

FAST

FOUNDATIONAL ANALYST SECURITY TRAINING



Capgemini 

Module 1 - Course Introduction

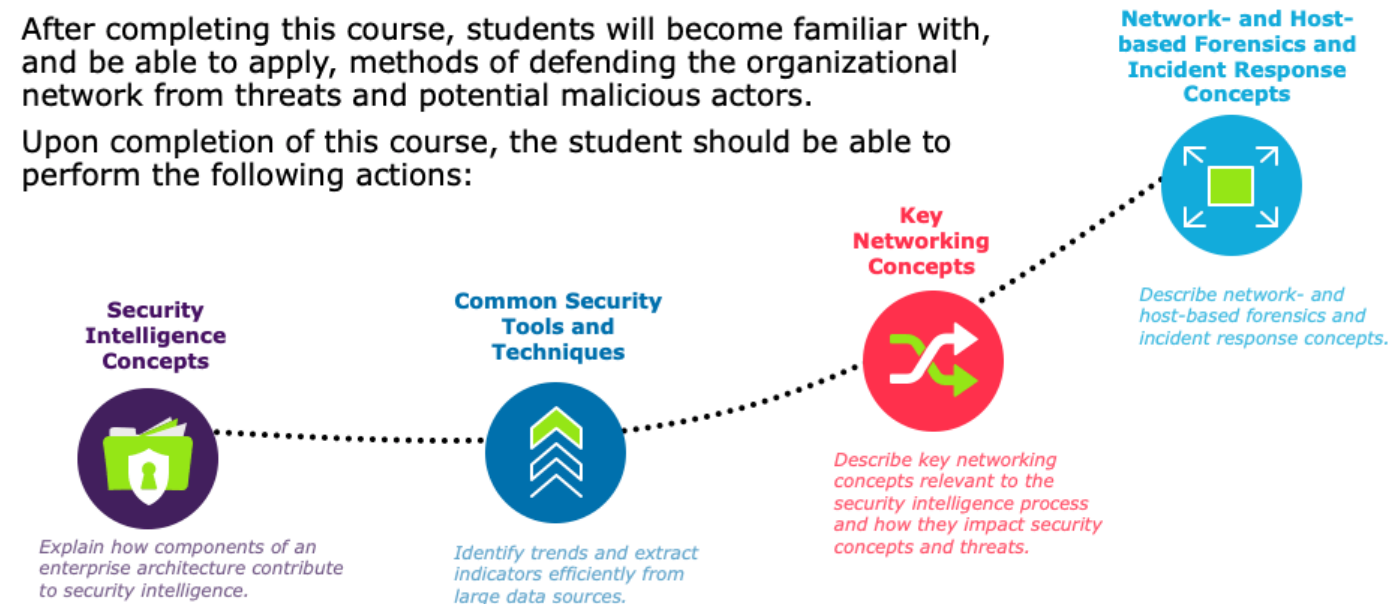


Course Learning Objectives



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:



Introductions and Disclaimer



Agenda



COURSE INTRODUCTION | COURSE EXPECTATIONS | COURSE LAYOUT

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



Introductions



Now tell me about **YOU!**

Let's go **around** the room; and tell us all your name,
your **job title**, what you hope to get out of this training,
and one **interesting** thing about yourself!

