



# **SharkFest'23 US AGENDA**

## **June 10-15, San Diego, California**



**All times are in the Pacific Time Zone.**

**Conference days run from:**

**9:00 through 6:15, with evening events from  
6:00/6:30-8:30**

- **Pre-Conference Classes (9:00-5:00)**
- **SharkFest'23 US Session Agenda**
- **Session Abstracts & Instructor Bios**

# SharkFest'23 US Conference Agenda

## Pre-Conference Classes

| <b>Pre-Conference Class I</b><br><br><b>Learn Wireshark! Analyzer Intro and TCP Deep Dive for NetOps and SecOps</b><br><br><b>INSTRUCTOR: Ross Bagurdes</b><br><br><b>Location: KIPJ Theatre</b><br><br>For Class Description and Outline, please visit:<br><a href="https://sharkfest.wireshark.org/sfus/registration-options/">https://sharkfest.wireshark.org/sfus/registration-options/</a> | Saturday, June 10 |   |
|---|-------------------|---|
|   | 8:00-9:00         | Check-in & Badge Pick up                |
|   | 8:00-9:00         | Breakfast                               |
|   | 9:00-12:00        | Class in session (with morning break)   |
|   | 12:00-1:00        | Lunch                                   |
|   | 1:00-5:00         | Class in session (with afternoon break) |
|   | Sunday, June 11   |   |
|   | 8:00-9:00         | Breakfast                               |
|   | 9:00-12:00        | Class in session (with morning break)   |
|   | 12:00-1:00        | Lunch                                   |
|   | 1:00-5:00         | Class in session (with afternoon break) |
| <b>Pre-Conference Class II</b><br><br><b>Troubleshooting Voice over IP with Wireshark</b><br><br><b>INSTRUCTOR: Sake Blok</b><br><br><b>Location: KIPJ EF</b><br><br>For Class Description and Outline, please visit:<br><a href="https://sharkfest.wireshark.org/sfus/registration-options/">https://sharkfest.wireshark.org/sfus/registration-options/</a>                                    | Monday, June 12   |   |
|   | 8:00-9:00         | Check-in & Badge Pick up                |
|   | 8:00-9:00         | Breakfast                               |
|   | 9:00-12:00        | Class in session (with morning break)   |
|   | 12:00-1:00        | Lunch                                   |
|   | 1:00-5:00         | Class in session (with afternoon break) |

## SharkFest Opening & Welcome Dinner

| <b>SharkFest'23 US</b><br><br><b>Welcome Dinner &amp; Sponsor Showcase</b><br><br><b>Garden of the Sea</b> | Monday, June 12 |  |
|--|-----------------|--|
|  | 12:00-6:00      | <b>SharkFest'23 US Check-In &amp; Badge Pick-Up</b>  |
|  | 1:00-5:00       | <b>Developer Den Drop-In</b>   |
|  | 6:00-8:30       | <b><i>SharkFest'23 US Welcome Dinner &amp; Sponsor Showcase</i></b><br><br><b>SharkFest'23 US Attendees Only</b> |


# SharkFest'23 US Conference Agenda

| Tuesday, June 13 |  |  |
|------------------|--|--|
| 9:00-10:00       | <b>KEYNOTE: "...So That's What We Did"</b><br><b>Gerald Combs &amp; Friends</b><br><br><b>KIPJ Theatre</b> |  |
| 10:00-10:15      | BREAK  |  |
| 10:15-11:30      | <b>(Beginner/Intermediate)</b><br><b>KIPJ Theatre</b>  | <b>(Intermediate/Advanced)</b><br><b>KIPJ EF</b>   |
|                  | <b>01</b><br><b>Capturing Packets in a Kubernetes Container System</b><br>Jeff Carrell                     | <b>02</b><br><b>More Mileage from Your Tools: Problem Isolation with TLS and TCP – Part 1 of 2 part workshop</b><br>George Cragg |
| 11:30-11:45      | BREAK  |  |
| 11:45-1:00       | <b>03</b><br><b>Stylin' with Wireshark Profilin'</b><br>Josh Clark   | <b>04</b><br><b>More Mileage from Your Tools: Problem Isolation with TLS and TCP – Part 2 of 2 part workshop</b><br>George Cragg |
| 1:00-2:00        | LUNCH  |  |
| 2:00-3:15        | <b>05</b><br><b>Packet Capture in Public Cloud</b><br>Stephen Donnelly                                     | <b>06</b><br><b>TCP Case Study Packet Analysis exhibits from high visibility, high stakes critical problems</b><br>Bill Alderson |
| 3:15-3:30        | BREAK  |  |
| 3:30-4:45        | <b>07</b><br><b>"I wish Wireshark" - add the missing pieces with Lua</b><br>Chuck Craft                    | <b>08</b><br><b>Wireshark plus Advanced Analytics – Better Together (Part 1 of 2-part workshop)</b><br>John Pittle               |
| 4:45-5:00        | BREAK  |  |
| 5:00-6:15        | <b>09</b><br><b>Capturing WiFi6E with Wireshark</b><br>Megumi Takeshita                                    | <b>10</b><br><b>Wireshark plus Advanced Analytics – Better Together (Part 2 of 2-part workshop)</b><br>John Pittle               |
| 6:30-8:30        | <b>Sponsor Technology Showcase Reception, Treasure Hunt &amp; Dinner</b><br><b>Garden of the Sea</b>       |  |

