★ THE WORLD'S LARGEST & MOST TRUSTED PROVIDER OF CYBER SECURITY TRAINING ★

SANS EMEA

# DFIR PRAGUE 2016

MON 3 – SAT 15 OCTOBER, 2016 #DFIRPRAGUE

## 8 SANS COURSES AND THE DIGITAL FORENSICS INCIDENT RESPONSE SUMMIT

**FOR408**
Windows Forensic Analysis

**FOR508**
Advanced Digital Forensics and Incident Response

**FOR518**
Mac Forensic Analysis

**FOR526**
Memory Forensics In-Depth

**FOR572**
Advanced Network Forensics and Analysis

**FOR578**
Cyber Threat Intelligence

**FOR585**
Advanced Smartphone Forensics

**FOR610**
Reverse-Engineering Malware Malware Analysis Tools and Techniques

Register online and see full course descriptions at **www.sans.org/dfir-prague-2016**

# ABOUT SANS

SANS is the world's largest provider of cyber security training. We now train over 40,000 cyber security professionals around the world each year. We operate across 30 geographic regions. In those regions SANS trains cyber security operatives and managers who work in government departments, for military bodies and for large commercial organisations.

# COURSES AT A GLANCE

| | | MO 3 | TU 4 | WE 5 | TH 6 | FR 7 | SA 8 | SU 9 | MO 10 | TU 11 | WE 12 | TH 13 | FR 14 | SA 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| FOR 408 | **Windows Forensic Analysis** *Chad Tilbury* | ● | ● | ● | ● | ● | ● | Digital Forensics Incident Response Summit – 9th Oct | | | | | | |
| FOR 508 | **Advanced Digital Forensics and Incident Response** *Jess Garcia* | | | | | | | | ● | ● | ● | ● | ● | ● |
| FOR 518 | **Mac Forensic Analysis** *Sarah Edwards* | ● | ● | ● | ● | ● | ● | | | | | | | |
| FOR 526 | **Memory Forensics In-Depth** *Jake Williams* | | | | | | | | ● | ● | ● | ● | ● | ● |
| FOR 572 | **Advanced Network Forensics and Analysis** *Philip Hagen* | | | | | | | | ● | ● | ● | ● | ● | ● |
| FOR 578 | **Cyber Threat Intelligence** *Jake Williams* | ● | ● | ● | ● | ● | | | | | | | | |
| FOR 585 | **Advanced Smartphone Forensics** *Cindy Murphy* | ● | ● | ● | ● | ● | ● | | | | | | | |
| FOR 610 | **Reverse-Engineering Malware: Malware Analysis Tools and Techniques** *Lenny Zeltser* | | | | | | | | ● | ● | ● | ● | ● | ● |

**REGISTER NOW** www.sans.org/dfir-prague-2016

# WELCOME TO DFIR PRAGUE 2016

**DFIR PRAGUE RUNS FROM THE 3RD OCTOBER – 15TH OCTOBER AT THE ANGELO HOTEL AND HOSTS 8 COURSES DRAWN FROM ACROSS THE SANS DFIR CURRICULUM.**

Registration fees include all courseware and training materials plus morning and afternoon break refreshments and lunch served in the hotel venue. Accommodation is not included.

Students are able to attend free evening functions. Please register online as soon as possible to secure a seat at DFIR Prague 2016.

Read on for course descriptions or visit www.sans.org/dfir-prague-2016


**VENUE**
Angelo Hotel Prague
Radlicka 1-G, Prague 5
Prague, CZ

**REGISTER NOW** www.sans.org/dfir-prague-2016

# CONTACT SANS

**www.sans.org/emea**
**Email:** emea@sans.org
**Tel:** +44 20 3384 3470

**Address:**
SANS EMEA, PO Box 124,
Swansea, SA3 9BB, UK
**@SANSEMEA**


**WWW.SANS.ORG/FOR408**

## WINDOWS FORENSIC ANALYSIS

CHAD TILBURY

This course focuses on building in-depth digital forensics knowledge of the Microsoft Windows operating systems. You'll learn to recover, analyse, and authenticate forensic data, and you will gain an understanding of how to track detailed user activity on your network and how to organise findings for use in incident response, internal investigations, and civil/criminal litigation.


