RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **TECH-T11**

DEEP DIVE ANALYSIS OF ENTERPRISE NETWORK SECURITY MECHANISMS

Dr. Avril Salter, AJ1VA, CCNP-W, CCNA-S, CWNE-350

Independent Consultant
Salter & Associates
@AvrilSalterUSA

The question that triggered this presentation

Why This Presentation Matters

- Common Enterprise Issues
  - Ambiguous network security protocols in use
  - Diversity of solutions
    - Across business units
    - Network line
    - User / equipment
  - Hardware and software variances
  - Monitoring
  - Feature complexity

Session Outline and Learning Objectives

Network security protocols

- SSH
- TLS
- IPsec
- 802.1X

Looking for commonalty to improve understanding

Evolutionary improvements

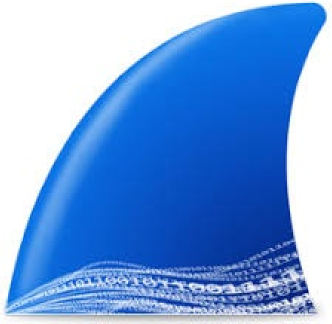
- Functionality
- Cryptographic algorithms
- Forward secrecy

Gain insights into where things are going

Today’s Presentation is Mostly Demonstrations

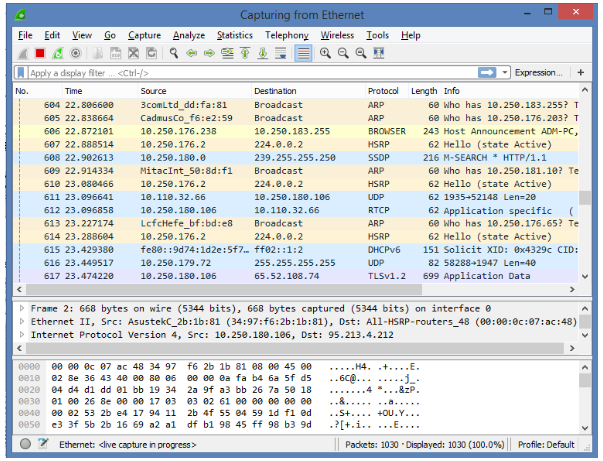
Wireshark

- Open source tool for packet analysis



PCAPs

- https://tinyurl.com/qohs6lk


Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

No.	Time	Source	Destination	Protocol	Length	Info
604	22.806600	3comLtd_dd:fa:81	Broadcast	ARP	60	Who has 10.250.183.255? T
605	22.838664	CadmusCo_f6:e2:59	Broadcast	ARP	60	Who has 10.250.176.203? T
606	22.872101	10.250.176.238	10.250.183.255	BROWSER	243	Host Announcement ADM-PC,
607	22.888514	10.250.176.2	224.0.0.2	HSRP	62	Hello (state Active)
608	22.902613	10.250.180.0	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
609	22.914334	MitacInt_50:8d:f1	Broadcast	ARP	60	Who has 10.250.181.10? Te
610	23.080466	10.250.176.2	224.0.0.2	HSRP	62	Hello (state Active)
611	23.096641	10.110.32.66	10.250.180.106	UDP	62	1935→52148 Len=20
612	23.096858	10.250.180.106	10.110.32.66	RTCP	62	Application specific (
613	23.227174	LcfcHefe_bf:bd:e8	Broadcast	ARP	60	Who has 10.250.176.65? Te
614	23.288604	10.250.176.2	224.0.0.2	HSRP	62	Hello (state Active)
615	23.429380	fe80::9d74:1d2e:5f7…	ff02::1:2	DHCPv6	151	Solicit XID: 0x4329c CID:
616	23.449517	10.250.179.72	255.255.255.255	UDP	82	58288→1947 Len=40
617	23.474220	10.250.180.106	65.52.108.74	TLSv1.2	699	Application Data

```
▷ Frame 2: 668 bytes on wire (5344 bits), 668 bytes captured (5344 bits) on interface 0
▷ Ethernet II, Src: AsustekC_2b:1b:81 (34:97:f6:2b:1b:81), Dst: All-HSRP-routers_48 (00:00:0c:07:ac:48)
▷ Internet Protocol Version 4, Src: 10.250.180.106, Dst: 95.213.4.212
```

```
0000  00 00 0c 07 ac 48 34 97  f6 2b 1b 81 08 00 45 00   .....H4. .+....E.
0010  02 8e 36 43 40 00 80 06  00 00 0a fa b4 6a 5f d5   ..6C@... .....j_.
0020  04 d4 d1 dd 01 bb 19 34  2a 9f a3 bb 26 7a 50 18   .......4 *...&zP.
0030  01 00 26 8e 00 00 17 03  03 02 61 00 00 00 00 00   ..&..... ..a.....
0040  00 02 53 2b e4 17 94 11  2b 4f 55 04 59 1d f1 0d   ..S+.... +OU.Y...
0050  e3 3f 5b 2b 16 69 a2 a1  df b1 98 45 ff 98 b3 9d   .?[+.i.. ...E....
```

Ethernet: <live capture in progress>
Packets: 1030 · Displayed: 1030 (100.0%)
Profile: Default

https://www.dropbox.com/sh/inxjtpt96lfxfng/AABTZ2gnHMOD4m-ngaLpy5nla?dl=0

Things to Observe

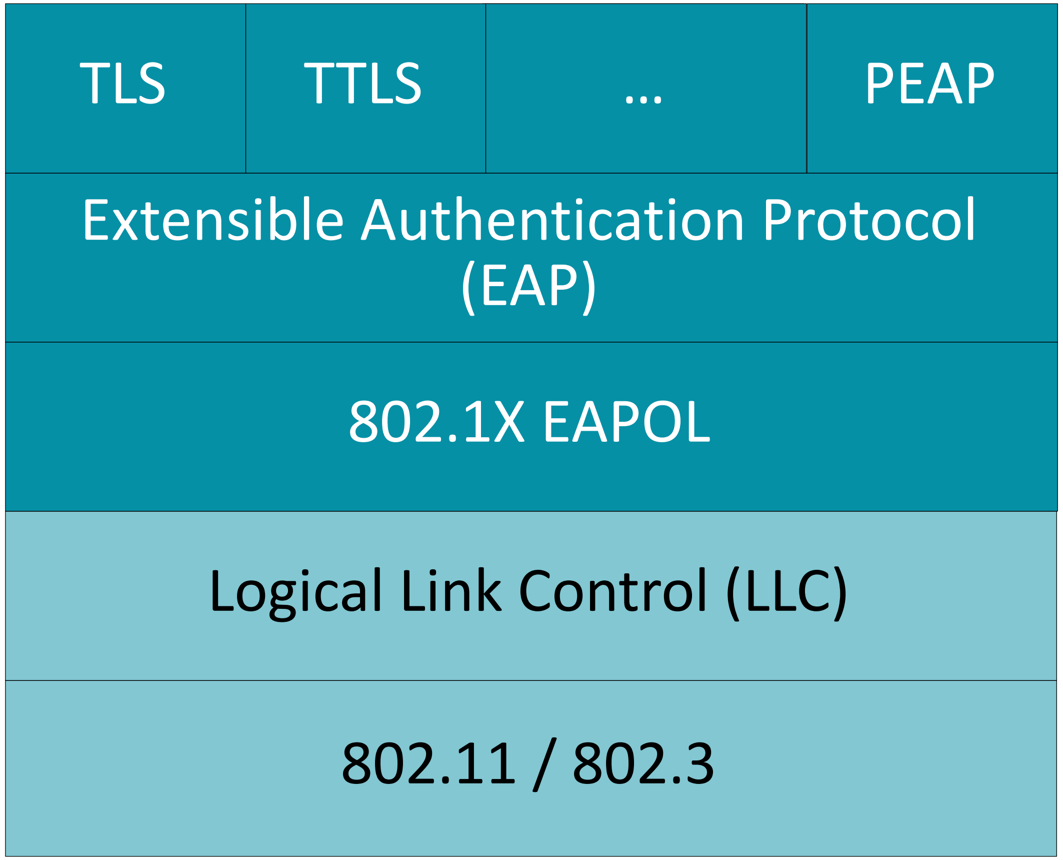
- Business goals drive the message flows
- Multiple protocols or layers required to deliver network security
- Same underlying security mechanisms
  - PSK, public/private cryptography
  - Sharing of keying material
  - Generate shared secret
  - Encryption, message integrity

Techniques that as security experts you are aware of

802.1X / EAP

Business Usage

Multiple Layers



TLS | TTLS | … | PEAP

Extensible Authentication Protocol (EAP)

802.1X EAPOL

Logical Link Control (LLC)

