PancakesCon

Cryptic Dependencies & Cryptic Crosswords

Presented by Maya Kaczorowski, Product Manager, GitHub
@mayakacz @MayaKaczorowski

@MayaKaczorowski

Maya Kaczorowski

Product Manager, Software Supply Chain Security

GitHub

Agenda

Part 1: **Cryptic dependencies**

- What’s a software supply chain
- Common types of attacks
- Examples of known attacks
- Best practices for developers
- How to report a vulnerability

Part 2: **Cryptic crosswords**

- What’s a cryptic crossword
- How clues are structured
- Common types of ~~attacks~~ clues
- Examples of ~~attacks~~ clues
- Making it even harder

@MayaKaczorowski

Let’s start with cryptic dependencies!

Every time you `pip install`, `go get`, or `mvn fetch` something, you're doing the equivalent of plugging a thumb drive you found on the sidewalk into your production server.

- Dan Lorenc

https://medium.com/better-programming/getting-serious-about-open-source-security-1d15609478fa

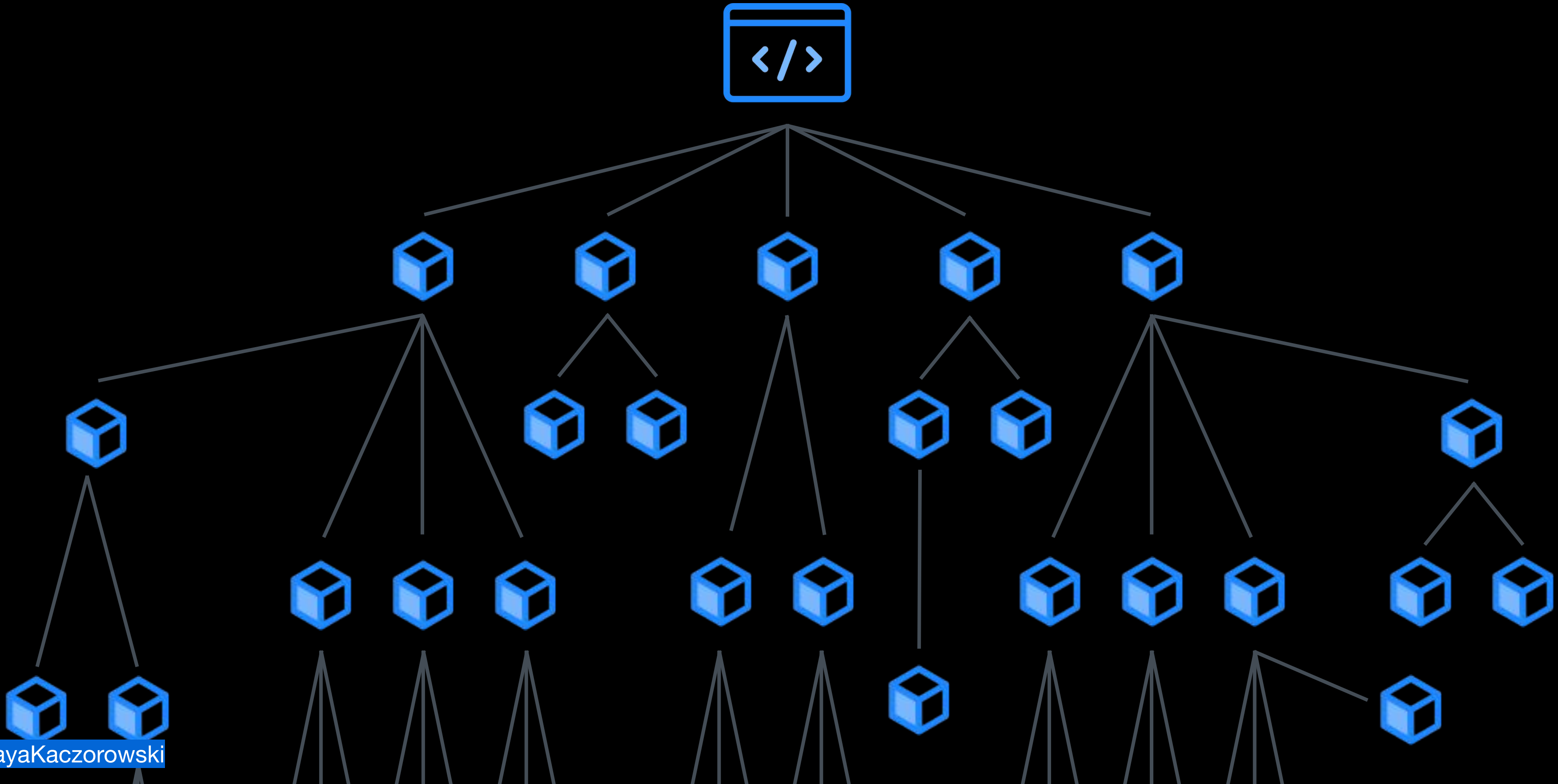
Why can we call dependencies “cryptic”?

