



SHARKFEST '13

Wireshark Developer and User Conference

Understanding Encryption Services Using Wireshark

Sunday June 16th 2013

Larry Greenblatt

Jedi Knight | InterNetwork Defense

SHARKFEST '13

UC Berkeley

June 16-19, 2013

About me

Musician:

- Gung Ho! - Lead Guitar / Vocals / Songwriter
- Philly's #1 Cyber Punk Band since 1980
 - Produced by Otto Capobianco



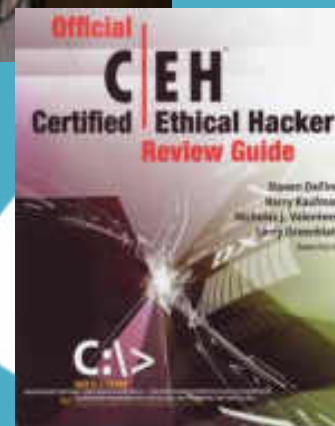
Martial Artist:

- Black Sash Taiji
3rd Degree Black Belt JLFS



Hobbies (my day job):

- Network nerd (& InfoSec geek) 1984
Consultant / Instructor / Author
CISM, CISSP, CEH, ECSA, Security+
Co-Founder of InterNetwork Defense



Just How Long Have I Been a Network Dweeb?

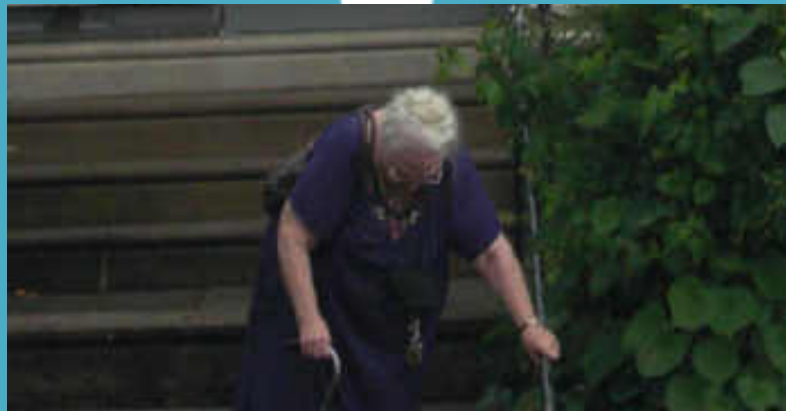


Guidelines from my Mother

Always suspect of anyone:

- “That's what they want you to think”
- “That's how they get you”
- “They get you coming and going”

Can tell you the Greek origin of any word



Guidelines from my band

You know you could mess somebody up
wit dat!

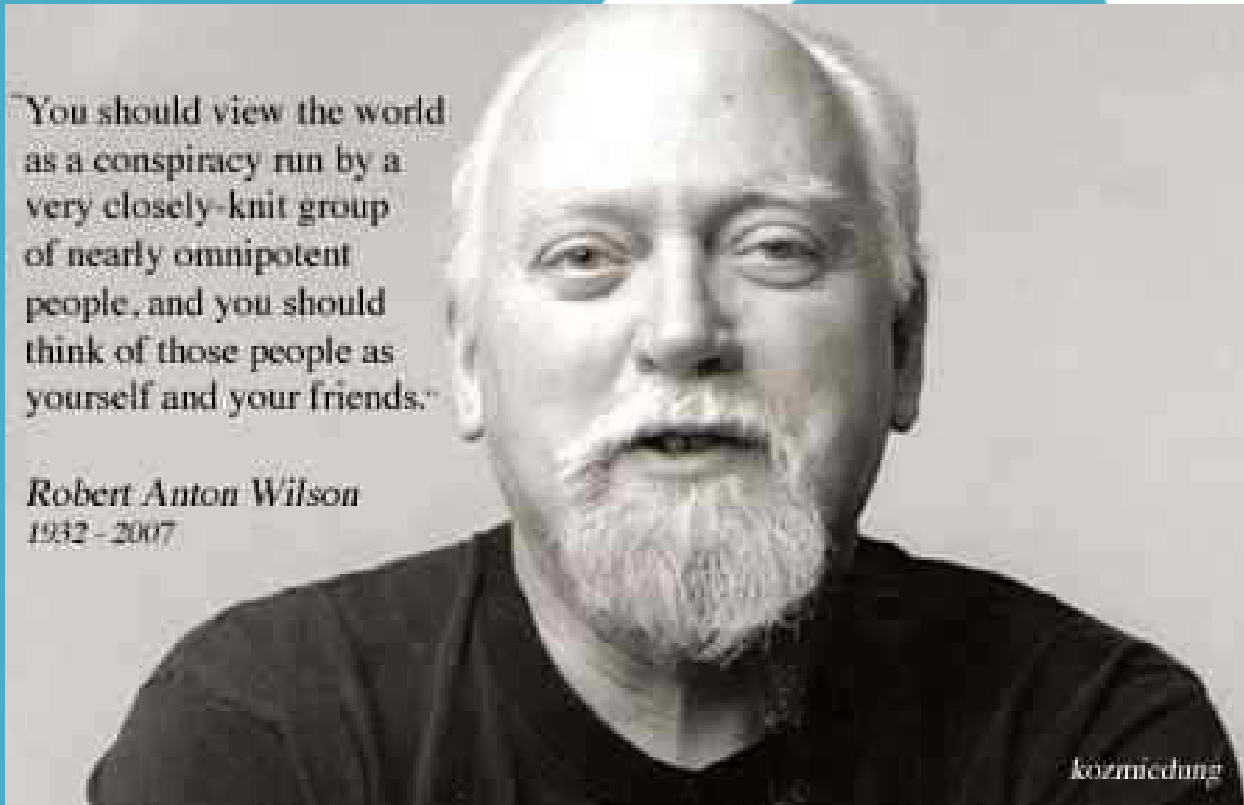


Guidelines from Robert Anton Wilson

“You Can't Speak Matter of Factually About Anything You Can't Measure”

You should view the world as a conspiracy run by a very closely-knit group of nearly omnipotent people, and you should think of those people as yourself and your friends.

Robert Anton Wilson
1932 - 2007



kozmedung

What is a Hacker?

RFC-2828

**"someone who figures things out
and makes something cool happen"**

Intro to Crypt0

with Bob & Alice

A Consumers Guide to:

- 1) Confidentiality
- 2) Authentication
- 3) Integrity
- 4) Non-Repudiation

By Employing:

Symmetric, **Asymmetric** and **Hashing** Algorithms

It is said that “Packets Do Not Lie”



The World's Most Popular Network Protocol Analyzer

Capture



Interface List

Live list of the capture interfaces (shows incoming packets)

Start capture on interface:

- Broadcom NetXtreme Gigabit Ethernet
- Microsoft
- MS Tunnel Interface Driver



Capture Options

Start a capture with detailed options

Capture Help



How to Capture

Step by step to a successful capture



Network Media

Specific information for capturing on Ethernet, WLAN, ...

Files



Open

Open a previously captured file

Open Recent:

D:\cxf\Documents\Packet Captures\chavte.pcap (203 KB)

Online



Website

Visit the project's website



User's Guide

The User's Guide (local version, if installed)

Security

Work with Wireshark as securely as possible

Wireshark: Capture Options

Capture

Interface: Local Broadcom NetXtreme Gigabit Ethernet; Driver: \Device\NPF_{C7F6...}

IP address: fe80::e802:2783:6985:9c1f, 10.16.30.79

Link-layer header type: Ethernet

Capture packets in promiscuous mode

Capture packets in pcap-ng format

Limit each packet to 65535 bytes

Buffer size: 1 megabyte(s)

Capture Filter: ether host fe80::e802:2783:6985:9c1f

Wireless Settings

Remote Settings

Compile BPF

Capture File(s)

File: Browse...