802.11 / 802.3

Evolution

Wired

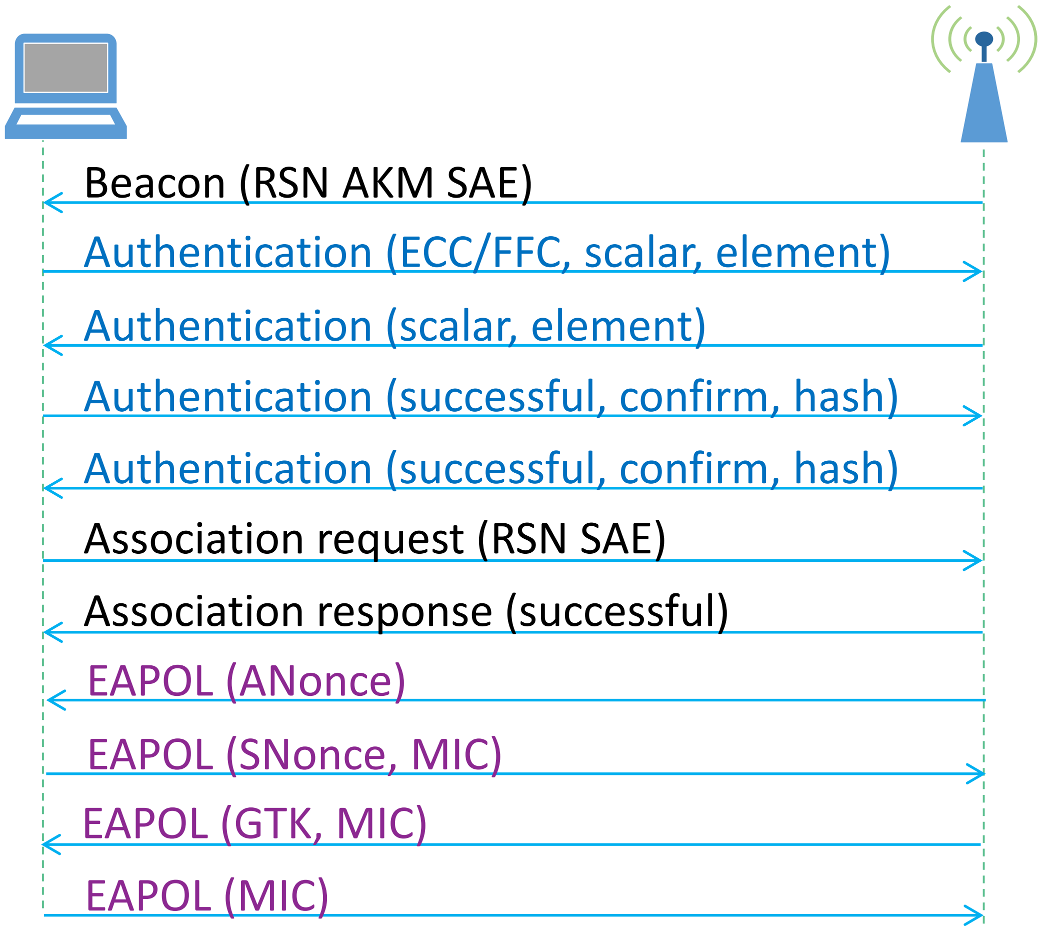
- MACsec
- MACsec Key Agreement (MKA)

Wireless

WPA3	
Personal	Enterprise
128 AES	192 AES
SAE	802.1X
PMF Mandatory	PMF Mandatory

802.1X EAPOL

WPA3-Personal



Beacon (RSN AKM SAE)

Authentication (ECC/FFC, scalar, element)

Authentication (scalar, element)

Authentication (successful, confirm, hash)

Authentication (successful, confirm, hash)

Association request (RSN SAE)

Association response (successful)

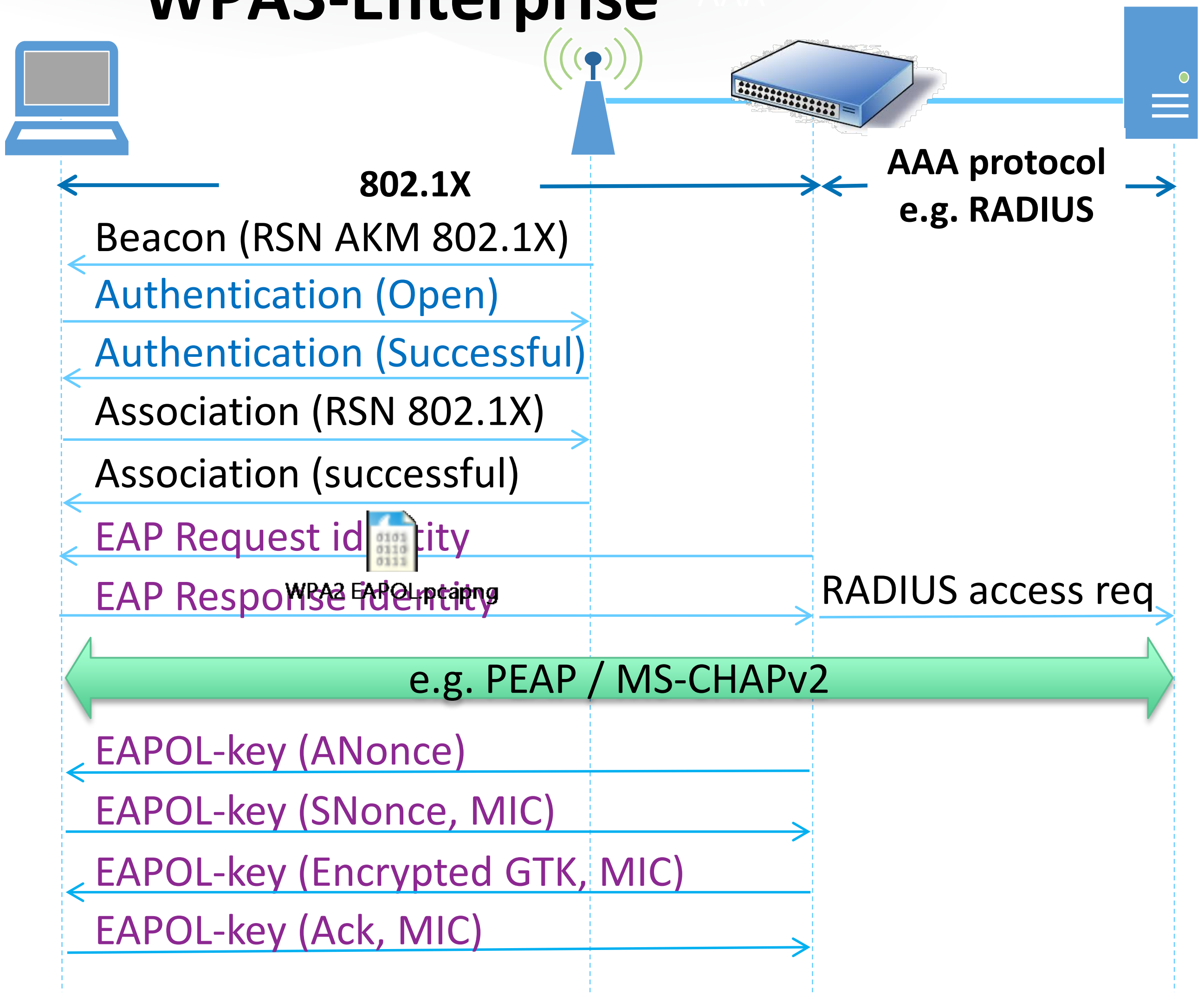
EAPOL (ANonce)

EAPOL (SNonce, MIC)

EAPOL (GTK, MIC)

EAPOL (MIC)

WPA3-Enterprise



802.1X

AAA protocol
e.g. RADIUS

Beacon (RSN AKM 802.1X)

Authentication (Open)

Authentication (Successful)

Association (RSN 802.1X)

Association (successful)

EAP Request identity

EAP Response identity

RADIUS access req

e.g. PEAP / MS-CHAPv2

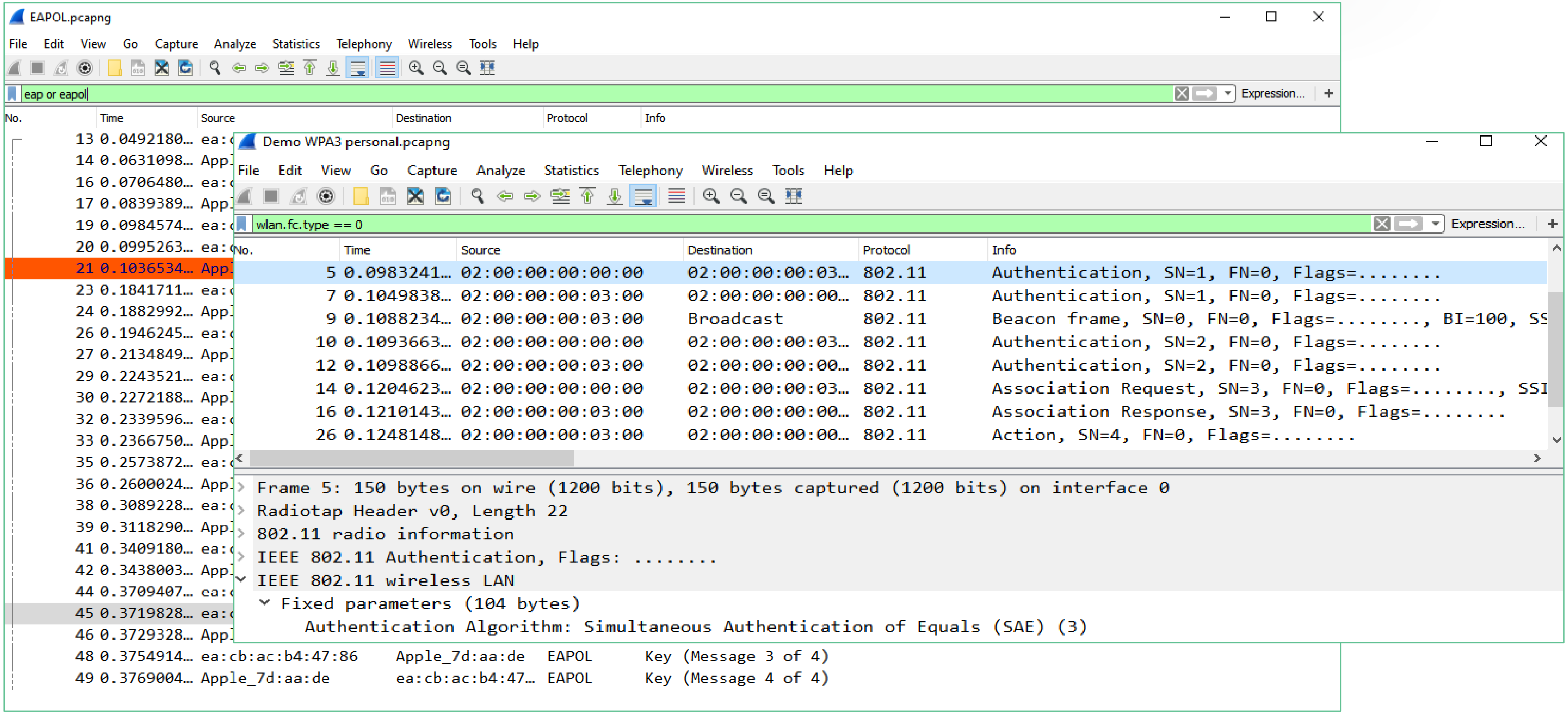
EAPOL-key (ANonce)

