SharkFest'21 Virtual US

AGENDA

(Draft, subject to change)

All times are in the
Pacific Daylight time zone.
Conference days run from:
8:00am through 6:00pm

- **Pre-Conference Classes**
- **SharkFest'21 Virtual Session Agenda**
- **Session Abstracts & Instructor Bios**

SharkFest'21 Virtual US Conference Agenda

Pre-Conference Classes

Sunday and Monday, September 12 & 13	
September 12 & 13 9:00 – 5:00	**Pre-Conference Class I** **Network Analysis and TCP Deep Dive with Wireshark** **INSTRUCTOR: Chris Greer** **For Class Description and Outline, please visit:** **https://sharkfestus.wireshark.org/register**
Tuesday, September 14	
9:00 – 5:00	**Pre-Conference Class II** **Next Generation Protocols** **&** **Advanced Network Analysis** **INSTRUCTOR: Phil Shade** **For Class Description and Outline, please visit:** **https://sharkfestus.wireshark.org/register**
Wednesday September 15	
9:00 – 5:00	**Pre-Conference Class III** **Analyzing Pcaps Faster with Filters** **INSTRUCTOR: Betty DuBois** **For Class Description and Outline, please visit:** **https://sharkfestus.wireshark.org/register**

SharkFest'21 Virtual US Conference Agenda

Thursday, September 16		
8:00-9:00	KEYNOTE: "*Latest Wireshark Developments & Road Map*" Gerald Combs & Friends	
9:00-9:15	BREAK	
9:15-10:15	**Zoom 1** **01** **Analyzing DNS from the Server Perspective** Betty DuBois	**Zoom 2** **02** **Network Forensics Analysis** Rami Al-Talhi
10:15-10:30	Q & A	
10:30-10:45	BREAK	
10:45-11:45	**03** **Visualizing TLS Encryption – making sense of TLS in Wireshark** Ross Bagurdes	**04** **Analyzing Megalodon Files** Jasper Bongertz
11:45-12:00	Q & A	
12:00-12:30	LUNCH	
12:30-1:30	**05** **Hello, what's your name?** **An overview of Wireshark's name resolution options (and it is not only for IP addresses!)** Sake Blok	**06** **Wireshark in use on LTE and 5G networks** Mark Stout
1:30-1:45	Q & A	
1:45-2:00	BREAK	
2:00-3:00	**07** **Intro to QUIC - The TCP Killer?** Chris Greer	**08** **Network Forensic Case Studies: Those Who Don't Learn from the Past Are Doomed to Repeat It** Phill Shade
3:00-3:15	Q & A	
3:15-3:30	BREAK	
3:30-4:30	**09** **Looking For "Packets" in all the "Right" Places** Patrick Kinnison	**10** **Back to the Packet Trenches** Hansang Bae
4:30-4:45	Q & A	
4:45-5:00	BREAK	
5:00-6:00	**11** **School from home: Watching the Wire with Wireshark** Anthony Efantis	**12** **Wireshark and Enterprise Packet Capture** Stephen Donnelly
6:00-6:15	Q & A	

SharkFest'21 Virtual US Conference Agenda

Friday, September 17		
8:00-9:00	**KEYNOTE: Steve McCanne, Coding CEO, Brim**	
9:00-9:15	**BREAK**	
	Zoom 1	**Zoom 2**
9:15-10:15	**13** **Analysis and Troubleshooting of IPsec VPNs** Jean-Paul Archier	**14** **How smart are my "things"? A traffic analysis of IoT Devices** Simone Mainardi
10:15-10:30	**Q & A**	
10:30-10:45	**BREAK**	
10:45-11:45	**15/16** **The Packet Doctors are in! Packet trace examinations with the experts** Drs. Blok, DuBois, Greer and Rogers	
11:45-12:00	**Q & A**	
12:00-12:30	**LUNCH**	
12:30-1:30	**17** **When it's NOT a "Network Problem" – Identifying Higher-Layer Issues in Packet Data** Wes Morgan	**18** **Intrusion Analysis and Threat Hunting with Suricata** Josh Stroschein and Peter Manev
1:30-1:45	**Q & A**	
1:45-2:00	**BREAK**	
2:00-3:00	**19** **How I Learned to Stop Worrying and Love the PCAP** Kary Rogers	**20** **Build Your Own IPv6 Learning Lab – for FREE (part 1)** Jeff Carrell
3:00-3:15	**Q & A**	
3:15-3:30	**BREAK**	
3:30-4:30	**21** **TCP SACK overview & impact on performance** John Pittle	**22** **Build Your Own IPv6 Learning Lab – for FREE (part 2)** Jeff Carrell
4:30-4:45	**Q & A**	
4:45-5:00	**BREAK**	
5:00-6:00	**23** **Wireshark and WiFi: capture techniques and challenges** George Cragg	**24** **Capturing goodies: Wireshark on iPad pro and utilization of extcap interfaces** Megumi Takeshita
6:00-6:15	**Q & A**	
6:15-6:20	**BREAK**	
6:20-6:50	**Closing Remarks and CTF Winners Announcement**	

