Ruben Valdez
Assignment: Lab 2
Network Analysis and Forensics

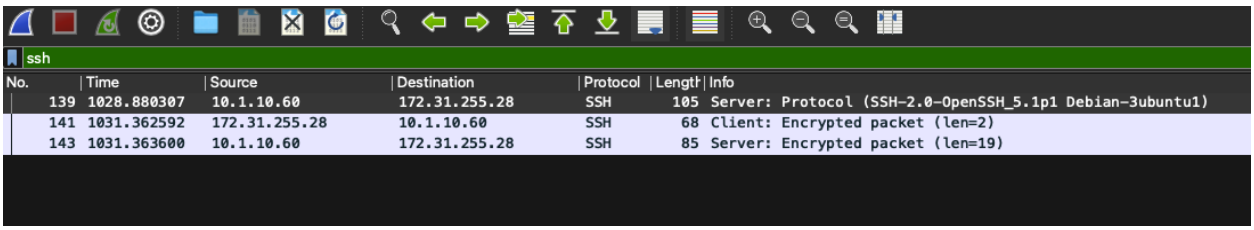
Spring 2025 | CSEC 5306
Computer Networks and Security
Prof. Alsmadi

Date: January 21, 2025

Section 1 – Initial recon and entry

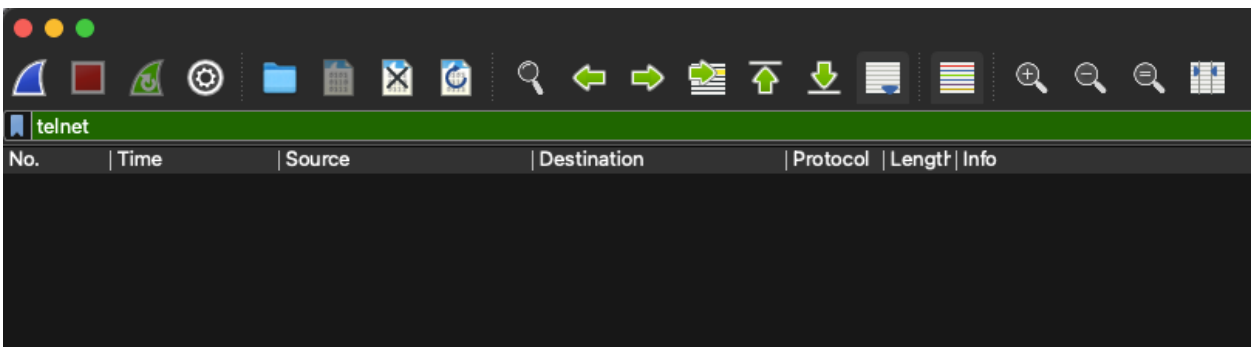
- Question 2:

SSH (22)



ssh

No.	Time	Source	Destination	Protocol	Length	Info
139	1028.880307	10.1.10.60	172.31.255.28	SSH	105	Server: Protocol (SSH-2.0-OpenSSH_5.1p1 Debian-3ubuntu1)
141	1031.362592	172.31.255.28	10.1.10.60	SSH	68	Client: Encrypted packet (len=2)
143	1031.363600	10.1.10.60	172.31.255.28	SSH	85	Server: Encrypted packet (len=19)



telnet

No.	Time	Source	Destination	Protocol	Length	Info

- Question 3

Port 2200 was open for 10.1.10.33 is it was the only IP that completed the 3-way handshake.

