Part 1

Zappers –
Creativity in the Fraud Arena

Richard T. Ainsworth

NESTOA

Monday - October 1, 2012 (1:15 – 2:30)

Theme: Market-place

This is a Mid-size business issue

(1) Skimming has been an individual fraud issue, not a market-place issue

(2) Phantom-ware applications show skimming entering the market-place:

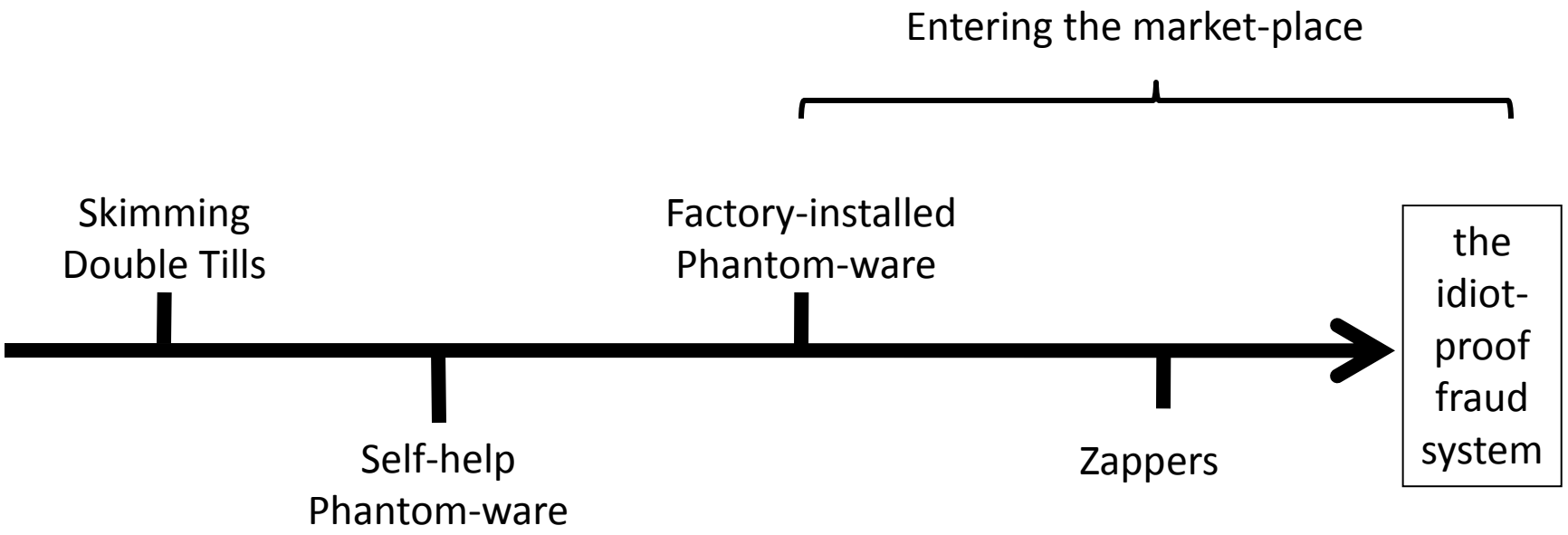
- Self-help phantom-ware
- Factory-installed phantom-ware

(3) Zappers developed next

- Installers, rogue developers, smaller developers

(4) Internet based programs

Development Time Line



Where are we going?

JUMP START by Robb Armstrong

Three US Zapper Cases & more ?

- Connecticut case – 1994
  - Custom made zapper (former NCR IT expert)
  - Zapper is kept in a hollowed out book in office
  - $17m (IRS income tax audit) – Customs uncovered
- Michigan case #1 – 2007
  - Zapper kept at owner's residence connected to ECRs at 13 restaurants
  - Skim $20m (4 years) sent to Hezbollah (Lebanon)
  - CIA mole (sister-in-law); wife in prison
  - Husband is fugitive from US (in Lebanon)
- Michigan case #2 – 2011
  - Installer (Journal Sales Remover program)
  - 2 strip clubs – over $500,00 gross sales
  - 5 years in prison (plea bargain – will talk

Ohio

US District Court, Northern District of Ohio, Western Division
3:12-cr-262-DAK (filed 5-22-2012)

- 18 people indicted - $3 million [Tarek Elkafrawi]
- FBI; ICE-HSI; Joint Terrorism Task Force [Egypt; Jordan; Lebanon]
- Change in POS (2010) – Internet access
- Two franchise fees [Equipment/land; royalty/advertising = 8% net sales].
- Manipulation of
  - Sales, payroll, false SSN, multiple SSN, 200+ illegal workers, underpaid for overtime, “New” system manipulation of hours worked, weekly central administration credit $2,300
  - Remote access to Ohio “new system” with “specific on-line software viewer” software from home computers – reset clock; manipulate cash transactions because tickets remained open; “new system” taken “off-line”

Found One

"I was able to see a zapper in person, interesting. I can not believe how easy it works."

- Icon [double click] + password
- Eliminate manually or automatic
- Maybe … 10 min.
- All ECRs must be off to re-index
- Installer identified (installed in 2008)
- Owner showed how it works
- Proof of deficiency difficult … estimates … will pay in full
- Will use Zapper for training …
  - Internally …… and on the road …..

State Legislative Activity 9/15

STATE	BILL	ACTION	STATE	BILL	ACTION
CT	HB 5421	Law	NC	SB 854	
FL	HB 7099	Veto	NY	SB 2854	
GA	HB 415	Law	OK	HB 2576	Law
IL	HB 6155		TN	SB 2194	
IN	HB 1337		UT	HB 96	Law
LA	SB 616	Law	WV	SB 411	Law
ME	LD 1764	Law			
MI	SB 768	Law			
MO	SB 840				

Talking & Researching

- Domestic (23):
  - ME, MA, CT, NY, WV, NC, AL, GA, FL, LA, TN, IL, IN, OH, MI, MO, OK, UT, TX, CA, WA, HI, WY
- International – Russian research institute:
  - Atlas Laboratory (cryptographic electronic journal) (36)
  - USA; Quebec; Sweden; Belgium; Ethiopia; Rwanda; Kenya; Serbia; Bosnia and Herzegovina; Macedonia; Montenegro; Bulgaria; Romania; Germany; Poland; Ukraine; Hungary; Venezuela; Puerto Rico; Chile; Ecuador; Brazil; Argentina; Greece; Italy; Croatia; Malta; Bangladesh; Netherlands; Ireland; Dominican Republic; Portugal; Norway; Iceland; New Zealand; Australia.