SharkFest'21 Virtual US Conference Agenda

Session Abstracts & Instructor Bios

(DRAFT - UPDATED FREQUENTLY)

THURSDAY, SEPTEMBER 16

8:00-9:00

KEYNOTE*: Latest Wireshark Developments & Road Map*
Gerald Combs & Friends

9:15-10:15

01 Analyzing DNS from the Server Perspective

Almost every application depends on DNS name resolution. Nobody wants to memorize IP addresses. You are probably familiar with how DNS works from the client side. Maybe you've even captured your own traffic to see it. But what about the server side? How does DNS really work, and how does it look in Wireshark? We will investigate the following topics in this session:

- Recursion
- Record Types
- Redirects
- Zone Transfers

You can't troubleshoot what you don't see, and you can't secure what you don't understand. See it all in Wireshark. Pcaps & Profiles will be made available before the session so you can follow along.

Instructor: Betty DuBois, Chief Detective, Packet Detectives
Betty is the Chief Detective for Packet Detectives, and has been solving mysteries since 1997. She troubleshoots the root cause of network and/or application issues. Experienced with a range of hardware and software solutions, she captures the right data, in the right place, and at the right time. Using packets to solve crimes against the network and applications, is her passion. Teaching others how to do the same, is her calling.

02 Network Forensics Analysis 

Advanced Persistent Threat (APT) groups do not like to have the evidence of their crime into their targets, usually, they would develop or use file-less malware to not leave any fingerprints traces proof their crime and unleashed their operations. Network forensics analysis became an essential skills to uncover APTs operation and identify what has happened by utilizing Wireshark and other open-source tools to analyze network packet captures (PCAP). In this lecture, we will introduce couple of APT attack scenarios and walk-through how to analyze them.

Instructor: Rami Al-Talhi
Rami has experience across different information security and cybersecurity fields for over 12 years. Worked as Incident Response Expert in the past for four years to handle different cyber incident and events. Provided DFIR and Cyber Range training for different regions in the world (Europe, Asia, Middle East and US). Dealt with different sophisticated APT cyber incident cases that ranging from cyber espionage until data destruction.

10:45-11:45

03 Visualizing TLS Encryption - making sense of TLS in Wireshark 

In this beginner level talk, you will learn the essentials of TLS encryption. We will start with a brief history of TLS which will both introduce the main concepts as well as provide the necessary vocabulary to understand the protocol. Then we will offer a visualization of TLS encryption to understand the encryption process, which will be valuable when we examine a Wireshark Capture of TLS encrypted packets. Then we will walk through how to capture session keys, decrypt traffic, and analyze the protocols being carried with TLS. You will leave this talk with a great visual to imagine TLS encryption, as well as everything you need to decrypt and examine TLS encryption.

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.

04 Analyzing Magalodon Files

In most cases, analysts are working with small files, often no more than a few Megabytes. Those kind of files are easily loaded into Wireshark, and filters and everything else works quickly enough to not slow the analyst down in the search for problems. But what happens when you suddenly have to work with Gigabytes, or even Terabytes of pcaps? Everything takes longer, and whatever the problem is, just loading all files into Wireshark isn't going to work. So different techniques are required, and this talk will go into how to "divide and conquer" the pcaps in a situation like that.