Use multiple files

Next file every 1 megabyte(s)

Next file every 1 minute(s)

Ring buffer with 2 files

Display Options

Update list of packets in real time

Automatic scrolling in live capture

Hide capture info dialog

Name Resolution

The Intelligent Consumer

welcome to the
Crypto-Mart

Aisle 1 Symmetric Algorithms (Shared Secret)



RC4
AES
Twofish
Blowfish
DES & 3DES
E0

Aisle 2 Asymmetric Algorithms (Public/Private)

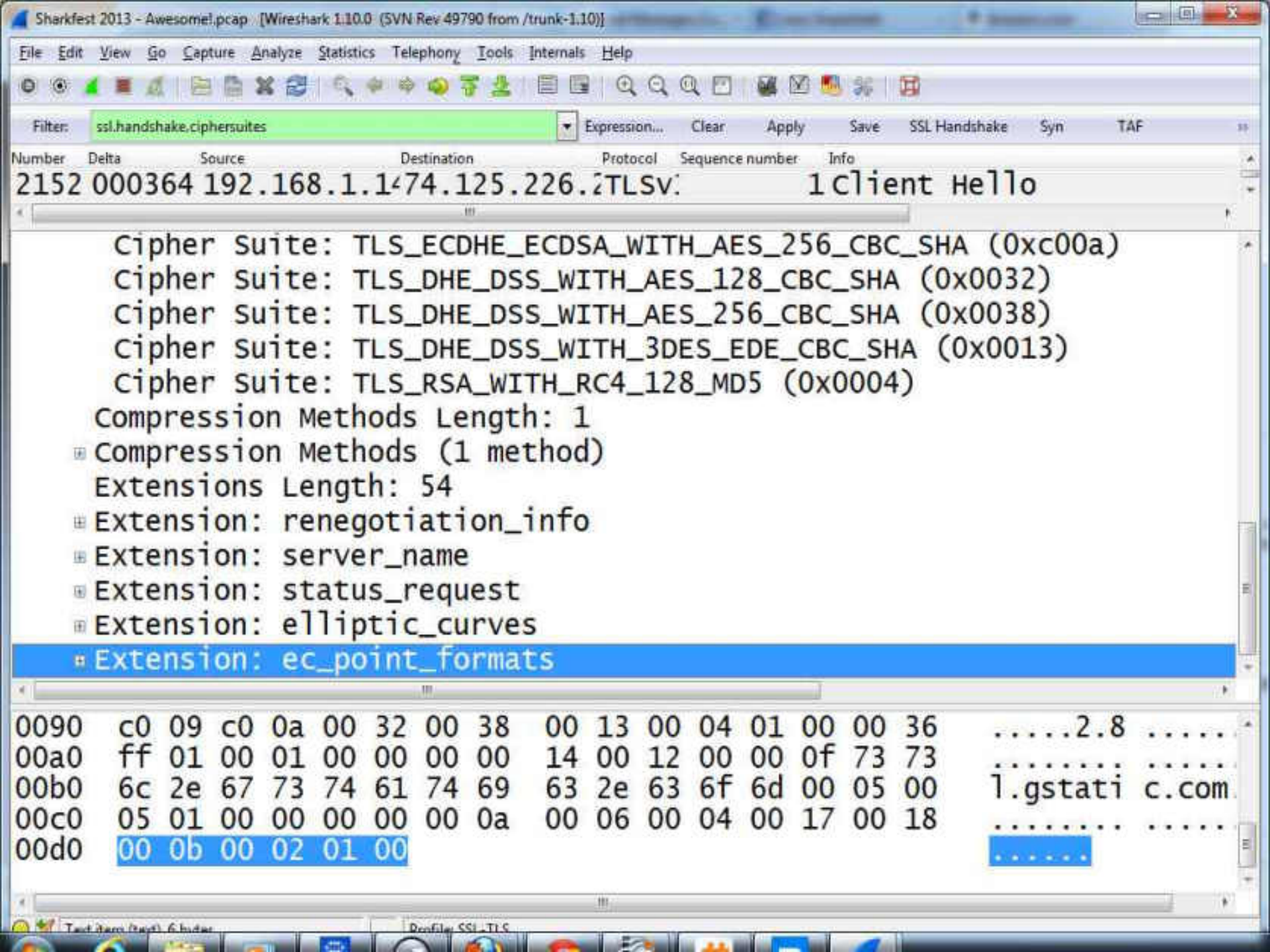


Diffie-Hellman
RSA
ECC
El Gamal

Aisle 3 Hashing Algorithms (Message Digests)



MD5
SHA1, SHA2 & SHA3
Skein
Whirlpool



Number	Delta	Source	Destination	Protocol	Sequence number	Info
2152	000364	192.168.1.1	74.125.226.2	TLSv1		client hello

- Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
- Cipher Suite: TLS_DHE_DSS_WITH_AES_128_CBC_SHA (0x0032)
- Cipher Suite: TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038)
- Cipher Suite: TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (0x0013)
- Cipher Suite: TLS_RSA_WITH_RC4_128_MD5 (0x0004)
- Compression Methods Length: 1
- Compression Methods (1 method)
- Extensions Length: 54
- Extension: renegotiation_info
- Extension: server_name
- Extension: status_request
- Extension: elliptic_curves
- Extension: ec_point_formats**

0090	c0	09	c0	0a	00	32	00	38	00	13	00	04	01	00	00	362.8
00a0	ff	01	00	01	00	00	00	00	14	00	12	00	00	0f	73	73
00b0	6c	2e	67	73	74	61	74	69	63	2e	63	6f	6d	00	05	00	1.gstati	c.com
00c0	05	01	00	00	00	00	00	0a	00	06	00	04	00	17	00	18
00d0	00	0b	00	02	01	00											

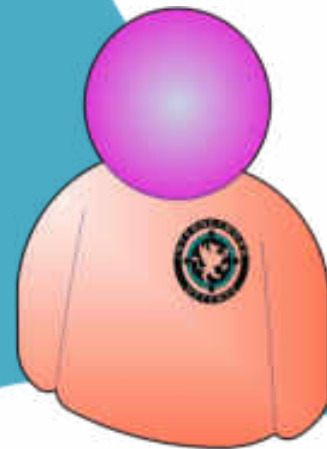
Part 1

Symmetric Encryption

- Bob wants to share a secret with Alice
 - *First they must both secretly agree on a shared key. **How?***



Bob



Alice

Symmetric Encryption

- **Strengths**
 - Fast
- **Challenges**
 - Key Agreement
 - Scalability
 - $N(N-1)/2$
- **Security Services:**
 - Confidentiality
 - Limited* authenticity

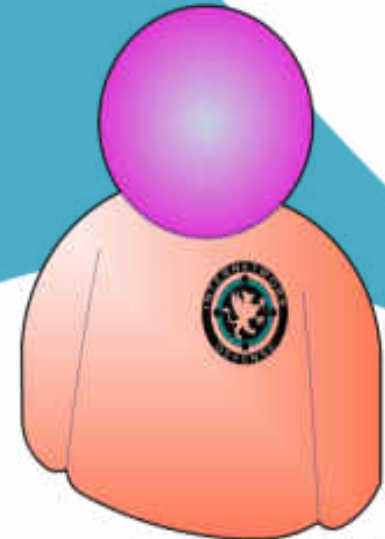
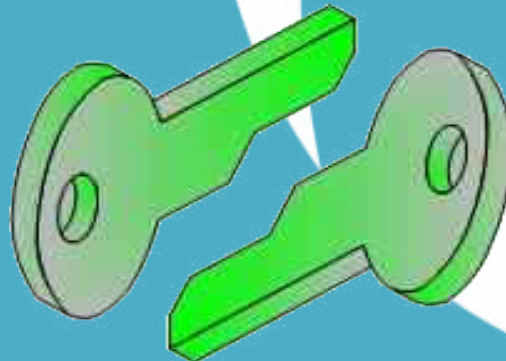


**Alice knows it is Bob, but she can't prove it!*

Part 2

Asymmetric Encryption

- Alice creates a related key pair
 - She keeps one to herself (*private key will sign*)
 - Gives the other to anyone who wants it (*public*)
 - Public key:
 - *ID card*
 - *PKI: Validates x.509 name*





Filter: x509af.subjectPublicKey Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
2251	0.268880	173.194.43.54	192.168.1.14	TLSv1	558	Certificate, Server Ke...

- [-] Certificate (id-at-commonName=mail.google.com,id-at-organizationName=...)
 - [-] signedCertificate
 - version: v3 (2)
 - serialNumber : 0x2b9f7ee5ca25a62514204782753a9bb9
 - [-] signature (shaWithRSAEncryption)
 - [-] issuer: rdnSequence (0)
 - [-] validity
 - [-] subject: rdnSequence (0)
 - [-] rdnSequence: 5 items (id-at-commonName=mail.google.com,id-at-orga
 - [-] subjectPublicKeyInfo
 - [-] algorithm (rsaEncryption)

0110	6c	65	2e	63	6f	6d	30	81	9f	30	0d	06	09	2a	86	48
0120	86	f7	0d	01	01	01	05	00	03	81	8d	00	30	81	89	02
0130	81	81	00	af	39	15	98	68	e4	92	fe	4f	4f	f1	bb	ff
0140	0d	2e	b0	fe	25	aa	bd	68	04	67	27	ea	6c	43	4c	a7
0150	6d	cb	c8	8f	7e	81	ee	87	26	25	10	12	54	33	9e	aa
0160	3d	9b	8f	8e	92	b3	4b	01	e3	f9	4a	29	c3	0f	fd	ac
0170	b7	d3	4c	97	29	3f	69	55	cf	70	83	04	af	2e	04	6e
0180	74	d6	0f	17	09	fe	9e	20	24	24	e3	c7	68	9c	ac	11
0190	bd	92	e4	b2	1b	09	f2	02	32	bb	55	1b	2d	16	5f	30
01a0	12	23	e2	4c	4a	8d	c2	da	3f	e1	b8	bf	f7	3a	b1	86
01b0	be	f0	e5	02	03	01	00	01	a3	81	e7	30	81	e4	30	0c

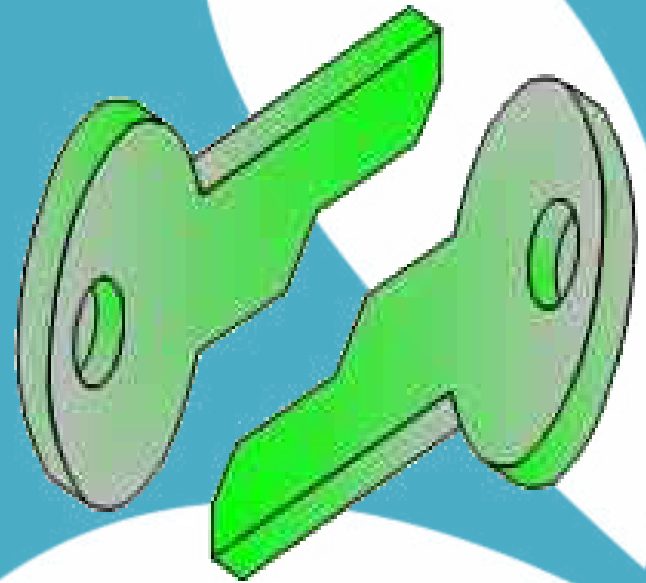
```

le.com0. .0...*.H
.....0...
...9..h ...00...
...%.h .g'.lCL.
m...~...&%..T3..
=.....K. ..J)....
..L.)?iU .p.....n
t.....$$..h...
.....2.U.-_0
#.LJ...?.....
.....0..0.

