SCHEDELEAKS

Tutto ciò che avreste voluto sapere sulle schede telefoniche

Rubrica a cura di Stefano Rossi e Gianfranco Marchese

ospitata da:

Schede Telefoniche .org

4th - Decoding and translation of codes

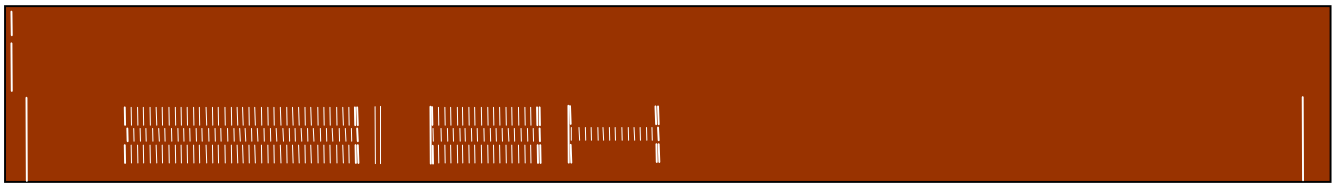
3 ° - Coding of Urmet telephone cards

Last revised: 01/08/2017 12:33

Decoding and translation of codes

3-Urmet telephone card encoding

As already seen in the paragraph "With the naked eye", here is what a phone card looks like when viewed through the magnetic lens:



Unlike normal magnetic cards, the phone card has its own magnetic strip broken into three bands, of which the first and third are the same. Because?

Unfortunately, there is no official information in this regard, so I can only put forward hypotheses that are not of an official nature.

Inside the phone card there are data but above all money! Being able to forge a phone card can give the attacker the opportunity to make phone calls at no cost to the telephone company. Hence the need to find a system capable of not allowing fraud, taking into account two major weaknesses:

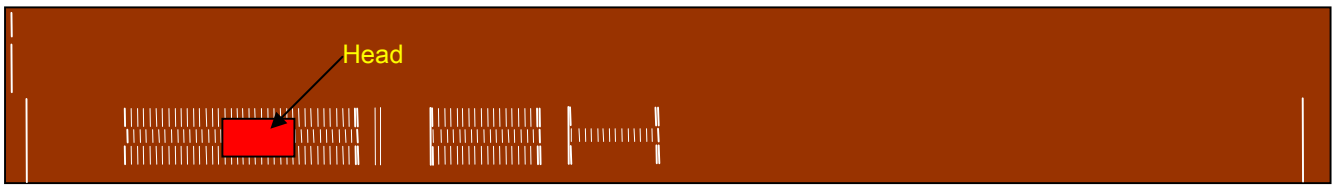
1. Telephone booths: these are scattered throughout the territory in even remote areas, without surveillance. The possibility that an attacker could steal an entire phone booth is not science fiction. Considering that inside the cabin there is all the technology necessary to decode the telephone card, the possibility could offer everything necessary to crack the system;

2. Telephone cards: it contains the information that allows you to make phone calls. It is easy to find and does not use alien technology: any head could read its content;

So both telephone cards and booths can give excellent ideas for decoding the system. Then? The three-band system seems to have been created precisely for this reason: normal badge and card writers cannot write a single track broken into three parts, so unless they have ad hoc writing heads (therefore not available easily on the market) it is impossible to faithfully reproduce the writing of the tracks.

And the reading?

Although the trace is split in three, the reading must be performed by means of a single head, the resulting signal will be the sum of the three bands read simultaneously:



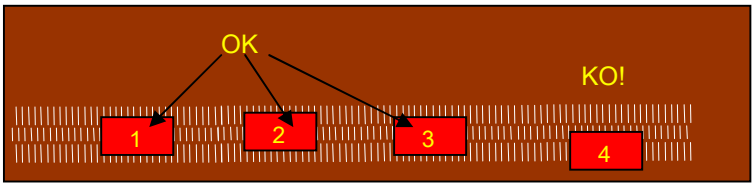
The final result of the reading will therefore be the simultaneous sum of the individual tracks:

MAGNETISM = (50% BAND 1) + (100% BAND 2) + (50% BAND 3)

This particular arrangement of the three bands means that even minimal vertical movements of the head ensure correct reading: the

central track will always be read at 100% while the remaining two will ensure an overall contribution equal to 100%.