# SharkFest'23 US Conference Agenda

| Wednesday, June 14 |  |   |
|--------------------|--|---|
| 9:00-10:00         | <b>KEYNOTE: "Network Protocol: Myths, Missteps, and Mysteries"</b><br><b>Radia Perlman</b><br><br><b>KIPJ Theatre</b>                    |   |
| 10:00-10:15        | BREAK  |   |
| 10:15-11:30        | <b>(Beginner/Intermediate)</b><br><b>KIPJ Theatre</b>  | <b>(Intermediate/Advanced)</b><br><b>KIPJ EF</b>  |
|                    | <b>11</b><br><b>Maintaining Dissector Quality</b><br>Martin Mathieson  | <b>12</b><br><b>Beyond Network Latency: Chasing Latency up the Stack</b><br>Josh Clark            |
| 11:30-11:45        | BREAK  |   |
| 11:45-1:00         | <b>13</b><br>The Packet Doctors are in! Packet trace examinations with the experts   |   |
| 1:00-2:00          | LUNCH  |   |
| 2:00-3:15          | <b>14</b><br><b>Dive into DNS over QUIC - DoQ</b><br>Betty DuBois  | <b>15</b><br><b>Your IPv6 is Being Attacked, How Do You Know?</b><br>Jeff Carrell                 |
| 3:15-3:30          | BREAK  |   |
| 3:30-4:45          | <b>16</b><br><b>Stepping up your packet analysis game by leveraging the Wireshark CLI tools (part 1 of 2-part workshop)</b><br>Sake Blok | <b>17</b><br><b>Kubeshark: The API Traffic Analyzer for Kubernetes</b><br>Alon Girmonsky          |
| 14:45-5:00         | BREAK  |   |
| 5:00-6:15          | <b>18</b><br><b>Stepping up your packet analysis game by leveraging the Wireshark CLI tools (part 2 of 2-part workshop)</b><br>Sake Blok | <b>19</b><br><b>Examining Efficiency Improvements of TLS 1.3 using Wireshark</b><br>Ross Bagurdes |
| 6:30-8:30          | <b>Sponsor Technology Showcase Reception, esPCAPe Group Packet Challenge &amp; Dinner</b><br><br><b>KIPJ ABCD</b>                        |   |

# SharkFest'23 US Conference Agenda

| Thursday, June 15 |  |   |
|-------------------|--|---|
| 9:00-10:00        | <p align="center"><b>SHARKBYTES</b></p> <p>SharkBytes consist of “little crunchy bits of wisdom.” Like popular TED talks, SharkBytes aim to inform, inspire, surprise, and delight by delivering a speech on a personal topic in under 5 minutes.<br/>           Information and a review of past SharkByte presentations can be found <a href="https://sharkfest.wireshark.org/sharkbytes">https://sharkfest.wireshark.org/sharkbytes</a><br/>           Email us your SharkByte session idea: <a href="mailto:sharkfest@wireshark.org">sharkfest@wireshark.org</a></p> <p align="center"><b>KIPJ Theatre</b></p> |   |
| 10:00-10:15       | BREAK  |   |
| 10:15-11:30       | (Beginner/Intermediate)<br>KIPJ Theatre  | (Intermediate/Advanced)<br>KIPJ EF  |
|                   | <p><b>20</b><br/> <b>How I Learned to Stop Worrying and Love the PCAP</b><br/>           Kary Rogers</p>   | <p><b>21</b><br/> <b>Applied Machine Learning for processing and reporting on large PCAP files</b><br/>           Anand Ravi and Johnny Ghibril</p> |
| 11:30-12:00       | BREAK  |   |
| 12:00-1:15        | <p><b>22</b><br/> <b>Wireshark and AI</b><br/>           Roland Knall</p>  | <p><b>23</b><br/> <b>QUIC Protocol Enterprise Overview &amp; Security Cautions</b><br/>           Bill Alderson</p>                                 |
| 1:15-1:30         | BREAK  |   |
| 1:30-2:45         | <p><b>24</b><br/> <b>Smart Move! - Tips and Tricks for Network Analysts</b><br/>           Jasper Bongertz</p>   | <p><b>25</b><br/> <b>SolarWinds Breach Report with Packet Analysis</b><br/>           Bill Alderson</p>   |
| 2:45-4:45         | <div>  <p align="center"><b>Closing Remarks and Farewell reception</b></p> <p align="center"><b>Garden of the Sea</b></p> </div>  |   |

# SharkFest'23 US Conference Agenda

## Session Abstracts & Instructor Bios

### TUESDAY, June 13

9:00-10:00

#### KEYNOTE: "...So That's What We Did" Gerald Combs & Friends

BREAK (10:00 – 10:15)

10:15-11:30

#### 01 Capturing Packets in a Kubernetes Container System

Network/application troubleshooting in a Kubernetes container based system poses unique challenges not quite like experienced in other systems. Challenges like not always access to the containers/pods to load tcpdump or other utilities, difficult to have realtime view of packet captures, and exporting pcap files outside the cluster. We will explore options for capturing packets in Kubernetes based systems.