```

Asymmetric Encryption

- **Advantages over symmetric**
 - Key Distribution
 - Scalability ($2N$)
 - Provides Non-Repudiation
- **Disadvantages**
 - Much slower
 - Requires Trusted 3rd Party
 - PKI Hierarchy
 - OpenPGP Web of Trust





Filter: ssl.handshake.certificate Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
2251	0.268880	173.194.43.54	192.168.1.14	TLSv1	558	Certificate, Server Ke...

- [-] Certificate (id-at-commonName=mail.google.com, id-at-organizationName=)

- [-] signedCertificate

- version: v3 (2)

- serialNumber : 0x2b9f7ee5ca25a62514204782753a9bb9

- [-] signature (shaWithRSAEncryption)

- [-] issuer: rdnSequence (0)

- [-] validity

- [-] subject: rdnSequence (0)

- rdnSequence: 5 items (id-at-commonName=mail.google.com, id-at-orga

- [-] subjectPublicKeyInfo

- algorithm (rsaEncryption)

- Padding: 0

- subjectPublicKey: 30818902818100af39159868e492fe4f4ff1bbff0d2eb0f

- [-] extensions: 4 items

- [-] algorithmIdentifier (shaWithRSAEncryption)

```

0000  16 03 01 06 5a 0b 00 06 56 00 06 53 00 03 26 30  ....Z... V..S..&
0010  82 03 22 30 82 02 8b a0 03 02 01 02 02 10 2b 9f  .."0.... +.
0020  70 05 07 25 06 25 14 20 47 82 75 23 0b b0 30 0d  % %  C u : 0

```



Filter: x509if.id

Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
2251	0.268880	173.194.43.54	192.168.1.14	TLSv1	558	Certificate, Server Ke-

- [-] Certificate (id-at-commonName=mail.google.com,id-at-organizationName=C
 - [-] signedCertificate
 - version: v3 (2)
 - serialNumber : 0x2b9f7ee5ca25a62514204782753a9bb9
 - [-] signature (shaWithRSAEncryption)
 - [-] issuer: rdnSequence (0)
 - [-] validity
 - [-] subject: rdnSequence (0)
 - [-] rdnSequence: 5 items (id-at-commonName=mail.google.com,id-at-orga
 - [-] subjectPublicKeyInfo
 - [-] algorithm (rsaEncryption)
 - Padding: 0
 - subjectPublicKey: 30818902818100af39159868e492fe4f4ff1bbff0d2eb0f
 - [-] extensions: 4 items
 - [-] algorithmIdentifier (shaWithRSAEncryption)

```

0000  16 03 01 06 5a 0b 00 06 56 00 06 53 00 03 26 30  ....Z... V..S..&0
0010  82 03 22 30 82 02 8b a0 03 02 01 02 02 10 2b 9f  .."0.... +.
0020  70 05 03 25 26 25 14 20 47 82 75 3a 0b b0 30 0d  ..e e r .. n

```

Frame (558 bytes)

Reassembled TCP (1848 bytes)



Filter: ssl.handshake.ciphersuite

Expression... Clear Apply

No.	Time	Source	Destination	Protoc	Length	Info
2127	0.005072	173.194.43.30	192.168.1.14	TLSv1	1484	Server H

Handshake Protocol: Server Hello

Handshake Type: Server Hello (2)

Length: 77

Version: TLS 1.0 (0x0301)

Random

Session ID Length: 32

Session ID: adf7fc0895c40eacdc257aa8f5093536cd2556b95ed611

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

Compression Method: null (0)

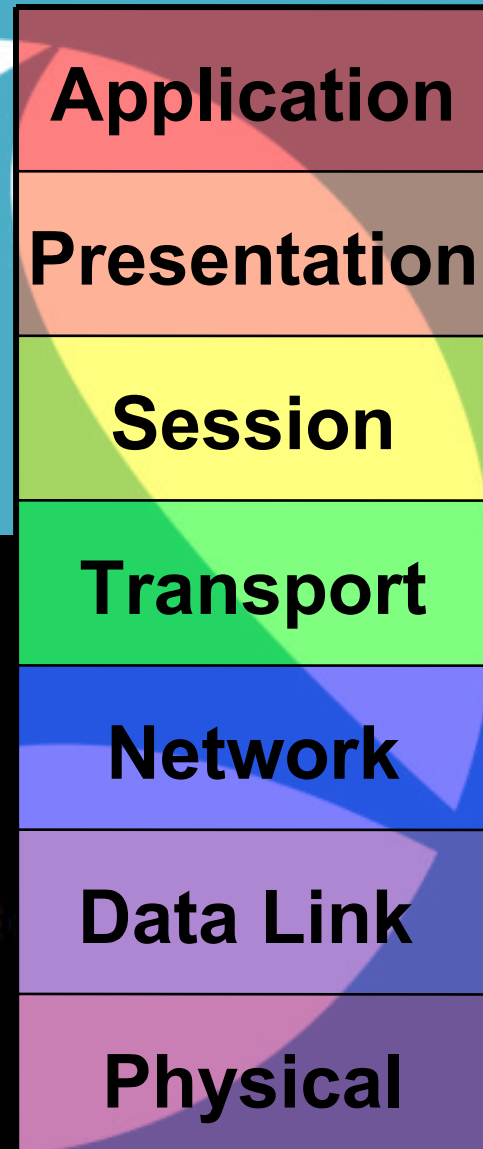
Extensions Length: 5

Extension: renegotiation_info

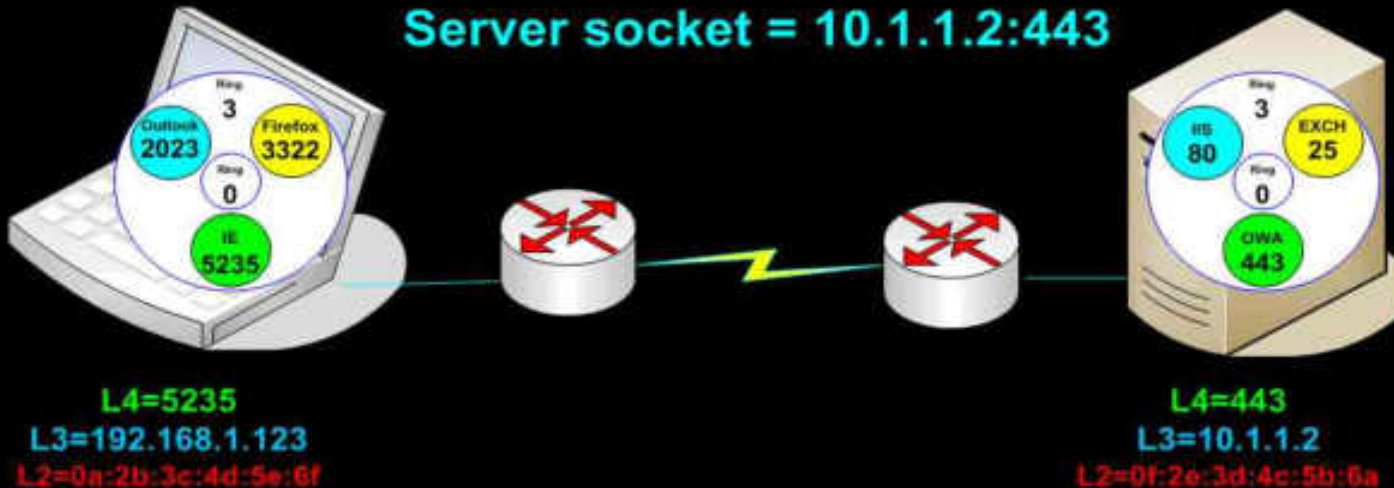
0080	49	c6	c0 13	00	00	05	ff	01	00	01	00	16	03	01	06	I. ...	
0090	e4	0b	00	06	e0	00	06	dd	00	04	23	30	82	04	1f	30
00a0	82	03	88	a0	03	02	01	02	02	0a	2c	09	98	87	00	00
00b0	00	00	58	1c	30	0d	06	09	2a	86	48	86	f7	0d	01	01	x 0

Where & What to Encrypt?