33	801.588075	10.1.10.33	172.31.255.28	TCP	60	2200 → 59632 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
40	801.643654	172.31.255.28	10.1.10.33	TCP	60	59632 → 2200 [RST] Seq=1 Win=0 Len=0
42	804.077670	172.31.255.28	10.1.10.33	TCP	60	59643 → 2200 [SYN] Seq=0 Win=2048 Len=0 MSS=1460
43	804.078786	10.1.10.33	172.31.255.28	TCP	60	2200 → 59643 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
46	804.148647	172.31.255.28	10.1.10.33	TCP	60	59643 → 2200 [RST] Seq=1 Win=0 Len=0
52	838.490909	172.31.255.28	10.1.10.33	TCP	60	62987 → 2200 [SYN] Seq=0 Win=3072 Len=0 MSS=1460
53	838.491869	10.1.10.33	172.31.255.28	TCP	60	2200 → 62987 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
54	838.574849	172.31.255.28	10.1.10.33	TCP	60	62987 → 2200 [RST] Seq=1 Win=0 Len=0
61	841.620326	172.31.255.28	10.1.10.33	TCP	60	62998 → 2200 [SYN] Seq=0 Win=3072 Len=0 MSS=1460
62	841.620454	10.1.10.33	172.31.255.28	TCP	60	2200 → 62998 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
66	841.702309	172.31.255.28	10.1.10.33	TCP	60	62998 → 2200 [RST] Seq=1 Win=0 Len=0
68	842.953872	172.31.255.28	10.1.10.33	TCP	60	62999 → 2200 [SYN] Seq=0 Win=4096 Len=0 MSS=1460
69	842.954330	10.1.10.33	172.31.255.28	TCP	60	2200 → 62999 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
70	843.014462	172.31.255.28	10.1.10.33	TCP	60	62999 → 2200 [RST] Seq=1 Win=0 Len=0
71	958.511357	172.31.255.28	10.1.10.33	TCP	74	40679 → 2200 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=1671690274 TSecr=0 WS=64
72	958.512696	10.1.10.33	172.31.255.28	TCP	74	2200 → 40679 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=129728427 TSecr=1671690274 WS=32
73	958.574598	172.31.255.28	10.1.10.33	TCP	66	40679 → 2200 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=1671690289 TSecr=129728427
74	958.613991	10.1.10.33	172.31.255.28	TCP	105	2200 → 40679 [PSH, ACK] Seq=1 Ack=1 Win=5792 Len=39 TSval=129728452 TSecr=1671690289
75	958.672209	172.31.255.28	10.1.10.33	TCP	66	40679 → 2200 [ACK] Seq=1 Ack=40 Win=5888 Len=0 TSval=1671690316 TSecr=129728452
80	959.971164	172.31.255.28	10.1.10.33	TCP	68	40679 → 2200 [PSH, ACK] Seq=1 Ack=40 Win=5888 Len=2 TSval=1671690640 TSecr=129728452
81	959.972733	10.1.10.33	172.31.255.28	TCP	66	2200 → 40679 [ACK] Seq=40 Ack=3 Win=5792 Len=0 TSval=129728791 TSecr=1671690640
82	959.972738	10.1.10.33	172.31.255.28	TCP	85	2200 → 40679 [PSH, ACK] Seq=40 Ack=3 Win=5792 Len=19 TSval=129728791 TSecr=1671690640

- Question 4

Doing a filter for SSH, I see there is OpenSSH_5.1p1 which is not an option in the selection of answers of either “OpenSSH_5.3p1” or “OpenSSH_5.2”.

ssh

No.	Time	Source	Destination	Protocol	Length	Info
139	1028.880307	10.1.10.60	172.31.255.28	SSH	105	Server: Protocol (SSH-2.0-OpenSSH_5.1p1 Debian-3ubuntu1)
141	1031.362592	172.31.255.28	10.1.10.60	SSH	68	Client: Encrypted packet (len=2)
143	1031.363600	10.1.10.60	172.31.255.28	SSH	85	Server: Encrypted packet (len=19)

```
Internet Protocol Version 4, Src: 10.1.10.60, Dst: 172.31.255.28
    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: 91
    Identification: 0xdc28 (56360)
    010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x9efb [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.1.10.60
    Destination Address: 172.31.255.28
Transmission Control Protocol, Src Port: 22, Dst Port: 53662, Seq: 1, Ack: 1, Len: 39
SSH Protocol
    Protocol: SSH-2.0-OpenSSH_5.1p1 Debian-3ubuntu1
    [Direction: server-to-client]
```