Solutions

- Penalize the Installer
- Do a sting with a false restaurant
- If there are privacy concerns with comprehensive technology solutions, opt for
  - severe (limited) enforcement (Oklahoma)
  - broad (conditional) enforcement (Missouri)
  - “bad apple” enforcement (New York)
- Split credit card payments

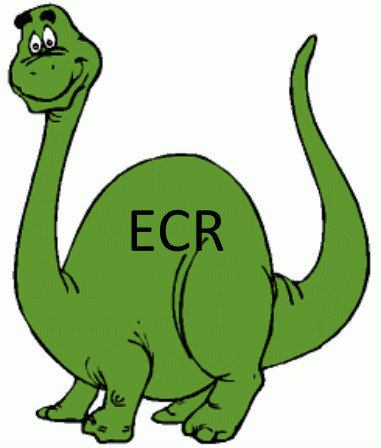
  - Ecuador, Russia, Turkey, Argentina, Brazil, Peru, Chile, Uruguay, Austria, Mexico, Colombia, Guatemala, El Salvador, Dominican Republic, and Costa Rica.

Problems

- Current technology solutions require a receipt

http://www.skatteverket.se/privat/kvitto/webbfilmedengelsktext.4.71004e4c133e23bf6db80003181.html

- Internet-based Zappers [Zapper-as-a-Service]
  - Six cases in Portugal
- Zappers have migrated into credit cards
  - United Kingdom, Portugal & Norway
- tablets/phones/hand-held devices
  - The ECR is a dinosaur
  - Big retail stores, hardware stores, coffee stores are moving away from ECRs …



Further Reading

- **An American Look at Zappers: A Paper for the Physikalisch-Technische Bundesanstalt, Revisionssicheres System Zur Aufzeichnung Von Kassenvorgängen Und Messinformationenthe http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2026140**
- **Zappers & Phantom-Ware: A Global Demand for Tax Fraud Technology http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1139826**
- **Zappers: Tax Fraud, Technology and Terrorist Funding http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1095266**

Thanks

- Richard T. Ainsworth
- ADP
  - Richard.Ainsworth@adp.com
- Boston University
  - vatprof@bu.edu

Part 2

Supplemental Slides

- Phantomware
- Details of a Zapped transaction (from a Swedish Zapper)
  - 11 slides
- 9 Ways to find a Zapper
  - 11 slides

Phantom-ware

There are two types:

Self-help

Factory Installed

Type 1 – Self-help Phantom-ware

- Modern ECRs can be re-programmed to eliminate the audit trail (critical records)
  - Z Reports (daily/periodic) – end of day report that records sales, taxes, media totals, discounts, voids, etc.
  - X Reports – same as Z Reports except they do not "reset" the system after being taken.
  - Electronic Journal – records all transactions (blow-by-blow) entered in the machine
- Programming is "secret" (not in user's manual) – limit access [bad employee issues]

Big coffee store...

Type 2 – Factory installed Phantom-ware

- Does not require re-programming
- Secret (hidden) functionality built in to ECR
  - Not discussed in user's manual
  - Not visible in menu structure
  - Commonly revealed only in oral communications with
    - » Installer
    - » Sales representative
- The idea is to remove the need to re-program
  - – Manufacturer looses "deniability"
  - – These programs have only one function

