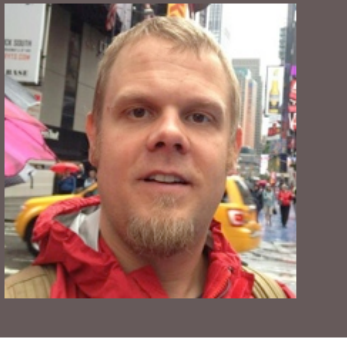
WIRESHARK TUTORIAL

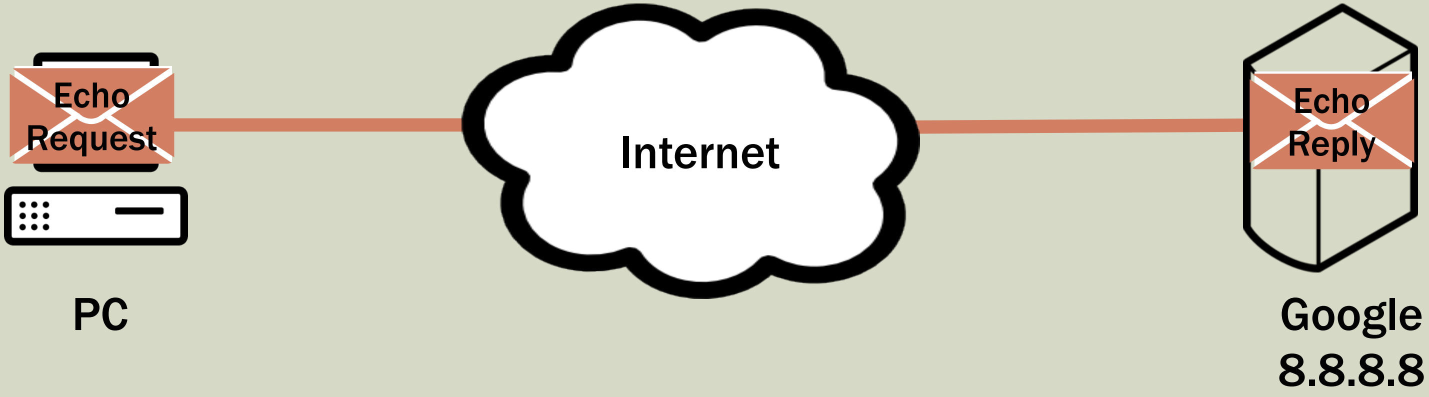
Introduction to capturing and analyzing packets

Ross Bagurdes
ross.bagurdes@outlook.com

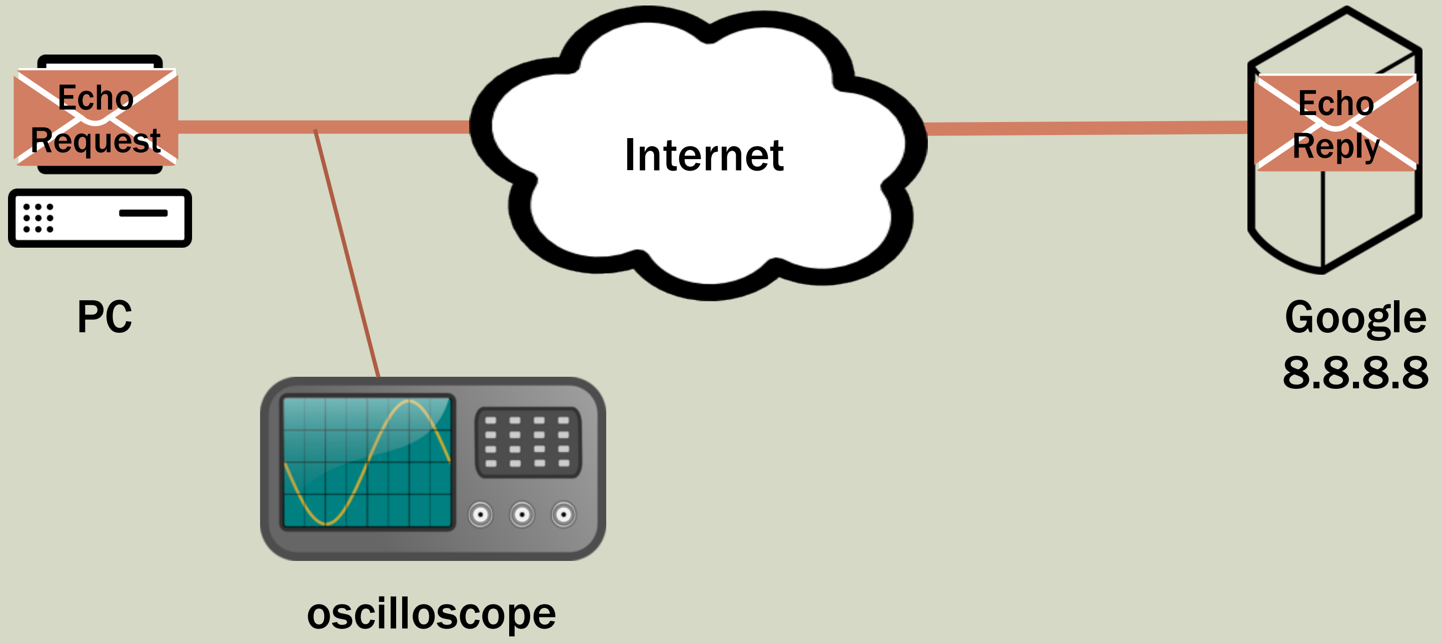
Engineer, IT Instructor,
Pluralsight Author, Nerdtastic Stuff