(It is expected that attendees have some Kubernetes background and/or hands-on knowledge, as this session is not Kubernetes training)

**Instructor: Jeff Carrell, Networking & Big Data Instructor/Course Developer, Hewlett Packard Enterprise**

Jeff is a frequent industry speaker, technical writer, IPv6 Forum Certified Trainer, and prior to HPE was a network instructor and course developer to major networking manufacturers. He is a technical lead and co-author for the book, Guide to TCP/IP: IPv6 and IPv4, 5th Edition and lead technical editor on Fundamentals of Communications and Networking, Second Edition. Jeff has been in the computer industry since 1979, built his first LAN in 1986, and is a long-time user of Wireshark.

#### 02 More Mileage from Your Tools: Problem Isolation with TLS and TCP – Part 1 of 2 part workshop

As a network tool, Wireshark is often used for diagnosis and to prove/disprove the network contribution to various communication problems that inevitably arise. Here we explore a case study of problem isolation down to a finer level than just 'it's not the network'.

**Instructor: George Cragg, Network Engineer, Draeger Medical Systems**

George Cragg is a full time network engineer for a medical device company. Past careers include tree farmer, designing tire filling machines, and Six-Sigma Black Belt in the semiconductor industry.

BREAK (11:30 – 11:45)

11:45-1:00

#### 03 Stylin' with Wireshark Profilin'

Let's create some Wireshark profiles that both look good and are easy to use! If, like me, you find yourself using Wireshark for hours on end, you know that both aesthetics and workflow are very important. It's tiring to look at jarring colors all day, and the extra inefficiencies of an unoptimized workflow can really slow you down. Let's address both of those problems.

Expect to learn basic color theory (emphasis on basic; I'm an engineer, after all). Expect to learn how to create a color palette and to build coloring rules from it. Expect to learn effective layout and column options. Expect to learn a good starter set of display filter buttons.

**Instructor: Josh Clark, Distributed Performance Engineer, Huntington National Bank**

Josh is a Distributed Performance Engineer at Huntington National Bank, which means he gets to have fun with all the weirdest problems in the most complex systems the bank implements. Wireshark is his tool of choice to figure things out.

# SharkFest'23 US Conference Agenda

## 04 More Mileage from Your Tools: Problem Isolation with TLS and TCP – Part 2 of 2 part workshop

As a network tool, Wireshark is often used for diagnosis and to prove/disprove the network contribution to various communication problems that inevitably arise. Here we explore a case study of problem isolation down to a finer level than just 'it's not the network'.

**Instructor: George Cragg, Network Engineer, Draeger Medical Systems**

George Cragg is a full time network engineer for a medical device company. Past careers include tree farmer, designing tire filling machines, and Six-Sigma Black Belt in the semiconductor industry.

**LUNCH (1:00 – 2:00)**

**2:00-3:15**

## 05 Packet Capture in Public Cloud

Is packet capture still relevant in public cloud environments? Aren't flow logs sufficient, and doesn't the cloud provider secure their network? We will look at the motivations and use cases for packet capture in Cloud, as well as practical techniques for AWS and Azure.

**Instructor: Stephen Donnelly, CTO, Endace**

Stephen has worked on packet capture and time-stamping systems for 20 years, earning his PhD for "High Precision Timing in Passive Measurements of Data Networks" from the University of Waikato, New Zealand. A founding employee of Endace, Stephen has developed FPGA-based packet capture and timing systems, clock synchronization systems, and high-performance network monitoring virtualization, and collaborated with customers in telcos, finance, test & measurement, enterprise, and government agencies to solve unique problems. Stephen is a contributor to the Wireshark, libpcap, Argus, and Suricata open-source projects.

## 06 TCP Case Study Packet Analysis exhibits from high visibility, high stakes critical problems

Case study exhibits from high visibility, high stakes critical problems from TCP Offload Engine (TOE) affecting the Iraq & Afghan Wars to 20,000 users affected by the dreaded "Chernobyl Packet" and many more never seen before TCP case study exhibits.

This discussion with exhibits discusses advanced TCP Window visualizations, TCP Selective ACK, Retransmission Recovery, and application delay characteristics visualized with WireShark charts with associated stories. Lots of fun for packet heads and executives alike.

**Instructor: Bill Alderson, CTO, Cogent Management**

Bill Alderson has been the go-to expert for such challenges for decades, working with Fortune 500 companies, stock exchanges, the Pentagon following 9/11, and the military on six deployments to Iraq and Afghanistan. His proficiency in high-stakes, high-visibility situations has enabled him to consult with C-suite executives in major institutions to definitively establish and verify contested technical truths.

