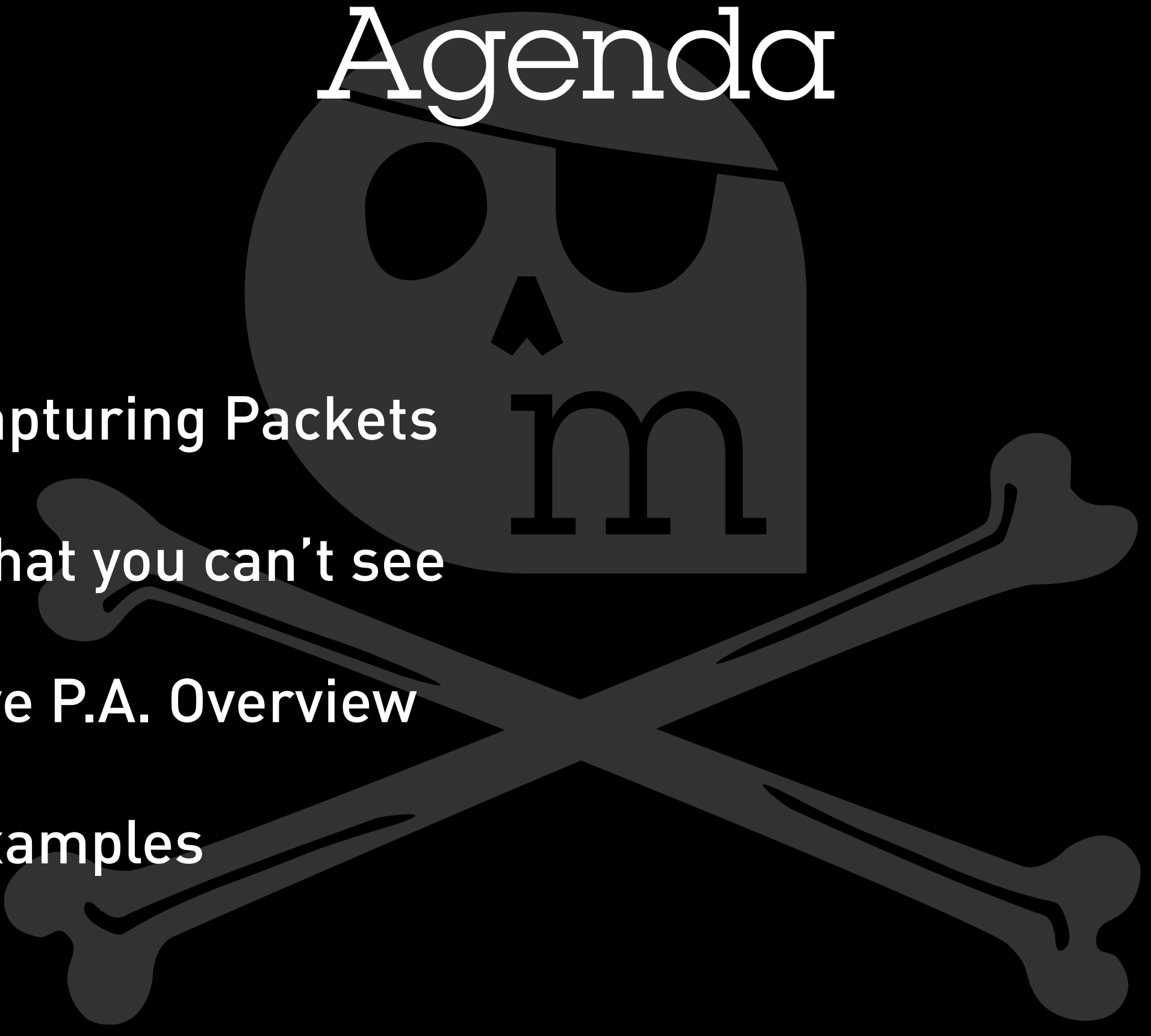




Wi-Fi Packet Analysis with Eye P.A.

Brian Tuttle
Geek Herder, MetaGeek

Agenda



- Capturing Packets
- What you can't see
- Eye P.A. Overview
- Examples

Agenda



- ➔ Eye P.A. Overview
- Capturing Packets
- What you can't see
- Examples

Agenda



- Eye P.A. Overview
- ➔ Capturing Packets
- What you can't see
- Examples

Capture at the AP

- Most reliably represents reality
- Can be done remotely
- Sometimes takes AP offline
- May not have all fields



Dedicated Adapter

- WildPackets Omnipeek Adapter
- Riverbed AirPcap
 - direct capture to Wireshark
 - direct capture to Eye P.A.
- Functional capture drivers
- No 802.11ac support
- USB limitations (2x2)



Use client adapter

- Tamosoft Commview
- Microsoft Network Monitor (no 802.11ac)
- Cheap/available
- Highly driver dependent
 - Data Rates unreliable
 - SNR Data unreliable
 - 40/80 MHz channels unavailable
- <http://www.tamos.com/products/commwifi/adapterlist.php>