Instructor: Jasper Bongertz, Principal Network Security Specialist, G Data Advanced Analytics GmbH

Jasper started working freelance in 1992 while he was studying computer science at the Technical University of Aachen. In 2009, Jasper became a Senior Consultant and trainer for Fast Lane, where he created a large training portfolio with a special focus on Wireshark and network hacking. In 2013, he joined Airbus CyberSecurity, focusing on IT security, Incident Response and Network Forensics, and moving on to become the Principal Network Security Specialist at G Data Advanced Analytics in August of 2019. Jasper is the creator of the packet analysis tool "TraceWrangler", which can be used to convert, edit and sanitize PCAP files. His blog regarding network analysis, network forensics and general security topics can be found at blog.packet-foo.com.

12:30-1:30

05 Hello, what's your name? An overview of Wireshark's name resolution options (and it is not only for IP addresses!)

There is a lot of data being displayed by Wireshark, some of the data can be associated with names. There can even be multiple sources for the name resolution process and it is not always clear how to properly use all the name resolution options. What are the pros and cons of each method and how do they work together. This session will shine a light on the different ways that Wireshark can translate numbers into names. We will look at the resolving of mac-addresses, IP/IPv6 addresses, port numbers, vlan IDs, SNMP OIDs and GeoIP information.

Instructor: Sake Blok, Relational Therapist for Computer Systems

Sake has been analyzing 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 analyzer 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.

06 Wireshark in use on LTE and 5G networks

Will walk through multiple examples for Wireshark's use in 4G, and 5G networks to solve real problems. Beginning with a brief overview of 4G, and 5G network connectivity, and interfaces. Followed by examples of traces on those interfaces.

Instructors: Mark Stout, Principle Enginner, T-Mobile

Mark is Principle Engineer for T-Mobile, focused on 4G, and 5G EPC nodes. He served as one of the first members to launch Sprints LTE service in 2009, and support 5G standalone today. Authored 3GPP contributions for the 23, and 29 series.

2:00-3:00

07 Intro to QUIC - The TCP Killer?

It's 2021 - QUIC has formally arrived as an RFC, but it has been here for years. You capture traffic to Google, YouTube, Facebook, Cloudflare, and many other services and no longer see TCP as the primary transport protocol. Yes, QUIC over UDP is here, and it is growing. Some even tout it as a "TCP Killer". No matter what our role within IT, QUIC is a protocol we should familiarize ourselves with. Let's take a dive into QUIC and learn about this rapidly-expanding transport protocol.

Instructor: Chris Greer, Network Analyst, Packet Pioneer

Chris Greer is a Network Analyst for Packet Pioneer. He has worked with companies around the world, helping them to solve pesky network problems at the packet level, primarily with Wireshark and other open-source tools. Chris has a passion for helping others to learn about packet

analysis and teaches Wireshark Courses to private companies as well as public audiences. You can follow him on his YouTube channel at - https://www.youtube.com/user/packetpioner

08 Network Forensic Case Studies - Those Who Don't Learn from the Past Are Doomed to Repeat It

History repeats itself" is an often-used quote that is especially relevant in this age of increasing cyber events and Intrusions... With the rise of Web 2.0 and the increasing sophistication of cyber intrusions to the rising specter of cyberwar, many network security professionals lose sight of the simple tricks that underlie many of the common hacking techniques. In this presentation, we will cover four network forensics case studies drawn from the real world and the presenter's experience to illustrate that what's old is, in fact, new again.

Instructor: Phill Shade, Owner, Merlion's Keep Consulting

Phill "Sherlock" Shade is a Senior Network / Forensics Investigator and founder of Merlion's Keep Consulting, specializing in all aspects of Network and Forensics Analysis. He is an internationally recognized Network Security and Forensics expert, drawing from his over 30 years of hands-on, real world experience. A member of the Global Cyber Response Team (GCRT), FBI InfraGard, Computer Security Institute, the IEEE and Volunteer at Cyber Warfare Forum Initiative, he is a frequent consultant for numerous international security, technology and government agencies.

3:30-4:30

09 Looking For "Packets" in all the "Right" Places

Knowing where to capture and how to capture packets on many different platforms can be a challenge. Wireshark is packed full of tools and tricks to help you focus on the "Right" information and get clean captures to analyze. This session takes a deeper look at how to setup Wireshark and various 3rd Party vendors to get the "Right" information in your trace files.

