SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE

SANS EMEA

OCTOBER 5TH TO 17TH 2015 – PRAGUE, CZECH REPUBLIC

SANS DFIR PRAGUE

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

DFIR NETWARS

8 SANS DFIR COURSES AND DIGITAL FORENSICS INCIDENT RESPONSE SUMMIT

Immersive Training ★ World Class Instructors ★ GIAC Certification ★ SANS@Night evening talks and networking ★ Social Functions

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/event/DFIRPRAGUE**

See inside for unique code – register and pay before September 2nd and **save €375**

HM Government
SANS is a Cyber Security Supplier to Government

GIAC

COURSES AT A GLANCE

SANS EMEA

		MON 05	TUE 06	WED 07	THU 08	FRI 09	SAT 10	SUN 11	MON 12	TUE 13	WED 14	THU 15	FRI 16	SAT 17
FOR 408	Windows Forensic Analysis	Rob Lee	PG 12 →											
FOR 508	Advanced Digital Forensics and Incident Response	Jess Garcia							PG 13 →					
FOR 518	Mac Forensic Analysis	Sarah Edwards	PG 14 →											
FOR 526	Memory Forensics In-Depth	Alissa Torres							PG 15 →					
FOR 572	Advanced Network Forensics and Analysis	Philip Hagen	PG 16 →											
FOR 578	Cyber Threat Intelligence	Robert M. Lee							PG 17 →					
FOR 585	Advanced Smartphone Forensics	Cindy Murphy	PG 18 →											
FOR 610	Reverse-Engineering Malware: Malware Analysis Tools and Techniques	Anuj Soni							PG 19 →					
	Digital Forensics Incident Response Summit	Chair: Jess Garcia						●						

Follow us on Twitter: @SANSEMEA @sansforensics #DFIRPrague

SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE

Register now: www.sans.org/DFIRPrague

WHY ATTEND SANS DFIR PRAGUE 2015?

Whether you're new to the field or a seasoned professional, SANS DFIR Summit & Training is the premier forensic training event created to help you tackle advanced DFIR issues.

Choose from eight SANS DFIR courses taught by industry experts, one day of talks at the European DFIR Summit and take advantage of the opportunity to have real discussions with the best leaders in the community.

Top 5 Reasons to Attend:

1. DFIR Focused Training - The event hosts all the Digital Forensics and
1. Incident Response training classes SANS has to offer in Europe. Eight classes across two weeks, all led by SANS Instructors.
2. Summit Talks - The summit is packed with trending talks and leading speakers covering the most innovative DFIR topics. Listen to informative and entertaining presentations and network with peers, SANS instructors and other leaders from the field of DFIR.
3. DFIR NetWars - Free if you sign up for a class: SANS DFIR NetWars is a hands-on, interactive learning environment that enables DFIR professionals to develop and master the skills they need to excel in their field.
4. FOR578 - Cyber Threat Intelligence SANS Course Launch. Debuting in Prague, this new track trains you and your team to detect, scope, and select resilient courses of action in response to intrusions and data breaches.
5. Prague - Bring your team to learn during the day and enjoy beautiful Old Town Prague in the evening with DFIR friends and colleagues. Time and again, we are told that the networking opportunities and industry connections made are a key value of an event like this.

"Cutting-edge research shared by those in the trenches and the front-lines of digital forensics and incident response. A must-attend event for every DFIR professional!"

Brad Garnett
Kemper CPA Group LLP

"This is a meeting of the greatest minds in DFIR. I was so impressed with the supportive community and feel I have made long-lasting friends plus fellow security partners."

Pete Hainlen
Mayo Clinic

"The Summit is a great way to get to know leaders, newcomers, and everyone in between. The networking at a smaller event like this is worth it alone – and the presentations make it much more valuable. It's always a great time."

Stacey Edwards
The Sylint Group

SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE

CONTENTS

Follow us on Twitter:
@SANSEMEA
@sansforensics
#DFIRPrague

SANS EMEA:
PO Box 124,
Swansea, SA3 9BB, UK

SANS EMEA

ABOUT SANS

SANS is the most trusted and by far the largest source for information security training and security certification in the world.

SANS provides intensive training designed to help you and your staff master the practical steps necessary for defending systems and networks against the most dangerous threats - the ones being actively exploited.

Why SANS is the best training and educational investment

- Intensive, hands-on immersion training with the highest-quality courseware in the industry.
- Incomparable instructors and authors who are industry experts and practitioners fighting the same cyber battles as you and discovering new ways to thwart attacks.
- Training that strengthens a student's ability to achieve a GIAC certification, which is unique in the field of information security certifications because it not only tests a candidate's knowledge, but also the candidate's ability to put that knowledge into practice in the real world.

Register now: www.sans.org/DFIRPrague

SANS DFIR PRAGUE 2015
REGISTRATION INFORMATION

REGISTER ONLINE AT: WWW.SANS.ORG/DFIRPRAGUE

REGISTER EARLY AND SAVE

Register for #DFIRPrague and pay before the 2nd of September and save €375 by entering the code EarlyBird15

All course prices are listed at sans.org/DFIRPRAGUE

GROUP SAVINGS
(APPLIES TO TUITION ONLY)

5-9 people = 5%

10 or more people = 10%

Early bird rates and/or other discounts cannot be combined with the group discount.

To obtain a group discount please email emea@sans.org.

TO REGISTER

To register, go to **sans.org/DFIRPRAGUE**
Select your course or courses and indicate whether you plan to test for GIAC certification.

How to tell if there is room available in a course: If the course is still open, the secure, online registration server will accept your registration. Sold-out courses will be removed from the online registration. Everyone with internet access must complete the online registration form. We do not take registrations by phone.

CONFIRMATION

Look for e-mail confirmation. It will arrive soon after you register. We recommend you register and pay early to ensure you get your first choice of courses.

An immediate e-mail confirmation is sent to you when the registration is submitted properly. If you have not received e-mail confirmation within two business days of registering, please call the SANS Registration office at +1 301-654-7267, 9:00am - 8:00pm Eastern Time or email emea@sans.org.

CANCELLATION

You may subsitute another person in your place at any time by sending an e-mail request to emea@sans.org.

