Indiana University of Pennsylvania's 2019

# GenCyber STUDENT CAMP

## June 24 - June 28, 2019

### CAMP DETAILS

- Cybersecurity Camp for Middle and High School Students
- Learn detailed information about cybersecurity
- Learn hacking defense techniques
- Acquire skills to land your dream job
- Do any of these topics interest you? Apply today!
  www.iup.edu/iupgencyber

### ADVANTAGES*

- Offered at no cost!
- Droid Inventor Kit for each participant!
- FREE lunch and afternoon snack!
- Instruction and mentorship from IUP faculty and other experts!
- Skills and knowledge for a growing career field!
- Apply NOW space is limited!

**Through this opportunity, you will learn safe online behavior, increase knowledge of cyberspace, and explore cybersecurity careers.**

**QUESTIONS?**
e-mail:
gen-cyber@iup.edu

**LOCATION**
IUP
Main Campus

**PROJECT PI**
Dr. Waleed Farag, Director,
IUP Institute for Cybersecurity

THIS PROGRAM IS PROUDLY SPONSORED BY:

*program is contingent on funding released by NSA

# PARTICIPATION ADVANTAGES

Offered at no cost!

Droid Inventor Kit for each participant!

FREE lunch and afternoon snack!

Instruction and mentorship from IUP faculty and other experts!

Skills and knowledge for a growing career field!

# HOW TO APPLY

Applications are accepted online only. To apply or view other important program information, please visit:

www.iup.edu/iupgencyber

# CAMP DATES

JUNE 24 - 28, 2019

# PROGRAM DIRECTORS

**Dr. Waleed Farag**
Director, Institute for Cybersecurity

**Dr. Soundararajan Ezekiel**
Professor, Computer Science

# PROUDLY SPONSORED BY:

GenCyber NSF National Security Agency IUP

# Summer 2019 GENCYBER Student Camp

# Presented by: IUP & NSA

# IUP GENCYBER

## SUMMER 2019 PROGRAM

**GenCyber is a national initiative that is supported by the National Science Foundation and the National Security Agency. This program has the following objectives:**

- Increase interest in cybersecurity careers and diversity in the cybersecurity workforce of the nation.
- Help all students understand correct and safe online behavior.
- Improve teaching methods for delivering cybersecurity content for K-12 curricula.

# THE FUNDED GRANT

Under the leadership of Dr. Waleed Farag, grant PI, IUP, along with a selected group of national universities, has again been awarded funding for four years in a row to run the GenCyber program in summer 2019.

This year, the camp is open to middle and high school students. The prospective camp will address essential security concepts in an interesting, novel approach to foster interest in cybersecurity among middle and high school students in western Pennsylvania.

# PROGRAM SUMMARY

This project will host one free (no cost to participants), five-weekday day camp in summer 2019. Instruction will be delivered by a team of professors with numerous backgrounds but established expertise in cybersecurity teaching and research.

The student camp will provide a uniformly distributed, engaging blend of delivery that includes direct instruction, group activities, structured discovery, and hands-on, laboratory, and informal instructional techniques to both individual and combined cohorts. Upon completion of the camp, participants will have a strong understanding of cybersecurity in addition to mastering basic skills that help them be safer online.

# DAILY CAMP SCHEDULE — DAY 1 - JUNE 24, 2019

| | MIDDLE SCHOOL | HIGH SCHOOL |
|---|---|---|
| 9:00 a.m. to 9:50 a.m. | IUP President, Dr. Driscoll Remarks<br>Welcome, Introduction to Team members, Orientation, Logistics<br>Dr. Farag - HSS 126 | |
| 9:50 a.m. to 10:00 a.m. | BREAK | |
| 10:00 a.m. to 10:50 a.m. | Cybersecurity Concepts<br>Dr. Farag - HSS 126 | |
| 10:50 a.m. to 11:00 a.m. | BREAK | |
| 11:00 a.m. to 11:50 a.m. | Session 1.1: Talk the Talk - Cybersecurity Concepts<br>Mrs. Gentile - 112A Stright Hall | Session 1.1: Internet of Things (IoT) Security/Monitoring<br>Dr. Ezekiel - 107A Stright Hall |
| 11:50 a.m. to 1:00 p.m. | LUNCH - 112B Stright Hall | |
| 1:00 p.m. to 1:50 p.m. | Session 1.2: Talk the Talk - Cybersecurity Concepts<br>Mrs. Gentile - 112A Stright Hall | Session 1.2: Internet of Things (IoT) Security/Monitoring<br>Dr. Ezekiel - 107A Stright Hall |
| 1:50 p.m. to 2:00 p.m. | BREAK | |
| 2:00 p.m. to 2:50 p.m. | Session 2.1: Finding Hidden Treasure (Programming with Alice) I<br>Mrs. Lint - 112A Stright Hall | Session 2.1: Cybersecurity Concepts<br>Mrs. Gentile - 107A Stright Hall |
| 2:50 p.m. to 3:10 p.m. | SNACK BREAK - 112B Stright Hall | |
| 3:10 p.m. to 4:00 p.m. | Session 2.2: Finding Hidden Treasure (Programming with Alice) I<br>Mrs. Lint - 112A Stright Hall | Session 2.2: Cybersecurity Concepts<br>Mrs. Gentile - 107A Stright Hall |

# DAILY CAMP SCHEDULE — DAY 2 - JUNE 25, 2019

| | MIDDLE SCHOOL | HIGH SCHOOL |
|---|---|---|
| 9:00 a.m. to 9:50 a.m. | Session 1.1: Personal Cybersecurity Practices<br>Mrs. Gentile - 112A Stright Hall | Session 1.1: Fundamentals of Information Security<br>Dr. Farag - 107A Stright Hall |
| 9:50 a.m. to 10:00 a.m. | BREAK | |
| 10:00 a.m. to 10:50 a.m. | Session 1.2: Personal Cybersecurity Practices<br>Mrs. Gentile - 112A Stright Hall | Session 1.2: Fundamentals of Information Security<br>Dr. Farag - 107A Stright Hall |
| 10:50 a.m. to 11:00 a.m. | BREAK | |
| 11:00 a.m. to 11:50 a.m. | Session 2.1: Unplugged Programming Activity<br>Mrs. Lint - 112A Stright Hall | Session 2.1: Digital Forensics Investigation<br>Dr. Ezekiel - 107A Stright Hall |
| 11:50 a.m. to 1:00 p.m. | WORKING LUNCH - Guest Speaker Mr. Brian Gouker, Division Chief, NSA College of Cyber - 112 A/B Stright Hall | |
| 1:00 p.m. to 1:50 p.m. | Session 2.2: Unplugged Programming Activity<br>Mrs. Lint - 112A Stright Hall | Session 2.2: Digital Forensics Investigation<br>Dr. Ezekiel - 107A Stright Hall |
| 1:50 p.m. to 2:00 p.m. | BREAK | |
| 2:00 p.m. to 2:50 p.m. | Session 3.1: Robots Programming (Droid Inventor Kit)<br>Dr. Farag - 327/329 Stright Hall | Session 3.1: Alice Programming Challenge<br>Mrs. Lint - 112A Stright Hall |
| 2:50 p.m. to 3:10 p.m. | SNACK BREAK - 112B Stright Hall | |
| 3:10 p.m. to 4:00 p.m. | Session 3.2: Robots Programming (Droid Inventor Kit)<br>Dr. Farag - 327/329 Stright Hall | Session 3.2: Alice Programming Challenge<br>Mrs. Lint - 112A Stright Hall |

# DAILY CAMP SCHEDULE — DAY 3 - JUNE 26, 2019

| | MIDDLE SCHOOL | HIGH SCHOOL |
|---|---|---|
| 9:00 a.m. to 9:50 a.m. | Session 1.1: Internet of Things (IoT) Security/Monitoring<br>Dr. Ezekiel - 107A Stright hall | Session 1.1: Airport Security Implementation<br>Dr. Ghani - Str 327/329 Stright Hall |
| 9:50 a.m. to 10:00 a.m. | BREAK | |
| 10:00 a.m. to 10:50 a.m. | Session 1.2: Internet of Things (IoT) Security/Monitoring<br>Dr. Ezekiel - 107A Stright hall | Session 1.2: Airport Security Implementation<br>Dr. Ghani - Str 327/329 Stright Hall |
| 10:50 a.m. to 11:00 a.m. | BREAK | |
| 11:00 a.m. to 11:50 a.m. | Session 2.1: Finding Hidden Treasure (Programming with Alice) II<br>Mrs. Lint - 112A Stright Hall | Session 2.1: Robots Programming (Droid Inventor Kit)<br>Dr. Farag - HSS 126 |
| 11:50 a.m. to 1:00 p.m. | WORKING LUNCH - IUP Provost Remarks followed by<br>Guest Speaker Mr. Tommy Chin, Security Researcher - 126 HSS | |
| 1:00 p.m. to 1:50 p.m. | Session 2.2: Finding Hidden Treasure (Programming with Alice) II<br>Mrs. Lint - 112A Stright Hall | Session 2.2: Robots Programming (Droid Inventor Kit)<br>Dr. Farag - HSS 126 |
| 1:50 p.m. to 2:00 p.m. | BREAK | |
| 2:00 p.m. to 2:50 p.m. | Session 3.1: Computational Thinking = Beautiful Minds + Powerful Machines<br>Mrs. Gentile - 112A Stright Hall | Session 3.1: Network Threats and Countermeasures<br>Dr. Wu - 107A Stright Hall |
| 2:50 p.m. to 3:10 p.m. | SNACK BREAK - 112B Stright Hall | |
| 3:10 p.m. to 4:00 p.m. | Session 3.2: Computational Thinking = Beautiful Minds + Powerful Machines<br>Mrs. Gentile - 112A Stright Hall | Session 3.2: Network Threats and Countermeasures<br>Dr. Wu - 107A Stright Hall |

# DAILY CAMP SCHEDULE — DAY 4 - JUNE 27, 2019

| | MIDDLE SCHOOL | HIGH SCHOOL |
|---|---|---|
| 9:00 a.m. to 9:50 a.m. | Session 1.1: How to Secure Networks - Examples and Demos<br>Dr. Wu - 107A Stright Hall | Session 1.1: Data Protection / Cryptography<br>Dr. Ali - 112A Stright Hall |
| 9:50 a.m. to 10:00 a.m. | BREAK | |
| 10:00 a.m. to 10:50 a.m. | Session 1.2: How to Secure Networks - Examples and Demos<br>Dr. Wu - 107A Stright Hall | Session 1.2: Data Protection / Cryptography<br>Dr. Ali - 112A Stright Hall |
| 10:50 a.m. to 11:00 a.m. | BREAK | |
| 11:00 a.m. to 11:50 a.m. | Session 2.1: Data Protection / Cryptography<br>Dr. Ali - 107A Stright Hall | Session 2.1: Can Students Help When the Grid Fails?<br>Dr. Jesson - 112A Stright Hall |
| 11:50 a.m. to 1:00 p.m. | LUNCH - Folger Hall | |
| 1:00 p.m. to 1:50 p.m. | Session 2.2: Data Protection / Cryptography<br>Dr. Ali - 107A Stright Hall | Session 2.2: Can Students Help When the Grid Fails?<br>Dr. Jesson - 112A Stright Hall |
| 1:50 p.m. to 2:00 p.m. | BREAK | |
| 2:00 p.m. to 2:50 p.m. | Session 3.1: Can Students Help When the Grid Fails?<br>Dr. Jesson - 112A Stright Hall | Session 3.1: Threat Modelling<br>Dr. Ghani – 107A Stright Hall |
| 2:50 p.m. to 3:10 p.m. | SNACK BREAK - 112B Stright Hall | |
| 3:10 p.m. to 4:00 p.m. | Session 3.2: Can Students Help When the Grid Fails?<br>Dr. Jesson - 112A Stright Hall | Session 3.2: Threat Modelling<br>Dr. Ghani – 107A Stright Hall |

# DAILY CAMP SCHEDULE — DAY 5 - JUNE 28, 2019

| | MIDDLE SCHOOL | HIGH SCHOOL |
|---|---|---|
| 9:00 a.m. to 9:50 a.m. | Session 1.1: Cyber Knowledge Fair<br>Mrs. Gentile/ Mrs. Lint - 112A/B Stright Hall | |
| 9:50 a.m. to 10:00 a.m. | BREAK | |
| 10:00 a.m. to 10:50 a.m. | Session 1.2: Cyber Knowledge Fair<br>Mrs. Gentile/ Mrs. Lint - 112A/B Stright Hall | |
| 10:50 a.m. to 11:00 a.m. | BREAK | |
| 11:00 a.m. to 11:50 a.m. | Session 2.1: End of Camp Competition<br>GenCyber Team - Outdoor/Stright Hall | |
| 11:50 a.m. to 1:00 p.m. | LUNCH - Folger Hall | |
| 1:00 p.m. to 1:50 p.m. | Session 2.2: End of Camp Competition<br>GenCyber Team - Outdoor/Stright Hall | |
| 1:50 p.m. to 2:00 p.m. | BREAK | |
| 2:00 p.m. to 2:50 p.m. | Session 3.1: End of Camp Competition/End of Camp Surveys<br>112 A/B Stright Hall | |
| 2:50 p.m. to 3:10 p.m. | SNACK BREAK - 112B Stright Hall | |
| 3:10 p.m. to 4:00 p.m. | Session 3.2: Certificate Award Ceremony<br>112 A/B Stright Hall | |

# Lesson Plan*

**LESSON TITLE:** Alice Programming Challenge

**SUMMARY:**

This activity will challenge the students to design and develop an Alice world from a given Scene set up. Students will be asked to incorporate a way to keep away from being seen by the incoming attackers.

**GRADE BAND:**

- ☐ K-2
- ☐ 3-5
- ☐ 6-8
- ☑ High School

**TIME REQUIRED:** 100 minutes

**LESSON LEARNING OUTCOMES: Upon completion of this lesson, students will be able to:**

**Outcome Examples**

| | |
|---|---|
| Design/Build<br>Test/Defend<br>Compare/Contrast<br>Apply/Use<br>Explain/Discuss<br>Identify/Describe | Students will be able to Apply/Use the Alice programming platform to complete the activity.<br>Students will Design/Build an Alice world that keeps an object away from an intruder thereby using the Cybersecurity concept of Think Like an Adversary when incorporating the events. |

**Materials List (i.e., string, digital diary, raspberry pi, web link, drone):**

Scene set up handouts (teacher provided)

**Describe any Previous Knowledge that may be Required:**

Previous knowledge of basic programming concepts such as methods, conditionals, looping, and sequencing is beneficial but not necessary.

**How will you facilitate the learning?**

- Describe the Warm-up Activity:

Introductory slides through which the instructor will introduce the Alice platform and all of its components so that the students can complete their activity. While the students work the instructor will facilitate with any necessary information about Alice so that the students can accomplish their task.

- Describe the Focused Activity:

Students are given a preset Scene and encouraged to add objects (characters) to the scene and to keep the main character from being found by any other characters that are trying to locate the main character.

Students need to think about all of the possible ways they could be found by an intruder to be able to design the event to keep them hidden.

- Describe the Teacher Instruction:

N/A

**Mapping to GenCyber Cybersecurity First Principles:**

| | | | |
|---|---|---|---|
| ☐ | Domain Separation | ☐ | Abstraction |
| ☐ | Process Isolation | ☐ | Data Hiding |
| ☐ | Resource Encapsulation | ☐ | Layering |
| ☐ | Modularity | ☐ | Simplicity |
| ☐ | Least Privilege | ☐ | Minimization |

**Mapping to GenCyber Cybersecurity Concepts:**

| | | | |
|---|---|---|---|
| ☐ | Defense in Depth | ☐ | Availability |
| ☐ | Confidentiality | ☑ | Think Like an Adversary |
| ☐ | Integrity | ☑ | Keep It Simple |

**Assessment of Learning:**

| TYPE (Examples listed below) | NAME/DESCRIPTION |
|---|---|
| Quiz/Test<br>Presentation<br>Project<br>Writing Assignment<br>Observation<br>Walk Around<br>Oral Questioning<br>Other | Observation<br>Presentation<br>Walk Around |

**Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)**

This is a visual exercise. Students who need accommodations will receive assistance as needed.

**Describe any Extension Activities (i.e., ideas for further work):**

Students can continue to work on this activity outside of camp if interested.

**Acknowledgements:**

The Alice programming platform is a product of Carnegie Mellon University.
All information regarding Alice can be found on alice.org.

# Lesson Plan*

**LESSON TITLE:** Cyber Knowledge Fair - Mrs. Lint and Mrs. Gentile - Friday, June 28, 2019

**SUMMARY:**

Students will prepare a 5-minute presentation to explain technology concepts gained during the week in all of the camp's various topics, and will explain how to incorporate the six GenCyber cybersecurity concepts into their respective topics to other camp participants.

**GRADE BAND:**

- ☐ K-2
- ☐ 3-5
- ☑ 6-8
- ☑ High School

**TIME REQUIRED:**

100 minutes

**LESSON LEARNING OUTCOMES: Upon completion of this lesson, students will be able to:**

**Outcome Examples**

| | |
|---|---|
| Design/Build<br>Test/Defend<br>Compare/Contrast<br>Apply/Use<br>Explain/Discuss<br>Identify/Describe | design brief, clear presentations about cybersecurity topics,<br><br>describe technological concepts and devices explored during the week in their presentations,<br><br>apply the six Cyber Security Concepts to technology topics from the week. |

**Materials List (i.e., string, digital diary, raspberry pi, web link, drone):**

Computers
Poster board
dice
spinners
timers
Legos or other building blocks
Robots

**Describe any Previous Knowledge that may be Required:**

Middleschoolers will have been exposed to the GenCyber cybersecurity concepts, Alice programming, the Internet of Things, cryptography, computational thinking, droids, secure networks, grid failure.

Highschoolers will have been exposed to the topics above in addition to threat modeling, digital forensics, threats and countermeasures, information security, airport security.

**How will you facilitate the learning?**

- Describe the Warm-up Activity:

9:00 - 9:05
Remind students that on this final day of camp, they will have to prove their learning in two ways - through a culminating activity and a post-test. This activity is meant for them to test their understanding in a fun way.
Divide middle and high school students, then place each level into groups of three.
Ask all groups to select a topic from the week's 8-9 topics out of a middle school hat or highschool hat.

Students with the same topics will gather together to brainstorm how best to teach that topic to others. They will be informed that they will present their topics 4 times as we all rotate through the fair.

- Describe the Focused Activity:

9:05 - 9:50
Students will be given the following set of expectations to guide development of their 5-minute presentation for the fair. They must do the following:
1. Introduce general uses of the topic through demonstration, model, physical game or on-line game
2. Demonstrate the most interesting aspects of the topic!
3. **Discuss which cybersecurity concept(s) is/are addressed in the topic**
4. Prepare to ask for and answer questions from audience

10:00 – 10:05
Allow the high school students time to finalize their set-ups of their stations.
Meanwhile, encourage middle schoolers to get into groups of three. Have them use their guided notes of the six cybersecurity concepts to use in reference as they circulate.

10:05 - 10:25
Students will rotate through each other's stations (first the middleschoolers will visit the highschoolers' stations, then vice versa)
1. Watch the demo or participate in the game
2. **Discuss which cybersecurity concept(s) is/are addressed in the topic**
3. Ask questions to improve your understanding of the topic

10:30 – 10:50
Students will switch roles with highschoolers traveling to at least 4 middleschoolers' stations

- Describe the Teacher Instruction:

After students have been well-organized into presentation groups, instructors will monitor the progress of their communication and collaboration.

Instructors will hand out written expectations for each group or post expectations on a screen if available.

Instructors will help to guide each group to focus on the requirements of their presentations and to clarify any application of the cybersecurity concepts they are using.

Instructors will monitor the time closely so that all have equal opportunity to present and participate.

Conclude with the expectation that the knowledge gained from the week will enable them to perform well in the camp's culminating activity as well as the camp post-test, given later that day.

**Mapping to GenCyber Cybersecurity First Principles:**

| | | | |
|---|---|---|---|
| ☐ | **Domain Separation** | ☐ | **Abstraction** |
| ☐ | **Process Isolation** | ☐ | **Data Hiding** |
| ☐ | **Resource Encapsulation** | ☐ | **Layering** |
| ☐ | **Modularity** | ☐ | **Simplicity** |
| ☐ | **Least Privilege** | ☐ | **Minimization** |

**Mapping to GenCyber Cybersecurity Concepts:**

| | | | |
|---|---|---|---|
| ☑ | **Defense in Depth** | ☑ | **Availability** |
| ☑ | **Confidentiality** | ☑ | **Think Like an Adversary** |
| ☑ | **Integrity** | ☑ | **Keep It Simple** |

**Assessment of Learning:**

| **TYPE (Examples listed below)** | **NAME/DESCRIPTION** |
|---|---|
| Quiz/Test<br>Presentation<br>Project<br>Writing Assignment<br>Observation<br>Walk Around<br>Oral Questioning<br>Other | Observation: As students share, demonstrate and collaborate ideas communicated<br><br>Physical model, game: As students play, demonstrate and build or demonstration<br><br>Strength of questioning: As teachers/students ask for clarification on the GenCyber cybersecurity concepts<br><br>Participation: As observers ask questions of each presentation |

**Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)**

Assistance may be needed for groups without a strong leader, which instructors and student assistants can provide.

**Describe any Extension Activities (i.e., ideas for further work):**

Students in this Gen-Cyber Cybersecurity Camp are expected to share knowledge and skills gained this week at their junior or senior highschools, and hopefully to maintain an interest in Cybersecurity- related careers.

**Acknowledgements:**

www.Gen-Cyber.com

# Lesson Plan*

**LESSON TITLE:** Digital Forensics

**SUMMARY:**

This lab will show how evidence is collected and verified with FTK Imager. We will collect evidence from USB Drives and create an Image of the drive and verify its collection. We then take that collected image and analyze it with Autopsy forensics to examine it's contents. After collecting and analyzing evidence, we will then examine the tools available in CAINE forensic workstation. The students will give a brief report about 3 tools they find in CAINE. Along with their findings in CAINE the students will discuss the evidence they collected and interesting things they learned about digital forensics.

**GRADE BAND:**

- ☐ K-2
- ☐ 6-8
- ☐ 3-5
- ☑ High School

**TIME REQUIRED:** 120 minutes

**LESSON LEARNING OUTCOMES: Upon completion of this lesson, students will be able to:**

| Outcome Examples | |
|---|---|
| Design/Build<br>Test/Defend<br>Compare/Contrast<br>Apply/Use<br>Explain/Discuss<br>Identify/Describe | Students will be able to create and use virtual machines to explore different operating systems as well as understand the benefits of using one. They will be able to collect and verify evidence using FTK Imager. They will also be able to take the evidence they collected and analyze it with Autopsy forensics. Students will also learn the basics about using a Linux based distribution. |

**Materials List (i.e., string, digital diary, raspberry pi, web link, drone):**

USB Drives
Computers
VM Ware
A Windows and CAINE Virtual Machine
FTK Imager
Autopsy forensics

**Describe any Previous Knowledge that may be Required:**

Basic knowledge of the criminal justice system.
Knowledge of using Windows.
How to use a USB Drive.

**How will you facilitate the learning?**

- Describe the Warm-up Activity:

The warm up will be a group discussion to understand what digital forensics is, it's importance in our society, and who uses it. We will also discuss what write blockers and virtual machines are, and the benefits of using them. The final part of the Warm-Up will be an introduction of the activities, the selection of "Forensic Teams", and the expectations of what they will be able to do at the completion of the labs.

- Describe the Focused Activity:

After the introductions, the teams will load a Virtual Machine of Windows 10 and use FTK Imager to collect and verify evidence from a USB Drive. Students will then take the collected evidence and analyze it in Autopsy forensics. The students will be able to see the differences between FTK Imager and Autopsy and identify the strengths and weaknesses of each software. Upon the completion of these activities, the students will take a "iso" and use it to create a virtual machine in VM Ware. After the creation of the virtual machine, the students will then load the virtual machine and explore a Ubuntu based distribution designed specifically for Digital Forensics. The students will then use the Internet to learn about the different tools available inside CAINE and write a basic report describing what some of these tools do, and how they can be used. In this report they will also discuss the things they learned and anything they found interesting in their evidence collection and analysis.

- Describe the Teacher Instruction:

Teachers will first introduce the topics discussed throughout the lab and give the students the fundamentals of Digital Forensics. After the start of the lab, the teachers will keep the students on track and assist in anything the students may be struggling with during the lab. The teachers role is to assist the students learning in any way the can, without directly completing the lab for them. The teachers will be available to help the students in any way they can.

