The Investigative Process by Chris Sanders

We use evidence to bridge the gap between perception and reality. The way we view evidence impacts how we answer specific questions about our reality (what happened). Transform data to answer questions more effectively. Pivoting between data sources is one of the best ways to answer questions during an analysis.

```
Observations -->
    (Questions <> Hypothesis <> Answers) -->
        Decisions based on "Evidence" and "Conclusions"
```

RECAP: Methods of Transforming Data

- Reduce: zoom in on specific data (shrink the timeline, exclude specific hosts)
- Expand: zoom out to all data (increase the timeline, include all hosts, etc.)
- Chart: visualize data (bars, lines, graphs, etc.)
- Aggregate: sort evidence by a unique data field
- Pivot:
  - Pivoting enables you to…
    - Connect data sources
    - Move between low/high context data
    - Move between network/host data
    - Move between internal/external data
  - How to Pivot
    a. Search a data Source
    b. Select a *value of interest* from your search results
    c. Search another data source for current *value of interest*

Evidence: Values of Interest and Pivoting Fields

- IP address (source/destination)
- IP/port
- Domain
- Username
- Filename
- Hash
- Process name

Data Sources: Memory, Disk, and Network

- Alerts (Snort, Suricata, Squil)
- Netflow (Zeek logs, SiLK)
- Transactions (Zeek logs)
- Statistics (Elastic stack)
- PCAP (tcpdump, Wireshark, Tshark)
- OSINT (VirusTotal, CrowdStrike)
- Web proxy logs
- Windows log
- Registry keys
- File system

Pivoting Examples

Observation
An IDS alert for a suspicious file download.

Question #1
Is this download legit or evil?

Search	Select	Search for Selected Value
Alert	IP	OSINT
Alert	IP:port	PCAP
PCAP	Domain	OSINT

Question 2
What does the download do?

Search	Select	Search for Selected Value
OSINT	Hash	VirusTotal

Question 3
Did the download execute?

Search	Select	Search for Selected Value
Sandbox	Dropper domain	http.log
Sandbox	Process name	System logs

Question 4
Did anyone else download this file?

Search	Select	Search for Selected Value
OSINT	Hash	files.log