Apple to the rescue

- Mac OSX Wireless Diagnostics
 - native, configurable packet capture
- 802.11ac capable hardware
 - if you have a newer laptop



Where to capture

- Where the problem is (DUH!)
- Get both sides, if possible
- Follow affected client(s)
 - know your channel plan



Agenda



- Eye P.A. Overview
- Capturing Packets
- ➔ What you can't see
- Examples

PLCP Headers/PPDU

- Represents a significant portion of airtime
- In general, “it just works”
- Information is transcribed to capture headers
 - PPI/Radiotap
 - accuracy/completeness are capture device dependent



Actual SNR

- MIMO
- Hardware differences
- If you suspect SNR issue
 - look for retransmits
 - try to capture at both ends



Invalid Packets

- Not indicative of a network problem
- Cannot be universally ignored
- Look for trustworthy trends

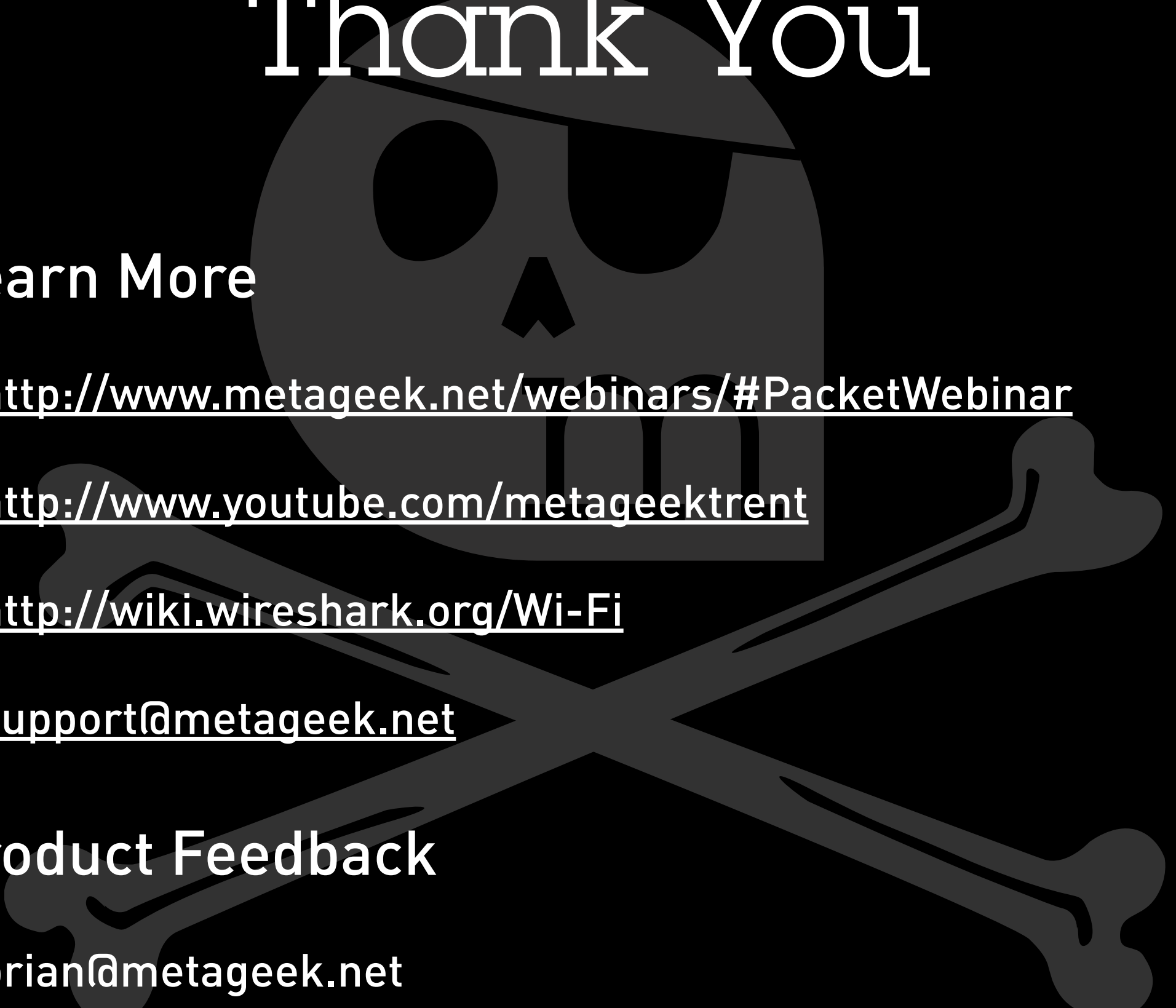


Agenda



- Eye P.A. Overview
- Capturing Packets
- What you can't see
- ➔ Examples

Thank You



- Learn More

- <http://www.metageek.net/webinars/#PacketWebinar>
- <http://www.youtube.com/metageektrent>
- <http://wiki.wireshark.org/Wi-Fi>
- support@metageek.net

- Product Feedback

- brian@metageek.net