SharkFest'18 US

June 23rd-28th, 2018

- Pre-Conference Class Schedules
- SharkFest'18 US Session & Events Agenda
- Session Abstracts & Requirements
- Instructor Bios

SharkFest'18 US Conference Agenda

Pre-Conference Courses and SharkFest'18 US Opening Schedule

WIRESHARK UNIVERSITY Pre-Conference Course *Troubleshooting with Wireshark* Hahn Auditorium	**Saturday**	**23 June 2018**
	7:30-9:00am	Laura Chappell's "Troubleshooting with Wireshark" Check-in and Badge Pick up
	7:30-9:00am	Continental Breakfast
	9:00am	Laptop Setup and Class begins (with morning break)
	12:00-1:00pm	Lunch Break
	1:00pm	Class Resumes (with afternoon break)
	5:00pm	Class day ends
	Sunday	**24 June 2018**
	8:00-9:00am	Continental Breakfast
	9:00am	Laptop Setup and Class begins (with morning break)
	12:00-1:00pm	Lunch Break
	1:00pm	Class Resumes (with afternoon break)
	5:00pm	Class day ends
	Monday	**25 June 2018**
	8:00-9:00am	Continental Breakfast
	9:00am	Laptop Setup and Class begins (with morning break)
	12:00- 1:00pm	Lunch Break
	1:00pm	Class Resumes (with afternoon break)
	5:00pm	Class ends **Attending SharkFest'18 US?** **See Tuesday Opening Schedule below**

	Monday	**25 June 2018**
	7:00am-7:30pm	Check-In & Badge Pick-Up for Malicious Traffic Hands-on Workshop & SharkFest'18 US (Registration Table, Museum 2nd Floor Foyer)
Malicious Traffic Hands-on Workshop	8:00am-5:00pm	Malicious Network Traffic Analysis Hands-On Workshop (Boole Classroom) **Workshop Registrants Only**
Developer Drop-In Workshop	1:00-5:00pm	Developer Drop-In Workshop (Developer Den – Grand Hall) **SharkFest'18 US Attendees Only**
SharkFest'18 US Welcome Dinner	6:00-8:30pm	***SharkFest Welcome Dinner & Sponsor Showcase*** **(Grand Hall)** **SharkFest'18 US Attendees Only**

SharkFest'18 US Conference Agenda

Tuesday 26 June 2018			
7:30-8:30am	**Breakfast - Grand Hall**		
7:30am-12:00pm	**SharkFest Check-in & Badge Pick-up**		
8:30-9:30am	***Keynote: "And Now We Are 20! Highlights from Wireshark's First 2 Decades"*** ***Gerald Combs & Friends*** ***(Hahn Auditorium)***		
	Hahn Auditorium	**Grand Hall Classroom**	**Boole Classroom**
9:30-9:45am	Break		
9:45-11:00am	**01** ▲▲ **In the Packet Trenches (Part 1)** Hansang Bae	**02** ▲ **An Introduction to Wireshark: Rookie to Veteran in 2 sessions (Part 1)** Betty DuBois	**03** ▲▲▲ **Writing a Wireshark Dissector: 3 ways to eat bytes** Graham Bloice
11:00-11:15am	Break		
11:15am-12:30pm	**04** ▲▲ **In the Packet Trenches (Part 2)** Hansang Bae	**05** ▲ **An Introduction to Wireshark: Rookie to Veteran in 2 sessions (Part 2)** Betty DuBois	**06** ▲▲ **Using more of the features of Wireshark to write better dissectors** Richard Sharpe
12:30-1:30pm	LUNCH		
1:30-2:45pm	**07** ▲▲ **Using Wireshark to solve real problems for real people: Step-by-step case studies in packet analysis** Kary Rogers	**08** ▲▲ **Traffic analysis of cryptocurrency & blockchain networks** Brad Palm & Brian Greunke	**09** ▲▲▲ **Developer Lightning Talks** Wireshark Core Developers
2:45-3:00pm	Break		
3:00-4:15pm	**10** ▲▲ **Hands-on analysis of multi-point captures** Christian Landström	**11** ▲▲ **Augmenting packet capture with contextual meta-data: the what, why, and how** Stephen Donnelly	**12** ▲▲ **Point and Shoot Packet! Point your packet effectively & Shoot the trouble with Wireshark** Megumi Takeshita
4:15-4:30 pm	Break		
4:30-6:00pm	**13** ▲▲▲ **Practical Tracewrangling: exploring capture file manipulation/extraction scenarios** Jasper Bongertz	**14** ▲▲ **BGP is not only a TCP session: Learning about the protocol that holds networks together** Werner Fischer	**15** ▲▲ **How to get 100% of your data off the wire** Greg Zemlin
6:00-8:30pm	**Sponsor Technology Showcase Reception, Treasure Hunt & Dinner** **(Museum 1st Floor Lobby)**		

Pick up your Packet Challenge Sheet at the WIRESHARKUNIVERSITY table in the REEF

SharkFest'18 US Conference Agenda

Wednesday	27 June 2018			
7:30-8:30am	**Breakfast – Grand Hall**			
8:30-9:30am	***Keynote: "Wireshark: The Microscope of the 21st Century"*** ***Usman Muzaffar, VP of Engineering, Cloudflare*** ***(Hahn Auditorium)***			
	Hahn Auditorium	**Grand Hall Classroom**	**Boole Classroom**	
9:45-11:00am	**16** ▲ **TCP - Tips, Tricks, & Traces (Part 1)** Chris Greer	**17** ▲▲ **extcap – Packet capture beyond libpcap/winpcap: bluetooth sniffing, android dumping & other fun stuff!** Roland Knall	**18** ▲▲ **Generating Wireshark Dissectors: A status report** Richard Sharpe	**Visit the Vendor Showcase in the Grand Hall REEF!**
11:00–11:15am	Break			
11:15am-12:30pm	**19** ▲▲ **TCP - Tips, Tricks, & Traces (Part 2)** Chris Greer	**20** ▲▲ **Wireshark in the "Real World": Top ways to use Wireshark in the real world of an IT engineer** Patrick Kinnison	**21** ▲▲▲ **sFlow: Theory & practice of a sampling technology and its analysis with Wireshark** Simone Mainardi	
12:30–1:30pm	LUNCH			
1:30–2:45pm	**22** ▲▲ **Writing a TCP analysis expert system** Jasper Bongertz	**23** ▲▲ **Playing with "*MATCHES*": Using regular expressions for fun & profit** Mike Hammond	**24** ▲ **Know Abnormal, Find Evil: A Wireshark Beginner's Guide for the Security Professional** Maher Adib	
2:45–3:00pm	Break			
3:00–4:15pm	**25** ▲▲ **A deep dive into SIP: everything you need to know to debug & troubleshoot SIP packets** Betty DuBois	**26** ▲▲ **Analyzing Windows malware traffic with Wireshark** Bradley Duncan	**27** ▲▲ **My TCP ain't your TCP: Stack behavior back then & today** Simon Lindermann	
4:15 – 4:30pm	Break			
4:30 – 6:00pm	**28** ▲▲ **The Packet Doctors are In! Packet trace examinations by the experts** Drs. Bae, Blok, Bongertz, Landström & Rogers	**29** ▲▲ **Baselining with Wireshark to identify & stop unwanted communications** Jon Ford	**30** ▲▲ **BGP is not only a TCP session: Learning about the protocol that holds networks together** Werner Fischer	
6:00–8:30pm	**Packet Palooza Group Packet Competition Dinner & Sponsor Showcase** **(Grand Hall)**			

