487.6

Capstone: Capture (and Present) the Flags

SANS

THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH | sans.org

PLEASE READ THE TERMS AND CONDITIONS OF THIS COURSEWARE LICENSE AGREEMENT ("CLA") CAREFULLY BEFORE USING ANY OF THE COURSEWARE ASSOCIATED WITH THE SANS COURSE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU (THE “USER”) AND SANS INSTITUTE FOR THE COURSEWARE. YOU AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU.

With the CLA, SANS Institute hereby grants User a personal, non-exclusive license to use the Courseware subject to the terms of this agreement. Courseware includes all printed materials, including course books and lab workbooks, as well as any digital or other media, virtual machines, and/or data sets distributed by SANS Institute to User for use in the SANS class associated with the Courseware. User agrees that the CLA is the complete and exclusive statement of agreement between SANS Institute and you and that this CLA supersedes any oral or written proposal, agreement or other communication relating to the subject matter of this CLA.

BY ACCEPTING THIS COURSEWARE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS CLA. BY ACCEPTING THIS SOFTWARE, YOU AGREE THAT ANY BREACH OF THE TERMS OF THIS CLA MAY CAUSE IRREPARABLE HARM AND SIGNIFICANT INJURY TO SANS INSTITUTE, AND THAT SANS INSTITUTE MAY ENFORCE THESE PROVISIONS BY INJUNCTION (WITHOUT THE NECESSITY OF POSTING BOND) SPECIFIC PERFORMANCE, OR OTHER EQUITABLE RELIEF.

If you do not agree, you may return the Courseware to SANS Institute for a full refund, if applicable.

User may not copy, reproduce, re-publish, distribute, display, modify or create derivative works based upon all or any portion of the Courseware, in any medium whether printed, electronic or otherwise, for any purpose, without the express prior written consent of SANS Institute. Additionally, User may not sell, rent, lease, trade, or otherwise transfer the Courseware in any way, shape, or form without the express written consent of SANS Institute.

If any provision of this CLA is declared unenforceable in any jurisdiction, then such provision shall be deemed to be severable from this CLA and shall not affect the remainder thereof. An amendment or addendum to this CLA may accompany this Courseware.

SANS acknowledges that any and all software and/or tools, graphics, images, tables, charts or graphs presented in this Courseware are the sole property of their respective trademark/registered/copyright owners, including:

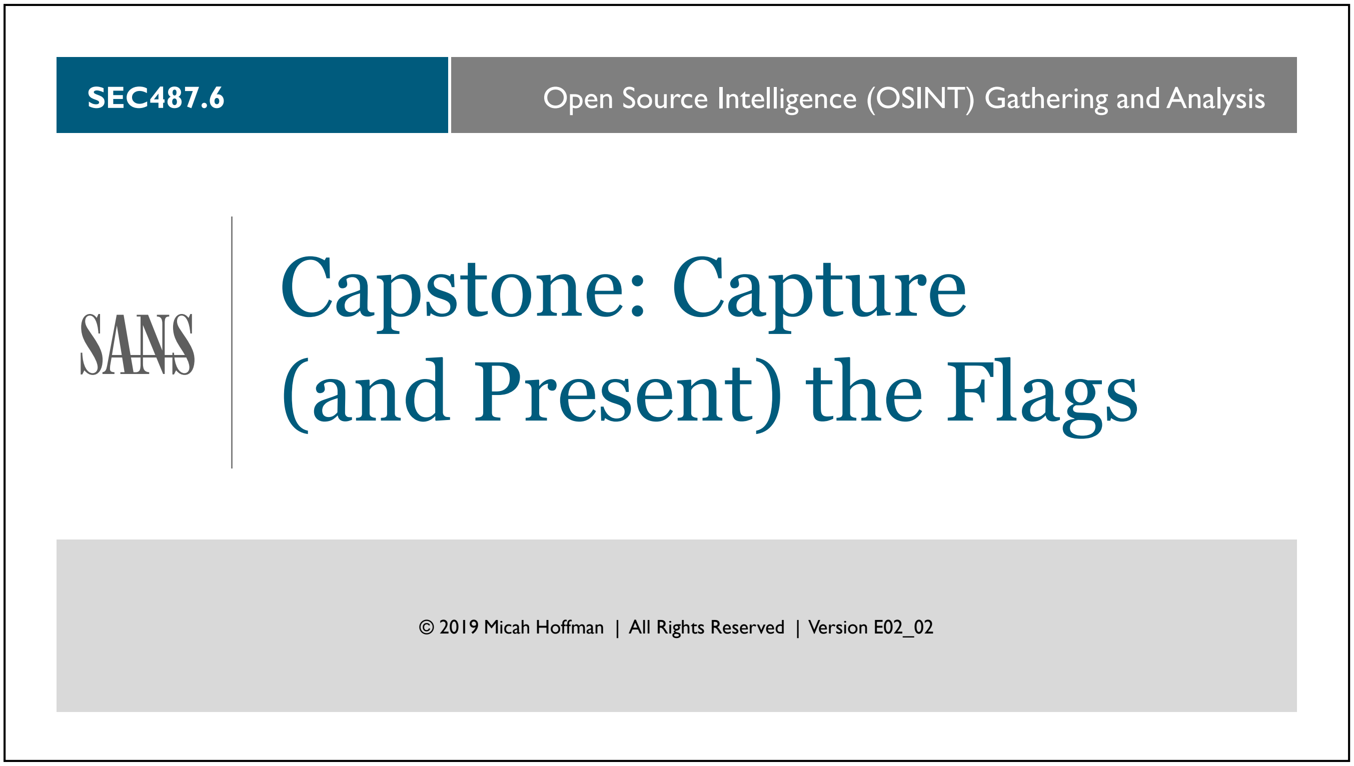
AirDrop, AirPort, AirPort Time Capsule, Apple, Apple Remote Desktop, Apple TV, App Nap, Back to My Mac, Boot Camp, Cocoa, FaceTime, FileVault, Finder, FireWire, FireWire logo, iCal, iChat, iLife, iMac, iMessage, iPad, iPad Air, iPad Mini, iPhone, iPhoto, iPod, iPod classic, iPod shuffle, iPod nano, iPod touch, iTunes, iTunes logo, iWork, Keychain, Keynote, Mac, Mac Logo, MacBook, MacBook Air, MacBook Pro, Macintosh, Mac OS, Mac Pro, Numbers, OS X, Pages, Passbook, Retina, Safari, Siri, Spaces, Spotlight, There’s an app for that, Time Capsule, Time Machine, Touch ID, Xcode, Xserve, App Store, and iCloud are registered trademarks of Apple Inc.

PMP and PMBOK are registered marks of PMI.

SOF-ELK® is a registered trademark of Lewes Technology Consulting, LLC. Used with permission.

SIFT® is a registered trademark of Harbingers, LLC. Used with permission.

Governing Law: This Agreement shall be governed by the laws of the State of Maryland, USA.

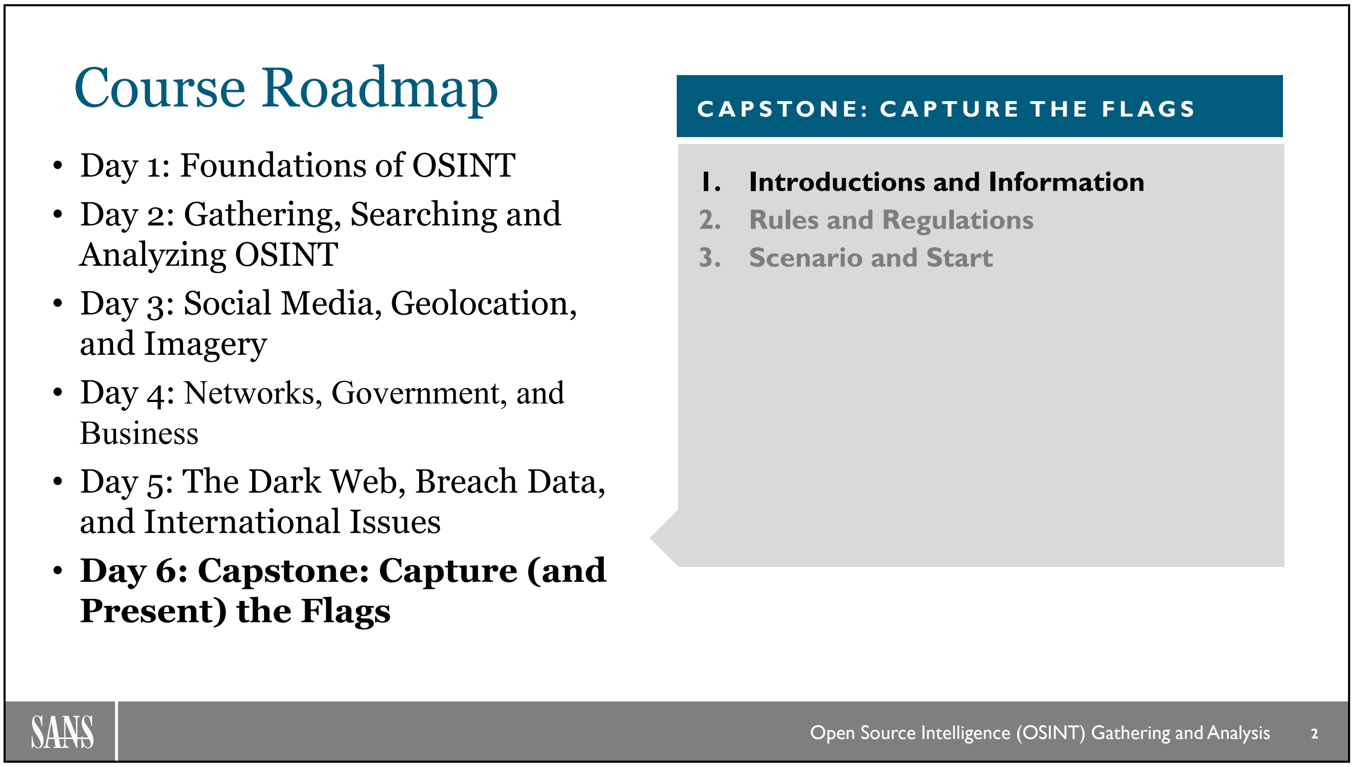


SEC487.6

Open Source Intelligence (OSINT) Gathering and Analysis

Capstone: Capture (and Present) the Flags

Welcome to SEC487 Open Source Intelligence (OSINT) Gathering and Analysis!



