E-mail forenzika

Petar Djerasimović
Predrag Pale

Q: Zašto koristimo e-mail?

Koje komunikacijske alate najčešće koristite?

A – Društvene mreže

B – WhatsApp, Viber , Skype …

C – SMS

D – E-mail

E – Sve

Zašto je e-mail važan?

- asinkrono
  - Svaki sudionik u komunikaciji komunicira kada želi
- nova komunikacijska kultura
  - kratko, često, brzo
  - vrlo slično verbalnoj komunikaciji
  - No ostavlja tragove, zapise o komunikaciji
- iznimno učinkovit za komunikacije jedan-na-više
  - dark side -> SPAM, HOAX, phishing, …
- mehanizam razmjene za bilokakav tip podataka
  - običan tekst, formatirani tekst,
  - audio, video,
  - binarni podatci, programi, …
- može se u potpunosti automatizirati
  - primanje i slanje
  - nemože se slati aplikacijama (npr. za pokretanje neke aktivnosti)
  - aplikacije mog uslati poruke
- stoga, računala mogu koristiti e-mail
  - za komunikaciju –> Internet of things ☺

Q: Zašto forenzika ima interes za e-mail poruke?

Koji dio e-mail poruke se lako može krivotvoriti?

A – Subject i pošiljatelj (From)

B – Pošiljatelj i datum

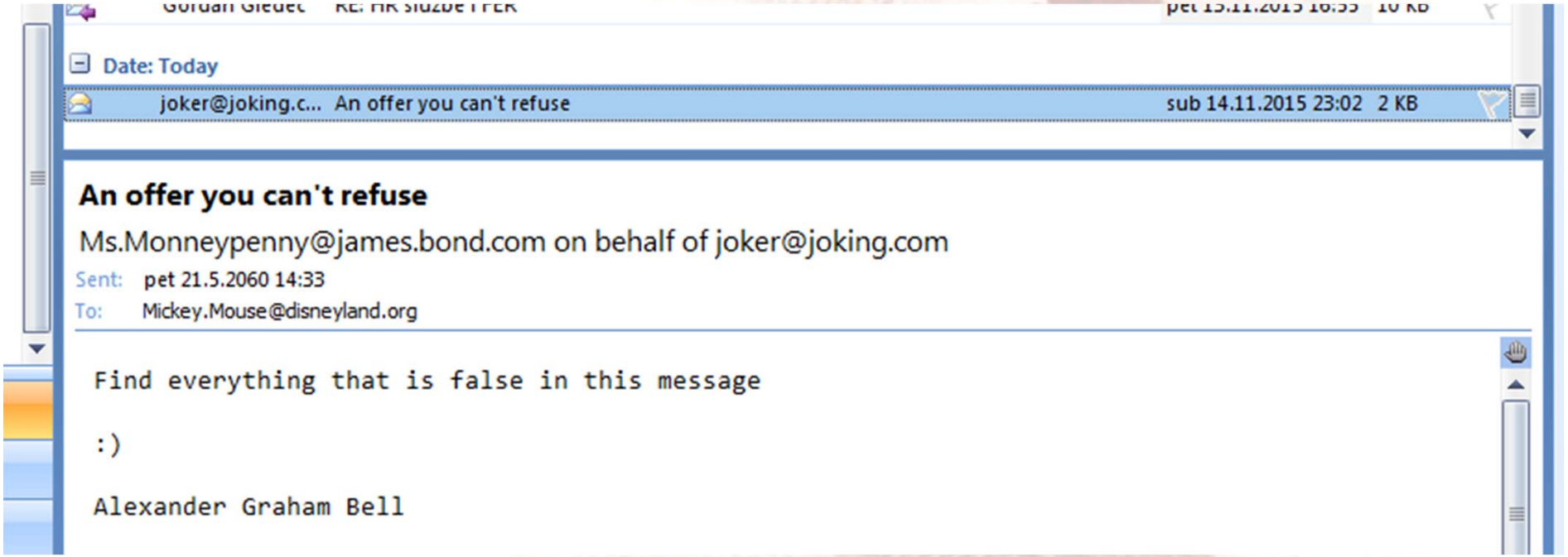
C – Samo pošiljatelj

D – Subject i tekst poruke (body)

E – Sve

Zašto forenzika ima interes za e-mail poruke?

- Jer se lako mogu krivotvoriti!!!
- Što se može krivotvoriti u e-mail poruci?



- Doslovno sve!!!

Sadržaj predavanja

- Kako mail **putuje**

- **Protokoli** koji se koriste

POP3
IMAP
MIME
SMTP

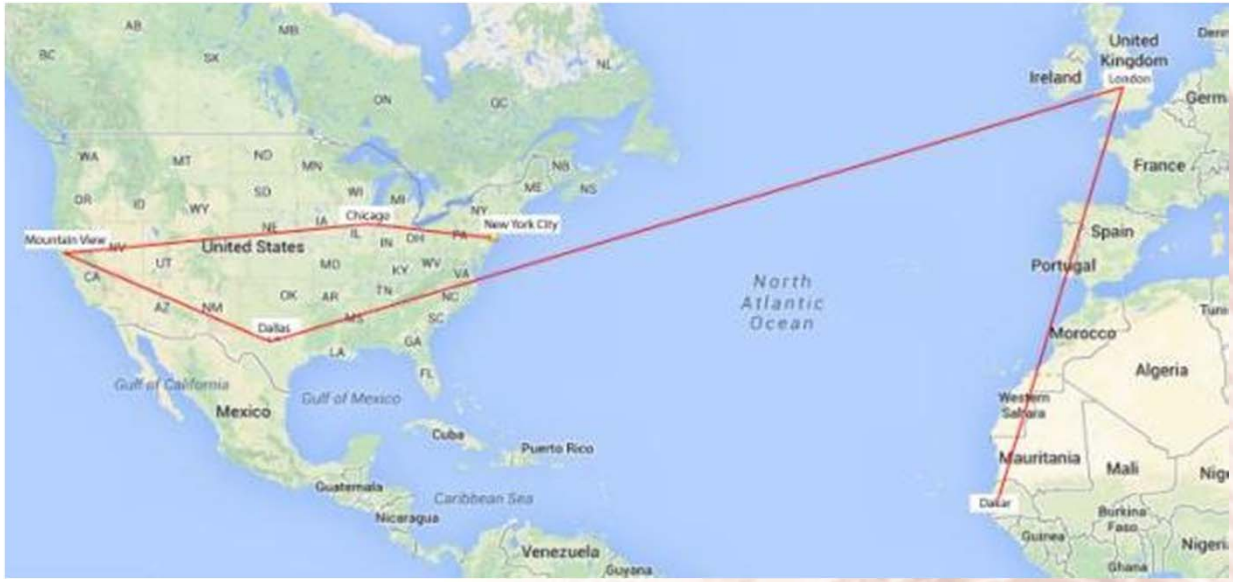
- **Zaglavlja** poruka

To:
From:
Date:
Received:
Subject:

- **Privitci**



- **Šifriranje**



Kako e-mail poruke putuju

E-mail sustav

1. korisnički agent (*eng. user agent*) (MUA)
   - **Komunicira** s korisnikom
   - **Komunicira** s **MTA**
     - Radi potrebe **slanja** e-mail poruka
     - **Pristupa primljenim porukama** pohranjenim na MTA
   - Popularni korisnički agenti:
     - mail, mailx, pine, elm, mutt
     - Outlook, Thunderbird, Eudora …
     - web agenti
       - Squirrel mail, RoundCube
       - Gmail, Yahoo, Hotmail


2. posrednik prijenosa poruka (*eng. message transfer agent*) (MTA)
   - mail transfer agent, mail relay
   - mail exchanger, mail server, MX host …
   - razmjenjuje poruke, s drugom MTA
   - popularni MTA sustavi:
     - postfix, exim, sendmail
     - MS Exchange
     - IBM Domino (Lotus Notes)


Q: Arhitektura za razmjenu e-mail poruka

Koliko MTA sustava ja potrebno za prijenos e-mail poruke?

A – najmanje 1

B – najmanje 2

C – najmanje 3

D – 2 ili više

E – niti jedan

Q: Arhitektura za razmjenu e-mail poruka - 2

Koliko MTA sustava je potrebno
za prijenos e-mail poruke, osim jednog kod pošiljatelja i jednog kod primatelja?