SharkFest'18 US Conference Agenda

Thursday	28 June 2018		
7:30-8:30am	Breakfast – Grand Hall		
8:30-9:30am	***SharkBytes*** ***(Hahn Auditorium)***		
	Hahn Auditorium	**Grand Hall Classroom**	**Boole**
9:45-11:00am	**31** ◢◢ **Traffic analysis of cryptocurrency & blockchain networks** Brad Palm & Brian Greunke	**32** ◢ **We'll never do it right: A look at security, what we're doing and how we're trying to fix things** Mike Kershaw	**33** ◢◢ **Wireshark CLI tools & scripting** Sake Blok
11:00-11:15am	Break		
11:15am-12:30pm	**34** ◢◢ **Patterns in TCP retransmissions: Using Wireshark to better understand the retransmission process** Scott Reid	**35** ◢◢ **Behind the Green Lock: Examining SSL encryption/decryption using Wireshark** Ross Bagurdes	**36** ◢◢ **Wireshark and beyond! Complementing your Wireshark analysis with other open source & low-cost tools** Mike Canney
12:30-1:30pm	LUNCH		
1:30-2:45pm	**37** ◢◢ **Packet monitoring in the days of IoT and Cloud** Luca Deri	**38** ◢◢ **Baselining with Wireshark to identify & stop unwanted communications** Jon Ford	**39** ◢◢ **Introduction to practical network signature development for open source IDS (Part 1)** Jason Williams & Jack Mott
2:45-3:00pm	Break		
3:00-4:15pm	**40** ◢◢◢ **Mangling packets on the fly with divert sockets: how to hack a Cisco router ACL** Kary Rogers	**41** ◢◢ **My TCP ain't your TCP: Stack behavior back then and today** Simon Lindermann	**42** ◢◢ **Introduction to practical network signature development for open source IDS (Part 2)** Jason Williams & Jack Mott
4:15-4:30pm	Break		
4:30-6:00pm	**43** ◢ **OPEN FORUM: Aha! Moments in packet analysis** Chris Greer	**44** ◢◢ **Analyzing Windows malware traffic with Wireshark** Bradley Duncan	**45** ◢◢ **Introduction to practical network signature development for open source IDS (Part 3)** Jason Williams & Jack Mott
6:15–6:30pm	**Closing Remarks& Packet Challenge Awards** **(Hahn Auditorium)**		
6:30-8:00pm	**Farewell Reception** **(Side Terrace – 1st Floor Museum)**		

Visit the Vendor Showcase in the Grand Hall REEF!

SharkFest'18 US Conference Agenda

Session Level Legend: Beginner = ▲ Intermediate = ▲▲ Advanced/Developer = ▲▲▲

TUESDAY, 26 JUNE

8:30-9:30am	**Keynote: "And Now We Are 20! Highlights from Wireshark's First 2 Decades"** **Gerald Combs & Friends**
9:45-11:00am	
Hahn Auditorium	**01 In the Packet Trenches (Part 1)** ▲▲ In this 2-part session, Hansang offers foundational troubleshooting practices that will assist in legacy, cloud, and transitioning networks. **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.
Grand Hall Classroom	**02 An Introduction to Wireshark: Rookie to Veteran in 2 sessions (Part 1)** ▲ Designed for those new to Wireshark or looking for a refresher on Wireshark 2.x features and foundational analysis techniques. Learn how to use Wireshark to find the culprit in three common mysteries: 1. Application X doesn't work 2. Application Y is slow 3. Application Z is dropping packets Learn the clues Wireshark gives: When the client asks the question, do they get a response? Is it a yes, or no? If yes, how long did it take? If no, how long did it take, and what was the error? What did the client try to do next? We'll use a combination of saved traces and live capture to learn the most efficient approach for locating these clues in Wireshark. **Bring your laptop! This is a hands-on event. Sessions files can be found at https://start.me/p/m6Ggno/sf18us** Please read Jasper Bongertz' "Network Capture Playbook" for best capture practices before attending the session. We won't have time to cover these important concepts. https://blog.packet-foo.com/2016/10/the-network-capture-playbook-part-1-ethernet-basics/ **Instructor: Betty DuBois, Chief Detective, Network Detectives and Wireshark U Instructor** Betty DuBois is the Chief Detective for Network Detectives. She has been analyzing networks since 1997, performing site isolations, application profiles, and network baselines for a wide variety of clients. As an instructor for Wireshark University, she is known for her ability to make a dry, complex subject fun and interesting, by using both humor and real-world examples.
Boole Classroom	**03 Writing a Wireshark Dissector: 3 Ways to Eat Bytes** ▲▲▲ The presentation outlines the 3 most popular methods to write a dissector, using plain text files with WSGD, using a Lua script file and finally a C dissector. An introduction to how dissectors fit into the Wireshark system is given, then each method is compared for ease of initial development, facilities offered and run-time performance. **Instructor: Graham Bloice, Software Developer, Trihedral UK Ltd. & Wireshark Core Developer** Graham is a Software Developer with Trihedral UK Limited where he helps produce their VTScada HMI\Scada toolkit. Graham is also a Wireshark core developer, mainly concentrating on the Windows build machinery and DNP3 dissectors. He uses Wireshark frequently in his day job when analysing telemetry protocols used in the SCADA world, and inter-machine traffic for the company's distributed SCADA product.
11:15am-12:30pm	
Hahn Auditorium	**04 In the Packet Trenches (Part 2)** ▲▲ In this 2-part session, Hansang offers foundational troubleshooting practices that will assist in legacy, cloud, and transitioning networks. **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.

