
FAST
FOUNDATIONAL ANALYST SECURITY TRAINING
TM
Capgemini
Foundational Analyst Security Training
© Capgemini 2019. All rights reserved | 1

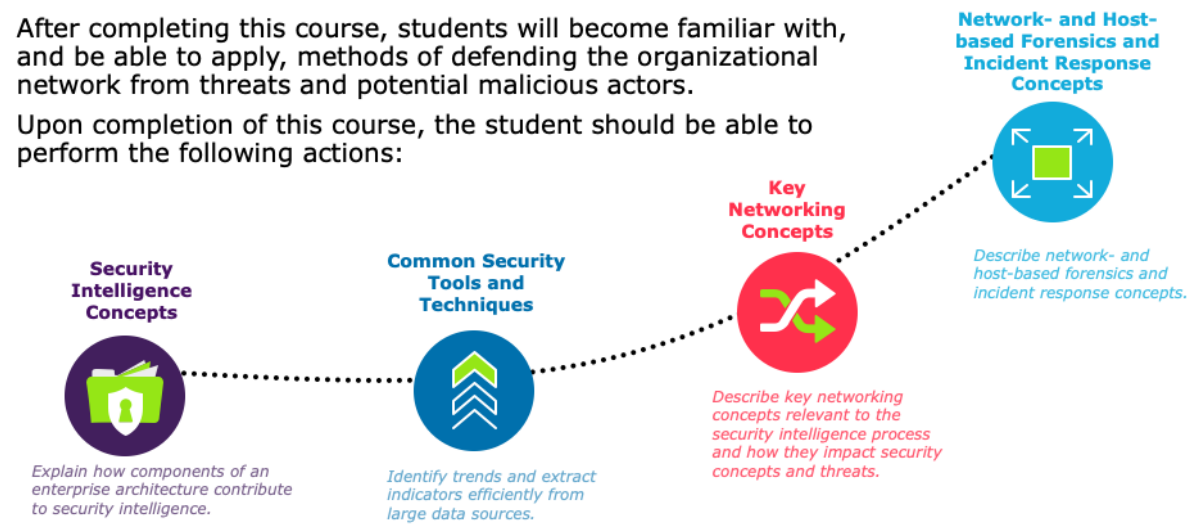
Welcome to the SOC Analyst Level 1 training course. During this course, you will learn many concepts that will be essential to your job as a SOC Analyst; likewise, this course provides extensive hands-on learning exercises to reinforce those skills.

You will become familiar with the Unified Enterprise Defense framework to remain ahead of security threats facing your organization.

Course Learning Objectives

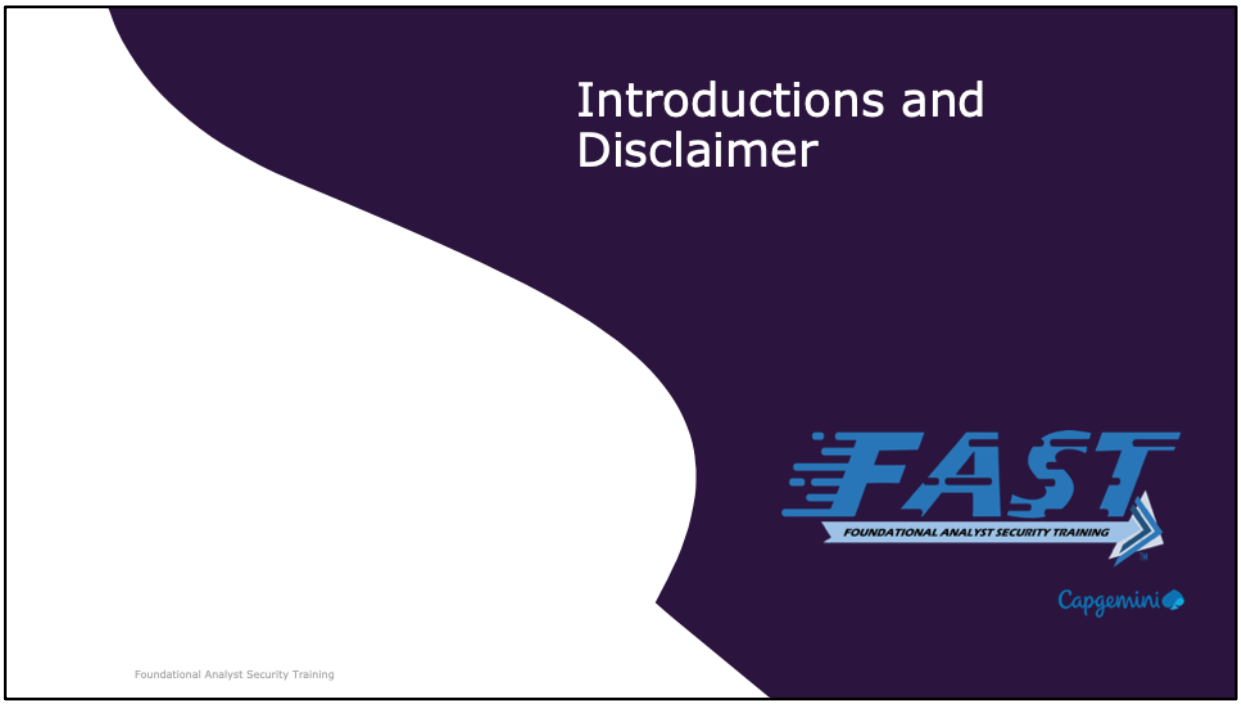
After completing this course, students will become familiar with, and be able to apply, methods of defending the organizational network from threats and potential malicious actors.

Upon completion of this course, the student should be able to perform the following actions:



FAST Foundational Analyst Security Training

 3



During this first section, we will cover a course introduction and a disclaimer about the course itself.

During this first, short module, we will cover some of the basic course expectations, including student and instructor introductions, course expectations of what the course offers and what it does not cover, and the layout of the course.