A – minimum 1

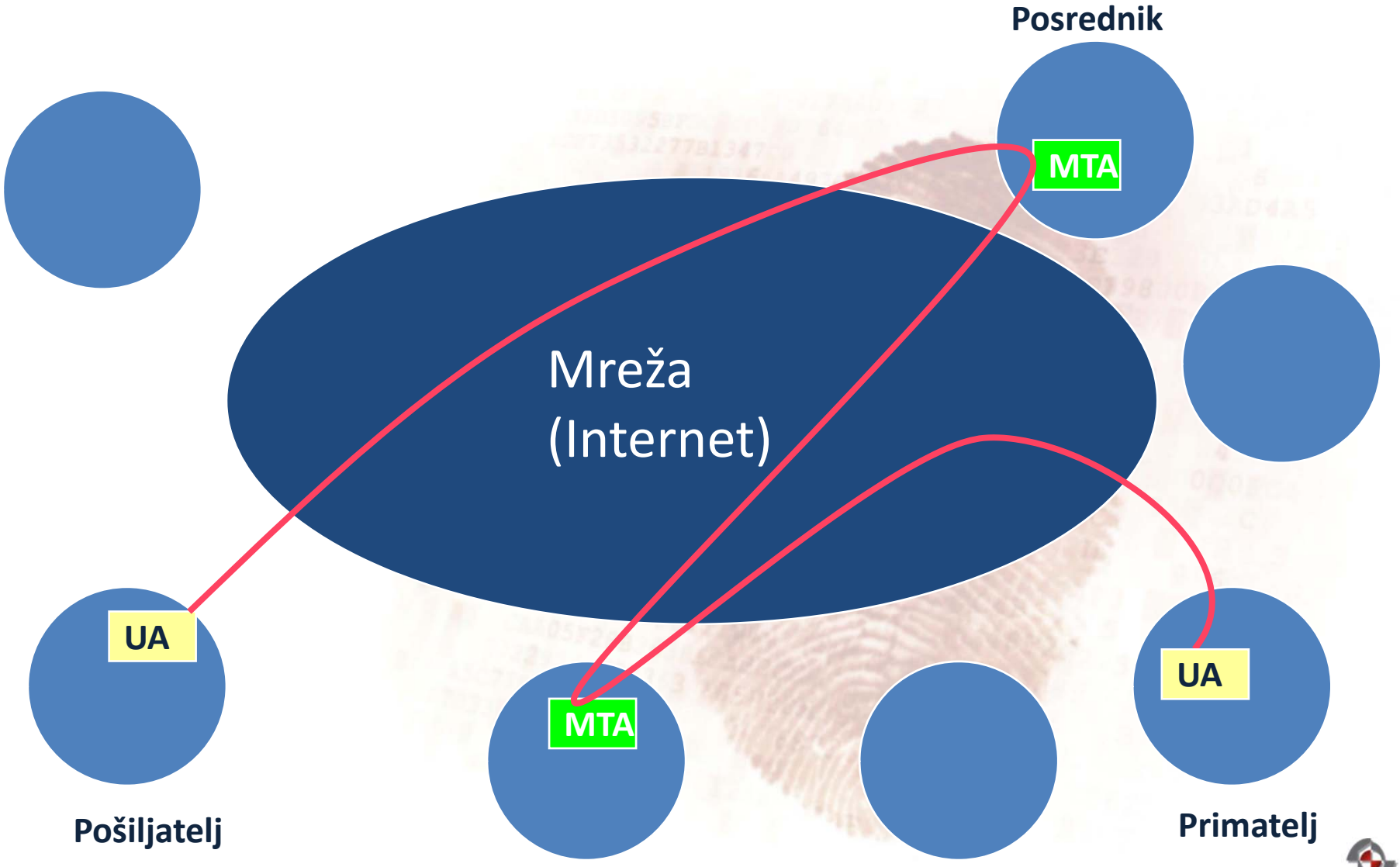
B – minimum 2

C – minimum 3

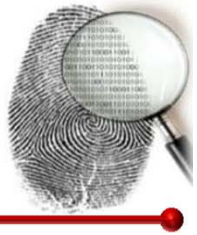
D – minimum 4

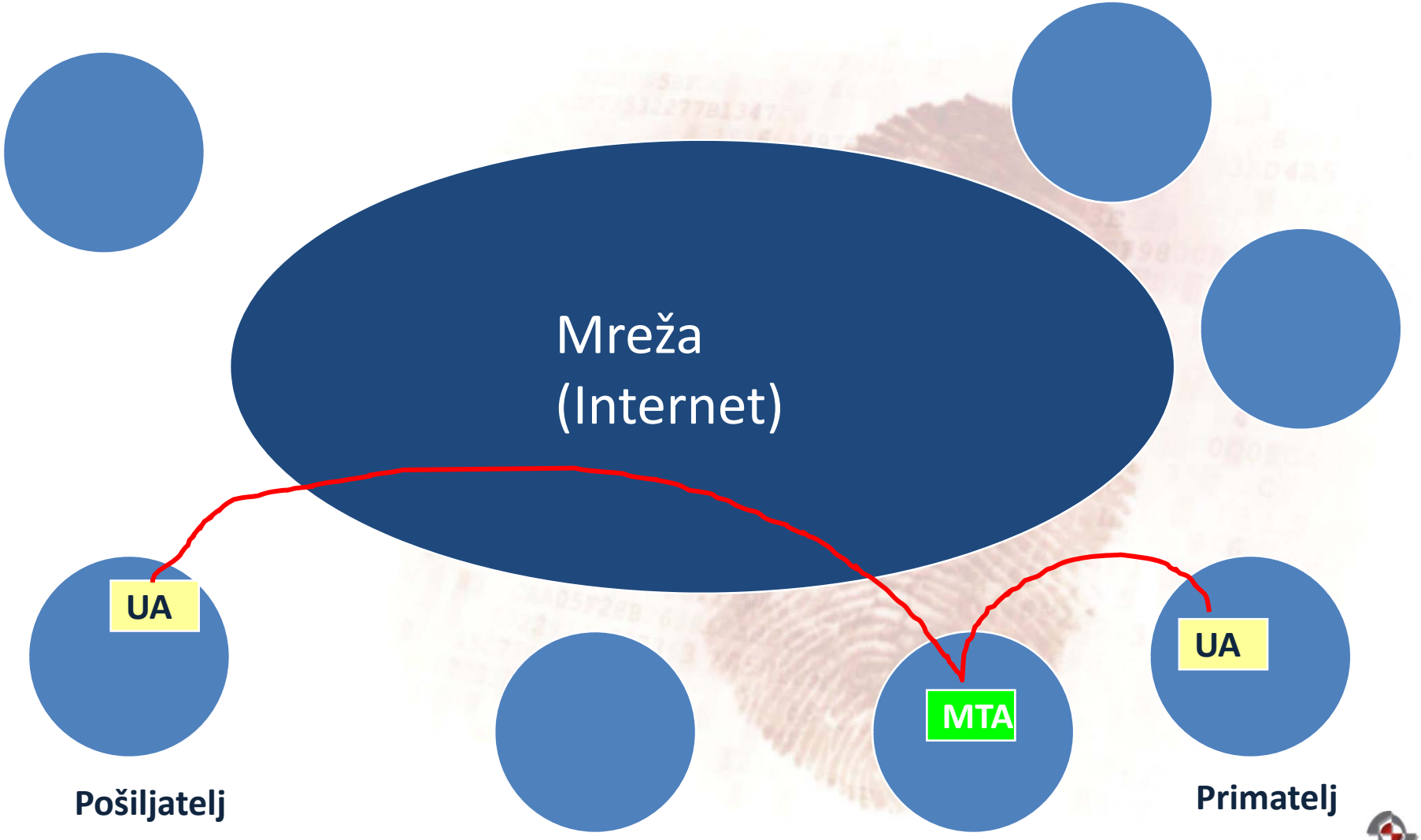
E – none

Neizravni prijenos - više MTA

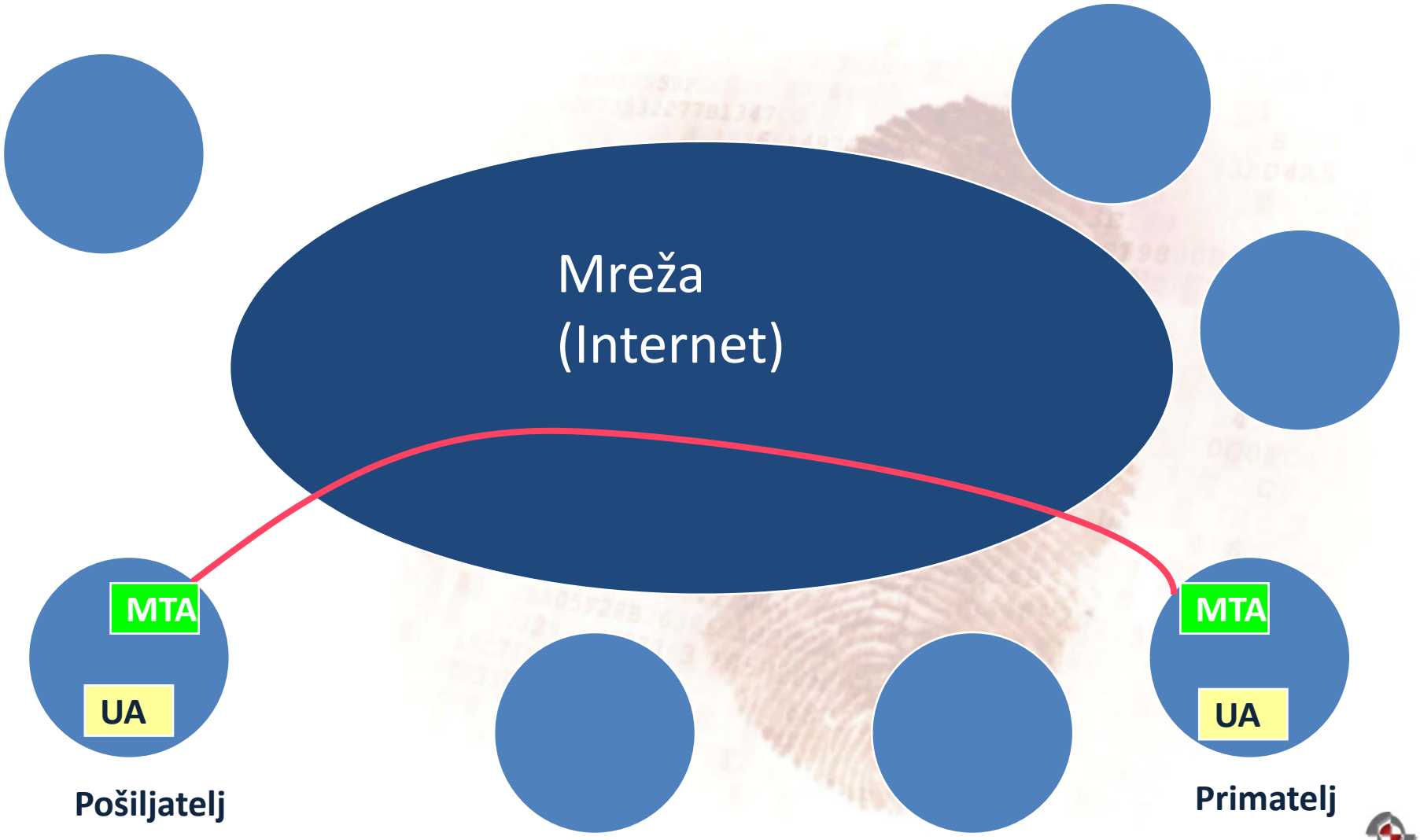


Neizravni prijenos – jedan MTA



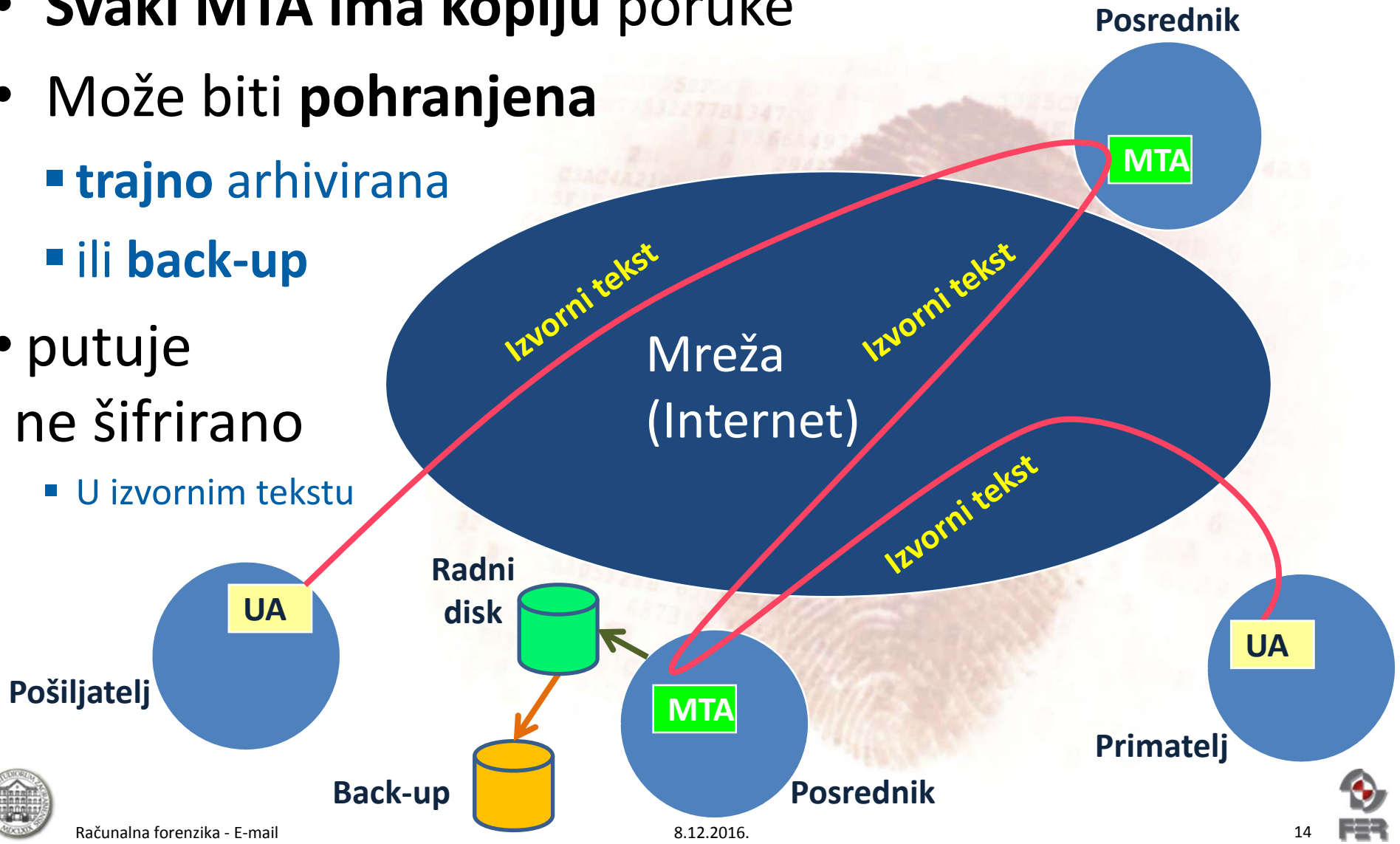


Peer—to—peer prijenos



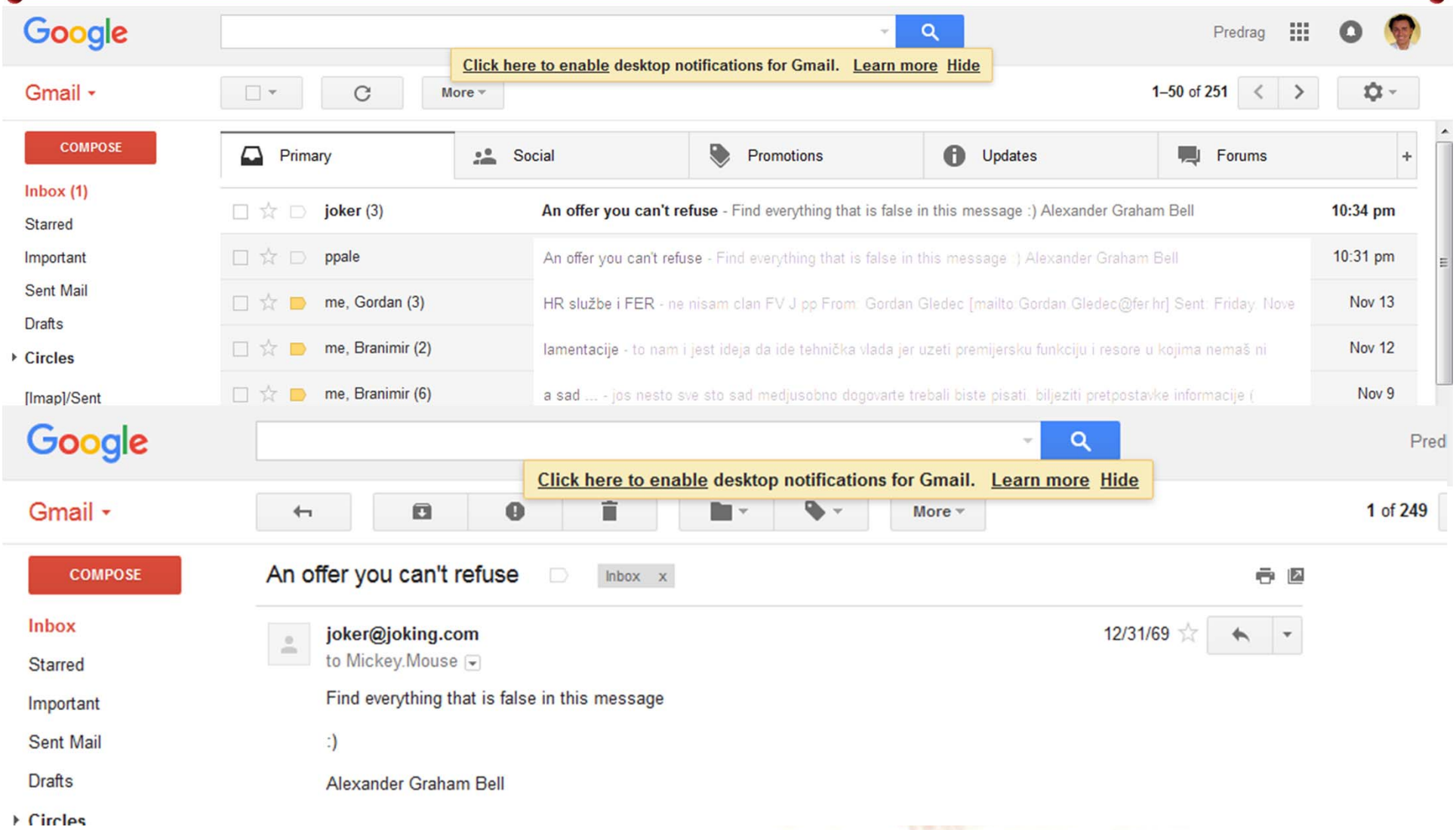
Sigurnost prijenosa poruka