Zappers

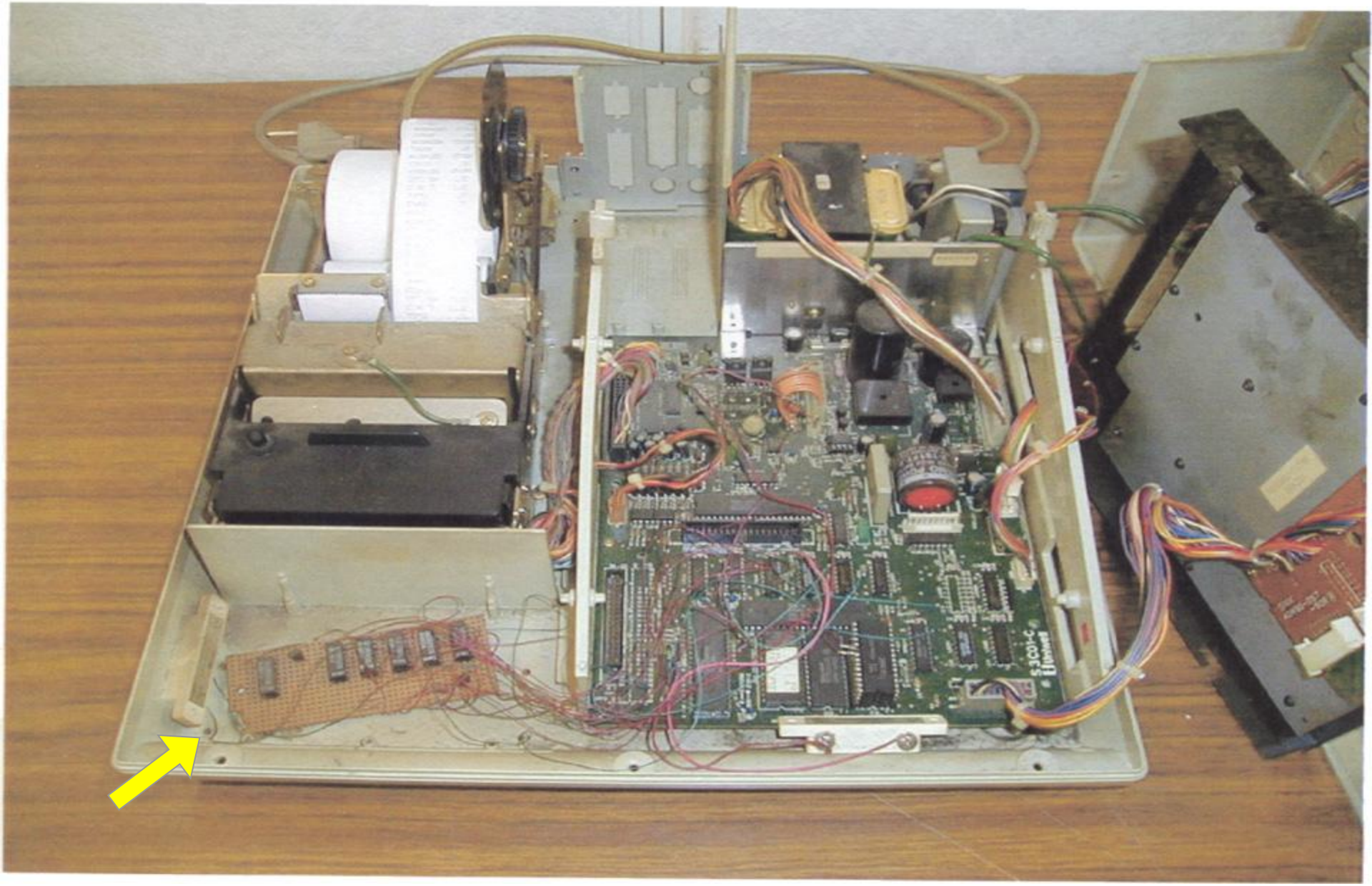
There are three generations

Zappers Past; Zappers Present; Zappers Yet to Come

Zapper from the Past

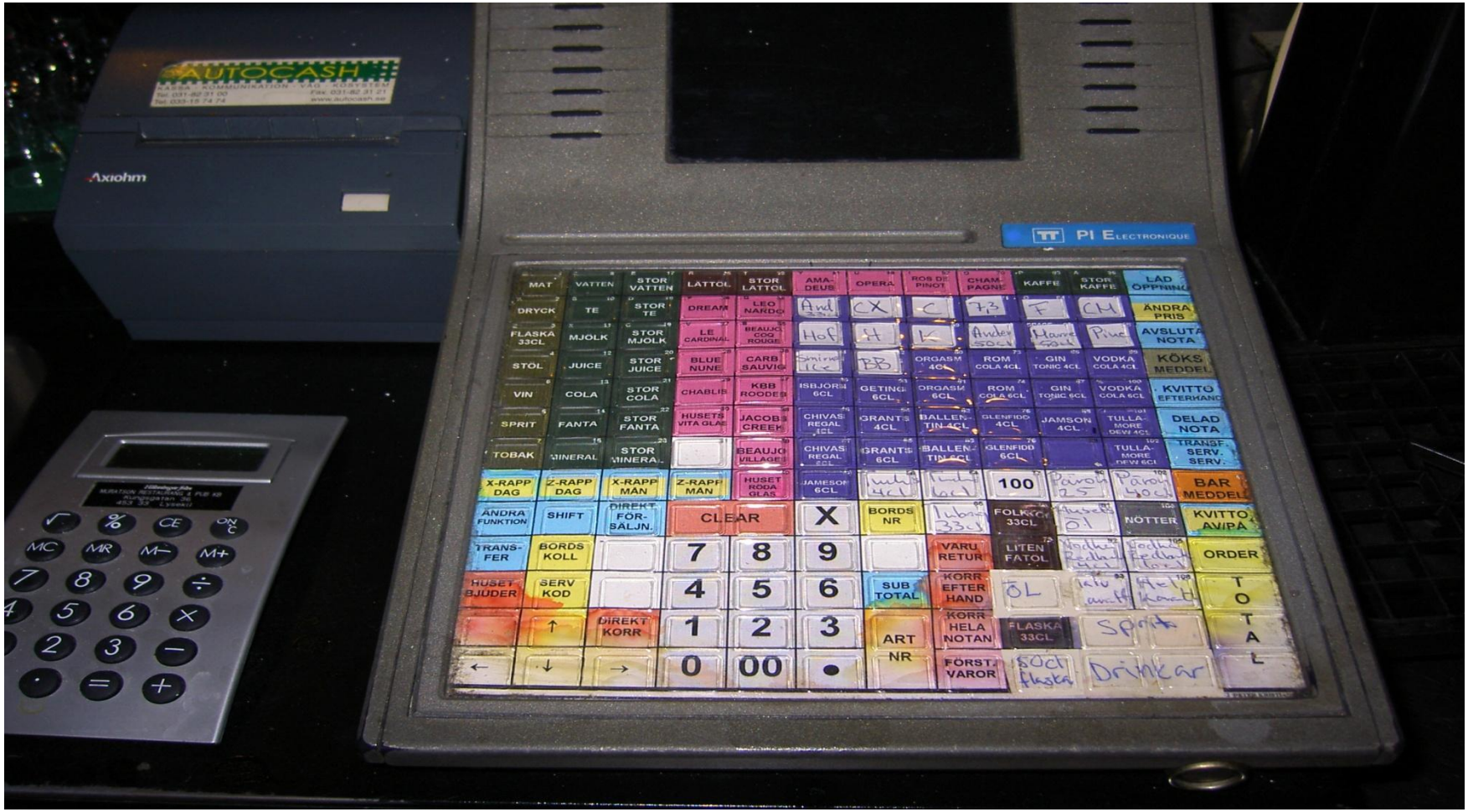
- This is an old Quebec Zapper. It has been "hard wired" into the ECR. The picture shows the top of the ECR removed, and the yellow arrow points to the device.
- When Zappers are added to ECRs this way it is very easy to find them.
- People only do it this way in jurisdictions that are not looking for them.

C00003.jpg (1280x960x16M jpeg)



Contemporary Zapper

Note: this Swedish zapper requires a lot of manual intervention.



A specific brand of cash register (blood)

Manufactured in Paris (since 1983)

Popular in Italy, Belgium, Portugal, Spain, Germany, Denmark, Australia, USA and North Africa.

Uses “Specific kind of” back-office program

Cash register is connected to a PC (in the back office) like the one on the following slide.

Back-Office PC

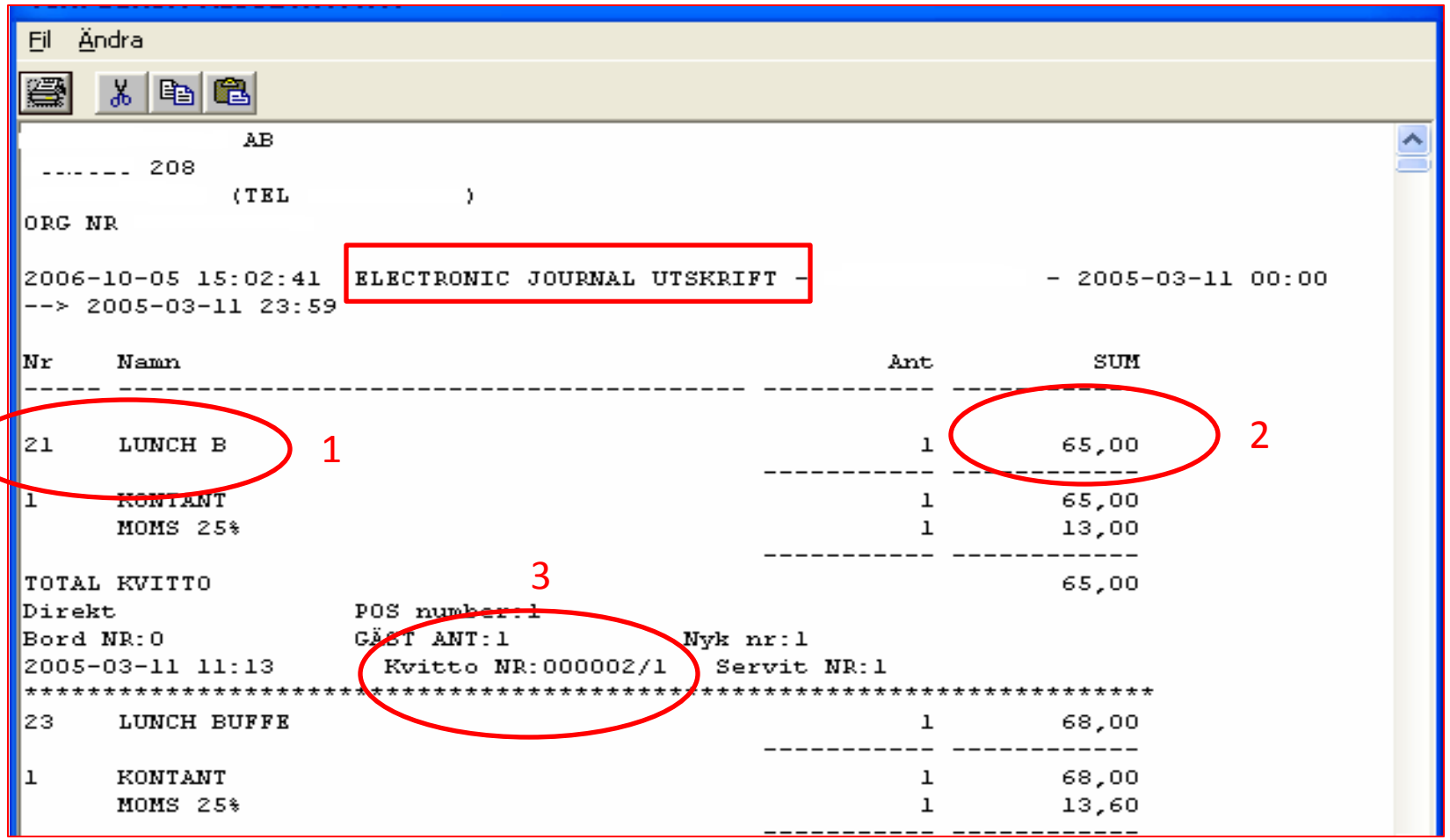
Notice the “dongle” (grey memory stick) protecting proprietary program