Grand Hall Classroom	**05 An Introduction to Wireshark: Rookie to Veteran in 2 sessions (Part 2)** Designed for those new to Wireshark or looking for a refresher on Wireshark 2.x features and foundational analysis techniques. Learn how to use Wireshark to find the culprit in three common mysteries: 1. Application X doesn't work 2. Application Y is slow 3. Application Z is dropping packets Learn the clues Wireshark gives: When the client asks the question, do they get a response? Is it a yes, or no? If yes, how long did it take? If no, how long did it take, and what was the error? What did the client try to do next? We'll use a combination of saved traces and live capture to learn the most efficient approach for locating these clues in Wireshark. **Bring your laptop! This is a hands-on event. Sessions files can be found at https://start.me/p/m6Ggno/sf18us** **Please read Jasper Bongertz' "Network Capture Playbook" for best capture practices before attending the session. We won't have time to cover these important concepts**. https://blog.packet-foo.com/2016/10/the-network-capture-playbook-part-1-ethernet-basics/ **Instructor: Betty DuBois, Chief Detective, Network Detectives and Wireshark U Instructor** Betty DuBois is the Chief Detective for Network Detectives. She has been analyzing networks since 1997, performing site isolations, application profiles, and network baselines for a wide variety of clients. As an instructor for Wireshark University, she is known for her ability to make a dry, complex subject fun and interesting, by using both humor and real-world examples..
Boole Classroom	**06 Using more of the features of Wireshark to write better dissectors** There are many features in Wireshark for dissector writers that many people do not seem aware of. Some are new, and some have been there for a long time. This presentation will expose people to both new and old techniques for writing better dissectors, including: * Using dissector tables * Easily adding units * Handling bit fields * Expert infos * etc We'll also make reference to real dissectors to illustrate the concepts involved. **Instructor: Richard Sharpe, Principal Software Engineer, Primary Data** Richard is a long-time contributor to Wireshark who has recently started working on the 802.11 and other dissectors, including the IEEE1905 and other protocols.
1:30-2:45pm	
Hahn Auditorium	**07 Using Wireshark to solve real problems for real people: Real-world packet analysis case studies** Stop banging your head on your desk trying to find root cause and solve performance problems. The answers are in the packets and this session will show you step-by-step in Wireshark how to solve real world case studies that had stumped others. Be the hero! **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.
Grand Hall Classroom	**08 Traffic analysis of cryptocurrency & blockchain networks** This will be a presentation on the networks and protocols used to support cryptocurrency and other blockchain based infrastructures. We will utilize Wireshark to dissect and analyze the behaviors of the underlying protocols which execute, validate, and secure the network. Since this is a relatively new space, we will explore the fundamentals of these technologies in an effort to build useful Wireshark profiles and dissectors to aid in the healthy adoption and support of the blockchain community. We will accomplish this by comparing and contrasting the technologies used for different cryptocurrencies, i.e. Bitcoin vs. Monero. This session will be valuable for those who are familiar with the blockchain space and have begun researching topics such as; consensus protocols, P2P, I2P, Stratum+TCP, and Kovri. **Instructor: Brad Palm, Network and Security Analyst & Brian Greunke, Security Advocate, BruteForce**

	Brad is an analyst working in the cybersecurity and network efficiency domains. He focuses on network capture and analysis for enterprise networks, testing emerging technologies and devices for the DoD, and utilizing captured traffic to influence developmental test scenarios. His professional interests include tinkering with open source virtualization/container/provisioning technologies, learning about software defined and mesh networking, and increasing the usability of secure information systems to facilitate wide scale adoption. brad@bruteforce.io Brian is a security advocate, technical leader, and full-stack developer with nearly 10 years of experience guiding technical teams in fast-paced, high-stakes environments. He enjoys exploring cutting edge technologies and using them to build security, decentralization, and privacy into the software and systems we use every day.
Boole Classroom	**09 Developer Bytes Lighting Talks** Developer Bytes Lightning Talks focus on small, interesting topics regarding Wireshark, its development, and use cases. We'll present a look behind the curtains, highlight features often overlooked, or present upcoming topics for future versions of Wireshark. This session delivers a range of Wireshark topics, such as: - Wireshark Git and CMake navigation - From protocol to dissector in 15 minutes - Making a company-internal build - Packet generation, prepare dummy data **Instructors: Wireshark Core Developers**
3:00-4:15pm	
Hahn Auditorium	**10 Hands-on analysis of multi-point captures** This session will take you on the challenging journey of analyzing performance issues throughout a whole network path. Loadbalancers, firewalls, proxy servers might be involved, and finding the right spot to analyze the problem is not always an easy task. This talk focuses multipoint capture file analysis and packet matching from different capture points. **This will be an interactive session with live analysis, so bring your Wireshark and join the fun!** **Instructor: Christian Landström Senior Consultant, Airbus DS CyberSecurity** Christian Landström has been working in IT since 2004, focusing strongly on network communications and IT security. After graduating in computer science in 2008, Christian joined Synerity Systems and then moved with the whole Synerity team to Fast Lane GmbH in 2009 as Senior Consultant for network analysis and security. Since 2013, he has been working as a Senior Consultants for Airbus Defence and Space CyberSecurity focusing on IT security, Incident Response and Network Forensics.
Grand Hall Classroom	**11 Augmenting Packet Capture with Contextual Meta-Data: the what, why & how** Full packet capture and archiving are increasingly important, providing "ground truth" evidence for investigating security incidents and performance issues. But captured packets by themselves lack context, such as where they were captured and the environment at the time of capture. Augmenting packet data with meta-data can provide useful context about when, where, and how packets were captured and the environment at the time of capture. This presentation will discuss what types of meta-data can be useful, what they can be useful for, and how meta-data can be encoded into packet capture to ensure permanent context to packets captured. **Instructor: Dr. 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.
Boole Classroom	**12 Point and Shoot Packet! Point your packet effectively and Shoot the trouble with Wireshark** When you debug, troubleshoot and inspect network troubles and security issues using Wireshark, you may just look at a trace files and watch each packet sequentially in detail. In this session, Megumi shows you some good ways to point packets using display/capture filters, graphs, and tshark. Each layer's header has important fields to analyze trace files. This session show you alternative focus points for your debugging, troubleshooting, and inspection and explains how to shoot the problem. **Instructor: Megumi Takeshita, Packet Otaku and Owner, Ikeriri Network Service** Megumi Takeshita, or Packet Otaku (Twitter: @ikeriri),runs a packet analysis company, Ikeriri Network Service, after having worked at BayNetworks and Nortel Networks in Japan. Ikeriri offers packet analysis support for troubleshooting, debugging and security inspection. Ikeriri is also a reseller of many wired/wireless capture and analysis devices and software for Riverbed, Metageek, Profitap, Dualcomm etc. Megumi has authored 10+ books about Wireshark and packet analysis in Japanese and she is one of contributors to the Wireshark project too.

