"UYR"
Under Your Radar

Covert Channel & Exfiltration

Ali Hadi / Mariam Khader

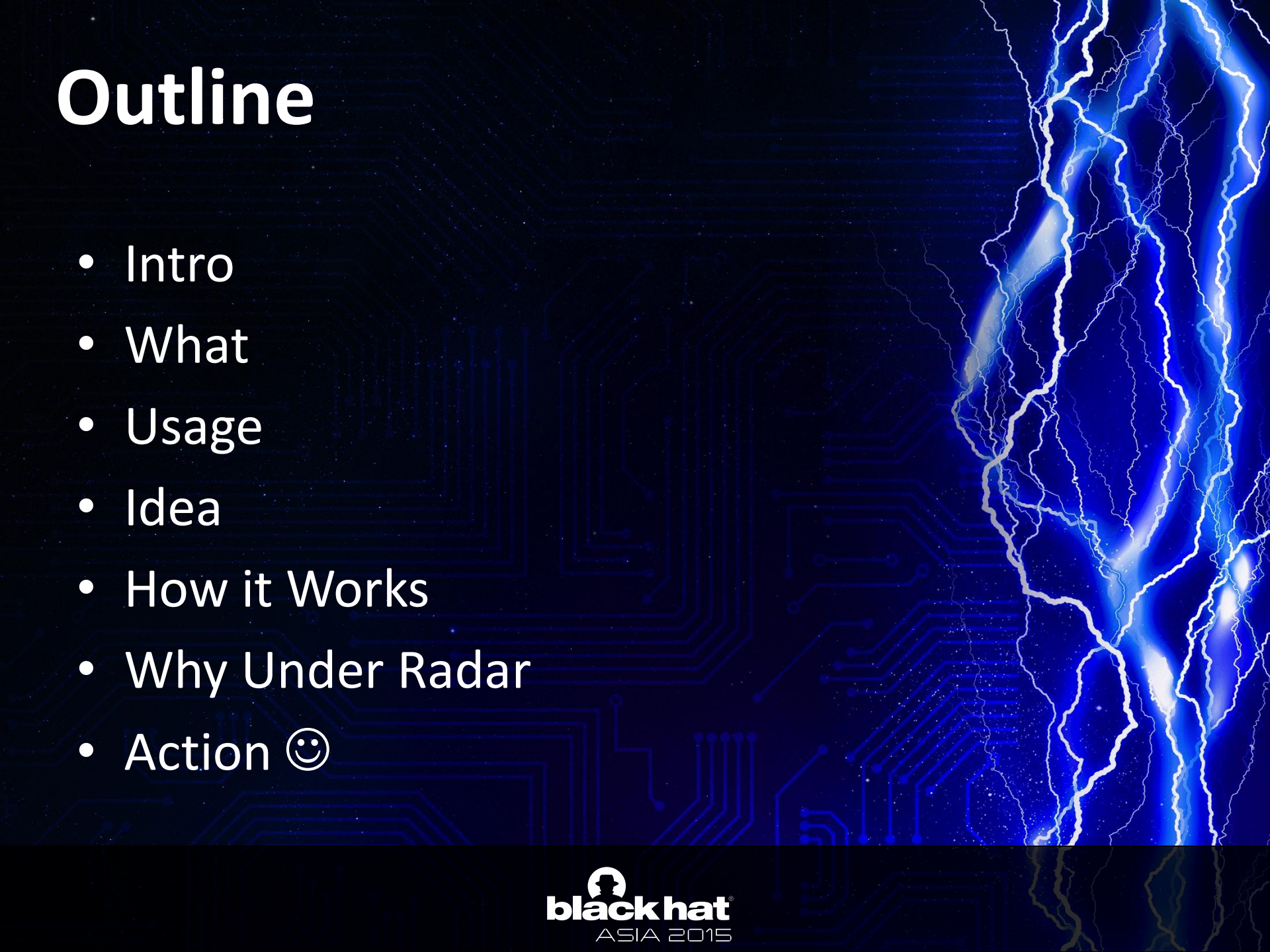
Princess Sumaya University for Technology (PSUT)

Amman/Jordan

black hat
ASIA 2015

Outline

- Intro
- What
- Usage
- Idea
- How it Works
- Why Under Radar
- Action ☺



Quick Intro.

