Identify Common Cyber Network Attacks with Wireshark

When to Break Out Wireshark for Threat Hunting

Chris Greer
Protocol Analyst/Wireshark Instructor

@packetpioneer www.packetpioneer.com

Stop. Download Wireshark.
Get sample trace files.
Ok, continue...

Module Overview

How to approach packet-level analysis for incident response

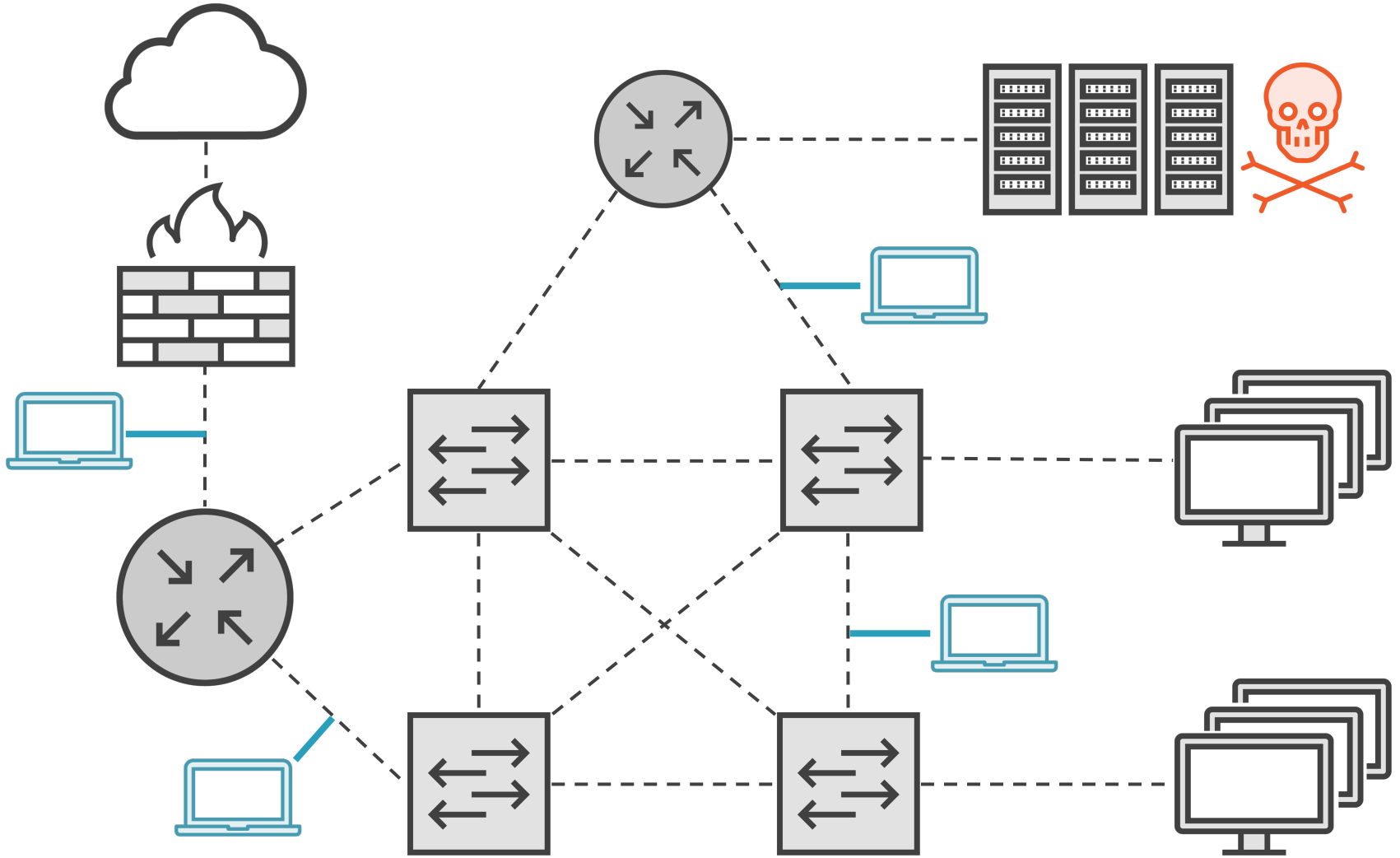
Where to capture? How to capture?

Where does Wireshark fit in?