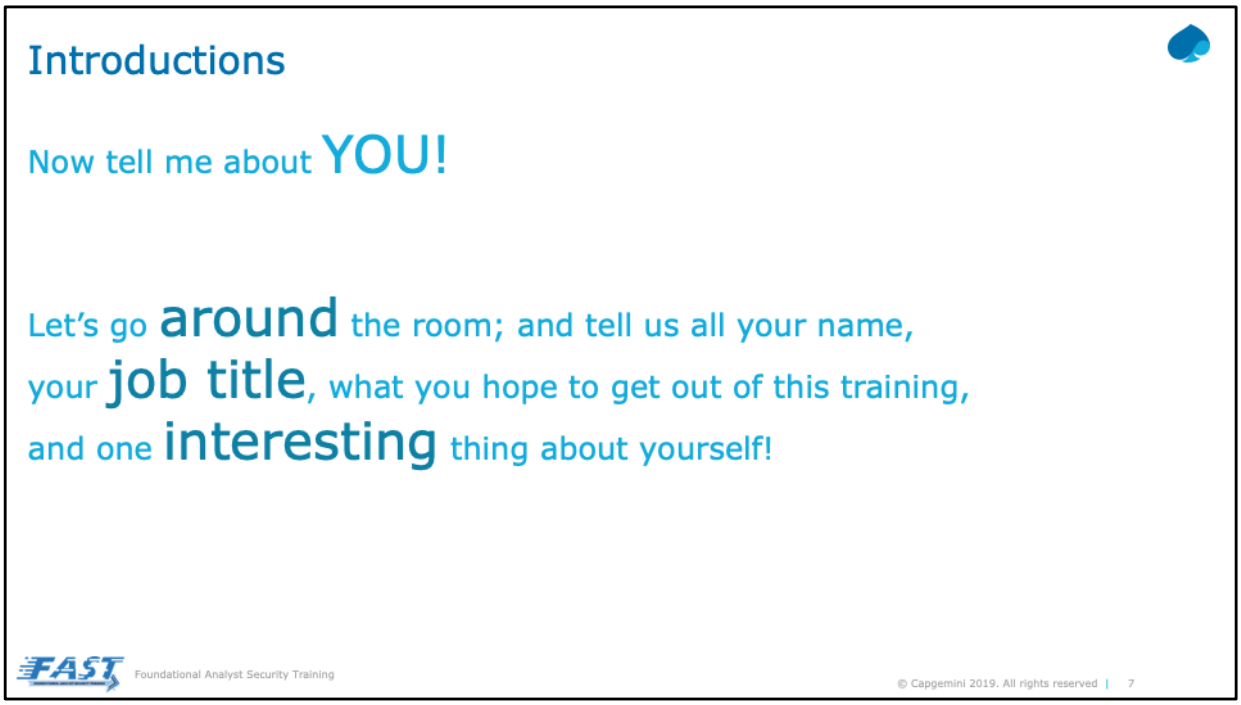
Christopher Morgan, GICSP

- SANS Global Industrial Cyber Security Professional
- Bachelor of Science in Cyber Security Management and Policy
  - Minor in Terrorism in Critical Infrastructure, from the University of Maryland University College

- Father
- Amateur sci-fi make-up artist
- Used to work offshore in oil and gas
- Served on nuclear submarines (Fast Attack)
- Began working for what is now Capgemini in 2016
  - Worked in Cyber Security for 9 years
  - Technical trainer for 13 years
  - Technology and maintenance for 24 years

FAST Foundational Analyst Security Training

 6



Instructor will provide an introduction.

Students will be asked to introduce themselves, including:

- Name
- Job title and function
- What they expect to get out of the course
- And anything else requested by the instructor(s)

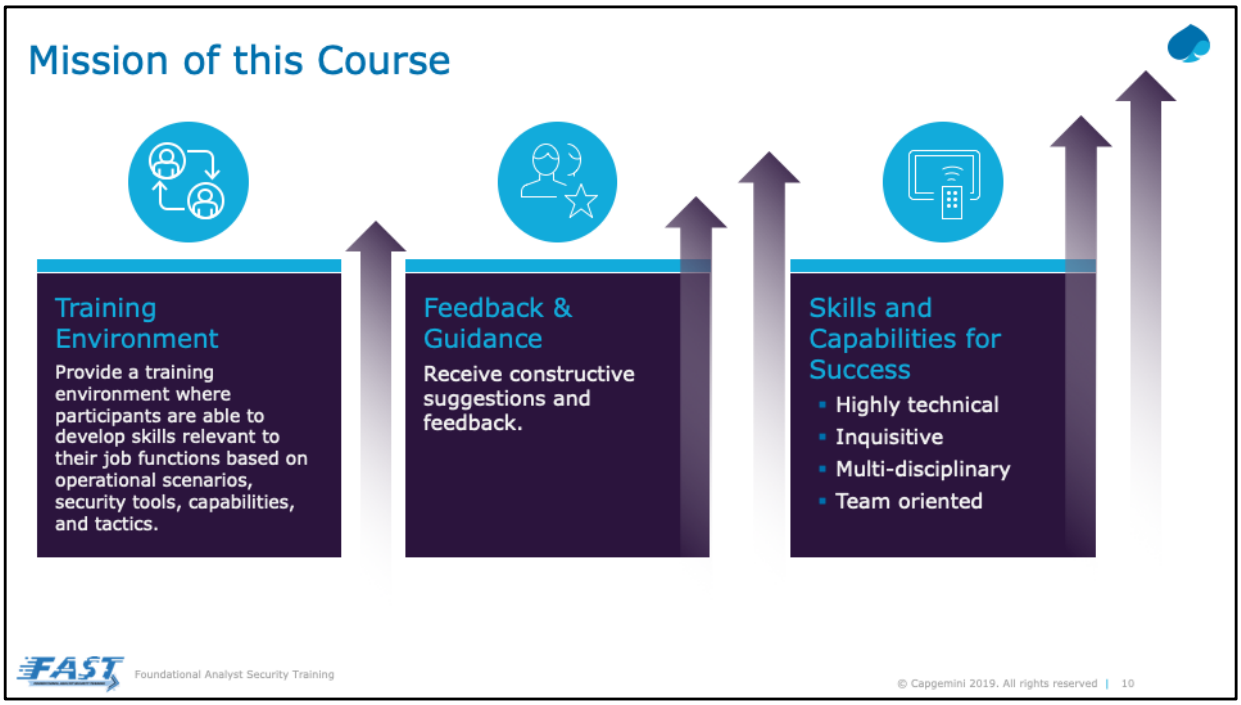
Course Introductions

FAST Foundational Analyst Security Training

During this course, you will have an opportunity to conduct a traffic and log file analysis on files. While these files are safe in a learning environment, you should always practice safe handling procedures in all SOC Analyst activities, including but not limited to:

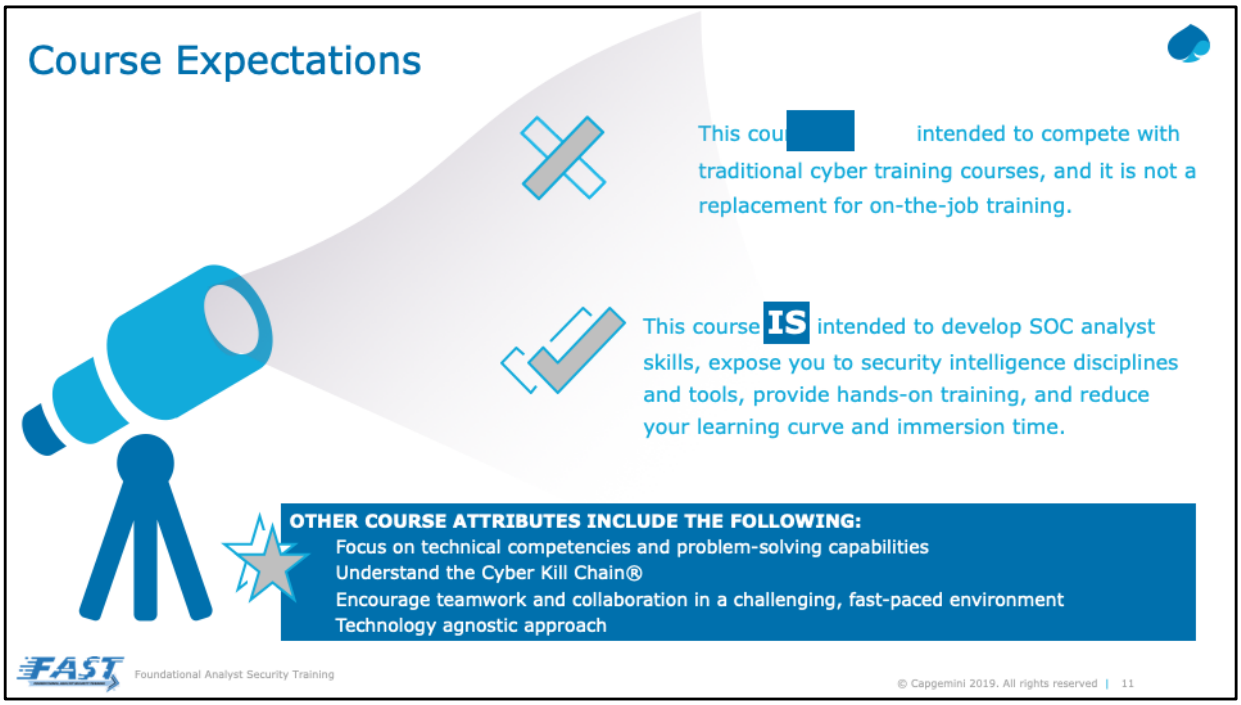
- Having a procedure - think through what you are going to do. Things will often change and you need to be adaptive, but you should always have a plan or a procedure that you are going to follow upfront.
- Quarantine - do not handle malware outside of a sandbox.
- Never “touch” the adversary infrastructure without fully considering the ramifications. Your actions could be intelligence to the adversary; thus, you need to carefully consider your actions and what intelligence that could provide the adversary.
- Keep your indicators private! Again, consider what intelligence that could provide the adversary, if they know your indicators.
- Get a second opinion before taking an action, especially if you are unsure of the right course of action.
- Know your classification guide and how that fits into your established procedures and plan of attack.

During this next section, we will cover a course mission and course expectations.



The overall mission of this course is to:

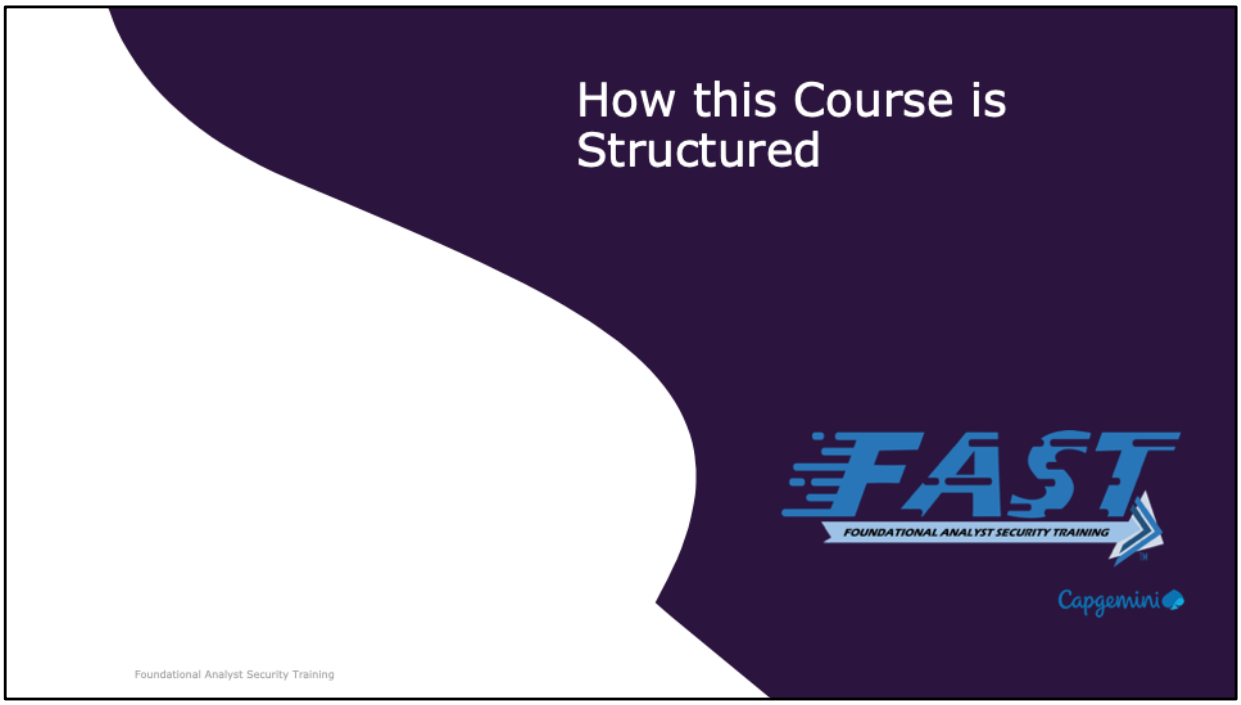
- Provide a training environment where participants are able to develop skills relevant to their job functions based on operational scenarios, security tools, capabilities, and tactics.
- Work in a team environment and build on each other's skills and capabilities. We want and expect you to work with the members of your team to learn from each other and to successfully complete the course exercises.
- Receive constructive suggestions and feedback. You will receive constructive suggestions and feedback throughout the course; thus, do not be offended by such feedback or suggestions – learn from them.
- The Skills and Capabilities Needed for Success include being highly technical, inquisitive, multi-disciplinary, and team oriented. This skills and capabilities are both needed for the course, and the course with improve each of these skills and capabilities as well.