EAPOL-key (SNonce, MIC)

EAPOL-key (Encrypted GTK, MIC)

EAPOL-key (Ack, MIC)

802.1X Demonstration



EAPOL.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

eap or eapol

```
No.   Time           Source              Destination        Protocol   Info
   13 0.0492180… ea:c
   14 0.0631098… Appl
   16 0.0706480… ea:c
   17 0.0839389… Appl
   19 0.0984574… ea:c
   20 0.0995263… ea:c
   21 0.1036534… Appl
   23 0.1841711… ea:c
   24 0.1882992… Appl
   26 0.1946245… ea:c
   27 0.2134849… Appl
   29 0.2243521… ea:c
   30 0.2272188… Appl
   32 0.2339596… ea:c
   33 0.2366750… Appl
   35 0.2573872… ea:c
   36 0.2600024… Appl
   38 0.3089228… ea:c
   39 0.3118290… Appl
   41 0.3409180… ea:c
   42 0.3438003… Appl
   44 0.3709407… ea:c
   45 0.3719828… ea:c
   46 0.3729328… Appl
   48 0.3754914… ea:cb:ac:b4:47:86   Apple_7d:aa:de     EAPOL      Key (Message 3 of 4)
   49 0.3769004… Apple_7d:aa:de      ea:cb:ac:b4:47…    EAPOL      Key (Message 4 of 4)
```

Demo WPA3 personal.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

wlan.fc.type == 0

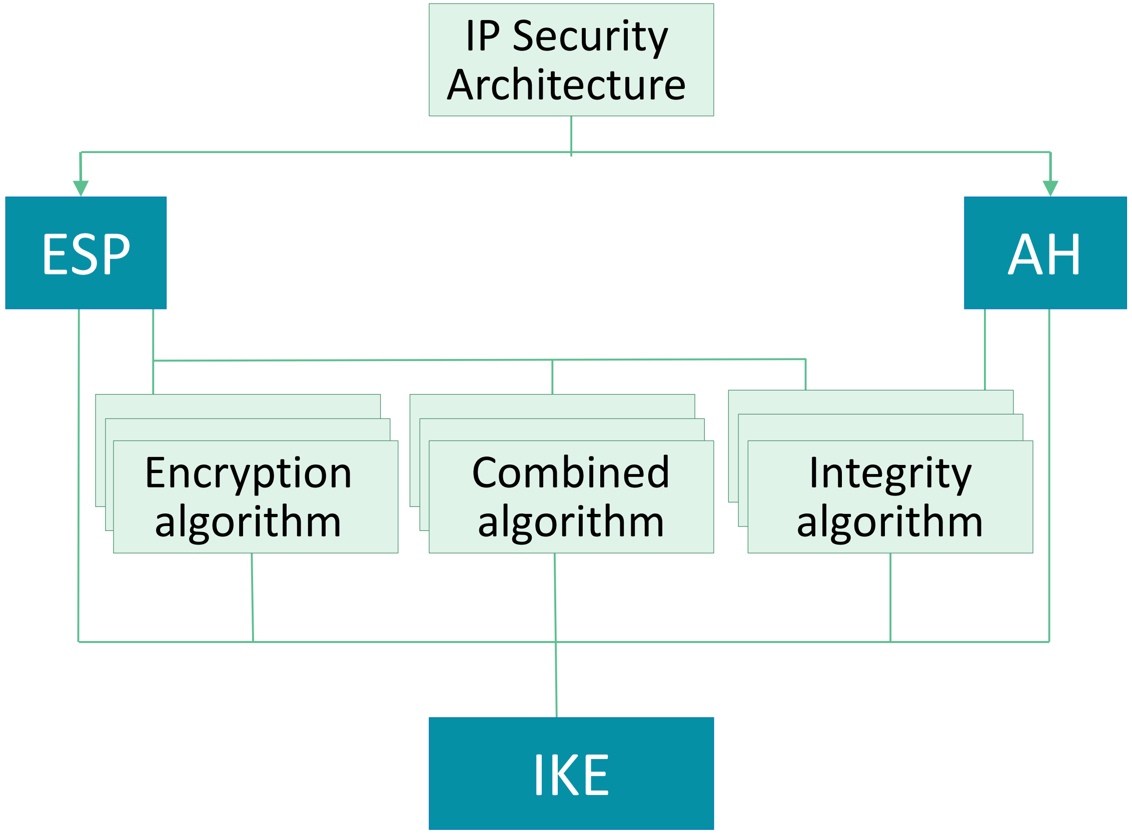
```
No.  Time          Source              Destination         Protocol  Info
   5 0.0983241… 02:00:00:00:00:00   02:00:00:00:03…    802.11    Authentication, SN=1, FN=0, Flags=........
   7 0.1049838… 02:00:00:00:03:00   02:00:00:00:00…    802.11    Authentication, SN=1, FN=0, Flags=........
   9 0.1088234… 02:00:00:00:03:00   Broadcast          802.11    Beacon frame, SN=0, FN=0, Flags=........, BI=100, SS
  10 0.1093663… 02:00:00:00:00:00   02:00:00:00:03…    802.11    Authentication, SN=2, FN=0, Flags=........
  12 0.1098866… 02:00:00:00:03:00   02:00:00:00:00…    802.11    Authentication, SN=2, FN=0, Flags=........
  14 0.1204623… 02:00:00:00:00:00   02:00:00:00:03…    802.11    Association Request, SN=3, FN=0, Flags=........, SSI
  16 0.1210143… 02:00:00:00:03:00   02:00:00:00:00…    802.11    Association Response, SN=3, FN=0, Flags=........
  26 0.1248148… 02:00:00:00:03:00   02:00:00:00:00…    802.11    Action, SN=4, FN=0, Flags=........
```

```
> Frame 5: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface 0
> Radiotap Header v0, Length 22
> 802.11 radio information
> IEEE 802.11 Authentication, Flags: ........
v IEEE 802.11 wireless LAN
  v Fixed parameters (104 bytes)
      Authentication Algorithm: Simultaneous Authentication of Equals (SAE) (3)
```

