SharkFest'19 US Agenda

UC Berkeley, Clark Kerr Campus

June 8th-13th, 2019

- Pre-Conference Classes
- SharkFest'19 US Session & Events Agenda
- Session Abstracts & Requirements
- Instructor Bios

SharkFest'19 US Conference Agenda

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

Pre-Conference Courses

Pre-Conference Class I **Wireshark Analysis Foundations** **INSTRUCTORS** **Chris Greer** **Jasper Bongertz** **Christian Landström** **Sake Blok** **(Krutch Auditorium)**	**Saturday**	**8 June 2019**
	8:00-9:00am	Check-in & Badge Pick up
	8:00-9:00am	Breakfast (Great Hall Dining Room)
	9:00am-12:00pm	Class in session (with morning breaks)
	12:00-1:00pm	LUNCH (Great Hall Dining Room)
	1:00-5:00pm	Class in session (with afternoon breaks)
	Sunday	**9 June 2019**
	8:00-9:00am	Breakfast (Great Hall Dining Room)
	9:00am-12:00pm	Class in session (with morning breaks)
	12:00-1:00pm	LUNCH (Great Hall Dining Room)
	1:00-5:00pm	Class in session (with afternoon breaks)
	Monday	**10 June 2019**
	8:00-9:00am	Breakfast (Great Hall Dining Room)
	9:00am-12:00pm	Class in session (with morning breaks)
	12:00-1:00pm	LUNCH (Great Hall Dining Room)
	1:00-5:00pm	Class in session (with afternoon breaks)
Pre-Conference Class II **Hunt Like a Shark** **INSTRUCTORS** **Brad Palm** **Ryan Richter** **Brian Greunke** **(Garden Room & Krutch Room 102)**	**Saturday**	**8 June 2019**
	8:00-9:00am	Check-in & Badge Pick up
	8:00-9:00am	Breakfast (Great Hall Dining Room)
	9:00am-12:00pm	Class in session (with morning breaks)
	12:00-1:00pm	LUNCH (Great Hall Dining Room)
	1:00-5:00pm	Class in session (with afternoon breaks)
	Sunday	**9 June 2019**
	8:00-9:00am	Breakfast (Great Hall Dining Room)
	9:00am-12:00pm	Class in session (with morning breaks)
	12:00-1:00pm	LUNCH (Great Hall Dining Room)
	1:00-5:00pm	Class in session (with afternoon breaks)
	Monday	**10 June 2019**
	8:00-9:00am	Breakfast (Great Hall Dining Room)
	9:00am-5:00pm	1:1 Mentoring with Brad Palm & Co. – Krutch Room 102 (with Breaks and LUNCH)

SharkFest'19 US Conference Agenda

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

SharkFest Opening & Welcome Dinner

	Monday	10 June 2019
SharkFest'19 US **Welcome Dinner & Sponsor Showcase** **(Gingko Lawn, Krutch Hallway)**	12:00-8:00pm	**SharkFest'19 US Check-In & Badge Pick-Up** (Registration Table, Krutch Auditorium Lobby)
	9:00-5:00pm	**SharkFest Shoal Mentoring Lab OPEN** (Krutch Room 102)
	1:00-5:00pm	**Developer Den Drop-In** **(**Executive Dining Room**)**
	6:00-8:30pm	***SharkFest'19 US Welcome Dinner & Sponsor Showcase*** **SharkFest'19 US Attendees Only**

SharkFest'19 US Conference Agenda

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

Tuesday 11 June 2019			
7:00-8:00am	**Breakfast – Grand Hall**		
7:00am-12:00pm	**SharkFest Check-in & Badge Pick-up (Krutch Auditorium Lobby)**		
8:00-9:00am	**KEYNOTE: "*Latest Wireshark Developments & Road Map*"** **Gerald Combs & Friends** **(Krutch Auditorium)**		
	KRUTCH AUDITORIUM	**GARDEN ROOM**	**KRUTCH ROOM 104**
9:00-9:15am	Break		
9:15-10:45am	01 **Back to the basics** Hansang Bae	02 **TLS encryption and decryption: What every IT engineer should know about TLS** Ross Bagurdes	03 **Writing a Wireshark Dissector: 3 ways to eat bytes** Graham Bloice
10:45-11:00am	Break		
11:00am-12:30pm	04 **Back to the trenches** Hansang Bae	05 **TLS debugging** Peter Wu	06 **Creating dissectors like a pro by generating dissectors** Richard Sharpe
12:30-1:30pm	**LUNCH**		
1:30-3:00pm	07 **To send or not to send? How TCP congestion control algorithms work** Vladimir Gerasimov	08 **How long is a packet? And does it really matter?** Dr. Stephen Donnelly	09 **When TCP reassembly gets complicated** Tom Peterson
3:00-3:15pm	Break		
3:15-4:45pm	10 **Solving packet capture challenges with only tshark** Sake Blok	11 **Taking a bite out of 100GB trace files** Betty DuBois	12 **Tracing the untraceable with Wireshark: a view under the hood** Roland Knall
4:45-5:00 pm	Break		
5:00-6:00pm	13 **Kismet & wireless security 101** Mike Kershaw	**VISIT the SharkFest Shoal Continuing Education Lab Krutch ROOM 102**	14 **Jumbo frames & how to catch them** Patrick Kinnison
6:00-8:30pm	**Sponsor Technology Showcase Reception, Treasure Hunt & Dinner** **(Krutch Auditorium)**		