- **Svaki MTA ima kopiju** poruke
- Može biti **pohranjena**
  - **trajno** arhivirana
  - ili **back-up**
- putuje ne šifrirano
  - U izvornim tekstu

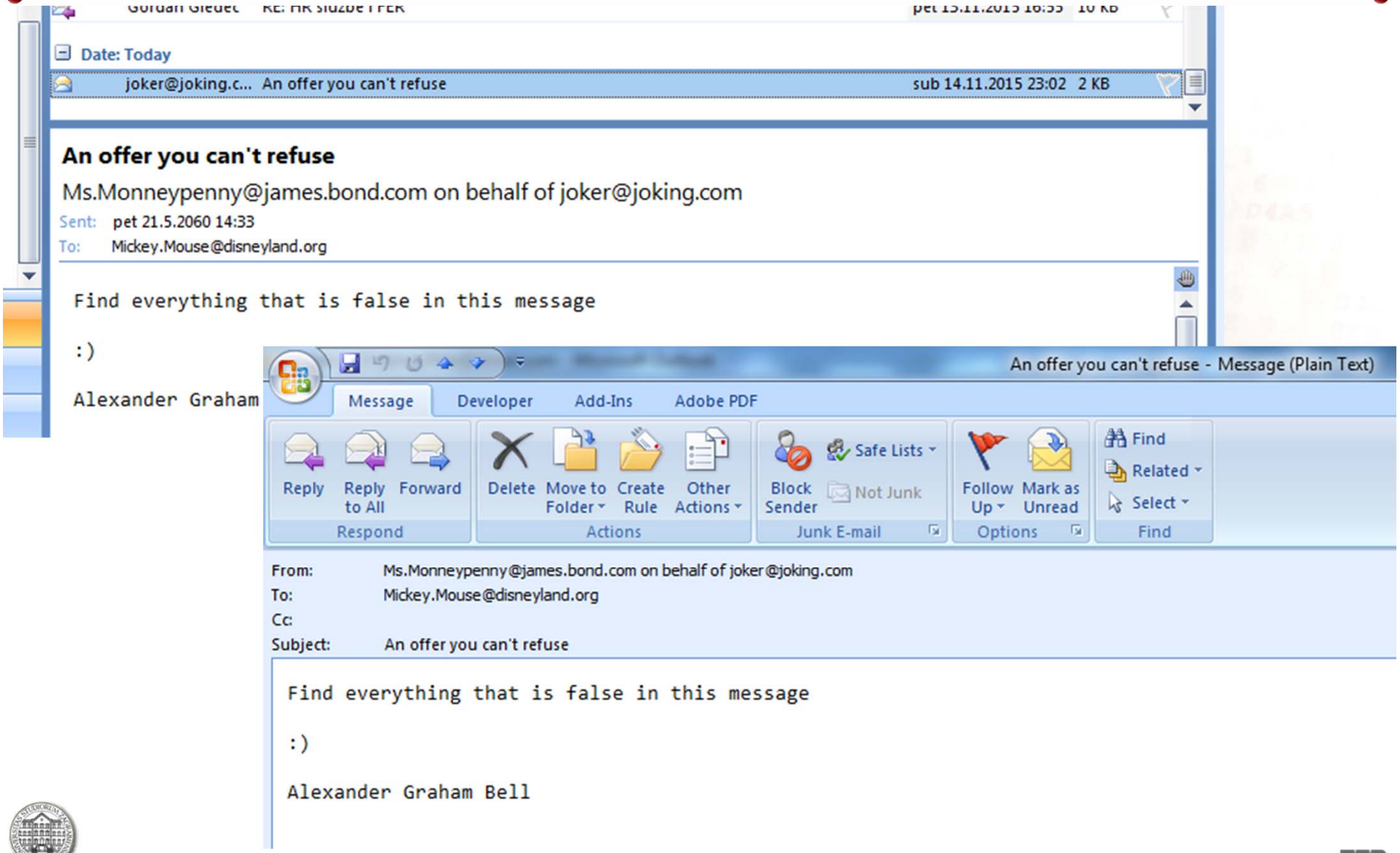


Autentičnost sadržaja e-mail poruka

Koliko je e-mail poruka autentična?



Pregled kroz drugi korisnički agent



Q: Autentičnost e-mail poruka

Koji dio e-mail poruke se lako može krivotvoriti?

A – Subject i pošiljatelj (From)

