

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?

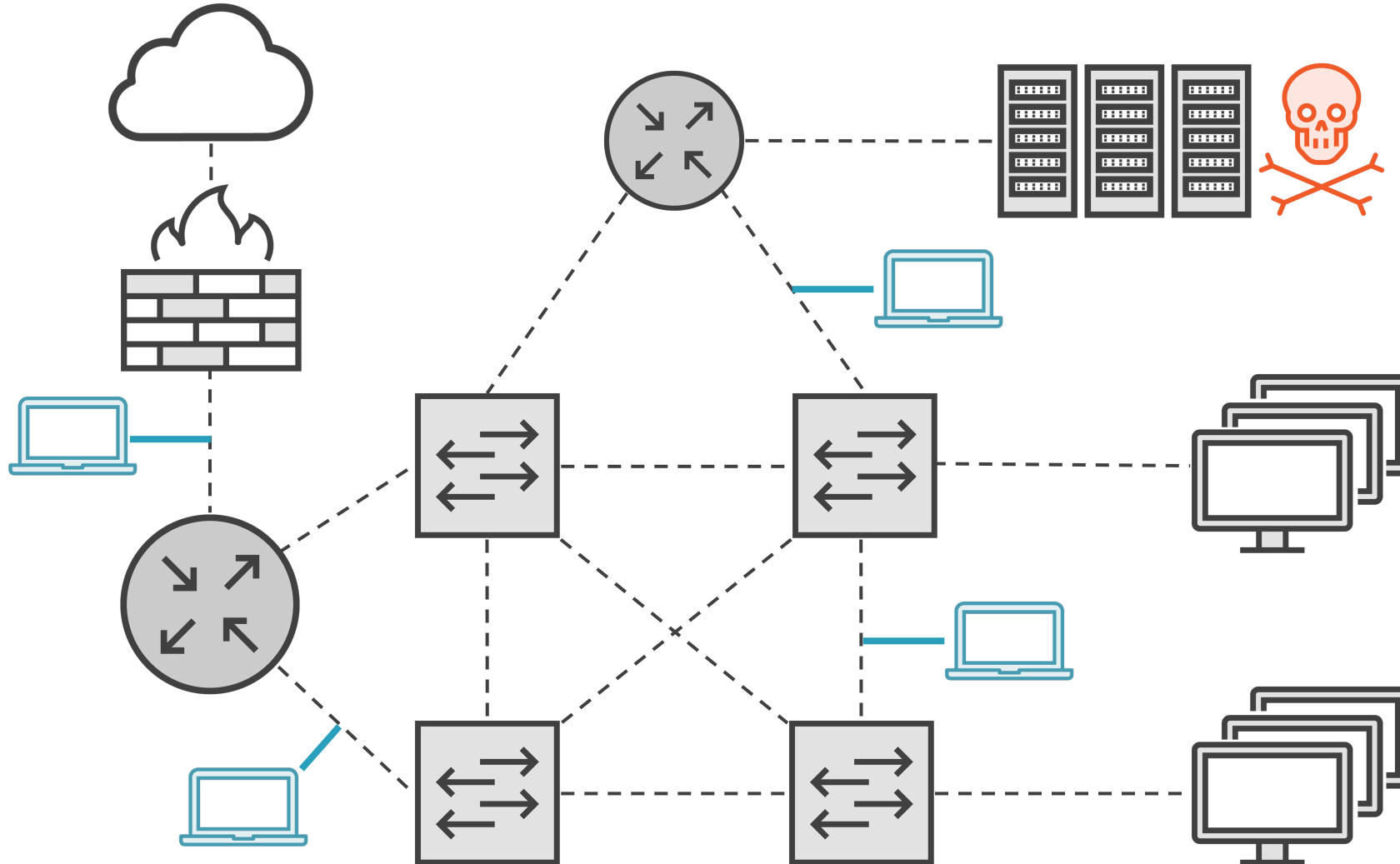
Where does Wireshark fit in?

