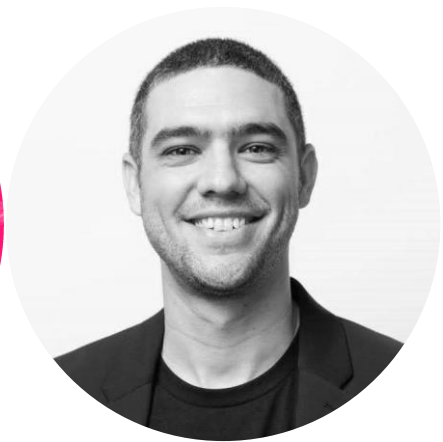


# Network Protocols for Security: DNS



**Brandon DeVault**

Principal Security Author, Pluralsight

@DeVaultSecurity | [www.devaultsecurity.com](http://www.devaultsecurity.com)



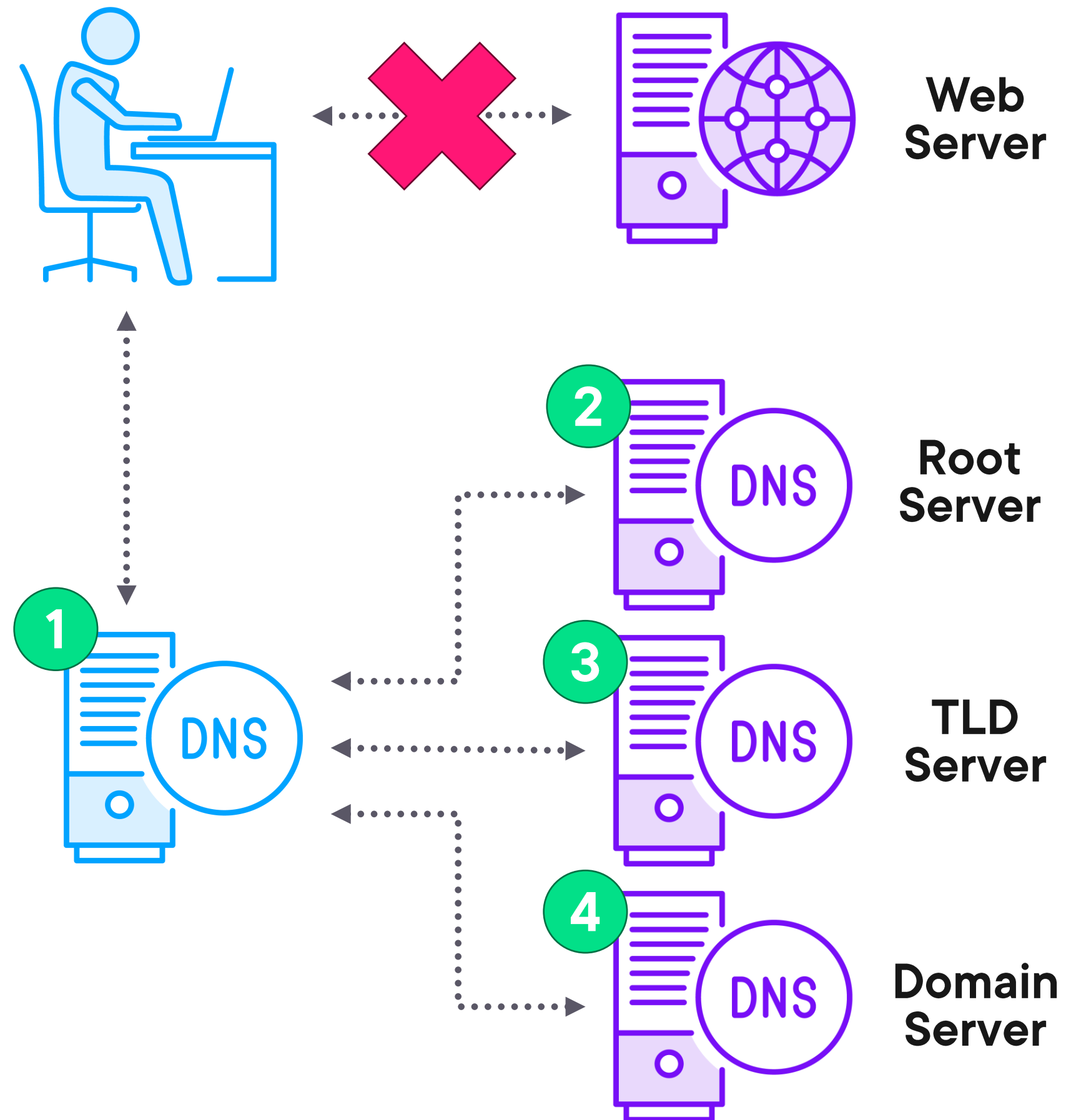
**Query:**  
**pluralsight.com?**



**Answer:**  
**A: 104.17.35.85**

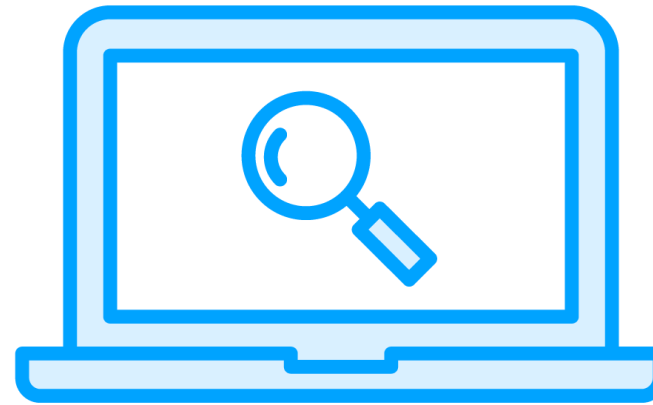
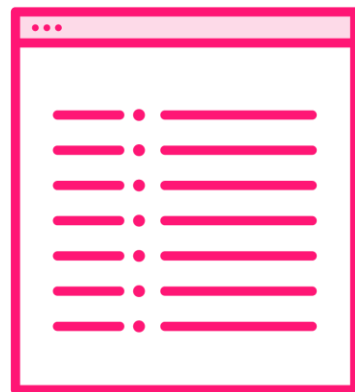