B – Pošiljatelj i datum

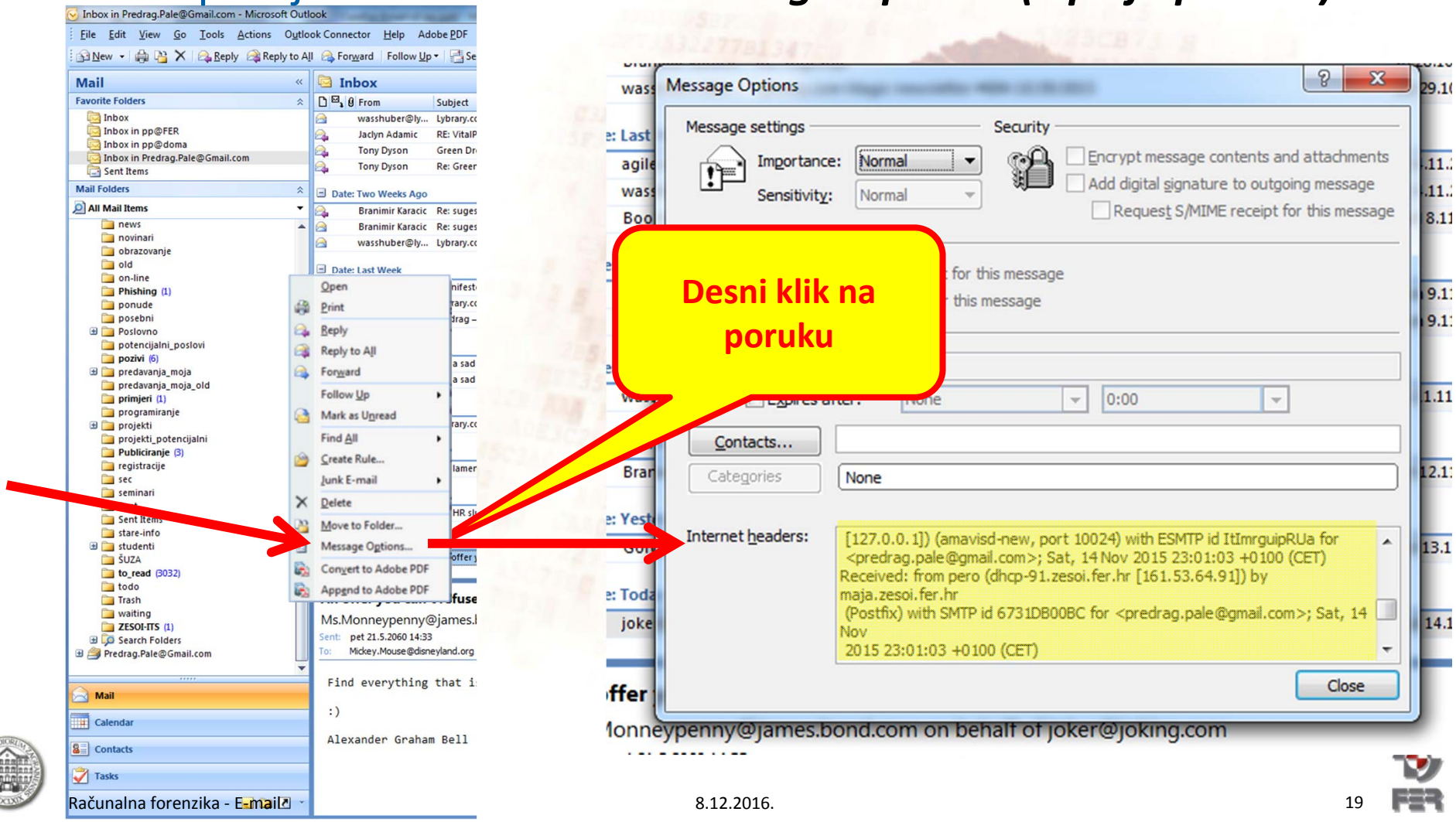
C – Samo pošiljatelj

D – Subject i tekst poruke (body)

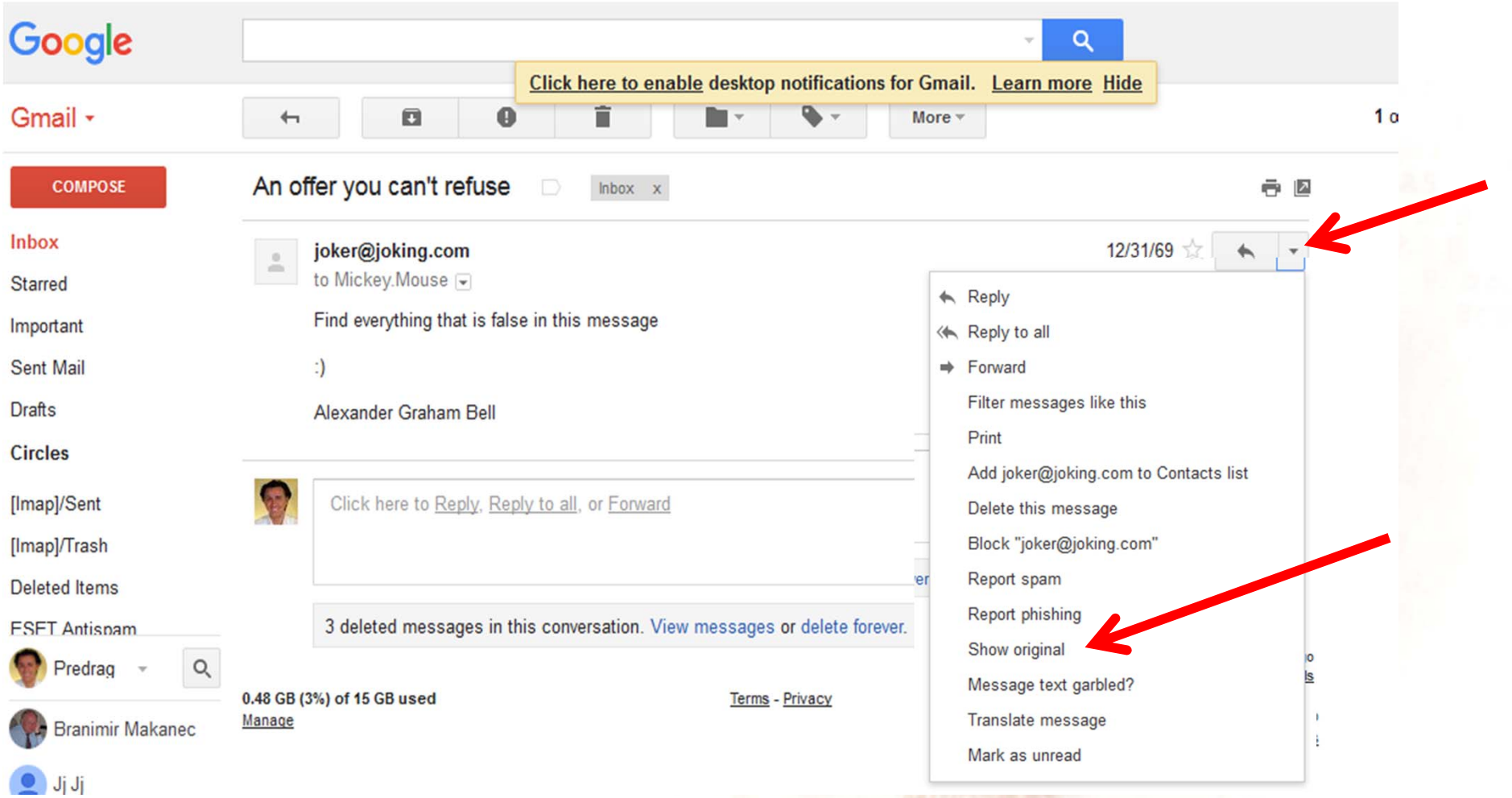
E – Sve

Za forenziku su potrebna zaglavlja poruka

- Može se dobiti kod svakog korisničkog agenta
  - Na primjer u MS Outlook: ***Message Options (Opcije poruka)***



Ili, primjer u Gmail

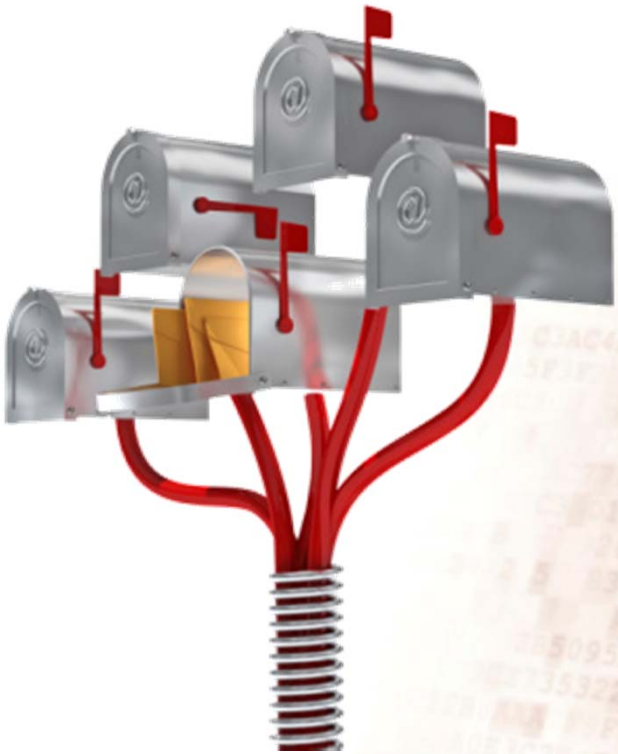


Analiza e-mail zaglavlja

```
Delivered-To: predrag.pale@gmail.com
Received: by 10.64.56.166 with SMTP id b6csp1745238ieq; Sat, 14 Nov 2015
 13:34:29 -0800 (PST)
Return-Path: <Albert.Zweistein@physics.world.org>
Received: from maja.zesoi.fer.hr (maja.zesoi.fer.hr. [2001:b68:16:70::64:3])
 by mx.google.com with ESMTP id 200si15266292wmk.102.2015.11.14.13.34.29 for
 <predrag.pale@gmail.com>; Sat, 14 Nov 2015 13:34:29 -0800 (PST)
Received-SPF: neutral (google.com: 2001:b68:16:70::64:3 is neither permitted
 nor denied by best guess record for domain of
 Albert.Zweistein@physics.world.org) client-ip=2001:b68:16:70::64:3;
Received: from localhost (localhost [127.0.0.1]) by maja.zesoi.fer.hr
 (Postfix) with ESMTP id 80195B00C8 for <predrag.pale@gmail.com>; Sat, 14 Nov
 2015 22:33:37 +0100 (CET)
Received: from maja.zesoi.fer.hr ([127.0.0.1]) by localhost (maja.zesoi.fer.hr
 [127.0.0.1]) (amavisd-new, port 10024) with ESMTP id YsNLov-uYHD7 for
 <predrag.pale@gmail.com>; Sat, 14 Nov 2015 22:33:35 +0100 (CET)
Received: from pero (dhcp-91.zesoi.fer.hr [161.53.64.91]) by maja.zesoi.fer.hr
 (Postfix) with SMTP id CC2F0B00BC for <predrag.pale@gmail.com>; Sat, 14 Nov
 2015 22:33:35 +0100 (CET)
To: Mickey.Mouse@disneyland.org
From: joker@joking.com
Subject: An offer you can't refuse
Sender: Ms.Monneypenny@james.bond.com
Date: Thu, 21 May 2060 05:33:29 -0700
Message-Id: <20151114213337.80195B00C8@maja.z
```

?!

