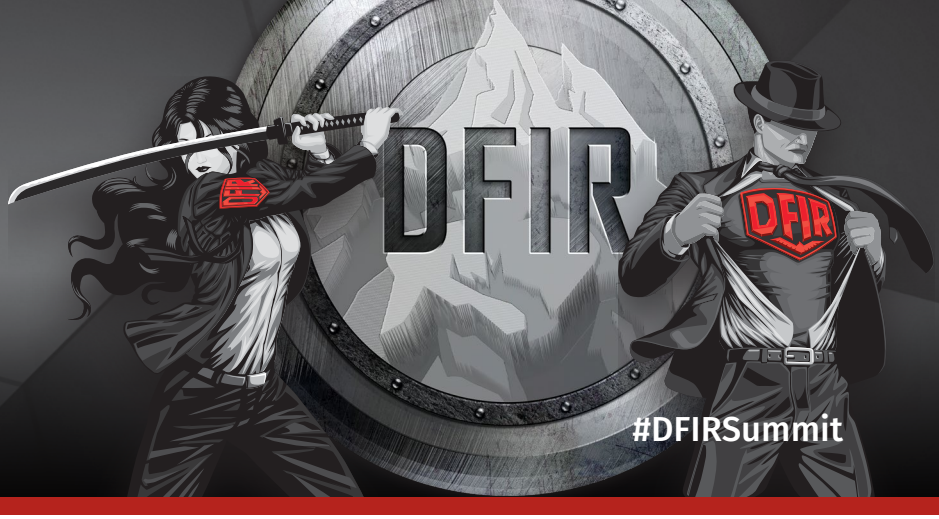
SANS DFIR SUMMIT 2021



Americas Session

Day 1 | Thursday, July 22

#DFIRSummit

View the complete agenda **here**.

9:00–9:15 AM EDT
13:00–13:15 UTC

Track 1 & Plenary

Welcome & Introductions
Philip Hagen, Senior Instructor, SANS Institute
Heather Mahalik, Senior Instructor, SANS Institute

9:15–10:00 AM EDT
13:15–14:00 UTC

Track 1 & Plenary

Keynote: Cobalt Strike Threat Hunting
Chad Tilbury, Senior Instructor, SANS Institute

10:05–10:40 AM EDT
14:05–14:40 UTC

Track 1 & Plenary

Automating Google Workspace Incident Response
Megan Roddie, Cyber Threat Researcher, IBM; SANS.edu Master's Candidate

Track 2

To the Moon! The Cyber Kill Chain Meets Blockchain
Jackie Koven, Solutions Architect, Chainalysis

10:40–10:50 AM EDT
14:40–14:50 UTC

Break

10:50–11:25 AM EDT
14:50–15:25 UTC

EZ Tools/KAPE: How to Contribute to and Benefit from Open Source Contributions
Andrew Rathbun, Senior Associate, Kroll

What Air Disaster Investigations Teach Us About Computer Forensics
Tony Drake, Senior Engineer, Security Intelligence, Intercontinental Exchange (ICE)

11:30 AM – 12:05 PM EDT
15:30–16:05 UTC

Greppin' Logs
Noah Rubin, Manager, Stroz Friedberg
Jon Stewart, Vice President, Stroz Friedberg

Order of Volatility in Modern Smartphone Forensics
Mattia Epifani, Instructor, SANS Institute

12:05–1:10 PM EDT
16:05–16:10 UTC

Lunch & Bonus Presentations

12:15–12:35 / 16:15–16:35 UTC — ***SANS.edu Information Session*** **(Hosted in Track 1 & Plenary)**
Kim Kafka

12:15–12:50 / 16:15–16:50 UTC — ***Sharing the Burden, the Single Source Dilemma in Incident Response*** **REGISTER HERE**
John Smith, Principal Sales Engineer, ExtraHop

