SharkFest'20 US Agenda

(Draft, subject to change)

Kansas City Marriott Downtown
July 11-16, 2020

- Pre-Conference Classes
- SharkFest'20 US Session & Events Agenda
- Session Abstracts & Requirements
- Instructor Bios

SharkFest'20 US Conference Agenda

Pre-Conference Courses

Pre-Conference Class I **Troubleshooting with Wireshark – Core Skills** INSTRUCTOR Chris Greer	Saturday	11 July 2020
	8:00-9:00am	Check-in & Badge Pick up (Basie Ballroom Foyer)
	8:00-9:00am	Breakfast (Basie C/C1)
	9:00am-12:00pm	Class in session (with morning breaks) – (Basie A/A1)
	12:00-1:00pm	Lunch (Basie C/C1)
	1:00-5:00pm	Class in session (with afternoon breaks) – (Basie A/A1)
	Sunday	**12 July 2020**
	8:00-9:00am	Breakfast (Basie C/C1)
	9:00am-12:00pm	Class in session (with morning breaks) – (Basie A/A1)
	12:00-1:00pm	Lunch (Basie C/C1)
	1:00-5:00pm	Class in session (with afternoon breaks) – (Basie A/A1)

Pre-Conference Class II **Wireshark Profiles – How to Analyze Trace Files Faster and Easier** INSTRUCTOR Betty DuBois	Monday	13 July 2020
	8:00-9:00am	Check-in & Badge Pick up (Basie Ballroom Foyer)
	8:00-9:00am	Breakfast (Basie C/C1)
	9:00am-12:00pm	Class in session (with morning breaks) - (Andy Kirk A/B)
	12:00-1:00pm	Lunch (Basie C/C1)
	1:00-5:00pm	Class in session (with afternoon breaks) - (Andy Kirk A/B)

Pre-Conference Class III **SSL/TLS Troubleshooting with Wireshark** INSTRUCTOR Sake Blok	Monday	13 July 2020
	8:00-9:00am	Check-in & Badge Pick up (Basie Ballroom Foyer)
	8:00-9:00am	Breakfast (Basie C/C1)
	9:00am-12:00pm	Class in session (with morning breaks) – (Julia Lee A/B)
	12:00-1:00pm	Lunch (Basie C/C1)
	1:00-5:00pm	Class in session (with afternoon breaks) – (Julia Lee A/B)

SharkFest'20 US Conference Agenda

SharkFest Opening & Welcome Dinner

	Monday	13 July 2020
SharkFest'20 US **Welcome Dinner & Sponsor Showcase** **(Basie BB1/CC1)**	12:00-8:00pm	**SharkFest US Check-In & Badge Pick-Up** (Registration Table, Basie Ballroom Foyer)
	9:00-5:00pm	**SharkFest Shoal Mentoring Lab OPEN** (Yardbird A)
	1:00-5:00pm	**Developer Den Drop-In** (Yardbird B)
	6:00-8:30pm	***SharkFest'20 US Welcome Dinner & Sponsor Showcase*** **SharkFest'20 US Attendees Only**

SharkFest'20 US Conference Agenda

Tuesday July 14, 2020

7:00-8:00am	**Breakfast – Basie BB1/CC1**		
7:00am-12:00pm	**SharkFest Check-in & Badge Pick-up (Basie Ballroom Foyer)**		
8:00-9:00am	**KEYNOTE: "*Latest Wireshark Developments & Road Map*" Gerald Combs & Friends (Basie A/A1)**		
	Basie A/A1	**Andy Kirk A/B**	**Julia Lee A/B**
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**  **IPv6 troubleshooting with Wireshark** Jeff Carrell
10:45-11:00am	**Break**		
11:00am-12:30pm	**04**  **Back to the Packet Trenches** Hansang Bae	**05**  **How long is a packet? And does it really matter?** Dr. Stephen Donnelly	**06**  **Analyzing 802.11 Powersave Mechanisms with Wireshark** George Cragg
12:30-1:30pm	**Lunch**		
1:30-3:00pm	**07**  **Trace File Case Files - How to analyze network issues 101** Jasper Bongertz	**08**  **When Hardware Goes Bad** Andrew Brown	**09**  **TLS debugging (title subject to change)** Peter Wu
3:00-3:15pm	**Break**		
3:15-4:45pm	**10**  **TBA** **Sake Blok**	**11**  **Why an Enterprise Visibility Platform is critical for effective Packet Analysis?** Keval Shah	**12**  **Jumbo frames & how to catch them** Patrick Kinnison
4:45-5:00 pm	Break		
5:00-6:00pm	**13**  **Kismet and Wireless Security 101** Mike Kershaw	**14**  **Troubleshooting Cloud Network Outages** Chris Hull	**VISIT the SharkFest Shoal Continuing Education Lab Yardbird A**
6:00-8:30pm	**Sponsor Technology Showcase Reception, Treasure Hunt & Dinner**		