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

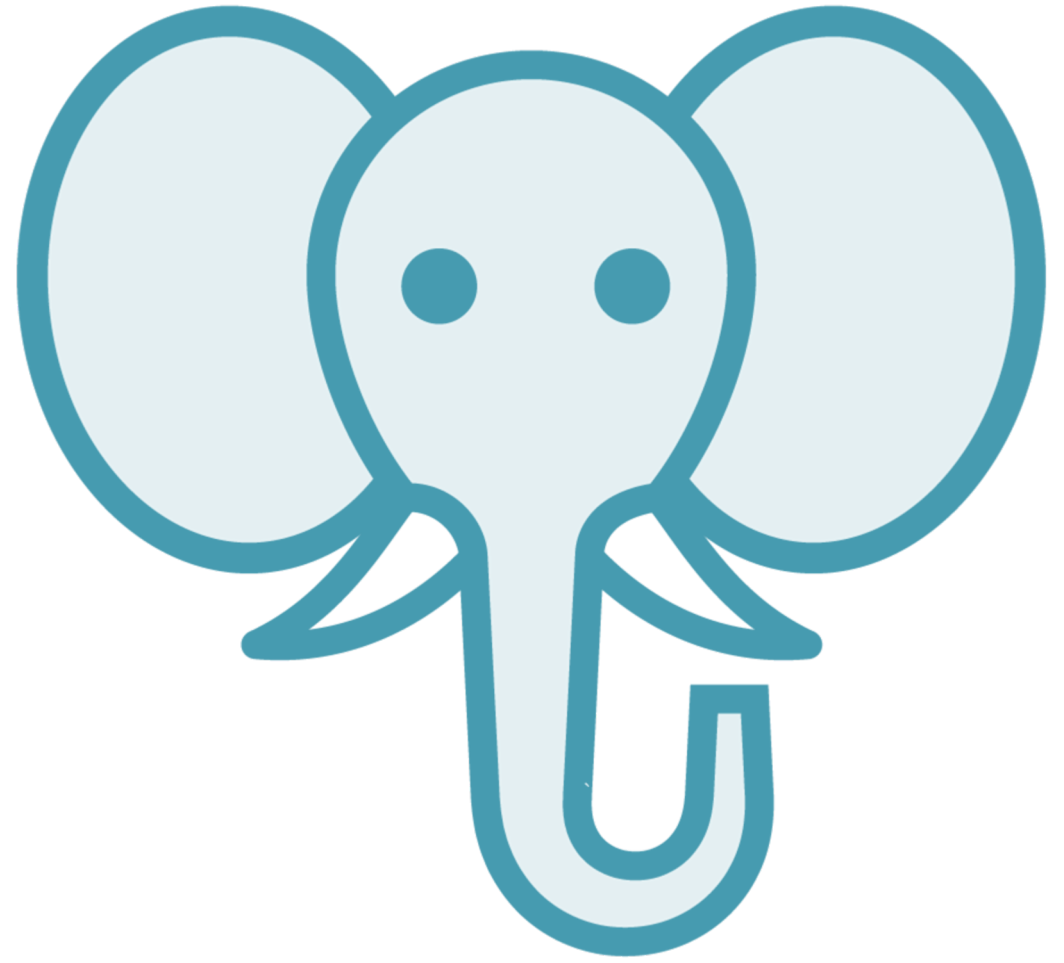
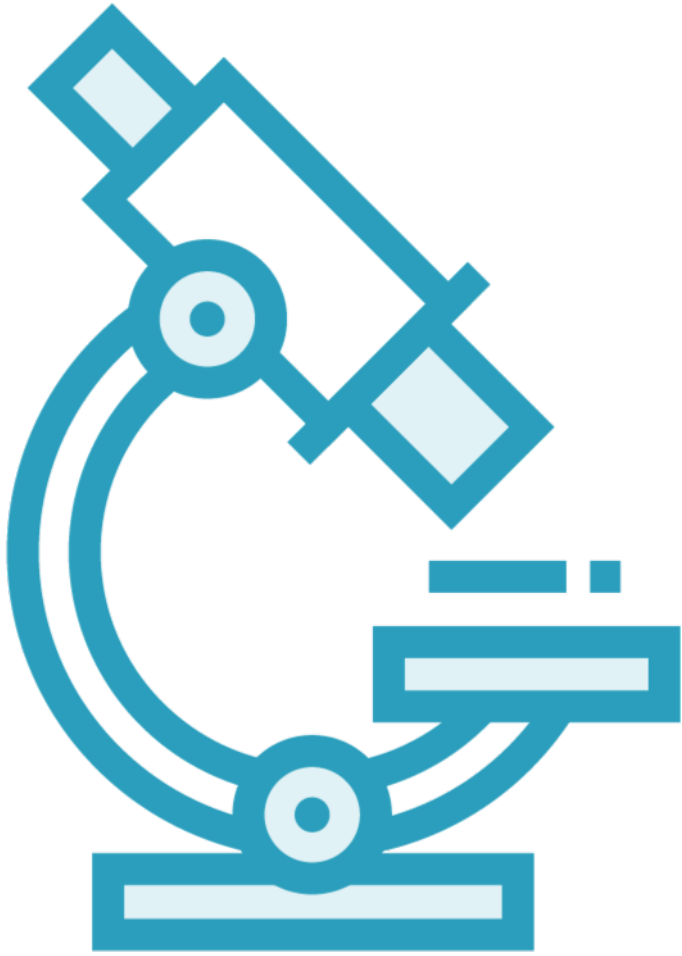
Meet James - Cybersecurity Engineer



