

nagra|star

90 Inverness Circle East
Englewood, CO 80112
303-706-5704

REPORT OF INVESTIGATION WITH REFERENCE TO

ANTHONY J. MALDONADO
5128 EAST ROBERTA DRIVE
CAVE CREEK, AZ

AND

PAUL THOMAS ST. JAMES
BARGAINTOWN LIQUIDATION
3401 WEST BUCKEYE ROAD
PHOENIX, AZ

FOR

Mr. Alan Guggenheim
CEO
Nagra|Star
90 Inverness Circle East
Englewood, CO 80112
303-706-5707

This report is confidential and is intended solely for the individual named above. If the information herein is disseminated, Nagra|Star does not accept any liability. Copy to the appropriate agency records.

March 23, 2001

Matter
Fi
Nortel Network/Denv

HIGHLY CONFIDENTIAL

Case No. SA CV03-950 DOC (JTL)

Exhibit No. 272

CASE NO.
SA CV 03-950 DOC (JTLx)
ECHOSTAR SATELLITE CORP., et al.,

vs.

NDS GROUP PLC, et al.

DEFENDANT'S EXHIBIT 374

DATE _____ IDEN.

DATE _____ EVID.

BY _____
Deputy Clerk

nagra|star

90 Inverness Circle East
Englewood, CO 80112
303-706-5704

REPORT OF INVESTIGATION WITH REFERENCE TO

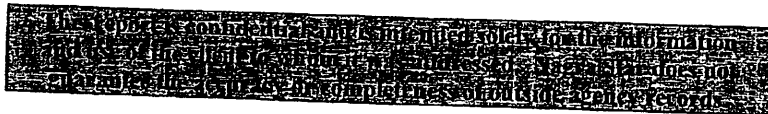
ANTHONY J. MALDONADO
5128 EAST ROBERTA DRIVE
CAVE CREEK, AZ

AND

PAUL THOMAS ST. JAMES
BARGAINTOWN LIQUIDATION
3401 WEST BUCKEYE ROAD
PHOENIX, AZ

FOR

Mr. Alan Guggenheim
CEO
Nagra|Star
90 Inverness Circle East
Englewood, CO 80112
303-706-5707



March 23, 2001

Exhibit No.:	374
Deponent:	Geist
Date/APR:	5-30-01
Hunter + Geist, Inc. 68	

Matter #: 802897-1
File #: C10002
Nortel Network/Denver, Colorado

HIGHLY CONFIDENTIAL

Case No. SA CV03-950 DOC (JTL)

ESC0113659

SUMMARY

Mr. Maldonado was using illegal satellite reception equipment of both EchoStar Communications and DirecTV for the theft of satellite signals of both companies.

Regarding EchoStar Communications Mr. Maldonado was modifying the receiver's TSOP and modifying smart cards to receive free satellite subscription service. He said the software he was using was Sorry Charlie and Winexplorer 4.4. Later in discussions he also admitted to using Prog as the primary modification software and activationhex. Mr. Maldonado said that this software was on his computers located at Bargaintown Liquidation. Mr. Maldonado said he does not use a blocker or an AVR for his television reception. Mr. Maldonado estimated that he had modified at least 60 receivers and cards to receive satellite signals illegally. All of the receivers had already been sold, or were ready to be shipped to a buyer in Nogales, NM.

Regarding DirecTV, Mr. Maldonado was asked where he received his DirecTV H and HU cards. He said they were purchased from pawnshops for about \$30.00 each with the receivers. He could not recall where he purchased the receivers. Mr. Maldonado said he would take the image from the H cards, which he read with BasicH; work in the 8000 area of the card and place the info onto a floppy. He said he was running a WTX (wildthing extreme) inside of a 486 computer he was using as an emulator for his DirecTV signal reception. Mr. Maldonado stated that he has had a subscription for 3 years to DirecTV in which he pays \$24.00 a month.

Matter #: 802897-1

File #: C10002

Nortel Network/Denver, Colorado

DETAILS

Investigator Gee accompanied Special Agents from the Phoenix, AZ office of the Federal Bureau of Investigations and the United States Postal Service on a raid on Mr. Anthony Maldonado's residence the morning of March 22, 2001. Federal authorities conducted the initial entry and search of the premises. Investigator Gee was notified that he could enter the premises to assist in the search and interview of Mr. Maldonado after authorities deemed it was safe to enter. SA Steve Belongia informed Mr. Maldonado that he was not being arrested nor detained and could leave at any time. Mr. Maldonado understood what SA Belongia was stating to him and agreed to speak to him concerning satellite signal theft.

Prior to the interview SA Belongia and Investigator Gee turned on Mr. Maldonado's big screen Sony television and the Dish Network Satellite system located in the living room off of the kitchen. The first channel that came up was channel 521 a pay per view account. Investigator Gee changed the channels to view channel 520 and 522. Each of these channels was a pay per view channel in which the signal was being received.

Mr. Maldonado was asked if he had a subscription for the services he was receiving and he said he did not. Investigator Gee checked the smart card within the receiver and noted the UA # as S0007616386 96. Investigator Gee later removed the card from the system and obtained the following information from the receiver.

RA # = 002799 4152-60
Smart Card ID = S0007616386-96
Software Version = P102CCJD-N
Location ID = 2DCD400E

A second card and receiver was confiscated at Mr. Maldonado's residence.

Card #: S0006846151 64
Receiver #: R0025986605

Investigator Gee asked Mr. Maldonado what zip code he was using and he was informed that he was using a Las Vegas zip code. The reason stated was that he knew the Las Vegas area received the Ecstasy channel and that is what people wanted when they purchased cards from him.

During the interview Mr. Maldonado stated that he was a System Administrator for Motorola, Inc.

Matter #: 802897-1
File #: C10002
Nortel Network/Denver, Colorado

Computers identified on the property were his laptop computer, two computers in his office in which one was Mr. St. James server for his website, one 486 computer in his bedroom which was an emulator for DirecTV satellite signal theft, one 486 computer in his vehicle and one 133 mhz computer in his living room in which he was using as an MP3 server with a 20 gig hard drive storage system. The computer being used to pirate DirecTV satellite reception did not have a smart card inside of it. Mr. Maldonado had modified his television to receive the emulation from the computer. When Mr. Maldonado discovered that his television was being confiscated by the authorities he stated that he tore it apart to fix a problem with it and never put it back together. Mr. Maldonado said that he has had the basic \$24.00 subscription to DirecTV. When asked why he still subscribed, he said he has had the subscription for 3 years and just never got rid of it.

Following this statement he asked why are you coming after me, why don't you go after the people on the websites posting how to do the stuff for free?

Mr. Maldonado said he met Mr. St. James 3 years ago. Mr. St. James advertised in the newspaper looking for technicians to repair equipment. Mr. Maldonado said that he would repair computers, televisions and other electronic equipment to be sold on Ebay by Mr. St. James. Mr. Maldonado also said that he worked on Bargaintowns website. Bargaintown is the business that Mr. St. James owns.

Mr. Maldonado initially stated that he learned everything he knows off of the Internet.

He said that he mostly uses it for personal use. Initially he said that he had maybe done a few cards for some friends. The last card that he modified and sold was done last week. By the end of the interview Mr. Maldonado admitted to modifying at least 60 receivers by removing the TSOP and reading the chip and making modifications to virgin cards. He said the virgin cards were needed and a Dish500 system was required in order to receive all of the satellite signals. He said he would use code line BSMV1. Mr. Maldonado said he didn't feel right about what he was doing and planned on getting out of the business after this last shipment of 20 receivers. The shipment would allow them to make the final \$5,000 of their \$25,000 investment.

When asked where he got the code he said he purchased it for \$25,000 from a guy named Jim LNU in Barrie, Ontario. Jim is described as being 5' 4", brown hair that is receding, brown eyes, 30-35 years old, and a mustache that has a space in the middle that is off to the side. Jim's nicks are dssking and dsschat. Mr. Maldonado's nicks are destnee, tigerider and sat-man. The websites Mr. Maldonado met and chatted with Jim are www.hitecsat.com, www.canuck.com and irc.canuck.net. Mr. Maldonado initially said that he thought that Jim quit about three weeks ago, but later said that he had been on vacation and was expected to hear from him again about 20 more receivers in a couple of weeks.

Matter #: 802897-1

File #: C10002

Nortel Network/Denver, Colorado

Jim's address that was being used is
Discount Distributors
336 Yonge, #345
Barrie, ON L4N 4C8
Cellular Phone: 705-715-1545

Jim is also using an address in Albany, New York, but investigator was unable write down the address. The address is in the custody of the FBI.

Mr. Maldonado said that all addresses are on his computer obtained from his office upstairs.

Payment of the \$25,000 was paid out of two accounts of Mr. Maldonado. One half came out of his personal account and the other half from his business account, baud_father. The money was given to him by Mr. St. James, which was paid on a company check from Mr. St. James's account. Mr. Maldonado's business, baud_father, comprises of web development and working on equipment.

Mr. Maldonado and Mr. St. James made two trips up to Canada in October and November of 2000. The first trip he received a brown box which allowed him to modify the cards and sale them. The box was described as having cables, 3 LED lights in front and using software PROG to make modifications.

He said the software he was using was Sorry Charlie and Winexplorer 4.4. Later in discussions he also admitted to using Prog as the primary modification software and activationhex. Mr. Maldonado said that this software was on his computers located at Bargaintown Liquidation. Mr. Maldonado said he does not use a blocker or an AVR for his television reception.

He said that after two weeks of owning the box received from Jim, Dish Network sent an ECM that took out their capabilities of modifying cards. He said that Jim then sent him the code that he currently was using to modify the cards he was selling to date and the card in his receiver in the living room had the code on it too.

Mr. Maldonado stated that he needed to receive Dish500 systems and the only way he was able to do that was by contacting a person named Julie LNU or Diane LNU in Canada who Jim referred him to. Mr. Maldonado said when he initially contacted Julie she said she could not help him. He said he immediately called Jim who called Julie. He said the next time he called she helped him.

Mr. Maldonado said that Julie told him that they receive the receivers and satellites directly from EchoStar. He said he did not know how, but was told this from Julie. Mr. Maldonado said the shipments are sent to him via UPS.

Matter #: 802897-1
File #: C10002
Nortel Network/Denver, Colorado

Mr. Maldonado said that they, himself and St. James, gave the receivers and cards they modify to a Mexican in Nogales, NM. Mr. Maldonado said he did not know who the Mexican was, but he said St. James would. Mr. Maldonado said the Mexican was selling the receivers and cards to people in Mexico and that is all that he knew.

Investigator Gee asked Mr. Maldonado if he was familiar with the nick Nipper? He said that he was and also knew him by the name of Nipper Claus too. Investigator Gee asked him if he knew who Nipper was. Mr. Maldonado believed it was either Jim or Jim's engineer, but he was not sure. He only knew that it had to be someone who was very knowledgeable of the card and Jim seems to have that knowledge.

Mr. Maldonado said that he was only able to 'unloop' the 01 and 02 cards. He said that he thinks the 09 cards could be 'unlooped' by Jim. Investigator Gee asked him how he knew this. He said that he didn't know for sure, but thought that he could, he added that if he couldn't, he was close. Investigator Gee asked Mr. Maldonado if he was cloning or emulating any cards or signals. He said that it couldn't be done; the conditional access system was too good.

When asked where he received his DirecTV H and HU cards, he said he purchased them from pawnshops for about \$30.00 each with the receivers. He could not recall where he purchased the receivers. Mr. Maldonado said he would take the image from the H cards, which he read with BasicH, work in the 8000 area of the card and place the info onto a floppy. He said he was running a WTX (wildthing extreme) inside of the computer he was using as an emulator for his DirecTV signal reception.

Mr. Maldonado said he was flashing the Atmel chips through his serial port. He said he purchased the device to do this with from Europe, an MK14 that he has had for 1-1/2 years. Investigator Gee asked him if he had purchased or used a VX Maxi or MX Mini from Europe and he said he had not heard of either one.

Mr. Maldonado was asked if he had ever used any of the Motorola equipment to look at the chip on the card, i.e., an electron microscope. He said that he never did and also did not believe Motorola had that type of technology at their facility.

Mr. Maldonado said that he went to college at the University of Phoenix, MCC (Mesa Community College??), and received most of his training from Motorola regarding computers.

Matter #: 802897-1

File #: C10002

Nortel Network/Denver, Colorado

ATTACHMENTS

1. Search Warrant issued by the State of Arizona
2. Search Plan of the Federal Bureau of Investigations

Matter #: 802897-1

File #: C10002

Nortel Network/Denver, Colorado

desktop -

Paul's server -

MP3 server -

Chan SZ2
SZ1
SEC } PPU
open

SAdmin - network

bought farm - Paul

that's all he did he said -

met Paul - worked in tech

Built website, bought books group,

6

486 in ~~the~~ bedroom - ^{evolution}
486 in garage (vehicle

computer in room (2)

- UA -

modified

computer running 486 in
bedroom controls Direct TV
under rock in front.
no card -

4

off of the internet learned
how to modify cards.

mostly personal use
prior to busts - knew someone
selling them.

1 year ago friend ^{was}
Gosh, guns, etc. Electron
shop on Mt. Dewell

personally doesn't know how
to write code -, reverse
engineer,

buy 1 sold over 5000

add in the program met 3
years ago

on payroll - cash, co. checks

development exp., contracts,
testing

Gargantuan website
design

at 4.0 + 2000, ^{UM} ~~at that~~

7

advised - mentioned that
were a lot

- unsure about Check (revenue)
whether to subscribe or
not to DirectTel \$24.00 per day

Why don't you go after
people who post on the
site

Emulator

5

built own emulator

does not have emulator
for Discs

Max 10 people sold to

how sold discs on
recession, none

helped Paul worked on
upgrading his system

local phone
- unknown wh

20' to Canada
cell # 705-715-1545
Toronto - Jim Linn
ph -
P.O. Box

Barry, ON
Shipping through UPS

2nd trip - Nov.
pick code up works
two weeks went down
\$25,000 wired from

30s-35 5-10 (B)
has a recording hair, 511
multitache - middle of
called Jim - to side of
ipr. canuck.net

dss king -
dss sat

Think he quite as of
3 weeks ago.

Paul - has two techs

site that doesn't get any hit
built site for Paul,
when housed - server unknown.
doesn't work - two or
three emails - server
sold anything

but - didn't - admit
yes

12

- BS mtr 1

Sorry Charlie 2.

no blocker -

activation script
20 units -

6 or 12 Echo -
old code

1/7 - checking pers.
4 - band father

Who's money? - Paul
gave doc from bus. acct

sell enough to make H.,
and quick

State code from developer
in Canada -

passed system with doc

Reorder issue: dist. #3
mail box - 336 4400
hotelsad.com
www.nick.com
428

When

UA - S000761 6586 96

RA # 002777 452-60

Smart Card ID =

Software Version:

P102CC JD - N

zip code - LV (die to exist)

Location ID = 20CD400E

85331

14

30 TSO's modified

didn't find rights

side business websites with
reality company

last doc sold a
week ago

30-60 units (now)

needs to have a
devel signal - units
hard to find -
found in Canada
102 says who gets
them

Woman - Diarrhea
Julie
add on computer
emailed -

Zipcode of card -

modified 6.0.0

read it then re-scan
back in.

says he does not know
how it is being on

19

Knows where chip is
being looked at.

he doesn't have access
at Motorola + doesn't
Think they have scope.

Ship part case down ^{to receive}
5 00 0 6 54 6 1 5 6 9
2 0 0 3 5 9 8 0 6 0 5

say
the
signature

like

can't

18
activation
hex

r3 hex.

winbox

destree

only virgin card

destree

tiger rider

Sat-man

- Win-eps 4.4
5b (vs.)

regular prog.

- to print in black box
than get code

he says Mexican as
the go to person.

Sets ~~out~~ to Mexico -
Mexican distributor - may
be selling down in Mexico -
asked why ^{he} said why
he didn't know - doesn't
want to know)

We stay away (he) tried
correcting himself.

20

Jim - Nipper - ?

can value 01-02

spies & cloning

Talk is in cap. @
buzen town

Killer par

22

old testing boards in
drawer said
doesn't make the
stuff - i.e. had down

@ in files - some
couple of times -

no warranty - buy us
is

overhead the cards through
- from shops -

\$20,000 made

pl conceal - on

- evaluate
serial comm chip to
cable through DV9 output
- use floppy on to boot

26

parts don't work

24
chip
of flash ATMEC data
making

of kshy through serial
part - \$50.00 from
Europe -

Brown programmer with
3 LED in front -
using prog. to
program

reg. programmer w/
medical crystal

vx maxi ≠
vx mini ≠

25
- storage max -
take image
ready with BasizH

miss 8006 area

place out of figg -

PGM write emulator
software - recover you
for architecture

WTX inside of computer

26

~~partner~~ partner doesn't
know how to program

He's not connected
with anyone but
he calls them
directly.

25

MK 14 for tracking
Atmel he's had for
1 1/2 years.

Went to school at
Univ. Pease, N.C. &
rec'd most of his
training of the Motorola



NAGRASTAR, 90 Inverness Circle East, Englewood,
CO 80112, USA, Tel: (303) 706-5700, Fax: (303) 706-5719

NAGRASTAR, Route de Genève 22, 1033 Cheseaux,
Switzerland, Tel: +41 21 732 04 00, Fax: +41 21 732 04 01

E-mail: nagrarstar@nagrarstar.com

Handwritten Notes of Mr. Jerry L. Gee, a.k.a. JJ
NagraStar Investigator

Notes taken during the interview of Mr. Anthony J. Maldonado conducted by SA Steve
A. Belongia, F.B.I., on March 22, 2001 at the residence of Mr. Anthony J. Maldonado,
5128 East Roberta Drive, Cave Creek, AZ.

Attached: 8 pages with 16 memo pages attached

Jerry L. Gee
Nagra|Star
Special Projects Investigator
90 Inverness Circle East
Englewood, CO 80112
Ph -303-706-5704
Fax - 866-422-6002
Cell - 303-669-8894



90 Inverness Circle East
Englewood, CO 80112
303-706-5700
303-706-5719

RE: Access Card S 00 0932 0682 92 Analysis

Card #S 00 0932 0682 92 was provided to NagraStar on January 2, 2001 to establish if the card received from EchoStar Signal Integrity via GBI & Associates via Maldonado had been tampered with in order to receive unauthorized satellite signals.

Following analysis, it was established that card S 00 0932 0682 92 had been tampered with to receive services without legal subscription.

Analysis of the modified card is attached. Indication of tampering was found within Record Sub, service range modified from range (0,x) to (7E00, FE00). The coding within the card indicates an illegal parameter.

Analysis of the modified card is attached. Indication of tampering was found within Record Sub, (0,x) to (0000,1FFF). The coding within the card indicates an illegal parameter.

Additionally Record IPPV was added opening event numbers for (0001, 7FFF) indicating that these lines have been changed illegally to receive unauthorized events and services.

All indication of analysis signifies that alteration to coding was conducted to steal and receive unauthorized satellite signals.

Analysis was conducted by: NagraStar, C. Gaillard

Cc: Guggenheim, Alan; Densmore, Russell



90 Inverness Circle East
Englewood, CO 80112
303-706-5700
303-706-5719

RE: Access Card S 00 0598 0753 Analysis

Card #S 00 0598 0753 was provided to NagraStar on January 2, 2001 to establish if the card received from EchoStar Signal Integrity via GBI & Associates via Maldonado had been tampered with in order to receive unauthorized satellite signals.

Following analysis it was established that card S 00 0598 0753 had been tampered with to receive services without legal subscription.

Analysis of the modified card is attached. Indication of tampering was found within Record Sub, service range modified from range (0,x) to (0000, 7FFF). The coding within the card indicates an illegal parameter.

Additionally Record IPPV was added opening event numbers for (0000, 7FFF) indicating that these lines have been changed illegally to receive unauthorized events and services.

All indications from this analysis show that alteration to coding was conducted to steal and receive unauthorized satellite signals.

Analysis was conducted by: NagraStar, C. Gaillard

Cc: Guggenheim, Alan; Densmore, Russell



U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to
File No. 295E-PX-68585

201 East Indianola Avenue

Phoenix, Arizona 85012
April 19, 2001

Mr. JJ Gee
NagraStar
90 Inverness Circle East
Englewood, Colorado 80112

RE: Anthony J. Maldonado & Paul T. St. James

Dear Mr. Gee:

Enclosed for your analysis is evidence seized pursuant to search warrants executed on March 22, 2001, at the residence of Anthony J. Maldonado and at Bargaintown Liquidation owned by Paul T. St. James. The specific items being forwarded are listed on the attached spreadsheet, and have been designated with following FBI "1B" numbers:

1B(85)

The majority of the evidence consists of Dish Network access cards. The remaining evidence consists of receivers and equipment suspected of being used to illegally modify access cards. It is requested that NagraStar conduct forensic examinations on all access cards to determine if they have been modified to receive unauthorized programming.

Evidence seized during the search warrants indicates that the subjects of this case were using a combination of software modifications to access cards and hardware modifications to receivers to facilitate the unauthorized reception of Dish Network programming. Accordingly, it is requested that NagraStar examine the receivers to determine if they have been so modified.

It is requested that the remaining items be examined and a narrative provided detailing what the items are, and how they are used to facilitate satellite piracy (if applicable).

Please detail your findings in a summary report listing each item examined by its "1B" number, item description and serial number. Include with the report a copy of your chain of custody records for the enclosed evidence.

HIGHLY CONFIDENTIAL

Case No. SA CV03-950 DOC (JTL)

ESC0113677

The report, chain of custody records and original evidence should be returned to Special Agent Stephen A. Belongia, 201 E. Indianola, Phoenix, Arizona 85012. SA Belongia can be reached at telephone number 602-650-3267 if you have any questions.

It requested that you sign and date the enclosed "FD-597 Receipt for Property Received/Returned/Released/Seized" on the "Received By:" line in the lower left hand corner of the form. Please return the form to SA Belongia in the enclosed return envelope as soon as possible.

Thank you very much for your assistance in this matter.

Sincerely,

Guadalupe Gonzalez
Special Agent In Charge

By: *Marcus M. Williams*
Marcus M. Williams
Supervising Special Agent

Enclosures: Form "FD-597"
Return envelope

UNITED STATES DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
Receipt for Property Received/Returned/Released/Seized

File # 295E-PX-68585

On (date) 4-26-01

- item(s) listed below were:
- Received From
 - Returned To
 - Released To
 - Seized

(Name) J.J. Gee
 (Street Address) Nagin Star
 (City) 90 Inverness Circle East
Englewood, CO 80112

Description of Item(s): IB(85)

(The remainder of the description area is crossed out with a large diagonal line.)

Received By: *[Signature]* (Signature) Received From: *[Signature]* (Signature)

Nagra|Star Smart Card Analysis Request Form
Confidential Client Attorney Privilege

Page - 1

Initiated By _____ FBI, Phoenix, AZ

Evidence Package 295 - PX - 68585 - 1B (28)

Network EchoStar ExpressVu Other _____

Received From RA's Law Enforcement Informant Nagra Other

Received From U.S. Dept. of Justice
 S.A. Steve Belongia
 201 East Indianola Avenue
 Phoenix, AZ 85012

Set Top Box Info

Model N/A

Software _____

Revision _____

Account Info

Status Active InActive Unknown

Cancel Date:

UA # Subscriber S 00 0761 6386 96

Concern - Establish if smart cards have been modified to receive stolen satellite television signals.

Confidential Client Attorney Privilege

Nagra|Star Smart Card Analysis Request Form
Confidential Client Attorney Privilege

Page - 2

Analysis -

Smart card - S 00 0761 6386 96

The coding area of the smart card was assigned to a receiver R0027994152.

Coding to the smart card allowing manipulation of EchoStar satellite programming was found within Record Sub (0000, 1FFF) and Record IPPV was modified to receive EchoStar satellite programming opening event numbers for (0000, 7FFF) indicating that these lines have been changed illegally to steal unauthorized events and services from EchoStar satellite programming.