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.

10 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, Field 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.

5:00-6:00

11 School from home. Watching the Wire with Wireshark

Since the pandemic has forced us all to work from home, and our kids to attend school virtually from home, naturally I wanted to take a peek at what was going through my home network. I discovered some traffic exchanged in clear text that gave insight into the content filtering on the school's Chromebooks. I started man-in-the-middling some of that traffic to learn what could be leveraged to bypass the content filtering. This lead to learning about PAC files, proxies and HTTP traffic handling.

Instructor: Anthony Efantis, Principal Network Engineer at Sealing Teach

Tony E. holds many industry certifications including: CCIE# 64908, GNFA, PCNSA & SEC+. He maintains a blog @ https://showipintbri.github.io and is the co-host on the Network Collective podcast and live stream: https://networkcollective.com . He enjoys participating in packet hacking challenges and CTF's at security conferences.

12 Wireshark and Enterprise Packet Capture

What motivates packet capture in Enterprise, and how applicable is Wireshark? We discuss the differences between on-demand, smart, and continuous packet capture strategies, and the practical techniques required. Performing and managing capture at large scale has its own challenges, and produces prodigious amounts of data. How can we find what we are looking for in huge packet trace datasets, and can Wireshark help?

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'21 Virtual US Conference Agenda

FRIDAY, SEPTEMBER 17

8:00-9:00

KEYNOTE: Steve McCanne, Coding CEO, Brim
The Zed Project: Stumbling Upon a New Data Model for Search and Analytics while Hacking Packets

8:00-9:00

Keynote: The Zed Project: Stumbling Upon a New Data Model for Search and Analytics while Hacking Packets
If you've ever tried to assemble operational infrastructure for search and analytics of network-oriented traffic logs, you know what a daunting task this can be. About three years ago, we embarked upon a project to explore search and analytics for Zeek and Suricata "sensors" running on live network taps or over archived PCAP files. Having experimented extensively with well-known, open-source search and analytics systems and after talking to a wide range of practitioners of such tech stacks, we noticed a recurring design pattern: a search cluster is often deployed to hold recent logs for interactive queries, while some sort of data lake is deployed in parallel to hold historical data for batch analytics.

We wondered if this bifurcation between search and analytics was fundamental or if we could tackle this problem with a different approach. We eventually concluded these silos arose at least in part from the bifurcation of the underlying data models themselves: search systems typically use the schemaless model of JSON while analytics systems use more structured formats like Parquet, enforcing one-or-the-other design decisions.

In this talk, I'll describe a new data model called Zed --- designed to unify the document model of JSON with the relational model of SQL databases --- where our ultimate goal is to converge search and analytics. I will then discuss how we've leveraged the Zed data model in a new query engine that operates over Zed data instead of JSON objects
or relational tables and admits a new query language that is a superset of SQL and log-search style languages. Finally, I'll outline our "work in progress" adapting the Zed system to a git-like data lake for cloud storage -- called a Zed lake --- providing time travel, live ingest, search indexes, and transactionally consistent views across distributed workers.

Speaker: Steve McCanne, Coding CEO, Brim
Steve McCanne is the "Coding CEO" at Brim, a small startup working on the open-source Zed Project and a new application called "Brim" that leverages Zed. Back in the days before the Web, Steve worked at the Lawrence Berkeley National Laboratory where he developed BPF, libpcap, the PCAP file format, and the tcpdump language and compiler,
while also working on the Real-time Transport Protocol (RTP) for Internet video when the telcos claimed that real-time Internet communication was impossible without end-to-end virtual-circuit guarantees. (Guess who was right?) After a brief stint in academia in the late '90s, Steve crossed over to the dark side, became a tech entrepreneur, and never looked back. He has founded several startups and took his '02 company and Sharkfest's sponsor, Riverbed, public in '06. After many years working in other areas of tech, Steve has returned to his roots, dabbling again with PCAPs, leading him to Zed and a whole new approach to network and IT observability data.

9:15-10:15

13 Analysis and troubleshooting of IPsec VPNs
With this session we intend to demonstrate how Wireshark can be used to analyze IPSec VPNs in site to site and remote access contexts. We will also present some dysfunctioning cases where Wireshark can be of some help.