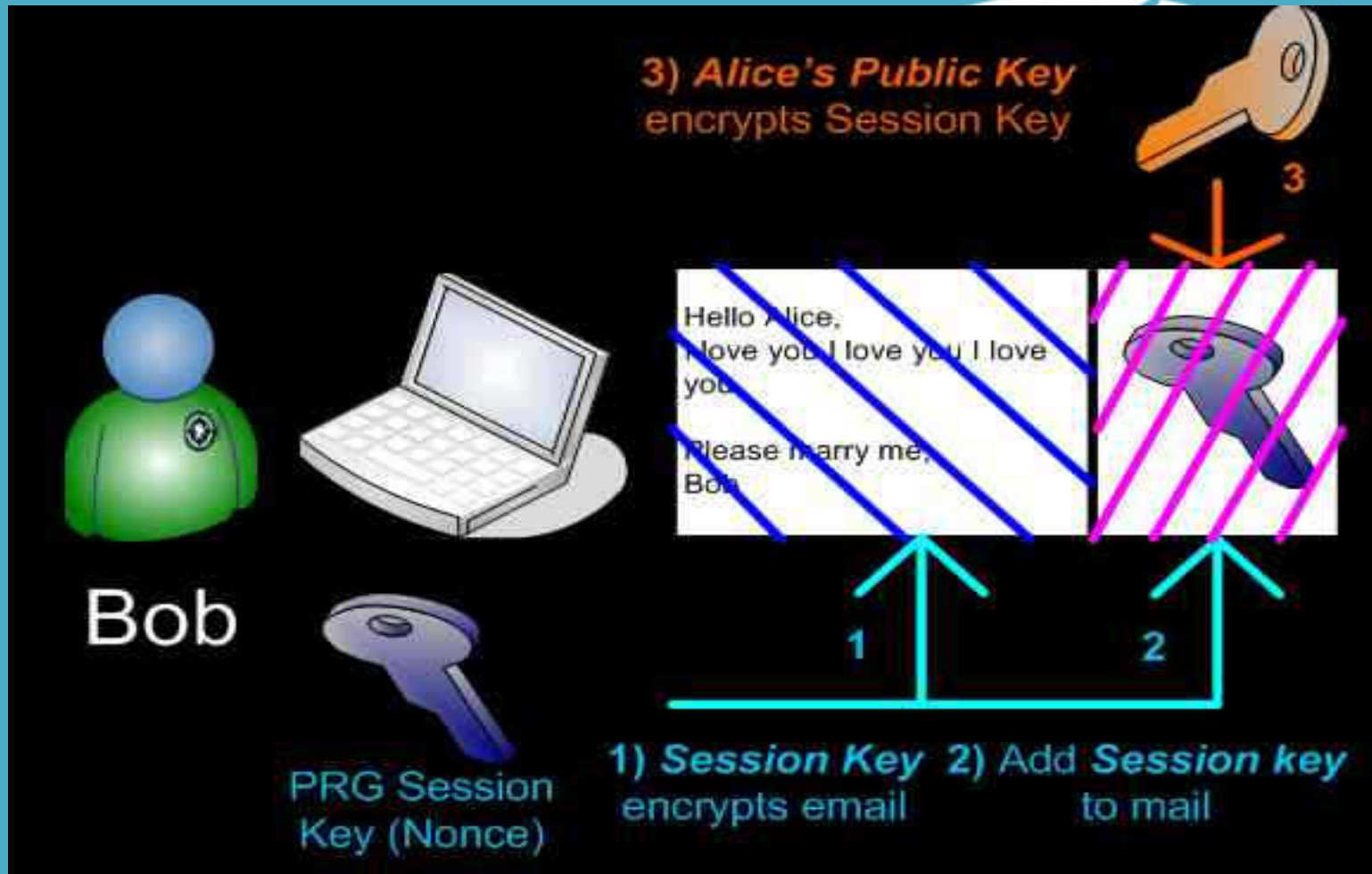
- **Application** (S/MIME, OpenPGP, SSH)
- **Presentation** (TrueCrypt, PKZip)
- **Transport** (SSL/TLS)
- **Network** (IPSec)
- **Link layer** (watch out! router support)



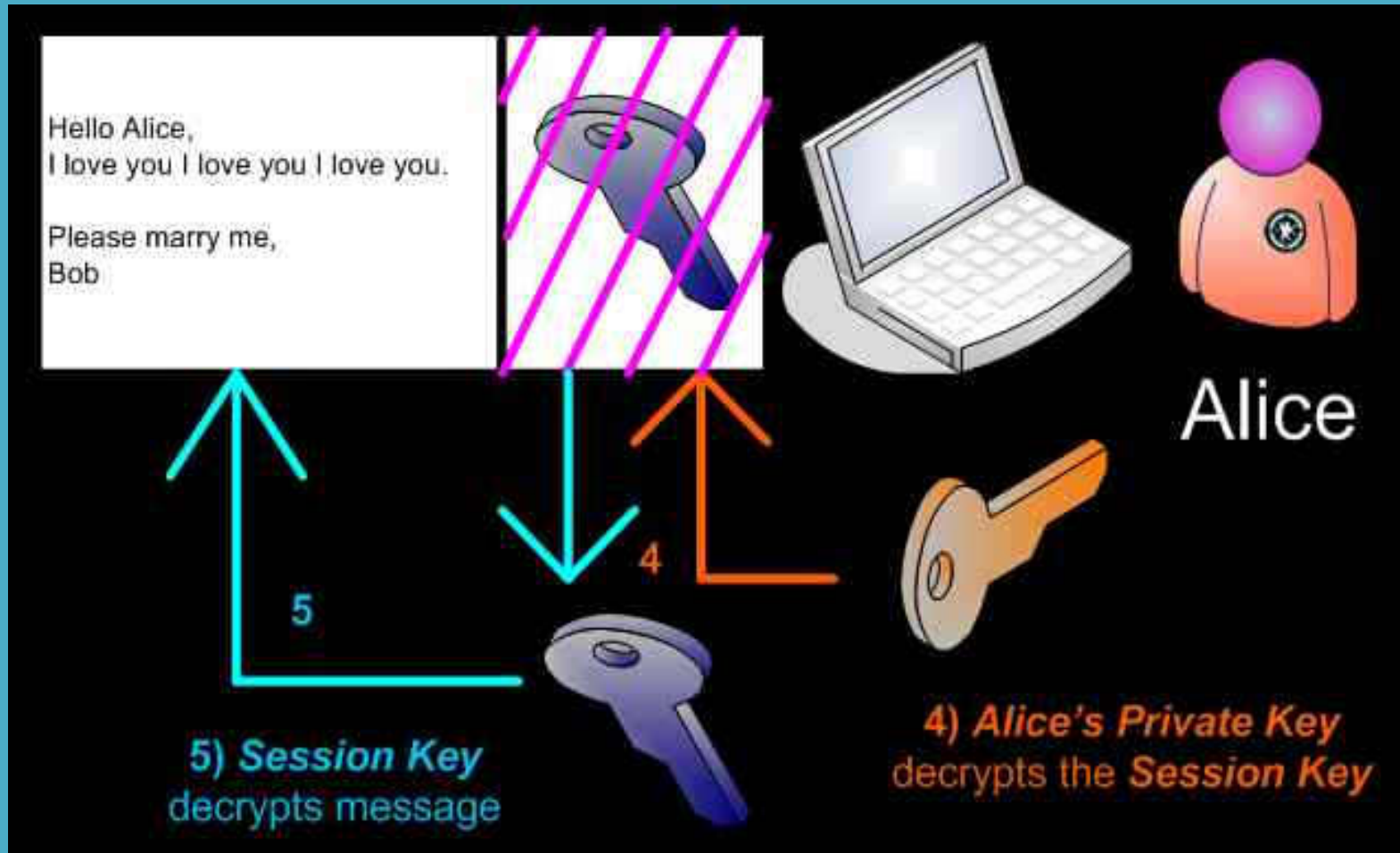
Client socket = 192.168.1.123:5235
Server socket = 10.1.1.2:443



Encrypting eMail



Decrypting eMail



Part 3

Hashing Algorithms

Understand Integrity checks with:

- a) Message Digests
- b) Message Authentication Codes
- c) Digital Signatures

Variable
size
input



Authenticating the Hash



- **Message Digest**
 - Not-Authenticated
- **Message Authentication Code (MAC)**
 - Authenticated Symmetrically
 - Authentication only (*message can be repudiated*)
- **Digital Signatures**
 - Authenticated Asymmetrically
 - Authentication
 - Non-Repudiation

