FOR509: Enterprise Cloud Forensics and Incident Response

Course Topics
• Cloud Infrastructure and IR data sources
• Microsoft 365 and Graph API Investigations
• Azure Incident Response
• AWS Incident Response
• Google Workspace Investigations
• GCP Incident Response

You Will Be Able To
• Learn and master the tools, techniques, and procedures necessary to effectively locate, identify, and collect data no matter where it is located
• Identify and utilize new data only available from cloud environments
• Utilize cloud-native tools to capture and extract traditional host evidence
• Quickly parse and filter large data sets using scalable technologies such as the Elastic Stack
• Understand what data is available in various cloud environments

Find the Storm in the Cloud

FOR509: Enterprise Cloud Forensics and Incident Response will help you:
• Understand forensic data only available in the cloud
• Implement best practices in cloud logging for DFIR
• Learn how to leverage Microsoft Azure, AWS and Google Cloud Platform resources to gather evidence
• Understand what logs Microsoft 365 and Google Workspace have available for analysts to review
• Learn how to move your forensic processes to the cloud for faster data processing

With FOR509: Enterprise Cloud Forensics and Incident Response, examiners will learn how each of the major cloud service providers (Microsoft Azure, Amazon AWS and Google Cloud Platform) are extending analysts’ capabilities with new evidence sources not available in traditional on-premise investigations. From cloud equivalents of network traffic monitoring to direct hypervisor interaction for evidence preservation, forensics is not dead. It is reborn with new technologies and capabilities.

Incident response and forensics are primarily about following breadcrumbs left behind by attackers. These breadcrumbs are primarily found in logs. Your knowledge of the investigation process is far more important than the mechanics of acquiring the logs.

This class is primarily a log analysis class to help examiners come up to speed quickly with cloud based investigation techniques. It’s critical to know which logs are available in the cloud, whether they are turned on by default, and how to interpret the meaning of the events they contain.

Numerous hands-on labs throughout the course will allow examiners to access evidence generated based on the most common incidents and investigations. Examiners will learn where to pull data from and how to analyze it to find evil. The data will be available in your VM rather than accessed directly via the cloud to ensure a consistent lab experience.

Business Takeaways
• Understand digital forensics and incident response as it applies to the cloud
• Identify malicious activities within the cloud
• Cost-effectively use cloud-native tools and services for DFIR
• Ensure the business is adequately prepared to respond to cloud incidents
• Decrease adversary dwell time in compromised cloud deployments

Business Takeaways

“FORS09 was absolutely awesome! The depth of knowledge is unparalleled. I see this becoming a very popular class in the future.”
—Terrie Myerchin, AT&T

“Thanks a lot for FOR509 course. I believe this course provides a great way to get a really compressed introduction into the different cloud service providers and what is forensically possible there.”
—Marc Stroebel, HvS-Consulting AG

sans.org/for509
• Watch a preview of this course
• Discover how to take this course: Online, In-Person
FOR509 is very much needed in the industry as there is very little training out there for Cloud DFIR. So the fact that this course exists and is huge.”

—Chester Le Bron Jr, Northwestern Mutual