SharkFest'23 ASIA AGENDA
April 17-19, Singapore

Conference days run from:
8:30 through 5:00, with evening events from 6:00-8:00

- **Pre-Conference Classes (10:00-5:00)**
- **SharkFest'23 ASIA Session Agenda**
- **Session Abstracts & Instructor Bios**

SharkFest'23 ASIA Conference Agenda

Pre-Conference Classes

Pre-Conference Class I **Making a good thing better: Optimization and Troubleshooting with Wireshark!** **INSTRUCTOR: Phill Shade** **For Class Description and Outline, please visit: https://sharkfest.wireshark.org/sfasia/registration-options/**	Monday, April 17 – Lecture Theatre 301	
	9:00-10:00	Check-in & Badge Pick up – Function Hall 3
	9:00-10:00	Breakfast – Function Hall 3
	10:00-1:00	Class in session (with morning break)
	1:00-2:00	Lunch
	2:00-5:00	Class in session (with afternoon break)
Pre-Conference Class II **SSL/TLS Troubleshooting with Wireshark** **INSTRUCTOR: Sake Blok** **For Class Description and Outline, please visit: https://sharkfest.wireshark.org/sfasia/registration-options/**	**Monday, April 17 – Auditorium 302**	
	9:00-10:00	Check-in & Badge Pick up – Function Hall 3
	9:00-10:00	Breakfast – Function Hall 3
	10:00-1:00	Class in session (with morning break)
	1:00-2:00	Lunch
	2:00-5:00	Class in session (with afternoon break)

SharkFest Opening & Welcome Dinner

SharkFest'23 ASIA **Welcome Dinner & Sponsor Showcase**	Monday, April 17 – Function Hall 3	
	12:00-6:00	**SharkFest'23 ASIA Check-In & Badge Pick-Up**
	1:00-5:00	**Developer Den Drop-In**
	6:00-8:00	***SharkFest'23 ASIA Welcome Dinner & Sponsor Showcase*** **SharkFest'23 ASIA Attendees Only**

SharkFest'23 ASIA Conference Agenda

Tuesday, April 18 – Auditorium 302	
9:30-10:30	**KEYNOTE: "*Latest Wireshark Developments & Road Map*"** **Gerald Combs & Friends**
10:30-10:45	**BREAK – Function Hall 3**
10:45-12:00	**01** **Use of Wireshark in LTE and 5G Networks** Mark Stout
12:00-12:15	**BREAK**
12:15-1:30	**02** **Visualize application traffic using Wireshark** Megumi Takeshita
1:30-2:30	**LUNCH – Function Hall 3**
2:30-3:45	**03** **Visualizing and Decrypting TLS 1.3** Ross Bagurdes
3:45-4:00	**BREAK**
4:00-5:15	**04** **How did that happen? - Packets may never lie, but...** Phill Shade
6:00-8:00	**Sponsor Technology Showcase Reception, Treasure Hunt & Dinner** **Function Hall 3**

SharkFest'23 ASIA Conference Agenda

Wednesday, April 19 - Auditorium 302	
9:15-10:30	**05** **TCP Performance and battling the bloat** Leigh Finch
10:30-10:45	**BREAK – Function Hall 3**
10:45-12:00	**06** **Abusing the Network – An Overview of Malicious Network Activity and How to Detect It** Phill Shade
12:00-1:00	**LUNCH – Function Hall 3**
1:00-2:15	**07** **LOG4SHELL: Getting to know your adversaries** Sake Blok
2:15-2:30	**BREAK - – Function Hall 3**
2:30-3:45	**08** **Zero Trust Framework to defend against latest Security Trends and Lessons Learned from Cyberwar** Mandana Javaheri
3:45-4:00	**BREAK**
4:00-5:15	**09** **The Interface Alphabet Soup. 10Mbit to 400Gbit, Everything You Wanted to Know About Layer 1 and Capture** Aaron Foo
5:15-6:30	**Closing Reception and Sponsor Technology Showcase** **Function Hall 3**

SharkFest'23 ASIA Conference Agenda

Session Abstracts & Instructor Bios

(DRAFT - UPDATED FREQUENTLY)

Tuesday, April 18

9:30-10:30

KEYNOTE*: Latest Wireshark Developments & Road Map*
Gerald Combs & Friends

BREAK (10:30-10:45)

10:45-12:00

01 Use of Wireshark in LTE and 5G Networks

This session will cover the most used protocols on LTE, and 5G. S1Ap, S1Ng, SCTP, GTPv1, GTPv2, diameter, and http2. Walk through actual setup of an LTE, and 5G data session. Demonstrate the setup and environment I use to get to the root cause quickly.