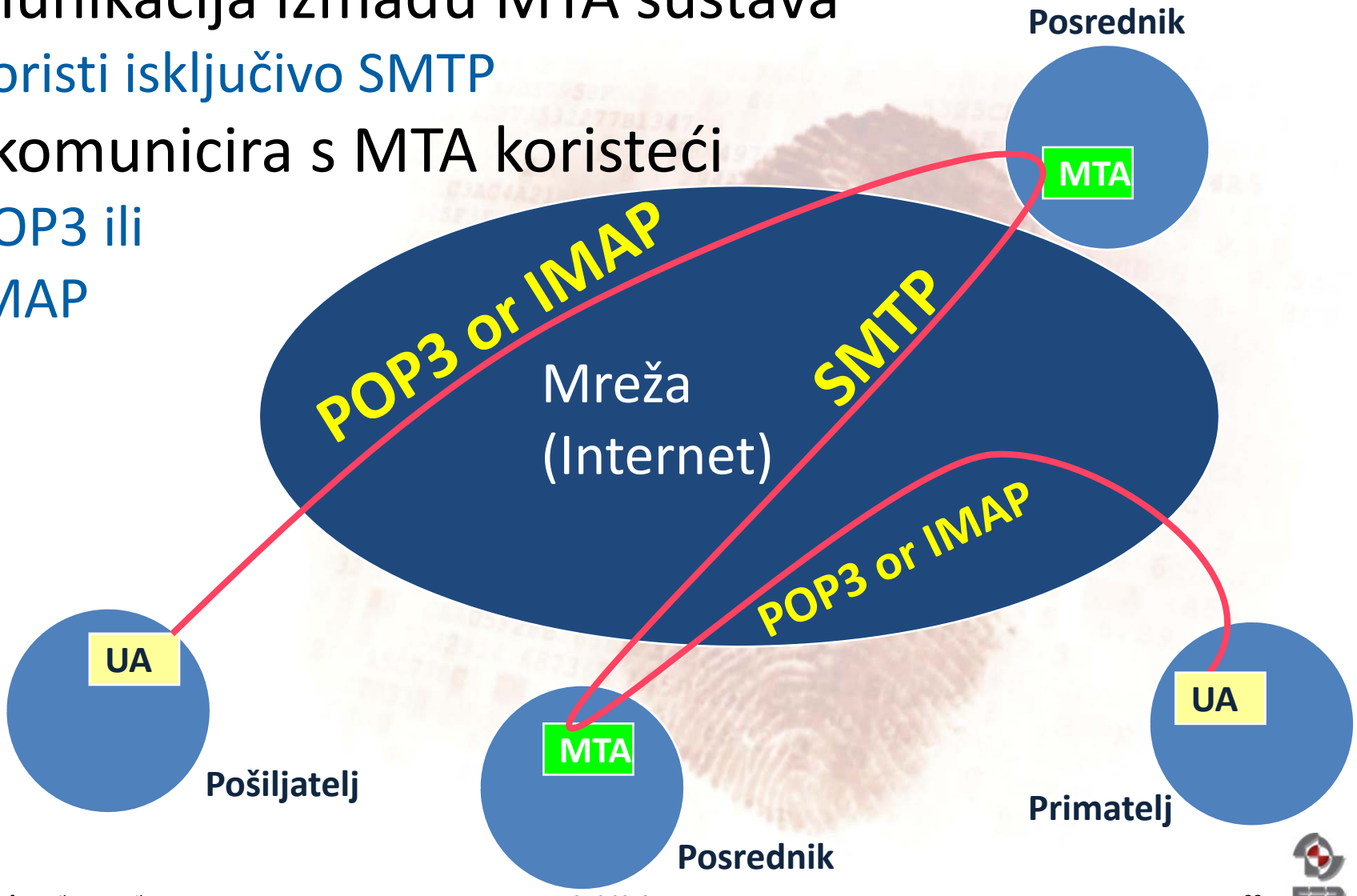
Tražiti prvi zapis (najniži na popisu) "Received:" liniju za **STVARNOG** pošiljatelja



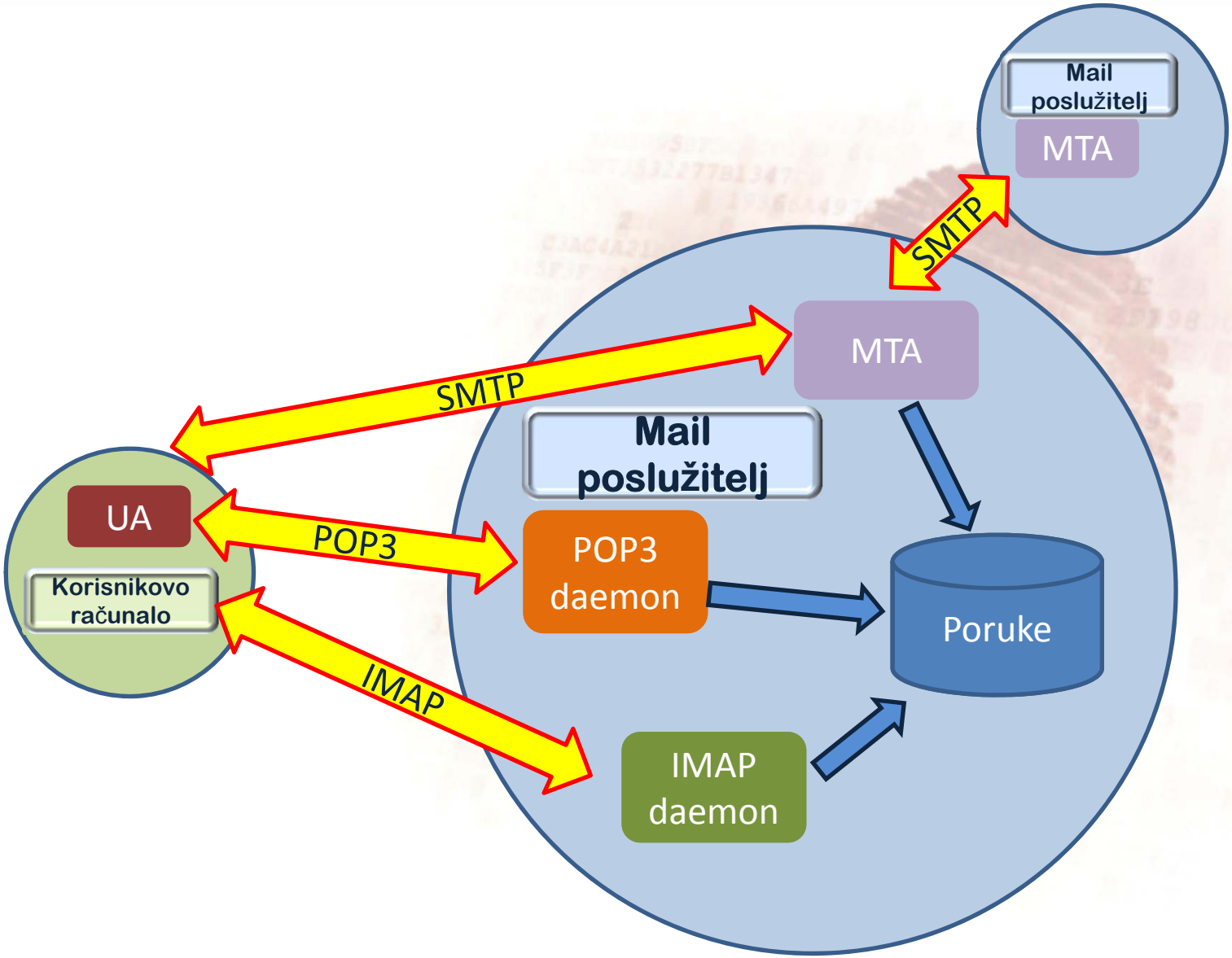
E-mail protokoli

Korištenje protokola za e-mail

- Komunikacija između MTA sustava
  - Koristi isključivo SMTP
- UA komunicira s MTA koristeći
  - POP3 ili
  - IMAP



E-mail protokoli i korištenje



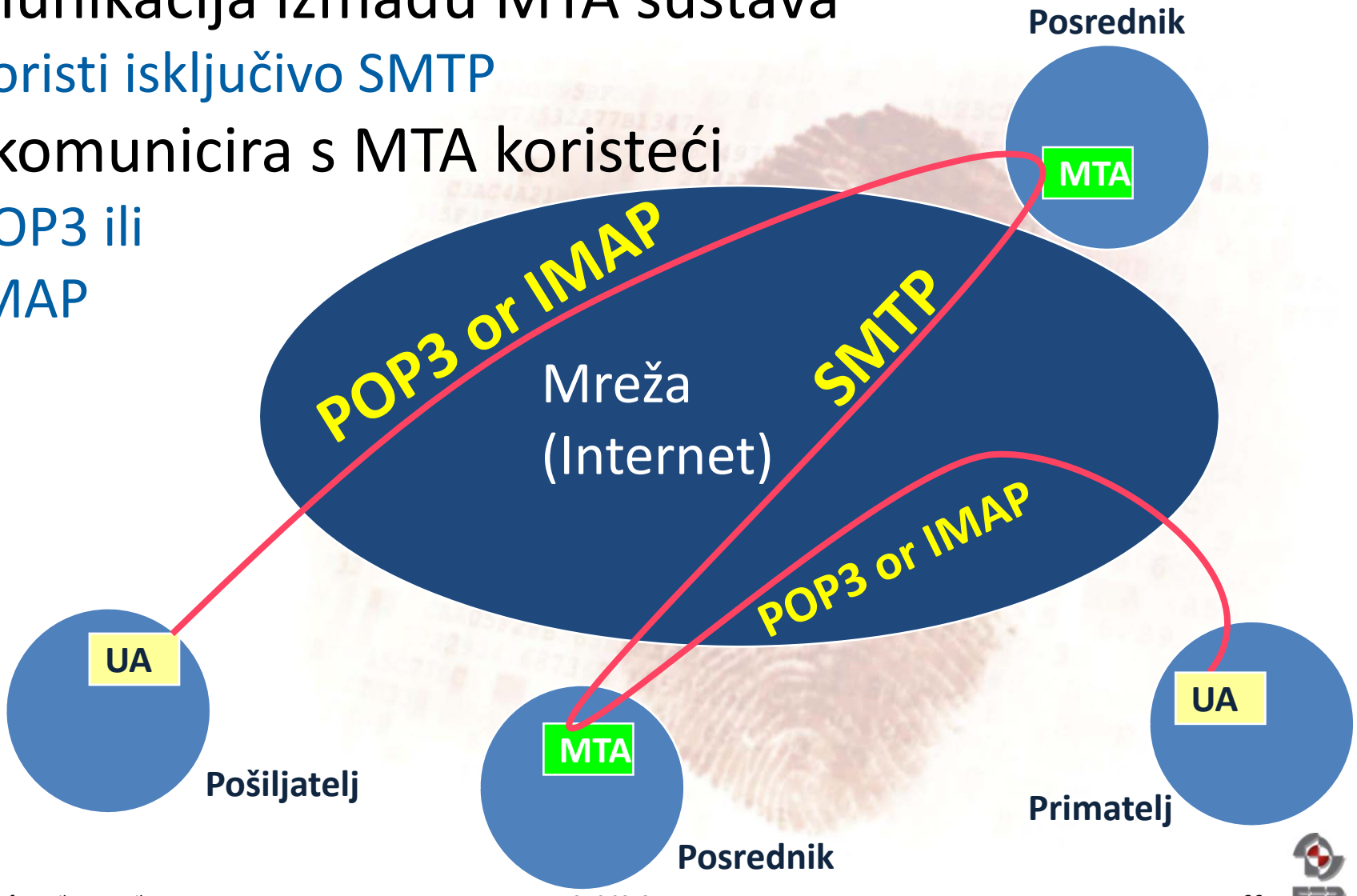
SMTP – Simple Mail Transfer Protocol

- MTA sustavi razmijenjuju poruke koristeći
  - Simple Mail Transfer Protocol
    - RFC 5321
      - ranije: 2821, 821
- Vrlo je star
  - i **zaista** vrlo jednostavan
    - **HELO** ana.zesoi.fer.hr
    - **MAIL FROM**: ppale
    - **RCPT TO**: comfor-test
    - **DATA**
    - Ovo je test poruka
    - .
    - **QUIT**
- Gotovo **ništa se ne provjerava**
  - **Sve** je moguće **krivotvoriti**

```
C:\Users\ppale>telnet maja.zesoi.fer.hr 25

220 maja.zesoi.fer.hr ESMTP Postfix
HELO pero
250 maja.zesoi.fer.hr
MAIL FROM: Albert.Zweistein@physics.world.org
250 2.1.0 Ok
RCPT TO: predrag.pale@gmail.com
250 2.1.0 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
To: Mickey.Mouse@disneyland.org
From: joker@joking.com
Subject: An offer you can't refuse
Sender: Ms.Monneypenny@james.bond.com
Date: Thu, 21 May 2060 05:33:29 -0700

Find everything that is false in this message

:)

Alexander Graham Bell
.
250 2.0.0 Ok: queued as 6FF17B00A8
QUIT
221 2.0.0 Bye
```

