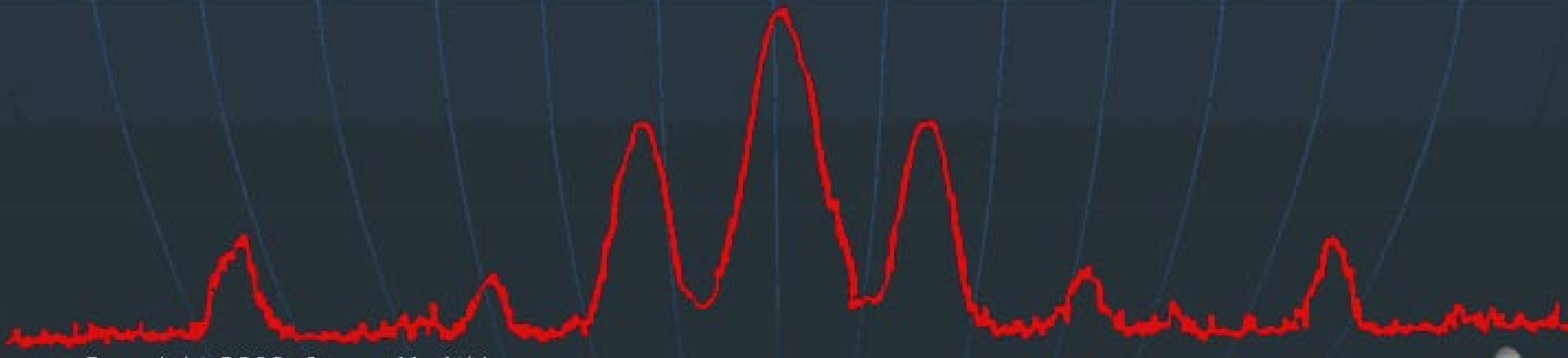
Phone Talk

Reston, VA - 2009

Be Afraid... Be Very Afraid...



The Bugs in Mr. Bell's Circuits

Telephone Bugging and Debugging

James M. Atkinson
Granite Island Group
www.tscm.com

Speaker Contact

James M. Atkinson
www.tscm.com

jmatk@tscm.com
(978) 546-3803

http://groups.google.com/group/TSCM-L2006

www.linkedin.com/in/jamesmatkinson

The Elegant Instrument

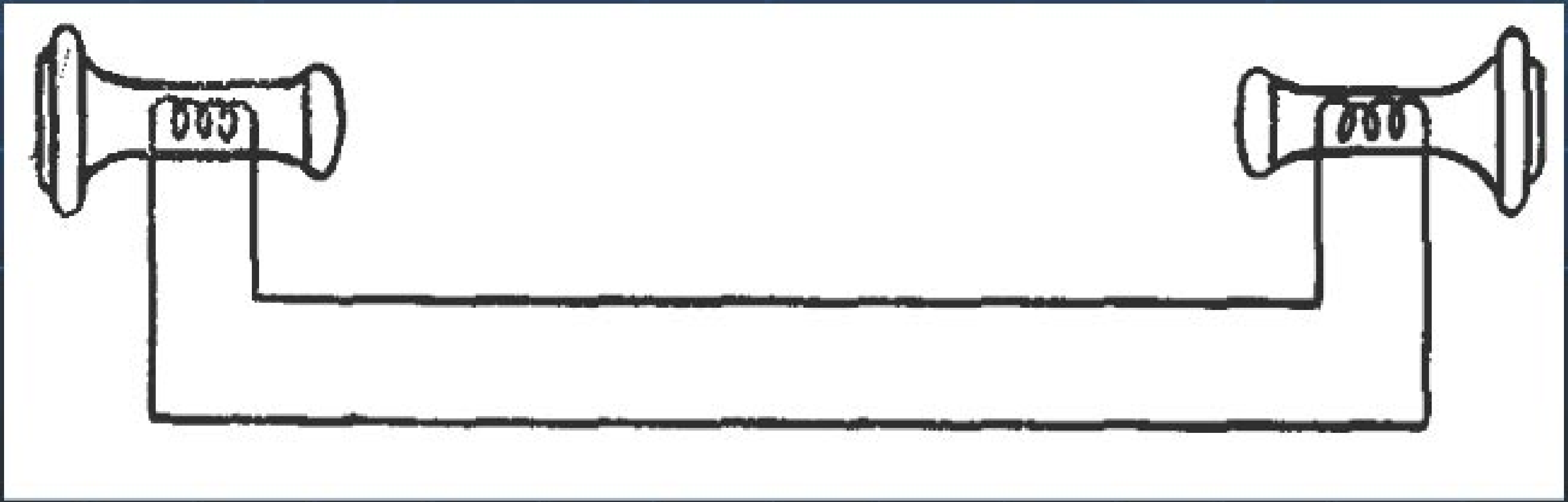
- The telephone instrument is one of the most elegant, and carefully designed of all electronic devices on Earth.