Instructor: Mark Stout, Principle Enginner, T-Mobile
Design, and Tech Support for Long-Term Evolution (LTE) mobile networks, and 5G for the last 21 years, in multiple countries. Active contributor to 3rd Generation Partnership Project (3GPP) 23, and 29 series. Currently the Principle Support Engineer for T-Mobile's LTE, Voice Over LTE (VoLTE), Internet of Things (IoT),and true 5G technology on the Packet Core network.

BREAK (12:00-12:15)

12:15-1:30

02 Visualize application traffic using Wireshark

Extend your Wireshark expression with the intelligent use of the Graph function. We know Wireshark is good at trace file investigation with 3000 over protocol dissectors, but it is also an excellent tool for visualizing traffic with a series of Graph functions. Megumi shows you TIPS and Tricks to use Wireshark as a graphical chart creation tool. Colourful charts tell you the traffic flow situation quickly, and those who are not users of Wireshark will also be satisfied.

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.

LUNCH (1:30-2:30)

2:30-3:45

03 Visualizing and Decrypting TLS 1.3

In this beginner level talk, you will learn the essentials of TLS encryption. 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. Then we will walk through how to capture session keys, decrypt traffic, and analyze the protocols being carried with TLS. You will leave this talk with a great visual to imagine TLS encryption, as well as everything you need to decrypt and examine TLS encryption in an HTTPs session.

Instructor: Ross Bagurdes, Bagurdes Technology, Network Engineer & Educator
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 University of Wisconsin Hospital and Clinics. Here he

worked with Extreme Networks, HP, Cisco, Tipping Point, among other network technology, as well as honed his Wireshark and protocol analysis skills. Until changing paths very recently, Ross spent 7 years teaching data networking at Madison College, and is currently authoring and producing IT training videos in Wireshark/Protocol Analysis, Cisco, and general networking topics for www.Pluralsight.com. In his free time, you'll find Ross and his dog, traveling, hiking, backpacking, or snowboarding somewhere in the western US.

BREAK (3:45-4:00)

4:00-5:15

04 How did that happen? - Packets may never lie, but...

Packets may never lie, but how do you find the packets telling you the truth? Join us as former Blackhat turned Forensics Investigator Phill Shade as he explores five real-world case studies from his files. He walks through how he approached each case, including what information he was given to base his analysis on. Attendees are required to bring their laptop with Wireshark already installed, and sample pcap files will be distributed to users if they desire.

Instructor: Phill Shade, Owner, Merlion's Keep Consulting

Phill "Sherlock" Shade is a Senior Network / Forensics Investigator and founder of Merlion's Keep Consulting, specializing in all aspects of Network and Forensics Analysis. He is an internationally recognized Network Security and Forensics expert, drawing from his over 30 years of hands-on, real world experience. A member of the Global Cyber Response Team (GCRT), FBI InfraGard, Computer Security Institute, the IEEE and Volunteer at Cyber Warfare Forum Initiative, he is a frequent consultant for numerous international security, technology and government agencies.

6:00-8:00

Sponsor Technology Showcase Reception, Treasure Hunt & Dinner

SharkFest'23 ASIA Conference Agenda

Wednesday, April 19

9:15-10:30

05 TCP Performance and battling the bloat

Not all TCP stacks are created equal and understanding how the different moving parts of a system work together is vital to ensuring that communications are efficient, fair, and (or) prioritised. In this talk Leigh will take you through the variables that impact performance and efficiency of communications, and how to avoid common pitfalls such as buffer bloat using Wireshark to visualise and measure performance.

Leigh Finch is a daily user of Wireshark and will take you through:

* How to tell the difference between an application problem and a transport network problem.
* How to configure router and QoS buffers.
* Predict performance of applications over different latencies.
* Determine the optimal TCP settings for different use cases.
* Identify the metrics matter when analysing performance problems.

Instructor: Leigh Finch, Distinguished Consultant and Senior Manager, Riverbed Professional Services
Leigh Finch is the distinguished consultant and Senior Manager for Riverbed Professional Services. He manages a team of consultants in the Asia Pacific Region, servicing clients in Australia, New Zealand and China as well as ASEAN.

With over 20 years of experience in the industry, Leigh has worked with a variety of customers in both the private and public sector, helping them deliver focused and strategic solutions that improve digital performance. Leigh's passion comes from a genuine commitment to his clients, ensuring that every challenge is met with innovative thinking and a drive to outperform targets.