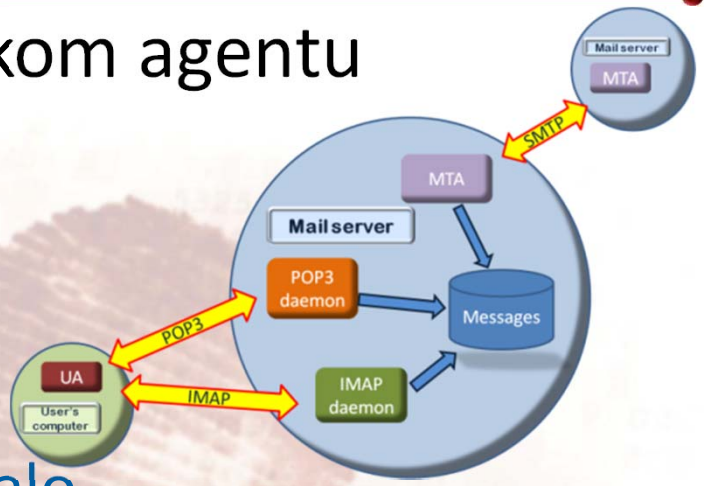
Korištenje protokola za e-mail

- Komunikacija između MTA sustava
  - Koristi isključivo SMTP
- UA komunicira s MTA koristeći
  - POP3 ili
  - IMAP



Protokoli korisničkog agenta: POP3 & IMAP

- Protokoli koji omogućuju korisničkom agentu da pristupi porukama pohranjenim na MTA



- POP3 - Post Office Protocol
  - **Kopira poruke** na korisnikovo računalo
  - Stoga, pristup istom korisničkom računu s drugog računala
    - Neće pronaći poruke koje su već pročitane

- IMAP - Internet Message Access Protocol
  - **Ostavlja poruke** na poslužitelju (MTA)
  - Poruke se mogu organizirati u **direktorije**
  - Pogodno za **pristupanje porukama s više računala**

POP3

- Post Office Protocol inačica 3
  - **Kopira poruke** na korisnikovo računalo
  - Stoga, **pristup istom** korisničkom **računu s drugog računala**
    - **Neće pronaći poruke** koje su već pročitane
- **Vrlo jednostavan** protokol
  - **USER** john
  - **PASS** ******
  - **LIST**
  - **RETR** msg#
  - **DELE** msg#
  - **RSET**
  - **QUIT**

```
C:\Users\ppale>telnet maja.zesoi.fer.hr 110
+OK
USER john
+OK
PASS xyz123
+OK
LIST
1124 4229
1125 19662
1126 1200
1127 1060
1128 1691
.
RETR 1128
+OK
Return-Path: <Albert.Zweistein@physics.world.org>
Delivered-To: ppale@ppale.net
Received: from pero (dhcp-91.zesoi.fer.hr [161.53.64.91])
        by maja.zesoi.fer.hr (Postfix)
            with SMTP id 8CEBEB00BC
        for <ppale@ppale.net>;
            Sat, 14 Nov 2015 21:07:39 +0100 (CET)
To: mister.important@maja.zesoi.fer.hr
From: joker@joking.com
Subject: An offer you can't refuse
Sender: Ms.Monneypenny@maja.zesoi.fer.hr
Date: Middleday, 32 May 2060 05:33:29 -0700

Message-Id: <20151114200741.DEA58B00C2@maja.zesoi.fer.hr>
Status: RO

this is a test mesaege
end
.
QUIT
C:\Users\ppale>
```

Format poruke

- Opisan u RFC 5322
  - ranije: 2822, 822

To:	Primaoc poruke
Cc:	Ostali primaoci (kopije poruke)
Bcc:	Ostali, “nevidljivi” primaoci (kopije poruke)
From:	Tko je pripremio poruku – autor
Sender:	Stvarni pošiljatlej poruke
Received:	Dodaje svaki MTA
Date:	Datum kada je poruka poslana
Message-Id:	Jedinstveni identifikator poruke
Subject:	Tema/naslov poruke

Q: Oblici adresa

Koje e-mail **adrese** su **identične**?

A – predrag.pale@fer.hr i predrag.pale@FER.HR

B – predrag.pale@fer.hr i PREDRAG.PALE@fer.hr

C – predrag.pale@fer.hr i Predrag.Pale@Fer.Hr

D – sve su iste – adrese ne ovie o velikim i malim slovima

E – nijedna nije ista – adrese ovise o velikim i malim slovima

Oblici e-mail adresa

- NE postoji **standard**
  - Svatko je slobodan napraviti svoju shemu
- Dva **najčešća** su:
  1. ppale@maja.zesoi.fer.hr
     - gdje "*ppale*" je obično **korisničko ime** (username) korisnika računala
       - problem: korisnička imena NISU **intuitivna**
     - i "*maja.zesoi.*" prestavlja mail poslužitelj koji se koristi
       - problem: može biti podložno promjenama (zbog tehničkih ili organizacijskih razloga)
  2. ✓ Predrag.Pale@FER.hr
     - **intuitivno** (jednostavno za pogoditi)
     - jednostavno za zapamtiti
     - neovisan o unutrašnjem ustrojstvu informacijskog sustava
     - neovisan o tehničkim i organizacijskim promjenama

Neki tvrde da ovaj oblik olakšava rad spamera i napadača

- VELIKA i mala slova se **ne razlikuju**

Privitci poruka

Potreba za privitcima

- **Osim tekstualnih** poruka
- **Imamo potrebu** razmjenjivati **ĆČĐŠŽčćđšž**
  - Tekst u **različitim jezicima** – koristeći posebne znakove
  - **formatirani** *tekst* **ĂĒŐŒŘąėğŋ**
- **Također trebamo** uključiti i poruku
  - fotografije, crteže, grafove, …
  - audio and video
  - Binarni sadržaj, programe, …






Q: Razmjena privitaka

Kako se **prenose** privitci?

A – Odvojeno od e-mail poruke, putem FTP protokola

B – Uz email poruku, putem HTTP protokola

C – Kao zasebna poruka, putem PGP protokola

D – Uz tijelo poruke, koristeći posebno kodiranje

E – Zasebno, kao datoteka

Postoji problem …

- SMTP
  - i MTA sustavi
- su **napravljeni prije mnogo vremena**
  - kada **nije bilo**
    - digitalnih fotografija, grafova, audio i video sadržaja
  - i samo **za engleski jezik**
    - koristeći **samo 7 bitno** ASCII kodiranje znakova

0101 0001

- stoga,
  - **iako** e-mail sadržaj i**ma 8-bitne** "znakove"
  - ne mogu sadržavati kodove
    - **0** do **31**
      - osim: 9 (TAB), 10 (NL), 13 (CR)
    - **128** do **255**

ASCII tablica - 7 bita

Dec	Hx	Oct	Char	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL (null)	32	20	040		Space	64	40	100	@	@	96	60	140	`	`
1	1	001	SOH (start of heading)	33	21	041	!	!	65	41	101	A	A	97	61	141	a	a
2	2	002	STX (start of text)	34	22	042	"	"	66	42	102	B	B	98	62	142	b	b
3	3	003	ETX (end of text)	35	23	043	#	#	67	43	103	C	C	99	63	143	c	c
4	4	004	EOT (end of transmission)	36	24	044	$	$	68	44	104	D	D	100	64	144	d	d
5	5	005	ENQ (enquiry)	37	25	045	%	%	69	45	105	E	E	101	65	145	e	e
6	6	006	ACK (acknowledge)	38	26	046	&	&	70	46	106	F	F	102	66	146	f	f
7	7	007	BEL (bell)	39	27	047	'	'	71	47	107	G	G	103	67	147	g	g
8	8	010	BS (backspace)	40	28	050	(	(	72	48	110	H	H	104	68	150	h	h
9	9	011	TAB (horizontal tab)	41	29	051	)	)	73	49	111	I	I	105	69	151	i	i
10	A	012	LF (NL line feed, new line)	42	2A	052	*	*	74	4A	112	J	J	106	6A	152	j	j
11	B	013	VT (vertical tab)	43	2B	053	+	+	75	4B	113	K	K	107	6B	153	k	k
12	C	014	FF (NP form feed, new page)	44	2C	054	,	,	76	4C	114	L	L	108	6C	154	l	l
13	D	015	CR (carriage return)	45	2D	055	-	-	77	4D	115	M	M	109	6D	155	m	m
14	E	016	SO (shift out)	46	2E	056	.	.	78	4E	116	N	N	110	6E	156	n	n
15	F	017	SI (shift in)	47	2F	057	/	/	79	4F	117	O	O	111	6F	157	o	o
16	10	020	DLE (data link escape)	48	30	060	0	0	80	50	120	P	P	112	70	160	p	p
17	11	021	DC1 (device control 1)	49	31	061	1	1	81	51	121	Q	Q	113	71	161	q	q
18	12	022	DC2 (device control 2)	50	32	062	2	2	82	52	122	R	R	114	72	162	r	r
19	13	023	DC3 (device control 3)	51	33	063	3	3	83	53	123	S	S	115	73	163	s	s
20	14	024	DC4 (device control 4)	52	34	064	4	4	84	54	124	T	T	116	74	164	t	t
21	15	025	NAK (negative acknowledge)	53	35	065	5	5	85	55	125	U	U	117	75	165	u	u
22	16	026	SYN (synchronous idle)	54	36	066	6	6	86	56	126	V	V	118	76	166	v	v
23	17	027	ETB (end of trans. block)	55	37	067	7	7	87	57	127	W	W	119	77	167	w	w
24	18	030	CAN (cancel)	56	38	070	8	8	88	58	130	X	X	120	78	170	x	x
25	19	031	EM (end of medium)	57	39	071	9	9	89	59	131	Y	Y	121	79	171	y	y
26	1A	032	SUB (substitute)	58	3A	072	:	:	90	5A	132	Z	Z	122	7A	172	z	z
27	1B	033	ESC (escape)	59	3B	073	;	;	91	5B	133	[	[	123	7B	173	{	{
28	1C	034	FS (file separator)	60	3C	074	<	<	92	5C	134	\	\	124	7C	174			|
29	1D	035	GS (group separator)	61	3D	075	=	=	93	5D	135	]	]	125	7D	175	}	}
30	1E	036	RS (record separator)	62	3E	076	>	>	94	5E	136	^	^	126	7E	176	~	~
31	1F	037	US (unit separator)	63	3F	077	?	?	95	5F	137	_	_	127	7F	177	&#127;	DEL