Cancellation requests by Sep 23rd, 2015, by emailing emea@sans.org

SANS EMEA

SANS IT SECURITY TRAINING AND YOUR

CAREER ROAD MAP

CORE COURSES

FUNCTION: CYBER OR IT SECURITY MANAGEMENT

Management of people, processes, and technologies is critical for maintaining proactive enterprise situational awareness and for the ongoing success of continuous monitoring efforts. Leadership must be armed with current knowledge and best practice examples to make timely and effective decisions that benefit the entire enterprise information infrastructure.

SAMPLE JOB TITLES:
Developer, Software architect, QA tester, Dev manager

CORE COURSES
301 ▸ 401 ▸ 501

- **MGT512** SANS Security Leadership Essentials For Managers with Knowledge Compression™ GSLC ✓
- **SEC440** 20 Critical Security Controls: Planning, Implementing, and Auditing
- **MGT414** SANS® +S™ Training Program for CISSP®Certification Exam
  - **MGT514** IT Security Strategic Planning, Policy & Leadership
- **MGT525** IT Project Management, Effective Communication, and PMP® Exam Prep GCPM
  - **MGT535** Incident Response Team Management
- **MGT433** Securing The Human: Building and Deploying an Effective Security Awareness Program ✓
- **LEG523** Law of Data Security and Investigations GLEG

FUNCTION: INFORMATION SECURITY

Responsible for research and analysis of security threats that may affect a company's assets, products or technical specifications. This analyst will dig into technical protocols and specifications for a greater understanding of security threats than most of his/her peers, identifying strategies to defend against attacks through intimate knowledge of the threats.

SAMPLE JOB TITLES:
IT security analyst , IT security engineer, IT security architect

- **SEC301** Intro to Information Security GISF
- **SEC401** Security Essentials Bootcamp Style GSEC ✓

CORE COURSES
301 ▸ 401

- **SEC501** Advanced Security Essentials Enterprise Defender GCED ✓
- **SEC504** Hacker Techniques, Exploits, and Incident Handling GCIH ✓

FUNCTION: INCIDENT RESPONSE

When the security of a system or network has been compromised, the incident responder is the first-line defense during the breach. The responder not only has to be technically astute, he/she must be able to handle stress under fire while navigating people, processes, and technology to help respond and mitigate a security incident.

SAMPLE JOB TITLES:
Security analyst/engineer, SOC analyst, Cyber threat analyst, CERT member, Malware analyst

CORE COURSES
301 ▸ 401 ▸ 504

Network Analysis

- **SEC503** Computer Forensic Investigations Windows In-Depth GCIA ✓
- **FOR572** Advanced Network Forensics and Analysis ✓
- **FOR578** Cyber Threat Intelligence ✓

Endpoint Analysis

- **FOR408** Windows Forensic Analysis GCFE ✓
- **FOR508** Advanced Digital Forensics and Incident Response GCFA ✓

Malware Analysis

- **FOR610** Reverse Engineering Malware: Malware Analysis Tools & Techniques GREM ✓

Specialisations

- **FOR526** Windows Memory Forensics In-Depth ✓
- **MGT535** Incident Response Team Management

FUNCTION: PENETRATION TESTING/ VULNERABILITY ASSESSMENT

Because offense must inform defense, these experts provide enormous value to an organization by applying attack techniques to find security vulnerabilities, analyze their business risk implications, and recommend mitigations before they are exploited by real-world attackers.

SAMPLE JOB TITLES:
Penetration tester, Vulnerability assessor, Ethical hacker, Red/Blue team member

CORE COURSES
301 ▸ 401 ▸ 504

Enterprise

- **SEC560** Network Penetration Testing and Ethical Hacking GPEN ✓
- **SEC561** Hands-on Penetration Testing for the InfoSec Pro ✓
- **SEC660** Advanced Penetration Testing, Exploits, & Ethical Hacking GXPN ✓
- **SEC760** Advanced Exploit Development for Penetration Testers ✓

Web

- **SEC542** Web App Penetration Testing and Ethical Hacking GWAPT ✓
- **SEC642** Advanced Web App Penetration Testing and Ethical Hack ✓

Wireless/ Mobile

- **SEC575** Mobile Device Security and Ethical Hacking GMOB ✓
- **SEC617** Wireless Ethical Hacking, Penetration Testing, and Defenses GAWN ✓

Lab Centred

- **SEC561** Intense Hands-on Pen Testing Skill Development (with SANS NetWars) ✓
- **SEC562** CyberCity Hands-on Kinetic Cyber Range Exercise ✓

Specialisations

- **SEC580** Metasploit Kung Fu for Enterprise Pen Testing ✓
- **SEC573** Python for Penetration Testers ✓

✓ = Live training available in EMEA

FUNCTION:

NETWORK OPS CENTER, SYSTEM ADMIN, SECURITY ARCHITECTURE

A network operations center (NOC) is a place from which IT professionals supervise, monitor and maintain the enterprise network. The network operations center is the focal point for network troubleshooting, software distribution and updating, router and system management, performance monitoring, and coordination with affiliated networks. The NOC works hand-in-hand with the SOC, which safeguards the enterprise and continuously monitors for threats against it.

SAMPLE JOB TITLES:
System/IT administrator, Security administrator , Security architect/engineer

CORE COURSES
301 ▸ 401 ▸ 501

- **SEC505** — Securing Windows and Resisting Malware — GCWN
- **SEC506** — Securing Linux/Unix — GCUX
- **SEC579** — Virtualization and Private Cloud Security
- **SEC566** — Implementing & Auditing the Twenty Critical Security Controls - In-Depth

FUNCTION:

RISK & COMPLIANCE/AUDITING/ GOVERNANCE TITLES

This expert assesses and reports risk to the organization by measuring compliance with policies, procedures, and standards. These experts make recommendations for improvements to make the organization more efficient and profitable through continuous monitoring risk management.

SAMPLE JOB TITLES:
Auditor, Compliance officer

- **SEC566** — Implementing & Auditing the Twenty Critical Security Controls - In-Depth
- **AUD507** — Auditing Networks, Perimeters, and Systems — GSNA

FUNCTION:

DEVELOPMENT SECURE DEVELOPMENT

The security-savvy software developer leads all developers in the creation of secure software, implementing secure programming techniques that are free from logical design and technical implementation flaws. This expert is ultimately responsible for ensuring customer software is free from vulnerabilities that can be exploited by an attacher.