- Steganography
  - Hiding the existence of the data
- Covert Channel
  - Unseen “secret” communication
- Exfiltration (aka *Exfil*)
  - Illegal retrieval of data from a compromised computer

Why Social Networks & Multimedia?

CISCO

EXPECTS VIDEO TO ACCOUNT FOR 69% OF ALL INTERNET TRAFFIC BY 2017

THE AVERAGE AMERICAN SPENT MORE THAN

20 HOURS

WATCHING ONLINE VIDEO IN SEPTEMBER 2013

facebook

46% OF TIME PEOPLE SHARE VIDEOS USING FACEBOOK

Windows Live Hotmail Gmail msn YAHOO!

40% OF THE TIME THEY USE EMAIL

twitter

14% THEY USE TWITTER

MOBILE VIDEO CONSUMPTION

INCREASED BY 41%

BETWEEN JANUARY 2013 & JUNE 2013

92% OF MOBILE VIDEO VIEWERS SHARE VIDEOS WITH OTHERS

MORE THAN 40%

OF YOUTUBE VIEWS ARE ON MOBILE DEVICES


YouTube
YOUTUBE RECEIVES MORE THAN
1,000,000,000
UNIQUE VISITORS EACH MONTH,
MORE THAN ANY OTHER CHANNEL,
APART FROM FACEBOOK

YouTube

THE WORLD'S LARGEST VIDEO SHARING PLATFORM

2nd LARGEST Search Engine

YouTube

YouTube 3rd Most Visited Website in the World

YouTube MOBILE gets over 100 Million views per day!

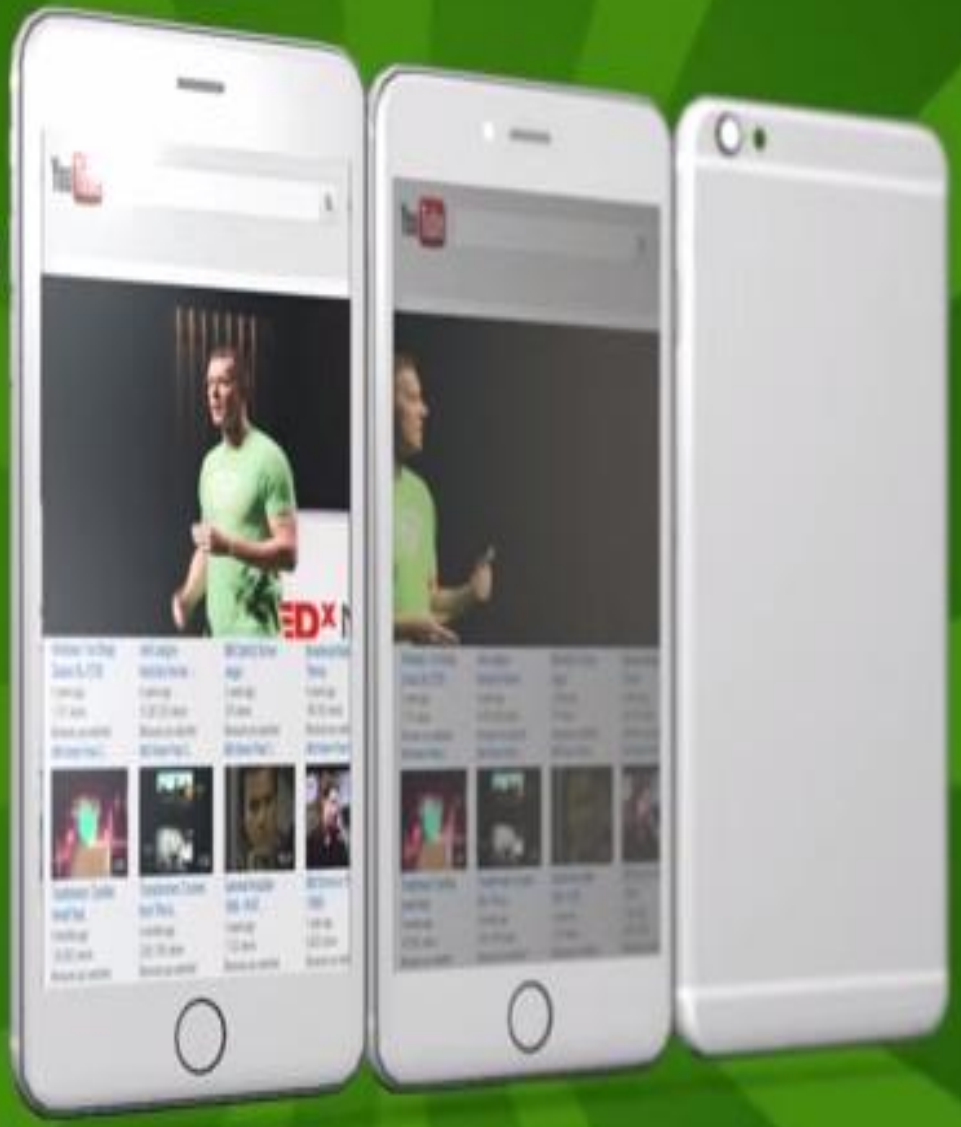
35 Hours of video footage is uploaded to the site every minute

