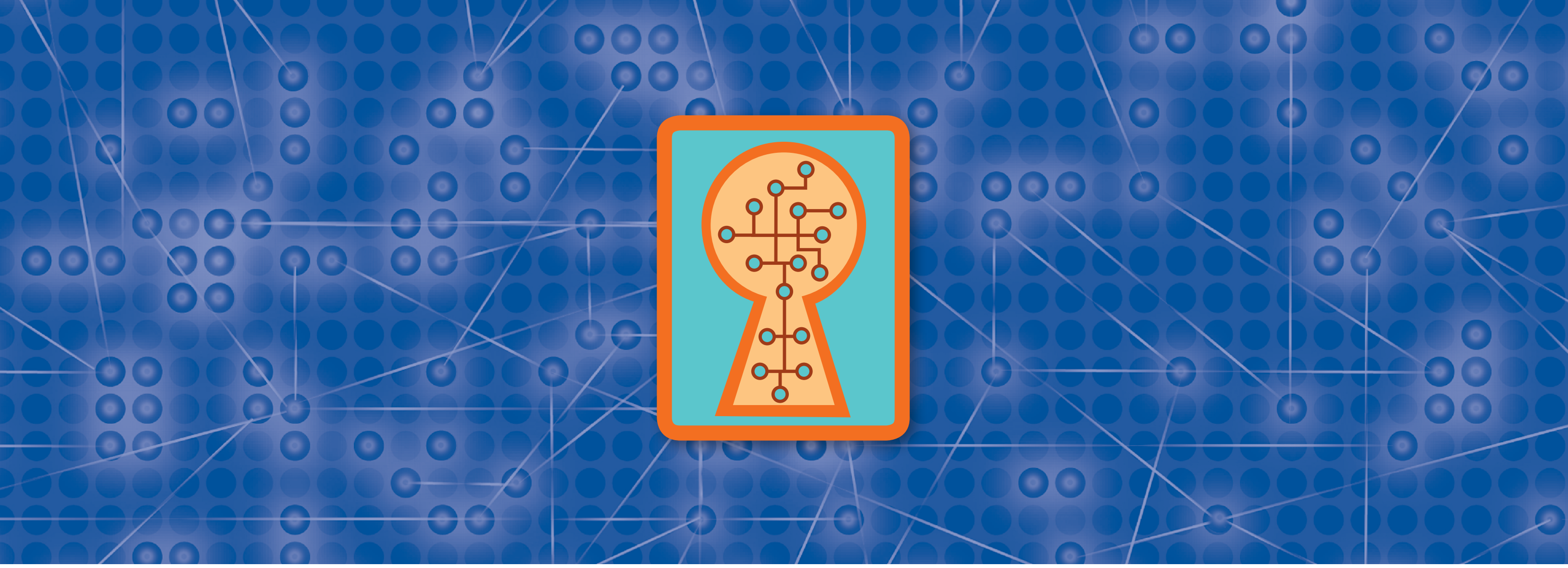


Badge 3: Cybersecurity Investigator

Cybersecurity investigators are detectives who solve cybercrimes by using what they know about technology, cybersecurity, and traditional law enforcement techniques. That means they look for clues and piece together information to figure out how a crime was committed. They have to notice small details, but also understand how the different parts of computer systems and programs work together.

Steps

1. **Look for clues about a fictional hack**
2. **Learn how traceroutes work**
3. **Solve a cybercrime**
4. **Role-play how to handle the crisis**
5. **Play a life-sized version of Minesweeper**

Purpose

When I have earned this badge, I'll understand ways cybersecurity investigators solve crimes.

STEP 1 Look for clues about a fictional hack

The warning sign that you've been hacked might not even look like a cybersecurity problem at first. Maybe sales have plummeted on your company website, even though you usually have lots of customers. Maybe your family's credit card suddenly isn't being accepted at stores or restaurants. Maybe your house was broken into while you were on vacation.