Source: www.LookupTables.com

ASCII tablica - 8 bita

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
0	NUL	DLE		0	@	P	‘	p	PAD	DCS	NBSP	°	Á	Ð	à	ð	0
1	SOH	DC1	!	1	A	Q	a	q	HOP	PU1	¡	±	À	Ñ	á	ñ	1
2	STX	DC2	"	2	B	R	b	r	BPH	PU2	¢	²	Â	Ò	â	ò	2
3	ETX	DC3	#	3	C	S	c	s	NBH	STS	£	³	Ã	Ó	ã	ó	3
4	EOT	DC4	$	4	D	T	d	t	IND	CCH	¤	´	Ä	Ô	ä	ô	4
5	ENQ	NAK	%	5	E	U	e	u	NEL	MW	¥	µ	Å	Õ	å	õ	5
6	ACK	SYN	&	6	F	V	f	v	SSA	SPA	¦	¶	Æ	Ö	æ	ö	6
7	BEL	ETB	'	7	G	W	g	w	ESA	EPA	§	·	Ç	×	ç	÷	7
8	BS	CAN	(	8	H	X	h	x	HTS	SOS	¨	¸	È	Ø	è	ø	8
9	TAB	EM	)	9	I	Y	i	y	HTJ	SGI	©	¹	É	Ù	é	ù	9
A	LF	SUB	*	:	J	Z	j	z	VTS	SCI	ª	º	Ê	Ú	ê	ú	A
B	VT	ESC	+	;	K	[	k	{	PLD	CSI	«	»	Ë	Û	ë	û	B
C	FF	FS	,	<	L	\	l	|	PLU	ST	¬	¼	Ì	Ü	ì	ü	C
D	CR	GS	-	=	M	]	m	}	RI	OSC		½	Í	Ý	í	ý	D
E	SO	RS	.	>	N	^	n	~	SS2	PM	®	¾	Î	Þ	î	þ	E
F	SI	US	/	?	O	_	o	DEL	SS3	APC	¯	¿	Ï	ß	ï	ÿ	F

Dopušpteno

Nije dopušteno

Rješenje

- Sve “novo” i “neobično”
  - će se staviti u **tijelo** poruke
  - ali **kodirano** na određeni način
  - tako da se samo **standardni 7-bitni** znakovi koriste
- dvije **najčešće** korištene sheme kodiranja:
  - **Quoted-printable** encoding
    - **ostavlja** “normalne” (7-bitne) znakove kakvi jesu
    - ali one koji imaju 8. bit postavljen na “1” **kodira** koristeći tri znaka
      - prefiks “=“ i
      - dva 7-bitna ASCII znaka koji predstavljaju heksadekadski ASCII kod znaka
    - na primjer: **Ä → =C4**
  - **Base 64** encoding
    - **kodira sve znakove u poruci**
    - **3 bajta** se kodiraju **koristeći 4 bajta**
    - dobiju se svi “razumljivi znakovi” (7 bita) prilikom prijenosa

      ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz1234567890+/
    - posljedica je da je, poruka **33% veća**

Base 64 encoding

1. pretvara 3 uzastopna bajta poruke
2. u 8 bita (24 bita ukupno)
3. dijeli ih u 4 dijela od 6 bita (24 bita ukupno)
4. 64 (dekadsko) se dodaje na svaki dio
5. Što rezultira u stvaranju “razumljivih znakova”

1	Originalan tekst	N				i				z			
	ASCII kodiranje (dekadsko)	78				105				122			
2	Stvarni niz bitova originala	**01**	**00**	**11**	**10**	**01**	**10**	**10**	**01**	**01**	**11**	**10**	**10**
3	6-bitna interpretacija	19+64 =				38				37			58
4	BASE64 abeceda	T				m				l			6
5	Konačni (kodirani) niz bitova	**01010100**				**01101101**				**01101100**			**00110110**

- Svaki niz bitova može se kodirati u “razumljive znakove”
  - dakle i **binarni** sadržaji

Mali problem s Base 64

- **što ako duljina** sadržaja za kodiranje nije **višekratnik od 3**?

N				i				z				2					
01	00	11	10	01	10	10	01	01	11	10	10	00	11	00	**10**	**?**	**?**
T				m				l				6				M	
																?	

- onda, se nadopunjuje s nulama do potrebne dujline

N				i				z				2					
01	00	11	10	01	10	10	01	01	11	10	10	00	11	00	**10**	**00**	**00**
T				m				l				6				M	
																g==	

- i na zadnji kodirani znak se dodaje **poseban znak** "="
  - stoga, kodirani blok može završiti sa 2, 1 ili 0 dodanih "=" znakova (eng. padding)

Kodiranje poruka

- Korisnički agent obavlja
  - kodiranje i dekodiranje 8-bitnog sadržaja poruke
- No, moraju znati:
  - da je poruka ili njezini dijelovi **kodirani**
  - **kako** je kodirana
  - **parametre** sadržaja kako bi ih ispravno interpretirala
    - grafičke
    - audio , video
    - programi
    - itd.
- Zapravo, također trebamo:
  - moći uključiti **više dijelova** binarnih informacija
    - u istoj poruci
  - a također i održati kompatibilnost sa starijim sustavima

Rješenje: MIME

- **Multipurpose Internet Mail Extensions**
- metoda za prijenos **bilo kakvog tipa** podataka
  - posebni znakovi, formatirani tekst,
  - grafovi, fotografije, audio, video, programi, binarni podatci …
- unutar tijela standardne e-mail poruke
- koristeći posebnu metodu kodiranja sadržaja
  - QP, Base64
- koristeći posebna zaglavlja
  - MIME-Version:
  - Content-Description:
  - Content-Id:
  - Content-Transfer-Encoding:
  - Content-Type:

MIME metoda

- e-mail **poruka** i dalje ima
  - **zaglavlja** i **tijelo**
  - slijedi rfc822
- ali tijelo može imati **više dijelova**
  - dijelovi su odvojeni posebno oznakom
    - **jedinstven** skup **znakova**
      - **Koji se ne nalazi** nigdje drugdje u poruci
    - obično **počinje** s nizom **“--“ znakova**
      - --=_NextPart_000_00B2_01D11F57.F5457240
    - završava također s “--“ oznakom
- **svaki dio** ima vlastito (MIME) **zaglavlje** i **tijelo**
  - neka MIME zaglavlja su također i u zaglavljima poruke

MIME zaglavlja - osnove

- Na **početku** uvijek postoji **identifikacijsko polje**
  - osnovni oblik: **MIME-Version: 1.0**
  - varijacije:
    - MIME-Version: 1.0 (produced by FER Mailer)
    - MIME-Version: 1.(produced for CompFor)
      - Zaglavlje označavaju komentare (prema "starom" RFC 822)
- **Content-Type** zaglavlje oblika:
  - Content-Type: type/subtype *[;parameter]
    - Govori korisničkom agentu **što da radi**, **kako postupati** s privitkom
  - Na primjer:
    - Content-Type: text/plain; charset=us-ascii (Plain text)
    - Content-Type: text/plain; charset="us-ascii"
- "inicijalni" (predefinirani) tipovi
  - text, image, audio, video, application
- kompozitni tipovi
  - multipart, message
- mehanizam nadogradnje:
    - ili registrirati ih (pri organizaciji IANA)
    - ili neregistriranim tipovima dati prefiks "X-"

MIME tipovi sadržaja (Content types)

Primjer: Content-Type: video/x-ms-wmv

- Tekst
  - Običan – zadana vrijednost
    - text/css
  - Richtext
- Slike
  - GIF, JPEG, PNG, BMP, …
    - image/png
- Audio
  - audio/x-wav
- Video
  - video/x-ms-wmv
- Aplikacije
  - application/pdf
  - Octet-stream
  - Postscript
- Poruke
  - Rfc822
    - Enkapsulira drugu poruku
  - Partial
    - MIME dijeli više datoteka
  - External-body
    - referenca na externi izvor podataka
- Multipart
  - Mixed
    - Više sadržaja prati poruku
  - Alternative
    - Isti podatci su prikazani više puta
  - Parallel
    - Dijelovi se trebaju gledati istovremeno
  - Digest
    - Svaki dio je posebna “poruka”

MIME zaglavlja - kodiranje

- Content-Transfer-Encoding
  - može biti u zaglavlju svakog dijela
    - neobavezno - postoje default vrijednosti
  - označava tip kodiranja
    7bita / 8bita / binarno / quoted-printable / base64 / ietf-token / x-token
  - 7bita ~= 8bita ~= binarno – oznaka da nije bilo transformacije sadržaja
  - ietf-token - format definiran starnards track RFC-om
    - i registriran pri IANA
  - x-token – privatni aplikacijski format
    - nije registriran pri IANA
  - vnd.token – format specifičan za pojedinog proizvođača
- Content-Disposition
    - Označava gdje treba prikazati privitak
  - **Inline**
    - Prikaz će biti na mjestu gdje se nalazi u poruci
    - Na primjer: ubačena slika
  - **Attachment**
    - Pohranjen kao eksterna datoteka
  - parameters: filename, dates, size
    - Ime datoteke se obično koristi kod pohrane sadržaja

MIME primjer: jednostavan e-mail

mail_text.txt (~/fer/racfor/mime-base64-res/mail_simpletext) - GVIM

Open Save SaveAll Print Undo Redo Cut Copy

```
MIME-Version: 1.0
Received: by 10.28.141.130 with HTTP; Tue, 13 Oct 2015 05:45:23 -0800 (PST)
Date: Tue, 13 Oct 2015 14:45:23 +0100
Delivered-To: petar.djerasimovic@gmail.com
Message-ID: <CAHO3kj7sGBoHgopJ5LmBk=A6vH9qWtz=rLiTR5F_v0PR3PSosg@mail.gmail.com>
Subject: Demo mail plain text
From: Petar Djerasimovic <petar.djerasimovic@gmail.com>
To: Petar Djerasimovic <petar.djerasimovic@gmail.com>
Content-Type: text/plain; charset=UTF-8

Jednostavan demo mail, tzv "plain text format".
~
```

Tekstualni prikaz sadržaja

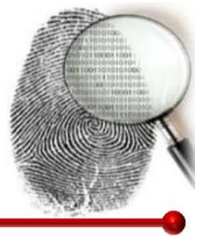
- Primjetiti:
  - tip je text/plain
  - samo zaglavlje i sadržaj
  - samo ASCII znakovi

MIME primjer: formatirani text

- Postoje dva sadržaja
  - svaki sa vlastitim Content-Type
- korisnički agent ih odvaja u dijelove

```
MIME-Version: 1.0
Received: by 10.28.141.130 with HTTP; Wed, 14 Oct 2015 09:56:29 -0800 (PST)
Date: Wed, 14 Oct 2015 18:56:29 +0100
Delivered-To: petar.djerasimovic@gmail.com
Message-ID: <CAHO3kj47=u6Oa-+cV4V5JEvYuzyVPt7Yy5GT6_-QNWFRbKDAcA@mail.gmail.com>
Subject: Demo formatirani tekst
From: Petar Djerasimovic <petar.djerasimovic@gmail.com>
To: Petar Djerasimovic <petar.djerasimovic@gmail.com>
Content-Type: multipart/alternative; boundary=001a114b2d665b73dd05237e61eb

--001a114b2d665b73dd05237e61eb
Content-Type: text/plain; charset=UTF-8

Ovo je *mail* s *formatiranim tekstom*

--001a114b2d665b73dd05237e61eb
Content-Type: text/html; charset=UTF-8
Content-Transfer-Encoding: quoted-printable

<div dir=3D"ltr">Ovo je <b>mail</b> s=C2=A0<i>formatiranim tekstom</i>.</di=
v>

--001a114b2d665b73dd05237e61eb--
```

MIME primjer: kodirani naslov



Naslov s jednim znakom: “Naslov_s_jednim_**ć**”

```
MIME-Version: 1.0
Received: by 10.28.141.130 with HTTP; Wed, 14 Oct 2015 10:51:45 -0800 (PST)
Date: Wed, 14 Oct 2015 19:51:45 +0100
Delivered-To: petar.djerasimovic@gmail.com
Message-ID: <CAHO3kj6-OgfXgx5hV3wrJC4WVDiMxv2BYerCb6fDz2Wf5T0m-A@mail.gmail.
Subject: =?UTF-8?Q?Naslov_s_jednim_=C4=87?=
From: Petar Djerasimovic <petar.djerasimovic@gmail.com>
To: Petar Djerasimovic <petar.djerasimovic@gmail.com>
Content-Type: multipart/alternative; boundary=001a114b07d6f9719705237f269d
```