SharkFest SHOAL MENTORING & SPONSOR VIRTUAL LABS – Yardbird A

SharkFest'20 US Conference Agenda

Wednesday	15 July 2020			
7:00-8:00am	**Breakfast – (Basie BB1/CC1)**			
8:00-9:00am	**Keynote by Chris Sanders (Basie A/A1)**			
	Basie A/A1	**Andy Kirk A/B**	**Julia Lee A/B**	
9:15-10:45am	**15** **TBA** Simon Lindermann	**16** **USB Analysis 101** Tomasz Moń	**17** **Dealing with difficult protocols and captures** Richard Sharpe	
10:45–11:00am	Break			
11:00am-12:30pm	**18** **Analyzing Honeypot Traffic** Tom Peterson	**19** **Practical Signature Development for Open Source IDS** Jack Mott || Jason Williams	**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** **Troubleshooting Cisco Software Defined Access Architectures with Wireshark** Josh Halley	**23** **Give Your Bytes a Name, Part I** Roland Knall	
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	**25** **Enterprise packet capture using a distributed Wireshark environment** Erick Powell	**26** **Give Your Bytes a Name, Part II** Roland Knall	
4:45 – 5:00pm	Break			
5:00– 6:00pm	**27** **TCP SACK overview & impact on performance** John Pittle	**28** **Automation TIPS & tricks Using Wireshark/tshark in Windows** Megumi Takeshita	**29** **TLS encryption & decryption: what every IT engineer should know about TLS** Ross Bagurdes	
6:00–8:30pm	**Sponsor Reception, Dinner & Group Packet Competition**			

DIVE INTO THE DEVELOPER DEN WITH GERALD COMBS & CORE DEVELOPERS
SharkFest SHOAL MENTORING & VIRTUAL LABS OPEN – Yardbird A

SharkFest'20 US Conference Agenda

Thursday	16 July 2019			
7:00-8:00am	**Breakfast – Basie BB1/CC1**			
8:00-9:00am	**SharkBytes – The Sharkfest Signature Lightning Talks Keynote**			
	Basie A/A1	**Andy Kirk A/B**	**Julia Lee A/B**	
9:15-10:45am	30 **Intrusion Analysis and Threat Hunting with Suricata** Josh Stroschein || Jack Mott	31 **Introduction to WAN Optimization (Part 1)** John Pittle	32 **Will it Packet? Capturing non-traditional packets when you don't have a NIC** Mike Kershaw	PACKET CHALLENGE SHEETS DUE BY 8 AM
10:45-11:00am	Break			
11:00am-12:30pm	33 **Trace File Case Files - How to analyze network issues 101** Jasper Bongertz	34 **Introduction to WAN Optimization (Part 2)** John Pittle	35 **IPv6: Build Your Own Lab Workshop, Part I** Jeff Carrell	
12:30–1:30pm	Lunch			
1:30–3:00pm	36 **Packet Command Line Foo** Christian Landström	37 **Improving packet capture in the DPDK** Stephen Hemminger	38 **Pv6: Build Your Own Lab Workshop, Part II** Jeff Carrell	
3:00-3:15pm	Break			
3:15-4:45pm	39 **A walkthrough of the Sharkfest Group & Individual Packet Challenges** Sake Blok, Jasper Bongertz & Christian Landström	40 **The other protocols (used in LTE)** Mark Stout	41 **BACNet and Wireshark for Beginners** Werner Fischer	
5:00-5:30pm	**Closing Remarks & Packet Challenge Awards**			
5:30-7:30pm	**Farewell Reception**			