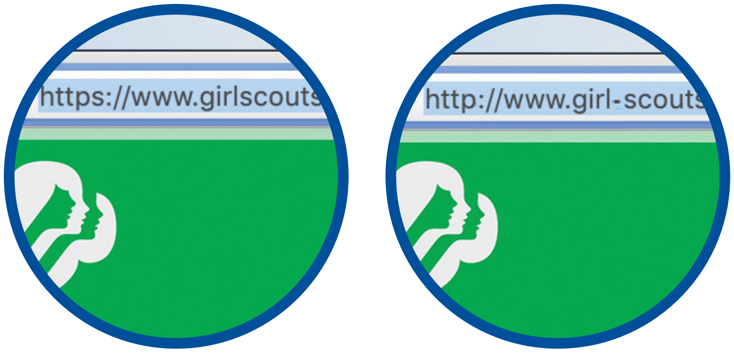
Were you hacked—or are these problems caused by something else? It could be that no one is buying your products because they don't like them. It could be that the credit card doesn't work because the magnetic strip is worn out. It could be that a burglar was watching houses in your neighborhood and noticed that no one was in your house for a few days.

Or it could be that a hacker is behind each problem. Use what you've learned about digital security to solve this cybercrime.

STEP 2 Learn how traceroutes work

When someone investigates a crime, they often recreate what happened. They look carefully at the crime scene and try to retrace the steps of the criminal. They look for footprints.

When information moves around the internet, it leaves footprints, too. Bits of information, called **data packets**, take a certain route to get from your computer to a website, for example. That route, or path, is called a **traceroute**. It lists all the stops your data packet makes along the path, like a trip itinerary. By studying traceroutes, cybersecurity investigators can see the path hackers' data packets took. Traceroutes can help investigators figure out where hackers are located or where they're sending or redirecting information.



https://www.girlscouts

http://www.girl-scouts

Another good way to discern a fake website is by checking the spelling in the URL.

Don't Be Insecure

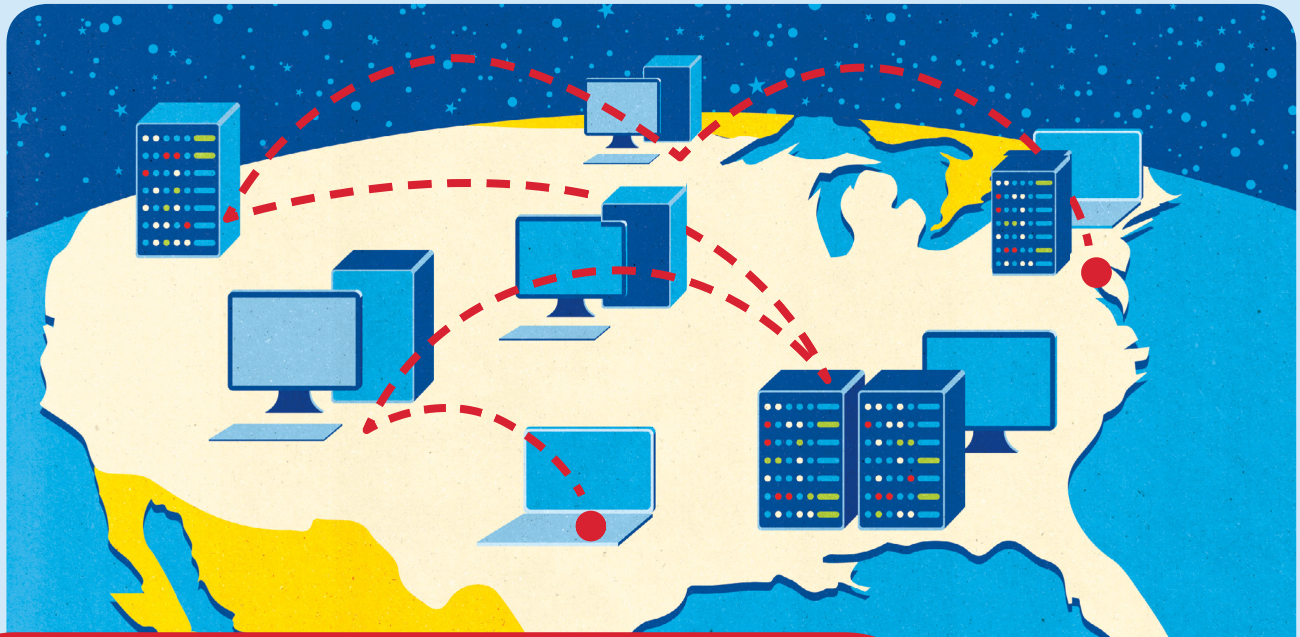
A regular http connection isn't secure. It sends your data over the internet in plain text, so anyone eavesdropping can see your information.