Course Introductions

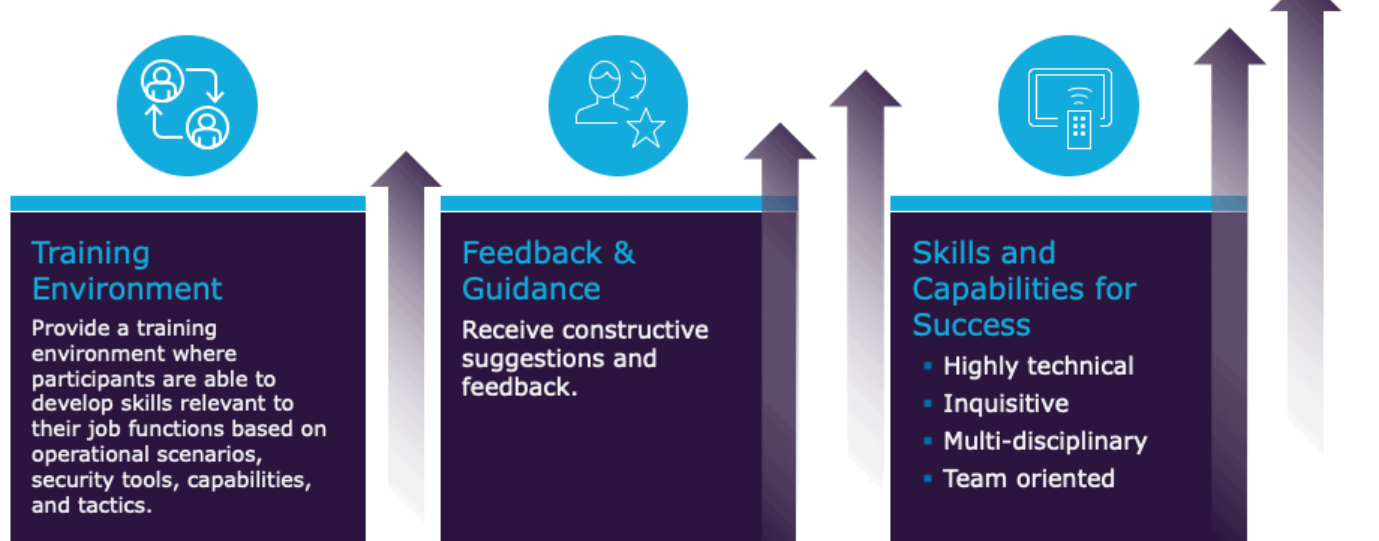


DISCLAIMER

Course Expectations



Mission of this Course



Course Expectations



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 **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 THE FOLLOWING:

- 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

How this Course is Structured





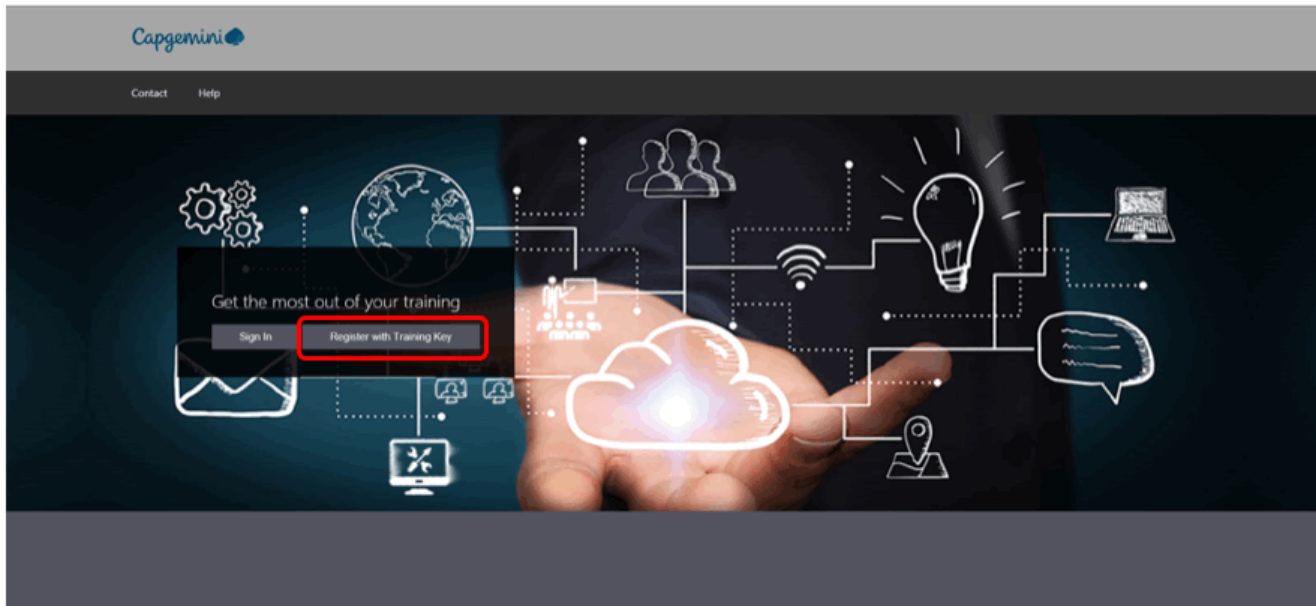
Course Agenda and Schedule

- We will take breaks as needed.
- Over 40 hours of content and exercises.
- The course is approximately half instruction and half hands-on exercises.
- Daily Schedule (times may change based on Day 1 consensus):
 - Hours: 8:00 a.m. – 5:00 p.m.
 - Lunch

Laboratory Introduction



Each of you will be given a key.