- They are also one of the easiest things to turn into bugs.

Telephone Vulnerability Points

Overly Simplified Telephone Circuit

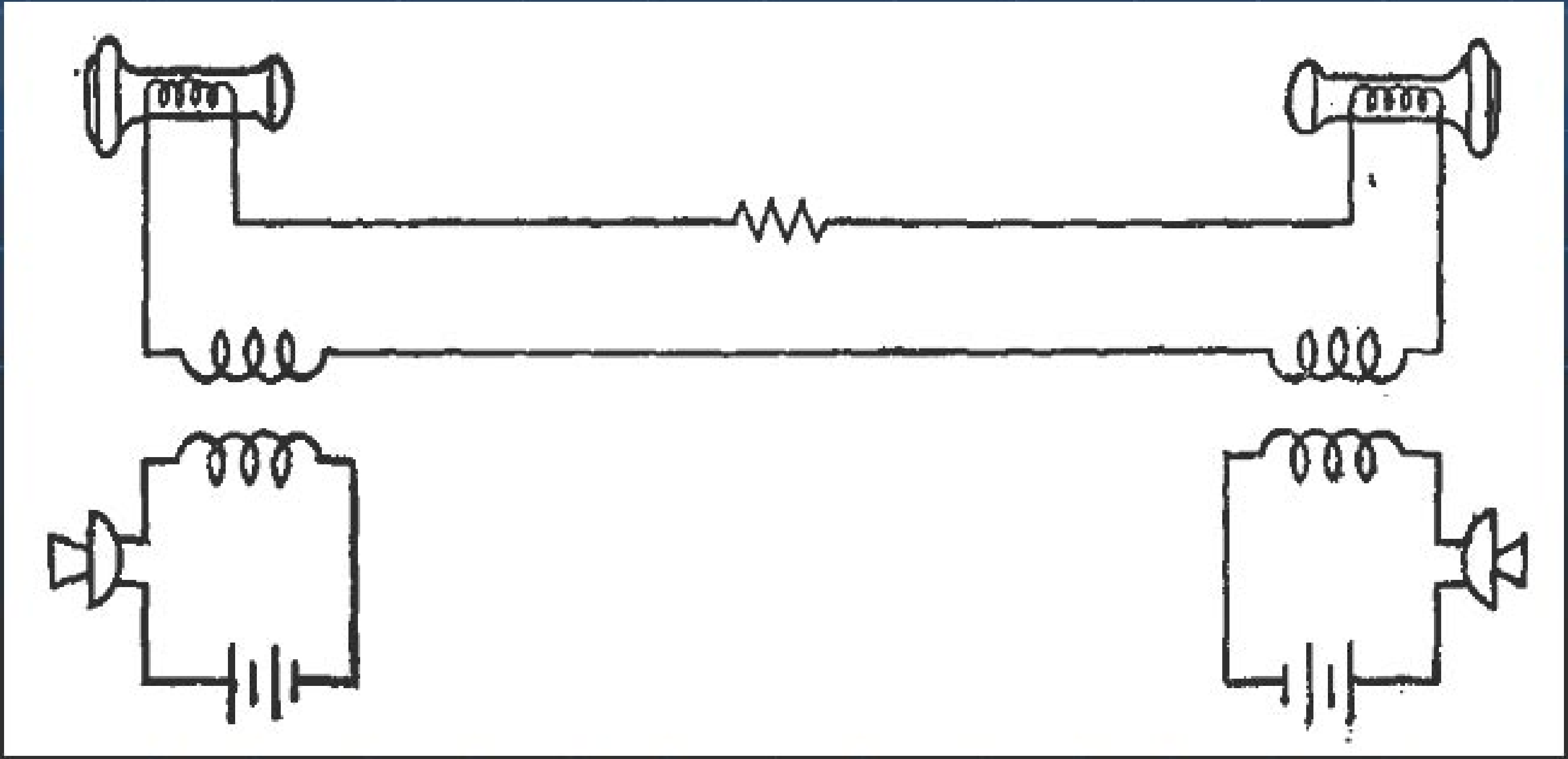
(No Battery Circuit – 2 transducers/inductors)



