

# GBPPR 'Zine



Issue #33 / The Monthly Journal of the American Hacker / December 2006

*"The president approached Herbert Shugart, the father of Randall Shugart, and held his hand out. To his astonishment, the handshake was declined. 'The blame for my son's death rests with the White House and you. You are not fit for command.' Clinton reeled under the onslaught, which continued for several moments. As Commander in Chief, President Clinton could have simply accepted responsibility for the loss and sympathized with a grieving father. Instead, he took fifteen minutes out of his schedule to explain to Herbert Shugart why the death of his son was not his fault. It was a craven performance that horrified the Pentagon officials who were present. Immediately after that meeting, White House officials tried to keep the incident quiet and it was successfully suppressed until the story appeared in the London Sunday Times."*

--- Excerpt from *The Next World War* by James Adams, discussing the death of an U.S. soldier in Somalia in 1993.

## Table of Contents

- ◆ **Page 2 / Bell System KS-8455 Test Set Description and Use**
  - ◆ Old school Bell System device for finding faults in outside plant telco wiring.
- ◆ **Page 7 / Nortel DMS-100 Audible Alarm Table (AUDALARM)**
  - ◆ Beep, Beep, Boop, Beep, Boop.
- ◆ **Page 9 / Nortel DMS-100 Customer Protection Table (CUSTPROT)**
  - ◆ Table data protection schemes on a DMS-100 switch.
- ◆ **Page 13 / Simple Night Vision Viewer**
  - ◆ Simple trick to turn an old video camera view finder into a night vision device.
- ◆ **Page 21 / Improvised Counter-I.E.D. Armor**
  - ◆ Finally, a use for Maxtor hard drives.
- ◆ **Page 42 / Rising From The Underground**
  - ◆ Reprint of a March 1994 Nuts & Volts article on HoHoCon '93.
- ◆ **Page 57 / Bonus**
  - ◆ Number One!
- ◆ **Page 58 / The End**
  - ◆ Editorial and rants.

# Bell System KS-8455 Test Set Description and Use

BELL SYSTEM PRACTICES  
Plant Series

SECTION 106-020-100  
Issue 2, July 1969  
AT&TCo Standard

## KS-8455 TEST SET DESCRIPTION AND USE

CONTENTS	PAGE
1. GENERAL . . . . .	1
2. DESCRIPTION . . . . .	1
3. INSULATION RESISTANCE MEASUREMENTS . . . . .	2
4. TESTS FOR GROUNDS . . . . .	3
5. SHORT CIRCUITS AND CROSSES . . . . .	3
6. BALLISTIC TESTS . . . . .	3
7. VOLTMETER TEST . . . . .	3
8. STRAPPED SLEEVE METHOD OF TESTING IN COMMUNITY DIAL OFFICES . . . . .	3
9. MAINTENANCE . . . . .	5

### 1. GENERAL

1.01 This section covers the description and use of the KS-8455 Test Set which is intended primarily to aid in locating cable or wire troubles in distribution plant.

1.02 This section is reissued to update the text material and illustrations.

### 2. DESCRIPTION

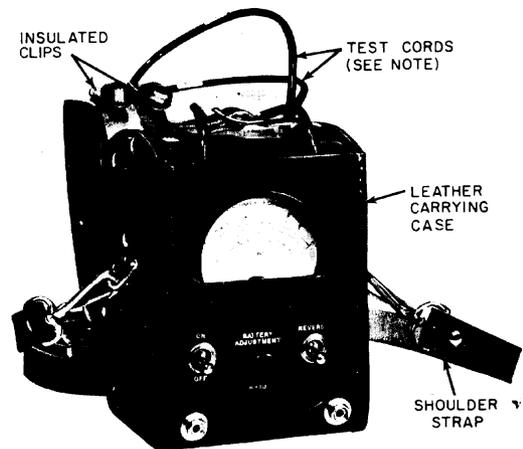
2.01 The KS-8455 Test Set (Fig. 1) consists of the following items:

- (a) KS-8455 L1 Test Set—Complete set except battery.
- (b) KS-8455 L2 Test Set—Volt-ohmmeter only. Battery not included.
- (c) ♦Two 6-foot W1AH test cords.—The neoprene covered cords are equipped with an insulated

spring clip at one end and a crimped solderless terminal at the other end. The cords are connected to the test set by machine screws located above the dial. The free ends of the cords are coiled and stored in the case behind the set when not in use.♦

(d) ♦A KS-8456 carrying case with shoulder strap. The front of the leather case has cutouts for operating the set without removing it from the case. The wrap-around flap cover is equipped with snap fasteners for securing the cover and protecting the test set during handling and transportation.♦

(e) ♦A 45-volt KS-14369 primary battery is required to operate the test set. The battery is not supplied with the set and must be ordered separately or purchased locally as described in 2.02.♦



NOTE:  
STORE CORDS BEHIND TEST SET  
WHEN NOT IN USE.

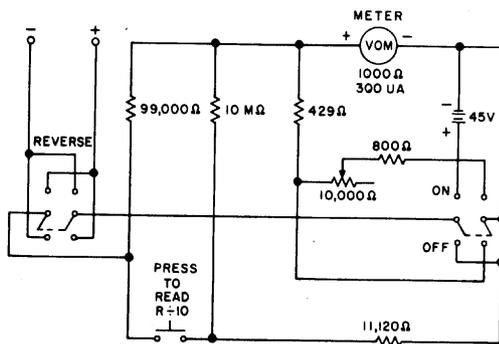
**Fig. 1—KS-8455 L1 Test Set**

# Bell System KS-8455 Test Set Description and Use

## SECTION 106-020-100

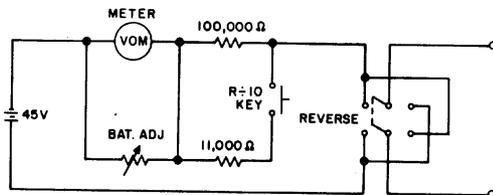
**2.02** ♦The KS-8455 Test Set is furnished without a battery. The 45-volt KS-14369 primary battery used in the test set must be ordered separately, or its equivalent, the commercial No. 455 Eveready Battery must be purchased locally.♦

**2.03** ♦Fig. 2 illustrates a schematic diagram of the KS-8455 Test Set. This circuit consists essentially of a microammeter, resistances, a 45-volt battery, and switches which permit setting up a voltmeter or ohmmeter circuit.♦



**Fig. 2—KS-8455 Test Set (Schematic Diagram)**

**2.04** Fig. 3 is a simplified schematic diagram of the ohmmeter circuit for which the ON-OFF switch must be in the ON position.

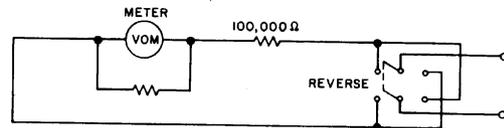


**Fig. 3—1 Ohmmeter Circuit—ON-OFF Switch at On Position**

**2.05** The ohmmeter circuit is used for:

- (a) Determining insulation resistance of a line, between wires or between one wire and ground.
- (b) Making ballistic tests to detect opens or to check bridged capacitor connections. The meter scale is calibrated to read insulation resistance directly in ohms, megohms, or "points" which correspond approximately to the "points" reading obtained on the voltmeter in the No. 2 Test Cabinet usually provided in community dial offices. The range of the ohmmeter is 0 to 2 megohms with the (R ÷ 10) key in the normal position; with this key depressed the range is 0 to 0.2 megohms.

**2.06** ♦Fig. 4 is a simplified schematic diagram of the voltmeter circuit for which the ON-OFF switch must be in the OFF position.♦



**Fig. 4—Voltmeter Circuit—ON-OFF Switch at OFF Position**

**2.07** The voltmeter circuit is used primarily for measuring line voltage and foreign EMF (dc voltages only).♦ The range of the voltmeter is 0 to 100 volts.

### 3. INSULATION RESISTANCE MEASUREMENTS

**3.01** Before making insulation resistance measurements adjust the set as follows:

- (1) Turn ON-OFF switch to ON.
- (2) Short circuit the two cords by clipping them together.
- (3) Turn BATTERY ADJUSTMENT knob until needle is at 100 on the "points" scale.

# Bell System KS-8455 Test Set Description and Use

ISS 2, SECTION 106-020-100

Repeat this adjustment from time to time to compensate for any change that may occur in the battery voltage.

**3.02** The procedures for using the KS-8455 Test Set to localize insulation faults are the same as those recommended in Section 462-800-500.

## 4. TESTS FOR GROUNDS

**4.01** To test for a fault to ground proceed as follows:

- (1) Open the line at a convenient location such as at a cable terminal or bridging point.
- (2) Connect one clip to ground. A suitable ground connection may be secured from the suspension strand or other associated grounded plant, from the grounded side of an adjacent line, or from a temporarily driven ground rod (Fig. 5).
- (3) Connect the other clip to the wire to be measured.
- (4) Throw ON-OFF key to ON.
- (5) read meter deflection. If read on the ohm or megohm scale, the reading indicates the insulation resistance of the measured wire to ground; if read on the "points" scale, the insulation resistance is obtained in terms of points.

## 5. SHORT CIRCUITS AND CROSSES

**5.01** To test for short circuits between wires of a pair or a cross between the wires of different pairs the procedure is the same as in Part 4, except that the clips are placed across the wires under test as shown in Fig. 6.

## 6. BALLISTIC TESTS

**6.01** The KS-8455 Test Set can be used in the same manner as the test desk voltmeter to detect opens or the presence of a capacitor on the line. Fig. 7 shows the method for making the test to detect an open on either an individual or party line. It also shows the procedure for testing for grounded ringers on party line circuits.

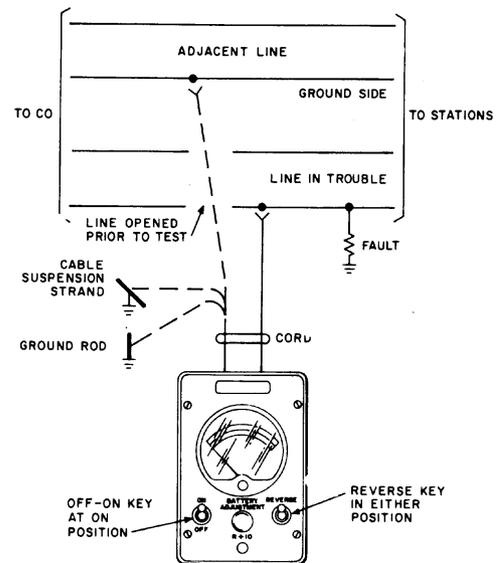


Fig. 5—Test for Grounds

**6.02** Having made the connections illustrated operate reverse (REV.) key back and forth slowly enough so the needle will return to zero at the end of each swing. If the needle deflects off the scale, keep the R  $\div 10$  key depressed while operating the reverse key.

## 7. VOLTMETER TESTS

**7.01** To use the KS-8455 Test Set as a dc voltmeter, place the ON-OFF key in the OFF position. Connect the clips across the circuit on which the voltage is to be measured. If the voltmeter reads backwards operate the reverse key. The reading on the points scale is the value of the applied potential in volts.

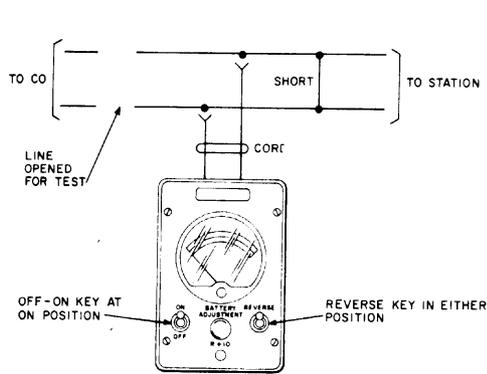
**7.02** The R  $\div 10$  key should not be depressed when taking voltmeter readings.

## 8. STRAPPED SLEEVE METHOD OF TESTING IN COMMUNITY DIAL OFFICES

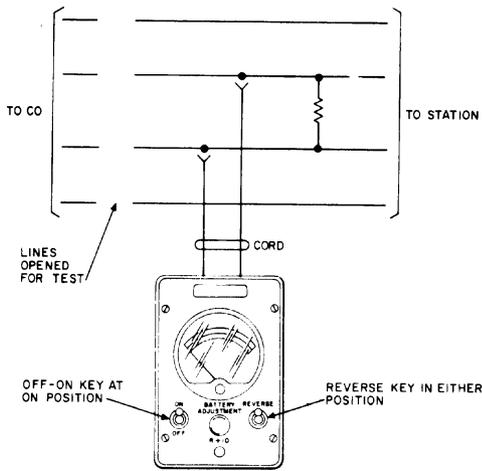
**8.01** In many instances testing with the KS-8455 Test Set may be facilitated by utilizing the operation of the cutoff relay which removes battery

# Bell System KS-8455 Test Set Description and Use

## SECTION 106-020-100



TEST FOR SHORT

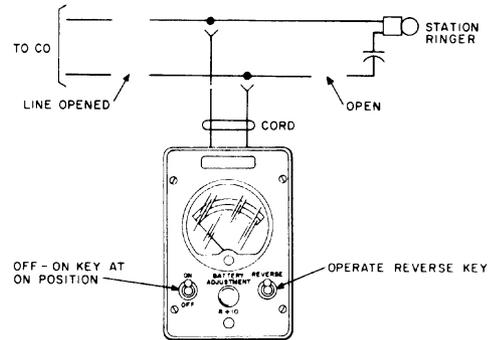


TEST FOR CROSS

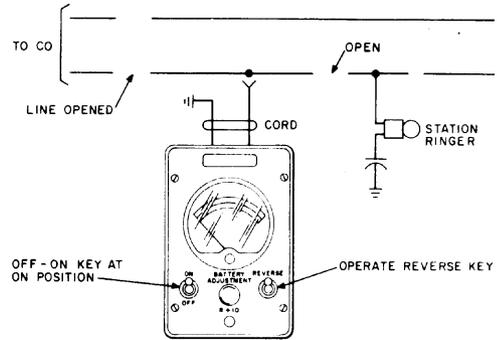
**Fig. 6—Test for Shorts and Crosses**

and ground from the line in trouble. This permits tests to be made at various locations on the line both "ahead" and "toward" the central office, and allows certain tests to be made on open wire sections without cutting the line. This test is made as follows:

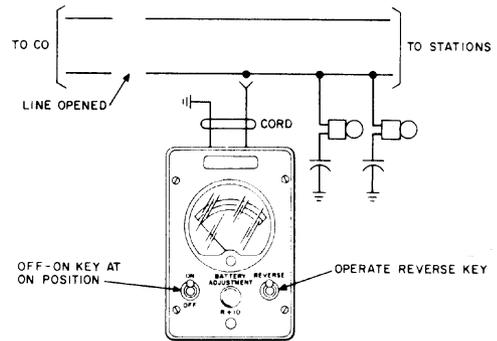
- (1) Tie the sleeve of a spare connector terminal to the sleeve of the connector terminal of the line in trouble at a common appearance



TEST FOR OPEN ON INDIVIDUAL LINE



TEST FOR OPEN ON PARTY LINE



BALLISTIC TEST FOR GROUNDED RINGERS

**Fig. 7—Test for Opens and Grounded Ringers**

# Bell System KS-8455 Test Set Description and Use

ISS 2, SECTION 106-020-100

(location of the common appearance differs in different types of offices). The strap may be removed after the tests, at the convenience of the tester, as no trouble will be caused while it is in place in the office with a standard strap or shunt cord.

(2) At the testing location of the line in trouble, connect a dial hand test set to an adjacent working line, if available, and dial the spare connector terminal.

—If a busy signal is encountered, it is an indication that the line to be tested is busy or has become permanent.

—If ringing signal is heard, it is an indication that the cut-off relay has operated and the line to be tested is open at the central office. As long as the connection to the spare connector terminal is held up and the ringing signal is heard, the line to be tested will remain in this condition.

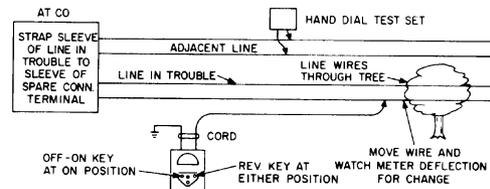
(3) If an adjacent line is not available for dialing the spare connector terminal, and if the fault on the line in trouble is not of sufficient value to interfere with dialing, use the hand test set on the line in trouble to call the test desk or operator at the master office. Have the test deskman or operator dial the spare connector terminal and hold the connection for a prearranged length of time, eg, two minutes. With the TALK-MON. key on the dial hand test set in the monitoring position, the combinationman may monitor on the line while the test deskman is placing the call. Evidence of the operation of the cut-off relay will be a click in the receiver of the hand set or a change in the volume of line noise.

(4) After the battery and ground have been removed from the line, proceed with the desired tests.

**8.02** A typical application of this method of testing is illustrated in Fig. 8.

## 9. MAINTENANCE OF TEST SET

**9.01** Reasonable care should be exercised in handling the test set. The set should be protected against unnecessary shocks or jars.



**Fig. 8—Strapped Sleeve Method Test**

**9.02** The battery should be replaced when it is impossible to adjust the meter needle to 100 on the points scale by use of the battery adjustment knob.

**9.03** To replace the battery (2.02) remove the set from the leather case. Remove the panel on the back of the set by taking out the four screws which hold it in place. Disconnect the old battery from the terminals (snap fasteners) and replace it with a new one. The terminals are so arranged that it is impossible to reverse the polarity.

# Nortel DMS-100 Audible Alarm Table (AUDALARM)

## Table Name

Audible Alarm Table

## Functional Description of Table AUDALARM

This table specifies the alarm level for log reports from the security subsystem. You cannot view and manipulate these reports. You can specify alarm levels for these reports in the following two methods:

- Through the use of table CMDS, you can specify if a report and alarm generates for each command.
- Through the use of table AUDALARM, you can specify an alarm level for logging each report.

Log devices *do not* print secret alarms. When a secret report causes an alarm, the alarm system generates a non-secret log. This non-secret log only records that an alarmed secret report is logged.

You cannot add or delete tuples from this table with the LOGUTIL facility at the Maintenance and Administration Position (MAP) terminal. The log system adds tuples automatically at restart time. Each log report has the alarm level set to No Alarm (NA) by default. The only correct user operation for this table is to change the alarm level of a report. Changes to the alarm level occur immediately. Restart is not required.

## Datafill Sequence & Table Size

You do not need to enter data in other tables before you enter data in table AUDALARM. One tuple is in this table for every secret log in the system (64 tuples maximum).

## Datafill

The following table describes datafill for table AUDALARM:

---

### *Table AUDALARM Field Descriptions*

<b>Field</b>	<b>Subfield</b>	<b>Entry</b>	<b>Explanation and Action</b>
LOGREP		Alphanumeric (16 characters maximum)	<i>Log Report</i> Enter a logname and report number, in the form of: logname\$reportnumber For example, SECU\$101. Only lognames and report numbers of secret logs are keys to this table.
ALARM		CR, MN, MJ, or NA	<i>Alarm Level</i> Enter the level of the alarm that the subsystem raises when a report is logged. The levels are, CR (Critical Alarm), MN (Minor Alarm), MJ (Major Alarm), or NA (No Alarm). The entry in this field can only be changed. You cannot add or delete tuples. The default entry for this field is "NA".

---

-End-

## **Datafill Example**

The system automatically inserts tuples in this table for each log report. The alarm level entries for these tuples are always set to the default value NA. The entries required to change the alarm level for log reports appear in the following table. These entries change log report `SECU$109` to *major*, and the alarm level for log report `SECU$111` to *minor*.