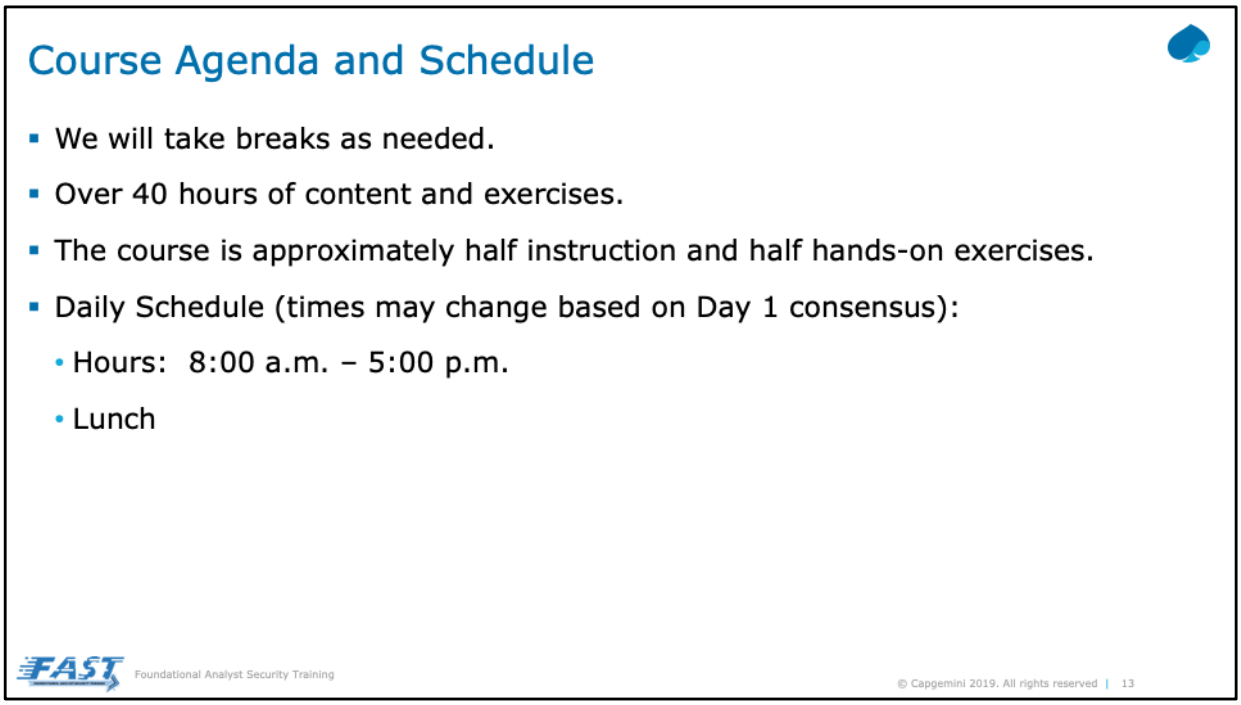
This course is NOT intended to compete with traditional cyber training courses, and it is not a replacement for on-the-job training. This course provides a broad overview of many SOC Analyst skills and capabilities. Each area covered in this course could be expanded into a full training course by itself. Likewise, after such training, you will continue to refine your skills and capabilities though on-the-job training.

This course IS intended to develop SOC Analyst skills, expose you to Security Intelligence disciplines and tools, provide hands-on training, and reduce your learning curve and immersion time. Other course attributes include:

- Focus on technical competencies and problem solving capabilities.
- Understand the Cyber Kill Chain®.
- Encourage teamwork and collaboration in a challenging, fast-paced environment.
- Technology agnostic approach.



During this next section, we will discuss the basic layout of the course.



During this course, we will take breaks as needed, typically a break every hour to hour and a half.

This course consists of 40+ hours of content and exercises over the next five days.

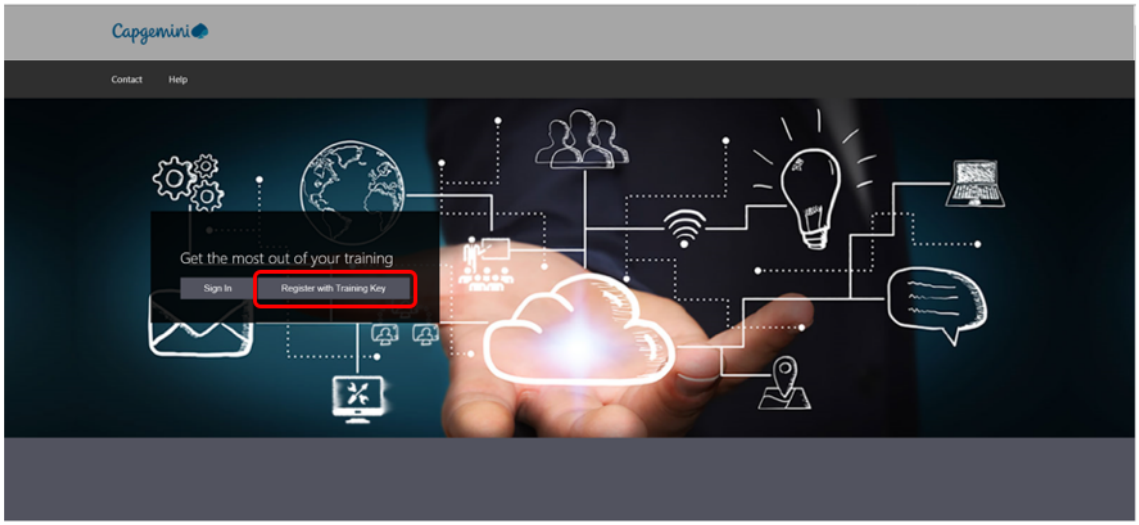
The course is about half instruction and half hands-on exercises, thus you will get plenty of hands-on training opportunities.

Each day we will begin at 8:00 AM and end at or about 5:00 PM (times may change based on day 1 consensus). We will take a break for lunch (at the time agreed upon during our day 1 discussion).

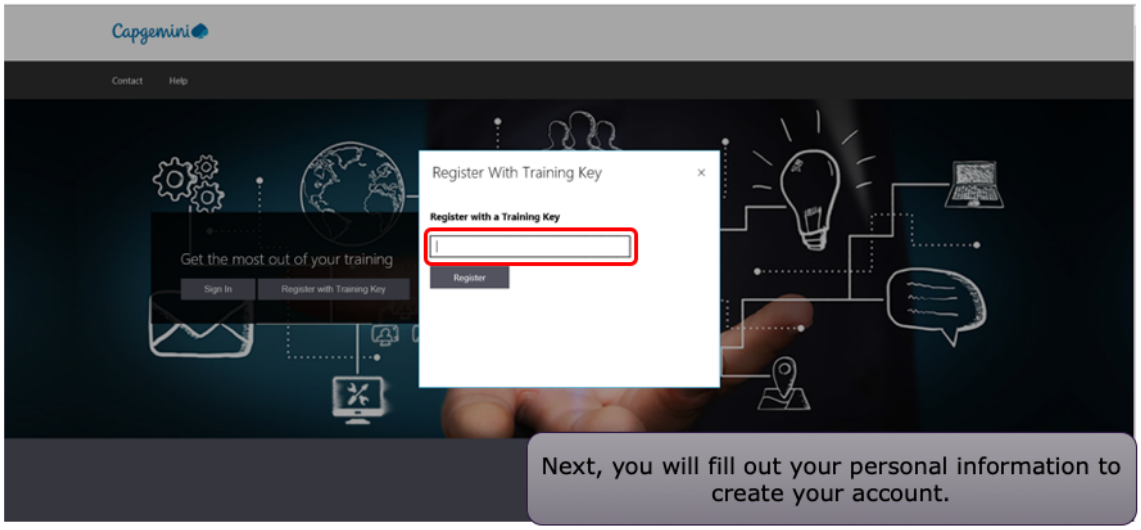
Laboratory Introduction

Capgemini

Each of you will be given a key.