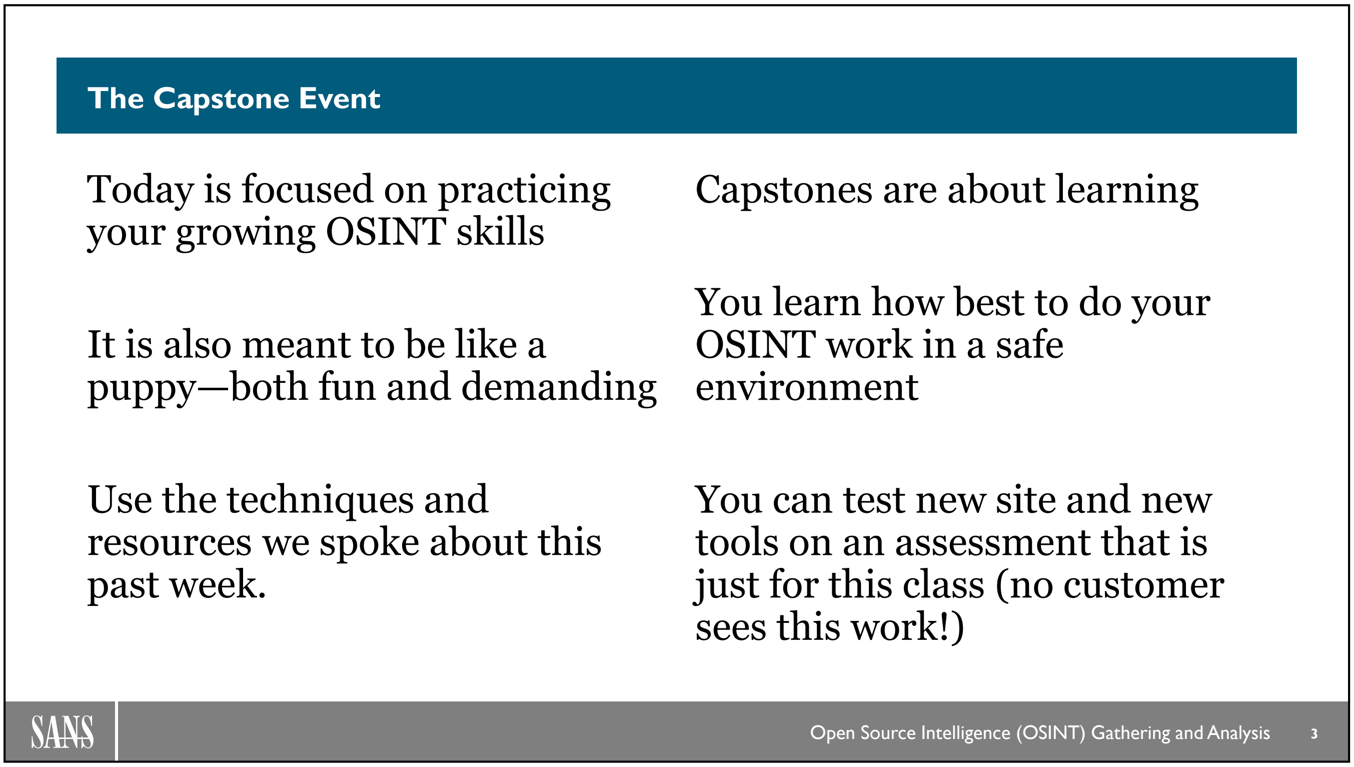
Course Roadmap

- Day 1: Foundations of OSINT
- Day 2: Gathering, Searching and Analyzing OSINT
- Day 3: Social Media, Geolocation, and Imagery
- Day 4: Networks, Government, and Business
- Day 5: The Dark Web, Breach Data, and International Issues
- **Day 6: Capstone: Capture (and Present) the Flags**

CAPSTONE: CAPTURE THE FLAGS

1. **Introductions and Information**
2. Rules and Regulations
3. Scenario and Start

This page intentionally left blank.



The Capstone Event

Today is focused on practicing your growing OSINT skills

It is also meant to be like a puppy—both fun and demanding

Use the techniques and resources we spoke about this past week.

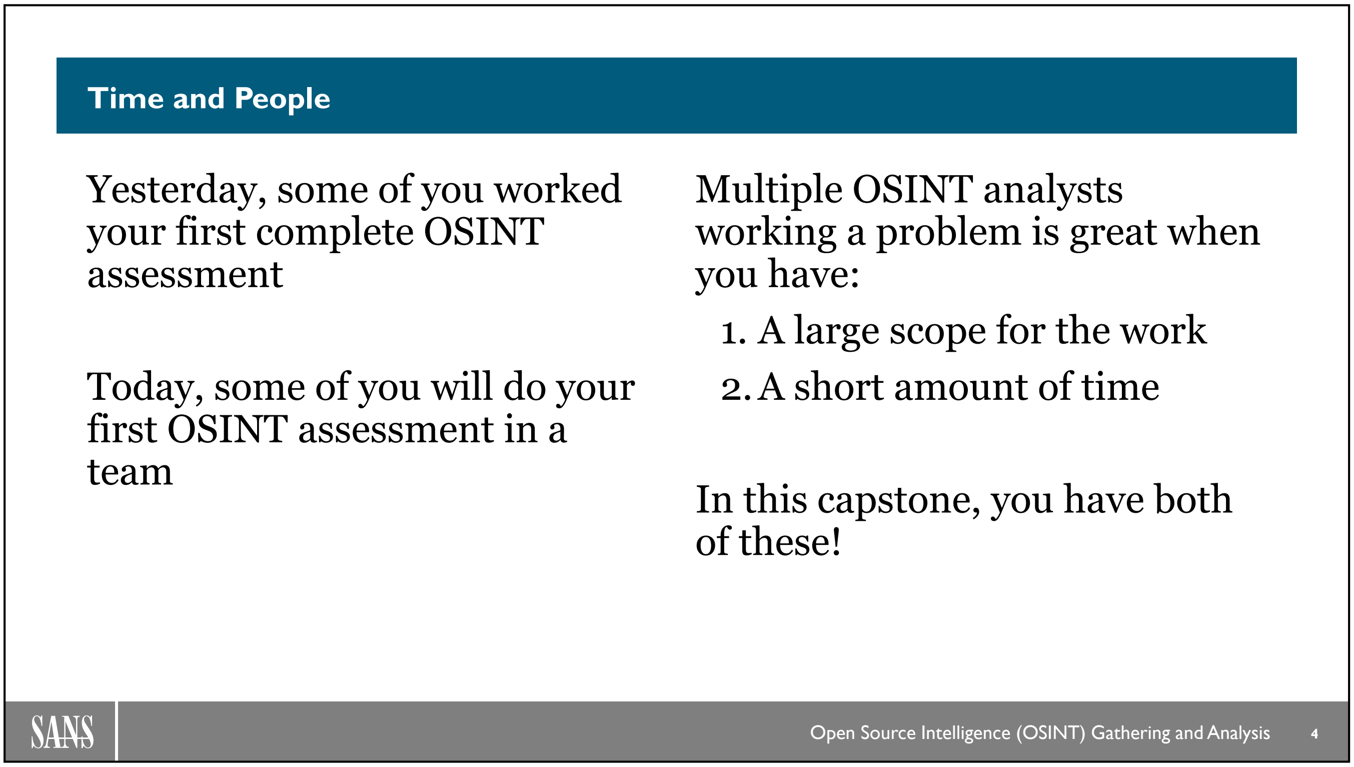
Capstones are about learning

You learn how best to do your OSINT work in a safe environment

You can test new site and new tools on an assessment that is just for this class (no customer sees this work!)

The Capstone Event

All week you have been learning techniques and new resources for gathering and analyzing OSINT data. Much like yesterday's Solo CTF, today, you will again practice your skills. The capstone event is just as much about learning as the previous five days been have. But instead of learning about a tool or web site, today you will be learning about implementing your knowledge. Today you will be able to try new tools and resources in an assessment that, outside of this course, does not matter. Experiment with your work here.



Time and People

Yesterday, some of you worked your first complete OSINT assessment

Today, some of you will do your first OSINT assessment in a team

Multiple OSINT analysts working a problem is great when you have:

1. A large scope for the work
2. A short amount of time

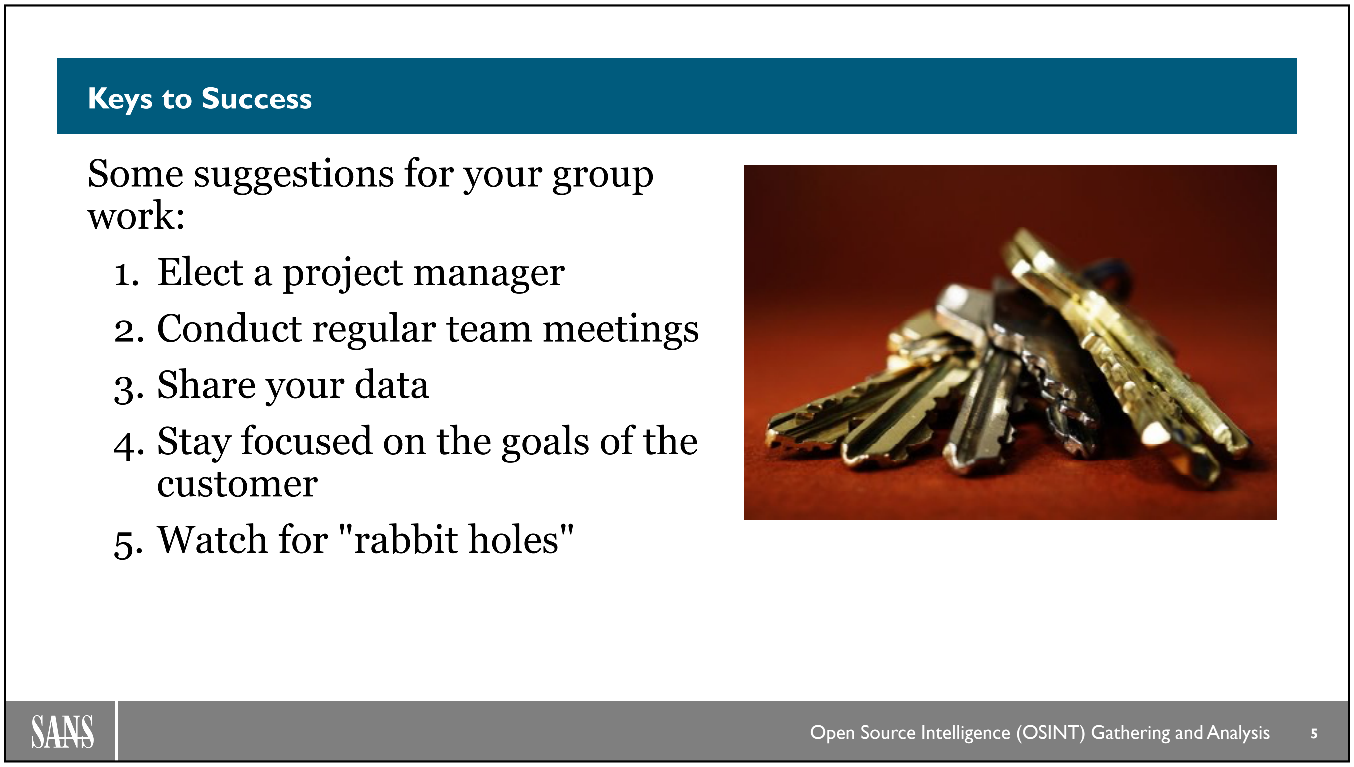
In this capstone, you have both of these!