Message Authentication Codes

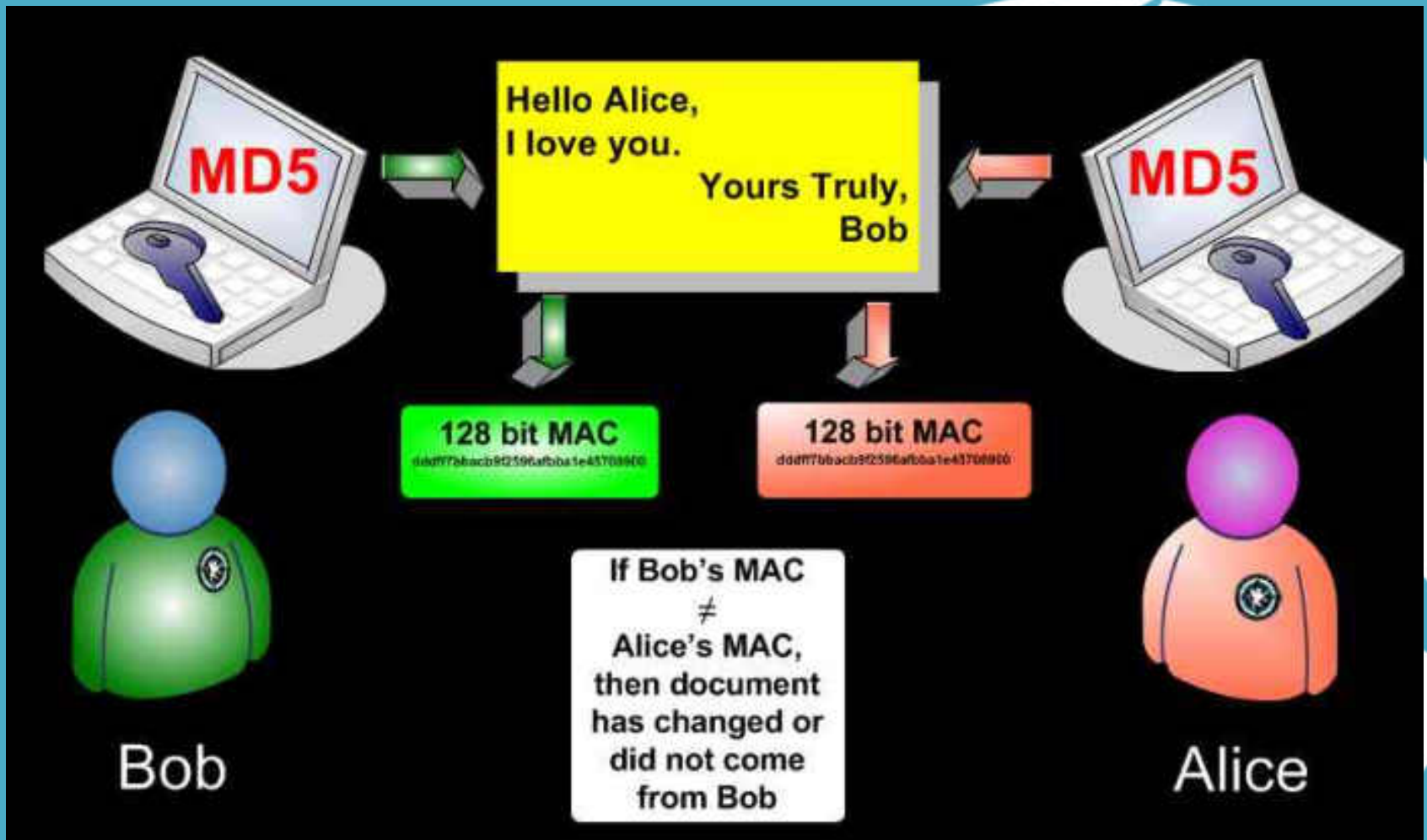
- Message digest is salted with symmetric key
 - Hash provides integrity
 - Symmetric key provides authenticity



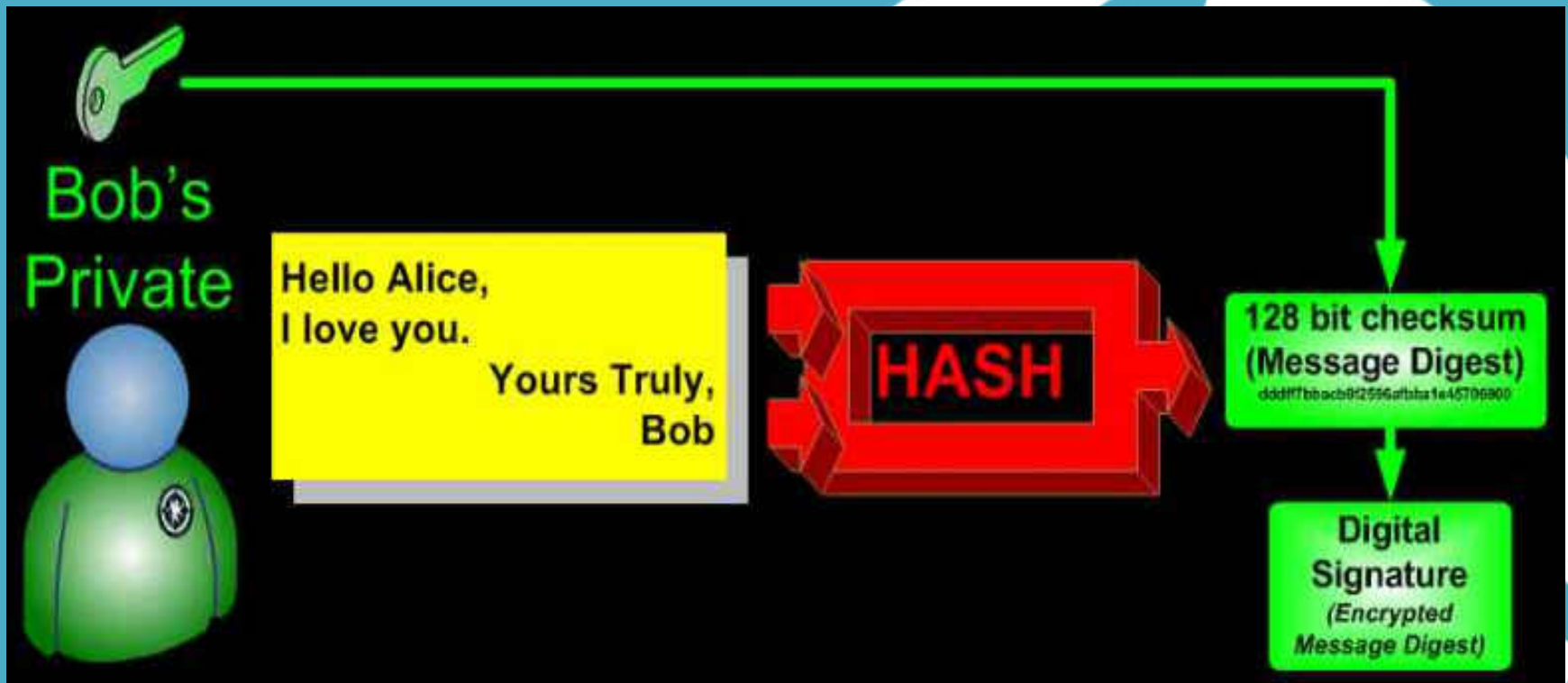
Important! - Does not provide non-repudiation

- Bob Claims "Alice sent the message"