**WWW.SANS.ORG/FOR508**

## ADVANCED DIGITAL FORENSICS AND INCIDENT RESPONSE

JESS GARCIA

This in-depth incident response course provides responders with advanced skills to hunt down, counter, and recover from a wide range of threats within enterprise networks, including APT adversaries, organised crime syndicates, and hactivism. Constantly updated, the course provides hands-on incident response tactics and techniques that elite responders are successfully using in real-world breach cases today.


**WWW.SANS.ORG/FOR518**

## MAC FORENSIC ANALYSIS

SARAH EDWARDS

Mac Forensic Analysis aims to form a well-rounded investigator by introducing Mac forensics into a Windows-based forensics world. This course focuses on topics such as the HFS+ file system, Mac specific data files, tracking user activity, system configuration, analysis and correlation of Mac logs, Mac applications, and Mac exclusive technologies. A computer forensic analyst who successfully completes the course will have the skills needed to take on a Mac forensics case.


**WWW.SANS.ORG/FOR526**

## MEMORY FORENSICS IN-DEPTH

JAKE WILLIAMS

This is a critical course for any serious DFIR investigator who wants to tackle advanced forensics, trusted insider, and incident response cases. In today's forensics cases, it is just as critical to understand memory structures, as it is to understand disk and registry structures. Having in-depth knowledge of Windows memory internals allows the examiner to access target data specific to the needs of the case at hand.

**REGISTER NOW** www.sans.org/dfir-prague-2016

WWW.SANS.ORG/FOR572

## ADVANCED NETWORK FORENSICS AND ANALYSIS

PHILIP HAGEN

FOR572 was built from the ground up to cover the most critical skills needed to mount efficient and effective post-incident response investigations. It covers the tools, technology and processes required to integrate network evidence sources into investigations, with a focus on efficiency and effectiveness.


WWW.SANS.ORG/FOR578

## CYBER THREAT INTELLIGENCE

JAKE WILLIAMS

When considering the value of threat intelligence, most individuals and organisations ask themselves three questions: What is threat intelligence? When am I ready for it? How do I use it? This class answers these questions and more at a critical point in the development of the field of threat intelligence in the wider community.


WWW.SANS.ORG/FOR585

## ADVANCED SMARTPHONE FORENSICS

CINDY MURPHY

This new course focuses on smartphones as sources of evidence, providing the necessary skills to handle mobile devices in a forensically sound manner, understand the different technologies, discover malware, and analyse the results for use in digital investigations by diving deeper into the file systems of each smartphone.


WWW.SANS.ORG/FOR610

## REVERSE-ENGINEERING MALWARE: MALWARE ANALYSIS TOOLS AND TECHNIQUES

LENNY ZELTSER

This popular malware analysis course has helped forensics investigators, malware specialists, incident responders and IT administrators assess malware threats. The course teaches a practical approach to examining malicious programs including spyware, bots, trojans and others that target and infect Windows systems.

SANS EMEA

# DIGITAL FORENSICS & INCIDENT RESPONSE SUMMIT

## 9th October
## chaired by Jess Garcia

SANS Digital Forensics & Incident Response Summit brings our most popular forensics courses, instructors, and expert speakers together in one place to offer the most comprehensive DFIR experiences. This must- attend event for you and your team is perfect for building the DFIR skills that will take you to that next level.