**Mapping to GenCyber Cybersecurity First Principles:**

| | | | |
|---|---|---|---|
| ☐ | Domain Separation | ☐ | Abstraction |
| ☐ | Process Isolation | ☐ | Data Hiding |
| ☐ | Resource Encapsulation | ☐ | Layering |
| ☐ | Modularity | ☐ | Simplicity |
| ☐ | Least Privilege | ☐ | Minimization |

**Mapping to GenCyber Cybersecurity Concepts:**

| | | | |
|---|---|---|---|
| ☑ | Defense in Depth | ☐ | Availability |
| ☑ | Confidentiality | ☑ | Think Like an Adversary |
| ☑ | Integrity | ☐ | Keep It Simple |

**Assessment of Learning:**

| TYPE (Examples listed below) | NAME/DESCRIPTION |
|---|---|
| Quiz/Test<br>Presentation<br>Project<br>Writing Assignment<br>Observation<br>Walk Around<br>Oral Questioning<br>Other | At the end of the lab, the students will discuss interesting things they found during their evidence collection and analysis. They will also report about different tools they examined in CAINE, and their functions. At the end of the lab a Kahoot will be used to assess how much information the students were able to retain during the lab activities. |

**Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)**

Accommodations will be made on a case by case basis. Any students will disabilities will be be given accommodations based on the disability present in that particular student.

**Describe any Extension Activities (i.e., ideas for further work):**

All of the software used is free to download and use by anyone allowing for a number of different activities for the students to complete. A list of resources will be available for every student to use after the camp is over. These resources include links to all of the software used, other digital forensics activities that are free and easy to use, and a variety of different evidence files that are free to use.

**Acknowledgements:**

# Lesson Plan*

**LESSON TITLE:** Robots Programming (Droid Inventor Kit)

**SUMMARY:**

This module introduces robot functions, operation, and potential for cybersecurity risks. The module starts with a brief history of robots and discussion of current and potential functions, as well as security weaknesses. The module then focuses on hands-on learning and experience, utilizing the "Little Bits Droid Inventor Kit." Students will learn how to build a simple circuit, manually operate the kit, as well as operate the kit through programming.

**GRADE BAND:**

- ☐ K-2
- ☐ 3-5
- ☑ 6-8
- ☑ High School

**TIME REQUIRED:** 120 minutes

**LESSON LEARNING OUTCOMES: Upon completion of this lesson, students will be able to:**

**Outcome Examples**

| | |
|---|---|
| Design/Build<br>Test/Defend<br>Compare/Contrast<br>Apply/Use<br>Explain/Discuss<br>Identify/Describe | Design/Build: Build a simple electronic circuit that controls the Droid Inventor Kit, as well as an obstacle course representing a cybersecurity system.<br>Compare/Contrast: Different methods of securing a system that is located within a small movable object.<br>Apply/Use: Apply new programming knowledge to operate Droid Inventor Kit. |

**Materials List (i.e., string, digital diary, raspberry pi, web link, drone):**

Droid Inventor Kits
Obstacle Course Components
Droid Inventor Kit App
Smart Device

**Describe any Previous Knowledge that may be Required:**

Basic team work and problem solving skills

**How will you facilitate the learning?**

- Describe the Warm-up Activity:

The module will begin with an interactive discussion on student opinions regarding robots, their use, and security weaknesses. This discussion will reinforce the cybersecurity concepts, and encourage the students to think differently about robots and their functions.

- Describe the Focused Activity:

-Discussion of robot use and the potential cyersecurity risks.
-Students will build their Droid Inventor Kit while learning about simple circuits.
-Students will design and construct an obstacle course that represents a cybersecurity defense system, and will compete against each other to navigate each obstacle course.
-Kahoot quizzes will be utilized to ensure knowledge retention.
-The varying degrees of difficulty in the obstacle course will allow for customization based on skill level.

- Describe the Teacher Instruction:

N/A

**Mapping to GenCyber Cybersecurity First Principles:**

| | | | |
|---|---|---|---|
| ☐ | Domain Separation | ☐ | Abstraction |
| ☐ | Process Isolation | ☐ | Data Hiding |
| ☐ | Resource Encapsulation | ☐ | Layering |
| ☐ | Modularity | ☐ | Simplicity |
| ☐ | Least Privilege | ☐ | Minimization |

**Mapping to GenCyber Cybersecurity Concepts:**

| | | | |
|---|---|---|---|
| ☑ | Defense in Depth | ☐ | Availability |
| ☐ | Confidentiality | ☑ | Think Like an Adversary |
| ☐ | Integrity | ☑ | Keep It Simple |

**Assessment of Learning:**

| TYPE (Examples listed below) | NAME/DESCRIPTION |
|---|---|
| Quiz/Test<br>Presentation<br>Project<br>Writing Assignment<br>Observation<br>Walk Around<br>Oral Questioning<br>Other | Observation of students during assembly/obstacle course design<br>Competitions through obstacle course navigation<br>Kahoot quizzes will be utilized to ensure knowledge retention.<br>Oral questions and walking around |

**Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)**

N/A

**Describe any Extension Activities (i.e., ideas for further work):**

Potential use and applications of robotics will be discussed so that students can use/apply these ideas and activities at their schools in engineering, science and similar clubs.

**Acknowledgements:**

N/A

# Lesson Plan*

**LESSON TITLE:** Airport Security Implementation

**SUMMARY:**

This is a hands-on workshop where high school students will be grouped to learn security of a large scale project. As an example, the students will create a physical airport and some ethical insider hackers will breach the security of the airport without letting the team know about that breach. The team will only know about that breach after the project is done. In this way, students will learn to be cautious about the insider threats.

**GRADE BAND:**

- ☐ K-2
- ☐ 6-8
- ☐ 3-5
- ☑ High School

**TIME REQUIRED:** 120 minutes

**LESSON LEARNING OUTCOMES: Upon completion of this lesson, students will be able to:**

**Outcome Examples**

| | |
|---|---|
| Design/Build<br>Test/Defend<br>Compare/Contrast<br>Apply/Use<br>Explain/Discuss<br>Identify/Describe | Demonstrate an in-depth understanding of the GenCyber Cybersecurity Concepts. |

**Materials List (i.e., string, digital diary, raspberry pi, web link, drone):**

Letter size papers, paper boards and markers.

**Describe any Previous Knowledge that may be Required:**

Basic understanding of safety and security.

**How will you facilitate the learning?**

- Describe the Warm-up Activity:

The instructor will show the pictures of airport, airplanes and runway, and explain the students how a cargo and passenger flight is operated. Student will partially assemble aircrafts using papers.

- Describe the Focused Activity:

The instructor will create teams to construct the airport. The instructor will show the requirements to build an airport. Each team will start working on this project. In the meantime, insider ethical hackers will be instructed to create breaches in the aircrafts and place unwanted objects in the airport not part of the requirements. Once each team is done with the project, the breaches will be found in the project. The students will learn to be cautious of the insider attack.

- Describe the Teacher Instruction:

This exercise requires some physical material to build the airport and breach its security. Such material includes, letter size paper, markers and blocks to show buildings of the airport (arrival, departure, Tower). However, no software is required for this activity.

**Mapping to GenCyber Cybersecurity First Principles:**

| | | | |
|---|---|---|---|
| ☐ | Domain Separation | ☐ | Abstraction |
| ☐ | Process Isolation | ☐ | Data Hiding |
| ☐ | Resource Encapsulation | ☐ | Layering |
| ☐ | Modularity | ☐ | Simplicity |
| ☐ | Least Privilege | ☐ | Minimization |

**Mapping to GenCyber Cybersecurity Concepts:**

| | | | |
|---|---|---|---|
| ☑ | Defense in Depth | ☐ | Availability |
| ☐ | Confidentiality | ☑ | Think Like an Adversary |
| ☐ | Integrity | ☐ | Keep It Simple |

**Assessment of Learning:**

| TYPE (Examples listed below) | NAME/DESCRIPTION |
|---|---|
| Quiz/Test<br>Presentation<br>Project<br>Writing Assignment<br>Observation<br>Walk Around<br>Oral Questioning<br>Other | Observation |

**Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)**

NA

**Describe any Extension Activities (i.e., ideas for further work):**

NA

**Acknowledgements:**

This exercise was developed by Imran Ghani.

# Lesson Plan*

**LESSON TITLE:** Threat Modeling using Powerpoint

**SUMMARY:**

This is a hands-on workshop where high school students will be grouped to learn how to brain-storm regarding security threats. This will be done using Threat Modeling approach (attack tree and misuse cases) where white boards and Powerpoint slides will be used by the instructor and students. The students will be given an understanding how to think like an attacker.

**GRADE BAND:**

- [ ] K-2
- [ ] 6-8
- [ ] 3-5
- [x] High School

**TIME REQUIRED:** 120 minutes

**LESSON LEARNING OUTCOMES: Upon completion of this lesson, students will be able to:**

**Outcome Examples**

| | |
|---|---|
| Design/Build<br>Test/Defend<br>Compare/Contrast<br>Apply/Use<br>Explain/Discuss<br>Identify/Describe | 1. Demonstrate an in-depth understanding of the GenCyber Cybersecurity Concepts.<br>2. Develop the skills needed to defeat various mal- and social engineering attacks.<br>3. Evaluate and analyze the availability of information systems while achieving defense in depth against Internet frauds |

**Materials List (i.e., string, digital diary, raspberry pi, web link, drone):**

White boards, Powerpoint software, markers

**Describe any Previous Knowledge that may be Required:**

Basic understanding of security attacks.

**How will you facilitate the learning?**

- Describe the Warm-up Activity:

The instructor will explain what is an attack tree and misuse case. He will demo an example of attack tree and misuse case diagrams. Then students will follow those example to create other threat models assigned by the instructor.

- Describe the Focused Activity:

The instructor will create example attack tree and misuse case diagrams. The instructor will show the requirements to be done. There will be two students in each team. Each team will start working on creating the assigned threat models and share and explain them to the whole class so.

- Describe the Teacher Instruction:

This exercise requires Powerpoint software installed on each computer.

**Mapping to GenCyber Cybersecurity First Principles:**

| | | | |
|---|---|---|---|
| ☐ | Domain Separation | ☐ | Abstraction |
| ☐ | Process Isolation | ☐ | Data Hiding |
| ☐ | Resource Encapsulation | ☐ | Layering |
| ☐ | Modularity | ☐ | Simplicity |
| ☐ | Least Privilege | ☐ | Minimization |

**Mapping to GenCyber Cybersecurity Concepts:**

| | | | |
|---|---|---|---|
| ☑ | Defense in Depth | ☐ | Availability |
| ☐ | Confidentiality | ☑ | Think Like an Adversary |
| ☐ | Integrity | ☐ | Keep It Simple |

**Assessment of Learning:**

| TYPE (Examples listed below) | NAME/DESCRIPTION |
|---|---|
| Quiz/Test<br>Presentation<br>Project<br>Writing Assignment<br>Observation<br>Walk Around<br>Oral Questioning<br>Other | Observation<br>Kahoot Quiz |

**Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)**

NA

**Describe any Extension Activities (i.e., ideas for further work):**

NA

**Acknowledgements:**

This exercise was developed by Imran Ghani.

# Lesson Plan*

**LESSON TITLE:** Cybersecurity and Homeland Security Skills: Can Students Help When the Grid Fails?

**SUMMARY:**

This workshop introduces students to meaningful Cybersecurity projects which will contribute to student knowledge and skill sets which will educate and prepare the students for a power grid or communications failure (terrorist or natural disaster attack). Imagine if your local power grid and cellphone failed and you were left standing in the dark and isolated without telephone or Internet access?

This workshop provides answers and offers communications preparation resources and solutions. Prepared and FCC-licensed students saved lives and quickly helped police and emergency communications. Students were using hand-held communications equipment to help the police!

**GRADE BAND:**

- ☐ K-2
- ☐ 3-5
- ☑ 6-8
- ☑ High School

**TIME REQUIRED:** 120 minutes

**LESSON LEARNING OUTCOMES: Upon completion of this lesson, students will be able to:**

**Outcome Examples**

| | |
|---|---|
| Design/Build<br>Test/Defend<br>Compare/Contrast<br>Apply/Use<br>Explain/Discuss<br>Identify/Describe | 1). Design and Defend your local Power Grid and Communications Network<br>2). Apply and use your knowledge of emergency communications during disasters<br>3). Participate in local emergency communications and FCC-License ARES Club<br>4). Identify and explain wireless signals & modulated spectra<br>5). Describe why knowledge of mathematics is fun and decode encrypted messages<br>6). Demonstrate how engineers actually develop cellular and satellite smartphones! |

**Materials List (i.e., string, digital diary, raspberry pi, web link, drone):**

Internet access, web browser, audio headset (recommended) or speaker, web links (below), digital diary.

Added STEM tools for motivating students to pursue a STEM education:

Professor Joe Jesson introduces to students the amazing ADI ADALM-PLUTO cellular and satellite smartphone development kit! This is the development tool of choice of engineers while developing wireless smartphones and Internet-of-Things devices!

**Describe any Previous Knowledge that may be Required:**

Problem Solving Skills, Basic Science & Math Skills, interest in STEM

**How will you facilitate the learning?**

- Describe the Warm-up Activity:

The power grid and cellphone, and Internet failure actually happened Sept 20th, 2017 as Hurricane Maria struck Puerto Rico with 155 mph winds! Present slides & Walk Around (ask students questions):

"HUMANITARIAN ASSISTANCE IN PUERTO RICO POST-HURRICANE MARIA"

- Describe the Focused Activity:

1). Initiate Q & A FCC Licensing Online Quiz offers the student flash cards linked to actual FCC questions from the question pool, online quizzes with grading, and automated repeat of subject matter as measured and needed to review:

Online Wireless Quiz: https://hamstudy.org/

2). Introduce signals analysis using online visualization (Spectrum FFT and Spectrum Waterfall) and discuss how various modulation occurs also using online visualizations and audio demodulation in various languages. Discuss how an RF Spectrum Server functions:

Signals Analysis Server: GITHUB: https://github.com/simonyiszk/openwebrx

Signals Global Map: https://sdr.hu/map

- Describe the Teacher Instruction:

Presentations and DHS Recommendations:

1). https://spectrum.ieee.org/static/special-report-puerto-rico-after-the-storm

2). Threats to Pharmaceutical Supply Chains:
https://www.dhs.gov/sites/default/files/publications/508%20-%20AEP%20Pharmaceutical%20Final%20w-DS%200792018.pdf

3). 2017 Hurricane ARRL Report:
http://www.arrl.org/files/file/Public%20Service/ARES/2017%20Hurricane%20Season%20AAR.pdf

**Mapping to GenCyber Cybersecurity First Principles:**

| | | | |
|---|---|---|---|
| ☐ | **Domain Separation** | ☐ | **Abstraction** |
| ☐ | **Process Isolation** | ☐ | **Data Hiding** |
| ☐ | **Resource Encapsulation** | ☐ | **Layering** |
| ☐ | **Modularity** | ☐ | **Simplicity** |
| ☐ | **Least Privilege** | ☐ | **Minimization** |

**Mapping to GenCyber Cybersecurity Concepts:**

| | | | |
|---|---|---|---|
| ☑ | **Defense in Depth** | ☑ | **Availability** |
| ☑ | **Confidentiality** | ☑ | **Think Like an Adversary** |
| ☑ | **Integrity** | ☐ | **Keep It Simple** |

**Assessment of Learning:**

| **TYPE (Examples listed below)** | **NAME/DESCRIPTION** |
|---|---|
| Quiz/Test<br>Presentation<br>Project<br>Writing Assignment<br>Observation<br>Walk Around<br>Oral Questioning<br>Other | A number of assessment approaches will be adopted:<br><br>1). Presentation of multiple cybersecurity and natural disaster scenarios<br><br>2). Oral questions and walking around<br><br>3). Q & A online and answer discussions |

**Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)**

| |
|---|
| N/A |

**Describe any Extension Activities (i.e., ideas for further work):**

1) Join & Participate:

** Indiana County Emergency Management **

FCC Training & License Testing: https://www.qsl.net/w3bmd/

Contact: N3QM, Bill McMillen, 724-397-2702, wkmcmillen@gmail.com

*********NOTE: YOU can help your local community!

**Acknowledgements:**

# Lesson Plan*

**LESSON TITLE:** Talk the Talk - Getting to Know the GenCyber Cybersecurity Concepts

**SUMMARY:**

In a variety of ways, students will interact with the cybersecurity concepts and vocabulary needed to be successful throughout the week of camp. Individual challenges, partner activities, group games and the creation of posters and videos (given time) will be used to make meaningful connections between the concepts and students' experiences.

**GRADE BAND:**

- ☐ K-2
- ☐ 3-5
- ☑ 6-8
- ☑ High School

**TIME REQUIRED:**

100 minutes

**LESSON LEARNING OUTCOMES: Upon completion of this lesson, students will be able to:**

**Outcome Examples**

| | |
|---|---|
| Design/Build<br>Test/Defend<br>Compare/Contrast<br>Apply/Use<br>Explain/Discuss<br>Identify/Describe | Identify the six GenCyber Cybersecurity Concepts<br>Discuss and provide examples of instances which apply the cybersecurity concepts.<br>Design creative posters which clearly define the GenCyber Cybersecurity Concepts.<br>Create a video offering information about each cybersecurity concept and utilizing the poster as an aid (given time) |

**Materials List (i.e., string, digital diary, raspberry pi, web link, drone):**

Instructional computer, as well as individual computers for students or cellphones
Guided notes
Prepared online learning tools (Quizizz, Quizlet, Gimkit, Flipgrid)
Posterboard
Markers
Masking Tape
Gmail accounts for each learner

**Describe any Previous Knowledge that may be Required:**

None

**How will you facilitate the learning?**

- Describe the Warm-up Activity:

Hook: Cute Facebook video of language barriers

Guided Notes: Define Six Cybersecurity Concepts explicitly. Provide examples.

- Describe the Focused Activity:

FIRST 50 MINUTES: Students will master the 6 Cybersecurity Concepts in a variety of games and reflective discussion

SECOND 50 MINUTES: Students will apply the 6 Cybersecurity Concepts in the creation of a poster to decorate camp with and in a Flipgrid video for the IUP GenCyber resources.

- Describe the Teacher Instruction:

FIRST 50 MINUTES:
1) Hook students with a cute video about language barriers.
2) Provide a concrete resource about the six GenCyber cybersecurity concepts via guided notes.
3) Allow for individual reflection with guided notes while completing a Quizizz.
4) Discuss the most missed questions on Quizizz or with any other areas of confusion.
5) Allow for partner communication about the cybersecurity concepts on Quizlet - play "Match."
6) Conduct a competition with the whole group using Gimkit.

SECOND 50 MINUTES:
5) Groups (2-3 students) brainstorm a poster defining and depicting each of the 6 cyber security concepts.

6) Create the poster with the following guidelines: neat, not crowded, clear definition, relevant examples listed, visual application to demonstrate the concept.

7) Create a Flipgrid Video (on cellphones if webcams are unavailable), using the poster as a visual aid.

**Mapping to GenCyber Cybersecurity First Principles:**

| | | | |
|---|---|---|---|
| ☐ | Domain Separation | ☐ | Abstraction |
| ☐ | Process Isolation | ☐ | Data Hiding |
| ☐ | Resource Encapsulation | ☐ | Layering |
| ☐ | Modularity | ☐ | Simplicity |
| ☐ | Least Privilege | ☐ | Minimization |

**Mapping to GenCyber Cybersecurity Concepts:**

| | | | |
|---|---|---|---|
| ☑ | Defense in Depth | ☑ | Availability |
| ☑ | Confidentiality | ☑ | Think Like an Adversary |
| ☑ | Integrity | ☑ | Keep It Simple |

**Assessment of Learning:**

| TYPE (Examples listed below) | NAME/DESCRIPTION |
|---|---|
| Quiz/Test<br>Presentation<br>Project<br>Writing Assignment<br>Observation<br>Walk Around<br>Oral Questioning<br>Other | Quizizz results for individuals (scores)<br>Quizlet results for partners (times)<br>Gimkit results for individuals (scores)<br>Poster content for groups<br>Flipgrid explanations for groups |

**Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)**

Students without Gmail accounts will need to create Gmail accounts for the activities.
Students with visual impairments may need to enlarge text on computer screens.
Students without cellphones or webcams may need to share with others.

Brighter, self-motivated or former campers could also study and apply the 10 GenCyber Cybersecurity Principles and examine their relationships to the 6 Concepts.

**Describe any Extension Activities (i.e., ideas for further work):**

The entire week of camp should contain lessons which continually cause the students to reflect on and apply the six GenCyber Cybersecurity Concepts.

**Acknowledgements:**

GenCyber Cyber-Security Concepts

# Lesson Plan*

**LESSON TITLE:** Data Protection/Cryptography

**SUMMARY:**

1. Learning how to protect sensitive data using encryption
2. Learning a brief history of cryptography (encryption/decryption)
3. Understanding the basic concepts of cryptography
4. Learning several basic cryptographic techniques
5. Hand-on practice on encryption/decryption using on-line tools

**GRADE BAND:**

- ☐ K-2
- ☑ 6-8
- ☐ 3-5
- ☑ High School

**TIME REQUIRED:** 120 minutes

**LESSON LEARNING OUTCOMES: Upon completion of this lesson, students will be able to:**

**Outcome Examples**

| | |
|---|---|
| Design/Build<br>Test/Defend<br>Compare/Contrast<br>Apply/Use<br>Explain/Discuss<br>Identify/Describe | Upon completion of the camp, participants will be able to:<br><br>1. Demonstrate an in-depth understanding of the GenCyber Cybersecurity Concepts.<br>2. Understand cryptographic basics and its role in securing data communications. |

**Materials List (i.e., string, digital diary, raspberry pi, web link, drone):**

Web Links:
1. Navajo Code Talker Died, June 13, 2018:
https://nowthisnews.com/videos/news/one-of-the-last-living-navajo-code-talkers-from-wwii-passed-away
2. Cryptography in 60 Seconds: https://www.youtube.com/watch?v=j5fOynJrNOk
3. Simple Cryptography: https://www.youtube.com/watch?v=ez0AOYl-i4k
4. Cryptography for Kids: https://kids.kiddle.co/Cryptography
5. Caesar cipher decryption tool: https://www.xarg.org/tools/caesar-cipher/ (good)
6. The Black Chamber: https://www.simonsingh.net/The_Black_Chamber/caesar.html

**Describe any Previous Knowledge that may be Required:**

Knowledge of Mathematics: Pre-Algebra, and Algebra

**How will you facilitate the learning?**

- Describe the Warm-up Activity:

1. Explaining the basics of data protection
2. Explaining and discussing the basics of cryptography
3. Brief discussion on the history of cryptography from Egypt to modern time
4. What are encryption and decryption and how they are performed
5. Difference between private and public key cryptography
6. Hand-on practices on various cryptographic techniques using online tools

- Describe the Focused Activity:

Hand-on Practices:
The students are asked to practice on various cryptographic techniques, such as Caesar Cipher, DES, AES, Private-key cryptography, Public-key cryptography using tools available on-line. They will encrypt a message (a plaintext) into cipher text and again decrypt the ciphertext back to the plain text.

Challenge:
For middle school students, easier ciphertext will be provided and asked to decrypt it to the plaintext using brute force technique.

For high school students, relatively harder ciphertext will be provided and asked to decrypt it (if they can) to the plaintext using brute force technique. In addition to that, more exercises will be assigned in this session.

- Describe the Teacher Instruction:

**Mapping to GenCyber Cybersecurity First Principles:**

| | | | |
|---|---|---|---|
| ☐ | Domain Separation | ☐ | Abstraction |
| ☐ | Process Isolation | ☐ | Data Hiding |
| ☐ | Resource Encapsulation | ☐ | Layering |
| ☐ | Modularity | ☐ | Simplicity |
| ☐ | Least Privilege | ☐ | Minimization |

**Mapping to GenCyber Cybersecurity Concepts:**

| | | | |
|---|---|---|---|
| ☑ | Defense in Depth | ☐ | Availability |
| ☑ | Confidentiality | ☑ | Think Like an Adversary |
| ☐ | Integrity | ☐ | Keep It Simple |

**Assessment of Learning:**

| TYPE (Examples listed below) | NAME/DESCRIPTION |
|---|---|
| Quiz/Test<br>Presentation<br>Project<br>Writing Assignment<br>Observation<br>Walk Around<br>Oral Questioning<br>Other | The instructor and TAs made observation while the activity was being performed.<br>The instructor and TAs walked around to observe how different group are performing.<br>The instructor and TAs asked oral questions when needed to ensure the students understood what they were doing and why.<br>The instructor and TAs made sure all group members were engaged in the activities.<br>The students were asked to present their final results. |

**Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)**

| |
|---|
| N/A |

**Describe any Extension Activities (i.e., ideas for further work):**

Activities could be extended to include more examples on decryption if students became more curious.