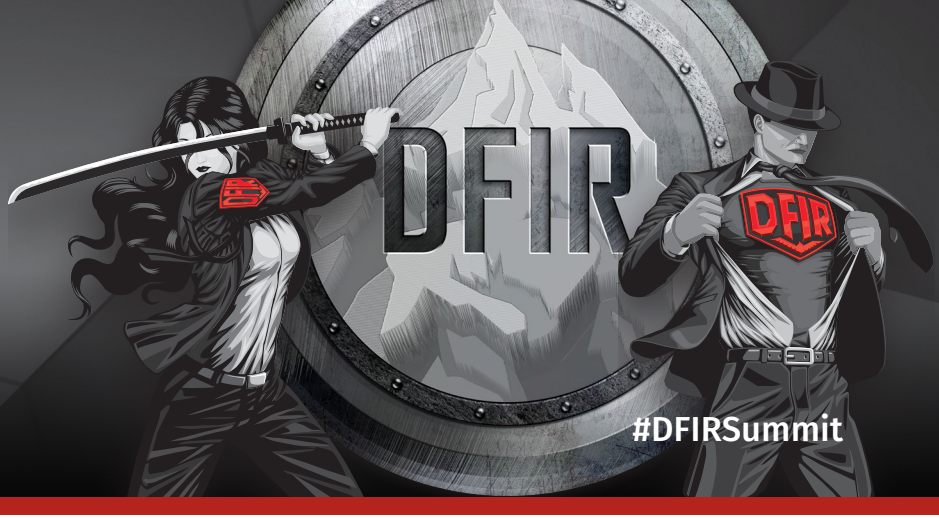
12:15–12:50 / 16:15–16:50 UTC — ***Taking XDR Beyond Detection and Response*** **REGISTER HERE**
Brock Bell, Consulting Director, Palo Alto Networks

12:35–12:55 / 16:35–16:55 UTC — ***2021 SANS DFIR Survey Results*** **(Hosted in Track 1 & Plenary)**
Jason Jordaan

CPEs & Certificate of Completion

- You will receive 12 CPEs for attending the SANS DFIR Summit – 6 for each day you attend – and 6 CPEs for attending the Solutions Track.
- Currently, we are not able to issue CPEs to those that view the Summit or Solutions Track recordings
- A Certificate of Completion will be available in your account after the conclusion of the Summit & Training on July 31
- SANS will automatically submit your CPEs to GIAC within 7-10 days after the event end date of July 31 – no action is required on your part.

SANS DFIR SUMMIT 2021



Americas Session (Continued)

Day 1 | Thursday, July 22

#DFIRSummit

View the complete agenda **here**.

1:15–1:50 PM EDT
17:15–17:50 UTC

Track 1 & Plenary

Panel: Validating Evidence for Courtroom Testimony

Moderator: Heather Mahalik, Senior Instructor, SANS Institute
John Bair, Senior Consultant, Digital Forensics; Testifying Expert, Lighthouse
Alexis Brignoni, Special Agent, Federal Law Enforcement
Mattia Epifani, Instructor, SANS Institute
Jessica Hyde, Magnet Forensics
Paul Lorentz, Technical Account Expert – Canada, Cellebrite
Christophe Poirier, Cybersecurity Team Leader, Edvance
Ian Whiffin, Senior Digital Intelligence Expert, Cellebrite
Mike Williamson, Forensic Consultant, Magnet Forensics

1:55–2:30 PM EDT
17:55–18:30 UTC

Track 1 & Plenary

A Holistic Approach to Defending Business Email Compromise Attacks

Korstiaan Stam, Founder, Invictus Incident Response

Track 2

Stringlifier: An Open Source Tool for Random String Classification

Vivek Malik, Security Engineer, Adobe
Kumar Vikramjeet, Security Engineer, Adobe

2:30–2:50 PM EDT
18:30–18:50 UTC

Break

2:50–3:25 PM EDT
18:50–19:25 UTC

Breaches Be Crazy

Eric Capuano, Certified Instructor, SANS Institute
Whitney Champion, Co-Founder & Lead Architect, Recon InfoSec

DFIR 101: Digital Forensics Essentials

Kathryn Hedley, Associate Instructor, SANS Institute

3:30–4:00 PM EDT
19:30–20:00 UTC

Track 1 & Plenary

Wrap-Up Panel

Philip Hagen, Senior Instructor, SANS Institute
Heather Mahalik, Senior Instructor, SANS Institute