SharkFest SHOAL MENTORING & SPONSOR VIRTUAL LABS – Krutch Room 102

SharkFest'19 US Conference Agenda

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

Wednesday	12 June 2019			
7:00-8:00am	**Breakfast – Grand Hall**			
8:00-9:00am	**KEYNOTE: *Mental Models for Using Network Evidence*** **Chris Sanders** **(Krutch Auditorium)**			
	KRUTCH AUDITORIUM	**GARDEN ROOM**	**KRUTCH ROOM 104**	
9:15-10:45am	15 **War Story: Troubleshooting issues on encrypted links** Christian Landström	16 **Wireshark visualization TIPS & tricks** Megumi Takeshita	17 **My TCP ain't your TCP – ain't no TCP?** Simon Lindermann	
10:45–11:00am	Break			
11:00am-12:30pm	18 **Practical tracewrangling: Exploring capture file manipulation/extraction** Jasper Bongertz	19 **TCP SACK overview & impact on performance** John Pittle	20 **Packets in. Packets out. Let's find out!** Maher Adib	
12:30–1:30pm	LUNCH			
1:30–3:00pm	21 **Using Wireshark to solve real problems for real people: step-by-step case studies in packet analysis** Kary Rogers	22 **Analyzing Windows malware traffic with Wireshark (Part 1)** Brad Duncan	23 **Developer bytes lightning talks** Wireshark Core Developers	
3:00-3:15pm	Break			
3:15–4:45pm	24 **The packet doctors are In! Packet trace examinations with the experts** Drs. Bae, Blok, Bongertz, Landström & Rogers	25 **Analyzing Windows malware traffic with Wireshark (Part 2)** Brad Duncan	26 **To send or not to send? How TCP congestion control algorithms work** Vladimir Gerasimov	
4:45 – 5:00pm	Break			
5:00– 6:00pm	27 **TBD**	**VISIT the SharkFest Shoal Continuing Education Lab in ROOM 102**	28 **TLS encryption & decryption: What every IT engineer should know about TLS** Ross Bagurdes	
6:00–8:30pm	**Lawrence Hall of Science Reception, Dinner & Group Competition**			

SharkFest

DIVE IN WITH GERALD COMBS & CORE DEVELOPERS AT THE DEVELOPER DEN!

SHOAL MENTORING & SPONSOR VIRTUAL LABS OPEN – Krutch Room 102

SharkFest'19 US Conference Agenda

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

Thursday	13 June 2019			
7:00-8:00am	**Breakfast – Grand Hall**			
8:00-9:00am	***SharkBytes*** **(Krutch Auditorium)**			
	KRUTCH AUDITORIUM	**GARDEN ROOM**	**KRUTCH ROOM 104**	
9:15-10:45am	29 **Automating cloud infrastructure for analysis of large network captures** Brad Palm & Brian Greunke	30 **Capture file format deep dive** Jasper Bongertz	31 **Can you really capture @10Gbps on a laptop?** Richard Sharpe	PACKET CHALLENGE SHEETS DUE BY 8 AM
10:45-11:00am	Break			
11:00am-12:30pm	32 **A deep dive into LDAP: Everything you need to know to debug and troubleshoot LDAP packets** Betty DuBois	33 **TCP split brain: Compare/ contrast TCP effects on client & server with Wireshark (Part 1)** John Pittle	34 **Solving the impossible** Scott Haugdahl & Mike Canney	
12:30–1:30pm	LUNCH			
1:30–3:00pm	35 **Troubleshooting slow networks** Chris Greer	36 **TCP split brain: Compare/ contrast TCP effects on client & server with Wireshark (Part 2)** John Pittle	37 **When TCP reassembly gets complicated** Tom Peterson	
3:00-3:15pm	Break			
3:15-4:45pm	38 **Using Wireshark to solve real problems for real people: step-by-step case studies in packet analysis** Kary Rogers	39 **TBD**	40 **Enrich your network visibility & analysis with Wireshark & ELK** Tajul Azhar Mohd Ariffin	
5:00-5:30pm	**Closing Remarks & Packet Challenge Awards** **(Krutch Auditorium)**			
5:30-7:30pm	**Farewell Reception** **(Gingko Lawn)**			