Notice the silver memory stick – this is the “zapper”

Restodata is programmed to automatically download all information about all transactions from all cash registers every morning at (for example) 5:00 am

Details of a “zapping” from Sweden

So, before manipulation here is the
electronic journal
the sales report
the sales receipt



Electronic Journal (before manipulation)

1. Item number 21 is a Lunch B
2. It cost 65,00 kroner
3. The receipt is number 2/1

AB

ORG NR.

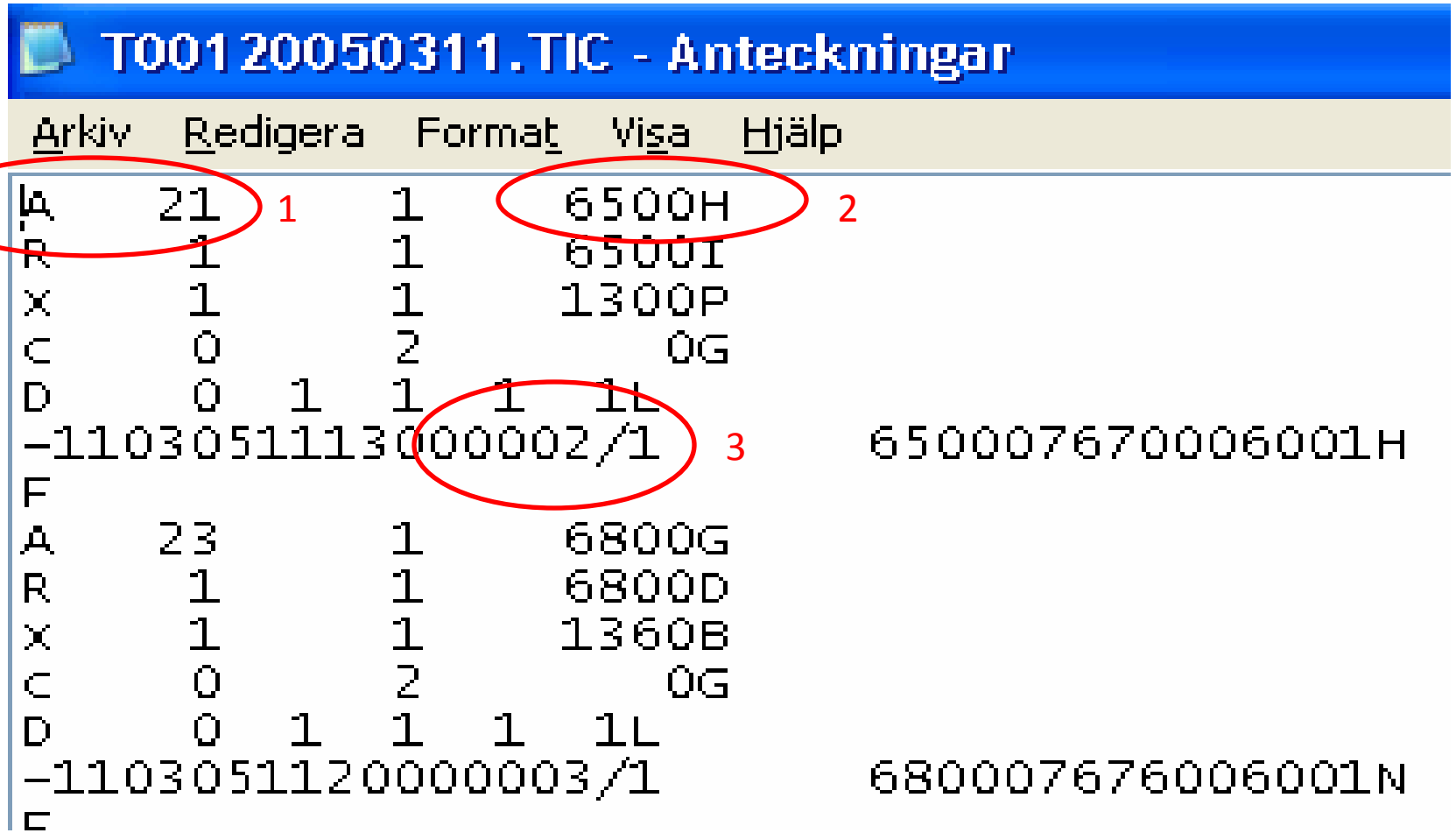
Förs.per familj

2005-03-11 till 2005-03-11

Namn	SUM
Unknown family	693,00 kr
AVHÄMTNING	1 701,01 kr
DRINK	340,00 kr
DRYCK	1 026,00 kr
MAT	19 981,00 kr
SPRIT	669,00 kr
STARKÖL	13 492,00 kr
VIN	3 144,00 kr
TOTAL	41 046,01 kr
Out of SALES :	0,00 kr
Rabatt :	-209,70 kr

Sales Report (before manipulation)

