

# Network TAP night

Natan Eliezer  
Chief Research Officer  
Digital Forensics Association  
Champlain College

# Disclaimer #1



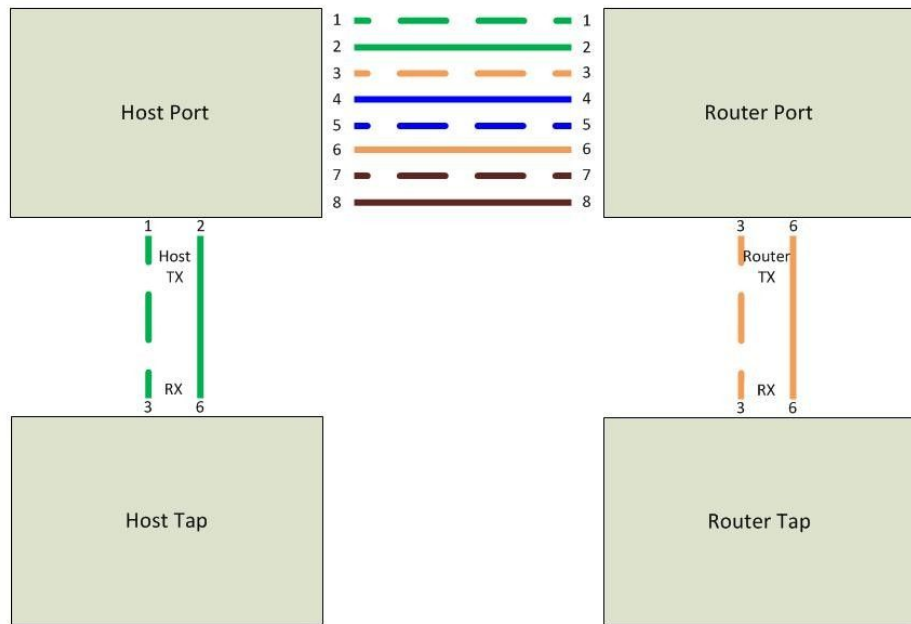
# Network forensics

- Why is it important
  - monitoring
- What is life like without network forensics?
  - ... its rough
- Why are TAPS important
  - Passive taps are undetectable
- Problems you might encounter...

# Disclaimer



# Building the TAP

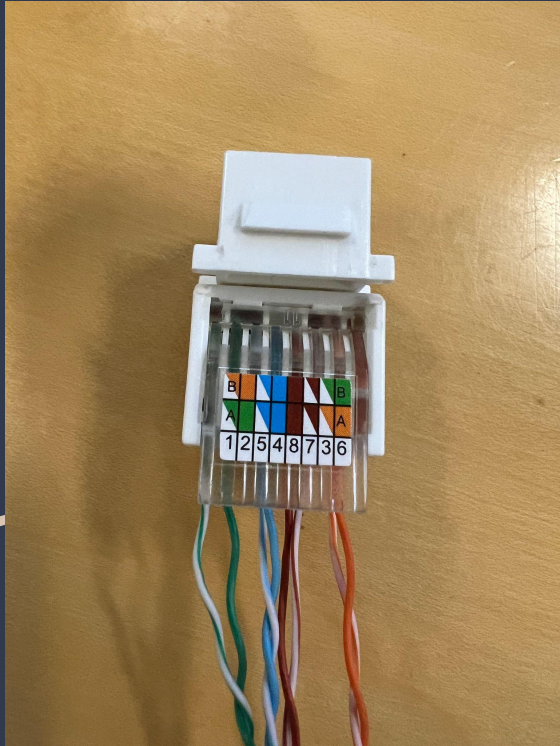


# Materials

- 3 ethernet jacks
- Ethernet cable
- 3 port wall plate
- Handy box
- Wire cutters



# Step 1 – Router side

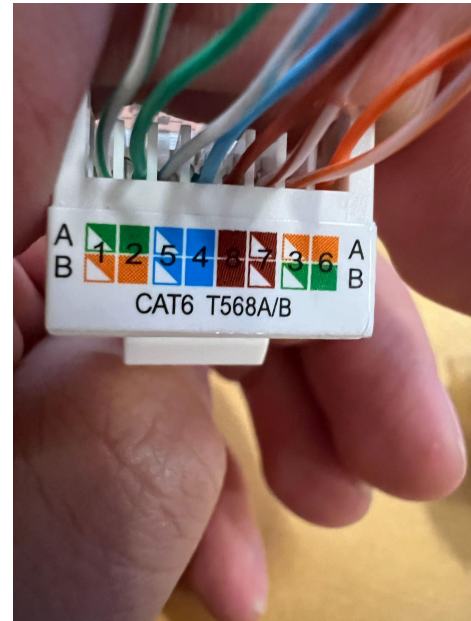


- Strip the ethernet cable to get 4 pairs of twisted wires
- Untangle just the ends of each cable
- Plug the color wire according to the ethernet jack
- Punch it down with the panel



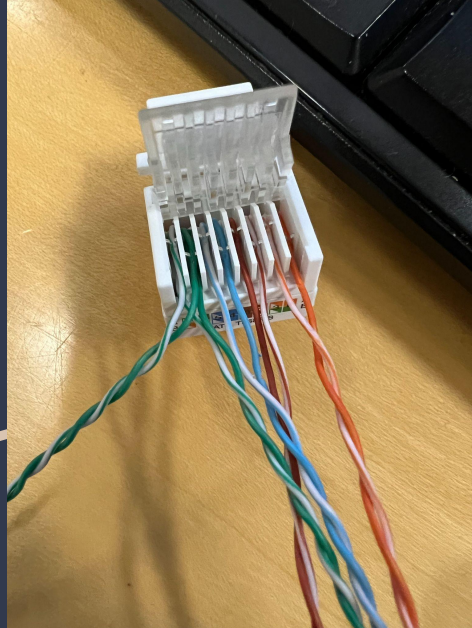
## Step 2 – Host side

- Wire the same colors to the 2nd jack
- Pretty much the same exact thing





# Step 3 – TAP



- Strip another section of wire and take only the Orange or Green wires
- Host
  - Wire the Solid Green/Striped Green from 1/2 on the host side
  - Wire them to 3/6 on the third jack
- Router
  - Wire the Solid Orange/Striped Orange from 3/6 on the router side
  - Wire them to 3/6 on the third jack