Adept in theory-based critical problem resolution and root cause analysis, Bill has trained and certified over 3,500 forensic technologists through his Certified NetAnalyst program. Many of his trainees have gone on to become accomplished CIOs and CISOs. Motivated by government and military leaders' requests for assistance in safeguarding national data.

**BREAK (3:15-3:30)**

**3:30 - 4:45**

## 07 "I wish Wireshark" - add the missing pieces with Lua

An existing field in a different format. New fields. Dissecting an unsupported protocol. Relate data across multiple packets. Custom statistics. Add menu items/utilities.

Sometimes just a little more information or existing information presented differently can facilitate packet analysis.

This session will look at examples from the Wireshark Ask Q&A site where a piece was missing from Wireshark and a Lua script helped in the solution.

After looking at "why" we will do the "how" deploying and modifying a template Lua post-dissector from the Wireshark wiki.

# SharkFest'23 US Conference Agenda

## **Instructor: Chuck Craft**

Chuck was a long time Wireshark dabbler (think HP-UX), got serious in 2019 (thanks Chris Greer) and was welcomed to the core developers in 2022. He has been working on networks since the days of the vampire tap (never got to use one). He does Wireshark support, contributes to the Wireshark code base and always on the lookout for interesting programming work.

## **08 Wireshark plus Advanced Analytics – Better Together (Part 1 of 2-part workshop)**

Real life troubleshooting a difficult 3<sup>rd</sup> party software performance issue with using Wireshark and Advanced Analytics

Description: Join us for a troubleshooting deep dive into solving a difficult problem occurring within Webex login from 2018, known as the 98% hang condition. We'll showcase how the partnership of Wireshark and Advanced Analytics can be leveraged to quickly isolate the fault domain. Captures will be provided for use during the session. Session is half presentation and half hands-on lab with Wireshark.

## **Instructor: John Pittle, Customer Experience CTO, Riverbed Technology, Inc.**

As a Performance Management Strategist, John helps his customers develop and execute strategies for integrating Performance Management as an IT discipline across the organization. He has been actively focused on Performance Engineering and Analysis for networks, systems, and applications since the early 90s; performance troubleshooting is his passion and joy. His packet analysis toolbox includes Wireshark (of course), as well as NetShark, AppResponse, Packet Analyzer, and Transaction Analyzer.

**BREAK (4:45 – 5:00)**

**5:00-6:15**

## **09 Capturing WiFi6E with Wireshark**

Spectrum analysis in 6GHz band and trace file analysis of WiFi6E using Wireshark. How to create capture environments in Windows, Linux and macOS.

WiFi6E implementation is (will be) released in Japan this year, as the United States has already started. Europe and the other world are also ready for 6GHz WiFi bands. It is time to analyse WiFi6E with Wireshark.

In this session, we capture IEEE802.11ax in 6GHz channels. And we dissect specified fields of the radiotap / IEEE 802.11 header in 6E trace files using Wireshark.

Megumi (JA1UVG) also demonstrates spectrum analysis in the 6GHz band and indicates how to create capture environments in Windows, Linux and macOS. The session also includes basics of radio technology basic and IEEE 802.11 standards.

## **Instructor: Megumi Takeshita, Packet Otaku and Owner, Ikeriri Network Service**

Megumi Takeshita, or Packet Otaku, runs a packet analysis company, Ikeriri Network Service, in Japan. Ikeriri offers services such as packet analysis for troubleshooting, debugging and security inspection. Ikeriri is also a reseller of wired/wireless capture and analysis devices and software for Riverbed, Metageek, Profitap, Dualcomm, and others. Megumi has authored 10+ books about Wireshark and packet analysis in Japanese and she is an avid contributor to the Wireshark project.

## **10 Wireshark plus Advanced Analytics – Better Together (Part 2 of 2-part workshop)**

Real life troubleshooting a difficult 3<sup>rd</sup> party software performance issue with using Wireshark and Advanced Analytics

Description: Join us for a troubleshooting deep dive into solving a difficult problem occurring within Webex login from 2018, known as the 98% hang condition. We'll showcase how the partnership of Wireshark and Advanced Analytics can be leveraged to quickly isolate the fault domain. Captures will be provided for use during the session. Session is half presentation and half hands-on lab with Wireshark.

## **Instructor: John Pittle, Customer Experience CTO, Riverbed Technology, Inc.**

As a Performance Management Strategist, John helps his customers develop and execute strategies for integrating Performance Management as an IT discipline across the organization. He has been actively focused on Performance Engineering and Analysis for networks, systems, and applications since the early 90s; performance troubleshooting is his passion and joy. His packet analysis toolbox includes Wireshark (of course), as well as NetShark, AppResponse, Packet Analyzer, and Transaction Analyzer.