SAMPLE JOB TITLES:
Developer, Software architect, QA tester, Development manager

Securing the Human for Developers STH.Developer
Application Security Awareness Modules

- **DEV522** — Defending Web Applications Security Essentials
  - **DEV541** — Secure Coding in Java/JEE: Developing Defensible Applications — GSNA
  - **DEV544** — Secure Coding in .NET: Developing Defensible Applications — GSNA

FUNCTION:

SECURITY OPERATIONS CENTER/INTRUSION DETECTION

Against cyber-related incidents, monitoring security, and protecting assets of the enterprise network and endpoints. SOC analysts are responsible for enterprise situational awareness and continuous surveillance, including monitoring traffic, blocking unwanted traffic to and from the Internet, and detecting any type of attack. Point solution security technologies are the starting point for hardening the network against possible intrusion attempts.

SAMPLE JOB TITLES:
Intrusion detection analyst, Security Operations Center analyst/engineer, CERT member, Cyber threat analyst

CORE COURSES
301 ▸ 401 ▸ 504

- Network Monitoring: **SEC502** — Perimeter Protection In-Depth — GCFW
- Network Monitoring: **SEC503** — Intrusion Detection In-Depth — GCIA
  - **FOR572** — Advanced Network Forensics & Analysis
    - **FOR578** — Cyber Threat Intelligence
- Network Monitoring: **SEC511** — Continuous Monitoring and Security Operations
- Endpoint Monitoring: **SEC501** — Advanced Security Essentials Enterprise Defender — GCED
  - **FOR508** — Advanced Digital Forensics and Incident Response — GCFA

FUNCTION:

DIGITAL FORENSIC INVESTIGATIONS & MEDIA EXPLOITATION

With today's ever-changing technologies and environments, it is inevitable that every organisation will deal with cybercrime, including fraud, insider threats, industrial espionage, and phishing. To help solve these challenges, organisations are hiring digital forensic professionals and relying on cybercrime law enforcement agents to piece together a comprehensive account of what happened.

SAMPLE JOB TITLES:
Computer crime investigator, Law enforcement, Digital investigations, Media exploitation analyst
Information technology litigation support and consultant analyst

- **FOR408** — Windows Forensic Analysis — GCFE
- **SEC504** — Hacker Techniques, Exploits, and Incident Handling — GCIH
  - **FOR508** — Advanced Digital Forensics and Incident Response — GCFA
    - **FOR526** — Windows Memory Forensics In-Depth
      - **FOR610** — Reverse Engineering Malware: Malware Analysis Tools & Techniques — GREM
  - **FOR585** — Advanced Smartphone and Mobile Device Forensics
  - **FOR518** — MAC Foremsic Analysis

FUNCTION:

INDUSTRIAL CONTROL SYSTEMS / SCADA

ICS-focused courses are designed to equip both security professionals and control system engineers with the knowledge and skills they need to safeguard our critical infrastructures.

SAMPLE JOB TITLES:
IT & OT Support, IT & OT Cybersecurity, ICS Engineer

SANS ICS410: ICS/SCADA Security Essentials — GICSP
Provides a set of standardized skills and knowledge for industrial cybersecurity professionals. The course is designed to ensure that the workforce involved in supporting and defending industrial control systems is trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats.

- **ICS515** — ICS Active Response and Defense & Response

Specialisations

- **SEC542** — Web App Penetration Testing & Ethical Hacking — GWAPT
- **SEC642** — Advanced Web App Penetration Testing & Ethical Hacking

SANS EUROPEAN DFIR Summit

Chaired by Jess Garcia, SANS DFIR Principle Instructor

Sunday 11 October, 2015

9:00 – 9:45 am	**Keynote: There's Something About WMI** This presentation will describe the purpose and components of Windows Management Instrumentation (WMI) from the incident response and forensics perspectives. Attendees will learn how targeted threats are using WMI during each phase of the compromise, case studies and examples, the artifacts generated by those activities, some of the tools used to interact with WMI, using WMI for persistent access that defeats antivirus and application whitelisting, and the benefits of enabling WMI trace logging for additional detection and improved analysis. **Christopher Glyer:** *Technical Director, MANDIANT, a FireEye Company* **Devon Kerr:** *Senior Consultant, MANDIANT, a FireEye Company*
9:45 – 10:30 am	**Inside Windows Phone 8: Forensic Acquisition and Analysis** A new operating system is growing in the mobile market: Windows Phone 8. Microsoft released this Mobile OS in 2013, and as of May 2015 it was in third position after Android and iOS for number of devices sold. In the last year more and more research has been developed regarding how to acquire data with JTAG techniques or based on BootROM exploit. The aim of this presentation is to illustrate the most commonly used procedures to extract data from Windows Phone 8 devices to obtain, when possible, a complete forensic image of the internal NAND, as well as to provide information about what can be extracted during analysis (internal data structure, file system, native apps, media files, third party apps, forensic artifacts, and so on). The talk will include a compelling case study of a criminal investigation of a home invasion and sexual assault where a Windows Phone 8 device provided crucial evidence resulting in a number of convictions. **Mattia Epifani:** *CEO, REALITY NET* **Cindy Murphy:** *MSc, Detective, Digital Forensics / Computer Crimes, Madison (WI) Police Department*