The following example MAP display shows sample datafill for table AUDALARM:

<b>LOGREP</b>	<b>ALARM</b>
<b>SECU\$109</b>	<b>MJ</b>
<b>SECU\$111</b>	<b>MN</b>

# ***Nortel DMS-100 Customer Protection Table (CUSPROT)***

## **Table Name**

Customer Protection Table

## **Functional Description of Table CUSPROT**

Table CUSTPROT defines the command class of users that can read, change, add, or delete tuples for each table. These tables are assigned in the switching unit.

The privilege class with *read* protection ability can read tuples from the table. The privilege class cannot update, add, or delete tuples from the table.

The privilege class with *update* protection ability can read and update. The privilege class cannot add or delete tuples from the table.

The privilege class with *all* protection ability can read, update, add, or delete tuples from the table.

If the switching unit has the feature BC1459, Partitioned Table Editor (PTE), a non-operating company user can use the tables entered in table OWNTAB (Ownership).

The privilege classes assigned to tables that are not entered in table OWNTAB are not assigned to non-operating company users. This action occurs so that non-operating company users do not have access to these tables.

To create new data, tables can add new tuples. These tables are read-only or change-only tables for non-operating company users. Read-only or change-only tables for non-operating company users appear in the following list:

- CLSVSCRC (Class of Service Screening Control)
- COSMAP (Network Class of Service Mapping)
- DIGCOL (IBN Digit Collection)
- FNPACONT (List of Foreign Numbering Plan Area Codes Subtables)
- HNPACONT (List of Home NPA Code Subtables)
- LCASCRCN (Local Calling Area Screening Control)
- TODHEAD (Time of Day Head)
- VFGENG (Virtual Facility Group Engineering)
- XLANAME (List of Translator Names)

Command `PERMIT` assigns privilege classes for commands and access to tables. A privilege class used in table CUSTPROT or table TERMDEV (Terminal Device) can appear in one table.

## **Security Table Enhancement Feature**

If the switching unit has feature BC1305, Security Table Enhancement (STE), the operating company can select the tables to monitor.

Feature STE allows the system to generate log reports if users modify or attempt to modify the customer data tables.

The privilege class assigned to the table controls access to customer data tables.

In an attempt to access a table, the privilege class of the user is matched against the privilege class of the table. If the two classes match, access to the table occurs.

Feature STE allows the operating company to monitor the tables and the users that access these tables.

If feature STE is activated, the following action occurs. The completed or terminated attempts to access a table are recorded in a log report to examine at a later time.

The system generates log reports for tables when you attempt to read and display a tuple. The system generates log reports for tables when you attempt to write the tuple.

Log TABL that feature STE introduces is a secret-type log. The system automatically routes all secret-type logs to the System Log (SYSLOG). Use of this feature can cause the SYSLOG log queue to flood. The operating company *must* minimize the number of tables monitored.

The operating company must monitor the following tables:

- CUSTAB (Customer)
- CUSTPROT (Customer Protection)
- DATASIZE (Data Size)
- OFCENG (Office Engineering)
- OFCOPT (Office Options)
- OFCSTD (Office Standard)
- OFCVAR (Office Variable)

The data store allocated to store the table access log reports is 20,000 words. This allocation allows storage of a maximum of 500 log reports of type TABL101 and TABL103. Each log report is 60 words. Log reports of type TABL100 and TABL102 are 20 words. The log queue can store from 333 to 1,000 log reports. This log storage depends on the type of log reports stored.

Nortel can activate or deactivate feature STE through a change in office parameter `MONITOR_TABLE_ACCESS` in table `OFCOPT`.

If Nortel activates office parameter `MONITOR_TABLE_ACCESS`, operating company personnel can activate or deactivate feature STE. This action occurs through a change in office parameter `TABLE_ACCESS_CONTROL` in table `OFCVAR`.

Authorized operating company personnel can activate or deactivate feature STE for specified tables (field `TABNAME`). This action occurs through a change in the values of fields `VALACC` (Valid Table Access Control) and `DENACC` (Denied Table Access Control) in table `CUSTPROT`.

If you set field `VALACC` to `WRITE`, the system generates a TABL101 log. The system generates a log each time you use table control to add, delete, or change a tuple.

If you set field `VALACC` to `ALL`, the system generates a TABL101 log. The system generates this log when the following action occurs. The log generates each time you use table control to write in the table to add, delete, or change a tuple. The system generates a TABL100 log each time you use table control to read or display the table.

If you set field `DENACC` to `WRITE`, the following action occurs. The system generates a TABL103 log each time you attempt to use table control to write in a table.

If you set field DENACC to ALL, the system generates a TABL103 log. The system generates this log each time you attempt to use table control to write in a table. The system generates TABL102 log each time you attempt to use table control to read or display a table.

The operating company can set the alarms for these logs. Change the correct tuples in table AUDALARM to set these alarms. The alarms that these logs generate turn off after approximately 15 seconds.

Table control automatically produces the first input for this table. Set the first value for the privilege classes to 15. Fields VALLACC and DENACC are set to OFF.

To change this table, the operating company must load the module ENGWRITE from the non-resident tape and enter command ENGWRITE ON.

For the first datafill, the operating company provides input for the tables with a minimum of one privilege class. This class must have a value that is not 15. Fields VALLACC and DENACC must not be OFF.

Use command REP (replace) for each entry you submit to change the default values assigned to this table.

### **Datafill Sequence & Table Size**

You must enter data in table CUSTAB before you enter data in table CUSTPROT. Table size is 0 to 2,047 tuples.

### **Datafill**

The following table describes datafill for table CUSTPROT:

*Table CUSTPROT Field Descriptions*

<b>Field</b>	<b>Subfield</b>	<b>Entry</b>	<b>Explanation and Action</b>
TABNAME		Alphanumeric (16 characters maximum)	<i>Table Name</i> Enter the table name.
READPROT		0 to 30	<i>Read Protection</i> Enter the privilege class that can read this table.
UPDTPROT		0 to 30	<i>Update Protection</i> Enter the privilege class that can read the table and update tuples. This class cannot add or delete tuples from the table.
ALLPROT		0 to 30	<i>All Protection</i> Enter the privilege class that can read, update, add, or delete tuples from the table.
VALLACC		ALL, OFF, or WRITE	<i>Correct Access</i> If TABL100 and TABL101 logs are a requirement, enter "ALL".

If feature BC1305 Security Table Enhancement is not provided or logs TABL100 and TABL101 are not requirements, enter "OFF".

If the switching unit has feature STE and TABL101 logs are a requirement, enter "WRITE".

DENACC

ALL, OFF,  
or WRITE

*Denied Access*

If TABL102 and TABL103 logs are a requirement, enter "ALL".

If the switching unit has feature STE and TABL103 logs are requirements, enter "WRITE".

If feature STE is not provided or logs TABL102 and TABL103 are not requirements, enter "OFF".

-End-

### **Datafill Example**

Table CLLI with privilege classes of 2, 4, and 6 appears in this example. The correct access and denied access options are off.

The following example MAP display shows sample datafill for table CUSTPROT:

TABNAME	READPROT	UPDTPROT	ALLPROT	VALACC	DENACC
CLLI	2	4	6	OFF	OFF

# Simple Night Vision Viewer

## Overview

A simple modification to the **Portable Video Camera Viewer** project as described in *GBPPR 'Zine #22* can turn it into a low-cost night vision device. All you need to do is add an external black & white CMOS video camera (which should have internal infrared LED lighting) and a SPDT switch. Harbor Freight Tools sells a perfect camera for this. The part number is 47546 and should be around \$30 when on sale. Wal-Mart also sells several tiny CMOS video security cameras which should also work. The Harbor Freight Tools version comes with six internal IR LEDs, a microphone for receiving audio, and can easily be powered from the viewer's own 9 volt battery. The addition of the SPDT switch will allow you to chose which video input is displayed on the viewer. This will allow you to use the **Portable Video Camera Viewer** for its original purpose of testing video surveillance installations inside Mosques.

Some of the specifications for the Harbor Freight Tools #47546 camera are below:

**Power Source** : 7.5 VDC @ 300 mA (9 VDC will work)  
**Image Sensor** : 1/4-inch CMOS  
**Scanning System** : 2:1 Interface  
**Resolution** : 350 TV Lines  
**S/N Ratio** : > 48 dB (AGC Off)  
**Min. Illuminance** : 0.0 Lux  
**AES** : 1/50-1/6000  
**Lens** : f=3.6 F=2.8  
**Gamma Correction** : 0.45  
**Sync Signals** : Horizontal = 15,750 Hz Vertical = 60 Hz (NTSC/EIA)  
**Video Output** : Composite 1.0 Vp-p @ 75 Ohms

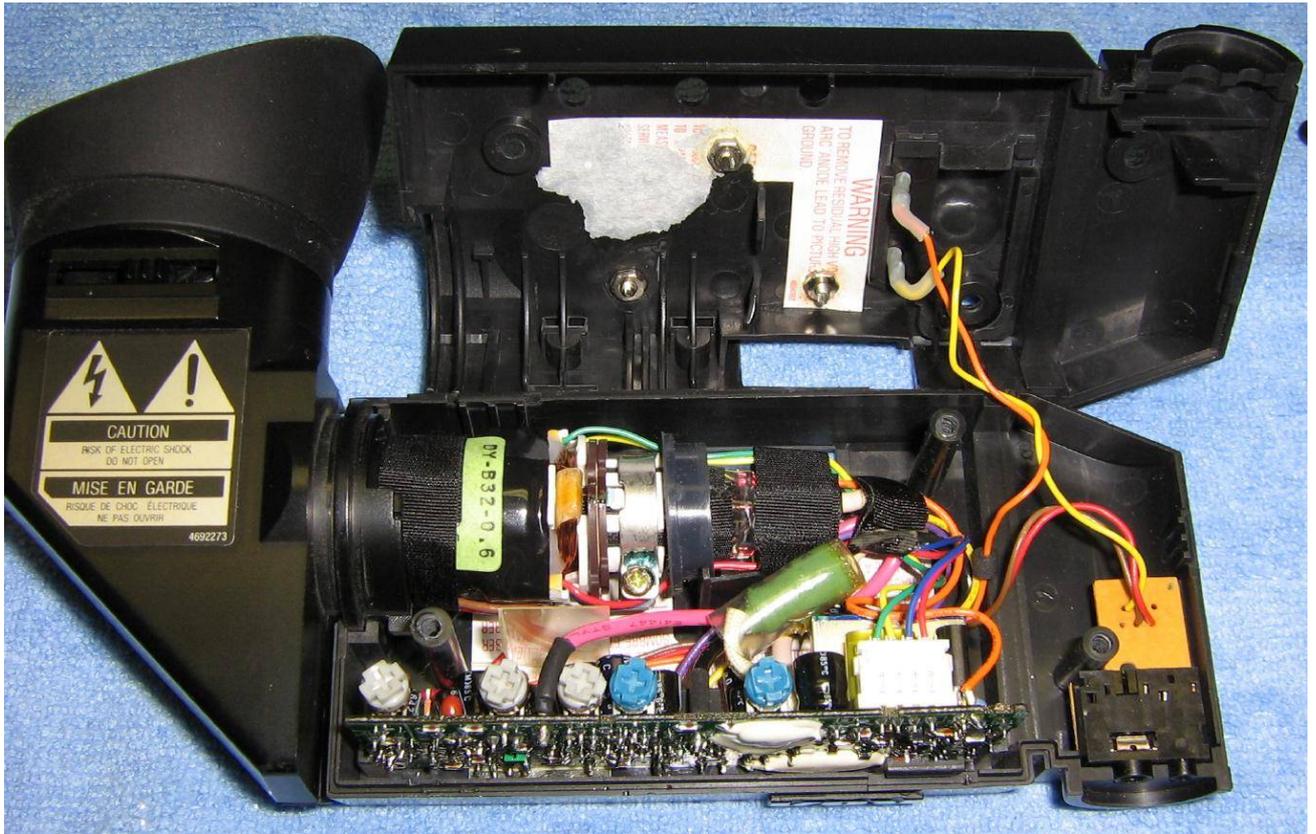
## Pictures & Construction



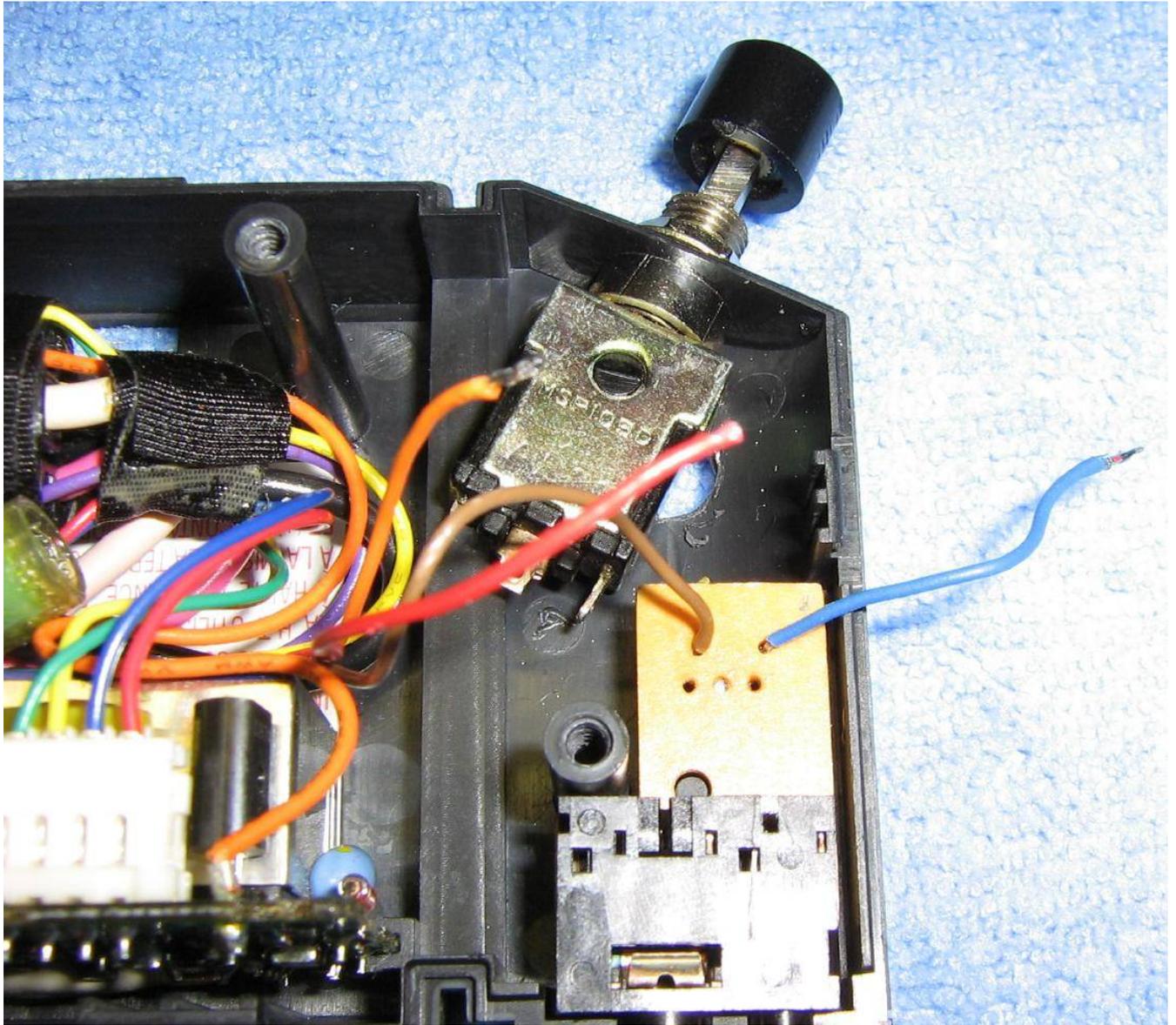
Overview of what's needed. The **Portable Video Camera Viewer** project from *GBPPR 'Zine #22* and a **Harbor Freight Tools #47546 CMOS Video Camera**.



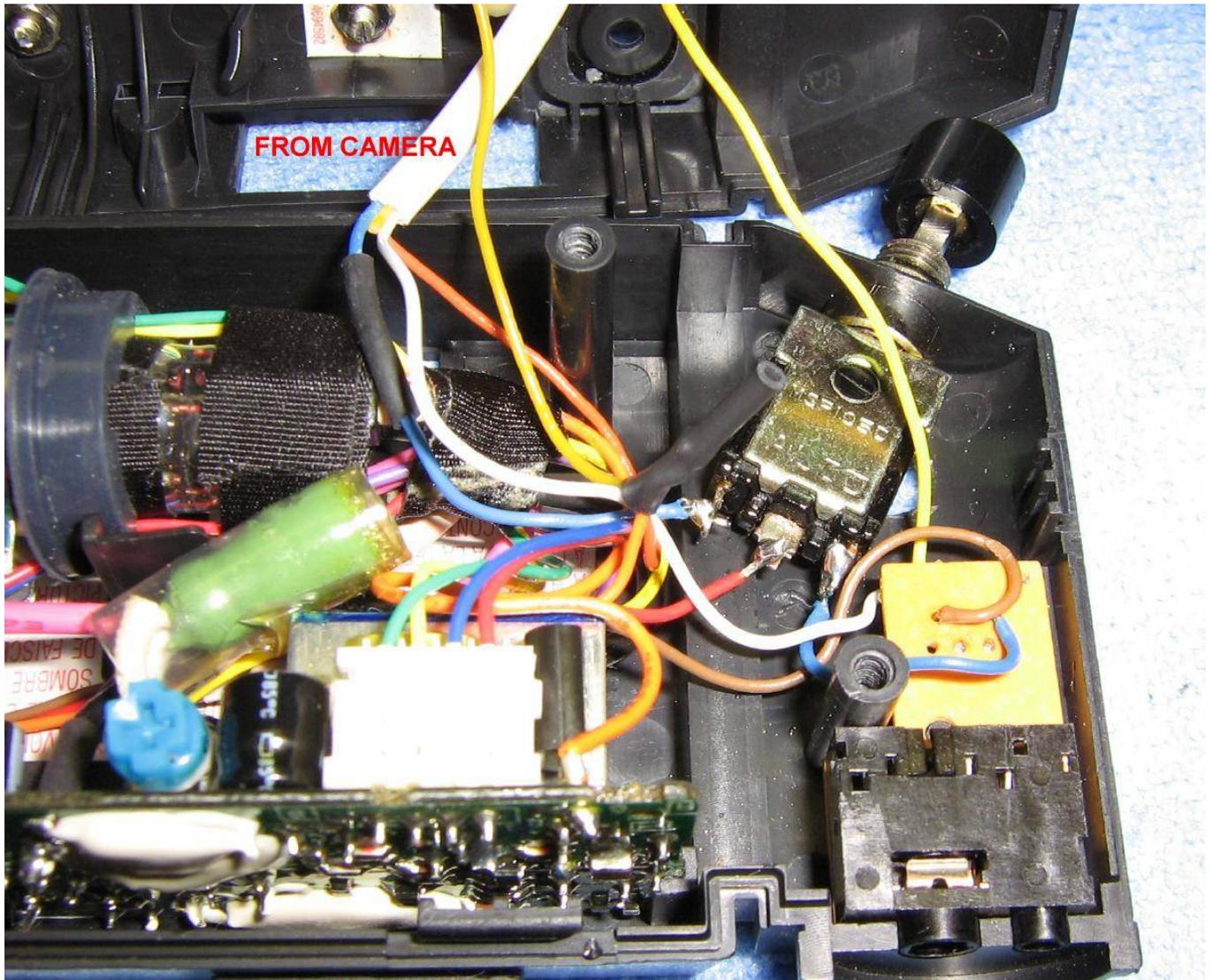
Closeup of the video camera. It is completely sealed inside a fairly weatherproof package. Six infrared LEDs are used for illumination when operating in the dark. The addition of more infrared LEDs with some type of focusing system will greatly increase the "night vision" performance of the camera.