A vast majority of code is open source

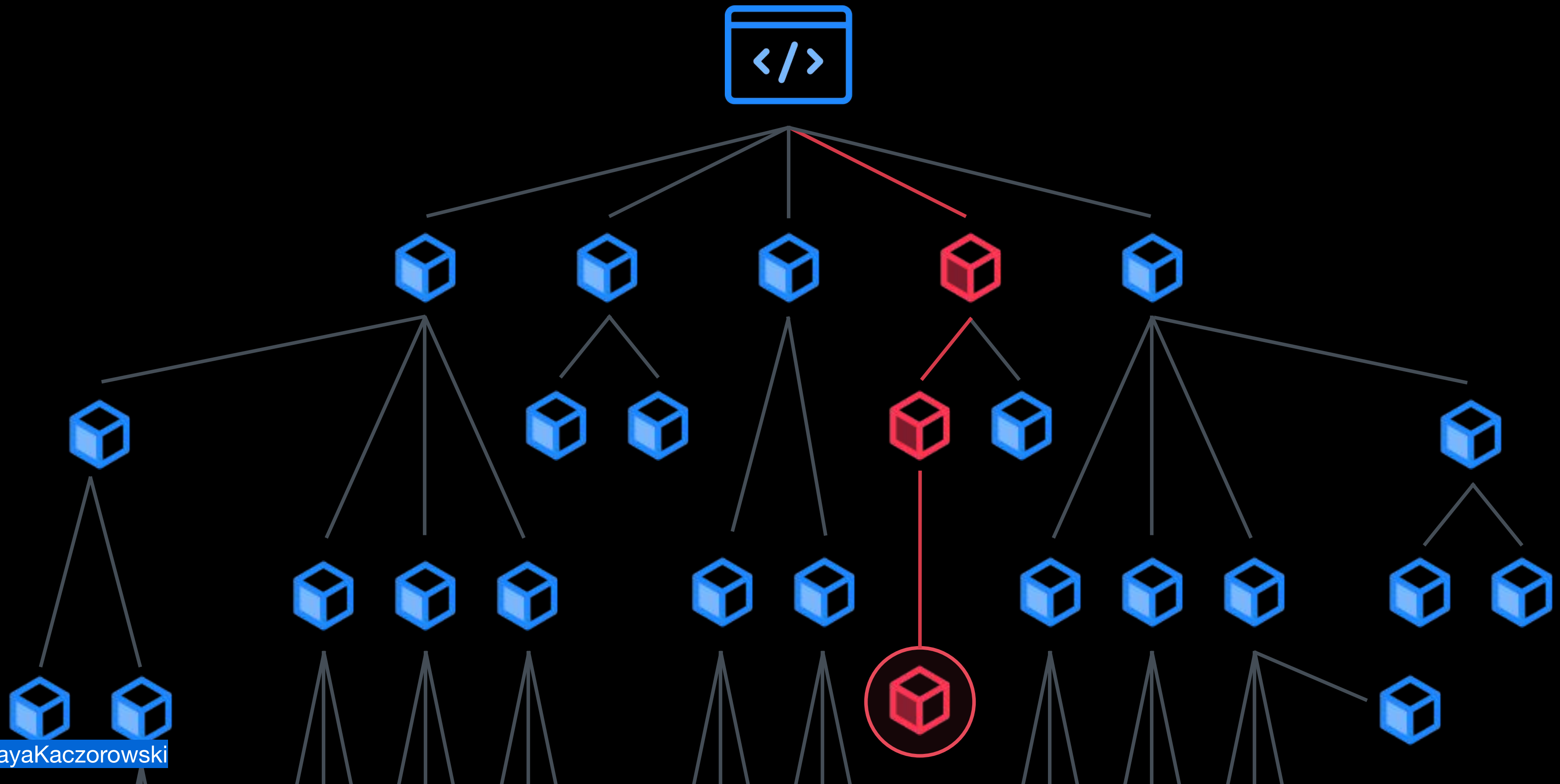
You don’t actually know what you’re running

- You don’t know what dependencies you have
- You don’t know what vulnerabilities you’ve introduced

A software supply chain is anything that touches your code - from development, through your CI/CD pipeline, until it gets deployed into production.



@MayaKaczorowski



@MayaKaczorowski

Supply chain attacks

Method

- Malicious code
  - e.g., backdoor, malware, known vulnerability
- Compromised build tool
- Compromised signing keys
- Account takeover
- Project takeover
- Accidental, e.g., typosquatting

Impact

- Backdoor, e.g., targeted, watering hole
- Malware, e.g., cryptocurrency mining
- Service disruption, e.g., deletion

event-stream

Widely used npm library

Method: Project takeover

“he emailed me and said he wanted to maintain the module, so I gave it to him. I don't get any thing from maintaining this module, and I don't even use it anymore, and havn't for years.”

Impact: Backdoor

Highly targeted to Copay developers, to distribute malware to capture credentials for Dash Copay bitcoin wallets

- `right9ctrl` volunteered to take over the package on GitHub, then added `flatmap-stream` as a dependency
- Another user `hugeglass` added malware to steal credentials to bitcoin wallets to `flatmap-stream`
- Profit

https://blog.npmjs.org/post/180565383195/details-about-the-event-stream-incident

left-pad

11-line npm library

Method: Deletion
“I think I have the right of deleting all my stuff”

Impact: Service disruption
Major packages like React

- `kik` library maintainer approached by Kik.com for copyright reasons
- Deletes 273 packages, including `left-pad`
- Reverted within 2 hours

https://qz.com/646467/how-one-programmer-broke-the-internet-by-deleting-a-tiny-piece-of-code/

docker123321

17 Docker Hub images

Method: Accidental
Easy to type registry name

Impact: Malware
Mining ~$90k of Monero

- 17 images in `docker123321` registry
- Contained malware since at least July 2017
- Suspected malware, positively identified as part of a cryptomining botnet
- Removed by Docker Hub in May 2018

https://kromtech.com/blog/security-center/cryptojacking-invades-cloud-how-modern-containerization-trend-is-exploited-by-attackers

bootstrap-sass

Malicious RubyGem

Method: Compromised signing keys?
New signed, published version with no code on GitHub

Impact: Backdoor
Tries to execute a cookie if in prod

- New version of RubyGem `bootstrap-sass` published
  - Same signing key
  - No GitHub repo
- Detected as suspicious and removed within an hour!
- ~1600 projects pulled in vulnerable version