Section 2: Initial Recon

- Question 5

10.1.10.15 and 10.1.10.13

```
Frame 376: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: PCSSystemtec_fb:b8:10 (08:00:27:fb:b8:10), Dst: GrandstreamN_20:3a:43 (00:0b:82:20:3a:43)
Internet Protocol Version 4, Src: 10.1.10.33, Dst: 10.1.10.15
Transmission Control Protocol, Src Port: 33853, Dst Port: 80, Seq: 0, Len: 0
```

```
Frame 133: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: GrandstreamN_21:ad:07 (00:0b:82:21:ad:07), Dst: PCSSystemtec_fb:b8:10 (08:00:27:fb:b8:10)
Internet Protocol Version 4, Src: 10.1.10.13, Dst: 10.1.10.33
Transmission Control Protocol, Src Port: 80, Dst Port: 40456, Seq: 0, Ack: 1, Len: 0
```

- Question 6

1 IP address had port 3389 open.

1031	25.797783	10.1.10.33	10.1.10.130	TCP	74	40709 → 3389 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=131203383 TSecr=0 WS=32
1032	25.797787	10.1.10.33	10.1.10.1	TCP	74	33891 → 3389 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=131203383 TSecr=0 WS=32
1037	25.797800	10.1.10.12	10.1.10.33	TCP	60	3389 → 37832 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1039	25.797806	10.1.10.29	10.1.10.33	TCP	60	3389 → 49390 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1040	25.797809	10.1.10.16	10.1.10.33	TCP	60	3389 → 43177 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1041	25.797812	10.1.10.27	10.1.10.33	TCP	60	3389 → 57181 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1045	25.797860	10.1.10.13	10.1.10.33	TCP	60	3389 → 52225 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1046	25.797863	10.1.10.15	10.1.10.33	TCP	60	3389 → 53526 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1063	25.801531	10.1.10.33	10.1.10.20	TCP	66	46009 → 3389 [RST, ACK] Seq=1 Ack=1 Win=5856 Len=0 TSval=131203384 TSecr=55798963
1068	25.801546	10.1.10.1	10.1.10.33	TCP	60	3389 → 33891 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1100	26.891244	10.1.10.33	10.1.10.130	TCP	74	40731 → 3389 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=131203656 TSecr=0 WS=32

- Question 7

10.1.10.29; Applying a filter for 'telnet', I was able to locate the only HMI connection in frame 1478.

```
> Frame 1478: 129 bytes on wire (1032 bits), 129 bytes captured (1032 bits)
> Ethernet II, Src: Ricoh_d1:a0:8b (00:00:74:d1:a0:8b), Dst: PCSSystemtec_fb:b8:10 (08:00:27:fb:b8:10)
> Internet Protocol Version 4, Src: 10.1.10.29, Dst: 10.1.10.33
> Transmission Control Protocol, Src Port: 23, Dst Port: 46823, Seq: 7, Ack: 28, Len: 63
v Telnet
    Data: \n
    Data: RICOH Maintenance Shell.   \n
    Data: \rUser access verification.\n
    Data: \rlogin:
```

- Question 8

10.1.10.10

1033	25.797789	10.1.10.33	10.1.10.10	TCP	74	46469 → 23 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=131203383 TSecr=0 WS=32
1043	25.797818	10.1.10.10	10.1.10.33	TCP	60	22 → 43195 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1067	25.801543	10.1.10.10	10.1.10.33	TCP	60	23 → 46469 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

10.1.10.16

1047	25.797866	10.1.10.33	10.1.10.16	TCP	74	55111 → 23 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=131203383 TSecr=0 WS=32
1064	25.801533	10.1.10.16	10.1.10.33	TCP	60	22 → 58462 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1071	25.801554	10.1.10.16	10.1.10.33	TCP	74	23 → 55111 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=963631296 TSecr=131203383 WS=1
1077	25.801669	10.1.10.33	10.1.10.16	TCP	66	55111 → 23 [ACK] Seq=1 Ack=1 Win=5856 Len=0 TSval=131203384 TSecr=963631296
1087	25.804691	10.1.10.33	10.1.10.16	TCP	66	55111 → 23 [RST, ACK] Seq=1 Ack=1 Win=5856 Len=0 TSval=131203384 TSecr=963631296
1092	25.819482	10.1.10.16	10.1.10.33	TELNET	81	Telnet Data ...
1096	25.819785	10.1.10.33	10.1.10.16	TCP	60	55111 → 23 [RST] Seq=1 Win=0 Len=0

