SharkFest'18 ASIA
April 9th - 11th, 2018

Nanyang Executive Center
Nanyang Technological University
Singapore

- Pre-Conference Troubleshooting Class Schedule
- SharkFest'18 ASIA Session & Events Agenda
- Session Abstracts & Requirements
- Instructor Bios

SharkFest'18 ASIA Conference Agenda

Session Level Legend: Beginner = Intermediate = Advanced/Developer =

Pre-Conference Troubleshooting Course and SharkFest'18 ASIA Opening Schedule

WIRESHARK UNIVERSITY
Pre-Conference Course

Troubleshooting with Wireshark
(Laura Chappell)

Monday	9 April 2018
7:30 - 9:00 am	Check-in and Badge Pick up
7:30 am	Breakfast
9:00 am	Laptop Setup and Class begins (with morning break)
12:00 pm	Lunch Break
1:00 pm	Class Resumes (with afternoon break)
5:00 pm	Class day ends **Attending SharkFest? See Monday Evening Schedule below.**

SharkFest'18 ASIA

Opening Schedule

Monday	9 April 2017
12:00-8:30 pm	**Check-In & Badge Pick-Up for SharkFest'18 ASIA**
1:00-5:00 pm	**Developer Drop-In Workshop** **SharkFest'18 ASIA Attendees Only**
6:00-8:00 pm	**Welcome Dinner & Sponsor Showcase Reception** **SharkFest'18 ASIA Attendees Only**

SharkFest'18 ASIA Conference Agenda

Session Level Legend: Beginner = Intermediate = Advanced/Developer =

Tuesday	10 April 2017	
7:30-8:30 am	**Breakfast**	
7:30am-12:00 pm	**SharkFest Check-in**	
8:30-9:30 am	***Keynote: "Wireshark: Past, Present & Future" - Gerald Combs & Friends*** **Auditorium**	
	Lecture Room 1	**Lecture Room 2**
9:30-9:45 am	Break	
9:45-11:00 am	**01** **In the Packet Trenches (Part 1)** Hansang Bae	**02** **Writing a Wireshark Dissector: 3 Ways to Eat Bytes** Graham Bloice
11:00-11:15 am	Break	
11:15 am-12:30 pm	**03** **In the Packet Trenches (Part 2)** Hansang Bae	**04** **Wireshark Saves the Day! A Beginner's Guide to Packet Analysis** Maher Adib
12:30-1:30 pm	LUNCH	
1:30-2:45 pm	**05** **Sneaking in by the Back Door: Hacking the non-standard layers with Wireshark (Part 1)** Phill Shade	**06** **Developer Bytes Lightning Talks** Wireshark Core Developers
2:45-3:00 pm	Break	
3:00-4:15 pm	**07** **Sneaking in by the Back Door: Hacking the non-standard layers with Wireshark (Part 2)** Phill Shade	**08** **TCP SACK Overview and Impact on Performance** John Pittle
4:15-4:30 pm	Break	
4:30-5:45 pm	**09** **Using Wireshark to Solve Real Problems for Real People: Step-by-Step Case Studies in Packet Analysis** Kary Rogers	**10** **Augmenting Packet Capture with Contextual Meta-Data: the what, why and how** Dr. Stephen Donnelly
6:00-8:00 pm	***Sponsor Technology Showcase Reception, Treasure Hunt & Dinner*** **Atrium**	

Pick up your Packet Challenge Sheet at the WIRESHARKUNIVERSITY table in the Atrium

SharkFest'18 ASIA Conference Agenda

Session Level Legend: Beginner = Intermediate = Advanced/Developer =

Wednesday	11 April 2018		
7:30 - 8:30 am	**Breakfast**		
	Lecture Room 1	**Lecture Room 2**	
8:45 - 10:00 am	11 **Wireshark CLI Tools and Scripting** Sake Blok	12 **Filter Maniacs: Tips & Techniques for Wireshark display & winpcap/libpcap capture filters** Megumi Takeshita	**Visit the Vendor Showcase in the ATRIUM**
10:00 – 10:15 am	Break		
10:15 - 11:30 am	13 **Designing a Packet Capture Strategy…and how it fits into an overall performance visibility strategy** John Pittle	14 **SSL/TLS Decryption: Uncovering Secrets** Peter Wu	
11:30 – 11:45 am	Break		
11:45 am – 1:00 pm	15 **LTE Explained... The Other Protocols** Mark Stout	16 **extcap – Packet Capture beyond libpcap/winpcap: Bluetooth Sniffing, Android Dumping & other Fun Stuff!** Roland Knall	
1:00 – 2:00 pm	LUNCH		
2:00 – 3:15 pm	17 **The Packet Doctors are In!** Drs. Bae, Blok and Chappell	18 **Understanding Throughput & TCP Windows: factors that can limit TCP throughput performance** Kary Rogers	
3:15 – 3:30 pm	Break		
3:30 – 5:15 pm	19 **SSL/TLS Decryption: Uncovering Secrets** Peter Wu	20 **How Did They Do That? Network Forensic Case Studies** Phill Shade	
5:30 – 6:00 pm	***Packet Challenge Awards, Closing Comments***		
6:00–8:00 pm	***Packet Palooza Group Packet Competition Dinner & Sponsor Showcase*** **Atrium**		

