SharkFest'20 Virtual Agenda

Online.
All times are in Pacific Daylight Time zone.
Conference days run from 8:00am PDT/5:00pm CET through 6:00pm PDT/3:00am CET

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

SharkFest'20 Virtual Conference Agenda

Pre-Conference Courses

Pre-Conference Class I	Monday 12 October 2020	
Troubleshooting with Wireshark – Core Skills	8:00am PDT/5:00pm CET - 5:00pm PDT/2am CET	
INSTRUCTOR Chris Greer	**Tuesday 13 October 2020**	
	8:00am PDT/5:00pm CET - 5:00pm PDT/2:00am CET	

Pre-Conference Class II	Wednesday 14 October 2020	
Wireshark Profiles – How to Analyze Trace Files Faster and Easier	8:00am PDT/5:00pm CET - 5:00pm PDT/2:00am CET	
INSTRUCTOR Betty DuBois		

Pre-Conference Class III	Wednesday 14 October 2020	
SSL/TLS Troubleshooting with Wireshark	8:00am PDT/5:00pm CET - 5:00pm PDT/2:00am CET	
INSTRUCTOR Sake Blok		

SharkFest'20 Virtual Conference Agenda

Thursday, October 15, 2020

8:00-9:00am	**KEYNOTE: "*Latest Wireshark Developments & Road Map*"** **Gerald Combs & Friends**	
	Zoom 1	**Zoom 2**
9:30-10:30	**01** **BACNet and Wireshark for Beginners** Werner Fischer	**02** **Going down the retransmission hole** Sake Blok
10:30-10:45	**Q & A**	
10:45-11:00	**BREAK**	
11:00am-12:00pm	**03** **IPv6 security assessment tools (aka IPv6 hacking tools)** Jeff Carrell	**04** **Improving packet capture in the DPDK** Stephen Hemminger
12:00-12:15	**Q & A**	
12:15-12:45	**LUNCH**	
12:45-1:45pm	**05** **Kismet and Wireless Security 101** Mike Kershaw	**06** **Back to the Packet Trenches** Hansang Bae
1:45-2:00	**Q & A**	
2:00-2:15	**BREAK**	
2:15-3:15	**07** **TLS encryption and decryption: What every IT engineer should know about TLS** Ross Bagurdes	**08** **Why an Enterprise Visibility Platform is critical for effective Packet Analysis?** Keval Shah
3:15-3:30	**Q & A**	
3:30-3:45	**BREAK**	
3:45-4:45	**09** **Troubleshooting Cloud Network Outages** Chris Hull	**10** **TCP SACK overview & impact on performance** John Pittle
4:45-5:00	**Q & A**	
5:00-5:15	**BREAK**	
5:15-6:15	**11** **Automation TIPS & tricks Using Wireshark/tshark in Windows** Megumi Takeshita	**12** **How long is a packet? And does it really matter?** Dr. Stephen Donnelly
6:15-6:30	**Q&A**	

SharkFest'20 Virtual Conference Agenda

Friday, 16 October 2020

8:00-9:00am	**Keynote: Vern Paxson, Professor of EECS, UC Berkeley/ Chief Scientist, Corelight, Inc.**	
	Zoom 1	**Zoom 2**
9:30-10:30	**13** **Make the bytes speak to you** Roland Knall	**14** **USB Analysis 101** Tomasz Moń
10:30-10:45	**Q & A**	
10:45-11:00	**BREAK**	
11:00-12:00	**15** **TLS debugging (title subject to change)** Peter Wu	**16** **The Packet Doctors are in! Packet trace examinations with the experts** Drs. Bae, Blok, Bongertz, & Landström
12:00-12:15	**Q & A**	
12:15-12:45	**LUNCH**	
12:45-1:45	**17** **Analyzing Honeypot Traffic** Tom Peterson	**18** **Intrusion Analysis and Threat Hunting with Suricata** Josh Stroschein || Jack Mott
1:45-2:00	**Q & A**	
2:00-2:15	**BREAK**	
2:15-3:15	**19** **The other protocols (used in LTE)** Mark Stout	**20** **Practical Signature Development for Open Source IDS** Jack Mott || Jason Williams
3:15-3:30	**Q & A**	
3:30-3:45	**BREAK**	
3:45-4:45	**21** **Ostinato - craft packets, generate traffic** Srivats P	**22** **Introduction to WAN Optimization** John Pittle
4:45-5:00	**Q & A**	
5:00-5:15	**BREAK**	
5:15-6:15	**23** **Solving Real World Case Studies** Kary Rogers	**24** **Analyzing 802.11 Powersave Mechanisms with Wireshark** George Cragg
6:15-6:30	**Q&A**	