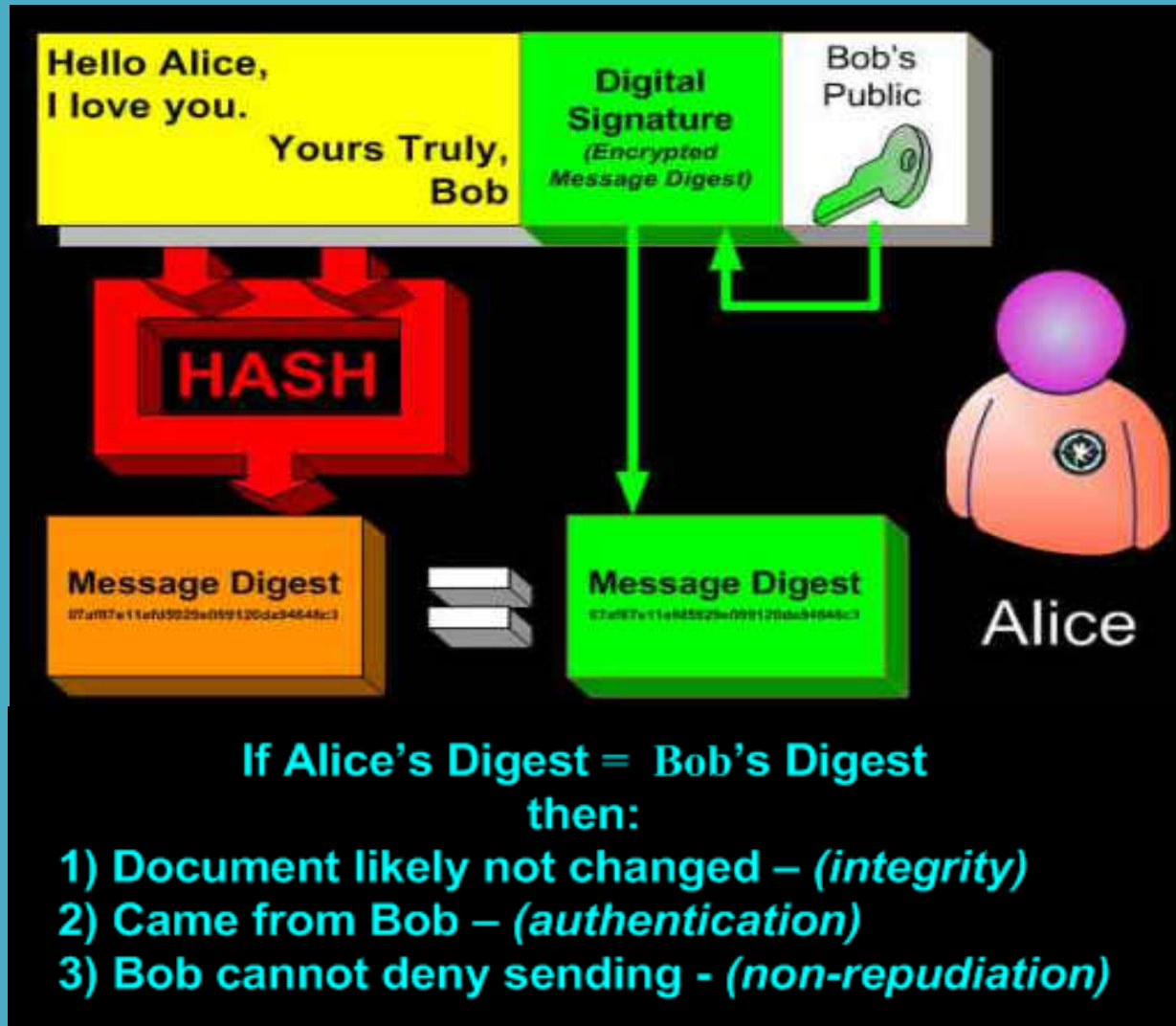
Message Authentication Codes



Signing a message



Validating the Signature





Filter: ssl.handshake.certificate

Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
2251	0.268880	173.194.43.54	192.168.1.14	TLSv1	558	Certifica

- [-] signedCertificate

- version: v3 (2)

- serialNumber : 0x2b9f7ee5ca25a62514204782753a9bb9

- [-] signature (shaWithRSAEncryption)

- [-] issuer: rdnSequence (0)

- [-] rdnSequence: 3 items (id-at-commonName=Thawte SGC CA

- [-] validity

- [-] subject: rdnSequence (0)

- [-] rdnSequence: 5 items (id-at-commonName=mail.google.co

- [-] subjectPublicKeyInfo

- [-] algorithm (rsaEncryption)

0020	7e	e5	ca	25	a6	25	14	20	47	82	75	3a	9b	b9	30	0d	~..%..%
0030	06	09	2a	86	48	86	f7	0d	01	01	05	05	00	30	4c	31	..*.H...
0040	0b	30	09	06	03	55	04	06	13	02	5a	41	31	25	30	23	.0...U..
0050	06	03	55	04	0a	13	1c	54	68	61	77	74	65	20	43	6f	..U...T
0060	6e	73	75	6c	74	69	6e	67	20	28	50	74	79	29	20	4c	nsulting
0070	74	64	2e	31	16	30	14	06	03	55	04	03	13	0d	54	68	td.1.0..

Frame (558 bytes)

Reassembled TCP (1848 bytes)

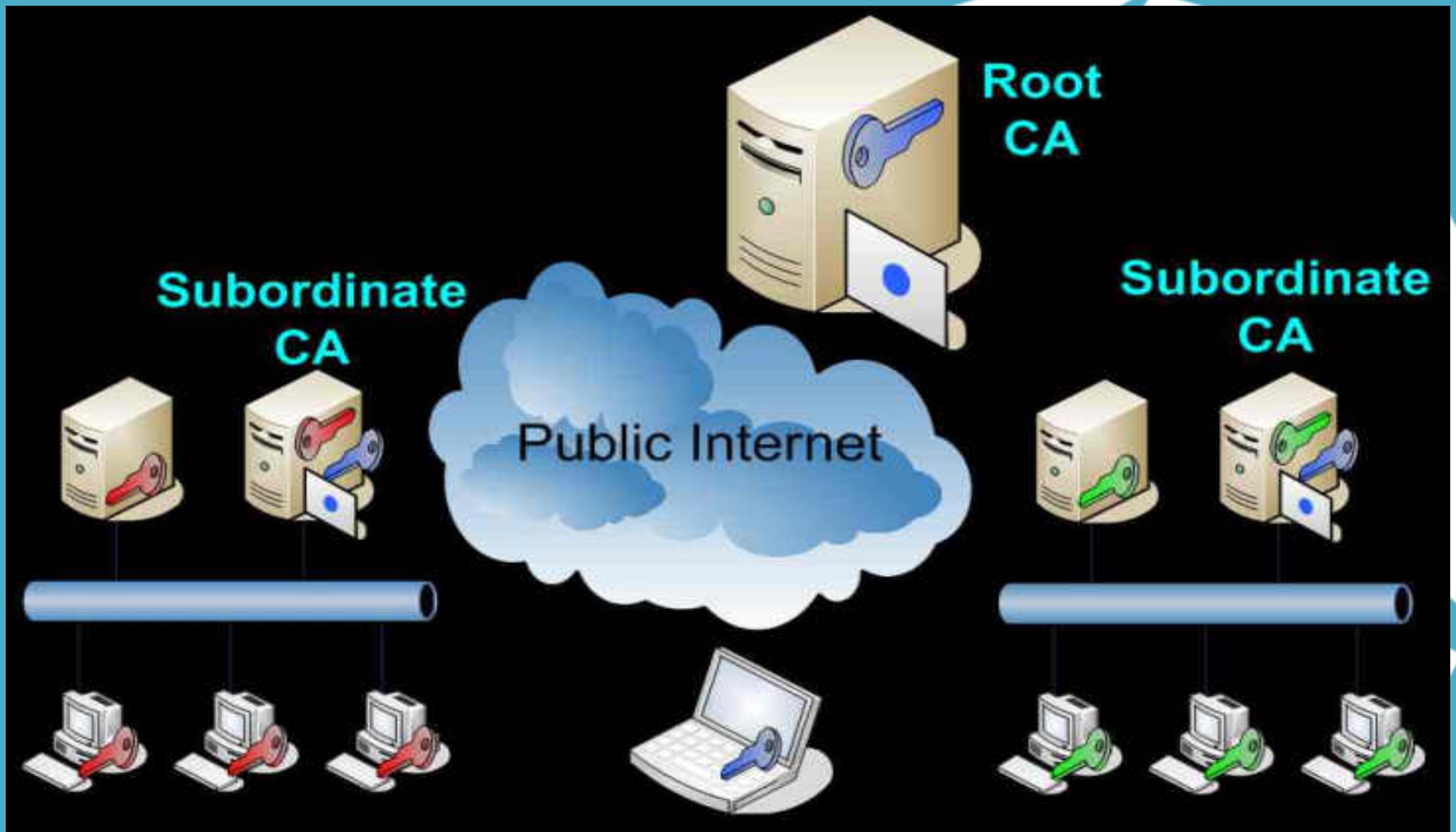
Who is a “Trusted 3rd party”

“Captain, the Federation's x.500 based hierarchical trust model of **PKI** is very logical. Perhaps we can trust the public **Certificate Authorities**”



“But Spock, I have never met **Thawte** or **Verisign**. I feel I can trust my friends. Call it a hunch, I trust OpenPGP more”

PKI Hierarchical Trust Model





Filter: x509af.issuer

Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
2251	0.268880	173.194.43.54	192.168.1.14	TLSv1	558	Certifica

- [-] Certificate (id-at-commonName=mail.google.com, id-at-organ
 - [-] signedCertificate
 - version: v3 (2)
 - serialNumber : 0x2b9f7ee5ca25a62514204782753a9bb9
 - [-] signature (shaWithRSAEncryption)
 - [-] issuer: rdnSequence (0)
 - [-] rdnSequence: 3 items (id-at-commonName=Thawte SGC CA
 - [-] validity
 - [-] subject: rdnSequence (0)
 - [-] rdnSequence: 5 items (id-at-commonName=mail.google.cc
 - [-] subjectPublicKeyInfo

0030	06	09	2a	86	48	86	f7	0d	01	01	05	05	00	30	4c	31	..*.H...
0040	0b	30	09	06	03	55	04	06	13	02	5a	41	31	25	30	23	.0...U..
0050	06	03	55	04	0a	13	1c	54	68	61	77	74	65	20	43	6f	..U...T
0060	6e	73	75	6c	74	69	6e	67	20	28	50	74	79	29	20	4c	nsulting
0070	74	64	2e	31	16	30	14	06	03	55	04	03	13	0d	54	68	td.1.0..
0080	61	77	74	65	20	53	47	43	20	43	41	30	1e	17	0d	31	awte SGC