10:30 – 11:00 am	**Networking Break and Vendor Expo**
11:00 – 11:45 am	**Forensic Analysis of sUAS (aka Drones)** Small Unmanned Aerial Systems (sUAS) aka "drones" are all the rage – they are invading your privacy, they are delivering your packages (and illegal drugs), they are even landing on the White House lawn. Where have they been? Where are they going? Who launched them? Let's find out. sUAS – emphasis on the final 'S' – are complex systems. The aerial platform alone often consists of a radio link, an autopilot, a photography sub-system, a GPS, and multiple other sensors. Each one of these components might contain a wealth of pieces to the answer to the above questions. Add in the ground control stations, the radio controller, and the video downlink system and you have a very complex computing environment running a variety of commercial, closed source, open source, and home brew software. And yes, there is already malware specifically targeting drones. During this presentation, we will walk through all of the components of a representative drone and discuss the forensic process and potential artifacts of each component, along with a presentation of the overall story told by the individual components. **David Kovar:** *Senior Manager, Ernst & Young's Advisory Center of Excellence*
11:45 am – 12:15 pm	**Investigating Security Incidents Involving Microsoft Exchange Using In-Mailbox Forensic Artefacts** In most large organisations, Microsoft Exchange is far more than a mail system: it is effectively the organisational memory, storing huge volumes of email interactions as well as calendar data, contacts, notes, task lists and other user data. Security incidents involving Exchange are made more complex by this range of data, for example it can be difficult to determine exactly what mailboxes were compromised and which data within each mailbox might have been accessed. Fortunately, the number of forensically-valuable artefacts inside Exchange mailboxes is increasing. Recent versions of Exchange store far more data within user mailboxes rather than on end-user devices, and recent versions of Outlook also create useful artefacts in some odd locations within the mailbox. When dealing with a modern Exchange infrastructure, or with Exchange Online in Office 365, these artefacts are rich enough to reconstruct malicious activity down to the level of individual emails accessed. Of particular interest for incident responders, this reconstruction can be done without touching client devices and without reference to Exchange logs or other formal audit trails. By walking through a specific incident scenario, this session will show some of the in-mailbox artefacts which can be used to investigate malicious activity in Exchange. We will reconstruct a range of attacker actions including initial mailbox compromise, mailbox access and exploration, data extraction and activity monitoring. We will also cover methods for identifying and researching additional artefacts and hopefully provide something of a roadmap for others interested in Exchange forensics. **Kevin McGlone:** *Digital Evidence Specialist, Cernam* **Owen O'Connor:** *VP of Digital Evidence, Cernam*

12:15 – 1:30 pm	**Lunch**
1:30 – 2:15 pm	**New Generation Timeline Tools: A Case Study** A moderately-sized institution of higher learning receives an ominous threat from a shadowy hacker group. A plucky band of misfits, armed only with open source forensic tools is the college's only hope. What happens next? Will our brave band ofheroes be able to stop the cyber terrorists in time? This talk will give you a good understanding of the new features in the Plaso and Timesketch forensic tools, as well as an insight into some of the analysis processes these tools enable. Rather than just talking about these features, you'll see how they're actually deployed in an investigative context. **Daniel White:** *Security Engineer, Google*
2:15 – 3:00 pm	**SOC Building to Shine Guide** This talk will discuss key items around building a security operations center and maturing it. Initially working through points on the importance of process and procedures, how to document and options to store and actively use documentation. A key component to any SOC is the discussion of hiring, on-boarding and training analysts and monitoring technology. Experience with ArcSight means it will be the platform for screenshots, use case development and actionable content as well as data-feed onboarding. After implementing a SOC, it is important to start maturing the processes, incident response within the SOC and the interactions with internal and external organizations. Lastly, the conversation will cover incident response, daily reactions to users, decisions and breaches with an example of a response to a virus outbreak. Often nuisance issues are the hardest to gain internal visibility but the security teams must address and this will offer suggestions on how to handle things when other groups are not as invested in security remediation. Going from detection to impact, and a hack back response the SOC analysts used to shut it down. The outbreak example will use the SANS Incident Response Model to walk through decisions made and how the issue was handled. Additionally, items from the Target breach will be considered. **Brandie Anderson:** *Head of OpSec Research, HP Security Research*
3:00 – 3:30 pm	**Networking Break and Vendor Expo**
3:30 – 4:15 pm	**Back to the Future with Document Malware** Just like fashion, what is old is new again. There has been a resurgence of document based malware this year. Documents are commonly shared over email and make perfect weapons against unsuspecting victims of phishing attacks. The ability to analyze these malicious documents and make them spill all their dirty secrets will provide a huge leg up on your investigations. The most common document formats and the best tools and techniques to analyze them will be covered. We will also look at some recent widespread campaigns and walkthrough how to analyze them and bypass their defenses. **Tyler Halfpop:** *Threat Researcher, Fidelis Cybersecurity*

4:15 – 5:00 pm

DFIR SANS360

This session features an array of top Digital Forensics and Incident Response experts discussing the coolest forensic technique, plugin, tool, command line, or script they used in the last year. They'll talk about the approach that really changed the outcome of a case they were working on. If you have never been to a lightning talk, it is an eye-opening experience. Each speaker has 360 seconds (six minutes) to deliver his or her message. This format allows SANS to present 10-12 experts within one hour, instead of the standard one presenter per hour. The compressed format gives you a clear and condensed message eliminating the fluff. If the topic isn't engaging, a new topic is just six minutes away.

Baselining Memory for Anomaly Detection
Alissa Torres
Certified Instructor, SANS Institute

Threat Intelligence and Thinking About How to Think
Robert M. Lee
Co-Founder, Dragos Security

What to Expect When You're Expecting Anonymous
Cindy Murphy
MSc, Detective, Digital Forensics / Computer Crimes, Madison (WI) Police Department

Six Minutes in Mac Heaven
Sarah Edwards
Test Engineer, Parsons Corporation

Need for Speed: Malware Edition
Anuj Soni
Booz Allen Hamilton

Temet Nosce : Know Thy Endpoint, Through and Through
Thomas V. Fischer
Principal Threat Researcher, Digital Guardian

Additional talks to come

FOR 408

WINDOWS FORENSIC ANALYSIS

Instructor: Rob Lee
Six-Day Program: Mon 5th – Sat 10th October 9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required

Follow us on Twitter
@SANSEMEA
@sansforensics
#DFIRPrague

Master Windows Forensics
You can't protect what you don't know about.

Windows Forensic Analysis focuses on a comprehensive and deep analysis of the latest Microsoft Windows operating systems. In this intermediate course, you will learn directly how forensic analysts track the second-by-second trail left behind by evildoers used in successful criminal prosecution, incident response, media exploitation or civil litigation.

FOR408 is continually updated: This course utilizes a brand-new intellectual property theft and corporate espionage case that took over 6 months to create. You work in the real world and your training should include real practice data. Our development team used incidents from their own experiences and investigations and created an incredibly rich and detailed scenario designed to immerse students in a true investigation.