I try to schematize below:



In the first case, the head is in a central position and reads exactly two halves of the upper and lower bands; in the second and third cases, however, the head is positioned non-symmetrically and occupies different portions of the first and third band: since the two bands are identical, the total contribution will always be the same:

1) MAGNETISM = (50% BAND 1) + (100% BAND 2) + (50% BAND 3)
2) MAGNETISM = (25% BAND 1) + (100% BAND 2) + (75% BAND 3)
3) MAGNETISM = (75% BAND 1) + (100% BAND 2) + (25% BAND 3)
4) MAGNETISM = (0% BAND_1) + (80% BAND 2) + (100% BAND 3)

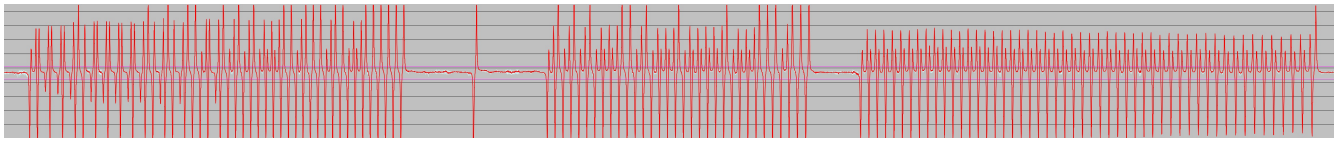
In the first three cases the result will always be the same, regardless of the vertical position of the head since the sum of bands 1 and 3 is 100%. In the fourth case the sum of 1 and 3 is always 100% but the central band is not completely covered so the final result will be incomplete.

For the reasons indicated in the introduction chapter, not having (and not wanting to have) original URMET instrumentation, it is necessary to rely on what can be found regularly on the market, such as a badge reader.

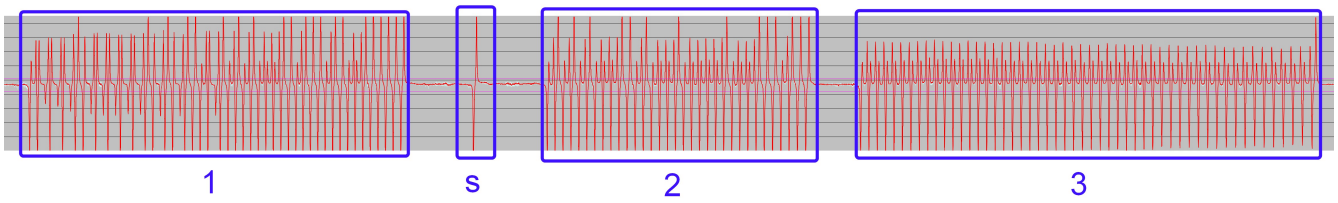
The readers on the market are designed to read magnetic strips encoded according to certain standards defined by the ISO. It is possible to use these heads to read a telephone card EVEN IF the size of the head is possibly not large enough to cover

perfectly the central one and two halves of the upper and lower ones: the result of the simultaneous reading of the three bands will therefore be different from the reading performed by the original URMET instrumentation built ad hoc.

By correctly positioning the head of the badge, analyzing the output thus produced by means of an oscilloscope, here's what we get:



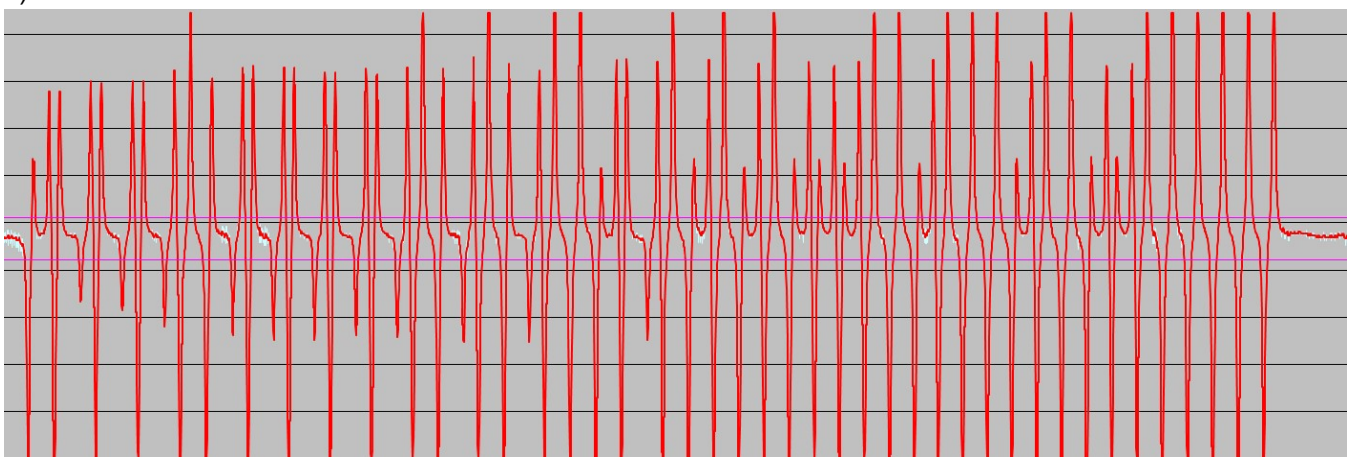
The magnetic stripe is evidently divided into several sections, each representing different information, except the section "S" which seems to have the sole function of separating sections 1 and 2:



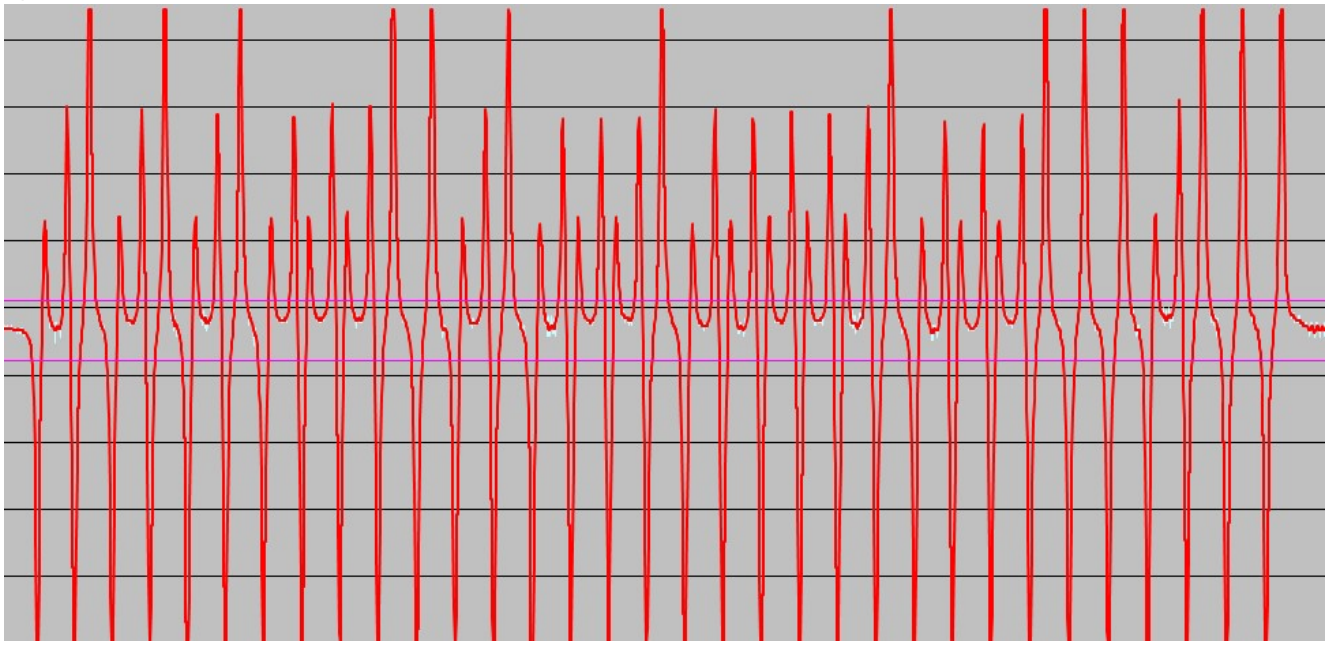
Each section is contained between a pair of positive / negative peaks that do not contribute to the determination of the bits.

