ICPAK

Uphold Public Interest

SOCIAL MEDIA & OPEN SOURCE INTELLIGENCE FOR INVESTIGATORS

Presentation by:

Faith Basiye

Head Forensic Services, KCB Bank Group, 13th October 2017

Pride Inn Paradise Beach Hotel, Mombasa

Uphold public interest

Presentation agenda

❑Social media
❑Social media landscape
❑Social media investigation
❑Open Source intelligence
❑Tools

Some Thoughts

“The Intelligence Community has to get used to the fact that it no longer controls most of the information.”

The Honorable Richard Kerr, former Deputy Director of Central Intelligence

Some Thoughts

Asked why he robbed banks, Willie Sutton famously replied: "Because that's where the money is."

Something similar can be said to explain why Investigators are paying more attention to social media these days – because that's where the people are!

Social Media Landscape

Social Media

Reason Why You Should Be Using Social Media as an Investigative tool

ICPAK
Uphold Public Interest

- ❑ More and more people are joining the online community
- ❑ 2/3 of the global internet population visit social network
- ❑ More people are spending more time on social media than any other major internet activity, including personal email

Reason Why You Should Be Using Social Media as an Investigative tool

□ Multi-platform use is on the rise:52% o online adults now use two or more social media sites

□ Social media is democratizing communications big time

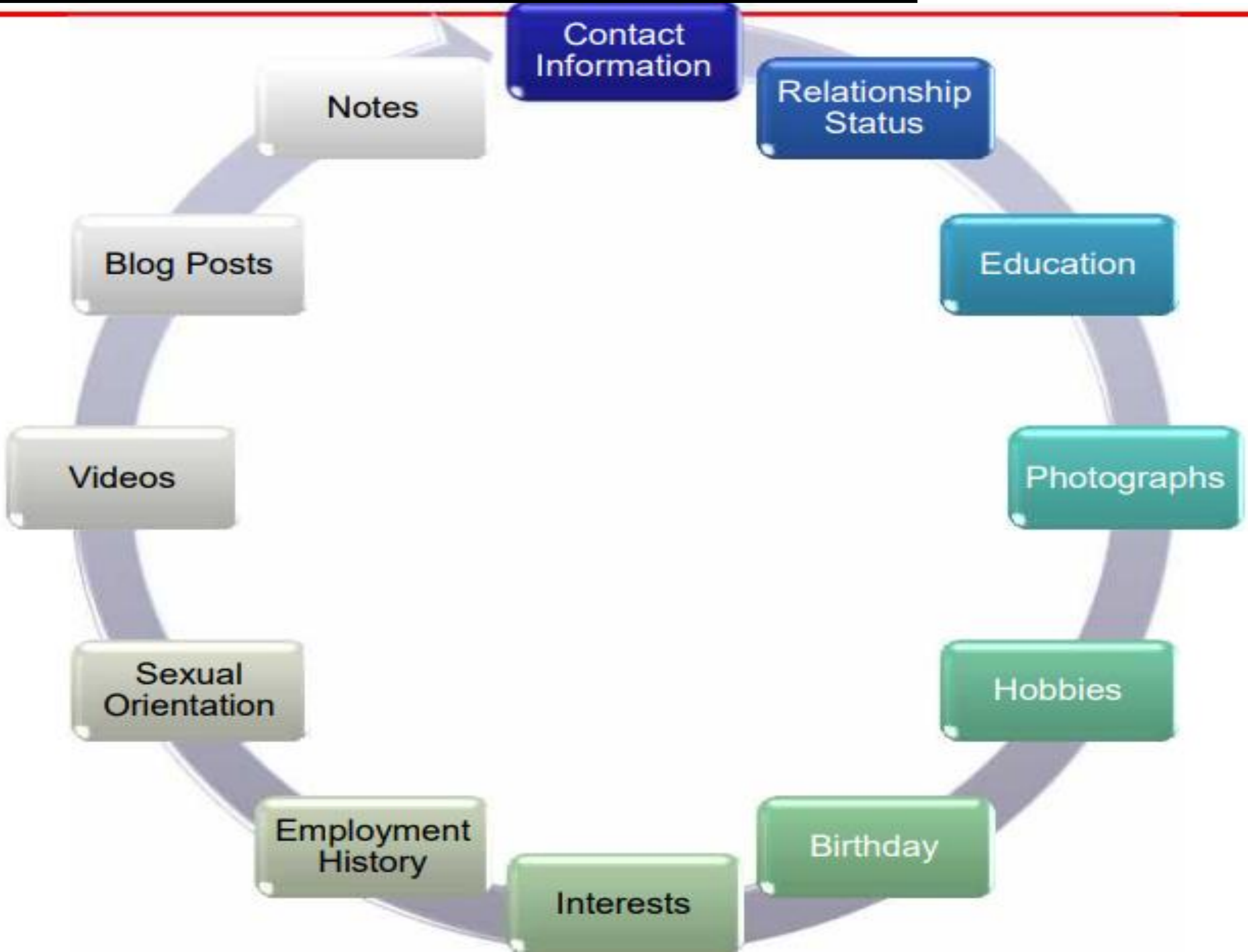
Reason Why You Should Be Using Social Media as an Investigative tool

