Hashing

Cybersecurity
Cryptography Day 3

© 2019 Trilogy Education Services, Inc.

Today’s Objectives

By the end of class, you will be able to:

- □ Describe hashing and hash functions
- □ Generate hashes on the command line using the CLI tools `md5sum` and `sha256sum`.
- □ Discuss how hashing assists forensics investigations.
- □ Crack password hashes with rainbow tables and hashcat.

Activity: Warm Up

In this activity, you’ll review the cryptography concepts you’ve learned so far.

Instructions sent via Slack.

Suggested Time:
15 Minutes

Times Up! Let’s Review.

Cryptography Warm-Up

Hashing and Data Integrity

Hashing

Hashing is used to generate a unique fingerprint for a piece of data.

- Just as encryption turns plaintext into a ciphertext, hashes turn plaintext into a signature.

- A hash function is a set of rules used to convert a plaintext into a signature

- The hash of the string “example”: `ddce269a1e3d054cae349621c198dd52`

- Even though has signatures are unintelligible (like cipher texts), they are used to protect integrity, not privacy.

Hashes to protect Integrity.

Hash functions have two properties that assist in Integrity protection.

Fixed-length output: Every hash output is the same length, regardless of plaintext input length.

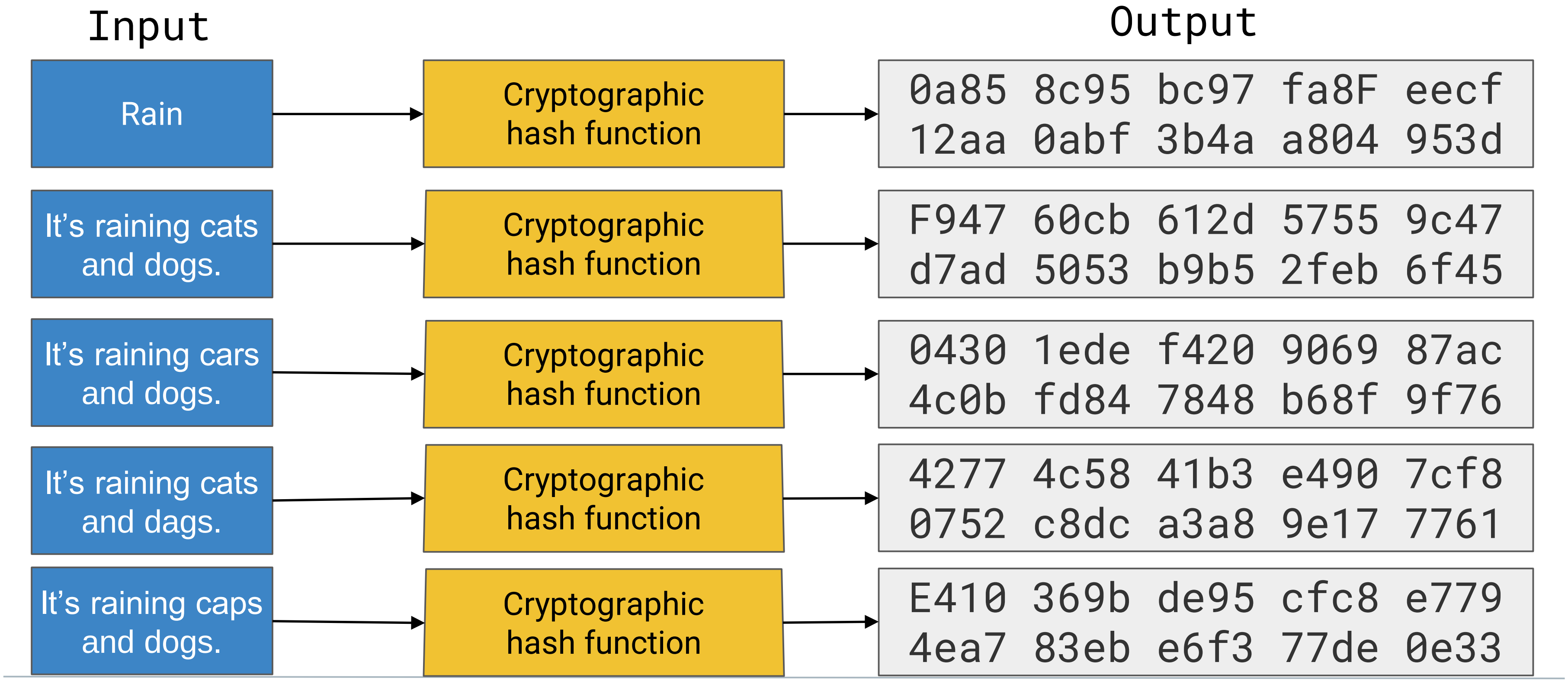
The string “text” will output a hash the same length as a file as larger as an OS.