Zooming:

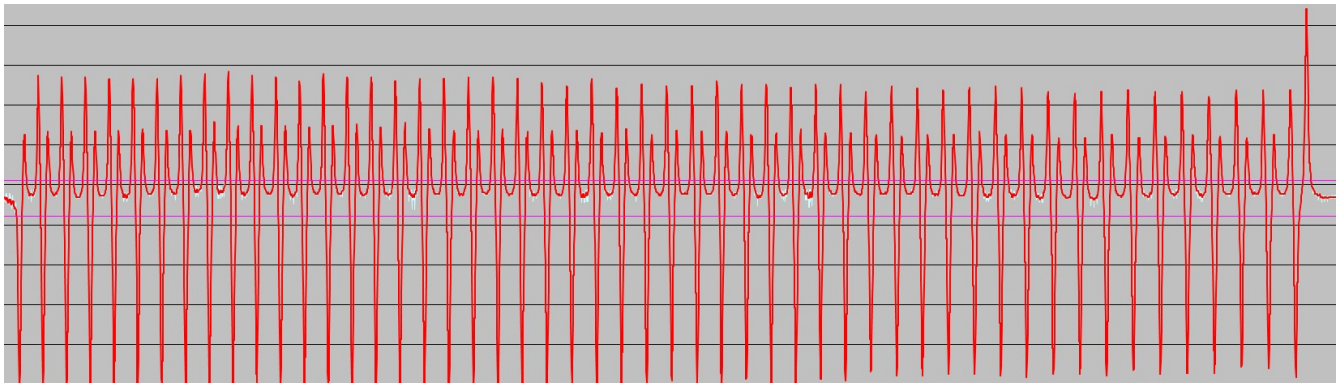
1)



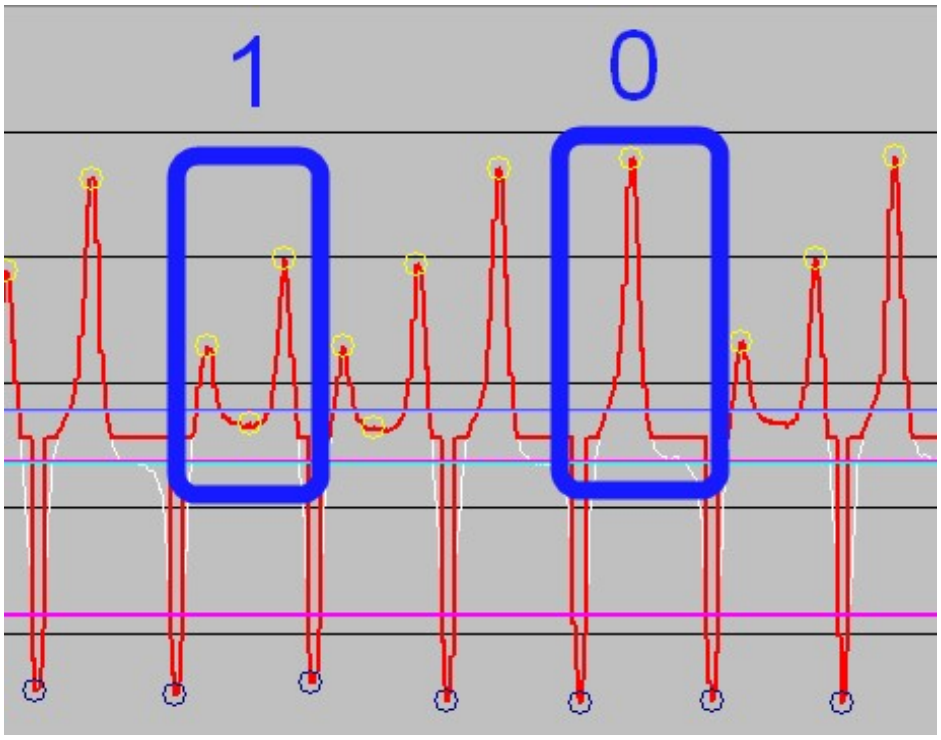
2)



3)



By carefully analyzing the band, it is possible to identify two types of configurations that follow one another (we have identified in this way the ways in which binary information is represented). Let's zoom in on the band and examine it in detail:



First of all, each information is contained between two negative peaks which thus constitute the clock of the signal. Specifically, between two negative peaks we can find two positive peaks or only one: if between two negative peaks we find only one positive peak then we have the information "0", if we have two positive peaks the information represented will be "1". In this way and for the entire band of the telephone card, the data is stored, bit by bit.