SANS

Open Source Intelligence (OSINT) Gathering and Analysis 4

Time and People

Yesterday may have been the first time that some of you performed a solo OSINT assessment. Today, you will work in teams to accomplish your OSINT goals. Working with other OSINT analysts is beneficial when we have a lot of work to do or a short time to get the assessment completed. In this capstone, you will have both of these.



Keys to Success

Some suggestions for your group work:

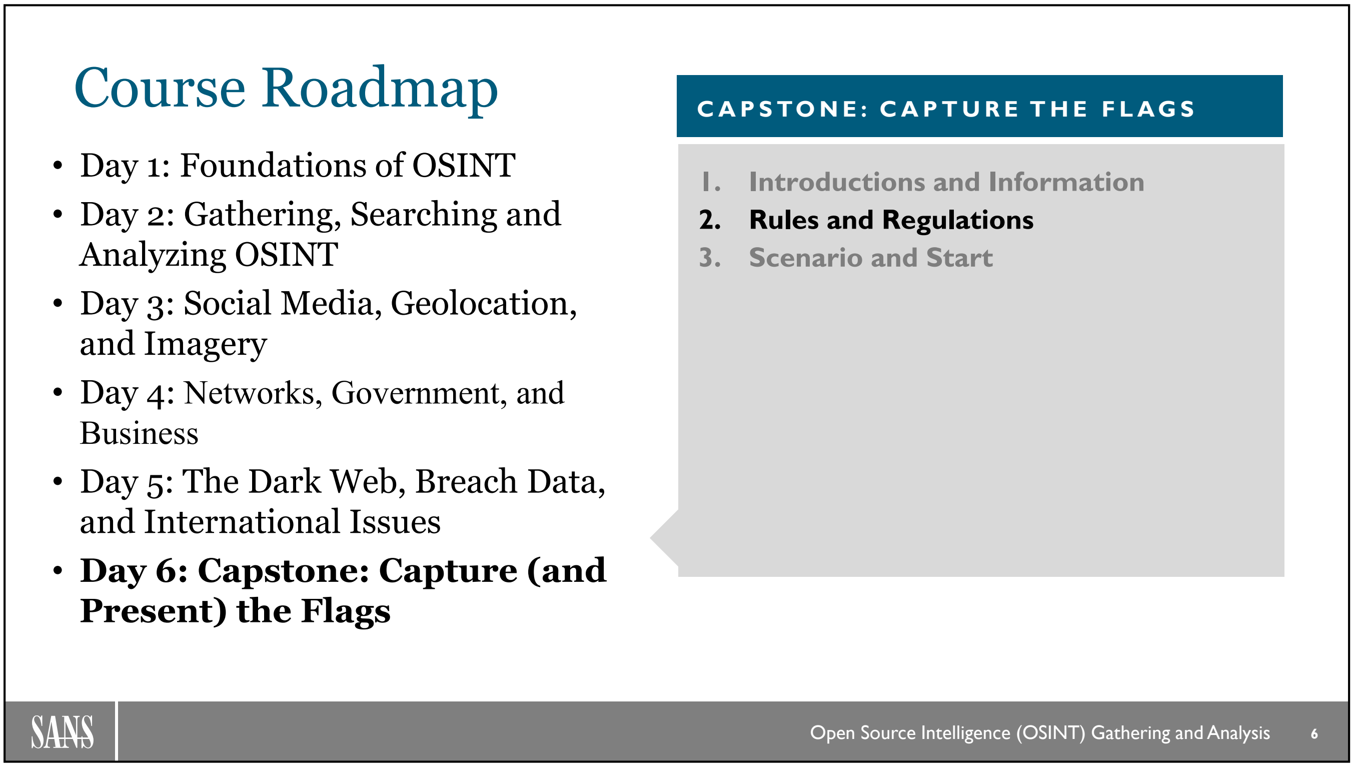
1. Elect a project manager
2. Conduct regular team meetings
3. Share your data
4. Stay focused on the goals of the customer
5. Watch for "rabbit holes"

Keys to Success

Working in groups can be hard for people who are used to working on projects by themselves. For people who have spent the past five days in a class and haven't really "worked" with each other, it can be even more challenging. We do have some tips for your capstone group-work, however:

1. **Elect a Project Manager** - Each group should have someone who takes charge over the work and ensures that the end product addresses your customer's issues.
2. **Conduct Team Meetings** - If you don't know what the other team members have found, then your part of the assessment may not be as complete. Share information and make course corrections to the work your group is doing.
3. **Share Your Data** - Make sure your teammates have access to the data you collect and the analyses you perform.
4. **Stay Focused** - There are many things that can distract us in our assessments. Some are not our fault, and some can be minimized or avoided. Keep the goals of your customer in mind as you perform your work, and constantly ask, "Is this important to the customer?"
5. **Watch for Rabbit Holes** - Rabbit holes are deep and narrow. Within OSINT, they are times when you find something interesting that you want to pursue. At first, it may have been important to the work, but now that you have worked on it for a while, it is not. An example of this is finding information about a subject's immediate family and then branching out to those people and their families, and their families, and so on. At first, your work was focused on the assignment. At a certain point, you need to reign in and refocus.

Image from https://sec487.info/pf, December 3, 2017.



Course Roadmap

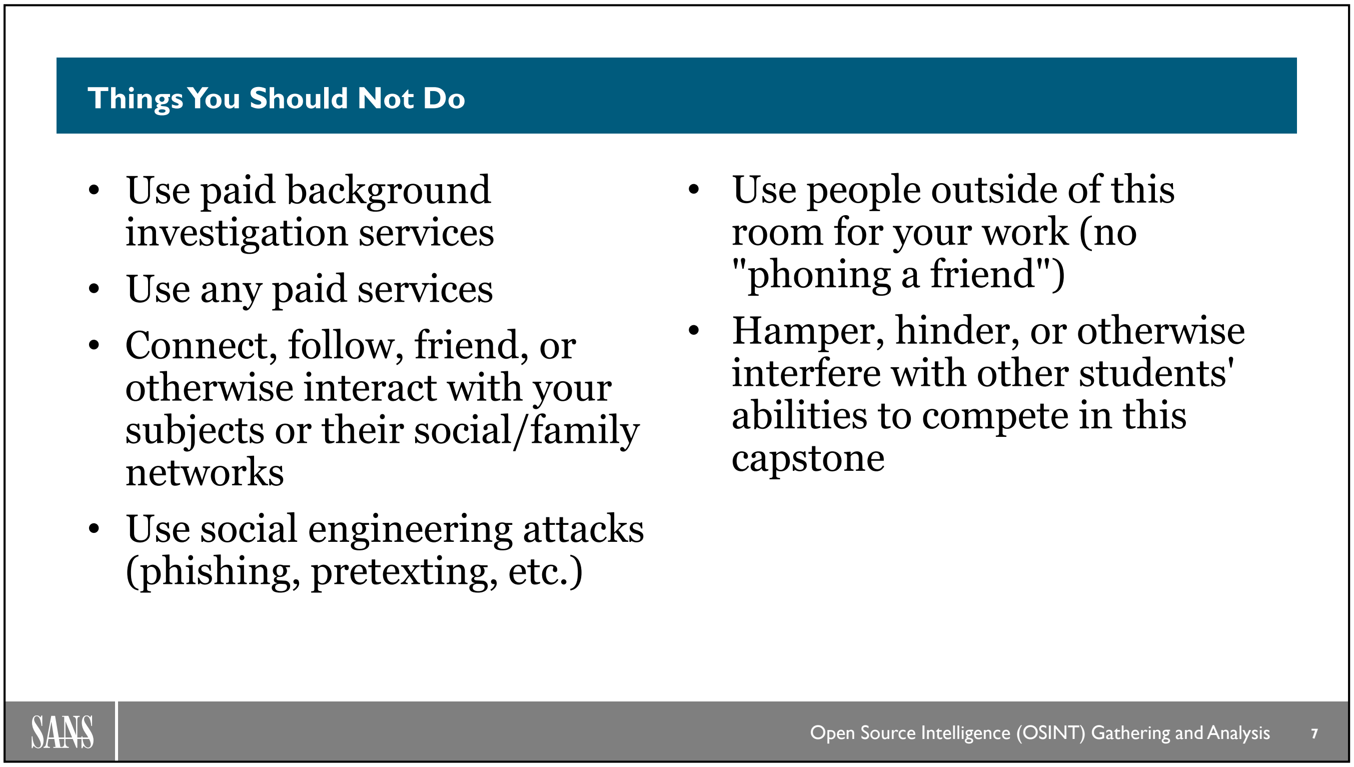
- Day 1: Foundations of OSINT
- Day 2: Gathering, Searching and Analyzing OSINT
- Day 3: Social Media, Geolocation, and Imagery
- Day 4: Networks, Government, and Business
- Day 5: The Dark Web, Breach Data, and International Issues
- **Day 6: Capstone: Capture (and Present) the Flags**

CAPSTONE: CAPTURE THE FLAGS

1. Introductions and Information
2. **Rules and Regulations**
3. Scenario and Start

SANS

This page intentionally left blank.