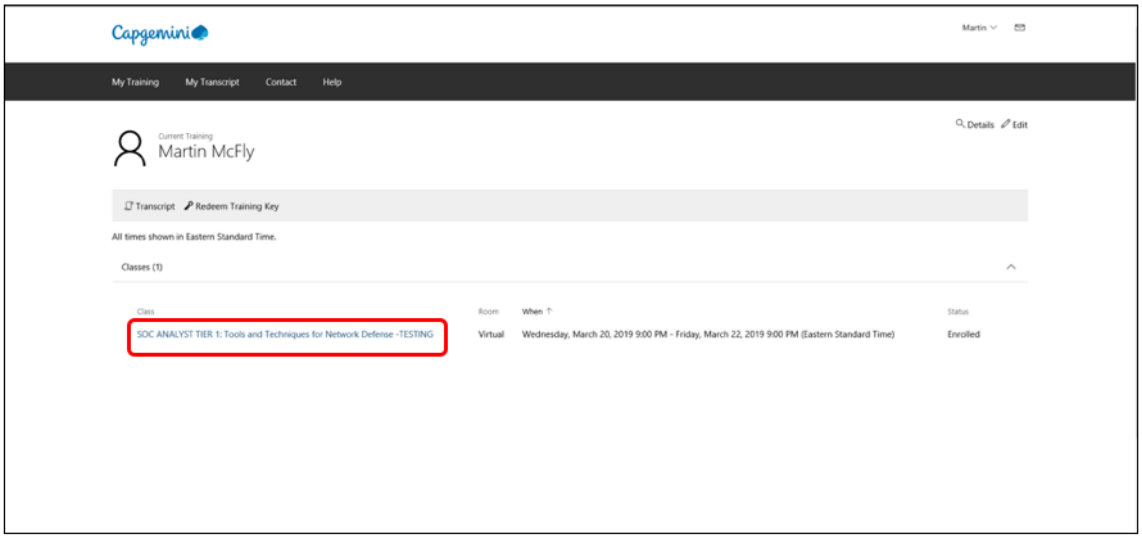


Use your key at https://capgeminicyber.learnondemand.net.

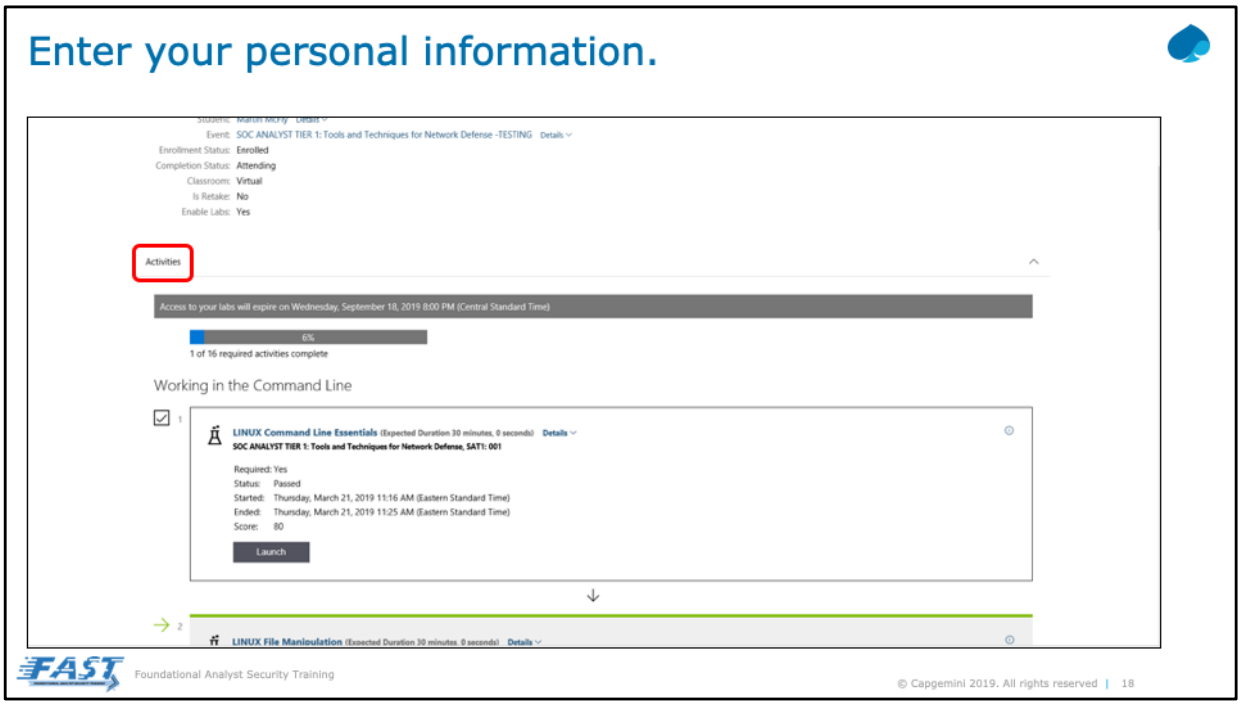


Next, you will fill out your personal information to create your account.

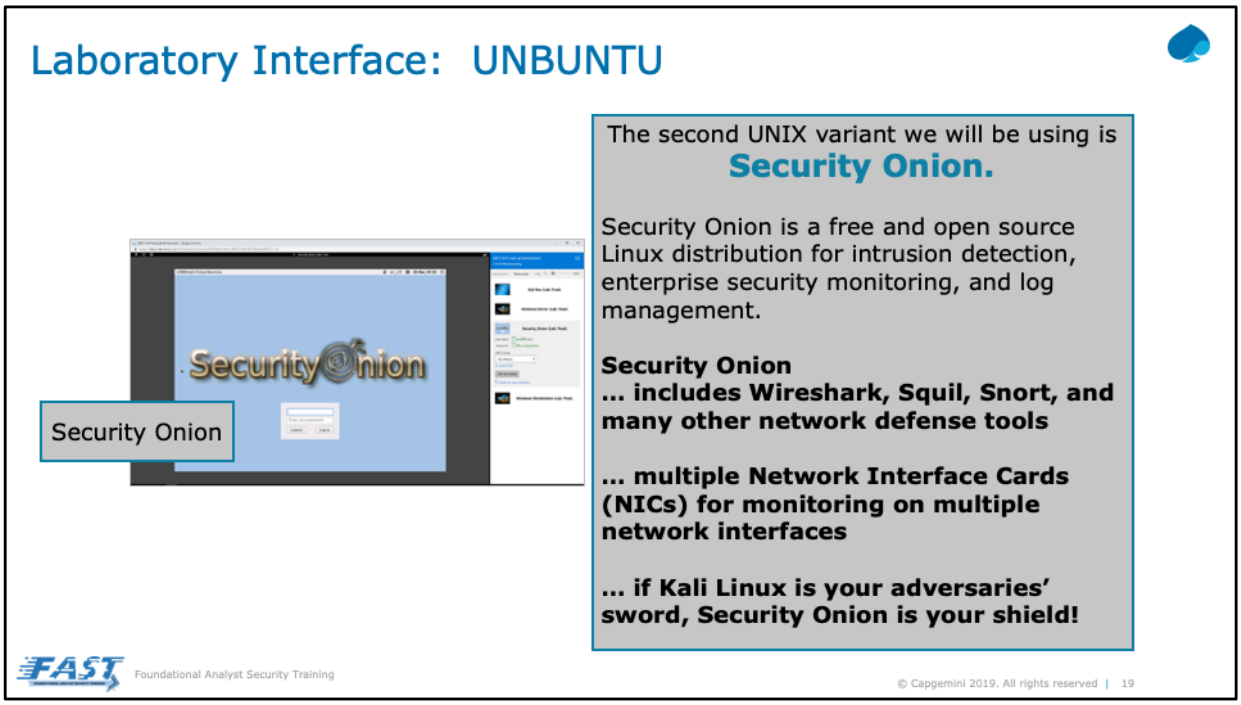
You will select SOC ANALYST TIER 1.