Sensitivity to small change: changing a small bit in the input completely changes the hash output.

The hash output of “abcdefg” will be completely different from “abcdefj”.

Hashing

Note the fixed-length output and sensitivity to small changes.

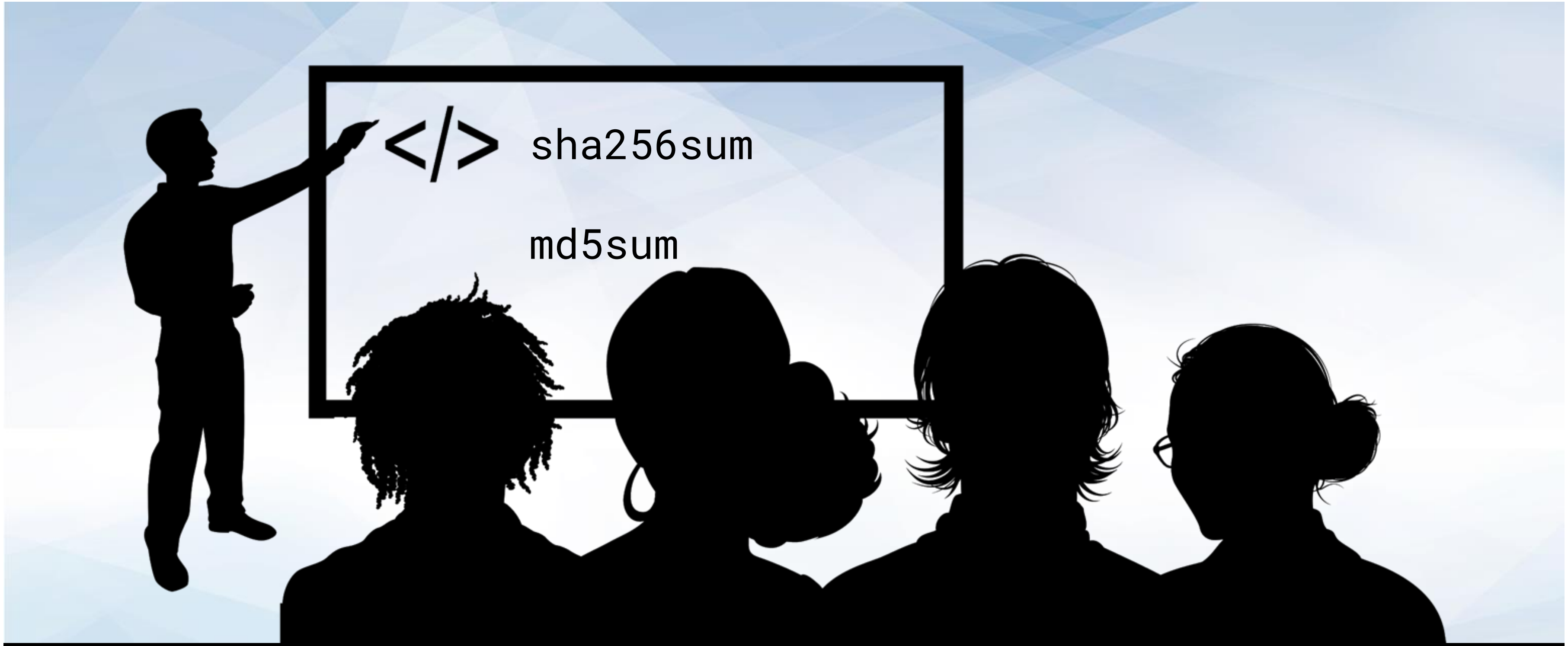


Input		Output
Rain	Cryptographic hash function	0a85 8c95 bc97 fa8F eecf 12aa 0abf 3b4a a804 953d
It’s raining cats and dogs.	Cryptographic hash function	F947 60cb 612d 5755 9c47 d7ad 5053 b9b5 2feb 6f45
It’s raining cars and dogs.	Cryptographic hash function	0430 1ede f420 9069 87ac 4c0b fd84 7848 b68f 9f76
It’s raining cats and dags.	Cryptographic hash function	4277 4c58 41b3 e490 7cf8 0752 c8dc a3a8 9e17 7761
It’s raining caps and dogs.	Cryptographic hash function	E410 369b de95 cfc8 e779 4ea7 83eb e6f3 77de 0e33