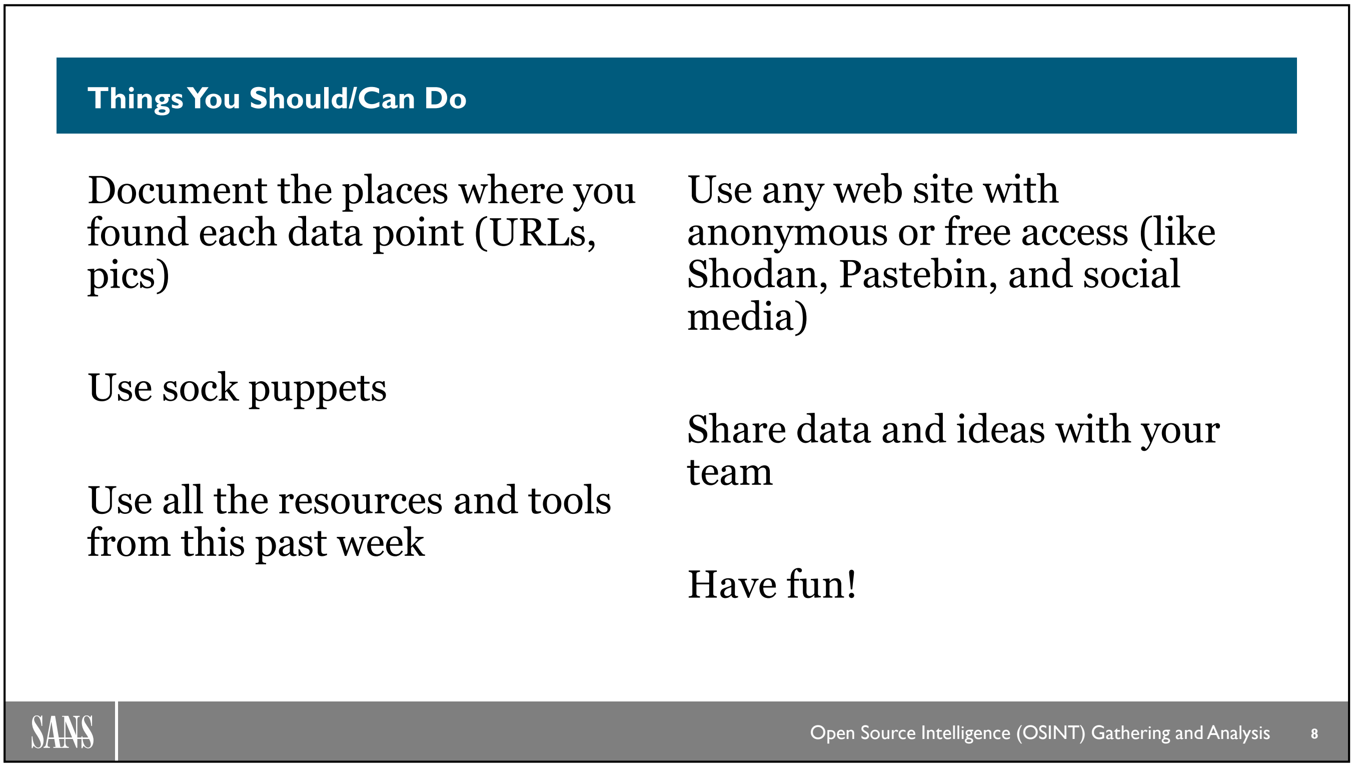
Things You Should Not Do

- Use paid background investigation services
- Use any paid services
- Connect, follow, friend, or otherwise interact with your subjects or their social/family networks
- Use social engineering attacks (phishing, pretexting, etc.)
- Use people outside of this room for your work (no "phoning a friend")
- Hamper, hinder, or otherwise interfere with other students' abilities to compete in this capstone

Things You Should Not Do

Let's set up some guidelines for today's competition so that everyone understands what is and what is not in scope. We first will discuss the things you should **NOT** do:

- Do not use paid background investigation services to speed up assessments. We realize that many of you may have access to some amazing paid services that can be used to create rapid, complete data pulls of a person or company. Today is about YOUR abilities to gather and analyze data, not some vendor's.
- Do not use any services that you or others would have to pay to gain access to.
- This should be a totally passive assessment. There is to be no physical or electronic engagement with the targets, their friends, colleagues, families, or other people they interact with.
- Just to be explicit, you are not allowed to phish, pretext, or perform other penetration testing or social engineering activities on targets (people, businesses, or other).
- Do not call, text, IM, Slack, tweet, post, or otherwise ask or get people outside this room to assist you or your team in any way.
- Do not make it harder for other teams that you are competing against to work their assessments.



Things You Should/Can Do

Document the places where you found each data point (URLs, pics)

Use sock puppets

Use all the resources and tools from this past week

Use any web site with anonymous or free access (like Shodan, Pastebin, and social media)

Share data and ideas with your team

Have fun!

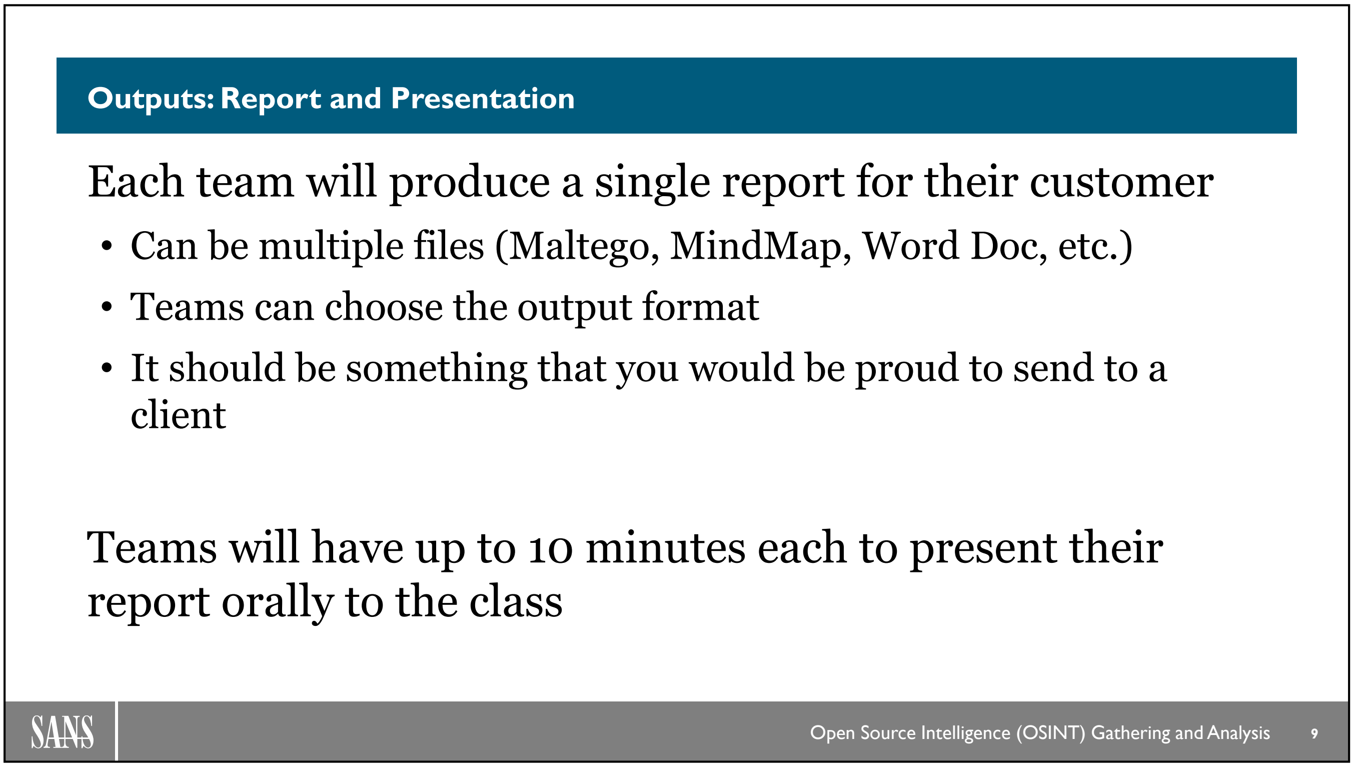
SANS

Open Source Intelligence (OSINT) Gathering and Analysis 8

Things You Should/Can Do

We also have things that you CAN do:

- All significant details should include where they were discovered. This can be URLs or tool outputs as well as screenshots. Document everything, as the instructor may perform spot checks of your content.
- You may use sock puppet accounts in places where you need them. If you do, be sure to note if data could only be found by using the sock puppets versus via unauthenticated means.
- You can use all the techniques, tools, and resources from this past week.
- You may use paid accounts from web sites such as Shodan, Pastebin, and Echosec to perform your work. If you have a question about whether you can or cannot use a certain paid resource, ask your instructor.
- Share your data, ideas, and techniques with your teammates. Help them learn!
- Have fun!