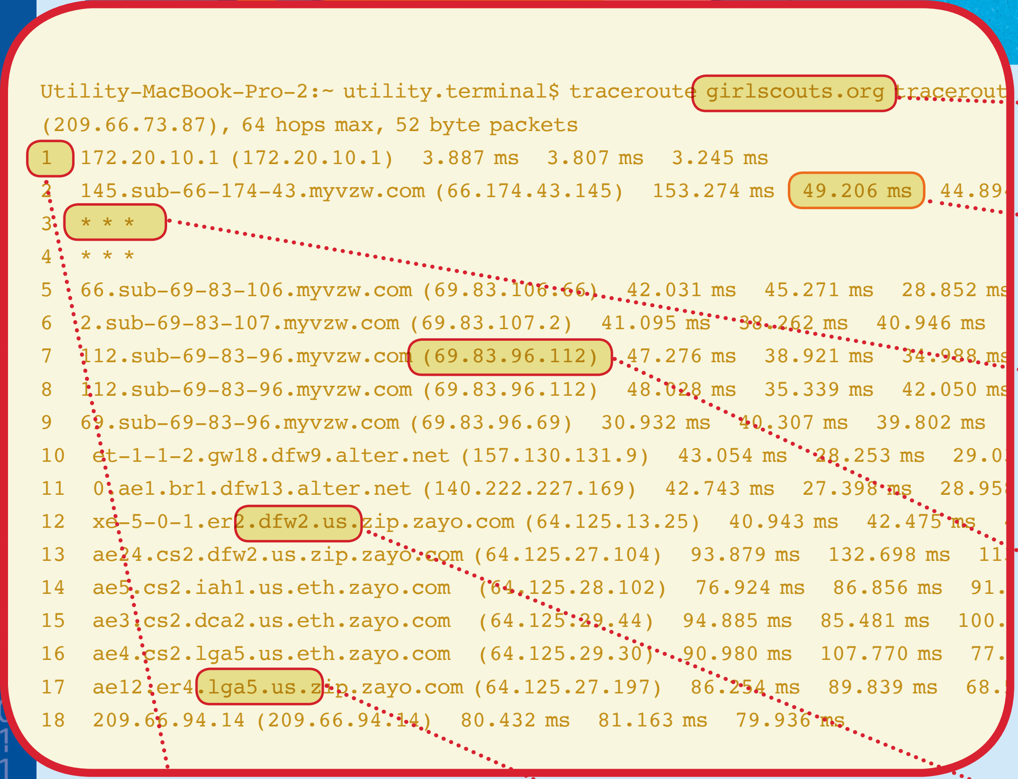
To protect people's information, programmers created HTTPS. That stands for "hypertext transfer protocol secure."

HTTPS connections are automatically encrypted and will notify you if a website you're visiting isn't secure. An HTTPS connection will have a lock icon and https:// in the web browser's address bar. If the https part is hidden, click inside the address bar; it will show the letters https before the site's URL.

Beware, though! Hackers constantly adapt to new security measures. They might add phony lock icons, create imposter sites, or send phishing emails to make their fake websites look like secure ones.