**Acknowledgements:**

N/A

# Lesson Plan*

**LESSON TITLE:** Network Threats and Countermeasures

**SUMMARY:**

This module will illustrate network threats, including typical Internet fraud Phishing attacks, as well as basic countermeasures against these threats. The important cybersecurity concepts, such as confidentiality and integrity, will be explained through the presentation of threats examples and commonly used security mechanisms against the frauds.

Through the hands-on activities, participants will learn the risk of threats, the vulnerability of networks, and the knowledge of choosing appropriate security mechanisms against the network attacks.

**GRADE BAND:**

- ☐ K-2
- ☐ 6-8
- ☐ 3-5
- ☑ High School

**TIME REQUIRED:** 120 minutes

**LESSON LEARNING OUTCOMES: Upon completion of this lesson, students will be able to:**

**Outcome Examples**

| | |
|---|---|
| Design/Build<br>Test/Defend<br>Compare/Contrast<br>Apply/Use<br>Explain/Discuss<br>Identify/Describe | Understand certain network threats including the man-in-the-middle attack that compromises confidentiality and integrity and phishing attack;<br>Understand basic countermeasures against these well-know network threats;<br>Understand how the security mechanisms work against the network threats;<br>Understand how to choose appropriate mechanisms against specific attacks. |

**Materials List (i.e., string, digital diary, raspberry pi, web link, drone):**

Module presentation materials prepared by the instructor;
CrypTool, an open-source educational software (https://www.cryptool.org/de/jcryptool);
Hands-on activity manual (prepared by the instructor);
A couple of YouTube on Internet and two-factor authentication
https://www.youtube.com/watch?v=ewrBalT_eBM
http://www.youtube.com/watch?v=r3EK6JYIvHE

**Describe any Previous Knowledge that may be Required:**

Basic mathematical concepts such as permutation and shifting of a block of letter (to understand simple example of encryption algorithms).

**How will you facilitate the learning?**

- Describe the Warm-up Activity:

The instructor will first show a demo on how the Internet/networks work;
Using a couple of examples, the instructor will explain how to use CrypTool to conduct encryption, create message authentication code and digital signature, and how to "attack" (that is, cryptographically analyze) ciphers and digital signatures. Then, students will complete the designed activities individually and in a small team (of 2 students).

- Describe the Focused Activity:

There will be four sets of activities designed for this module:
(1) To understand the countermeasures against compromise of confidentiality (the man-in-the-middle attacks), students will complete hands-on activities including operating encryption using various ciphers and cryptanalysis of well-known ciphers. These hands-on activities will be conducted using CrypTool.
(2) To understand the security mechanisms against compromise of integrity, students will complete activities for message digest creation using hash algorithms and vulnerability analysis of hash algorithms. These are all hands-on activities.
(3) To understand the countermeasures against email-phishing attacks, students will complete hands-on activities for email authentication using digital signature. They will learn digital signature creation and verification through the hands-on tasks.
(3) To understand digital certificate and public-key infrastructure (PKI), students will complete hands-on activities for verifying the digital certificate of any given web server, and use an online tool to evaluate the security rating of any given web server.

- Describe the Teacher Instruction:

The instructor will explain the common network threats, including confidentiality compromise, integrity compromise, phishing attack, and the well-known security mechanisms against these threats, presenting well-designed slides, which are followed by hands-on activities.

The module is conducted with 4 sections (approximately 25 minutes for each) -- each section starts with the teacher's instructions, being followed by students' hands-on activities. For example, the 3rd section is organized as:

The instructor will explain what is phishing attack, and show several examples of phishing attacks. Then, two types of countermeasures against phishing attacks will be explained, that is, two-factor authentication and email authentication through digital signature. These instructions are followed by a demo/video on two-factor authentication and hands-on activities on digital signature creation and verification.

**Mapping to GenCyber Cybersecurity First Principles:**

| | | | |
|---|---|---|---|
| ☐ | Domain Separation | ☐ | Abstraction |
| ☐ | Process Isolation | ☐ | Data Hiding |
| ☐ | Resource Encapsulation | ☐ | Layering |
| ☐ | Modularity | ☐ | Simplicity |
| ☐ | Least Privilege | ☐ | Minimization |

**Mapping to GenCyber Cybersecurity Concepts:**

| | | | |
|---|---|---|---|
| ☐ | Defense in Depth | ☐ | Availability |
| ☑ | Confidentiality | ☑ | Think Like an Adversary |
| ☑ | Integrity | ☐ | Keep It Simple |

**Assessment of Learning:**

| TYPE (Examples listed below) | NAME/DESCRIPTION |
|---|---|
| Quiz/Test<br>Presentation<br>Project<br>Writing Assignment<br>Observation<br>Walk Around<br>Oral Questioning<br>Other | Observation:<br>The hands-on activities are provided for students to complete individually or in a team of 2 students. The instructor will observe the progresses made by students, assess their understanding and provide further instructions if necessary.<br><br>Presentation and Oral Questioning:<br>During the hands-on activities, students will be asked questions that are pre-designed; they are expected to correctly answer the questions after successfully complete certain steps of the hands-on activities. |

**Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)**

Many of the learning contents are supported by pictures/diagrams or multimedia materials. For students who need any extra instructions, the instructor would try to provide individual help.

**Describe any Extension Activities (i.e., ideas for further work):**

The instructions, presentations, and hands-on activities are designed at an appropriate complexity level to suit the participants. Further work for this module can be an extended coverage of more network threats and in-depth analysis of certain countermeasures, depending on students' mathematics background and computer science knowledge.

**Acknowledgements:**

# Lesson Plan*

**LESSON TITLE:** Internet of Things (IoT) Security/Monitoring

**SUMMARY:**

This module will discuss IoT devices, it's User Service Platform (USP) and Sensors. Participants will be familiarized with the concept of IoT, learning how these systems can be controlled from just about anywhere on the globe using the Internet. Specifically, this IoT Device Simulation module will introduce the students to the IBM's Bluemix platform using the Watson IoT platform, a Cloudant noSQL database, and Node-RED to create a flow which captures simulated sensor data which can then be manipulated, visualized, and stored in a database.

**GRADE BAND:**

- ☐ K-2
- ☐ 3-5
- ☑ 6-8
- ☑ High School

**TIME REQUIRED:**

120 minutes

**LESSON LEARNING OUTCOMES: Upon completion of this lesson, students will be able to:**

**Outcome Examples**

| | |
|---|---|
| Design/Build<br>Test/Defend<br>Compare/Contrast<br>Apply/Use<br>Explain/Discuss<br>Identify/Describe | Develop an understanding of embedded devices and the Internet of Things.<br>Design Node-RED based flows<br>Use simulated devices within the flows and visualize sensor data |

**Materials List (i.e., string, digital diary, raspberry pi, web link, drone):**

IBM Bluemix
CloudFoundry Command Line Interface (CLI)

**Describe any Previous Knowledge that may be Required:**

Basic knowledge of JavaScript/Node.js would be helpful but is not required.

**How will you facilitate the learning?**

- Describe the Warm-up Activity:

The warm up activity will involve setting up users with an IBM Bluemix account and showing how to login to the Bluemix API using the CloudFoundry Command Line Interface (CLI). Students will then push and provision their workspaces to their individual accounts and shown the basics of Node-RED's functionality and the Watson IoT dashboard.

- Describe the Focused Activity:

The focus activity will involve the simulation of a device which contains sensor data which can be extracted and fed to the Node-RED platform. The students will then create a Node-RED flow using various nodes in order to manipulate the extracted data which allows for visualization, storing the data in a noSQL database, as well as creating event driven functions based on changes in the sensor data. The visualization of the data will be done by creating a Node-RED dashboard which takes the sensor data as input and creates a time based line graph. Each of the nodes within the flow will be programmed using JavaScript to extract sensor information, collect data, perform actions based on changes in the sensor data, and output the data to a Node-RED dashboard and a noSQL database.

Moreover, students will be taught step-by-step how to create an IBM Bluemix account and use the CloudFoundry CLI in order to provision their workspace with the Watson IoT platform and Node-RED. The instructor will then show the students the basics of both platforms, focusing especially on the functionality of Node-RED and how the nodes function and can be manipulated between each other. The instructor will follow along with the students in how to create the flow, simulated sensor device, and use the Watson IoT Dashboard and Cloudant noSQL database.

- Describe the Teacher Instruction:

N/A

**Mapping to GenCyber Cybersecurity First Principles:**

| | | | |
|---|---|---|---|
| ☐ | Domain Separation | ☐ | Abstraction |
| ☐ | Process Isolation | ☐ | Data Hiding |
| ☐ | Resource Encapsulation | ☐ | Layering |
| ☐ | Modularity | ☐ | Simplicity |
| ☐ | Least Privilege | ☐ | Minimization |

**Mapping to GenCyber Cybersecurity Concepts:**

| | | | |
|---|---|---|---|
| ☑ | Defense in Depth | ☑ | Availability |
| ☑ | Confidentiality | ☐ | Think Like an Adversary |
| ☐ | Integrity | ☑ | Keep It Simple |

**Assessment of Learning:**

| TYPE (Examples listed below) | NAME/DESCRIPTION |
|---|---|
| Quiz/Test<br>Presentation<br>Project<br>Writing Assignment<br>Observation<br>Walk Around<br>Oral Questioning<br>Other | The assessment of learning will be a project in which the students will create and provision their Watson IoT platform and Node-RED implementation. |

**Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)**

| |
|---|
| N/A |

**Describe any Extension Activities (i.e., ideas for further work):**

Extension activies could include showing students how to further extend their implementations/flows to be used with real world sensors/actuators such as Raspberry PIs which would allow students to collect real-world data or use Node-RED to automate IoT functions.

**Acknowledgements:**

Acknowledgements to IBM, the Cloud Foundry Foundation, the Node.js foundation, and Node-RED.

# Lesson Plan*

**LESSON TITLE:** Fundamentals of Information Security

**SUMMARY:**

This module presents essential fundamentals of information security concepts including Confidentiality, Integrity, Availability, and non-repudiation. Various components of a typical information system will be presented including software, hardware, data, users, etc. The module will highlight the importance of humans as a central component of any system and how human errors are the typical cause of system compromises. The common saying that "humans are the weakest link of the security chain" will be expounded with several real-world examples. In such context, other cybersecurity concepts will be fully explained. The concept of Keep It Simple will be introduced as a technique that will help minimize human errors as participants will have a better understanding of the systems they need to defend. Additionally, when discussing various components of an information system, the concept of Defense in Depth will yield itself well. For example, the discussion will include an explanation of how various components can be viewed as different layers of security that attackers must then defeat to conduct a successful attack. Moreover, common attacker motivations will be discussed which will familiarize participants with adversary mindsets and introduce essential ethical aspects.

**GRADE BAND:**

- ☐ K-2
- ☐ 6-8
- ☐ 3-5
- ☑ High School

**TIME REQUIRED:** 120 minutes

**LESSON LEARNING OUTCOMES: Upon completion of this lesson, students will be able to:**

| Outcome Examples | |
|---|---|
| Design/Build<br>Test/Defend<br>Compare/Contrast<br>Apply/Use<br>Explain/Discuss<br>Identify/Describe | 1. Demonstrate an in-depth understanding of the GenCyber Cybersecurity Concepts.<br>2. Evaluate and analyze the availability of information systems while achieving defense in depth against Internet frauds. |

**Materials List (i.e., string, digital diary, raspberry pi, web link, drone):**

Lab Computers
Internet Access
Account on GenCyber Coins system
Lab handouts

**Describe any Previous Knowledge that may be Required:**

Basic Math and problem solving skills.

**How will you facilitate the learning?**

- Describe the Warm-up Activity:

The instructor will explain the basic components of a typical Information system and discuss how we can protect these systems while making explicit links to the six GenCyber Cybersecurity concepts. Several examples will be used to hook the students on the discussion with emphasis on the 4 C's (Communication, Collaboration, Creativity, and Critical thinking).

- Describe the Focused Activity:

This module is designed to be taught in a highly interactive environment in which all attendees will be active participants in the learning process. To achieve this, one approach is to use a series of lab-based activities to enable students to “do it yourself” to enhance their comprehension of taught contents. Such lab activities include "Bug Bounty" and "Reconnaissance" from the GenCyber Coin Site. One other approach is to use mobile technology to enhance participant involvement using their phones (BYOD) to participate in interactive exercises such as online quizzes (Kahoot) and simulations.

Bug Bounty: This tool allows students to "think like an adversary" and attempt to find bugs in the GenCyber Coin game website. Secure coding concepts, ethical hacking, and human error will be discussed as students work through finding the bugs.

Reconnaissance: This game again encourages students to "think like an adversary" by conducting social engineering based research on the GenCyber faculty and staff. This activity provides a more in depth and hands-on look into how human error, and the human desire to share personal information, may cause breaches in security. This activity will be introduced in this module, and can be conducted during the remainder of camp.

- Describe the Teacher Instruction:

N/A

**Mapping to GenCyber Cybersecurity First Principles:**

| | | | |
|---|---|---|---|
| ☐ | Domain Separation | ☐ | Abstraction |
| ☐ | Process Isolation | ☐ | Data Hiding |
| ☐ | Resource Encapsulation | ☐ | Layering |
| ☐ | Modularity | ☐ | Simplicity |
| ☐ | Least Privilege | ☐ | Minimization |

**Mapping to GenCyber Cybersecurity Concepts:**

| | | | |
|---|---|---|---|
| ☑ | Defense in Depth | ☑ | Availability |
| ☑ | Confidentiality | ☑ | Think Like an Adversary |
| ☑ | Integrity | ☑ | Keep It Simple |

**Assessment of Learning:**

| TYPE (Examples listed below) | NAME/DESCRIPTION |
|---|---|
| Quiz/Test<br>Presentation<br>Project<br>Writing Assignment<br>Observation<br>Walk Around<br>Oral Questioning<br>Other | A number of assessment approaches will be adopted:<br>1- Regular observation of campers performance in the given tasks<br>2- Interactive competitive quizzes as discussed above.<br>3- Oral questions and walking around. |

**Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)**

N/A

**Describe any Extension Activities (i.e., ideas for further work):**

Potential use and applications of the covered activities will be discussed so that students can use/apply these ideas and activities at their schools in programming, science and similar clubs. Students will also have access to the GenCyber Coin game indefinitely, and can continue learning and exploring on the site.

**Acknowledgements:**

Many thanks for Ms. Lydia Taylor for her excellent contributions to the design and testing of this module's activities.

Many thanks to Dr. Vitaly Ford for the use of his interactive and engaging GenCyber Coin Game website.

# Lesson Plan*

**LESSON TITLE:** Beautiful Minds + Powerful Machines = Computational Thinking  Mrs. Gentile  Wed

**SUMMARY:**

Students will use computational thinking to solve real problems in a fun, competitive environment where cybersecurity concepts are explored and applied quickly.

**GRADE BAND:**

- [ ] K-2
- [x] 6-8
- [ ] 3-5
- [ ] High School

**TIME REQUIRED:**

100 minutes

**LESSON LEARNING OUTCOMES: Upon completion of this lesson, students will be able to:**

**Outcome Examples**

| | |
|---|---|
| Design/Build<br>Test/Defend<br>Compare/Contrast<br>Apply/Use<br>Explain/Discuss<br>Identify/Describe | explain how the GenCyber cybersecurity concepts were modeled, and<br><br>apply mathematics to solve real problems, some involving programming and use of computers |

**Materials List (i.e., string, digital diary, raspberry pi, web link, drone):**

Breakout EDU kit with teacher-made problems
Slide presentation w/ facts and video embedded
graphing calculators
computers
prize

**Describe any Previous Knowledge that may be Required:**

Use of graphing calculators or www.desmos.com to solve systems

Ability to use spreadsheets and write simple spreadsheet formulas

**How will you facilitate the learning?**

- Describe the Warm-up Activity:

Show brief video about the shortage of cybersecurity specialists.

Hold a brief discussion about what all employers want - problem solvers who collaborate well, communicate clearly, are creative and think critically. Today, students will be given the opportunity to crack codes while exhibiting these characteristics.

- Describe the Focused Activity:

Students will be given a series of mathematical problems and/or riddles to solve in their mixed grade level teams. The answer to each problem is the code or key that opens a lock to one of the boxes. Inside the box, they will find a piece of a clue that helps them to uncover a "treasure." Students will need to complete every task in order to have access to the "treasure." As they solve, they will be asked about the cybersecurity concepts inherent in the design of the activity.

- Describe the Teacher Instruction:

Instructor will welcome students and open with the video about the shortage of cybersecurity professionals. A brief discussion will follow encouraging students to identify the characteristics of employees companies would seek. Students will then be grouped and given their first challenge, reminding them to collaborate well, think critically, be creative and communicate clearly.

As students complete challenges and attempt to open the boxes, they will be reminded of the GenCyber cybersecurity concepts of "Defense in Depth" and "Confidentiality," as they are given authorization to information after completing a layer of tasks. They will be instructed to open boxes only with supervision of an instructor or a student assistant so that the "Integrity" of the information is not compromised. If students fail to solve the problem correctly, they will be handed a "Denial of Service" slip, reminding them that the information is not "Available" to them at this time.

The group which solves all of the problems and opens all of the boxes first will receive a small prize.

Closure to the activity will be a summary of trending college majors related to data and cybersecurity:

| | | |
|---|---|---|
| Data Analytics | Predictive Statistics | Applied Mathematics |
| Data Science | Intelligence Analysis | Cybersecurity |

**Mapping to GenCyber Cybersecurity First Principles:**

| | | | |
|---|---|---|---|
| ☐ | Domain Separation | ☐ | Abstraction |
| ☐ | Process Isolation | ☐ | Data Hiding |
| ☐ | Resource Encapsulation | ☐ | Layering |
| ☐ | Modularity | ☐ | Simplicity |
| ☐ | Least Privilege | ☐ | Minimization |

**Mapping to GenCyber Cybersecurity Concepts:**

| | | | |
|---|---|---|---|
| ☑ | Defense in Depth | ☑ | Availability |
| ☑ | Confidentiality | ☐ | Think Like an Adversary |
| ☑ | Integrity | ☐ | Keep It Simple |

**Assessment of Learning:**

| TYPE (Examples listed below) | NAME/DESCRIPTION |
|---|---|
| Quiz/Test<br>Presentation<br>Project<br>Writing Assignment<br>Observation<br>Walk Around<br>Oral Questioning<br>Other | Observation of problem completion and positive student interaction, encouraging the "soft skills" wanted by employers<br><br>Written answers to mathematical problems solved with computational thinking<br><br>Oral Questioning about the concepts of Defense in Depth, Confidentiality, Integrity, and Availability |

**Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)**

Students with physical dexterity problems may not be able to open combination locks, relying on a group member to do so.

Students with visual disabilities may need to enlarge the computer screen.

**Describe any Extension Activities (i.e., ideas for further work):**

Students could research college majors at schools with which they are familiar to see how data science and cybersecurity opportunities are addressed there.

Students could explore other methods of cryptography used throughout history.

Students could continue their exploration of the power of spreadsheets through online tutorials.

Students could continue to explore graphing calculator technology through www.desmos.com.

**Acknowledgements:**

www.Gen-Cyber.com

# Lesson Plan*

**LESSON TITLE:** Cyber Knowledge Fair - Mrs. Lint and Mrs. Gentile - Friday, June 28, 2019

**SUMMARY:**

Students will prepare a 5-minute presentation to explain technology concepts gained during the week in all of the camp's various topics, and will explain how to incorporate the six GenCyber cybersecurity concepts into their respective topics to other camp participants.

**GRADE BAND:**

- ☐ K-2
- ☐ 3-5
- ☑ 6-8
- ☑ High School

**TIME REQUIRED:**

100 minutes

**LESSON LEARNING OUTCOMES: Upon completion of this lesson, students will be able to:**

**Outcome Examples**

| | |
|---|---|
| Design/Build<br>Test/Defend<br>Compare/Contrast<br>Apply/Use<br>Explain/Discuss<br>Identify/Describe | design brief, clear presentations about cybersecurity topics,<br><br>describe technological concepts and devices explored during the week in their presentations,<br><br>apply the six Cyber Security Concepts to technology topics from the week. |

**Materials List (i.e., string, digital diary, raspberry pi, web link, drone):**

Computers
Poster board
dice
spinners
timers
Legos or other building blocks
Robots

**Describe any Previous Knowledge that may be Required:**

Middleschoolers will have been exposed to the GenCyber cybersecurity concepts, Alice programming, the Internet of Things, cryptography, computational thinking, droids, secure networks, grid failure.

Highschoolers will have been exposed to the topics above in addition to threat modeling, digital forensics, threats and countermeasures, information security, airport security.

**How will you facilitate the learning?**

- Describe the Warm-up Activity:

9:00 - 9:05
Remind students that on this final day of camp, they will have to prove their learning in two ways - through a culminating activity and a post-test. This activity is meant for them to test their understanding in a fun way.
Divide middle and high school students, then place each level into groups of three.
Ask all groups to select a topic from the week's 8-9 topics out of a middle school hat or highschool hat.

Students with the same topics will gather together to brainstorm how best to teach that topic to others. They will be informed that they will present their topics 4 times as we all rotate through the fair.

- Describe the Focused Activity:

9:05 - 9:50
Students will be given the following set of expectations to guide development of their 5-minute presentation for the fair. They must do the following:
1. Introduce general uses of the topic through demonstration, model, physical game or on-line game
2. Demonstrate the most interesting aspects of the topic!
3. **Discuss which cybersecurity concept(s) is/are addressed in the topic**
4. Prepare to ask for and answer questions from audience

10:00 – 10:05
Allow the high school students time to finalize their set-ups of their stations.
Meanwhile, encourage middle schoolers to get into groups of three. Have them use their guided notes of the six cybersecurity concepts to use in reference as they circulate.

10:05 - 10:25
Students will rotate through each other's stations (first the middleschoolers will visit the highschoolers' stations, then vice versa)
1. Watch the demo or participate in the game
2. **Discuss which cybersecurity concept(s) is/are addressed in the topic**
3. Ask questions to improve your understanding of the topic

10:30 – 10:50
Students will switch roles with highschoolers traveling to at least 4 middleschoolers' stations

- Describe the Teacher Instruction:

After students have been well-organized into presentation groups, instructors will monitor the progress of their communication and collaboration.

Instructors will hand out written expectations for each group or post expectations on a screen if available.

Instructors will help to guide each group to focus on the requirements of their presentations and to clarify any application of the cybersecurity concepts they are using.

Instructors will monitor the time closely so that all have equal opportunity to present and participate.

Conclude with the expectation that the knowledge gained from the week will enable them to perform well in the camp's culminating activity as well as the camp post-test, given later that day.

**Mapping to GenCyber Cybersecurity First Principles:**

| | | | |
|---|---|---|---|
| ☐ | **Domain Separation** | ☐ | **Abstraction** |
| ☐ | **Process Isolation** | ☐ | **Data Hiding** |
| ☐ | **Resource Encapsulation** | ☐ | **Layering** |
| ☐ | **Modularity** | ☐ | **Simplicity** |
| ☐ | **Least Privilege** | ☐ | **Minimization** |

**Mapping to GenCyber Cybersecurity Concepts:**

| | | | |
|---|---|---|---|
| ☑ | **Defense in Depth** | ☑ | **Availability** |
| ☑ | **Confidentiality** | ☑ | **Think Like an Adversary** |
| ☑ | **Integrity** | ☑ | **Keep It Simple** |

**Assessment of Learning:**

| **TYPE (Examples listed below)** | **NAME/DESCRIPTION** |
|---|---|
| Quiz/Test<br>Presentation<br>Project<br>Writing Assignment<br>Observation<br>Walk Around<br>Oral Questioning<br>Other | Observation: As students share, demonstrate and collaborate ideas communicated<br><br>Physical model, game: As students play, demonstrate and build or demonstration<br><br>Strength of questioning: As teachers/students ask for clarification on the GenCyber cybersecurity concepts<br><br>Participation: As observers ask questions of each presentation |

**Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)**

Assistance may be needed for groups without a strong leader, which instructors and student assistants can provide.

**Describe any Extension Activities (i.e., ideas for further work):**

Students in this Gen-Cyber Cybersecurity Camp are expected to share knowledge and skills gained this week at their junior or senior highschools, and hopefully to maintain an interest in Cybersecurity- related careers.

**Acknowledgements:**

www.Gen-Cyber.com

# Lesson Plan*

**LESSON TITLE:** Robots Programming (Droid Inventor Kit)

**SUMMARY:**

This module introduces robot functions, operation, and potential for cybersecurity risks. The module starts with a brief history of robots and discussion of current and potential functions, as well as security weaknesses. The module then focuses on hands-on learning and experience, utilizing the "Little Bits Droid Inventor Kit." Students will learn how to build a simple circuit, manually operate the kit, as well as operate the kit through programming.