4:00–5:00 PM EDT
20:00–21:00 UTC

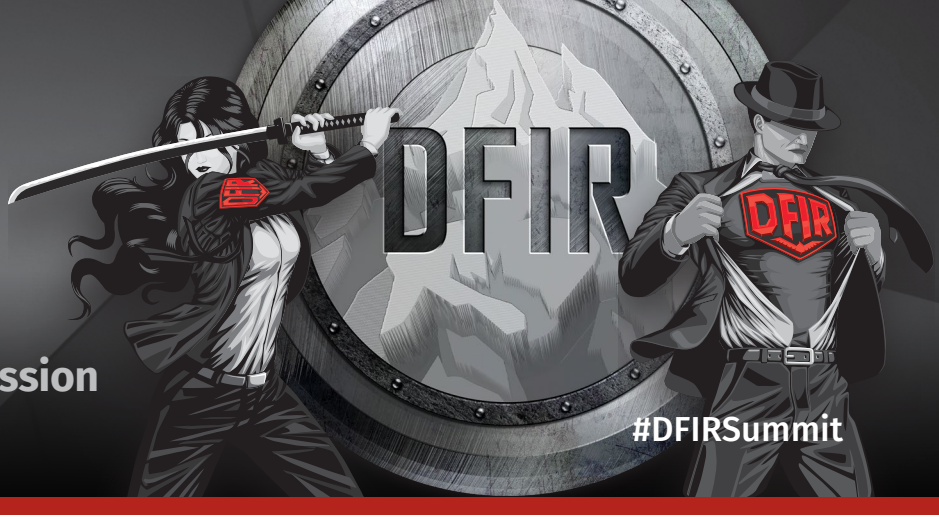
SANS.edu Happy Hour with Current Students and Staff

Please join SANS.edu for an informational happy hour. We will have representatives from both the Admissions and Academic Advising Team as guests on this panel. There will be live Q&A and conversation . We hope to see you there!

CPEs & Certificate of Completion

- You will receive 12 CPEs for attending the SANS DFIR Summit – 6 for each day you attend – and 6 CPEs for attending the Solutions Track.
- Currently, we are not able to issue CPEs to those that view the Summit or Solutions Track recordings
- A Certificate of Completion will be available in your account after the conclusion of the Summit & Training on July 31
- SANS will automatically submit your CPEs to GIAC within 7-10 days after the event end date of July 31 – no action is required on your part.

SANS DFIR SUMMIT 2021



Europe, Middle East & Africa Session

Day 2 | Friday, July 23

#DFIRSummit

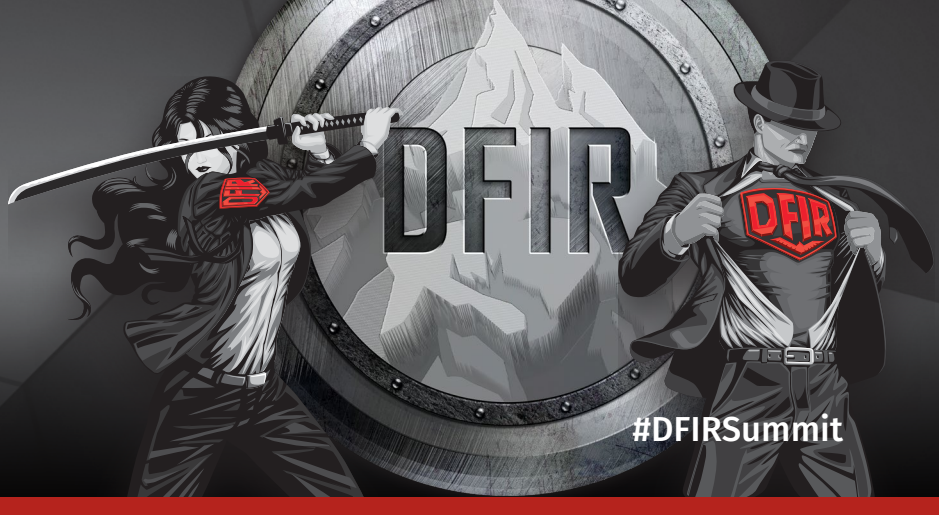
View the complete agenda **here**.