EVESDROPPING



EVESDROPPING – OLD SCHOOL



EVESDROPPING – OLD SCHOOL

```
0000000000001100001010011111101100110101100011000101010101001010101
0101110101000010101010101001010100101010101010010010101010101000101010
1010001010110111010100010101010101010101010001010101010100101010101010
1110101000010101010101001010100101010101010010010101010101000101010101
0001010110111010100010101010101010101010001010101010100101010101010111
0101000010101010101001010100101010101010010010101010101000101010101000
1010110111010100010101010101010101010001010101010100101010101010111010
1000010101010101001010100101010101010010011010101000101010101010001010
1101110101000101010101010101010101000101010101010010101010101011101010 00
0101010101010010101001010101010100100101010101000101010101010001010110
1110101000101010101010101010101000101010101010010101010101011101010000 10
1010101010010101001010101010100100101010101000101010101010001010110111
0101000101010101010101010101000101010101010010101010101011101010000101 01
0101010010101001010101010100100101010101000101010101010001010110111010
1000101010101010101010101000101010101010010101010101011101010000101010 10
1010010101001010101010100100101010101000101010
```

PARSE BITS

0000 0000 0101 0000 0101 0110 1110 0110 0101 0011 0110 0011

0000 0000 0000 1100 0010 1001 1111 1011 0011 0101 1000 1100

0000 1000 0000 0000

Destination MAC	Source MAC	L3 Type	Packet
00:50:56:E6:53:63	00:0C:29:FB:35:8C	0x0800	Packet Data

Indicates IPv4 Packet

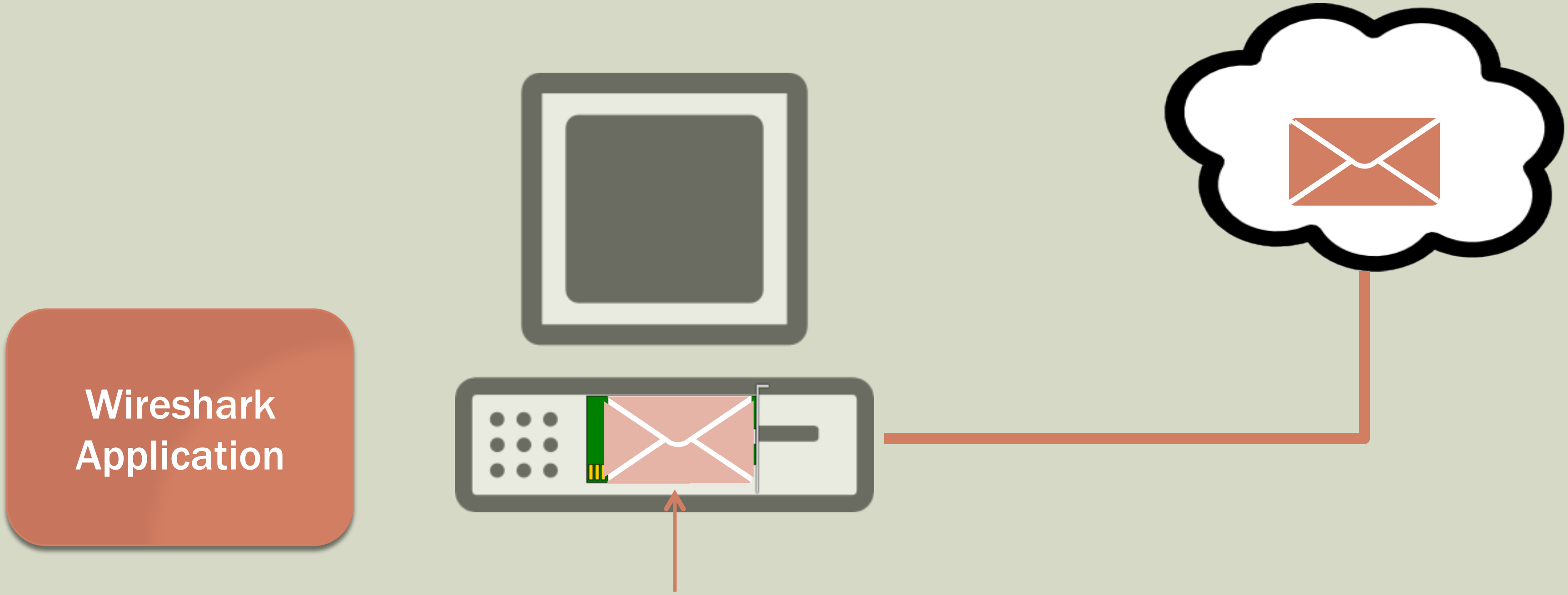
RFC 791

PARSE PACKET HEADER

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version|  IHL  |Type of Service|          Total Length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Identification        |Flags|      Fragment Offset    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Time to Live |    Protocol   |         Header Checksum       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Source Address                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Destination Address                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Options                    |    Padding    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

RFC 791

EVESDROPPING – OLD SCHOOL



Wireshark Application

Network Interface Card
+
WinPcap or LibPcap driver

DEMONSTRATION

PERFORMING A BASIC PACKET CAPTURE