We need this for comparison later



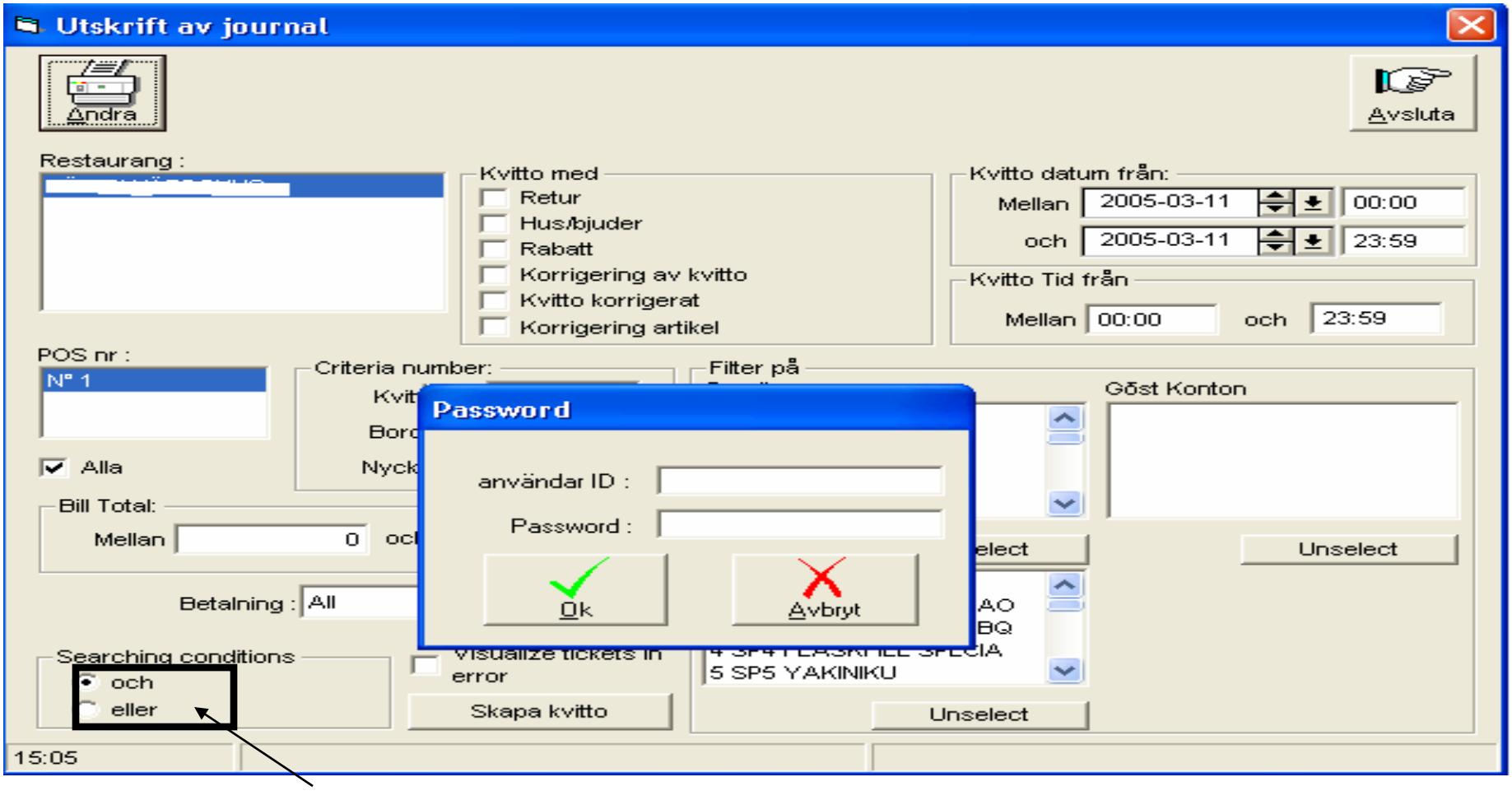
Sales receipt (before manipulation)

These are in the ".TIC" files (for "tickets"). Notice:

1. Item number 21
2. Sales price of 65,00 kroner
3. Ticket number (receipt number) 2/1

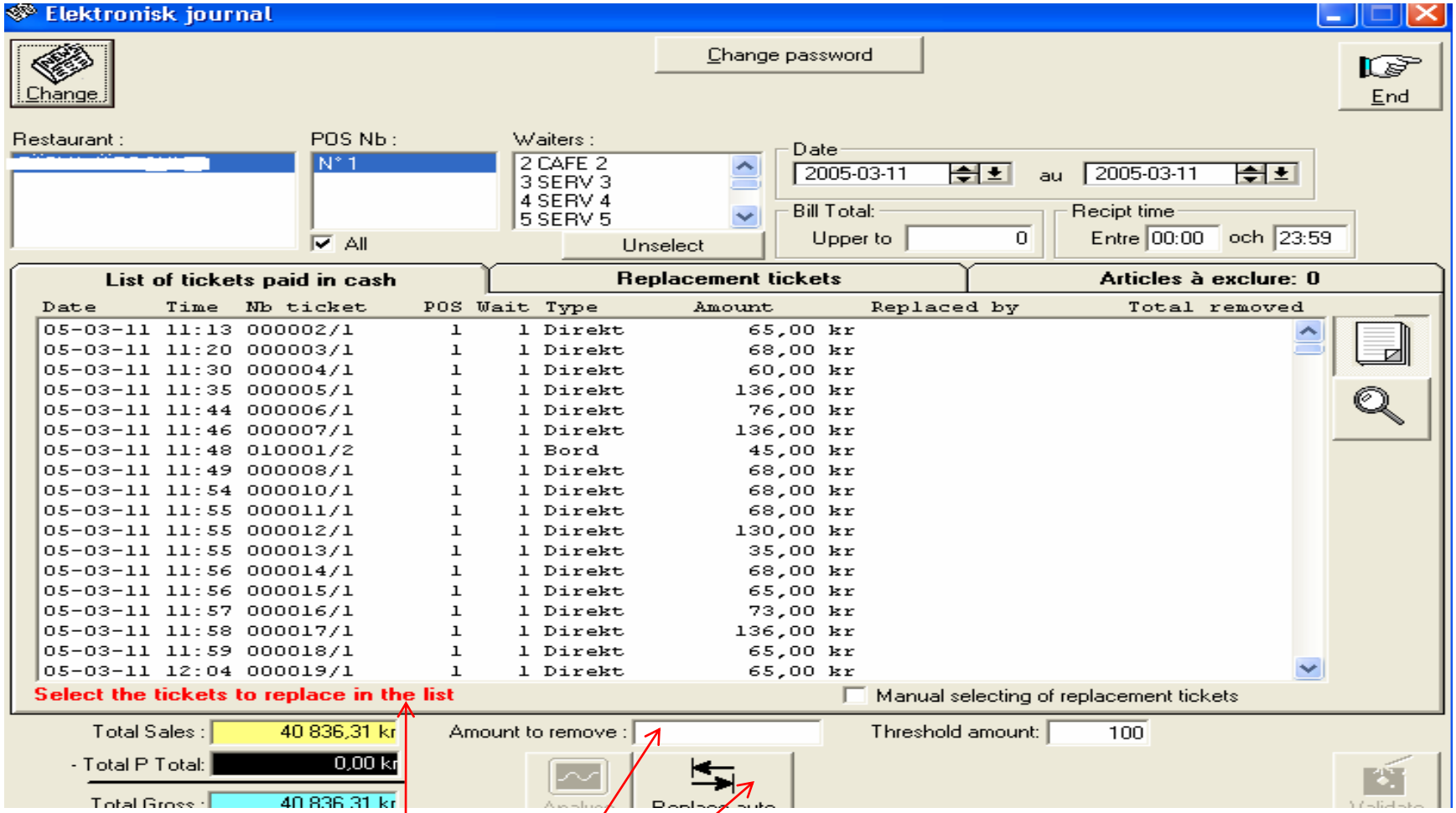
To manipulate the data you insert the zapper (silver memory stick)

There is a new version of the CMDCAR.DLL program on the zapper



Double-Click on the secret module

It is not all that apparent what you need to do here, but by double clicking in the box in the lower left, entering an ID and a password, you will get to the next screen – the Electronic Journal (which can be adjusted).