4:30-6:00pm	
Hahn Auditorium	**13 Practical Tracewrangling: Exploring capture file manipulation/extraction scenarios** Sometimes, scrolling through the packet list while filtering and inspecting the packet decodes in Wireshark isn't the right thing to do at the beginning. When the amount of packets becomes overwhelming, you need a strategy to reduce the haystack to a smaller pile you can work with without getting lost all the time. This is where Tracewrangler can help a lot, offering various extraction techniques. While Wireshark is capable of reading almost any kind of network packet or frame you throw at it, some other tools may not be that versatile. Sometimes, link layer types like Linux Cooked Capture (SLL), tunneling layers or MPLS shims make it impossible to process capture with your favorite tool because it doesn't understand those layers. Tracewrangler can help, modifying your capture files in an adaptive way without breaking layer relationships. 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.
Grand Hall Classroom	**14 BGP is not only a TCP session: Learning about the protocol that holds networks together** Border Gateway Protocol (BGP) is a standardized exterior gateway protocol designed to exchange routing and reachability information among autonomous systems (AS) on the Internet - this is what Wikipedia tells us. But BGP is more right now - not only focused on internet but also on local network and data centers. In this sessions, we will investigate sample trace files and thoroughly review the dissector of BGP together. Please bring your own Wireshark and a powerful text editor to follow the session. The presenter will share his experience and the secrets he is using to learn and extend his protocol knowledge over the years with Wireshark and you. Instructor: Werner Fischer, Principal Networking Consultant, avodaq AG Werner Fischer is a long-term Dual-CCIE (R/S, Security) with over 20 years of experience in the networking arena. At avodaq, Werner works as a Principal Networking Consultant on System Architectures. He provides design guidance in key projects and is responsible for transferring new technology of networking solutions to internal and external audiences. Werner holds numerous industry certificates and has been a Sniffer Certified Master since 2003, VMware Certified Professional (4/5/6) and has also attained the Gold Certified Engineer status from the IPv6 Forum. Prior to joining avodaq, Werner worked as a Network Project Engineer for Siemens AG.
Boole Classroom	**15 How to get 100% of your data off the wire** Wireshark is a great tool, used globally for packet analysis, but how do you get the data to it? You have 2 options, using a Network TAP or a SPAN port. A Network TAP ensures that Wireshark will get all of the data necessary for comprehensive packet analysis. A SPAN port on the other hand, randomly drops packets when it becomes oversubscribed, hindering Wireshark's analysis ability. In the likely scenario that you're using a laptop to run Wireshark, you'll need to use an Aggregator TAP to ensure that both sides of the conversation are sent to Wireshark for analysis. Additionally, if you're only able to see a limited amount of data on a PC, Filtering TAPs can be used to ensure monitoring ports are not oversubscribed with unneeded data. In this presentation we'll demonstrate how to use a network TAP to get all of the data off of the wire and analyzed via Wireshark. Instructor: Greg Zemlin, Product Manager, Garland Technology Greg Zemlin is a Product Manager at Garland Technology, a technology partner with Wireshark. Greg is currently working on the research and development of Garland Technology's new products including the virtual test access point. He has over 8 years of experience in the industry and has extensive expertise in product management, hardware design, and hardware/software verification.

Session Level Legend: Beginner = ▲ Intermediate = ▲▲ Advanced/Developer = ▲▲▲

WEDNESDAY, 27 JUNE

8:30 - 9:30am — **Keynote: "Wireshark: The Microscope of the 21st Century"**
Usman Muzaffar, VP of Engineering, Cloudflare

9:45-11:00am

Hahn Auditorium

16 TCP - Tips, Tricks, & Traces (Part 1) ▲

Performance problems can often be isolated using the transport layer. But how can we identify what is actually broken if we don't know how it should work in the first place? In this interactive session, we will examine:

- The TCP handshake and TCP Options
- TCP Windows
- TCP Retransmissions
- TCP Selective Acknowledgements
- and more!

A sample trace file will be provided so you can follow along. Additionally, a few case studies will be presented that show how aspects of TCP can be leveraged to find root cause.

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.

Grand Hall Classroom

17 extcap – Packet capture beyond libpcap/winpcap: bluetooth sniffing, android dumping & other fun stuff! ▲

extcap is the external capture interface for Wireshark. This course will show the configuration of the interfaces and their general capabilities. Also writing your own utilities in Python and C-Code will be demonstrated and, additionally, a live-demonstration of capturing data via an RF-transmission will be shown.

Instructor: Roland Knall, Wireshark Core Developer

Roland is a Software System Architect for machine safety protocols at B&R Industrial Automation, a division of ABB. He started developing software some 20 years ago and has seen nearly all parts of software development, but focusing the last 10 years on industrial machine applications and mainly on systems in the area of industrial ethernet. He has been a Core Developer of Wireshark since 2016 and focuses mainly on the integration of external capture devices as well as UI improvements.

Boole Classroom

18 Generating Wireshark Dissectors: A status report ▲▲

I presented a session at SharkFest'17 EUROPE on generating Wireshark Dissectors from XDR and suggested that I was working on generating them from a simple protocol description using the ANTLR4 tool. I have developed code that can now generate a dissector using a simple description of a protocol and this presentation is a progress report on my efforts and shows how to generate complex dissectors from a protocol description.