Hash Use Cases

The following are some use cases for hashes:

- Websites store hashes of passwords in their databases, rather than the plaintext password.
- Antivirus scanners use hashes to to “fingerprint” files.
- Verify integrity and establish trust in records that underlie cryptocurrencies.
- Confirm that a files was downloaded without corruption.



Instructor Demonstration

Generating Hsshes with the CLI

Activity: Inspecting and Generating Password Hashes

In this activity, you will md5sum and sha256sum to generate hashes of simple strings..*and more!*

Instructions sent via Slack.

Suggested Time:
15 Minutes

Times Up! Let’s Review.

Inspecting and Generating Password Hashes

Activity: Hashes and Computer Forensics

In this activity, you will read an article about digital evidence in court cass and answer questions.

Suggested Time:
8 Minutes

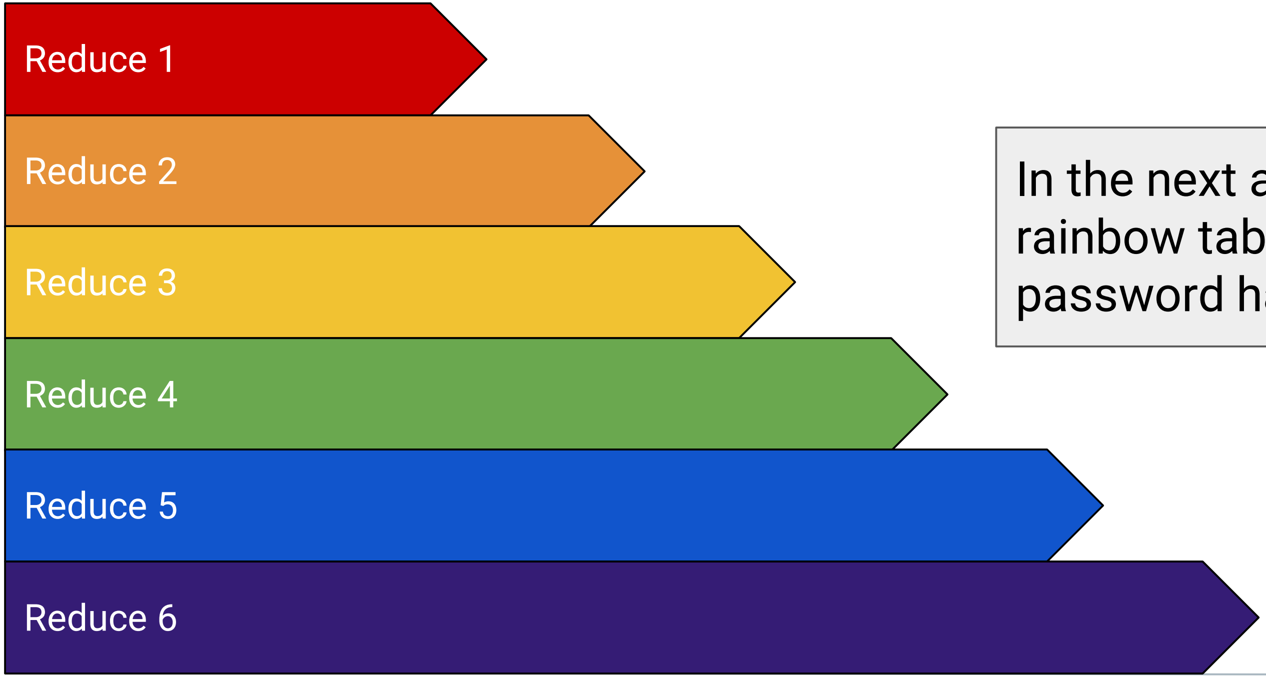
Times Up! Let’s Review.

Hashes and Computer Forensics

Rainbow Tables

Rainbow Tables

Although password hashes can not be inverted, they could still be cracked.
But it will take either a lot of time or a lot of disk space...