“Manipulate-able” Electronic Journal

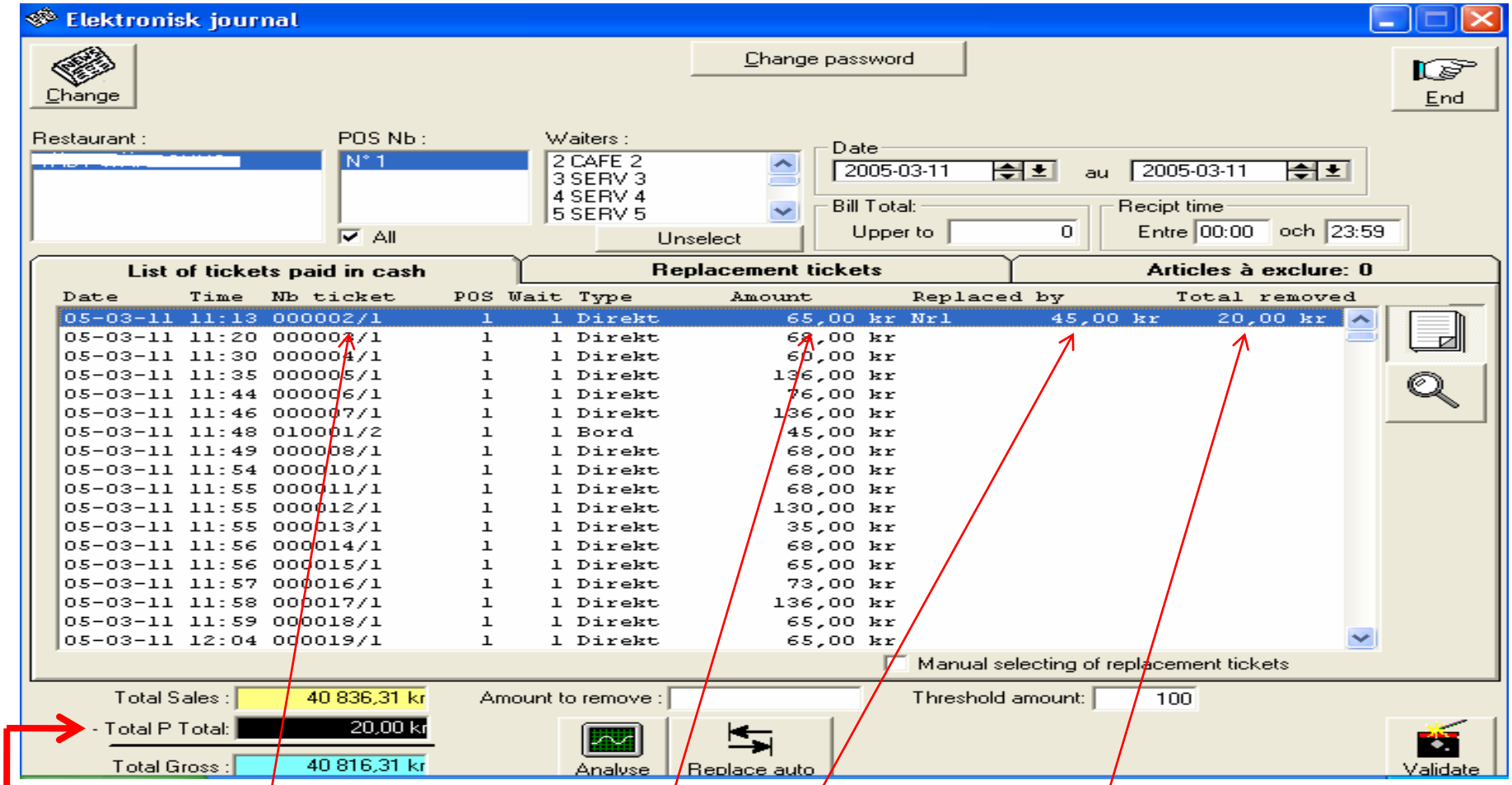
Notice that we can either

(1) select a ticket to adjust, or

(2) auto-replace

So, assume we take the selection of a ticket approach … (1),

When we select the first item (ticket number 2/1) we then get …

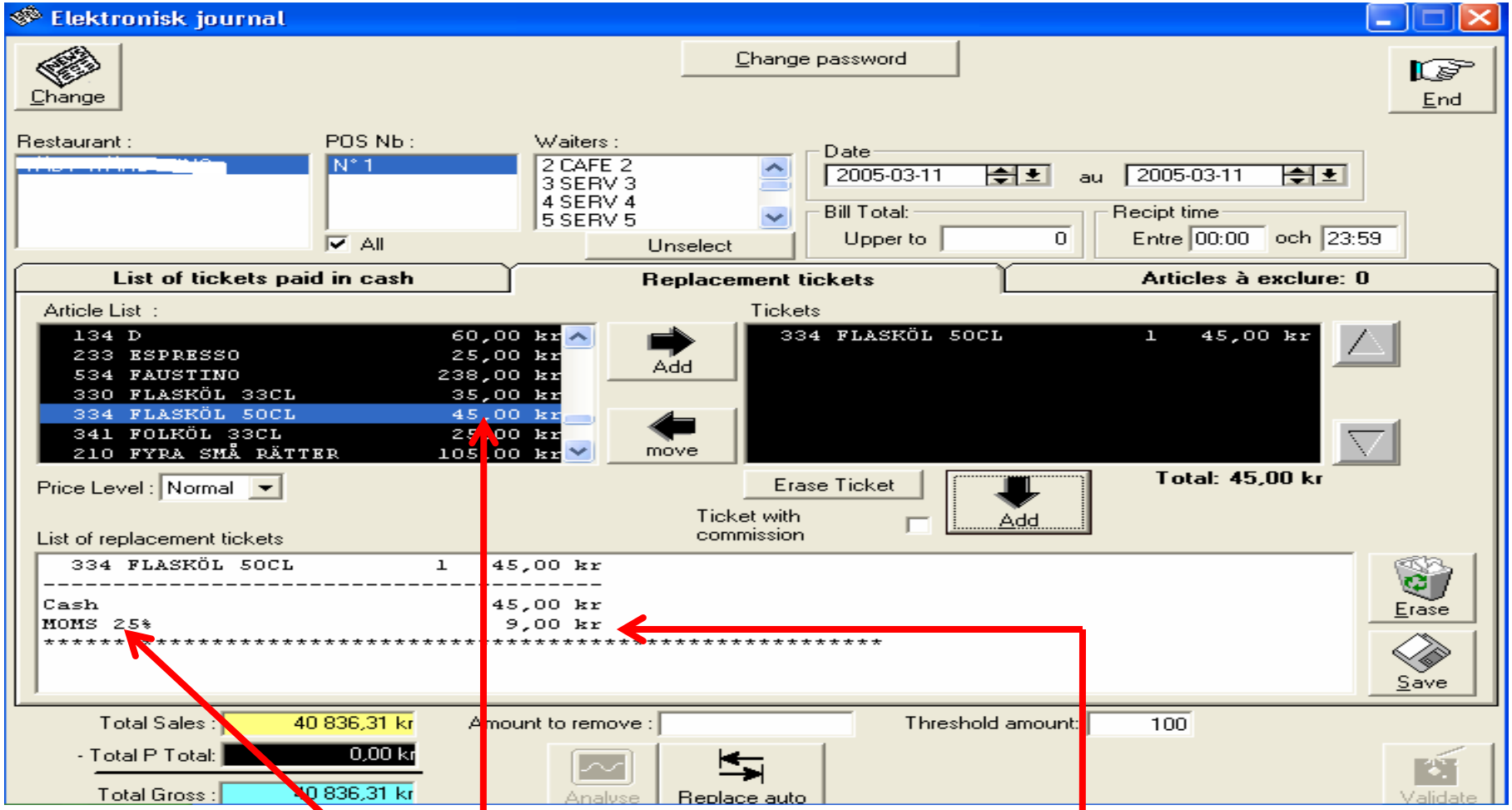


Manipulated Electronic Journal (pro-forma)

Here is what we have done so far – is this enough manipulation?

Ticket 2/1 has been changed from 65,00 to 45,00 with a reduction of 20,00 on this ticket