Frame (558 bytes)

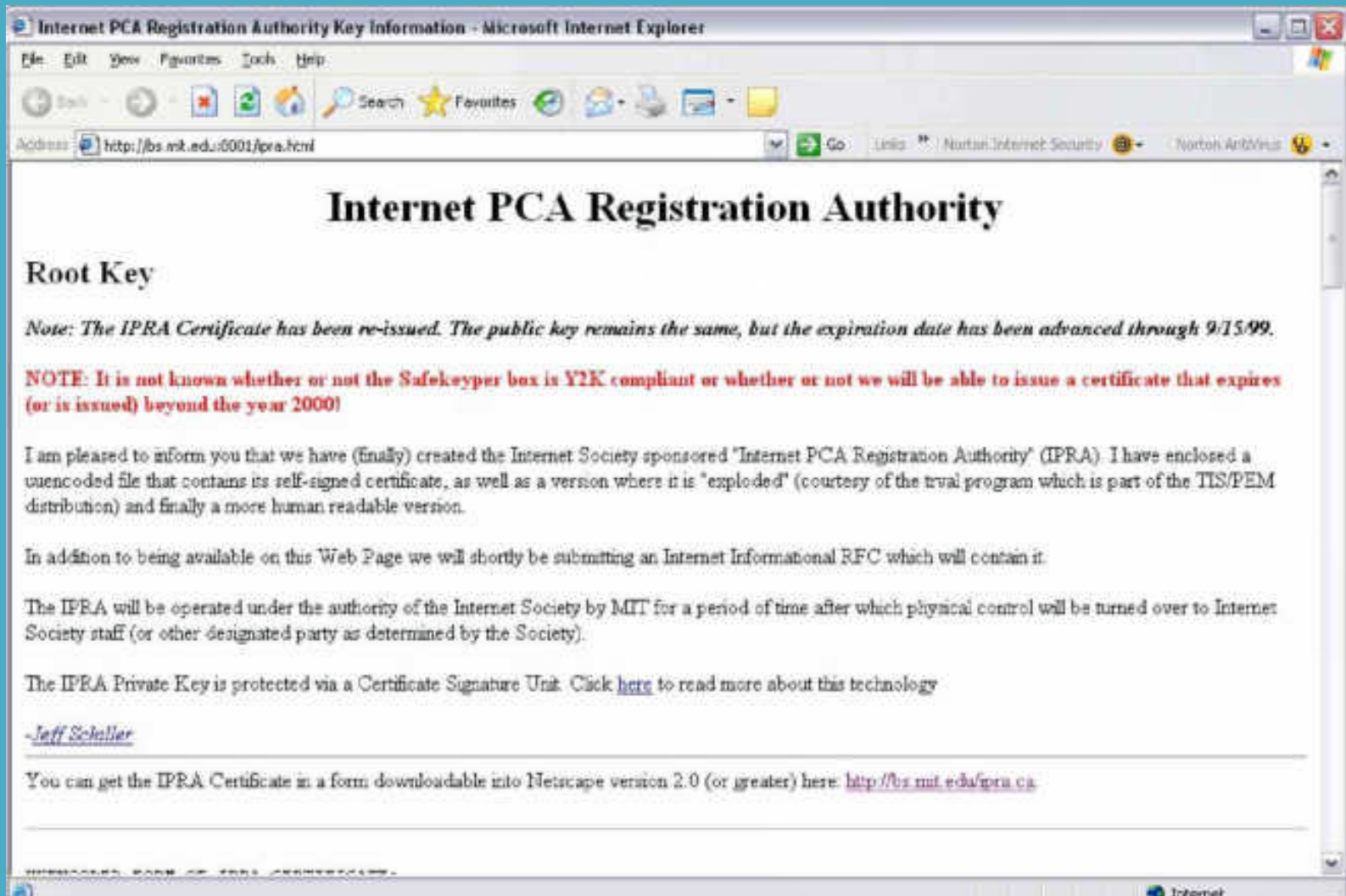
Reassembled TCP (1848 bytes)

Why Trust a CA?

RFC-3280 (updated in 4630)

- **Top tier**
 - Internet Policy Registration Authority (IPRA)
 - *Internet PCA Registration Authority (MIT), ?*
- **Second tier**
 - Policy Certification Authorities (PCAs)
 - *UNINETT, DFN-PCA, SURFnetPCA*
- **Third tier**
 - Certification Authorities (CAs)
 - *VeriSign, Deutsche Telekom, Thawte, etc.*

Internet PCA Registration Authority



Internet PCA Registration Authority



Certificate Revocation

Compromised Private Keys

- Certificate Revocation Lists (CRL)
- Online Certificate Status Protocol (OCSP)
- Problems:
 - Client checking may be disabled
 - Browsers configured to fail soft
 - Upstream servers may block CRL
 - Compromised CA certificates
 - Algorithms cracked
 - More...

Fraudulent

Fraudulent

Fraudulent,

Fraudulent,



Filter: x509ce.GeneralName == 6 Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
2251	0.268880	173.194.43.54	192.168.1.14	TLSv1	558	Certificate, Server Key Exchang

- [-] extensions: 4 items
 - [-] Extension (id-ce-basicConstraints)
 - Extension Id: 2.5.29.19 (id-ce-basicConstraints)
 - critical: True
 - BasicConstraintsSyntax
 - [-] Extension (id-ce-cRLDistributionPoints)
 - Extension Id: 2.5.29.31 (id-ce-cRLDistributionPoints)
 - [-] CRLDistPointsSyntax: 1 item
 - [-] DistributionPoint
 - [-] distributionPoint: fullName (0)
 - [-] fullName: 1 item
 - [-] GeneralName: uniformResourceIdentifier (6)
 - [uniformResourceIdentifier: http://cr1.thawte.com/ThawteSGCCA.cr1](http://cr1.thawte.com/ThawteSGCCA.cr1)
 - [-] Extension (id-ce-extKeyUsage)
 - Extension Id: 2.5.29.37 (id-ce-extKeyUsage)

```

01c0 06 03 55 1d 13 01 01 ff 04 02 30 00 30 36 06 03  ..U..... ..0.06..
01d0 55 1d 1f 04 2f 30 2d 30 2b a0 29 a0 27 86 25 68  U.../0-0 +.)'.%h
01e0 24 24 20 35 2f 2f 63 72 6c 2e 74 68 61 77 74 65  ttp://cr1.thawte

```

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

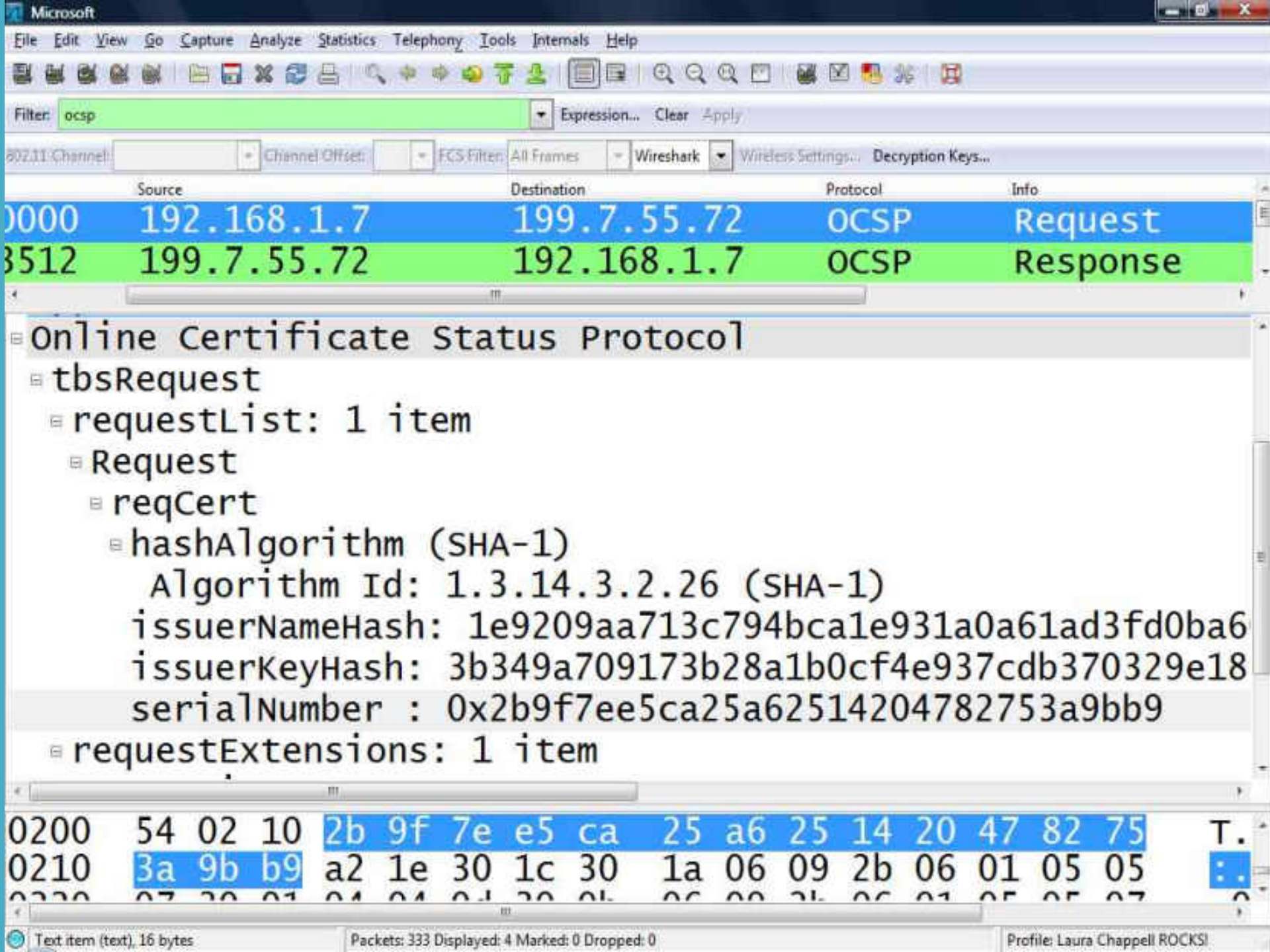
Filter: `pkixImplicit.accessLocation == 6` Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
2251	0.000283	173.194.43.54	192.168.1.14	TLSv1	558	Certificate, Server Key Exchange