You will learn...

- to perform in-depth Windows forensic analysis
- how to determine files stolen during an IP theft how to track a user's every movement inside the Windows OS
- how to identify programs executed by the user
- to examine event logs, registry, jump lists, and more

Register now
www.sans.org/DFIRPrague

"This is by far the best training I have ever had. My forensic knowledge increased more in the last 5 days than in the last year."

Vito Rocco, UNLV

FOR 508

ADVANCED DIGITAL FORENSICS AND INCIDENT RESPONSE

Instructor: Jess Garcia
Six-Day Program: Mon 12th – Sat 17th October 9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required

Gather your incident response team It's time to go hunting

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, organized crime syndicates, and hactivism.

FOR508 trains digital forensic analysts and incident response teams to identify, contain, and remediate sophisticated threats using APT groups and financial crime syndicates. A hands-on lab – developed from a real-world targeted attack on an enterprise network leads you through the challenges and solutions.

Follow us on Twitter
@SANSEMEA
@sansforensics
#DFIRPrague

You will learn...

- how to track Advanced Persistent Threats in your enterprise Perform incident response on any remote enterprise system
- how to examine memory to discover active malware
- to perform timeline analysis to track the steps of an attacker on your systems
- how to discover unknown malware on any system
- how to perform deep dive analysis to discover data hidden by anti-forensics

Register now
www.sans.org/DFIRPrague

"The most in-depth, state-of-the-art IR course I can imagine. It's the first time I think defense can actually gain an advantage."

Kai Thomsen, AUDI AG

FOR 518

MAC FORENSIC ANALYSIS

Instructor: Sarah Edwards
Six-Day Program: Mon 5th – Sat 10th October 9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required

Follow us on Twitter
@SANSEMEA
@sansforensics
#DFIRPrague

Forensicate differently

FOR518: 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.

This course provides the tools and techniques necessary to take on any Mac case without hesitation. The intense hands-on forensic analysis skills taught enable Windows-based investigators to broaden their analysis capabilities and have the confidence and knowledge to comfortably analyse any Mac or iOS system.

You will learn...

- to analyze and parse the Hierarchical File System (HFS+) file system
- to recognize the specific domains of the logical file system and Mac-specific file types
- to understand and profile users through their data files and preference configurations
- to determine how a system has been used or compromised
- to analyze numerous Mac-specific technologies

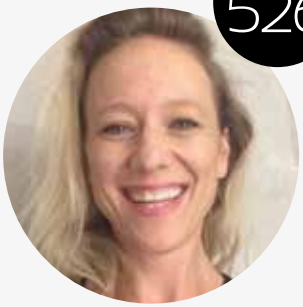
Register now
www.sans.org/DFIRPrague

"I have not encountered a Mac class this in-depth that covers the file structure so well."

Craig Goldsmith, OCSD

FOR 526

MEMORY FORENSICS IN-DEPTH



Instructor: Alissa Torres
Six-Day Program: Mon 12th – Sat 17th October, 9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required

Malware can hide, but it must run

Memory analysis is now a crucial skill for any incident responder who is analyzing intrusions. The malware paradox is key to understanding that while intruders are becoming more advanced with anti-forensic tactics and techniques, it is impossible to hide their footprints completely from a skilled incident responder performing memory analysis. professionals through acquisition, validation, and memory analysis with real-world and malware-laden memory images.

FOR526 draws on best practices and recommendations from experts in the field to guide DFIR professionals through acquisition, validation, and memory analysis with real-world and malware-laden memory images. It provides the critical skills necessary for digital forensics examiners and incident responders to successfully perform live system memory triage and analyse captured memory images. The course uses the most effective freeware and open-source tools in the industry today and provides an in-depth understanding of how these tools work.

Follow us on Twitter
@SANSEMEA
@sansforensics
#DFIRPrague

You will learn...

- to utilize stream-based data parsing tools to extract AES-encryption keys
- to capture, examine and analyze physical memory image and structures
- Windows, Mac, and Linux Memory Analysis Covered
- to conduct Live System Memory Analysis
- how to extract and analyze packed and non-packed PE binaries from memory
- to gain insight into the latest anti-memory analysis techniques and how to overcome them

Register now
www.sans.org/DFIRPrague

"Totally awesome, relevant and eye opening. I want to learn more every day."

Matthew Britton, Blue Cross Blue Shield of Louisiana

FOR 572

ADVANCED NETWORK FORENSICS AND ANALYSIS

Instructor: Philip Hagen
Six-Day Program: Mon 5th – Sat 10th October, 9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required

Follow us on Twitter
@SANSEMEA
@sansforensics
#DFIRPrague

Bad guys are talking– we'll teach you to listen

This course was built from the ground up to cover the most critical skills needed to mount efficient and effective incident response investigations. We focus on the knowledge necessary to expand the forensic mindset from residual data on the storage media from a system or device to the transient communications that occurred in the past or continue to occur.

FOR572 covers the tools, technology, and processes required to integrate network evidence sources into your investigations, with a focus on efficiency and effectiveness. It includes the full spectrum of network evidence, including high-level NetFlow analysis, low-level pcap exploration, ancillary network log examination, and more. Learn how to leverage existing infrastructure devices that may contain months or years of valuable evidence as well as how to place new collection platforms while an incident is already under way.

You will learn...

- to extract files from network packet captures and proxy cache files
- to use historical NetFlow data to identify relevant past network occurrences
- how to reverse engineer custom network protocols to decrypt captured SSL traffic to identify attackers actions
- how to incorporate log data into a comprehensive analytic process
- how attackers leverage man-in-the-middle tools how to analyze network protocols and wireless network traffic

Register now
www.sans.org/DFIRPrague

"I research ICS/SCADA environments. I think FOR572 presents a better approach at detecting malware then a more traditional approach does."

Niklas Vilhelm, Norwegian National Security Authority

FOR 578

CYBER THREAT INTELLIGENCE

Instructor: Robert M. Lee
Five-Day Program: Mon 12th – Fri 16th October, 9:00am - 5:00pm
30 CPE/CMU Credits
Laptop Required

There is no teacher but the enemy!

