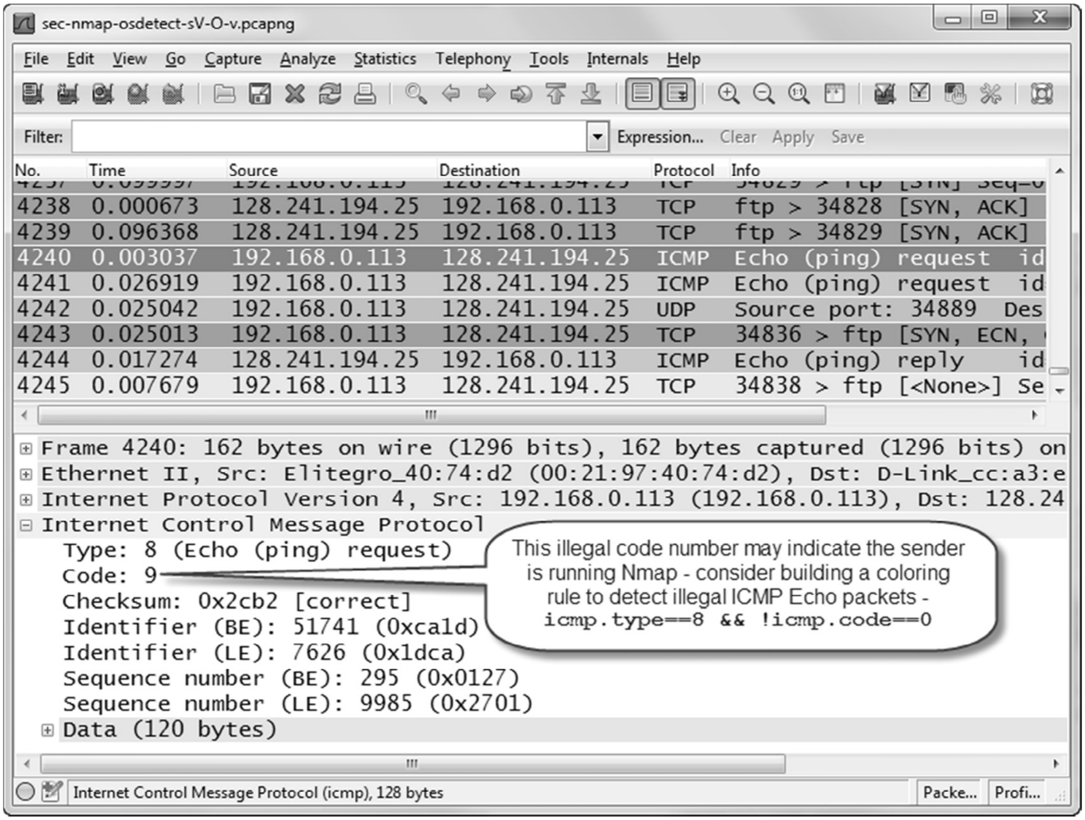
Recognize Unusual Traffic Patterns

In order to recognize unusual traffic patterns, you must first recognize normal traffic patterns. Baselines are essential in differentiating traffic types.

Using penetration testing, reconnaissance and mapping tools to generate unusual traffic enables you to correlate this type of traffic with these tools. For example, in Figure 356 we have captured an OS fingerprinting operation performed with Nmap. In some of the ICMP Echo Request packets, the code field is set at 9. This is unique as the specification indicates the code field of an ICMP Echo Request packet should be 0.


sec-nmap-osdetect-sV-O-v.pcapng
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.  Time      Source          Destination     Protocol Info
4237 0.099997  192.168.0.113   128.241.194.25  TCP      34829 > ftp [SYN] Seq=0
4238 0.000673  128.241.194.25  192.168.0.113   TCP      ftp > 34828 [SYN, ACK]
4239 0.096368  128.241.194.25  192.168.0.113   TCP      ftp > 34829 [SYN, ACK]
4240 0.003037  192.168.0.113   128.241.194.25  ICMP     Echo (ping) request  id
4241 0.026919  192.168.0.113   128.241.194.25  ICMP     Echo (ping) request  id
4242 0.025042  192.168.0.113   128.241.194.25  UDP      Source port: 34889  Des
4243 0.025013  192.168.0.113   128.241.194.25  TCP      34836 > ftp [SYN, ECN,
4244 0.017274  128.241.194.25  192.168.0.113   ICMP     Echo (ping) reply    id
4245 0.007679  192.168.0.113   128.241.194.25  TCP      34838 > ftp [<None>] Se
```

```
⊞ Frame 4240: 162 bytes on wire (1296 bits), 162 bytes captured (1296 bits) on
⊞ Ethernet II, Src: Elitegro_40:74:d2 (00:21:97:40:74:d2), Dst: D-Link_cc:a3:e
⊞ Internet Protocol Version 4, Src: 192.168.0.113 (192.168.0.113), Dst: 128.24
⊟ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 9
    Checksum: 0x2cb2 [correct]
    Identifier (BE): 51741 (0xca1d)
    Identifier (LE): 7626 (0x1dca)
    Sequence number (BE): 295 (0x0127)
    Sequence number (LE): 9985 (0x2701)
  ⊞ Data (120 bytes)
```

This illegal code number may indicate the sender is running Nmap - consider building a coloring rule to detect illegal ICMP Echo packets - `icmp.type==8 && !icmp.code==0`

Internet Control Message Protocol (icmp), 128 bytes

Figure 356. Unusual traffic patterns may identify the tool used on the network [sec-nmap-osdetect-sV-O-v.pcapng]