Telephone Vulnerability Points

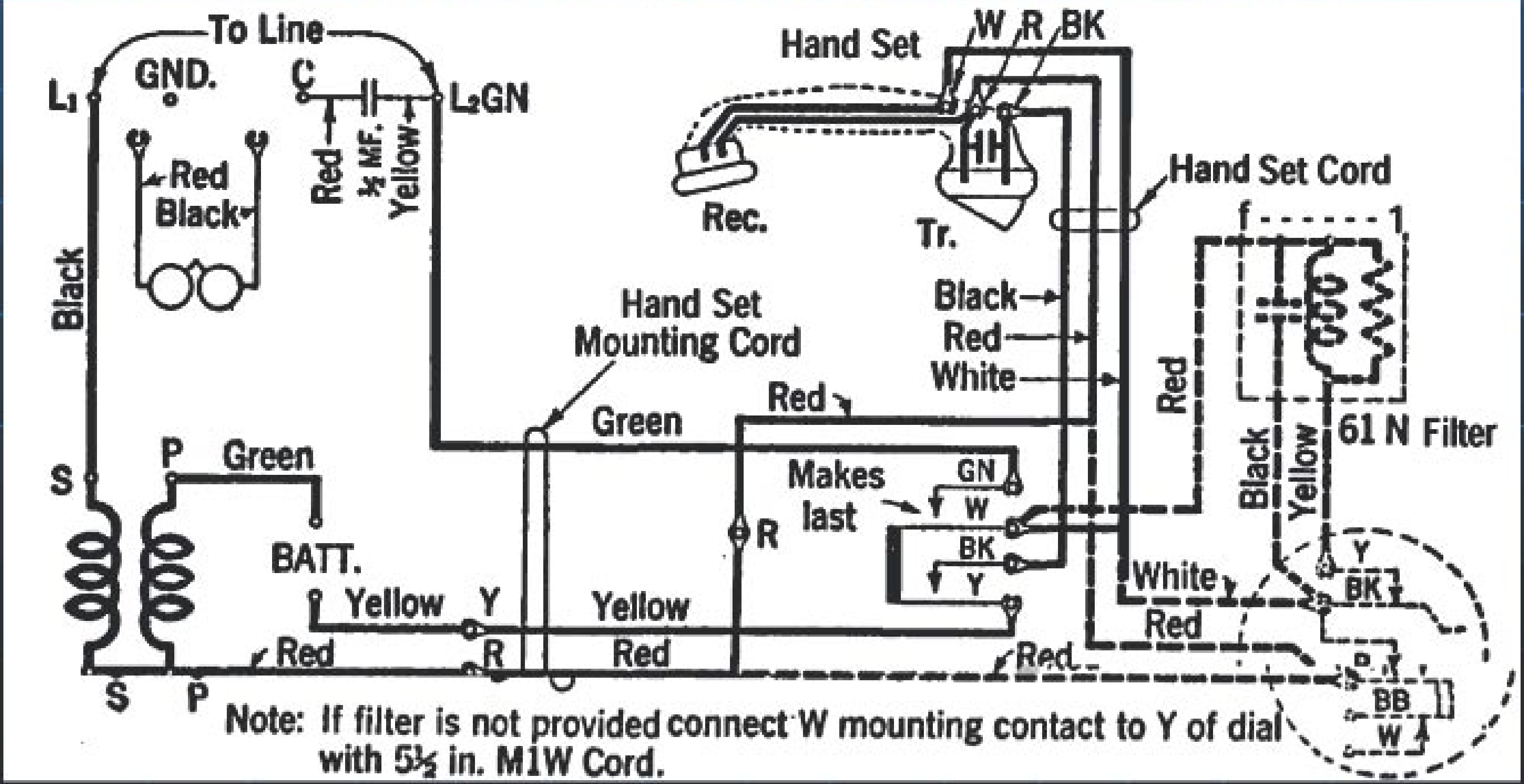
Less Simplified Telephone Circuit

(Local Battery Circuit – 4 transducers, 6 inductors)