**6:30-8:30**

**Sponsor Technology Showcase Reception, Treasure Hunt & Dinner**



# SharkFest'23 US Conference Agenda

## WEDNESDAY, June 14

9:00-10:00

### KEYNOTE: "Network Protocol: Myths, Missteps, and Mysteries" Radia Perlman

BREAK (10:00 – 10:15)

10:15-11:30

#### 11 Maintaining Dissector Quality

What can we do to maintain the quality of the many dissectors that have been added to Wireshark over the past 25 years, and what can we do to check the quality of new dissector code as it is added to the project? Learn about the hurdles dissector code must clear before and after being merged into the Wireshark codebase, and how interesting bugs seen during review sometimes lead to new automated checks - to find similar existing bugs and help prevent new ones.

This talk will discuss the various things that we do to ensure the quality of dissectors, while trying to make the process not be too onerous for prospective contributors. The code is checked against various compilers, packaging tools, checked builds, test suites, various checking scripts before it may be merged.

After successful human code review and merging, it can also be fuzzed and (of course) used and broken by real users. Lots of the issues that we detect are indisputably errors that must be fixed, but many others still require human interpretation. Expect to learn more about how dissectors can show the protocol fields they find in frames, and what can happen when API usage goes bad.

**Instructor: Martin Mathieson, Software Engineer, Wireshark Core Developer**

Martin is a software engineer from the UK who in recent years has mostly worked on mobile telecoms test equipment. And, since 2006, he has been proud to call himself a Wireshark core developer.

#### 12 Beyond Network Latency: Chasing Latency up the Stack

"The website is slow, so the network must be having an issue."

Network engineers skilled with Wireshark are masters of responding to statements like this one. With one peek at the iRTT, one scroll through the TCP stream, and one long-running ping to the web server, network latency can be disproven. But how do we take the next step? How do we help a server admin or application owner identify exactly what is happening?

Packets can isolate latency at the network, the server, and the application, and this talk will walk through how to find and understand those latencies.

Expect a review of identifying network latency. Expect to learn how to isolate both server and application latency. Expect to learn how network data propagates through a Linux server and where it makes pit stops along the way.

**Instructor: Josh Clark, Distributed Performance Engineer, Huntington National Bank**

Josh is a Distributed Performance Engineer at Huntington National Bank, which means he gets to have fun with all the weirdest problems in the most complex systems the bank implements. Wireshark is his tool of choice to figure things out.

BREAK (11:30 – 11:45)

11:45-1:00

#### 13 The Packet Doctors are in! Packet trace examinations with the experts

The experts on this panel have been asked to look at a trace file and help find a reason for certain behaviors by attendees at many SharkFests. Based on this, they've decided to create a public forum for examining individual trace files with a broader audience for a collective learning experience. Trace files will be gathered from attendees prior to SharkFest and only given to the panel members during the session so that the "not-knowing what to expect and whether it can be solved" experience of working through an unknown trace file can be preserved.

# SharkFest'23 US Conference Agenda

Come to this session and learn to ask the right questions and look at packets in different ways.

PLEASE SEND PERPLEXING TRACE FILES FOR ANALYSIS BY THE PANEL TO [jasper@packet-foo.com](mailto:jasper@packet-foo.com) PRIOR TO SHARKFEST!

LUNCH (1:00 – 2:00)

2:00-3:15

## 14 Dive into DNS over QUIC - DoQ

DNS is one of the last protocols left that uses clear text. With the implementations of DNS over TLS and DNS over HTTPs, that is steadily changing. However, DoT and DoH are not without their drawbacks. Enter DNS over QUIC aka DoQ, and RFC9250.

This presentation will cover how DoQ works in resolvers, authoritative servers and zone transfers. Pcaps will be provided via [CloudShark Enterprise Hosted](#) so you can follow along.

### Instructor: Betty DuBois, Mystery Solver, Packet Detectives

[Betty DuBois](#) unlocks the power of packets to resolve NetOps and SecOps issues. Founder of Packet Detectives, an application & network performance consulting and training firm the Washington, D.C area. She has been solving packet mysteries since 1997.

Experienced with a range of hardware and software packet capture solutions, she captures the right data, in the right place, and at the right time to find the real culprit.

Using packets to solve crimes against networks and applications is her passion. Teaching others to do the same is her calling.

## 15 Your IPv6 is Being Attacked, How Do You Know?

You have implemented IPv6 - yee-ha! Now it is being attacked, how do you know?

Are the IPv6 enabled clients complaining of "slowness"? If so, you may have rogue IPv6 routers and/or DHCPv6 servers on the network.

Are some client systems not able to obtain an IPv6 address? You may have a rogue system answering for all the DAD queries.

Wireshark configuration profiles, display filters, and color rules can provide specific focus when troubleshooting reported IPv6 problems, and how to effectively and expeditiously determine what could be the root cause.

This will be a hands-on/follow Jeff session with provided trace files, so be sure to bring your laptop with Wireshark installed.