Inside the "stock" **Portable Video Camera Viewer** as we left it. External video input is on the lower-right.

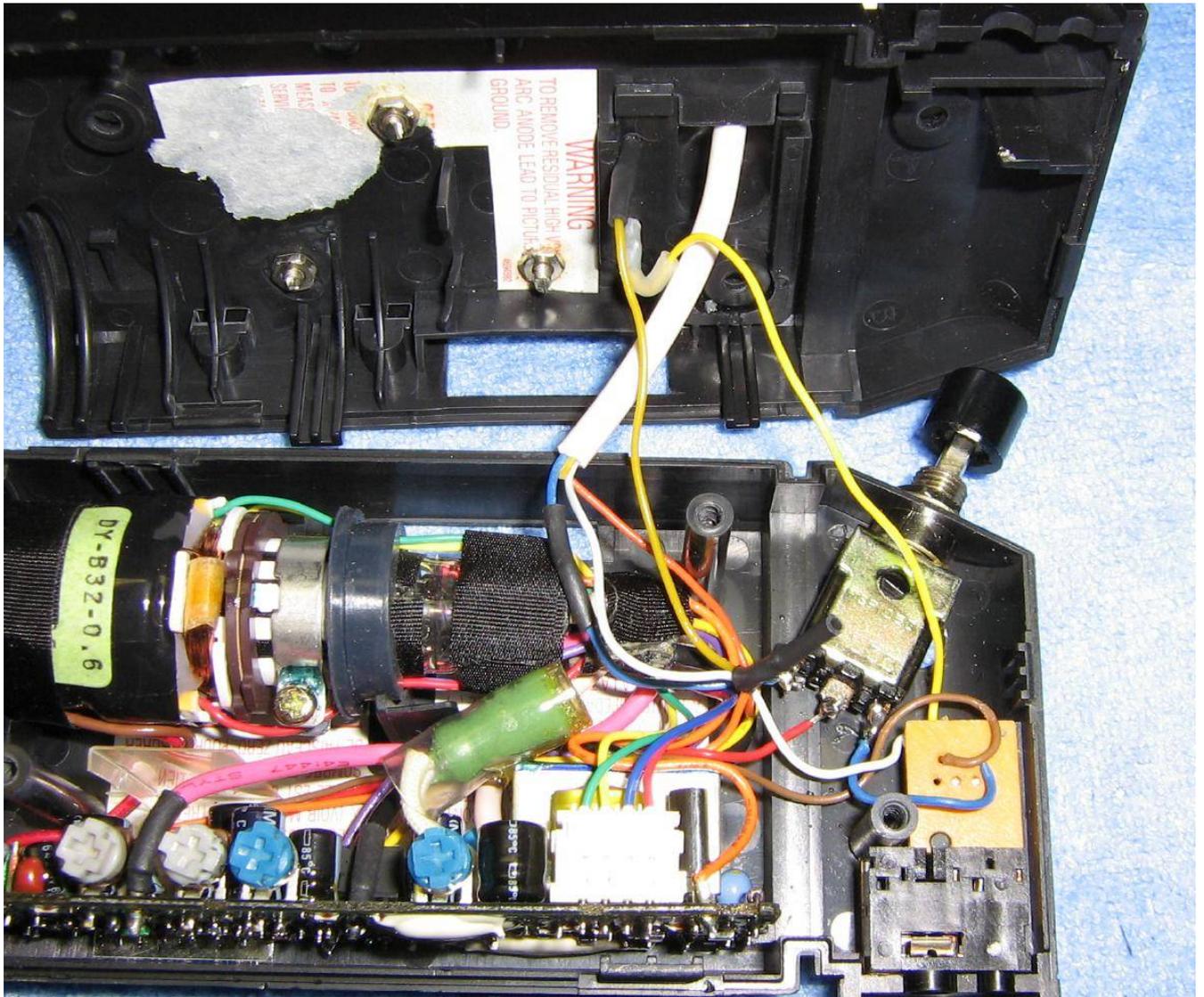


Find a convenient location and install a SPDT switch. This will select between which video input is sent to the viewer's display. The external video input still comes in via the 1/8-inch panel jack and is soldered to the other pole on the input selector switch.



Wires resolder in. The **RED** wire on the center terminal of the SPDT switch is the viewer's main video input. The **BLUE** wire on the right is from the 1/8-inch external video input jack, and the *other BLUE* wire (left side) is the video input from the CMOS night vision camera.

Splice in the **ORANGE** wire from the CMOS camera into the viewer's main +9 VDC power line. The **WHITE** wire is ground. Be sure everything shares a common ground! The **YELLOW** wire from the CMOS camera is the audio line, and is not used. You can cut it off.



Alternate view. Be sure nothing is shorted out.

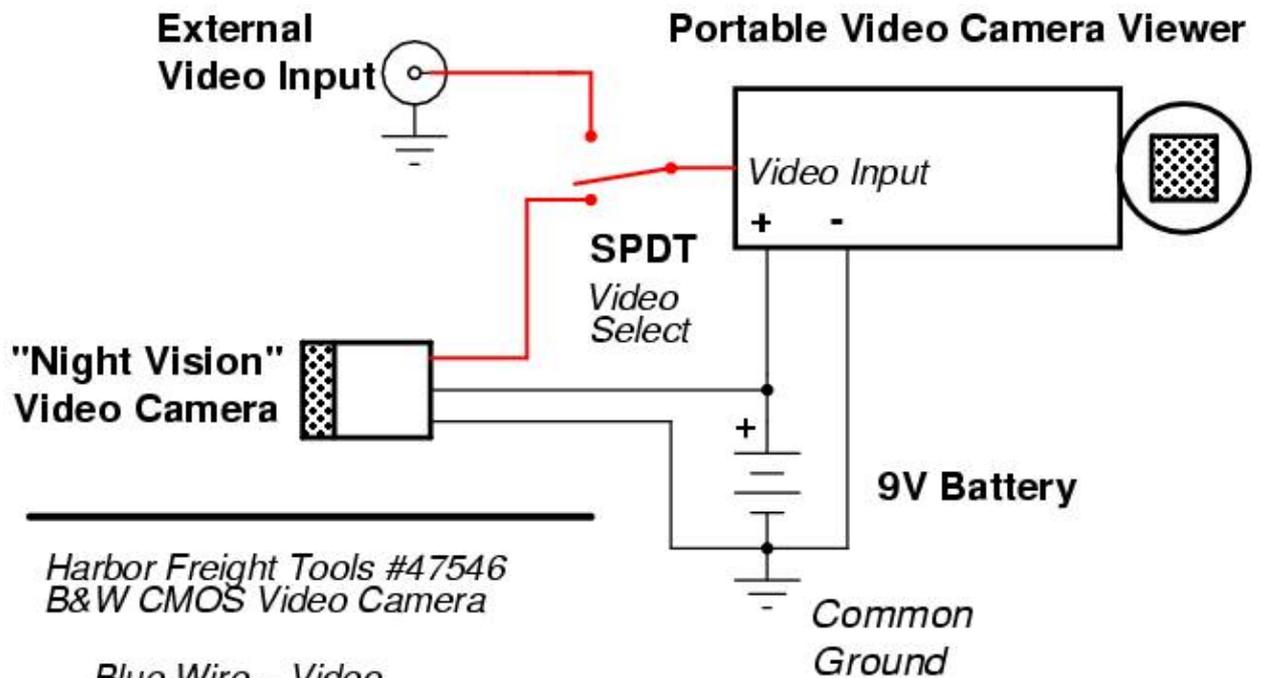


Epoxy the camera to a suitable location on the outside of the **Portable Video Camera Viewer**. Be sure it is pointed in the right direction and "right-side" up – test this ahead of time! Also be sure no screws or adjustment holes are covered up.



Finished rear view.

**Block Diagram**



Harbor Freight Tools #47546  
B&W CMOS Video Camera

- Blue Wire = Video
- White Wire = Ground
- Orange Wire = +9 VDC
- Yellow Wire = Audio (Not Used)

# ***Improvised Counter-I.E.D. Armor***

## **Overview**

A few years ago, a very interesting article on TechCentralStation.com entitled "Send it, and We'll Figure Out How to Use It" appeared. This article was about how military personnel are using scavenged and improvised hardware to help them when they are on the battlefield babysitting those fucking useless Eurosavages. A lot of the ideas in this article are very clever and should be looked into further.

*Excerpt from "Send it, and We'll Figure Out How to Use It":*

### **Glass Ceramics**

Good old Corningware bowls bounce off concrete, but its ballistic resistance pales in comparison to the tougher stuff that glass makers transform into well named hard discs for computer memory drives. Cheap and readily manufactured, such materials approach the fracture toughness per unit weight of honest to gosh armor ceramics. Adding cesium to the precursor melt beefs up the computer grades, and mass production -- we're talking stovetops and windowpanes here -- can turn them out faster than silicon or boron carbide.

### **Scrap Kevlar Cloth**

Any kind of aramid -- twaron, Kevlar, Whatever -- and almost any high tenacity fiber webbing or scrim, from Spectra to Nomex, are vast improvements on the lack of it for those with time and glue on their hands to reinforce their motley improvisations.

Apparently, the coatings on hard drive platters make them ideal for use as very light-weight improvised armor plating. These could be useful for protection against the metal shrapnel used in most Improvised Explosive Devices (IED) or suicide bombers belts. I doubt these will stop a 7.62x39 mm round, though. Also useful in battle, are scraps of Kevlar material. These are often "thrown away" daily in the form of cut or heat resistant mechanics gloves, Goodyear "SilentArmor" automobile tires, or even some high-performance bicycle tires (the kind that are puncture resistant). These all contain bits of Kevlar material which can be utilized as patches for real or improvised armor.



**Kevlar XL Mechanic's Gloves (Harbor Freight Tools #92173) & Goodyear Fortera SUV Tires**

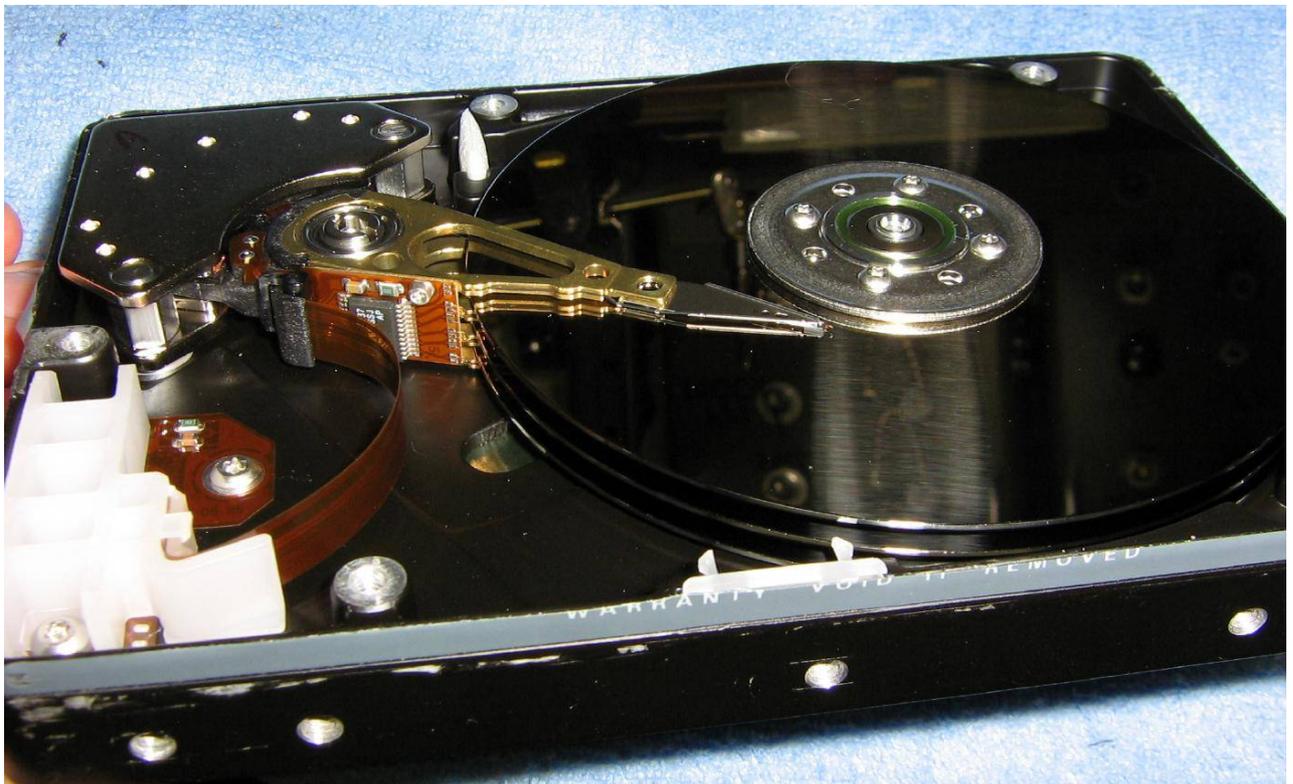
## Pictures & Notes



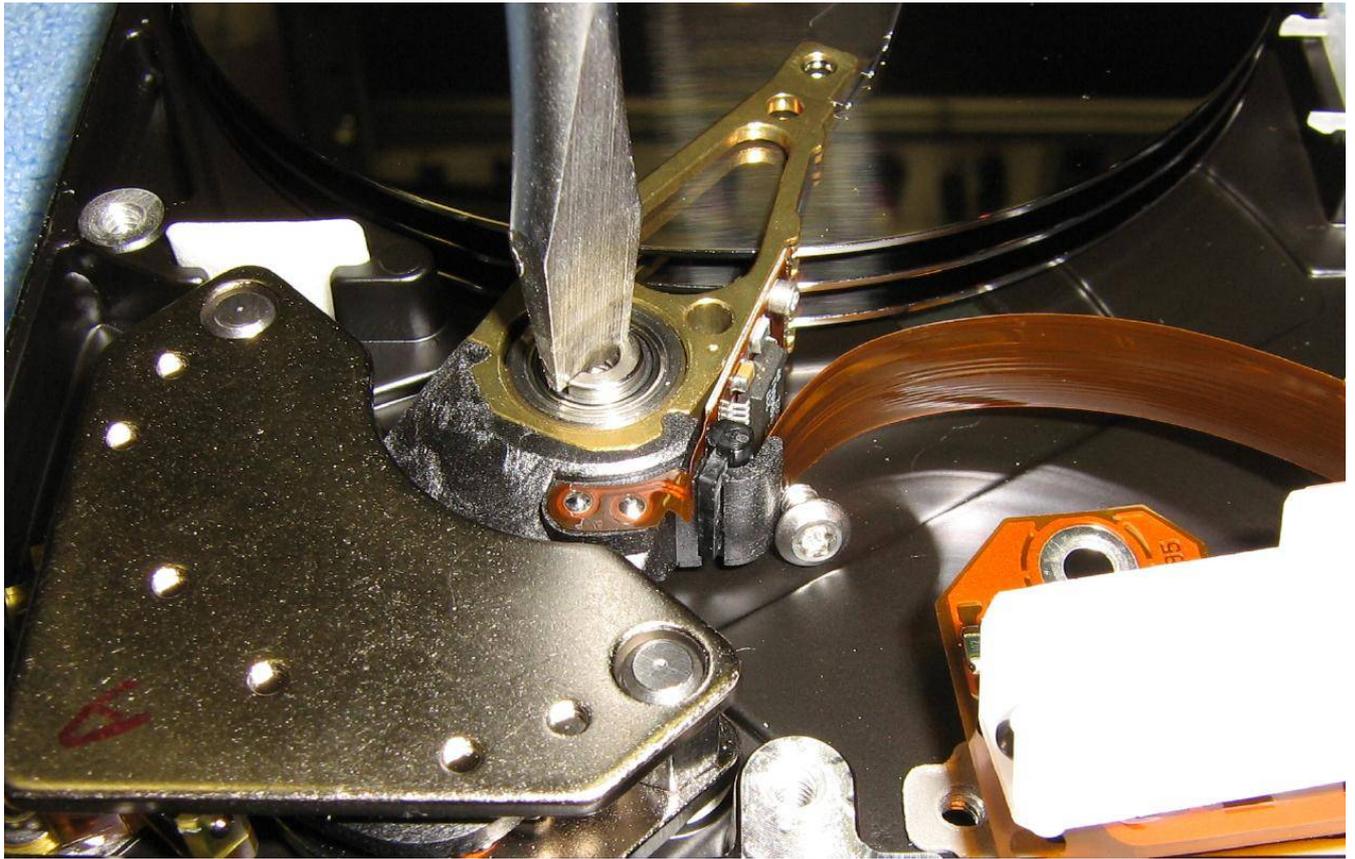
The two old hard drives used for this experiment. There may be a large difference in platter size and strength between manufacturers. I have no idea.



Take the hard drives apart using Torx screwdrivers and an X-acto knife. Save the controller PC board as it is a good source of surface mount components.



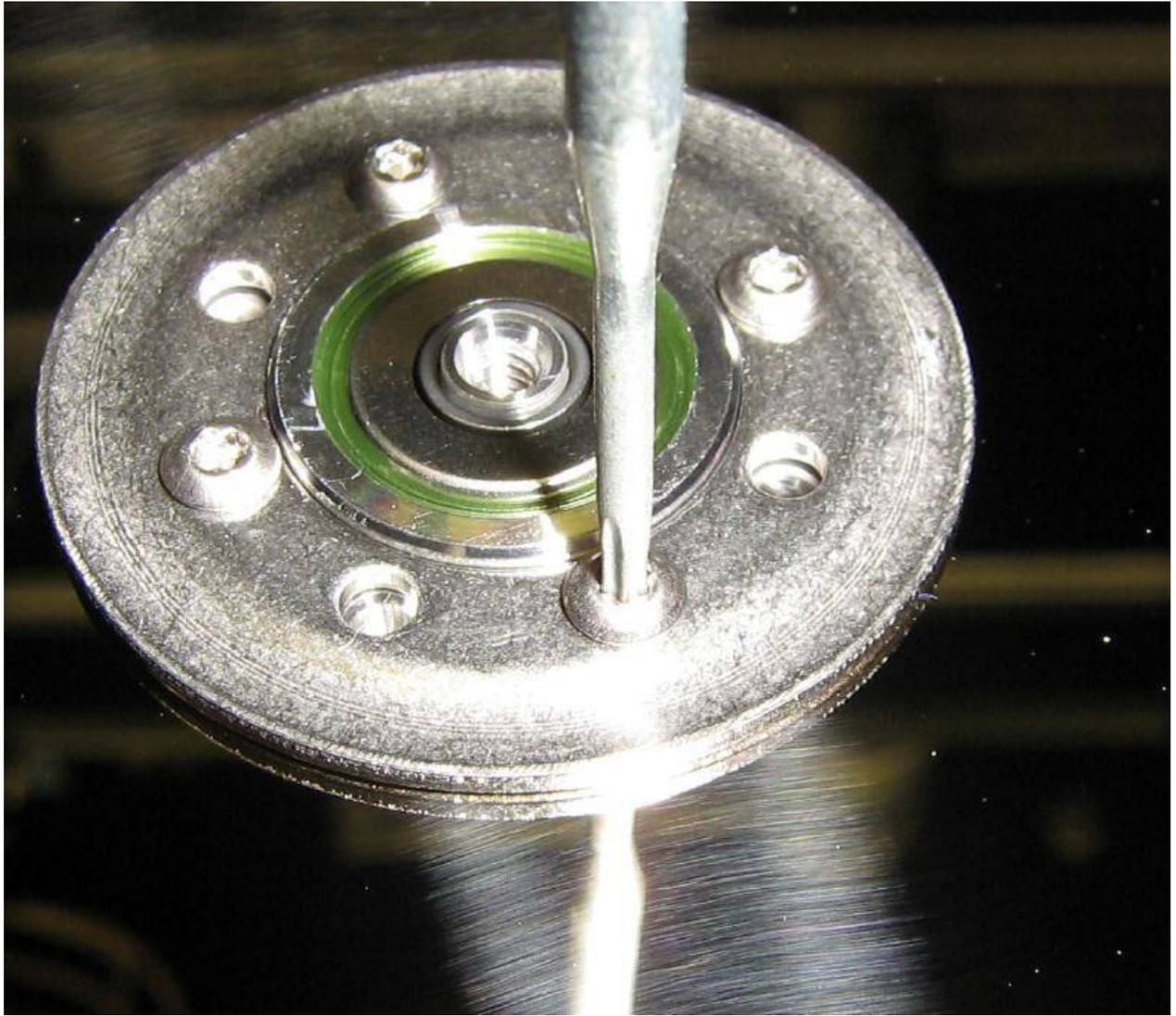
Hard drive internal view.