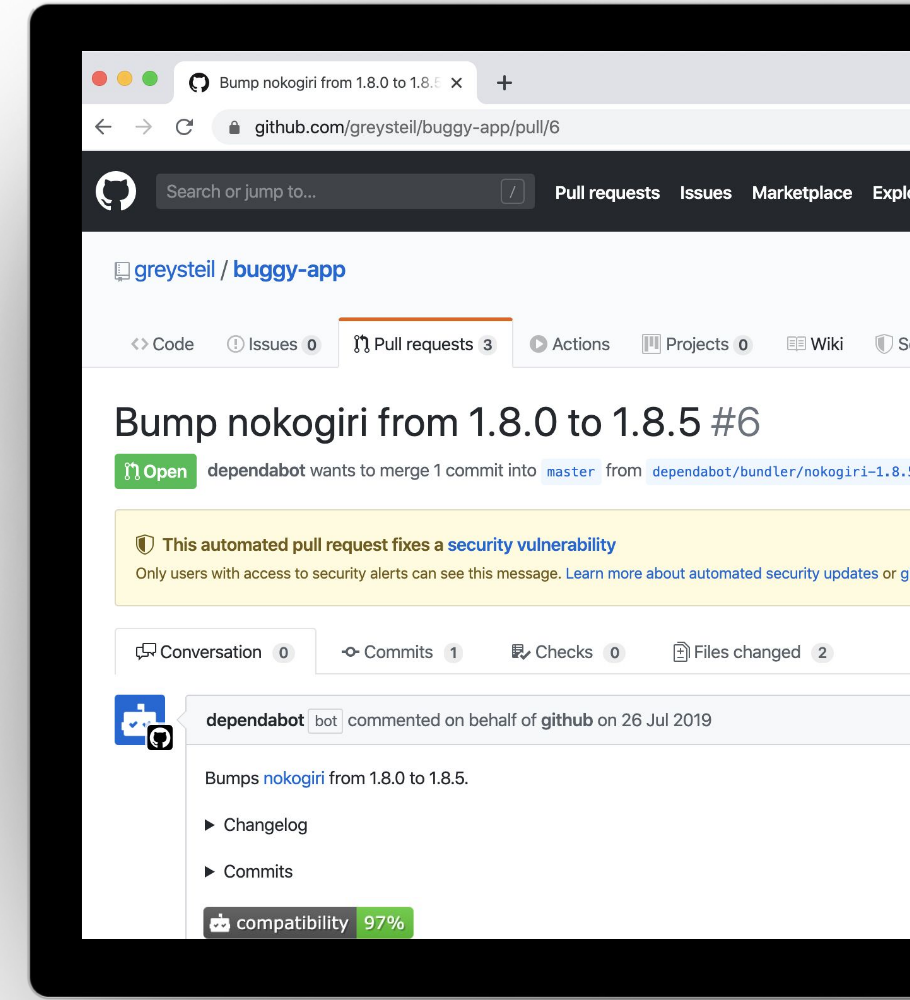
https://snyk.io/blog/malicious-remote-code-execution-backdoor-discovered-in-the-popular-bootstrap-sass-ruby-gem/

What can you do, as a developer?

- Figure out your dependencies
  - Declare them explicitly
- Remove unnecessary dependencies
- Automate security updates
  - If your testing isn't that good, pay attention to security advisories
- Trust but verify
  - Security audits
  - Scan code, packages, e.g., `npm audit`
  - Check checksums

Turn on these GitHub features!

- [Security alerts]() to notify you of vulnerabilities in code dependencies
- [Automated Security updates]() generate a PR to move to a fixed version
- Generated automatically when a new vulnerable dependency is found
- Supports Composer, Maven, npm, NuGet, pip, and RubyGems



Bump nokogiri from 1.8.0 to 1.8.5 #6

Open dependabot wants to merge 1 commit into `master` from `dependabot/bundler/nokogiri-1.8.`

This automated pull request fixes a security vulnerability

Only users with access to security alerts can see this message. Learn more about automated security updates or g

dependabot bot commented on behalf of github on 26 Jul 2019

Bumps nokogiri from 1.8.0 to 1.8.5.

▸ Changelog

▸ Commits

compatibility 97%

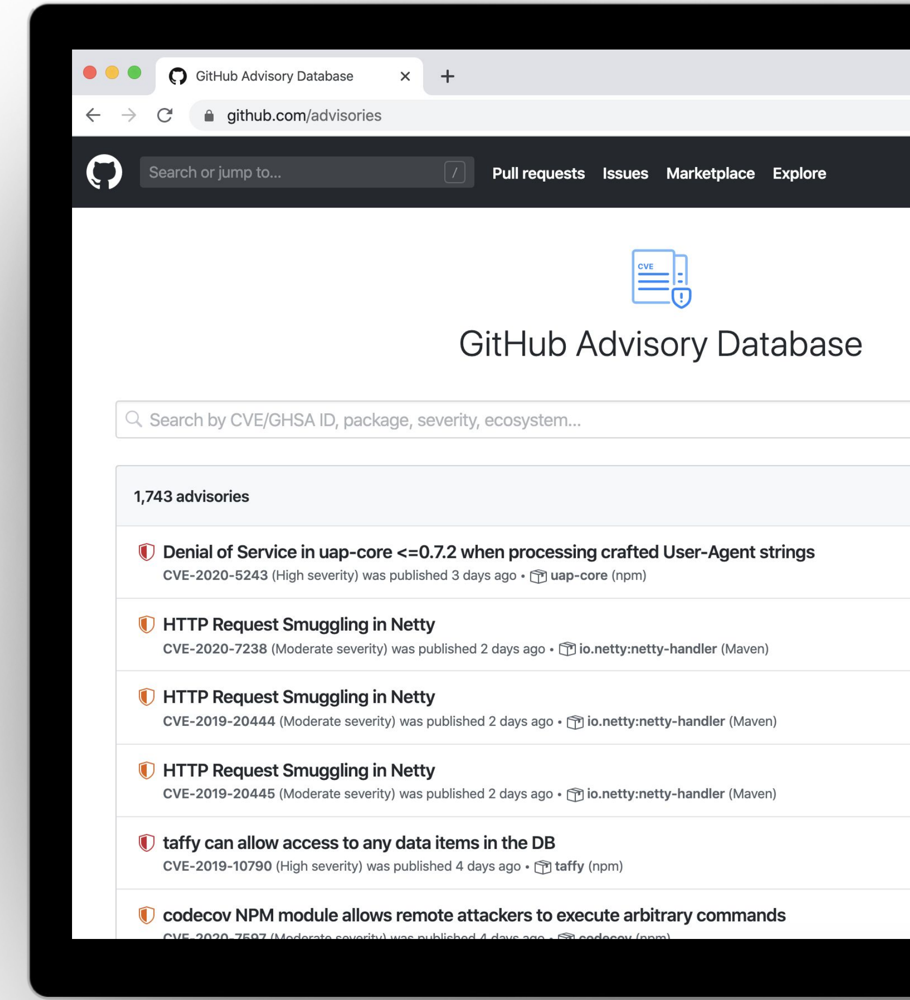
@MayaKaczorowski

If you find a vulnerability, what should you do?

- If you're not the maintainer: Disclose responsibly
  - Check the project's instructions, email maintainer
  - Check the security.md file
- If you're the maintainer:
  - Security Advisory
  - Kubernetes' security release process
  - Create a security.md file

Create a Security Advisory

- **Security Advisories** are used to disclose vulnerabilities in projects hosted on GitHub
- If applicable, GitHub can also help you get a CVE
- Curated and aggregated with third-party sources into GitHub's Advisory Database, which is open source



GitHub Advisory Database

Search by CVE/GHSA ID, package, severity, ecosystem...