Instructor: Richard Sharpe, Principal Software Engineer, Primary Data

Richard is a long-time contributor to Wireshark who has recently started working on the 802.11 and other dissectors, including the IEEE1905 and other protocols.

11:15am – 12:30pm

Hahn Auditorium

19 TCP - Tips, Tricks, & Traces (Part 2) ▲▲

Performance problems can often be isolated using the transport layer. But how can we identify what is actually broken if we don't know how it should work in the first place? In this interactive session, we will examine:

- The TCP handshake and TCP Options
- TCP Windows
- TCP Retransmissions
- TCP Selective Acknowledgements
- and more!

A sample trace file will be provided so you can follow along. Additionally, a few case studies will be presented that show how aspects of TCP can be leveraged to find root cause.

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.
Grand Hall Classroom	**20 Wireshark in the "Real World": Top ways to use Wireshark in the real world of an IT engineer** After a couple of decades working in IT, I finally found a tool that I literally use every day in my job... Wireshark. My goal for this session is to explain how Wireshark has allowed me to address everyday challenges in the "Real World" of an IT Engineer, including: * Finding out just how bad those developers are at documenting how their application works. * Why are my backups taking so long to complete? * Internet Bandwidth Hogs....Who is it this time? * It worked yesterday, why isn't it working now? * Can we just move that server to the "Cloud"? * DNS Name Resolution... It doesn't always send ya where you want to go. * I didn't know that I was causing a problem!!! * Sometimes end users are wannabe hackers too. 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.
Boole Classroom	**21 sFlow: Theory and practice of a sampling technology and its analysis with Wireshark** sFlow is sampling technology for monitoring traffic in high-speed networks. sFlow agents, embedded in switches and routers, periodically sample and export raw packets as well as network interface statistics to an sFlow collector. Sampling makes sFlow suitable to provide network-wide visibility, by enabling the continuous monitoring of tens, or even hundreds, of multi-Gigabit switches and routers. Sampling processes, although unable to offer 100% exact results, are able to provide results with a statistically-quantifiable accuracy. This session provides a detailed overview of sFlow, and demonstrates the suitability of Wireshark as an sFlow collector. When operating in this (unconventional) mode, Wireshark is not only able to analyze sampled packets at scale, but also to display new indicators such as switching and routing information as well as links status, load and congestion. 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 Data Scientist. He is interested in computer networking, parallel and distributed algorithms, Internet measurements and data analysis.
1:30 – 2:45pm	
Hahn Auditorium	**22 Writing a TCP analysis expert system** TCP is a protocol that may seem simple, but can be quite complex to analyze. Most network analyzers have an expert system to help detect common problems, but I wanted to write my own just for the fun of it (that, and because it's useful). This talk will show what I have done so far, what the pitfalls are, and what the next steps could be. 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.
Grand Hall Classroom	**23 Playing with "*MATCHES*": Using regular expressions for fun and profit** Are there credit-card numbers in your packets? Social Security numbers? Other kinds of sensitive info? How do you know? It's time to take your search for text inside of packets beyond simple equality tests and the CONTAINS operator. Unleash the flexibility of regular expressions to identify patterns of bytes that just can't be found using simple wildcard searches. In this relaxed, interactive session, we'll introduce you to the primary elements of Wireshark's regular expression syntax, making you comfortable with this powerful but easily misunderstood feature. Instructor: Mike Hammond, Senior Technical Trainer, Global Knowledge Mike is a veteran technology trainer in the IT Professional space, delivering engaging training sessions on Windows, UNIX, and networking topics. A Wireshark Certified Network Analyst and Wireshark Certified Trainer, Mike delivers 5-day "Troubleshooting TCP/IP Networks with Wireshark" classes through Global Knowledge - the industry's leading IT and business skills training provider. Mike also is an avid chess player and strategy board game fan, a proud husband, and an exhausted father of two swimmers and a gymnast. He types 50 words per minute using the Dvorak keyboard layout, as all thinking people should.

Boole Classroom	**24 Know Abnormal, Find Evil: A Wireshark Beginner's Guide for the Security Professional** Wireshark is the de facto analysis tool across many fields. It's one of my go-to, ultimate security tools for verification and validation. When investigating possible security incidents, most of us start by firing up Wireshark and looking for packets relating to a breach or issue running inside the network/security infrastructure or devices. Sometimes it's very hard to locate issues and we don't know where to start. In this hands-on lab, the presenter will share his concept of "Intercept, Listen, Discover, and Be Evil" with protocols by walking through real world exercises designed to help ascertain breach possibilities, spotting the difference between abnormal and normal traffic and demonstrating how to navigate and customize your Wireshark dashboard. This is suitable for those who want to start learning and using Wireshark from a security perspective. **Please bring your laptop with Wireshark pre-installed.** **Instructor: Maher Adib, (WCNA, CCIE#25094), Principal Consultant, Ofisgate Sdn Bhd** Maher's first exposure to packet analysis was in 2000 when he downloaded Ethereal (now known as Wireshark) and was instantly fascinated. His love for the open source analyzer has led to a near-daily commitment to using the tool to discover what is really going on with network infrastructures. As Technical Lead for Ofisgate Sdn Bhd in Kuala Lumpur, he has architected Cyber Range, a realistic training platform for red and blue teaming scenarios mimicking real-world incidents using Wireshark packet analysis capabilities as one of the primary weapons. Maher is an active member of, and frequent presenter at, local and international IT-related community events such as Durian Conference, Malaysia Open Source Community meetings and, of course, SharkFest!
3:00 – 4:15pm	
Hahn Auditorium	**25 A Deep Dive into SIP: Everything you need to know to debug and troubleshoot SIP packets** SIP is the most popular VoIP control protocol in use. Take a deep dive into the SIP headers and flows, to learn how they can be used for troubleshooting incomplete or dropped calls. Session Description Protocol (SDP) will also be examined. **Please bring your laptop to follow along. Traces and a profile will be made available at** https://start.me/p/m6Ggno/sf18us. **Instructor: Betty DuBois, Chief Detective, Network Detectives and Wireshark U Instructor** Betty DuBois is the Chief Detective for Network Detectives. She has been analyzing networks since 1997, performing fault isolations, application profiles, and network baselines for a wide variety of clients. As an instructor for Wireshark University, she is known for her ability to make a dry, complex subject fun and interesting, by using both humor and real-world examples.
Grand Hall Classroom	**26 Analyzing Windows malware traffic with Wireshark** This lab is designed to help people use Wireshark to investigate Windows-based malware activity from a packet capture (pcap) of network traffic and identify the root cause. Participants review initial infection activity and post-infection traffic seen from recent examples of Windows malware. The lab begins by configuring Wireshark from the default settings to better examine HTTP traffic. Scenarios include: 1: Searching for malicious traffic based on an IDS alert 2: Attempting to find the root cause based on indicators in the network traffic 3: Identifying an infection without a specific alert to guide you This lab includes several tips on how to filter traffic in Wireshark, and the instructor provides insight into these Windows-based infections. **Instructor: Bradley Duncan, Threat Intelligence Analyst, Palo Alto Networks - Unit 42** After 21 years of classified intelligence work for the US Air Force, Brad transitioned to cyber security in 2010, and he is a currently a Threat Intelligence Analyst for Palo Alto Networks Unit 42. Brad specializes in network traffic analysis. He is also a handler for the Internet Storm Center (ISC) and has posted more than 100 diaries at isc.sans.edu. Brad routinely blogs technical details and analysis of infection traffic at www.malware-traffic-analysis.net, where he provides traffic analysis exercises and over 1,300 malware and pcap samples to a growing community of information security professionals.
Boole Classroom	**27 My TCP ain't your TCP: Stack behavior back then and today** From the first specs to modern implementations, TCP stack behaviours have changed quite a bit and are still subject to major changes when new versions of operating systems are released. This session provides an overview of how TCP improvements evolved up to the recent Windows updates and is aimed at sharing must-have knowledge of modern implementation features like receive window auto-tuning, congestion window algorithms, and more. **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!