IPsec

Business Usage

Multiple Layers



Evolution of IKE

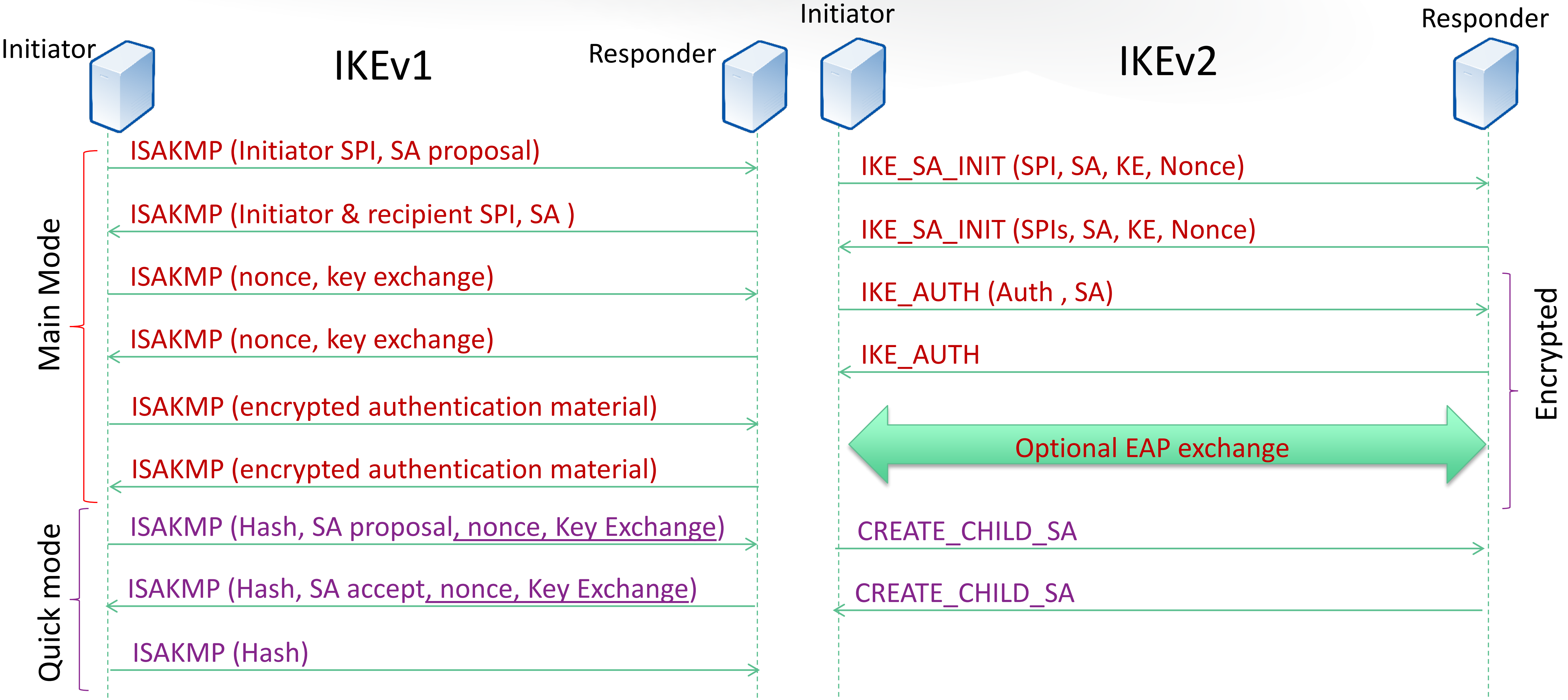
IKEv1

- Phase 1 Main mode
  - IKE SA Negotiation
  - 6 Messages
- Phase 2 Quick Mode
  - IPSec SA Negotiation
  - 3 messages
- Validate peers
  - Pre-Shared Keys
  - Certificates

IKEv2

- Phase 1
  - 4 messages
  - Encrypts after 2 messages
- Phase 2 Creates first CHILD SA
- New DH values, encryption & hashing algorithms
- Adds EAP
- Possible future changes
  - Labeled IPsec

Evolution of IKE



IKEv1

Initiator

Responder

Main Mode

ISAKMP (Initiator SPI, SA proposal)

ISAKMP (Initiator & recipient SPI, SA)

ISAKMP (nonce, key exchange)

ISAKMP (nonce, key exchange)

ISAKMP (encrypted authentication material)

ISAKMP (encrypted authentication material)

Quick mode

ISAKMP (Hash, SA proposal, nonce, Key Exchange)

ISAKMP (Hash, SA accept, nonce, Key Exchange)

ISAKMP (Hash)

IKEv2

Initiator

Responder

IKE_SA_INIT (SPI, SA, KE, Nonce)

IKE_SA_INIT (SPIs, SA, KE, Nonce)

IKE_AUTH (Auth , SA)