Instructor: Jean-Paul Archier, Consultant and Trainer, JPACONSEIL
Jean-Paul has been working as a System and Network Engineer for more than 30 years. Since 2010, he has run his own company and is mainly focused on network training and consultancy. He is the author of several books for the French publisher ENI: VPN, IPv6, Cisco ASA, Postfix. He regularly gives training sessions on Wireshark and other network-related topics. Recently, a European VOIP Solution Provider asked him to build and dispense Wireshark training sessions for its resellers, focused specifically on SIP troubleshooting. As a certified trainer, he also delivers training about VPNs and network security for WatchGuard resellers and clients.

14 How Smart Are My "Things"? A Traffic Analysis of IoT Devices

The Internet of Things (IoT) is quickly becoming a relevant part of our everyday life. This opens up to a series of implications as IoT devices are in general low-cost, weakly-secured devices able to create shortcuts between the Internet and our private networks.

In this session we will focus on the behavior of a group of IoT devices operated on a testbed network. We will use Wireshark to analyze more than one month worth of packets to investigate their activities in the short- and in the long-run.By the end of this session, you will learn the protocols used by IoT devices to communicate and upgrade themselves. Eventually, you will gain enough awareness to understand the implications of operating IoT devices in a personal or industrial environment, to avoid trading automation and control for privacy and security.

Instructor: Simone Mainardi, Senior Data Scientist, ntop

Simone Mainardi received his BSc, MSc and PhD degrees in Computer Science from the University of Pisa, Faculty of Information Engineering. He worked as a research associate both at the University of Pisa and at the Institute for Informatics and Telematics (IIT) of the Italian National Research Council (CNR). He is now with ntop as a Senior Software Developer. He is interested in computer networking, parallel and distributed algorithms, Internet measurements and data analysis.

10:45-11:45

15 & 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 prior to SharkFest and only given to the panel members 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 SEND PERPLEXING TRACE FILES FOR ANALYSIS BY THE PANEL TO jasper@packet-foo.com PRIOR TO SHARKFEST!

12:30-1:30

17 When It's NOT a "Network Problem" - Identifying Higher-Layer Issues in Packet Data

While most professionals view packet captures as necessary only when investigating potential "network problems", one can often use packet data to draw important inferences and conclusions about conditions at higher layers of the OSI stack. In our time together, we'll walk through multiple examples of problems that were initially diagnosed through packet/protocol analysis, even though their ultimate root causes were found in the upper layers of the stack. We'll also talk about customizing Wireshark's look-and-feel to give you a better perspective on "what's going on up there". You'll leave this session with a better understanding of just how far packet analysis can REALLY take you in problem determination and performance analysis.

Instructor: Wes Morgan

Wes has been around computing and networks for 40+ years, with most of that time spent as either a systems administrator or software support engineer. Along the way, he became a full-stack troubleshooter, tracking down environmental glitches in customer environments around the world. He has seen almost every form of "blame the network" that mankind has invented. Wireshark has been a part of his everyday toolkit since the days of Ethereal 0.4 (or thereabouts).

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.

Instructors: Josh Stroschein, Director of Training and Peter Manev, QA/Trainer, 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.

Peter has been involved with Suricata IDS/IPS/NSM from its very early days in 2009 as QA lead, currently a Suricata executive council member. Peter has 15 years experience in the IT industry, including enterprise and government level IT security practice. As an adamant admirer and explorer of innovative open source security software he is also one of the creators of SELKS - an open source threat detection security distro. He is also one of the founders of Stamus Networks, a company providing security solutions based on Suricata.

SharkFest'21 Virtual US Conference Agenda

2:00-3:00

19 How I Learned to Stop Worrying and Love the PCAP

Everyone knows the packets don't lie but opening a pcap can be overwhelming if you're new to Wireshark. In this session we'll start from the very beginning of narrowing down the problem to setting up Wireshark to looking for the problem. This is a hands on session with quizzes and exercises along the way.