HOW TO READ A TRACEROUTE

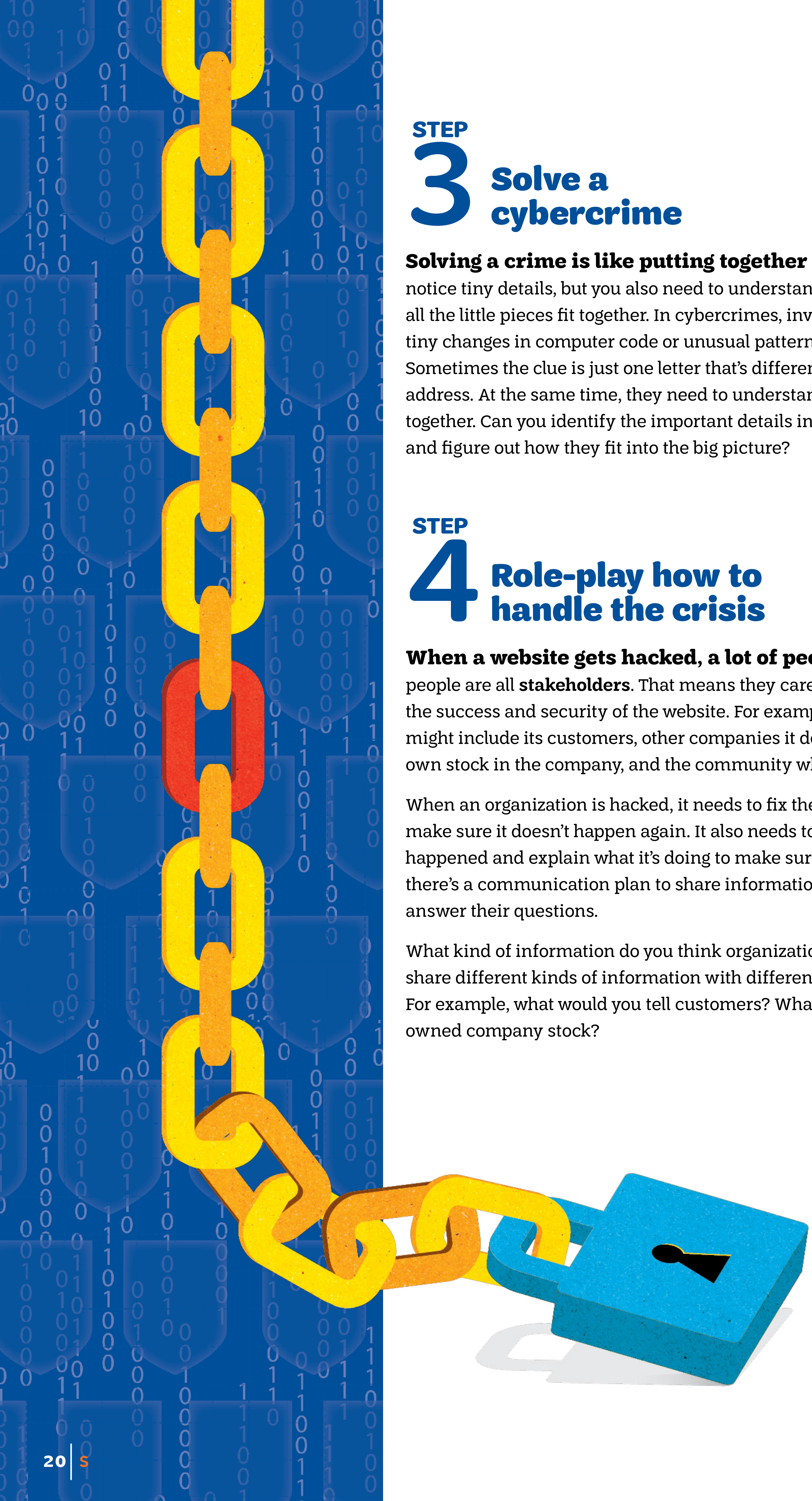




```
Utility-MacBook-Pro-2:~ utility.terminal$ traceroute girlscouts.org tracerout
(209.66.73.87), 64 hops max, 52 byte packets
1  172.20.10.1 (172.20.10.1)  3.887 ms  3.807 ms  3.245 ms
2  145.sub-66-174-43.myvzw.com (66.174.43.145)  153.274 ms  49.206 ms  44.89
3  * * *
4  * * *
5  66.sub-69-83-106.myvzw.com (69.83.106.66)  42.031 ms  45.271 ms  28.852 ms
6  2.sub-69-83-107.myvzw.com (69.83.107.2)  41.095 ms  38.262 ms  40.946 ms
7  112.sub-69-83-96.myvzw.com (69.83.96.112)  47.276 ms  38.921 ms  34.988 ms
8  112.sub-69-83-96.myvzw.com (69.83.96.112)  48.028 ms  35.339 ms  42.050 ms
9  69.sub-69-83-96.myvzw.com (69.83.96.69)  30.932 ms  40.307 ms  39.802 ms
10  et-1-1-2.gw18.dfw9.alter.net (157.130.131.9)  43.054 ms  28.253 ms  29.0
11  0.ae1.br1.dfw13.alter.net (140.222.227.169)  42.743 ms  27.398 ms  28.95
12  xe-5-0-1.er2.dfw2.us.zip.zayo.com (64.125.13.25)  40.943 ms  42.475 ms
13  ae24.cs2.dfw2.us.zip.zayo.com (64.125.27.104)  93.879 ms  132.698 ms  11
14  ae5.cs2.iah1.us.eth.zayo.com  (64.125.28.102)  76.924 ms  86.856 ms  91.
15  ae3.cs2.dca2.us.eth.zayo.com  (64.125.29.44)  94.885 ms  85.481 ms  100.
16  ae4.cs2.lga5.us.eth.zayo.com  (64.125.29.30)  90.980 ms  107.770 ms  77.
17  ae12.er4.lga5.us.zip.zayo.com (64.125.27.197)  86.254 ms  89.839 ms  68.
18  209.66.94.14 (209.66.94.14)  80.432 ms  81.163 ms  79.936 ms
```

