



# Advanced IP Analysis

# Advanced IP Analysis

- » Understanding and working with the IP Header
- » What is the Internet Protocol (IP)?
  - Layer 3
  - Routing (source and destination IP addresses)
  - Others
- » Wireshark analysis
  - What can you find in the IP header?

# Advanced IP Analysis

4-bit	8-bit	16-bit	32-bit	
Ver.	Header Length	Type of Service	Total Length	
Identification			Flags	Offset
Time To Live	Protocol		Checksum	
Source Address				
Destination Address				
Options and Padding				

# Advanced IP Analysis

- [-] Internet Protocol Version 4, Src: 10.170.170.11 (10.170.170.11), Dst: 10.121.90.106 (10.121.90.106)
  - Version: 4
  - Header Length: 20 bytes
  - [+] Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    - Total Length: 71
    - Identification: 0x3d66 (15718)
  - [+] Flags: 0x00
    - Fragment offset: 0
    - Time to live: 123
    - Protocol: UDP (17)
  - [+] Header checksum: 0xe8a7 [correct]
    - Source: 10.170.170.11 (10.170.170.11)
    - Destination: 10.121.90.106 (10.121.90.106)
    - [Source GeoIP: Unknown]
    - [Destination GeoIP: Unknown]
- [+] User Datagram Protocol, Src Port: 53 (53), Dst Port: 58157 (58157)
- [+] Domain Name System (response)

# Questions?