✓ 

Signature
is Valid

Digitally signed by
Jerry Gee
DN: cn=Jerry Gee,
o=NagraStar,
c=US
Date: 2003.08.14
08:14:47Z
Reason: I am the
owner of this
document

Jerry L. Gee
Special Projects Investigator
NagraStar L.L.C.

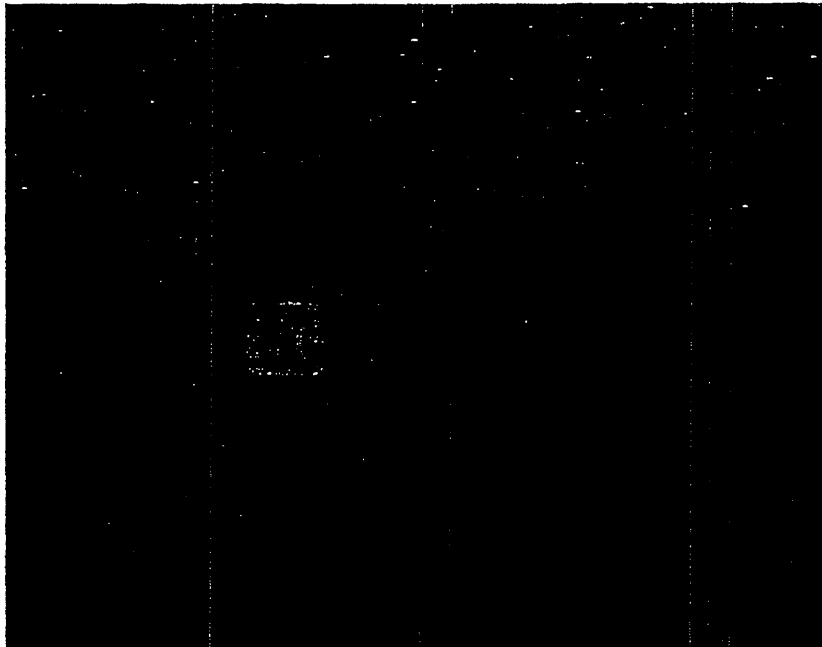
Confidential Client Attorney Privilege

Nagra|Star Smart Card Analysis Request Form
Confidential Client Attorney Privilege

Page - 3

NAGRASTAR
PHOTOGRAPHIC EXHIBIT

CASE #: 295 - PX - 68585 - 1B (28)



Confidential Client Attorney Privilege

HIGHLY CONFIDENTIAL

Case No. SA CV03-950 DOC (JTL)

ESC0113684

Nagra|Star Smart Card Analysis Request Form
Confidential Client Attorney Privilege

Page - 1

Initiated By _____ FBI, Phoenix, AZ

Evidence Package __ 295 - PX - 68585 - 1B (150) _____

Network EchoStar ExpressVu Other _____

Received From RA's Law Enforcement Informant Nagra Other

Received From U.S. Dept. of Justice
 S.A. Steve Belongia
 201 East Indianola Avenue
 Phoenix, AZ 85012

Set Top Box Info

Model _____ N/A _____

Software _____

Revision _____

Account Info

Status Active InActive Unknown

Cancel Date:

UA # Subscriber _____ S 00 0819 7531 34 _____

Concern - Establish if smart cards have been modified to receive stolen satellite television signals.

Confidential Client Attorney Privilege

Nagra|Star Smart Card Analysis Request Form
Confidential Client Attorney Privilege

Page - 2

Analysis -

Smart card - S 00 0819 7531 34

The coding area of the smart card was assigned to a receiver R0028007314.

Coding to the smart card allowing manipulation of EchoStar satellite programming within the Record Sub area is considered normal, (0000, 1000) Record IPPV was modified to receive EchoStar satellite programming opening event numbers for (0001, 7FFF) indicating that these lines have been changed illegally to steal unauthorized events and services from EchoStar satellite programming.

✓ 

Signature
of Verifier

Digitally signed by
Jerry L. Gee
DN: cn=Jerry L. Gee,
ou=NagraStar,
o=NagraStar,
c=US
Date: 2007.08.14
10:28:00 -0700
Reason: I am the
author of this
document

Jerry L. Gee
Special Projects Investigator
NagraStar L.L.C.

Confidential Client Attorney Privilege

Nagra|Star Smart Card Analysis Request Form
Confidential Client Attorney Privilege

Page - 3

NAGRASTAR
PHOTOGRAPHIC EXHIBIT

CASE #: 295 - PX - 68585 - 1B (150)



Confidential Client Attorney Privilege

Nagra|Star Smart Card Analysis Request Form
Confidential Client Attorney Privilege

Page - 1

Initiated By _____ FBI, Phoenix, AZ

Evidence Package _295 - PX - 68585 - 1B (152)_____

Network EchoStar ExpressVu Other _____

Received From RA's Law Enforcement Informant Nagra Other

Received From U.S. Dept. of Justice
 S.A. Steve Belongia
 201 East Indianola Avenue
 Phoenix, AZ 85012

Set Top Box Info

Model _____ N/A _____

Software _____

Revision _____

Account Info

Status Active InActive Unknown

Cancel Date:

UA # Subscriber _____ S 00 1111 6771 79 _____

Concern - Establish if smart cards have been modified to receive stolen satellite television signals.

Confidential Client Attorney Privilege

Nagra|Star Smart Card Analysis Request Form
Confidential Client Attorney Privilege

Page - 2

Analysis -

Smart card - S 00 1111 6771 79

The smart card had not been assigned to a specific receiver.

The smart card had not been modified.

✓ 
Signature
Date

Signature required by
Jerry Gee
2345 Technology Blvd.
San Diego, CA 92161
U.S.A.
Date: 08/26/10
08:00:00 AM
Printed: 1 on 10
Confidential
Contact

Jerry L. Gee
Special Projects Investigator
NagraStar L.L.C.

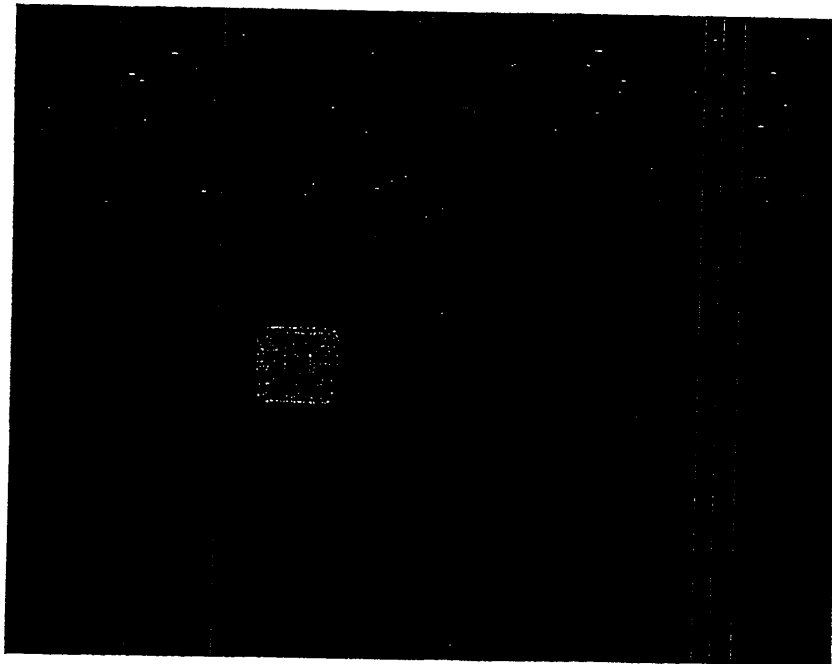
Confidential Client Attorney Privilege

Nagra|Star Smart Card Analysis Request Form
Confidential Client Attorney Privilege

Page - 3

NAGRASTAR
PHOTOGRAPHIC EXHIBIT

CASE #: 295 - PX - 68585 - 1B (152)



Confidential Client Attorney Privilege

HIGHLY CONFIDENTIAL

Case No. SA CV03-950 DOC (JTL)

ESC0113690

ANTHONY J. MALDONADO & PAUL T. ST. JAMES
FBI CASE #: 295E-PX-68585
(Dish Network Evidence)

I(B) #	Item Description	Serial #	CAM ID
135	Dish Network Access Card	S 00 0676 3120 31	-
135	Dish Network Access Card	S 00 0676 3101 12	-
135	Dish Network Access Card	S 00 0679 0555 64	-
136	Dish access card inserted into JVC receiver RFJCLJ01388N	S 00 0684 6151 64	R0025986605
28	Echostar Receiver containing Dish access card #S 00 0761 6386 96	RDECTK13818E	R0027994152
28	Dish Network Access Card inserted into Echostar Receiver s/n R0027994152	S 00 0761 6386 96	R0027994152
138	Dish Network Access Card inside receiver RFABNH08633F	S 00 0269 7572 91	
138	Dish Network Access Card inside receiver RFJCLJ01237M	S 00 0677 0885 04	R0026041782
139	Dish Network Access Card inside receiver RFJCLJ02141M	S 00 0684 9559	R0025608715
139	Dish Network Access Card inside receiver RFJCLJ00253M	S 00 0659 2570 77	R0025972871
139	Dish Network Access Card inside receiver WDEBWI33058H	S 00 0605 7925 45	R0023664210
140	EMP-30 Device Programmer from Needham's Electronics	n/a	-
140	Black circuit board "DIP48"	n/a	-
140	Red plastic case containing 12 4.5" x 13/16" black circuit boards labeled "EMP-30..."	n/a	-
140	Dish Network Access Card inside receiver RDECKPK05959G	S 00 1111 6909 19	R0029493114
140	Dish Network Access Card inside receiver RDECPK82785H	S 00 1126 5306 28	R0031039825
140	Dish Network Access Card inside receiver RDECKPK74714H	S 00 1184 2783 83	R 003077061
140	Dish Network Access Card inside receiver RDECPK80196H	S 00 1158 5794 00	R0031031380
140	Dish Network Access Card inside receiver RDECPK82807H	S 00 1151 3058 73	R0031034189
140	Dish Network Access Card inside receiver RDECPK8116H	S 00 1153 2668 72	R0031031146
140	Dish Network Access Card inside receiver RDECPK79084H	S 00 1171 7597 10	R0031039708
140	Dish Network Access Card inside receiver RDACAJ01995B	S 00 0370 4290 02	R0022258517
140	Dish Network Access Card inside receiver RDECUH13746M	S 00 0374 8583 01	R0021399229
140	Dish Network Access Card inside receiver RDECPK82795H	S 00 1139 8679 00	R0031034067
140	Dish Network Access Card inside receiver RDECPK82934H	S 00 1184 2454 74	R0031031515
140	Dish Network Access Card inside receiver RFECNK20405F	S 00 1129 9058 72	R0029123898
141	Dish Network Access Card inside receiver RDECTK11441E	S 00 0819 7483 85	R0027986829
142	Dish Network Access Card inside receiver RDECTK11436E	S 00 0819 7488 90	R0027993928
143	Dish Network Access Card inside receiver RDECPK05975G	S 00 1111 6893 02	R0029328363
144	Dish Network Access Card inside receiver RDECPK05963G	S 00 1111 6905 15	R0029328524
145	Dish Network Access Card inside receiver RDECPK81146H	S 00 1151 2975 89	R0030784080
146	Dish Network Access Card inside receiver RDECPK82798H	S 00 1126 5308 30	R0031039770
147	Dish Network Access Card inside receiver RDECPK05974G	S 00 1111 6894 03	R0029328515
148	Dish Network Access Card inside receiver R0030457152	S 00 1143 6001 05	R0030457152

1(B) #	Item Description	Serial #	CAM ID
149	Dish Network Access Card inside receiver RDECTK11438E	S 00 0819 7486 88	R0027988848
150	Dish Network model 4900 receiver containing access card S 00 0819 7531 34	RDECTK11422E	R0028007314
150	Dish Network Access Card inside receiver RDECTK11422E	S 00 0819 7531 34	R0028007314
151	Dish Network Access Card inside receiver RDECPK80190H	S 00 1158 5795 01	R0031031270
152	Dish Network model 3900 receiver containing access card S 00 1111 6771 79	RDECPK05885G	R0029328466
152	Dish Network Access Card inside receiver RDECPK05885G	S 00 1111 6771 79	R0029328466
153	Dish Network Access Card inside receiver RDECPK81167H	S 00 1184 2450 70	R0030765165
154	EMP-30 Device Programmer from Needham's Electronics with "Condor" 12VAC power supply	n/a	-
154	Generic 9 Pin Card Reader ID#67610C4, housed in tan plastic box	67610C4	-
88	Dish Network Access Card	S 00 1126 8251 56	-
88	Dish Network Access Card	S 00 1143 6012 16	-
88	Dish Network Access Card	S 00 1143 6059 63	-
88	Dish Network Access Card	S 00 1123 7674 95	-
88	Dish Network Access Card	S 00 1111 6907 17	-
88	Dish Network Access Card	S 00 1143 5918 21	-
88	Dish Network Access Card	S 00 1143 6000 04	-
88	Dish Network Access Card	S 00 1289 3425 44	-
88	Dish Network Access Card	S 00 1129 9044 58	-
88	Dish Network Access Card	S 00 1120 1355 58	-
88	Dish Network Access Card	S 00 1168 1257 75	-
88	Dish Network Access Card	S 00 1115 2013 29	-
88	Dish Network Access Card	S 00 1155 2379 96	-
88	Dish Network Access Card	S 00 1220 7435 48	-
88	Dish Network Access Card	S 00 1115 1988 03	-
88	Dish Network Access Card	S 00 1115 2006 22	-
88	Dish Network Access Card	S 00 1135 1195 01	-
88	Dish Network Access Card	S 00 1115 1999 14	-
88	Dish Network Access Card	S 00 1151 8645 47	-
88	Dish Network Access Card	S 00 1168 1258 76	-
88	Dish Network Access Card	S 00 1184 2745 45	-
88	Dish Network Access Card	S 00 1228 8205 21	-
88	Dish Network Access Card	S 00 1168 1299 17	-
88	Dish Network Access Card	S 00 1129 9046 60	-
88	Dish Network Access Card	S 00 1120 1356 59	-
88	Dish Network Access Card	S 00 1117 7154 68	-
88	Dish Network Access Card	S 00 1123 7675 96	-
88	Dish Network Access Card	S 00 1123 7673 94	-
88	Dish Network Access Card	S 00 1120 0554 72	-
88	Dish Network Access Card	S 00 1111 6886 95	-
88	Dish Network Access Card	S 00 1143 6064 68	-
88	Dish Network Access Card	S 00 1151 1293 13	-
88	Dish Network Access Card	S 00 1143 6006 10	-
88	Dish Network Access Card	S 00 0761 6416 27	-

1(B) #	Item Description	Serial #	CAM ID
88	Dish Network Access Card	S 00 0296 3393 02	-
88	Dish Network Access Card	S 00 0085 0346 62	-
88	Dish Network Access Card	S 00 0215 4589 06	-
88	Dish Network Access Card	S 00 0843 7971 86	-
88	Dish Network Access Card	S 00 0150 7845 58	-
88	Dish Network Access Card	S 00 0604 8427 44	-
88	Dish Network Access Card	S 00 0742 4935 40	-
156	Dish Network Access Card	S 00 0665 3245 61	-

UNITED STATES DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
Receipt for Property Received/Returned/Released/Seized

File # 295E-PX-68585

On (date) X 4/18/01

- item(s) listed below were:
- Received From
 - Returned To
 - Released To
 - Seized

(Name) JJ Gee
 (Street Address) NagraStar
 (City) 90 Inverness Circle East
Englewood, Colorado 80112

Description of Item(s):

<u>1B (28)</u>	<u>1B (143)</u>	<u>1B (152)</u>
<u>1B (88)</u>	<u>1B (144)</u>	<u>1B (153)</u>
<u>1B (135)</u>	<u>1B (145)</u>	<u>1B (154)</u>
<u>1B (136)</u>	<u>1B (146)</u>	<u>1B (156)</u>
<u>1B (138)</u>	<u>1B (147)</u>	
<u>1B (139)</u>	<u>1B (148)</u>	
<u>1B (140)</u>	<u>1B (149)</u>	
<u>1B (141)</u>	<u>1B (150)</u>	
<u>1B (142)</u>	<u>1B (151)</u>	

Received By: [Signature] (Signature) Received From: Ste A. Belong (Signature)

REMARKS: NagraStar Copy



U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to
File No. 295E-PX-68585

201 East Indianola Avenue

Phoenix, Arizona 85012
April 12, 2001

Mr. JJ Gee
NagraStar
90 Inverness Circle East
Englewood, Colorado 80112

RE: Anthony J. Maldonado & Paul T. St. James

Dear Mr. Gee:

Enclosed for your analysis is evidence seized pursuant to search warrants executed on March 22, 2001, at the residence of Anthony J. Maldonado and at Bargaintown Liquidation owned by Paul T. St. James. The specific items being forwarded are listed on the attached spreadsheet, and have been designated with following FBI "1B" numbers:

1B(28)	1B(143)	1B(152)
1B(88)	1B(144)	1B(153)
1B(135)	1B(145)	1B(154)
1B(136)	1B(146)	1B(156)
1B(138)	1B(147)	
1B(139)	1B(148)	
1B(140)	1B(149)	
1B(141)	1B(150)	
1B(142)	1B(151)	

The majority of the evidence consists of Dish Network access cards. The remaining evidence consists of receivers and equipment suspected of being used to illegally modify access cards. It is requested that NagraStar conduct forensic examinations on all access cards to determine if they have been modified to receive unauthorized programming.

Evidence seized during the search warrants indicates that the subjects of this case were using a combination of software modifications to access cards and hardware modifications to receivers to facilitate the unauthorized reception of Dish Network programming. Accordingly, it is requested that NagraStar examine the receivers to determine if they have been so modified.

It is requested that the remaining items be examined and a narrative provided detailing what the items are, and how they are used to facilitate satellite piracy (if applicable).

Please detail your findings in a summary report listing each item examined by its "1B" number, item description and serial number. Include with the report a copy of your chain of custody records for the enclosed evidence.

The report, chain of custody records and original evidence should be returned to Special Agent Stephen A. Belongia, 201 E. Indianola, Phoenix, Arizona 85012. SA Belongia can be reached at telephone number 602-650-3267 if you have any questions.

It requested that you sign and date the enclosed "FD-597 Receipt for Property Received/Returned/Released/Seized" on the "Received By:" line in the lower left hand corner of the form. Please return the form to SA Belongia in the enclosed return envelope as soon as possible.

Thank you very much for your assistance in this matter.

Sincerely,

Guadalupe Gonzalez
Special Agent In Charge

By: *Marcus M. Williams*
Marcus M. Williams
Supervising Special Agent

Enclosures: Evidence spreadsheet
Form "FD-597"
Return envelope

cc: R. Densmore, Echostar Technologies

ANTHONY J. MALDONADO & PAUL ST. JAMES
 FBI CASE #: 295E-PX-68585

Qty	New	Item #	(B) Description	Item #	Revised Description	Serial #	CAN ID	Forwarder
(Q)	(B)							Dish DirectTV

18Q2 to 18Q3 Malbonado & Paul James

7	1	3	Dish Network Card	1	Dish Network Access Card	S 00 0676 3120 31		X
				1	Dish Network Access Card	S 00 0676 3101 12		X
				1	Dish Network Access Card	S 00 0679 0555 64		X

14	1	1	Green Circuit Board Labeled "Unlooper"	1	Green Circuit Board Labeled "Unlooper" & HUI/Loader	n/a		X
----	---	---	--	---	---	-----	--	---

18	3	3	JVC Satellite Receiver CAYD SER #R0025986605 W/Dish Network Card Inserted #S-00-0684-6151-64	3	JVC Satellite Receiver with Dish access card #S 00 0684 6151 64	RXCJL01388N	R0025986605	X
				3	Dish access card inserted into JVC receiver RXCJL01388N	S 00 0684 6151 64	R0025986605	X
18	4	4	Small Board Topaz in Color 21-117	4	Small topaz circuit board with number 21-117	n/a		

25	1	1	DirectTV Receiver w/stand, Model RDRD4200E Serial #033473943	1	RCA DirectTV plus receiver with DirectTV access card 0001 7880 0843 inserted	033473943		X
				1	DirectTV access card inserted inside RCA receiver #N 033473943	0001 7880 0843		X

27	1	4	DirectTV Card 000176758712, 000176001980, 000179818232, 000416422418	1	DirectTV Access Card (period 3)	0001 1674 8712		X
				1	DirectTV Access Card (period 3)	0001 7600 1980		X
				1	DirectTV Access Card (period 3)	0001 7981 8232		X
				1	DirectTV Access Card (period 3)	0004 1642 2418		X
27	2	2	DSS Cards 000128360922, 000128654951	2	DirectTV Access Card	0001 2836 0922		X
				2	DirectTV Access Card	0001 2865 4951		X
27	3	1	Circuit Board Marking Interphase Ltd - MK14	3	1 Circuit Board Marking Interphase Ltd - MK14	n/a		X
				3	1 tan plastic box housing a circuit board inside, within battery compartment are the numbers 602471	n/a		X

28	1	1	Echo Star-Dish Receiver SN: RDRCTK13818E	1	EchoStar Receiver containing Dish access card #S 00 0761 6386 96	RDRCTK13818E	R0027994132	X
				1	Dish Network Access Card inserted into EchoStar Receiver #N R0027994132	S 00 0761 6386 96	R0027994132	X

30	1	1	DirectTV access card #0003 2301 7648	1	DirectTV Access Card	0003 2301 7648		X
----	---	---	--------------------------------------	---	----------------------	----------------	--	---

END ITEMS SEIZED FROM MALDONADO'S RESIDENCE

18Q3 to 18Q18 Bargelstern Liquidation/Paul St. James

32	1	2	Access cards from DirectTV	1	DirectTV Access Card	0001 7647 7651		X
				1	DirectTV Access Card	0001 8650 5806		X
30	2	2	Dish Brand Receiver Model 100 Serial #R00159256099	2	Dish model 1000 receiver containing access card S 00 0269 7572 91	RFABNH08633F		X
				2	Dish Network Access Card inside receiver RFABNH08633F	S 00 0269 7572 91		X
30	3	3	Dish Brand Receiver model 3700, Serial R0026041782	3	Dish model 3700 receiver containing access card S 00 0677 0885 04	RXCJL01237M	R0026041782	X
				3	Dish Network Access Card inside receiver RXCJL01237M	S 00 0677 0885 04	R0026041782	X