SharkFest'19 US Conference Agenda

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

TUESDAY, 11 JUNE

8:00-9:00am	**KEYNOTE: *"Latest Wireshark Developments & Road Map"*** **Gerald Combs & Friends** **(Krutch Auditorium)**
9:15-10:45am	
Krutch Auditorium	**01 Back to the basics** When using Wireshark for the first time, it can be an overwhelming and bewildering experience. In this session, we'll take a step back and understand TCP/IP from a troubleshooter's perspective. What does it mean to have retransmissions? Is there a problem? Is it important? What steps should I take to try and narrow down the issue: Are there any helpful guides?" If you've ever opened a trace file and said 'Now what the hell do I do?', this session is for you. **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 CTO for the company. With his broad knowledge of protocol analysis in a complex enterprise infrastructure, Hansang brings a unique perspective to packet analysis.
Garden Room	**02 TLS encryption and decryption: What every IT engineer should know about TLS** Any reputable website or application will encrypt data communication over networks. This is great step forward in providing quality network security, however, it can leave engineers in the dark when it comes to troubleshooting applications using Wireshark. Learn how SSL/TLS works to encrypt traffic in this easy to understand breakdown of the protocol. Ross will use Wireshark to describe the details of SSL/TLS operation, observing each step of the handshake and how it leads to the bulk encryption of data. Intended for an engineer who understands the basics of encryption but would like to learn more about: -TLS 1.2 and 1.3 handshakes -Key Exchange operation -Capturing and using session keys to decrypt captures. You'll leave this session with a visual understanding of TLS operation and be able to easily decrypt your captures, in order to troubleshoot the application data contained within. **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.
Krutch Room 104	**03 Writing a Wireshark dissector: 3 ways to eat bytes** The presentation outlines the 3 most popular methods for writing 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.

SharkFest'19 US Conference Agenda

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

11:00am-12:30pm	
Krutch Auditorium	**04 Back to the trenches** In the session, Hansang provides real-world troubleshooting examples and interacts with attendees in addressing various TCP analysis scenarios. **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.
Garden Room	**05 TLS debugging** **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 has worked on an actual TLS 1.3 implementation at Cloudflare.
Krutch Room 104	**06 Using more of the features of Wireshark to write better dissectors** There are many features in Wireshark for dissector writers that many people do not seem aware of. Some are new, but most have been there for a long time. This presentation will give people the tools to write better dissectors, including: * Using range strings to convert protocol fields into string * Using custom dissectors to handle complicated protocol fields * Using dissector tables * Easily adding units * Handling bit fields * Expert infos It will also make reference to real dissectors to illustrate the concepts involved. **Instructor: Richard Sharpe, Founding Software Engineer, Hammerspace** Richard Sharpe is a software engineer who works on NFS and SMB and is a contributor to Wireshark and Samba. He has worked on a number of Wireshark dissectors and currently works on the Wi-Fi dissector suite a lot.
1:30-3:00pm	
Krutch Auditorium	**07 To send or not to send? how TCP congestion control algorithms work** This session is fully dedicated to the topic of TCP congestion control and will explain: - Why TCP congestion control is necessary - The history of its development - What the fixed terms: "cliff", "congestion collapse", "global synchronization" mean - Why this problem is so difficult to solve even now - Current approaches to handle TCP congestion We will compare different TCP congestion control algorithms (using sample trace files and Wireshark) with an emphasis on the most recent ones (CUBIC, CDG, BBR) and learn what main ideas are implemented in different kinds of TCP congestion control. We'll also take a look at some tricks like "Hybrid slow start" as a part of CUBIC algorithm, and several ways to trick the sender's behavior. **Instructor: Vladimir Gerasimov, Network Engineer, Packettrain.NET** Vladimir Gerasimov currently works as a Network Engineer for Unitop LTD - a company building networks and IP video surveillance systems for customers. He has been working in IT for more than 12 years, and 7 years ago he has shifted to Network Protocol Analysis with the main focus on TCP and Application performance analysis. Vladimir runs personal blog and he is also a creator and administrator of the largest Russian-speaking group regarding Network Protocol Analysis.
Garden Room	**08 How long is a packet? And does it really matter?** This will be an introductory level talk about Ethernet and IP networking focusing on packet length, bandwidth, and debugging issues. Can you trust Wireshark and your packet capture system? We consider what factors can affect