IKE_AUTH

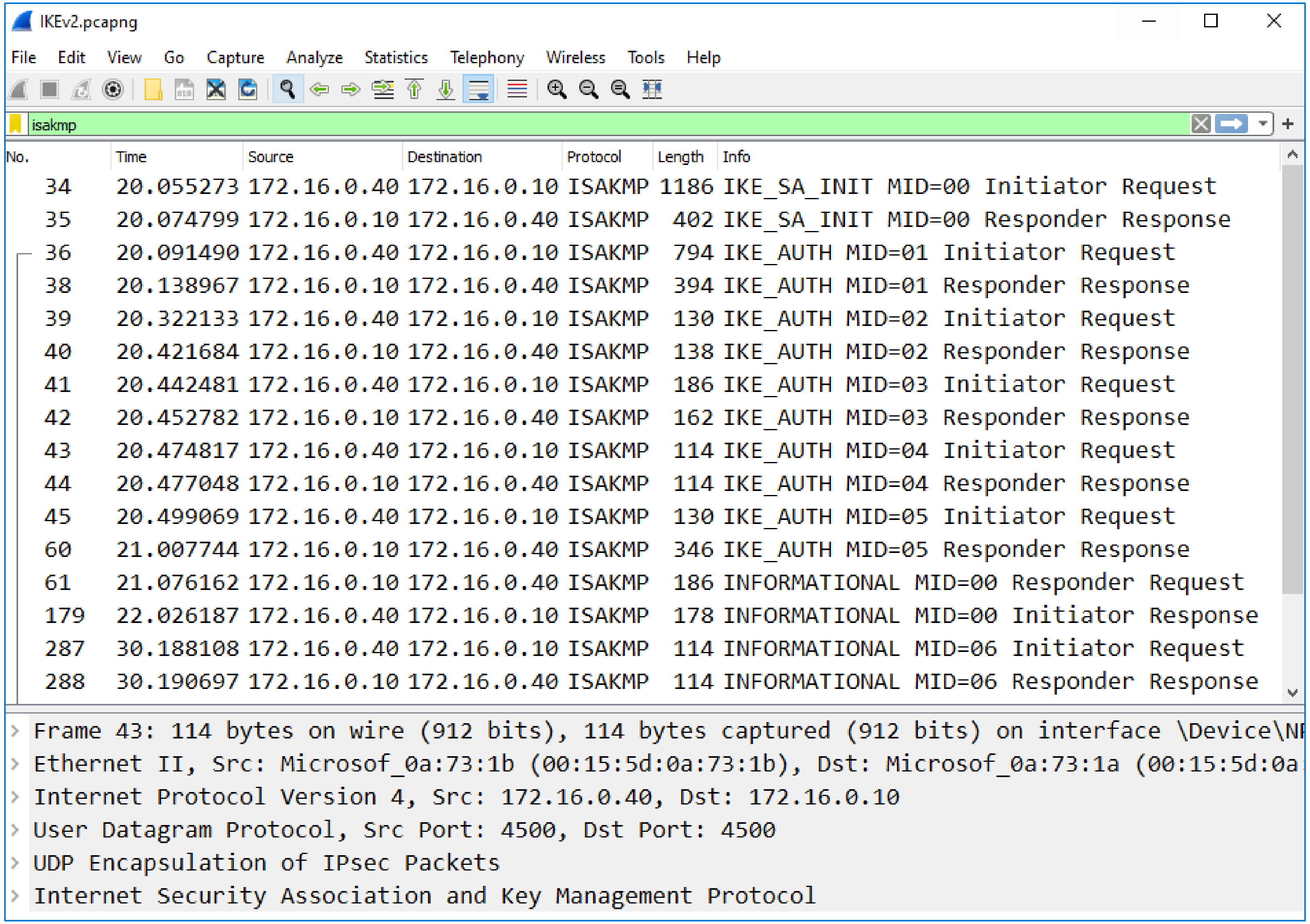
Optional EAP exchange

Encrypted

CREATE_CHILD_SA

CREATE_CHILD_SA

IKE v2 Demonstration



isakmp

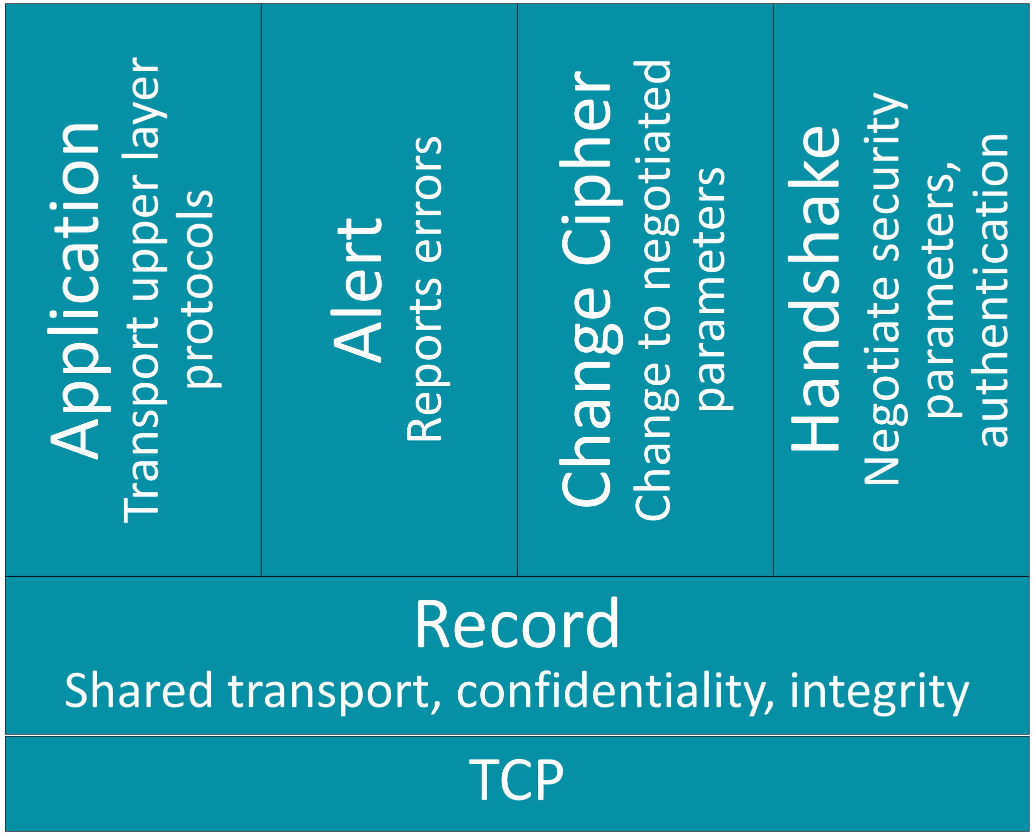
```
No.     Time      Source      Destination Protocol Length Info
  34    20.055273 172.16.0.40 172.16.0.10 ISAKMP 1186 IKE_SA_INIT MID=00 Initiator Request
  35    20.074799 172.16.0.10 172.16.0.40 ISAKMP  402 IKE_SA_INIT MID=00 Responder Response
  36    20.091490 172.16.0.40 172.16.0.10 ISAKMP  794 IKE_AUTH MID=01 Initiator Request
  38    20.138967 172.16.0.10 172.16.0.40 ISAKMP  394 IKE_AUTH MID=01 Responder Response
  39    20.322133 172.16.0.40 172.16.0.10 ISAKMP  130 IKE_AUTH MID=02 Initiator Request
  40    20.421684 172.16.0.10 172.16.0.40 ISAKMP  138 IKE_AUTH MID=02 Responder Response
  41    20.442481 172.16.0.40 172.16.0.10 ISAKMP  186 IKE_AUTH MID=03 Initiator Request
  42    20.452782 172.16.0.10 172.16.0.40 ISAKMP  162 IKE_AUTH MID=03 Responder Response
  43    20.474817 172.16.0.40 172.16.0.10 ISAKMP  114 IKE_AUTH MID=04 Initiator Request
  44    20.477048 172.16.0.10 172.16.0.40 ISAKMP  114 IKE_AUTH MID=04 Responder Response
  45    20.499069 172.16.0.40 172.16.0.10 ISAKMP  130 IKE_AUTH MID=05 Initiator Request
  60    21.007744 172.16.0.10 172.16.0.40 ISAKMP  346 IKE_AUTH MID=05 Responder Response
  61    21.076162 172.16.0.10 172.16.0.40 ISAKMP  186 INFORMATIONAL MID=00 Responder Request
  179   22.026187 172.16.0.40 172.16.0.10 ISAKMP  178 INFORMATIONAL MID=00 Initiator Response
  287   30.188108 172.16.0.40 172.16.0.10 ISAKMP  114 INFORMATIONAL MID=06 Initiator Request
  288   30.190697 172.16.0.10 172.16.0.40 ISAKMP  114 INFORMATIONAL MID=06 Responder Response
```

```
> Frame 43: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface \Device\NF
> Ethernet II, Src: Microsof_0a:73:1b (00:15:5d:0a:73:1b), Dst: Microsof_0a:73:1a (00:15:5d:0a
> Internet Protocol Version 4, Src: 172.16.0.40, Dst: 172.16.0.10
> User Datagram Protocol, Src Port: 4500, Dst Port: 4500
> UDP Encapsulation of IPsec Packets
> Internet Security Association and Key Management Protocol
```

TLS

Business Usage

Multiple Layers



Application
Transport upper layer protocols

Alert
Reports errors

Change Cipher
Change to negotiated parameters

Handshake
Negotiate security parameters, authentication

Record
Shared transport, confidentiality, integrity

TCP

Evolution of TLS

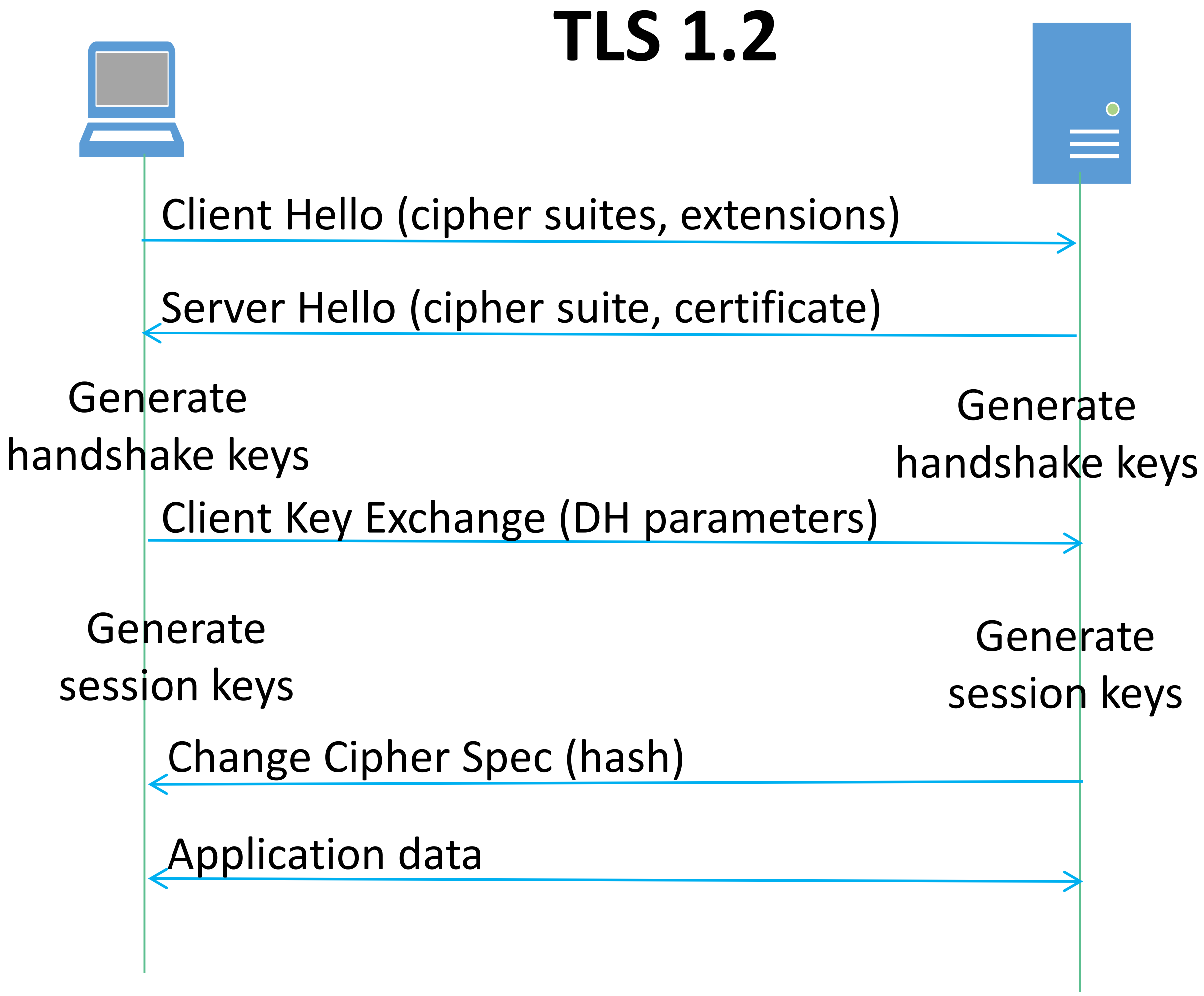
TLS1.2

- IETF RFC 5246
- Incrementally modified and enhanced
- Recommended version since 2008
- Increasing number of attacks
- Performance concerns

TLS 1.3

- IETF RFC 8446
- Finalized March 2018
- Major redesign
- Cryptographic changes
  - Supported encryption algorithms
  - Messages to negotiate a session
  - PSK with DHE

Evolution of TLS



TLS 1.2

Client Hello (cipher suites, extensions)

Server Hello (cipher suite, certificate)