10:00–10:15 UTC 6:00–6:15 AM EDT	Track 1 & Plenary ***Welcome & Opening Remarks – EMEA*** Jason Jordaan, Certified Instructor, SANS Institute
10:15–10:50 UTC 6:15–6:50 AM EDT	Track 1 & Plenary ***Exploring Windows Command-Line Obfuscation*** Wietze Beukema, Threat Detection Engineer, PwC UK
10:55–11:30 UTC 6:55–7:30 AM EDT	Track 1 & Plenary ***Forensic Analysis of Xiaomi IoT Ecosystem*** Evangelos Dragonas, Digital Forensics Researcher, University of Piraeus
11:35–12:10 UTC 7:35–8:10 AM EDT	Track 1 & Plenary ***Incident Response 9-Line*** Gerard Johansen, Principal Incident Handler, Fortalice Solutions
12:15–12:50 UTC 8:15–8:50 AM EDT	Track 1 & Plenary ***IR Playbooks: A New Open Source Resource*** Mathieu Saulnier, Sr. Manager, Incident Response, Syntax
12:50–13:00 UTC 8:50–9:00 AM EDT	**Break**

CPEs & Certificate of Completion

- You will receive 12 CPEs for attending the SANS DFIR Summit – 6 for each day you attend – and 6 CPEs for attending the Solutions Track.
- Currently, we are not able to issue CPEs to those that view the Summit or Solutions Track recordings
- A Certificate of Completion will be available in your account after the conclusion of the Summit & Training on July 31
- SANS will automatically submit your CPEs to GIAC within 7-10 days after the event end date of July 31 – no action is required on your part.

SANS DFIR SUMMIT 2021



Americas Session

Day 2 | Friday, July 23

#DFIRSummit

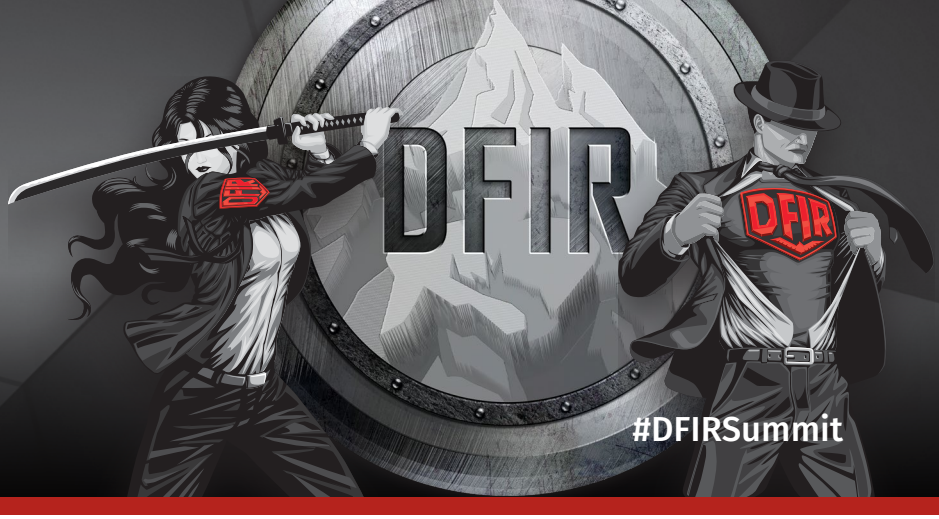
View the complete agenda **here**.

9:00–9:15 AM EDT 13:00–13:15 UTC	Track 1 & Plenary ***Welcome – Americas Day 2*** Philip Hagen, Senior Instructor, SANS Institute Heather Mahalik, Senior Instructor, SANS Institute
9:15–9:55 AM EDT 13:15–13:55 UTC	Track 1 & Plenary ***The Future of Work: Finding Evil Without Losing Your Mind – A Keynote Conversation About Keeping Mental Health and Wellness at the Center*** Melinda Lee Ferguson, Vice President of UK & Ireland, VMware Heather Mahalik, Senior Instructor, SANS Institute
10:00–10:35 AM EDT 14:00–14:35 UTC	Track 1 & Plenary ***Scoring and Judging Artifacts in Autopsy*** Brian Carrier, CTO, Basis Technology
10:35–10:40 AM EDT 14:35–14:40 UTC	**Break**
10:40–11:15 AM EDT 14:40–15:15 UTC	Track 1 & Plenary ***UFOs (Unidentified Forensic Objects)*** Ian Whiffin, Senior Digital Intelligence Expert, Cellebrite
11:20–11:55 AM EDT 15:20–15:55 UTC	Track 1 & Plenary ***Reporting for Digital Forensics*** Jason Wilkins, Digital Forensics Examiner, Clayton County Police Dept.
11:55 AM – 1:00 PM EDT 15:55–17:00 UTC	**Lunch & Bonus Presentation** 12:15–12:45 / 16:15–16:45 UTC ***SANS DFIR: What's New and What's Next*** **Philip Hagen**, Senior Instructor, SANS Institute **Heather Mahalik**, Senior Instructor, SANS Institute