	reported packet length. How do we define, measure, and report bandwidth. What is the Bandwidth Delay Product, and do you still need to tune systems for it. What are some of the networking problems that can be caused by packet length issues, and how can you spot them. **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.
Krutch Room 104	**09 When TCP reassembly gets complicated** Armed with a pcap file, we can examine and analyze the packets that were sent and how they were responded to on the network. We rely on our tools to show us how a TCP stream was reassembled or to give us a list of HTTP websites accessed in a pcap file. But what happens when TCP segments overlap or when new options like TCP Fast Open are used? Does every device and tool reassemble TCP exactly the same in all cases? Are the latest TCP options supported by all of the tools we use? Could this be used to disguise malicious behavior? In this session, we'll look at how TCP packets are processed by operating systems, including Linux and Windows, and compare this to tools such as Wireshark and Suricata. When these don't match, we'll look at the packets themselves and go over ways to test how the packets are really being processed. If you know how TCP reassembly works when packets are received simply out of order you might be surprised to see what happens when we look at packet scenarios during this session! **Instructor: Tom Peterson, Developer, CloudShark** Tom works at CloudShark helping bring pcap analysis to the web. Getting started with networking in 2005 performing testing at the InterOperability Lab at UNH, he began by learning IPv6 and moved from there testing IPsec, firewalls, and other network security devices. Testing a variety of protocols and devices has led to a passion of looking for strange behavior in a pcap file and getting to the bottom of it.
3:15-4:45pm	
Krutch Auditorium	**10 Solving (SharkFest) packet capture challenges with tshark alone: Get exact answers from trace files in an automated way** Manual analysis of trace files with Wireshark is very valuable. But what if you need to extract information from trace files on a regular basis? How do you get the information out of a trace file with tshark so that it can be repeated in an automated way? In this session, Sake will show you how to extract specific data from a trace file, how to post process the data to get statistics, or present it in a better way. He will also spend some time on how to prevent false positives that would corrupt the results. The session will be presented by live-demoing the techniques on packet capture challenges from past Sharkfests. **(So if you would like to solve this years' capture challenge with tshark, make sure you get inspired during this session!)** **Instructor: Sake Blok, Relational Therapist for Computer Systems** Sake has been analysing 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 analyser 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.
Garden Room	**11 Taking a Bite out of a 100G Trace Files: Learn best practices for working with large (tens or hundreds of gigs) data sets** Working with large data sets can be challenging. In this session, we will use Wireshark and tshark to learn many of the ways to still analyze the packets you need from a multi-gig trace file without the smoke coming out of your computer. Bring your laptop to follow along. Traces and a profile will be made available at https://bettydubois.com/sf19us The files will start at 100M and get successively larger, so that you can choose what size you are comfortable working with. **Instructor: Betty DuBois, Chief Detective, Packet Detectives** Betty is the Chief Detective for Packet Detectives, and has been solving mysteries since 1997. She troubleshoots the root cause of network and/or application issues. Experienced with a range of hardware and software solutions, she captures the right data, in the right place, and at the right time. Using packets to solve crimes against the network and applications, is her passion. Teaching others how to do the same, is her calling.

SharkFest'19 US Conference Agenda

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

Krutch Room 104	**12 Tracing the untraceable with Wireshark: a view under the hood** In our day-to-day lives as packet analysts, we often come across issues that invite investigations under the hood that are not easily accessible. This presentation shows some methods for gaining a foothold in illusive situations using Wireshark as a generic sniffing tool (especially when there are no packets to be sniffed initially). **Instructor: Roland Knall, Core Developer, Wireshark Foundation** 25 years of software development experience, still looking for those puzzles that evade an obvious solution. Main focus these days is UI design as well as accessibility of software. And to boldly go where no packets have gone before...
5:00-6:00pm	
Krutch Auditorium	**13 Kismet and wireless security 101** **Instructor: Mike Kershaw, Wi-Fi Hacker. Kismet Wireless** Mike Kershaw is the author of the Kismet wireless security tool, as well as a number of other open source wireless-related software and hardware projects, and has been involved in wireless in some form or another for nearly 17 years.
Krutch Room 104	**14 Jumbo frames and how to catch them: The challenges that come with hunting for bigger game!!!** Jumbo Frames present some unique challenges that require us to use some different capture and packet analysis techniques. From how we capture the packets to how we analyze and troubleshoot issues, Jumbo packets require some new packet analysis skills. In this session, we'll cover: • How to set up to capture those bigger packets.... • How to be sure and catch the packets we are hunting for ... • How to use ICMP to troubleshoot those pesky Jumbo Frame Problems…. • Why are the captures so large? • Analyzing iSCSI traffic in your datacenters **Instructor: Patrick Kinnison, Lead WAN Analyst, Southern Farm Bureau Casualty Insurance Company** Over the last 20+ years, I've worked as a boots-on-the-ground IT engineer for a variety of different companies engaged in business ranging from manufacturing, construction, retail, and insurance. I work every day solving complex IT issues. Having seen and experienced many changes in the IT business over the years, I can speak first-hand of the real-world situations that IT engineers face every day. Wireshark had truly changed the way I do my job and is one of the most powerful tools I have in my Super Engineer "Propeller Head" Tool Belt.