1,743 advisories

Denial of Service in uap-core <=0.7.2 when processing crafted User-Agent strings
CVE-2020-5243 (High severity) was published 3 days ago • **uap-core** (npm)

HTTP Request Smuggling in Netty
CVE-2020-7238 (Moderate severity) was published 2 days ago • **io.netty:netty-handler** (Maven)

HTTP Request Smuggling in Netty
CVE-2019-20444 (Moderate severity) was published 2 days ago • **io.netty:netty-handler** (Maven)

HTTP Request Smuggling in Netty
CVE-2019-20445 (Moderate severity) was published 2 days ago • **io.netty:netty-handler** (Maven)

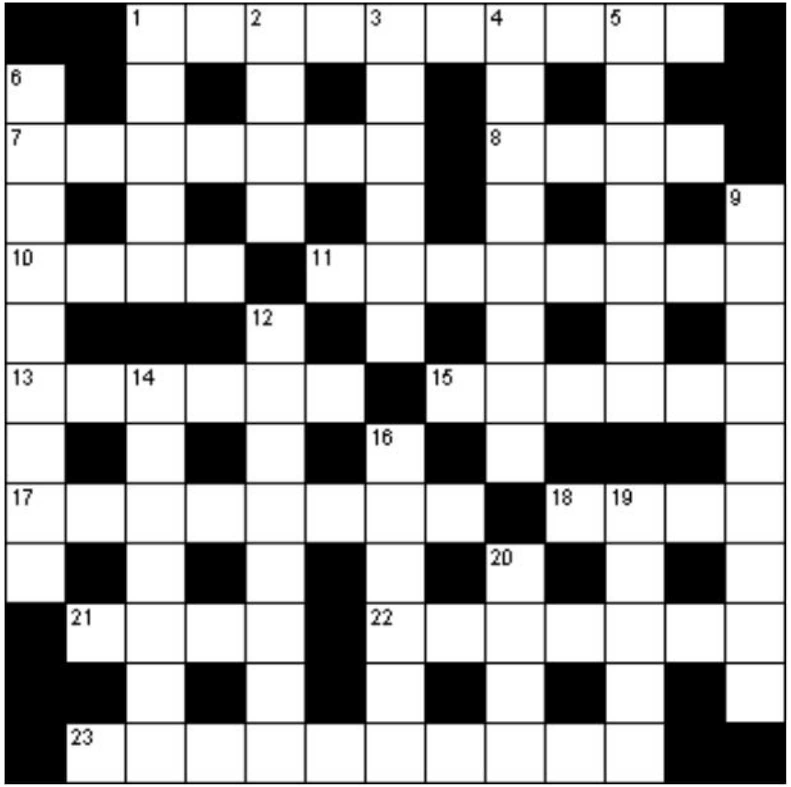
taffy can allow access to any data items in the DB
CVE-2019-10790 (High severity) was published 4 days ago • **taffy** (npm)

codecov NPM module allows remote attackers to execute arbitrary commands
CVE-2020-7597 (Moderate severity) was published 4 days ago • **codecov** (npm)

OK, now for cryptic crosswords!

@MayaKaczorowski

21 March



@MayaKaczorowski

In a cryptic crossword,

Each individual clue is its own puzzle.

A good cryptic clue contains three elements:

- a precise definition;
- a fair subsidiary indication;
- nothing else.

- Azed

Literal

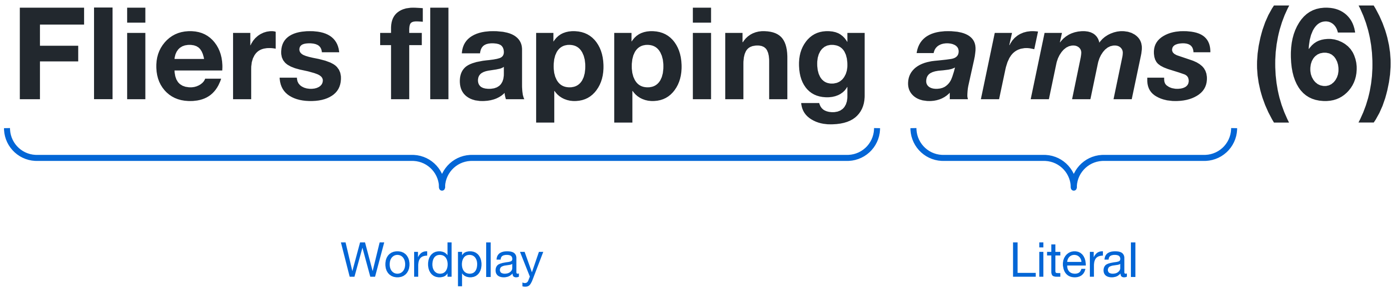
- Clues the meaning of the words
- Like a normal crossword clue

+

Wordplay

- Clues how to modify words and letters
- Like a rebus
- Standard patterns

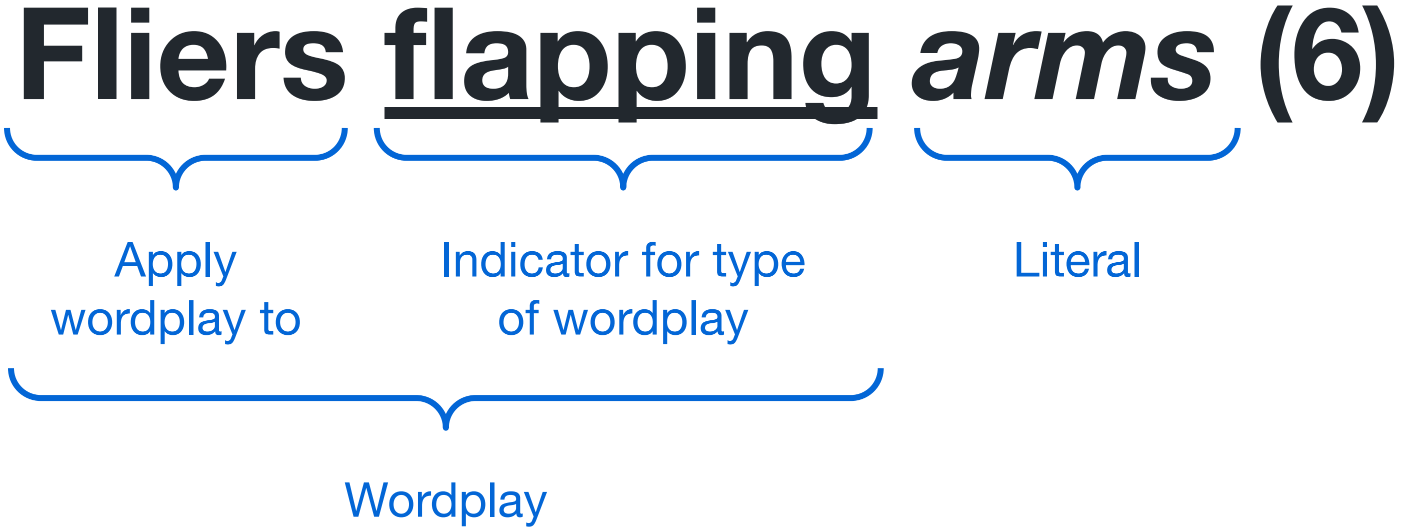
Fliers flapping arms (6)