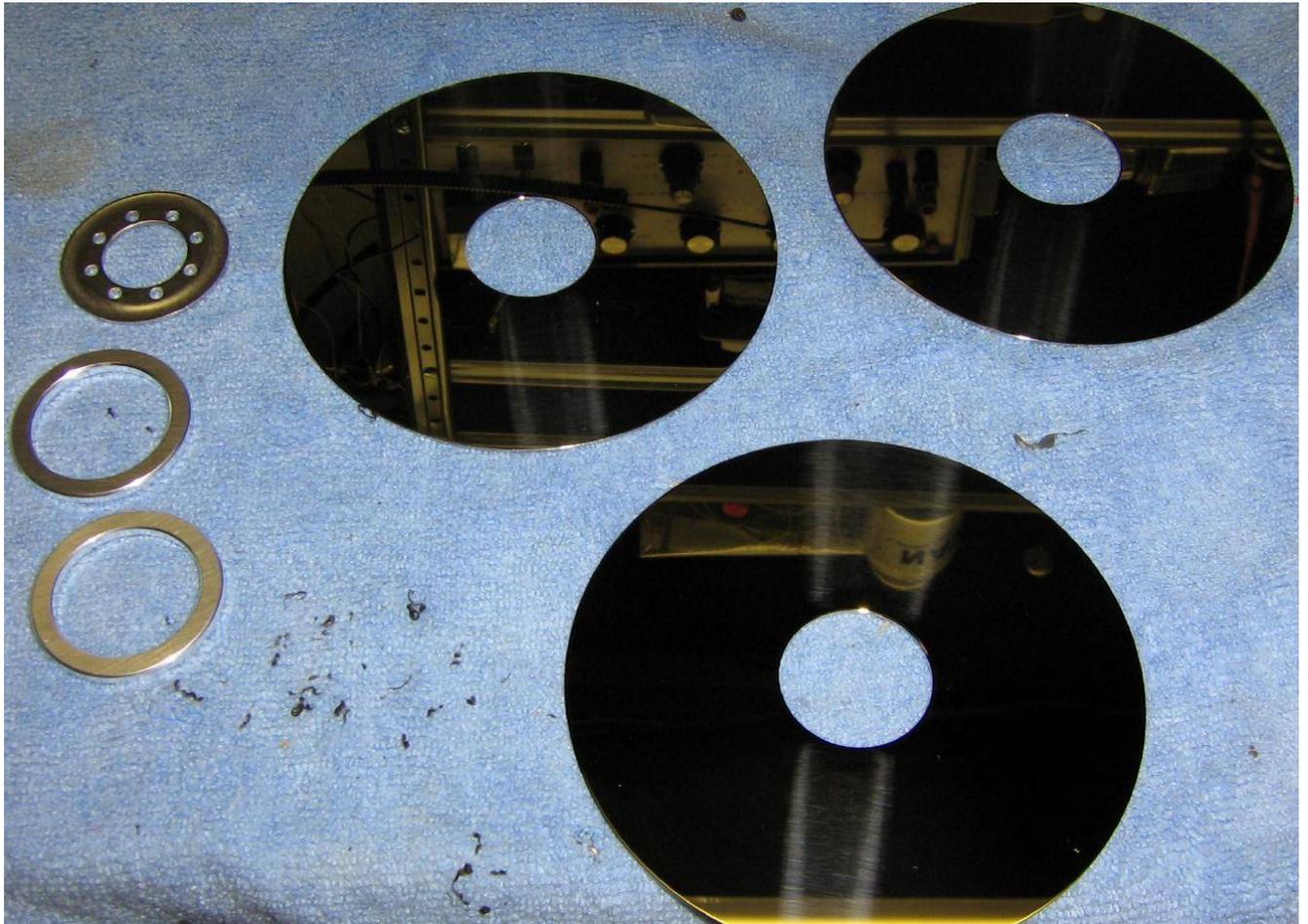
Remove the armature for the drive's magnetic head using a regular screwdriver as shown above.



Remove the rest of the mechanical pieces. The magnets on the lower-left are very powerful and can be useful in other projects.



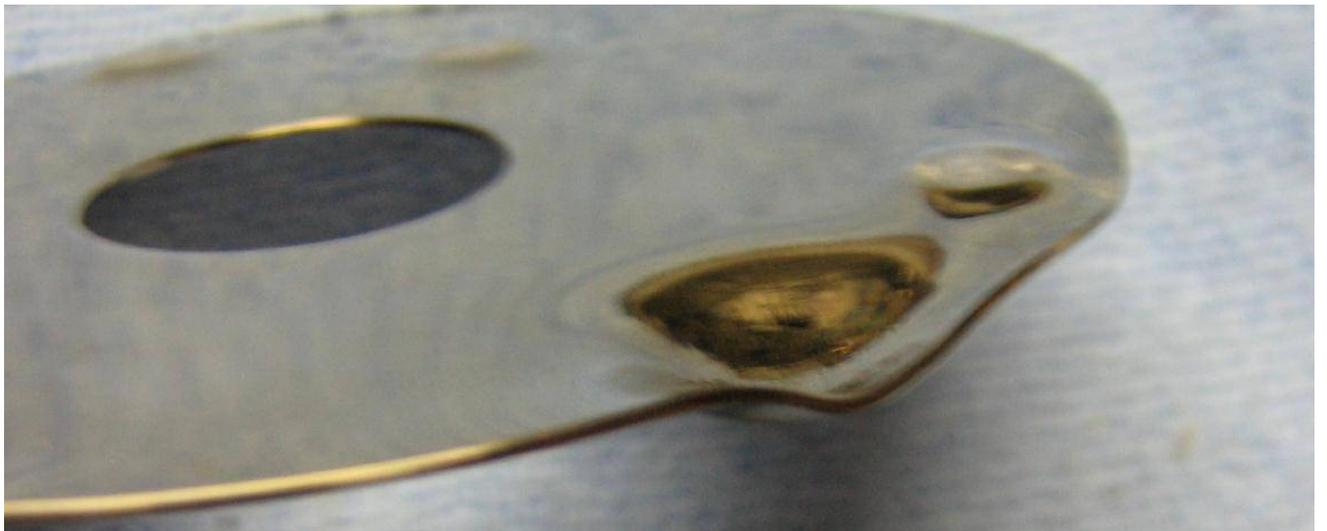
Remove the plate which holds the drive's platters down. This is usually a small #6 Torx screw.



Then remove the individual platters. There are usually two or three platters in each hard drive.



Initial strength test using a ball peen hammer. The individual drive platters appear to be very light (0.5 oz) aluminum discs with some sort of coating. Maybe it's the coating that gives them strength?



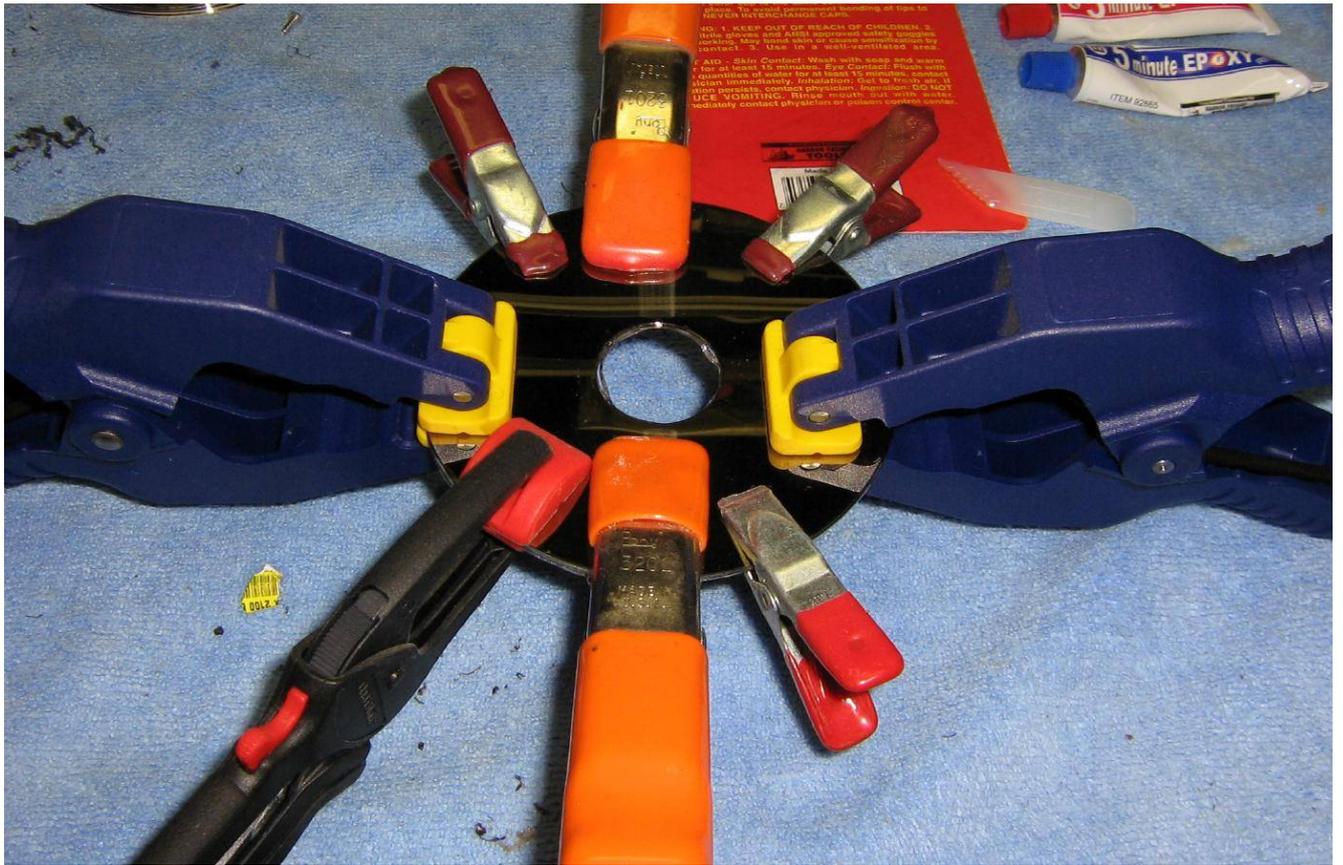
Close up of a hammer hit on a single disk platter.



Some of the two-part epoxy resins and putties used for this test. Use the epoxy resin (left) to sandwich two disk platters together for greater strength, then use the epoxy putty to hold the improvised armor in the location you need.



Spread the epoxy resin out along one of the platters.



Then clamp another one on top of it. Let it cure for at least five minutes.

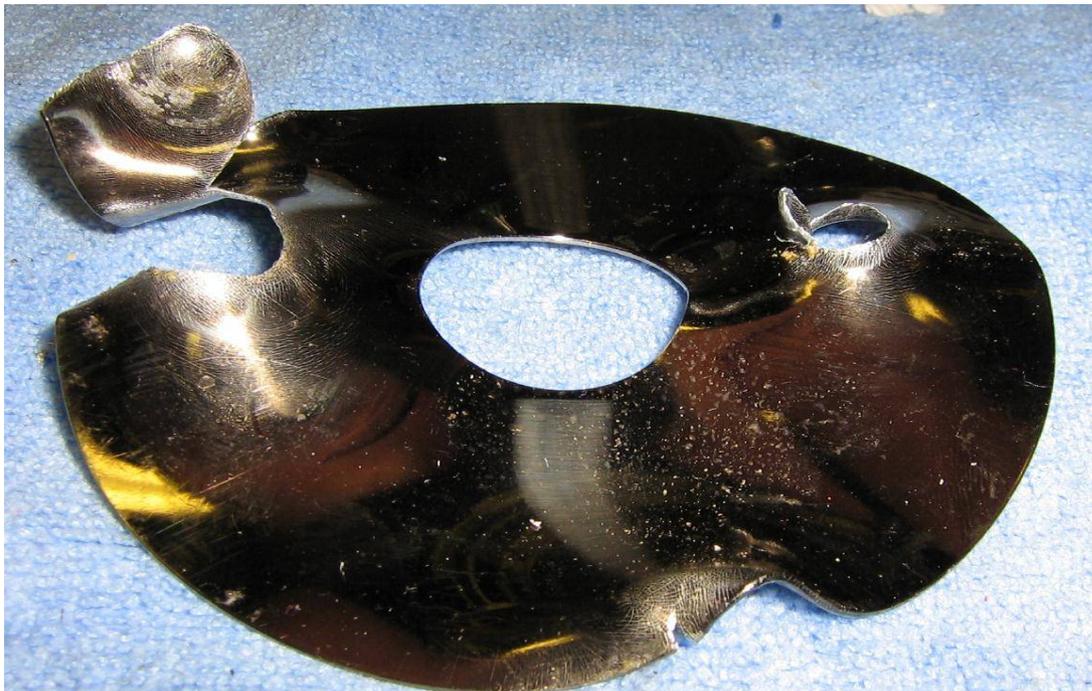


Here are three sandwiched dual-platters epoxied together. Each one overlaps, covering the center hole on the platters underneath it.



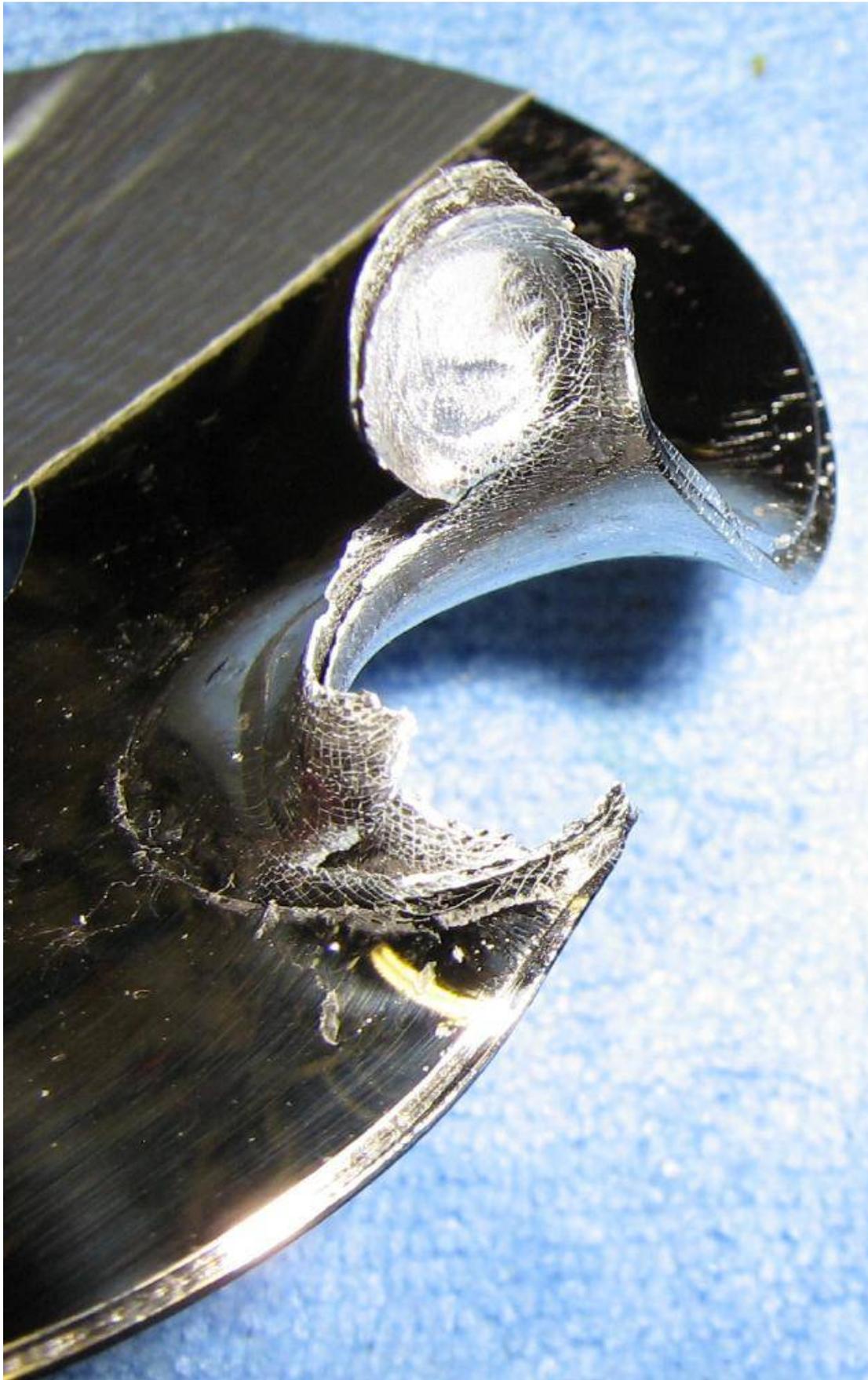
Then place them inside a Kevlar lined mechanics glove for added protection from shrapnel and fire burns.

### **Real World Testing**



Single hard drive platter. .45 Colt 200 grain lead ball (8.3 grains Unique) on the left, .22 LR (Remington Thunderbolt) on the right.