Use your key at <https://capgemini.cyber.learnondemand.net>.




The screenshot shows the Capgemini website interface. At the top, the Capgemini logo is on the left, and 'Contact' and 'Help' links are on the right. The main content area has a dark background with white line-art icons representing various concepts like gears, a globe, a lightbulb, a laptop, a speech bubble, and a location pin. A modal window titled 'Register With Training Key' is centered on the screen. Inside the modal, the text 'Register with a Training Key' is followed by a text input field, which is highlighted with a red rectangle. Below the input field is a 'Register' button. In the background of the website, there is a 'Sign In' button and a 'Register with Training Key' button. At the bottom of the modal, there is a grey box with the text: 'Next, you will fill out your personal information to create your account.'



You will select SOC ANALYST TIER 1.





 Martin ▾ 


My TrainingMy TranscriptContactHelp

 Current Training
Martin McFly

 Details  Edit

 Transcript  Redeem Training Key

All times shown in Eastern Standard Time.

Classes (1) 

Class	Room	When ↑	Status
SOC ANALYST TIER 1: Tools and Techniques for Network Defense -TESTING	Virtual	Wednesday, March 20, 2019 9:00 PM - Friday, March 22, 2019 9:00 PM (Eastern Standard Time)	Enrolled

Enter your personal information.



Student: **Martin Michy** Details ▾

Event: **SOC ANALYST TIER 1: Tools and Techniques for Network Defense -TESTING** Details ▾

Enrollment Status: **Enrolled**

Completion Status: **Attending**

Classroom: **Virtual**

Is Retake: **No**

Enable Labs: **Yes**

Activities ^

Access to your labs will expire on Wednesday, September 10, 2019 8:00 PM (Central Standard Time)

6%

1 of 16 required activities complete

Working in the Command Line

☒ 1

LINUX Command Line Essentials (Expected Duration 30 minutes, 0 seconds) Details ▾

SOC ANALYST TIER 1: Tools and Techniques for Network Defense, SAT1: 001

Required: Yes

Status: Passed

Started: Thursday, March 21, 2019 11:16 AM (Eastern Standard Time)

Ended: Thursday, March 21, 2019 11:25 AM (Eastern Standard Time)

Score: 80

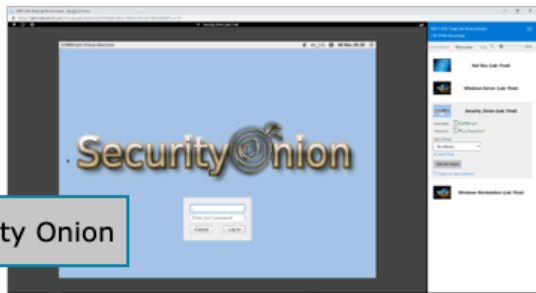
Launch

↓

→ 2

LINUX File Manipulation (Expected Duration 30 minutes, 0 seconds) Details ▾

Laboratory Interface: UNBUNTU



The second UNIX variant we will be using is **Security Onion.**

Security Onion is a free and open source Linux distribution for intrusion detection, enterprise security monitoring, and log management.

Security Onion

... includes Wireshark, Squid, Snort, and many other network defense tools

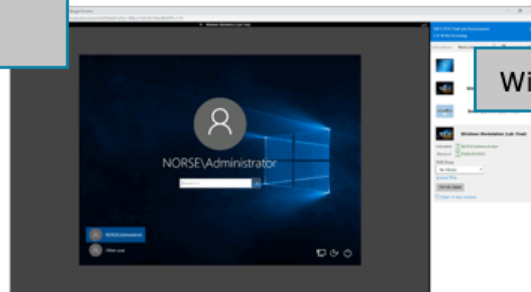
... multiple Network Interface Cards (NICs) for monitoring on multiple network interfaces

... if Kali Linux is your adversaries' sword, Security Onion is your shield!

Laboratory Interface: Windows Machines



We will also be using
Windows 10.