During a targeted attack, an organization needs the best incident response and hunting team in the field, poised to combat these threats and armed with intelligence about how they operate. FOR578: Cyber Threat Intelligence will train you and your team to respond, detect, scope, and stop intrusions and data breaches.

The collection, classification, and exploitation of knowledge about adversaries - collectively known as cyber threat intelligence - gives network defenders information superiority that can be used to reduce the adversary's likelihood of success with each subsequent intrusion attempt.

Follow us on Twitter
@SANSEMEA
@sansforensics
#DFIRPrague

You will learn...

- how to determine the role of cyber threat intelligence in their jobs
- how to know the analysis of an intrusion by a sophisticated actor is complete
- to identify, extract, prioritize, and leverage intelligence from advanced persistent threat (APT) intrusions
- how to expand upon existing intelligence to build profiles of adversary groups
- to leverage collected intelligence to improve success in defending against and responding to future intrusions
- how to manage, share, and receive intelligence on APT actors

Register now
www.sans.org/DFIRPrague

"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."

Robert M. Lee, FOR578 Course Author

FOR 585

ADVANCED SMARTPHONE FORENSICS

Instructor: Cindy Murphy
Six-Day Program: Mon 5th – Sat 10th October, 9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required

Follow us on Twitter
@SANSEMEA
@sansforensics
#DFIRPrague

Your texts and apps can and will be used against you

FOR585: Advanced Smartphone Forensics teaches real-life, hands-on skills that help digital forensic examiners, law enforcement officers, and information security professionals handle investigations involving even the most complex smartphones currently available.

This 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 analyze the results for use in digital investigations. The exercises in this class cover the best tools currently available to conduct smartphone and mobile device forensics, and provide detailed instructions on how to manually decode data tools sometimes overlook.

You will learn...

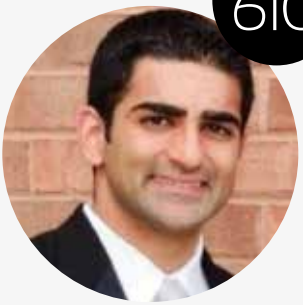
- to manually parse and decode data from smartphones and smartphone applications
- to detect hidden malware and spyware on smartphones
- how to interpret file systems on smartphones
- to recover artifacts and location-based and GPS information
- to perform advanced forensic examinations of data structures and data-carving
- how to reconstruct events surrounding a crime
- to decrypt locked backup files and bypass smartphone locks

Register now
www.sans.org/DFIRPrague

"The topics covered in the course can be considered advanced but are also very practical. Topics such as parsing and searching devices not supported by commercial tools and digging in hex for deleted artifacts are extremely important."
Matthew Edmondson

FOR 610

REVERSE-ENGINEERING MALWARE: MALWARE ANALYSIS TOOLS AND TECHNIQUES



Instructor: Anuj Soni
Six-Day Program: Mon 12th – Sat 17th October, 9:00am - 5:00pm
36 CPE/CMU Credits
Laptop Required

Turn malware inside-out

This popular malware analysis course has helped forensic investigators, incident responders acquire practical skills for examining malicious programs that target Microsoft Windows. This training also teaches how to reverse-engineer web browser malware implemented in JavaScript and Flash, as well as malicious documents, such as PDF and Microsoft Office files.

FOR610 explores malware analysis tools and techniques in depth. Acquire the practical skills to examine malicious programs that target and infect Windows systems. This course builds a strong foundation for reverse-engineering malicious software using a variety of system and network monitoring utilities, a disassembler, a debugger, and other tools useful for turning malware inside out.

Follow us on Twitter
@SANSEMEA
@sansforensics
#DFIRPrague

You will learn...

- to build an isolated lab for analyzing malicious code
- how to employ network and system-monitoring tools for malware analysis
- how to examine malicious JavaScript, VB Script and ActionScript
- to use a disassembler and debugger to analyze malicious Windows executables
- how to bypass a variety of defensive mechanisms designed by malware authors
- how to derive Indicators of Compromise (IOCs) from malicious executables Utilize practical memory forensics techniques to understand malware capabilities

Register now
www.sans.org/DFIRPrague

"FOR610 should be required training for all forensic investigators. It is necessary for awareness, analysis, and reporting of threats."

Paul Gunnerson, U.S. Army

SANS instructors are considered the best in the world. Not only do they meet SANS' stringent requirements for excellence, they are also all real-world practitioners. The instructors ensure that what you learn in class will be up to date and relevant to your job.

We have an outstanding line up of European and US-based instructors at SANS DFIR Prague 2015. Read on for profiles of this elite group.

SARAH EDWARDS

Certified Instructor

Sarah is a senior digital forensic analyst who has worked with various federal law enforcement agencies. She has performed a variety of investigations including computer intrusions, criminal, counter-intelligence, counter-narcotic, and counter-terrorism.

Sarah's research and analytical interests include Mac forensics, mobile device forensics, digital profiling, and malware reverse engineering. Sarah has presented at the following industry conferences; Shmoocon, CEIC, BsidesNOLA, TechnoSecurity, HTCIA, and the SANS DFIR Summit.

She has a Bachelor of Science in Information Technology from Rochester Institute of Technology and a Master's in Information Assurance from Capitol College.

JESS GARCIA

Principle Instructor

Jess Garcia is founder and technical lead of One eSecurity, a global Information Security company specialised in Incident Response and Digital Forensics.

With near 20 years in the field, and an active researcher in the area of innovation for Digital Forensics, Incident Response and Malware Analysis, Jess is today an internationally recognised Digital Forensics and Cybersecurity expert, having led the response and forensic investigation of some of the the world's biggest incidents in recent times.

A Principal SANS instructor, with almost 15 years of teaching experience, Jess is also a regular invited speaker at security conferences worldwide.

Previously, Jess worked for 10 years in the Spanish Space Agency, where he collaborated as a security advisor with the European Space Agency, NASA, and other international organisations. Jess holds a Masters of Science in Telecommunications Engineering + Computer Science from the Univ. Politecnica de Madrid.

PHILIP HAGEN

Certified Instructor

Philip Hagen has been working in the information security field since 1998, running the full spectrum including deep technical tasks, management of an entire computer forensic services portfolio, and executive responsibilities.