CPEs & Certificate of Completion

- You will receive 12 CPEs for attending the SANS DFIR Summit – 6 for each day you attend – and 6 CPEs for attending the Solutions Track.
- Currently, we are not able to issue CPEs to those that view the Summit or Solutions Track recordings
- A Certificate of Completion will be available in your account after the conclusion of the Summit & Training on July 31
- SANS will automatically submit your CPEs to GIAC within 7-10 days after the event end date of July 31 – no action is required on your part.

SANS DFIR SUMMIT 2021



Americas Session (Continued)

Day 2 | Friday, July 23

#DFIRSummit

View the complete agenda **here**.

1:00–1:35 PM EDT 17:00–17:35 UTC	Track 1 & Plenary ***Where Have UAL Been?*** Brian Moran, CTO, BriMor Labs Kevin Stokes, Senior Associate – Cyber Response Services, KPMG
1:40–2:15 PM EDT 17:40–18:15 UTC	Track 1 & Plenary ***OCR'ing the Bitmap Cache Puzzle*** Drew Luckenbaugh, Cyber Security Services Associate, KPMG
2:15–2:25 PM EDT 18:15–18:25 UTC	**Break**
2:25–3:00 PM EDT 18:25–19:00 UTC	Track 1 & Plenary ***Crossing the Threshold: Analysis of the Facebook Portal Mini*** Jessica Hyde, Magnet Forensics Nicole Odom, Forensic Scientist – Digital & Multimedia Evidence, Virginia Dept. of Forensic Science Sarah Hayes, Digital Forensics Researcher, Hexordia
3:00–3:35 PM EDT 19:00–19:35 UTC	Track 1 & Plenary ***Forensic 4Cast Awards*** Lee Whitfield, Certified Instructor, SANS Institute
3:35–4:15 PM EDT 19:35–20:15 UTC	***Wrap-Up Panel*** Philip Hagen, Senior Instructor, SANS Institute Heather Mahalik, Senior Instructor, SANS Institute

CPEs & Certificate of Completion

- You will receive 12 CPEs for attending the SANS DFIR Summit – 6 for each day you attend – and 6 CPEs for attending the Solutions Track.
- Currently, we are not able to issue CPEs to those that view the Summit or Solutions Track recordings
- A Certificate of Completion will be available in your account after the conclusion of the Summit & Training on July 31
- SANS will automatically submit your CPEs to GIAC within 7-10 days after the event end date of July 31 – no action is required on your part.

SANS DFIR SUMMIT 2021

The DFIR Summit Solutions Track showcases case-studies and thought leadership to provide security practitioners with the latest industry leading products and services they can use to improve their forensic and incident response capabilities.

