



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

Pre-Conference Courses

<p>Pre-Conference Class I</p> <p>Wireshark Analysis Foundations</p> <p>INSTRUCTORS Chris Greer Jasper Bongertz Christian Landström Sake Blok</p> <p>(Krutch Auditorium)</p>	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)
	6:00-8:00pm	Pre-Conference Class Attendee Dinner Reception – Garden Room Patio
	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)	
<p>Pre-Conference Class II</p> <p>Hunt Like a Shark</p> <p>INSTRUCTORS Brad Palm Ryan Richter Brian Greunke</p> <p>(Garden Room)</p>	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 & Lunch)

SharkFest'19 US Conference Agenda

SharkFest Opening & Welcome Dinner

 SharkFest'19 US Welcome Dinner & Sponsor Showcase (Ginkgo Lawn, Krutch Hallway)	Monday 10 June 2019	
	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	<i>SharkFest'19 US Welcome Dinner & Sponsor Showcase</i> SharkFest'19 US Attendees Only	

SharkFest'19 US Conference Agenda

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	<p align="center">KEYNOTE: “Latest Wireshark Developments & Road Map” Gerald Combs & Friends (Krutch Auditorium)</p>		
	KRUTCH AUDITORIUM	GARDEN ROOM	KRUTCH ROOM 104
9:00-9:15am	Break		
9:15-10:45am	01  War story: troubleshooting issues on encrypted links Christian Landström	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  Solving (SharkFest) packet capture challenges with only tshark Sake Blok	05  How long is a packet? And does it really matter? Dr. Stephen Donnelly	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  Taking a bite out of 100GB files Betty DuBois	09  TLS debugging Peter Wu
3:00-3:15pm	Break		
3:15-4:45pm	10  IPv6 troubleshooting with Wireshark Jeff Carrell	11  When TCP reassembly gets complicated Tom Peterson	12  Jumbo frames & how to catch them Patrick Kinnison
4:45-5:00 pm	Break		
5:00-6:00pm	13  Kismet & wireless security 101 Mike Kershaw	14  Tracing the untraceable with Wireshark: a view under the hood Roland Knall	VISIT the SharkFest Shoal Continuing Education Lab Krutch ROOM 102
6:00-8:30pm	Sponsor Technology Showcase Reception, Treasure Hunt & Dinner (Krutch Lobby & Gingko Courtyard)		

SharkFest SHOAL MENTORING & SPONSOR VIRTUAL LABS – Krutch Room 102

SharkFest'19 US Conference Agenda

Wednesday		12 June 2019		
7:00-8:00am	Breakfast – Grand Hall			
8:00-9:00am	KEYNOTE: <i>Mental Models for Using Network Evidence</i> Chris Sanders (Krutch Auditorium)			
	KRUTCH AUDITORIUM	GARDEN ROOM	KRUTCH ROOM 104	
9:15-10:45am	15  Automating cloud infrastructure for analysis of large network captures Brad Palm & Brian Greunke	16  My TCP ain't your TCP – ain't no TCP? Simon Lindermann	17  TLS1.3, DNS over HTTPs, DNS over TLS, QUIC, IPv6 PDM & more! Nalini Elkins	DIVE INTO THE DEVELOPER DEN WITH GERALD COMBS & CORE DEVELOPERS SharkFest SHOAL MENTORING & VIRTUAL LABS OPEN – Krutch Room 102
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  IPv6 security assessment tools (aka IPv6 hacking tools) Jeff Carrell	
12:30–1:30pm	Lunch & LEARN – RCPE – What it is and Why It's Important – John Pittle (Room 104)			
1:30–3:00pm	21  Troubleshooting slow networks Chris Greer	22  Analyzing Windows malware traffic with Wireshark (Part 1) Brad Duncan	23  To send or not to send? How TCP congestion control algorithms work Vladimir Gerasimov	
3:00-3:15pm	Break			
3:15–4:45pm	24  The Packet Doctors are In! Packet trace examinations with the experts Drs. Blok, Bongertz, & Landström	25  Analyzing Windows malware traffic with Wireshark (Part 2) Brad Duncan	26  TLS encryption & decryption: what every IT engineer should know about TLS Ross Bagurdes	
4:45 – 5:00pm	Break			
5:00– 6:00pm	27  Developer bytes lightning talks Wireshark Core Developers	28  Wireshark visualization TIPS & tricks Megumi Takeshita	29  Kismet & wireless security 101 Mike Kershaw	
6:00–8:30pm	Lawrence Hall of Science Sponsor Reception, Dinner & Group Competition			