SharkFest'20 US Conference Agenda

TUESDAY, 14 JULY – THIS SECTION TO BE UPDATED SOON

8:00-9:00am	**KEYNOTE: *Latest Wireshark Developments & Road Map*** **Gerald Combs & Friends** **(Krutch Auditorium)**
9:15-10:45am	
Basie A/A1	**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.
Andy Kirk A/B	**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.
Julia Lee A/B	**03 IPv6 troubleshooting with Wireshark** 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"? 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. **This will be a hands-on/follow-Jeff session with trace files provided, so be sure to bring your laptop with Wireshark installed!** **Instructor: Jeff Carrell, Network Consultant, Network Conversions** Jeff Carrell is a Networking & Big Data Instructor at Hewlett Packard Enterprise and participates in course development. Jeff is a frequent industry speaker, technical writer, IPv6 Forum Certified Trainer, and prior to HPE was a network instructor and course developer to major networking manufacturers. He is a technical lead and co-author for the book, Guide to TCP/IP: IPv6 and IPv4, 5th

	Edition and lead technical editor on Fundamentals of Communications and Networking, Second Edition. Jeff has been in the computer industry since 1979, built his first LAN in 1986, and is a long-time user of Wireshark.

11:00am-12:30pm	
Basie A/A1	**04 Back to the packet 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.
Andy Kirk A/B	**05 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.
Julia Lee A/B	**06 Analyzing 802.11 Powersave Mechanisms with Wireshark**  Did you ever complain that your battery powered device did not last long enough? There are multiple mechanisms available to 802.11 devices to help improve battery life, sometimes at the cost of latency. Wireshark is a great tool to see these protocols in action and demonstrate the various setup and operational parameters with the intent on being able to diagnose and debug issues. **Instructor: George Cragg, Network Engineer, Draeger Medical Systems** George Cragg is a full time network engineer in a software team that makes medical devices to work on Hospital IT networks.
1:30-3:00pm	
Basie A/A1	**07 Trace Files Case Files – How to analyze network issues 101**  **Abstract will be available soon** **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.
Andy Kirk A/B	**08 When Hardware Goes Bad - Stories of Faulty Network Devices and Using Wireshark to Find Them**  When packets are money and customers call over a single drop, reliability in network devices is paramount. Unfortunately the fact that hardware is purpose-built to pass packets doesn't mean that it gets the job done 100% of the time. When things go wrong (especially when it's only a tiny fraction of the time) finding the root cause of the issue can be extremely tricky. **Instructor: Andrew Brown, Director, Network Engineering, Cboe Global Markets** Andrew Brown was one of thirteen founding members of BATS, an upstart company created to take on NASDAQ and the New York Stock Exchange. The company grew to hundreds of employees operating multiple equities and options markets before being acquired by the Chicago Board Options Exchange in 2017. The

	combined company now operates equities, options, and futures markets as well as foreign exchange markets with a presence in both the US and Europe.
Julia Lee A/B	**09 TLS debugging (title subject to change)** 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
3:15-4:45pm	
Basie A/A1	10. **TBA** 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.
Andy Kirk A/B	**11 Why an Enterprise Visibility Platform is critical for effective Packet Analysis? - In Digital Transformation era, Packet Level Visibility is key for Performance & Monitoring Tools** In today's era of Digital Transformation and the data velocity that we encounter across our Enterprise Networks, it has become challenging to manage and monitor the performance metrics. And this complexity has given birth or I should say have enhanced the purpose of Packet Analytics and Monitoring Tools. Wireshark is more consumed across enterprises now than every before, the same goes for Enterprise tools that fall in the product categories of Network Performance Monitoring, Security Analytics, Forensics Research, IOT and many more. Instructor: Keval Shah, Solution Sales Engineer, Gigamon Keval Shah has 12+ years of technical consulting and solution engineering experience in the field of Enterprise Networking & Security. He has enjoyed architecting and transforming businesses.
Julia Lee A/B	**12 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.
5:00-6:00pm	

Basie A/A1	**13 Kismet and wireless security 101** 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. **Instructor: Mike Kershaw, Wi-Fi Hacker. Kismet Wireless** 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.
Andy Kirk A/B	14 **Troubleshooting Cloud Network Outages** This presentation describes the monitoring and analytics that have provided visibility to connectivity issues inside the public cloud, SaaS and third party provider environments. The examples are based on applications which are extremely sensitive to outages and delays where even a 1-second outage causes significant impact. How do we detect these failures, and what inferences can be made regarding root cause? Our goal is to provide the most reliable services to our customers, through improving the performance and availability of our services running in the cloud. **Instructor: Chris Hull, Principal Network Engineer. Capital One** Chris Hull is a network engineer and packet analysis expert, currently working network operations at Capital One. He previously worked at OPNET/Riverbed, first as a developer, and later in professional services. In OPNET, he developed and lead the STAR24 service, where they provided a quick response, guaranteed, application and network performance troubleshooting service. This experience has carried through to Capital One, where he provides network incident top-level escalation analyses and support their move to a zero datacenter footprint.