Windows 10

Laboratory Interface



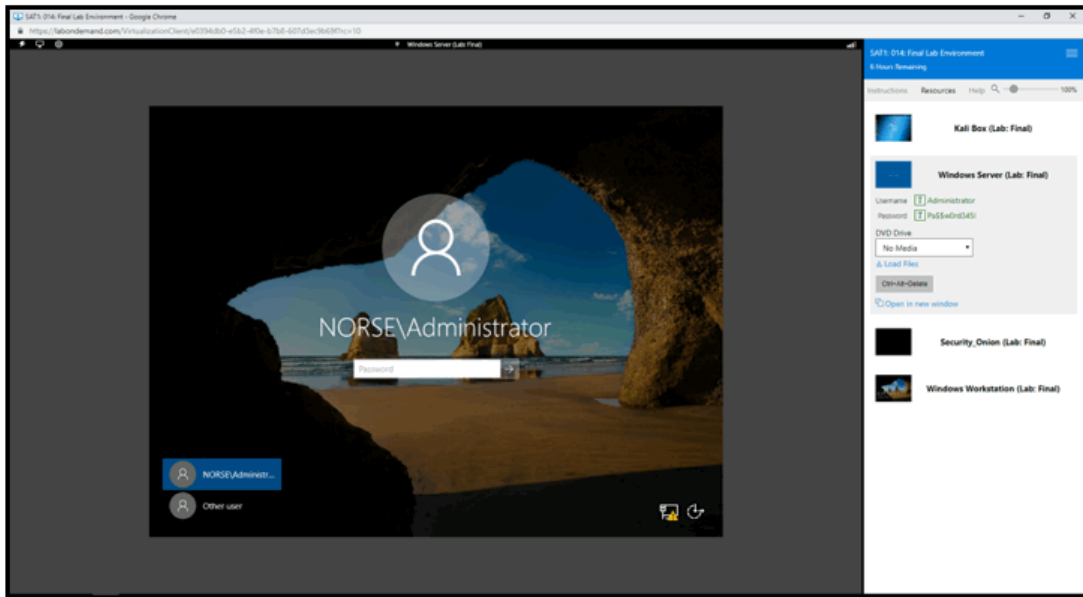
LABORATORY FEATURES:

Operating Systems:	Ubuntu, Windows 10	RAM:	~10GB
		Hard Disk:	~25-80GB

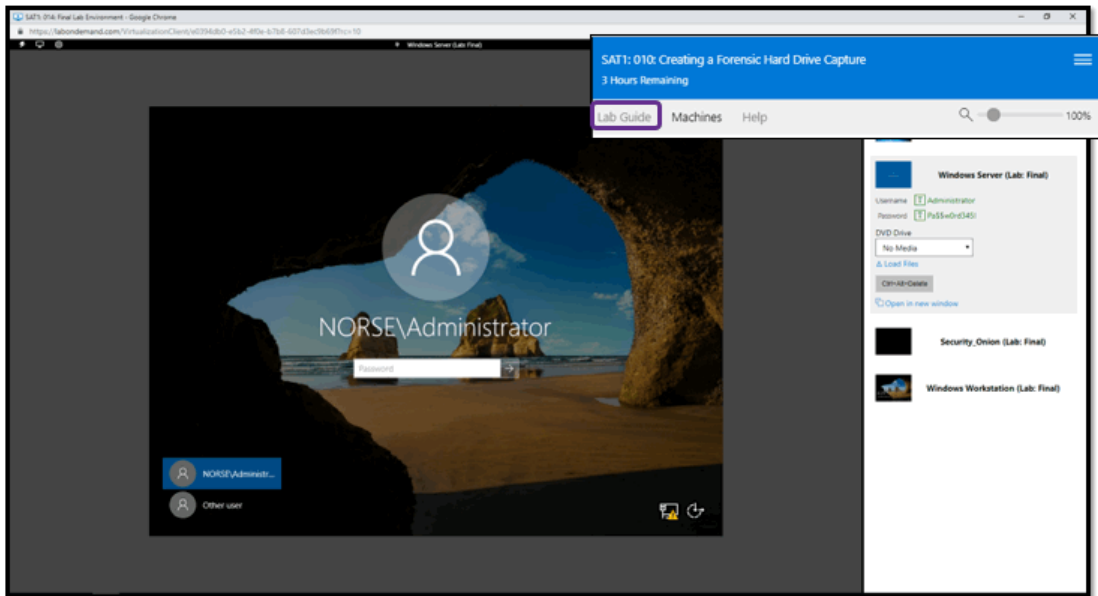
Internet Access: Yes*

Installed Software: Varies by laboratory and machine, but all typical software types are included.