As previously mentioned, this course consists of about 50% hands-on exercises. For the hands-on exercises, you will connect to an online lab environment and the lab account information will be provided to each student accordingly.



As previously mentioned, this course consists of about 50% hands-on exercises. For the hands-on exercises, you will connect to an online lab environment and the lab account information will be provided to each student accordingly.



Security Onion

Security Onion is a free and open source Linux distribution for intrusion detection, enterprise security monitoring, and log management. It includes Elasticsearch, Logstash, Kibana, Snort, Suricata, Bro, Wazuh, Sguil, Squert, CyberChef, NetworkMiner, and many other security tools. The easy-to-use Setup wizard allows you to build an army of distributed sensors for your enterprise in minutes!

For more information about Security Onion not contained in this Documentation, please see our community site at https://securityonion.net.

Security Onion Solutions, LLC

Doug Burks started Security Onion as a free and open source project in 2008 and then founded Security Onion Solutions, LLC in 2014.

Security Onion Solutions, LLC is the only official provider of training, professional services, and hardware appliances for Security Onion.

For more information about these products and services, please see our corporate site at https://securityonionsolutions.com.

Documentation

Formats

This documentation is published online at https://securityonion.net/docs. If you are

viewing an offline version of this documentation but have Internet access, you might want to switch to the online version at https://securityonion.net/docs to see the latest version.
This documentation is also available in PDF format:
https://readthedocs.org/projects/securityonion/downloads/pdf/latest/

Authors

Security Onion Solutions is the primary author and maintainer of this documentation. Some content has been contributed by members of our community. Thanks to all the folks who have contributed to this documentation over the years!

Contributing

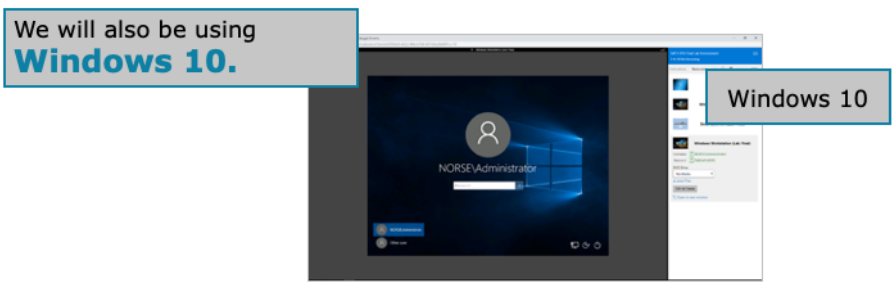
We welcome your contributions to our documentation! We will review any suggestions and apply them if appropriate.
If you are accessing the online version of the documentation and notice that a particular page has incorrect information, you can submit corrections by clicking the Edit on GitHub button in the upper right corner of each page.
To submit a new page, you can submit a pull request (PR) to the following repo:
https://github.com/Security-Onion-Solutions/securityonion-docs

Naming Convention

Our goal is to allow you to easily guess and type the URL of the documentation you want to go to.
For example, if you want to read more about Suricata, you can type the following into your browser:
https://securityonion.net/docs/suricata
To achieve this goal, new documentation pages should use the following naming convention:
all lowercase
.rst file extension
ideally, the name of the page should be one simple word (for example: suricata.rst)
try to avoid symbols such as hyphens and underscores
if symbols are required, hyphens are preferred to underscores

Next Previous

Laboratory Interface: Windows Machines



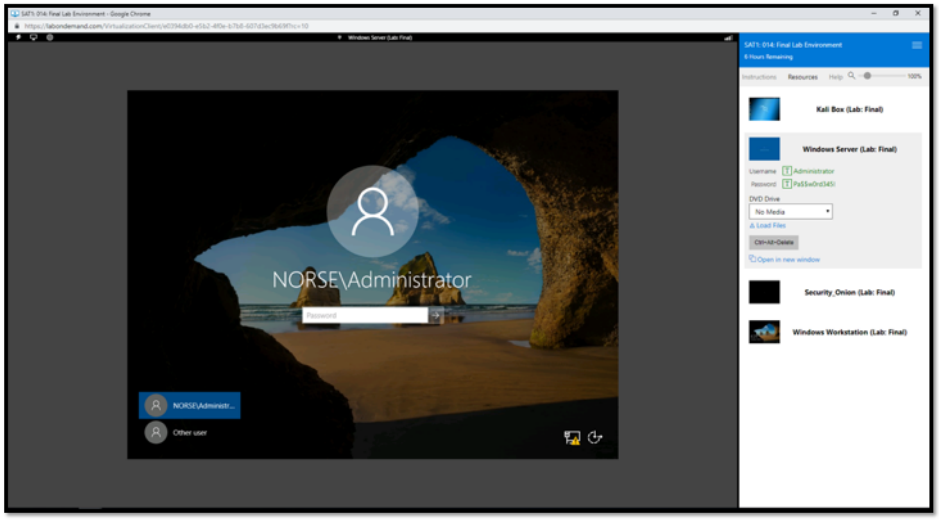
We will also be using two Windows 10 machines for investigations and tracking. Both of these machines are on the network together, and you will have access to the domain servers if you need them

Laboratory Interface

LABORATORY FEATURES:

Operating Systems:	Ubuntu, Windows 10	RAM: Hard Disk:	~10GB ~25-80GB
Internet Access:	Yes*		
Installed Software:	Varies by laboratory and machine, but all typical software types are included.		