SharkFest'20 US Conference Agenda

WEDNESDAY, 15 JULY

8:00-9:00am	**KEYNOTE: Chris Sanders**
9:15-10:45am	
Basie A/A1	**15 TBA** 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!"
Andy Kirk A/B	**16 USB Analysis 101** Pretty much everyone uses USB, yet so few know how it works under the hood. This presentation explains basic concepts behind USB and how they relate to Wireshark. Getting familiar with USB on your own can be intimidating task, especially if you have no prior USB programming experience. Hopefully the talk will provide clear enough explaination so you can avoid scratching your head due to common misconceptions. Instructor: Tomasz Mon Tomasz is the author of USBPcap - a kernel driver that enables software USB capture on Windows. Tomasz is also Wireshark Core Developer and contributor to various Open Source projects (e.g. OpenVizsla USB hardware sniffer).
Julia Lee A/B	**17 Dealing with difficult protocols and captures** While many protocols are relatively easy to handle, some require extra effort to make sure they can be handled without generating too many malformed packet exceptions and incorrect dissections. 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.
11:00am-12:30pm	
Basie A/A1	**18 Analyzing Honeypot Traffic** Securing a network starts with configuring a minimal set of services and only accepting the traffic required for those services. A honeypot is configured to attract the opposite and can be used to detect and analyze potential threats. In this session we will discuss the different types of honeypots and what each type is designed for. Next we'll look at how to deploy a TCP honeypot to accept all of the traffic sent to a server on the internet and how to analyze a capture file of this. We'll examine how to use Wireshark for this as well as tools including Suricata and Zeek. What do you think will happen when we listen to all of the traffic being sent? Instructor: Tom Peterson, Sr. Technology Specialist, CloudShark Tom works at CloudShark helping bring pcap analysis to the web. Getting started with networking at 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.
Andy Kirk A/B	**19 Practical Signature Development for Open Source IDS** In Practical Signature Development for Open Source IDS, you will learn expert methods and techniques for writing network signatures to efficiently hunt and detect the greatest and most common threats facing organizations today. You will gain invaluable information and insight into the usage of modern network analysis systems to maximize your ability to detect and prevent intrusions. Open-source tools such as Suricata and Wireshark will be used to learn traffic analysis fundamentals, custom signature writing and how to test your signatures for accuracy and performance. The latest threats such as keylogger/stealers, ransomware, cryptocurrency miners, phishing attacks, malicious documents and crimeware backdoors will be used throughout the course to provide ample hands-on experience. By the end of this course, you will be able to analyze and interpret hostile network traffic to create agile rules for detection and mitigation.

	Instructors: Jack Mott and Jason Williams, Security Researchers, OISF / Proofpoint Jack Mott is a security researcher who focuses on open source solutions to detect, track and hunt malware and malicious activity. He has been a signature writer for the Emerging Threats team for several years, producing community/premium Suricata signatures to help protect networks worldwide. Jack is a strong believer in the open source mission as well as helping people and organizations solve security issues with open source solutions. Jason is a security researcher with global enterprise experience in detecting, hunting and remediating threats with open source technologies. Primarily focusing on network communications, Jason has written thousands of commercial and community Suricata rules for Emerging Threats to help defenders protect their networks.
Julia Lee A/B	**20 IPv6 security assessment tools (aka IPv6 hacking tools)** 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. 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. **Instructor: Jeff Carrell, Network Consultant, Network Conversions** Jeff Carrell is a Networking & Big Data Instructor at Hewlett Packard Enterprise and participates in course development. Jeff is a frequent industry speaker, technical writer, IPv6 Forum Certified Trainer, and prior to HPE was a network instructor and course developer to major networking manufacturers. He is a technical lead and co-author for the book, Guide to TCP/IP: IPv6 and IPv4, 5th Edition and lead technical editor on Fundamentals of Communications and Networking, Second Edition. Jeff has been in the computer industry since 1979, built his first LAN in 1986, and is a long-time user of Wireshark.
1:30-3:00pm	
Basie A/A1	**21 Troubleshooting slow networks** 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: • 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 Bring your copy of Wireshark and let's have some fun! **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.
Andy Kirk A/B	**22 Troubleshooting Cisco Software Defined Access Architectures with Wireshark** With modern network infrastructures taking away from classic layer 2 topologies, and mechanisms such as spanning tree, new troubleshooting methodologies are needed to focus on protocols such as LISP and VXLAN. This session takes a deep dive into how the call flows of the packets traverse SDA networks and how you can best leverage Wireshark to troubleshoot these scenarios. **Instructor: Josh Halley, Sr. Solution Architect, Cisco Systems**