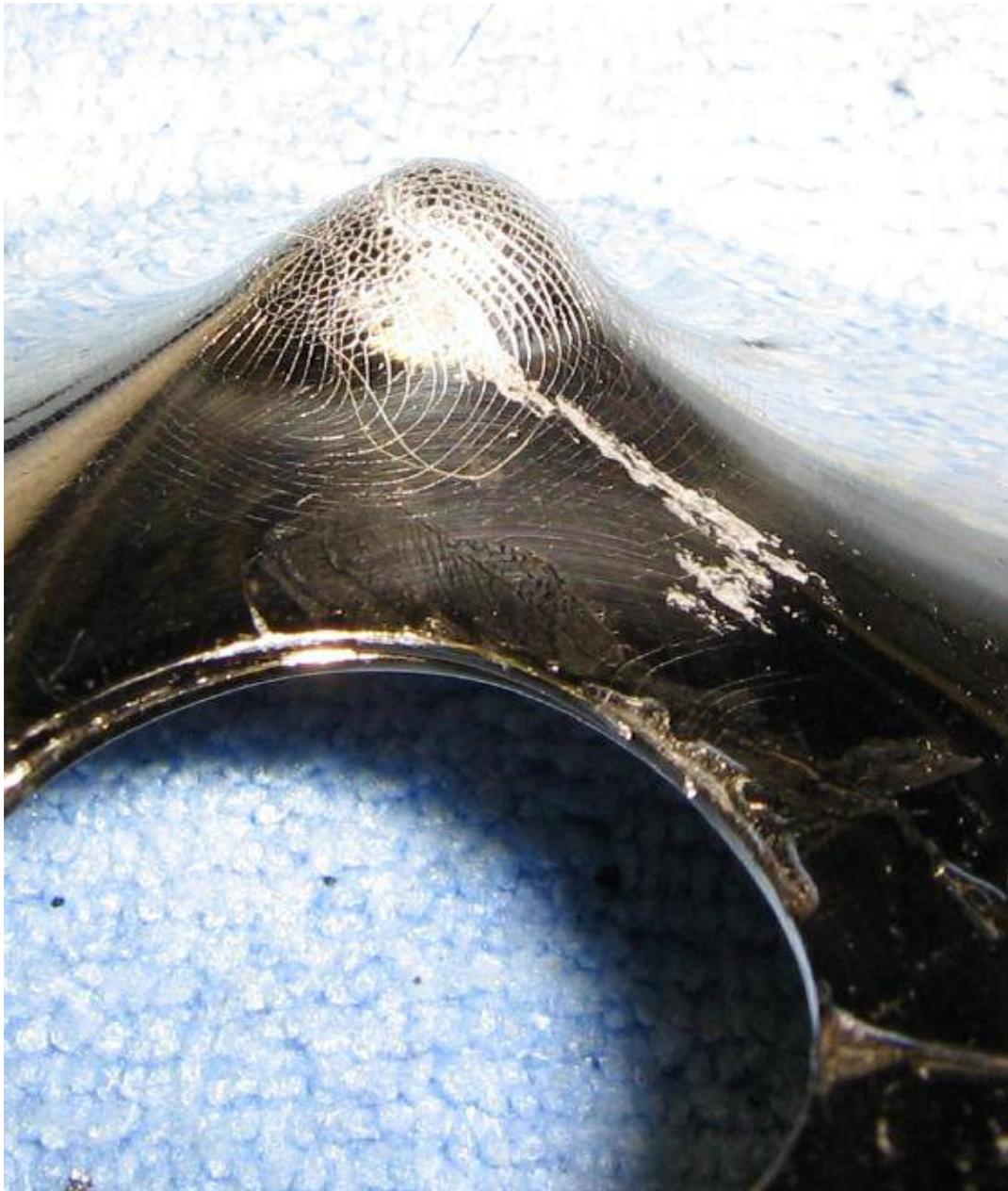
All shots were from Ruger revolvers at 20 feet. The idea was to simulate shrapnel. All the epoxy bonds broke when hit.



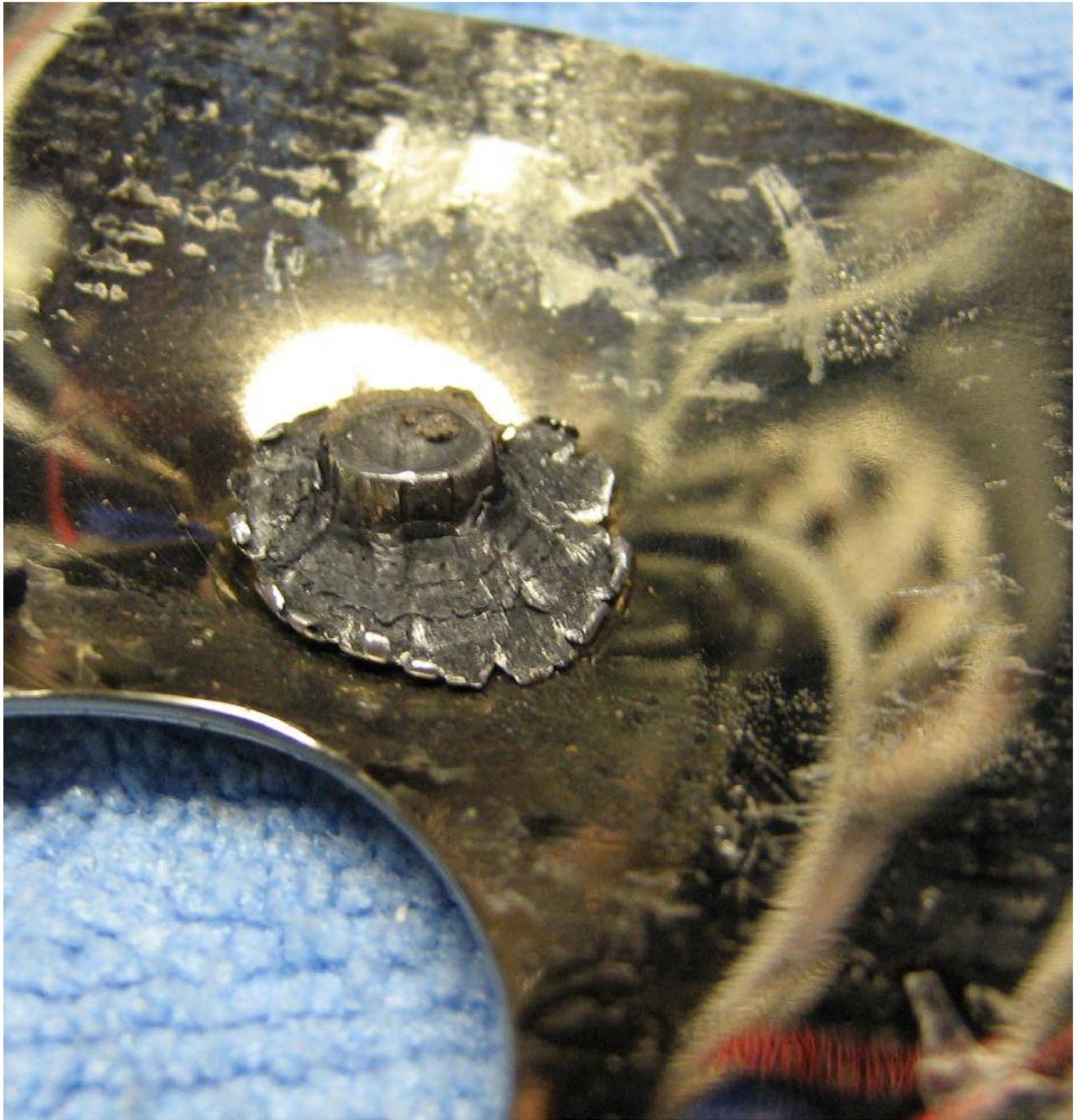
Dual hard drive platters epoxied together – .45 Colt exit.



Dual hard drive platters epoxied together – .22 LR. Stopped completely.



Rear view of the stopped .22 LR shot.



A different set of dual hard drive platters epoxied together – .22 LR with the same results.



A different test with the dual hard drive platters behind a pair of heavy leather gloves – .45 Colt went straight through. The idea is that thick leather can be used to reduce or even prevent any flesh burns from IEDs.



Exit wounds.



Dual hard drive platter combination close up. Exits.



The heavy leather gloves and dual hard drive platter combination could catch the .22 LR bullets.

## **Send it, and We'll Figure Out How to Use It**

December 21, 2004 – From: [www.techcentralstation.com](http://www.techcentralstation.com)

By Russell Seitz

What could a soldier in Iraq possibly do with a slab of armor plate or bulletproof glass? More than a defense procurement bureaucrat in Washington; hence the wise words of General De Long, USMC, Ret. on MSNBC last week: "Send it, and we'll figure out how to use it."

He was expressing the wisdom of military experience going back to the day Ugh the Grunt discovered his trusty jade ax; besides braining cave bears, could deflect the flint spears tossed by his irascible Neanderthal neighbors.

Soon this Neolithic genius studded a mammoth hide with clamshells, and composite armor was born. Within a hundred generations, Ugh's descendants were pinching Saigon man hole covers to put under their helicopter seats, and complaining to Congressmen about late flak armor deliveries. Today, plus ca change,

Middle America has a heartening tendency to actually do things for troops in the field. When grunts wrote home noting it was 140 degrees inside their tents, but that the Revolution In Military Affairs provided them with electricity to power tactical laptops, good people mobbed Walmart's to send \$99 air conditioners to the nation's sons and daughters using one of the DOD's Really Good Things : The APO . It delivers parcels, even those containing air conditioners, to war zones with FedEx speed at 4th Class prices.

So what could Santa deliver to good kids spending the holidays under fire?

The stores are bare of humvee armor kits, or this essay would be pointless. Having already exhorted the Beltway denizens to twist the arms of the Scrooges managing our stay-at-home Euroallies' arsenals, here are a few thoughts on the right stuff to fill Kevlar stockings in record time. They range from off the shelf -- or out of the scrapyard -- to industrial processes whose speed takes precedence over economy.

### **Hillbilly Electronic Countermeasures**

The Islamists' latest attempt to blow up Pakistan's president with roadside explosives ran afoul of a handy gadget called a VIP2 Road Ranger -- an electronic jammer that keeps radio controlled bombs from being triggered while their intended target is within lethal range. The Pentagon may pay about ten grand for gold-plated Mil Spec models, but the free market price of the same technology is closer to a microwave oven -- or a gray-market traffic radar jammer.

### **Used Tires**

Not just any ones, and not the whole donut. What's needed is a program to round up and skive off the Kevlar belts that rim the nation's mountains of balding aircraft radials. This would spare our landfills while affording ingenious Gunnies a prime raw material for spanning hard to fit gaps in improvised explosion shields.

## **Glass Ceramics**

Good old Corningware bowls bounce off concrete, but its ballistic resistance pales in comparison to the tougher stuff that glass makers transform into well named hard discs for computer memory drives. Cheap and readily manufactured, such materials approach the fracture toughness per unit weight of honest to gosh armor ceramics. Adding cesium to the precursor melt beefs up the computer grades, and mass production -- we're talking stovetops and windowpanes here -- can turn them out faster than silicon or boron carbide.

## **Scrap Kevlar Cloth**

Any kind of aramid -- twaron, Kevlar, Whatever -- and almost any high tenacity fiber webbing or scrim, from Spectra to Nomex, are vast improvements on the lack of it for those with time and glue on their hands to reinforce their motley improvisations.

## **Adhesives**

Duct tape kills. If you want to save a lot of lives for a little money, fast, investing it in seriously good epoxies and elastomers with energy absorbing fillers like microballoons is a highly portable way to go. If I sent one thing to Iraq, it would be high tenacity ways and means of enhancing the bonding of the catch as catch can vehicle armor people in theater improvise.

## **Small Halon Fire Extinguishers**

The kind you can no longer buy, because they are hell on the ozone layer. So are third degree burns on human skin. If you've got 'em, in your closet or kitchen, send 'em, They are needed and they work so well that I would not want to be the DA who tries invoking the Montreal Convention to keep them out of vehicles going in harm's way.

## *Rising From The Underground*



*By Damien Thorn. Originally appeared in Nuts & Volts Magazine, March 1994.*

This is HoHoCon '93. A meeting of minds sponsored by hackers, believe it or not. Since many of the attendees are people sometimes viewed as the digital delinquents of the electronic frontier, it seems rather odd that they would be involved in a conference, but it's actually not as unthinkable as it first sounds.

So what exactly is HoHoCon? According to the press release, it 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." And that's pretty much what it is, along with a small measure of adolescent misbehavior, dumpster diving at the local telco, and generally driving the staff crazy at the hotel hosting the event.

Since the coverage in the computer trade magazines tends to be very brief and sensationalistic, this article aims to provide more of a blow-by-blow description of the events constituting HoHoCon '93. Both the positive and negative occurrences are described, and some people will no doubt find the whole scenario disturbing. If you can suspend your natural tendency to make value judgements, you might just discover that you can learn something from a conference like this.

### **Background & Perspective**

Since many people have little understanding of cyberspace or the computer underground, a bit of background is probably in order. Cyberspace basically consists of the sum of all the computers and networks that are interconnected and intertwined throughout the world. The activity occurring on these nets between the thousands of host systems is happening in what is referred to as "cyberspace." Your connection to a local bulletin board system or host computer connects you to cyberspace. Electronic mail travels through cyberspace to get from the point of origin to its destination, and may pass through many systems in the process. When you teleconference with other users or participate in a forum on systems such as CompuServe, you've interacted with other people in cyberspace.

Traversing this electronic land and going from place to place to "meet" people or interact with them through electronic messages has become rather commonplace. Cyberspace is a term that still conjures up fanciful mental imagery, but you've no doubt been there and thought little of it. Even packet radio networks are a part of cyberspace, creating virtual communities over the airwaves.

In general, entering this mysterious sounding virtual world is accomplished with a simple local phone call to a node on a network. Your modem-equipped personal computer makes a connection and there you are! Your monitor becomes your portal. The words and images on the screen are as close as you can get to actually being there. The only physical existence in this virtual world are the electrons zipping through the telephone company cables and satellite links that tie all the machines together.

The Internet is currently considered the mother of all networks and the favorite domain of anyone seriously involved in the computer underground. This mammoth network links almost all government and university computers, as well as organizations and corporations involved in research for the National Science Foundation or Department of Defense. On any given evening, hundreds of people meet electronically on this net, splintered into small groups discussing any given topic.

Defining a "hacker" is a difficult task, and tends to further stereotypes. It's probably safe to say that most are addicted to technology. Some ignore the boundaries of the law, and crave the adrenaline rush that comes from beating the system. A few take this heady power over computer hardware to the extreme and wreak havoc and cause damage. Others are at the opposite end of the spectrum and are involved in the security end of computer systems.

Interests and activities run the gamut. While some are certainly involved in illegal activities, many more are gratified by simply **exploring** technology. A large number of us fall into this category, and can easily express how things work. Marketing directors and public relations staff only show us one side of products and technology. But there is always much more beyond the surface. Plenty of nooks and crannies to explore. Untapped potential to discover. Absorbing aspects that can only be seen when you look underneath or around the side of some particular technology.

Cellular communications is an excellent example. If we took the cellular industry's word a few years back, we'd believe that fraud can't happen. That our calls are private and can't be monitored. All they wanted us to comprehend was how to dial a number, press send, and pay the bill. But now we know better. We know about fraud, cloning, and monitoring calls. We know how cellular phones are programmed and how many phones have an integrated diagnostic mode that allows you to do interesting things.

These explorations of technology are neutral, in my opinion. The positive or negative end result occurs with the specific application of the information. One parallel is to look at a drug like morphine. Derived from the naturally occurring opium in the poppy plant, it is simply a substance – a particular arrangement of molecules. In the hands of a physician, the chemical provides many clinical benefits. The same substance in the hands of a drug abuser becomes a tool for self-destruction. Such pros and cons are not inherent, but lie with the given use.

The road to discovery is what I think hacking is really all about. Pushing technology a little beyond the limit to see what happens. Unfortunately, some of the people who explore are malicious people, and there are a few technologically sophisticated criminals within the ranks. The results are sometimes exploited. The point is to understand that the "dangerous hacker" who crashes systems is an exception, and not the rule.

As for those who disregard the law, the most common offense is the unauthorized access and use of remote computer systems. Pretty common among teenagers who are rebellious and still testing limits during the natural struggle that results in adulthood, most mean no intentional harm. Over the years, these attempts to break (or "hack") into a system have become the standard definition of the term hacker – much to the dismay of the computer pioneers who wore the label with pride.

While acknowledging that these types of hacks cause problems and a great deal of anguish for the victims, Judas Gerard, a hacker from California questions the perception that these young people are as ill-intentioned as the government portrays them to be in the media. Judas believes that governmental agencies are embarrassed and feel threatened by the fact children can access their computers.

"When you have kids romping through your computers, how do you think they feel? For every publicly exposed incident like the German kids seriously compromising the internal network of NASA, there have been hundreds of other explorations of systems. If such relatively unsophisticated people can get in, what do you think foreign intelligence agents can do?" asks Judas rhetorically.

"Disinformation and unconstitutional raids like 'Operation Sundevil' are the result of governmental frustration," claims Judas. "Some young man reads an unclassified online document and is charged with treason, much to the delight of the news media. A bunch of laptop computers get stolen from a military base by a government employee and sold on the open market. It is discovered that these computers contain classified Desert Storm battle plans. What happens? A two paragraph mention on a newswire, and we never hear about it again. Truth and justice? Not by a long shot."

While Judas' views certainly don't tow the party line, it is apparent that he believes most of the illegal hacking taking place is akin to graffiti spray painted on buildings by less technically sophisticated teens. He relates that these occurrences are more adolescent pranks than nefarious plots as often reported in the press, explaining, "It's a challenge for them. They just don't consider how the system operator is going to feel about the situation at the other end of the connection. Those administrators get seriously unhappy about things like that, and can't tell a kid from an industrial spy over a network connection."

Moving on to HoHoCon itself, you'll see some examples of this delinquent behavior and disregard for the rights of others, but this is not the focus of the conference. This is really a forum where hackers, security people, law enforcement, and attorneys can interact; exchange information, and ideas. This is where members of the computer underground can air their collective views on a variety of subjects ranging from President Clinton's controversial "Clipper Chip" encryption technology (complete with built-in back door), to the ramifications of computer viruses. HoHoCon is not a "how-to-back" seminar.

## **Friday – The Prelude to a 'Con**

HoHoCon '93 officially ran from Friday, December 17th through Sunday the 20th at the Austin North Towers Hilton in Texas. The actual formal conference was scheduled to last most of the day on Saturday. The rest of the weekend consisted of small, informal meetings and socializing throughout the hotel.

These small group discussions are an important part of the conference, as this is where most of the interaction between participants took place. The hotel lobby contained at least one knot of

constantly changing faces almost 24–hours per day. This informal sub–conference was dubbed "LobbyCon" by many of the attendees.

Although the Hilton staff were obviously unsure what to make of this motley assortment of people, they encouraged the non–stop use of the lobby in the hopes that people would quit running around the hotel. As you'll soon understand, these conferences generally have to find a home at a different hotel each year. The misconduct of some attendees leaves the management with the feeling that their establishment is under siege.

The problems began Friday afternoon when stickers bearing the likeness of the pipe–smoking "Bob" (of the Church of the Subgenius) began appearing, stuck to various surfaces in the hotel common areas. Later in the evening, hotel security discovered a phone line running down the hall between two rooms at the associated Super–8 motel complex next door.

The security guard entered the room and found two teens sitting in front of laptop computers. One of the young men was the occupant of the room next door, and he had run the long cord from his room into this room so that he could sit with his friend and compute. Noticing that both laptops were connected to some remote system via modem, the guard became convinced that all manner of nefarious virus–spreading, system–crashing activity must be taking place, in addition to the obvious toll fraud.

The manager quickly summoned the Austin police and had the hotel telephone operator print the phone bills for the two rooms, anticipating that the records would be necessary evidence for the Grand Jury indictment he was envisioning.

One of the boy's phone bills was eight pages long, but almost all the calls were local. The total amount owed to the hotel was less than three dollars, and the officers determined that the computer account being accessed was legitimately assigned to one of the teens. A big production had been made out of nothing, fueled by the fear of the "evil hacker" stereotype. That these were high school freshmen at best was of no mitigation to the hotel management, who summarily evicted the youths.

Meanwhile, back in the lobby of the Hilton several people were monitoring the police communications on their scanners. Being a resourceful journalist, I had brought my portable scanner and OptoElectronics 3000A frequency counter as well, and had long since determined that the radios used by the Hilton were transmitting on 466.010 MHz.