Currently, Phil is an Evangelist at Red Canary, where engages with current and future customers of Red Canary's managed threat detection service to ensure their use of the service is best aligned for success in the face of existing and future threats.

Phil started his security career while attending the US Air Force Academy, with research covering both the academic and practical sides of security. He served in the Air Force as a communications officer at Beale AFB and the Pentagon. In 2003, Phil shifted to a government contractor, providing technical services for various IT and information security projects. These included systems that demanded 24x7x365 functionality. He later managed a team of 85 computer forensic professionals in the national security sector. He has provided forensic consulting services for law enforcement, government, and commercial clients prior to joining the Red Canary team. Phil is also a certified instructor for the SANS Institute, and is the course lead and co-author of FOR572, Advanced Network Forensics and Analysis.

ROB LEE

Fellow

Rob Lee is an entrepreneur and consultant in the Washington, DC area, specializing in information security, incident response, and digital forensics. Rob is currently the curriculum lead and author for digital forensic and incident response training at the SANS Institute in addition to owning his own firm. Rob has more than 15 years of experience in computer forensics, vulnerability and exploit discovery, intrusion detection/prevention, and incident response.

Rob graduated from the U.S. Air Force Academy and served in the U.S. Air Force as a founding member of the 609th Information Warfare Squadron, the first U.S. military operational unit focused on information warfare. Rob co-authored the book Know Your Enemy, 2nd Edition. Rob earned his MBA from Georgetown University in Washington DC. He was awarded the Digital Forensic Examiner of the Year from the Forensic 4Cast Awards. Rob is an ardent blogger about computer forensics and incident response topics at the SANS Computer Forensic Blog. Rob is also a co-author of the MANDIANT threat intelligence report M-Trends: The Advanced Persistent Threat.

ROBERT M. LEE

Certified Instructor

Robert M. Lee is a co-founder at the critical infrastructure cyber security company Dragos Security LLC where he has a passion for control system packet analysis, digital forensics, and threat intelligence research. He is the course author of SANS ICS515 - "Active Defence and Incident Response" and the co-author of SANS FOR578 - "Cyber Threat Intelligence." He is a passionate educator although he should not be confused with the other Rob Lee at SANS - that Rob Lee is cooler but has less hair.

Robert obtained his start in cyber security in the U.S. Air Force where he currently serves as a Cyber Warfare Operations Officer. He has performed defence, intelligence, and attack missions in various government organisations including the establishment of a first-of-its-kind ICS/SCADA cyber threat intelligence and intrusion analysis mission. Robert routinely writes articles and journals in publications such as Control Engineering, Air and Space Power Journal, Wired, and Passcode. He is also a frequent speaker at conferences and is currently pursuing his PhD at Kings College London with research into the cyber security of control systems. Robert is also the author of the book "SCADA and Me" and the web-comic www.LittleBobbyComic.com

CINDY MURPHY

Certified Instructor

Cindy Murphy is a Detective with the City of Madison, WI Police Department and has been a Law Enforcement Officer since 1985. She is a certified forensic examiner and has been involved in computer forensics since 1999. Det.

Murphy has directly participated in the examination of many hundreds of hard drives, cell phones, and other items of digital evidence pursuant to criminal investigations including financial crimes, homicides, missing persons, computer intrusions, sexual assaults, child pornography, and various other crimes. She has testified as a computer forensics expert in state and federal court on numerous occasions, using her knowledge and skills to assist in the successful investigation and prosecution of criminal cases involving digital evidence. She also helped to develop the digital forensics certificate program at Madison Area Technical College.

She is a certified SANS instructor and co-authored and teaches the Advanced Mobile Device Forensics (FOR585) course for the SANS Institute. She has presented internationally on various digital forensics topics and frequently writes articles and whitepapers for the community on various forensics-related topics.

ANUJ SONI

Certified Instructor

Anuj Soni is a Senior Incident Responder at Booz Allen Hamilton, where he leads forensic, malware, and network analysis efforts to investigate security incidents. Since entering the information security field in 2005, Anuj has performed numerous intrusion investigations to help government and commercial clients mitigate attacks against the enterprise. His malware hunt skills and technical analysis abilities have resulted in the successful identification, containment, and remediation of multiple threat actor groups. Anuj has analysed over 400 malware samples to assess function, purpose, and impact, and his recommendations have improved the security posture of the organisations he supports.

Sought after as a technical thought leader and adviser, Anuj excels not only in delivering rigorous forensic analysis, but also in process development, knowledge management, and team leadership to accelerate incident response efforts. Anuj shares his knowledge and experience often by teaching for SANS and presenting at events including the U.S. Cyber Crime Conference, SANS DFIR Summit, and the Computer and Enterprise Investigations Conference (CEIC).

ALISSA TORRES

Certified Instructor

Alissa Torres is a certified SANS instructor, specialising in advanced computer forensics and incident response. Her industry experience includes serving in the trenches as part of the Mandiant Computer Incident Response Team (MCIRT) as an incident handler and working on an internal security team as a digital forensic investigator.

She has extensive experience in information security, spanning government, academic, and corporate environments and holds a Bachelors degree from University of Virginia and a Masters from University of Maryland in Information Technology. Alissa has taught as an instructor at the Defense Cyber Investigations Training Academy (DCITA), delivering incident response and network basics to security professionals entering the forensics community.

She has presented at various industry conferences and numerous B-Sides events. In addition to being a GIAC Certified Forensic Analyst (GCFA), she holds the GCFE, GPEN, CISSP, EnCE, CFCE, MCT and CTT+.

EVENT LOCATION & TRAVEL INFORMATION SANS DFIR PRAGUE 2015

Event Location: Angelo Hotel Prague Radlická 3216/1G, 150 00 Praha, Czech Republic
Telephone: +420 234 801 111 **E-mail:** info@angelohotel.com **Website:** www.vi-hotels.com/en/angelo-prague

Arriving by public transport

The easiest way to get to the Angelo Hotel from the main train station is by tram. The tram stop is located directly in front of the station. Take tram no.9 in the direction of "Sídliště Řepy" and get off at the "Anděl" tram stop.
From Holešovice train station: From Holešovice station, take metro line C to "Florenc" station. Change to yellow line B towards "Zličín" and go five stops to "Anděl".