That's over 18 million hours of footage in a single year!

OVER 3,000,000,000 VIDEOS are viewed every single day!

BY 2018 VIDEO
WILL ACCOUNT FOR

OVER 2/3
OF MOBILE USAGE



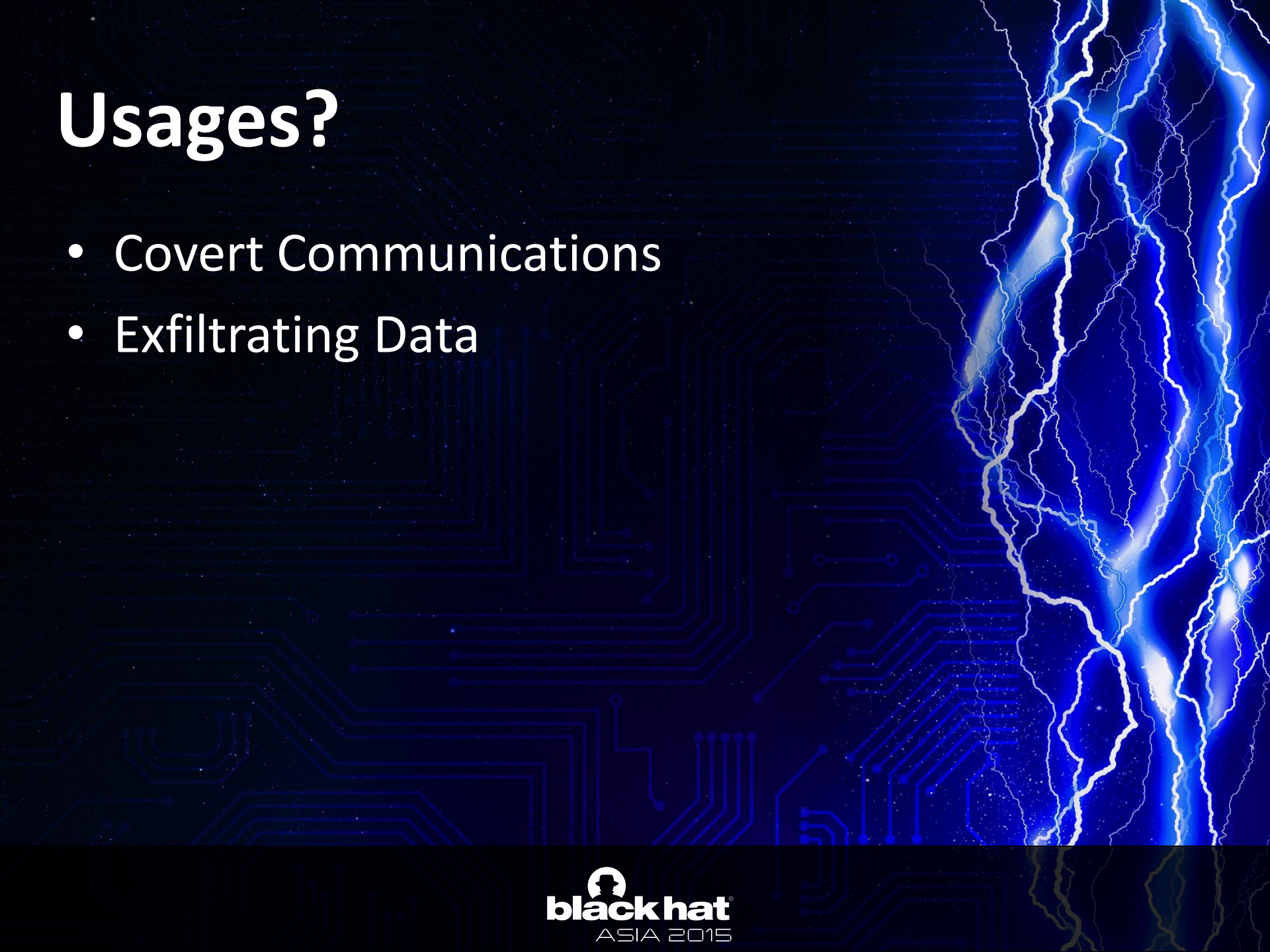
Hackers Exfiltrating Data with Video Steganography via Cloud Video Services [1]