### Instructor: Jeff Carrell, Networking & Big Data Instructor/Course Developer, Hewlett Packard Enterprise

Jeff is a frequent industry speaker, technical writer, IPv6 Forum Certified Trainer, and prior to HPE was a network instructor and course developer to major networking manufacturers. He is a technical lead and co-author for the book, Guide to TCP/IP: IPv6 and IPv4, 5th Edition and lead technical editor on Fundamentals of Communications and Networking, Second Edition. Jeff has been in the computer industry since 1979, built his first LAN in 1986, and is a long-time user of Wireshark.

BREAK (3:15 – 3:30)

3:30-4:45

## 16 Stepping up your packet analysis game by leveraging the Wireshark CLI tools (2-part workshop)

In this 2-slot HANDS-ON workshop you will add the Wireshark CLI tools to your toolbox in order to increase efficiency in analysing packet capture data. Preprocessing pcap files on the command-line (directly or with scripting) will greatly enhance the speed by which you can analyse the packets you need in Wireshark.

You will also practice with extracting data from pcap files that is hard to do with Wireshark. Being able to report on just any combination of fields in statistical overviews could help in pinpointing the root cause of an issue or enhance your understanding of the data flows in your environment.

# SharkFest'23 US Conference Agenda

## **Instructor: Sake Blok, Relational Therapist for Computer Systems**

Sake has been analyzing packets for over 15 years. While working for a reseller of networking equipment, he discovered many bugs in devices from multiple vendors and presented his findings to the vendors to fix the issues. He also discovered many configuration issues that have led to functional problems or performance issues in applications running over the network. These issues were then resolved based on the reports presented to his customers. In 2009, Sake started the company SYN-bit to provide network analysis services to enterprises across Europe. During his work, Sake started developing functionality for Wireshark that he missed while working with the analyzer in his day-to-day job. He also enhanced multiple protocol dissectors to suit his analysis needs. In 2007, Sake joined the Wireshark Core Development team.

## **17 Kubeshark: The API Traffic Analyzer for Kubernetes**

**\*\*Kubernetes\*\*** distributed and highly dynamic nature makes K8s network a blindspot. It introduces many challenges that relate to network analysis for purposes of investigation, debugging and troubleshooting, threat hunting and security threat detection.

[Kubeshark] (<https://github.com/kubeshark/kubeshark>) is a new open-source tool that provides real-time protocol-level visibility into K8s network, capturing and monitoring all traffic and payloads going in, out and across containers, pods, nodes and clusters. In this hands-on workshop we will learn how to set up Kubeshark, view protocol-level real-time K8s traffic, automate the detection of suspicious network behaviors, conditionally generate PCAP files, export the PCAPs as well as telemetry data to tools such as S3, Grafana and Elastic.

**\*\*Workshop:\*\*** [Kubeshark](<https://github.com/kubeshark/kubeshark>): The API Traffic Analyzer for Kubernetes

**\*\*Why attend:\*\*** Learn how to gain real-time protocol-level visibility to K8s traffic, and conditionally generate and export PCAPs and telemetry data.

**\*\*Who should attend\*\*:** Devops, SREs, AppSec and Security Engineers that deal with K8s deployments

**\*\*Pre-requisites:\*\***

1. Having minikube and kubectl installed.
2. (Optional) Some K8s app (e.g. [this one](<https://github.com/kubeshark/sock-shop-demo>))

**\*\*Workshop Topics:\*\***

1. View real-time traffic
2. Use a rich query language to filter and search for specific information that is hiding in the network
3. Use Javascript to create rich detection rules
4. Conditionally generate PCAPs and upload to S3
5. Export metrics to Grafana

## **Instructor: Alon Girmonsky, Co-Creator and Maintainer of Kubeshark**

An executive by day and a coder by night, Alon Girmonsky is a repeat entrepreneur with a track record of building successful infrastructure companies. Most recently he founded BlazeMeter, a load and performance testing company that was acquired by CA technologies. Alon is the co-creator and a maintainer of Kubeshark.

**BREAK (4:45 – 5:00)**

**5:00-6:15**

## **18 Stepping up your packet analysis game by leveraging the Wireshark CLI tools (2-part workshop)**

In this 2-slot HANDS-ON workshop you will add the Wireshark CLI tools to your toolbox in order to increase efficiency in analysing packet capture data. Preprocessing pcap files on the command-line (directly or switch scripting) will greatly enhance the speed by which you can analyse the packets you need in Wireshark.

You will also practice with extracting data from pcap files that is hard to do with Wireshark. Being able to report on just any combination of fields in statistical overviews could help in pinpointing the root cause of an issue or enhance your understanding of the data flows in your environment.

## **Instructor: Sake Blok, Relational Therapist for Computer Systems**

Sake has been analyzing packets for over 15 years. While working for a reseller of networking equipment, he discovered many bugs in devices from multiple vendors and presented his findings to the vendors to fix the issues. He also discovered many configuration issues that have led to

# SharkFest'23 US Conference Agenda

functional problems or performance issues in applications running over the network. These issues were then resolved based on the reports presented to his customers. In 2009, Sake started the company SYN-bit to provide network analysis services to enterprises across Europe. During his work, Sake started developing functionality for Wireshark that he missed while working with the analyzer in his day-to-day job. He also enhanced multiple protocol dissectors to suit his analysis needs. In 2007, Sake joined the Wireshark Core Development team.