Generate handshake keys

Generate handshake keys

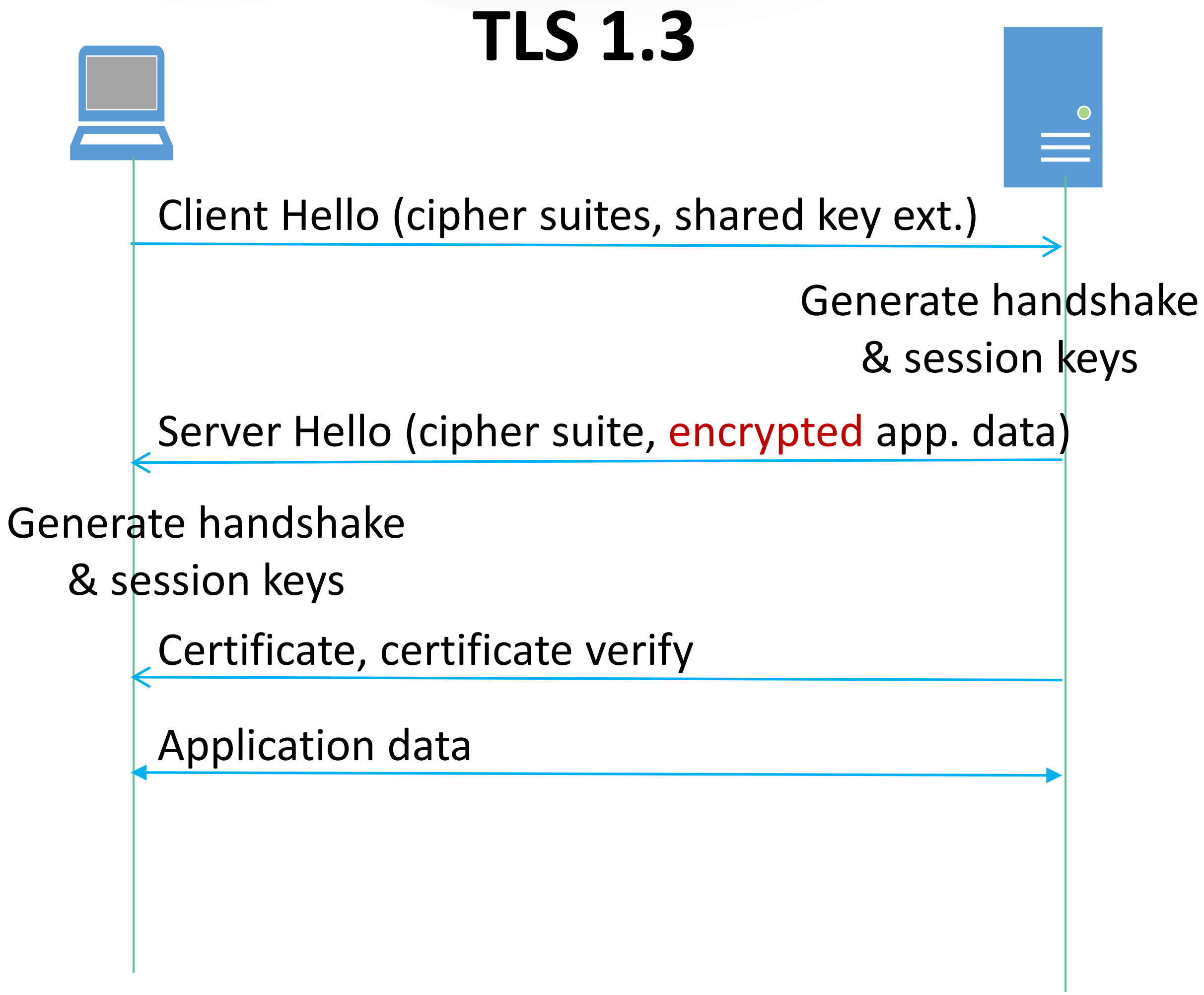
Client Key Exchange (DH parameters)

Generate session keys

Generate session keys

Change Cipher Spec (hash)

Application data



TLS 1.3

Client Hello (cipher suites, shared key ext.)

Generate handshake & session keys

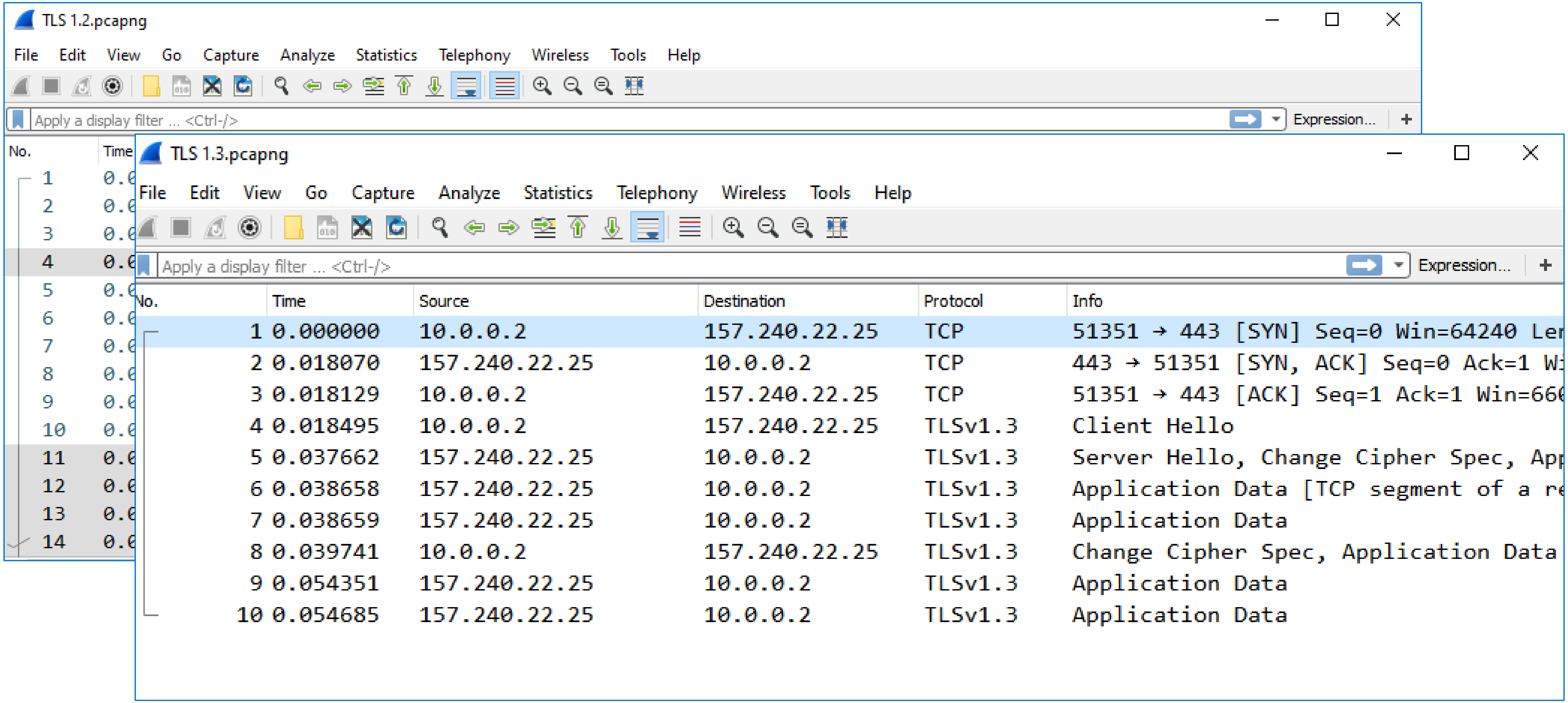
Server Hello (cipher suite, encrypted app. data)

Generate handshake & session keys

Certificate, certificate verify

Application data

TLS 1.2 and TLS 1.3 Demonstration


TLS 1.2.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
TLS 1.3.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

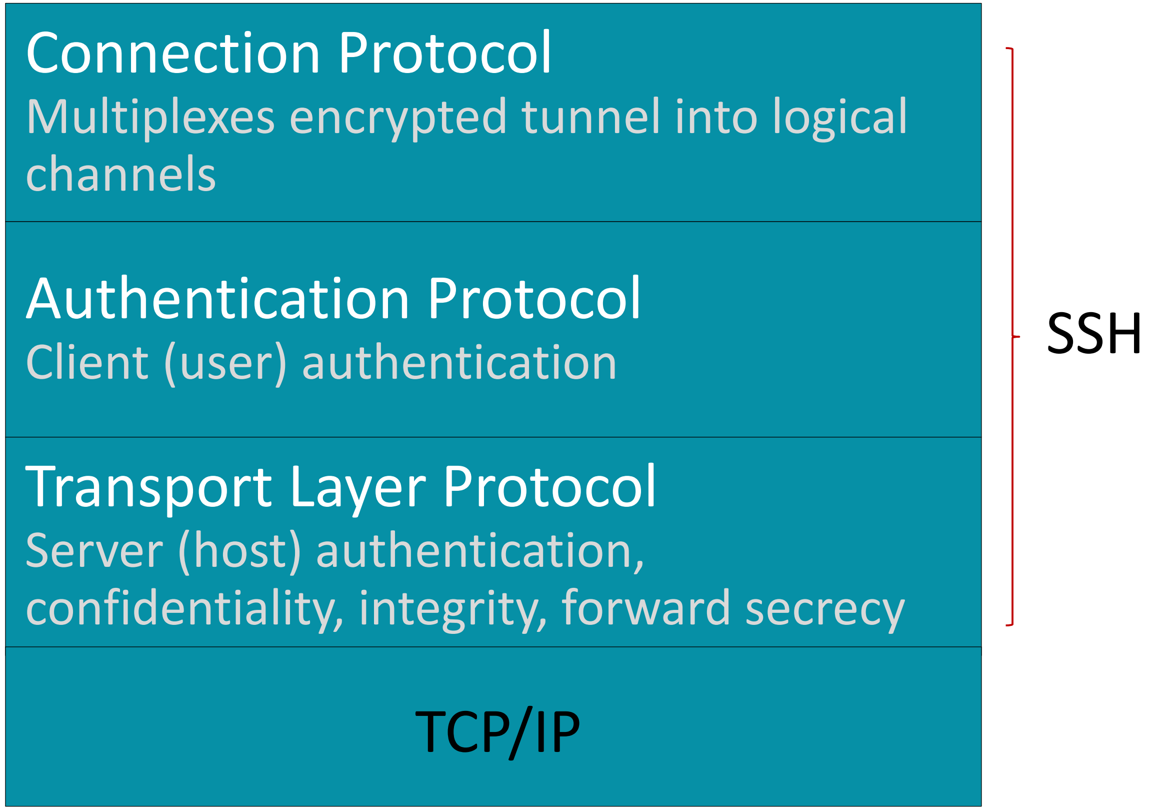
```
No.   Time
 1    0.0
 2    0.0
 3    0.0
 4    0.0
 5    0.0
 6    0.0
 7    0.0
 8    0.0
 9    0.0
10    0.0
11    0.0
12    0.0
13    0.0
14    0.0
```

```
No.  Time      Source          Destination     Protocol  Info
  1 0.000000  10.0.0.2        157.240.22.25   TCP       51351 → 443 [SYN] Seq=0 Win=64240 Len
  2 0.018070  157.240.22.25   10.0.0.2        TCP       443 → 51351 [SYN, ACK] Seq=0 Ack=1 Wi
  3 0.018129  10.0.0.2        157.240.22.25   TCP       51351 → 443 [ACK] Seq=1 Ack=1 Win=66
  4 0.018495  10.0.0.2        157.240.22.25   TLSv1.3   Client Hello
  5 0.037662  157.240.22.25   10.0.0.2        TLSv1.3   Server Hello, Change Cipher Spec, App
  6 0.038658  157.240.22.25   10.0.0.2        TLSv1.3   Application Data [TCP segment of a re
  7 0.038659  157.240.22.25   10.0.0.2        TLSv1.3   Application Data
  8 0.039741  10.0.0.2        157.240.22.25   TLSv1.3   Change Cipher Spec, Application Data
  9 0.054351  157.240.22.25   10.0.0.2        TLSv1.3   Application Data
 10 0.054685  157.240.22.25   10.0.0.2        TLSv1.3   Application Data
```