Let's try to hazard the following graph:

A) How the magnetic band is magnetized;

A ') The translation into Times of the three magnetic bands as if we were reading them one by one;

B) The sum of the three magnetic bands seen as if it were a single band;

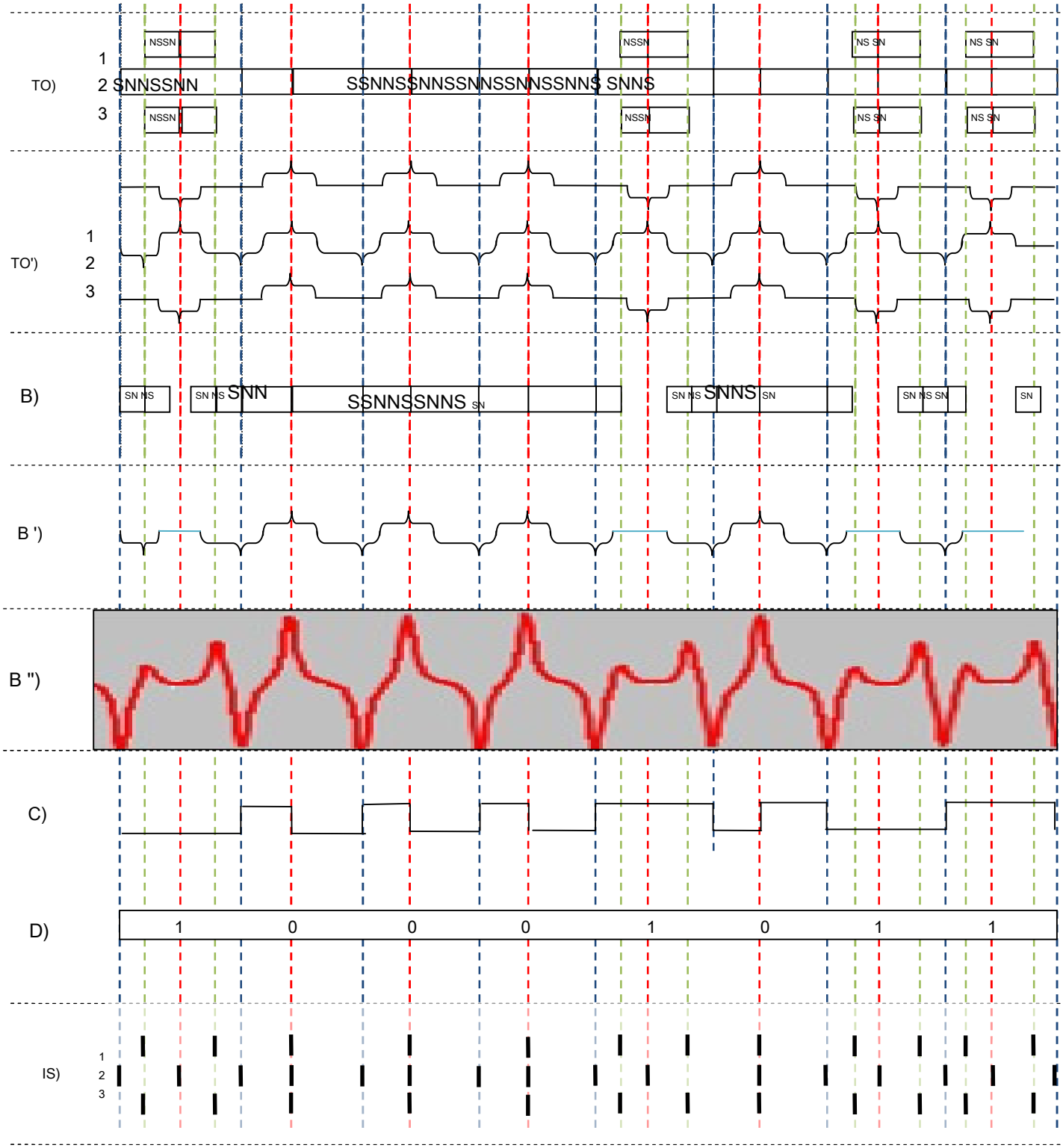
B ') The translation in Volts of the three magnetic bands read by means of a single head;