Org. (B)	New Item #	(B) Description	Item #	Revised Description	Serial #	CAM ID	Dish	DirectV
51	1	20025008715 on floor	1	JVC Dish Network model 2700 receiver containing access card S 00 0684 9359 60	RDCCL002141M	R0025608715	X	
			1	Dish Network Access Card Inside receiver RDCCL002141M	S 00 0684 9359	R0025608715		X
51	2	20025972871	2	JVC Dish Network model 2700 receiver containing access card S 00 0659 2370 77	RPEC100253M	R0025972871	X	
			2	Dish Network Access Card Inside receiver RPEC100253M	S 00 0659 2370 77	R0025972871		X
51	3	Dish with card MS serial R0023664210	3	Dish Network model 7100 receiver containing access card S 00 0605 7923 45	WDBRW133038H	R0023664210	X	
			3	Dish Network Access Card Inside receiver WDBRW133038H	S 00 0605 7923 45	R0023664210		X
55	1	Box Labeled programming device	1	BNP-30 Device Programmer from Neodhan's Electronics	N/A		X	
			1	Black circuit board "DTP48"	N/A		X	
			1	Red plastic case containing 12 4.5" x 13/16" Black circuit boards labeled "BNP-30..."	N/A		X	
55	2	3900/Serial RDBCPK039590	2	Dish Receiver containing access card S 00 1114 6909 19	RDBCPK03959G	R0029493114	X	
			2	Dish Network Access Card Inside receiver RDBCPK039590	S 00 1114 6909 19	R0029493114		X
55	7	3900/Serial RDBCPK42785H	7	Dish model 3900 receiver containing access card S 00 1126 5306 28	RDBCPK42785H	R0031039825	X	
			7	Dish Network Access Card Inside receiver RDBCPK42785H	S 00 1126 5306 28	R0031039825		X
55	8	3900/Serial RDBCPK4714H	8	Dish model 3900 receiver containing access card S 00 1184 2783 83	RDBCPK4714H	R 003077061	X	
			8	Dish Network Access Card Inside receiver RDBCPK4714H	S 00 1184 2783 83	R 003077061		X
55	9	3900/Serial RDBCPK40196H	9	Dish model 3900 receiver containing access card S 00 1138 5194 00	RDBCPK40196H	R0031031380	X	
			9	Dish Network Access Card Inside receiver RDBCPK40196H	S 00 1138 5194 00	R0031031380		X
55	10	3900/Serial RDBCPK32807H	10	Dish model 3900 receiver containing access card S 00 1131 3058 13	RDBCPK32807H	R0031034189	X	
			10	Dish Network Access Card Inside receiver RDBCPK32807H	S 00 1131 3058 13	R0031034189		X
55	11	3900/Serial RDBCPK81161H	11	Dish model 3900 receiver containing access card S 00 1133 2668 72	RDBCPK81161H	R0031031146	X	
			11	Dish Network Access Card Inside receiver RDBCPK81161H	S 00 1133 2668 72	R0031031146		X
55	12	3900/Serial RDBCPK79084H	12	Dish model 3900 receiver containing access card S 00 1171 7597 10	RDBCPK79084H	R0031039708	X	
			12	Dish Network Access Card Inside receiver RDBCPK79084H	S 00 1171 7597 10	R0031039708		X
55	14	2700/Serial RDACA101995B	14	Dish model 2700 receiver containing access card S 00 0370 4290 02	RDACA101995B	R002228517	X	
			14	Dish Network Access Card Inside receiver RDACA101995B	S 00 0370 4290 02	R002228517		X
55	15	4700/Serial RDECVH13746M	15	Dish model 4700 receiver containing access card S 00 0374 8383 01	RDECVH13746M	R0021399229	X	
			15	Dish Network Access Card Inside receiver RDECVH13746M	S 00 0374 8383 01	R0021399229		X
55	16	3900/Serial RDBCPK82795H	16	Dish model 3900 receiver containing access card S 00 1139 8679 00	RDBCPK82795H	R0031034067	X	
			16	Dish Network Access Card Inside receiver RDBCPK82795H	S 00 1139 8679 00	R0031034067		X
55	17	3900/Serial RDBCPK42934H	17	Dish model 3900 receiver containing access card S 00 1184 2454 74	RDBCPK42934H	R0031031515	X	
			17	Dish Network Access Card Inside receiver RDBCPK42934H	S 00 1184 2454 74	R0031031515		X
55	18	31800/Serial RDECNK20105F	18	Dish model 31800 receiver containing access card S 00 1129 9058 72	RDECNK20105F	R0029123898	X	
			18	Dish Network Access Card Inside receiver RDECNK20105F	S 00 1129 9058 72	R0029123898		X
55	19	2700/Serial RDACLJ1478M	19	Dish model 2700 receiver (no card)	RDACLJ1478M	R0029123498	X	
			19	Dish Network Access Card Inside receiver RDACLJ1478M	S 00 0819 7483 55	R0027986829		X
65	1	Dish Network satellite receiver serial R0027986829	1	Complete Dish Network satellite system including dish, receiver, access card, etc.	N/A		X	
			1	Dish Network model 4900 receiver containing access card S 00 0819 7483 55	RDBCTK11441B	R0027986829		X
			1	Dish Network Access Card Inside receiver RDBCTK11441B	S 00 0819 7483 55	R0027986829		X

Org (ID)	New Item #	(ID) Description	Item #	Revised Description	Serial #	CAM ID	Dish	DirectV
	66	Dish Network satellite receiver serial R0027993928	1	Complete Dish Network satellite system including dish, receiver, access card, etc.	n/a			
				Dish Network model 4900 receiver containing access card S 00 0819 7488 90	RDBCTR11436E	R0027993928		
				Dish Network Access Card Inside receiver RDBCTR11436E	S 00 0819 7488 90	R0027993928		X
	67	Dish Network satellite receiver serial R0027984398, on the box	1	Box for Dish Network satellite system including dish and hardware (no receiver); sticker indicating box is for model 4922 receiver, s/a RDBCTR11424E, snat card dn S 00 0819 7329 32	n/a			
	68	Dish Network Satellite Receiver Serial R0020949914	1	Dish model 3000 receiver (no card)	RDBR1G10557B			
	69	Dish Network satellite receiver serial R0029328363	1	Complete Dish Network satellite system including dish, receiver, access card, etc.	n/a			
				Dish Network model 3900 receiver containing access card S 00 1111 6893 02	RDBCTR05975G	R0029328363		
				Dish Network Access Card Inside receiver RDBCTR05975G	S 00 1111 6893 02	R0029328363		X
	70	Dish Network satellite receiver serial R0029328324	1	Complete Dish Network satellite system including dish, receiver, access card, etc.	n/a			
				Dish Network model 3900 receiver containing access card S 00 1111 6905 15	RDBCTR05963G	R0029328324		
				Dish Network Access Card Inside receiver RDBCTR05963G	S 00 1111 6905 15	R0029328324		X
	71	Dish Network satellite receiver serial R0030784080	1	Complete Dish Network satellite system including dish, receiver, access card, etc.	n/a			
				Dish Network model 3900 receiver containing access card S 00 1131 2975 89	RDBCTR81146H	R0030784080		
				Dish Network Access Card Inside receiver RDBCTR81146H	S 00 1131 2975 89	R0030784080		X
	72	Dish Network satellite receiver serial R0031039770	1	Complete Dish Network satellite system including dish, receiver, access card, etc.	n/a			
				Dish Network model 3900 receiver containing access card S 00 1126 3308 30	RDBCTR82798H	R0031039770		
				Dish Network Access Card Inside receiver RDBCTR82798H	S 00 1126 3308 30	R0031039770		X
	73	Dish Network Satellite Receiver Serial R0020324355	1	Dish model 3000 receiver (no card)	YDDB1G02460E			

Orig. New (B)	Item #	(B) Description	Item #	Revised Description	Serial #	CAM ID	Dish	DirectV
	74	Dish Network satellite receiver serial R0029328515	1	Complete Dish Network satellite system including dish, receiver, access card, etc.	n/a			
				Dish Network model 3900 receiver containing access card \$ 00 1111				
				6894 03	RDBCPK03974G	R0029328515		
				Dish Network Access Card inside receiver RDBCPK03974G	\$ 00 1111 6894 03	R0029328515		X
	75	Dish Network satellite receiver serial R0030457152	1	Dish model 2800 receiver containing access card \$ 00 1143 6001 05				
				Dish Network Access Card inside receiver R0030457152	\$ 00 1143 6001 05	RUECVK43893K	R0030457152	X
	76	Dish Network satellite receiver serial R0027988848	1	Complete Dish Network satellite system including dish, receiver, access card, etc.	n/a			
				Dish Network model 4900 receiver containing access card \$ 00 0819				
				7486 88	RDBCTK11438E	R0027988848		
				Dish Network Access Card inside receiver RDBCTK11438E	\$ 00 0819 7486 88	R0027988848		X
	77	Dish Network satellite receiver serial R0028007314	1	Complete Dish Network satellite system including dish, receiver, access card, etc.	n/a			
				Dish Network model 4900 receiver containing access card \$ 00 0819				
				7531 34	RDBCTK11422E	R0028007314		X
				Dish Network Access Card inside receiver RDBCTK11422E	\$ 00 0819 7531 34	R0028007314		X
	78	Dish Network satellite receiver serial R0031031270	1	Complete Dish Network satellite system including dish, receiver, access card, etc.	n/a			
				Dish Network model 3900 receiver containing access card \$ 00 1156				
				5795 01	RDBCPK80190H	R0031031270		
				Dish Network Access Card inside receiver RDBCPK80190H	\$ 00 1156 5795 01	R0031031270		X
	79	Dish Network satellite receiver serial R0029328466	1	Complete Dish Network satellite system including dish, receiver, access card, etc.	n/a			
				Dish Network model 3900 receiver containing access card \$ 00 1111				
				6771 79	RDBCPK03885G	R0029328466		X
				Dish Network Access Card inside receiver RDBCPK03885G	\$ 00 1111 6771 79	R0029328466		X
	80	Dish Network satellite receiver serial R0030765165	1	Complete Dish Network satellite system including dish, receiver, access card, etc.	n/a			
				Dish Network model 3900 receiver containing access card \$ 00 1184				
				2450 70	RDBCPK81167H	R0030765165		
				Dish Network Access Card inside receiver RDBCPK81167H	\$ 00 1184 2450 70	R0030765165		X

QTR	New Item #	(Q) Description	Item #	Revised Description	Serial #	QAM ID	Dir	Dir
83	1	Box addressed to Paul St. James Containing 46 "unlooper"	1	46 green "unlooper", box addressed to Paul St. James	n/a			X
86	1	Needham's Electronic EMP-30	1	EMP-30 Device Programmer from Needham's Electronics with "Condor"	n/a			X
85	2	Generic 9 Pin Card Reader ID#67610C4	1	Generic 9 Pin Card Reader ID#67610C4, housed in tan plastic box	67610C4			X
88	1	Small baggy containing 33 Dial Network cards found in toolbox notes above	1					
				Dial Network Access Card	5 00 1126 8251 56			X
				Dial Network Access Card	5 00 1143 6012 16			X
				Dial Network Access Card	5 00 1143 6019 63			X
				Dial Network Access Card	5 00 1123 7674 95			X
				Dial Network Access Card	5 00 1111 6907 12			X
				Dial Network Access Card	5 00 1143 5918 21			X
				Dial Network Access Card	5 00 1143 6000 04			X
				Dial Network Access Card	5 00 1289 3423 44			X
				Dial Network Access Card	5 00 1129 9044 58			X
				Dial Network Access Card	5 00 1120 1355 58			X
				Dial Network Access Card	5 00 1168 1297 75			X
				Dial Network Access Card	5 00 1115 2013 29			X
				Dial Network Access Card	5 00 1135 2379 96			X
				Dial Network Access Card	5 00 1220 7453 48			X
				Dial Network Access Card	5 00 1115 1988 03			X
				Dial Network Access Card	5 00 1115 2006 22			X
				Dial Network Access Card	5 00 1135 1193 01			X
				Dial Network Access Card	5 00 1115 1999 14			X
				Dial Network Access Card	5 00 1151 8043 47			X
				Dial Network Access Card	5 00 1168 1258 76			X
				Dial Network Access Card	5 00 1184 3743 45			X
				Dial Network Access Card	5 00 1228 8205 21			X
				Dial Network Access Card	5 00 1168 1299 17			X
				Dial Network Access Card	5 00 1129 9046 60			X
				Dial Network Access Card	5 00 1120 1356 59			X
				Dial Network Access Card	5 00 1117 7154 68			X
				Dial Network Access Card	5 00 1123 7673 94			X
				Dial Network Access Card	5 00 1143 6064 10			X
				Dial Network Access Card	5 00 1151 1293 13			X
				Dial Network Access Card	5 00 0761 6416 22			X
				Dial Network Access Card	5 00 0296 3193 02			X
				Dial Network Access Card	5 00 0083 0346 62			X
				Dial Network Access Card	5 00 0215 4389 06			X
				Dial Network Access Card	5 00 0343 7971 86			X
				Dial Network Access Card	5 00 0150 7843 58			X
				Dial Network Access Card	5 00 0604 8437 44			X
				Dial Network Access Card	5 00 0742 4935 40			X
88	2	6 Dial Network Cards	2					
				Dial Network Access Card	5 00 0761 6416 22			X
				Dial Network Access Card	5 00 0296 3193 02			X
				Dial Network Access Card	5 00 0083 0346 62			X
				Dial Network Access Card	5 00 0215 4389 06			X
				Dial Network Access Card	5 00 0343 7971 86			X
				Dial Network Access Card	5 00 0150 7843 58			X
				Dial Network Access Card	5 00 0604 8437 44			X
				Dial Network Access Card	5 00 0742 4935 40			X
94	1	1 H Card & Blocker	1	6.25" x 3.25" green blocker containing DirecTV access card 0001 6701	n/a			X

Orig (1B)	New (1B)	Item #	(1B) Description	Item #	Revised Description	Serial #	CAM ID	Disb	DirectV
94	2	30 H Card		1	Revised Description				
				2	Inside 6.25" x 2.25" green blocker	0001 6701 2061			X
94				2	DirectV access card	0003 2528 0493			X
94				2	DirectV access card	0003 2197 1707			X
94				2	DirectV access card	0002 0242 7209			X
94				2	DirectV access card	0001 8032 3859			X
94				2	DirectV access card	0001 7875 3393			X
94				2	DirectV access card	0001 8174 4855			X
94				2	DirectV access card	0001 7583 9513			X
94				2	DirectV access card	0001 7953 3807			X
94				2	DirectV access card	0001 7487 0451			X
94				2	DirectV access card	0001 8558 4504			X
94				2	DirectV access card	0001 7439 0757			X
94				2	DirectV access card	0001 7429 7291			X
94				2	DirectV access card	0001 7812 5142			X
94				2	DirectV access card	0001 8148 9154			X
94				2	DirectV access card	0001 8576 1772			X
94				2	DirectV access card	0001 7440 6215			X
94				2	DirectV access card	0001 7860 9830			X
94				2	DirectV access card	0001 8176 9415			X
94				2	DirectV access card	0001 2245 4851			X
94				2	DirectV access card	0001 7429 4025			X
94				2	DirectV access card	0003 3108 9144			X
94				2	DirectV access card	0003 3869 1702			X
94				2	DirectV access card	0001 8645 4260			X
94				2	DirectV access card	0001 7601 5600			X
94				2	DirectV access card	0001 8656 8051			X
94				2	DirectV access card	0001 7964 2475			X
94				2	DirectV access card	0001 7965 6939			X
94				2	DirectV access card	0001 8319 7894			X
94				2	DirectV access card	0001 7439 3973			X
94				2	DirectV access card	0001 7437 5253			X
94				2	DirectV access card	0001 8110 7210			X
94				2	DirectV access card	0001 7639 1407			X
94				2	DirectV access card	0002 3030 7241			X
94				2	DirectV access card	0001 5852 2292			X
95	1	1 Receiver		1	RCA DirectV receiver containing access card 0003 3714 5296	904328330			X
				1	DirectV access card inside receiver 904328330	0003 3714 5296			X
1B(119) to 1B(123) Paul Hammerman Residences									
119	1	5 satellite cards		1	DirectV access card	0003 3611 5381			X
				2	DirectV access card	0002 0606 4461			X
				3	DirectV access card	0001 5110 6366			X
				4	Dish Network Access Card	3 00 0665 3245 61			X
122	1	One RCA satellite receiver w/word serial #638447493		1	RCA DirectV model DRD303RA receiver containing access card 0003 3991 2156	638447493			X
				1	DirectV access card inside receiver 638447493	0003 3991 2156			X
123	1	DSS Manuals (3 Volumes) and One Video		1	DSS Bible (3 volumes) pg 6 of 7	n/a			X

Qty	New	Item #	(19) Description	Item #	Revised Description	Serial #	CAM ID	Dish	DirectV
125	1	DSS Access Card		1	VHS video "The DSS Video"	N/A			X
									X

18(24) to 18(25) Bayfieldtown Lodge/Donor/Parl St. 4/08



- [profile](#)
- [register](#)
- [1333 members](#)
- [faq](#)
- [search](#)
- [home](#)
- [Email This Page to Someone!](#)
- [Show a Printable Version](#)

[Go to first unread post](#)

Hitec Satellite Chat Forum > Echostar
Clearing Password in IRD

[< Last Thread](#) [Next Thread >](#)

[new thread](#) [post reply](#)

Author	Thread
destnee Member in Training	Has anybody been able to clear the password in the IRD. I have a few units that have the password set and can't seem to get rid of it.

Registered: Oct 2000
Posts: 30



01-16-2001 11:13 AM

- [profile](#)
- [mail](#)
- [www](#)
- [search](#)
- [edit/delete](#)
- [quote](#)

IP: [Logged](#)

destnee
Member in Training

up

Registered: Oct 2000
Posts: 30

01-16-2001 03:56 PM

- [profile](#)
- [mail](#)
- [www](#)
- [search](#)
- [edit/delete](#)
- [quote](#)

IP: [Logged](#)

ZED
Moderator



Registered: Jan 2000
Posts: 628

A search of the forum would have brought this up but here it is. Just go to the memory dump (menu, 6, 3, info, right arrow, left arrow) and when your there hit the tv/video button. Unplug or just power off with the power button on the front of the receiver and thats it, memory cleared.

ZED

01-16-2001 06:57 PM

- [profile](#)
- [mail](#)
- [www](#)
- [search](#)
- [edit/delete](#)
- [quote](#)

IP: [Logged](#)

All times are PT (US)

[new thread](#) [post reply](#)

Forum Jump:

[< Last Thread](#) [Next Thread >](#)

Forum Rules:

Who Can Read The Forum? Any registered user or guest.
Who Can Post New Topics? Any registered user.
Who Can Post Replies? Any registered user.
Changes: Messages can be edited by their author. Messages can be deleted by their author.
Posts: HTML code is OFF. [Smilies](#) are ON. [vB code](#) is ON. [IMG] code is ON.

Admin Options:

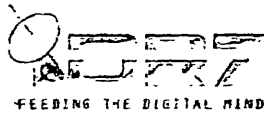
[Open / Close Thread](#)
[Move Thread](#)
[Delete Thread](#)
[Edit Thread](#)

[< Contact Us - Hitec Satellite >](#)

http://chat.hitecsat.com/showthread.php?threadid=9772

13123
2463

1/17/2001



Profile Register Members Help Search Home
Login @DR7 E-mail Signup @DR7 E-mail Upload New Files

Email This Page to Someone
Show a Printable Version

Go to first unread post

DR7 Digital Chat Forum > Echostar Technical Forum
Resetting Password on DN IRD

< Last Thread

new thread post reply

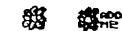
Author

Thread

destnea
Junior Member

Anyone know how to reset the lockout password on a Dish IRD?
Thanks...

Registered: Nov 2000
Posts: 29



01-16-2001 04:00 PM

profile search edit/delete quote

IP: Logged

Milton
Senior Member

destnea - have you tried a search on the word "password" in the Echostar General Forum? This question has been answered many times in the past and a search will return posts with the answer.

Registered: Aug 1999
Posts: 114

Here is one of my favorites. I verified this about 6 months ago so I don't know if the locations are valid.

Let us know if it works!

From a post from Star:

There is an alternate method, which will not destroy your saved data in the IRD. You are already in the diagnostic menu/memory dump.

Go to the following memory location: NVM 01C0: 00000000 00000000 87090000 00000000

The above represents a password of 0987. The msb is in the first nibble second byte, the lsb of the password is in the first nibble first byte.

Hope this helps for next time.

StarLog

01-16-2001 07:05 PM

profile search edit/delete quote

IP: Logged

Mikeyl
Senior Member

Clear password

Registered: Aug 1999
Posts: 304

This method will clear NVRAM and the password with it. I believe I saw this posted before on this site...but maybe it was PD....(Uniwiz posted this I believe)...

Master reset: (Clears password and favorites, clear NVRAM):

[MENU] [6 (system setup)] [3 (Diagnostics)]
 (Do these quickly [INFO] [RIGHT ARROW] [LEFT ARROW])
 Note this will bring you to the memory dump screen
 At this point hit the [TV/VIDEO] button. The screen will say NVRAM is corrupt - it
 will be cleared once the [POWER] button on front panel is pressed. So hit
 [POWER] on FRONT PANEL. When it comes back up - password and favorites
 are cleared.

Memory Dump (by itself):

[MENU] [6 (system setup)] [3 (Diagnostics)]
 (Do these quickly [INFO] [RIGHT ARROW] [LEFT ARROW])

As suggested in the previous posts the password IS stored in the location
 specified earlier. You can use that method to change/clear password as well
 without destroying your saved settings...

Hope this helps...

[Edited by Mikey! on 01-16-2001 at 10:10 PM]

Have a great day!

Mike

01-16-2001 09:48 PM

IP: Logged

destnee
 Junior Member

Thanks, I usually do a search but forgot this time.... Brain problems this week,
 that damn flu thats going around.

Registered: Nov 2000
 Posts: 29



01-17-2001 02:58 PM

IP: Logged

All times are PST (US)

new thread

post reply

[< Last Thread](#)

Forum Jump:

Forum Rules:

Who Can Read The Forum? Any registered user or guest.

Who Can Post New Topics? Any registered user.

Who Can Post Replies? Any registered user.

Changes: Messages can be edited by their author. Messages can be deleted by their author.

Posts: HTML code is OFF. Smilies are ON. vB code is ON. [IMG] code is ON.

Admin Options:

[Open / Close Thread](#)













[Move Thread](#)

[Delete Thread](#)














[Edit Thread](#)










[< Contact DR7 Support - DR7 - Feeding the Digital Mind >](#)
















Powered by: vBulletin Version 1.1.5
 Copyright © Jelsoft Enterprises Limited 2000.


