What: UYR?

- New application layer covert channel and exfil system
- Applies multimedia stego techniques
- Hard for Radars to detect what's being sent

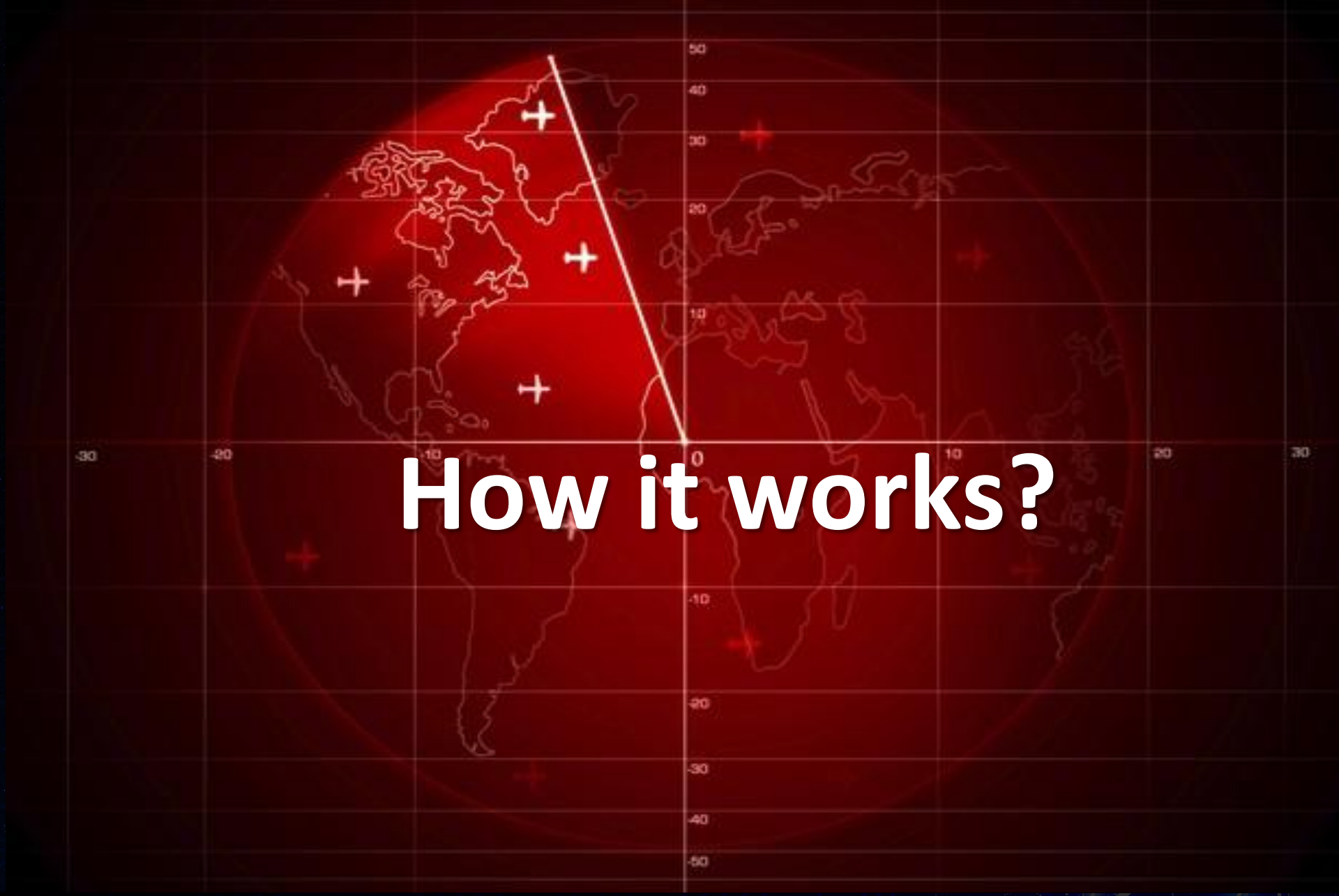
Usages?