SharkFest'19 US Conference Agenda

Thursday		13 June 2019			
7:00-8:00am	Breakfast – Grand Hall				
8:00-9:00am	KEYNOTE: A Brief Annotated History of Capture Loris Degioanni (Krutch Auditorium)				
	KRUTCH AUDITORIUM	GARDEN ROOM	KRUTCH ROOM 104		
9:15-10:45am	30  Back to the basics Hansang Bae	31  TCP split brain: compare/contrast TCP effects on client & server with Wireshark (Part 1) John Pittle	32  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	33  Back to the packet trenches Hansang Bae	34  TCP split brain: compare/contrast TCP effects on client & server with Wireshark (Part 2) John Pittle	35  Solving the impossible Mike Canney		
12:30-1:30pm	Lunch				
1:30-3:00pm	36  Capture file format deep dive Jasper Bongertz	37  A deep dive into LDAP: Everything you need to know to debug and troubleshoot LDAP packets Betty DuBois	38  Enrich your network visibility & analysis with Wireshark & ELK Tajul Azhar Mohd Ariffin		
3:00-3:15pm	Break				
3:15-4:45pm	39  Using Wireshark to solve real problems for real people: step-by-step case studies in packet analysis Kary Rogers	40  Troubleshooting slow networks Chris Greer	41  Wireshark visualization TIPS & tricks Megumi Takeshita		
5:00-5:30pm	 Closing Remarks & Packet Challenge Awards (Krutch Auditorium)				
5:30-7:30pm	Farewell Reception (Ginkgo Lawn)				

SharkFest'19 US Conference Agenda

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 War story: troubleshooting issues on encrypted links 

In this session, we will re-perform a real analysis job and analyze severe connectivity issues between two sites where the WAN link is fully encrypted. With four capture points in parallel, we will see what happened on the wire, how to deal with customers, vendors and service providers playing the blame game, and learn how to analyze unknown protocols.

Instructor: Christian Landström Senior Consultant, Airbus DS CyberSecurity

Christian Landström works as Incident Response and security audit expert at Airbus Defence and Space CyberSecurity. Working in IT since 2004, with a strong focus on network communications and IT security, he graduated in computer science in 2008 and joined Synerity Systems and afterwards moved with the whole Synerity team to work for Fast Lane GmbH. There, Christian created and delivered various Network Analysis Trainings and worked as Senior Consultant for network analysis and IT security. In 2013, he started working for Airbus Defence and Space CyberSecurity focusing on IT security, Incident Response and Network Forensics. He shares his passion about network analysis together with Jasper and Eddi from the original Synerity Team on the Sharkfest conferences and on the blog.packet-foo.com.

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.

11:00am-12:30pm

<p>Krutch Auditorium</p>	<p>04 Solving (SharkFest) packet capture challenges with tshark alone: Get exact answers from trace files in an automated way 🚀🚀</p> <p>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!)</p> <p><u>Instructor: Sake Blok, Relational Therapist for Computer Systems</u></p> <p>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.</p>
<p>Garden Room</p>	<p>05 How long is a packet? And does it really matter? 🚀</p> <p>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.</p> <p><u>Instructor: Stephen Donnelly, CTO, Endace</u></p> <p>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.</p>
<p>Krutch Room 104</p>	<p>06 Creating dissectors like a pro by generating dissectors 🚀🚀</p> <p>The Wireshark dissector generator I have been working on for a while now can generate C and Lua dissectors and dissectors from a simple description of a protocol. This talk will show you how to quickly generate dissectors for any protocol, and how to make the best use of the dissector generator.</p> <p><u>Instructor: Richard Sharpe, Founding Software Engineer, Hammerspace</u></p> <p>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.</p>