SharkFest'18 ASIA Bios & Abstracts

Session Level Legend: Beginner = Intermediate = Advanced/Developer =

TUESDAY, 10 APRIL

8:30–9:30 am	**Keynote** ***"The Past, Present & Future of Wireshark"*** **Gerald Combs & Friends**
9:45 - 11:00 am	
Lecture Room 1	**01 In the Packet Trenches (Part 1)** In an increasingly prevalent cloud and Saas-based networking world, foundational troubleshooting practices are destined to change. In this 2-part session, Hansang will review on and off-prem cloud and SaaS troubleshooting scenarios when trying to identify root cause. He'll also discuss what it will be like as you adopt the cloud, how to capture in AWS, and how different cloud vendors may or may not have TCP/IP Offload Engines to address latency issues when uploading. He'll also show how one-sided traces to a SaaS vendor can be diagnosed. **Instructor: Hansang Bae, CTO, Riverbed Technology** Hansang Bae led the Network/Application Performance Engineering Team with direct responsibility for Packet Capture Infrastructure at Citi until July, 2012 when he joined Riverbed Technology as Director of Cascade Product Architecture. He has since taken on the role of Chief Scientist and then CTO for the company. With his broad knowledge of protocol analysis in a complex enterprise infrastructure, Hansang brings a unique perspective to packet analysis.
Lecture Room 2	**02 Writing a Wireshark Dissector: 3 Ways to Eat Bytes** The presentation outlines the 3 most popular methods to write a dissector, using plain text files with WSGD, using a Lua script file and finally a C dissector. An introduction to how dissectors fit into the Wireshark system is given, then each method is compared for ease of initial development, facilities offered and run-time performance. **Instructor: Graham Bloice, Software Developer, Trihedral UK Ltd. & Wireshark Core Developer** Graham is a Software Developer with Trihedral UK Limited where he helps produce their VTScada HMI\Scada toolkit. Graham is also a Wireshark core developer, mainly concentrating on the Windows build machinery and DNP3 dissectors. He uses Wireshark frequently in his day job when analysing telemetry protocols used in the SCADA world, and inter-machine traffic for the company's distributed SCADA product.
11:15 am – 12:30 pm	
Lecture Room 1	**03 In the Packet Trenches (Part 2)** In an increasingly prevalent cloud and Saas-based networking world, foundational troubleshooting practices are destined to change. In this 2-part session, Hansang will review on and off-prem cloud and SaaS troubleshooting scenarios when trying to identify root cause. He'll also discuss what it will be like as you adopt the cloud, how to capture in AWS, and how different cloud vendors may or may not have TCP/IP Offload Engines to address latency issues when uploading. He'll also show how one-sided traces to a SaaS vendor can be diagnosed. **Instructor: Hansang Bae, CTO, Riverbed Technology** Hansang Bae led the Network/Application Performance Engineering Team with direct responsibility for Packet Capture Infrastructure at Citi until July, 2012 when he joined Riverbed Technology as Director of Cascade Product Architecture. He has since taken on the role of Chief Scientist and then CTO for the company. With his broad knowledge of protocol analysis in a complex enterprise infrastructure, Hansang brings a unique perspective to packet analysis.
Lecture Room 2	**04 Wireshark Saves the Day! A Beginner's Guide to Packet Analysis (Hands-On Lab)** The presenter will share his experience and the techniques he's developed over the years of doing packet analysis with Wireshark so that when your network or application is not performing as expected, you'll feel confident in firing up Wireshark and looking for an answer! This Hands-On Lab will guide the Wireshark beginner through the Wireshark UI and explore basic features and functionality like the navigation button, capture filters, display filters, column configuration, and how to create a shortcut button to make your packet analysis exercises easy. You'll learn to identify the correct fields in packet contents and look for clues to quickly and accurately diagnose networking issues. **Instructor: Maher Adib, Principal Consultant, Ofisgate Sdn Bhd** Maher's first exposure to packet analysis was in 2000 when he downloaded Ethereal (now known as Wireshark) and was instantly fascinated. His love for the open source analyzer has led to a near-daily commitment to using the tool to