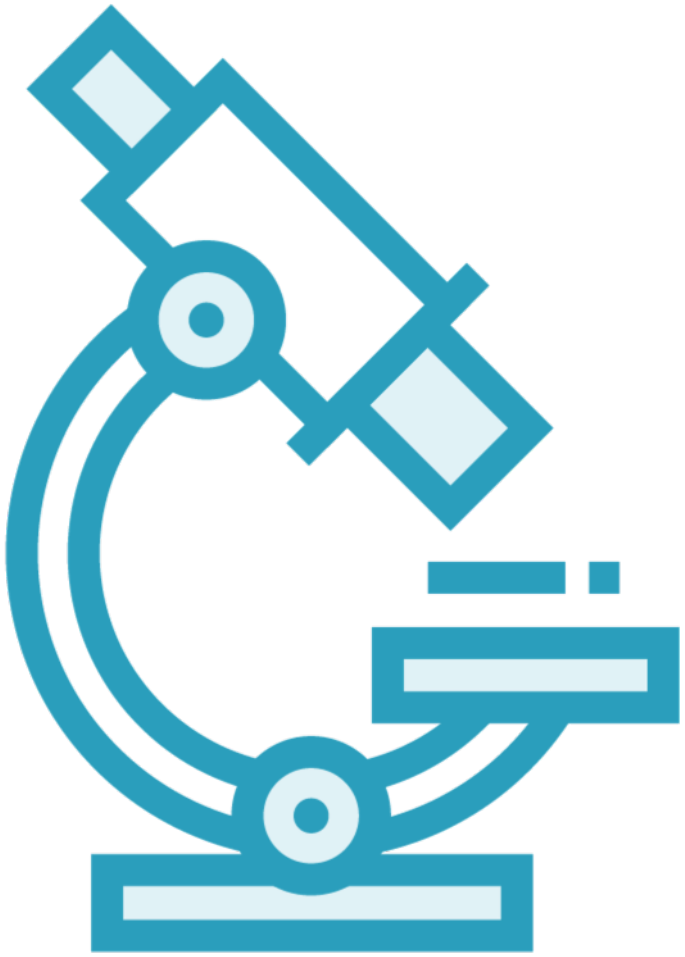
Packet Analysis and the MITRE ATT&CK Framework/Cyber Kill Chain