Q = QP-encoding
B = BASE64

Kodiranje bira korisnički agent

Naslov s više znakova: Hrvatski znakovi izvan ASCII tablice su **čćđšž** odnosno veliko **ČĆĐŠŽ**

```
MIME-Version: 1.0
Received: by 10.28.141.130 with HTTP; Wed, 14 Oct 2015 11:09:16 -0800 (PST)
Date: Wed, 14 Oct 2015 20:09:16 +0100
Delivered-To: petar.djerasimovic@gmail.com
Message-ID: <CAHO3ki4nMumLvhJ9n=Kz1d5TwzLqqvMJbmn9HihtfCM3qD1_TA@mail.gmail.com>
Subject: =?UTF-8?B?SHJ2YXRza2kgem5ha292aSBpenZhbiBBU0NJSSB0YWJsaWNlIHN1IMSNxIfEkcWhxb4gbw==?=
    =?UTF-8?B?ZG5vc25vIHZlbGlrbyDEjMSGxJDFoMW9?=
From: Petar Djerasimovic <petar.djerasimovic@gmail.com>
To: Petar Djerasimovic <petar.djerasimovic@gmail.com>
Content-Type: multipart/alternative; boundary=001a11443b1aa7168a05237f6582
```

MIME primjer: e-mail s priloženom video datotekom

- Content-Type: multipart/mixed
- E-mail sadrži:
  - **text** (text/plain)
  - s proslijeđenom e-mail porukom
    - sadrži **video** (video/mp4)
      - kao **privitak**

```
MIME-Version: 1.0
Received: by 10.28.141.130 with HTTP; Thu, 15 Oct 2015 07:53:07 -0800 (PST)
In-Reply-To: <563634fb.6116c20a.44fe.373c@mx.google.com>
References: <563634fb.6116c20a.44fe.373c@mx.google.com>
Date: Thu, 15 Oct 2015 16:53:07 +0100
Delivered-To: petar.djerasimovic@gmail.com
Message-ID: <CAHO3kj7BsKC0PJLEb0MrOUPF8ySg5ZrzDeKWxf81BSXCJ=7q8g@mail.gmail.com>
Subject: Fwd: Vib download link
From: Petar Djerasimovic <petar.djerasimovic@gmail.com>
To: Petar Djerasimovic <petar.djerasimovic@gmail.com>
Content-Type: multipart/mixed; boundary=001a1148ef6227d74305237ca818

--001a1148ef6227d74305237ca818
Content-Type: text/plain; charset=UTF-8

kratak film (596K)


---------- Forwarded message ----------
From:  <vib.download@gmail.com>
Date: Thu, Oct 15, 2015 at 4:51 PM
Subject: Vib download link
To: petar.djerasimovic@gmail.com


Your download link:
http://s3-eu-west-1.amazonaws.com/vibbed-videos/040658982ebbbfa6e3890bed156af1f7160e08f03

--001a1148ef6227d74305237ca818
Content-Type: video/mp4;
    name="040658982ebbbfa6e3890bed156af1f7160e08f03907eace5f60988d.mp4"
Content-Disposition: attachment;
    filename="040658982ebbbfa6e3890bed156af1f7160e08f03907eace5f60988d.mp4"
Content-Transfer-Encoding: base64
X-Attachment-Id: f_iggp58kc0

AAAAIGZ0eXBpc29tAAACAGlzb21pc28yYXZjMW1wNDEAAAAIZnJlZQAJLzttZGF0AAACrAYF//+o
3EXpvebZSLeWLNgg2SPu73gyNjQgLSBjb3JlIDE0MiByNTAgZGQ3OWE2MSAtIEguMjY0L01QRUct
NCBBVkMgY29kZWMgLSBDb3B5bGVmdCAyMDAzLTIwMTQgLSBodHRwOi8vd3d3LnZpZGVvbGFuLm9y

                    (. . .)

swAJKn0AAABhdWR0YQAAAFltZXRhAAAAAAAAACFoZGxyAAAAAAAAAABtZGlyYXBwbAAAAAAAAAAA
AAAAACxpbHN0AAAAJKl0b28AAAAcZGF0YQAAAAEAAAAATGF2ZjU2LjQuMTAx
--001a1148ef6227d74305237ca818--
```

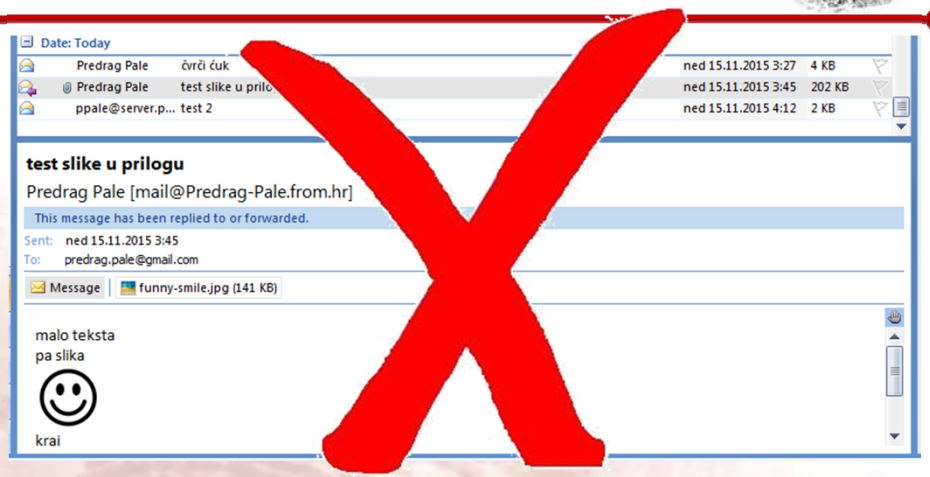
Ekstrakcija i dekodiranje sadržaja

- koristeći **e-mail** poruku iz prethodne prikaznice
  - zadnji dio poruke
    - **odvojen** zadnjim parom razdjelnika (eng. delimiter)
  - ručno je **pohranjen** u datoteku naziva "***encoded***"
  - i poslana na aplikaciju za dekodiranje "***base64***"
    - rezultat je pohranjen u datoteku naziva "***decoded***"
  - dva alata su se koristila za detekciju tipa sadržaja u datoteci
    - ***trID*** → detektira **MPEG-4** video
    - ***file*** → detektira **MPEG** v4

```
petar@asus$ head -n 3 encoded
AAAAIGZ0eXBpc29tAAACAGlzb21pc28yYXZjMW1wNDEAAAAIZnJlZQAJLzttZGF0AAACrAYF//+o
3EXpvebZSLeWLNgg2SPu73gyNjQgLSBjb3JlIDE0MiByNTAgZGQ3OWE2MSAtIEguMjY0L01QRUct
NCBBVkMgY29kZWMgLSBDb3B5bGVmdCAyMDAzLTIwMTQgLSBodHRwOi8vd3d3LnZpZGVvbGFuLm9y
petar@asus$ tail -n 2 encoded
swAJKn0AAABhdWR0YQAAAFltZXRhAAAAAAAAACFoZGxyAAAAAAAAAABtZGlyYXBwbAAAAAAAAAAA
AAAAACxpbHN0AAAAJKl0b28AAAAcZGF0YQAAAAEAAAAATGF2ZjU2LjQuMTAx
petar@asus$ base64 -d encoded > decoded
petar@asus$ trid -n:2 decoded
TrID/64 - File Identifier v2.20 - (C) 2003-15 By M.Pontello
Definitions found:  5968
Analyzing...
Collecting data from file: decoded
 36.7% (.M4V) MPEG-4 Video (70005/3/23)
 33.0% (.M4R) iPhone Ringtone (63004/2/19)
petar@asus$ file decoded
decoded: ISO Media, MPEG v4 system, version 1
```

Forenzička analiza privitaka

- MIME dijelovi mogu
  - **nedostajati**
  - **biti korumpirani**
    - **oštećeni**
    - **namjerno** izmijenjeni



- stoga, u analizi
  - **ne možemo se nasloniti na** obično čitanje privitaka
    - standardnim korisničkim agentima
  - **već moramo**
    - **analizirati** MIME dijelove
    - **ekstrahirati** ih u datoteke
    - koristiti posebne alate za konverziju
    - te provjeriti njuhov **tip** i, konačno, provjeriti **sadržaj**

Šifriranje e-mail poruka

Q: Šifriranje e-mail poruka

Kako se e-mail poruke šifriraju?

A – Koriste se različiti e-mail protokoli (ne SMTP)

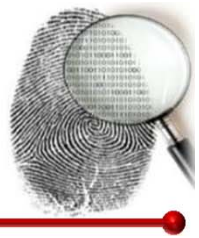
B – Koriste se različiti UA i MTA

C – Cijela poruka je šifrirana (zaglavlje i tijelo)

D – Tijelo (ili dijelovi) poruke su šifrirani

E – Nije moguće šifrirati e-mail poruke

E-mail poruke se mogu šifrirati



- MIME se koristi
- MIME dijelovi su šifrirani
  - ali ne i zaglavlje poruke
  - S/MIME – Secure MIME
    - autentifikacija, integritet poruke, neporecivost izvora poruke, privatnost i tajnost podataka
    - Content_Type: application/pkcs7-mime
- nekoliko metoda
  - PGP- Pretty Good Privacy
  - GnuPG – GNU Privacy Guard

Što smo naučili

- Kako e-mail **putuje**
  - između MTA sustava (min 2)
  - između UA i MTA

- **Protokol**(i)
  - MTA koristi SMTP
  - UA koristi POP3 ili IMAP

SMTP POP3 IMAP

- **Zaglavlja** poruka
  - mogu se krivotroviti
  - analizirati prvu (najnižu) “Received:” liniju zaglavlja

To: From: Date: Subject: Received:

- **Privitci** poruka
  - su u tijelu poruka
  - kodirani koristeći MIME
  - mogu biti ručno analizirani

MIME

- **Šifrirani** e-mail
  - MIME dijelovi su šifrirani
  - zaglavlaj nisu šifrirana
    - a ponekad i dijelovi tijela poruke

S/MIME

Standardi

- RFC 5321 – SMTP
  - stariji 2821, 821
- RFC 5322 – message format
  - stariji 2822, 822

- RFC 1939 – POP3
  - stariji 1722,1460, 1225, 1081
- RFC 1176 – IMAP
  - stariji 1203, 1064

- RFC 1521, 1522 – MIME
  - stariji : 1341, 1342
  - noviji: RFC 2045, 2046, 2047, 2048, 2049, 4288, 4289

- RFCs 3369, 3370, 3850, 3851 – S/MIME
- RFC 4880, 3156 – OpenPGP
  - stariji : 1991, 2440

Napredno korištenje e-maila

- automatski **odgovori**
- **ulaz** u aplikacijama – **izlaz** iz aplikacija
- automatske **akcije**
- **mehanizmi za prijenos** datoteka


RacFor.zesoi.fer.hr
RacFor@zesoi.fer.hr