Fliers flapping *arms* (6)

Wordplay

Literal



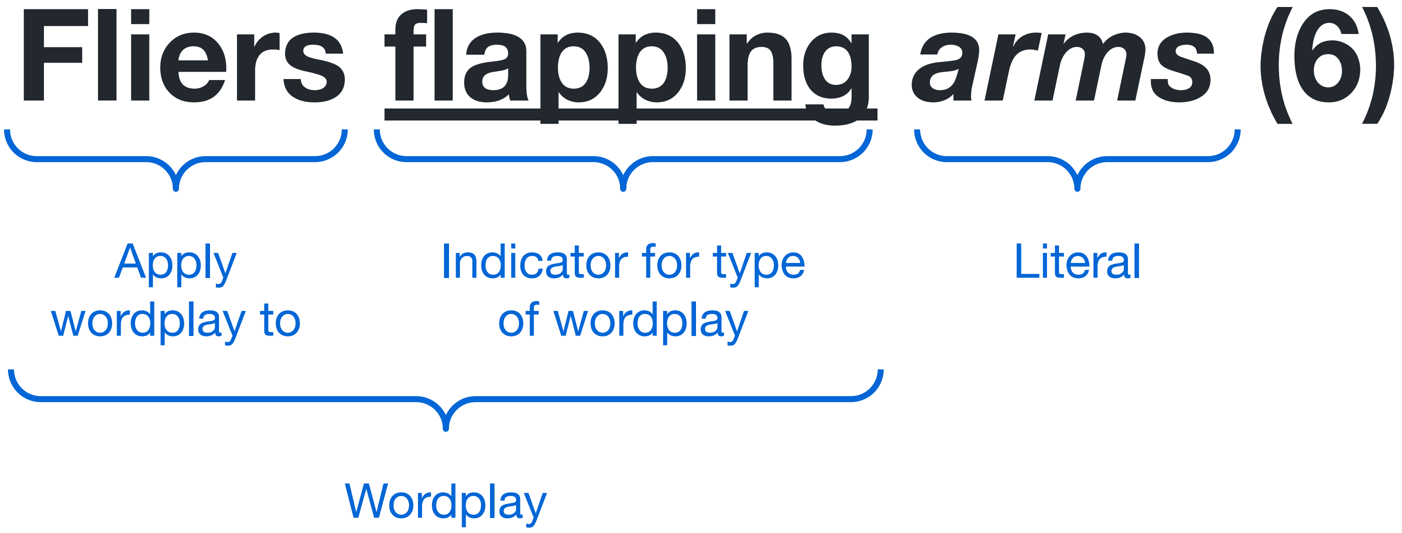
Fliers flapping *arms* (6)

Apply wordplay to

Indicator for type of wordplay

Literal

Wordplay



Fliers flapping *arms* (6)

Apply wordplay to

Indicator for type of wordplay

Literal

Wordplay

= RIFLES

Types of wordplay

- Anagram
- Addition
- Removal
- Reversal
- Hidden
- Homophone

- **Anagram**
- Addition
- Removal
- Reversal
- Hidden
- Homophone

@MayaKaczorowski

Example of wordplay

Scattered rain in the *country* (4)

IRAN

Indicator for this type of wordplay

“changed”

“worked”

“in error”

“upset”

- Anagram
- **Addition**
- Removal
- Reversal
- Hidden
- Homophone

Example of wordplay

Arrive holding container *to join together* (5)

COMBINE

Indicator for this type of wordplay

"in"

"with"

"retain"

"hold"

@MayaKaczorowski

- Anagram
- Addition
- **Removal**
- Reversal
- Hidden
- Homophone

Example of wordplay

Remove end of off *adorable* (3)

CUT

Indicator for this type of wordplay

“cut”

“short”

“almost”

“headless”

- Anagram
- Addition
- Removal
- **Reversal**
- Hidden
- Homophone

Example of wordplay

Ring up about one *garden shrub* (5)

LILAC

Indicator for this type of wordplay

“in reverse”

“up”

- Anagram
- Addition
- Removal
- Reversal
- **Hidden**
- Homophone

Example of wordplay

Portents some women scorn (5)

OMENS

Indicator for this type of wordplay

“in”

“some”

“oddly”

“first of”

@MayaKaczorowski

- Anagram
- Addition
- Removal
- Reversal
- Hidden
- **Homophone**

Example of wordplay

Discuss location in *vision* (5)

SIGHT

Indicator for this type of wordplay

“hears”

“so to speak”

“said”

Punctuation?!?