**GRADE BAND:**

- ☐ K-2
- ☐ 3-5
- ☑ 6-8
- ☑ High School

**TIME REQUIRED:** 120 minutes

**LESSON LEARNING OUTCOMES: Upon completion of this lesson, students will be able to:**

**Outcome Examples**

| | |
|---|---|
| Design/Build<br>Test/Defend<br>Compare/Contrast<br>Apply/Use<br>Explain/Discuss<br>Identify/Describe | Design/Build: Build a simple electronic circuit that controls the Droid Inventor Kit, as well as an obstacle course representing a cybersecurity system.<br>Compare/Contrast: Different methods of securing a system that is located within a small movable object.<br>Apply/Use: Apply new programming knowledge to operate Droid Inventor Kit. |

**Materials List (i.e., string, digital diary, raspberry pi, web link, drone):**

Droid Inventor Kits
Obstacle Course Components
Droid Inventor Kit App
Smart Device

**Describe any Previous Knowledge that may be Required:**

Basic team work and problem solving skills

**How will you facilitate the learning?**

- Describe the Warm-up Activity:

The module will begin with an interactive discussion on student opinions regarding robots, their use, and security weaknesses. This discussion will reinforce the cybersecurity concepts, and encourage the students to think differently about robots and their functions.

- Describe the Focused Activity:

-Discussion of robot use and the potential cyersecurity risks.
-Students will build their Droid Inventor Kit while learning about simple circuits.
-Students will design and construct an obstacle course that represents a cybersecurity defense system, and will compete against each other to navigate each obstacle course.
-Kahoot quizzes will be utilized to ensure knowledge retention.
-The varying degrees of difficulty in the obstacle course will allow for customization based on skill level.

- Describe the Teacher Instruction:

N/A

**Mapping to GenCyber Cybersecurity First Principles:**

| | | | |
|---|---|---|---|
| ☐ | Domain Separation | ☐ | Abstraction |
| ☐ | Process Isolation | ☐ | Data Hiding |
| ☐ | Resource Encapsulation | ☐ | Layering |
| ☐ | Modularity | ☐ | Simplicity |
| ☐ | Least Privilege | ☐ | Minimization |

**Mapping to GenCyber Cybersecurity Concepts:**

| | | | |
|---|---|---|---|
| ☑ | Defense in Depth | ☐ | Availability |
| ☐ | Confidentiality | ☑ | Think Like an Adversary |
| ☐ | Integrity | ☑ | Keep It Simple |

**Assessment of Learning:**

| TYPE (Examples listed below) | NAME/DESCRIPTION |
|---|---|
| Quiz/Test<br>Presentation<br>Project<br>Writing Assignment<br>Observation<br>Walk Around<br>Oral Questioning<br>Other | Observation of students during assembly/obstacle course design<br>Competitions through obstacle course navigation<br>Kahoot quizzes will be utilized to ensure knowledge retention.<br>Oral questions and walking around |

**Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)**

N/A

**Describe any Extension Activities (i.e., ideas for further work):**

Potential use and applications of robotics will be discussed so that students can use/apply these ideas and activities at their schools in engineering, science and similar clubs.

**Acknowledgements:**

N/A

# Lesson Plan*

**LESSON TITLE:** Cybersecurity and Homeland Security Skills: Can Students Help When the Grid Fails?

**SUMMARY:**

This workshop introduces students to meaningful Cybersecurity projects which will contribute to student knowledge and skill sets which will educate and prepare the students for a power grid or communications failure (terrorist or natural disaster attack). Imagine if your local power grid and cellphone failed and you were left standing in the dark and isolated without telephone or Internet access?

This workshop provides answers and offers communications preparation resources and solutions. Prepared and FCC-licensed students saved lives and quickly helped police and emergency communications. Students were using hand-held communications equipment to help the police!

**GRADE BAND:**

- ☐ K-2
- ☐ 3-5
- ☑ 6-8
- ☑ High School

**TIME REQUIRED:** 120 minutes

**LESSON LEARNING OUTCOMES: Upon completion of this lesson, students will be able to:**

**Outcome Examples**

| | |
|---|---|
| Design/Build<br>Test/Defend<br>Compare/Contrast<br>Apply/Use<br>Explain/Discuss<br>Identify/Describe | 1). Design and Defend your local Power Grid and Communications Network<br>2). Apply and use your knowledge of emergency communications during disasters<br>3). Participate in local emergency communications and FCC-License ARES Club<br>4). Identify and explain wireless signals & modulated spectra<br>5). Describe why knowledge of mathematics is fun and decode encrypted messages<br>6). Demonstrate how engineers actually develop cellular and satellite smartphones! |

**Materials List (i.e., string, digital diary, raspberry pi, web link, drone):**

Internet access, web browser, audio headset (recommended) or speaker, web links (below), digital diary.

Added STEM tools for motivating students to pursue a STEM education:

Professor Joe Jesson introduces to students the amazing ADI ADALM-PLUTO cellular and satellite smartphone development kit! This is the development tool of choice of engineers while developing wireless smartphones and Internet-of-Things devices!

**Describe any Previous Knowledge that may be Required:**

Problem Solving Skills, Basic Science & Math Skills, interest in STEM

**How will you facilitate the learning?**

- Describe the Warm-up Activity:

The power grid and cellphone, and Internet failure actually happened Sept 20th, 2017 as Hurricane Maria struck Puerto Rico with 155 mph winds! Present slides & Walk Around (ask students questions):

"HUMANITARIAN ASSISTANCE IN PUERTO RICO POST-HURRICANE MARIA"

- Describe the Focused Activity:

1). Initiate Q & A FCC Licensing Online Quiz offers the student flash cards linked to actual FCC questions from the question pool, online quizzes with grading, and automated repeat of subject matter as measured and needed to review:

Online Wireless Quiz: https://hamstudy.org/

2). Introduce signals analysis using online visualization (Spectrum FFT and Spectrum Waterfall) and discuss how various modulation occurs also using online visualizations and audio demodulation in various languages. Discuss how an RF Spectrum Server functions:

Signals Analysis Server: GITHUB: https://github.com/simonyiszk/openwebrx

Signals Global Map: https://sdr.hu/map

- Describe the Teacher Instruction:

Presentations and DHS Recommendations:

1). https://spectrum.ieee.org/static/special-report-puerto-rico-after-the-storm

2). Threats to Pharmaceutical Supply Chains:
https://www.dhs.gov/sites/default/files/publications/508%20-%20AEP%20Pharmaceutical%20Final%20w-DS%200792018.pdf

3). 2017 Hurricane ARRL Report:
http://www.arrl.org/files/file/Public%20Service/ARES/2017%20Hurricane%20Season%20AAR.pdf

**Mapping to GenCyber Cybersecurity First Principles:**

| | | | |
|---|---|---|---|
| ☐ | **Domain Separation** | ☐ | **Abstraction** |
| ☐ | **Process Isolation** | ☐ | **Data Hiding** |
| ☐ | **Resource Encapsulation** | ☐ | **Layering** |
| ☐ | **Modularity** | ☐ | **Simplicity** |
| ☐ | **Least Privilege** | ☐ | **Minimization** |

**Mapping to GenCyber Cybersecurity Concepts:**

| | | | |
|---|---|---|---|
| ☑ | **Defense in Depth** | ☑ | **Availability** |
| ☑ | **Confidentiality** | ☑ | **Think Like an Adversary** |
| ☑ | **Integrity** | ☐ | **Keep It Simple** |

**Assessment of Learning:**

| **TYPE (Examples listed below)** | **NAME/DESCRIPTION** |
|---|---|
| Quiz/Test<br>Presentation<br>Project<br>Writing Assignment<br>Observation<br>Walk Around<br>Oral Questioning<br>Other | A number of assessment approaches will be adopted:<br><br>1). Presentation of multiple cybersecurity and natural disaster scenarios<br><br>2). Oral questions and walking around<br><br>3). Q & A online and answer discussions |

**Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)**

| |
|---|
| N/A |

**Describe any Extension Activities (i.e., ideas for further work):**

1) Join & Participate:

** Indiana County Emergency Management **

FCC Training & License Testing: https://www.qsl.net/w3bmd/

Contact: N3QM, Bill McMillen, 724-397-2702, wkmcmillen@gmail.com

*********NOTE: YOU can help your local community!

**Acknowledgements:**

# Lesson Plan*

**LESSON TITLE:** Finding Hidden Treasure (Programming with Alice) - Part 1

**SUMMARY:**

This activity will teach and/or build the students knowledge of programming concepts. Through building an Alice world students will find a way to defend their hidden treasure by layering, camouflage, and interactive events.

**GRADE BAND:**

- [ ] K-2
- [x] 6-8
- [ ] 3-5
- [ ] High School

**TIME REQUIRED:** 100 minutes

**LESSON LEARNING OUTCOMES: Upon completion of this lesson, students will be able to:**

**Outcome Examples**

| | |
|---|---|
| Design/Build<br>Test/Defend<br>Compare/Contrast<br>Apply/Use<br>Explain/Discuss<br>Identify/Describe | Students will learn to Design/Build with Alice.<br>Students will Apply/Use their programming skills through the Alice platform reinforcing or learning programming concepts of conditionals, loops, events, and logical sequencing.<br>Students will design an in depth defense of their treasure to assure security. |

**Materials List (i.e., string, digital diary, raspberry pi, web link, drone):**

Two pocket folders
Scene Design handout

**Describe any Previous Knowledge that may be Required:**

Previous programming skills would be beneficial but not mandatory.

**How will you facilitate the learning?**

- Describe the Warm-up Activity:

Video clip on finding Hidden Treasure

Start a discussion
If you have treasure how would you hide it so no one else could find it?

- Describe the Focused Activity:

The focused activity on Day 1 is on the design and building of the scene(s) in the world where the treasure will be hidden.

Prior to design students will have the opportunity to search through Alice to find out what they have available in the object classes to work with in their design choice.

- Describe the Teacher Instruction:

Instruction through slide presentation in order to teach Alice

How to add objects
How to add methods
How to utilize events

**Mapping to GenCyber Cybersecurity First Principles:**

| | | | |
|---|---|---|---|
| ☐ | Domain Separation | ☐ | Abstraction |
| ☐ | Process Isolation | ☐ | Data Hiding |
| ☐ | Resource Encapsulation | ☐ | Layering |
| ☐ | Modularity | ☐ | Simplicity |
| ☐ | Least Privilege | ☐ | Minimization |

**Mapping to GenCyber Cybersecurity Concepts:**

| | | | |
|---|---|---|---|
| ☑ | Defense in Depth | ☐ | Availability |
| ☐ | Confidentiality | ☑ | Think Like an Adversary |
| ☐ | Integrity | ☑ | Keep It Simple |

**Assessment of Learning:**

| TYPE (Examples listed below) | NAME/DESCRIPTION |
|---|---|
| Quiz/Test<br>Presentation<br>Project<br>Writing Assignment<br>Observation<br>Walk Around<br>Oral Questioning<br>Other | Walk around<br>Observation |

**Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)**

Accommodations will be provided if needed.

**Describe any Extension Activities (i.e., ideas for further work):**

**Acknowledgements:**

Alice is a CMU produced coding environment and all details can be seen at alice.org

# Lesson Plan*

**LESSON TITLE:** Finding Hidden Treasure (Programming with Alice) - Part 2

**SUMMARY:**

In this activity students will continue to use and build on their knowledge of programming concepts. Students will continue and complete building their 3D Alice world for finding their hidden treasure

**GRADE BAND:**

- [ ] K-2
- [x] 6-8
- [ ] 3-5
- [ ] High School

**TIME REQUIRED:**

100 minutes

**LESSON LEARNING OUTCOMES: Upon completion of this lesson, students will be able to:**

**Outcome Examples**

| | |
|---|---|
| Design/Build<br>Test/Defend<br>Compare/Contrast<br>Apply/Use<br>Explain/Discuss<br>Identify/Describe | Students will complete their individual 3D worlds in Alice.<br>Students will be prepared to present their worlds and explain the depth of defense of their design. |

**Materials List (i.e., string, digital diary, raspberry pi, web link, drone):**

N/A

**Describe any Previous Knowledge that may be Required:**

Students will have completed the Finding Hidden Treasure - Part 1

**How will you facilitate the learning?**

- Describe the Warm-up Activity:

Reinforcement of the presentation from Day 1 will be presented if needed.

Teach will answer questions and aid in student growth in Alice environment.

- Describe the Focused Activity:

The focused activity for Day 2 will be for the students to complete their projects. They will have defended their hidden treasure through interactive events in their Alice World.

- Describe the Teacher Instruction:

Instruction will be through:
Reinforcing the information provided in Day 1.
Aiding students in questions regarding their defense.

**Mapping to GenCyber Cybersecurity First Principles:**

| | | | |
|---|---|---|---|
| ☐ | Domain Separation | ☐ | Abstraction |
| ☐ | Process Isolation | ☐ | Data Hiding |
| ☐ | Resource Encapsulation | ☐ | Layering |
| ☐ | Modularity | ☐ | Simplicity |
| ☐ | Least Privilege | ☐ | Minimization |

**Mapping to GenCyber Cybersecurity Concepts:**

| | | | |
|---|---|---|---|
| ☑ | Defense in Depth | ☐ | Availability |
| ☐ | Confidentiality | ☑ | Think Like an Adversary |
| ☐ | Integrity | ☑ | Keep It Simple |

**Assessment of Learning:**

| TYPE (Examples listed below) | NAME/DESCRIPTION |
|---|---|
| Quiz/Test<br>Presentation<br>Project<br>Writing Assignment<br>Observation<br>Walk Around<br>Oral Questioning<br>Other | Project<br>Presentation |

**Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)**

Accommodations will be provided if needed for visually impaired students or students who may need reading accommodations.

**Describe any Extension Activities (i.e., ideas for further work):**

Students can download Alice 2.5 from alice.org and continue to explore and utilize the environment to enhance their programming skills.

**Acknowledgements:**

Alice is a product developed by Carnegie Mellon University, Pittsburgh, PA

All information can be obtained at alice.org.

# Lesson Plan*

**LESSON TITLE:** Talk the Talk - Getting to Know the GenCyber Cybersecurity Concepts

**SUMMARY:**

In a variety of ways, students will interact with the cybersecurity concepts and vocabulary needed to be successful throughout the week of camp. Individual challenges, partner activities, group games and the creation of posters and videos (given time) will be used to make meaningful connections between the concepts and students' experiences.

**GRADE BAND:**

- ☐ K-2
- ☐ 3-5
- ☑ 6-8
- ☑ High School

**TIME REQUIRED:**

100 minutes

**LESSON LEARNING OUTCOMES: Upon completion of this lesson, students will be able to:**

**Outcome Examples**

| | |
|---|---|
| Design/Build<br>Test/Defend<br>Compare/Contrast<br>Apply/Use<br>Explain/Discuss<br>Identify/Describe | Identify the six GenCyber Cybersecurity Concepts<br>Discuss and provide examples of instances which apply the cybersecurity concepts.<br>Design creative posters which clearly define the GenCyber Cybersecurity Concepts.<br>Create a video offering information about each cybersecurity concept and utilizing the poster as an aid (given time) |

**Materials List (i.e., string, digital diary, raspberry pi, web link, drone):**

Instructional computer, as well as individual computers for students or cellphones
Guided notes
Prepared online learning tools (Quizizz, Quizlet, Gimkit, Flipgrid)
Posterboard
Markers
Masking Tape
Gmail accounts for each learner

**Describe any Previous Knowledge that may be Required:**

None

**How will you facilitate the learning?**

- Describe the Warm-up Activity:

Hook: Cute Facebook video of language barriers

Guided Notes: Define Six Cybersecurity Concepts explicitly. Provide examples.

- Describe the Focused Activity:

FIRST 50 MINUTES: Students will master the 6 Cybersecurity Concepts in a variety of games and reflective discussion

SECOND 50 MINUTES: Students will apply the 6 Cybersecurity Concepts in the creation of a poster to decorate camp with and in a Flipgrid video for the IUP GenCyber resources.

- Describe the Teacher Instruction:

FIRST 50 MINUTES:
1) Hook students with a cute video about language barriers.
2) Provide a concrete resource about the six GenCyber cybersecurity concepts via guided notes.
3) Allow for individual reflection with guided notes while completing a Quizizz.
4) Discuss the most missed questions on Quizizz or with any other areas of confusion.
5) Allow for partner communication about the cybersecurity concepts on Quizlet - play "Match."
6) Conduct a competition with the whole group using Gimkit.

SECOND 50 MINUTES:
5) Groups (2-3 students) brainstorm a poster defining and depicting each of the 6 cyber security concepts.

6) Create the poster with the following guidelines: neat, not crowded, clear definition, relevant examples listed, visual application to demonstrate the concept.

7) Create a Flipgrid Video (on cellphones if webcams are unavailable), using the poster as a visual aid.

**Mapping to GenCyber Cybersecurity First Principles:**

| | | | |
|---|---|---|---|
| ☐ | Domain Separation | ☐ | Abstraction |
| ☐ | Process Isolation | ☐ | Data Hiding |
| ☐ | Resource Encapsulation | ☐ | Layering |
| ☐ | Modularity | ☐ | Simplicity |
| ☐ | Least Privilege | ☐ | Minimization |

**Mapping to GenCyber Cybersecurity Concepts:**

| | | | |
|---|---|---|---|
| ☑ | Defense in Depth | ☑ | Availability |
| ☑ | Confidentiality | ☑ | Think Like an Adversary |
| ☑ | Integrity | ☑ | Keep It Simple |

**Assessment of Learning:**

| TYPE (Examples listed below) | NAME/DESCRIPTION |
|---|---|
| Quiz/Test<br>Presentation<br>Project<br>Writing Assignment<br>Observation<br>Walk Around<br>Oral Questioning<br>Other | Quizizz results for individuals (scores)<br>Quizlet results for partners (times)<br>Gimkit results for individuals (scores)<br>Poster content for groups<br>Flipgrid explanations for groups |

**Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)**

Students without Gmail accounts will need to create Gmail accounts for the activities.
Students with visual impairments may need to enlarge text on computer screens.
Students without cellphones or webcams may need to share with others.

Brighter, self-motivated or former campers could also study and apply the 10 GenCyber Cybersecurity Principles and examine their relationships to the 6 Concepts.

**Describe any Extension Activities (i.e., ideas for further work):**

The entire week of camp should contain lessons which continually cause the students to reflect on and apply the six GenCyber Cybersecurity Concepts.

**Acknowledgements:**

GenCyber Cyber-Security Concepts

# Lesson Plan*

**LESSON TITLE:** Unplugged Programming Activity

**SUMMARY:**

Students will utilize given simple movement commands to interact with their peers and direct them using these commands to accomplish simple tasks.

Students will be modeling the Karl activities found in programming to form knowledge on functions and their uses and necessity as a programming concept.

**GRADE BAND:**

- [ ] K-2
- [x] 6-8
- [ ] 3-5
- [ ] High School

**TIME REQUIRED:** 100 minutes

**LESSON LEARNING OUTCOMES: Upon completion of this lesson, students will be able to:**

**Outcome Examples**

| | |
|---|---|
| Design/Build<br>Test/Defend<br>Compare/Contrast<br>Apply/Use<br>Explain/Discuss<br>Identify/Describe | Students will apply/use simple movement commands to direct their peers to complete tasks/activities.<br><br>Students will design/build functions by joining commands in an efficient manner to complete more involved tasks/activities. |

**Materials List (i.e., string, digital diary, raspberry pi, web link, drone):**

Paper for documentation
Pens, pencils, or markers
6 yard sticks
6x6 Grid (teacher provided)
30 Yellow cardboard discs (teacher provided)

**Describe any Previous Knowledge that may be Required:**

No previous knowledge is necessary

**How will you facilitate the learning?**

- Describe the Warm-up Activity:

During introduction to the activity the students will be introcuded to the 6 x 6 grid.

Strudents will be divided into groups of 3(2 if 3 is not feasible) and given supplies.

- Describe the Focused Activity:

To start:
Each group will be given a set of limited movement statements
Move forward
Turn right
Pick up ball

One student in each group will be the moving pawn on the grid
One student will be the secretary to record movements
Student will come up with the smallest amount of commands necessary to have each of the activities completed.

Activity 1:
Starting at the far left lower quadrant move the pawn horizontally through the grid to arrive at the upper right quadrant.
Activity 2:
Students discuss how they can shorten the amount of commands and still produce the same results.
Activity 3:
With the yard stick placed after the 3rd five have the students get commands so that the pawn can go from left to right along the lower row of the grid without going through the yard stick.
See extension activities for additional activities.

- Describe the Teacher Instruction:

Teach will give all students the commands that they are limited to.

Teacher will observe and encourage or instruct groups as needed.

**Mapping to GenCyber Cybersecurity First Principles:**

| | | | |
|---|---|---|---|
| ☐ | Domain Separation | ☐ | Abstraction |
| ☐ | Process Isolation | ☐ | Data Hiding |
| ☐ | Resource Encapsulation | ☐ | Layering |
| ☐ | Modularity | ☐ | Simplicity |
| ☐ | Least Privilege | ☐ | Minimization |

**Mapping to GenCyber Cybersecurity Concepts:**

| | | | |
|---|---|---|---|
| ☐ | Defense in Depth | ☐ | Availability |
| ☐ | Confidentiality | ☐ | Think Like an Adversary |
| ☐ | Integrity | ☑ | Keep It Simple |

**Assessment of Learning:**

| TYPE (Examples listed below) | NAME/DESCRIPTION |
|---|---|
| Quiz/Test<br>Presentation<br>Project<br>Writing Assignment<br>Observation<br>Walk Around<br>Oral Questioning<br>Other | Presentation<br><br>Observation |

**Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)**

Students with physical limitations may not be able to be the pawn in this activity. however, they can work as secretary or with the group to come up with instructions.

**Describe any Extension Activities (i.e., ideas for further work):**

Include functions
- canMoveForward()
- isBallPresent()
- takeBall()

Activity 4:

Using the new functions have the pawn go from the bottom left corner to the top right corner and pick up any ball that is in its way before moving ahead. Pawn should be able to pick up balls when randomly placed on the grid.

Challenge Activity:

Come up with an activity that uses all of the given commands and functions and uses the balls and the yard stick to come up with an additional and unique activity to allow the pawn to do.

**Acknowledgements:**

This activity is based on Karel programming activities based off of Karel: the Robot and educational programming tool designed by Richard E. Pettis.

# Lesson Plan*

**LESSON TITLE:** Data Protection/Cryptography

**SUMMARY:**

1. Learning how to protect sensitive data using encryption
2. Learning a brief history of cryptography (encryption/decryption)
3. Understanding the basic concepts of cryptography
4. Learning several basic cryptographic techniques
5. Hand-on practice on encryption/decryption using on-line tools

**GRADE BAND:**

- ☐ K-2
- ☑ 6-8
- ☐ 3-5
- ☑ High School

**TIME REQUIRED:** 120 minutes

**LESSON LEARNING OUTCOMES: Upon completion of this lesson, students will be able to:**

**Outcome Examples**

| | |
|---|---|
| Design/Build<br>Test/Defend<br>Compare/Contrast<br>Apply/Use<br>Explain/Discuss<br>Identify/Describe | Upon completion of the camp, participants will be able to:<br><br>1. Demonstrate an in-depth understanding of the GenCyber Cybersecurity Concepts.<br>2. Understand cryptographic basics and its role in securing data communications. |

**Materials List (i.e., string, digital diary, raspberry pi, web link, drone):**

Web Links:
1. Navajo Code Talker Died, June 13, 2018:
https://nowthisnews.com/videos/news/one-of-the-last-living-navajo-code-talkers-from-wwii-passed-away
2. Cryptography in 60 Seconds: https://www.youtube.com/watch?v=j5fOynJrNOk
3. Simple Cryptography: https://www.youtube.com/watch?v=ez0AOYl-i4k
4. Cryptography for Kids: https://kids.kiddle.co/Cryptography
5. Caesar cipher decryption tool: https://www.xarg.org/tools/caesar-cipher/ (good)
6. The Black Chamber: https://www.simonsingh.net/The_Black_Chamber/caesar.html

**Describe any Previous Knowledge that may be Required:**

Knowledge of Mathematics: Pre-Algebra, and Algebra

**How will you facilitate the learning?**

- Describe the Warm-up Activity:

1. Explaining the basics of data protection
2. Explaining and discussing the basics of cryptography
3. Brief discussion on the history of cryptography from Egypt to modern time
4. What are encryption and decryption and how they are performed
5. Difference between private and public key cryptography
6. Hand-on practices on various cryptographic techniques using online tools

- Describe the Focused Activity:

Hand-on Practices:
The students are asked to practice on various cryptographic techniques, such as Caesar Cipher, DES, AES, Private-key cryptography, Public-key cryptography using tools available on-line. They will encrypt a message (a plaintext) into cipher text and again decrypt the ciphertext back to the plain text.