	-Pasha
cat5 unregistered	   <p>Model 2000 ex-sub HTS uhf 9fcofff ird# notinversed. Next 8 bytes are the KEY to the city! thanks DR7 THE CRACK STUNT GUY SCG and all that have helped</p>
mellvin unregistered	   <p>Info on the 4000 (subbed):</p> <p>Data on \$87A0 is repeated on \$FBA0 except the Key --</p> <p>\$FBA0: CORRRRRRRRTTTTTTTTTTTTTSSSSSS \$FBB0: SS3130434E000000KKKKKKKKKKKKKK</p> <p>Where R: Rcvr ID (reversed) T: Bootstrap version (ASCII) S: Software version (ASCII) 3130434E: "10CN"(seems ASCII ??) K: Secret key (reversed)</p> <p>Location \$9FD0FFF0 is all zeroes (subbed)</p> <p>[This message has been edited by mellvin (edited 01-12-99).] [This message has been edited by mellvin (edited 01-12-99).]</p>
Eric Cartman unregistered	   <p>IRD Key/ID: CONFIRMED on one model 3000 at address \$8700 and CONFIRMED on one model 4000 at address \$8A70. I have no way to confirm the secret key on either of the receivers so I will just take everyones word for it.</p> <p>Thanks everone,</p>
Barefooter unregistered	   <p>Garfy...</p> <p>I have a 2350 at least that's what it say's on the back ...on the info screen it says 4000... found my ird# at FBA0 and 8A70...very close to where the 4000 keys seem to be...the next 16 bytes are the same in both locations.... haven't pulled the tsop and did a dump to confirm... am waiting on a programmer and am going to try the avr dual with the master hex with the first 8 bytes following reversed (as it appears in the memory dump) and if that doesn't work the next 8 bytes and if still no luck the first and second 8 bytes inversed (reverse from the dump)...do you have a AM29F010 as mine does in front of the tsop?...will pull the</p>





















	<p>tsop if all else fails...anyone else have any other suggestions... always open to new idea...can't believe how much I have learned here.</p> <p>DR7 keep up the great work !!...</p>
<p>Goodguy unregistered</p>	<p>Bigdish was that DVHS a subbed box?</p>
<p>BigDish Newbie Posts: 3 Registered: Sep 1999</p>	<p>Goodguy. Yes it was a subbed box.</p>
<p>Mikef unregistered</p>	<p>i have a subbed 1000 series and in 9FD0FFF0 it is all 0's</p> <p>where else can i look????????????????????????????????</p>
<p>mellvin unregistered</p>	<p>On model 1000 (subbed):</p> <p>I found the IRD (not reversed) in \$8955, but the key is not there. Just bootstrap info in ASCII.</p> <p>Another post someone mentioned location \$15120, but not true on mine.</p> <p>I'll keep looking...</p> <p>-mellvin</p>
<p>DrNeuron Newbie Posts: 4 Registered: Sep 1999</p>	<p>Model 1000: I also found IRD# at 15565 (from memory- I'll update later from home) with the ascii data as before, but I think that the keys follow the ascii data.</p> <p>Tonight, I'll load up the card with these numbers and see if they are the keys. Will update post with more info later.</p> <p>DrNeuron</p>
<p>jazzercz unregistered</p>	<p>I believe that for all systems which are new and just out of the box and</p>

	<p>not connected to the datastream, 9FD0FFF0 is the place to find your IRD # followed by your secret key. I was wondering if a Master Reset would return the IRD into the "new, not connected" state?</p> <p>If someone wants to try it, here is what I would suggest:</p> <ol style="list-style-type: none"> 1) disconnect your box from the datastream 2) do a master reset. <ul style="list-style-type: none"> -Turn your E* IRD on -Using remote, press MENU 6 1 -Using remote, press the following sequence INFO BROWSE THEME -Press the TV/VIDEO button and then the IRD's front power button. 3) Now go into the memory dump and look at location 9FD0FFF0 and see if the first 4 bytes are your IRD number. If so, then the next 8 bytes are probably your secret key. <p>Let us know if this works or not.</p> <p>-J</p>
<p>Yakshumash unregistered</p>	<p>  </p> <p>Excellent idea jazzercz (-@-), I will try it and post result.</p> <p>[This message has been edited by Yakshumash (edited 01-14-99).]</p>
<p>Yakshumash unregistered</p>	<p>  </p> <p>Jazzercz- I tried what you suggested. It did not work. BUT it had some unexpected results. This is a model 4000. It had the key at the end of the line \$FB50, it was still there but the box ID several lines before was gone. I know it was there previous because thats how I traced the key. I wonder- did the receiver get a code update to make finding the key harder or did the master reset remove it ?</p>
<p>cimeron Member</p> <p>Posts: 24 Registered: Nov 1999</p>	<p>   </p> <p>Yak. : I was wondering was your 4000 sub'd?? If so did your sub work after the master reset?? I am wondering what effects the master reset has on the CAM or the sub' of an ird. Will it just go back to being a normal sub'd box?? Any ideas? Thanks.</p>
<p>jazzercz unregistered</p>	<p>  </p> <p>Yakshumash - RATS... Thanks for the effort. I am not certain why the IRD # went away, but it is not important anyway. The private key at the end of \$fbb0 is the real gem.</p> <p>It seems that somehow we can use the master reset to our advantage...</p>

	just have to put my thinking cap on again...
Yakshumash <small>unregistered</small>	   <p>It looks like all of what I surmised was incorrect. The location SFb70 looks like it is in ram. I can only get the box id back by putting in my sub(also answers your question cimeron). So this is probably a buffered command- Which when I looked at it had all the ascii bytes Uniwiz was telling me to put in to remove the unauthorizd messaged, except several were changed and the bytes are offset relative to the Key.</p> <p>In the xfile I see:</p> <pre>xx xx xx xx aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa zz kk kk kk kk kk kk kk</pre> <p>In Memory I see:</p> <pre>xx xx xx xx aa aa aa aa aa aa aa aa aa aa aa aa aa aa aa zz zz kk kk kk kk kk kk kk kk</pre> <p>xx= box ID aa= ascii bytes zz= zeros kk= key bytes</p> <p>So the real message may be padded with a few more zeros or the box ID may be out of position.</p> <p>Stuntguy/Stymie/Uniwiz you guys have any explanation for this. Is absolute position in the string important ?</p> <p>[This message has been edited by Yakshumash (edited 01-14-99).]</p>
Tylon <small>unregistered</small>	   <p>I have a ex-subbed 4000. With the info I have gathered on this thread, I have 2 choices for a secret key. Should I just try 2 different modded bat files or any suggestions? My ird # is not at 8a70, but is at 9fd0fff0. I would assume the key is after this address and not the fbb0.....2 choices for a key. What to do?</p>
Tylon <small>unregistered</small>	   <p>Just looked at bat gen. site. It has a place for ird# (8 byte digits correct?) Secret key (16 byte digits) and cam id (8 hex bytes). This may sound stupid, but I can't convert my cam id to 4 bytes (00000...xxxxxx)Any help gang ☺</p>

<p>Yakshumash unregistered</p>	<p>  </p> <p>You may need to pad it with leading zeros.</p>
<p>Dragonmaster Member</p> <p>Posts: 60 Registered: Aug 1999</p>	<p>  </p> <p>I tried the master reset routine, it worked for me on a 3000, found the box id and keys at 9fd0ff0, loaded them into AVR mod and nada, got channel guide and music, checked and reached, ohm'd pcb. Everything good on the pcb, Went to the batt.bin generation site, loaded all info and programmed v3 batt with bin. Worked first time. I have used Dual AVR b4 and it works. Could something be different in a screen dump compared to a manual tscop dump?</p>
<p>jazzercz unregistered</p>	<p>  </p> <p>Master Reset:</p> <p>Yak - 4000 - did not work Dragon - 3000 - Did work, but dual avr stopped and bat worked?</p> <p>Hmmm... this is strange, but there is promise here.</p> <p>Anyone know how to do a master reset on a 1000 box?</p>
<p>mellvin unregistered</p>	<p>  </p> <p>more on model 1000 subbed:</p> <p>Looks like the key is on \$1557C in the same format as the other models, I didn't confirm:</p> <p>\$15560: ????????? ?RRRRRR RRAAAAAA AAAAAAAA \$15570: AAAAAAAA AAAAAAAA AAZZZZZZ KKKKKKKK \$15580: KKKKKKKK ?????????</p> <p>R = IRD A = ascii Z = zero K = KEY</p> <p>-mellvin</p>
<p>litow unregistered</p>	<p>  </p> <p>Model 3000 IRD # in \$8700 and \$14BE5 Secret Key in \$14BFC-14C00 Confirmed. Unit works fine in all channels with a single AVR.</p>

	[This message has been edited by litow (edited 01-15-99).]
ZoRaQ unregistered	   FYI: Those ASCII (AA AA AA) Bytes are the bootstrap and software version numbers that appear on the information screen.
Ty1on unregistered	   Have loaded a key (the first 8 bytes after id at 9fd0ff0) and all I get is black screen.. Wrong key? Using bat with prev.subbed 4000. Any help would be apprec.  Figured it out.....confirms with mellivyn's findings for an EX-sub  [This message has been edited by Ty1on (edited 01-16-99).]
Barefooter unregistered	   Model: 2350 IRD Key/ID: Confirm at \$8A70 and FBA0 (reversed at both locations) Secret key: The last 8 bytes on line \$FB00 (not reversed) Subbed/No-Sub: Previously Subbed (cancelled) No Mod Looks the same as 4000...working with Dual AVR no blackouts
Garfy unregistered	   Thanks for the info Barefooter.. Garfy.
handyman unregistered	   Model: 3000 Subbed: Top 100 147C0: 00ZZZZZZ 00RRRRRR RRBBBBBB BBBBBBBB 147D0: BBBBBSSS SSSSSSSS SS000000 KKKKKKKK 147E0: KKKKKKKK ???0000 FFFF0000 00000000 Z= Zip Code R= Receiver ID B= Bootstrap version (ASCII) S= Software version (ASCII) K= Secret Key

	<p>Also found Receiver ID at location 8840 but no secret key in that area.</p> <p>Has anyone thought that the reason the Keys float around so much from receiver to receiver could be do to what program package you are subscribed to?</p> <p>If Subbed that is. :-)</p>
<p>StuntGuy Member</p> <p>Posts: 153 Registered: Sep 1999</p>	<p>   </p> <p>I can confirm Melvin's findings: On my non-sub, non-mod 1000, the key is at 1557C-15583.</p> <p>-s</p>
<p>jershu unregistered</p>	<p>  </p> <p>I found my key on E at 9fd0fff0 but i see postings like \$14bfo \$14bco where do i find these? I am using the memory dump on screen method. Whats this \$ sign for ?</p>
<p>jazzercz unregistered</p>	<p>  </p> <p>jershu, just ignore the \$, it specifies that the address is hex.</p>
<p>jershu unregistered</p>	<p>  </p> <p>jazzercz: thanks for the quick reply, OK I will ignore the \$ sign, but 9FD0FFF0 is 4 bytes or 8 hex , the \$14BF0 is only 5 Hex. When I enter these hex in the lower left hand box of the memory map location what do I enter? If I enter 14BF0 , it still leaves me with 3 I dont know. Sorry if I sound ignorant </p>
<p>jazzercz unregistered</p>	<p>  </p> <p>Put zeros in front... Example, 14BF0 should be entered as 00014BF0.</p>
<p>jazzercz unregistered</p>	<p>  </p> <p>Well, on a 1000 subbed box, 1557C was zeroes. In fact, all of the memory in that area was zeroes. So for a 1000 subbed box, there are some discrepencies...</p>

Name: Russ Densmore

SEARCH PLAN

Case #: 295E-PX-68585

- A. MISSION AND SEARCH LOCATIONS
- B. BACKGROUND/BRIEFING INFORMATION
- C. SUBJECTS/TARGETS
- D. PERSONNEL, SEARCH TEAMS & ASSIGNMENTS
- E. COMMUNICATIONS
- F. EMERGENCY POINTS OF CONTACT & PHONE NUMBERS
- G. PROTOCOL
- H. ATTACHMENTS

Pre-search briefing: 2:30 pm on Wednesday March 21, 2001

Staging will occur at 8:00 am on Thursday, March 22, 2001
Searches will commence at approx. 8:30 am on Thursday, March 22, 2001

NOTE: THIS SEARCH WARRANT IS SEALED

A. MISSION AND SEARCH LOCATIONS

To execute search warrants at/of the following locations/individuals/automobiles:

Locations:

**Site #1: 5128 E. Roberta Drive, Cave Creek, Arizona
[Personal residence of Anthony J. Maldonado]**

Staging Location: Giant Gas Station parking lot, corner of Dynamite Road and Tatum Boulevard in Cave Creek (4740 E. Dynamite Boulevard)

**Site #2: 3401 W. Buckeye Road, Suite #3, Phoenix, Arizona
[Warehouse for Bargaintown Liquidation]**

Staging Location: 35th Avenue and Cocopah (2 blocks south of Buckeye). Stage at the east end of Cocopah which is a dead end cul-de-sac.

Individuals:

- **Anthony J. Maldonado, a male standing approximately 6'1", weighing approximately 180 pounds with brown hair, having a birth date of 9/22/1967 and a social security number (omitted).**
- **Paul Thomas St. James, a male standing approximately 6'3", weighing approximately 230 pounds with brown hair, having a birth date of 5/12/1967 and a social security number of (omitted).**

Vehicles:

- **1998 Jeep Cherokee, Arizona license plate 611EAW, owned by Anthony J. Maldonado**
- **1995 Dodge Pickup, New Jersey license plate GL 200S, owned by Paul T. St. James**

See attached search packets for site descriptions, staging locations, directions and photographs.

B. BACKGROUND/BRIEFING INFORMATION

FBI Case #: 295E-PX-68585

Case Title: ANTHONY J. MALDONADO

Violations:

A.R.S. 13-1003 Conspiracy
A.R.S. 13-1802 Theft of Services
A.R.S. 13-2310 Fraud Schemes
A.R.S. 13-2317 Money Laundering
A.R.S. 13-2312 Illegal Enterprise

Case Agent:

	<u>PH #</u>	<u>Pgr#</u>	<u>Cell #</u>
SA Stephen A. Belongia (FBI)	602-650-3267	602-227-5420	602-319-5161
Assistant A.G. Gale Thackeray	602-542-8424	-	602-542-5997 (fax)

Division:

Phoenix 602-279-5511 602-604-3440 (fax)

Case Background/Synopsis:

Anthony J. Maldonado and Paul T. St. James are suspected of programing, selling and distributing illegally modified access cards for both the DirecTV and DISH Network satellite systems. Maldonado is a network engineer at Motorola's Information Technology Group, and other Motorola employees are suspected of distributing illegal access cards for Maldonado. Maldonado has been observed programming DirecTV cards on his Sony VAIO notebook computer at work. It is believed that Maldonado may have as many as 800 DirecTV customers representing programming losses of over \$2,000,000 per year (conservatively). The revenue from sales of said cards likely exceeds \$300,000.

Maldonado is currently only "servicing" DirecTV access cards and is not believed to be distributing additional cards. Cards require "servicing" due to electronic counter measures (ECMs) which are initiated by DirecTV as part of their anti-piracy efforts. ECMs cause illegal access cards to "freeze-up" rending them useless. The programmer (Maldonado) must then reprogram the cards in order to continue to illegally receive free programming.

Maldonado has recently focused his piracy efforts at the DISH Network satellite system (a competitor to DirecTV). Maldonado and financier/partner, Paul T. St. James, allegedly paid \$80,000 to purchase the computer code to "hack" DISH Network access cards. It is believed that the code was purchased from an unidentified Canadian hacker. Most of the

"top tier" computer programmers/hackers who are capable of compromising DirecTV and DISH cards reside in Canada.

Maldonado and St. James have established an Internet website, www.kobalt.com.mx, through which they sell illegally modified DISH systems (including the dish, receiver and access card). Maldonado and St. James purchase unmodified systems through various local retailers including CostCo, as well as out-of-state retailers such as Bulverde Home Theater in Texas. The access cards for these systems are modified, and the unit is repackaged and sent to customers. Customers believe that Kobalt.com is a Mexican based company, but checks are sent to a mail drop in Nogales (282 N. Grand Court Plaza, PMB 144, Nogales, Arizona; Everyday Mail). An undercover purchase revealed that Maldonado communicates with customers using the screen name "baud_father.com". One communication included the following disclaimer:

"I understand...that I am responsible to know whether or not these cards or programming are legal in the area I am asking Kobalt.com.mx to send this/these products. I am also not part of any task force or government agency working against satellite pirates and I further agree that anything I receive from Kobalt.com.mx can not be used as evidence in any form..."

It has been determined that 50 unmodified DISH systems were shipped from Bulverde Home Theater in Texas, to a warehouse owned by Paul T. St. James, 3401 W. Buckeye Road, Suite 3, in Phoenix. One of these 50 units was then modified and sent to investigators acting in an undercover capacity. Suit 3 includes office and warehouse space for Bargaintown Liquidators, owned by St. James. Maldonado and St. James have been observed meeting at the location after business hours, and it is believe that it's the location where the DISH systems are modified and repackaged for delivery to website customers.

It is believed that the website for www.kobalt.com.mx may be contained on a laptop computer owned by Maldonado or St. James.

The case is being prosecuted by the Arizona Attorney General's Office.

C. SUBJECTS/TARGETS The primary targets of the investigation are as follows:



Name: Anthony J. Maldonado
Height: 6'1"
Weight: 180 Lbs.
Hair: Brown
DOB: 09/22/1967
SSN: 527-99-6546
Criminal: 1988 - Burglary
1991 - DUI



Name: Paul T. St. James
Height: 6'3"
Weight: 230 Lbs.
Hair: Brown
DOB: 05/12/1967
SSN: 136-78-6908
Criminal: 1985 - Burglary

D. PERSONNEL SEARCH TEAMS & ASSIGNMENTS

<u>Name</u>	<u>Agency</u>	<u>Site</u>	<u>Assignment(s)</u>
• SA Stephen Belongia	FBI	1	Team Leader/Interview/Searcher
• Inspector John Zemblidge	USPIS	1	Room Labeling/Diagram/Searcher
• SA Deb Adamo	FBI	1	Searcher/Evidence Control
• SA Eugene Kaili	FBI	1	Photographer/Searcher
• SA Rich Esler	FBI	1	Searcher/Photo Log
• SA John Treadwell	FBI (Cart)	1	Computers/Searcher
• SA Shari Mcallister	FBI	1	Searcher
• SA Jim Conner	FBI	1	Searcher
• Russ Densmore	Dish	1	Technical Advisor
• SA Julie Halferty	FBI	2	Team Leader/Interview/Searcher
• SA Dee Simpson	FBI	2	Room Labeling/Searcher
• SA Dan Orr	FBI	2	Data Sheets/Diagram/Searcher
• SA Ann Fasano	FBI	2	Searcher/Evidence Control
• SA John Lewis	FBI (Cart)	2	Computers/Searcher
• SA Mike Gallante	FBI	2	Searcher
• SA Marilyn Sheveland	FBI	2	Searcher
• SA Brian Fuller	FBI	2	Searcher
• Detective Mike Sechez	PPD	2	Searcher
• Dawn Langston	FBI	2	Photographer/Photo Log
• JJ Gee	Nagra/Dish	2	Technical Advisor

Team Leaders will also:

- 1) Serve warrant(s)
- 2) Prepare FD-302
- 3) Make other assignments as necessary

Entry & Controlling the Search Scene:

(omitted)...DirecTV and DISH Network technical advisors and support personal will remain at the staging locations until the sites have been fully secured...(omitted).

E. COMMUNICATIONS

FBI Radio Channel(s)
(Omitted)

	<u>Team #</u>	<u>Pgr#</u>	<u>Cell #</u>
SA Steve Belongia	1	602-227-5420	602-319-5161
Inspector John Zemblidge	1	-	602-690-6107
SA Julie Halferty	2	602-409-7685	602-908-8731
SA Brian Fuller	2	602-213-9050	602-316-5019

F. EMERGENCY POINTS OF CONTACT & PHONE NUMBERS

Emergency: 911

Agency Main Numbers:
- FBI (602)279-5511

Medical Facilities:

Site #1
Paradise Valley Hospital
3929 East Bell Road, Phoenix
(602)923-5000

Site #2
Phoenix Memorial Hospital
1201 S. 7th Avenue, Phoenix
(602)258-5111

G. PROTOCOL

(Omitted)

H. ATTACHMENTS

1. Site Packages (1 & 2)
2. Items to be seized & List of the most important items to be seized
3. Photos of DirecTV and DISH System hardware and piracy equipment

NOTE: THIS SEARCH WARRANT IS SEALED

SITE #1

**5128 E. ROBERTA DRIVE
CAVE CREEK, ARIZONA**

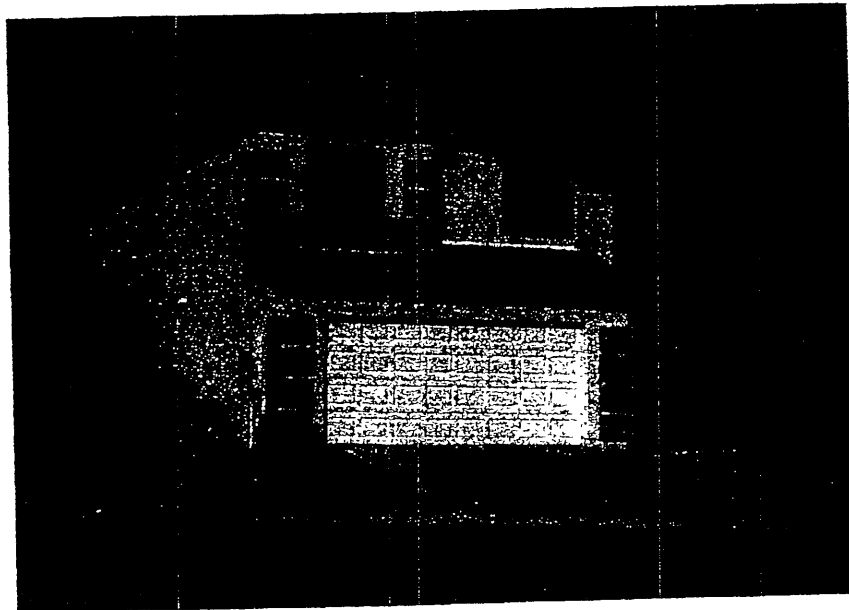
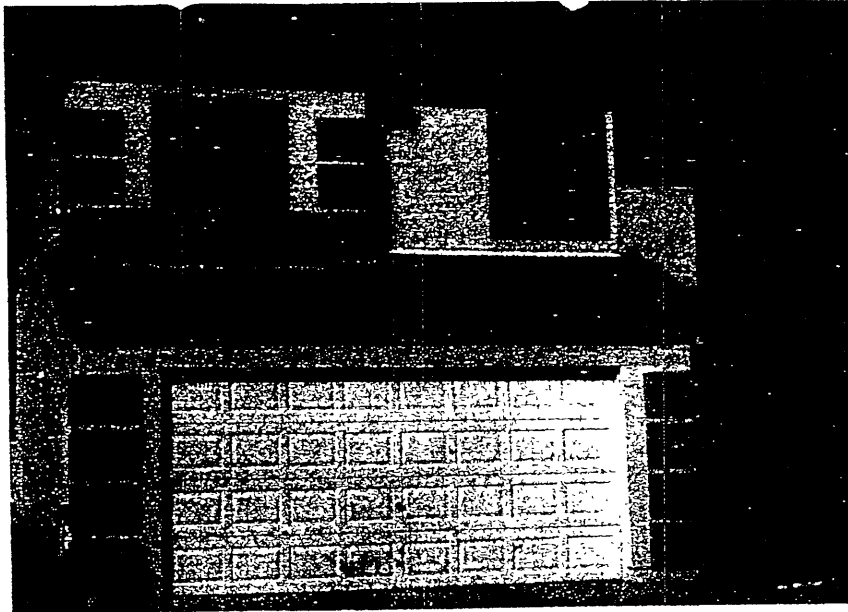
Residence of Anthony J. Maldonado

Site Description :

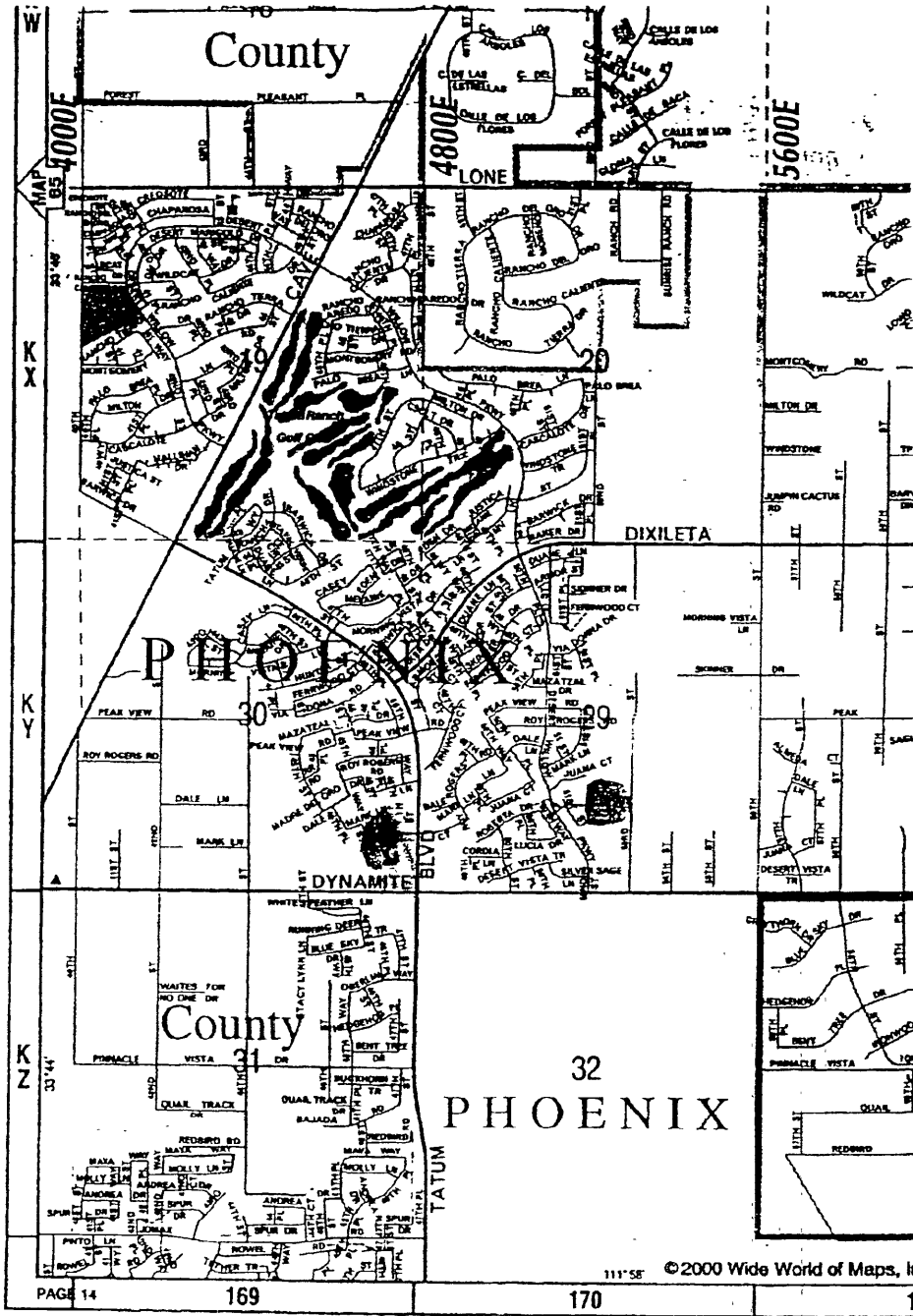
This is a two story cream colored residence with a rounded tile roof and a two car garage. On each side of the garage are four decorative raised squares which are brown in color. On the third square on the right (east) side of the garage are the numbers "5128". To the east of the property is a block wall and a horse property. The residence is the last house on the north side of a cul-de-sac. There is a large rock situated left (west) of the garage. The entrance to the residence is on the right (east) side of the garage and is lit with landscape lights. The location is the principal residence of Anthony J. Maldonado.