Leigh is a sought-after commentator on digital performance management and regularly presents at industry forums and webinars. Most recently Leigh presented at MilCIS 2022 on optimising satellite communications and threat hunting at Security Xchange Singapore.

BREAK (10:30-10:45)

10:45-12:00

06 Abusing the Network – An Overview of Malicious Network Activity and How to Detect It

Pcap files are now routinely gathered during legal and network investigations. This presentation assists the cyber-investigator in developing a solid cyber-investigation profile for use with open-source tools such as Wireshark. It includes detailed configuration information, basic settings, forensics color rules, and filters. Selected hands-on exercises are available for practice, and the instructor will provide a sample Forensics Profile to get you started. Attendees are required to bring their laptop with Wireshark already installed, and sample pcap files will be distributed to users if they desire.

Instructor: Phill Shade, Owner, Merlion's Keep Consulting
Phill "Sherlock" Shade is a Senior Network / Forensics Investigator and founder of Merlion's Keep Consulting, specializing in all aspects of Network and Forensics Analysis. He is an internationally recognized Network Security and Forensics expert, drawing from his over 30 years of hands-on, real world experience. A member of the Global Cyber Response Team (GCRT), FBI InfraGard, Computer Security Institute, the IEEE and Volunteer at Cyber Warfare Forum Initiative, he is a frequent consultant for numerous international security, technology and government agencies.

LUNCH (12:00-1:00)

1:00-2:15

07 LOG4SHELL: Getting to know your adversaries

What does a LOG4SHELL attack look like on the network and how to analyze the LOG4SHELL attack (including some of its deployed exploits) with Wireshark.

In December 2021, the IT world was shaken up by a CVE with score 10. A vulnerability in the widely used log4j logging library allowed an attacker to run arbitrary code on the system by making it log a specific string. As a lot of elements in the logging comes from user controlled data, the exploit was very easy use.In order to understand the attack and it's impact, I reproduced an attack in my LAB. And after that, I set up a honeypot to collect attack samples. I went one step further and set up an isolated system and deliberately infected it with some of the exploits to see what it would do. In this talk I will walk through the process of (safely) setting up the LAB systems, the honeypot and the infected victim. The captured traffic will be analyzed with Wireshark and some hints and tips on how to use Wireshark in a security context will be given.

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.

BREAK (2:15-2:30)

2:30-3:45

08 Zero Trust Framework to defend against latest Security Trends and Lessons Learned from Cyberwar

In this session, you will learn about the latest Cybersecurity trends as well as Microsoft's lesson learned from the Cyberwar between Ukraine and Russia and how to leverage the Zero Trust Framework to minimize and mitigate the cybersecurity risks.

Instructor: Mandana Javaheri, Head of Security Solutions, Microsoft Asia

With more than 20 years of experience in cybersecurity and networking industries, Mandana Javaheri is Microsoft Asia's Head of Security Solutions. She leads a team of security specialists and trusted advisors that help customers define their security strategy and secure their business operations by modernizing their security infrastructure.

Prior to this role, Javaheri led the Microsoft Security, Compliance, and Identity Partner Development team globally. She also brings experience from previous roles including CTO and Head of Technology Alliances at Savvius, a network forensics company, where she defined product and technology directions as well as led strategic partnerships, product management and development.

4:00-5:15

09 The Interface Alphabet Soup. 10Mbit to 400Gbit, Everything You Wanted to Know About Layer 1 and Capture

We go through the physical layer both logically, form factor and whats practical for the interface alphabet soup. Discussing RJ45, SFP, SFP28, SFP56, QSFP, QSFP28, QSFP56, QSFP-DD, FEC, PAM4, SX, LX, SR, LR, SR4, LR4, CWDM4, BIDI, DAC, Active/Passive AOE, SC, LC, MPO12, MPO24. Including how to capture each protocol.

Instructor: Aaron Foo, FMADIO

FPGA Engineer, Software Engineer & Entrepreneur, Aaron Foo leads FMADIO, a company with a packet capture appliance which does so much more than just recording data. In a previous life Aaron worked on FPGA pre-trade risk solutions. In a previous, previous life he was a key engineer for the Playstation console. In a previous, previous, previous life he squeezed the maximum performance from GPUs when they first arrived in the form of Nvidia RIVA128 (1997). He also collects cacti.

5:15-6:30

Closing Reception & Sponsor Technology Showcase