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	
	Zoom 1	Zoom 2
9:15-10:15	**01** **Wireshark and WiFi: capture techniques and challenges** George Cragg	**02** **TBA**
10:15-10:30	Q & A	
10:30-10:45	BREAK	
10:45-11:45	**03** **Intrusion Analysis and Threat Hunting with Suricata** Josh Stroschein and Peter Manev	**04** **TBA**
11:45-12:00	Q & A	
12:00-12:30	LUNCH	
12:30-1:30	**05** **Looking For "Packets" in all the "Right" Places** Patrick Kinnison	**06** **Network Forensics Analysis** Rami Al-Talhi
1:30-1:45	Q & A	
1:45-2:00	BREAK	
2:00-3:00	**07** **Wireshark in use on LTE and 5G networks** Mark Stout	**08** **Back to the Packet Trenches** Hansang Bae
3:00-3:15	Q & A	
3:15-3:30	BREAK	
3:30-4:30	**09** **Intro to QUIC - The TCP Killer?** Chris Greer	**10** **Introduction to WAN optimization** John Pittle
4:30-4:45	Q & A	
4:45-5:00	BREAK	
5:00-6:00	**11** **TBA**	**12** **TBA**
6:00-6:15	Q & A	

SharkFest'21 Virtual US Conference Agenda

Friday, September 17		
8:00-9:00	**KEYNOTE:**	
9:00-9:15	**BREAK**	
9:15-10:15	**Zoom 1**	**Zoom 2**
	13  **TBA** Dr. Stephen Donnelly	**14**  **TBA** Sake Blok
10:15-10:30	**Q & A**	
10:30-10:45	**BREAK**	
10:45-11:45	**15**  **TBA**	**16**  **The Packet Doctors are in! Packet trace examinations with the experts** Drs. Bae, Blok, Bongertz & Landström
11:45-12:00	**Q & A**	
12:00-12:30	**LUNCH**	
12:30-1:30	**17**  TBA	**18**  **Dissecting WiFi6 using Wireshark** Megumi Takeshita
1:30-1:45	**Q & A**	
1:45-2:00	**BREAK**	
2:00-3:00	**19**  **Trace Files Case Files** Jasper Bongertz	**20**  **TBA**
3:00-3:15	**Q & A**	
3:15-3:30	**BREAK**	
3:30-4:30	**21**  **TBA**	**22**  **TBA**
4:30-4:45	**Q & A**	
4:45-5:00	**BREAK**	
5:00-6:00	**23**  TBA	**24**  **TBA**
	Q & A	

SharkFest'21 Virtual US Conference Agenda

Session Abstracts & Instructor Bios

(DRAFT - UPDATED FREQUENTLY)

THURSDAY, SEPTEMBER 17

8:00-9:00

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

9:15-10:15

01 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.

02 TBA

Instructor:

10:45-11:45

03 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, Director of Training, 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.

04 TBA

Instructor:

SharkFest'21 Virtual US Conference Agenda

12:30-1:30

05 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.

06 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.

2:00-3:00

07 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.

08 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.

3:30-4:30

09 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

10 Introduction to WAN optimization

WAN Optimization technologies are present in many customer network environments, and have recently evolved to become even more important for Cloud, SaaS, and WFH distributed users. In this introductory session we will explore the key features, benefits, and design patterns of WAN Optimization from a network traffic perspective. We will use Wiresahark to explore sample traffic captures that highlight the expected behavior and measure the performance benefits of WAN Optimization.

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.

5:00-6:00

11

12

SharkFest'21 Virtual US Conference Agenda

FRIDAY, SEPTEMBER 18

8:00-9:00

KEYNOTE:

8:00-9:00

Keynote:

9:15-10:15

13 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.

14 TBA

Instructor:

10:45-11:45

15 TBA

Instructor:

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!

SharkFest'21 Virtual US Conference Agenda

12:30-1:30

17 TBA

Instructor:

18 Dissecting WiFi6 using WIreshark

It's time to capture WiFi6 and dissect IEEE802.11ax using Wireshark!! new method to capture traffic and filter, profile and so on. Wireless protocol evolves year by year, now new HE (High-Efficiency) ages comes to us, the instructor will show you IEEE802.11ax protocols and the difference with former WiFi, And she will demonstrate the way to capture WiFi6 with new software/hardware. The session will also include a WiFi6 specified profile including display filter/ filter button, coloring rule and so on.

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.

2:00-3:00

19 Trace File Case Files

Working with packet capture (=trace) files usually means trying to find something quite specific. This can be indicators for connection problems, or verifying that there are data elements present/not present that you expect to troubleshoot how a protocol behaves. Sometimes it's also about finding security issues, or patterns of an attack. In this talk we will walk through a couple of problem situations to see how they can be addressed, and maybe show a few tricks that you hadn't seen before.

Instructor: Jasper Bongertz, Network Security, Airbus CyberSecurity

Jasper Bongertz is a network security expert with focus on network forensics and incident response at Airbus CyberSecurity. He 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.

20 TBA

Instructor:

3:30-4:30

21 TBA

Instructor:

22 TBA

Instructor:

SharkFest'21 Virtual US Conference Agenda

5:00-6:00
23 TBA
24 TBA
5:00-6:00