Staging Location:

Giant Gas Station, Corner of Dynamite Road and Tatum Boulevard (4740 E. Dynamite Boulevard).



**SITE #1
5128 E. ROBERTA DRIVE
CAVE CREEK, ARIZONA**



SITE #1

5128 E. Roberta Drive
Cave Creek, AZ

- ① Search Site: 5128 E. Roberta Drive
- ② Staging Location: Giant Gas Station, corner of Dynamite Road and Tatum Blvd. (4740 E. Dynamite Blvd.)

SITE #2

3401 W. BUCKEYE ROAD, SUITE 3 PHOENIX, ARIZONA

Business/warehouse for Bargintown Liquidation

Site Description :

A large warehouse building on the south side of West Buckeye Road in Phoenix. The entry parking lot to the warehouse is to the east of 3401 West Buckeye. The building is clearly marked with the numerals "3401" on the north and east facing walls near the top of the building at the northeast corner of the structure. There are two clearly marked tenants of the structure, AutoFit and Bargintown which have the company names affixed to the east facing wall of the warehouse. AutoFit's suites are located at the northern most part of the warehouse. Bargintown's sign is located directly over a red-tile roof facade which is situated above the entrance to Suite 3. On the east facing wall of Suite 3 is a large glass window with the following lettering:

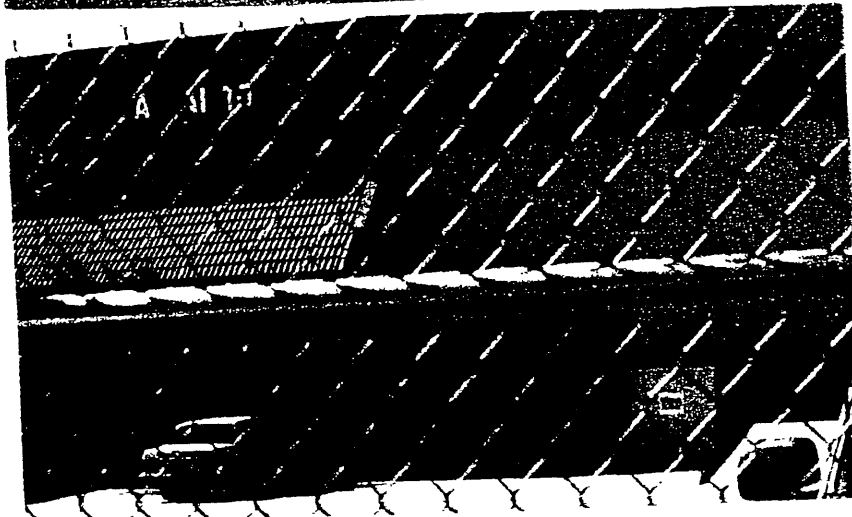
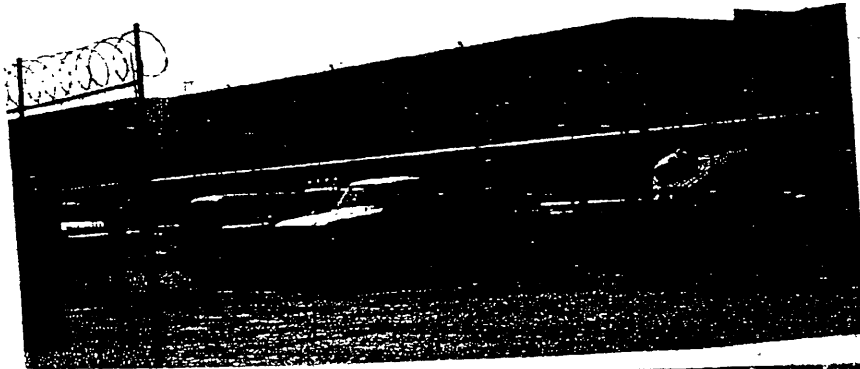
Bargintown Liquidation
34__ W. Buckeye, Suite 3
Phoenix, AZ 85009
(602)223-2003
www.bargintown.com

To the left of the window is a glass entry door which is accessed by walking up cement steps on the east side of the building. There is a Suite 4/Suite D located to the south (left) of Suite 3 which appears to be vacant. Suite 4 has a "Dream Lounger" logo on the window and a similar sign on the door.

Suite 3 further consists of two metal roll-up doors located to the north (right) of the entrance to Suite 3. The doors provide access to warehouse space for Suite 3.

Staging Location:

35th Avenue and Cocopah (2 blocks south of Buckeye). Stage at the east end of Cocopah which is a dead end cul-de-sac; drive over the railroad tracks, past the Phoenix Rescue Mission and the Insulfoam building on the south(right) side of the street, and the Arizona State Prison complex on the north (left) side of the street. NOTE: Drive slowly over the tracks!

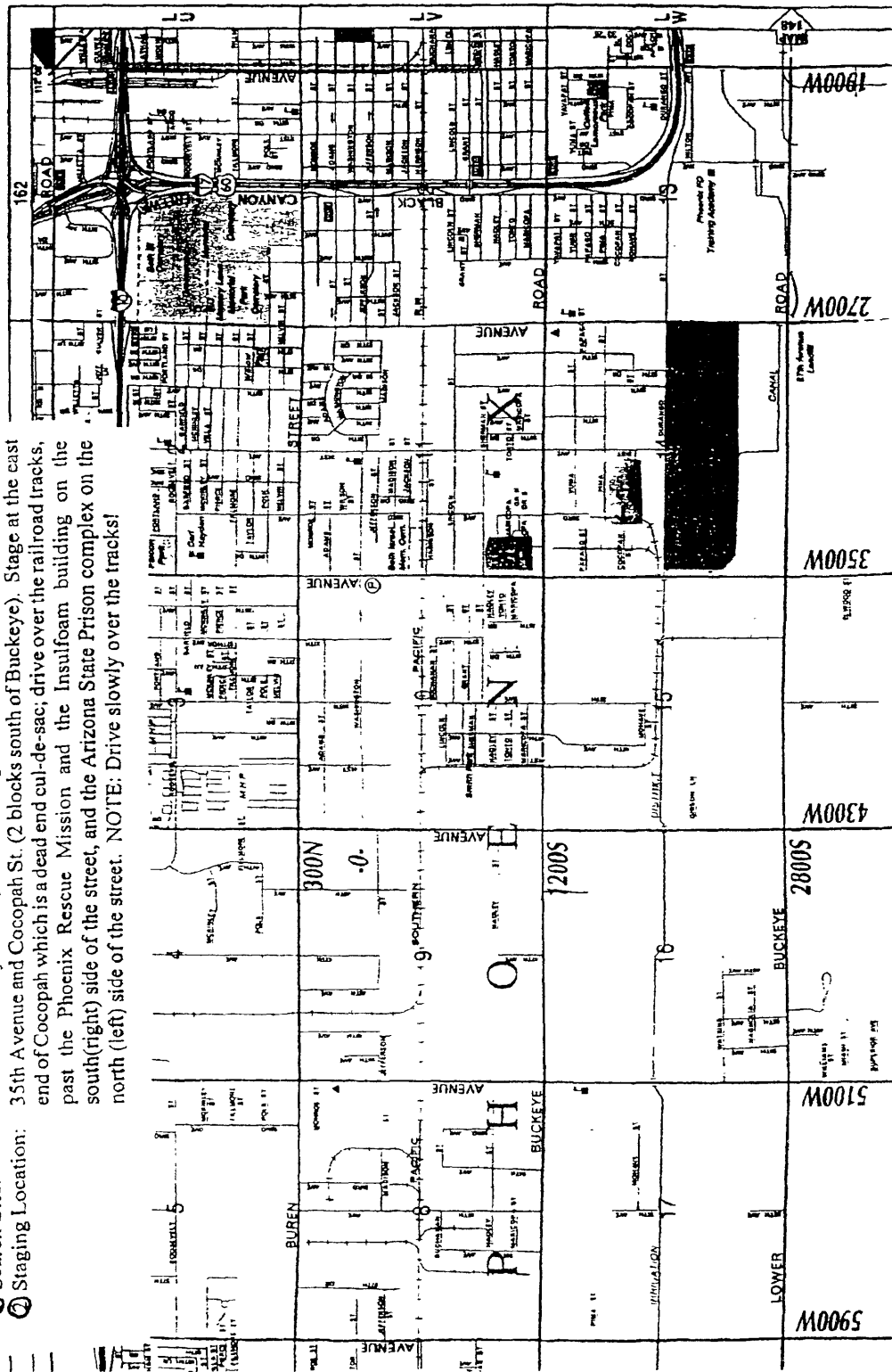


SITE #2
3401 W. BUCKEYE, SUITE #3
PHOENIX, ARIZONA

ATTN #2

3401 W. Buckeye Road, Suite 3
Phoenix, Arizona

- ① Search Site: 3401 W. Buckeye Road, Suite 3 (Bargaintown)
- ② Staging Location: 35th Avenue and Cocopah St. (2 blocks south of Buckeye). Stage at the east end of Cocopah which is a dead end cul-de-sac; drive over the railroad tracks, past the Phoenix Rescue Mission and the Insulfoam building on the south(right) side of the street, and the Arizona State Prison complex on the north (left) side of the street. NOTE: Drive slowly over the tracks!



MOST IMPORTANT ITEMS TO BE SEIZED

1. Anything related to:

Kobalt
282 North Grand Court Plaza
PMB 144
Nogales, Arizona 85621
www.kobalt.com.mx
2. Anything related to the screen name "baud_father" or "**baud_father@hotmail.com**"; e-mail to/from **paul@bargaintown.com** or bargaintown.com relating to satellite systems
3. Any documents related to satellite TV (i.e. DirecTV, DSS, Dish Network, Echostar Technologies, satellite signal piracy, etc.)
4. Bank account information for:
 - a) The account used to purchase the code for Dish Network (this will be established via an interview of the subject by the team leader and most likely will only apply to Site #2)
 - b) The account used to deposit customer funds resulting from the sale of DirecTV access cards (this will be established via an interview of the subject by the team leader and most likely will only apply to Site #1, Anthony J. Maldonado)
 - c) The account used to deposit customer funds resulting from the sale of Dish Network systems (this will be established via an interview of the subject by the team leader and could apply to either Sites 1 or 2)
5. Satellite piracy hardware or software. See search packets for photos and utilize the technical advisors from DirecTV and Dish Network.
6. All DirecTV and Dish Network access cards, and all integrated receivers-decoders (IRDs). Satellite dishes will not be taken.
7. All laptop computers belonging to Anthony Maldonado or Paul St. James. Other computers to be determined by team leaders.
8. Documents showing the secretion or investment of assets, and receipts for significant household purchases (Site #1 only)
9. Customer lists and UPS/Postal/FedEx records related to individuals who have purchased DirecTV or Dish Network access cards or other equipment;
10. Copies of money orders from individuals who purchased Dish Network systems.
11. Travel records for trips to Canada, phone records for calls made to Canada and other documents related to Canada
12. Records and marketing materials related to the purchases of Dish Network satellite systems from vendors such as Costco, Belverde Home Theater in Texas, etc.
13. Documents related to "Pat Clark"

**Federal Bureau of Investigation
County of Maricopa, State of Arizona**

Search Warrant

Warrant # SW2001-000143

To any peace officer in Maricopa County:

Proof by affidavit having been made this day before me by Special Agent Stephen A. Belongia, I am satisfied there is probable cause to believe that:

(X) On the persons of: (1) Anthony J. Maldonado, a male standing approximately 6'1", weighing approximately 180 pounds, with brown hair, having a birth date of 9/22/1967 and a social security number of 527-99-6546; and (2) Paul Thomas St. James, a male standing approximately 6'3", weighing approximately 230 pounds, with brown hair, having a birth date of 05/12/1967 and a social security number of 136-78-6908.

(X) At the locations known as: (1) 5128 E. Roberta Drive, Cave Creek, Arizona: This is a two story creme color residence with a rounded tile roof and a two car garage. On each side of the garage are four decorative raised squares, which are brown in color. On the third square on the right (east) side of the garage are the numbers 5128. To the east of the property is a block wall and a horse property. The residence is the last house on the north side of a cul-de-sac. There is a large rock on the left (west) side of the garage. The entrance to the residence is on the right (east) side of the garage and is lit with landscape lights. The location is the principal residence of Anthony J. Maldonado; (2) 3401 W. Buckeye Road, Suite 3, Phoenix, Arizona including any and all warehouse and storage space held as part of the occupancy thereof. This location is a large warehouse building on the south side of West Buckeye Road in Phoenix. The entry parking lot to the warehouse is to the east of 3401 West Buckeye. The building is clearly marked with the numerals "3401" on the north and east facing walls near the top of the building at the northeast corner of the structure. There are two clearly marked tenants of the structure, AutoFit and Bargaintown which have their company

names affixed to the east-facing wall of the warehouse. AutoFit's suites are located at the northern-most part of the warehouse. Bargaintown's sign is located directly above a red-tile roof facade, which is situated above the entrance to Suite 3. On the east facing wall of Suite 3 is a large glass window with the following lettering:

Bargaintown Liquidation
34__ (sic) W. Buckeye, Suite 3
Phoenix, AZ 85009
(602)223-2003
www.bargaintown.com

To the left of the window is a glass entry door that is accessed by walking up cement steps on the east side of the building. Suite 3 further consists of two metal roll-up doors located to the north (right) of the entrance to Suite 3. The doors provide access to warehouse space for Suite 3. There is a "Suite 4/Suite D" located to the south (left) of Suite 3 which appears to be vacant. Suite 4 has a "Dream Lounger" logo on the window and a similar sign on the door.

(X) In the electronic mail (e-mail) accounts "baud_father@hotmail.com" (to be served on the national headquarters of MSN Hotmail, Inc., 1065 La Avenida, Building 4, Mountain View, California 94043) and "paul@bargaintown.com" (to be served on Paul T. St. James and/or One Call Communications, Inc., 801 Congressional Boulevard, Carmel, Indiana 46032).

(X) In the vehicles described as: (1) Anthony J. Maldonado's 1998 Jeep Cherokee, Arizona license plate "611EAW"; and (2) Paul T. St. James' 1995 Dodge pickup, New Jersey license plate GL 200S.

(X) On/In the electronic devices described as follows: Any computer that may contain the storage of data including, but not limited to, type written notes and photo image(s), computer hard drives, media, discs, tapes and all other storage devices.

In the County of Maricopa, State of Arizona, there is now being possessed or concealed certain property or things described as:

1. Any and all electronic data processing and storage devices, computers and computer systems including central processing units; internal and peripheral storage devices such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage devices or other memory storage devices; peripheral input/output devices such as keyboards, printers, video display monitors, optical readers and related communication devices such as modems; together with system documentation, operating logs and documentation, software and instruction manuals, handwritten notes, logs, user names, passwords and lists.
2. All of the records below, whether stored on paper, on magnetic media such as tape, cassette, disk, diskette or on memory storage devices such as optical disks, programmable instruments such as telephones, "electronic address books", calculators or any other storage media, together with indicia of use, ownership, possession or control of such records.
 - a. Legal documents including purchase or lease agreements tending to show occupancy and/or ownership of: (1) 5128 E. Roberta Drive, Cave Creek, Arizona; and (2) 3401 W. Buckeye Road, Suite 3, Phoenix, Arizona.
 - b. Any and all documents relating to the e-mail account "baud_father@hotmail.com" and the screen name "baud_father", including but not limited to electronic mail, personal identification, bills, receipts, canceled mail, bank statements, etc.
 - c. Any and all documents including e-mail and chat logs related to account(s) with any Internet, "On Line" or Bulletin Board Services including but not limited to bills, receipts, canceled checks, bank statements, applications and advertisements.
 - d. Any and all diaries, logs, notations, telephone/address books, telephone answering machine tapes, correspondence and/or any other documentation tending to show any correspondence with any companies or person supplying, purchasing, distributing or trading satellite television equipment, including but not limited to devices used to alter satellite television access cards.
 - e. Financial Records - People involved in Fraudulent Crimes often generate a substantial volume of cash. The profits generated by fraudulent means are used to purchase luxury items, vehicle, major appliances, jewelry and real property. These records are invaluable in determining how much profit the perpetrator is making above legitimate reported income and locating how these people utilize the profits from illegal transactions. These records include bank accounts, statements, deposits and withdrawals, loan agreements, sales receipts, investment agreements, income tax records, money wire transfer receipts, etc. It is known that these records are often stored in paper form. It is further known that these records may

also be stored in the form of electronic or magnetic media on recording tapes, microchips, diskettes, disks, disk drives and other electronic and magnetic media storage devices.

- f. Any and all satellite equipment including receivers, dishes and access cards; any and all devices and equipment capable of being used to alter, modify or program satellite access cards including but not limited to descramblers, programmers and encoders.
- g. U.S. Currency – People involved in Fraudulent Crimes often obtain cash funds or negotiable items obtained by fraudulent means that are turned into cash funds during the facilitation of this crime. U.S. Currency transactions by the perpetrator can often go undocumented and represent tangible assets for the perpetrator(s). Currency can then be reinvested to make the money appear “legitimate”, and is often used to obtain personal assets, etc.
- h. Postal Records and Other Commercial Carrier Records – People who commit Fraudulent Crimes often use the United States Postal Service or other private mail and parcel services to facilitate their crime. Things retained by the offender include but are not limited to: Express Mail labels, Commercial Mail Receiving Agency and mail forwarding records, wrapping material, boxes, blank invoices, etc. Perpetrators often retain copies of the postal or express mail shipping receipts and invoices in order to maintain their records.
- i. Telephone Records / Name and Address Records – Telephone bills provide a record of all long distance toll calls which aid in the identification of co-conspirators and the frequency they are contacted. It is known that these records are often stored in paper form. It is further known that these records may also be stored in the form of electronic or magnetic media on recording tapes, microchips, diskettes, disk, disk drives and other electronic and magnetic media storage devices.
- j. International travel records including itineraries, tickets, receipts and passports.

Which property or things:

- were used as a means for committing a public offense(s).
- are being possessed with the intent to use as a means of committing a public offense(s).
- constitutes evidence tending to show that a public offense has been committed, or tending to show that Anthony J. Maldonado, Paul T. St. James, customers thereof, and others known and unknown, have committed the offense(s).

(X) such public offense being: Fraud, Theft of Services, Illegal Control of an Enterprise, Money Laundering and Conspiracy, from January 1, 2000 to present.

You are therefore commanded:

- (X) in the daytime (excluding the time period between 10:00PM and 6:30AM)
() in the nighttime (good cause therefore having been shown)

To make a search of the above-mentioned persons, locations, vehicles, e-mail accounts, and any and all electronic data processing and storage devices, computers and computer systems found within the curtilage of the above listed locations, vehicles or persons. If you find the same or any part thereof, to retain such in your custody or in the custody of the Federal Bureau of Investigation, as provided by A.R.S. 13-3920. Return this warrant to me within five (5) days of the date thereof, as directed by A.R.S. 13-3918.

Given under my hand and dated this 29th day of March, 2001.



Judge
Superior Court, State of Arizona

DIRECTV

HARDWARE



NDS Smart Cards

- NDS smart cards provide subscription programming security controls for broadcasters and program providers.
- Proprietary programming resides within custom circuitry beneath the smart card's gold foil contacts.
- NDS smart cards are similar in size to credit cards; (85.60mm x 53.98mm x 0.76mm).
- Each smart card is identified by unique, electronic identity markings on the bottom.
- Illicitly modified smart cards may not have visibly distinctive alterations.

Copyright 2000, NDS Americas Inc., All rights reserved.



DIRECTV



mm 1 2 3 4 5 6 7 8 9

Period 1

Period 2

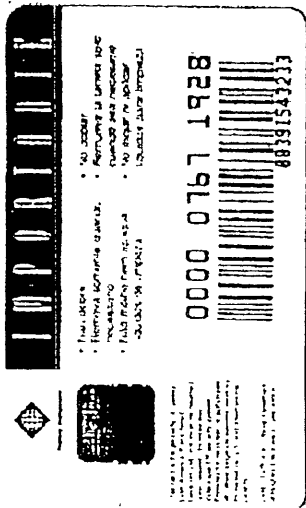
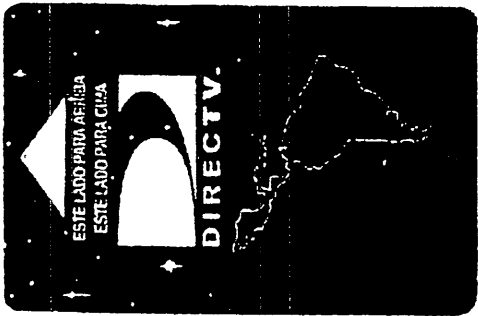
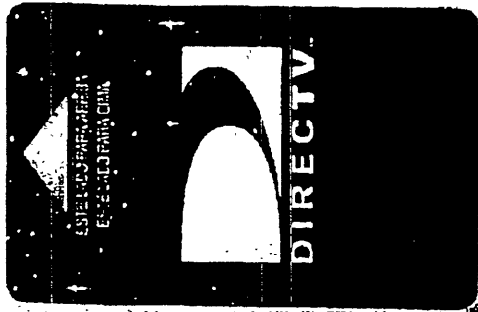
Period 3



Copyright 2000, NDS Americas Inc., All rights reserved.

NDS

GLA Smart Cards

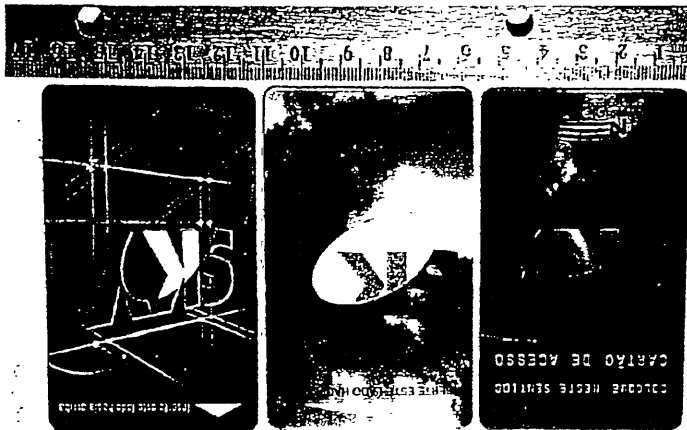


• DIRECTV GLA program services may not be subscribed to from addresses within the U. S.

