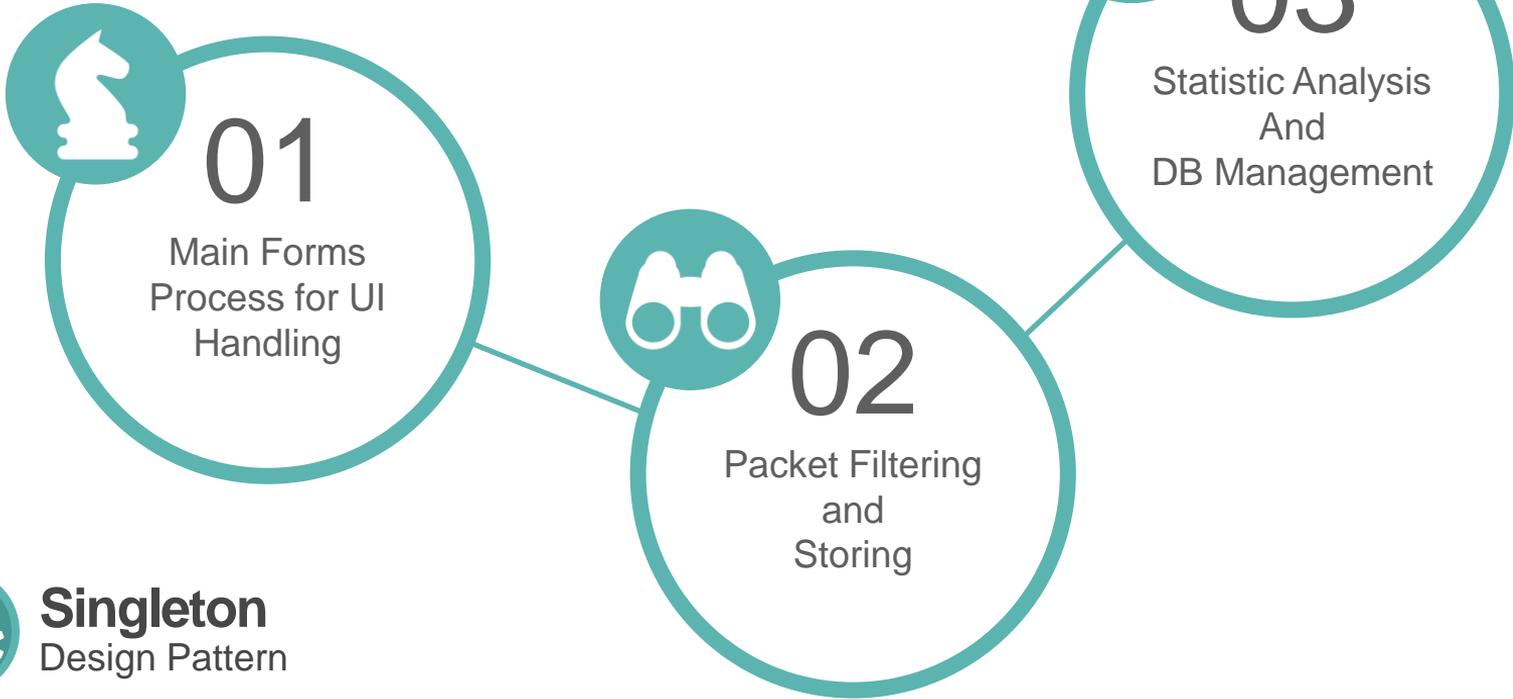Analysis of Network Packets

Infrastructure

6

Sort Options

Table View

Graphic View

Multithreaded Execution and Design Patterns

01
Main Forms
Process for UI
Handling

02
Packet Filtering
and
Storing

03
Statistic Analysis
And
DB Management

Singleton
Design Pattern

Statistic Data Structure

Statistic unit

Statistic unit

1 IN

2 IN

1 IN

2 IN

Statistic unit

Source IP and port, Destination IP and port …

Sub-Statistic unit for interval

Count, Size, Intervals, Average size …
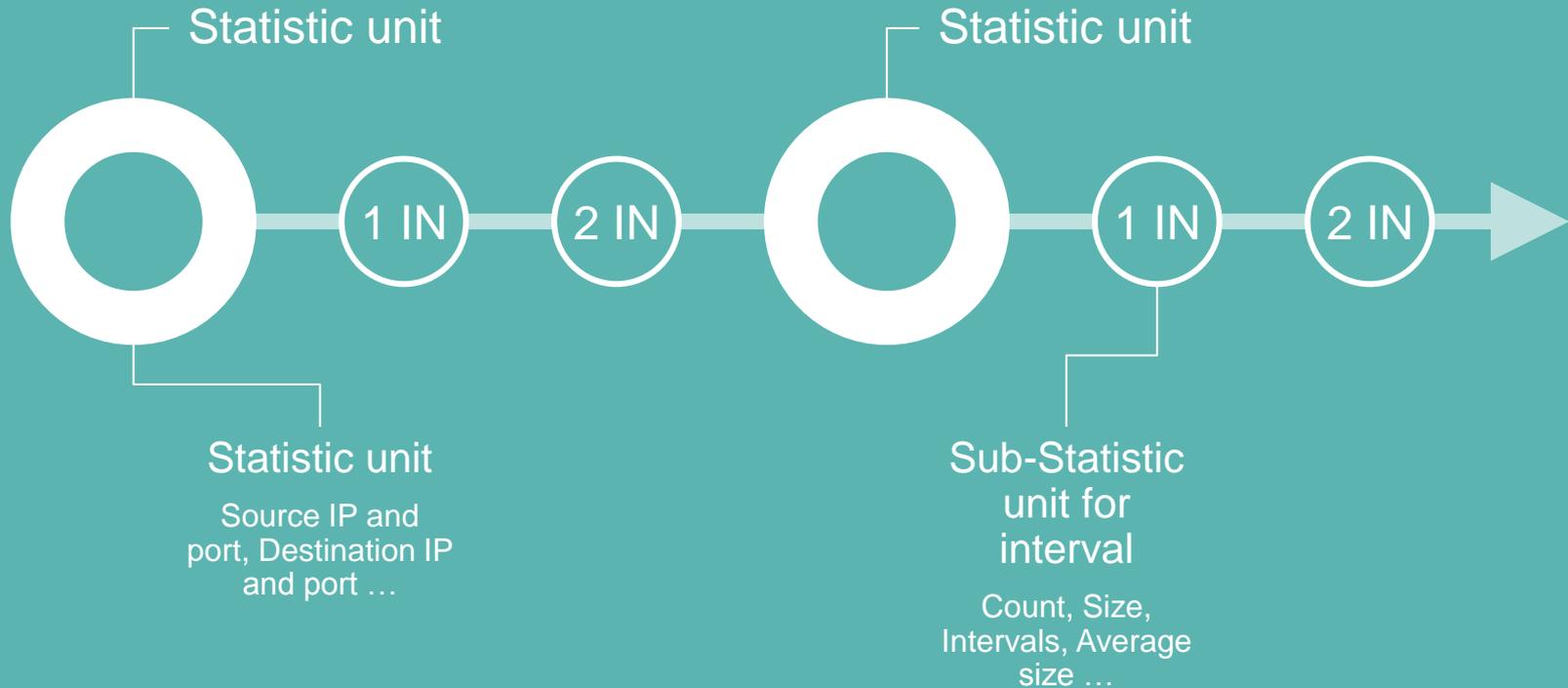
Application Lifecycle and Features