Solutions Track

Day 2 | Friday, July 23

#DFIRSummit

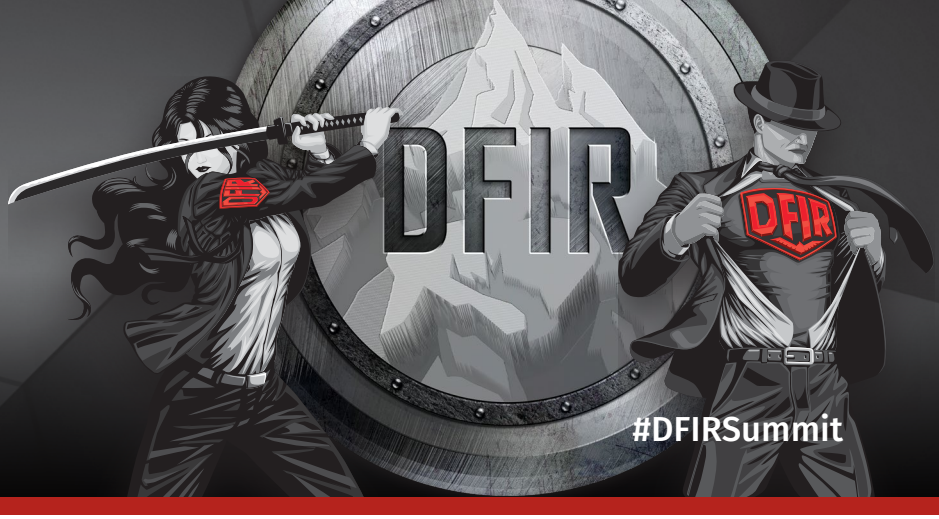
View agenda and register here.

10:00–10:15 AM EDT 14:00–14:15 UTC	***Welcome & Introduction*** Mari DeGrazia, Certified Instructor, SANS Institute
10:15–10:50 AM EDT 14:15–14:50 UTC	***Identifying and Leveraging DNS Abuse with DomainTools Iris*** Taylor Wilkes-Pierce, Senior Sales Engineer, DomainTools
10:50–11:25 AM EDT 14:50–15:25 UTC	***Ransomware Under Review: Leveraging Cloud Investigations When Data is the Hostage*** Keith Manville, Technical Solutions Architect, Cisco Umbrella
11:25 AM – 12:00 PM EDT 15:25–16:00 UTC	***Threat Intelligence in the Mobile Space*** Alex Jay Balan, Security Research Director, Bitdefender
12:00–12:10 PM EDT 16:00–16:10 UTC	**Break**
12:10–12:50 PM EDT 16:10–16:50 UTC	***Digital Forensics and the Enterprise Cloud: A Panel Discussion*** *Moderator:* Jessica Hyde, Director of Forensics, Magnet Forensics *Panelists:* Kirk Arthur, Sr. Director, WW Public Safety and Justice, Microsoft David Cowen, Certified Instructor, SANS Institute Jamie McQuaid, Technical Forensic Consultant, Magnet Forensics
12:50–1:00 PM EDT 16:50–17:00 UTC	**Break**
1:00–1:35 PM EDT 17:00–17:35 UTC	***Hunting Advanced Threats with Forensic Analysis*** Jason Mical, Global Cybersecurity Evangelist, Devo
1:35–2:10 PM EDT 17:35–18:10 UTC	***Exploiting NDR to Cultivate Decision Advantage*** Bernard Brantley, CISO, Corelight
2:10–2:45 PM EDT 18:10–18:45 UTC	***Exploring Incident Response: Four Common Mistakes*** Seth Geftic, Director, Endpoint Security Group, Sophos
2:45–3:00 PM EDT 18:45–19:00 UTC	**Break**
3:00–3:35 PM EDT 19:00–19:35 UTC	***Conducting Modern Digital Investigations in a Remote Workforce*** James Kritselis, Senior Solutions Consultant, OpenText
3:35–4:10 PM EDT 19:35–20:10 UTC	***Death, Taxes, and Ransomware: Make the Inevitable, Avoidable*** Arif Khan, Senior Director, NA Technical Services, Pentera
4:10–4:45 PM EDT 20:10–20:45 UTC	***Buff Your Cloud Game*** James Campbell, CEO & CO-Founder, Cado Security Al Carchrie, Head of Solution Management, Cado Security
4:45–5:00 PM EDT 20:45–21:00 UTC	***Wrap-Up*** Mari DeGrazia, Certified Instructor, SANS Institute

CPEs & Certificate of Completion

- You will receive 12 CPEs for attending the SANS DFIR Summit – 6 for each day you attend – and 6 CPEs for attending the Solutions Track.
- Currently, we are not able to issue CPEs to those that view the Summit or Solutions Track recordings
- A Certificate of Completion will be available in your account after the conclusion of the Summit & Training on July 31
- SANS will automatically submit your CPEs to GIAC within 7-10 days after the event end date of July 31 – no action is required on your part.