Copyright 2000, NDS Americas Inc., All rights reserved.



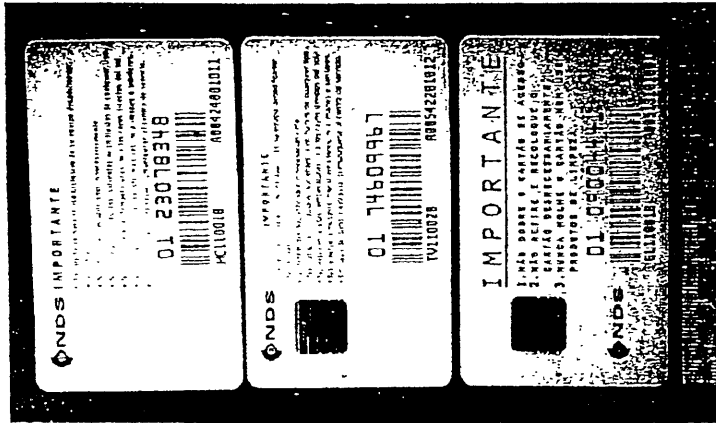
SKY Latin America Smart Cards



Multicountry

Innova

Netsat



• SKY Latin America program services may not be subscribed to from addresses within the U.S.

Copyright 2000, NDS Americas Inc., All rights reserved.



Integrated Receiver Decoder (IRD)

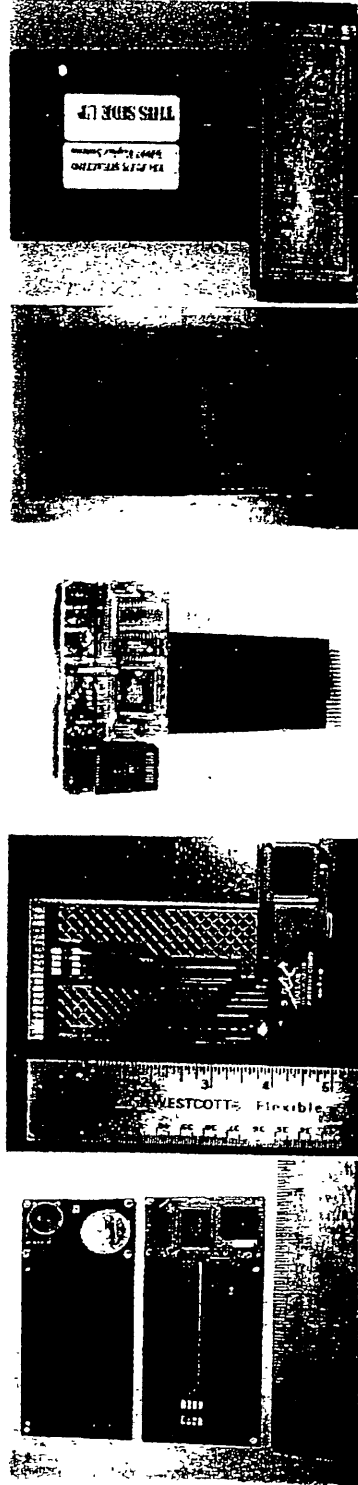


Copyright 2000, NDS Americas Inc., All rights reserved.



Satellite Signal Theft

- A variety of printed circuit boards (PCBs), shown below, emulated and bypassed Period 1 (first generation) NDS smart card security.
- These printed circuit boards included the "battery card", "L card", "T card", "I card", and "Next Generation card". These PCB devices became obsolete in June, 1996 when NDS introduced the Period 2 (second generation) smart card.



Copyright 2000, NDS Americas Inc., All rights reserved.



NDS ISO-7816 Smart Card Programmers

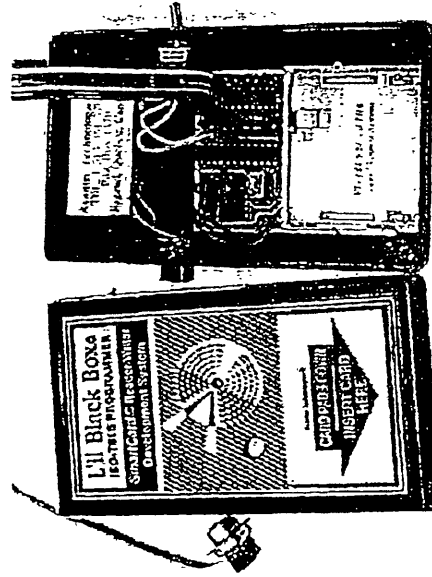
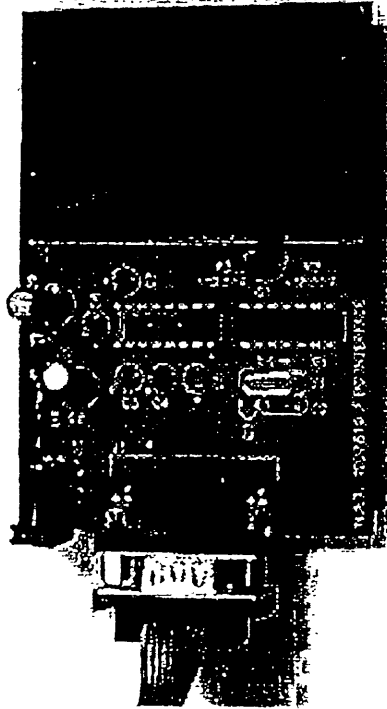
- A smart card that has been illicitly modified may be subject to Electronic Counter Measures (ECMs).
- An ECM is a computer instruction that may disable illicit software in a modified smart card.
- An ECM is sent "over the air" via satellite to all smart cards and is intended to disable only illicit software in modified smart cards.
- Hacker's may refer to disabled smart cards as being "99d" (ninety-nined), "00d" (zeroed), "double O'd", "FF'd", "looped", "dead", or "killed", etc.

Copyright 2000, NDS Americas Inc. All rights reserved.



ISO-7816 Smart Card Programmers

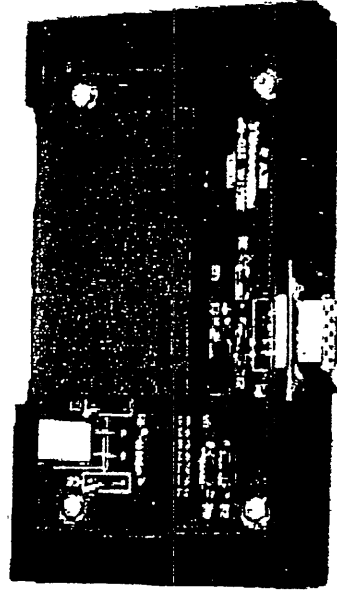
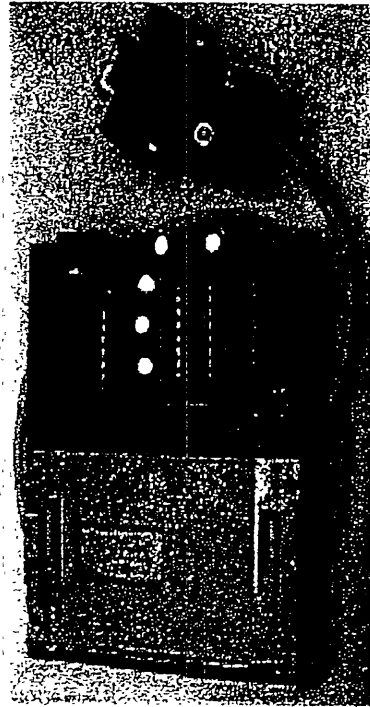
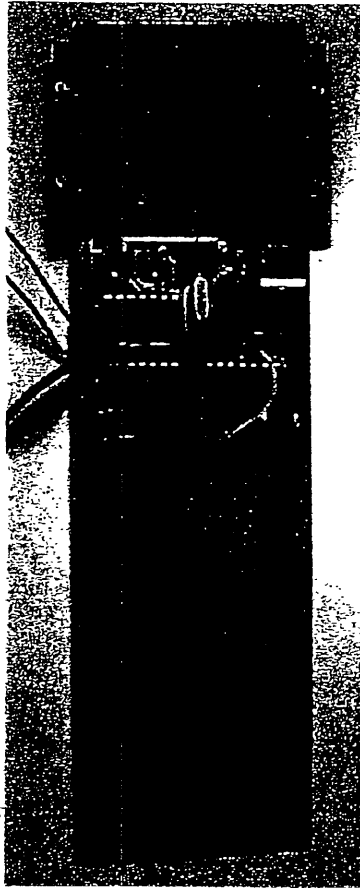
- A variety of ISO-7816 programming devices were developed to illicitly modify NDS smart cards.
- ISO-7816 programmers vary in shape and size and can be used to facilitate satellite signal theft.



Copyright 2000, NDS Americas Inc., All rights reserved.

NDS

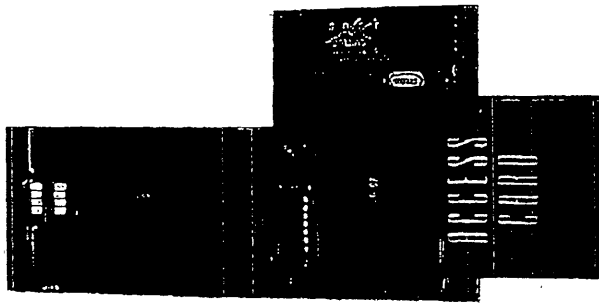
ISO-7816 Smart Card Programmers



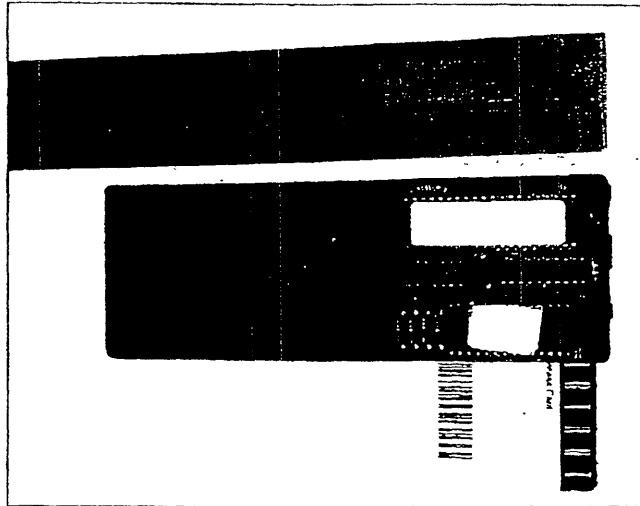
Copyright 2000, NDS Americas Inc., All rights reserved.

- A variety of PCB devices were developed to illicitly circumvent NDS smart card security routines.
- Hackers market these PCB devices as “wedges”, “blockers”, etc. These devices function only with an NDS smart card.
- These PCB devices are typically similar in width and thickness to NDS smart cards, but vary in length.
- These PCB devices have electrical contacts on the bottom, similar to those on NDS smart cards.
- These PCB devices are designed primarily for satellite signal theft.

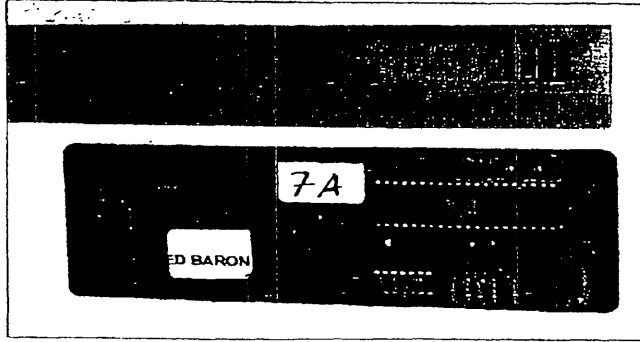
NDS Illicit PCB Devices



DDT card



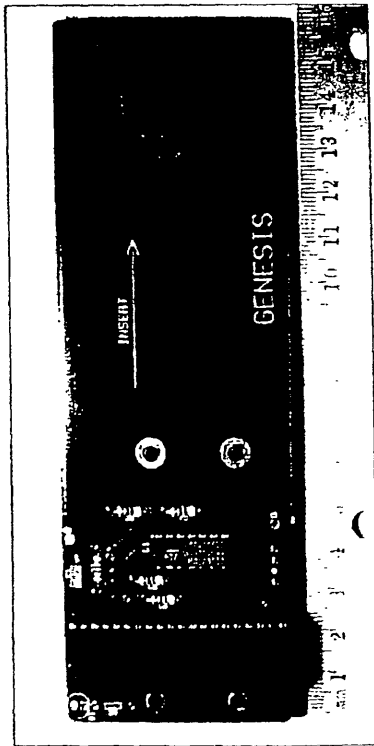
Combo card



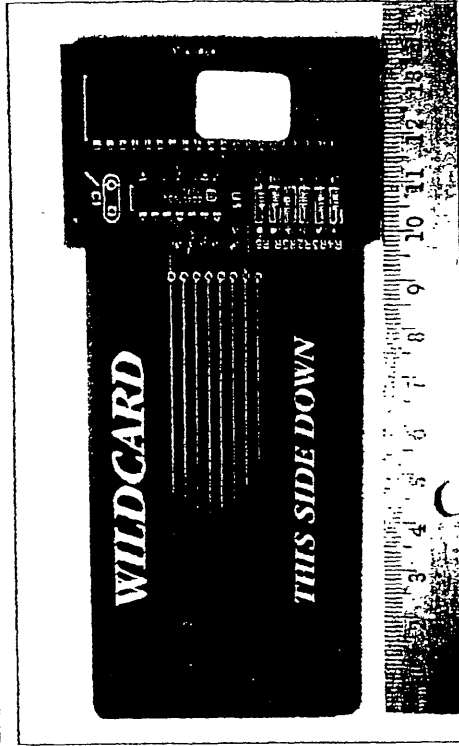
Red Baron
DATS card



Illicit PCB Devices



Genesis PCB

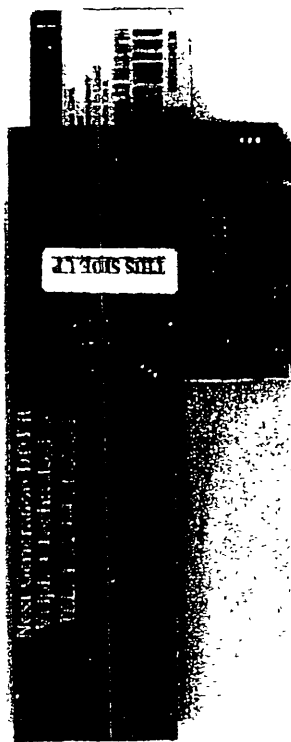


Wildcard PCB

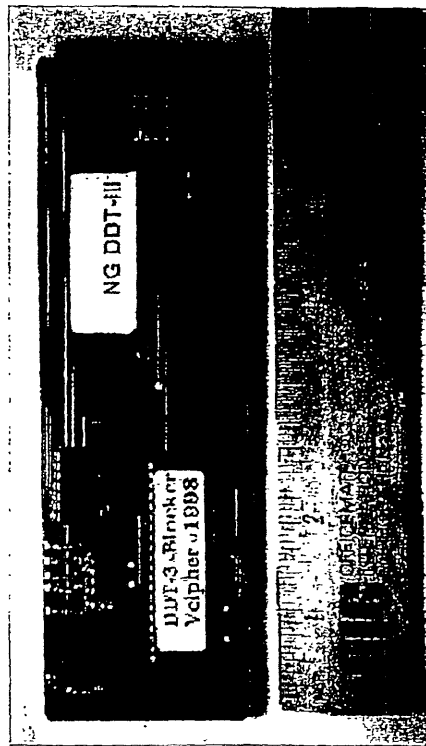
Copyright 2000, NDS Americas Inc., All rights reserved.

NDS

Illicit PCB Devices



**Next Generation
DDT-II**



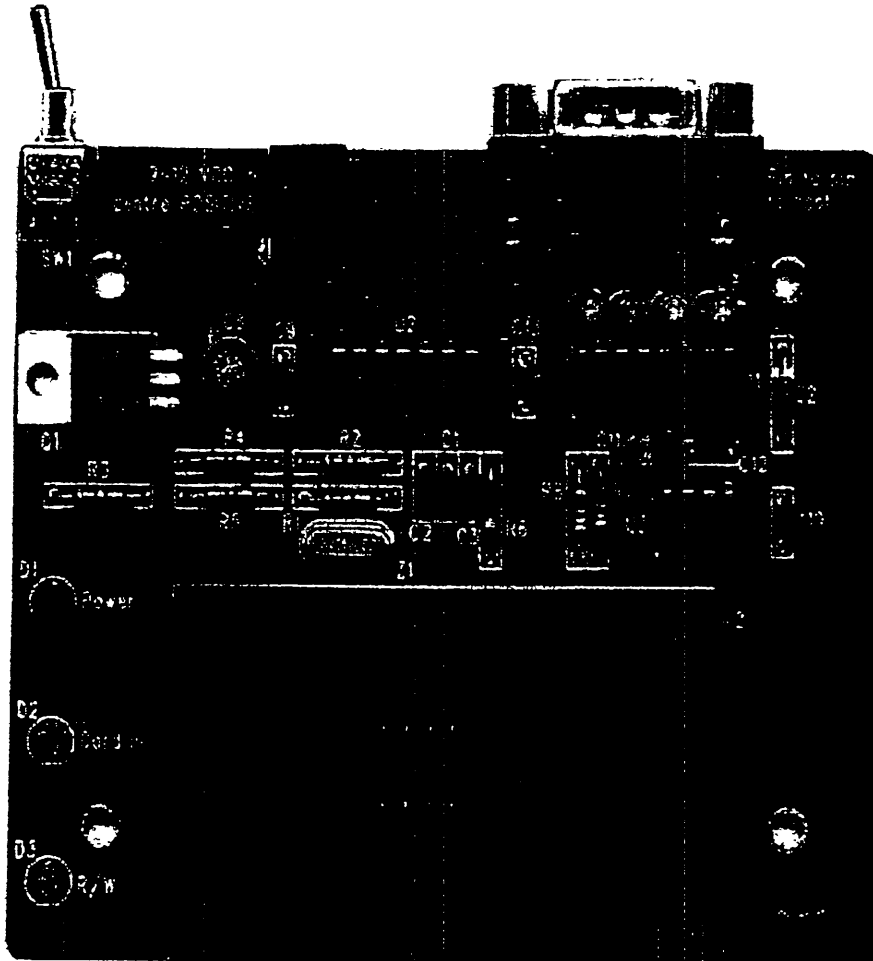
**Next Generation
DDT-III Blocker**

Copyright 2000, NDS America Inc., All rights reserved.