Secure Shell (SSH)

Business Usage

Three layers



Connection Protocol
Multiplexes encrypted tunnel into logical channels

Authentication Protocol
Client (user) authentication

Transport Layer Protocol
Server (host) authentication, confidentiality, integrity, forward secrecy

TCP/IP

Evolution of SSH

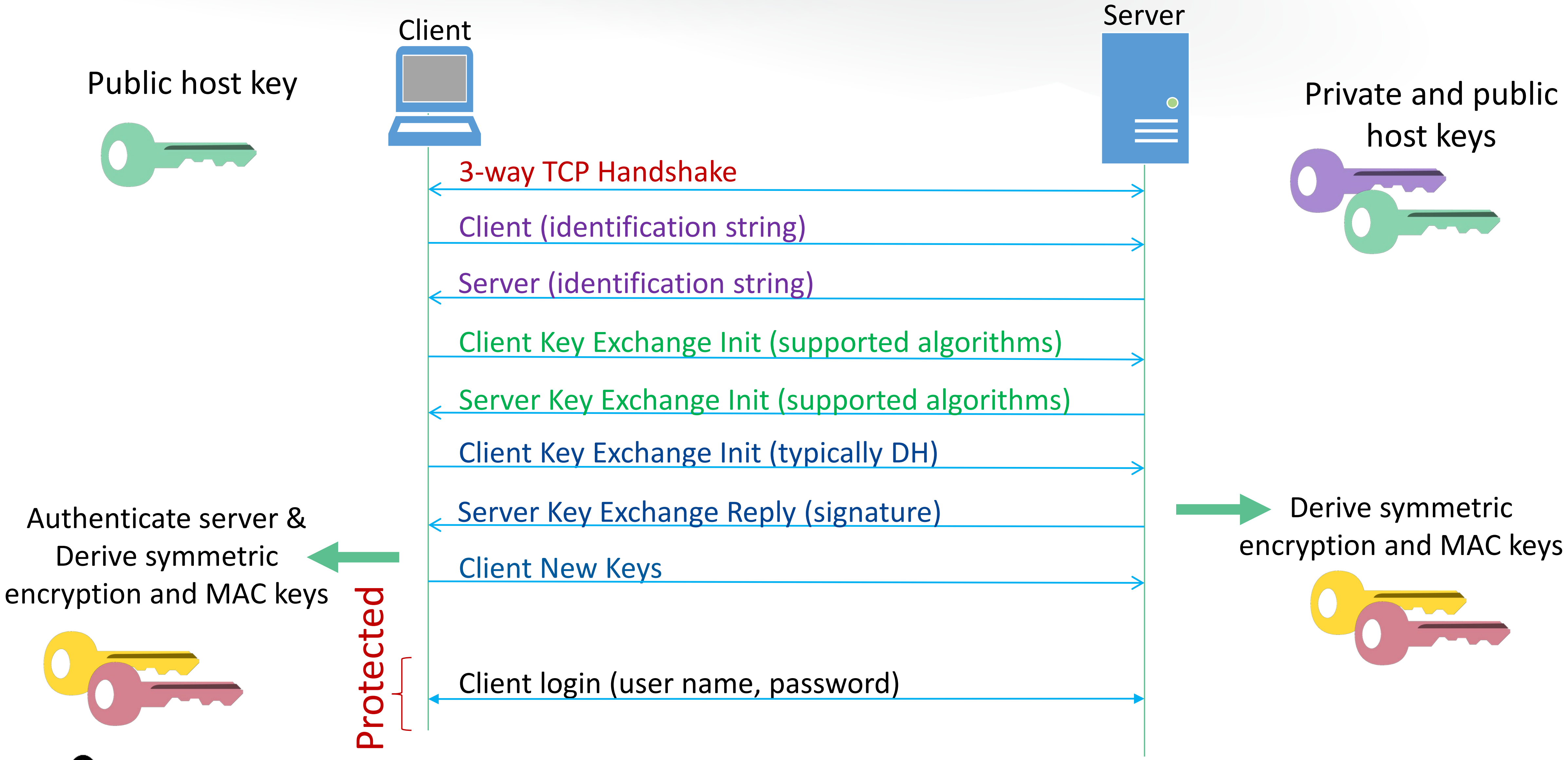
SSHv2

- Different protocol to SSHv1
- Only host keys
- Stronger encryption ciphers
- Message integrity checking
- Support for public keys certificates
- OpenSSH

Extensions

- Stronger cryptography
  - Elliptic curve
  - SHA-256, SHA-512
- Negotiation mechanism RFC 8308

SSH



Client

Server

Public host key

Private and public host keys

3-way TCP Handshake

Client (identification string)

Server (identification string)

Client Key Exchange Init (supported algorithms)

Server Key Exchange Init (supported algorithms)

Client Key Exchange Init (typically DH)

Server Key Exchange Reply (signature)

Derive symmetric encryption and MAC keys

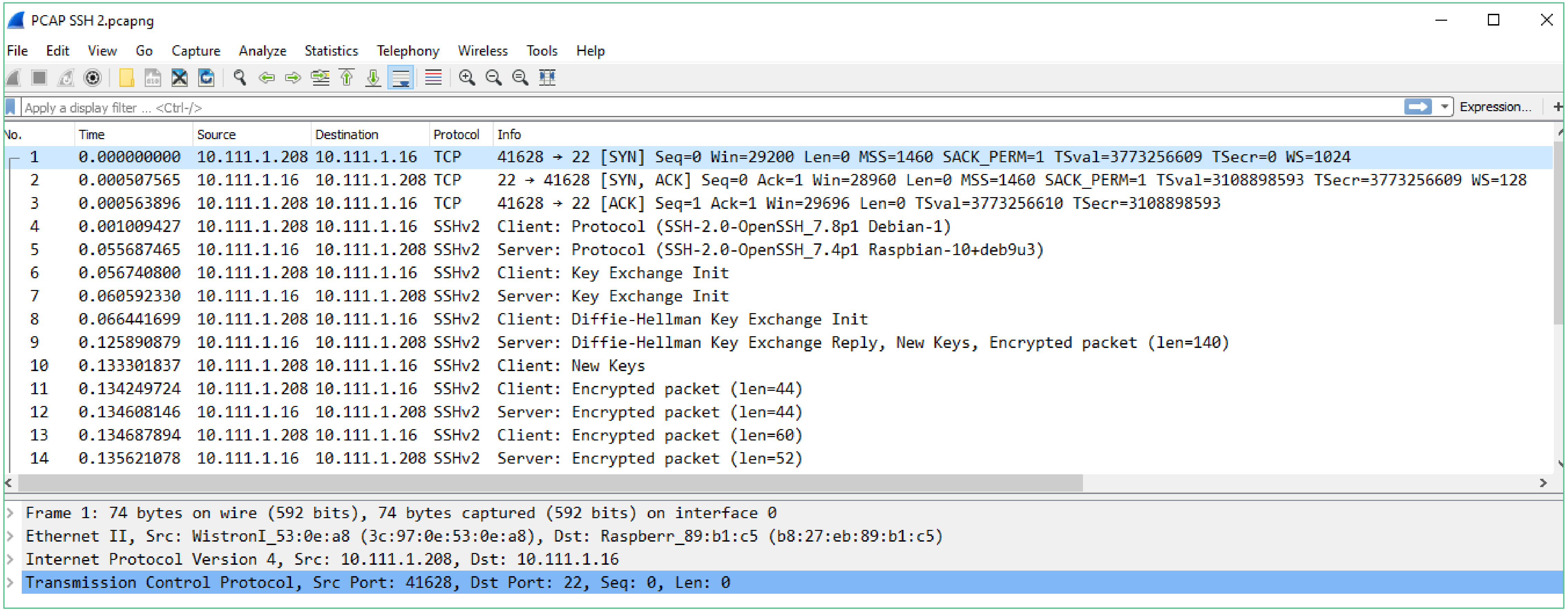
Authenticate server & Derive symmetric encryption and MAC keys