- The website to which the user ran the traceroute.
- The time it took to make the hop (e.g. 49.206 milliseconds).
- Asterisks mean that either the identity of the "hop" is private or that the request timed out.
- IP (internet protocol) address: any device connected to a network has its own IP address, a series of unique numbers.

- Each number represents one stop, or "hop," that the data packets make on their way.
- LGA=LaGuardia (airport), New York City. The Girl Scouts website is hosted in New York City.
- Many traceroutes use codes that refer to locations around the globe (DFW = Dallas Fort Worth).



STEP 3 Solve a cybercrime

Solving a crime is like putting together a puzzle. You need to notice tiny details, but you also need to understand the bigger picture of how all the little pieces fit together. In cybercrimes, investigators need to notice tiny changes in computer code or unusual patterns in how sites are being used. Sometimes the clue is just one letter that's different in a code, email, or web address. At the same time, they need to understand how all the details work together. Can you identify the important details in code or traceroutes and figure out how they fit into the big picture?

STEP 4 Role-play how to handle the crisis

When a website gets hacked, a lot of people are affected. Those people are all **stakeholders**. That means they care about, or have "a stake in," the success and security of the website. For example, a business's stakeholders might include its customers, other companies it does business with, people who own stock in the company, and the community where it does business.

When an organization is hacked, it needs to fix the problem and take steps to make sure it doesn't happen again. It also needs to tell stakeholders about what happened and explain what it's doing to make sure the site is secure. Usually, there's a communication plan to share information with stakeholders and answer their questions.

What kind of information do you think organizations should share? Would you share different kinds of information with different groups of stakeholders? For example, what would you tell customers? What would you tell people who owned company stock?

SAVE MONEY WITH CYBERSECURITY

Cybercrime is expensive. When databases or websites get hacked, it costs the targeted organization a lot of money. Sometimes hackers steal trade secrets, such as information about how products are made (secret recipes!) or plans for new products in development.

The kinds of things that usually get stolen in a hack are:

- Personal information, such as addresses, dates of birth, or health information
- Credit card information
- Social Security numbers
- Trade secrets, corporate information, or software source code

When a shopping website gets hacked, it loses sales and customers, but the company also has to spend money to recover from the cybercrime. They need to:

- Research and fix the problem with their computers
- Notify customers, shareholders, and other stakeholders
- Create public relations campaigns to regain customers' trust
- Pay to have customers' credit cards reissued, repair stolen identities, or monitor their credit scores

Companies that experience a data breach can see their stock prices drop. The confidence in their brand name can also take a big hit for years after the event. That means that, even after the security problem is solved, customers may not return because they don't trust the company anymore.

Solving a cybercrime and recovering from it are very expensive. It's better to prevent these crimes from happening in the first place by having a strong cybersecurity system.

STEP

5 Play a life-sized version of Minesweeper

Protecting your organization from cybercrime is like playing Minesweeper. Your goal is to keep your computers and data safe so your organization can accomplish its goals.

You create “defenses” for your computer systems, such as training your employees about cybersecurity, backing up your data, and hiring white hat hackers to look for weakness. At the same time, black hat hackers are looking for the same weaknesses in your cybersecurity system, so they can break into your computers. They place “mines” like phishing or spoofing emails, or they take advantage of out-of-date software that can be more easily hacked.

If you can help your organization do its job without getting hacked by avoiding the hackers’ “mines,” you and your organization win!

Now that I’ve earned this badge, I can give service by:

- Creating an escape room to teach others how cybersecurity experts investigate hacks.
- Researching careers in cybersecurity investigation and sharing what I’ve learned with other students.
- Organizing a workshop to teach others how to run traceroutes.

I’m inspired to: