3 0.018886 192.168.2.44 40.77.226.247 TCP 66 53250→443 [SYN] Seq=311487167 Win=8192 Len=0 MSS=1460 WS=256 SACK\_PERM=1

Frame 3: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0

Interface id: 0 (\Device\NPF\_{FDD33FCF-140C-487B-BDCC-4F2DF0A16862})

Encapsulation type: Ethernet (1)

Arrival Time: Apr 13, 2017 16:19:22.248683000 Paris, Madrid (heure dt)

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1492093162.248683000 seconds

[Time delta from previous captured frame: 0.001114000 seconds]

[Time delta from previous displayed frame: 0.000000000 seconds]

[Time since reference or first frame: 0.018886000 seconds]

Frame Number: 3

Frame Length: 66 bytes (528 bits)

Capture Length: 66 bytes (528 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:tcp]

[Coloring Rule Name: \_\_\_conversation\_color\_filter\_\_\_01]

[Coloring Rule String: (ip.addr eq 192.168.2.44 and ip.addr eq 40.77.226.247) and (tcp.port eq 53250 and tcp.port eq 443)] Ethernet II, Src: IntelCor\_38:fd:1a (28:b2:bd:38:fd:1a), Dst: LexCompu\_09:2c:74 (4c:02:89:09:2c:74)

Destination: LexCompu\_09:2c:74 (4c:02:89:09:2c:74)

Address: LexCompu\_09:2c:74 (4c:02:89:09:2c:74)

.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)

.... ...0 .... .... .... .... = IG bit: Individual address (unicast)

Source: IntelCor\_38:fd:1a (28:b2:bd:38:fd:1a)

Address: IntelCor\_38:fd:1a (28:b2:bd:38:fd:1a)

.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)

.... ...0 .... .... .... .... = IG bit: Individual address (unicast) Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.168.2.44, Dst: 40.77.226.247

0100 .... = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

0000 00.. = Differentiated Services Codepoint: Default (0)

.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0) Total Length: 52

Identification: 0x3f01 (16129)

Flags: 0x02 (Don't Fragment)

0... .... = Reserved bit: Not set

.1.. .... = Don't fragment: Set

..0. .... = More fragments: Not set

Fragment offset: 0

Time to live: 128

Protocol: TCP (6)

Header checksum: 0xeda9 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.2.44

Destination: 40.77.226.247

[Source GeoIP: Unknown]

[Destination GeoIP: Unknown]

Transmission Control Protocol, Src Port: 53250, Dst Port: 443, Seq: 311487167, Len: 0

Source Port: 53250

Destination Port: 443

[Stream index: 0]

[TCP Segment Len: 0]

Sequence number: 311487167 Acknowledgment number: 0

Header Length: 32 bytes

Flags: 0x002 (SYN)

000. .... .... = Reserved: Not set

...0 .... .... = Nonce: Not set

.... 0... .... = Congestion Window Reduced (CWR): Not set

.... .0.. .... = ECN-Echo: Not set

.... ..0. .... = Urgent: Not set

.... ...0 .... = Acknowledgment: Not set

.... .... 0... = Push: Not set

.... .... .0.. = Reset: Not set

.... .... ..1. = Syn: Set

[Expert Info (Chat/Sequence): Connection establish request (SYN): server port 443]

[Connection establish request (SYN): server port 443]

[Severity level: Chat]

[Group: Sequence]

.... .... ...0 = Fin: Not set

[TCP Flags: ··········S·]

Window size value: 8192

[Calculated window size: 8192]

Checksum: 0xb1e9 [unverified] [Checksum Status: Unverified] Urgent pointer: 0

Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted

Maximum segment size: 1460 bytes

Kind: Maximum Segment Size (2)

Length: 4

MSS Value: 1460

No-Operation (NOP)

# Type: 1

# 0... .... = Copy on fragmentation: No

.00. .... = Class: Control (0)

...0 0001 = Number: No-Operation (NOP) (1)

Window scale: 8 (multiply by 256)

Kind: Window Scale (3)

# Length: 3

Shift count: 8

[Multiplier: 256]

No-Operation (NOP)

Type: 1

0... .... = Copy on fragmentation: No

.00. .... = Class: Control (0)

...0 0001 = Number: No-Operation (NOP) (1)

No-Operation (NOP)

Type: 1

0... .... = Copy on fragmentation: No

.00. .... = Class: Control (0)

...0 0001 = Number: No-Operation (NOP) (1)

TCP SACK Permitted Option: True

Kind: SACK Permitted (4)

Length: 2

4 0.020830 40.77.226.247 192.168.2.44 TCP 66 443→53250 [SYN, ACK] Seq=3076558735 Ack=311487168 Win=14600 Len=0 MSS=1460 SACK\_PERM=1 WS=16

Frame 4: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0

Interface id: 0 (\Device\NPF\_{FDD33FCF-140C-487B-BDCC-4F2DF0A16862})

Encapsulation type: Ethernet (1)

Arrival Time: Apr 13, 2017 16:19:22.250627000 Paris, Madrid (heure dt)

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1492093162.250627000 seconds

[Time delta from previous captured frame: 0.001944000 seconds]

[Time delta from previous displayed frame: 0.001944000 seconds]

[Time since reference or first frame: 0.020830000 seconds]

Frame Number: 4

Frame Length: 66 bytes (528 bits)

Capture Length: 66 bytes (528 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:tcp]

[Coloring Rule Name: \_\_\_conversation\_color\_filter\_\_\_01]

[Coloring Rule String: (ip.addr eq 192.168.2.44 and ip.addr eq 40.77.226.247) and (tcp.port eq 53250 and tcp.port eq 443)] Ethernet II, Src: LexCompu\_09:2c:74 (4c:02:89:09:2c:74), Dst: IntelCor\_38:fd:1a (28:b2:bd:38:fd:1a)

Destination: IntelCor\_38:fd:1a (28:b2:bd:38:fd:1a)

Address: IntelCor\_38:fd:1a (28:b2:bd:38:fd:1a)

.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)

.... ...0 .... .... .... .... = IG bit: Individual address (unicast)

Source: LexCompu\_09:2c:74 (4c:02:89:09:2c:74)

Address: LexCompu\_09:2c:74 (4c:02:89:09:2c:74)

.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)

.... ...0 .... .... .... .... = IG bit: Individual address (unicast) Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 40.77.226.247, Dst: 192.168.2.44

0100 .... = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

0000 00.. = Differentiated Services Codepoint: Default (0)

.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0) Total Length: 52

Identification: 0x0000 (0)

Flags: 0x02 (Don't Fragment)

0... .... = Reserved bit: Not set

.1.. .... = Don't fragment: Set

..0. .... = More fragments: Not set

Fragment offset: 0

Time to live: 64

Protocol: TCP (6)

Header checksum: 0x6cab [validation disabled] [Header checksum status: Unverified]

Source: 40.77.226.247

Destination: 192.168.2.44

[Source GeoIP: Unknown]

[Destination GeoIP: Unknown]

Transmission Control Protocol, Src Port: 443, Dst Port: 53250, Seq: 3076558735, Ack: 311487168, Len: 0

Source Port: 443

Destination Port: 53250

[Stream index: 0]

[TCP Segment Len: 0]

Sequence number: 3076558735

Acknowledgment number: 311487168

Header Length: 32 bytes

Flags: 0x012 (SYN, ACK)

000. .... .... = Reserved: Not set

...0 .... .... = Nonce: Not set

.... 0... .... = Congestion Window Reduced (CWR): Not set

.... .0.. .... = ECN-Echo: Not set

.... ..0. .... = Urgent: Not set

.... ...1 .... = Acknowledgment: Set

.... .... 0... = Push: Not set

.... .... .0.. = Reset: Not set

.... .... ..1. = Syn: Set

[Expert Info (Chat/Sequence): Connection establish acknowledge (SYN+ACK): server port 443]

[Connection establish acknowledge (SYN+ACK): server port 443]

[Severity level: Chat]

[Group: Sequence]

.... .... ...0 = Fin: Not set

[TCP Flags: ·······A··S·]

Window size value: 14600

[Calculated window size: 14600]

Checksum: 0x51e4 [unverified]

[Checksum Status: Unverified] Urgent pointer: 0

Options: (12 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted, No-Operation (NOP), Window scale

Maximum segment size: 1460 bytes

Kind: Maximum Segment Size (2)

Length: 4

MSS Value: 1460

No-Operation (NOP)

Type: 1

0... .... = Copy on fragmentation: No

.00. .... = Class: Control (0)

...0 0001 = Number: No-Operation (NOP) (1)

No-Operation (NOP)

Type: 1

0... .... = Copy on fragmentation: No

.00. .... = Class: Control (0)

...0 0001 = Number: No-Operation (NOP) (1)

TCP SACK Permitted Option: True

Kind: SACK Permitted (4)

Length: 2

No-Operation (NOP)

Type: 1

0... .... = Copy on fragmentation: No

.00. .... = Class: Control (0)

...0 0001 = Number: No-Operation (NOP) (1)

Window scale: 4 (multiply by 16)

Kind: Window Scale (3)

Length: 3

Shift count: 4

[Multiplier: 16]

[SEQ/ACK analysis]

[This is an ACK to the segment in frame: 3]

[The RTT to ACK the segment was: 0.001944000 seconds]

[iRTT: 0.002183000 seconds]

5 0.021069 192.168.2.44 40.77.226.247 TCP 54 53250→443 [ACK] Seq=311487168 Ack=3076558736 Win=65536 Len=0

Frame 5: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0

Interface id: 0 (\Device\NPF\_{FDD33FCF-140C-487B-BDCC-4F2DF0A16862}) Encapsulation type: Ethernet (1)

Arrival Time: Apr 13, 2017 16:19:22.250866000 Paris, Madrid (heure dt)

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1492093162.250866000 seconds

[Time delta from previous captured frame: 0.000239000 seconds]

[Time delta from previous displayed frame: 0.000239000 seconds]

[Time since reference or first frame: 0.021069000 seconds]

Frame Number: 5

Frame Length: 54 bytes (432 bits)

Capture Length: 54 bytes (432 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:tcp]

[Coloring Rule Name: \_\_\_conversation\_color\_filter\_\_\_01]

[Coloring Rule String: (ip.addr eq 192.168.2.44 and ip.addr eq 40.77.226.247) and (tcp.port eq 53250 and tcp.port eq 443)] Ethernet II, Src: IntelCor\_38:fd:1a (28:b2:bd:38:fd:1a), Dst: LexCompu\_09:2c:74 (4c:02:89:09:2c:74) Destination: LexCompu\_09:2c:74 (4c:02:89:09:2c:74)

Address: LexCompu\_09:2c:74 (4c:02:89:09:2c:74)

.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)

.... ...0 .... .... .... .... = IG bit: Individual address (unicast)

Source: IntelCor\_38:fd:1a (28:b2:bd:38:fd:1a)

Address: IntelCor\_38:fd:1a (28:b2:bd:38:fd:1a)

.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)

.... ...0 .... .... .... .... = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.168.2.44, Dst: 40.77.226.247 0100 .... = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

0000 00.. = Differentiated Services Codepoint: Default (0)

.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0) Total Length: 40

Identification: 0x3f02 (16130)

Flags: 0x02 (Don't Fragment)

0... .... = Reserved bit: Not set

.1.. .... = Don't fragment: Set

..0. .... = More fragments: Not set

Fragment offset: 0 Time to live: 128

Protocol: TCP (6)

Header checksum: 0xedb4 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.2.44

Destination: 40.77.226.247

[Source GeoIP: Unknown]

[Destination GeoIP: Unknown]

Transmission Control Protocol, Src Port: 53250, Dst Port: 443, Seq: 311487168, Ack: 3076558736, Len: 0

Source Port: 53250

Destination Port: 443

[Stream index: 0]

[TCP Segment Len: 0]

Sequence number: 311487168

Acknowledgment number: 3076558736

Header Length: 20 bytes

Flags: 0x010 (ACK)

000. .... .... = Reserved: Not set

...0 .... .... = Nonce: Not set

.... 0... .... = Congestion Window Reduced (CWR): Not set

.... .0.. .... = ECN-Echo: Not set

.... ..0. .... = Urgent: Not set

.... ...1 .... = Acknowledgment: Set

.... .... 0... = Push: Not set

.... .... .0.. = Reset: Not set

.... .... ..0. = Syn: Not set

.... .... ...0 = Fin: Not set

[TCP Flags: ·······A····]

Window size value: 256

[Calculated window size: 65536]

[Window size scaling factor: 256]

Checksum: 0xcabb [unverified]

[Checksum Status: Unverified]

Urgent pointer: 0

[SEQ/ACK analysis]

[This is an ACK to the segment in frame: 4]

[The RTT to ACK the segment was: 0.000239000 seconds]

[iRTT: 0.002183000 seconds]

6 0.022433 192.168.2.44 40.77.226.247 TLSv1 196 Client Hello