Social media is like word of mouth on STEROIDS

13,000,000,000

The number of minutes spent on Facebook each day.

Social Media Profile



Contact Information

Relationship Status

Education

Photographs

Hobbies

Birthday

Interests

Employment History

Sexual Orientation

Videos

Blog Posts

Notes

Social Media Investigations

❑Investigate who an individual or business associate with:

FB- who are their friends

twitter- who does the individual or business follow or re-tweet

LinkedIn- organizations the individual or business belong to

Social Media Investigations

- ❑Google search algorithm- e.g “Faith Basiye” site: Instagram.com
- ❑Communications pattern
- ❑Times of activity and location data
- ❑Apps- what apps are being used and their purpose and information

Social Media Investigations

❑Consider searching for an individual's friends or family members

❑Don't leave footprints- browse LinkedIn in private mode

❑Photographs and videos can be useful for searching- google Reverse image and bing Image match search; fotoforensics.com

Social Media Investigations

- Google search algorithm- e.g “Faith Basiye” site: Instagram.com
- Communications pattern
- Times and places of activity
- Apps- what apps are being used and their purpose and information

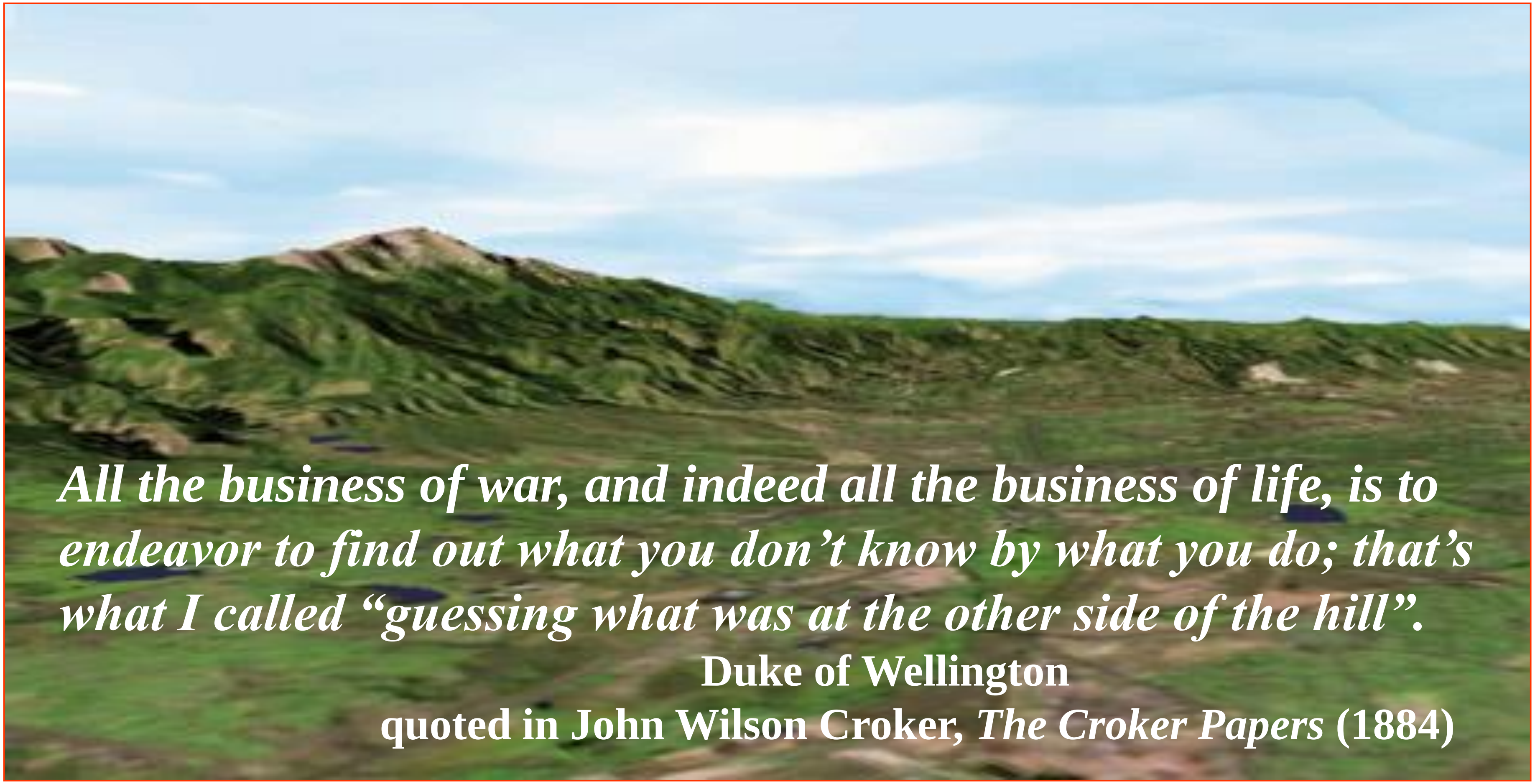
Investigative tools

- ❑Checkdesk, Bridge, Yomapic and Echosec

New

- ❑Montage- search for videos and tag specific moments
- ❑Hunch.ly- organizes information during online investigations by tracking activity and continually creating snapshots
- ❑Warwire- geotagged images, monitor locations and social media accounts

What's on the other side of the hill?



All the business of war, and indeed all the business of life, is to endeavor to find out what you don't know by what you do; that's what I called "guessing what was at the other side of the hill".

Duke of Wellington

quoted in John Wilson Croker, *The Croker Papers* (1884)

OSINT Definitions

- ❑ Open Source Data