1:30-3:00pm

<p>Krutch Auditorium</p>	<p>07 To send or not to send? How TCP congestion control algorithms work 🚀🚀🚀</p> <p>This session is fully dedicated to the topic of TCP congestion control and will explain:</p> <ul style="list-style-type: none"> - 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 <p>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.</p> <p><u>Instructor: Vladimir Gerasimov, Network Engineer, Packettrain.NET</u></p> <p>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 shifted to Network Protocol Analysis with</p>
---------------------------------	--

SharkFest'19 US Conference Agenda

	<p>the main focus on TCP and application performance analysis. Vladimir runs a personal blog and is also a creator and administrator of the largest Russian-speaking Network Protocol Analysis group.</p>
Garden Room	<p>08 Taking a bite out of 100G Trace Files: Learn best practices for working with large data sets </p> <p>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://www.bettydubois.com/sharkfest. The files will start at 100M and get successively larger, so that you can choose what size you are comfortable working with.</p> <p>Instructor: Betty DuBois, Chief Detective, Packet Detectives</p> <p>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.</p>
Krutch Room 104	<p>09 TLS debugging </p> <p>Instructor: Peter Wu, Wireshark Core Developer</p> <p>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.</p>
3:15-4:45pm	
Krutch Auditorium	<p>10 IPv6 troubleshooting with Wireshark </p> <p>Whether you know it or not, IPv6 is running on your network, but is it working as you need or expect it to? Do you know what the Router Advertisement is configured as? Do you have "rogue" IPv6 routers on your network? Are the IPv6 enabled clients complaining of "slowness"?</p> <p>Many technologists use Wireshark for validation of network operations and troubleshooting potential network problems. This session will briefly review IPv6 fundamentals and then dive into configuring Wireshark to assist in viewing IPv6 more effectively. Wireshark configuration profiles, display filters, and color rules can provide specific focus when troubleshooting reported IPv6 problems, and how to effectively and expeditiously determine what could be the root cause.</p> <p>This will be a hands-on/follow-Jeff session with trace files provided, so be sure to bring your laptop with Wireshark installed!</p> <p>Instructor: Jeff Carrell, Network Consultant, Network Conversions</p> <p>Jeff Carrell is a Network Instructor at Hewlett Packard Enterprise. Jeff facilitates many networking courses offered by HPE, serves as a SME for customized courses for specific customer requirements, and participates in course development.</p> <p>Jeff is a frequent industry speaker, technical writer, IPv6 Forum Certified Trainer, and prior to HPE was a network instructor and course developer to major networking manufacturers. He is a technical lead and co-author for the book, Guide to TCP/IP: IPv6 and IPv4, 5th Edition and lead technical editor on Fundamentals of Communications and Networking, Second Edition. Jeff is a long-time user of Wireshark.</p>
Garden Room	<p>11 When TCP reassembly gets complicated </p> <p>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!</p> <p>Instructor: Tom Peterson, Developer, CloudShark</p> <p>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.</p>

SharkFest'19 US Conference Agenda

<p>Krutch Room 104</p>	<p>12 Jumbo frames and how to catch them: The challenges that come with hunting for bigger game!!!  </p> <p>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:</p> <ul style="list-style-type: none"> • 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 <p>Instructor: Patrick Kinnison, Lead WAN Analyst, Southern Farm Bureau Casualty Insurance Company</p> <p>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.</p>
<p>5:00-6:00pm</p>	
<p>Krutch Auditorium</p>	<p>13 Kismet and wireless security 101 </p> <p>Kismet has been around for over 15 years, but new development has expanded it beyond Wi-Fi capture, added a new web-based interface, and enabled streaming capture from remote sensors. Learn about the new features in Kismet, how to get Wi-Fi capture on the cheap, how to integrate it with tools like Wireshark and TShark for wireless capture, and how to talk to the Kismet API to make your own tools and automate capture.</p> <p>Instructor: Mike Kershaw, Wi-Fi Hacker, Kismet Wireless</p> <p>Mike Kershaw is the author of several open source tools, including Kismet, a Wi-Fi and general wireless capture tool and IDS, as well as other open source hardware and software projects, typically related to wireless technologies.</p>
<p>Garden Room</p>	<p>14 Tracing the untraceable with Wireshark: a view under the hood  </p> <p>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).</p> <p>Instructor: Roland Knall, Core Developer, Wireshark Foundation</p> <p>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...</p>

WEDNESDAY, 12 JUNE

KEYNOTE: *Mental Models for Using Network Evidence*

Chris Sanders
(Krutch Auditorium)

The network evidence we parse with Wireshark often presents a problem of too much data, rather than not enough. In a complex domain, humans rely on simplifying strategies to organize our thoughts and make sense of the mountains of information available to us. In this presentation, I'll describe common mental models used for gathering and analyzing network evidence. We'll tie these models to practical use cases provided by Wireshark features and provide a framework for how you can approach evidence efficiently by asking the right questions.