SANS DFIR SUMMIT 2021



Time Zones | Day 1 (Thu, July 22+)

PACIFIC	6AM	7AM	8AM	9AM	10AM	11AM	12PM	1PM	2PM	3PM	4PM	5PM	6PM	7PM	8PM	9PM	10PM	11PM	12AM				
CENTRAL	6AM	7AM	8AM	9AM	10AM	11AM	12PM	1PM	2PM	3PM	4PM	5PM	6PM	7PM	8PM	9PM	10PM	11PM	12AM				
EASTERN	6AM	7AM	8AM	9AM	10AM	11AM	12PM	1PM	2PM	3PM	4PM	5PM	6PM	7PM	8PM	9PM	10PM	11PM	12AM				
BRITISH SUMMER TIME	6AM	7AM	8AM	9AM	10AM	11AM	12PM	1PM	2PM	3PM	4PM	5PM	6PM	7PM	8PM	9PM	10PM	11PM	12AM				
CENTRAL EUROPEAN SUMMER TIME	6AM	7AM	8AM	9AM	10AM	11AM	12PM	1PM	2PM	3PM	4PM	5PM	6PM	7PM	8PM	9PM	10PM	11PM	12AM				
INDIA	6AM	7AM	8AM	9AM	10AM	11AM	12PM	1PM	2PM	3PM	4PM	5PM	6PM	7PM	8PM	9PM	10PM	11PM	12AM	→ 1:30AM FRIDAY			
SINGAPORE	6AM	7AM	8AM	9AM	10AM	11AM	12PM	1PM	2PM	3PM	4PM	5PM	6PM	7PM	8PM	9PM	10PM	11PM	12AM	→ 4:00AM FRIDAY			
AUSTRALIAN EASTERN	6AM	7AM	8AM	9AM	10AM	11AM	12PM	1PM	2PM	3PM	4PM	5PM	6PM	7PM	8PM	9PM	10PM	11PM	12AM	→ 7:00AM FRIDAY			
UTC	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00	20:00	21:00	22:00	23:00	0:00	1:00	2:00	3:00	4:00				

Time Zones | Day 2 (Fri, July 23+)

PACIFIC	3AM	4AM	5AM	6AM	7AM	8AM	9AM	10AM	11AM	12PM	1PM	2PM	3PM	4PM	5PM	6PM	7PM	8PM	9PM				
CENTRAL	3AM	4AM	5AM	6AM	7AM	8AM	9AM	10AM	11AM	12PM	1PM	2PM	3PM	4PM	5PM	6PM	7PM	8PM	9PM				
EASTERN	3AM	4AM	5AM	6AM	7AM	8AM	9AM	10AM	11AM	12PM	1PM	2PM	3PM	4PM	5PM	6PM	7PM	8PM	9PM				
BRITISH SUMMER TIME	3AM	4AM	5AM	6AM	7AM	8AM	9AM	10AM	11AM	12PM	1PM	2PM	3PM	4PM	5PM	6PM	7PM	8PM	9PM				
CENTRAL EUROPEAN SUMMER TIME	3AM	4AM	5AM	6AM	7AM	8AM	9AM	10AM	11AM	12PM	1PM	2PM	3PM	4PM	5PM	6PM	7PM	8PM	9PM				
INDIA	3AM	4AM	5AM	6AM	7AM	8AM	9AM	10AM	11AM	12PM	1PM	2PM	3PM	4PM	5PM	6PM	7PM	8PM	9PM	→ 1:30AM SATURDAY			
SINGAPORE	3AM	4AM	5AM	6AM	7AM	8AM	9AM	10AM	11AM	12PM	1PM	2PM	3PM	4PM	5PM	6PM	7PM	8PM	9PM	→ 4:00AM SATURDAY			
AUSTRALIAN EASTERN	3AM	4AM	5AM	6AM	7AM	8AM	9AM	10AM	11AM	12PM	1PM	2PM	3PM	4PM	5PM	6PM	7PM	8PM	9PM	→ 5:00AM SATURDAY			
UTC	7:00	8:00	9:00	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00	20:00	21:00	22:00	23:00	0:00	1:00				