Challenge:
For middle school students, easier ciphertext will be provided and asked to decrypt it to the plaintext using brute force technique.

For high school students, relatively harder ciphertext will be provided and asked to decrypt it (if they can) to the plaintext using brute force technique. In addition to that, more exercises will be assigned in this session.

- Describe the Teacher Instruction:

**Mapping to GenCyber Cybersecurity First Principles:**

| | | | |
|---|---|---|---|
| ☐ | Domain Separation | ☐ | Abstraction |
| ☐ | Process Isolation | ☐ | Data Hiding |
| ☐ | Resource Encapsulation | ☐ | Layering |
| ☐ | Modularity | ☐ | Simplicity |
| ☐ | Least Privilege | ☐ | Minimization |

**Mapping to GenCyber Cybersecurity Concepts:**

| | | | |
|---|---|---|---|
| ☑ | Defense in Depth | ☐ | Availability |
| ☑ | Confidentiality | ☑ | Think Like an Adversary |
| ☐ | Integrity | ☐ | Keep It Simple |

**Assessment of Learning:**

| TYPE (Examples listed below) | NAME/DESCRIPTION |
|---|---|
| Quiz/Test<br>Presentation<br>Project<br>Writing Assignment<br>Observation<br>Walk Around<br>Oral Questioning<br>Other | The instructor and TAs made observation while the activity was being performed.<br>The instructor and TAs walked around to observe how different group are performing.<br>The instructor and TAs asked oral questions when needed to ensure the students understood what they were doing and why.<br>The instructor and TAs made sure all group members were engaged in the activities.<br>The students were asked to present their final results. |

**Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)**

| |
|---|
| N/A |

**Describe any Extension Activities (i.e., ideas for further work):**

Activities could be extended to include more examples on decryption if students became more curious.

**Acknowledgements:**

N/A

# Lesson Plan*

**LESSON TITLE:** How to Secure Networks – Examples and Demos

**SUMMARY:**

This module will illustrate several examples of attacks on computer networks and the mechanisms used to secure networks. Specifically, we will show the attacks that compromise data confidentiality and integrity, including the man-in-the-middle attacks and Phishing attacks, and the countermeasures against these attacks.

The module will include presentation and instructions for explanation of these attacks and security mechanisms, being followed by hands-on activities to be completed by students.

**GRADE BAND:**

- [ ] K-2
- [x] 6-8
- [ ] 3-5
- [ ] High School

**TIME REQUIRED:** 120 minutes

**LESSON LEARNING OUTCOMES: Upon completion of this lesson, students will be able to:**

**Outcome Examples**

| | |
|---|---|
| Design/Build<br>Test/Defend<br>Compare/Contrast<br>Apply/Use<br>Explain/Discuss<br>Identify/Describe | Understand the man-in-the-middle attack that compromises confidentiality and integrity and phishing attack;<br>Understand basic encryption techniques against the confidentiality compromise;<br>Understand basic techniques of message authentication against integrity compromise;<br>Understand basic countermeasures against phishing attacks. |

**Materials List (i.e., string, digital diary, raspberry pi, web link, drone):**

Module presentation materials prepared by the instructor;
CrypTool, an open-source educational software (https://www.cryptool.org/de/jcryptool);
Hands-on activity manual (prepared by the instructor);
A couple of YouTube on Internet and two-factor authentication
https://www.youtube.com/watch?v=ewrBalT_eBM
http://www.youtube.com/watch?v=r3EK6JYIvHE

**Describe any Previous Knowledge that may be Required:**

Basic skills of using computers to run simple software

**How will you facilitate the learning?**

- Describe the Warm-up Activity:

The warm-up activity includes the following:
First show a demo on how networks work;
The instructor will then explain how to use CrypTool to conduct encryption and create message digests, and how to "attack" (that is, cryptographically analyze) ciphers and hash functions.
(Then, students will be able to complete the designed activities individually and in a small team of 2 students).

- Describe the Focused Activity:

The focused activity is designed to suit students in years 6-8, including the following tasks:

To complete hands-on tasks including operating encryption using various ciphers and cryptanalysis of well-known ciphers. These hands-on activities will be conducted using CrypTool. These would enhance students' understanding of countermeasures against compromise of confidentiality (the man-in-the-middle attacks);

To complete activities for message digest creation using hash algorithms and vulnerability analysis of hash algorithms. These would help students understand the security mechanisms against integrity compromise;

To complete hands-on activities for email authentication using digital signature. These help students understand the countermeasures against phishing attacks.

- Describe the Teacher Instruction:

The instructor will explain several attacks on computer networks, including confidentiality compromise, integrity compromise, and phishing attack. Also, the well-known security mechanisms against these threats will be explained.

For example, regarding phishing attack, the instructor will first explain what is phishing attack, and show several examples of phishing attacks. Then, two types of countermeasures against phishing attacks will be explained, that is, two-factor authentication and email authentication through digital signature. These instructions are followed by a demo/video on two-factor authentication and hands-on activities on digital signature creation and verification.

**Mapping to GenCyber Cybersecurity First Principles:**

| | | | |
|---|---|---|---|
| ☐ | Domain Separation | ☐ | Abstraction |
| ☐ | Process Isolation | ☐ | Data Hiding |
| ☐ | Resource Encapsulation | ☐ | Layering |
| ☐ | Modularity | ☐ | Simplicity |
| ☐ | Least Privilege | ☐ | Minimization |

**Mapping to GenCyber Cybersecurity Concepts:**

| | | | |
|---|---|---|---|
| ☐ | Defense in Depth | ☐ | Availability |
| ☑ | Confidentiality | ☑ | Think Like an Adversary |
| ☑ | Integrity | ☐ | Keep It Simple |

**Assessment of Learning:**

| TYPE (Examples listed below) | NAME/DESCRIPTION |
|---|---|
| Quiz/Test<br>Presentation<br>Project<br>Writing Assignment<br>Observation<br>Walk Around<br>Oral Questioning<br>Other | Observation:<br>The hands-on activities are provided for students to complete individually or in a team of 2 students. The instructor will observe the progresses made by students, assess their understanding and provide further instructions if necessary.<br><br>Presentation and Oral Questioning:<br>During the hands-on activities, students will be asked questions that are pre-designed; they are expected to correctly answer the questions after successfully complete certain steps of the hands-on activities. |

**Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)**

Many of the learning contents are supported by pictures/diagrams or multimedia materials. For students who need any extra instructions, the instructor would try to provide individual help.

**Describe any Extension Activities (i.e., ideas for further work):**

The instructions and hands-on activities are designed to suit students in years 6-8. Further work for this module can be an extended coverage of more network threats and corresponding countermeasures, depending on students' background.

**Acknowledgements:**

# Lesson Plan*

**LESSON TITLE:** Internet of Things (IoT) Security/Monitoring

**SUMMARY:**

This module will discuss IoT devices, it's User Service Platform (USP) and Sensors. Participants will be familiarized with the concept of IoT, learning how these systems can be controlled from just about anywhere on the globe using the Internet. Specifically, this IoT Device Simulation module will introduce the students to the IBM's Bluemix platform using the Watson IoT platform, a Cloudant noSQL database, and Node-RED to create a flow which captures simulated sensor data which can then be manipulated, visualized, and stored in a database.

**GRADE BAND:**

- ☐ K-2
- ☐ 3-5
- ☑ 6-8
- ☑ High School

**TIME REQUIRED:**

120 minutes

**LESSON LEARNING OUTCOMES: Upon completion of this lesson, students will be able to:**

**Outcome Examples**

| | |
|---|---|
| Design/Build<br>Test/Defend<br>Compare/Contrast<br>Apply/Use<br>Explain/Discuss<br>Identify/Describe | Develop an understanding of embedded devices and the Internet of Things.<br>Design Node-RED based flows<br>Use simulated devices within the flows and visualize sensor data |

**Materials List (i.e., string, digital diary, raspberry pi, web link, drone):**

IBM Bluemix
CloudFoundry Command Line Interface (CLI)

**Describe any Previous Knowledge that may be Required:**

Basic knowledge of JavaScript/Node.js would be helpful but is not required.

**How will you facilitate the learning?**

- Describe the Warm-up Activity:

The warm up activity will involve setting up users with an IBM Bluemix account and showing how to login to the Bluemix API using the CloudFoundry Command Line Interface (CLI). Students will then push and provision their workspaces to their individual accounts and shown the basics of Node-RED's functionality and the Watson IoT dashboard.

- Describe the Focused Activity:

The focus activity will involve the simulation of a device which contains sensor data which can be extracted and fed to the Node-RED platform. The students will then create a Node-RED flow using various nodes in order to manipulate the extracted data which allows for visualization, storing the data in a noSQL database, as well as creating event driven functions based on changes in the sensor data. The visualization of the data will be done by creating a Node-RED dashboard which takes the sensor data as input and creates a time based line graph. Each of the nodes within the flow will be programmed using JavaScript to extract sensor information, collect data, perform actions based on changes in the sensor data, and output the data to a Node-RED dashboard and a noSQL database.

Moreover, students will be taught step-by-step how to create an IBM Bluemix account and use the CloudFoundry CLI in order to provision their workspace with the Watson IoT platform and Node-RED. The instructor will then show the students the basics of both platforms, focusing especially on the functionality of Node-RED and how the nodes function and can be manipulated between each other. The instructor will follow along with the students in how to create the flow, simulated sensor device, and use the Watson IoT Dashboard and Cloudant noSQL database.

- Describe the Teacher Instruction:

N/A

**Mapping to GenCyber Cybersecurity First Principles:**

| | | | |
|---|---|---|---|
| ☐ | Domain Separation | ☐ | Abstraction |
| ☐ | Process Isolation | ☐ | Data Hiding |
| ☐ | Resource Encapsulation | ☐ | Layering |
| ☐ | Modularity | ☐ | Simplicity |
| ☐ | Least Privilege | ☐ | Minimization |

**Mapping to GenCyber Cybersecurity Concepts:**

| | | | |
|---|---|---|---|
| ☑ | Defense in Depth | ☑ | Availability |
| ☑ | Confidentiality | ☐ | Think Like an Adversary |
| ☐ | Integrity | ☑ | Keep It Simple |

**Assessment of Learning:**

| TYPE (Examples listed below) | NAME/DESCRIPTION |
|---|---|
| Quiz/Test<br>Presentation<br>Project<br>Writing Assignment<br>Observation<br>Walk Around<br>Oral Questioning<br>Other | The assessment of learning will be a project in which the students will create and provision their Watson IoT platform and Node-RED implementation. |

**Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)**

| |
|---|
| N/A |

**Describe any Extension Activities (i.e., ideas for further work):**

Extension activies could include showing students how to further extend their implementations/flows to be used with real world sensors/actuators such as Raspberry PIs which would allow students to collect real-world data or use Node-RED to automate IoT functions.

**Acknowledgements:**

Acknowledgements to IBM, the Cloud Foundry Foundation, the Node.js foundation, and Node-RED.

# Lesson Plan*

**LESSON TITLE:** Personal Cybersecurity Practices - Mrs. Gentile Tuesday 6/25/19 - Middle School

**SUMMARY:**

Students will explore personal computing practices which help to protect them in their online work and play. With so many areas to cover, students will be given the task of becoming experts in one practice in particular, and then share what they learned on a poster.

**GRADE BAND:**

- ☐ K-2
- ☐ 3-5
- ☑ 6-8
- ☐ High School

**TIME REQUIRED:**

100 minutes

**LESSON LEARNING OUTCOMES: Upon completion of this lesson, students will be able to:**

**Outcome Examples**

| | |
|---|---|
| Design/Build<br>Test/Defend<br>Compare/Contrast<br>Apply/Use<br>Explain/Discuss<br>Identify/Describe | identify personal methods of ensuring cybersecurity in work and play,<br>discuss such methods within the class, and<br>design a poster which details student learning. |

**Materials List (i.e., string, digital diary, raspberry pi, web link, drone):**

Post-it Notes
Computers and specific websites
Guided Notepage
Posterboard - cut into fourths
Markers
Masking tape

**Describe any Previous Knowledge that may be Required:**

Experience with computers, video games and social media would be helpful.

**How will you facilitate the learning?**

- Describe the Warm-up Activity:

Hook: Have students place 3 post-it notes on the board where certain personal cybersecurity topics are given to indicate in which topics they could offer any advice. Encourage a brief discussion to discover what they know or what topics I may have missed.

- Describe the Focused Activity:

FIRST 50 MINUTES:
Students will choose one topic off the board related to personal cybersecurity which they will research.

SECOND 50 MINUTES:
Students will create a small poster highlighting an important personal cybersecurity measure everyone should know. These posters will immediately be displayed in the hallways around camp.

- Describe the Teacher Instruction:

1) Provide the hook: As students enter the room, ask them to place their names on three post-it notes which they will place on the board under topics about which they feel they know something. Complete a brief follow-up discussion as described above.

2) Have students choose a topic that doesn't have any or many post-it notes under it. From a list of suggested resources, students will explore the games, videos, images which describe a particular personal cybersecurity tip or application, or they may find information on their own. As they learn, each of them will complete a guided notesheet, which expects them to also consider which of the six cybersecurity concepts are most applied in their topics.

3) Students will be given a 1/4 of a posterboard on which to neatly, creatively post the advice they researched. At the bottom, they will indicate which GenCyber Cybersecurity Concept is applied in their advice.

4) In conclusion, ask students to name a practice students have never considered before. Also ask students for questions they may have, which others could answer, using my own questions as needed for encouragement.

**Mapping to GenCyber Cybersecurity First Principles:**

| | | | |
|---|---|---|---|
| ☐ | Domain Separation | ☐ | Abstraction |
| ☐ | Process Isolation | ☐ | Data Hiding |
| ☐ | Resource Encapsulation | ☐ | Layering |
| ☐ | Modularity | ☐ | Simplicity |
| ☐ | Least Privilege | ☐ | Minimization |

**Mapping to GenCyber Cybersecurity Concepts:**

| | | | |
|---|---|---|---|
| ☑ | Defense in Depth | ☑ | Availability |
| ☑ | Confidentiality | ☑ | Think Like an Adversary |
| ☑ | Integrity | ☐ | Keep It Simple |

**Assessment of Learning:**

| TYPE (Examples listed below) | NAME/DESCRIPTION |
|---|---|
| Quiz/Test<br>Presentation<br>Project<br>Writing Assignment<br>Observation<br>Walk Around<br>Oral Questioning<br>Other | Students' guided notetaking sheets are complete and reflect understanding of the vocabulary and cybersecurity issues in their chosen topics.<br><br>Posters depict clear, sound advice and are labeled with a related GenCyber Cybersecurity Concept. |

**Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)**

Students with visual impairments may need to enlarge text on computer screens.

Brighter, self-motivated or former campers could also study and apply the 10 GenCyber Cybersecurity Principles and examine their relationships to the 6 Concepts in their personal cybersecurity topics.

**Describe any Extension Activities (i.e., ideas for further work):**

The entire week of camp should contain lessons which continually cause the students to reflect on and apply the six GenCyber Cybersecurity Concepts to their own personal computing, gaming and use of social media.

**Acknowledgements:**

pbslearningmedia.org/resource

# Joe Jesson's Workshop

**Title:** Can Students Help When the Grid Fails?

**Description:**
This workshop introduces students to meaningful Cybersecurity projects which will contribute to student knowledge and skill sets which will educate and prepare the students for a power grid or communications failure (terrorist or natural disaster attack). Imagine if your local power grid and cellphone failed and you were left standing in the dark and isolated without telephone or Internet access?

This workshop provides answers and offers communications preparation resources and solutions. Prepared and FCC-licensed students saved lives and quickly helped police and emergency communications. Students were using hand-held communications equipment to help the police!

**Bio:**
Joseph Jesson has 25+ years in the embedded wireless system, Telemetry, Telematics, M2M, and the Internet of things (IoT) space. Joe is currently the Chair of the Princeton IEEE Life Group and CEO of RFSigint, a wireless & IoT patent/IP portfolio analystics company. Joe has held the Chief Technology Officer (CTO) position at General Electric, where he was awarded the GE Edison Award in 2007. Currently, he is Adjunct Professor at The College of New Jersey (since 2013) and teaches Digital Design, Circuit and Electronics Lab, Embedded Systems and Embedded Labs, Control Theory and Controls Lab, etc. Joe has held CTO positions at Able Devices, Assurenet, Software and Systems Architecture positions at Amoco/ BP, Product Manager at OAK Technology, and staff engineering positions at Motorola and The University of Chicago. Joe has a Master's degree from DePaul University in Chicago and is currently working on his PhD dissertation at NJCU in Jersey City, NJ.

# Tommy Chin's Talk

**Title:** From Concepts to Practicality: The Impacts of Neglecting Security Practices

**Description:**
Today's world often reinforces the concepts of cyber hygiene and security awareness through methods such as instructional PowerPoint slides, posters, and email. A concern of the existing security awareness efforts is that they lack an explanation of the consequences for not following these rules and recommendations. This presentation provides an overview of some of the impacts of neglecting security practices and demonstrates a series of offensive security (hacking) tools.

**Bio:**
Tommy Chin is a Security Researcher at GRIMM and focuses his background in networking, machine learning, moving target defenses, and target tracking. He holds several awards, certifications, and degrees. Tommy serves as a publication reviewer for several publishers such as IEEE, Elsevier, and John Wiley & Sons.

# Major Infrastructure Power and Communications Cyber Risks

IUP GENCYBER 2019 CAMP

ADJUNCT PROF JOE JESSON
jessonj@tcnj.edu
jejesson4@gmail.com

# Cyber Security Risks – Communications Risks

## COMMUNICATIONS WORKSHOP OUTLINE

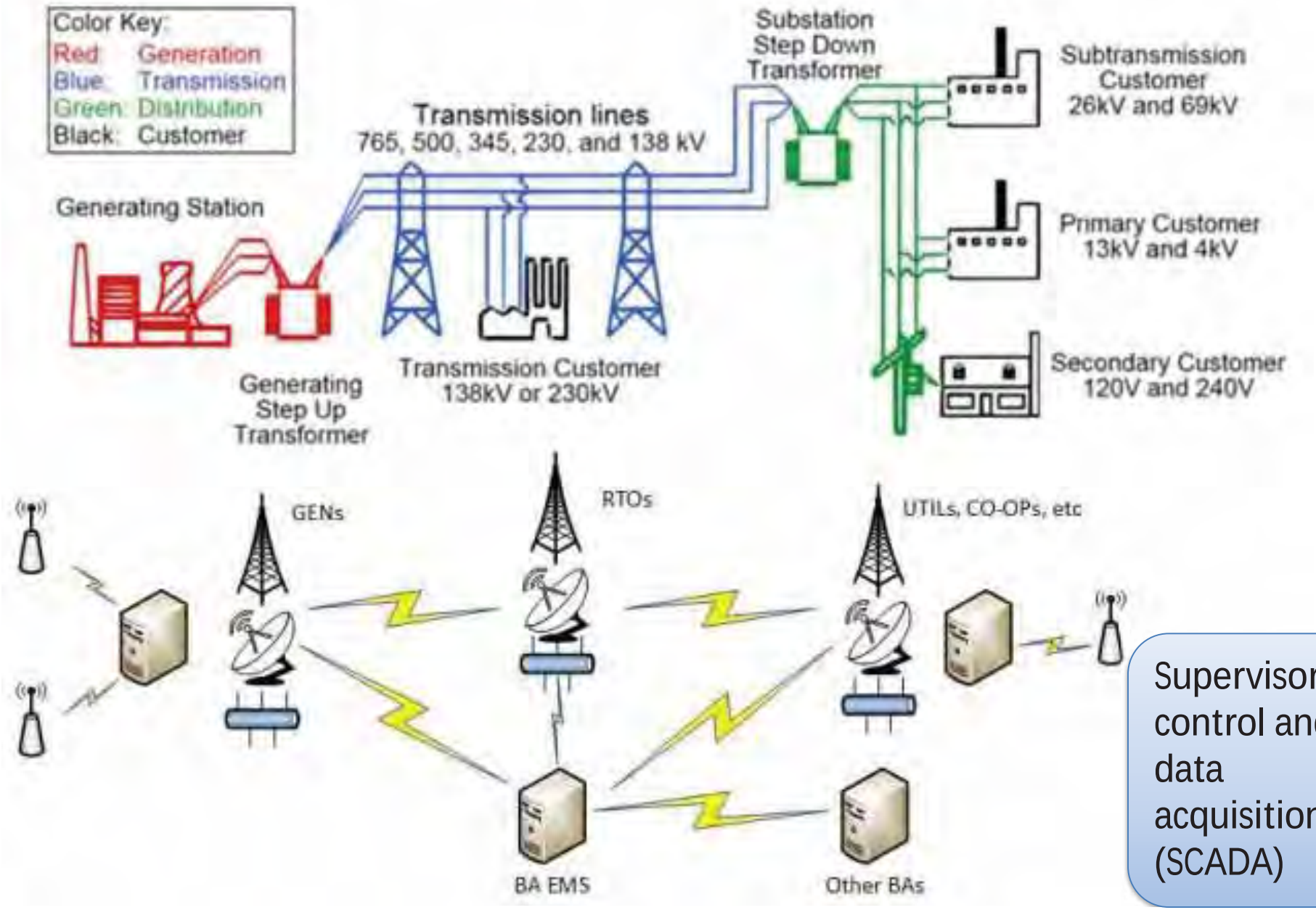
1) **POWER GRID RISKS**
   - Terrorist Attacks on the Grid/Transformers
   - Hacking Supervisory Control and Data acquisition (SCADA)
   - Nuclear-Induced Electromagnetic Pulse (EMP)
   - Corona Mass Ejection – The Carrington Event
2) **COMMUNICATIONS DURING A DISASTER**
   - Amateur Radio
   - Military / FEMA Communication
   - UAS AT&T Base Station
   - Google Balloon LTE Base Station
3) **HANDS-ON FCC LICENSE & DISASTER MANAGEMENT**
   - Getting Started - Online FCC License Learning Module
4) **HANDS-ON SPECTRUM MONITORING**
   - Monitor International Spectrum!
5) **WHY IS DATA ENCRYPTION CRITICAL TODAY?**
   - Aircraft Communications
   - Man-in-The-Middle Attack

# A POWER GRID DIRECT PHYSICAL TERRORIST ATTACK

# A POWER GRID DIRECT PHYSICAL TERRORIST ATTACK


Gunfire from semiautomatic weapons did extensive damage to 17 transformers 2013 attack on an electric substation near San Jose that nearly knocked out Silicon Valley. power supply that sent grid operators scrambling to avoid a blackout

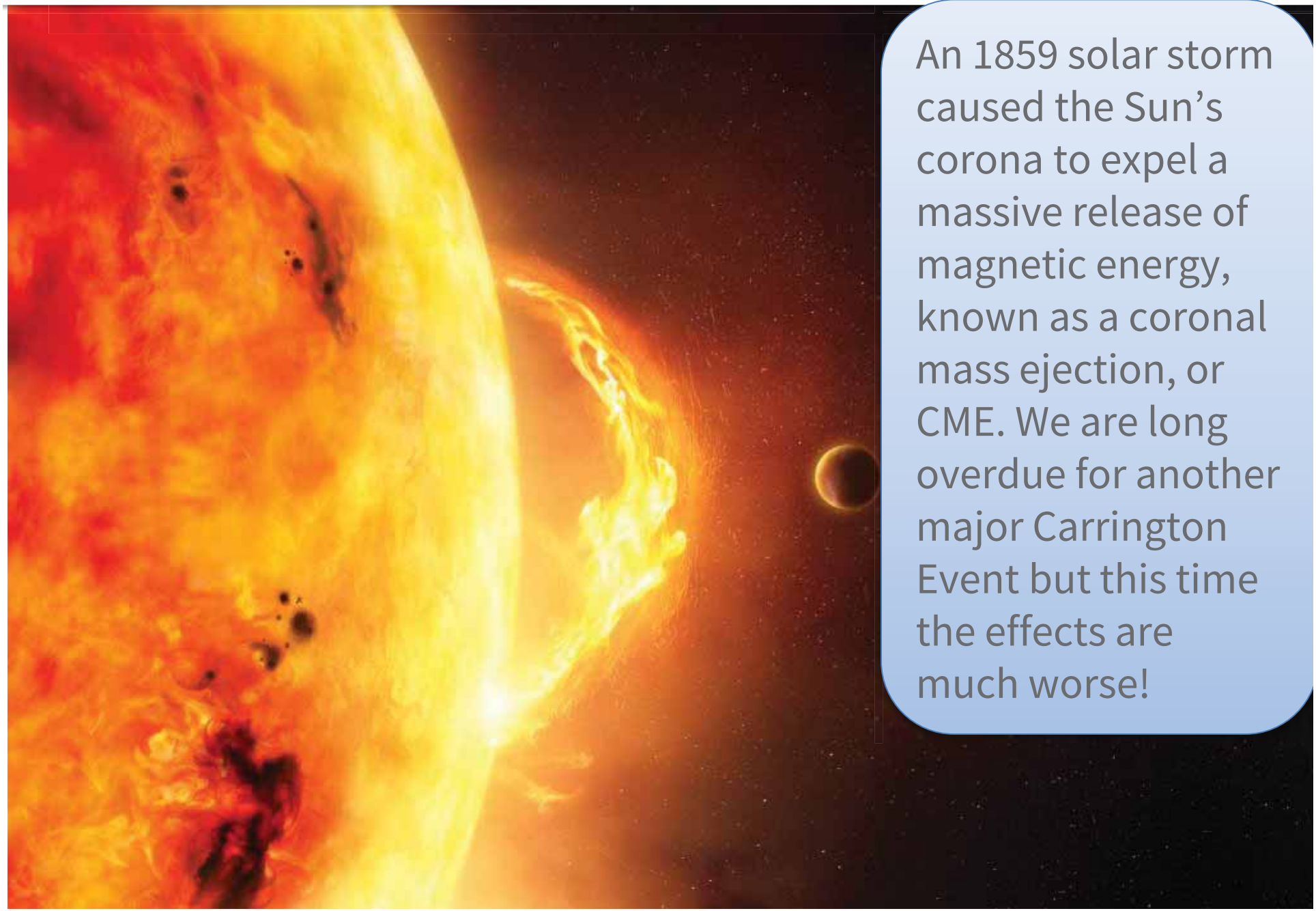
# A POWER GRID CONTROL NETWORK SCADA ATTACK




