eEvidence

The 4 steps of the eEvidence way

1. eEvid request
The eEvid certification begins right when the email to be attested is received at eEvidence.

2. Digital footprints (hash)
Unique hashes are obtained from the original email and from any attached files it may contain.

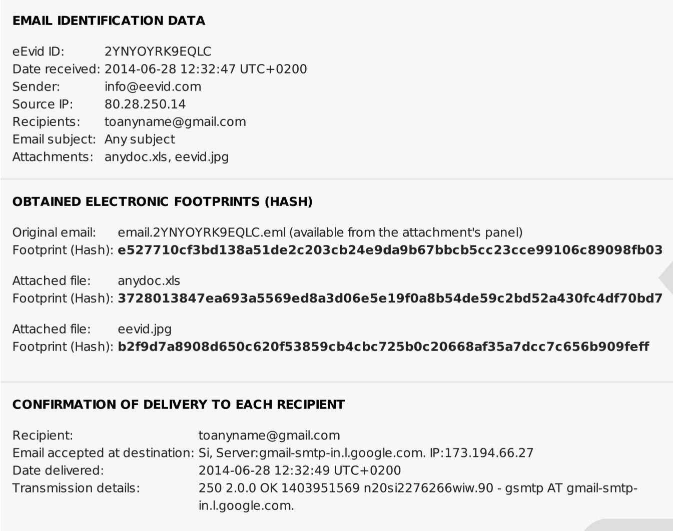
3. Email delivery
By a standard SMTP connection, the email is delivered to the destination server and the transmission is recorded.

4. The eEvid.Cert is issued
Electronic evidence of the contents and delivery of the email, as a digitally signed PDF format file.

The eEvid.Cert electronic evidence

Unique key identifying the eEvid.Cert and basic data copied from the original email header, according to the Internet Message Format standard (RFC 5322).

It includes the names of any attached file the email may contain.



EMAIL IDENTIFICATION DATA

eEvid ID: 2YNYOYRK9EQLC
Date received: 2014-06-28 12:32:47 UTC+0200
Sender: info@eevid.com
Source IP: 80.28.250.14
Recipients: toanyname@gmail.com
Email subject: Any subject
Attachments: anydoc.xls, eevid.jpg

OBTAINED ELECTRONIC FOOTPRINTS (HASH)

Original email: email.2YNYOYRK9EQLC.eml (available from the attachment's panel)
Footprint (Hash): **e527710cf3bd138a51de2c203cb24e9da9b67bbcb5cc23cce99106c89098fb03**

Attached file: anydoc.xls
Footprint (Hash): **3728013847ea693a5569ed8a3d06e5e19f0a8b54de59c2bd52a430fc4df70bd7**

Attached file: eevid.jpg
Footprint (Hash): **b2f9d7a8908d650c620f53859cb4cbc725b0c20668af35a7dcc7c656b909feff**

CONFIRMATION OF DELIVERY TO EACH RECIPIENT

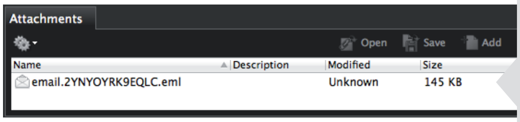
Recipient: toanyname@gmail.com
Email accepted at destination: Si, Server:gmail-smtp-in.l.google.com. IP:173.194.66.27
Date delivered: 2014-06-28 12:32:49 UTC+0200
Transmission details: 250 2.0.0 OK 1403951569 n20si2276266wiw.90 - gsmtp AT gmail-smtp-in.l.google.com.

Hashes from the original email and from any file attached to the email.

The hash value is a unique fingerprint of a data set, such as a file, obtained by a hash function. For a given file and its copies, the resulting hash value will always be the same, provided the file has not changed. If at some point a file returns a different hash, it means that the file has been modified.

Details of the email acceptance by the recipient's mail server, according to the SMTP (Simple Mail Transfer Protocol, RFC 5321) standard.

The transmission details show the name and IP address of the destination server, as well as the id key that the destination server uses to internally identify the email.



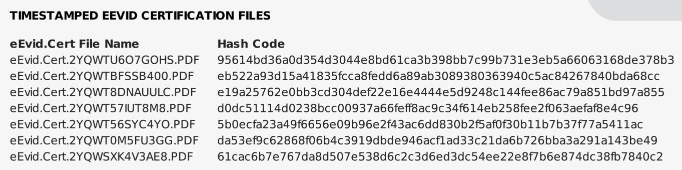
Name	Description	Modified	Size
email.2YNYOYRK9EQLC.eml		Unknown	145 KB

The eEvid.Cert PDF contains, as an attachment, a full copy of the original email in .eml standard format.

Use Adobe Reader or Adobe Acrobat to view and save the copy of the original email.

eEvid Daily Report

Daily PDF file, digitally signed and time-stamped. It contains a hash value for each eEvid.Cert issued the day before, setting its date.



TIMESTAMPED EEVID CERTIFICATION FILES

eEvid.Cert File Name	Hash Code
eEvid.Cert.2YQWTU6O7GOHS.PDF	95614bd36a0d354d3044e8bd61ca3b398bb7c99b731e3eb5a66063168de378b3
eEvid.Cert.2YQWTBFSSB400.PDF	eb522a93d15a41835fcca8fedd6a89ab3089380363940c5ac84267840bda68cc
eEvid.Cert.2YQWT8DNAUULC.PDF	e19a25762e0bb3cd304def22e16e4444e5d9248c144fee86ac79a851bd97a855
eEvid.Cert.2YQWT57IUT8M8.PDF	d0dc51114d0238bcc00937a66feff8ac9c34f614eb258fee2f063aefaf8e4c96
eEvid.Cert.2YQWT56SYC4YO.PDF	5b0ecfa23a49f6656e09b96e2f43ac6dd830b2f5af0f30b11b7b37f77a5411ac
eEvid.Cert.2YQWT0M5FU3GG.PDF	da53ef9c62868f06b4c3919dbde946acf1ad33c21da6b726bba3a291a143be49
eEvid.Cert.2YQWSXK4V3AE8.PDF	61cac6b7e767da8d507e538d6c2c3d6ed3dc54ee22e8f7b6e874dc38fb7840c2

Glossary of terms

EEVIDENCE. The owner of the eEvidence service. **eEvid ID**. Alphanumeric code that uniquely identifies each eEvid. **Date received.** Date and time in which the email to be processed is received by eEvidence. **UTC**. World's primary time standard. **Sender**. Email address from which the the email to be certified has been received. **Source IP**. IP address from were the email has been transmitted to eEvidence. **Recipients**. Email addresses to which the email must be delivered. **Email subject**. Text included in the original email subject field. **Attachments**. Name of every file attached to the original email, if any. **Footprint (Hash)**. Unique encryption code obtained by means of the SHA 256 cryptographic algorithm from the original email and from every file attached to it. **Email accepted at destination**. Acceptance of delivery confirmed by the recipient's mail server and, if provided and indicated, the alphanumeric code with which the recipient's mail server has uniquely identified and registered the email internally.. **Date delivered**. Date and time in which the email has been accepted by the recpient's mail server. **Transmission details**. Relevant information of the SMTP transmission between eEvidence and the recipient's mail server during the delivery and acceptance of the email. **Digital signature**. Mathematical scheme that confirms that the contents of a digitally signed document has not been altered since the signature was applied. **Trusted timestam**. Digital timestampt provided by a Time Stamping Authority (TSA) that proves the existence of a document before a certain point in time and that its contents has not been altered since then.