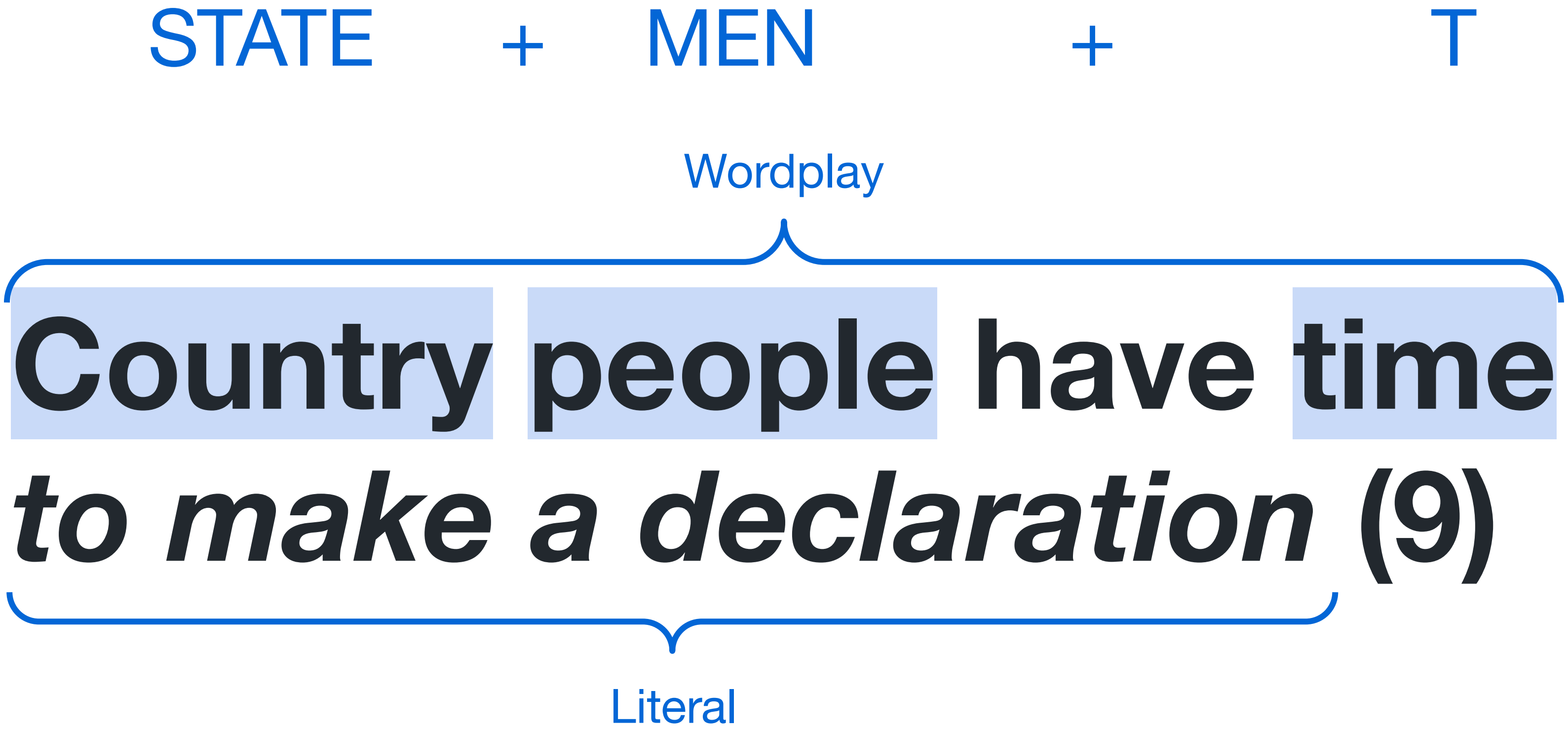
- Try breaking, up the clue "anywhere," that works

Country people have time to make a declaration (9)

Wordplay

Country people have time *to make a declaration* (9)

Literal



STATE + MEN + T

Wordplay

Country people have time ***to make a declaration*** **(9)**

Literal

STATE + MEN + T

Wordplay

Country people have time ***to make a declaration*** **(9)**

Literal

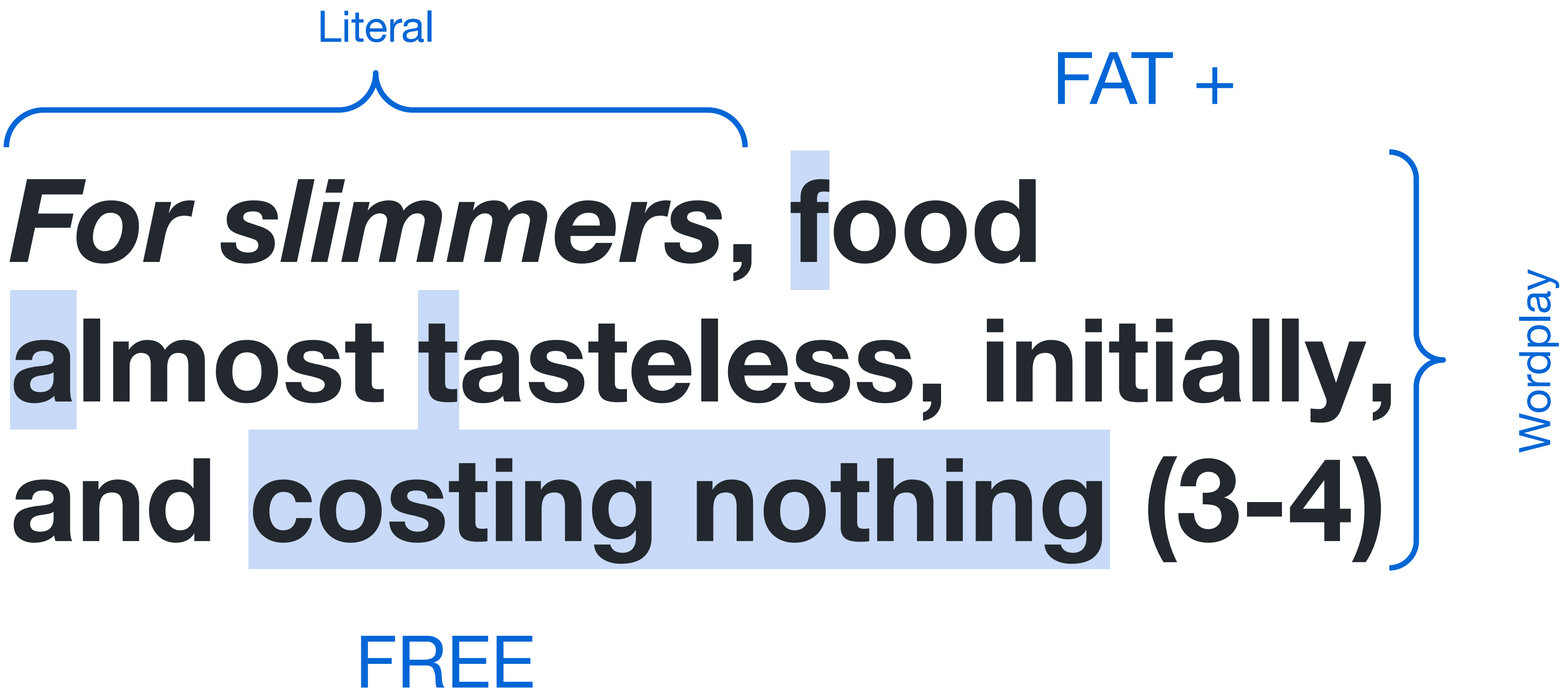
= STATEMENT

For slimmers, food almost tasteless, initially, and costing nothing (3-4)