As night was falling, a group of us walked across the street to the mall to have some dinner. Accompanying me were Net Distortion, Excaliber and Legacy Irreverent, sysop of the "CyberPunk System" – an underground BBS in Wichita, Kansas. Having communicated with Legacy online and accessed his system for almost two years, it was great to finally meet the man behind the computer screen.

Since most people use an alias when riding the networks (as you may have noticed by the handles used herein), all you ever really get to know is the persona presented on your monitor. The opportunity to finally meet people in person with whom you've communicated over time is one of the definite personal benefits of gatherings such as HoHoCon. It was refreshing, and many false assumptions about people were destroyed throughout the weekend.

After dinner, we returned to the Hilton to find a gentlemen engaged in animated conversation with a hacker known as Citizen Fish. This was Michel E. Kabay, Ph.D., president of the Jinbu Corporation of Montreal. In addition to his information management company, Dr. Kabay serves as director of education for the National Computer Security Association.

Feverishly taking notes on his laptop computer, Dr. Kabay probed deeply into the motivations behind various activities ranging from the writing of computer viruses to illegally accessing mainframe systems. Spending over an hour involved in this round-robin discussion, I couldn't help but note Dr. Kabay's astonishment at some of the things he was learning. Having flown in from Canada, Dr. Kabay realized he was receiving an education he couldn't have purchased elsewhere at any price.

Computers, being the machines that they are, tend to depersonalize interactions between people. As one of the more progressive people in the security field, it was no wonder that Dr. Kabay spent most of his time exploring the human issues such as motivation and attitude. No seminar on computer security can effectively capture those elements. In return, the hackers participating in the discussion were exposed to the attitudes and personal concerns of information services managers.

Dr. Kabay enlightened us by explaining that even the most non-destructive penetration of a computer system can cost a company large amounts of money, untold man-hours, and possibly the loss of data. While the hacker may have relatively innocent motives, and just take an apparently harmless look around the files on the machine, a proper security response can be mammoth. The crux of the issue is not that someone managed to breach the system security, but rather that the company management no longer can be absolutely sure of the integrity of the data on the system.

Destroyed was the assumption that someone could "innocently" hack at someone's system for the challenge without causing problems. The computer industry openly admits that the overwhelming majority of theft and tampering occurs at the hands of the corporations' own employees, and the bulk of the computer security policy and procedures are designed to protect systems from their own workers, not malicious outsiders. But any compromise of a system is taken seriously, prank or not.

## **Saturday – The Conference**

At about 10:00 Saturday morning, attendees began lining up outside the ballroom where the conference itself was to be held. Manning the registration table were 'dFx' and his associate from the text file writing group Cult of the Dead Cow ('cDc'). On a side note, we'll be referring to dFx by his first name – Jesse – from here on with his permission.

Registration fees were only \$5.00 per individual, or \$25.00 for a corporate representative. Raffle tickets were also being sold, and approximately 350 people registered for the conference. As people were filing into the ballroom, Bernie R. Milligan, President of Communications & Toll Fraud Specialists in Houston, was busy taking picture after picture of the attendees. This disturbed some of the hackers, and many seemed amused when Mr. Milligan's camera finally jammed and he left the area.

The conference eventually got underway, and after an introduction by Jesse, the first speaker approached the podium. This was Bruce Sterling, author of *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*. Mr. Sterling's book is perhaps one of the best works describing the sociological aspects of the goings on in cyberspace. Unlike other authors, he paints a compelling picture of the human side of the computer underground.

During his speech, Mr. Sterling said that he had decided to give away his book in electronic form via the Internet, much to his publisher's horror and his personal financial ruin. This was his way of "giving back" some of what he had received from the computer underground. Sterling then moved onto his major theme, a call to action regarding viruses.

"You shouldn't be spreading viruses that only [mess] with grandmothers who have PCs. There is no freedom in writing and spreading viruses. It does not increase anybody's options, it does not empower people in any way, it does not make communication more fluid, it does not increase the speed of transmission of ideas," he said exhorted the audience.

"People who write viruses may pretend to be rebels of some kind, but those people are lick-spittles," exclaimed Sterling. Continuing, he said, "Corporate security people go to expensive corporate security meetings that cost fifteen hundred bucks to get in, not five dollars [like HoHoCon]. They learn how to defeat viruses, and they can keep viruses at bay from their own little, tight grey-suited [systems]. Meanwhile, all these viruses made up by these creepy Iron Maiden-listening little dork kids from Bulgaria go off and screw up the machines of hippies, grandmothers, school teachers and other helpless human beings ... information wants to be free, okay? It doesn't want to be *infected!*"

After Sterling's impassioned speech, next up was Ray Kaplan, an industry security consultant from Arizona. In his opening remarks, Kaplan said, "People want to know which side Kaplan is on. I'm here because I love the technology, I love to meet people, share things, and figure stuff out. I'm not a criminal, I don't bust people – I'm not a Fed on the other side – I'm just here because I'm a lot like most of you. I hope you'll use that to temper your view of my remarks."

Kaplan went on to suggest that HoHoCon be teleconferenced or videoconferenced rather than limiting it to a fixed number of people in a room. After introducing a young lady described as a "struggling independent video producer" who was video taping the conference, he launched into the main subject of his talk.

He believes that it is time for the underground community to pull together and collect, verify, and widely distribute vulnerability information about various computer security problems. "My idea is that we need ... an intrusion reporting and vulnerability tracking database." He also indicated that he was aware of the existence of a "gaping hole" in the VMS operating system, and requested anyone with information about this security problem to talk to him after the conference. Kaplan related that "DEC [Digital Equipment Corporation] and the incident response community is not being very kind to us [about providing details regardless the bug]."

In an earnest discussion about hacker ethics, Kaplan states, "Do illegal things and the cops will be on you. I know that, because I know Feds [federal agents]. If you have visibility, they'll come after you. Do immoral things ... and your future prospects for employment will be diminished. Nothing breaks my heart worse than to see a talented [hacker] get chased away from gainful employment where he could do the world some good because of some indiscretion committed when he or she was too young to understand the violent rebellious nature of society toward anybody who steps out of line with the status quo."

Next up was the two-man cryptography panel comprised of Douglas Barnes and Jim McCoy, members of Austin's chapter of the Electronic Frontier Foundation. Barnes began, "I have a public service announcement here as a result of the things that happened last night [at the hotel]. It's very important for people to practice this. I want everyone to repeat after me: 'I want to talk to my lawyer.' After the crowd repeated the phrase several times, Barnes concluded, "This PSA has been brought to you by the Austin Cryptographers' Workshop."

The basic content of this self-described cipherpunk's presentation was to advocate the use of encryption for files and mail being sent across networks, whether or not the information was sensitive. The most difficult hurdle to overcome is the attitude that people who use encryption must have something to hide. Barnes explained that this is not really a valid assumption, especially

based on the number of machines a message must pass through to get from point A to point B.

Barnes feels as more people begin using encryption on an everyday basis, encryption will no longer be viewed as a technology used only by people with something to hide. Additionally, the use of encryption often reduces liability since the operators of various systems are unable to read these packets of e-mail and files. No system administrator can be held accountable for, or blamed for, the release of information of which they have no knowledge.

After the cryptography panel, Jesse displayed the official HoHoCon '93 T-shirts which were on sale at the event. The word NARC is emblazoned across the front, and the "top-ten narc list" printed on the back.

The next speaker was Netta Gilboa, the publisher and editor of a new quarterly magazine known as *Gray Areas*. The magazine's slogan is "In life, there is no black and white, only *Gray Areas*," which is exactly what the magazine covers. Recent issues have covered topics ranging from bootleg audio cassettes to computer viruses. Look for the 'zine at your local Barnes and Noble bookstore.

Continuing with the magazine theme, your truly spoke next, somewhat nervously providing an overview of Nuts & Volts. About twenty-five percent of the attendees were familiar with the magazine, and seemed relieved to discover who I was, based on my omnipresent tape recorder and Nikon. Moving to firmer ground, I spent about ten minutes fielding questions related to cellular technology.

After I thankfully sat down, John Draper, known as "Captain Crunch" gave his talk. Draper is probably one of the oldest phone phreaks who still participates in "the scene" – as it is called. Gaining notoriety years ago for his development and experimentation with the toll-fraud device known as a "blue box," Draper's handle originated when he discovered that the toy whistle included in a box of a Captain Crunch cereal happened to emit a frequency of 2600 Hz when blown. This particular frequency was of significance because it was used to blow off a toll trunk prior to sending multi-frequency (MF) routing signals down the trunk with the blue box to establish a connection anywhere in the world.

Today most of the network is digital and an MF generating device such as the blue box is all but useless due to the lack of inband signalling in most areas. The device is not completely dead in the water though, because blue boxing does continue today, using several little-known methods of accessing international trunks.

Draper began his speech by disparaging any law enforcement officials in attendance, and explained how he had hacked the in-flight phone service on his way to the conference. "They still have a few bugs to work out in the 'airphone' system," he joked, moving on to discuss his involvement in the Rave scene (much to the disbelief of the audience) where he encouraged the use of free encryption programs such as Pretty Good Privacy (PGP). After declining a few cat-calls asking him to demonstrate his dancing style, the venerable phreak discussed his experiences exploring the phone system in the former Soviet Union. This led rather naturally to a talk by a software developer from Russia.

Just before introducing the men comprising Legion of Doom Communications, Jesse thanked the various media representatives who had attended to provide coverage of the event. Aside from those of us who had spoken, personnel from the *Los Angeles Times*, *Vibe Magazine*, and a crew from a Japanese television network were some of the others present.

As the group from LOD Communications approached the podium, a barrage of camera flashes erupted to capture the moment on film. Other than perhaps New York's Phiber Optik, no group of hackers in the United States has received as much media coverage in recent years as the infamous Legion of Doom.

With the allegedly illegal activities behind them, LOD Communications was formed to preserve the history of the computer underground and make it available to others. The participants in this endeavor attending the conference included Lex Luthor, Phantom Phreaker, Erik Bloodaxe, Professor Falken, and Mark Tabas.

Lex Luthor, as founder of the Legion of Doom, explained the "Digital Archaeology" project LOD Communications initially conceived in 1986. Taking turns at the podium, members described their work at collecting and compiling message bases and files from many of the classic underground bulletin board systems from the early 1980s.

"I think that our project is really positive for a lot of reasons. One, the historical perspective. You can look back and see what was going on at the time. Two, a lot of the theoretical background you can still apply to today's underground," relates Phantom Phreaker. "Three, I think the social scene was different then. This was before [magazines like] *Wired*, *Mondo 2000*. This was when *TAP* and *2600* were around. It's a whole different ball game today, but to understand what happened in the past and the history of this contributed to the underground as it exists today."

They are also looking for messages and text files from BBS systems of this era, regardless of the type of computer or size of the disk. Hard copy is also appreciated.

Luthor then introduced Frosty from SotMESC, an abbreviation for Spur of the Moment Elite Social Club, and made a \$50.00 donation to his scholarship fund. Frosty described their intention of funding scholarships for young people in the hacker community.

Erik Bloodaxe, editor of *Phrack Magazine*, remained at the podium and exhibited he "Hacker Wars" T-shirts that were available in the rear of the conference room. He also mentioned that he was going to produce a second run of the coveted "Legion of Doom – Internet World Tour" T-shirts from 1991. He then demonstrated equipment that is part of an emerging technology.

"Those of you who are ham enthusiasts are very familiar with the concept of packet radio. It seems that a lot of companies have decided that, 'Gee that's a pretty good idea.' At the present, there are two commercial packet radio services that are in operation in America. One is run by a company called Ardis that is a joint venture between IBM and Motorola. If you see IBM service reps or other people walking around with a little white keyboard-like thing ... they are communicating back and forth over this Ardis network."

Pulling several devices from their protective cases, Bloodaxe showed the crowd several wireless modems that use both the Aris and RAM data networks. He went on to describe the RadioMail service that allows Internet e-mail to be exchanged over these networks.

His presentation wound down after a discussion of advances in paging networks and some of the packet protocols used by these commercial service providers. The subject of intercepting the packets being transmitted over these wireless mediums was brought up by an audience member.

A rather odd talk then ensued regarding a group of hackers who allegedly found evidence of alien life forms within government documents stored on systems that were accessed via dialups hidden within an unassigned telephone prefix in Virginia. Being a very convoluted and controversial

topic, you'll have to get the full details from a back issue of *Phrack* if you have an interest in extraterrestrials and the apparent cover-up.

The raffle was held next, and a ton of stuff was given away. The best prize was a complete multimedia PC.

The second to last speakers were Count Zero and Kingpin from Restricted Data Transmission (RDT) of Boston. Count Zero discussed hundreds of government bulletin boards that are publicly accessible, and arranged to have a point-to-point demonstration of packet radio after the conference. Several handouts were distributed, including a two-page summary of reprogramming access codes for various cellular telephones.

Kingpin described a device the group was working on that generates a variety of communication signalling tones, as well as several pieces of cellular test equipment they hoped to design and produce at an affordable price.

The final speaker of the conference was a relatively famous computer-savvy attorney practicing in the Texas area.

"To give an idea of where [lawyers] are at right now, I was talking to the head computer lawyer in Houston – the guy who appoints people to committees. He asked me what I had been doing, and I told him I had been defending some people charged with misconduct on the Internet and things like that. He listened to me talk for awhile and then says, 'What's the Internet?'" He concludes, "We [the legal profession] have a long way to go."

### **PartyCon '93**

A party atmosphere pretty much enveloped the conference-goers Saturday night. Most people rejoined their clique-like small groups in various rooms of the hotel, but everyone seemed more relaxed and congenial. On Friday night people had tended to be a bit snobbish and self-absorbed, which is not unusual behavior for some in the hacker scene.

The *creme de la creme* of the hacker computer underground were gathered here, and the social pecking order is an important formality to many. In a world where people come to know you by little more than words on a screen and a pseudonymous handle, quite a bit of knowledge and effort is required to "hack" yourself a rung on the social ladder. A great number of text files and other tutorials are not really written for altruistic sharing of knowledge, but rather to establish the author's credentials and gain the associated respect and recognition from the underground community.

While some might view this as petty or counterproductive, it's just the way it is in cyberspace where many people pretend to be something (or someone) that they are not. An explanation of how one becomes a member of the 'elite' ranks is the subject of an article unto itself. The end result is that a certain amount of social order is present in what might otherwise be chaos.

Since I'm discussing the subject, it is worth mentioning that several of the men whom I consider part of the elite cadre turned out to be quite different than I anticipated. Erik Bloodaxe, editor of the online magazine *Phrack*, is an excellent example. He was friendly and a far more down-to-earth guy than expected, and didn't fit the egomaniacal image I had erroneously managed to form of him.

I personally believe that *Phrack* contains more informative and insightful information than any other source. Since he's taken over publication, it now runs 300–400 pages per issue when printed out. Best of all, it's free to individuals not involved in the computer or security industry.

In a second floor room of the adjacent motel, an impromptu local area network (LAN) had been set up by a group of university students and had mysteriously become a host on the Internet named "hohocon.com" thanks to a little hacker magic. With at least seven nodes running on the net at any given time, this room was in full swing during the entire three-day conference. Continuous activity included various forms of "net surfing" like Internet relay chat (IRC), or coding new software for the Unix operating system.

Meanwhile, back at LobbyCon in the Hilton, the great paranoia race was on. A recurring pass-time was playing "spot the fed" – trying to guess who in attendance might be with the FBI or Secret Service. Bernie Milligan had returned and been noted in the parking lot writing down license plate numbers and was now wandering the hotel.

Shortly after that bulletin, a few people were speculating about an elderly woman who had been sitting alone on the couch for over an hour, occasionally muttering to herself. Suddenly one of the 'con attendees walked into the lobby and swore that this same lady had been hanging out in the lobby of a Las Vegas hotel earlier in the year during a similar hacker conference known as Def Con.

A plan was quickly formulated after the OptoElectronics frequency counter failed to detect any RF emanating from her general area. Armed with the knowledge that she must be with the Secret Service, I accompanied a few hackers to the hotel restaurant and picked up several pots of coffee and a tray full of cups. Offering this woman a cup of coffee and pouring it for her was to be the subterfuge allowing us to get close enough to take very "near field" readings of any radio activity that might be taking place under her overcoat.

Upon returning to LobbyCon the woman had mysteriously vanished – just like the man wearing a beer cap that had been spotted hanging out suspiciously near the payphones.

Many of the tired hackers were ecstatic to note the appearance of the coffee, so it didn't go to waste. Food was a little less plentiful, and it didn't take long for a story to circulate about the two guys who risked federal prison by trying to have pizza delivered, charged to a stolen credit card number. Fortunately for the pair (and the local Domino's Pizza), the plot failed. Turns out the young man on the phone couldn't read the number written down by his partner in crime. Based on the invalid card number, Domino's declined to deliver, and I resolved to stay as far away from the bank of payphones as possible.

On another front, some resourceful person had discovered that dialing extension 5199 connected you to the maintenance dialup port for the hotel's PBX system. The operator had to keep a watchful eye on her terminal all night to prevent anyone from logging in. Apparently she later gave some of the guys home-baked cookies to spread the word that she didn't care what anyone did as long as they stayed out of the innards of her telephone system.

Saturday was a long day for everyone involved.

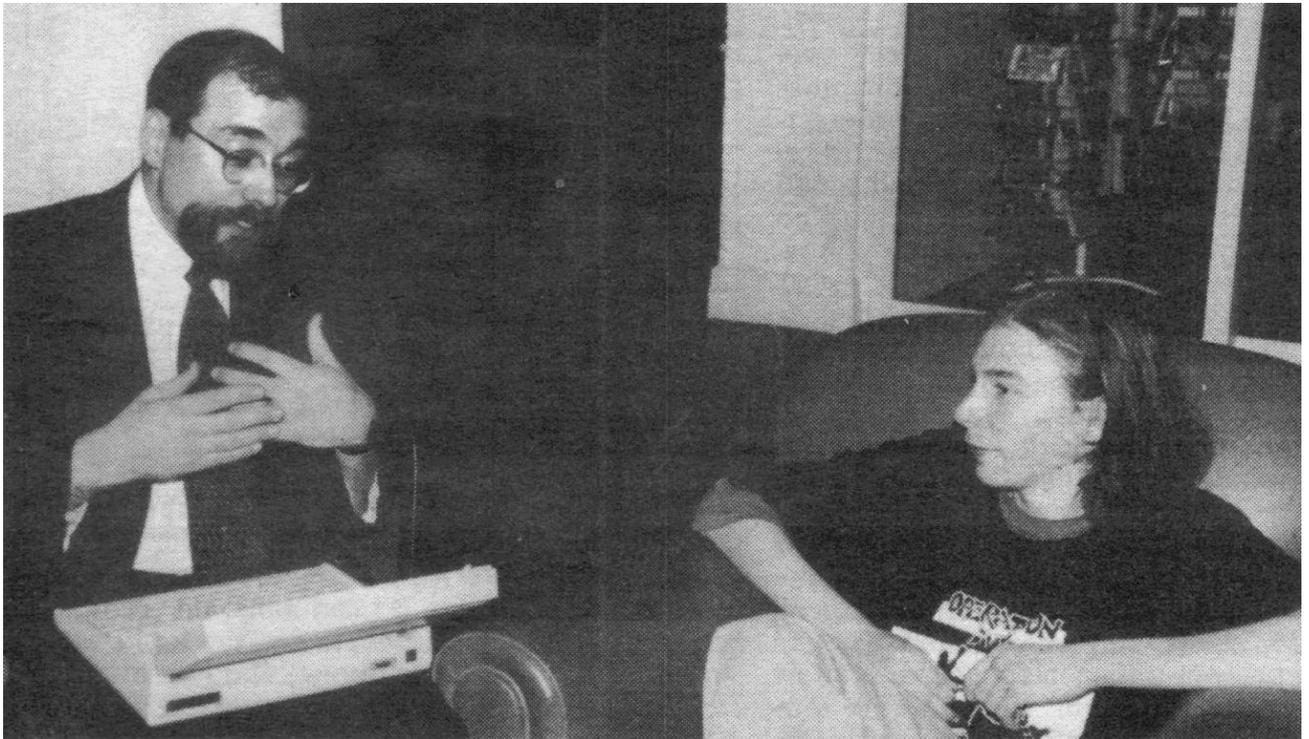
## **Sunday – Conference Closing**

Being the last day of the conference and devoid of any planned activity, Sunday was pretty relaxing. Other than the theft of a telephone receiver from a lobby phone and a smoke bomb in the Super-8 Motel causing a fire alarm and evacuation at 2:00 AM, it was also fairly calm. The Austin police declined to come out and investigate the case of the missing receiver, and the hotel staff did not discover that one of the elevator control panels had been unscrewed to gain access to the "private" top floors of the hotel (which require a special card key). Some suspected that these inaccessible concierge floors had been converted to a command post by federal agents.