- [-] Certificate (id-at-commonName=mail.google.com,id-at-organizationName=Google Inc,
 - [-] signedCertificate
 - version: v3 (2)
 - serialNumber : 0x2b9f7ee5ca25a62514204782753a9bb9
 - [-] signature (shawithRSAEncryption)
 - [-] issuer: rdnSequence (0)
 - [-] validity
 - [-] subject: rdnSequence (0)
 - [-] subjectPublicKeyInfo
 - [-] extensions: 4 items
 - [-] Extension (id-ce-basicConstraints)
 - [-] Extension (id-ce-cRLDistributionPoints)
 - [-] Extension (id-ce-extKeyUsage)
 - [-] Extension (id-pe-authorityInfoAccessSyntax)
 - Extension Id: 1.3.6.1.5.5.7.1.1 (id-pe-authorityInfoAccessSyntax)
 - [-] AuthorityInfoAccessSyntax: 2 items
 - [-] AccessDescription
 - accessMethod: 1.3.6.1.5.5.7.48.1 (id-pkix.48.1)
 - [-] accessLocation: 6
 - [uniformResourceIdentifier: http://ocsp.thawte.com](http://ocsp.thawte.com)

0240	06 08 2b 06 01 05 05 07 30 01 86 16 68 74 74 70	...+..... 0...http
0250	3a 2f 2f 6f 63 73 70 2e 74 68 61 77 74 65 2e 63	://ocsp.thawte.c
0260	6f 6d 30 3e 06 08 2b 06 01 05 05 07 30 02 86 32	om0>..+.0..2
0270	68 74 74 70 3a 2f 2f 77 77 77 2e 74 68 61 77 74	http://w ww.thawt
0280	65 2e 63 6f 6d 2f 72 65 70 6f 73 69 74 6f 72 79	e.com/re pository

Frame (558 bytes) Reassembled TCP (1848 bytes)



Certificates

Intended purpose:

<All>

Trusted Root Certification Authorities

Trusted Publishers










Untrusted Publishers

Issued To:

Issued By

Expiratio...

Friendly Name

 global trustee	UTN-USERFirst-Hardw...	3/14/2014	Fraudulent
 login.live.com	UTN-USERFirst-Hardw...	3/14/2014	Fraudulent
 login.skype.com	UTN-USERFirst-Hardw...	3/14/2014	Fraudulent
 login.yahoo.com	UTN-USERFirst-Hardw...	3/14/2014	Fraudulent
 login.yahoo.com	UTN-USERFirst-Hardw...	3/14/2014	Fraudulent
 login.yahoo.com	UTN-USERFirst-Hardw...	3/14/2014	Fraudulent
 mail.google.com	UTN-USERFirst-Hardw...	3/14/2014	Fraudulent
 Microsoft Corporation	VeriSign Commercial S...	1/31/2002	Fraudulent, NOT...
 Microsoft Corporation	VeriSign Commercial S...	1/30/2002	Fraudulent, NOT...

Import...

Export...

Remove

Advanced

Certificate intended purposes

Server Authentication, Client Authentication

How Well Does Certificate Revocation Really Work?

Detecting Certificate Authority compromises and web browser collusion

Posted March 22nd, 2011 by ierror in [ssl/tls ca for certificates torbrowser](#)

Thanks to Ian Gallagher, Seth Schoen, Jesse Burns, Chris Palmer, and other anonymous birds for their invaluable feedback on this writeup.

The Tor Project has long understood that the [certification authority](#) (CA) model of trust on the internet is susceptible to various methods of compromise. Without strong anonymity, the ability to perform targeted attacks with the blessing of a CA key is serious. In the past, I've worked on [attacks relating to SSL/TLS trust models](#) and for quite some time, I've hunted for evidence of non-academic CA compromise in the wild.

I've also looked for special kinds of cooperation between CAs and browsers. Proof of collusion will give us facts. It will also give us a real understanding of the faith placed in the strength of the underlying systems.

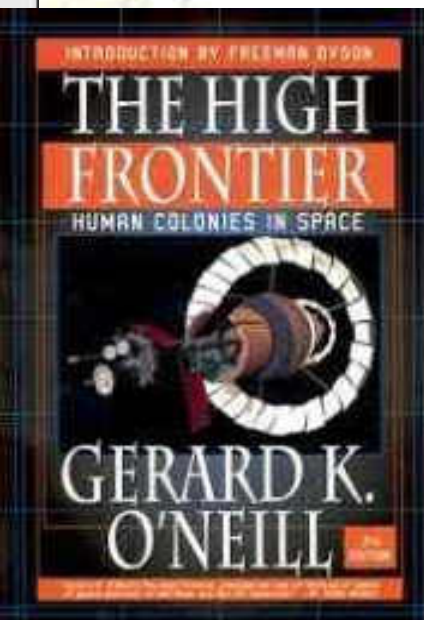
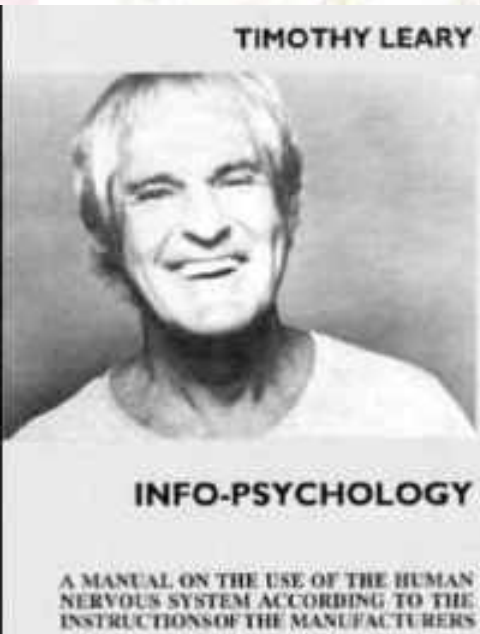
Does certificate revocation really work? [No, it does not](#). How much faith does a vendor actually put into revocation, when verifiable evidence of malice is detected or known? Not much, and that's the subject of this writing.

Last week, a smoking gun came into sight: A Certification Authority appeared to be compromised in some capacity, and the attacker issued themselves valid HTTPS

Where Are We Going?

Life on the Planet Earth, through the instrumentality of the human nervous system, has begun to migrate from the Womb Planet, to escape from gene pools, to establish colonies in high orbit, from whence it can more accessibly contact and communicate with Life in the Galaxy.

Men and women who know from whence they come and where they are going, who share a vision beyond the local-mundane will emerge from the larval gene-pools and as cyber (pilot) individuals, who learn quickly, work effectively, grow naturally, socialize lovingly and evolve gracefully. It is probably true that species coast along on serene stupidity until faced with an evolutionary challenge; at which point individuals leave the primitive collectives and become very smarter very faster. (Timothy Leary -1976)



Bruce Schneier Facts

Things you might not know about Bruce Schneier

[Contact](#)

[Random RSS Feed](#)

[Top 10 Facts](#)

[Suggest Fact](#)

Top 10 voted Bruce Schneier Facts

When Bruce Schneier observes a quantum particle, it remains in the same state until he has finished observing it.

17646 votes

Bruce Schneier knows Alice and Bob's shared secret.

6579 votes

Vs lbh nfxrq Oehpr Fpuarvre gb qrpelcg guvf, ur'q pehfu lbhe fxhyy jvgu uvf ynhtu.

2048 votes

Most people use passwords. Some people use passphrases. Bruce Schneier uses an epic passpoem, detailing the life and works of seven mythical Norse heroes.

1976 votes

Bruce Schneier's secure handshake is so strong, you won't be able to exchange keys with anyone else for days.

1925 votes

Bruce Schneier once decrypted a box of AlphaBits.

Thank You!