- Covert Communications
- Exfiltrating Data



Idea?

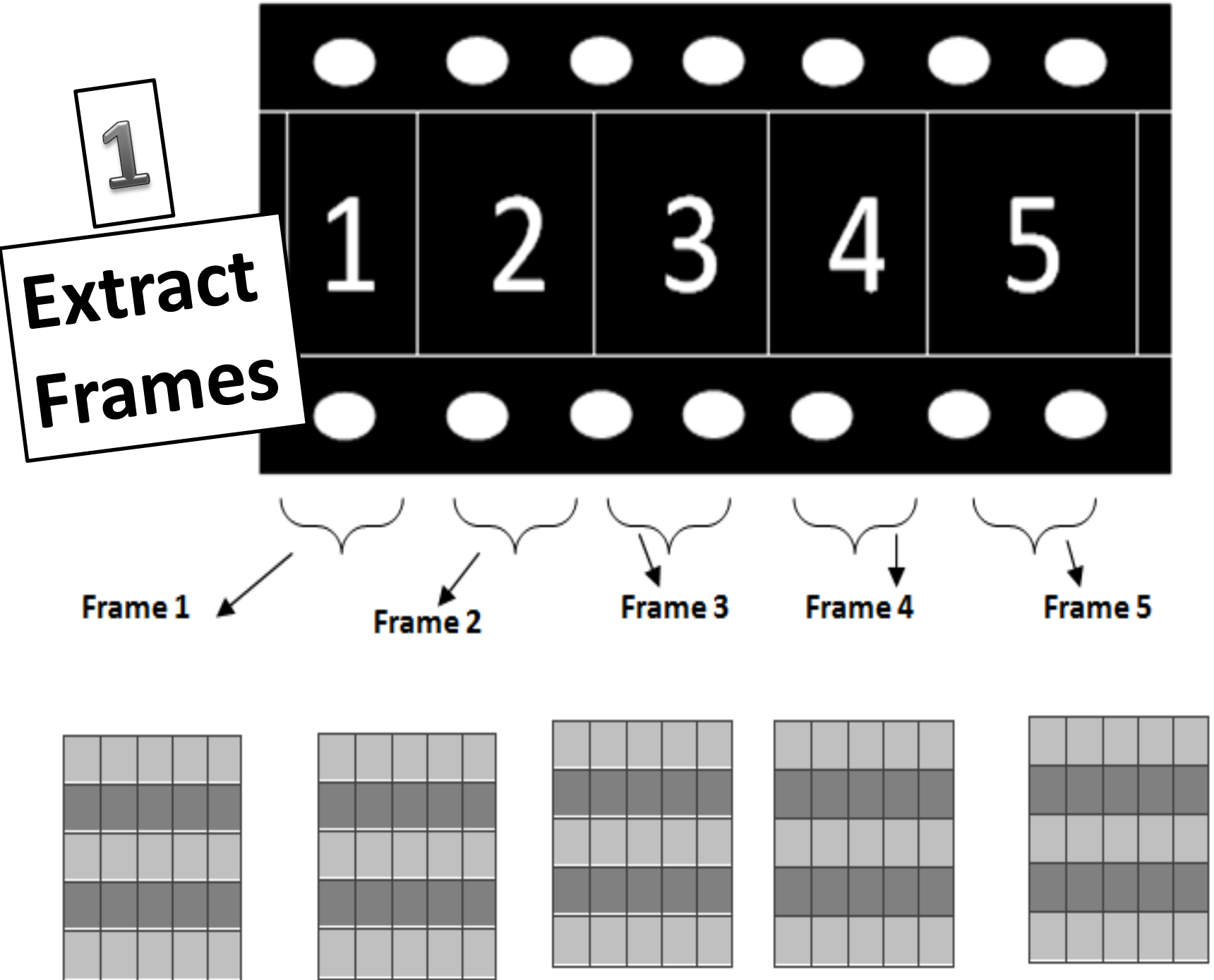
- No real data is transmitted!
- Only data transmitted is a bunch of numbers (key)!