Outputs: Report and Presentation

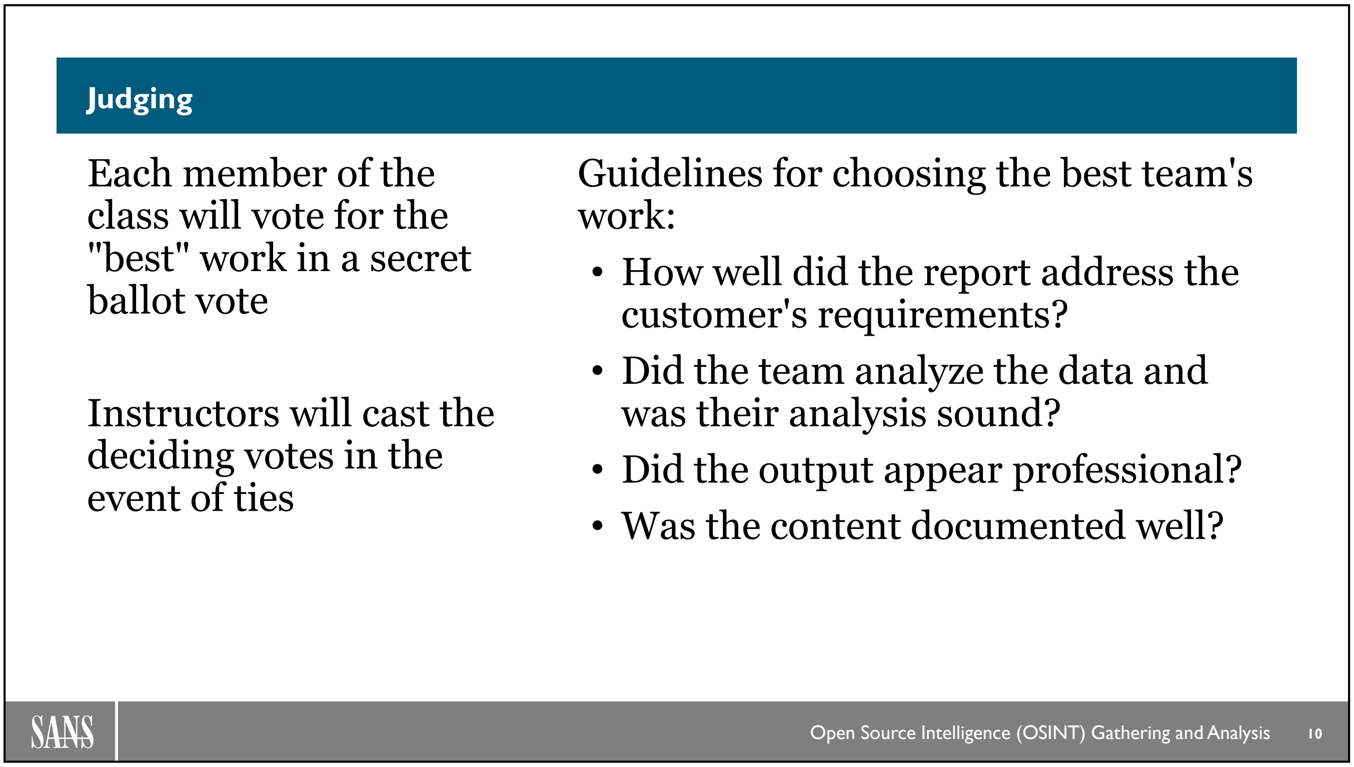
Each team will produce a single report for their customer

- Can be multiple files (Maltego, MindMap, Word Doc, etc.)
- Teams can choose the output format
- It should be something that you would be proud to send to a client

Teams will have up to 10 minutes each to present their report orally to the class

Outputs: Report and Presentation

Each team will need to combine each member's data into a single document. The type of document and format is left to the teams to decide. The report should be professional and represent the team's work.



Judging

Each member of the class will vote for the "best" work in a secret ballot vote

Instructors will cast the deciding votes in the event of ties

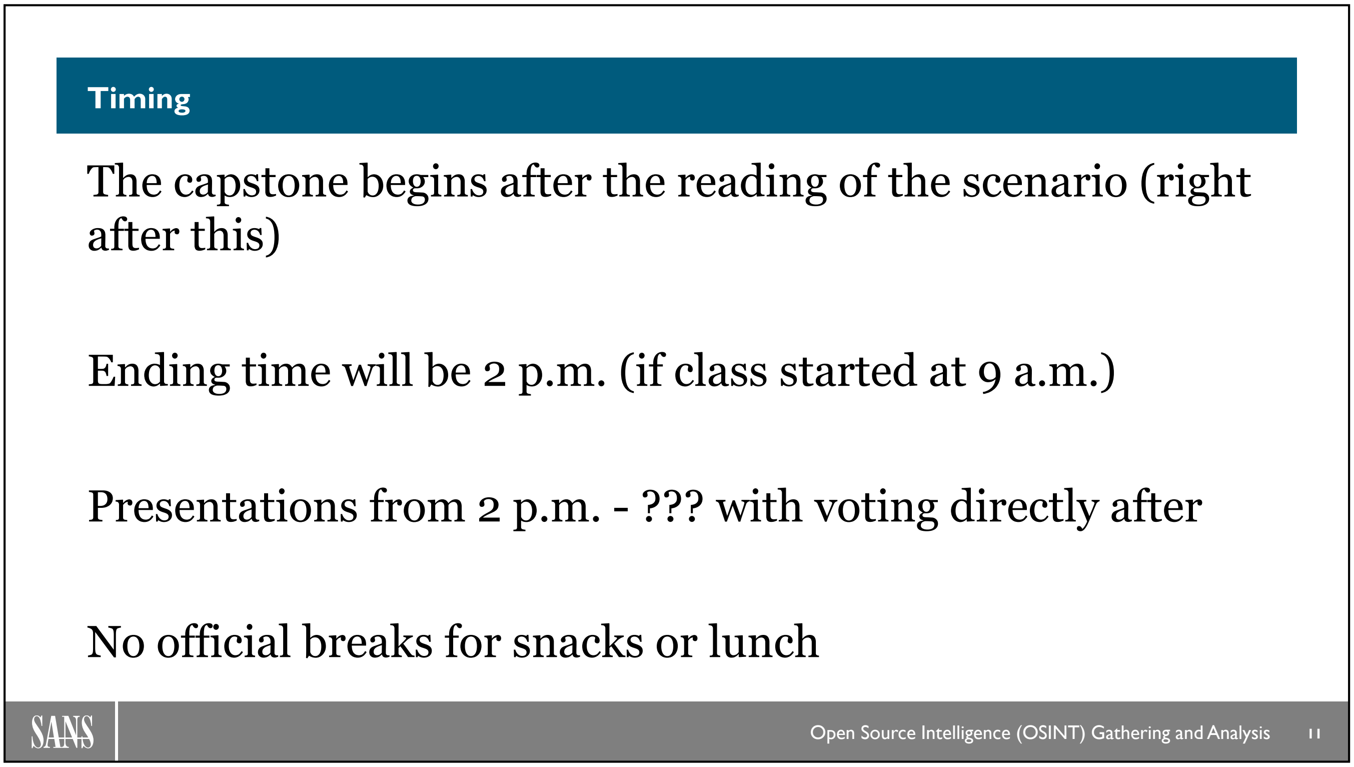
Guidelines for choosing the best team's work:

- How well did the report address the customer's requirements?
- Did the team analyze the data and was their analysis sound?
- Did the output appear professional?
- Was the content documented well?

Judging

After each team presents a 10-minute overview of their work to the class, each class member will vote on which team had the "best" work. Each member of the class will have a single vote that they can cast for one of the teams.

While what makes "the best" work can be somewhat subjective, we suggest that you consider the questions in the above slide when choosing your favorite presentation.



Timing

The capstone begins after the reading of the scenario (right after this)

Ending time will be 2 p.m. (if class started at 9 a.m.)

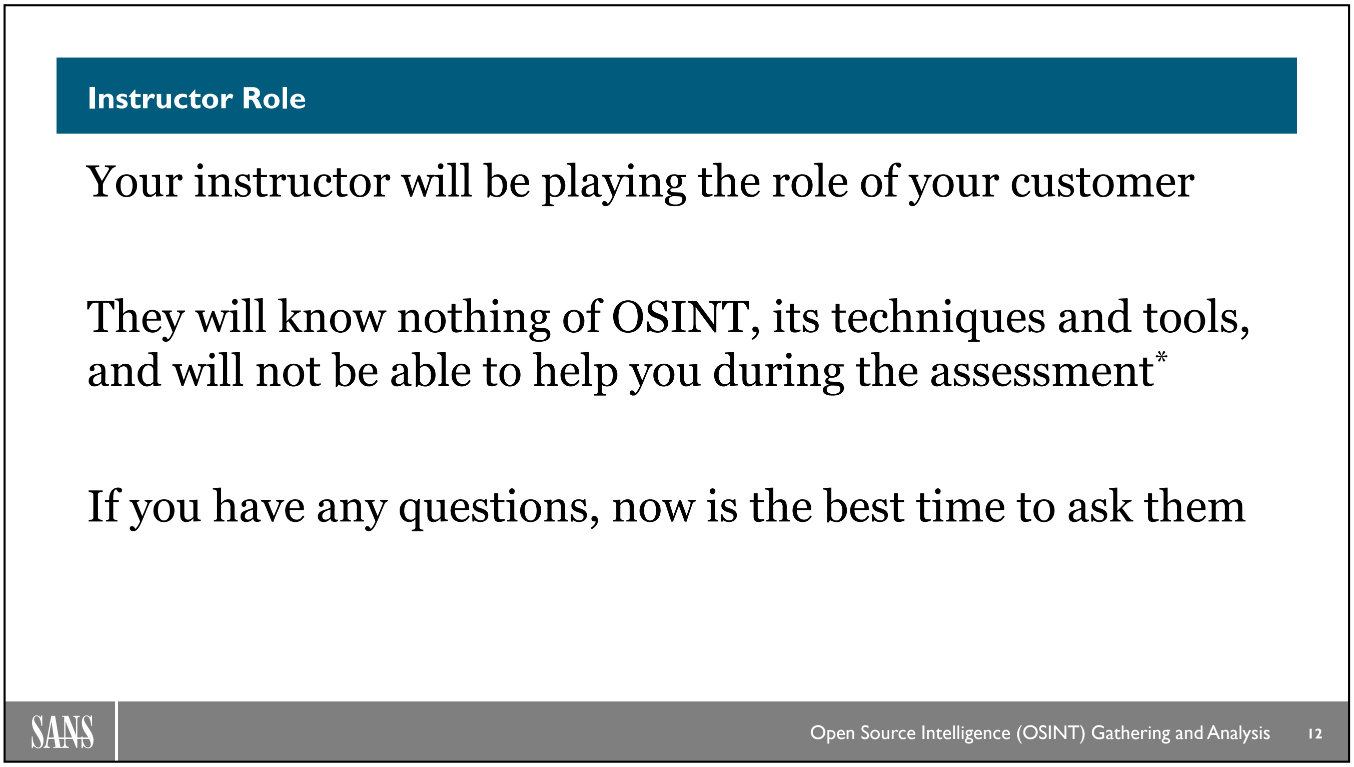
Presentations from 2 p.m. - ??? with voting directly after

No official breaks for snacks or lunch

Timing

After these rules, we will go over the scenario that each team will use in their OSINT assessment. As long as class began around 9 a.m., the capstone will complete at 2 p.m., with presentations after it. Once the presentations of the teams are finished, the class will vote for the best work.

Students may take breaks whenever they wish, but the capstone will not stop or pause (under normal circumstances) for lunch or breaks until it ends.