Literal

***For slimmers*, food almost tasteless, initially, and costing nothing (3-4)**

Wordplay



Literal

FAT +

For slimmers, **food almost tasteless, initially, and costing nothing (3-4)**

Wordplay

FREE

@MayaKaczorowski

Literal

FAT +

***For slimmers,* food almost tasteless, initially, and costing nothing (3-4)**

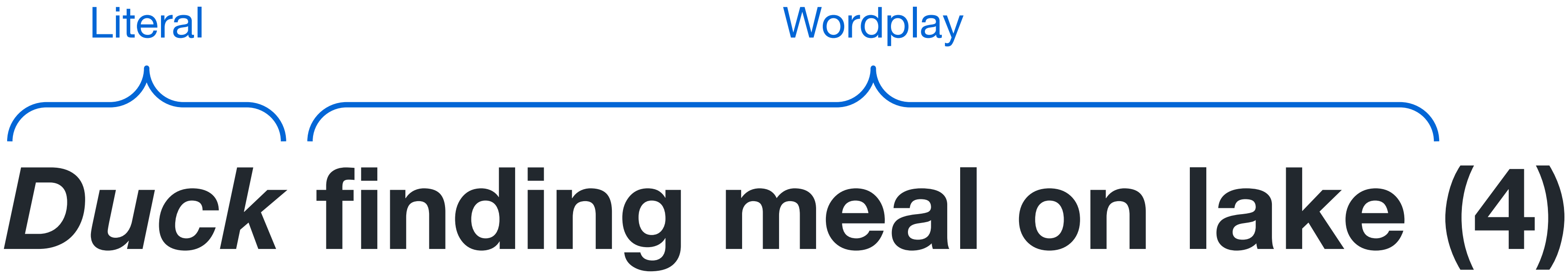
Wordplay

FREE

= FAT-FREE

@MayaKaczorowski

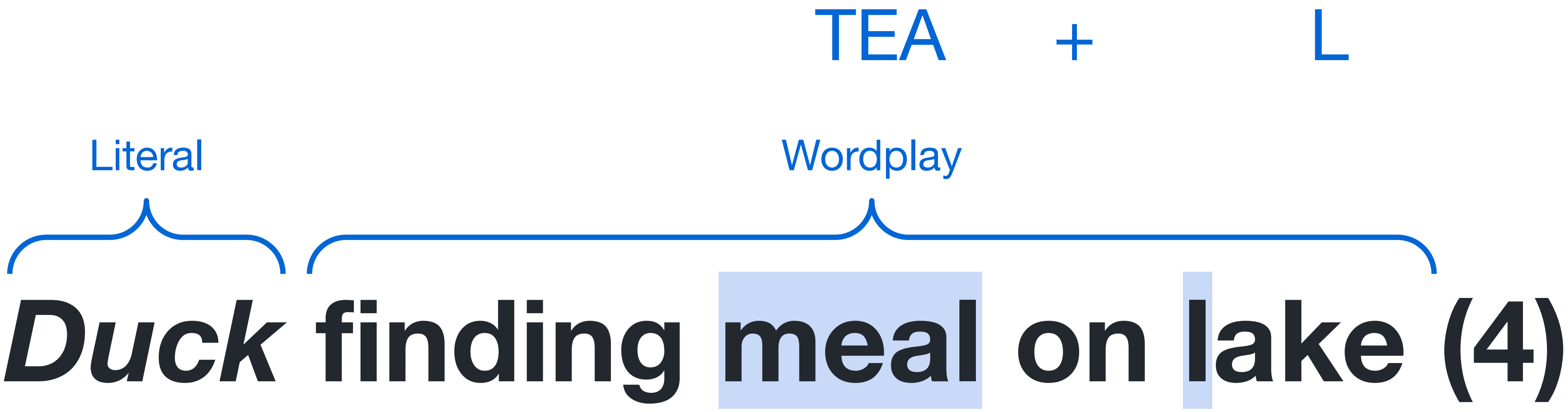
Duck finding meal on lake (4)