Supervisory control and data acquisition (SCADA)

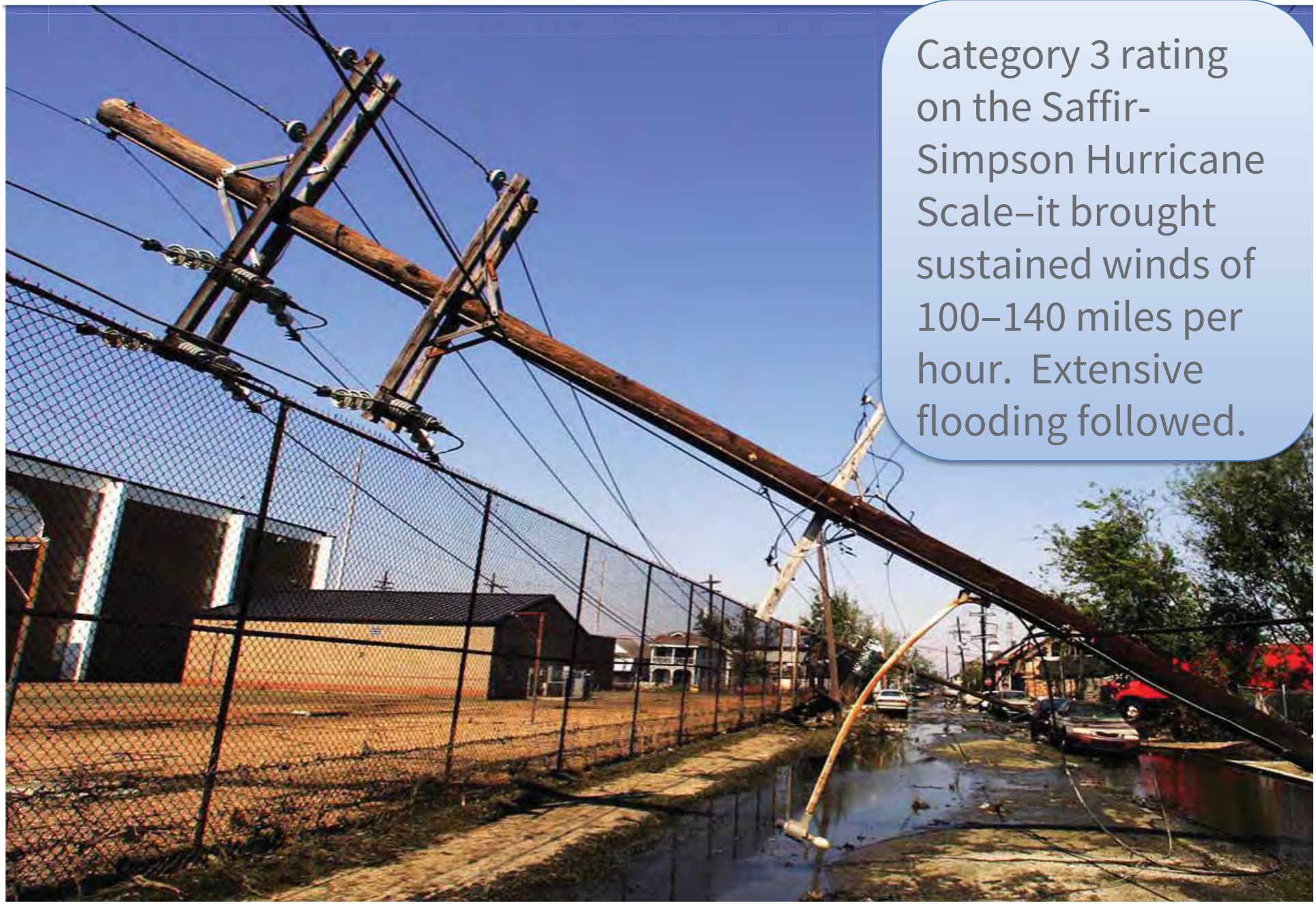
# NUCLEAR BOMB – ELECTROMAGNETIC PULSE (EMP)

# CORONA MASS EJECTION – THE CARRINGTON EVENT



An 1859 solar storm caused the Sun's corona to expel a massive release of magnetic energy, known as a coronal mass ejection, or CME. We are long overdue for another major Carrington Event but this time the effects are much worse!

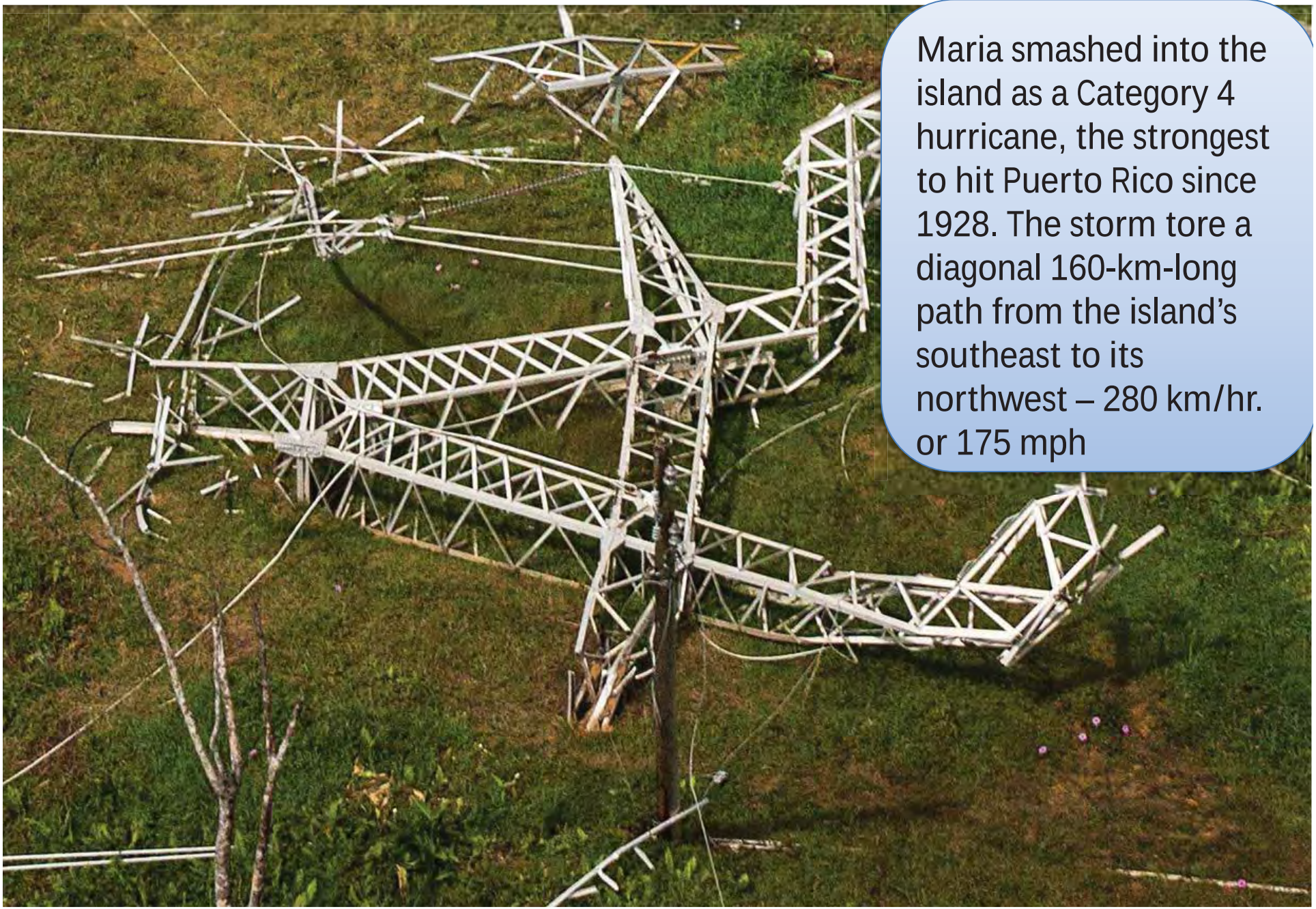
# HURRICANE KATRINA – 2005 CATEGORY 3 & FLOODING



Category 3 rating on the Saffir-Simpson Hurricane Scale–it brought sustained winds of 100–140 miles per hour. Extensive flooding followed.

# HURRICANE MARIA – 2017 CATEGORY 4 & AGING GRID

# HURRICANE MARIA – 2017 CATEGORY 4 & AGING GRID



Maria smashed into the island as a Category 4 hurricane, the strongest to hit Puerto Rico since 1928. The storm tore a diagonal 160-km-long path from the island's southeast to its northwest – 280 km/hr. or 175 mph

# HURRICANE MARIA – AMATEUR RADIO COMMUNICATIONS


Direct HF Amateur Radio
Global Communications

# HURRICANE MARIA – AMATEUR RADIO COMMUNICATIONS

Solar powered (PV) portable amateur radio system. Does not need the power grid or the cellular communications network! From Dominica.

# HURRICANE MARIA – AMATEUR RADIO COMMUNICATIONS

OFF-GRID, OFF-NETWORK SOLAR or GENERATOR-POWERED SYSTEM

COOPER HOSPITAL, WORLD-WIDE REACH!

Readiness | Response | Recovery


## Command-Runner™

### Portable Communication & Command System

The Command-Runner™ provides a customizable, mobile platform for command, communications, data and incident management. The secure, weather resistant enclosure can be configured with radios, VoIP, Wi-Fi, computers, monitors, cameras, printers, drawers and charging ports to support nearly any type of field operation.

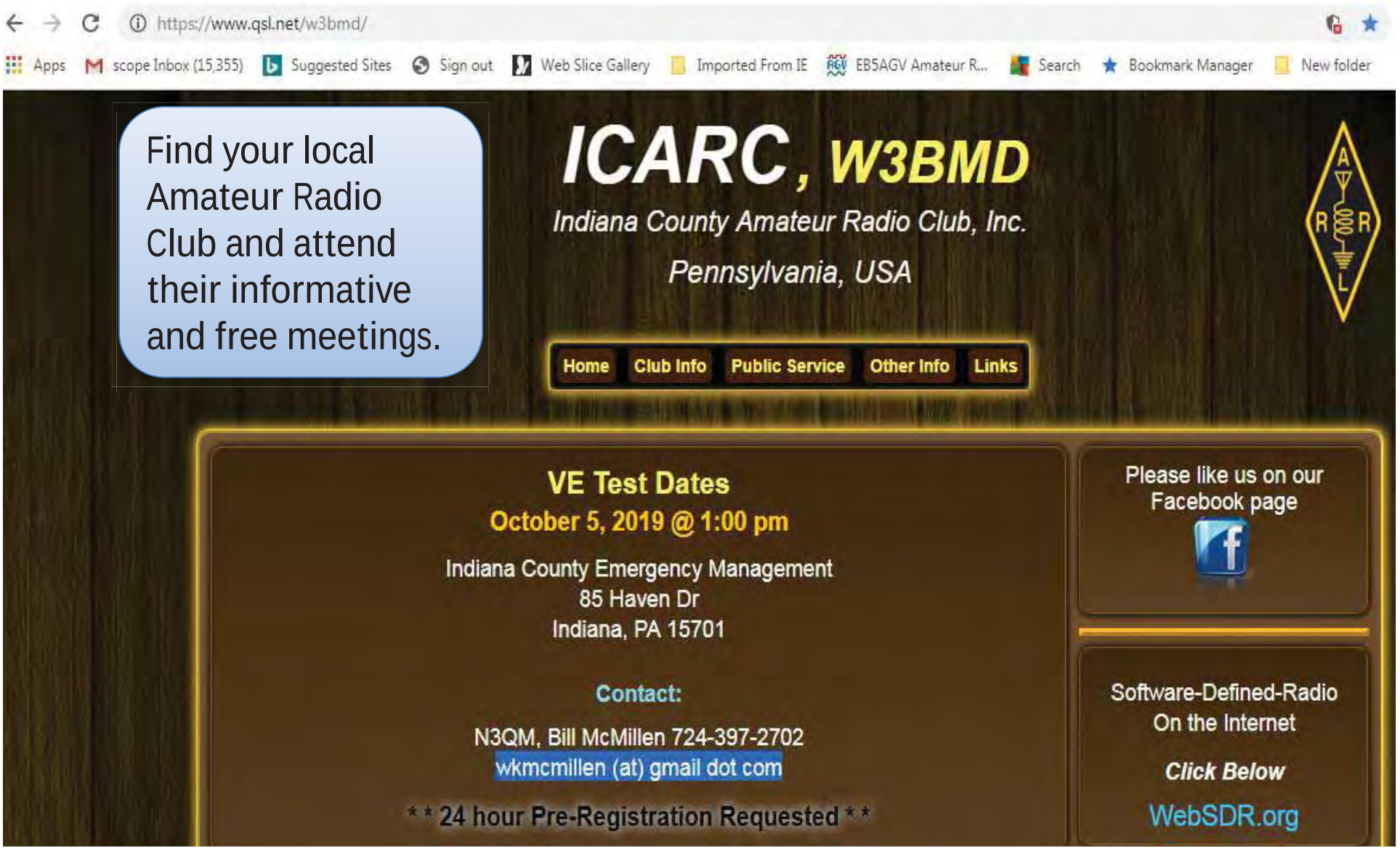
The unit rolls like a cart, then easily mounts to any vehicle's 2" trailer hitch where it rides, wheels up, like a cargo carrier. A single person can transport and deploy an all-in-one command center in minutes.

# EMERGENCY COMMUNICATIONS – HURRICANE MARIA STRUCK DOMINICA @ 175 mph, CAT 5

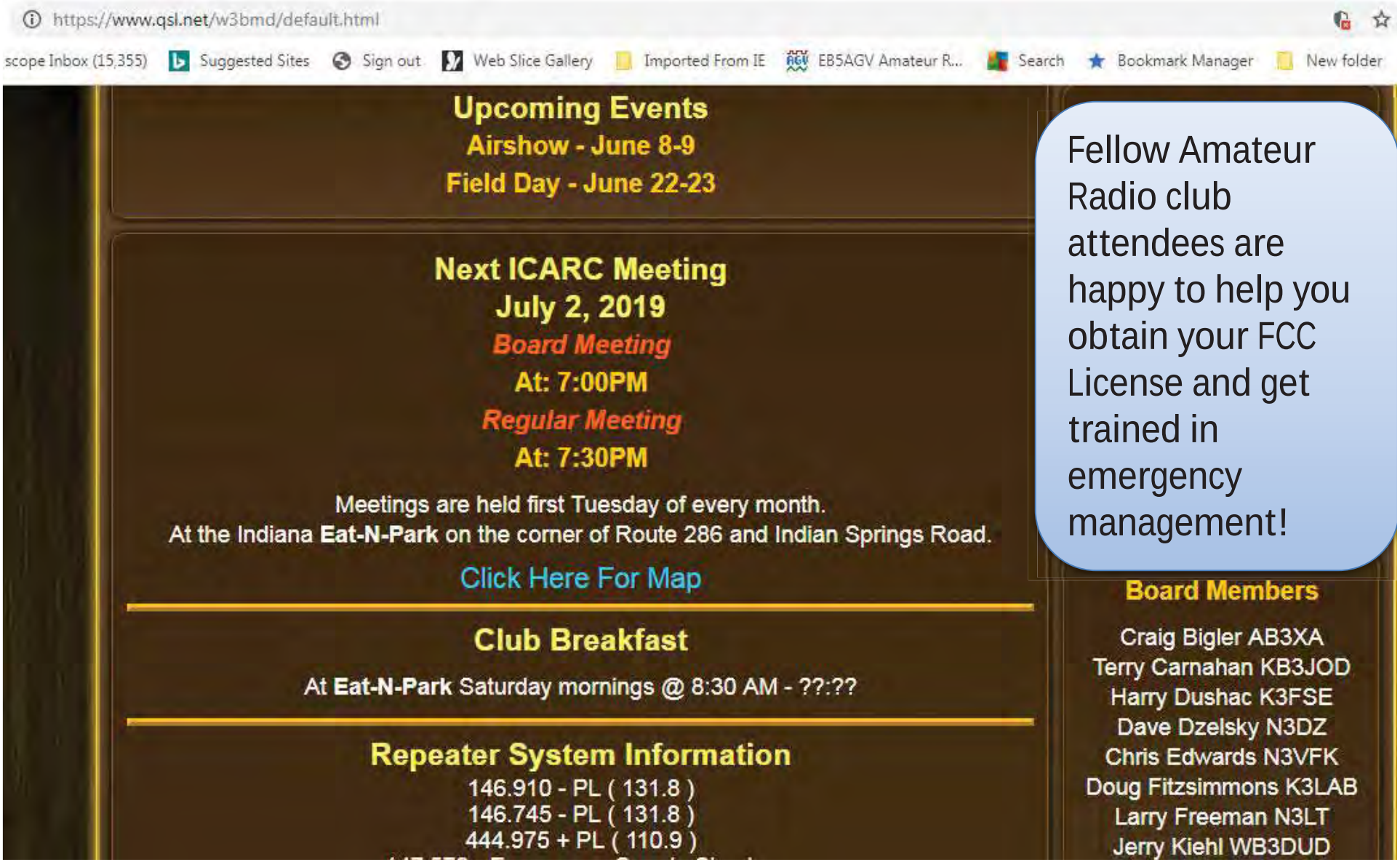

**Amateur radio** operators were in touch with other amateur radio operators from the very first day, 9/20, and continues to this day.

When cellphones and all forms of standard communication fails, amateur radio will get through. Coverage of several thousand miles is not unusual and can provide a resilient and effective mean of two-way communications

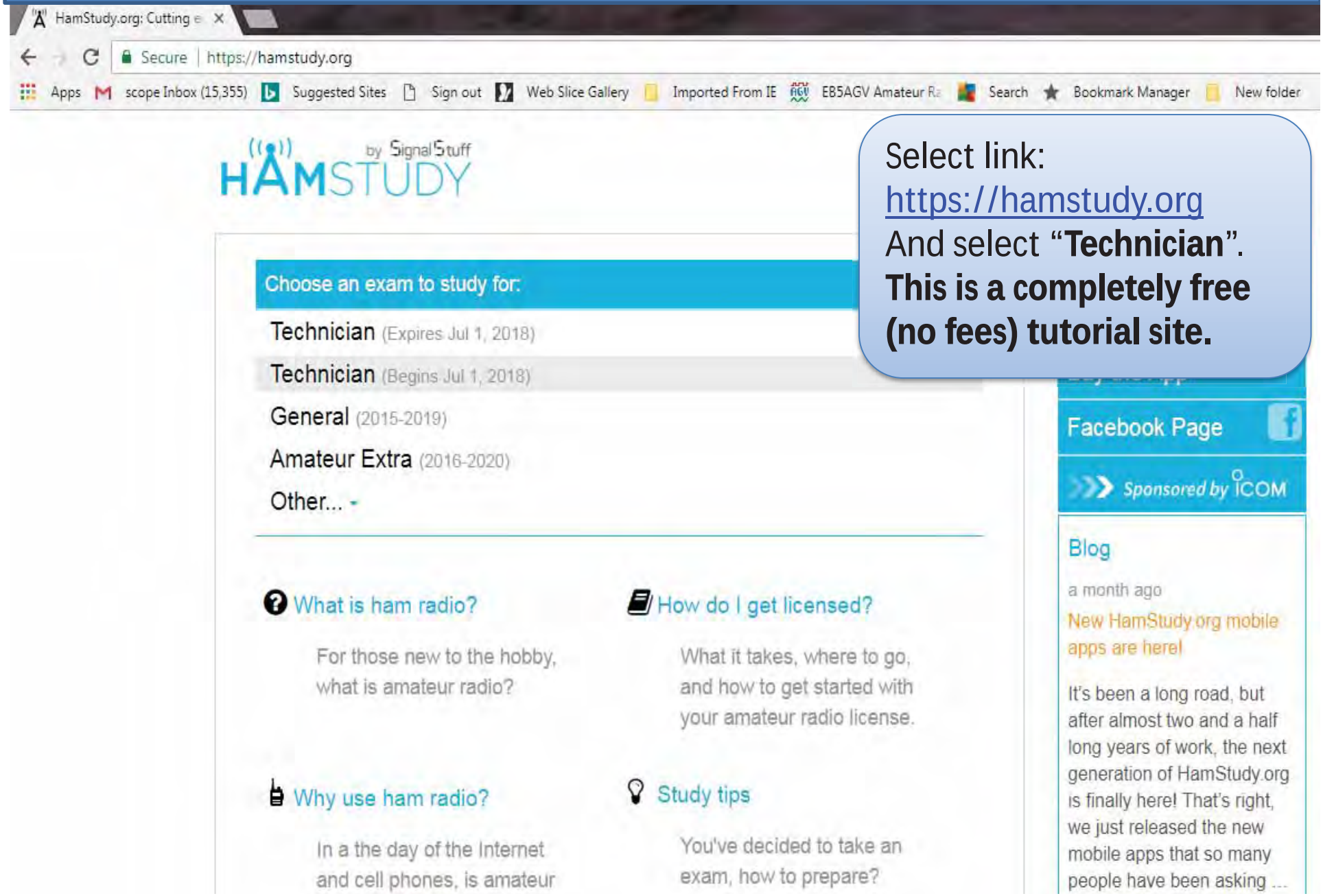
# INDIANA COUNTY EMERGENCY MANAGEMENT RADIO CLUB: https://www.qsl.net/w3bmd/