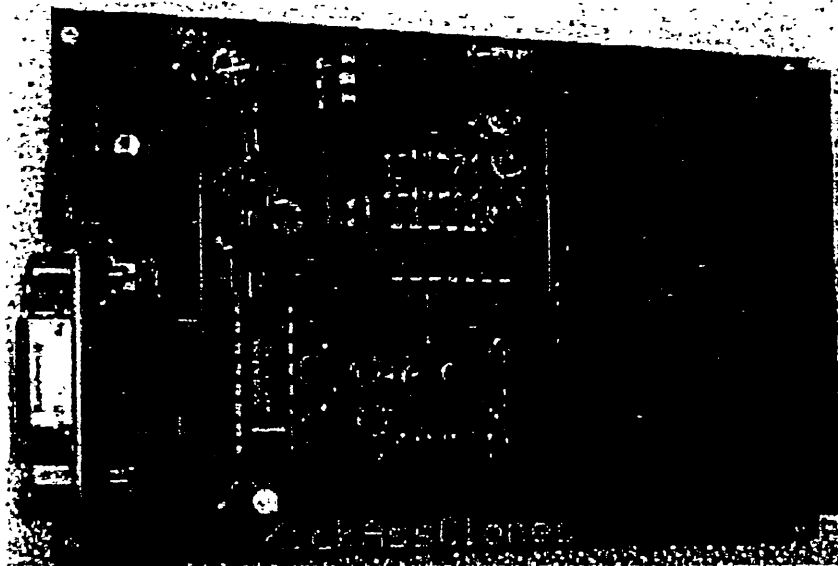
DISH

NETWORK

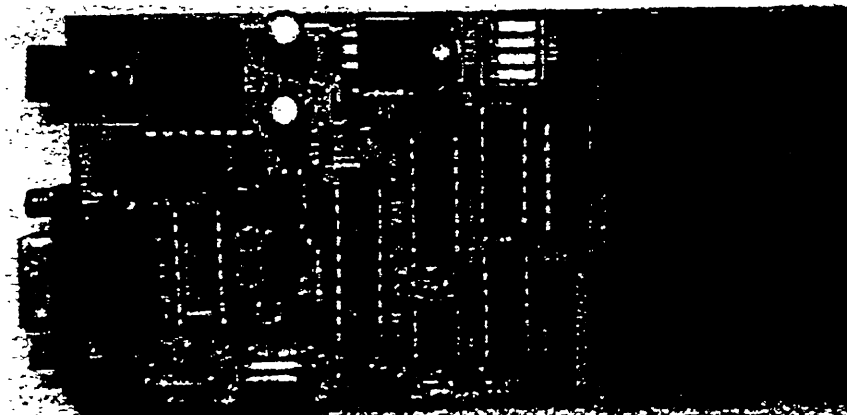
HARDWARE



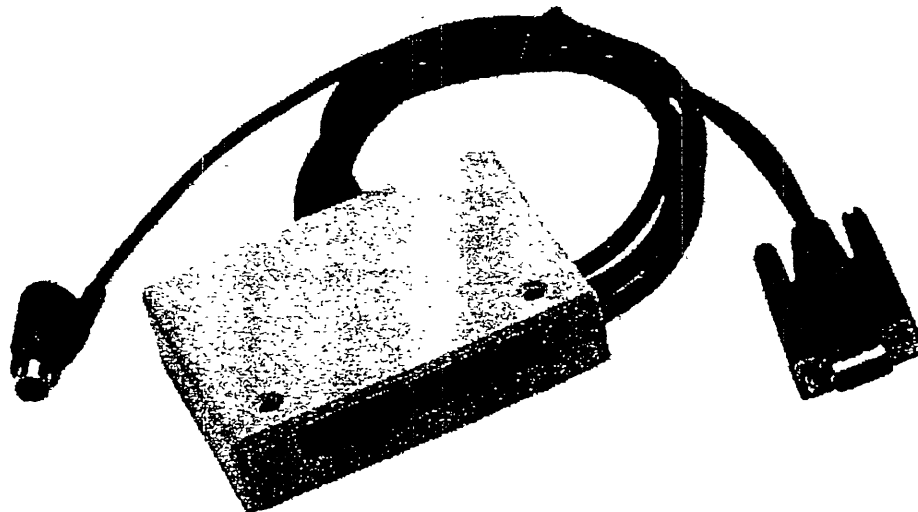
7816 PROGRAMMER



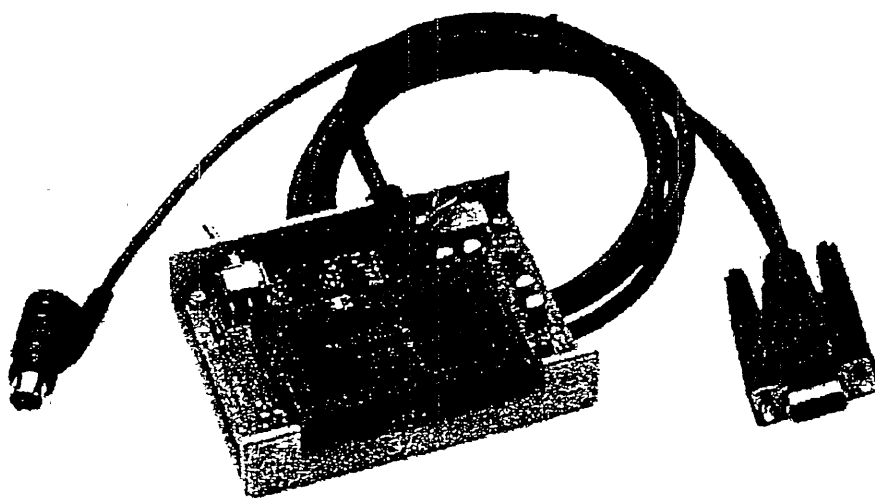
PROGRAMMER

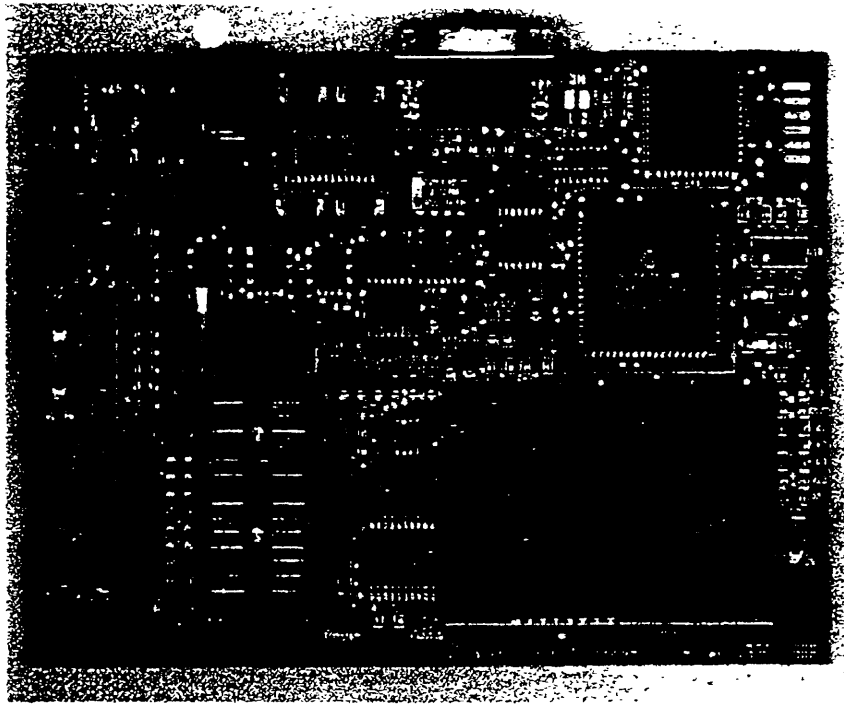


UNLOOPER

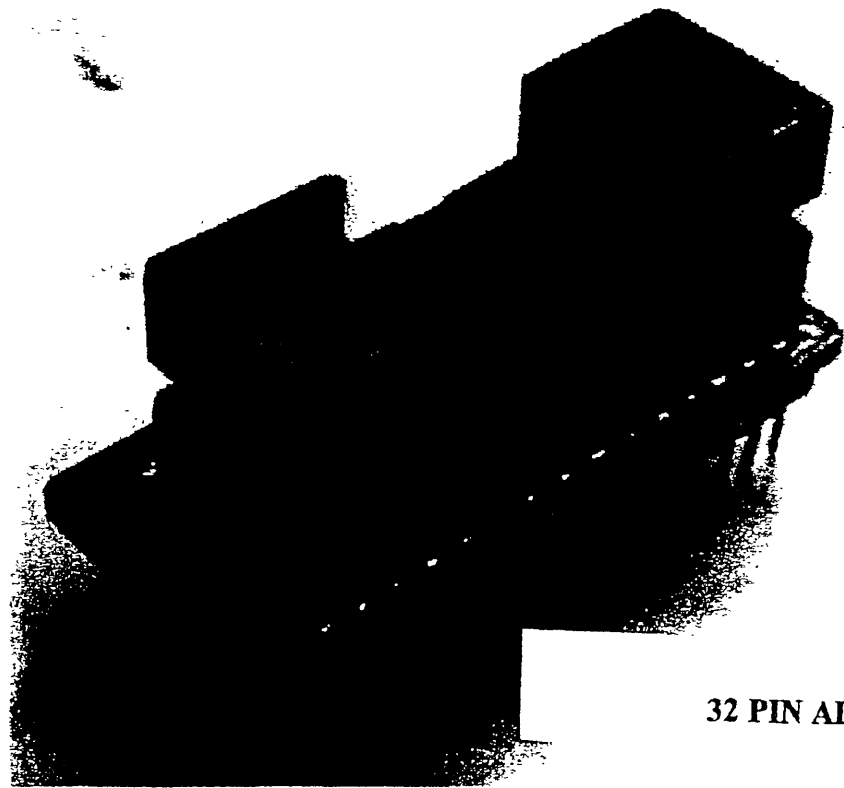


IS0-2 PROGRAMMER

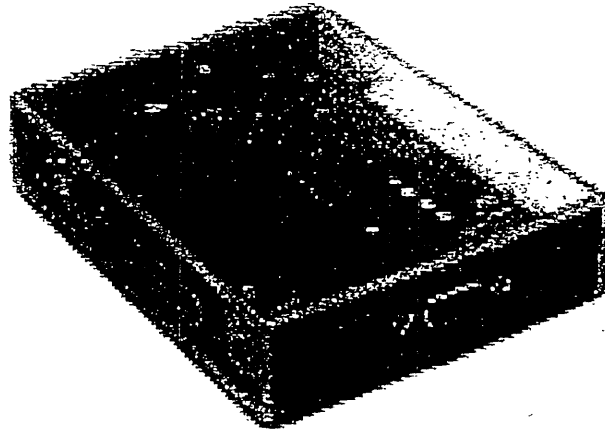




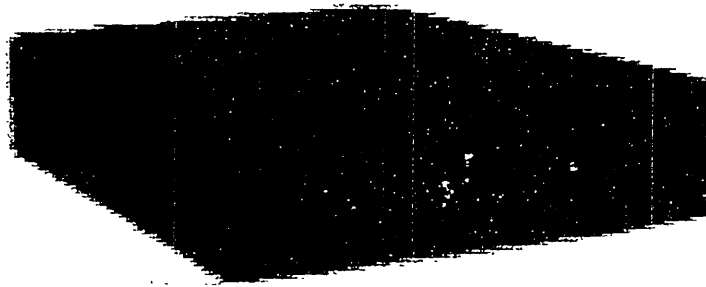
VX MAXI



32 PIN ADAPTER



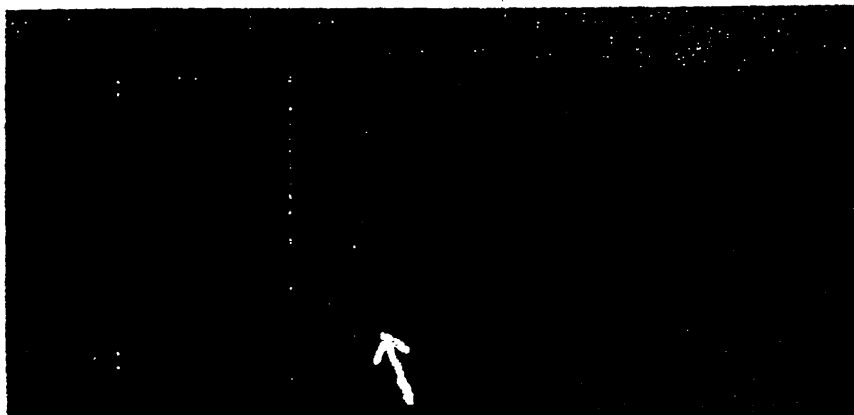
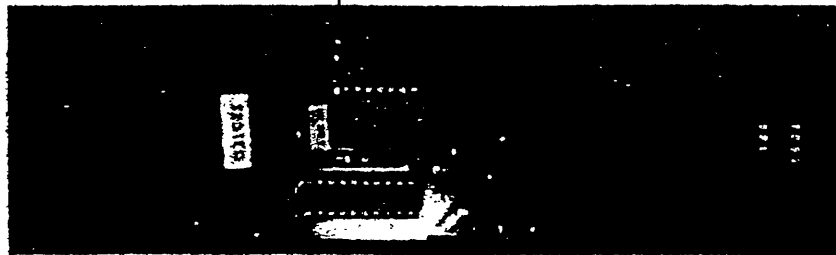
WT2

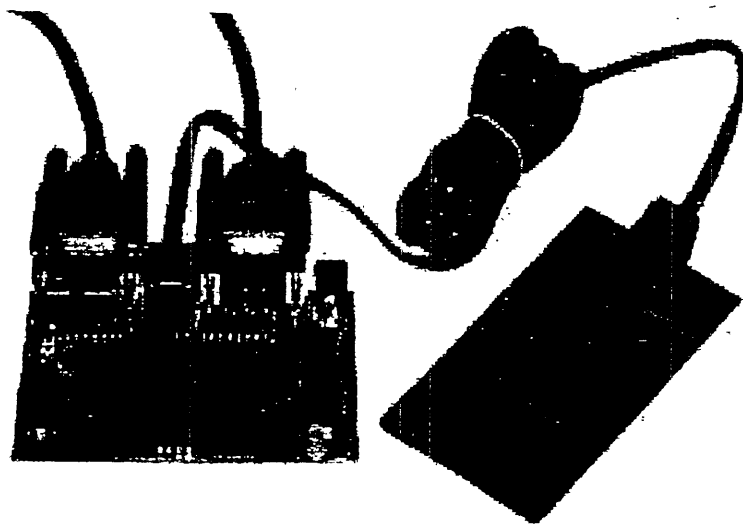


WTX

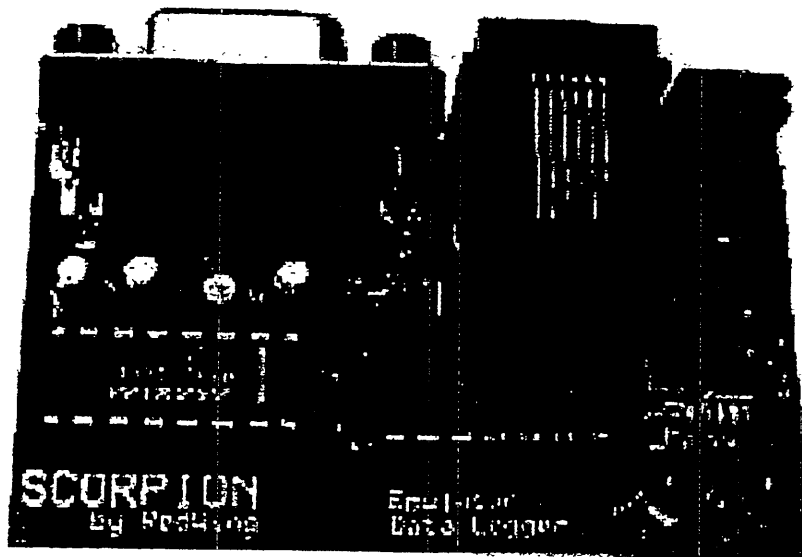


BLOCKER

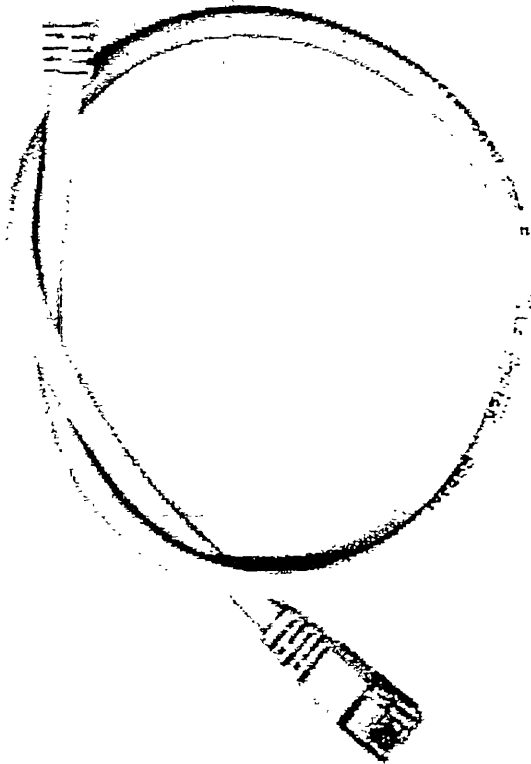




SCORPION EMULATOR



EMULATOR/DATA LOGGER



LOGGER

COPY

Affidavit for Search Warrant
County of Maricopa
State of Arizona

Warrant # _____

Your affiant, Special Agent Stephen A. Belongia of the Federal Bureau of Investigation (FBI), duly sworn, hereby deposes and says:

1. That between on or about January 1, 2000 to present, in the County of Maricopa, State of Arizona, Anthony J. Maldonado, Paul Thomas St. James, customers thereof, and others known and unknown have been and are committing the crimes of Fraud, Theft of Services, Illegal Control of an Enterprise, Money Laundering, and Conspiracy by illegally altering/programming satellite access cards to be able to view satellite services without having to pay for such services.

2. That your affiant has probable cause to believe and he does believe there is now certain property or things that were used as a means for committing the public offense of Fraud, Theft of Services, Illegal Control of an Enterprise, Money Laundering, and Conspiracy, located:

a. On the persons of: (1) Anthony J. Maldonado, a male standing approximately 6'1", weighing approximately 180 pounds, with brown hair, having a birth date of 9/22/1967 and a social security number of 527-99-6546; and (2) Paul Thomas St. James, a male standing approximately 6'3", weighing approximately 230 pounds, with brown hair, having a birth date of 05/12/1967 and a social security number of 136-78-6908.

b. At the locations known as: (1) 5128 E. Roberta Drive, Cave Creek, Arizona. This is a two-story creme colored residence with a rounded tile roof and a two-car garage. On each side of the garage are four decorative raised squares which are brown in color. On the third square

on the right (east) side of the garage are the numbers "5128". To the east of the property is a block wall and a horse property. The residence is the last house on the north side of a cul-de-sac. There is a large rock situated left (west) of the garage. The entrance to the residence is on the right (east) side of the garage and is lit with landscape lights. The location is the principal residence of Anthony J. Maldonado; (2) 3401 W. Buckeye Road, Suite 3, Phoenix, Arizona including any and all warehouse and storage space held as part of the occupancy thereof. This location is a large warehouse building on the south side of West Buckeye Road in Phoenix. The entry parking lot to the warehouse is to the east of 3401 West Buckeye. The building is clearly marked with the numerals "3401" on the north and east facing walls near the top of the building at the northeast corner of the structure. There are two clearly marked tenants of the structure, AutoFit and Bargaintown, which have their company names affixed to the east-facing wall of the warehouse. AutoFit's suites are located at the northern-most part of the warehouse. Bargaintown's sign is located directly above a red-tile roof facade which is situated above the entrance to Suite 3. On the east-facing wall of Suite 3 is a large glass window with the following lettering:

Bargaintown Liquidation
34_(sic) W. Buckeye, Suite 3
Phoenix, AZ 85009
(602)223-2003
www.bargaintown.com

To the left of the window is a glass entry door that is accessed by walking up cement steps on the east side of the building. Suite 3 further consists of two metal roll-up doors located to the north (right) of the entrance to Suite 3. The doors provide access to warehouse space for Suite 3. There is a "Suite 4/Suite D" located to the south (left) of Suite 3 which appears to be vacant. Suite 4 has a "Dream Lounger" logo on the window and a similar sign on the door.

c. In the electronic mail (e-mail) accounts "baud_father@hotmail.com" (to be served on the national headquarters of MSN Hotmail, Inc., 1065 La Avenida, Building 4, Mountain View, California 94043) and "paul@bargaintown.com" (to be served on Paul T. St. James and/or One Call Communications, Inc., 801 Congressional Boulevard, Carmel, Indiana 46032).

d. On/In the electronic devices described as follows: Any computer that may contain the storage of data including, but not limited to, type written notes and photo image(s), computer hard drives, media, discs, tapes and all other storage devices.

e. In the vehicles described as: (1) Anthony J. Maldonado's 1998 Jeep Cherokee, Arizona license plate "611EAW"; and (2) Paul T. St. James' 1995 Dodge pickup, New Jersey license plate GL 200S.

3. Said property or things are believed to be possessed with the intent to use as a means of committing Fraud, Theft of Services, Illegal Control of an Enterprise, Money Laundering and Conspiracy. Said property or things include any item constituting evidence which tends to show that Anthony J. Maldonado, Paul Thomas St. James, customers thereof, and others known and unknown, have committed said offenses.

4. Said property or things are described as follows:

a. Any and all electronic data processing and storage devices, computers and computer systems including central processing units; internal and peripheral storage devices such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage devices or other memory storage devices; peripheral input/output devices such as keyboards, printers, video display monitors, optical readers and related communication devices such as modems; together with system documentation, operating logs and documentation, software and instruction manuals, handwritten notes, logs, user names, passwords and lists.

b. All of the records below, whether stored on paper, on magnetic media such as tape, cassette, disk, diskette or on memory storage devices such as optical disks, programmable instruments such as telephones, "electronic address books", calculators or any other storage media, together with indicia of use, ownership, possession or control of such records.

i. Legal documents including purchase or lease agreements tending to show occupancy and/or ownership of: (1) 5128 E. Roberta Drive, Cave Creek, Arizona; and (2) 3401 W. Buckeye Road, Suite 3, Phoenix, Arizona.

ii. Any and all documents relating to the e-mail account "baud_father@hotmail.com" and the screen name "baud_father", including but not limited to electronic mail, personal identification, bills, receipts, canceled mail, bank statements, etc.

iii. Any and all documents including e-mail and chat logs related to account(s) with any Internet, "On Line" or Bulletin Board Services including but not limited to bills, receipts, canceled checks, bank statements, applications and advertisements.

iv. Any and all diaries, logs, notations, telephone/address books, telephone answering machine tapes, correspondence and/or any other documentation tending to show any correspondence with any companies or person supplying, purchasing, distributing or trading satellite television equipment, including but not limited to devices used to alter satellite television access cards.

v. Financial Records - People involved in Fraudulent Crimes often generate a substantial volume of cash. The profits generated by fraudulent means are used to purchase luxury items, vehicle, major appliances, jewelry and real property. These records are invaluable in determining how much profit the perpetrator is making above legitimate reported income and locating how these people utilize the profits from illegal transactions. These records include bank accounts, statements deposits and withdrawals, loan agreements, sales receipts, investment agreements, income tax records, money wire transfer receipts, etc. It is known that these records are often stored in paper form. It is further known that these records may also be stored in the form of electronic or magnetic media on recording tapes, microchips, diskettes, disk, disk drives and other electronic and magnetic media storage devices.

vi. Any and all satellite equipment including receivers, dishes and access cards; any and all devices and equipment capable of being used to alter, modify or program satellite access cards including but not limited to descramblers, programmers and encoders.

vii. U.S. Currency - People involved in Fraudulent Crimes often obtain cash funds or negotiable items obtained by fraudulent means that are turned into cash funds during the facilitation of this crime. U.S. Currency transactions by the perpetrator can often go undocumented and represent tangible assets for the perpetrator(s). Currency can then be reinvested to make the money appear "legitimate", and is often used to obtain personal assets, etc.

viii. Postal Records and Other Commercial Carrier Records - People who commit Fraudulent Crimes often use the United States Postal Service or other private mail and parcel services to facilitate their crime. Items retained by the offender include but are not limited to: Express Mail labels, Commercial Mail Receiving Agency and mail forwarding records, wrapping

material, boxes, blank invoices, etc. Perpetrators often retain copies of the postal or express mail shipping receipts and invoices in order to maintain their records.

ix. Telephone Records / Name and Address Records - Telephone bills provide a record of all long distance toll calls which aid in the identification of co-conspirators and the frequency they are contacted. It is known that these records are often stored in paper form. It is further known that these records may also be stored in the form of electronic or magnetic media on recording tapes, microchips, diskettes, disks, disk drives and other electronic and magnetic media storage devices.

x. International travel records including itineraries, tickets, receipts and passports.

The following facts establish probable cause for believing that grounds exist for the issuance of a search warrant for the aforementioned items:

5. This affidavit is based on investigation conducted by myself and other law enforcement agents, by individuals working for and on behalf of the victims, DirecTV (also known as DSS) and EchoStar Technologies Corporation (also known as DISH), and by Motorola Computer Group internal investigators. I am familiar with the facts and circumstances of this investigation, and I believe there is probable cause to believe that certain items described above, which constitute evidence and fruits of violations of various Arizona criminal statutes, will be found on the subject persons, at the subject locations, on/in the subject electronic devices, and within the subject vehicles and e-mail accounts described above.

DESCRIPTION OF DIRECTV AND ITS TECHNOLOGY

6. During this investigation, I spoke with representatives of DirecTV and learned the following information about the DirecTV satellite system:

a. DirecTV, a California corporation, has invested more than \$1 billion to develop the United States' first direct broadcast satellite system. DirecTV delivers approximately

210 channels of digital entertainment and informational television programming to homes and businesses in the United States equipped with DirecTV hardware consisting of an 18-inch satellite dish, an integrated receiver/decoder ("IRD") and a DirecTV programming access card which is necessary to operate the IRD. DirecTV's programming currently includes major cable networks, major studio movies and special event programming offered on a pay-per-view basis, and a variety of other sports and special interest programs and packages.

b. NDS Americas, Inc. (NDS) is a developer and supplier of proprietary encryption and "smart card" technology. Among other things, NDS produces the programming access card that allows DirecTV to scramble and unscramble satellite transmissions. The access cards, which are manufactured outside the United States, are sold to consumers as an integrated component of the IRD, and each access card is assigned a unique electronic serial number.

c. All programming distributed by DirecTV is delivered to DirecTV's broadcast centers in Castle Rock, Colorado and Los Angeles, California. At the broadcast centers, DirecTV digitizes and compresses the programming. The resulting signal is encrypted (electronically scrambled) by DirecTV to prevent unauthorized reception. DirecTV then transmits the signal from the broadcast centers to five satellites located in stationary orbit approximately 22,300 miles above the equator.

d. The satellites relay the encrypted signal back to earth, where it can be received by DirecTV's subscribers equipped with satellite receiving dishes and IRDs. The signal is received by the dish and transmitted by wire to the IRD. The IRD (a box approximately the size of a VCR) acts like a computer to process the incoming signal using the credit card sized access card. The access card is inserted into the IRD through a slot in the IRD.

e. The DirecTV access card is sold as an integrated component of the IRD. After a subscriber installs the dish and IRD at his or her home, business, etc. and purchases one or more programming packages, DirecTV electronically activates the subscriber's access card by sending a signal through the satellite data stream. The access card acts as a reprogrammable microprocessor and uses "smart card" technology to: (1) control which DirecTV programming the subscriber receives; and (2) capture and transmit to DirecTV the subscriber's pay-per-view purchases.

f. The access card is a key component in DirecTV's security and accounting systems, as more specifically described below:

i. Security System: To prevent unauthorized signal reception and program viewing, DirecTV's transmissions of television programming are encrypted at DirecTV's broadcast/signal uplink centers. The access card enables the subscriber's IRD to decrypt the signals thereby permitting viewing of programs in accordance with the subscriber's authorized subscription package and pay-per-view purchases.

ii. Accounting System: The access card also handles the tracking of DirecTV pay-per view programming. Pay-per-view purchases are made using a remote control and are recorded on the microprocessor in the subscriber's access card. The access card periodically transmits this viewing history by initiating a telephone call (by means of a modem within the IRD) to DirecTV's Conditional Access Management Center ("CAMC") in Castle Rock. From the CAMC, the information is forwarded to DirecTV's billing system.

g. Beginning in 1995, devices have been available which allow the unauthorized unscrambling of DirecTV programming services without payment of the required fees. These devices have included counterfeit access cards consisting of printed circuit boards with computer

chips mounted on them. It is also possible to reprogram the microprocessor imbedded in the original access card to allow unauthorized and completely free viewing of all DirecTV programming. These products have been advertised on the Internet, in local newspapers, in underground satellite publications and by word-of-mouth. They are also frequently sold by retail satellite equipment dealers. As a result of the theft of satellite television services through the use of counterfeit access cards and reprogrammed original access cards, DirecTV has experienced significant costs and losses associated with lost programming revenue, card replacement, investigative expenses, legal expenses, and periodic electronic signal updates. As an illustration, the cost for replacing DirecTV's first generation access card was in excess of \$25 million.