Telephone Vulnerability Points

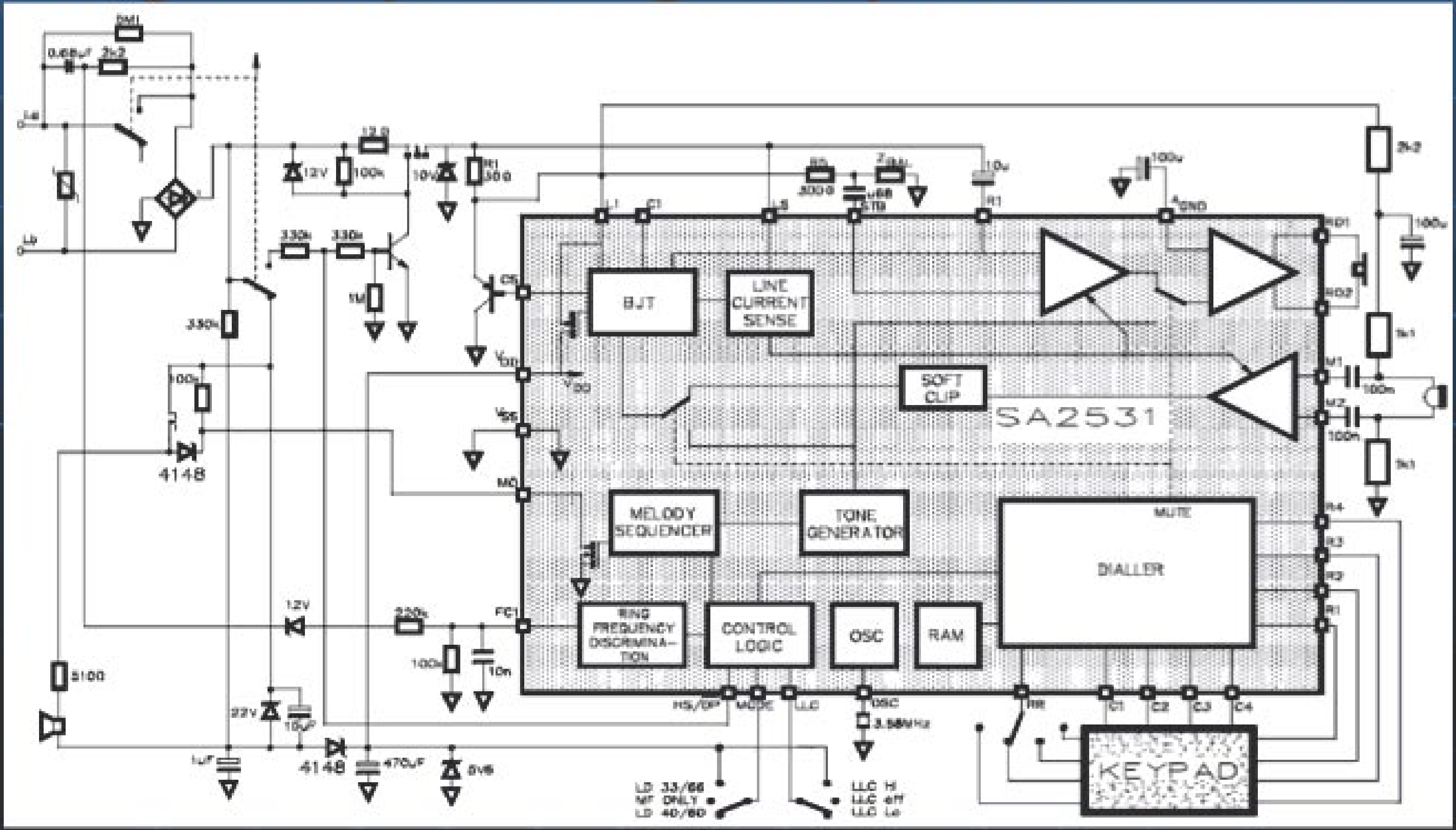
Old WECO Analog Telephone Circuit



Note: If filter is not provided connect W mounting contact to Y of dial with 5½ in. M1W Cord.