SharkFest'19 US Conference Agenda

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

WEDNESDAY, 12 JUNE

8:00-9:00am	**KEYNOTE: Mental Models for Using Network Evidence** **Chris Sanders** **(Krutch Auditorium)**
9:15-10:45am	
Krutch Auditorium	**15 War Story: Troubleshooting issues on encrypted links** Instructor: Christian Landström Senior Consultant, Airbus DS CyberSecurity Christian Landström has been working in IT since 2004, focusing strongly on network communications and IT security. After graduating in computer science in 2008, Christian joined Synerity Systems and then moved with the whole Synerity team to Fast Lane GmbH in 2009 as Senior Consultant for network analysis and security. Since 2013, he has been working as a Senior Consultants for Airbus Defence and Space CyberSecurity focusing on IT security, Incident Response and Network Forensics.
Garden Room	**16 Wireshark visualization TIPS & tricks** Wireshark has many features allowing you to analyze network traffic and dissect almost all protocols. Wireshark also has CLI tools to automate trace inspection tasks. Once data has been collected, would you like to enhance reports to easily visualize that data with pie charts, histograms and nice diagrams? In this session, Megumi will show you easy and useful ways to enhance your report with interesting visuals, providing visualization TIPS and tricks that derive beautiful graphs from your trace files. She'll use not only Wireshark IO and TCP stream graphs, but also external tools and scripts to visualize traffic. 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.
Krutch Room 104	**17 My TCP ain't your TCP – ain't no TCP? How new implementations speed up the internet and make engineers drink** From the first specs to modern implementations, TCP stack behaviours have changed quite a bit and are still subject to major changes when new versions of operating systems are released. The big IT players are pushing self-developed solutions. Established, long-standardized protocols are having a hard time gaining proper attention, with some of them working on totally different OSI layers. In this session, we are going to think outside the box and explore a few alternatives to our well known and beloved TCP and the implications for our daily operations. Instructor: Simon Lindermann, Network Engineer, Miele Since successfully completing his IT Specialist apprenticeship, Simon has been working as a Network Engineer for a German household appliance manufacturer. While working on projects in various global locations, he discovered his passion for network analysis so, along with his job at Miele, Simon started doing freelance troubleshooting work following the slogan "Only packets tell the truth!
11:00am-12:30pm	
Krutch Auditorium	**18 Practical Tracewrangling: Exploring capture file manipulation/extraction scenarios** Sometimes, scrolling through the packet list while filtering and inspecting the packet decodes in Wireshark isn't the right thing to do at the beginning. When the amount of packets becomes overwhelming, you need a strategy to reduce the haystack to a smaller pile you can work with without getting lost all the time. This is where Tracewrangler can help a lot, offering various extraction techniques. While Wireshark is capable of reading almost any kind of network packet or frame you throw at it, some other tools may not be that versatile. Sometimes, link layer types like Linux Cooked Capture (SLL), tunneling layers or MPLS shims make it impossible to process capture with your favorite tool because it doesn't understand those layers. Tracewrangler can help, modifying your capture files in an adaptive way without breaking layer relationships. Instructor: Jasper Bongertz, Sr. Technical Consultant, Airbus Defence & Space CyberSecurity Jasper Bongertz is a Senior Technical Consultant for Airbus Defence and Space CyberSecurity. He started working freelance in 1992 when he began studying computer science at the Technical University of Aachen, eventually moving to Airbus to focus on IT security, Incident Response and Network Forensics.