DESCRIPTION OF ECHOSTAR TECHNOLOGIES CORP.(DISH) & ITS TECHNOLOGY

7. During this investigation, I spoke with representatives of Echostar Technologies and learned the following information about the Dish Network satellite system:

a. Dish Network delivers approximately 700 channels of digital entertainment and informational television programming to homes and business in the United States and its territories. Dish Network utilizes hardware to accomplish the transmission of its signal. The hardware includes an 18-inch satellite dish, an Integrated Receiver/Decoder ("IRD") and a Dish Network smart-card which is necessary to operate the IRD. Dish Network's programming currently includes major cable networks, major studio movies and special event programming offered on a pay-per-view basis, and a variety of other sports and special interest programs and packages.

b. Nagravision is a conditional access system provider and supplier of proprietary encryption and smart-card technology. Nagravision produces the smart-card that allows Dish Network to encrypt and decrypt satellite transmissions. The smart-cards, which are

manufactured outside the United States, are provided to consumers as an integrated component of the IRD. Each smart-card is assigned a unique electronic serial number which must be properly married to the IRD for proper functioning. Dish Network retains legal ownership of its smart-cards at all times.

c. All programming distributed by Dish Network is delivered to Dish Network's up-link center in Cheyenne, Wyoming. At the up-link center, Dish Network digitizes and compresses the programming. The resulting signal is encrypted by Nagravision to prevent unauthorized reception. Dish Network then transmits the signal from Cheyenne to six satellites located in geo-synchronous orbit over the continental United States.

d. The satellites relay the encrypted signal back to earth where it can be received by Dish Network's subscribers equipped with satellite receiving dishes and IRD's. The signal is received by the dish and transmitted by wire to the IRD. The IRD acts as a computer to process the incoming encrypted signal utilizing the smart-card. The smart-card is credit card sized, and is loaded into a slot in the IRD.

e. After installation of the dish and IRD at a residence or business, Dish Network electronically activates the subscriber's smart-card by sending a signal through the satellite data stream. The amount and type of programming activated depends on the services ordered and paid for by the subscriber. The smart-card acts as a re-programmable microprocessor that controls which programs will be decrypted based on the programming package or other programming specifically purchased by the subscriber.

f. The smart-card is a key component of Dish Network's security and accounting systems as described below:

i. Security System: To prevent unauthorized signal reception and programming, Dish Network transmissions of television programming are encrypted at Dish Network's up-link facilities. The smart-card enables the subscriber's IRD to decrypt the signals and permits viewing in accordance with the subscriber's authorized subscription package and pay-per-view purchases.

ii. Accounting System: The smart-card also handles the tracking of Dish Network pay-per-view programming. Impulse pay-per-view purchases are made using a hand-help remote control device and are recorded on the microprocessor in the subscriber's smart-card. At periodic intervals, the IRD transmits the viewing history by initiating a telephone call (via modem within the IRD) to Dish Network's up-link facility. The collected information is then transmitted to Dish Network's billing center.

g. Starting in 1998, devices have been available which allow the decryption of Dish Network's programming services without authorization and without payment of the necessary fees. Devices utilized to obtain unauthorized reception include, but are not limited to, smart-cards, software, "programmers", "un-loopers", emulators, "blockers", "AVR's", and computers. These products have been advertised on the Internet, in local publications and in underground satellite publications. They are often sold by retail satellite equipment dealers as well. The result of the theft of satellite television services through the use of altered smart-cards and other programming equipment has cost Dish Network significant losses in revenue. These losses include lost programming revenue, investigative expenses, legal expenses and card replacement costs. Dish Network has also incurred costs for having to periodically update its signal to curtail these activities.

INVESTIGATION

8. In November, 2000, representatives of DirecTV's Signal Integrity Office advised the FBI of an ongoing investigation into the programming, distribution and possession of illegally modified access cards for the DirecTV satellite system. The primary target of the investigation was Anthony J. Maldonado, a network engineer for Motorola Computer Group in Tempe, Arizona. To facilitate its investigation in Phoenix, DirecTV retained the services of retired FBI Agent Al Zumpf, a private investigator for GBI and Associates. Subsequent to opening their case, DirecTV learned that Rick Pitocco of Motorola's Global Security Office was also investigating the matter. Thereafter, Motorola agreed to cooperate with the DirecTV investigation.

9. The results of the collective investigations by the FBI, DirecTV, Echostar Technologies (DISH), and Motorola revealed that Anthony J. Maldonado was illegally modifying and distributing DirecTV access cards. It was further determined that beginning in approximately September, 2000, Maldonado and his partner, Paul T. St. James, began modifying and distributing illegal access cards for the DISH satellite system via a Mexican based Internet Website.

10. During the course of the investigation, Pitocco provided the following e-mail messages to/from Maldonado's Motorola e-mail account:

- i. Date: March 23, 2000
From: Tony Maldonado
To: Paul St. James; Chris Crawford; Gerado Hernandez; J.I. Lee;
Henry Chung; Jim Jones; Troy Young; Norman Collins.
Re: Stuff

"Hope this helps you guys, with your TV viewing!!! I will be doing some mods but if (you) guys could help it would be great!!!" Attached to the e-mail was information regarding IRD receivers, reboot procedures and ways to prevent DirecTV from "writing to your receiver". The author of the document is listed as "The Baud Father".

ii. The following e-mails are related:

Date: July 10, 2000
From: Tony Maldonado
To: Al Berumen; Cris Crawford; J.L Lee; Troy Young
Re: Stuff

"I have some stuff for sale to help with viewing pleasure...250
eggs, for one piece of ham, ready to go."

Date: July 11, 2000 (6:02 AM)
From: Troy Young
To: Tony Maldonado
Re: Stuff

"Are you talking about the H* Hack?..."

(Note: H* refers to DirecTV access cards)

Date: July 11, 2000 (8:51 AM)
From: Tony Maldonado
To: Troy Young
Re: Stuff

"I have extra H cards..."

iii. Date: August 25, 2000
From: Tony Maldonado
To: 'paul@bargaintown.com'
Re: DSS History

"Here is a little history lesson about the DSS system from the
beginning."

Attached to the e-mail was an eight page narrative detailing
the development of the DSS (DirecTV) system including a discussion of encryption methods and the
history of "hacking" DSS/DirecTV access cards.

iv. Date: September 26, 2000
From: Paul St. James [paul@bargaintown.com]
To: Tony Maldonado
Re: Canada Info.

This e-mail consisted of an itinerary for a trip to Toronto,

Canada. The e-mail indicated that both Maldonado and Paul St. James were scheduled to make the trip on September 7, 2000. The e-mail is signed by "Paul St. James (602)233-2003".

(Based on discussion with DirecTV and DISH security personal, it is known that many of the top tier hackers who have been responsible for compromising DirecTV and DISH access cards reside in Canada.)

v. Date: October 21, 2000
From: Paul St. James [paul@bargaintown.com]
To: Tony Maldonado
Re: Disclaimer

"I think this should be added to all order forms. I stole the language from another site that does (off color type stuff)... 'I understand that I must be at least 21 years of age to order any satellite cards or programming from Kobalt.com and that I am responsible to know whether or (sic) these cards or programming are legal in the area I am asking Kobalt.com to send this/these cards. I am also not part of any task force or government agency working against satellite pirates and I further agree that anything I receive from Kobalt.com can not be used as evidence in any form. I agree to take full responsibility for this/these satellite cards/programming.'"

vi. Date: October 23, 2000
From: Paul St. James [paul@bargaintown.com]
To: Tony Maldonado
Re: To Do List

"...4. Get last name so we can wire money, 5. Put website on laptop..."

vii. Date: October 26, 2000
From: Paul St. James [paul@bargaintown.com]
To: Tony Maldonado
Re: New Address

"Kobalt
282 North Grand Court Plaza
PMB 144
Nogales, AZ 85621"

viii. Date: November 2, 2000
From: Paul St. James [paul@bargaintown.com]
To: Tony Maldonado
Re: Foreign system

"...If I turn my Dish 500 (DISH satellite system) towards the

foreign station sat (satellite) today, will I see those stations or do you have to do a further modification?... (I have a guy who wants 10 units if I can show him these stations)."

ix. Date: November 10, 2000
From: Troy Young
To: Tony Maldonado
Re: H

"...are you still doing H (DirecTV) cards. If so I have a new one for you to do..."

x. Date: December 5, 2000
From: Tony Maldonado
To: Al Berumen; Chris Crawford; J.L. Lee; Joe Balderrama;
Norman Collins; Pete Goolsby; Troy Young
Re: New Site

"My new site for dishes, pass it around <http://www.kobalt.com.mx>. Thanks."

xi. Date: December 18, 2000
From: Tony Maldonado
To: 'Bargaintown'

"Paul here is the address to ship the 4922 unit (DISH system). He wants us to make up an address and not use Bargaintown address. He sent me 525.00 cash for the unit... You will get a FedEx package on Monday morning for the 4922 receiver. I sent it under Richard Weinstein I think and enclosed cash. The address to send it to is; Andrew Lucin, 28005 Pontevedra Drive, Rancho Palos Verdes, California 90275, (310)832-8641. I also included funds to ship it to him. If you could send that out on Monday and send me a track # that would be great. I will have more orders coming to you this week. Also could you label it CMOS Ltd for the shipper and make up an address in CA. Thank you."

xii. Date: January 26, 2001
From: Tony Maldonado
To: 'Bargaintown'
Re: Texas

"Here is the phone for the guy in Texas, I already gave them Bargaintown's name. They should know the story about the B stock. Bulverde Home Theater, 2749 Bulverde Rd, Bulverde, Texas 78163, (800)358-5894..."

11. On November 26, 2000, Al Zumpf of GBI and Associates, working on behalf of

DirecTV and DISH, obtained a five-page printout of the Internet website <http://www.kobalt.com.mx>.

The site advertises various DISH systems for sale and includes the following statements:

- a. Complete Satellite Systems - Programmed
- b. These Dish Network receivers are fully enabled to view ALL channels!!
- c. Apply future patches, fixes or extract keys from card 50.00 US
- d. Thank you for viewing our site, this is our debut on the world wide web. We had been an underground company but decided to take our product public...The Dish Software is an autoroll 3m and has been running since October 1999. Due to the nature of this business we will be offering a 6 month warranty on the access card only. If the card goes down we will attempt to fix it and return the card to you ASAP!! After the warranty period has expired there will be a flat 50.00 repair/reprogramming fee.
- e. **DISCLAIMER.** By entering this site I promise that I will NOT be using any of these devices to steal DirecTV or Dish Network programming. If I live in the USA, I realize I am committing a CRIME by using these devices on DirecTV or Dish Network cards. Furthermore I am well aware that these devices are for educational use and not to be used to defraud any business legally selling programming in my area.

12. In November, 2000, using the undercover screen name of "Susiek1010@aol.com", Zumpf initiated a covert purchase of a DISH system via the Internet Website www.kobalt.com.mx. Zumpf also requested a modified DirecTV access card for his "parents". The following e-mail correspondence is related to the transaction:

a. Date: 11/28/2000 (7:41 PM)
From: baud_father@hotmail.com (Baud Father)
To: Susiek1010@aol.com

"...we currently have the 4922 and 2700 in stock (DISH Network systems)...4922 system is 600.00 US 2700 system is 450.00 US...cash or international US postal money order...All money orders must have all carbon copies intact and the name must be left blank...We will send all products by UPS from the US since our mail system here in Mexico is very slow and not reliable...I understand that I must be at least 21 years of age to order any products from Kobalt.com.mx and that I am responsible to know whether or not these cards or programming are legal in the area I am asking Kobalt.com.mx to send this/these products. I am also not part of any task force or government agency working against satellite pirates and I further agree that anything I receive from Kobalt.com.mx can not be used as evidence in any form. I agree to take full

responsibility for this/these satellite products/programming. Kobalt 282 North Grand Court Plaza, PMB 144, Nogales, AZ 85621..."

b. Date: 11/28/2000 (8:57 PM)
From: Susiek1010
To: baud_father@hotmail.com

"...Also, I have a DSS (DirecTV) access card that I would like to have modified to receive all channels. Can you do this for me? I'd like to give the card to my parents as a Christmas present...If you can do this, what would be the cost? Should I send the card to your Nogales address..."

c. Date: 11/30/2000
From: baud_father@hotmail.com (Baud Father)
To: Susiek1010@aol.com

"We ship same day UPS ground so depending on where you live it could take 2 to 5 days. If you want one I will make sure it's there by Christmas, we want to make everyone happy. I really don't do DSS (DirecTV) but if you buy a DISH system I will program an H card...for 50.00 US...We do warranty all DISH cards from going down."

d. Date: 12/8/2000
From: baud_father@hotmail.com (Baud Father)
To: Susiek1010

"...We have been selling these things like crazy..."

13. On December 7, 2000, Zumpf sent a \$500 International Postal Money Order, #74053414337, and a DirecTV access card, #000060964012, to the Kobalt, 282 North Grand Court Plaza, PMB 144, Nogales, Arizona 85621. \$450 was for the illegally modified Dish System, and \$50 was for the modification of the DirecTV access card.

14. On December 14, 2000, Zumpf received two UPS packages/boxes shipped from Everyday Mail, 282 N. Grand Court Plaza Drive, Nogales, Arizona. The boxes were wrapped in brown packaging paper and were shipped to "Susie Kelly", Zumpf's undercover alias. The first package weighed approximately 16 pounds and contained a DISH Network satellite dish and various

equipment. The second package contained: (1) a DISH Network integrated receiver/decoder (IRD), model 2800, serial number RDECVK20965G; (2) access card "S 00 0932 0682 92" for the DISH System; and (3) DirecTV access card "0001 6345 9522" which was contained in a small plastic bag within the box (Note: as detailed in paragraph 13 above, Zumpf originally sent Kobalt DirecTV access card #000060964012).

a. Affixed to the first box containing the satellite dish was the following UPS mailing label:

From: Shipping & Receiving Dept.
Bulverde Home Theater
2749 Bulverde Road
Bulverde, TX 78163

To: Paul Thomas St. James
(602)233-2003
3401 West Buckeye Road, Suite 3
Phoenix, AZ 85009

The label noted that the box was "2 of 50", and indicates that the box was first shipped from Bulverde Home Theater in Texas to Paul St. James at 3401 W. Buckeye Road, Suite 3 in Phoenix. The box was then apparently shipped from Everyday Mail in Nogales, Arizona to Susie Kelly, Zumpf's undercover alias.

b. Zumpf forwarded the DirecTV access card, "0001 6345 9522", to NDS Americas, Inc. who conducted a forensic evaluation to determine if the card had been illegally modified. On December 19, 2000, NDS advised that said access card "was illicitly modified for the primary purpose of satellite signal theft".

c. Zumpf forwarded the Dish System access card, "S 00 0932 0682 92", to Russ Densmore, Security Manager at Echostar Technologies Corp. (the owner of DISH). Densmore sent

the card to NagraStar, the manufacturer of its access cards, and a forensic evaluation was conducted to determine if the card had been illegally modified. NagraStar advised that access card "S 00 0932 0682 92" had "been tampered with to receive services without legal subscription...all indication of analysis signifies that alteration to coding was conducted to steal and receive unauthorized satellite signals."

15. As noted in paragraph 10 above, several e-mails were sent to or received from "Paul St. James" at the e-mail address paul@bargaintown.com". A review of the Qwest Business White Pages revealed a listing for Bargaintown Liquidators at 3401 W. Buckeye Road, Phoenix, Arizona, phone number (602)233-2003 (the same phone number used by Paul St. James in the 9/26/00 e-mail). This phone number is also printed on the window of Bargaintown Liquidators, 3401 W. Buckeye Suite 3 in Phoenix. In addition, the Discovery database, which provides credit header information, contained a listing, dated 4/2000, for Paul T. St. James at 3401 W. Buckeye Road, Suite 3, Phoenix, Arizona.

16. A search of Maricopa County property records revealed that Anthony Joseph Maldonado purchased the residence at 5128 E. Roberta Drive, Cave Creek, Arizona 85331 in May, 1999.

17. On December 20, 2000, Zumpf advised that telephone number 602-233-2003 was listed as the business telephone of DirecTV subscriber Pat Clark, 2104 E. Sapium Way, Phoenix, Arizona 85048.

18. During the investigation, I retrieved the following items from a garbage can located at Maldonado's residence, 5128 E. Roberta Drive, Cave Creek, Arizona:

Date Retrieved: December 20, 2000

a. Five-page printout of Internet web-page "<http://www.bulverdehometheater.com/index.htm>". The printout advertises electronics for sale from Bulverde Home Theater, phone number (800)358-5894. Page one of the printout includes advertisements for Dish Network and DirecTV satellite systems. A date on the pages indicates the material was printed on 11/21/2000.

Date Retrieved: January 4, 2001

- b. The following information from an empty Dish Network satellite system box:
- i. Smart Card Number: S000761638696
 - ii. Serial Number: RDECTK1381E
 - iii. Receiver CaId #: R0027994152
 - iv. Product Data: 4922T

(Russ Densmore of Echostar Technologies advised that as of March 5, 2001, the above receiver and smart-card are listed as "stock-shelved". A listing of "stock-shelved" indicates that the receiver and smart-card have not been activated for service by Dish Network. The receiver and smart-card were originally shipped to Costco Wholesale in Tolleson, Arizona.)

Date Retrieved: January 18, 2001

- c. NEBS Service & Repair catalogue cover addressed to "Anthony Joseph Maldo(sic) The Baud Father", 5128 E. Roberta Drive, Cave Creek, Arizona 85331.
- d. One half of a "CitiBusiness" solicitation letter addressed to "Anthony J. Maldonado The Baud Father", 5128 E. Roberta Drive, Cave Creek, Arizona 85331.
- e. Advanta credit card solicitation letter addressed to "Anthony Maldonado Owner Baud Father", 5128 E. Roberta Drive, Cave Creek, Arizona 85331.

f. DHL air bill and \$48 invoice from Video Printer Inc., Morganville, New Jersey for a "Sony NP-FM50 Battery".

19. On January 19, 2001, surveillance was conducted of Bargaintown Liquidators, 3401 W. Buckeye Road, Suite 3. The following noteworthy items were observed:

(All times are approximate)

a. 4:30 pm: An unidentified male was observed peering into the passenger side of a grey truck. The truck was subsequently determined to be a Dodge pickup bearing New Jersey license plate GL 200S registered to Paul St. James. The male walked from the truck and entered the south (left) roll-up door located on the north side of the entrance to Suite 3.

b. 4:32 pm: An unidentified male wearing a yellow shirt was observed throwing trash into a dumpster from the north (right) roll-up door located on the north side of the entrance to Suite 3.

c. 4:46 pm: An unidentified male wearing a white shirt and red baseball cap was observed throwing a pallet into a dumpster from the north (right) roll-up door located on the north side of the entrance to Suite 3.

d. 4:54 pm: An unidentified individual was observed exiting the south (left) roll-up door, located on the north side of Suite 3, and placing something in back of the grey truck. The individual then returned inside the building through the roll-up door.

e. 5:15 pm: A conversion van arrived and parked next to the grey pickup. The van was subsequently determined to bear Arizona license plate 373EPD registered to Paul Thomas St. James.

f. 5:23 pm: Both roll-up doors on north side of Suite 3 were closed.

g. 5:28 pm: A Jeep Cherokee arrived and parked next to the grey truck and the conversion van. An unidentified male was observed exiting the Jeep and entering Suite 3. The Jeep was subsequently determined to bear Arizona license plate 611EAW registered to Anthony Maldonado.

h. 6:45 pm: The grey truck, Jeep Cherokee and conversion van exit the location.

20. On February 21, 2001, I entered the public lobby of Suite 3 and observed the

following:

- a. An "L" shaped glass display case on the south and west walls of the suite;
- b. A DSS/DirecTV satellite dish affixed to the wall above the display case;
- c. A hallway and what appeared to be a series of offices on the north (right) side

of the hall; on the south (left) side of the hallway, a room containing a copy machine was observed.

21. On March 5, 2001, Jim Whalen of DirecTV, Signal Integrity Division, advised the

following:

"On January 21, 2001, DirecTV and NDS Americas, Inc. launched an electronic countermeasure (ECM) through the data stream for the purpose of deactivating illegal Period 2 access cards. This ECM was the most effective countermeasure ever sent by DirecTV and NDS. It effectively disabled thousands of illegally modified H cards and rendered them useless. However, shortly thereafter, the Period (HU) access card was compromised and those involved in H card piracy moved to illegally modifying the HU card. It should also be noted that the H card can still be effectively utilized if used in conjunction with an emulator board and computer. The emulator board is a device which plugs into an Integrated Receiver-Decoder and acts like a genuine H card even though it isn't. The emulator board circumvents the DirecTV/NDS ECMs and allows for illegal satellite reception of all DirecTV programming. Electronic countermeasures are launched daily in an effort to combat satellite piracy and have a limited impact on the criminal activity."

22. Your affiant requests that a search warrant be issued commanding an immediate search to be made of the persons, locations, vehicles, e-mail accounts, and/or electronic devices described herein for the property and things herein described and that the same be retained in the custody of affiant or in the custody of the agency which affiant represents and disposed of according to law, pursuant to A.R.S. 13-3920.

23. It is anticipated that representatives from DirecTV and EchoStar Technologies will be present at the search sites acting as technical advisors to law enforcement agents.

Steph A. Belong
Federal Bureau of Investigation

Subscribed and sworn to before me this 2nd day of March, 2001.

[Signature]
Judge
Superior Court, State of Arizona

COPY

GBI & Associates
3030 N. Third Street
Suite 200
Tel: 602-241-8555
Fax: 602-241-8544
Phoenix, Arizona 85012
e mail: gbiassociates@att.net
Web: www:gbiassociates.com

December 7, 2000

Mr. Russ Densmore
Security Manager
Echostar Technologies Corp.
90 Inverness Circle East
Englewood, CO 80112

Re: Anthony J. Maldonado
GBI File 200-43A

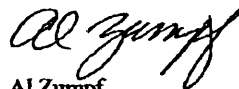
Dear Mr. Densmore:

Enclosed is Dish Network access card S 00 0598 0753. This is the subbed Dish card you furnished in conjunction with our investigation in captioned matter. The card had been provided to Maldonado who allegedly modified it to illegally receive all Dish Network channels.

Also enclosed is an original evidence inventory form to maintain 'chain of custody'. Please advise the results of your laboratory examination of the card.

Thank you for your assistance in this matter.

Very truly yours,



Al Zumpf
Managing Partner

1 cc: James F. Whalen, Signal Integrity, DirecTV

DISH NETWORK EVIDENCE INVENTORY FORM

A. FILE NUMBER GBI 200-43A

B. SOURCE OF PROPERTY AL ZUMPF

C. PROPERTY RETAINED:

<u>Item No.</u>	<u>Description</u>	<u>Container</u>	<u>Quantity</u>	<u>Date</u>
<u>1</u>	<u>DISH CARD 500 0598 0753</u>	<u>ENVELOPE</u>	<u>1</u>	<u>12/7/00</u>
<u>2</u>	<u>FEDEX AIRBILL</u>	<u>"</u>	<u>"</u>	<u>"</u>
	<u># 8214 4859 6522</u>			

D. CHAIN OF CUSTODY

<u>Date Received</u>	<u>Signature</u>	<u>Item No.</u>	<u>No. of items</u>
<u>12/5/00</u>	<u>AL ZUMPF</u>	<u>1</u>	<u>1</u>
<u>12/6/00</u>	<u>[Signature]</u>	<u>1</u>	<u>1</u>
<u>12/6/00</u>	<u>[Signature]</u>	<u>2</u>	<u>1</u>
<u>1/9/01</u>	<u>[Signature]</u>	<u>1</u>	<u>1</u>
<u>2/6/01</u>	<u>[Signature]</u>	<u>1</u>	<u>1</u>
<u>2/16/01</u>	<u>[Signature]</u>	<u>1</u>	<u>1</u>