	discover what is really going on with network infrastructures. As Technical Lead for Ofisgate Sdn Bhd in Kuala Lumpur, he has architected Cyber Range, a realistic training platform for red and blue teaming scenarios mimicking real-world scenarios using Wireshark packet analysis capabilities as one of the primary weapons. Maher is an active member of, and frequent presenter at, local and international IT-related community events such as Durian Conference, Malaysia Open Source Community meetings and, of course, SharkFest!
1:30 – 2:45 pm	
Lecture Room 1	**05 Sneaking in the Back Door: Hacking the non-standard layers with Wireshark (BYOD) – Part 1** Security teams and investigators routinely examine OSI Layers 4-7 (TCP/Applications) for clues when investigating potentially-illegal/hacking intrusions. Few ever think to look lower in the stack for either defense or investigation. Using Wireshark and other open-source tools, we'll examine some favorite tricks for penetrating networks using detailed, and sometimes forgotten, knowledge of OSI layers 2 and 3. **ATTENDEES WILL NEED TO BRING THEIR OWN LAPTOPS WITH WIRESHARK INSTALLED. SAMPLE PCAP FILES WILL BE DISTRIBUTED.** **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.
Lecture Room 2	**06 Developer Bytes Lighting Talks** Developer Bytes Lightning Talks focus on small, interesting topics regarding Wireshark, its development, and use cases. We will present a look behind the curtains, highlight features often overlooked, or present upcoming topics for future versions of Wireshark. This session focuses on a range of Wireshark topics, such as: - Wireshark Git and CMake navigation - From protocol to dissector in 15 minutes - Making a company-internal build - Packet generation, prepare dummy data **Instructors: Wireshark Core Developers**
3:00 – 4:15 pm	
Lecture Room 1	**07 Sneaking in the Back Door: Hacking the non-standard layers with Wireshark (BYOD) – Part 2** Security teams and investigators routinely examine OSI Layers 4-7 (TCP/Applications) for clues when investigating potentially-illegal/hacking intrusions. Few ever think to look lower in the stack for either defense or investigation. Using Wireshark and other open-source tools, we'll examine some favorite tricks for penetrating networks using detailed, and sometimes forgotten, knowledge of OSI layers 2 and 3. **ATTENDEES WILL NEED TO BRING THEIR OWN LAPTOPS WITH WIRESHARK INSTALLED. SAMPLE PCAP FILES WILL BE DISTRIBUTED.** **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.
Lecture Room 2	**08 TCP SACK Overview and Impact on Performance** TCP SACK is an important performance enhancement to TCP. Learn the details of how to interpret the SACK field and relate to performance of the application. **Instructor: John Pittle, Distinguished Performance Consultant, Riverbed Technology, Inc.** Actively focused on Performance Engineering 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, Transaction Analyzer, IT Guru, Sniffer, HP Network Advisor, and the list goes on. Sr. Performance Consultant with OPNET Technologies since 2005, then came to Riverbed with the OPNET acquisition in 2012. Working as the America's Distinguished Performance Consultant since 2015 reflecting expertise in the entire

	portfolio of Riverbed visibility and performance analysis products, as well as technical leadership within the consulting practice for complex performance related customer engagements.
4:30 - 5:45 pm	
Lecture Room 1	**09 Using Wireshark to Solve Real Problems for Real People: Step-by-Step Real-World Case Studies in Packet Analysis** Stop banging your head on your desk trying to find root cause and solve performance problems. The answers are in the packets and this lively, animated session will show you step-by-step in Wireshark how to solve real world case studies that have stumped others. Be the hero! **Instructor: Kary Rogers, Director, Staff Engineering, Riverbed Technology** Kary first learned the value of packet analysis helping customers solve difficult issues in Riverbed TAC, and has since moved onto a management role for the company. Not wanting to lose the skills he fought hard to learn, he started a packet analysis website, PacketBomb.com, where he posts tutorials and case studies for the hapless network engineer struggling to prove that it's not the network.
Lecture Room 2	**10 Augmenting Packet Capture with Contextual Meta-Data: the what, why & how** Full packet capture and archiving are increasingly important, providing "ground truth" evidence for investigating security incidents and performance issues. But captured packets by themselves lack context, such as where they were captured and the environment at the time of capture. Augmenting packet data with meta-data can provide uselful context about when, where, and how packets were captured and the environment at the time of capture. This presentation will discuss what types of meta-data can be useful, what they can be useful for, and how meta-data can be encoded into packet capture to ensure permanent context to packets captured. **Instructor: Dr. 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.