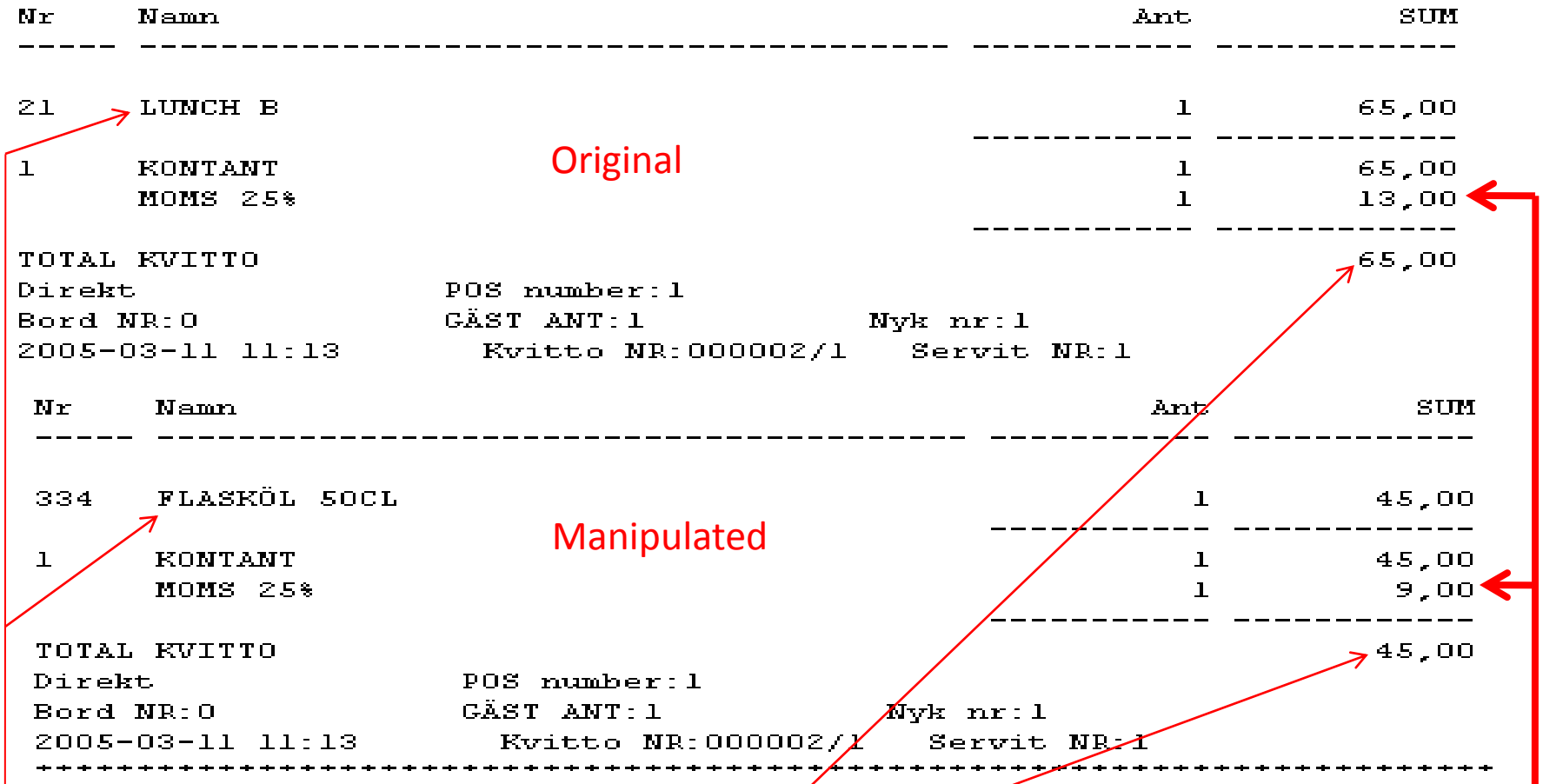
There is a running total kept (in case you want to remove more)



Replace the Lunch Buffet (65,00) – with a beer (45,00)

Notice the price reduction (we could have gone lower) – Notice the tax reduction

The Swedish VAT is at 25%



Nr	Namn	Ant	SUM
21	LUNCH B	1	65,00
1	KONTANT	1	65,00
	MOMS 25%	1	13,00
TOTAL KVITTO			65,00

Direkt POS number:1
Bord NR:0 GÄST ANT:1 Nyk nr:1
2005-03-11 11:13 Kvitto NR:000002/1 Servit NR:1