In this session, you'll learn what to do before you ever fire up Wireshark. We'll go over how to narrow down a problem so it's less overwhelming. How to understand the problem better than the people who are reporting it. If you define the problem specifically, the analysis is so much easy later. We'll cover how to verify you have the data you need and how to setup Wireshark to increase your chance of success. Then we'll begin analysis and try to find the issue. At the start, you'll download pcaps and follow along as we try to find why a web page is loading slowly.

Instructor: Kary Rogers, Senior Director of Services Excellence, ZScaler
Kary has spent many years solving difficult system, network, and application problems by looking at the packets. Even though he's been in management for a while, he still occasionally finds himself chasing the high of unraveling a packet mystery. He has a YouTube channel called PacketBomb where he posts Wireshark videos or has a live stream with your favorite packeteers.

20 Build Your Own IPv6 Learning Lab – for FREE (Part 1)

Many of us have either been there or are there, wanting to obtain/gain more technical knowledge and proficiency in IPv6. One of the stumbling blocks in this process has traditionally been access to equipment to do so. Over the more recent years, building a virtual lab has helped us tremendously in this problem, but we still have to work within the boundaries of budget.

This session is about building a no-cost virtual lab environment specifically targeted to gain experience on IPv6.

We will cover one specific process of building an IPv6 lab system based on a virtual machine platform, on both Windows and Linux hosts. The core of the system will be based on a "community version" software router for "real" IPv6 routing scenarios, have multiple network segments and multiple client OS's. In addition, Wireshark will be used to view specific IPv6 protocol components and verify IPv6 operations.

Instructor: Jeff Carrell, Networking & Big Data Instructor/Course Developer, Hewlett Packard Enteprise
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.

3:30-4:30

21 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, Services CTO, Riverbed Technology, Inc.
As an IT Performance Management Strategist, John helps his customers develop and execute strategies for integrating Performance Management as an IT discipline across their organizations. He has been actively focused on Performance Engineering and Analysis best practices 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.

22 Build Your Own IPv6 Learning Lab – for FREE (Part 2)

Many of us have either been there or are there, wanting to obtain/gain more technical knowledge and proficiency in IPv6. One of the stumbling blocks in this process has traditionally been access to equipment to do so. Over the more recent years, building a virtual lab has helped us tremendously in this problem, but we still have to work within the boundaries of budget.

This session is about building a no-cost virtual lab environment specifically targeted to gain experience on IPv6.

We will cover one specific process of building an IPv6 lab system based on a virtual machine platform, on both Windows and Linux hosts. The core of the system will be based on a "community version" software router for "real" IPv6 routing scenarios, have multiple network segments and multiple client OS's. In addition, Wireshark will be used to view specific IPv6 protocol components and verify IPv6 operations.

Instructor: Jeff Carrell, Networking & Big Data Instructor/Course Developer, Hewlett Packard Enteprise
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.

5:00-6:00

23 Wireshark and WiFi: capture techniques and challenges

Capturing packets over the air (OTA) can be a great way to troubleshoot certain network connectivity problems. However, it is not always straightforward to collect 802.11 frames: availability of specific hardware at the right time and place is likely necessary for a successful capture session. We will discuss some of the various hardware platforms that can be used for OTA captures and how to use Wireshark to validate that the capture file contains a reasonable representation of the wireless communication under review.

Instructor: George Cragg, Network Engineer, Draeger Medical Systems
George Cragg is a full time network engineer for a medical device company. Past careers include tree farmer, designing tire filling machines, and Six-Sigma Black Belt in the semiconductor industry.

24 Wireshark OTG, Extend your Wireshark with extcap, iPad and Pi

--TIPS and tricks of extcap and make use of Wireshark everywhere, any capture sources
Do you imagine your tablet can run Wireshark, Yes you can get Wireshark OTG.
Megumi will show you TIPS and tricks to use Wireshark with iPad Pro and Raspberry Pi.
You may not install many extcap interface that is not installed in default settings,
It's time to make use of extcap interface such as sshdump.
We can create our own customized extcap interface in easy way on Windows environment.
Actual demonstration extend your Wireshark's extcap interface!!

Megumi uses iPad Pro, Raspberry Pi and Windows10 environment.
Linux bash and Windows command prompt programming skills help you understand the session well.

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.

6:20-6:50

Closing Remarks and CTF Winners Announcement