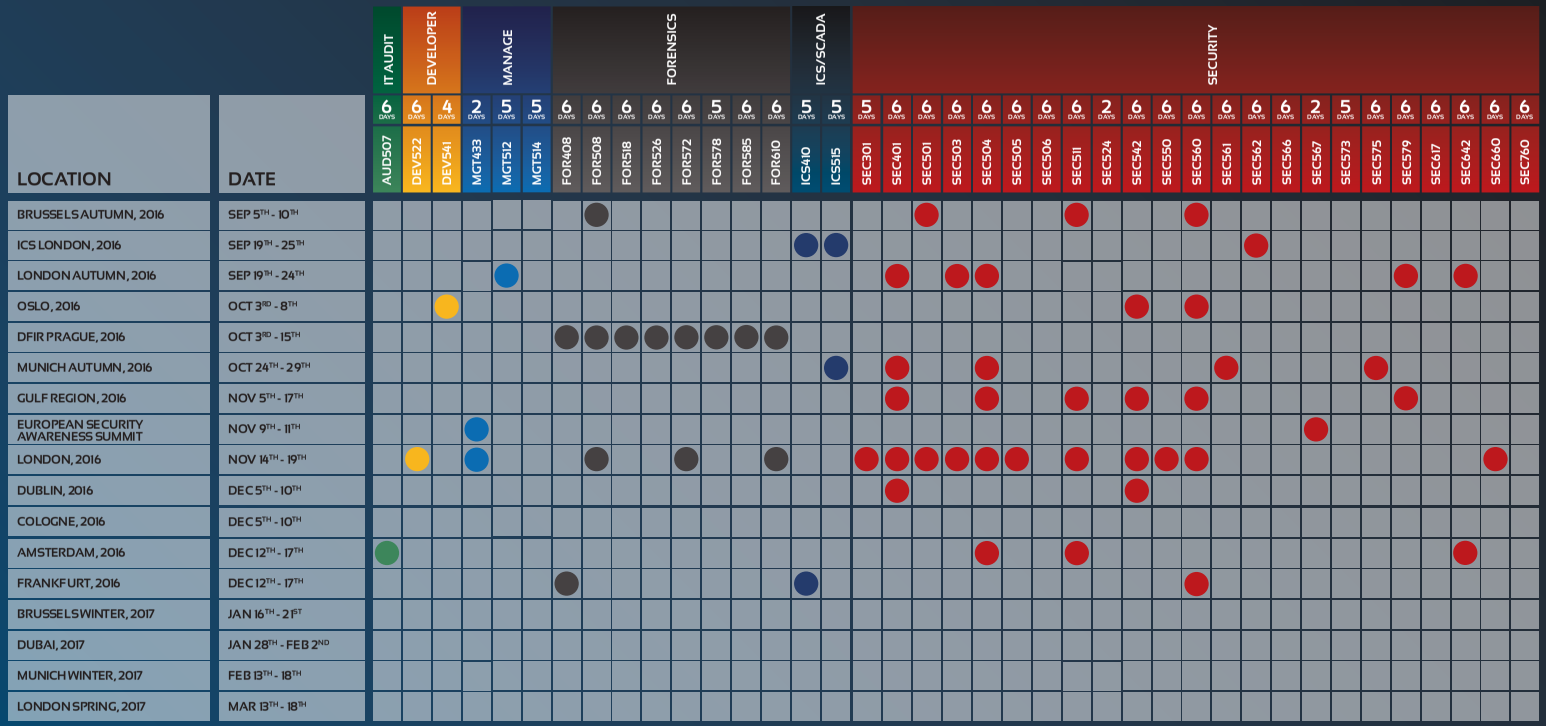
## Top 3 Reasons to Attend:

1. **Expert DFIR Speakers** – 1 day packed with expert talks keeping you up to date on the latest DFIR techniques and tradecraft.
2. **DFIR-Focused Training** – DFIR Prague hosts eight SANS DFIR training classes covering every topic that SANS DFIR can offer.
3. **Community** – Not-to-be-missed annual event for the DFIR community. Join your peers in the industry to tackle advanced DFIR issues.

**To find out more and register see:**
**www.sans.org/dfir-prague-2016**

# FUTURE SANS EMEA TRAINING EVENTS

For a full list of training events, please visit www.sans.org




V20 A5

Most courses are also available online, via SANS OnDemand. Contact emea@sans.org for information.

Dates, locations and courses offered subject to change