8:00-9:00am

About Chris

Chris Sanders is the founder of [Applied Network Defense](#) and has extensive experience supporting multiple Fortune 500 companies and government/military agencies. He has authored several books and articles, including the international best seller "Practical Packet Analysis" from No Starch Press, currently in its third edition, and "Applied Network Security Monitoring" from Syngress. Both books have been translated into multiple languages, and have collectively sold tens of thousands of copies. Chris currently holds several industry certifications, including the SANS GSE distinction.

Chris is originally from Mayfield, KY. Growing up in a rural area, he saw the transformative power that education could have on lives and its ability to end generational poverty. He started the [Rural Technology Fund](#) in 2008 with the mission of helping bridge the digital divide between rural and urban areas. The RTF has put computer science education materials in the hands of over 75,000 students. Applied Network Defense was founded with a similar goal as the Rural Tech Fund, but instead focuses on providing high quality information security training at a fair price. Chris is passionate about education and helping information security practitioners further their careers and positively impact the organizations they serve.

9:15-10:45am

Krutch
Auditorium

15 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 circumstances 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

16 My TCP ain't your TCP ain't no TCP? how new implementations speed up the internet & 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. Big IT players push self-developed solutions. Established, long-standardized protocols are having a hard time gaining proper attention, with some 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!"

SharkFest'19 US Conference Agenda

<p>Krutch Room 104</p>	<p>17 TLS1.3, DNS over HTTPS, DNS over TLS, QUIC, IPv6 PDM & more! Exploring new protocols being worked on at the IETF </p> <p>Many new protocols are being worked on at the IETF. Some are RFCs already. Others will soon gain that status. These protocols include: TLS1.3, DNS over HTTPs, DNS over TLS and QUIC. A fundamental premise that all of these protocols share is that metadata may be misused. So, more and more of the packet is being encrypted. How will this impact diagnostics and troubleshooting? If many of the protocol headers themselves are encrypted, how will we get performance information?</p> <p>One new RFC (RFC8250) for IPv6 Performance Diagnostics and Metrics tries to give us back some of the information we need. This session will discuss these new protocols and show packet flows for each.</p> <p><u>Instructor: Nalini Elkins, CEO, Inside Products</u></p> <p>Nalini is the CEO and Founder of Inside Products. She has also been the CEO / CTO of 3 other high-tech companies. Her area of technical expertise is in performance metrics for wide area networking. Her latest standard is RFC8250: Performance Metrics and Diagnostics for IPv6. She is a commercial software product developer whose products have been marketed by IBM as well as other major software vendors. She received the A.A. Michelson award (given once a year) in 2014 from the Computer Measurement Group for her contributions to the industry. Her IP Problem Finder products are expert system analytic tools incorporating Wireshark output. She loves Wireshark! Packets don't lie.</p>
<p>11:00am-12:30pm</p>	
<p>Krutch Auditorium</p>	<p>18 Practical Tracewrangling: Exploring capture file manipulation/extraction scenarios </p> <p>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.</p> <p>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.</p> <p><u>Instructor: Jasper Bongertz, Sr. Technical Consultant, Airbus Defence & Space CyberSecurity</u></p> <p>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.</p>
<p>Garden Room</p>	<p>19 TCP SACK Overview and Impact on Performance </p> <p>TCP SACK is an important performance enhancement to TCP. Learn the details of how to interpret the SACK field and relate it to performance of the application.</p> <p><u>Instructor: John Pittle, Distinguished Performance Consultant, Riverbed Technology, Inc.</u></p> <p>As a Performance Management Strategist, John helps his customers develop and execute strategies for integrating Performance Management as an IT discipline across the organization. He has been actively focused on Performance Engineering and Analysis for networks, systems, and applications since the early 90s; performance troubleshooting is his passion and joy. His packet analysis toolbox includes Wireshark (of course), as well as NetShark, AppResponse, Packet Analyzer, and Transaction Analyzer.</p>
<p>Krutch Room 104</p>	<p>20 IPv6 security assessment tools (aka IPv6 hacking tools) </p> <p>In networking, IP as we call it is actually Internet Protocol version 4 (IPv4). Internet Protocol version 6 (IPv6) is the replacement for IP running in today's networks. 19 years after the initial release of IPv6 we observe that most networks are not formally implementing IPv6, however, most modern desktop/server OS's have had IPv6 enabled for 8+ years. That means many IT departments and technologists don't understand that IPv6 is in fact all over their networks nor what the potential implications are.</p> <p>This session will briefly review IPv6 fundamentals and then dive into configuring Wireshark to assist in viewing IPv6 more effectively. Various IPv6 Security tools will be used to cause issues on an isolated IPv6 network, we will then review those operations with Wireshark, as well as review the affected IPv6 operations on the IPv6 clients.</p> <p><u>Instructor: Jeff Carrell, Network Consultant, Network Conversions</u></p> <p>Jeff Carrell is a Network Instructor at Hewlett Packard Enterprise. Jeff facilitates many networking courses offered by HPE, serves as a SME for customized courses for specific customer requirements, and participates in course development.</p> <p>Jeff is a frequent industry speaker, technical writer, IPv6 Forum Certified Trainer, and prior to HPE was a network instructor and course developer to major networking manufacturers. He is a technical lead and co-author for the book, Guide to TCP/IP: IPv6 and IPv4, 5th Edition and lead technical editor on Fundamentals of Communications and Networking, Second Edition. Jeff is a long-time user of Wireshark.</p>
<p>1:30-3:00pm</p>	