- ❑ Open Source Information
- ❑ Open Source Intelligence
- ❑ *Validated* Open Source Intelligence

Only the in-house analyst can do this

OSINT Sources

❑Media-television, press, newspapers, magazines

❑Internet- social media, blogs, online forums

❑Public Government Data- gazette, speeches, briefings, directories

❑Professional and Academic Publications- journals, conferences

❑Grey Literature- graduate thesis

❑Commercial Data- financial &industrial evaluations

OSINT is a Process

- □ DISCOVERY--Know Who Knows

  Just enough from just the right mix of sources
- □ DISCRIMINATION--Know What's What

  Rapid source evaluation and data validation
- □ DISTILLATION--Know What's Hot

  Answer the right question, in the right way
- □ DELIVERY--Know Who's Who

  It's not delivered until right person understands

Step change

- ❑All this information cannot be found on a suspect’s hard drive

OSINT tools

- ❑ Maltego- covers both infrastructure and personal reconnaissance
- ❑ Shodan- grabs data from ports
- ❑ Metagoofil- extract metadata from target including MAC address
- ❑ Google hacking database
- ❑ The FOCA- network infrastructure mapping tool great for information extraction
- ❑ Exchangeable Image File Format (Exif) data viewers- geolocation for images on smartphones and cameras

OSINT tools

- ❑ Exchangeable Image File Format (Exif) data viewers- geo-location for images on smartphones and cameras
- ❑ Social Engineering toolkit- tool for various attack scenerios
- ❑ Cyberstalking tools for reconnaissance
- ❑ Passive recon- Mozilla Firfox add-ons in form of plugins

In Conclusion

- ❑ Everyone loves the magic bullet or the secret sauce. But you know what? It's not always that easy. Sometimes you just need some good old-fashioned time and sweat
- ❑ The social web is not structured in a way that lets you click a few buttons and have everything at your fingertips
- ❑ The only way you are going to become a good social media investigator is to join the party

Thank you!