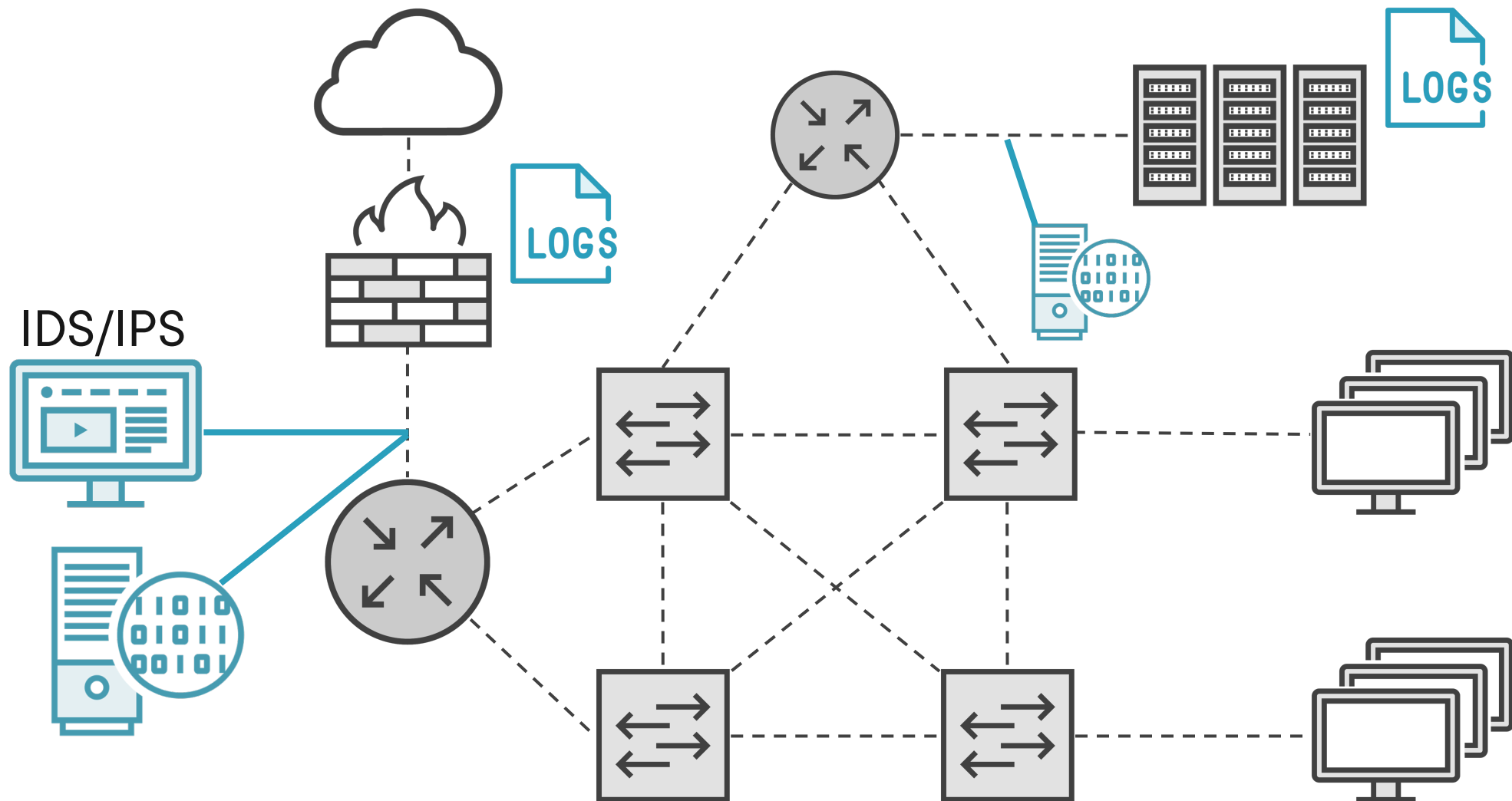
Globomantics – Suspected Cyber Attack



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 screenshot displays the Wireshark network protocol analyzer interface. The top pane shows a list of captured packets, with packet 482 highlighted in red, indicating a TCP Reset (RST) flag. The bottom pane shows the detailed view of packet 482, which is a Transmission Control Protocol (TCP) segment. The details pane shows the following information:

- Frame 472: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
- Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: 10.0.2.15
- Internet Protocol Version 4, Src: 192.168.0.21, Dst: 10.0.2.15
- Transmission Control Protocol, Src Port: http (80), Dst Port: 43563
- Source Port: http (80)
- Destination Port: 43563 (43563)
- [Stream index: 99]
- [TCP Segment Len: 0]
- Sequence Number: 1 (relative sequence number)
- Sequence Number (raw): 2990518198
- [Next Sequence Number: 1 (relative sequence number)]
- Acknowledgment Number: 0
- Acknowledgment number (raw): 0