Original

Nr	Namn	Ant	SUM
334	FLASKÖL 50CL	1	45,00
1	KONTANT	1	45,00
	MOMS 25%	1	9,00
TOTAL KVITTO			45,00

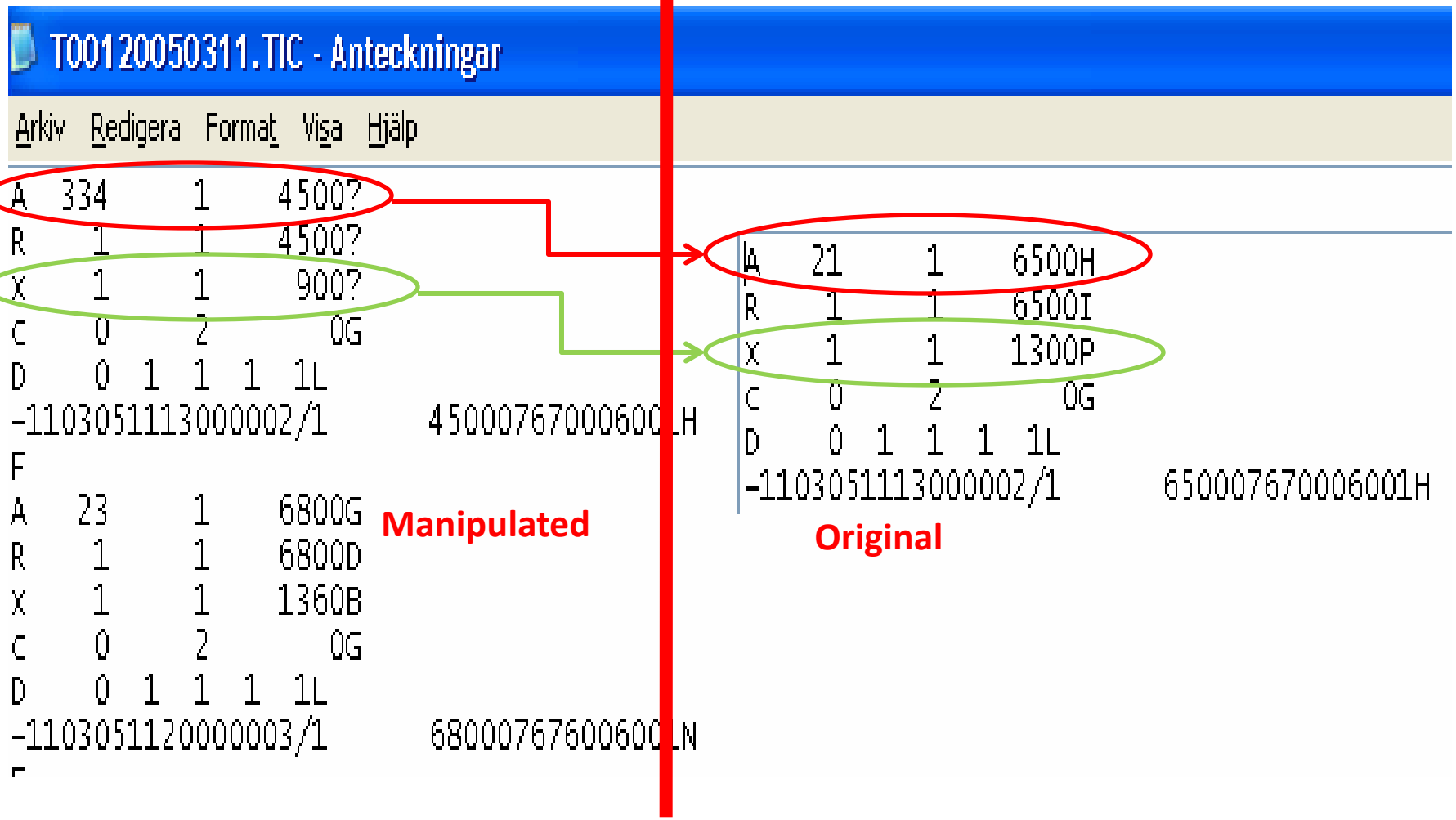
Direkt POS number:1
Bord NR:0 GÄST ANT:1 Nyk nr:1
2005-03-11 11:13 Kvitto NR:000002/1 Servit NR:1

Manipulated

Comparison: Original & Manipulated Electronic Journal

Notice the reduction in gross sales & the reduction in tax.

If this record is tied into inventory control, adjustments in related purchases will be necessary [some zappers will do this for you] because you may have just “sold” more beer than you ordered



Comparison of the TIC-files – Manipulated & Original

Notice the "?" in the Manipulated version in contrast with the letters "H", "I" & "P" in the original version. This one of the tell-tale signs of manipulation in this particular program. It may indicate that the system has not been correctly updated since the manipulation procedure.

Supplement 2

9 Ways to find a Zapper

How do you find Sales suppression devices?

- 1. Stealth visits before audit
- 2. Set up a dummy store
- 3. Detailed examination of ECR printouts
- 4. Concentrate on “high risk” businesses
- 5. Audit lead from a different “rigorous audit”
- 6. Audit lead from another jurisdiction
- 7. Find and follow the corrupt installer
- 8. Work collaboratively with absent owners
- 9. Read the 250 Quebec cases in your spare time to learn the fact patterns … and other stuff …

1. Stealth visits before audit

- This is how Revenue Quebec found its first Zapper in 1997
- Auditor visited a restaurant before opening an audit, saved her receipts, and looked for records in the TIC files of the ECR.
- Requires some luck

2. Set up a dummy store

- This is what the Canadian Broadcasting Corporation did in Montreal.
- ECR salesman approached CBC and explained factory-installed Zappers
  - Company was subsidiary of a US ECR distribution business
  - Salesmen actually gave interviews to CBC
- Connecticut has reported the similar activity in complaints by “honest” ECR sales people

3. Detailed examination of ECR printouts

- Swedish approach
  - There is a Swedish ECR lab in the government's training facility that has a number of corrupted ECRs for practice & training of auditors
- South Carolina attorney looking for this kind of evidence in court case
- Requires knowledge of ECR programs – they are specific to ECR types not generic

4. Concentrate on "high risk" businesses

- Not:
  - If Mom or Pop runs the cash register
  - If publicly held enterprise
- Yes:
  - If multiple locations with a remote but actively engaged owner [La Shish (Detroit); Ronan (Australia)]
  - Employees are paid wages under the table
  - Unusual ratio of cash-credit transactions

5. Audit lead from a different "rigorous audit"

- Zappers leave a cash hoard that is difficult to dispose of – don't stop with the initial audit, push to find the Zapper:
  - Audit shows that many employees are paid in cash [Dudok (Netherlands)
  - Cash taken off shore- US Customs [Stew Leonard's Dairy (CT)]
  - Cash sent to Hezbollah – Homeland Security [La Shish (MI)]
  - Normal lavish lifestyle evidence [Aleef Garage (UK)]

6. Audit lead from another jurisdiction

- Ontario picks up leads from Quebec
- New York should do the same with Quebec
- Frequently the devices spread in ethnic communities that have business ties to jurisdictions where this fraud is common [Brazil; Venezuela; Quebec]
  - Austria & Germany found similar Zappers in 600 Chinese restaurants – started in Austria with a Chinese grad student in a technology school – Germany followed the Austrian lead on audits

7. Find and follow the corrupt installer

- Revenue Quebec uses search warrants against installers simultaneously with a search of a restaurant.
  - Dudok (Netherlands) installers are correcting the system during an IRS audit to hide data
  - Boutique programmers – makers of specialty cash register programs [Roy (Quebec)]

8. Work collaboratively with “absent” owners

- Absentee owners can be victims of the management company [Celine Dion (Quebec)].
- Franchise holders [McDonalds; Burger King; Duncan Donuts] that get a royalty per sale in the store [Cincinnati, Ohio (2007) – IRS]
- A business that hires too many computer savvy students could be a victim.

9. Read the 250 Quebec cases in your spare time to learn the fact patterns

- Revenue Quebec publishes summaries of all the ongoing cases on the web.

- Go to: http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiques/ev-fisc/2008/janvier.asp