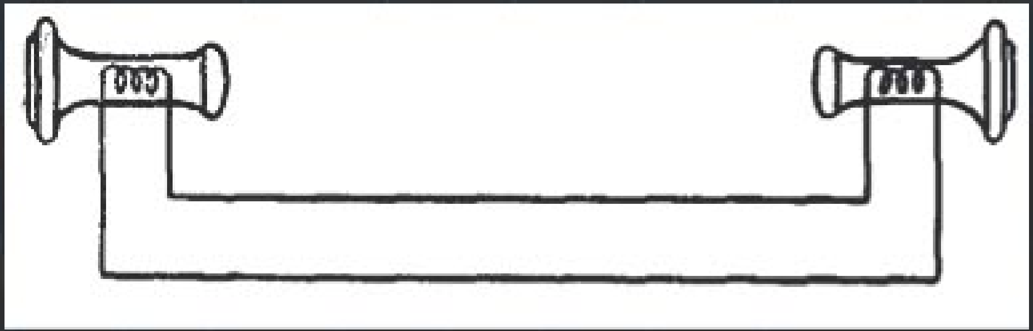
Telephone Vulnerability Points

Single Chip Analog Telephone Circuit



Telephone Vulnerability Points

1. Instrument
2. Local Distribution/In-House Wiring
3. Local Switch/PBX
4. Demarcation/Network Interface
5. Transmission
6. Switching Systems