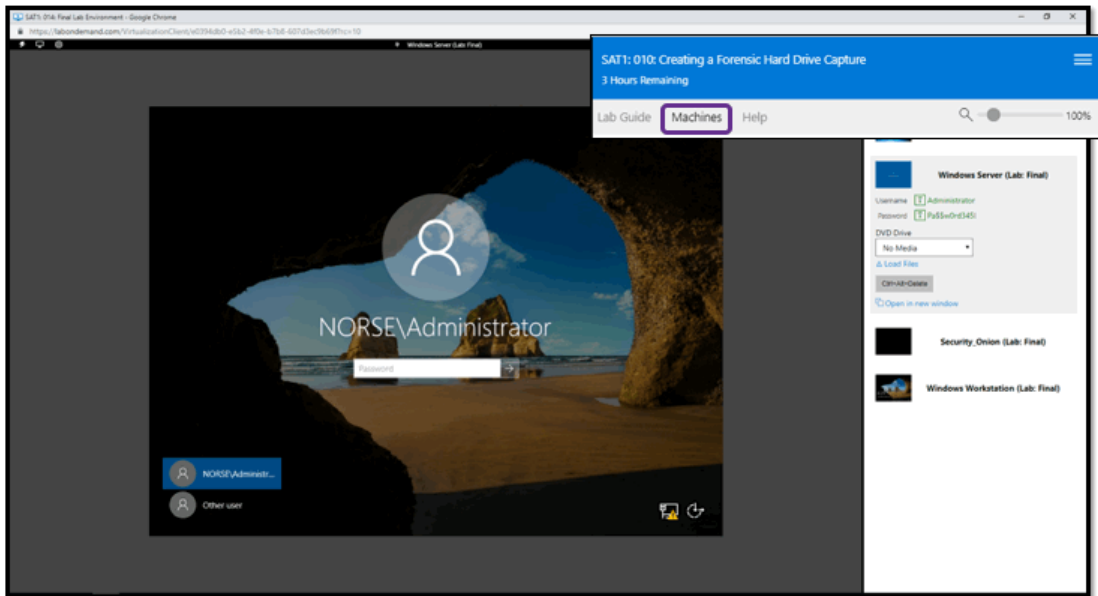
Laboratory Interface (cont.)



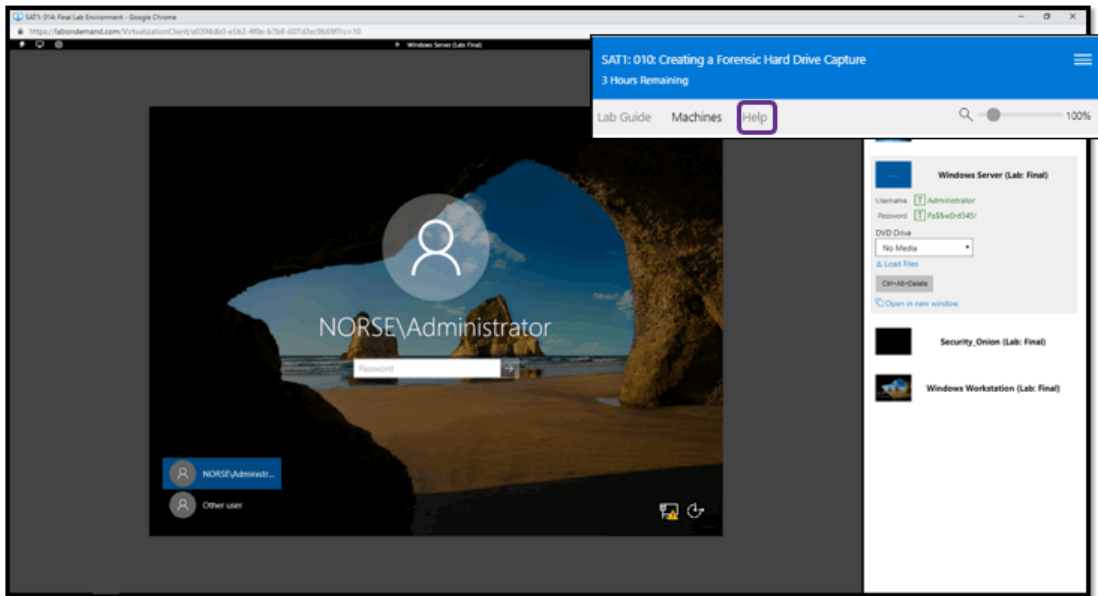
Laboratory Interface (cont.)