10.1.10.27

1052	25.798741	10.1.10.33	10.1.10.27	TCP	74	57356 → 23 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=131203383 TSecr=0 WS=32
1066	25.801540	10.1.10.27	10.1.10.33	TCP	60	22 → 54441 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1073	25.801658	10.1.10.27	10.1.10.33	TCP	74	23 → 57356 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=117781539 TSecr=131203383 WS=1
1079	25.801911	10.1.10.33	10.1.10.27	TCP	66	57356 → 23 [ACK] Seq=1 Ack=1 Win=5856 Len=0 TSval=131203384 TSecr=117781539
1088	25.804707	10.1.10.33	10.1.10.27	TCP	66	57356 → 23 [RST, ACK] Seq=1 Ack=1 Win=5856 Len=0 TSval=131203384 TSecr=117781539

Section 3 – SCADA Protocols

- Question 14

admin | root | guest

```
> Frame 243: 731 bytes on wire (5848 bits), 731 bytes captu
> Ethernet II, Src: PCSSystemtec_fb:b8:10 (08:00:27:fb:b8:1
> Internet Protocol Version 4, Src: 10.1.10.33, Dst: 10.1.1
> Transmission Control Protocol, Src Port: 46053, Dst Port:
v Hypertext Transfer Protocol
  > GET /dataview.htm HTTP/1.1\r\n
    Host: 10.1.10.130\r\n
    User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv
    Accept: text/html,application/xhtml+xml,application/xm
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 115\r\n
    Connection: keep-alive\r\n
    Referer: http://10.1.10.130/navtree.htm\r\n
  v [truncated]Authorization: Digest username="guest", re
      username="guest"
      realm="1763-L16BWA B/9.00"
      nonce="a4b8c8d7e0f6a7b2c3d2e4f5a4b7c5d2e7f"
      uri="/dataview.htm"
      algorithm=MD5
      response="ebb5aa5ceba186ce5fbd0547cf6cf922"
      qop=auth
      nc=00000001
    \r\n
    [Full request URI: http://10.1.10.130/dataview.htm]
    [HTTP request 1/1]
```

```
> Frame 1028: 731 bytes on wire (5848 bits), 731 bytes captu
> Ethernet II, Src: PCSSystemtec_fb:b8:10 (08:00:27:fb:b8:10
> Internet Protocol Version 4, Src: 10.1.10.33, Dst: 10.1.10
> Transmission Control Protocol, Src Port: 46120, Dst Port:
v Hypertext Transfer Protocol
  > GET /diagover.htm HTTP/1.1\r\n
    Host: 10.1.10.130\r\n
    User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:
    Accept: text/html,application/xhtml+xml,application/xml
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 115\r\n
    Connection: keep-alive\r\n
    Referer: http://10.1.10.130/navtree.htm\r\n
  v [truncated]Authorization: Digest username="admin", rea
      username="admin"
      realm="1763-L16BWA B/9.00"
      nonce="a4b8c8d7e0f6a7b2c3d2e4f5a4b7c5d2e7f"
      uri="/diagover.htm"
      algorithm=MD5
      response="f639a4351771f0ad71dc2e92abf2f081"
      qop=auth
      nc=00000001
    \r\n
    [Full request URI: http://10.1.10.130/diagover.htm]
    [HTTP request 1/1]
```

```
> Frame 1050: 730 bytes on wire (5840 bits), 730 bytes captur
> Ethernet II, Src: PCSSystemtec_fb:b8:10 (08:00:27:fb:b8:10)
> Internet Protocol Version 4, Src: 10.1.10.33, Dst: 10.1.10.
> Transmission Control Protocol, Src Port: 46124, Dst Port: 8
v Hypertext Transfer Protocol
  > GET /diagover.htm HTTP/1.1\r\n
    Host: 10.1.10.130\r\n
    User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.
    Accept: text/html,application/xhtml+xml,application/xml;q
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 115\r\n
    Connection: keep-alive\r\n
    Referer: http://10.1.10.130/navtree.htm\r\n
  v [truncated]Authorization: Digest username="root", realm=
      username="root"
      realm="1763-L16BWA B/9.00"
      nonce="a4b8c8d7e0f6a7b2c3d2e4f5a4b7c5d2e7f"
      uri="/diagover.htm"
      algorithm=MD5
      response="7cef1b26f92414bafc1bc2f52d4902e9"
      qop=auth
      nc=00000001
    \r\n
    [Full request URI: http://10.1.10.130/diagover.htm]
    [HTTP request 1/1]
```