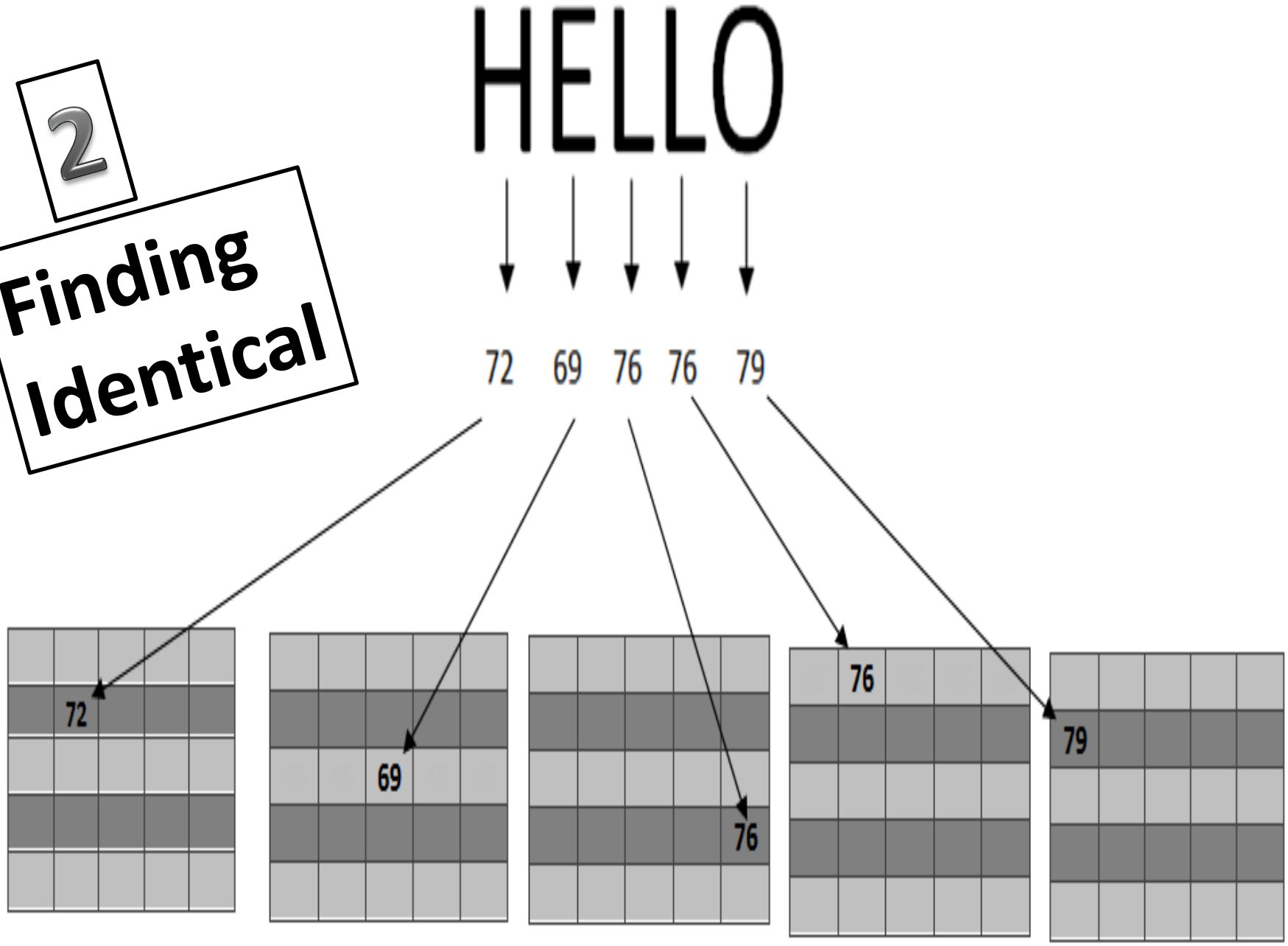
How it works?