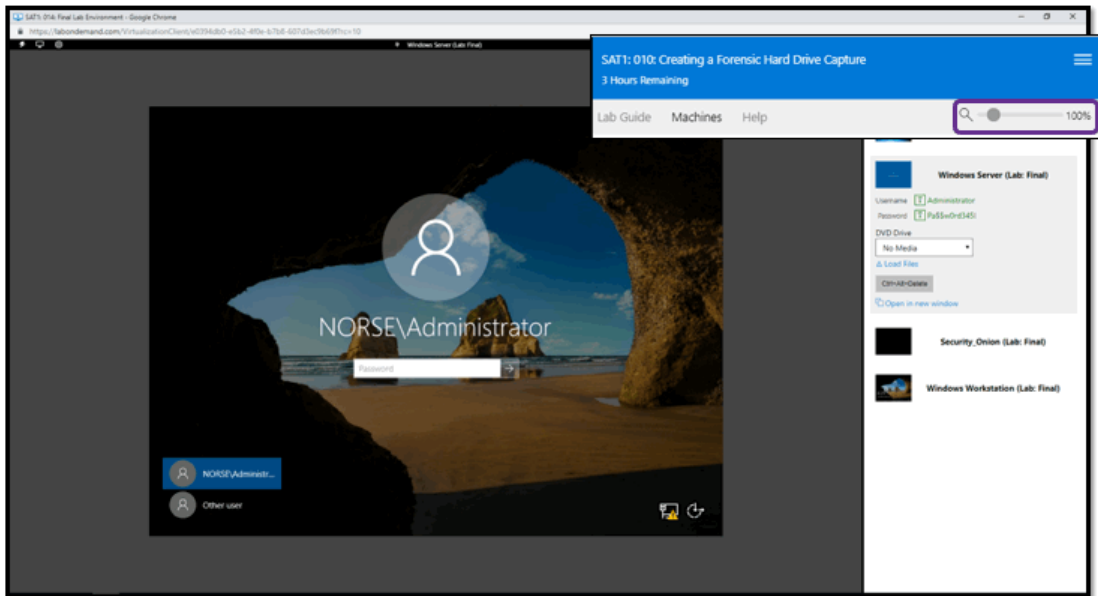
Laboratory Interface (cont.)



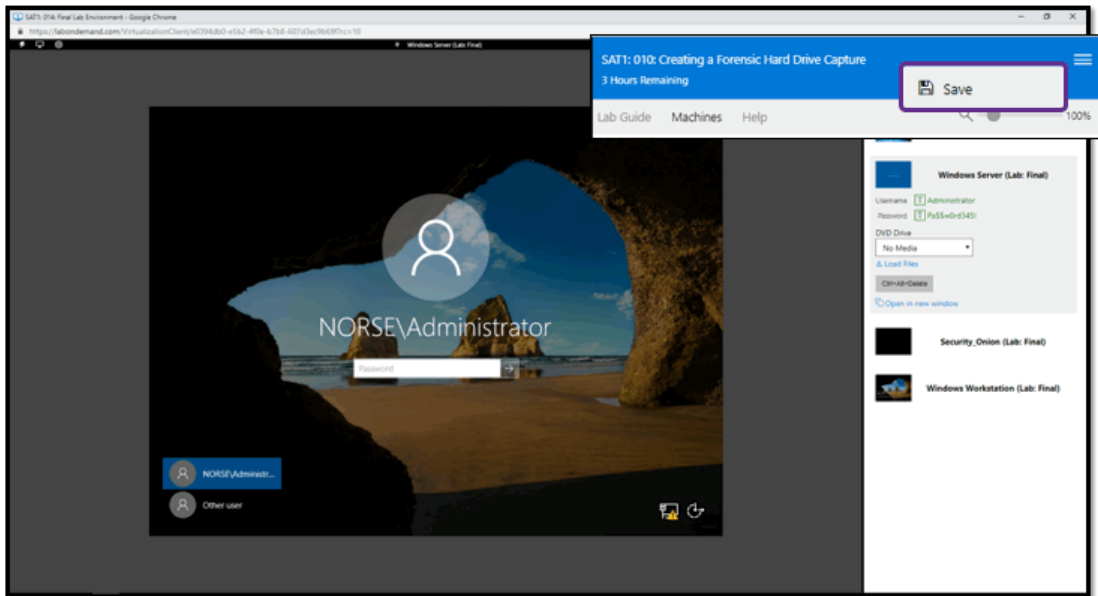
Laboratory Interface (cont.)



Laboratory Interface (cont.)



Laboratory Interface (cont.)



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?



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