## 19 Examining Efficiency Improvements of TLS 1.3 using Wireshark

In this session, we will examine the basics of TLS encryption, and examine the key differences between TLS 1.2 and TLS 1.3, measuring the efficiencies gained in TLS 1.3 in Wireshark. We will start with a brief history of TLS which will both introduce the main concepts as well as provide the necessary vocabulary to understand the protocol. Then we will offer a visualization of TLS encryption to understand the encryption process, which will be valuable when we examine a Wireshark Capture of TLS encrypted packets. Next we will examine captures of TLS 1.2 and TLS 1.3 sessions to the same website, comparing the efficiencies gained in TLS 1.3, while examining how to measure the efficiency using tools in Wireshark.

### Instructor: Ross Bagurdes, Network Engineer & Educator, Bagurdes Technology

Ross has had a diverse career in engineering, beginning as a structural engineer, then project engineer for a gas utility, Ross was always quickly assigned the de-facto network administrator, typically after no one else was brave enough to break, and later fix, the network. Ross eventually ended up working as a network engineer designing and implementing enterprise networks for a major university hospital. Here he worked with Extreme Networks, HP, Cisco, Tipping Point, among other network technology, as well as honed his Wireshark and protocol analysis skills. Ross spent 7 years teaching data networking at Madison College, and in 2017 started authoring and producing IT training videos in Wireshark/Protocol Analysis, Cisco, and general networking topics for [www.Pluralsight.com](http://www.Pluralsight.com). In his free time, you'll find Ross and his dog at the beach swimming and surfing, traveling, hiking, or snowboarding somewhere in the western US.

6:30-8:30

**Sponsor Technology Showcase, esPCAPe Group Packet Challenge, Reception & Dinner**

# SharkFest'23 US Conference Agenda

## THURSDAY, June 15

9:00-10:00

### SharkBytes

BREAK (10:00 – 10:15)

10:15-11:30

#### 20 How I Learned to Stop Worrying and Love the PCAP

Everyone knows the packets don't lie but opening a pcap can be overwhelming if you're new to Wireshark. In this session we'll start from the very beginning of narrowing down the problem to setting up Wireshark to looking for the problem. This is a hands on session with quizzes and exercises along the way.

In this session, you'll learn what to do before you ever fire up Wireshark. We'll go over how to narrow down a problem so it's less overwhelming. How to understand the problem better than the people who are reporting it. If you define the problem specifically, the analysis is so much easier later. We'll cover how to verify you have the data you need and how to setup Wireshark to increase your chance of success. Then we'll begin analysis and try to find the issue. At the start, you'll download pcaps and follow along as we try to find why a web page is loading slowly.

**Instructor: Kary Rogers, Senior Director of Services Excellence, ZScaler**

Kary has spent many years solving difficult system, network, and application problems by looking at the packets. Even though he's been in management for a while, he still occasionally finds himself chasing the high of unraveling a packet mystery. He has a YouTube channel called PacketBomb where he posts Wireshark videos or has a live stream with your favorite packeteers.

#### 21 Applied Machine Learning for processing and reporting on large PCAP files

Analyzing Packet captures for large trace files with several thousands of packets has limitations and challenges in Wireshark. We will present how Machine learning and Artificial Intelligence based insights for packet capture analysis can significantly accelerate time towards troubleshooting by isolating and identifying root errors/catastrophic network failures before loading into Wireshark for in-depth analysis. Join us for a demo that will cover where the network failure occurs, by looking at:

1. PCAP Analytics and insights that provide critical statistics
2. Interactive call flow visualizations to swiftly identify root error/s that correspond to frame numbers in the trace file
3. Granular protocol-correlated analysis to uncover anomalies
4. Machine learning driven insights for Pass/Fail classification of call flows and identify behavior of packets in the trace.

**Instructor: Anand Ravi, Engineer and Lead Architect, B-Yond and Johnny Ghibril**

Anand is seasoned Engineer and Lead Architect at B-YOND. He holds a Master's degree in Telecommunications and has over a decade of hands-on experience in network testing and operations. Over the years, he has helped operators navigate multiple technology transitions through hands-on network certification as a member or field testing, labs, operations, and maintenance engineering teams. He has also led programs that combined people+automation to scale processes to meet the expanding complexity and scale with 5G adoption.

BREAK (11:30 – 12:00)

12:00-1:15

#### 22 Wireshark and AI

AI is the new hot thing in town. In this session we demonstrate, how you can use AI with Wireshark for filtering, asking the right questions or giving the right inputs to gain the most from it. Additionally we demonstrate a fast and easy way to write your own protocol dissector by using the AI

**Instructor: Roland Knall, Wireshark Core Developer**

Roland has been a software developer for around 25 years, 8 of which he has developed for Wireshark and 6 of those as a Core Developer. He has seen all beginning with web and basic UI development and more recently focusing on embedded systems.