SharkFest'19 US Conference Agenda

<p>Krutch Auditorium</p>	<p>21 Troubleshooting slow networks </p> <p>The dreaded spinning wheel or slow file transfer bar. Why, in 2019, with lightning fast network connections spanning the globe, do we still battle network slowness? In this session, we are going to use hands-on scenarios to examine the cause of slow network performance. We will especially focus on file transfers across high bandwidth, high latency connections, and show why TCP can have a tough time fully utilizing these types of links. We will learn:</p> <ul style="list-style-type: none"> • How to measure throughput on file transfers • How to determine if packet loss is the culprit • Why TCP Congestion Control really matters in file transfers <p>Bring your copy of Wireshark and let's have some fun!</p> <p><u>Instructor: Chris Greer, Network Analyst, Packet Pioneer</u></p> <p>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.</p>
<p>Garden Room</p>	<p>22 Analyzing Windows malware traffic with Wireshark (part 1) </p> <p>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:</p> <ul style="list-style-type: none"> • Searching for malicious traffic based on an IDS alert • Attempting to find the root cause based on indicators in the network traffic <p>The instructor includes several tips on how to filter traffic in Wireshark and provides insight into these Windows-based infections.</p> <p><u>Instructor: Bradley Duncan, Threat Intelligence Analyst, Palo Alto Networks - Unit 42</u></p> <p>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.</p>
<p>Krutch Room 104</p>	<p>23 To Send or Not to Send? how TCP congestion control algorithms work </p> <p>This session is fully dedicated to the topic of TCP congestion control and will explain:</p> <ul style="list-style-type: none"> - 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 <p>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.</p> <p><u>Instructor: Vladimir Gerasimov, Network Engineer, Packettrain.NET</u></p> <p>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.</p>
<p>3:15-4:45pm</p>	
<p>Krutch Auditorium</p>	<p>24 The Packet Doctors are In! Packet trace examinations with the experts </p> <p>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.</p> <p>PLEASE BRING PERPLEXING TRACE FILES FOR ANALYSIS BY THE PANEL!</p> <p><u>Packet Surgeons: Drs. Blok, Bongertz, & Landström</u></p>

SharkFest'19 US Conference Agenda

<p>Garden Room</p>	<p>25 Analyzing Windows malware traffic with Wireshark (part 2) </p> <p>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:</p> <ul style="list-style-type: none"> • Searching for malicious traffic based on an IDS alert • Attempting to find the root cause based on indicators in the network traffic <p>The instructor includes tips on how to filter traffic in Wireshark and provides insight into these Windows-based infections.</p> <p>Instructor: Bradley Duncan, Threat Intelligence Analyst, Palo Alto Networks - Unit 42</p> <p>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.</p>
<p>Krutch Room 104</p>	<p>26 TLS encryption and decryption: What every IT engineer should know about TLS </p> <p>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:</p> <ul style="list-style-type: none"> -TLS 1.2 and 1.3 handshakes -Key Exchange operation -Capturing and using session keys to decrypt captures. <p>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.</p> <p>Instructor: Ross Bagurdes, Bagurdes Technology, Network Engineer & Educator</p> <p>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.</p>
<p>5:00-6:00pm</p>	
<p>Krutch Auditorium</p>	<p>27 Developer bytes lightning talks </p> <p>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.</p> <p><u>Instructors: Wireshark Core Developers</u></p>
<p>Garden Room</p>	<p>28 Wireshark visualization TIPS & tricks </p> <p>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.</p> <p>Instructor: Megumi Takeshita, Packet Otaku and Owner, Ikeriri Network Service</p> <p>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.</p>
<p>Krutch Room 104</p>	<p>29 Kismet and wireless security 101 </p> <p>Kismet has been around for over 15 years, but new development has expanded it beyond Wi-Fi capture, added a new web-based interface, and enabled streaming capture from remote sensors. Learn about the new features in Kismet, how to get Wi-Fi capture on the cheap, how to integrate it with tools like Wireshark and TShark for wireless capture, and how to talk to the Kismet API to make your own tools and automate capture.</p> <p>Instructor: Mike Kershaw, Wi-Fi Hacker, Kismet Wireless</p>

SharkFest'19 US Conference Agenda

Mike Kershaw is the author of several open source tools, including Kismet, a Wi-Fi and general wireless capture tool and IDS, as well as other open source hardware and software projects, typically related to wireless technologies.

THURSDAY, 13 JUNE

<p>8:00-9:00am</p>	<p align="center">KEYNOTE: A Brief Annotated History of Capture Loris Degioanni (Krutch Auditorium)</p> <p>Loris Degioanni is a capture nerd.</p> <p>He created WinPcap™, the packet capture library for Windows. He was the initial mind behind the pcap-ng standard, universally used to store capture data. He was the co-founder of CACE Technologies, which employed Ethereal/Wireshark open source project creator, Gerald Combs. Recently, as the founder of Sysdig, he created a family of Open Source tools that capture, filter and store system calls, applying the same concepts and workflows that are at the base of packet capture.</p> <p>As you can imagine, Loris has seen a number of interesting things in his time and, in this keynote, he will tell you some of them. He'll go through the history of this field, explaining how some of the tools you use on a daily basis work under the hood. He'll also tell you the reasons why they were designed the way they are, how the new generation of tools was inspired by the old one, where we are, today, technology-wise, and where we'll go in the next years.</p> <p>This 25-year journey will bring you from the original 1993 design of libpcap to the most recent technical advances like eBPF, covering software, hardware and people and include history, technical deep dives and fun facts.</p>
<p>9:15 – 10:45am</p>	
<p align="center">Krutch Auditorium</p>	<p>30 Back to the basics </p> <p>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.</p> <p><u>Instructor: Hansang Bae, CTO, Riverbed Technology</u></p> <p>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.</p>
<p align="center">Garden Room</p>	<p>31 TCP split brain: compare/contrast TCP effects on client and server with Wireshark (Part 1)  </p> <p>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.</p> <p><u>Instructor: John Pittle, Distinguished Performance Consultant, Riverbed Technology, Inc.</u></p> <p>As a Performance Management Strategist, John helps his customers develop and execute strategies for integrating Performance Management as an IT discipline across the organization. He has been actively focused on Performance Engineering and Analysis for networks, systems, and applications since the early 90s; performance troubleshooting is his passion and joy. His packet analysis toolbox includes Wireshark (of course), as well as NetShark, AppResponse, Packet Analyzer, and Transaction Analyzer.</p>
<p align="center">Krutch Room 104</p>	<p>32 Can you really capture @10Gbps on a laptop? What you need and how to handle dropped packets  </p> <p>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.</p> <p><u>Instructor: Richard Sharpe, Founding Software Engineer, Hammerspace</u></p> <p>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.</p>