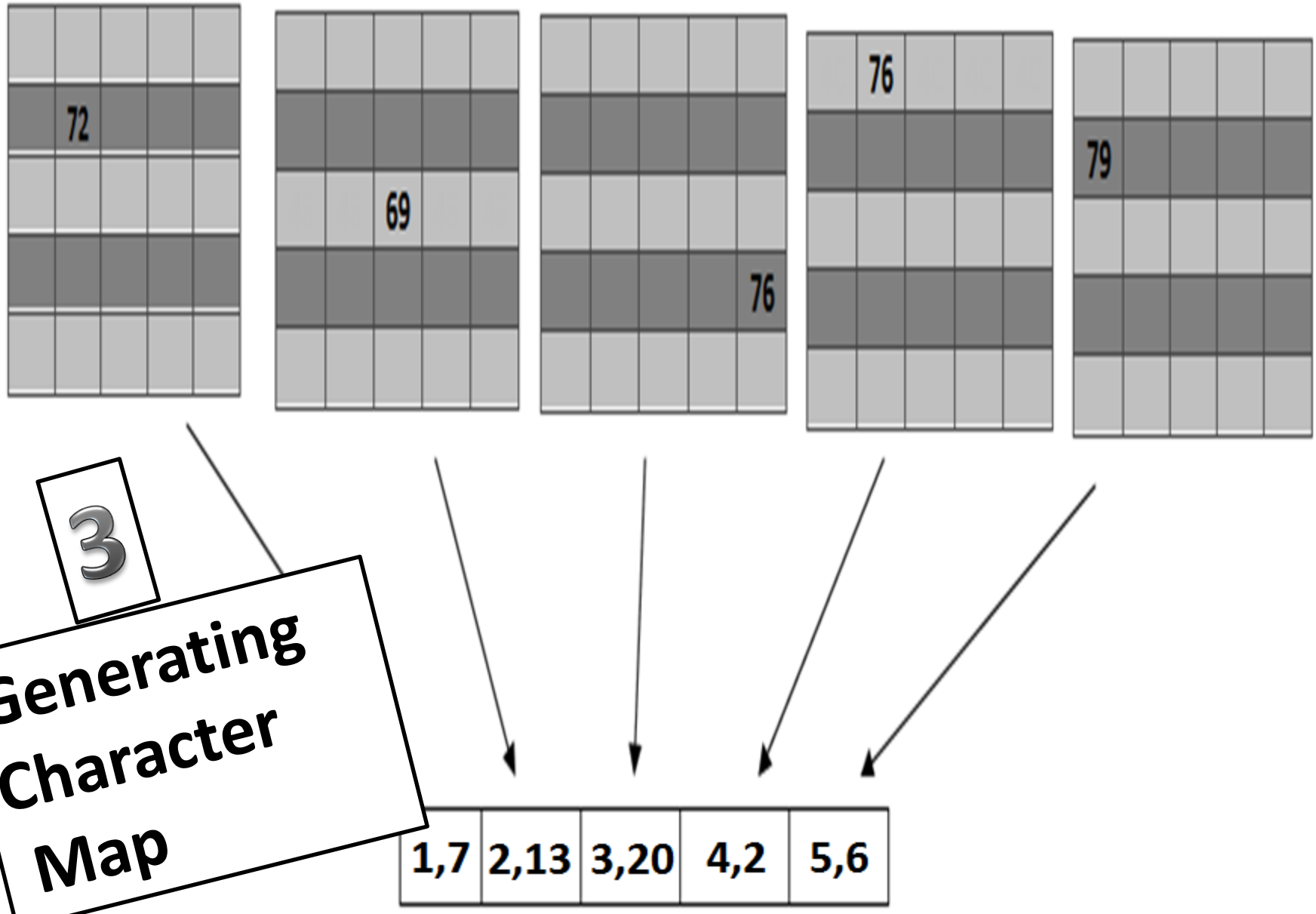
Protocol Agreements

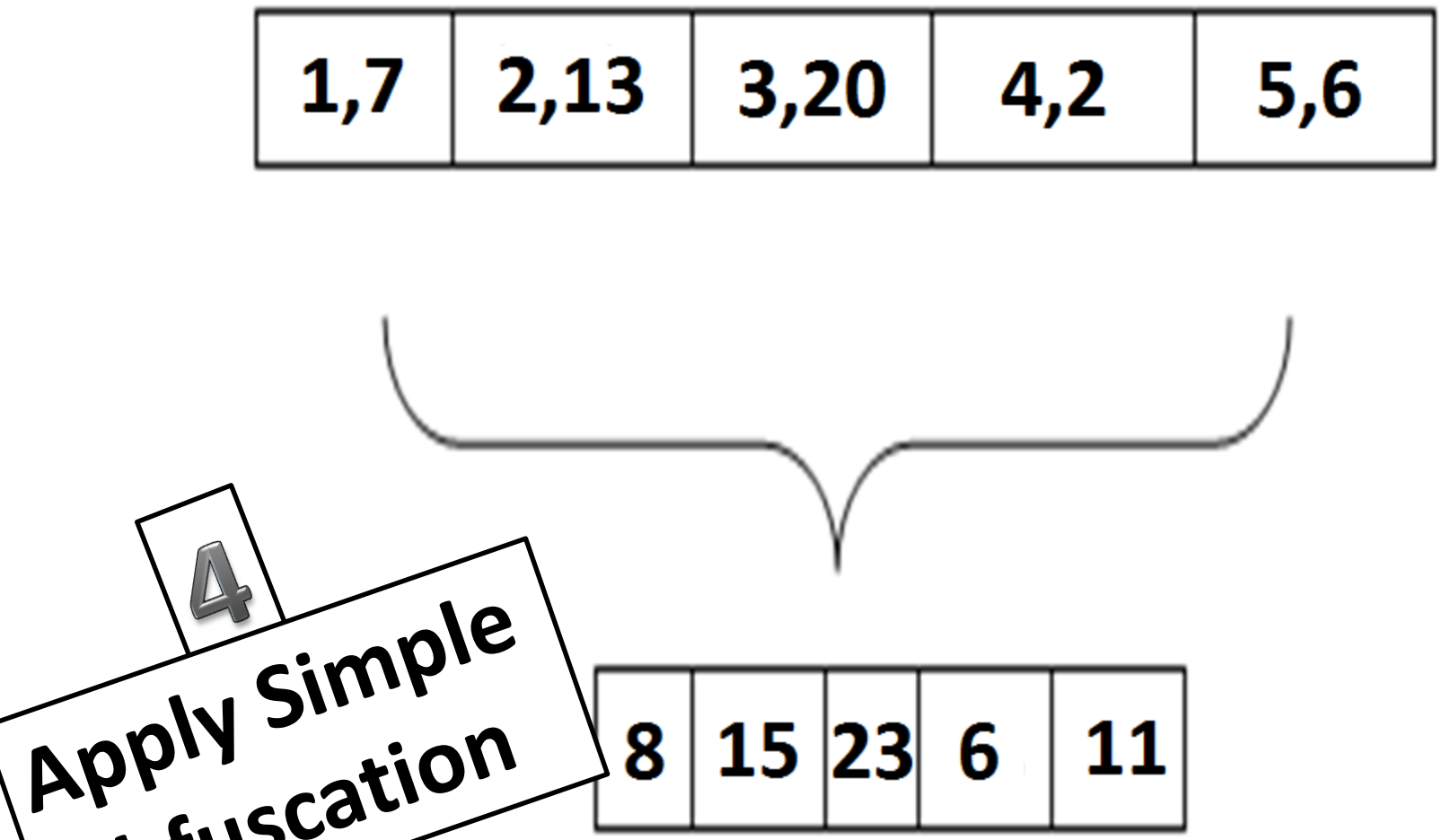
- Social Media Used
- Video Used


1
Extract Frames
1
2
3
4
5
Frame 1
Frame 2
Frame 3
Frame 4
Frame 5

2 Finding Identical




72
69
76
76
79
3
Generating Character Map
1,7
2,13
3,20
4,2
5,6


1,7
2,13
3,20
4,2
5,6
4
Apply Simple Obfuscation
8
15
23
6
11


Twitter
Upload Character Map

Extract Hidden Message/Data

Why Hard to Detect?

Evade current detection techniques

- UYR has no signature
- No pattern or anomaly
- No proof to correlate between the video + image used


Action

References

[1] http://tripwire.com/state-of-security/incident-detection/hackers-exfiltrating-data-with-video-steganography-via-cloud-video-services/

[2] Youtube, Cisco, and Google Stats, http://jlbmedia.com/online-video-impact-2014

[3] https://www.youtube.com/watch?v=QfVVfB_UHeA

[4] Twitter Stats, http://www.statisticbrain.com/twitter-statistics/

[5] UYR, https://github.com/Mariam118/UYR

Ali Hadi @binaryz0ne

Mariam Khader @MariamKhader118

Special Thanks

Princess Sumaya University for Technology (PSUT), our families, friends, security4arabs, and all those who supported us!