# SharkFest'23 US Conference Agenda

## 23 QUIC Protocol Enterprise Overview & Security Cautions

QUIC Protocol overview by 40 year career Packetman007 for enterprises to rapidly understand how QUIC works with diagrams not found in rfc's. Wireshark side by side TCP vs QUIC benchmark results. Security cautions for enterprises.

IETF's rfc 9000, QUIC, already impacts all O/S, web browsers and servers, Google, YouTube, Meta, while Microsoft is rolling out QUIC in future 2022 Server, Outlook, Exchange, 365, file access and RDP communications impacting internal operations. Linux, Apple and other systems and database transport protocols are similarly transitioning. Firewall vendors do not yet support QUIC as the protocol headers are encrypted making QUIC "blind" to all middle devices such as firewalls, load balancers, deep inspection systems, data loss prevention (DLP). QUIC uses UDP Port 443, not TCP that has intrinsic firewall protocol syntax providing enterprise network protections by existing firewalls that UDP does not, requiring additional understanding and immediate mitigation. Bill will explain why QUIC is needed, its 3-10x speed improvement over discrete TCP / SSL / HTTP providing while providing monitoring suggestions with security cautions. Bill will demonstrate Wireshark QUIC decryption and chart discrete stream performance inside QUIC Connections and enablements by QUIC to harness 5G bandwidth and rapid mobile reconnects.

### Instructor: Bill Alderson, CTO, Cogent Management

Bill Alderson has been the go-to expert for such challenges for decades, working with Fortune 500 companies, stock exchanges, the Pentagon following 9/11, and the military on six deployments to Iraq and Afghanistan. His proficiency in high-stakes, high-visibility situations has enabled him to consult with C-suite executives in major institutions to definitively establish and verify contested technical truths.

Adept in theory-based critical problem resolution and root cause analysis, Bill has trained and certified over 3,500 forensic technologists through his Certified NetAnalyst program. Many of his trainees have gone on to become accomplished CIOs and CISOs. Motivated by government and military leaders' requests for assistance in safeguarding national data.

**BREAK (1:15-1:30)**

**1:30-2:45**

## 24 Smart Move! - Tips and Tricks for Network Analysts

Analyzing network packets can be made easier or even elegant with the right ideas on how to approach the problem that needs to be solved. This talk will present a couple of problem scenarios and analytic challenges and some smart ways to get to the answers we need. This will include the use (and explanation) of display and capture filters, coloring rules, command line tools and general Wireshark workflows.

### Instructor: Jasper Bongertz, Network Security Expert, G DATA Advanced Analytics

Jasper Bongertz is a network security expert with focus on network forensics and incident response at G DATA Advanced Analytics in Bochum, Germany. He started working freelance in 1992 while he was studying computer science at the Technical University of Aachen. In 2009, Jasper became a Senior Consultant and trainer for Fast Lane, where he created a large training portfolio with a special focus on Wireshark and network hacking. In 2013, he joined Airbus CyberSecurity, focusing on IT security, Incident Response and Network Forensics, before moving on and joining G DATA Advanced Analytics in August 2019 as the Principal Network Security Specialist and Head of Incident Response. Jasper is the creator of the packet analysis tool "TraceWrangler", which can be used to convert, edit and sanitize PCAP files. His blog regarding packet capture, network analysis, network forensics and general security topics can be found at [blog.packet-foo.com](https://blog.packet-foo.com).

## 25 SolarWinds Breach Report with Packet Analysis

SolarWinds who, what, when where and why, the 5 W's explained, diagrams of the 11 evading steps, who bears responsibility by step with WireShark packet analysis and unique observations on how to prevent and avoid supply chain compromise.

SolarWinds Supply Chain Attack, notwithstanding nation-state criminal involvement, a global blame game continues – but are we denying reality? It seems we did not lock our own doors with FBI, CIA, and NSA, themselves culpable for losing their Red-Team hacking tools criminals now use against the world. Opinions aside, startling facts remain.

### Instructor: Bill Alderson, CTO, Cogent Management

Bill Alderson has been the go-to expert for such challenges for decades, working with Fortune 500 companies, stock exchanges, the Pentagon following 9/11, and the military on six deployments to Iraq and Afghanistan. His proficiency in high-stakes, high-visibility situations has enabled him to consult with C-suite executives in major institutions to definitively establish and verify contested technical truths.

# SharkFest'23 US Conference Agenda

Adept in theory-based critical problem resolution and root cause analysis, Bill has trained and certified over 3,500 forensic technologists through his Certified NetAnalyst program. Many of his trainees have gone on to become accomplished CIOs and CISOs. Motivated by government and military leaders' requests for assistance in safeguarding national data.

**2:45-4:45**

**Closing Remarks & Farewell Reception**