Instructor Role

Your instructor will be playing the role of your customer

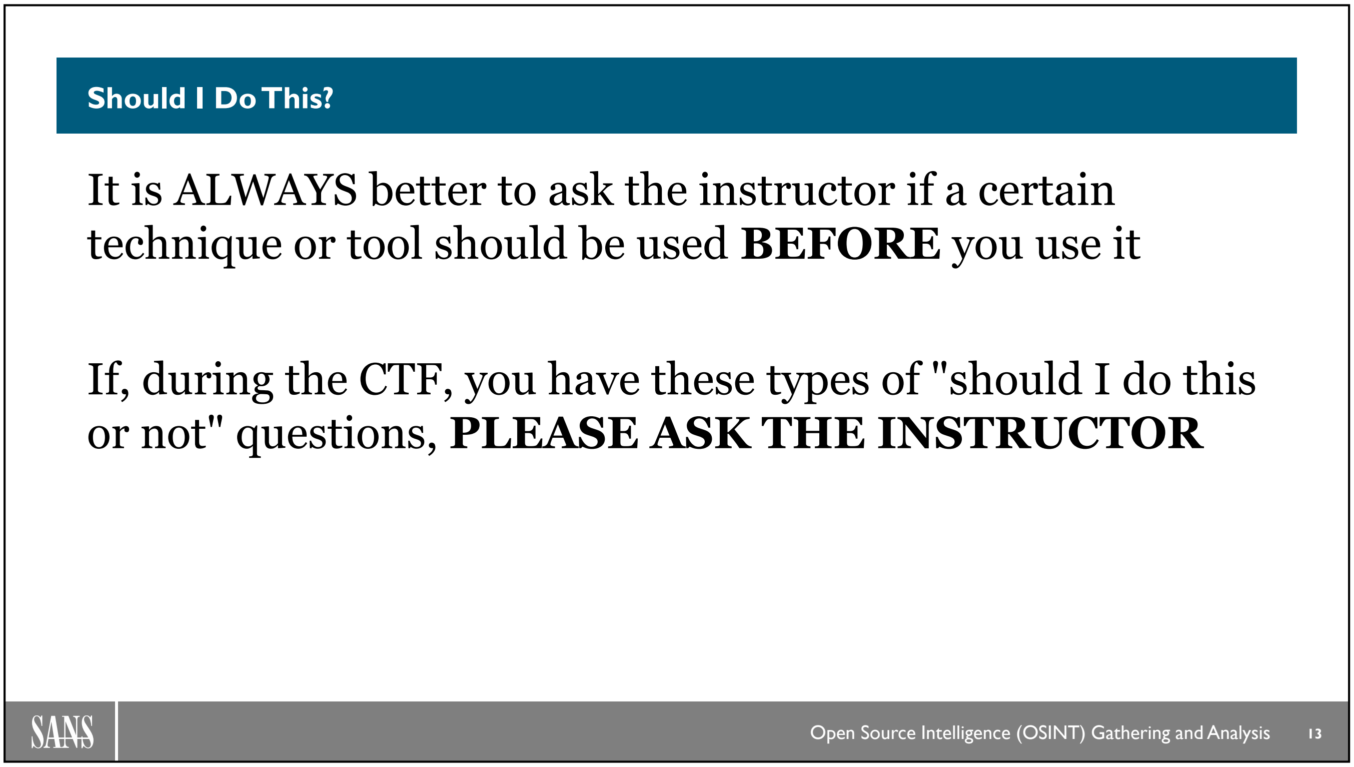
They will know nothing of OSINT, its techniques and tools, and will not be able to help you during the assessment*

If you have any questions, now is the best time to ask them

Instructor Role

After the scenario is read in the next module, the instructor will become your client. As your customer, the instructor will magically forget all knowledge of OSINT techniques, tips, tricks, and resources. This "capstone amnesia" is quite common and is temporary, lasting until about 2 p.m. or so.

* The exceptions to the "instructor will not help you" rule is if your system breaks, you experience network failures, your VPN IP gets blocked by key resources, and other similar phenomena. If these unexpected things happen, the instructor can, at their discretion, assist.



Should I Do This?

It is ALWAYS better to ask the instructor if a certain technique or tool should be used **BEFORE** you use it

If, during the CTF, you have these types of "should I do this or not" questions, **PLEASE ASK THE INSTRUCTOR**

Should I Do This?

Ask the instructor if you have questions about running a certain tool or using a technique during the CTF. They will guide you.

Last Chance

Have questions?

Ask them now!

SANS Open Source Intelligence (OSINT) Gathering and Analysis 14

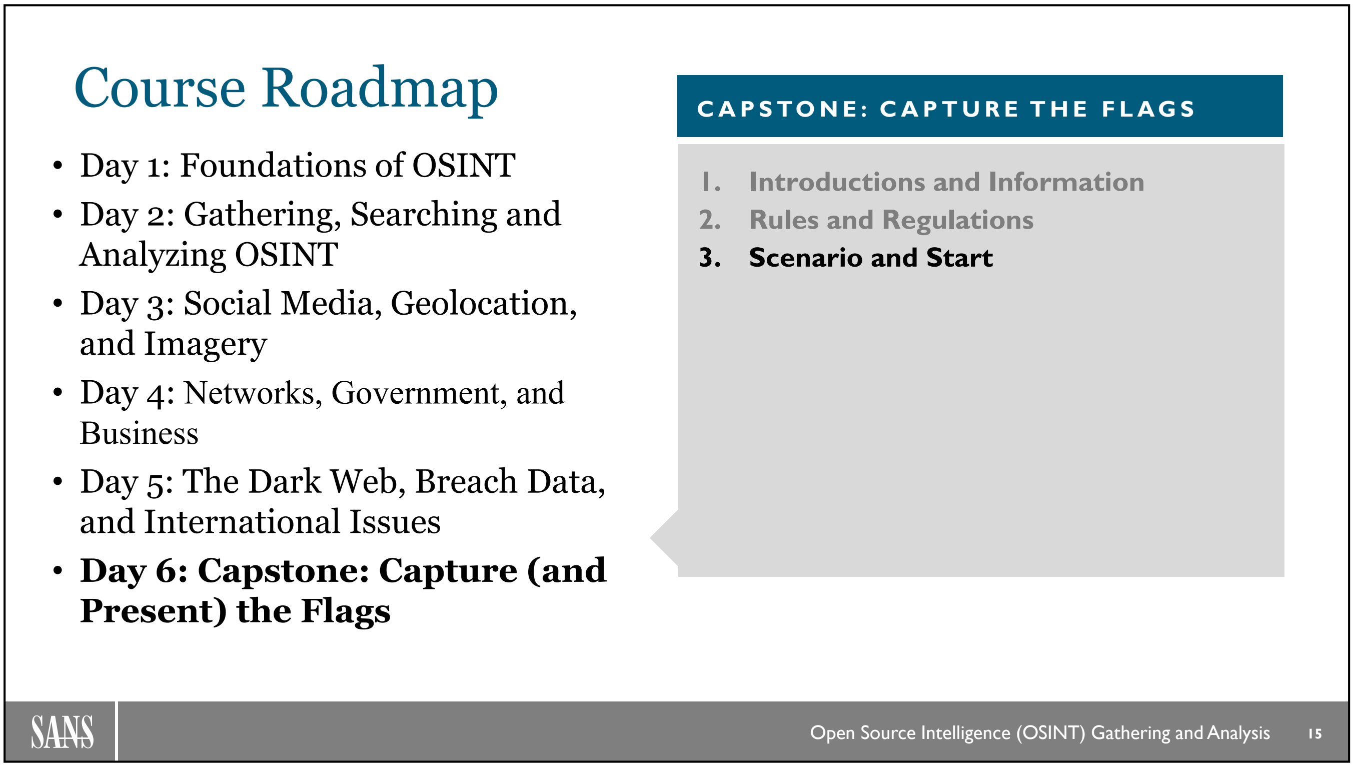
Last Chance

If you have questions, ask your instructor now.

Sample questions might be:

- Who are these women?
- Why are they in a field?
- Are those rotary-style phones in their hands?
- How can they use the phones? Those were not wireless.
- Why are they using phones to talk if they are that close to each other?

Image from https://sec487.info/pg, December 3, 2017.



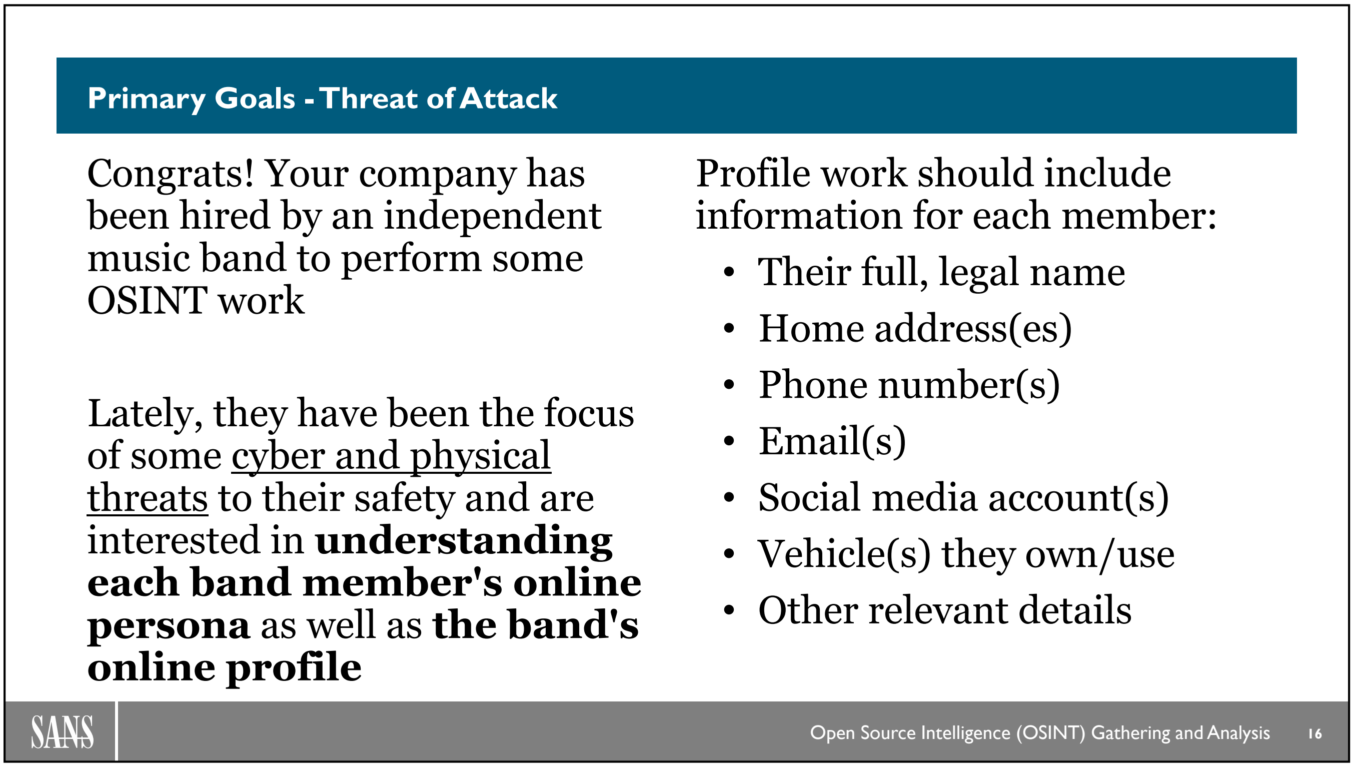
Course Roadmap

- Day 1: Foundations of OSINT
- Day 2: Gathering, Searching and Analyzing OSINT
- Day 3: Social Media, Geolocation, and Imagery
- Day 4: Networks, Government, and Business
- Day 5: The Dark Web, Breach Data, and International Issues
- **Day 6: Capstone: Capture (and Present) the Flags**

CAPSTONE: CAPTURE THE FLAGS

1. Introductions and Information
2. Rules and Regulations
3. **Scenario and Start**

This page intentionally left blank.