4:30 – 6:00pm	
Hahn Auditorium	**28 The Packet Doctors are In! Packet Trace Reviews 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 created a public forum for examining individual trace files with a broader audience for a collective learning experience. Ideally, 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!** Surgeons on Call: Hansang Bae, Jasper Bongertz, Christian Landström, Sake Blok
Grand Hall Classroom	**29 Baselining with Wireshark to identify & stop unwanted communications: Clearing away the forest to see the trees** Wireshark, in conjunction with other online tools, can be used to baseline network traffic - whether on a laptop, home network, or office network. It also can be used to help identify and filter out normal everyday traffic and clutter. Utilizing the Display Filter Macros, Statistics and online tools can help quickly identify suspicious traffic. This, along with tools like ProcessHacker or even netstat, can be used to identify processes communicating across the network. The goal of this session is to help you identify unwanted communications and stop them. This is likely to be a hands-on session, so please bring your laptop!! Instructor: Jon Ford, Web Application Security Analyst, MainNerve LLC Jon is a Web Application Security Analyst with MainNerve, Llc. He performs a variety of other jobs as well, from penetration testing of network systems, to wireless (802.11) exploitation to teaching personal cyber security and all the way up to doing dishes and taking out the trash. Jon has used Wireshark extensively in all of these jobs, minus the trash and dishes, but hopes to find a way to incorporate Wireshark into those duties as well one day. MainNerve LLC specializes in network and information security services and technology innovations. The company's mission is to help organizations assess and manage risks associated with critical assets. MainNerve exists to fill the critical gap in cybersecurity technology and expertise for the SMB market by employing critical subject matter expertise and supporting that with state-of-the-art technologies and affordable solutions.
Boole Classroom	**30 BGP is not only a TCP session: Learning about the protocol that holds networks together** Border Gateway Protocol (BGP) is a standardized exterior gateway protocol designed to exchange routing and reachability information among autonomous systems (AS) on the Internet - this is what Wikipedia tells us. But BGP is more right now - not only focused on internet but also on local network and data centers. In this sessions, we will investigate sample trace files and thoroughly review the dissector of BGP together. Please bring your own Wireshark and a powerful text editor to follow the session. The presenter will share his experience and the secrets he is using to learn and extend his protocol knowledge over the years with Wireshark and you. Instructor: Werner Fischer, Principal Networking Consultant, avodaq AG Werner Fischer is a long-term Dual-CCIE (R/S, Security) with over 20 years of experience in the networking arena. At avodaq, Werner works as a Principal Networking Consultant on System Architectures. He provides design guidance in key projects and is responsible for transferring new technology of networking solutions to internal and external audiences. Werner holds numerous industry certificates and has been a Sniffer Certified Master since 2003, VMware Certified Professional (4/5/6) and has also attained the Gold Certified Engineer status from the IPv6 Forum. Prior to joining avodaq, Werner worked as a Network Project Engineer for Siemens AG.

SharkFest'18 US Conference Agenda

Session Level Legend: Beginner = ▲ Intermediate = ▲▲ Advanced/Developer = ▲▲▲

THURSDAY, 28 JUNE

8:30 – 9:30am	**SharkBytes!**
Hahn Auditorium	
9:45 – 11:00am	
Hahn Auditorium	**31 Traffic analysis of cryptocurrency & blockchain networks ▲▲** This will be a presentation on the networks and protocols used to support cryptocurrency and other blockchain based infrastructures. We will utilize Wireshark to dissect and analyze the behaviors of the underlying protocols which execute, validate, and secure the network. Since this is a relatively new space, we will explore the fundamentals of these technologies in an effort to build useful Wireshark profiles and dissectors to aid in the healthy adoption and support of the blockchain community. We will accomplish this by comparing and contrasting the technologies used for different cryptocurrencies, i.e. Bitcoin vs. Monero. This session will be valuable for those who are familiar with the blockchain space and have begun researching topics such as; consensus protocols, P2P, I2P, Stratum+TCP, and Kovri. **Instructor: Brad Palm, Network and Security Analyst & Brian Gruenke, Security Advocate, BruteForce** Brad is an analyst working in the cybersecurity and network efficiency domains. He focuses on network capture and analysis for enterprise networks, testing emerging technologies and devices for the DoD, and utilizing captured traffic to influence developmental test scenarios. His professional interests include tinkering with open source virtualization/container/provisioning technologies, learning about software defined and mesh networking, and increasing the usability of secure information systems to facilitate wide scale adoption. brad@bruteforce.io Brian is a security advocate, technical leader, and full-stack developer with nearly 10 years of experience guiding technical teams in fast-paced, high-stakes environments. He enjoys exploring cutting edge techno
Grand Hall Classroom	**32 We'll never do it right: A look at security, what we're doing and how we're trying to fix things ▲** Follow the yellow brick (or silver silicon) road and down the rabbit hole of how we're failing at security at almost every level from user interfaces, networking, embedded hardware, manufacturing and supply line security, and hardware chip design. Patches are totally 2017; when are you doing your CPU Upgrade Tuesdays now? **Instructor: Mike Kershaw, Wi-Fi Hacker. Kismet Wireless** Mike Kershaw is the author of the Kismet wireless security tool, as well as a number of other open source wireless related software and hardware projects, and has been involved in wireless in some form or another for nearly 17 years.
Boole Classroom	**33 Wireshark CLI tools and scripting ▲▲** While working in a GUI environment is great, there are advantages to working in a Command Line Interface (CLI). In this session, you'll get become familiar with some of the Wireshark CLI tools (tshark, editcap, mergecap and capinfos). The basic usage of the tools will be discussed first before diving into more advanced usage when integrating with other commands to create new ways of processing pcap(ng) files. **Sake Blok, Relational Therapist for Computer Systems, SYN-bit.nl** Sake has been analyzing packets since the end of the last century. In the course of his work, he discovered many bugs in devices and presented his findings to the vendors to fix the issues. He also discovered configuration issues that led to functional problems or performance issues in applications running over the network. These issues were resolved based on reports Sake presented to his customers. In 2009, Sake started the company SYN-bit to provide network analysis services to enterprises across Europe. As part of his work to service his customers, Sake started developing extra functionality for Wireshark that he missed in his day-to-day job. He also enhanced multiple protocol dissectors to suit his analysis needs. In 2007, he was asked by Gerald to join the Wireshark Core Development team.

SharkFest'18 US Conference Agenda

11:15am – 12:30pm	
Hahn Auditorium	**34 Patterns in TCP retransmissions: Using Wireshark to better understand the retransmission process** In this interactive session, we'll go through several real-life troubleshooting examples and use Wireshark to see what is really happening when Wireshark indicates that data has been retransmitted. The presentation format will be an interactive, Q & A-type one to allow attendees to maximize their "take-away" knowledge from this session. **This is a Wireshark hands-on event. Attendees are, of course, encouraged to bring their laptops. The presentation format will also accommodate attendees without laptops.** **Instructor: Scott Reid, Technical Specialist, VGRIT** Scott Reid is a member of the Problem Analysis Group of the IT department at a large health care organization in Sweden and has been using Wireshark and its predecessor, Ethereal, for over ten years. In his position as Technical Specialist, he uses Wireshark daily for a range of functions - from benchmarking to development and pre-production testing to troubleshooting large-scale IT systems. An extensive variety of protocols and technologies are examined and evaluated regularly, and Wireshark is often used while giving presentations to demonstrate the details and particulars of a case.
Grand Hall Classroom	**35 Behind the Green Lock: Examining SSL encryption/decryption using Wireshark** You use SSL/TLS every day, in nearly every conversation, with nearly every network device you own. 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. This session will dive into the details of: - SSL/TLS History - TLS Handshake - Public/Private key encryption protocols and operation - Data Encryption protocol and quality of encryption - Capturing a session key and decryption TLS session in Wireshark You'll leave this session with an excellent understanding of SSL/TLS in this simple yet deep explanation of the protocol. **Instructor: Ross Bagurdes, Engineer/Educator, Bagurdes Technology** 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.
Boole Classroom	**36 Wireshark & beyond! Complementing Wireshark analysis with other open source & low-cost tools** Wireshark is a fantastic analyzer and I use it daily. However, there are multiple other tools that complement Wireshark that every analyst should incorporate into their toolkit. In this session, we will look at real world troubleshooting case studies where we take a deep dive into the sea of packets and learn how to swim with the Sharks using multiple free and low cost tools, each with their own unique benefits. After all, every good 'fisherperson' has a tackle box with multiple lures! Topics to include: • Mining data from "The 100 Gigabyte" trace file • PCAP Packet data warehousing • Quick and dirty TCP troubleshooting • Building your own Capture to Disk Appliance • Network Packet Forensics • Network Emulation • Personal, pocket network TAP **Instructor: Mike Canney, Principal Performance Analyst, Packet Fetcher** Specializing in providing application and network performance consulting services over the past 26 years, Mike has helped 1,000's of companies identify and resolve their application and network performance issues. Mike has also developed courseware, taught engineers how to identify, remediate, and prevent network and application issues by analyzing traffic flows at the packet level, and been a guest speaker at many industry trade shows (such as Networld Interop, multiple SharkFests and Cisco Networkers) throughout the United States delivering sessions on the topic of application performance analysis.

Application network-ability assessments (ANA), network performance troubleshooting, and deep level packet analysis are some of Mike's specialties. He's also well-versed in multiple sniffer technologies, network modeling, application performance management, load testing, and QA presentation.

1:30-2:45pm

Hahn Auditorium

37 Packet monitoring in the IoT and Cloud Days

The advent of cloud services and IoT devices has changed traffic patterns. Listening to music or dimming the light can be done using your voice or a mobile application that performs this action by talking to a cloud service. This trend has changed traffic patterns observed in networks, forced us to rethink edge network security, and made service discovery a key technology as users demand zero-configuration networks. This talk covers in detail how network devices advertise themselves in networks, how you can use Wireshark to analyze this network traffic, and the privacy issues involved when using modern technologies in everyday life.

Instructor: Luca Deri, Founder & Leader, ntop Project, CS Lecturer, University of Pisa

Luca Deri is the leader of the ntop project (www.ntop.org), aimed at developing an open-source monitoring platform for high-speed traffic analysis. He worked for University College of London and IBM Research prior to receiving his PhD at the University of Berne with a thesis on software components for traffic monitoring applications. Well known in the open-source and Linux community, he currently shares his time between the ntop project and the University of Pisa where he has been appointed as lecturer for the CS department.

Grand Hall Classroom

38 Baselining with Wireshark to identify & stop unwanted communications: Clearing away the forest to see the trees

Wireshark, in conjunction with other online tools, can be used to baseline network traffic - whether on a laptop, home network, or office network. It also can be used to help identify and filter out normal everyday traffic and clutter. Utilizing the Display Filter Macros, Statistics and online tools can help quickly identify suspicious traffic. This, along with tools like ProcessHacker or even netstat, can be used to identify processes communicating across the network. The goal of this session is to help you identify unwanted communications and stop them. This is likely to be a hands-on session, so please bring your laptop!!