Client New Keys

Protected

Client login (user name, password)

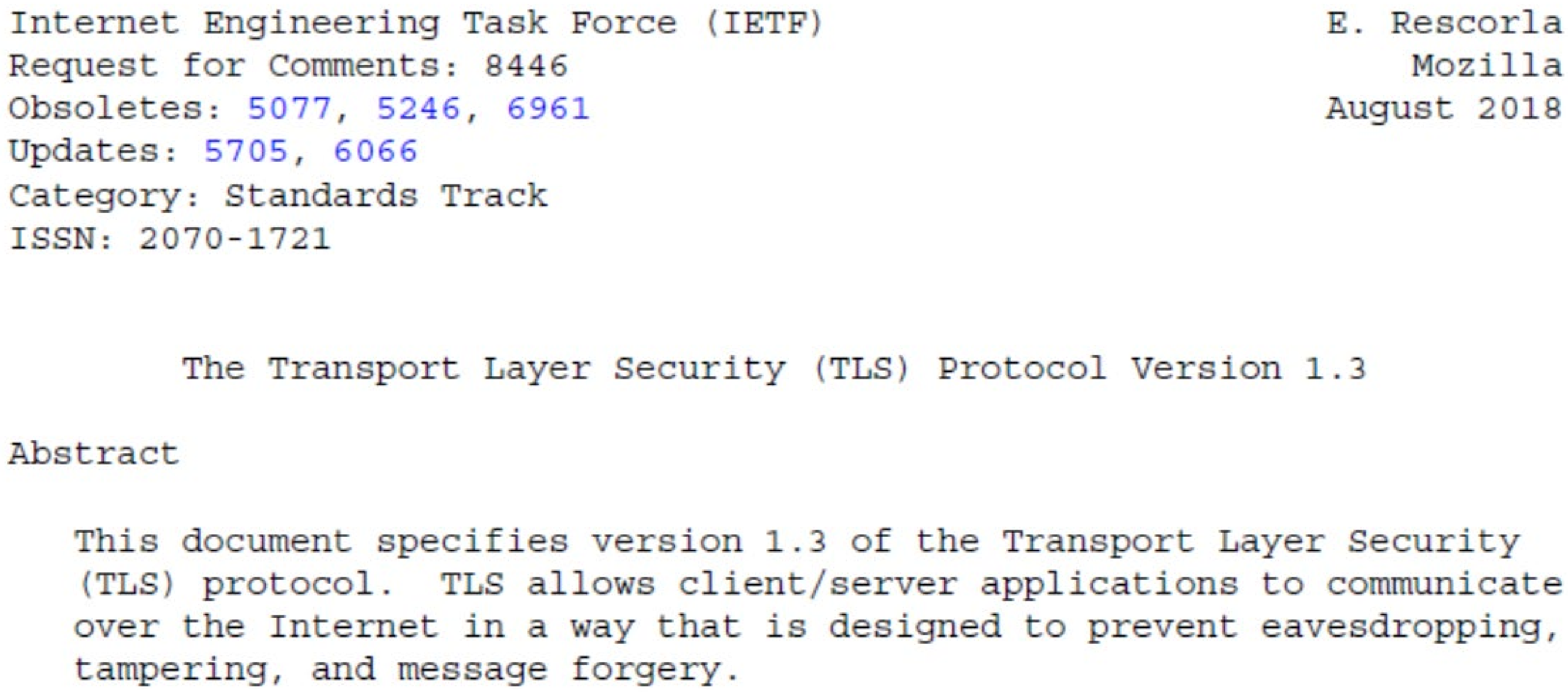
SSH2 Demonstration



```
No.  Time         Source       Destination  Protocol Info
1    0.000000000  10.111.1.208 10.111.1.16  TCP      41628 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3773256609 TSecr=0 WS=1024
2    0.000507565  10.111.1.16  10.111.1.208 TCP      22 → 41628 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=3108898593 TSecr=3773256609 WS=128
3    0.000563896  10.111.1.208 10.111.1.16  TCP      41628 → 22 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=3773256610 TSecr=3108898593
4    0.001009427  10.111.1.208 10.111.1.16  SSHv2    Client: Protocol (SSH-2.0-OpenSSH_7.8p1 Debian-1)
5    0.055687465  10.111.1.16  10.111.1.208 SSHv2    Server: Protocol (SSH-2.0-OpenSSH_7.4p1 Raspbian-10+deb9u3)
6    0.056740800  10.111.1.208 10.111.1.16  SSHv2    Client: Key Exchange Init
7    0.060592330  10.111.1.16  10.111.1.208 SSHv2    Server: Key Exchange Init
8    0.066441699  10.111.1.208 10.111.1.16  SSHv2    Client: Diffie-Hellman Key Exchange Init
9    0.125890879  10.111.1.16  10.111.1.208 SSHv2    Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=140)
10   0.133301837  10.111.1.208 10.111.1.16  SSHv2    Client: New Keys
11   0.134249724  10.111.1.208 10.111.1.16  SSHv2    Client: Encrypted packet (len=44)
12   0.134608146  10.111.1.16  10.111.1.208 SSHv2    Server: Encrypted packet (len=44)
13   0.134687894  10.111.1.208 10.111.1.16  SSHv2    Client: Encrypted packet (len=60)
14   0.135621078  10.111.1.16  10.111.1.208 SSHv2    Server: Encrypted packet (len=52)
```

```
> Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: WistronI_53:0e:a8 (3c:97:0e:53:0e:a8), Dst: Raspberr_89:b1:c5 (b8:27:eb:89:b1:c5)
> Internet Protocol Version 4, Src: 10.111.1.208, Dst: 10.111.1.16
> Transmission Control Protocol, Src Port: 41628, Dst Port: 22, Seq: 0, Len: 0
```

The Best Reference is the Specification



```
Internet Engineering Task Force (IETF)                      E. Rescorla
Request for Comments: 8446                                      Mozilla
Obsoletes: 5077, 5246, 6961                                 August 2018
Updates: 5705, 6066
Category: Standards Track
ISSN: 2070-1721


        The Transport Layer Security (TLS) Protocol Version 1.3

Abstract

   This document specifies version 1.3 of the Transport Layer Security
   (TLS) protocol.  TLS allows client/server applications to communicate
   over the Internet in a way that is designed to prevent eavesdropping,
   tampering, and message forgery.
```

Next Steps

7 DAYS

Find

What protocols are you using?

- Get permission
- Capture traffic

30 DAYS

Explore

What fields attributes are important?

- Download technical specifications
- Look up definitions

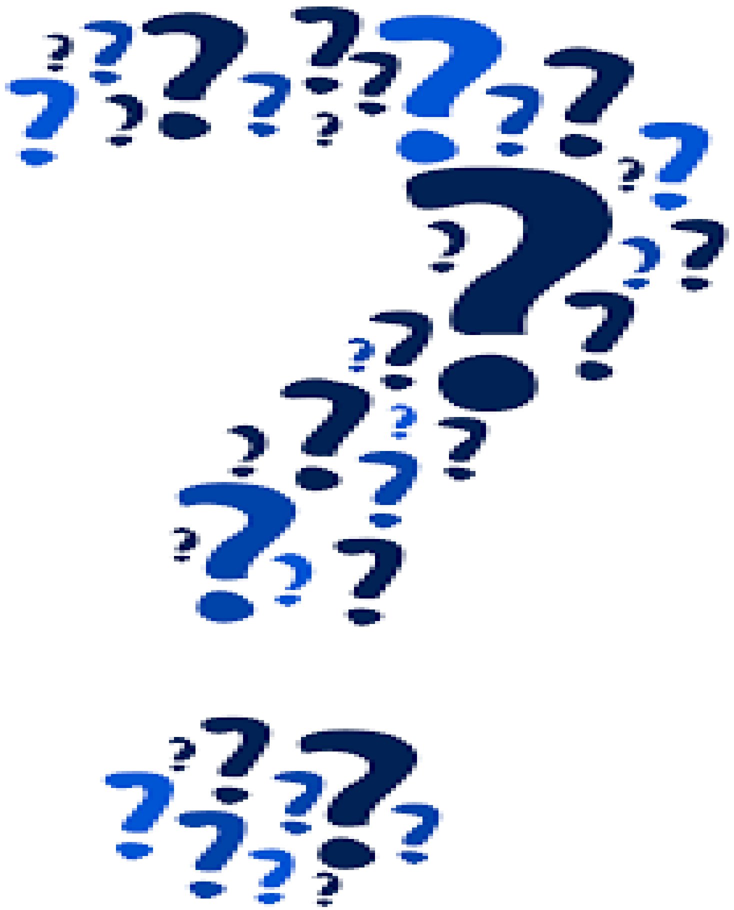
90 DAYS

Discover

What future access needs are essential?

- IoT
- 5G

Thank you for listening ☺



www.**linkedin**.com/in/**avrilsalter**

@avrilsalterUSA