# INDIANA COUNTY EMERGENCY MANAGEMENT RADIO CLUB: https://www.qsl.net/w3bmd/

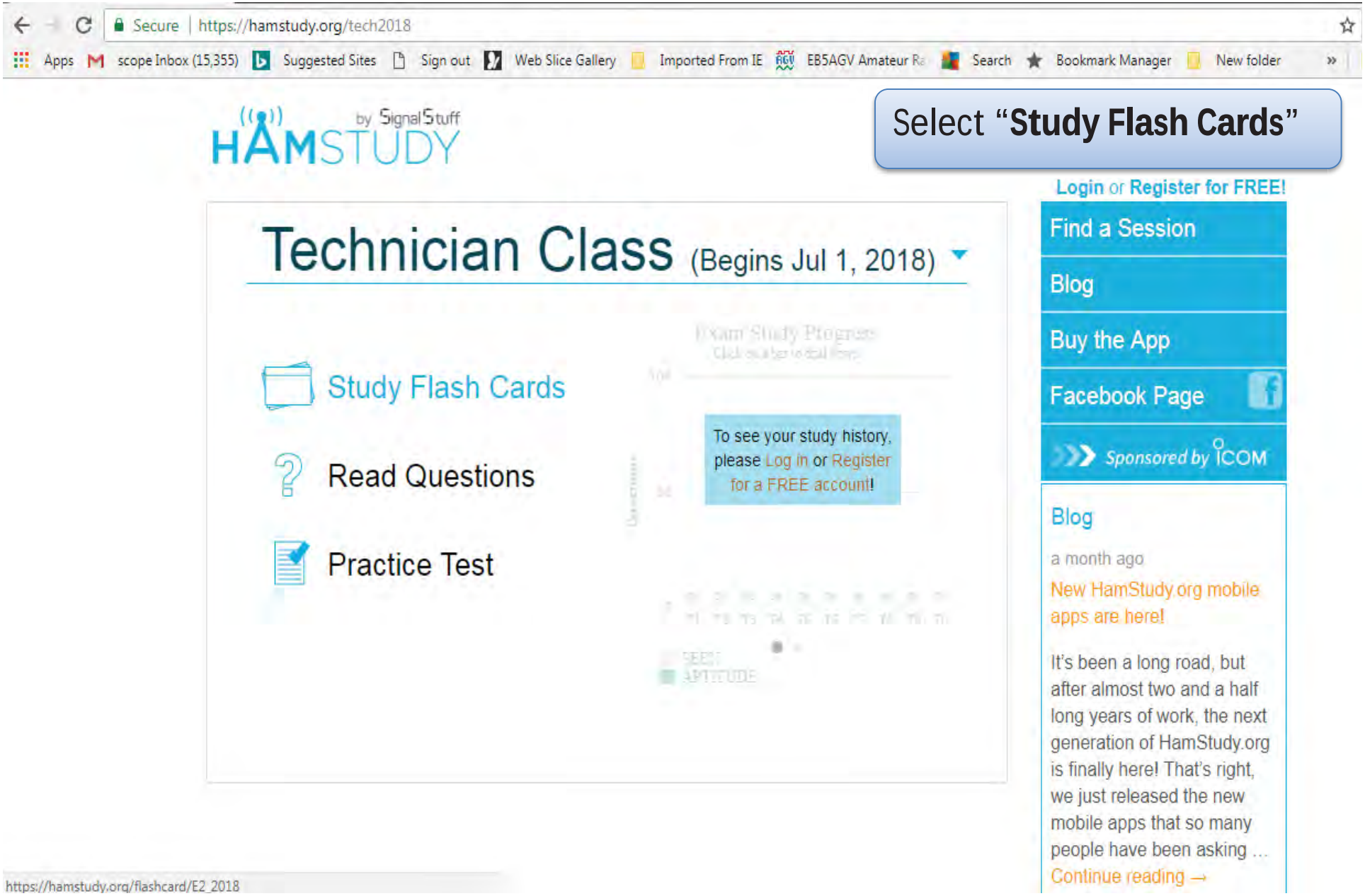


# HANDS-ON: ONLINE FCC LEARNING MODULE



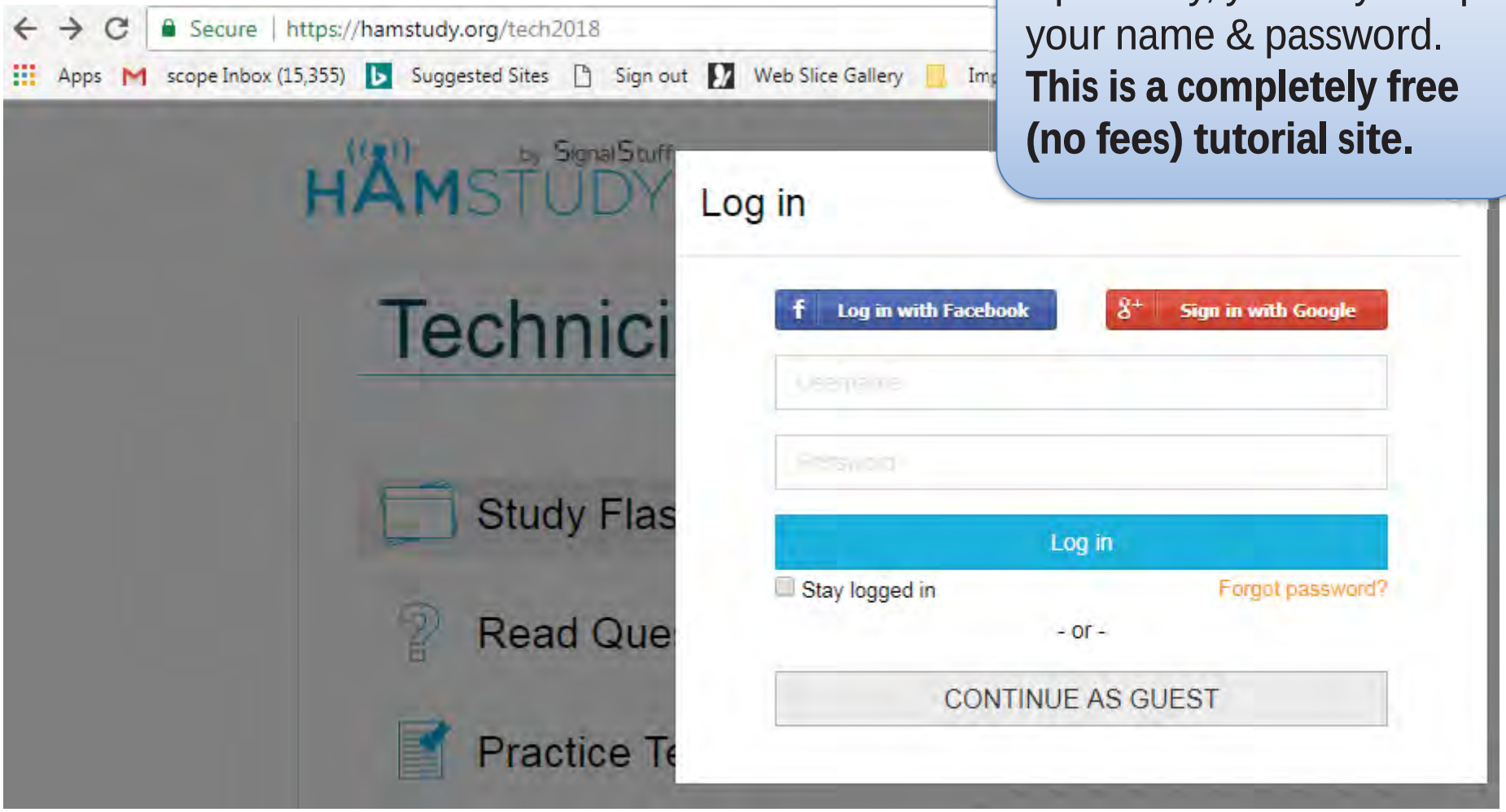

Select link:
https://hamstudy.org
And select "**Technician**".
**This is a completely free (no fees) tutorial site.**

# HANDS-ON: ONLINE FCC LEARNING MODULE

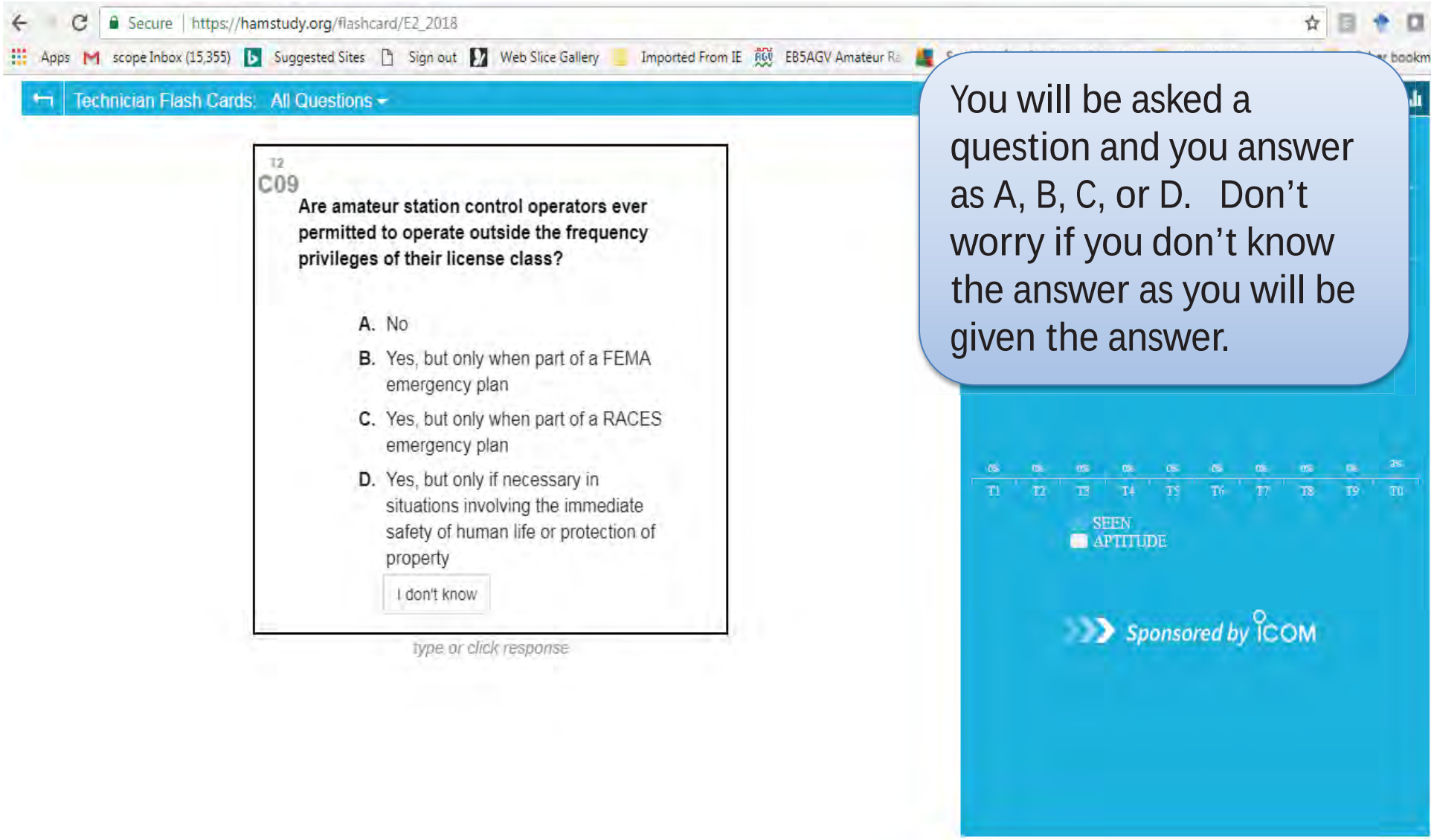


# HANDS-ON: ONLINE FCC LEARNING MODULE

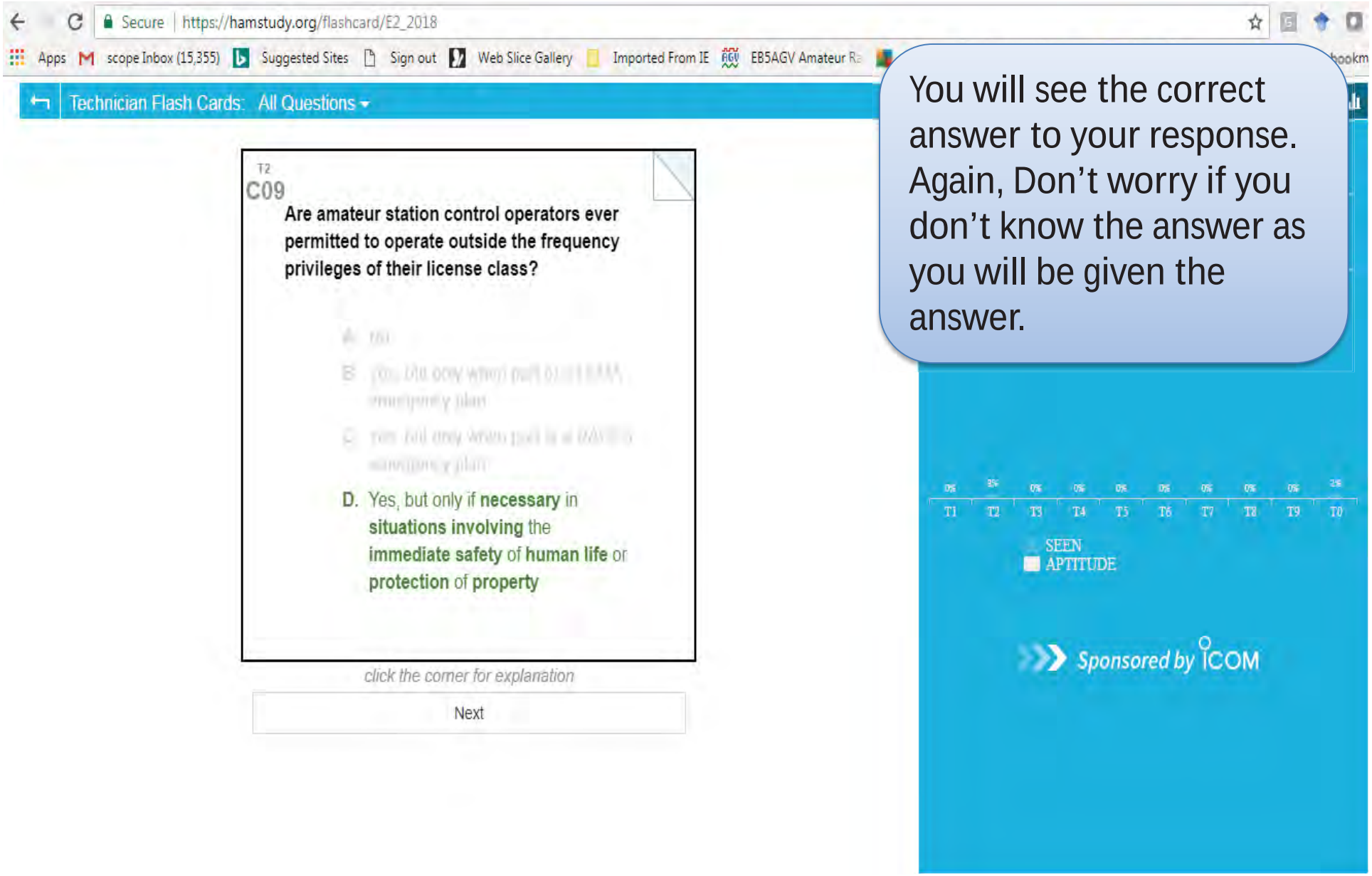
Optionally, you may setup your name & password. **This is a completely free (no fees) tutorial site.**



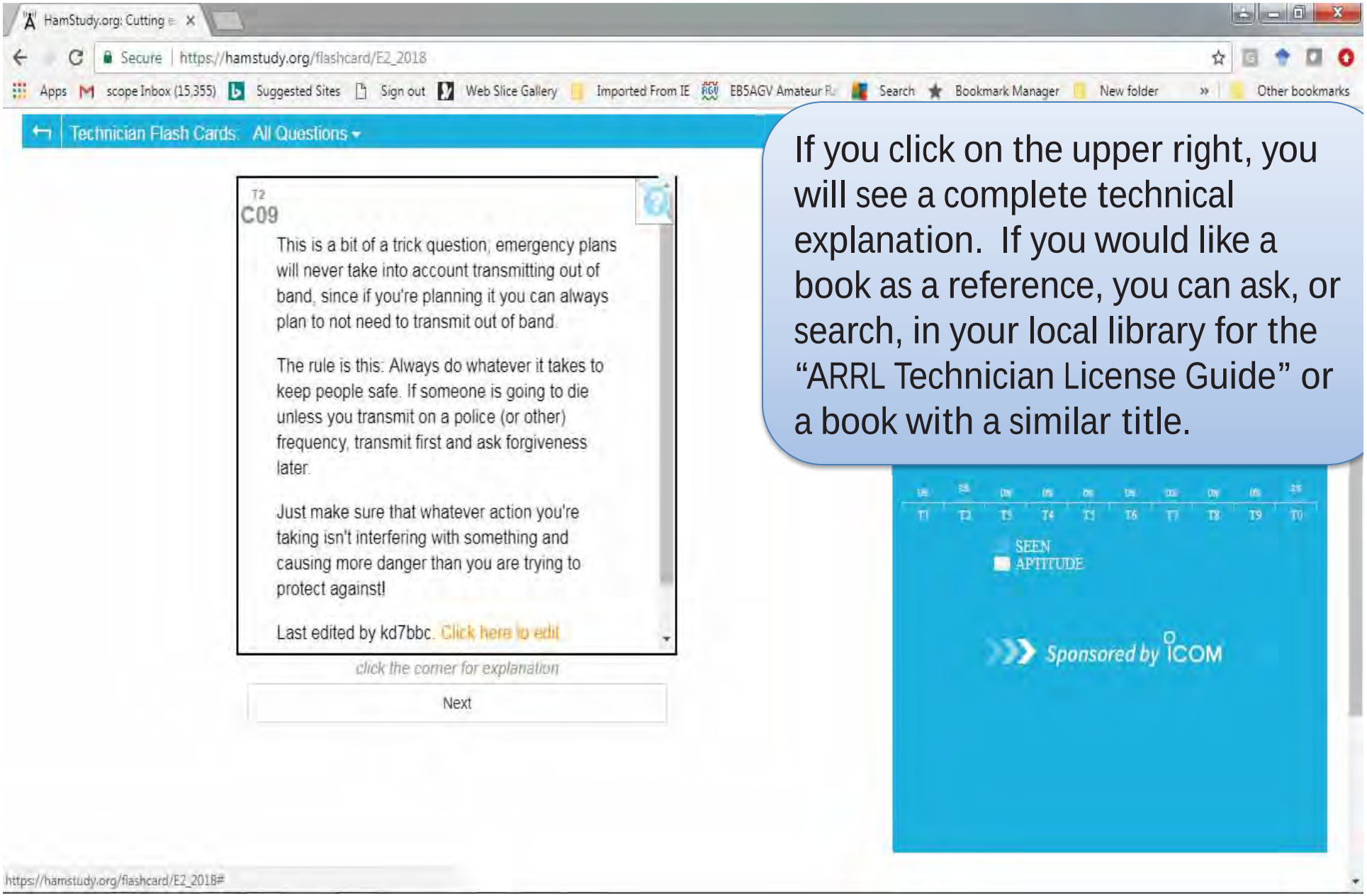
# HANDS-ON: ONLINE FCC LEARNING MODULE



# HANDS-ON: ONLINE FCC LEARNING MODULE



# HANDS-ON: ONLINE FCC LEARNING MODULE




If you click on the upper right, you will see a complete technical explanation. If you would like a book as a reference, you can ask, or search, in your local library for the "ARRL Technician License Guide" or a book with a similar title.

# HURRICANE MARIA – HARRIS MILITARY HF PHONE & DATA


The Harris Falcon series of HF MIL radios, including the RF-5800H, RF7800H and RF-300H manpack HF radios, are designed for confident operation in emergent conditions

Harris planned for establishment of a basic HF network supporting voice and e-mail • Provide several RF-5800H manpacks for use in Puerto Rico • Utilize Harris' Rochester test site with an RF-7835 1kW power amplifier and 10MHz log periodic antenna

# HURRICANE MARIA – FEMA SATELLITE PHONE & INTERNET


FEMA Satellite communications

# HURRICANE MARIA – AT&T SATELLITE PHONE & INTERNET


11/06/2017
AT&T is using an LTE cell payload UAV to offer connectivity to Puerto Ricans who lost wireless service after Hurricane Maria and live in a 40-mile (max) area under the UAV CELL ON WINGS.

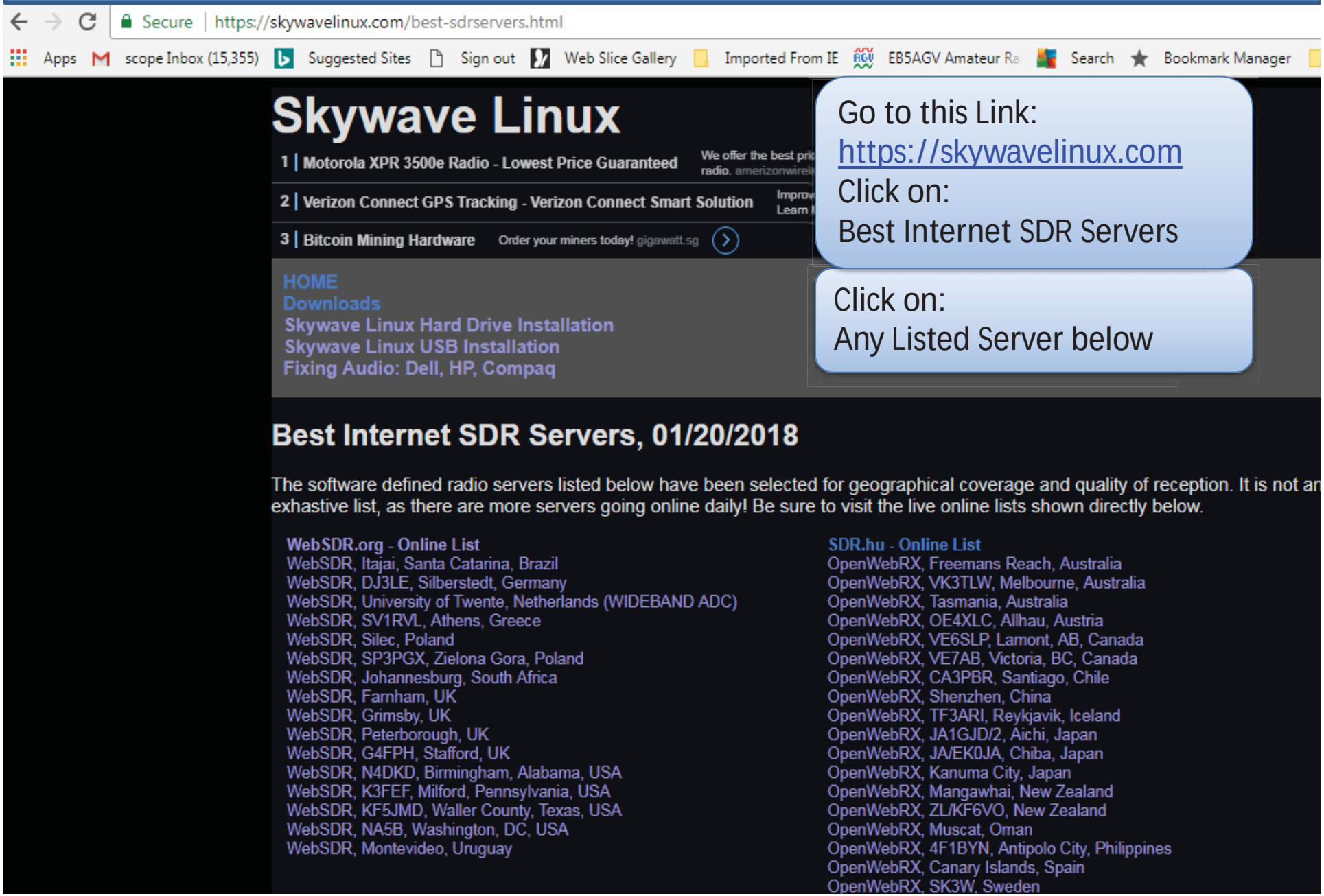
This photo was taken over a month after hurricane Maria devastated Puerto Rico where 48 percent of cell sites remain inoperative.