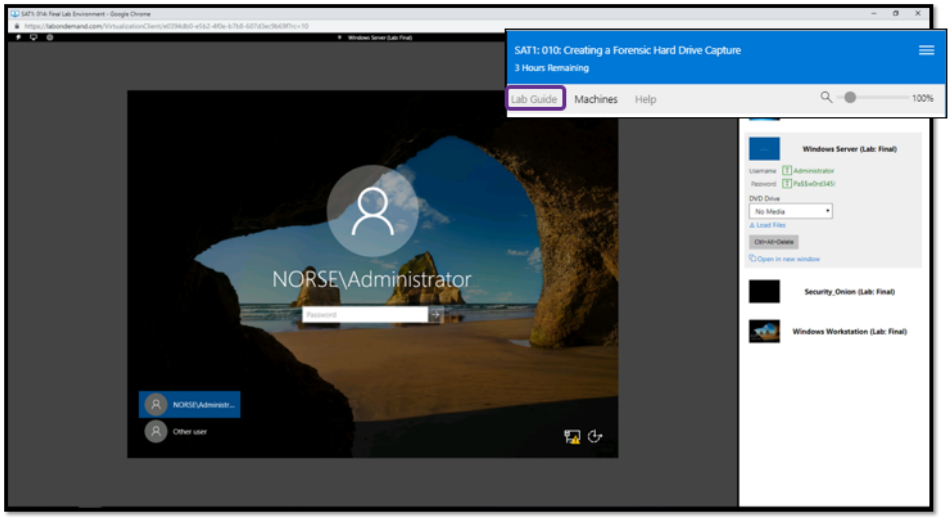
Laboratory Interface (cont.)



In this screenshot, you see a sample lab showing a portion of the **instructions** for the lab and the title of the lab module as well as the amount of time remaining, at the top of the Lab Console. Adjacent to the Instructions tab in the Lab Console are two additional tabs; **Resources** and **Help**.

Instructions: All instructions written in idl-md will be rendered in the Instructions tab.

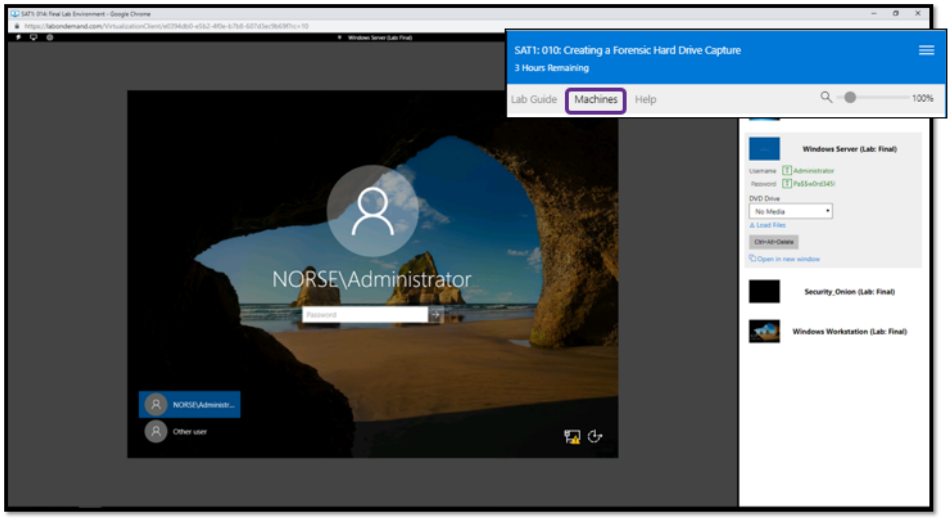
Laboratory Interface (cont.)



In this screenshot, you see a sample lab showing a portion of the **instructions** for the lab and the title of the lab module as well as the amount of time remaining, at the top of the Lab Console. Adjacent to the Instructions tab in the Lab Console are two additional tabs; **Resources** and **Help**.

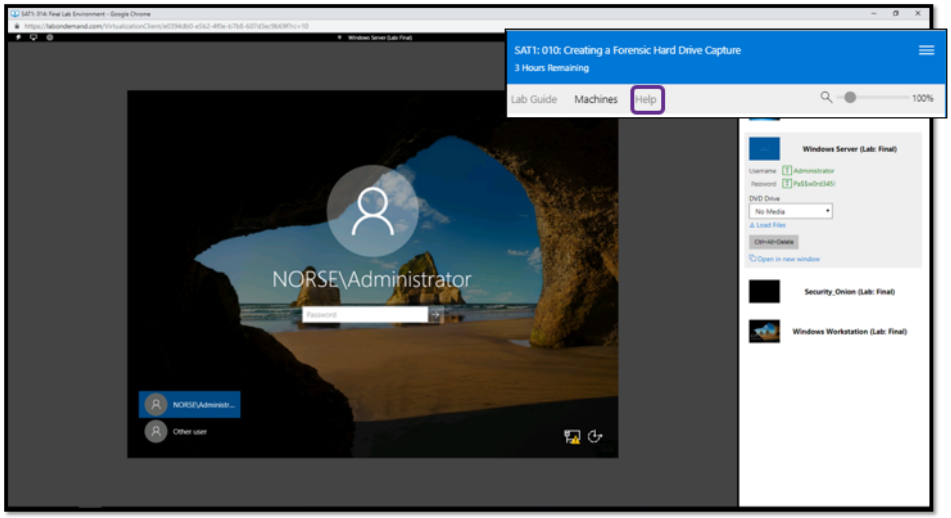
Instructions: All instructions written in idl-md will be rendered in the Instructions tab.

Laboratory Interface (cont.)



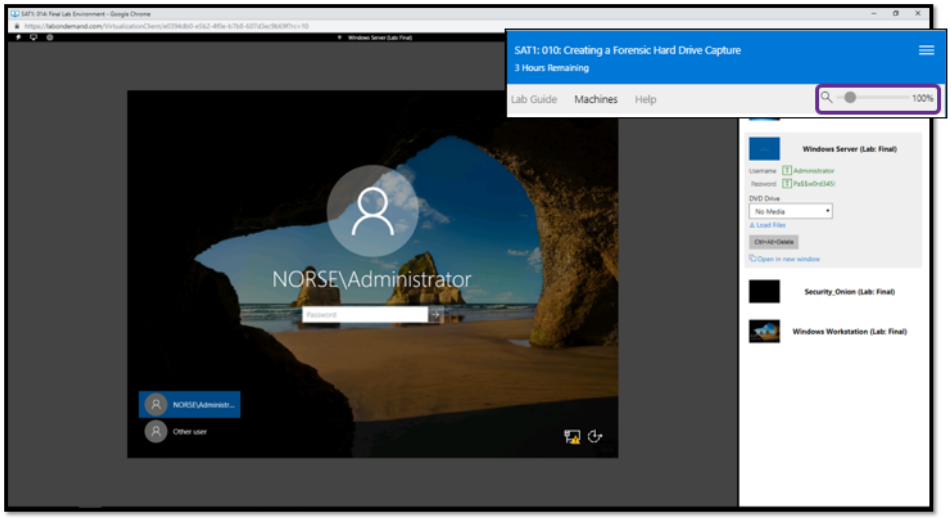
Resources: The Resources tab allows the user to select a resource that they want to view (such as a cloud portal, a managed virtual machine, or a URL). Users can also insert/remove optical media into managed virtual machines from the Resources tab.