All in all, the day consisted of farewells, "quality" conversation, and plans being made for future conferences, none of which will be held at the Austin North Hilton Towers and Super-8 Motel for obvious reasons. Although the income generated by the conference was substantial and the damage minimal, hotels tend to frown on hosting a three-day technological frat party ... and that's pretty much the atmosphere once the day-long conference itself is over.

While my observations and opinions of HoHoCon '93 as described are no doubt colored by my perceptions and beliefs, I hope that enough groundwork was laid so that the non-hacker can appreciate the significance of this event. Many people, myself included, learned a great deal and benefitted from the opportunity to meet some of the major players in the computer underground, despite all the shenanigans.

I feel the lesson to be learned about hackers, even if one is unable to comprehend anything else, is that these people come from all walks of life and are pretty decent people. They run the occupational gamut from the unemployed to engineers at government think-tanks. The common denominations are an above-average intelligence and a fascination with computers and technology.



**Photo 1 – Michel E. Kabay, Ph.D. interviews Citizen Fish**



Photo 2 – Jesse Dryden displays the official "Top Ten NARC List" HoHoCon '93 T-shirt.

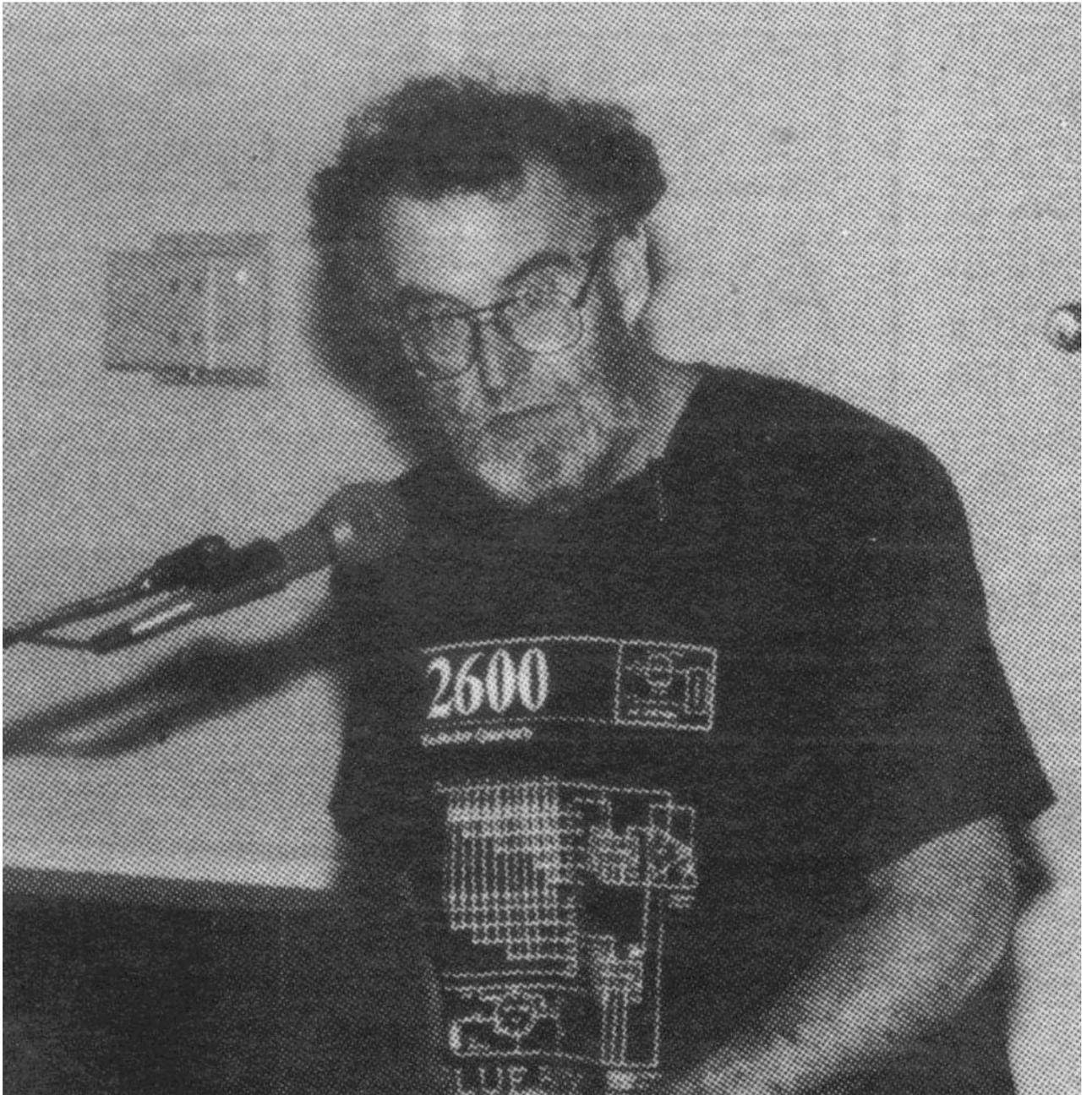


Photo 3 – John Draper (Captain Crunch)

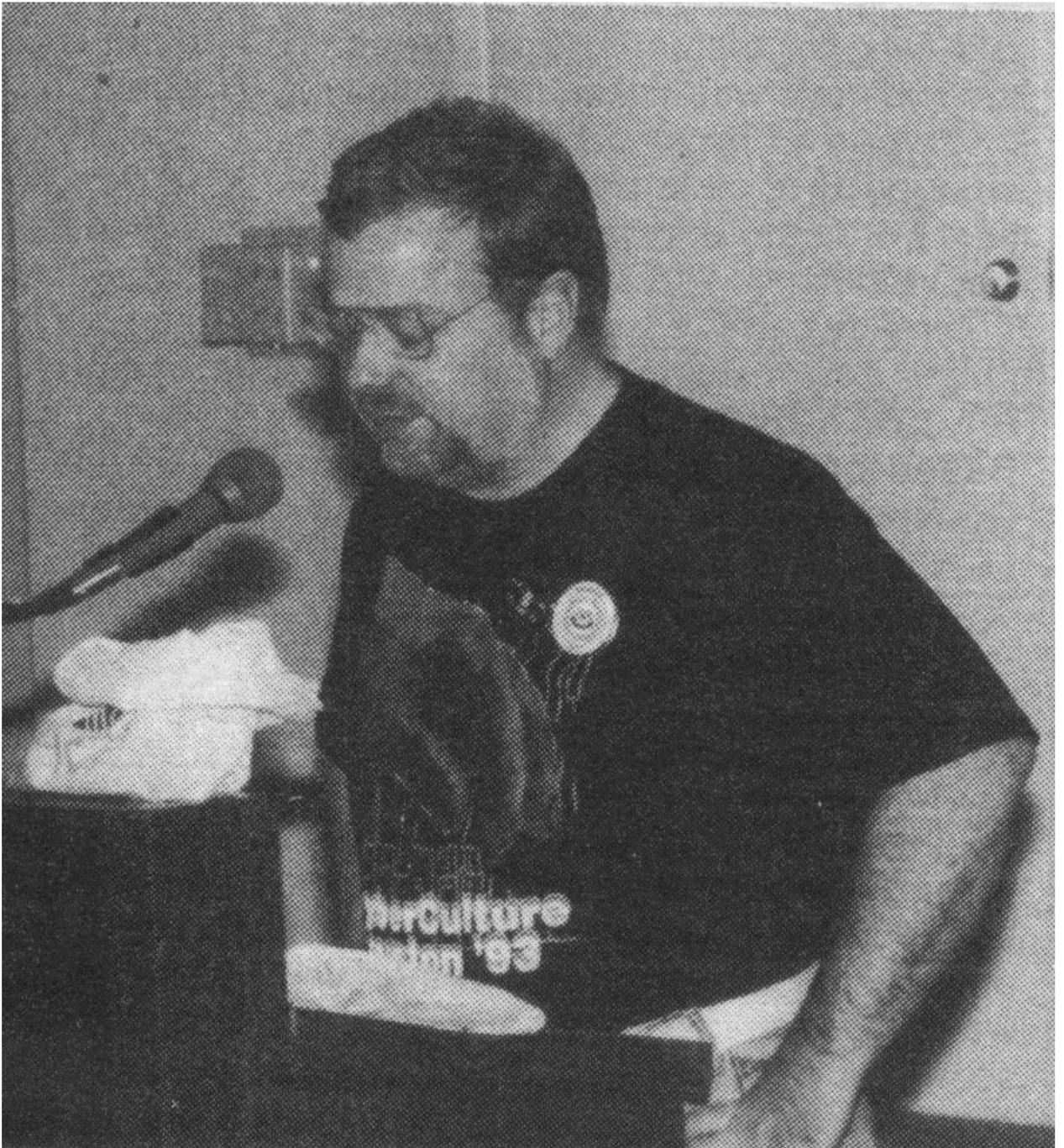


Photo 4 – Steve Ryan



**Photo 5 – LOD Communications**

# Bonus

Yahoo! My Yahoo! Mail Welcome, Guest [Sign In]

Web Images Video Audio Directory Local News Shopping More »

**YAHOO!** SEARCH download 2600 hacker quarterly magazine Search

Answers Search Services | Advanced

Search Results 1 - 10 of about 29,000 for download 2600 hacker quarterly magazine - 0.11 s

1. [\\$2600 Magazine Information](#)  
Download them off eMule you dumbass! ( BitTorrent ... Pay Your \$5.50 **Quarterly** - Ask No Questions. Other Magazines. What makes a good **hacker magazine?** ...  
[gbppr.dyndns.org/PROJ/2600/index.html](http://gbppr.dyndns.org/PROJ/2600/index.html) - 364k - [Cached](#) - [More from this site](#)
2. [2600 | Off The Hook](#)  
You can also automatically **download** the show every week using "podcasting" software. ... **2600 Magazine**. P.O. Box 752. Middle Island, NY 11953. Telephone: 631 ...  
[www.2600.com/offthehook](http://www.2600.com/offthehook) - 13k - [Cached](#) - [More from this site](#)
3. [Yahoo! Podcasts Search Results for quarterly](#)  
MAKE **Magazine** (4)MAKE is a **quarterly** publication from O'Reilly for ... **2600: The Hacker Quarterly** Rate and Review The **Hacker Quarterly**. Free. 0 Subscribers ...  
[podcasts.yahoo.com/search?t=1&p+=quarterly](http://podcasts.yahoo.com/search?t=1&p+=quarterly) - 25k - [Cached](#) - [More from this site](#)
4. [Hacker Quarterly Magazine Collection \(Winter, Spring, Summer Edition\) " \[r3m\]Team Internet Blog! daily updated!](#)  
... Benchmark Chat Install HDD **Download** Desktop Enhancements Print & Scan Data ... to George Orwell's Nineteen Eighty-Four) and his company **2600** Enterprises, Inc. ...  
[r3mteam.org/2006/09/06/hacker\\_quarterly\\_magazine\\_collection\\_winters...](http://r3mteam.org/2006/09/06/hacker_quarterly_magazine_collection_winters...) - 45k - [Cached](#) - [More from this site](#)
5. [ComputerUser.com News: Appeals court to take more time to ponder DeCSS case](#)  
Lawyers representing "**hacker quarterly**" **2600 Magazine** said it was "good news" ... Reported by Newsbytes.com, <http://www.newsbytes.com>. **Download** to handheld device ...  
[www.computeruser.com/news/01/05/15/news4.html](http://www.computeruser.com/news/01/05/15/news4.html) - 39k - [Cached](#) - [More from this site](#)
6. [2600: The Hacker Quarterly @ podcast.com](#)  
want the convenience of having our magazine come directly to your home office ... the last few days trying to download all

## End of Issue #33



Any Questions?

---

### Editorial and Rants

*Eurosavage Logic: Club Gitmo = Bad, Throwing People Into the Sea = Good*

### Greece Denies Dumping Illegal Immigrants into the Sea

September 28, 2006 – From: [www.spiegel.de](http://www.spiegel.de)

Illegal migrants rescued by the Turkish Coast Guard in the Aegean Sea claimed Greek officials had thrown them overboard. If their story is true, it's an international scandal. It also calls attention to another hotspot for immigrants trying to reach Europe.

Greek authorities have denied knowledge of an alleged incident in which Greek officials threw illegal immigrants into the Aegean Sea off the coast of Turkey. On Tuesday morning, some 31 illegals were plucked out of the sea near the Turkish coastal city of Izmir. **They claimed that the Greek Coast Guard had thrown them into the water. They did so, said one survivor, "without even asking if we could swim," according to Turkey's state-owned Anatolia news agency. Six people have reportedly drowned; three are missing.**

Greek officials denied the charges in general terms. "We never throw people into the sea," said Haris Bournias, a Greek Coast Guard commander on the island of Chios. Turkey's coastline is a major transit area for illegal immigrants trying to reach Europe, and Bournias said smugglers regularly set immigrants adrift in little boats without lights. "Many people drown that way in the straits," said Bournias, and in fact early reports in the Turkish media claimed the survivors had washed ashore after their boat sank off the Turkish coast.

Still, on Wednesday Turkey's Foreign Ministry lodged an official complaint through diplomatic channels in Athens. "Greek authorities have been increasingly dumping some groups of illegal

migrants in Turkish waters in violation of a bilateral agreement to return them," said ministry spokesman Namik Tan in a statement, adding that "the mentioned practice cannot continue."

According to reports, the survivors included Palestinians, Lebanese, Tunisians, Iraqis and one Algerian. Residents on the coast of Izmir had called the Turkish Coast Guard on Tuesday morning after being awakened by barking dogs and cries for help. The survivors claimed that they had set off from Izmir province in a boat and landed on Chios. But they were captured by uniformed Greeks who placed them on a Coast Guard ship that carried them back toward Izmir, where they were tossed into the sea. **"Two of our friends drowned in front of our eyes," Muhammedi Alti, a Lebanese national, told the Anatolia news agency. "I still can't believe what we have lived through ... We had thought that human rights would be more valuable in Europe."**

---

*I hope the Muslims destroy Eurosavage-Land.*

### **Across Europe, Worries on Islam Spread to Center**

October 11, 2006 – From: [www.nytimes.com](http://www.nytimes.com)

By Dan Bilefsky & Ian Fisher

BRUSSELS, Oct. 10 — Europe appears to be crossing an invisible line regarding its Muslim minorities: more people in the political mainstream are arguing that Islam cannot be reconciled with European values.

"You saw what happened with the pope," said Patrick Gonman, 43, the owner of Raga, a funky wine bar in downtown Antwerp, 25 miles from here. "He said Islam is an aggressive religion. And the next day they kill a nun somewhere and make his point.

"Rationality is gone."

Mr. Gonman is hardly an extremist. In fact, he organized a protest last week in which 20 bars and restaurants closed on the night when a far-right party with an anti-Muslim message held a rally nearby.

His worry is shared by centrists across Europe angry at terror attacks in the name of religion on a continent that has largely abandoned it, and disturbed that any criticism of Islam or Muslim immigration provokes threats of violence.

**For years those who raised their voices were mostly on the far right. Now those normally seen as moderates — ordinary people as well as politicians — are asking whether once unquestioned values of tolerance and multiculturalism should have limits.**

Former Foreign Secretary Jack Straw of Britain, a prominent Labor politician, seemed to sum up the moment when he wrote last week that he felt uncomfortable addressing women whose faces were covered with a veil. The veil, he wrote, is a "visible statement of separation and difference."

When Pope Benedict XVI made the speech last month that included a quotation calling aspects of Islam "evil and inhuman," it seemed to unleash such feelings. Muslims berated him for stigmatizing their culture, while non-Muslims applauded him for bravely speaking a hard truth.

The line between open criticism of another group or religion and bigotry can be a thin one, and many Muslims worry that it is being crossed more and more.

Whatever the motivations, "the reality is that views on both sides are becoming more extreme," said Imam Wahid Pedersen, a prominent Dane who is a convert to Islam. "It has become politically correct to attack Islam, and this is making it hard for moderates on both sides to remain reasonable." Mr. Pedersen fears that onetime moderates are baiting Muslims, the very people they say should integrate into Europe.

The worries about extremism are real. The Belgian far-right party, Vlaams Belang, took 20.5 percent of the vote in city elections last Sunday, five percentage points higher than in 2000. In Antwerp, its base, though, its performance improved barely, suggesting to some experts that its power might be peaking.

In Austria this month, right-wing parties also polled well, on a campaign promise that had rarely been made openly: that Austria should start to deport its immigrants. Vlaams Belang, too, has suggested "repatriation" for immigrants who do not make greater efforts to integrate.

The idea is unthinkable to mainstream leaders, but many Muslims still fear that the day -- or at least a debate on the topic -- may be a terror attack away.

"I think the time will come," said Amir Shafe, 34, a Pakistani who earns a good living selling clothes at a market in Antwerp. He deplores terrorism and said he himself did not sense hostility in Belgium. But he said, "We are now thinking of going back to our country, before that time comes."

Many experts note that there is a deep and troubled history between Islam and Europe, with the Crusaders and the Ottoman Empire jostling each other for centuries and bloodily defining the boundaries of Christianity and Islam. A sense of guilt over Europe's colonial past and then World War II, when intolerance exploded into mass murder, allowed a large migration to occur without any uncomfortable debates over the real differences between migrant and host.

Then the terror attacks of Sept. 11, 2001, jolted Europe into new awareness and worry.

The subsequent bombings in Madrid and London, and the murder of the Dutch filmmaker Theo van Gogh by a Dutch-born Moroccan stand as examples of the extreme. But many Europeans -- even those who generally support immigration -- have begun talking more bluntly about cultural differences, specifically about Muslims' deep religious beliefs and social values, which are far more conservative than those of most Europeans on issues like women's rights and homosexuality.

"A lot of people, progressive ones -- we are not talking about nationalists or the extreme right -- are saying, 'Now we have this religion, it plays a role and it challenges our assumptions about what we learned in the 60's and 70's,'" said Joost Lagendik, a Dutch member of the European Parliament for the Green Left Party, who is active on Muslim issues.

"So there is this fear," he said, "that we are being transported back in a time machine where we have to explain to our immigrants that there is equality between men and women, and gays should be treated properly. Now there is the idea we have to do it again."

Now Europeans are discussing the limits of tolerance, the right with increasing stridency and the left with trepidation.