Arriving by air:

From Václav Havel Airport Prague: Take bus No. 191 (a stop is located directly in front of Terminal 1 and Terminal 2) from the airport to the "Anděl" stop.

Arriving by car

From Václav Havel Airport Prague:
From the airport, follow the signs to Pilsen / R1 and take exit 26 for "Pražský okruh". Continue on through Karlovarská, Bělohorská and Patočkova streets. Merge onto Pražský okruh (slight left) and continue directly onto Strahov Tunnel. Exit onto Plzeňská and after approx. 400 m turn right onto Radlická. The hotel will be on the left.

From Nuremberg / Pilsen:
Take highway D5 and exit after km 151. Turn left onto Bucharova and continue for 1,3 km onto Radlická. Turn left after 4,4 km to stay on Radlická. The hotel will be on the right.

From Vienna / Brno:
Follow Highway D1 to Prag and exit onto 5. května. Merge onto jižní spojka and follow this highway for 5,7 km to Barrandov Bridge. After another 3,9 km, take the exit toward Smíchov / Radlice and continue onto Radlická. The hotel will be on the right.

For your convenience, please use the following GPS coordinates: N50°4'13.746" E14°24'5.753" or our address: Radlická 1g, 150 00 Prague 5

Hotel

The stylish Angelo Hotel is located 100 metres from the Andel metro stop and a 5-minute journey from Prague's historical centre. It features air-conditioned rooms with tea/coffee makers and satellite TV.

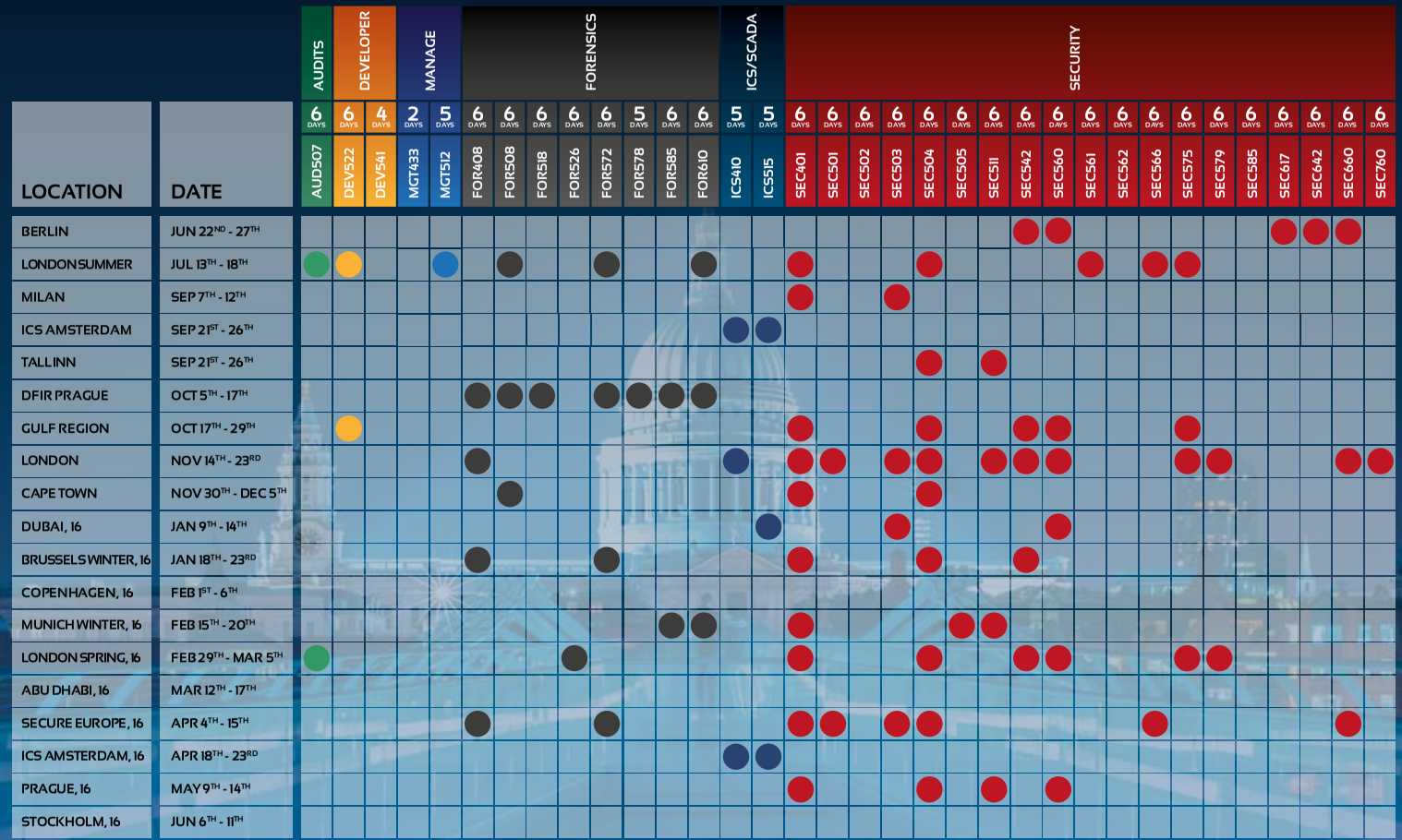
Located just a 3-minute walk from the green Mrazovka Hill and close to the Anděl City and Nový Smíchov Shopping Centre, all rooms at Hotel Angelo Prague are equipped with the latest technology like DVD players, internet access and plasma TVs.

There are several bus and tram stops in the immediate vicinity, and guests can easily visit the busy Wenceslas Square and the popular Mala Strana quarter, with its cafes and Baroque monuments. Both sites are located just 4.5 km away from the hotel. Attendees of SANS DFIR Prague will receive a special room rate of €110 per night for a single room or €120 per night for a double room, including VAT and breakfast. This special rate can only be guaranteed for reservations made before September 4th.

For a reservation form please contact emea_events@sans.org

FUTURE SANS EMEA TRAINING EVENTS 2015/16

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



V10- A5

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

Dates, Locations and Courses offered subject to change