Literal

Wordplay

Duck **finding meal on lake (4)**

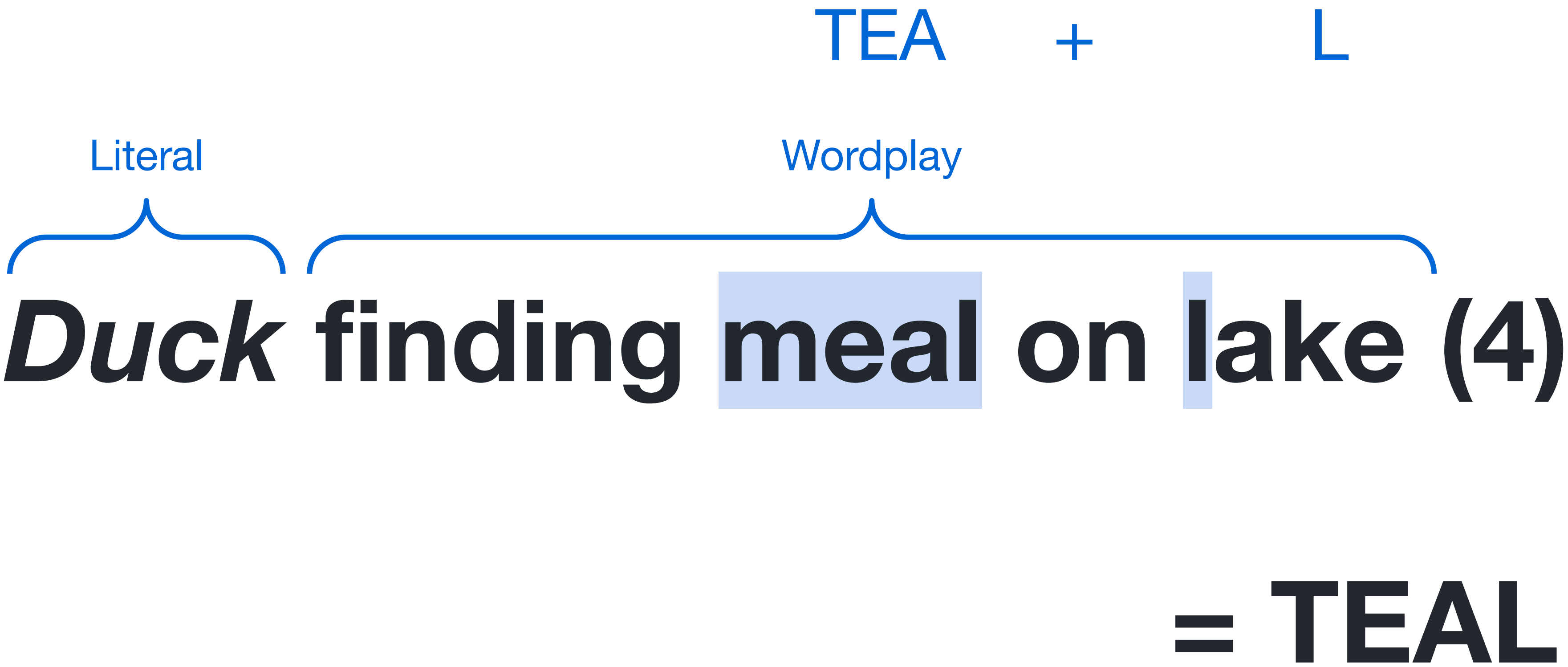


TEA + L

Literal

Wordplay

***Duck* finding meal on lake (4)**



TEA + L

Literal

Wordplay

Duck **finding meal on lake (4)**

= TEAL

@MayaKaczorowski

Let's make it harder!

Double definitions

Care for business (7)

CONCERN

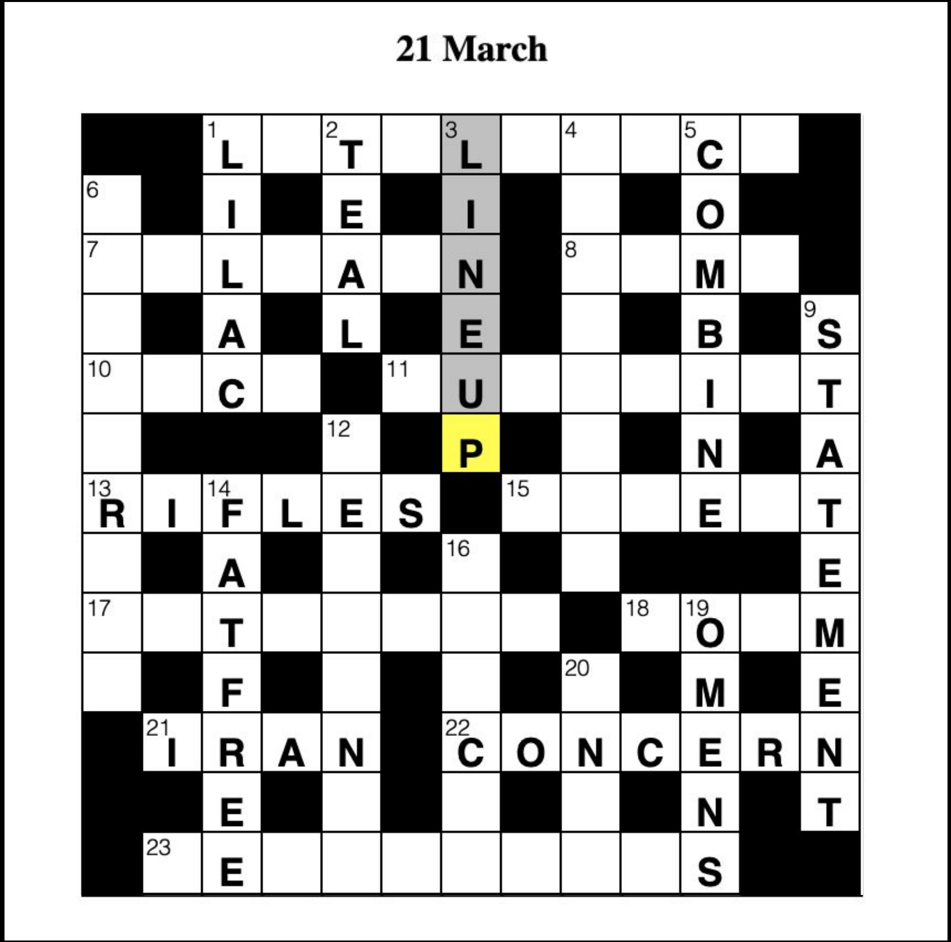
Extra(?) cryptic?

Queue to see railway being repaired? (4,2)

LINE UP

Variety cryptics

The puzzle will have extra letters, words, or changes



21 March

■	■	1 L		2 T		3 L		4		5 C		■
6	■	I	■	E	■	I	■		■	O	■	■
7		L		A		N	■	8		M		■
	■	A	■	L	■	E	■		■	B	■	9 S
10		C		■	11	U				I		T
	■	■	■	12	■	P	■		■	N	■	A
13 R	I	14 F	L	E	S	■	15			E		T
	■	A	■		■	16	■		■	■	■	E
17		T						■	18	19 O		M
	■	F	■		■		■	20	■	M	■	E
■	21 I	R	A	N	■	22 C	O	N	C	E	R	N
■	■	E	■		■		■		■	N	■	T
■	23	E								S	■	■

@MayaKaczorowski

Some of my favourite clues 🤩

Brief run, as of luck, for shot takers (6)

STREAK

- “Shooting Hoops”, Mar 2016, Cryptic News, Wall Street Journal

Curves for dad (he’s with sister) (11)

PARENTHESIS

- Puzzle Boat 6, Oct 2019, Puzzles and Answers Magazine

Learn more:
Dependency management

Supply chain compromises:
https://github.com/cncf/sig-security/tree/master/supply-chain-security/compromises

Turn on security alerts:
https://help.github.com/en/github/managing-security-vulnerabilities/about-security-alerts-for-vulnerable-dependencies
Turn on automated security updates:
https://help.github.com/en/github/managing-security-vulnerabilities/configuring-automated-security-updates
Create a security advisory:
https://help.github.com/en/github/managing-security-vulnerabilities/creating-a-security-advisory

@MayaKaczorowski

Learn more:
Cryptic crosswords

Learning tools

- “How to crack cryptic crosswords”, Tim Moorey

Puzzles

- https://simplydailypuzzles.com/daily-cryptic/ EASY
- Cryptic News, Wall Street Journal MED-HARD
- www.crypticallstars.com HARD

Questions? Concerns? Comments?