	Josh Halley is a Senior Solution Architect within the CX Technology and Transformation Group at Cisco. Focusing on next generation validation and deployment of new features, functionality and automation.
Julia Lee A/B	**23 Give Your Bytes a name, Part I** This course provides starting point for developing dissectors and discusses strategies for developing your own dissector as well as integration of Wireshark features like expert information or reassembly. By providing a simple protocol together with an example capture, we will take you step-by-step on creating a dissector. You will learn how the dissection engine works, how reassembly is handled by Wireshark and how to best handle field names. It is a base-line for developing your own dissectors and hould act as a reference point for future dissector implementations. Instructor: Roland Knall, Wireshark Core Developer Roland is a software enthusiast with more than 20 years experience in the field of software development and architecture. For the last 10 years his main focus has been Industrial Automation and VoIP, as well as managing software development teams. He has been a Core Developer of Wireshark since 2016 with the main focus on the UI.
3:15-4:45pm	
Basie A/A1	**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 Surgeons: Drs. Bae, Blok, Bongertz, & Landström
Andy Kirk A/B	**25 Enterprise packet capture using a distributed Wireshark environment** Using Wireshark to solve users' questions often requires collecting data at network points with unrealistic means of capturing data effectively. Remote assistance can be limited in both time and knowledge. While a globally distributed Wireshark install base can help to overcome these issues, often other challenges are created. Addressing multiple (100 or more) installations of systems running Wireshark requires patching of both Wireshark and the OS. In addition, tracking hardware failures and network connections for each of these systems can also be problematic. This session's objective is to discuss deployment of potential architecture designs meant to relieve those challenges. We will discuss concepts for building a distributed Wireshark deployment with tips and tricks, lessons learned and benefits gained. Instructor: Erick Powell, ENTS, Texas Instruments Erick Powell is a senior network SME at a fortune 200 company. Areas of expertise include routing/switching, packet broker network designs, overseeing capture appliance deployments, network monitoring / management / automation / mapping and of course, packet capture analysis. With over 25 years of network experience, Erick has developed and participated in multiple open source projects and has worked with numerous vendors in resolving software bugs and product enhancements. Requested involvement in one such company's Technical Advisory Board continues due to his inherent drive to ensure tool-sets function as designed. Erick also holds exclusive membership on his company's highly respected technical expert team.
Julia Lee A/B	**26. Give Your Bytes a name, Part I** This course provides starting point for developing dissectors and discusses strategies for developing your own dissector as well as integration of Wireshark features like expert information or reassembly. By providing a simple protocol together with an example capture, we will take you step-by-step on creating a dissector. You will learn how the dissection engine works, how reassembly is handled by Wireshark and how to best handle field names. It is a base-line for developing your own dissectors and hould act as a reference point for future dissector implementations. Instructor: Roland Knall, Wireshark Core Developer

	Roland is a software enthusiast with more than 20 years experience in the field of software development and architecture. For the last 10 years his main focus has been Industrial Automation and VoIP, as well as managing software development teams. He has been a Core Developer of Wireshark since 2016 with the main focus on the UI.
5:00-6:00pm	
Basie A/A1	**27 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 it to performance of the application. **Instructor: John Pittle, Distinguished Performance Consultant, Riverbed Technology, Inc.** As a Performance Management Strategist, John helps his customers develop and execute strategies for integrating Performance Management as an IT discipline across the organization. He has been actively focused on Performance Engineering and Analysis for networks, systems, and applications since the early 90s; performance troubleshooting is his passion and joy. His packet analysis toolbox includes Wireshark (of course), as well as NetShark, AppResponse, Packet Analyzer, and Transaction Analyzer.
Andy Kirk A/B	**28 Automation TIPS & tricks Using Wireshark/tshark in Windows** 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.
Julia Lee A/B	**29 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'20 US Conference Agenda

THURSDAY, 16 JULY

8:00-9:00am	**SharkBytes**
9:15 – 10:45am	
Basie A/A1	**30 Intrusion Analysis and Threat Huntin with Suricata** In today's threat landscape, sophisticated adversaries have routinely demonstrated the ability to compromise enterprise networks and remain hidden for extended periods of time. In Intrusion Analysis and Threat Hunting with Suricata, you will learn how to dig deep into network traffic to identify key evidence that a compromise has occurred, learn how to deal with new forms of attack, and develop the skills necessary to proactively search for evidence of new breaches. We will explore all phases of adversary tactics and techniques - from delivery mechanisms to post-infection traffic and data exfiltration to get hands-on analysis experience. Open-source tools such as Suricata, Moloch and Kibana will be utilized to generate data, perform exhaustive traffic analysis, and develop comprehensive threat hunting strategies. By the end of this course, you will have the knowledge and skills necessary to discover new threats in your network and build an effective threat hunting program. **Instructor: John Stroschein and Jack Mott, Open Information Security Foundation** Josh is an experienced malware analyst and reverse engineer who has a passion for sharing his knowledge with others. He is the Director of Training for OISF, where he leads all training activity for the foundation and is also responsible for academic outreach and developing research initiatives. Josh is an accomplished trainer, providing training in the aforementioned subject areas at BlackHat, DerbyCon, Toorcon, Hack-In-The-Box, Suricon and other public and private venues. Josh is an Assistant Professor of Cyber Security at Dakota State University where he teaches malware analysis and reverse engineering, an author on Pluralsight, and a threat researcher for Bromium. Jack Mott is a security researcher who focuses on open source solutions to detect, track and hunt malware and malicious activity. He has been a signature writer for the Emerging Threats team for several years, producing community/premium Suricata signatures to help protect networks worldwide. Jack is a strong believer in the open source mission as well as helping people and organizations solve security issues with open source solutions.
Andy Kirk A/B	**31 Introduction to WAN Optimization Wireshark (Part 1)** **Instructor: John Pittle, Distinguished Performance Consultant, Riverbed Technology, Inc.** As a Performance Management Strategist, John helps his customers develop and execute strategies for integrating Performance Management as an IT discipline across the organization. He has been actively focused on Performance Engineering and Analysis for networks, systems, and applications since the early 90s; performance troubleshooting is his passion and joy. His packet analysis toolbox includes Wireshark (of course), as well as NetShark, AppResponse, Packet Analyzer, and Transaction Analyzer.
Julia Lee A/B	**32 Will it packet? Capturing non-traditional packets when you don't have a NIC** Not everything that generates packets has a NIC, drivers, or an easy way to capture and analyze their communication - but with some inexpensive hardware you can start looking at packets from non-traditional devices like thermometers, power meters, and even airplanes! A look into software defined radio, flexible hardware radios, and connecting esoteric data to tools like Wireshark and Kismet. **Instructor: Mike Kershaw, Wi-Fi Hacker, Kismet Wireless** 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.
11:00am – 12:30pm	
Basie A/A1	**33 Trace File Case Files – How to analyze network issues 101** **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.
Andy Kirk A/B	**34 Introduction to WAN Optimization (part 2)** Instructor: John Pittle, Distinguished Performance Consultant, Riverbed Technology, Inc. As a Performance Management Strategist, John helps his customers develop and execute strategies for integrating Performance Management as an IT discipline across the organization. He has been actively focused on Performance Engineering and Analysis for networks, systems, and applications since the early 90s; performance troubleshooting is his passion and joy. His packet analysis toolbox includes Wireshark (of course), as well as NetShark, AppResponse, Packet Analyzer, and Transaction Analyzer.
Julia Lee A/B	**35 IPv6: Build Your Own Lab Workshop, Part I** The IPv6: Build Your Own Lab Workshop is a hands-on workshop intended for IT professionals, architects, engineers, developers, and technicians, who want to obtain hands-on exposure with IPv6. Instructor: Jeff Carrell, Network Consultant, Network Conversions Jeff Carrell is a Networking & Big Data Instructor at Hewlett Packard Enterprise and participates in course development. Jeff is a frequent industry speaker, technical writer, IPv6 Forum Certified Trainer, and prior to HPE was a network instructor and course developer to major networking manufacturers. He is a technical lead and co-author for the book, Guide to TCP/IP: IPv6 and IPv4, 5th Edition and lead technical editor on Fundamentals of Communications and Networking, Second Edition. Jeff has been in the computer industry since 1979, built his first LAN in 1986, and is a long-time user of Wireshark.
1:30-3:00pm	
Basie A/A1	**36 Packet Command Line Foo** 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.
Andy Kirk A/B	**37 Improving Packet Capture in the DPDK - Speed, useability, and saving sharks** The Dataplane Development Kit (DPDK) is a software library widely used to build network applications and appliances. It supports a limited version of packet capture using pcap but it is low performance and hard to use. This talk will focus on ongoing work to improve usability, performance and internal interfaces. The new version supports pcapng and BPF filtering and is designed to get the performance of DPDK with the usability of tshark tool set. Instructor: Stephen Hemminger, Team Leader Azure Networking, Microsoft Stephen has been active in development of the Linux kernel and userspace networking solutions since 2005. He is maintainer of the Linux iproute2 utilities and member of the DPDK Technical Board. Stephen has written many network drivers for both Linux and in userspace including netem, vxlan, and Hyper-V devices. Many of his contributions have involved integrating so many different networking pieces that he decided to give himself the title of Network Plumber.
Julia Lee A/B	38 **IPv6: Build Your Own Lab Workshop, Part II** The IPv6: Build Your Own Lab Workshop is a hands-on workshop intended for IT professionals, architects, engineers, developers, and technicians, who want to obtain hands-on exposure with IPv6.