Reduce 1

Reduce 2

Reduce 3

Reduce 4

Reduce 5

Reduce 6

In the next activity, we'll look at how rainbow tables can be used to crack password hashes

Activity: Cracking Passwords with Rainbow Tables

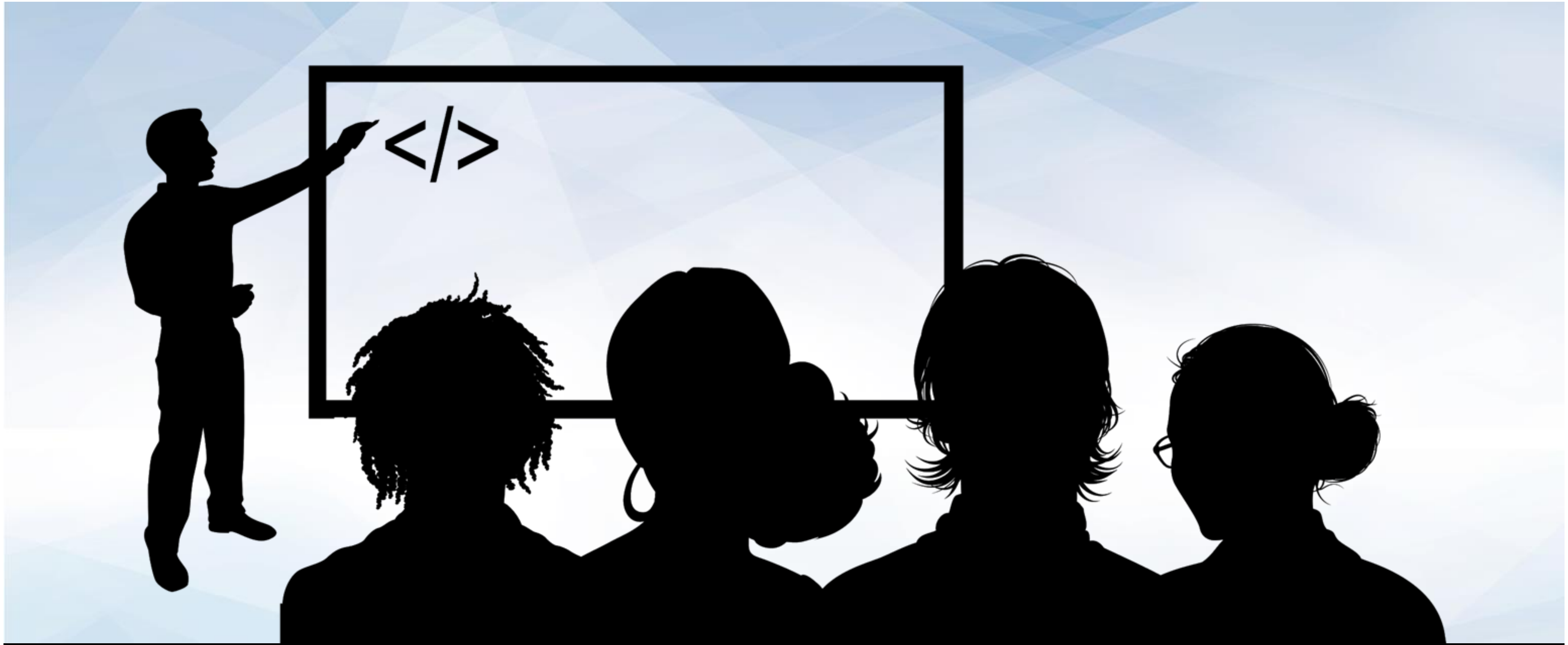
In this activity, you will read an article about the function, purpose and limitation of rainbow tables, then answer corresponding questions.

Instructions sent via Slack.

Suggested Time:
8 Minutes

Times Up! Let’s Review.

Rainbow Tables



Instructor Demonstration

Cracking Passwords with Hashcat

Activity: Hashcats

In this activity, you will identify the hash and hashcat flags for three files.

Instructions sent via Slack.

Suggested Time:
15 Minutes

Times Up! Let’s Review.

Hashcat Activity

Today’s Objectives

By the end of class, you will be able to:

- ☑ Describe hashing and hash functions
- ☑ Generate hashes on the command line using the CLI tools `md5sum` and `sha256sum`.
- ☑ Discuss how hashing assists forensics investigations.
- ☑ Crack password hashes with rainbow tables and hashcat.