DFIR Summit

Agenda | Thursday, July 16

SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE

#DFIRSummit

Times are U.S. Eastern Time

9:00–9:15 am

Hosted in DFIR Track 1 & General Sessions

Welcome & Opening Remarks

Phil Hagen @PhilHagen, Senior Instructor, SANS Institute
Heather Mahalik @heathermahalik, Senior Instructor, SANS Institute
Rob Lee @robtlee, Fellow, SANS Institute

ADD TO CALENDAR

9:15–10:00 am

Hosted in DFIR Track 1 & General Sessions

Keynote: A DFIRent Side of DFIR: Forensicating for Black Lives and Other Social Justice Issues

Matt Mitchell @geminiimatt, Hacker; Security Researcher; Tech Fellow to the BUILD Program at the Ford Foundation

ADD TO CALENDAR

	DFIR TRACK 1 & GENERAL SESSIONS	DFIR TRACK 2
10:05–10:40 am	***You Need a PROcess to Check Your Running Processes and Modules. The Bad Guys, and Red Teams are Coming After Them!*** **Michael Gough** @MichaelGoughTX, Principal Incident Response, NCC Group ADD TO CALENDAR	***Kansa for Enterprise Scale Threat Hunting*** **Jonathan Ketchum** @Un1d1g1t, Threat Hunter/InfoSec Analyst, USAA ADD TO CALENDAR
10:40–10:55 am	**Break**	
10:55–11:30 am	***Data Science for DFIR – The Force Awakens*** **Jess Garcia** @j3ssgarcia, Lead DFIR Analyst/CEO, One eSecurity ADD TO CALENDAR	***Making Memories: Using Memory Analysis for Faster Response to User Investigations*** **Aaron Sparling** @osintlabworks, Digital Forensics Examiner, Portland Police Bureau **Jessica Hyde** @B1N2H3X, Director of Forensics, Magnet Forensics; Adjunct Professor, George Mason University ADD TO CALENDAR
11:30–11:40 am	**Break**	
11:40 am – 12:15 pm	***Using Big DFIR Data in Autopsy and Other Tools*** **Brian Carrier**, CTO, Basis Technology ADD TO CALENDAR	***Healthy Android Exams: Timelining Digital Wellbeing Data*** **Alexis Brignoni** @AlexisBrignoni, Special Agent, Federal Law Enforcement **Joshua Hickman**, Senior Associate, Kroll ADD TO CALENDAR
12:15–1:30 pm	**Lunch**	
	12:40–1:05 pm ***Think Like a Threat Actor to Handle Remote Work Risks*** *presented by* ***NetEnrich*** **Brandon Hoffman** @BrandonSHoffman, @NetEnrich, CISO & Head of Security Strategy, NetEnrich ADD TO CALENDAR	12:40–1:05 pm ***Man In the Mirror: Upping Your Threat Hunting Game By Seeing Yourself Like An Attacker*** *presented by* ***Randori*** **Eric McIntyre** @pwnpnw, @RandoriSecurity, Director of R&D, Randori ADD TO CALENDAR

DFIR Summit

Agenda | Thursday, July 16 (Continued)

#DFIRSummit

Times are U.S. Eastern Time

	DFIR TRACK 1 & GENERAL SESSIONS	DFIR TRACK 2
1:30–2:05 pm	***If at First You Don't Succeed, Try Something Else*** **Jim Clausing** @jclausing, Principal Member – Technical Staff, AT&T ADD TO CALENDAR	***Captain's Log: Take Your Application Log Analysis from Starfleet to Star Fleek*** **David Pany**, Manager, Mandiant **Ryan Tomcik**, Consultant, Mandiant ADD TO CALENDAR
2:10–2:45 pm	***Extract and Visualize Data from URLs Using Unfurl*** **Ryan Benson** @_RyanBenson, Security Engineer, Google ADD TO CALENDAR	***Just Forensics, Mercifully*** **Lee Whitfield** @lee_whitfield, Senior Technical Adviser, SANS ADD TO CALENDAR
2:45–3:00 pm	**Break**	
3:00–3:35 pm	***What the DLL is Happening? A Practical Approach to Identifying SOH.*** **Frank McClain**, Senior Detection Engineer, Red Canary ADD TO CALENDAR	***Lucky (iOS) #13: Time to Press Your Bets*** **Jared Barnhart**, Mobile Forensic Engineer, Principal, Parsons Corporation ADD TO CALENDAR
3:40–4:15 pm	***Did I Do That? Understanding Action and Artifacts in Real Time*** **Matthew Seyer** @forensic_matt, Manager, KPMG **David Cowen** @HECFBlog, Managing Director, KPMG ADD TO CALENDAR	***capa: Automatically Identify Malware Capabilities*** **Willi Ballenthin**, Senior Staff Reverse Engineer, FLARE/FireEye **Moritz Raabe**, Staff Reverse Engineer, FLARE/FireEye ADD TO CALENDAR
4:20–4:55 pm	***Long Live Linux Forensics*** **Ali Hadi**, Assistant Professor and Cybersecurity Researcher, Champlain College **Brendan Brown** and **Victor Griswold**, Senior Digital Forensics Students, Champlain College ADD TO CALENDAR	***Forensic Marriage: The Love/Hate Relationship Between eDiscovery and DFIR*** **Sarah Konunchuk** @SarahKonun13, IR Forensic Investigator, CFC Response **Andrew Konunchuk** @AndrewKonu, Data Operations Analyst, DISCO ADD TO CALENDAR
4:55–5:00 pm	Hosted in DFIR Track 1 & General Sessions ***Day 1 Wrap-up*** **Phil Hagen** @PhilHagen, Senior Instructor, SANS Institute **Heather Mahalik** @heathermahalik, Senior Instructor, SANS Institute **Rob Lee** @robtlee, Fellow, SANS Institute ADD TO CALENDAR	

DFIR Summit

Agenda | Friday, July 17

SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE

#DFIRSummit

Times are U.S. Eastern Time

8:45–8:50 am

Hosted in DFIR Track & General Sessions
Day 2 Welcome
Phil Hagen @PhilHagen, Senior Instructor, SANS Institute
Heather Mahalik @heathermahalik, Senior Instructor, SANS Institute
Rob Lee @robtlee, Fellow, SANS Institute
Lodrina Cherne @hexplates, Certified Instructor, SANS Institute
ADD TO CALENDAR

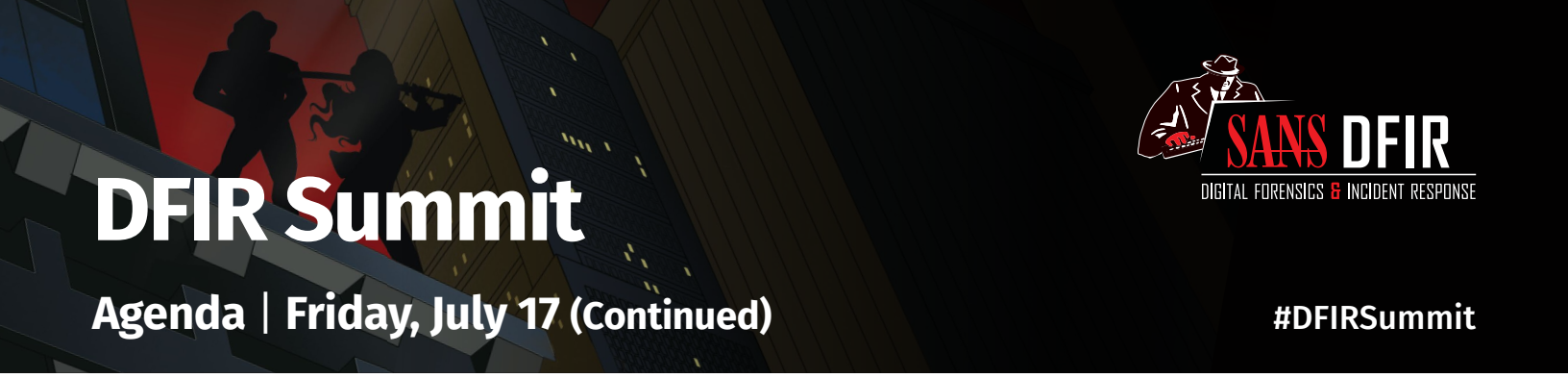
8:50–9:25 am

Hosted in DFIR Track & General Sessions
Keynote: Strengthening Trust in DFIR
Eoghan Casey, Author of Digital Evidence and Computer Crime
Daryl Pfeif, Founder & CEO, Digital Forensics Solutions
ADD TO CALENDAR

9:25–10:00 am

Hosted in DFIR Track & General Sessions
Keynote: Learning at Scale
Lodrina Cherne @hexplates, Certified Instructor, SANS Institute
ADD TO CALENDAR

	DFIR TRACK & GENERAL SESSIONS	SOLUTIONS TRACK
10:05–10:40 am	***Help! We Need an Adult! Engaging an External IR Team*** **Liz Waddell** @vlsin, Incident Commander, Talos Incident Response ADD TO CALENDAR	***Putting Big Data to Work in DFIR*** ***presented by DEVO*** **Jason Mical** @devo_Inc, Global Cyber Security Evangelist ADD TO CALENDAR
10:40–10:50 am	**Break**	
10:50–11:25 am	***Forensic Analysis of the Apple HomePod and the Apple HomeKit Environment*** **Mattia Epifani**, Digital Forensics Analyst, Reality Net – System Solutions ADD TO CALENDAR	***How Not to Ruin Your Day: Avoiding Common Threat Hunting Mistakes*** ***presented by Palo Alto Networks*** **Menachem Perlman** @PaloAltoNtwks, Sr. Manager, Threat Hunting ADD TO CALENDAR
11:25–11:35 am	**Break**	
11:35 am – 12:10 pm	***Hunting Bad Guys that Use TOR in Real Time*** **Milind Bhargava**, Founder, Mjolnir Security ADD TO CALENDAR	***Profiling Threat Actors in DNS*** ***presented by DomainTools*** **Taylor Wilkes-Pierce** @tw_pierce, @DomainTools, Senior Sales Engineer ADD TO CALENDAR
12:15–12:25 pm	***Using Storytelling to Be Heard and Remembered*** **Frank McClain** @littlemac042, Senior Detection Engineer, Red Canary ADD TO CALENDAR	
12:25–1:30 pm	**Lunch**	



DFIR Summit

Agenda | Friday, July 17 (Continued)

#DFIRSummit

Times are U.S. Eastern Time

	DFIR TRACK & GENERAL SESSIONS	SOLUTIONS TRACK
1:30–2:05 pm	***From Threat Research to Organizational Threat Detection*** **O'Shea Bowens** @SirMuDbl00d, Founder & CEO, Null Hat Security **Nico "Socks" Smith** @nicolaismith1, U.S. Army Air National Guard ADD TO CALENDAR	***Completing the Triad, The Case For Leading With NDR*** *presented by* ***ExtraHop*** **John Smith** @jmsazboy, @ExtraHop, Principal Sales Engineer ADD TO CALENDAR
2:10–2:45 pm	***DFIR To Go*** **Phil Hagen** @PhilHagen, Senior Instructor, SANS Institute **Heather Mahalik** @heathermahalik, Senior Instructor, SANS Institute ADD TO CALENDAR	***Empowering DFIR Through Automation and Orchestration – Enhancing Your Artifacts with Threat Intelligence*** *presented by* ***ThreatConnect*** **Iain Davison** @ThreatConnect, Security Architect and Technical Director of Strategic Alliances ADD TO CALENDAR
2:45–3:00 pm	**Break**	
3:00–3:15 pm	***Cyber Sleuth: Education and Immersion for the Next Generation*** **Daryl Pfeif**, Founder & CEO, Digital Forensics Solutions ADD TO CALENDAR	3:00–3:35 pm ***Accelerate Your Threat Hunting and IR with Next-Gen NDR+EDR*** *presented by* ***Microsoft*** *and* ***BlueHexagon*** **Balaji Prasad** @introspect, @bluehexagonai, VP or Products, Blue Hexagon **Arun Raman** @arunraman, @bluehexagonai, Principal Architect, Blue Hexagon **Heike Ritter** @HeikeRitter, @Microsoft, Senior Program Manager, Microsoft ADD TO CALENDAR
3:15–4:15 pm	***The DFIRlympics*** **Mari DeGrazia** @MariDeGrazia **Brian Moran** @BrianJMoran ADD TO CALENDAR	3:40–4:15 pm ***Dig Deeper: Acquisition and Analysis of AWS Cloud Data*** *presented by* ***MagnetForensics*** **Trey Amick** @amick_trey, @MagnetForensics, Manager, Forensic Consultants **Curtis Mutter** @cmutter79, @MagnetForensics, Senior Product Manager ADD TO CALENDAR
4:15–5:00 pm	Hosted in DFIR Track & General Sessions ***Forensic 4cast Awards*** **Lee Whitfield** @lee_whitfield, Senior Technical Adviser, SANS ADD TO CALENDAR	