	Instructor: Jeff Carrell, Network Consultant, Network Conversions Jeff Carrell is a Networking & Big Data Instructor at Hewlett Packard Enterprise and participates in course development. Jeff is a frequent industry speaker, technical writer, IPv6 Forum Certified Trainer, and prior to HPE was a network instructor and course developer to major networking manufacturers. He is a technical lead and co-author for the book, Guide to TCP/IP: IPv6 and IPv4, 5th Edition and lead technical editor on Fundamentals of Communications and Networking, Second Edition. Jeff has been in the computer industry since 1979, built his first LAN in 1986, and is a long-time user of Wireshark.
3:15-4:45pm	
Basie A/A1	**39 A walkthrough of the SharkFest Group & Individual Packet Challenges** Instructor: Sake Blok, Jasper Bongertz & Christian Landstrom
Andy Kirk A/B	40 **The other protocols (used in LTE) - the other Layer 4 protocol SCTP, as well as 3GPP based GTP, and Diameter** This session will walk attendees through multiple LTE, VoLTE, flows and failures to demonstrate how Wireshark can assist with protocols like S1AP, GTP, and Diameter. Also how to get through the large datasets that 5G produces in order to troubleshoot individual flow issues. Instructor: Mark Stout, Mobile Support Engineer, Sprint Design, and Tech Support in Code Division Multiple Access (CDMA) and Long-Term Evolution (LTE) mobile networks, and now 5G for the last 21 years, in multiple countries. Active contributor to 3rd Generation Partnership Project (3GPP) 23, and 29 series. Currently the Lead Support Engineer for Sprint's LTE, Voice Over LTE (VoLTE), Internet of Things (IoT),and true 5G technology on the Packet Core network.
Julia Lee A/B	**41 BACNet and Wireshark for Beginners** BACnet, the ASHRAE building automation and control networking protocol, is a most exciting one to study. This session is a step forward in providing basic details of the protocol itself, which can leave technical staff in the dark when they haven't a clue what's going on with the bits on the wire and these kind of communications. Troubleshooting these kinds of protocols with Wireshark provides a chance to apply the analyser in a way that allows you to gain a solid and lasting knowledge of packet analysis techniques. Instructor: Werner Fischer, Infrustructure Manager, avodaq AG Werner has been an active and avid SharkFest supporter for many years, serving the community in various locations around the globe - Singapore, USA, and Europe – by using and teaching the same tool at each stop - Wireshark. That's Werner. Werner is also a long-term Dual-CCIE (R/S, Security) with over 20 years of experience in the networking arena. At avodaq, Werner works as a Manager Infrastructure on System Architectures.