Austrians in their recent election complained about public schools in Vienna being nearly full with Muslim students and blamed the successive governments that allowed it to happen.

Some Dutch Muslims have expressed support for insurgents in Iraq over Dutch peacekeepers there, on the theory that their prime loyalty is to a Muslim country under invasion.

So strong is the fear that Dutch values of tolerance are under siege that the government last winter introduced a primer on those values for prospective newcomers to Dutch life: a DVD briefly showing topless women and two men kissing. The film does not explicitly mention Muslims, but its target audience is as clear as its message: embrace our culture or leave.

Perhaps most wrenching has been the issue of free speech and expression, and the growing fear that any criticism of Islam could provoke violence.

In France last month, a high school teacher went into hiding after receiving death threats for writing an article calling the Prophet Muhammad "a merciless warlord, a looter, a mass murderer of Jews and a polygamist." In Germany a Mozart opera with a scene of Muhammad's severed head was canceled because of security fears.

With each incident, mainstream leaders are speaking more plainly. "Self-censorship does not help us against people who want to practice violence in the name of Islam," Chancellor Angela Merkel of Germany said in criticizing the opera's cancellation. "It makes no sense to retreat."

**The backlash is revealing itself in other ways. Last month the British home secretary, John Reid, called on Muslim parents to keep a close watch on their children. "There's no nice way of saying this," he told a Muslim group in East London. "These fanatics are looking to groom and brainwash children, including your children, for suicide bombing, grooming them to kill themselves to murder others."**

Many Muslims say this new mood is suddenly imposing expectations that never existed before that Muslims be exactly like their European hosts.

Dyab Abou Jahjah, a Lebanese-born activist here in Belgium, said that for years Europeans had emphasized "citizenship and human rights," the notion that Muslim immigrants had the responsibility to obey the law but could otherwise live with their traditions.

"Then someone comes and says it's different than that," said Mr. Jahjah, who opposes assimilation. "You have to dump your culture and religion. It's a different deal now."

Lianne Duinberke, 34, who works at a market in the racially mixed northern section of Antwerp, said: "Before I was very eager to tell people I was married to a Muslim. Now I hesitate." She has been with her husband, a Tunisian, for 12 years, and they have three children.

Many Europeans, she said, have not been accepting of Muslims, especially since 9/11. On the other hand, she said, Muslims truly are different culturally: No amount of explanation about free speech could convince her husband that the publication of cartoons lampooning Muhammad in a Danish newspaper was in any way justified.

When asked if she was optimistic or pessimistic about the future of Muslim immigration in Europe, she found it hard to answer. She finally gave a defeated smile. "I am trying to be optimistic," she said. "But if you see the global problems before the people, then you really can't be."

---

Words can't express how incompetent these people are.



### **The United States and North Korea Reach Agreement on Nuclear Program**

US Department of State Dispatch, Oct 31, 1994

Statement at a White House briefing, Washington, DC, October 18, 1994.

Good afternoon. I am pleased that the United States and North Korea yesterday reached agreement on the text of a framework document on North Korea's nuclear program. This agreement will help to achieve a long-standing and vital American objective – an end to the threat of nuclear proliferation on the Korean Peninsula. This agreement is good for the United States, good for our allies, and good for the safety of the entire world. It reduces the danger of the threat of nuclear weapons spreading in the region. It is a crucial step toward drawing North Korea into the global community.

I want to begin by thanking Secretary Christopher and our chief negotiator, Ambassador-at-large Bob Gallucci, for seeing these negotiations through. I asked Bob if he had had any sleep – since he is going to answer all of your technical questions about this agreement – and he said that he had had some sleep. So be somewhat gentle with him. After meeting with my chief national security advisers, and at their unanimous recommendation, I am instructing Ambassador Gallucci to return to Geneva on Friday for the purpose of signing an agreement.

The United States has been concerned about the possibility that North Korea has been developing nuclear weapons since the 1980s. Three administrations have tried to bring this nuclear program under international control. There is nothing more important to our security and to the world's stability than preventing the spread of nuclear weapons and ballistic missiles. The United States has an unshakable commitment to protect our ally and our fellow demurest – South Korea. A total of 38,000 American troops stationed on the peninsula are the guarantors of that commitment.

Today, after 16 months of intense and difficult negotiations with North Korea, we have completed an agreement that will make the United States, the Korean Peninsula, and the world safer. Under the agreement, North Korea has agreed to freeze its existing nuclear program and to accept internal inspection of all existing facilities.

This agreement represents the first step on the road to a nuclear-free Korean Peninsula. It does not rely on trust. Compliance will be certified by the International Atomic Energy Agency (IAEA). The United States and North Korea have also agreed to ease trade restrictions and to move toward establishing liaison offices in each others capital. These offices will ease North Korea's isolation.

From the start of the negotiations, we have consulted closely with South Korea, Japan, and other interested parties. We will continue to work closely with our allies and with the Congress as our relationship with North Korea develops.

Throughout this Administration, the fight against the spread of nuclear weapons has been among our most important international priorities, and we have made great progress toward removing nuclear weapons from Ukraine, Kazakhstan, and Belarus. Nuclear weapons in Russia are no longer targeted on our citizens. Today, all Americans should know that as a result of this achievement on Korea, our nation will be safer, and the future of our people more secure.

Now I will ask Ambassador Gallucci to come up, make a statement, and answer your questions. Robert Gallucci.

I would like to make a few comments about the agreement itself. The President put it in a broader strategic context of our national interests in non-proliferation and regional security. I want to say a word or two about the substance of the agreement and then try to answer your questions.

The agreement addresses concerns we have had about the North Korean nuclear program with respect to past activities, current activities, and future activities. The question of what North Korea did in the past – how much plutonium it separated – is the issue that arose between the IAEA doing its inspections and DPRK finding that it would not accept what they called special inspections. That was brought to the Security Council, and that resulted in a number of Security Council presidential statements and resolutions.

The question of what North Korea did in the past can be resolved by the IAEA only if the IAEA has access to the information in sites it needs. Under the terms of the agreement, that access will be provided. The DPRK will agree to the implementation of its full-scope safeguards agreement and

whatever is required by the IAEA – whatever the IAEA deems necessary to resolve the questions of the past.

The implementation of that portion of the framework document takes place over a period of time. The implementation must be completed before significant nuclear components of the first nuclear reactor that would be constructed in North Korea are delivered.

The agreement envisions the provision of two light–water reactors – and the first point I am making is that in the course of the delivery of component for that reactor, before any nuclear components are delivered, the question of past nuclear activities and the full compliance of North Korea with its IAEA safeguards obligations will be taken care of – will be addressed. That is the question of the past. With respect to the present, North Korea has an operating, small, five–megawatt reactor that produced the plutonium – however much plutonium they now have – produced the spent fuel that is now in the storage pond which contains 25 to 30 kilograms of plutonium. North Korea has also a reprocessing facility that they have expanded in capacity. These are the most significant components of the current nuclear program. Under the terms of the agreement, the current nuclear program is frozen. That means that the five–megawatt reactor will not restart. That means that the reprocessing facility will be sealed and will not be operated again. That means that the fuel that is in the pond will stay in the pond. All of these provision will be monitored by the International Atomic Energy Agency, as the President said. That addresses the current problems of both further separation of plutonium from spent fuel and further production of plutonium in a nuclear reactor.

With respect to the future, the North Korean nuclear program includes two large gas graphite reactors. One rated at 50 megawatts electric; the other at 200 megawatts electric. If these reactors were to be completed, they would produce hundreds of kilogram of plutonium a year.

The spent fuel, as I said, that is in the pond – if that were to be reprocessed – would right away be a source of plutonium for four or five nuclear weapons. This is the future problem that we are seeking to address, and under the agreement, the facilities that are under construction would be frozen. Under the agreement, all the facilities the ones under construction and the ones currently existing in North Korea – would be dismantled over the course of the construction of the light–water reactor project.

The spent fuel that is in the pond not only will not be reprocessed, according to the terms of the framework document, but the North Koreans will agree to cooperate in the shipment of that spent fuel out of North Korea so that there is no source of plutonium in North Korea. This is the way we propose to address our concerns, as I said – grouping them into past, present, and future.

The agreement, of course, provides that the North Koreans receive assistance from the international community in achieving legitimate energy objectives. A light–water reactor project roughly on the order of 2,000 megawatts or two 1,000–megawatt light–water reactors will be provided over a period of years. We would hope in the near term to move to a contract phase and then for construction to begin.

As I think you know, the United States has been consulting with a number of governments about the financing of this project. We envision the Republic of Korea and Japan playing essential roles in the financing and construction of that facility.

In addition to the light–water reactor project, the framework document provides that the energy needs of North Korea that arise from the freezing and ultimate dismantlement of the nuclear reactors that would have produced energy – that those energy needs be addressed by the international community. Again, the United States will take the lead in supplying heavy oil over the

next 10 years, or that period of time between now and when the light–water reactors might be expected to come on line. So we will, with other countries, attempt to meet the North Korean energy needs that they forego – energy that they forego as a result of the freezing of the reactor either extant or under construction In addition, the framework document provides for what we call negative security assurance, assuring that the United States, with respect to a party – North Korea – to the Non Proliferation Treaty will not, in essence, suffer the threat or use of nuclear weapons.

At this point I will stop. I will say with respect to the status of the agreement again, so you will understand we are in ad referendum posture with respect to the agreement. As the President said, I will return on Friday for the purpose of signing the agreement

---

*Bawahahahah!!! You ungrateful bastards deserve this.*

*I can only hope you start killing each other ... again!*

### **German Population Plunge Irreversible, Federal Stats Office Admits**

November 9, 2006 – From: [www.lifesite.net](http://www.lifesite.net)

By Gudrun Schultz

BERLIN, Germany, November 9, 2006 (LifeSiteNews.com) – Germany's downward spiral in population is no longer reversible, the country's federal statistics office said Tuesday. The birthrate has dropped so low that immigration numbers cannot compensate.

The fall in the population can no longer be stopped, vice–president Walter Rademacher with the Federal Statistics Office said, reported Agence France–Presse.

Germany has the lowest birthrate in Europe, with an average of 1.36 children per woman. Despite government incentives to encourage larger families, the population is dropping rapidly and that trend will continue, with an expected loss of as much as 12 million by 2050. That would mean about a 15 percent drop from the country's current population of 82.4 million, the German news source Deutsche Welle reported today.

The low birthrate will cause the German population to age dramatically over the next 40 years—last year there were 144,000 more deaths than births, and that number could increase to 600,000 by 2050, the FSO forecast stated.

With a 22 percent reduction in the workforce and increasing costs for senior assistance and medical care, the drop in population is expected to have a radical impact on the nations economy, along with the welfare budget.

I wouldn't like to use the word bankrupt because its a major challenge for the social insurance systems, thats for certain, Radermacher said in an interview with DW–Radio. But the first thing is to reform the social insurance systemsWe can learn from other countriesIn every case, you need someone who has to work and give you some earnings.

The projections tell us the development of demographic trends will be even more dramatic in the eastern part of Germany, Radermacher said. This is because of the fertility rates in the eastern part of Germany, because of internal migration with the borders of Germany and many other demographic factors.

While immigrants are increasingly relied upon to compensate for low birth rates in European countries, Radermacher said even factoring in a projected annual influx of 100,000–200,000 migrants won't prevent the population plunge.

Even those people who are immigrants adopt after a couple years the lifestyle and the number of children per family. So the assumption that immigrants will stick to their habits is simply not true.

**Germany has one of the largest populations of Muslim immigrants in Western Europe, with a Muslim community of over 3 million. That trend is expected to continue, leading some demographic trend-watchers to warn that the country is well on the way to becoming a Muslim state by 2050, Deutsche Welle reported.**

**The Brussels Journal reported last month that one third of all European children will be born to Muslim families by 2025. There are an estimated 50 million Muslims living in Europe today—that number is expected to double over the next twenty years.**

The population losses faced by Germany reflect a trend occurring across Europe—The European Unions statistics agency Eurostat has predicted an overall drop in Europe's population of 7 million people by 2050.

The demographic decline coincides with a dramatic drop in Christian religious belief and a consequent rejection of Christian morality and emphasis on the benefits of family life and children.

---

*Arrested for telling the truth ... in a school!*

### **Teacher Arrested, Accused Of Anti-Islam Tirade**

September 13, 2006 – From: [www.thedenverchannel.com](http://www.thedenverchannel.com)

GAITHERSBURG, Md. — A Maryland substitute teacher was arrested after an alleged anti-Islamic tirade in front of high school students.

Carol Joan McVey, 49, was charged with resisting arrest, trespassing, disorderly conduct and disturbing the peace.

Police said McVey became upset when she heard some students at Gaithersburg High School, who were being assisted by another teacher, practicing a speech and using some Arabic words.

The Washington Post said she reacted after overhearing the group utter an Islamic greeting of peace.

**Charging documents allege McVey shouted, "Islam doesn't mean peace, it means killing everyone for peace" and "Because of you, our families died in New York!"**

It's not known if anyone who heard the alleged remarks is Muslim.

Authorities said McVey went to the school office to express her displeasure about the speech and the assisting teacher and was told by the principal that her services were no longer needed at the school.

Police said she refused to leave and was escorted from the school by the educational facilities officer.

While being escorted from the building, McVey allegedly yelled at a Hispanic teacher about the inappropriateness of speaking to students in languages other than English.

Once the substitute teacher was outside, police said, she tried to re-enter the school and the school's educational facilities officer attempted to place her under arrest, but she resisted and an additional officer was called to assist.

Police said McVey was released on her own recognizance.

---

*No! This can't be true!*

### **Nigerian Leaders 'Stole' \$380bn**

October 20, 2006 – From: [news.bbc.co.uk](http://news.bbc.co.uk)

More than \$380bn has either been stolen or wasted by Nigerian governments since independence in 1960, the chief corruption fighter has said.

#### **Nuhu Ribadu told the BBC that Nigeria has "nothing much" to show for the missing money.**

He said the worst period for corruption was the 1980s and '90s, but currently two-thirds of governors are being investigated by Mr. Ribadu's agency.

Nigeria is Africa's biggest oil exporter but most people are poor.

The country is regularly ranked as one of the most corrupt by graft watchdog Transparency International.

President Olusegun Obasanjo declared a state of emergency in Ekiti State on Thursday after the governor was found guilty of siphoning state funds into personal bank accounts and receiving kickbacks.

#### Political Corruption

Mr. Ribadu said he had come up with his figure of \$380bn stolen or wasted since independence "easily" through records kept by the Nigerian central bank and the ministry of finance.

"Basically, this money has gone to waste, nothing much to show for it," he told the BBC's Network Africa programme.

"Of course, probably part of it will have gone to outside stealing."

Mr. Obasanjo's critics say the fight against corruption is being used to victimise his opponents ahead of next year's elections.

Mr. Obasanjo is not standing after an attempt to let him seek a third term was defeated.

But Mr. Ribadu denied he has a political motive in his fight against corruption.

"When you are doing this kind of work, you will always be accused of one thing or another."

Last month, Vice-President Atiku Abubakar was indicted on charges of corruption, which could stop him from running for office.

He denies allegations he diverted \$125m into personal business interests.

Mr. Ribadu has led Nigeria's battle against corruption as chairman of the Economic and Financial Crimes Commission (EFCC).

The EFCC says in the past two years it has recovered more than \$5bn and has successfully prosecuted 82 people.

### Money Laundering

Mr. Ribadu told the BBC that \$140m had been recovered from one unnamed former Nigerian leader and that nearly \$400m of illegally gained assets had been identified in the possession of a former governor of Bayelsa State.

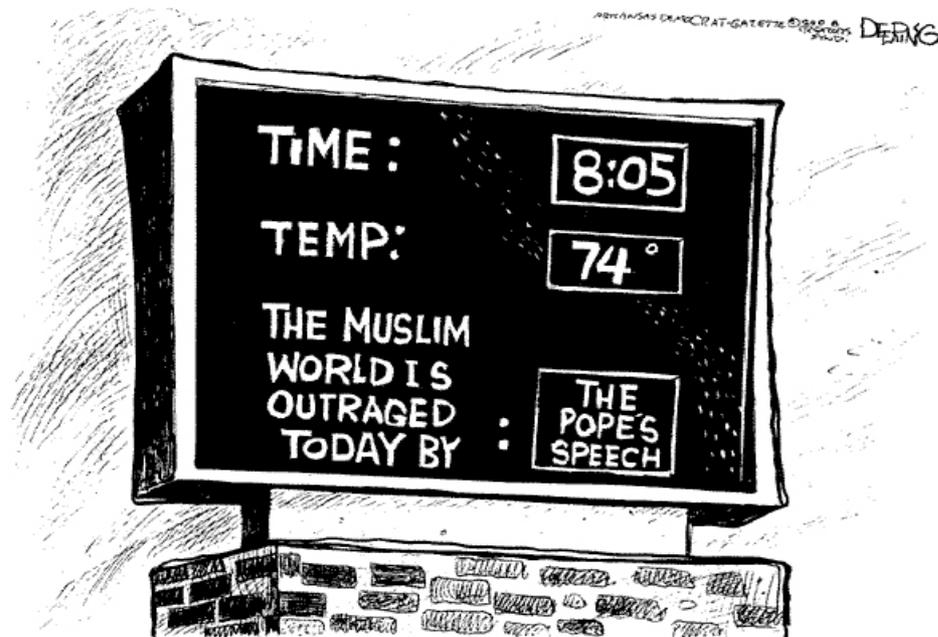
Last year, Nigeria recovered \$458m found in Swiss bank accounts linked to the country's late military ruler Sani Abacha.

Mr. Abacha was in power from 1993 to 1998 and is thought to have embezzled billions of dollars.

Last year his son, Abba Sani Abacha, was charged with money laundering and fraud after being extradited to Switzerland.

Despite the missing money Nigeria has managed to pay off its multi-billion dollar debt to the Paris Club of major lenders, thanks to high oil prices.

About \$5bn is still owed to other lenders including the World Bank and the private sector.



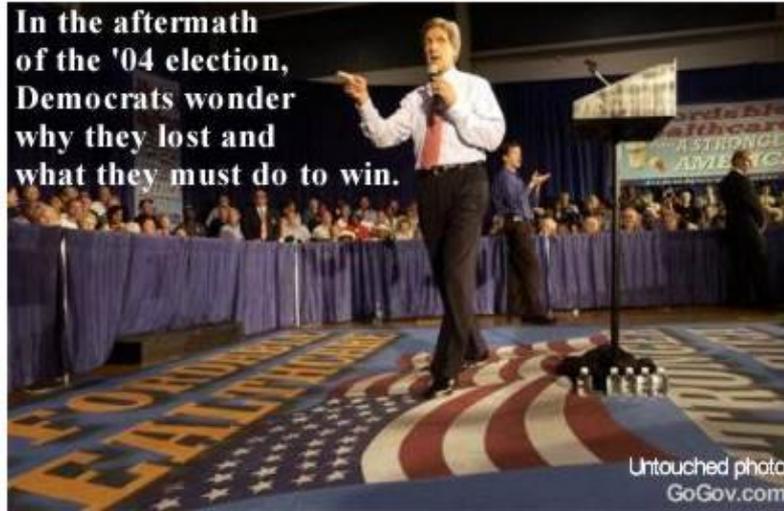


**What liberal bias?**

Debunking *Newsweek's* Article on Afghanistan:

<http://www.defenselink.mil/home/dodupdate/correct-record/documents/20061005.html>

In the aftermath of the '04 election, Democrats wonder why they lost and what they must do to win.



**It's not only what you do.  
It's what you must never do too!**