Primary Goals - Threat of Attack

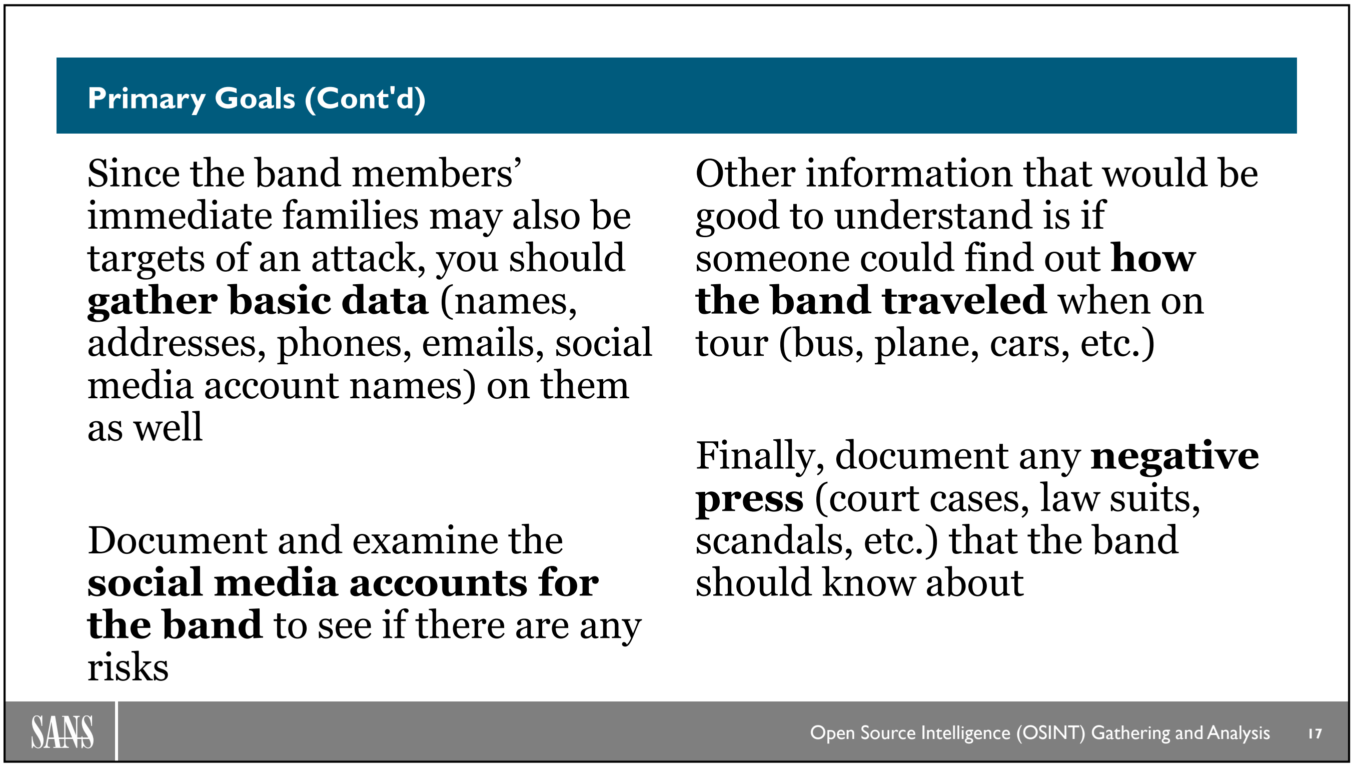
Congrats! Your company has been hired by an independent music band to perform some OSINT work

Lately, they have been the focus of some <u>cyber and physical threats</u> to their safety and are interested in **understanding each band member's online persona** as well as **the band's online profile**

Profile work should include information for each member:

- Their full, legal name
- Home address(es)
- Phone number(s)
- Email(s)
- Social media account(s)
- Vehicle(s) they own/use
- Other relevant details

This page intentionally left blank.



Primary Goals (Cont'd)

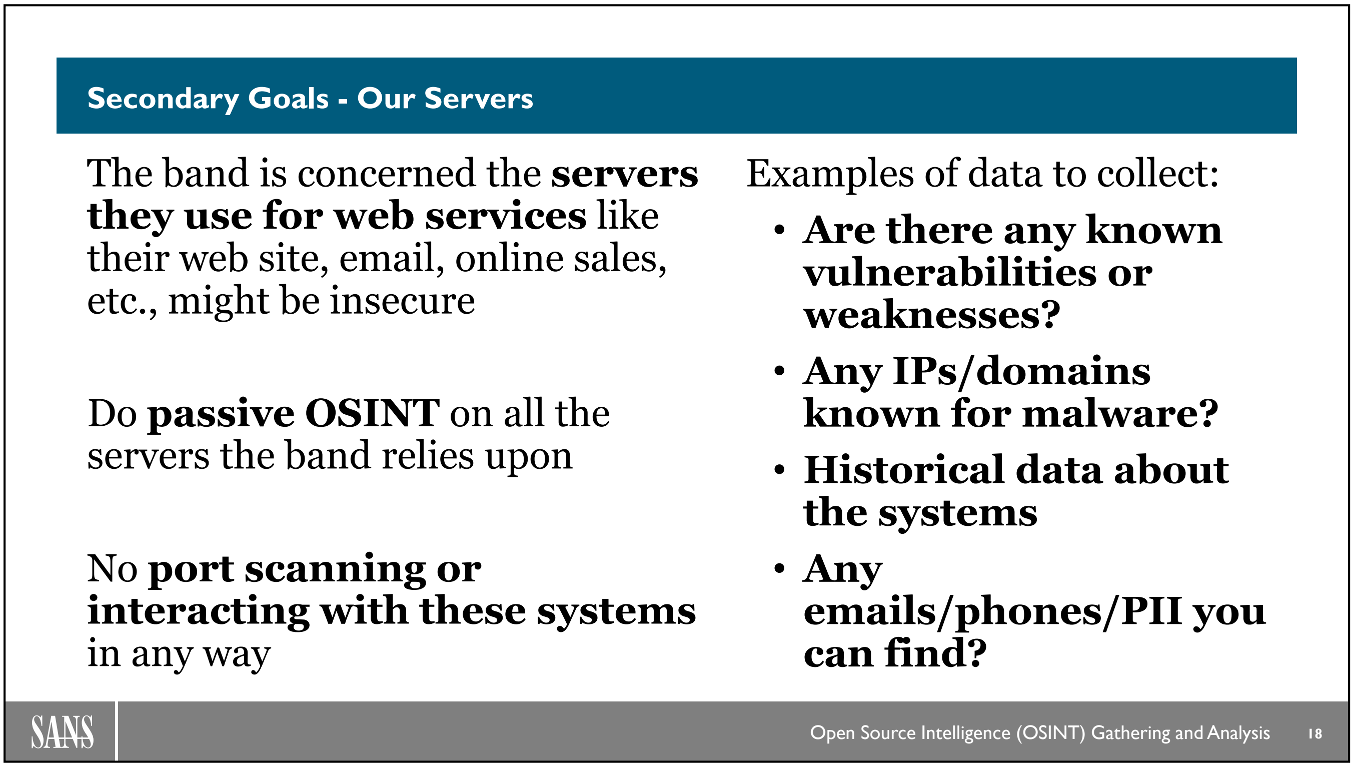
Since the band members' immediate families may also be targets of an attack, you should **gather basic data** (names, addresses, phones, emails, social media account names) on them as well

Document and examine the **social media accounts for the band** to see if there are any risks

Other information that would be good to understand is if someone could find out **how the band traveled** when on tour (bus, plane, cars, etc.)

Finally, document any **negative press** (court cases, law suits, scandals, etc.) that the band should know about

This page intentionally left blank.