Section 4: PLC Web Recon

- Question 17

A-B WWW/0.1

```
> Frame 9: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: RSAutomation_02:52:51 (00:0f:73:02:52:51), Dst: PCSSystemtec_fb:b8:10 (08:00:27:fb:b8:10)
> Internet Protocol Version 4, Src: 10.1.10.130, Dst: 10.1.10.33
> Transmission Control Protocol, Src Port: 80, Dst Port: 46032, Seq: 947, Ack: 381, Len: 0
> [3 Reassembled TCP Segments (946 bytes): #5(105), #7(841), #9(0)]
v Hypertext Transfer Protocol
  v HTTP/1.0 200 OK\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.0 200 OK\r\n]
      Response Version: HTTP/1.0
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Server: A-B WWW/0.1\r\n
    Expires: Thu, 01 Dec 1994 16:00:00 GMT\r\n
    Content-Type: text/html\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.051268000 seconds]
    [Request in frame: 4]
    [Request URI: http://10.1.10.130/]
    File Data: 841 bytes
> Line-based text data: text/html (9 lines)
```

Section 5: HMI Web Recon

- Questions 29

21222

```
> Frame 21222: 82 bytes on wire (656 bits), 82 bytes captured (656 bits)
> Ethernet II, Src: RSAutomation_02:52:51 (00:0f:73:02:52:51), Dst: Dell_ab:23:be (14:fe:b5:ab:23:be)
> Internet Protocol Version 4, Src: 10.1.10.130, Dst: 10.1.10.20
v Transmission Control Protocol, Src Port: 44818, Dst Port: 49348, Seq: 1, Ack: 29, Len: 28
    Source Port: 44818
    Destination Port: 49348
    [Stream index: 90]
  > [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 28]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 218431857
    [Next Sequence Number: 29    (relative sequence number)]
    Acknowledgment Number: 29    (relative ack number)
    Acknowledgment number (raw): 2415816062
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 2000
    [Calculated window size: 2000]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x7490 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (28 bytes)
    [PDU Size: 28]
v EtherNet/IP (Industrial Protocol), Session: 0x9A3F2CC1, Register Session
  v Encapsulation Header
      Command: Register Session (0x0065)
      Length: 4
      Session Handle: 0x9a3f2cc1
      Status: Success (0x00000000)
      Sender Context: 455645524553542b
      Options: 0x00000000
  v Command Specific Data
      Protocol Version: 1
      Option Flags: 0x0000
```

```
> Frame 20796: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
> Ethernet II, Src: 54:52:55:53:54:1f (54:52:55:53:54:1f), Dst: Dell_ab:23:be (14:fe:b5:ab:23:be)
v Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: RSAutomation_02:52:51 (00:0f:73:02:52:51)
    Sender IP address: 10.1.10.130
    Target MAC address: Dell_ab:23:be (14:fe:b5:ab:23:be)
    Target IP address: 10.1.10.20
```

```
> Frame 20784: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
> Ethernet II, Src: 54:52:55:53:54:1f (54:52:55:53:54:1f), Dst: Apple_48:d0:ee (10:9a:dd:48:d0:ee)
v Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: RSAutomation_02:52:51 (00:0f:73:02:52:51)
    Sender IP address: 10.1.10.130
    Target MAC address: Apple_48:d0:ee (10:9a:dd:48:d0:ee)
    Target IP address: 10.1.10.35
```

```
> Frame 20795: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
> Ethernet II, Src: 54:52:55:53:54:1f (54:52:55:53:54:1f), Dst: RSAutomation_02:52:51 (00:0f:73:02:52:51)
v Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: Dell_ab:23:be (14:fe:b5:ab:23:be)
    Sender IP address: 10.1.10.20
    Target MAC address: RSAutomation_02:52:51 (00:0f:73:02:52:51)
    Target IP address: 10.1.10.130
```