Choose Network Device

Packets Handling

Statistic Analysis

Visual Analysis

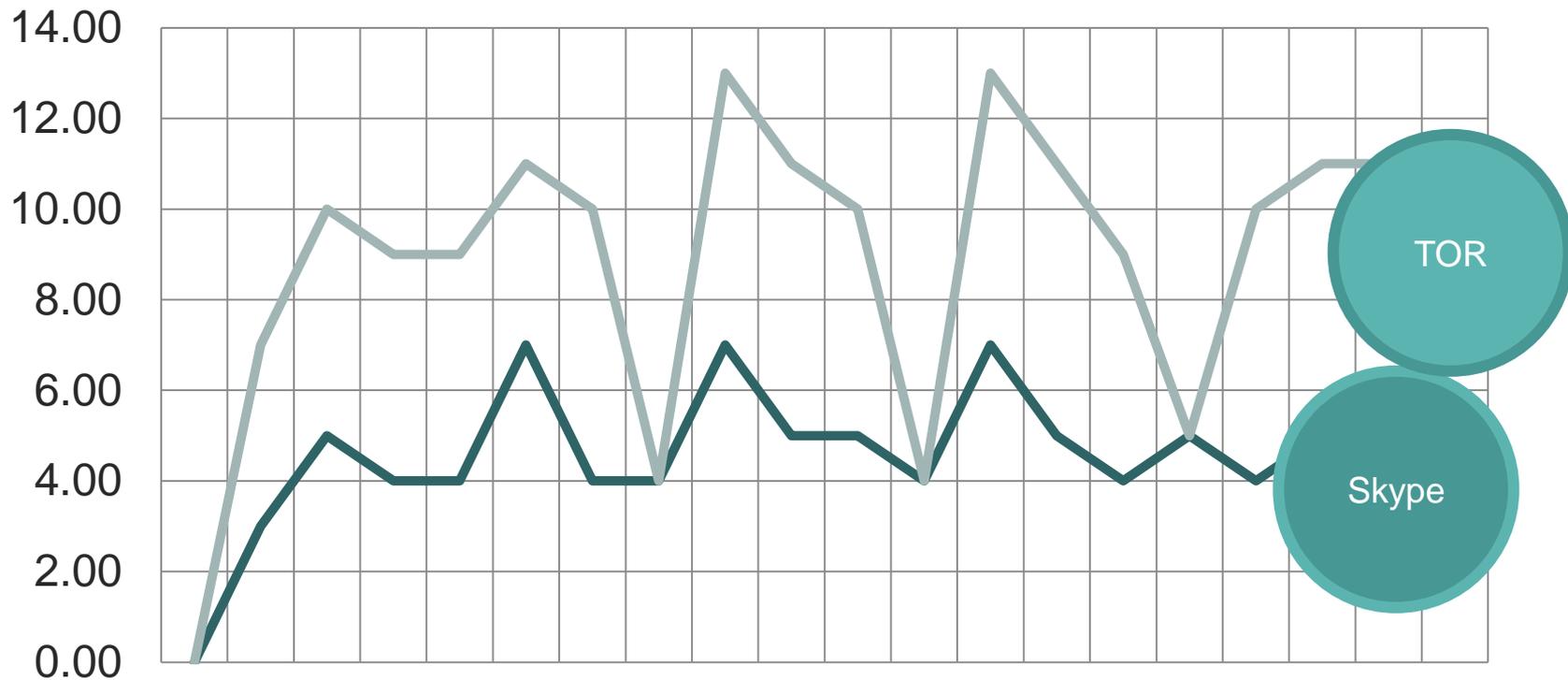Export / Import XML DB

Interactivity

Exit Application
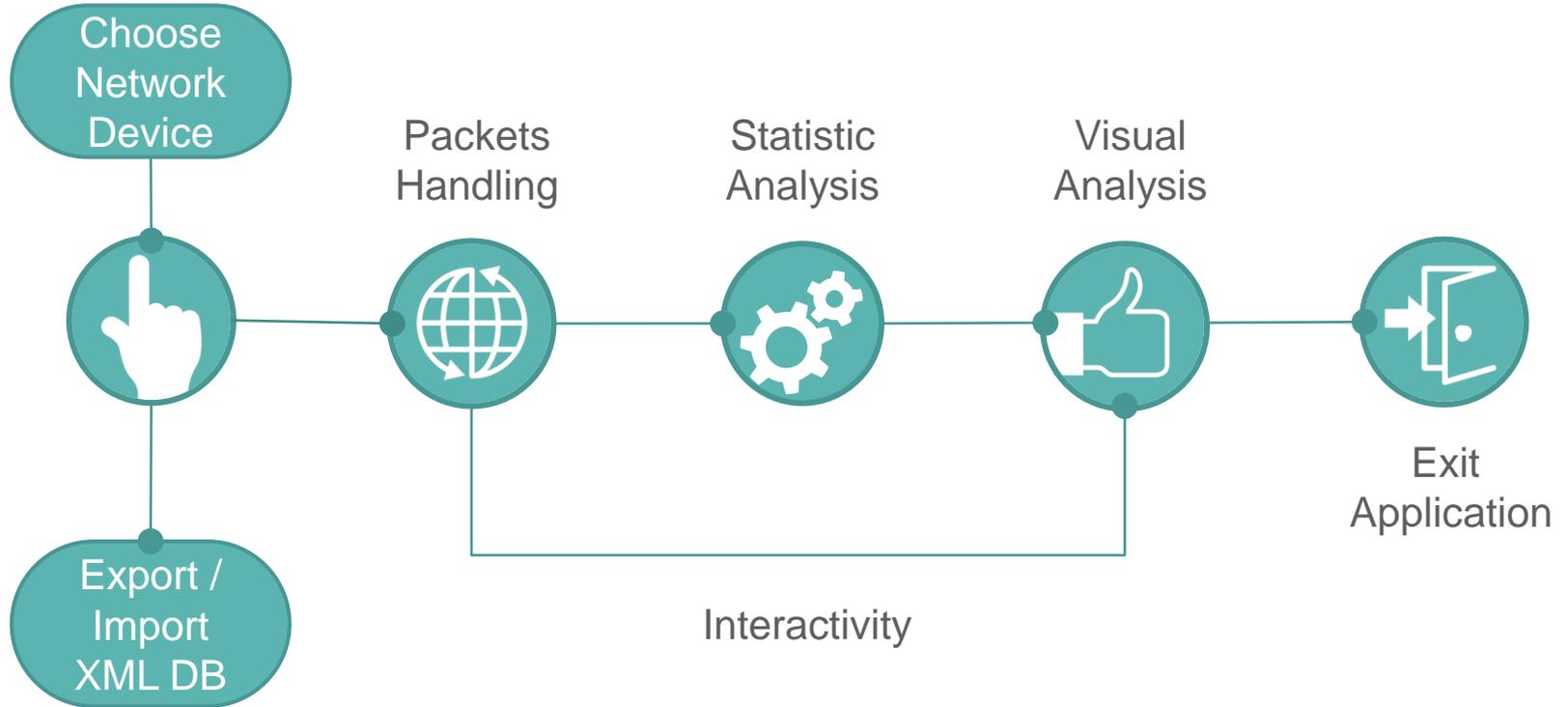
10

Step 3
Simulation and Optimization in Obfuscation Modeling

SkypeMorph Obfuscation Simulation

Network Traffic

12

Step 4

Conclusion

13 Conclusion

The DPI system is a complete solution for deep traffic analysis. We can conclude after simulation and tests that our statistics data shows that SkypeMorph has a sensible difference from Skype traffic. This difference can be a base for automatic statistical analysis to determinate the Tor traffic on specific station.