SharkFest'19 US Conference Agenda

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

Garden Room	**19 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.
Krutch Room 104	**20 Packets in. Packets out. Let's find out!** Wireshark is the de facto analysis tool across many IT fields of endeavor. It's one of my go-to, ultimate security tools for verification and validation. The concept is simple: Intercept, Listen, Discover, and Be Evil! with protocols by walking through some packets. From the packet level knowledge you've acquired, we'll take it to the next level in hacking, exploiting, manipulating and doing the evil stuff to understand some of the security threats we're all faced with. This session is suitable for those who want to start learning and using Wireshark from a security perspective. **Instructor: Maher Adib, (WCNA, CCIE#25094), 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 incidents 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!
1:30-3:00pm	
Krutch Auditorium	**21 Using Wireshark to solve real problems for real people: Real-world packet analysis case studies** Stop banging your head on your desk trying to find root cause and solve performance problems. The answers are in the packets and this session will show you step-by-step in Wireshark how to solve real world case studies that had 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.
Garden Room	**22 Analyzing Windows malware traffic with Wireshark (part 1)** This lab is part 1 of a 2 part lab designed to help people use Wireshark to investigate Windows-based malware activity from a packet capture (pcap) of network traffic based on alerts from an Intrusion Detection System (IDS). The material covers both initial infection activity and post-infection traffic from examples of mass-distribution of Windows malware. Scenarios include: • Searching for malicious traffic based on an IDS alert • Attempting to find the root cause based on indicators in the network traffic The instructor includes several tips on how to filter traffic in Wireshark and provides insight into these Windows-based infections. **Instructor: Bradley Duncan, Threat Intelligence Analyst, Palo Alto Networks - Unit 42** After 21 years of classified intelligence work for the US Air Force, Brad transitioned to cyber security in 2010, and he is a currently a Threat Intelligence Analyst for Palo Alto Networks Unit 42. Brad specializes in network traffic analysis. He is also a handler for the Internet Storm Center (ISC) and has posted more than 100 diaries at isc.sans.edu. Brad routinely blogs technical details and analysis of infection traffic at www.malware-traffic-analysis.net, where he provides traffic analysis exercises and over 1,300 malware and pcap samples to a growing community of information security professionals.
Krutch Room 104	**23 Developer Bytes Lightning Talks** Developer Bytes Lightning Talks focus on small, interesting topics regarding Wireshark, its development, and use cases. We'll present a look behind the curtains, highlight features often overlooked, or present upcoming topics for future versions of Wireshark. This session delivers 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
3:15-4:45pm	
Krutch Auditorium	**24 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 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. Come to this session and learn to ask the right questions and look at packets in different ways. PLEASE BRING PERPLEXING TRACE FILES FOR ANALYSIS BY THE PANEL! Packet Doctors: Dr. Bae, Dr. Bongertz, Dr. Landström, Dr. Blok, Dr. Rogers
Garden Room	**25 Analyzing Windows malware traffic with Wireshark (part 2)** This lab is part 2 of a 2 part lab designed to help people use Wireshark to investigate Windows-based malware activity from a packet capture (pcap) of network traffic based on alerts from an Intrusion Detection System (IDS). The material covers both initial infection activity and post-infection traffic from examples of mass-distribution of Windows malware. Scenarios include: • Searching for malicious traffic based on an IDS alert • Attempting to find the root cause based on indicators in the network traffic The instructor includes several tips on how to filter traffic in Wireshark and provides insight into these Windows-based infections. Instructor: Bradley Duncan, Threat Intelligence Analyst, Palo Alto Networks - Unit 42 After 21 years of classified intelligence work for the US Air Force, Brad transitioned to cyber security in 2010, and he is a currently a Threat Intelligence Analyst for Palo Alto Networks Unit 42. Brad specializes in network traffic analysis. He is also a handler for the Internet Storm Center (ISC) and has posted more than 100 diaries at isc.sans.edu. Brad routinely blogs technical details and analysis of infection traffic at www.malware-traffic-analysis.net, where he provides traffic analysis exercises and over 1,300 malware and pcap samples to a growing community of information security professionals.
Krutch Room 104	**26 To Send or Not to Send? how TCP congestion control algorithms work** This session is fully dedicated to the topic of TCP congestion control and will explain: - Why TCP congestion control is necessary - The history of its development - What the fixed terms: "cliff", "congestion collapse", "global synchronization" mean - Why this problem is so difficult to solve even now - Current approaches to handle TCP congestion We will compare different TCP congestion control algorithms (using sample trace files and Wireshark) with an emphasis on the most recent ones (CUBIC, CDG, BBR) and learn what main ideas are implemented in different kinds of TCP congestion control. We'll also take a look at some tricks like "Hybrid slow start" as a part of CUBIC algorithm, and several ways to trick the sender's behavior. Instructor: Vladimir Gerasimov, Network Engineer, Packettrain.NET Vladimir Gerasimov currently works as a Network Engineer for Unitop LTD - a company building networks and IP video surveillance systems for customers. He has been working in IT for more than 12 years, and 7 years ago he has shifted to Network Protocol Analysis with the main focus on TCP and Application performance analysis. Vladimir runs personal blog and he is also a creator and administrator of the largest Russian-speaking group regarding Network Protocol Analysis.
5:00-6:00pm	
Krutch Auditorium	**27 TBD**
Krutch Room 104	**28 TLS encryption and decryption**: What every IT engineer should know about TLS Any reputable website or application will encrypt data communication over networks. This is great step forward in providing quality network security, however, it can leave engineers in the dark when it comes to troubleshooting applications using Wireshark.

	Learn how SSL/TLS works to encrypt traffic in this easy to understand breakdown of the protocol. Ross will use Wireshark to describe the details of SSL/TLS operation, observing each step of the handshake and how it leads to the bulk encryption of data. Intended for an engineer who understands the basics of encryption but would like to learn more about: -TLS 1.2 and 1.3 handshakes -Key Exchange operation -Capturing and using session keys to decrypt captures. You'll leave this session with a visual understanding of TLS operation and be able to easily decrypt your captures, in order to troubleshoot the application data contained within. **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.