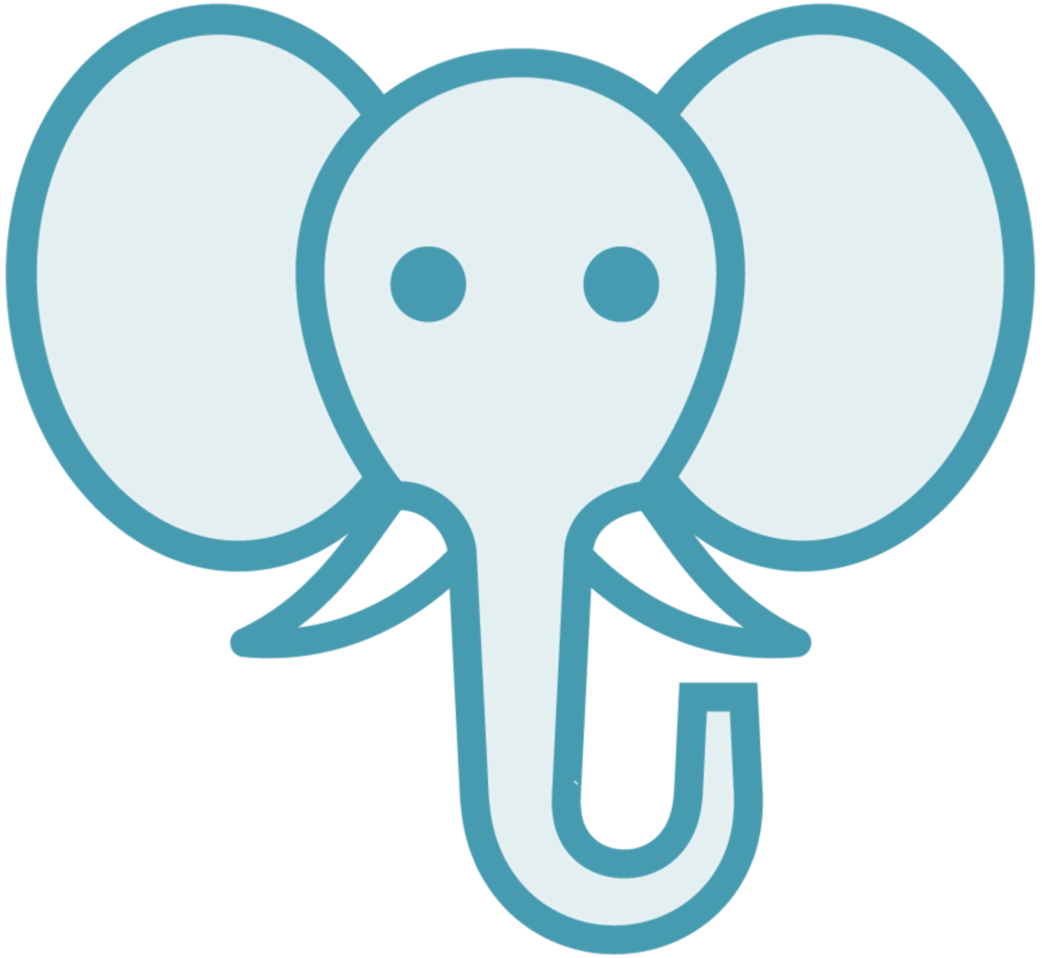
Meet James - Cybersecurity Engineer

Globomantics – Suspected Cyber Attack

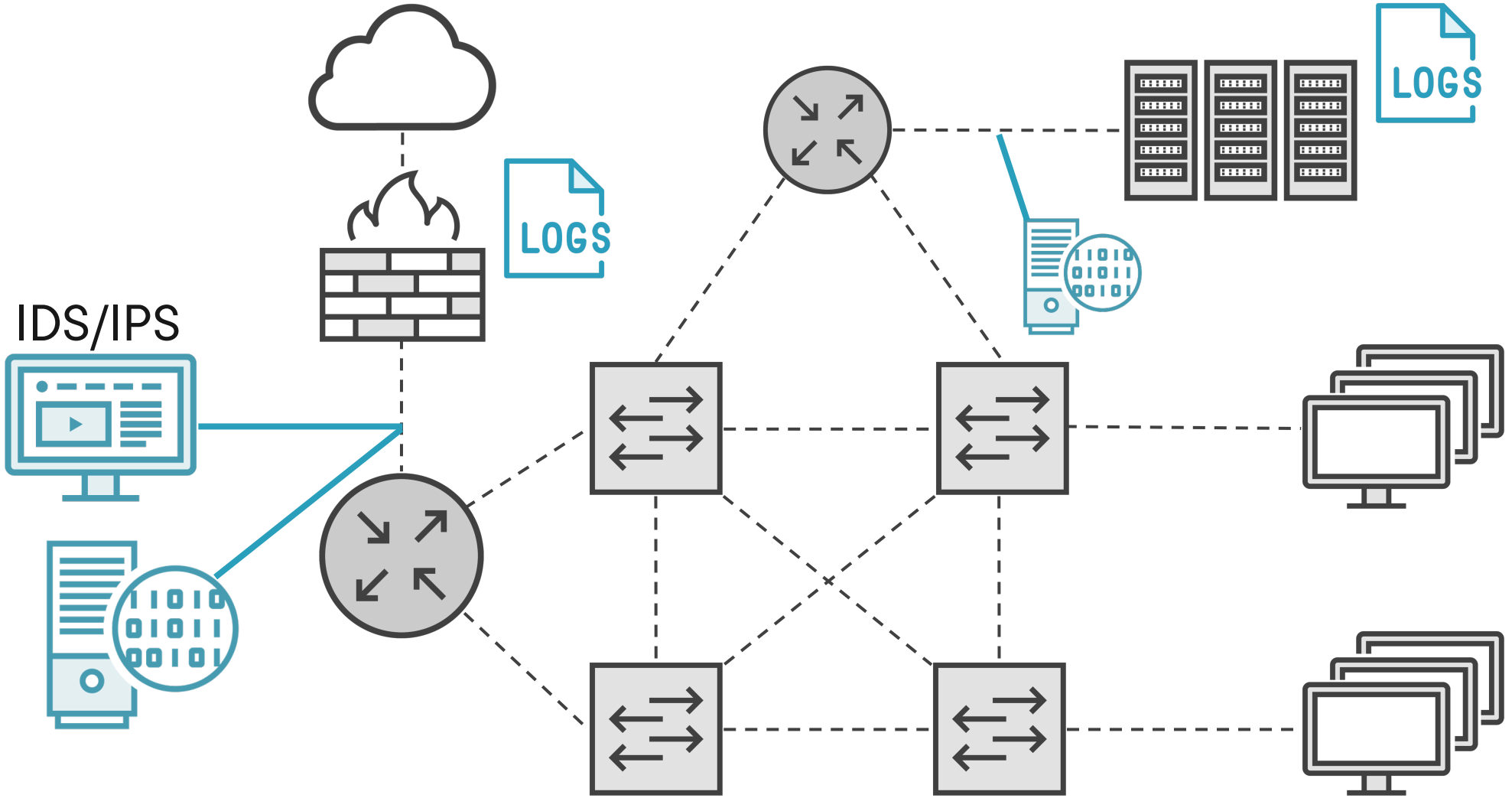


Wireshark is a Microscope





Start with Alerts and Logs



Two Important Pieces of Information

Time

Who

Analyzing Traffic in Wireshark

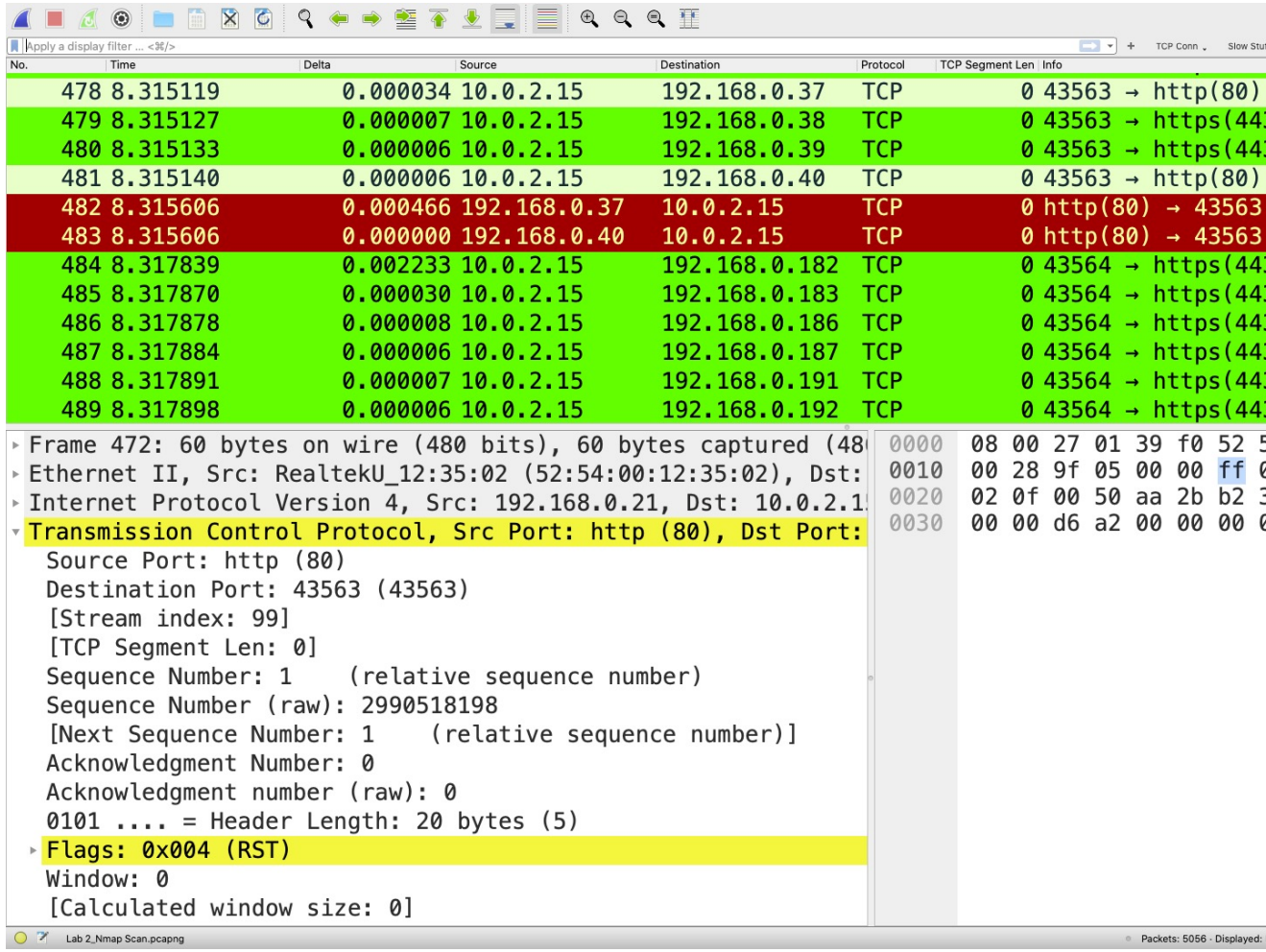
Statistics

Filtering/Coloring Rules

Custom Columns

Exporting Objects/Files

GeoIP Location



The MITRE ATT&CK Framework and Cyber Kill Chain

Attacks Follow a Pattern

MITRE ATT&CK or Cyber Kill Chain (Partial)

Attacks are constantly evolving. This course will teach you the basics, but keep learning.

Module Overview

How to approach packet-level analysis for incident response

Where to capture? How to capture?

Where does Wireshark fit in?

Packet Analysis and the MITRE ATT&CK Framework/Cyber Kill Chain