SharkFest'18 ASIA Bios & Abstracts

Session Level Legend: Beginner = Intermediate = Advanced/Developer =

WEDNESDAY, 11 APRIL

8:45 - 10:00 am

Lecture Room 1

11 Wireshark CLI Tools and Scripting

While working in a GUI environment is great, there are advantages to working in a Command Line Interface (CLI). In this session, you'll get become familiar with some of the Wireshark CLI tools (tshark, editcap, mergecap and capinfos). The basic usage of the tools will be discussed first before diving into more advanced usage when integrating with other commands to create new ways of processing pcap(ng) files.

Sake Blok, Relational Therapist for Computer Systems, SYN-bit.nl

Sake has been analyzing packets since the end of the last century. In the course of his work, he discovered many bugs in devices and presented his findings to the vendors to fix the issues. He also discovered configuration issues that led to functional problems or performance issues in applications running over the network. These issues were resolved based on reports Sake presented to his customers. In 2009, Sake started the company SYN-bit to provide network analysis services to enterprises across Europe. As part of his work to service his customers, Sake started developing extra functionality for Wireshark that he missed in his day-to-day job. He also enhanced multiple protocol dissectors to suit his analysis needs. In 2007, he was asked by Gerald to join the Wireshark Core Development team.

Lecture Room 2

12 Filter Maniacs: Tips & Tricks for Wireshark Display & winpcap/libpcap Capture Filters

Wireshark has strong functions to filter packets by Display Filters and winpcap/libpcap Capture Filters. With these filters, you can choose packets of interest and reduce the size of trace files. In this session, Megumi will show you practical tips and convenient techniques for using both types of filters. You may also find another magical way to filter packets.

Instructor: Megumi Takeshita, Packet Otaku and Founder, Ikeriri Network Service, Tokyo

Megumi Takeshita, Packet Otaku (Twitter:@ikeriri), runs a packet analysis company, Ikeriri Network Service, in Japan. Ikeriri provides packet analysis services for troubleshooting, debugging, and network security inspections and is also a reseller of products and services from Rivered Technology, MetaGeek, Profitap, Dualcomm, and other related technology vendors. Megumi has authored more than 10 books on Wireshark and packet analysis in Japanese and is an avid contributor to the Wireshark project.

10:15 am – 11:45 pm

Lecture Room 1

13 Designing a Requirements-based Packet Capture Strategy…and how it fits into an overall performance visibility strategy

Learn how to create a requirements-based packet capture strategy for your organization. Understand how packets are a cornerstone to your performance management capabilities and how to create a roadmap that you can use to communicate priorities and performance management capabilities that bring value to the business.

Instructor: John Pittle, Distinguished Performance Consultant, Riverbed Technology, Inc.

Actively focused on Performance Engineering 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, Transaction Analyzer, IT Guru, Sniffer, HP Network Advisor, and the list goes on. Sr. Performance Consultant with OPNET Technologies since 2005, then came to Riverbed with the OPNET acquisition in 2012. Working as the America's Distinguished Performance Consultant since 2015 reflecting expertise in the entire portfolio of Riverbed visibility and performance analysis products, as well as technical leadership within the consulting practice for complex performance related customer engagements.

Lecture Room 2

14 SSL/TLS Decryption: uncovering secrets

Troubleshooting and debugging applications or reverse engineering protocols that use SSL/TLS can be a pain since the data is encrypted. Decryption of such data is possible in Wireshark if you have access to the appropriate secrets. This session will show you how to obtain the required secret information and give a background on the relevant TLS handshake details. You will understand why possession of the server RSA key file is not always sufficient and what alternatives are available. Once decrypted data is available, you will finally be able to make use of several Wireshark and Tshark features to help you with analysis.