SharkFest'19 US Conference Agenda

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

THURSDAY, 13 NOVEMBER

8:00-9:00am	 ***SharkBytes (Krutch Auditorium)***
9:15 – 10:45am	
Krutch Auditorium	**29 Automating cloud infrastructure for analysis of large network captures** Often, we're required to analyze large captures containing GB/TB of network data. Analysis on captures of this scale can be time consuming, require specialized (and expensive) hardware, or require detailed processing using multiple tools before Wireshark is even opened. On-demand cloud services can assist in these circumstance by providing high-powered resources, but managing, configuring and using these services can be cumbersome. This talk will discuss processes, procedures and tools an analyst can use to quickly and easily utilize cloud services in analysis efforts of large pcaps. We'll discuss the use of familiar analysis tools like Moloch, tcpdump, tshark, and (of course) Wireshark in cloud environments and how best to leverage different cloud platforms and services to automate the use of these tools. **Instructors: Brad Palm, Network and Security Analyst & Brian Greunke, Security Advocate, BruteForce** Brad is a seasoned problem solver and convergent thinker who enjoys the challenges of merging the physical and virtual worlds. As an analyst working in the cybersecurity and network efficiency domains, he focuses on network capture and analysis for enterprise networks, testing emerging technologies and devices for customers, and utilizing captured traffic to influence developmental test scenarios. His professional interests include tinkering with open source virtualization/container/provisioning technologies, learning about software defined and mesh networking, and increasing the usability of secure information systems to facilitate wide scale adoption. Brian is a security advocate, technical leader, and full-stack developer with nearly 10 years of experience guiding technical teams in fast-paced, high-stakes environments. He enjoys exploring cutting edge technologies and using them to build security, decentralization, and privacy into the software and systems we use every day.
Garden Room	**30 Capture file format deep dive** **Instructor: Jasper Bongertz, Sr. Technical Consultant, Airbus Defence & Space CyberSecurity** Jasper Bongertz is a Senior Technical Consultant for Airbus Defence and Space CyberSecurity. He started working freelance in 1992 when he began studying computer science at the Technical University of Aachen, eventually moving to Airbus to focus on IT security, Incident Response and Network Forensics.
Krutch Room 104	**31 Can you really capture @10Gbps on a laptop? What you need and how to handle dropped packets** There are times when you need to be able to capture packets at high rates and need to see all of them or at least a 95% of them. However, you also don't have access to enormous racks of equipment, and you would like a relatively portable solution. In this session, we'll present experiences with capturing at high rates with a laptop (albeit a well-configured laptop) and associated achieved. We'll also show how to repair captures that have seen packet drops, using as an example experiences in tracking down a bug in the Mac OS X smbfs module that was causing SMB connections to be lost. These techniques will allow you to make the most of the captures that you do manage to get at such high speeds. **Instructor: Richard Sharpe, Founding Software Engineer, Hammerspace** Richard Sharpe is a software engineer who works on NFS and SMB and is a contributor to Wireshark and Samba. He has worked on a number of Wireshark dissectors and currently works on the Wi-Fi dissector suite a lot.

SharkFest'19 US Conference Agenda

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

11:00am – 12:30pm	
Krutch Auditorium	**32 A deep dive into LDAP: Everything you need to know to debug and troubleshoot LDAP packets** LDAP's purpose is to authenticate clients to a directory server(s), then store and retrieve data based on a criteria. It seems simple. It's even vendor neutral. Yet, when something goes wrong, life in Active Directory stops. In this session, we will use trace files and Wireshark to both understand the protocol, and troubleshoot it. Bring your laptop to follow along. Traces and a profile will be made available at https://bettydubois.com/sf19us. **Instructor: Betty DuBois, Chief Detective, Packet Detectives** Betty is the Chief Detective for Packet Detectives, and has been solving mysteries since 1997. She troubleshoots the root cause of network and/or application issues. Experienced with a range of hardware and software solutions, she captures the right data, in the right place, and at the right time. Using packets to solve crimes against the network and applications, is her passion. Teaching others how to do the same, is her calling.
Garden Room	**33 TCP split brain: Compare/contrast TCP effects on client and server with Wireshark (Part 1)** In this session, we'll explore the independent, and inter-dependent, TCP behaviors as viewed from both sides of a connection with Wireshark. Observe how each side makes assumptions about the other side based on the traffic it sees and the traffic it doesn't see. **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.
Krutch Room 104	**34 Solving the impossible** Performance problems continue to plague a major application. You are the go-to guy when all else fails to find the root cause. On top of that, you also need to come up with a solution. Coincidentally, you are the packet guy. The Wireshark guy. Are you up to the task? In this session, we'll examine some very challenging performance issues that would have been nearly impossible to solve without packet analysis. One problem started out described as a 'white screen' by end-users. Another involved painfully slow data migration to the cloud running up against a fast approaching deadline. We'll throw in one or two additional case studies, time permitting. You'll get the full background, the approach, and see the traces that ultimately provided the answers with expert (read human) interpretation. Don't miss this action-packed and unique "tag team" approach by grizzled analysis veterans Mike Canney and J. Scott Haugdahl. **Instructors: Scott Haugdahl, Founder, VisiblePackets & Mike Canney, Principal Performance Analyst, Packet Fetcher** Entrepreneur and author, Mr. Haugdahl's career took him from traveling the world over on business, teaching thousands of professionals the fine art of packet analysis, to founding a successful company focused on packet analysis and expert systems, to architecture and design of high-end enterprise network visibility fabrics for US Bank and Blue Cross Blue Shield of MN. As of late, Mr. Haugdahl enjoys the rapid changes in corporate IT, brought on by evolution in cloud technologies. Whenever possible, he enjoys travel, photography, and kicking back with a good mystery novel. Specializing in providing application and network performance consulting services over the past 26 years, Mike Canney has helped 1,000's of companies identify and resolve their application and network performance issues. Mike has also developed courseware, taught engineers how to identify, remediate, and prevent network and application issues by analyzing traffic flows at the packet level, and been a guest speaker at many industry trade shows (such as Networld Interop, multiple SharkFests and Cisco Networkers) throughout the United States delivering sessions on the topic of application performance analysis.
1:30-3:00pm	
Krutch Auditorium	**35 Troubleshooting slow networks** **Instructor: Chris Greer, Network Analyst, Packet Pioneer** Chris Greer is a Network Analyst for Packet Pioneer LLC. Chris has several years of experience in analyzing and troubleshooting networks. He regularly assists companies in tracking down the source of network and application performance problems using a variety of protocol analysis and monitoring tools including Wireshark. When he isn't hunting down problems at the packet level, he can be found teaching Wireshark classes and writing articles for technical blogs and online magazines.