Secondary Goals - Our Servers

The band is concerned the **servers they use for web services** like their web site, email, online sales, etc., might be insecure

Do **passive OSINT** on all the servers the band relies upon

No **port scanning or interacting with these systems** in any way

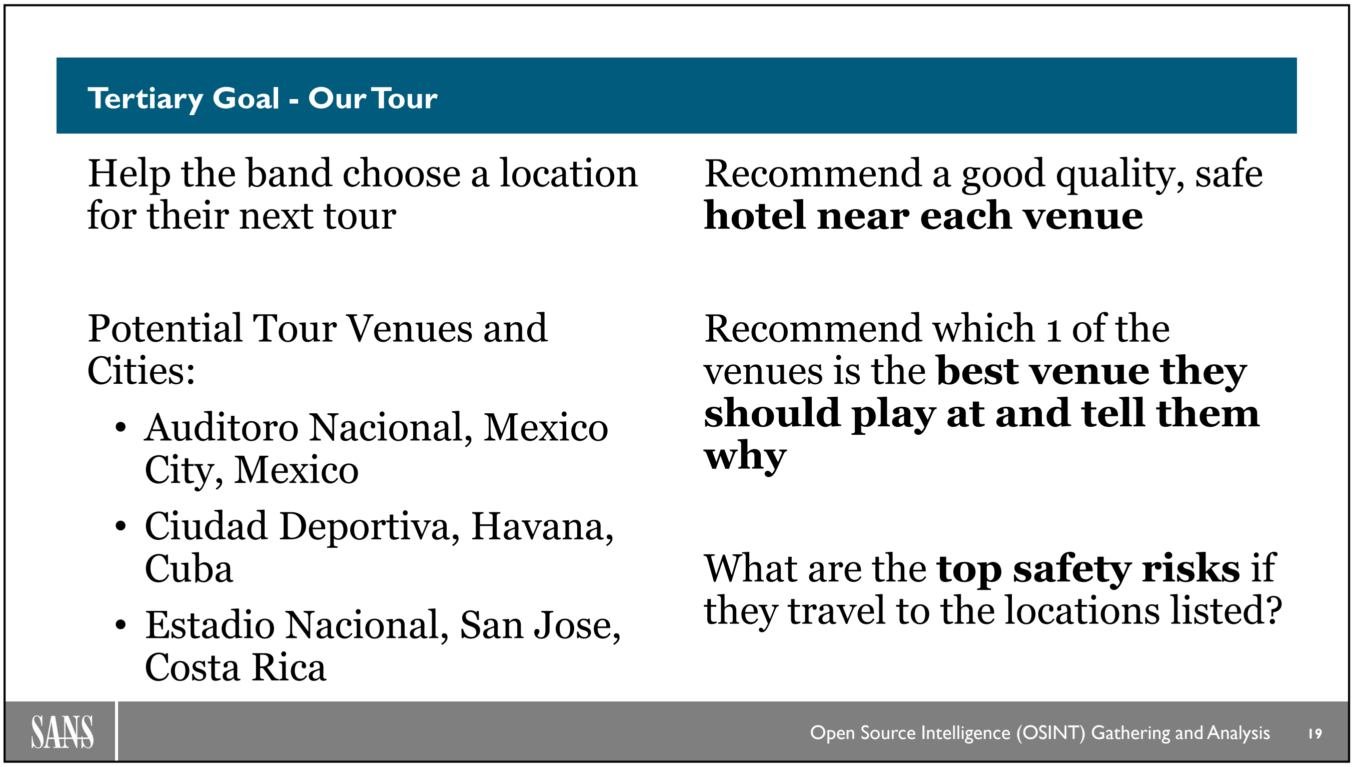
Examples of data to collect:

- **Are there any known vulnerabilities or weaknesses?**
- **Any IPs/domains known for malware?**
- **Historical data about the systems**
- **Any emails/phones/PII you can find?**

SANS

Open Source Intelligence (OSINT) Gathering and Analysis 18

This page intentionally left blank.



Tertiary Goal - Our Tour

Help the band choose a location for their next tour

Potential Tour Venues and Cities:

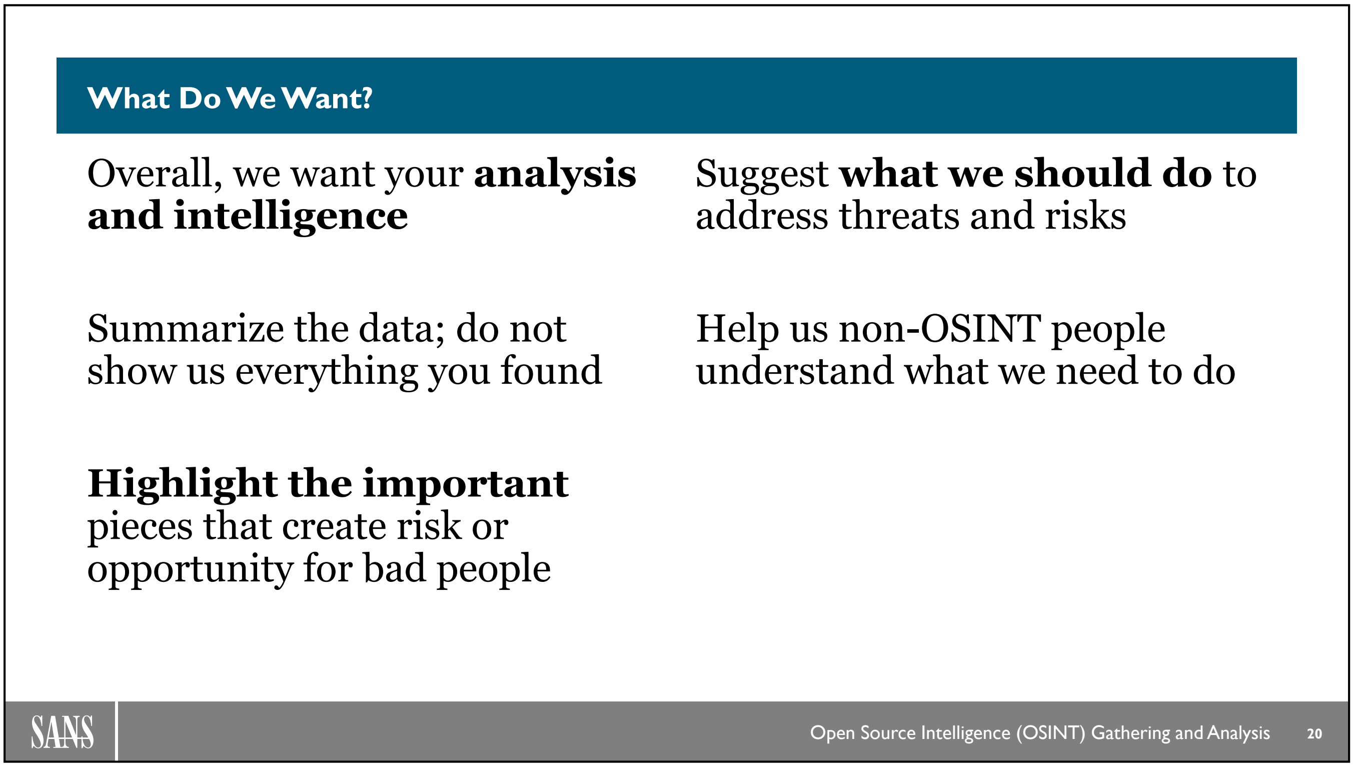
- Auditoro Nacional, Mexico City, Mexico
- Ciudad Deportiva, Havana, Cuba
- Estadio Nacional, San Jose, Costa Rica

Recommend a good quality, safe **hotel near each venue**

Recommend which 1 of the venues is the **best venue they should play at and tell them why**

What are the **top safety risks** if they travel to the locations listed?

This page intentionally left blank.



What Do We Want?

Overall, we want your **analysis and intelligence**

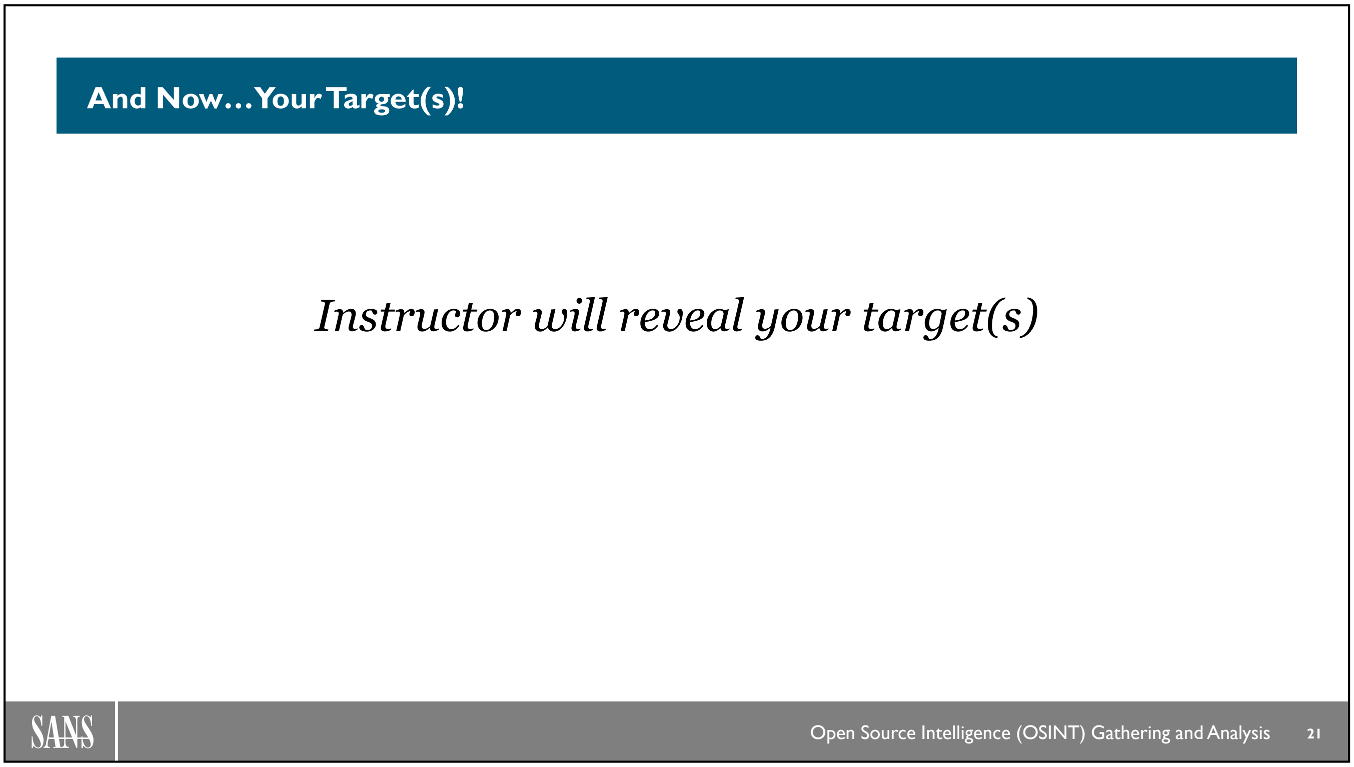
Summarize the data; do not show us everything you found

Highlight the important pieces that create risk or opportunity for bad people

Suggest **what we should do** to address threats and risks

Help us non-OSINT people understand what we need to do

This page intentionally left blank.



And Now…Your Target(s)!

Instructor will reveal your target(s)

This page intentionally left blank.

This page intentionally left blank.

Index