SharkFest'19 US Conference Agenda

11:00am – 12:30pm

<p>Krutch Auditorium</p>	<p>33 Back to the packet trenches </p> <p>In the session, Hansang provides real-world troubleshooting examples and interacts with attendees in addressing various TCP analysis scenarios.</p> <p><u>Instructor: Hansang Bae, CTO, Riverbed Technology</u></p> <p>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.</p>
<p>Garden Room</p>	<p>34 TCP split brain: compare/contrast TCP effects on client and server with Wireshark (part 2) </p> <p>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.</p> <p><u>Instructor: John Pittle, Distinguished Performance Consultant, Riverbed Technology, Inc.</u></p> <p>As a Performance Management Strategist, John helps his customers develop and execute strategies for integrating Performance Management as an IT discipline across the organization. He has been actively focused on Performance Engineering and Analysis for networks, systems, and applications since the early 90s; performance troubleshooting is his passion and joy. His packet analysis toolbox includes Wireshark (of course), as well as NetShark, AppResponse, Packet Analyzer, and Transaction Analyzer.</p>
<p>Krutch Room 104</p>	<p>35 Solving the impossible </p> <p>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.</p> <p><u>Instructor: Mike Canney, Principal Performance Analyst, Packet Fetcher</u></p> <p>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</p>

1:30-3:00pm

<p>Krutch Auditorium</p>	<p>36 Capture file format deep dive </p> <p>When packets are captured from the wire, they always end up in a file on disk, even if Wireshark is closed without saving the data. That's because a temporary file is created during capture and, depending on further activity, it ends up somewhere else or is deleted when the packets are discarded. There is a surprisingly large number of file formats available to store packets, the most common ones being pcap and pcapng. This talk will dive into a couple of file formats and highlight the differences, advantages and disadvantages of pcapng and pcap, and is aimed at giving attendees the information required to choose the best file format for their causes. We'll also dive into some of the stranger aspects of writing packets to disk.</p> <p><u>Instructor: Jasper Bongertz, Sr. Technical Consultant, Airbus Defence & Space CyberSecurity</u></p> <p>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.</p>
<p>Garden Room</p>	<p>37 A deep dive into LDAP: Everything you need to know to debug and troubleshoot LDAP packets </p> <p>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://www.bettydubois.com/sharkfest.</p> <p><u>Instructor: Betty DuBois, Chief Detective, Packet Detectives</u></p> <p>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</p>

SharkFest'19 US Conference Agenda

	<p>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.</p>
<p>Krutch Room 104</p>	<p>38 Enrich your network visibility & analysis with Wireshark & ELK </p> <p>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.</p> <p><u>Instructor: Tajul Azhar Mohd Tajul Ariffin, Lecturer, Polytecnic Mersing, Johor</u></p> <p>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.</p>
<p>3:15-4:45pm</p>	
<p>Krutch Auditorium</p>	<p>39 Using Wireshark to solve real problems for real people: Real-world packet analysis case studies </p> <p>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!</p> <p><u>Instructor: Kary Rogers, Director, Staff Engineering, Riverbed Technology</u></p> <p>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</p>
<p>Garden Room</p>	<p>40 Troubleshooting slow networks </p> <p>The dreaded spinning wheel or slow file transfer bar. Why, in 2019, with lightning fast network connections spanning the globe, do we still battle network slowness? In this session, we are going to use hands-on scenarios to examine the cause of slow network performance. We will especially focus on file transfers across high bandwidth, high latency connections, and show why TCP can have a tough time fully utilizing these types of links. We will learn:</p> <ul style="list-style-type: none"> • How to measure throughput on file transfers • How to determine if packet loss is the culprit • Why TCP Congestion Control really matters in file transfers <p>Bring your copy of Wireshark and let's have some fun!</p> <p><u>Instructor: Chris Greer, Network Analyst, Packet Pioneer</u></p> <p>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.</p>
<p>Krutch Room 104</p>	<p>41 Wireshark visualization TIPS & Tricks </p> <p>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.</p> <p><u>Instructor: Megumi Takeshita, Packet Otaku and Owner, Ikeriri Network Service</u></p> <p>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.</p>