Garden Room	**36 TCP split brain: Compare/contrast TCP effects on client and server with Wireshark (part 2)** In this session, we'll explore the independent, and inter-dependent, TCP behaviors as viewed from both sides of a connection with Wireshark. Observe how each side makes assumptions about the other side based on the traffic it sees and the traffic it doesn't see. **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.
Krutch Room 104	**37 When TCP reassembly gets complicated** Armed with a pcap file, we can examine and analyze the packets that were sent and how they were responded to on the network. We rely on our tools to show us how a TCP stream was reassembled or to give us a list of HTTP websites accessed in a pcap file. But what happens when TCP segments overlap or when new options like TCP Fast Open are used? Does every device and tool reassemble TCP exactly the same in all cases? Are the latest TCP options supported by all of the tools we use? Could this be used to disguise malicious behavior? In this session, we'll look at how TCP packets are processed by operating systems, including Linux and Windows, and compare this to tools such as Wireshark and Suricata. When these don't match, we'll look at the packets themselves and go over ways to test how the packets are really being processed. If you know how TCP reassembly works when packets are received simply out of order you might be surprised to see what happens when we look at packet scenarios during this session! **Instructor: Tom Peterson, Developer, CloudShark** Tom works at CloudShark helping bring pcap analysis to the web. Getting started with networking in 2005 performing testing at the InterOperability Lab at UNH, he began by learning IPv6 and moved from there testing IPsec, firewalls, and other network security devices. Testing a variety of protocols and devices has led to a passion of looking for strange behavior in a pcap file and getting to the bottom of it.
3:15-4:45pm	
Krutch Auditorium	**38 Using Wireshark to solve real problems for real people: Real-world packet analysis case studies** Stop banging your head on your desk trying to find root cause and solve performance problems. The answers are in the packets and this session will show you step-by-step in Wireshark how to solve real world case studies that had 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.
Garden Room	**39 TBD**
Krutch Room 104	**40 Enrich your network visibility & analysis with Wireshark & ELK** Network administrators & security analysts need the fastest, most reliable methods for packet capturing and analysis. Being able to look deeply into network behaviour based on metadata and payload provided by Wireshark helps resolve issues quickly when troubleshooting or addressing network attacks. With the ability to capture & decode 3,000 protocols and over 22,700 field types, Wireshark is the perfect tool to monitor and secure modern networks. Elastic Stack (ELK) complements Wireshark with its pipelining capabilities that enable thorough network analysis. In this session, we'll work with Wireshark & ELK features to speed up & enhance your problem-solving exercises. **Instructor: Tajul Azhar Mohd Tajul Ariffin, Lecturer, Polytecnic Mersing, Johor** Network visibility has become a key topic for Tajul Azhar Mohd Tajul Ariffin as an InfoSec lecturer and researcher. As a speaker at various InfoSec events in Malaysia, he is inspired by the phrase "packets never lie". He frequently introduces Elastic Stack as a medium to analyze all traffic in his Cyber Range Lab and, as a Blue Team Specialist, he builds visibility with Wireshark and Elastic Stack as a shortcut for students to understand networking concepts in the real world.

SharkFest'19 US Conference Agenda

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