Instructor: Peter Wu, Wireshark Core Developer

Peter Wu is a Masters student in Information Security at the Eindhoven University of Technology, and contributor to many open source projects. His contribution to Wireshark started in 2013 with SSL decryption improvements in order to

	assist in analyzing encrypted application traffic. Peter added TLS 1.3 decryption support to Wireshark and at Cloudflare, he has worked on an actual TLS 1.3 implementation.
11:45 - 1:00 pm	
Lecture Room 1	**15 LTE Explained... The Other Protocols** This session will walk attendees through multiple LTE flows and failures to demonstrate how Wireshark can assist with S1AP, GTP, and Diameter issues. **Instructor: Mark Stout, Tech Support Engineer, Sprint** Mark has worked in the enterprise wireless space for over 19 years and has turned up Code Division Multiple Access (CDMA) and Long-Term Evolution (LTE) high-speed wireless networks around the world. He is currently the Lead Support Engineer for Sprint's LTE technology on the Evolved Packet Core (EPC) network, which is a framework for providing converged voice and data on a 4G LTE network.
Lecture Room 2	**16 extcap – Packet Capture beyond libpcap/winpcap: Bluetooth Sniffing, Android Dumping & other Fun Stuff!** This presentation focuses on extcap, the external capture interface for Wireshark, and its application in modern-day scenarios. The capabilities of extcap and how to write its own utility with Python and C-code will be demonstrated. Bluetooth sniffing functions, dumping of log files from an Android phone, and some new debugging techniques for dissector development will also be covered. **Instructor: Roland Knall, Wireshark Core Developer** Roland is a Software System Architect for machine safety protocols at B&R Industrial Automation, a division of ABB. He started developing software over 20 years ago and has experienced nearly all facets of the software development process. For the last 10 years, his focus has been on industrial machine applications mainly on systems in the area of industrial Ethernet. Roland has been a Wireshark Core Developer since 2016, contributing to the integration of external capture devices as well as UI improvements.
2:00 – 3:15 pm	
Lecture Room 1	**17 The Packet Doctors are In! Packet Trace Diagnoses by the Experts** The experts on this panel have been asked to review trace files and help find a reason for certain behaviors by attendees at many SharkFests. Based on these experiences, they've created this session to surgically examine trace files with a broader audience for a collective learning experience. Trace files will be gathered from attendees during the session so that the "not-knowing what to expect and whether it can be solved" thrill of working with an unknown trace can be preserved. Come to this session and learn to ask the right questions and look at packets from new and varied perspectives! **PLEASE BRING PERPLEXING TRACE FILES FOR ANALYSIS BY THE PANEL** **Surgical Staff: Hansang Bae, Sake Blok, Laura Chappell**
Lecture Room 2	**18 Understanding Throughput and TCP Windows: A walk-through of the factors that can limit TCP throughput performance** Receive windows, congestion windows, and send buffers, oh my! In this session, Kary will demonstrate examples of the different factors on the sender and receiver end that can limit TCP throughput performance. **Instructor: Kary Rogers, Director, Staff Engineering, Riverbed Technology** Kary first learned the value of packet analysis helping customers solve difficult issues in Riverbed TAC, and has since moved onto a management role for the company. Not wanting to lose the skills he fought hard to learn, he started a packet analysis website, PacketBomb.com, where he posts tutorials and case studies for the hapless network engineer struggling to prove that it's not the network.
3:30 – 5:15 pm	
Lecture Room 1	**19 SSL/TLS Decryption: uncovering secrets** Troubleshooting and debugging applications or reverse engineering protocols that use SSL/TLS can be a pain since the data is encrypted. Decryption of such data is possible in Wireshark if you have access to the appropriate secrets. This session will show you how to obtain the required secret information and give a background on the relevant TLS handshake details. You will understand why possession of the server RSA key file is not always sufficient and what alternatives are available. Once decrypted data is available, you will finally be able to make use of several Wireshark and Tshark features to help you with analysis. **Instructor: Peter Wu, Wireshark Core Developer** Peter Wu is a Masters student in Information Security at the Eindhoven University of Technology, and contributor to many open source projects. His contribution to Wireshark started in 2013 with SSL decryption improvements in order to assist in analyzing

	encrypted application traffic. Peter added TLS 1.3 decryption support to Wireshark and at Cloudflare, he has worked on an actual TLS 1.3 implementation.
Lecture Room 2	**20 How Did They Do That? Network Forensic Case Studies** The ringing of the telephone heralds the news that every network security professional dreads: "I think the network has been hacked". Suddenly, you're faced with answering questions you hoped never to encounter, such as: 1. Who was the intruder? 2. How did the intruder penetrate your security precautions? 3. What damage has been done? Did the intruder leave anything such as a new user account, a Trojan horse or perhaps some new type of Worm of Bot software behind? 4. Did you capture sufficient data to analyze and reproduce the attack and verify that the fix will work? This session will demonstrate how to use Wireshark to find answers and prepare you for the eventuality of being hacked. **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.