- 0101 = Header Length: 20 bytes (5)
- Flags: 0x0004 (RST)
- Window: 0
- [Calculated window size: 0]

The packet list shows the following data:

No.	Time	Delta	Source	Destination	Protocol	TCP Segment Len	Info
478	8.315119	0.000034	10.0.2.15	192.168.0.37	TCP	0	43563 → http(80)
479	8.315127	0.000007	10.0.2.15	192.168.0.38	TCP	0	43563 → https(44)
480	8.315133	0.000006	10.0.2.15	192.168.0.39	TCP	0	43563 → https(44)
481	8.315140	0.000006	10.0.2.15	192.168.0.40	TCP	0	43563 → http(80)
482	8.315606	0.000466	192.168.0.37	10.0.2.15	TCP	0	http(80) → 43563
483	8.315606	0.000000	192.168.0.40	10.0.2.15	TCP	0	http(80) → 43563
484	8.317839	0.002233	10.0.2.15	192.168.0.182	TCP	0	43564 → https(44)
485	8.317870	0.000030	10.0.2.15	192.168.0.183	TCP	0	43564 → https(44)
486	8.317878	0.000008	10.0.2.15	192.168.0.186	TCP	0	43564 → https(44)
487	8.317884	0.000006	10.0.2.15	192.168.0.187	TCP	0	43564 → https(44)
488	8.317891	0.000007	10.0.2.15	192.168.0.191	TCP	0	43564 → https(44)
489	8.317898	0.000006	10.0.2.15	192.168.0.192	TCP	0	43564 → https(44)

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