SharkFest'20 Virtual Conference Agenda

THURSDAY, 15 OCT – THIS SECTION TO BE UPDATED SOON

8:00-9:00am	**KEYNOTE*: Latest Wireshark Developments & Road Map*** **Gerald Combs & Friends**
9:30-10:30	
	01 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, Infrastructure 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.
	02 Going down the retransmission hole During the analysis of one problem, I noticed some strange behavior (unrelated to what I was investigating). There were TCP retransmissions that did not make sense to me. Showing the (anonimized) traces to some usual suspects at Sharkfest'19 did not result in a logical explanation either. So I put on my detective hat and started to investigate. I detected the same retransmission pattern on many Windows servers, also with different OS versions. So I created a case with the Microsoft Windows Networking support team. It took about 6 months to get to the bottom of this case and ended in two confirmed bugs in the Windows Server TCP implementation. During this talk I will take you along on the long journey that resulted in these two bugs and teach you about Microsofts TCP templates along the way. Hold tight while we go... down the retransmission hole! **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.

SharkFest'20 Virtual Conference Agenda

11:00am-12:00pm	
	03 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.
	04 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.
12:45-1:45pm	
	05 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.
	06 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, Netspoke** Hansang Bae led the Network/Application Performance Engineering Team with direct responsibility for Packet Capture Infrastructure at Citi until July, 2012. Since then he has been the CTO for Riverbed and currently works as Field CTO of Netskope. With his broad knowledge of protocol analysis in a complex enterprise infrastructure, Hansang brings a unique perspective to packet analysis.

SharkFest'20 Virtual Conference Agenda

2:15-3:15pm

07 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 a 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.

08 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.

3:45-4:45pm

09 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, Distinguished 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.

	10 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.
5:15-6:15pm	
	11 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.
	12 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.

SharkFest'20 Virtual Conference Agenda

FRIDAY, 16 OCT

8:00-9:00am	KEYNOTE: Vern Paxson, Professor of EECS, UC Berkeley/ Chief Scientist, Corelight, Inc.
9:30-10:30am	
	13 Make the bytes speak to you In this session, you will take a look at how dissection is organized in Wireshark's engine and how to write your first dissector. Also includes a few pointers on how to organize your protocols, what good practices are and where to go next 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.
	14 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 explanation 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).**
11:00am-12:00pm	
	15 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
	16 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
12:45-1:45pm	
	17 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.

18 Intrusion Analysis and Threat Hunting 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.

2:15-3:15

19 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.

20 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.
3:45-4:45pm	
	21 Ostinato - craft packets, generate traffic What is Ostinato? Think of it as Wireshark in Reverse. Wireshark takes a packet and dissects it into protocol headers and protocol fields. Ostinato takes protocol headers and fields to create a packet. But it's not just a pcap editor or replayer. It's much more. It's a comprehensive tool for network engineers to test and troubleshoot networks. In this session, Ostinato author, Srivats P will introduce you to the architecture, capabilities and features of Ostinato. **Instructor: Srivats P, Creator and Developer of Ostinato** Srivats P is the creator and developer of Ostinato which is a personal project. In his day job, he works as a data plane developer at a leading networking vendor and has developed L2/L3 software for a broad spectrum of devices fom home routers to DSLAMs to edge and core routers over his career spanning more than 20 years.
	22 Introduction to WAN Optimization Wireshark **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.
5:15-6:15pm	
	23 Solving Real World Case Studies Kary helps strangers on the internet solve their application and network issues with packet analysis. These are their stories. **Instructor: Kary Rogers, Director, Staff Engineering, Riverbed Technology** Kary first learned the value of packet analysis helping customers solve difficult issues in Riverbed TAC, and has since moved onto a management role for the company. Not wanting to lose the skills he fought hard to learn, he started a packet analysis website, PacketBomb.com, where he posts tutorials and case studies for the hapless network engineer struggling to prove that it's not the network
	24 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.