Laboratory Interface (cont.)



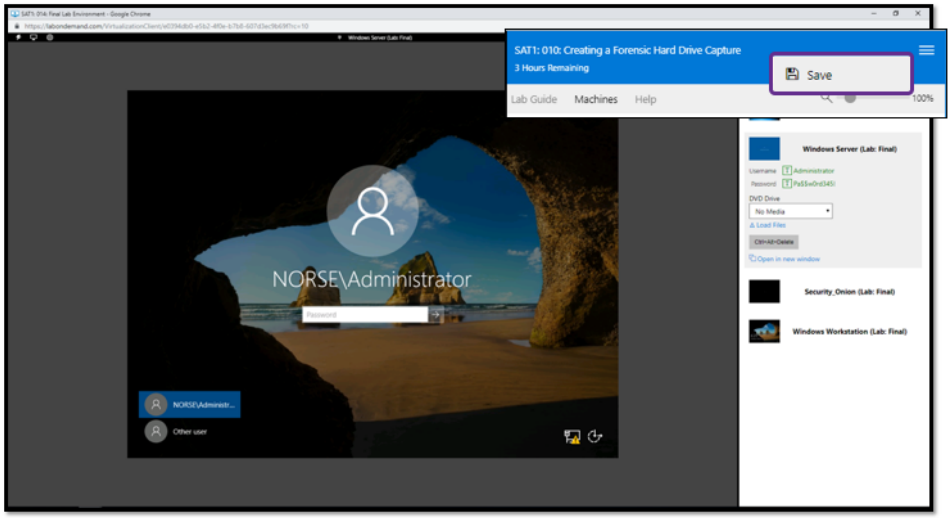
Help: The Help tab allows users to change the theme of the Lab Client, or change the Machine Remote Controller (if the lab has managed VMs). It also provides users with the ID of their lab instance along with other relevant details (depending on the type of lab launched), and links to view a FAQ, submit a support request, or report a bug.

Laboratory Interface (cont.)



Zoom: This allows the user to adjust the zoom level of the lab instructions to make the text larger or smaller.

Laboratory Interface (cont.)

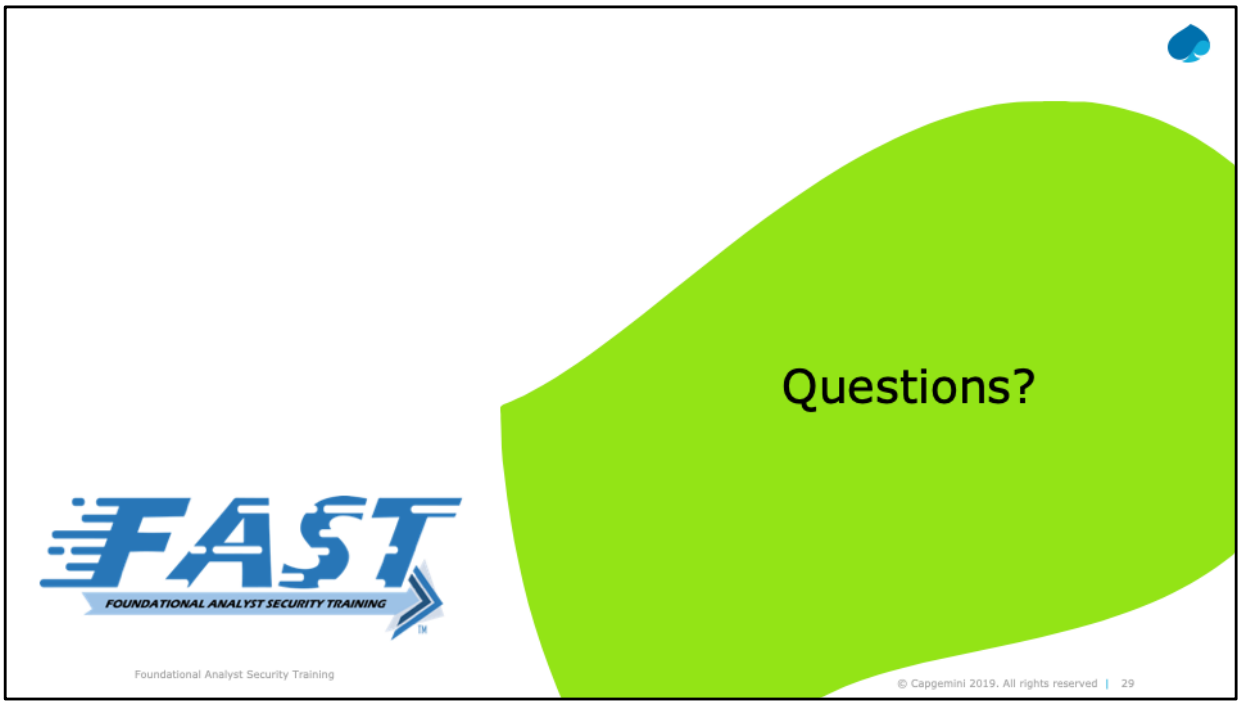


Save/Exit menu: This menu is represented by three horizontal lines, in the upper-right corner of the Lab Console. This menu allows the lab to be saved (if saving is enabled on the lab by the lab author), or end the lab. This menu also allows lab authors to edit the lab instructions.
Resource Portal

This class will be a great experience if you do one thing…

The best ways to get maximum value out of this class is to participate in the lectures and the labs, ask questions, challenge assumptions, and try to have fun.

I am a very interactive instructor; I move around, I talk a lot, but interrupt me! I like it!


Questions?
FAST
FOUNDATIONAL ANALYST SECURITY TRAINING
Foundational Analyst Security Training
© Capgemini 2019. All rights reserved | 29


FAST
FOUNDATIONAL ANALYST SECURITY TRAINING
People matter, results count.
This presentation contains information that may be privileged or confidential and is the property of the CapGemini Group.
Copyright © 2019 CapGemini. All rights reserved.
About CapGemini
A global leader in consulting, technology services and digital transformation, CapGemini is at the forefront of innovation to address the entire breadth of clients' opportunities in the evolving world of cloud, digital and platforms. Building on its strong 50-year heritage and deep industry-specific expertise, CapGemini enables organizations to realize their business ambitions through an array of services from strategy to operations. CapGemini is driven by the conviction that the business value of technology comes from and through people. It is a multicultural company of 200,000 team members in over 40 countries. The Group reported 2017 global revenues of EUR 12.8 billion.
Learn more about us at
www.capgemini.com