Instructor: Jon Ford, Web Application Security Analyst, MainNerve LLC

Jon is a Web Application Security Analyst with MainNerve, Llc. He performs a variety of other jobs as well, from penetration testing of network systems, to wireless (802.11) exploitation to teaching personal cyber security and all the way up to doing dishes and taking out the trash. Jon has used Wireshark extensively in all of these jobs, minus the trash and dishes, but hopes to find a way to incorporate Wireshark into those duties as well one day. MainNerve LLC specializes in network and information security services and technology innovations. The company's mission is to help organizations assess and manage risks associated with critical assets. MainNerve exists to fill the critical gap in cybersecurity technology and expertise for the SMB market by employing critical subject matter expertise and supporting that with state-of-the-art technologies and affordable solutions.

Boole Classroom

39 Introduction to practical network signature development for open source IDS (Part 1)

In this 3-part, hands-on session, you'll learn methods and techniques for writing network signatures to efficiently detect the greatest threats facing organizations today. This class is designed for an analyst who spends their days investigating and responding to network IDS alerts and has something everyone can take back with them-- entry level or expert. Students will gain invaluable information and knowledge including usage, theory, malware traffic analysis fundamentals, and enhanced signature writing for Open Source IDS such as Suricata and Snort. Students will leave the class armed with the knowledge of how to write quality IDS signatures for their environment, enhancing their organization's ability to respond and detect threats.

The instructor will provide a virtual machine with all the exercises and copies of the slides in PDF format as well as cheat sheets and reference materials.

Instructors: Jason Williams & Jack Mott, Security Researchers, OISF / Proofpoint

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.

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.

3:00-4:15pm

Hahn Auditorium	**40 Mangling Packets on the Fly With Divert Sockets: How to hack a Cisco router ACL** Presentation on the use of divert sockets which allow actions on packets passing through the host system firewall. A case study will be presented on how to circumvent the TCP "established" keyword in Cisco router ACLs. **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.
Grand Hall Classroom	**41 My TCP ain't your TCP: Stack behavior back then and today** From the first specs to modern implementations, TCP stack behaviours have changed quite a bit and are still subject to major changes when new versions of operating systems are released. This session provides an overview of how TCP improvements evolved up to the recent Windows updates and is aimed at sharing must-have knowledge of modern implementation features like receive window auto-tuning, congestion window algorithms, and more. **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 locations around the world, 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!
Boole Classroom	**42 Introduction to practical network signature development for open source IDS (Part 2)** In this 3-part, hands-on session, you'll learn methods and techniques for writing network signatures to efficiently detect the greatest threats facing organizations today. This class is designed for an analyst who spends their days investigating and responding to network IDS alerts and has something everyone can take back with them-- entry level or expert. Students will gain invaluable information and knowledge including usage, theory, malware traffic analysis fundamentals, and enhanced signature writing for Open Source IDS such as Suricata and Snort. Students will leave the class armed with the knowledge of how to write quality IDS signatures for their environment, enhancing their organization's ability to respond and detect threats. **The instructor will provide a virtual machine with all the exercises and copies of the slides in PDF format as well as cheat sheets and reference materials.** **Instructors: Jason Williams & Jack Mott, Security Researchers, OISF / Proofpoint** 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. 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.

4:30-6:00pm

Hahn Auditorium	**43 OPEN FORUM: Aha! Moments in packet analysis** SharkFest has proven to be a ripe environment for exchanging tribal knowledge about those moments when a Wireshark discovery was made that seemed a breakthrough in an individual's use of the tool or step-up in their packet analysis skill set. This forum, moderated by Chris Greer, opens the floor to attendees to learn from one another by revealing their Wireshark Aha! moments. Have you created a personal Wireshark configuration that makes a particular diagnostic exercise a breeze? Stumbled onto a feature in Wireshark that blew you away? **Bring your trace files to share your discoveries with the crowd and enlighten fellow attendees!** **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.
Grand Hall Classroom	**44 Analyzing Windows malware traffic with Wireshark** This lab is designed to help people use Wireshark to investigate Windows-based malware activity from a packet capture (pcap) of network traffic and identify the root cause. Participants review initial infection activity and post-infection traffic seen from recent examples of Windows malware. The lab begins by configuring Wireshark from the default settings to better examine HTTP traffic. Scenarios include: 1: Searching for malicious traffic based on an IDS alert 2: Attempting to find the root cause based on indicators in the network traffic 3: Identifying an infection without a specific alert to guide you This lab includes several tips on how to filter traffic in Wireshark, and the instructor provides insight into these Windows-based infections. Instructor: Bradley Duncan, Threat Intelligence Analyst, Palo Alto Networks - Unit 42 After 21 years of classified intelligence work for the US Air Force, Brad transitioned to cyber security in 2010, and he is a currently a Threat Intelligence Analyst for Palo Alto Networks Unit 42. Brad specializes in network traffic analysis. He is also a handler for the Internet Storm Center (ISC) and has posted more than 100 diaries at isc.sans.edu. Brad routinely blogs technical details and analysis of infection traffic at www.malware-traffic-analysis.net, where he provides traffic analysis exercises and over 1,300 malware and pcap samples to a growing community of information security professionals.
Boole Classroom	**45 Introduction to practical network signature development for open source IDS (Part 3)** In this 3-part, hands-on session, you'll learn methods and techniques for writing network signatures to efficiently detect the greatest threats facing organizations today. This class is designed for an analyst who spends their days investigating and responding to network IDS alerts and has something everyone can take back with them-- entry level or expert. Students will gain invaluable information and knowledge including usage, theory, malware traffic analysis fundamentals, and enhanced signature writing for Open Source IDS such as Suricata and Snort. Students will leave the class armed with the knowledge of how to write quality IDS signatures for their environment, enhancing their organization's ability to respond and detect threats. **The instructor will provide a virtual machine with all the exercises and copies of the slides in PDF format as well as cheat sheets and reference materials.** Instructors: Jason Williams & Jack Mott, Security Researchers, OISF / Proofpoint 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. 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.
6:15-6:30pm	**Closing Comments Packet and Challenge Awards** **Gerald Combs & Friends**
6:30-8:00pm	**Farewell Reception – Side Terrace – 1st Floor Museum**