pluralsight.com?





**Browser  
Cache**



**Operating System  
Cache**



**DNS Server  
Cache**



# Zeek

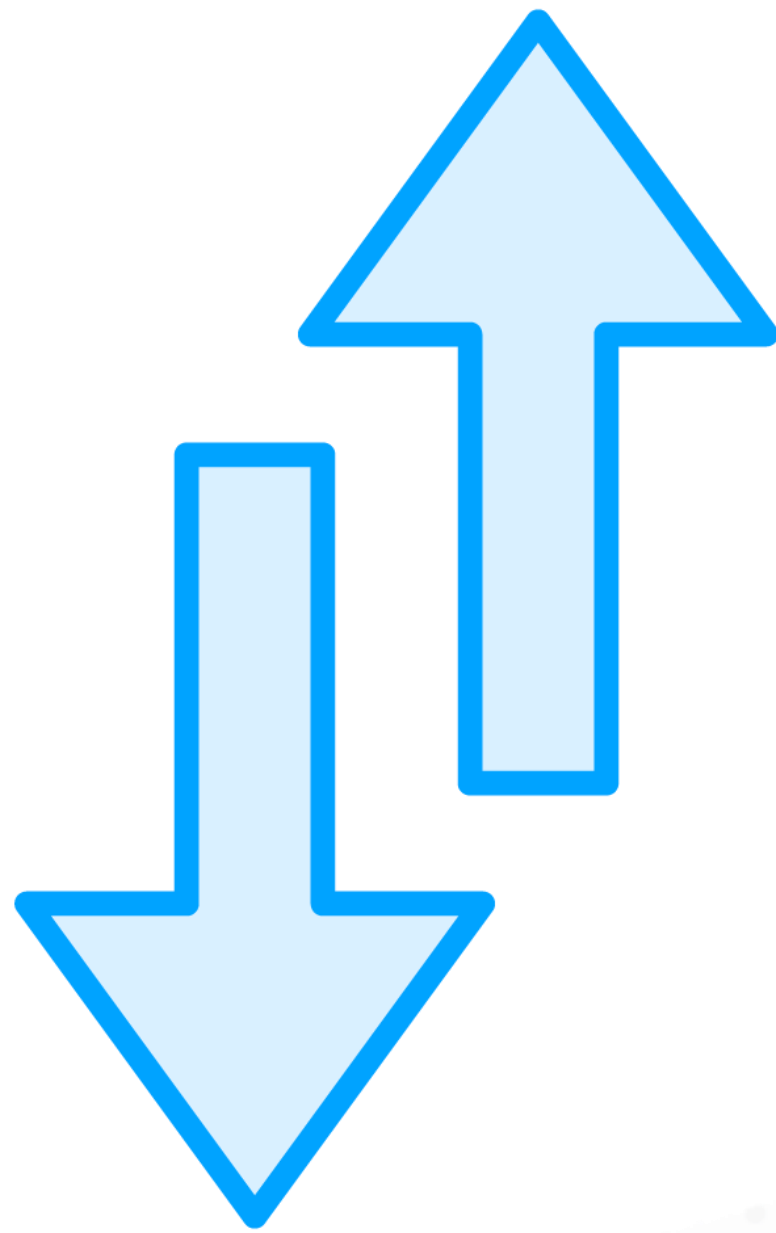


**Passive, open-source traffic Analysis platform**

**Generates logs for network protocols and sessions**

**Extensible through scripts**

# Entropy



G7#r\$!2z9L (high entropy)

4bR9kQ

Abcdef

Abcabc

aaaaaaaa (low entropy)