# HURRICANE MARIA – ALPHABET'S (GOOGLE) LTE BALLOON

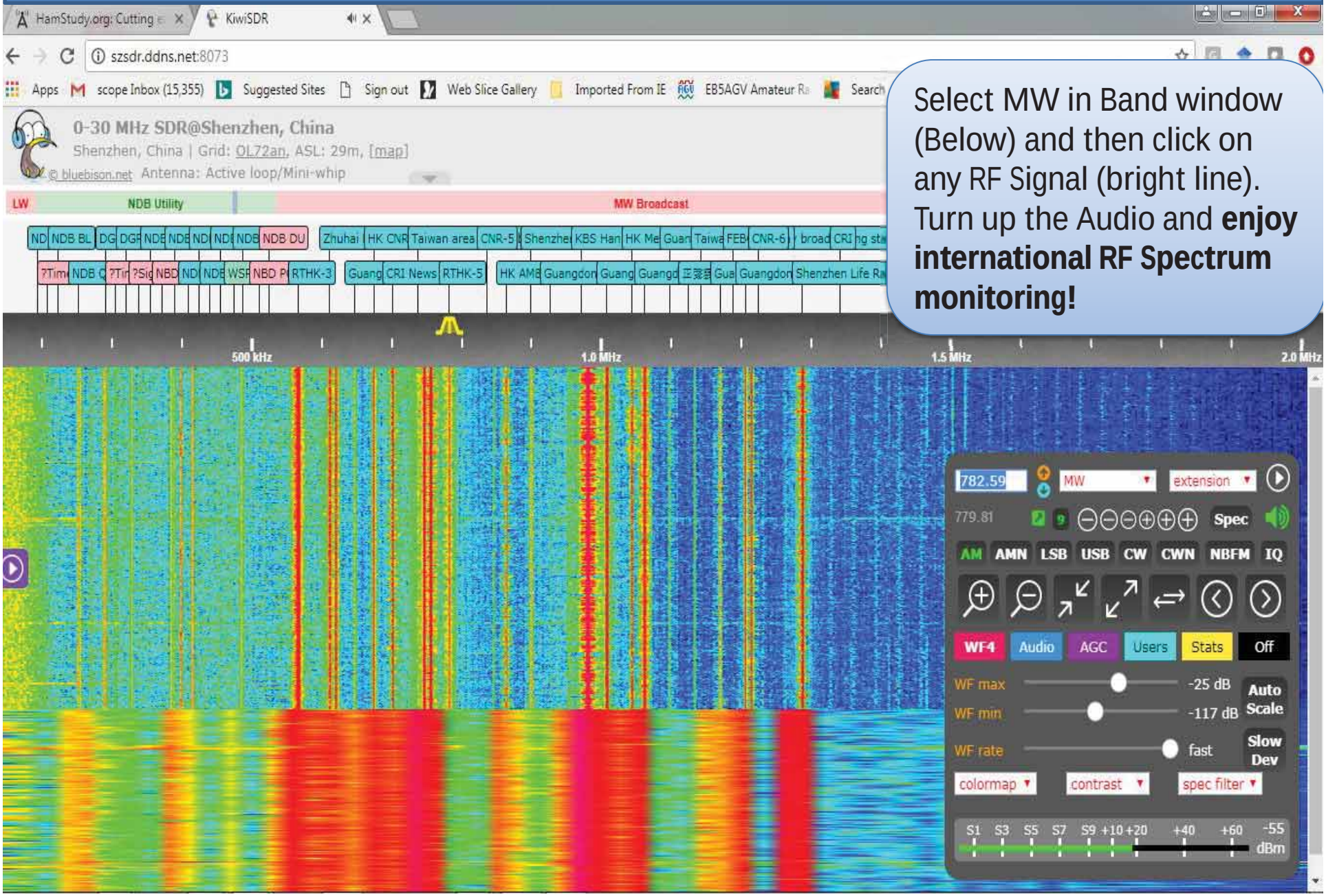

Project Loon, which belongs to Alphabet's company X, floats 2 balloons up to 20 kilometers (12 miles) and offers to 200,000 people service in Puerto Rico after hurricane Maria.

Alphabet's X indicated "basic Internet communications" including email, text messaging (but not voice service), and limited web access to more than 200,000 people.

# HANDS-ON: REMOTE SPECTRUM MONITORING



# HANDS-ON: REMOTE SPECTRUM MONITORING




Select MW in Band window (Below) and then click on any RF Signal (bright line). Turn up the Audio and **enjoy international RF Spectrum monitoring!**

# REMOTE SPECTRUM SERVER AT HOME (OPTIONAL FUN & LEARN LINUX AND RF)

If you would like to setup your own RF Spectrum server at home, acquire a hardware USB-based software defined radio (SDR):

Low-cost SDR dongle:
RTL2831U (Amazon) ~$25


Complete SDR Development System:
ADALM-PLUTO (Mouser Electronics) ~$145

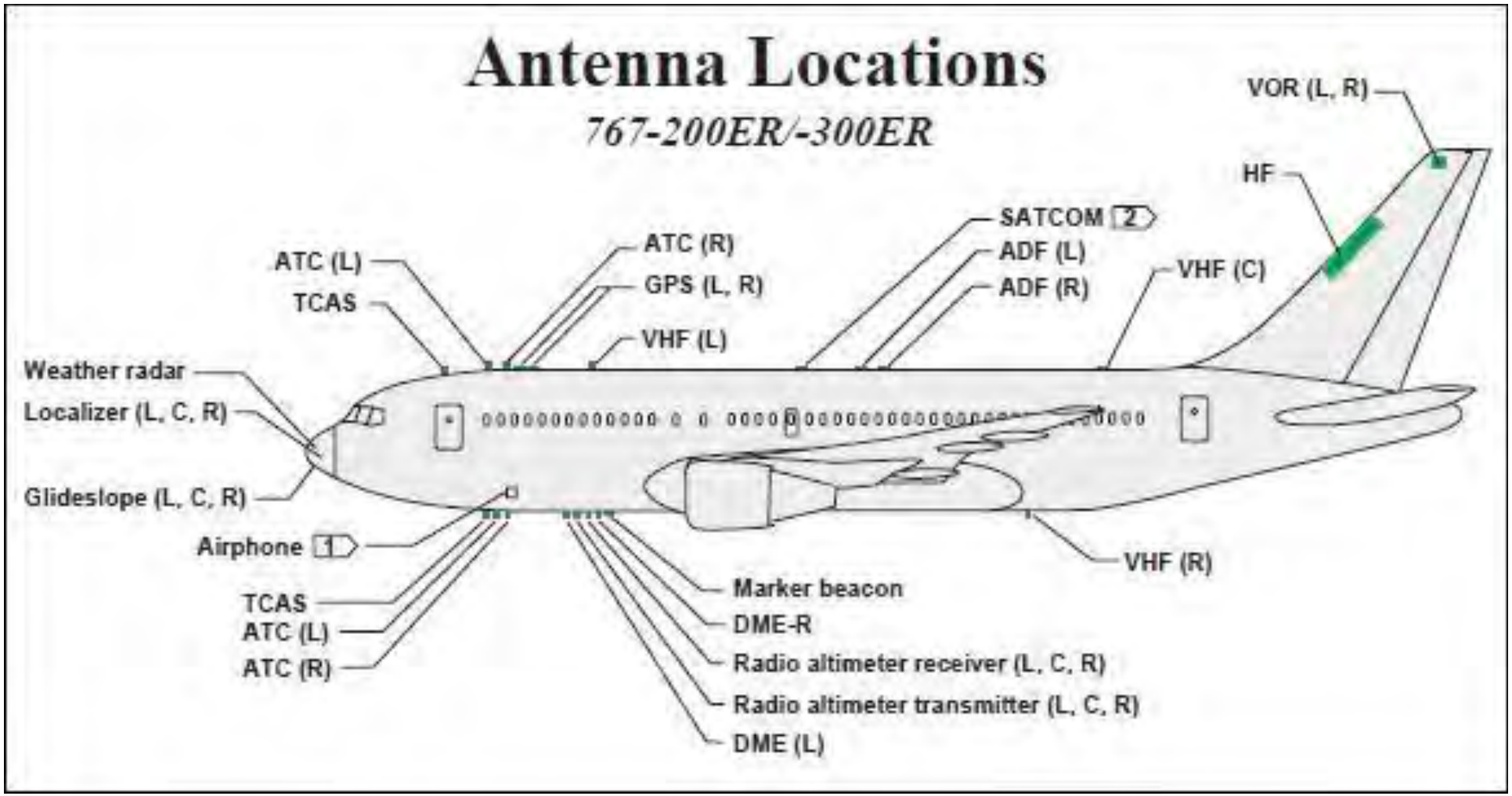
# REMOTE SPECTRUM SERVER AT HOME (OPTIONAL FUN & LEARN LINUX AND RF)

If you would like to setup your own RF Spectrum server at home, obtain a Linux server and follow the Linux software server directions at https://sdr.hu/openwebrx and links provided by the hardware provider and the ADALM-PLUTO offers advanced educational material (books, labs) for engineers designing SDR transmitters and complete cellular femtocells.

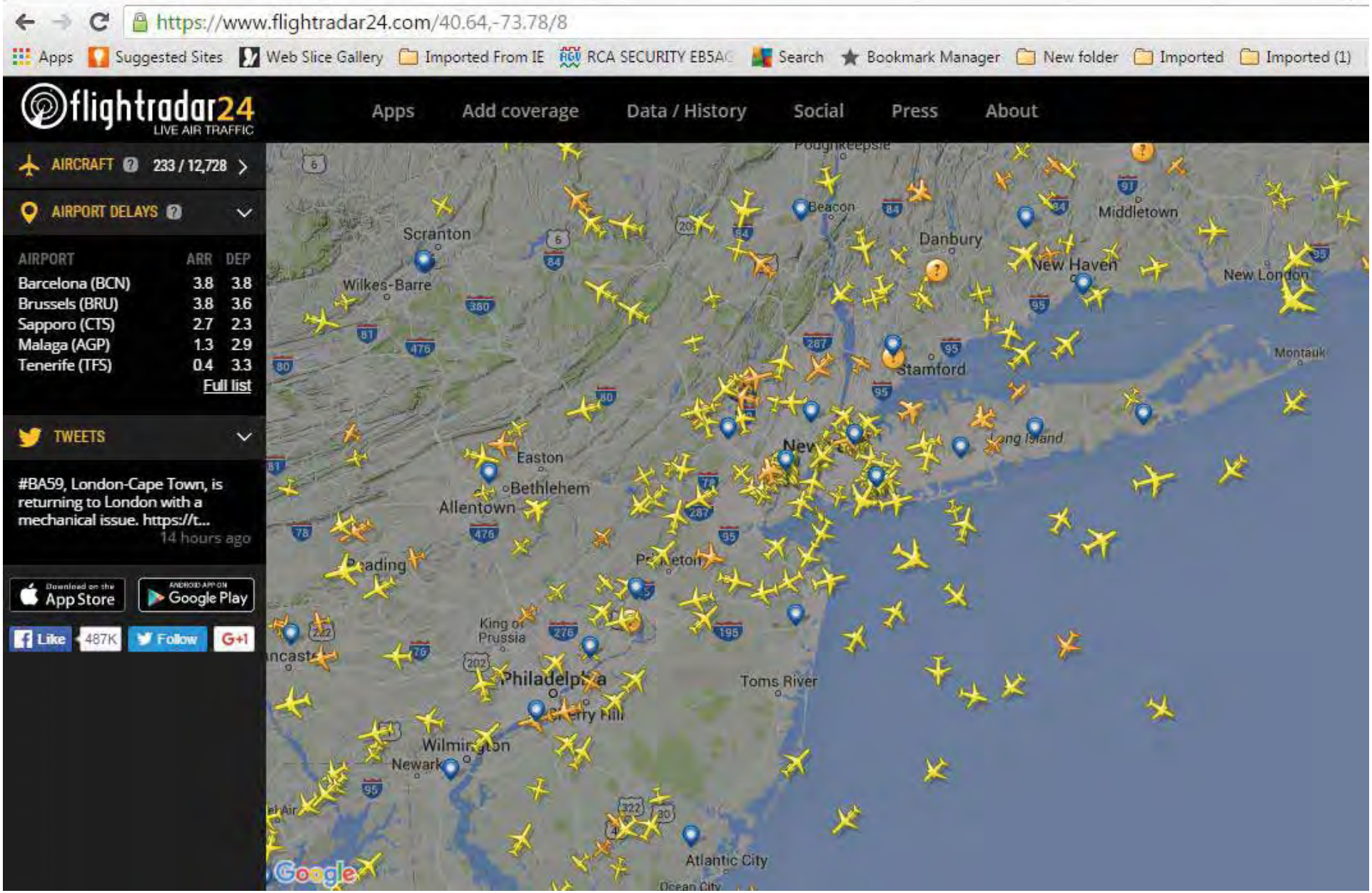
Low-cost SDR dongle:
RTL2831U (Amazon)


Complete SDR Development System:
ADALM-PLUTO (Mouser Electronics)

# RISKS OF MINIMAL OR NO ENCRYPTION



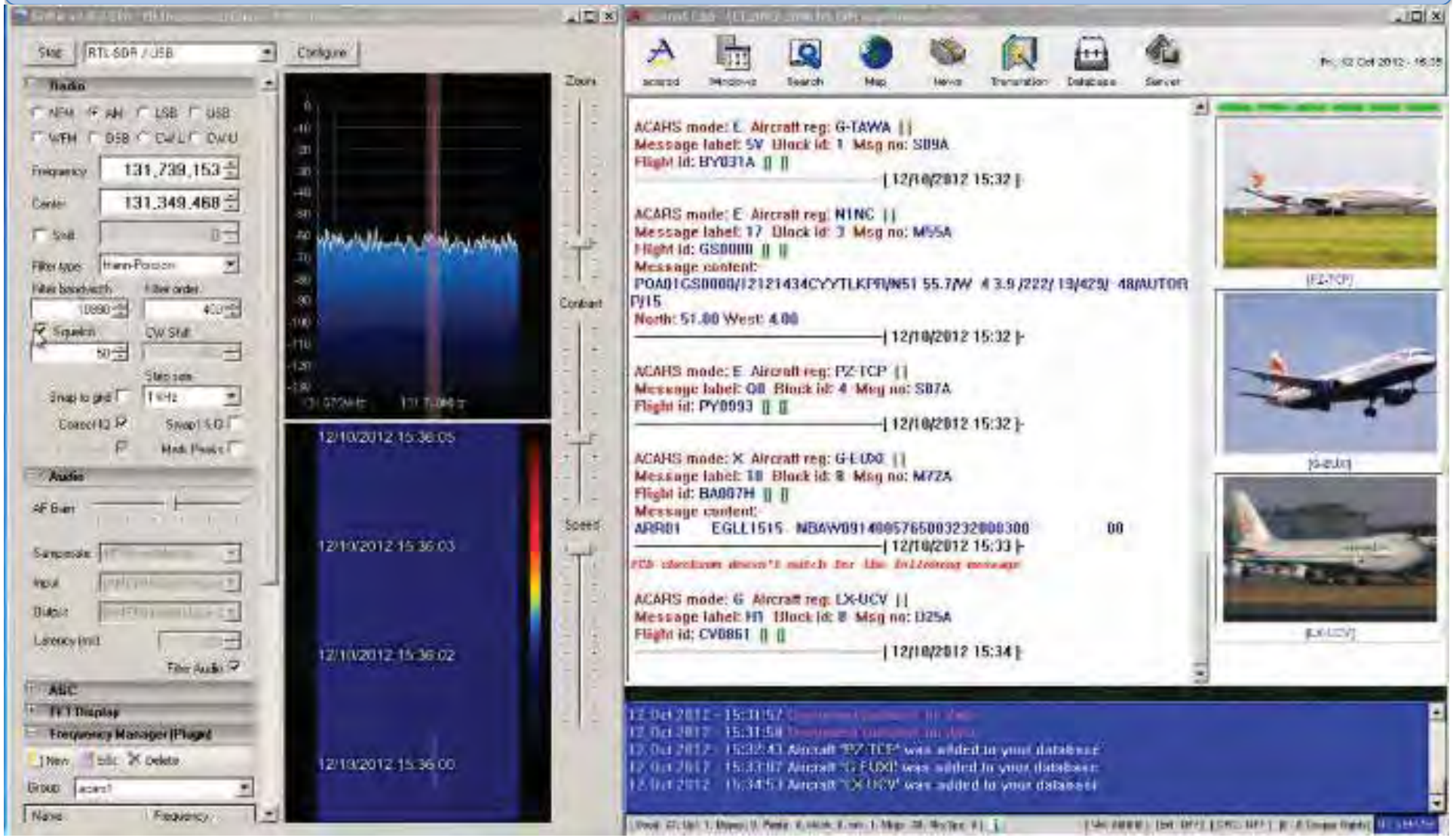
# AIRCRAFT TRANSPONDERS




https://www.flightradar24.com/40.64,-73.78/8

# RISKS - UNENCRYPTED AIRCRAFT ACARS

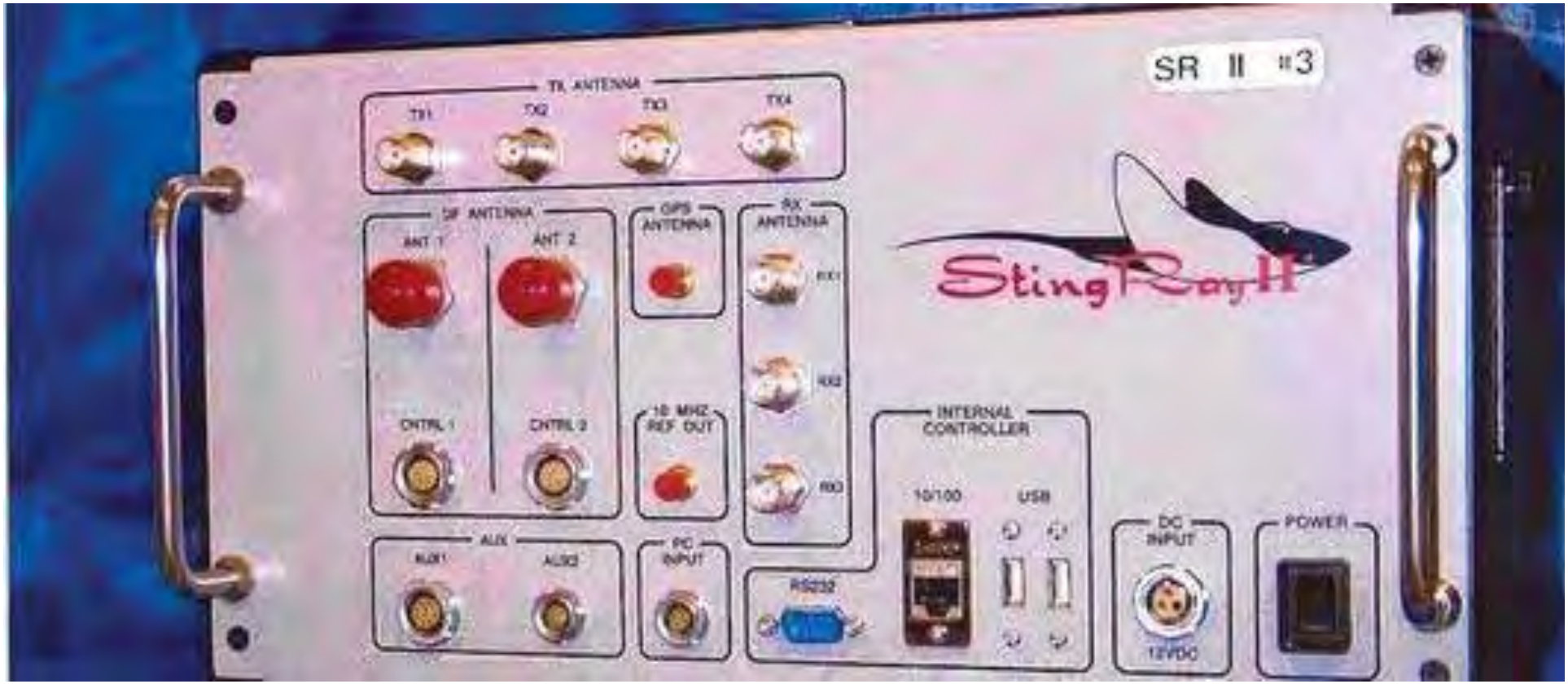
AIRCRAFT ACARS IS VHF, HF, AND SATELLITE



# MAN-IN-THE-MIDDLE CELLULAR INTERCEPTION

$400k BOX ACTS AS A BASE STATION (BTS) OR 2G TOWER

OPEN BTS UNIT ALSO WORKS WELL, APPLIED TO UNLOCKING SIMS



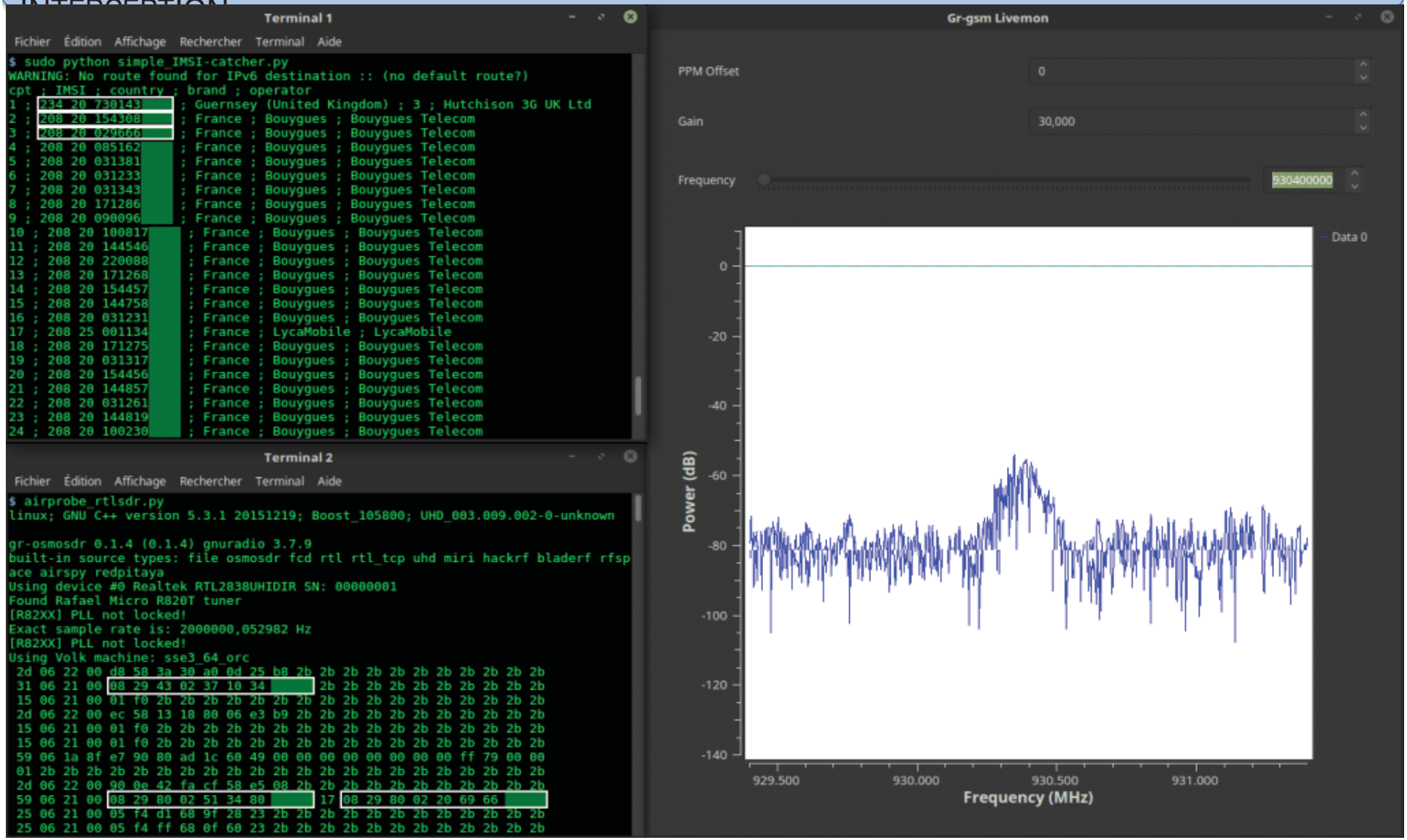

LOOKS LIKE A BTS (BASE STATION) TO A HANDSET

Handset is told to switch to 2G (RC5) if in LTE Region

http://cloakers.org/stingray-cell-tower/

# RISKS -SDR CELLULAR IMSI INTERCEPTION

## $7 SDR PASSIVE INTERNATIONAL MOBILE SUBSCRIBER IDENTITY (IMSI) SUBSCRIBER (PYTHON) INTERCEPTION




https://www.youtube.com/channel/UC4cMTOPJf_ixWyGW1u48yrw

# WIRELESS SECURITY RISKS CONCLUSIONS

- ✓ MIDDLE- & HIGH-SCHOOL STUDENTS CAN HELP DURING DISASTERS!
- ✓ EXISTING WIRELESS STANDARDS ARE NOT SECURE
- ✓ CYBER SECURITY REQUIRES YOU TO BE A LIFE-LONG LEARNER
- ✓ PURSUE A CAREER YOU LOVE AND YOU WILL HAVE FUN IN YOUR CAREER
- ✓ MIDDLE- & HIGH-SCHOOL STUDENTS MUST EMBRACE STEM TO SOLVE:
  - ✓ MINIMAL WL ENCRYPTION STANDARD – TODAY - IS AES256
  - ✓ AIRPLANE ACARS AND TRANSPONDER WIRELESS SYSTEMS MAY BE COMPROMISED AND SPOOFED
  - ✓ GSM RC5 ENCRYPTION STANDARDS ARE COMPROMISED
  - ✓ POLICE DIGITIZED VOICE TRAFFIC IS OFTEN IN THE CLEAR
  - ✓ FUTURE IoT IMPLEMENTATIONS REQUIRE IMPROVED ENCRYPTION STANDARDS