B ") What is actually being read by the magnetic head. B " is the only certain graph, all the others are hypotheses born on the basis of this;

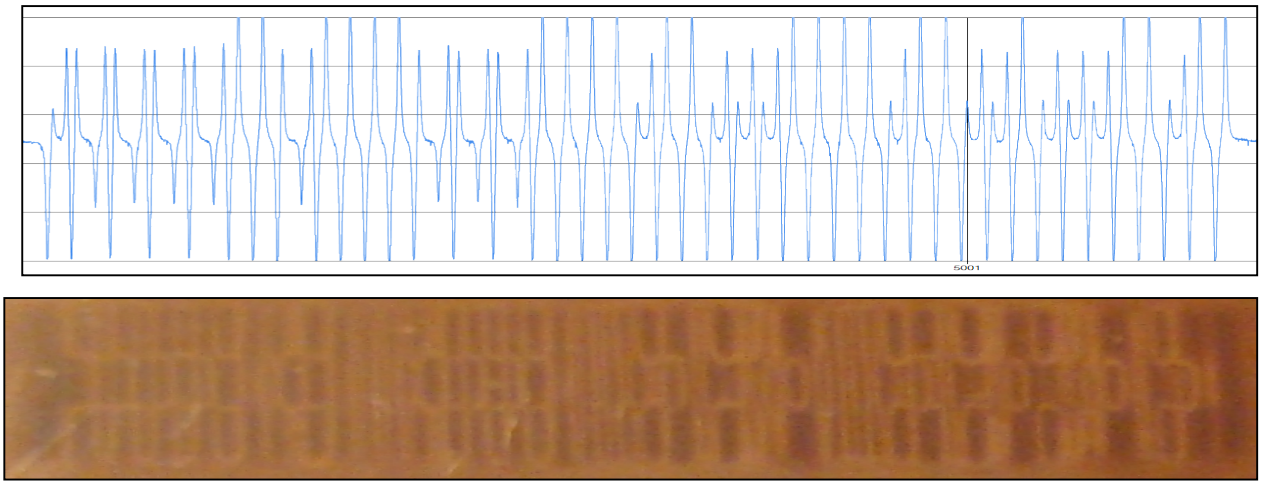
C) Translation in digital wave of the sinusoidal genal of B ';
D) Bit translation of the signal;
E) How the Arnold magnetic loupe magnetic strip is seen.

TabsLeaks

Everything you ever wanted to know about calling cards



Below instead I show the same card seen on the Arnold magnetic loupe and the translation in Volts of the same portion of band read by the machine



TabsLeaks

Everything you ever wanted to know about calling cards

Address book hosted by:

Schede Telefoniche .org

Recommended pages

Indemnify

Everything you will find in this document (photos, information, graphics, news, etc) is published for the sole purpose of information of collector interest, obtained on the basis of personal deductions and studies, sometimes inspired by information found verbally. None of the information contained in this document was found in violation of the laws in force or through the use of tools that are not permitted or restricted. No responsibility is assumed in relation to both the content and the use that third parties may make of it.

No content has an official nature nor is it confirmed by telephone companies or any other company / company / body / person named directly or indirectly within this document.

Gianfranco Marchese, Stefano Rossi and the Schetetelefoniche.org site, and all those involved in the drafting of this document, will not assume any responsibility deriving from incorrect use of what is written on it, including, by way of example and not exhaustive:

- materials contents in sites / documents of third parties reachable / reachable directly / indirectly from indications / links contained in this document;
- errors, inaccuracies and omissions which, however, are always possible. Therefore, we decline any responsibility for errors, inaccuracies and omissions that may be present on the site;

Therefore, the writers will not be required under any circumstances, for any reason whatsoever, to answer for damages, losses, damage to goods including data, or other economic or commercial losses, prejudices of any kind that third parties may suffer due to the contact made. with this document, or following the use of what is published therein, even if informed of the possibility of such damage, or if such damage is foreseeable.

This document does not constitute a newspaper; However, it is not periodic and is updated according to the availability and the availability of the materials (of the provisions, articles and materials contained therein). Therefore, it cannot be considered in any way an editorial product pursuant to Law no. 62 of

7.03.2001.