Average Business Instrument

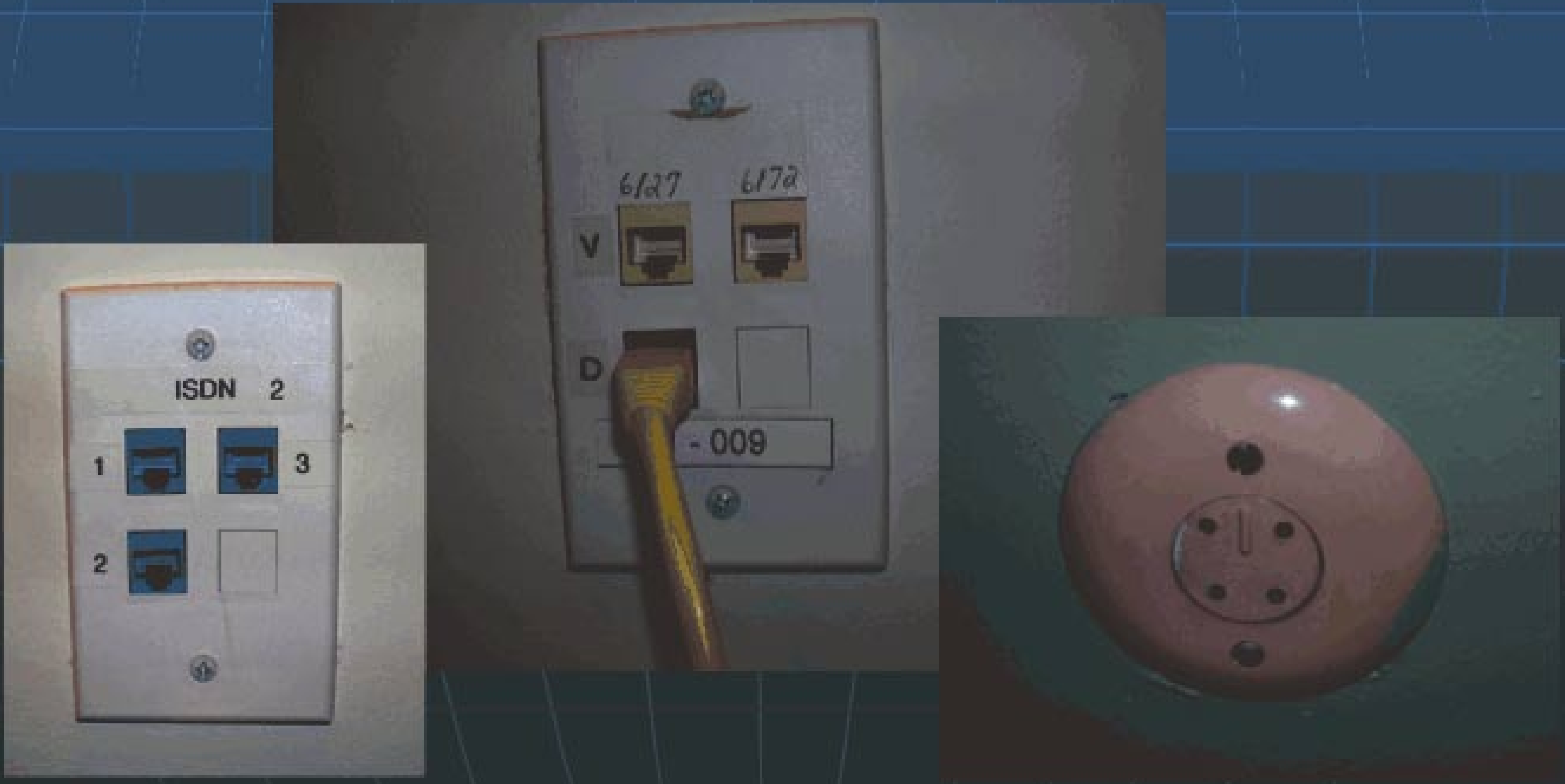
A Spies Best Friend

Wall Jacks

Most people do not understand what goes on behind this jack

New vs Old

(8-48 vs 2-4 conductors)

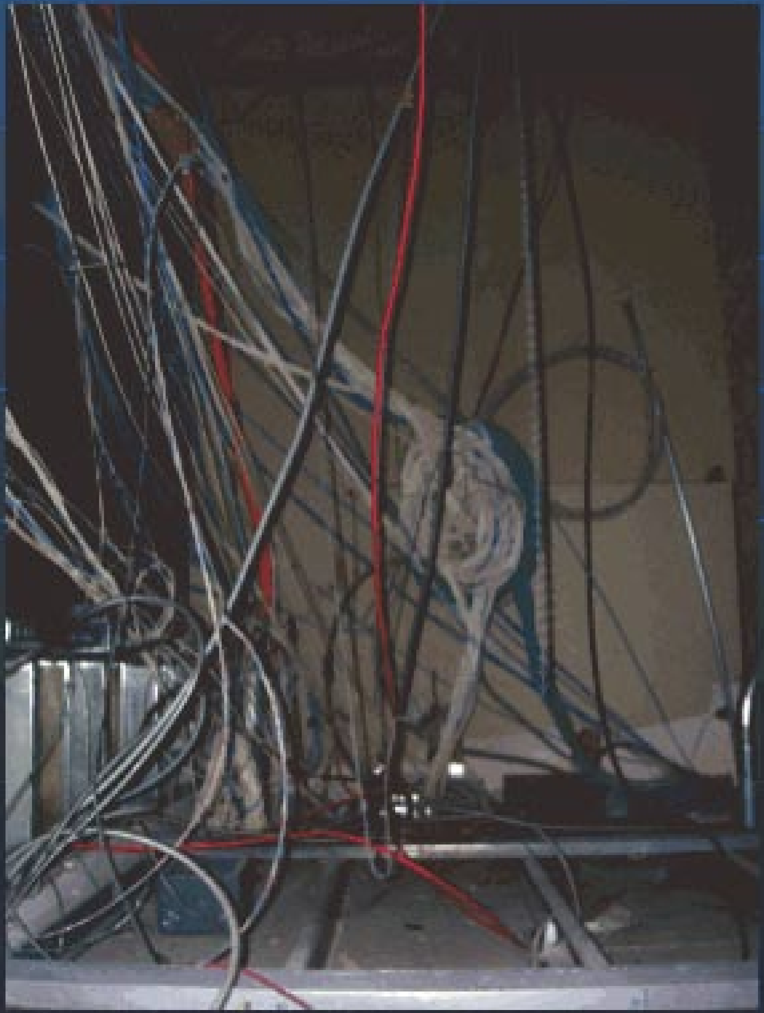


Typical Wiring Chaos

Defense Facility

1. Above Drop Ceiling
2. Mad Jumble
3. No Documentation
4. Wire Pwnage
5. Common Problem
6. Audio Recorder

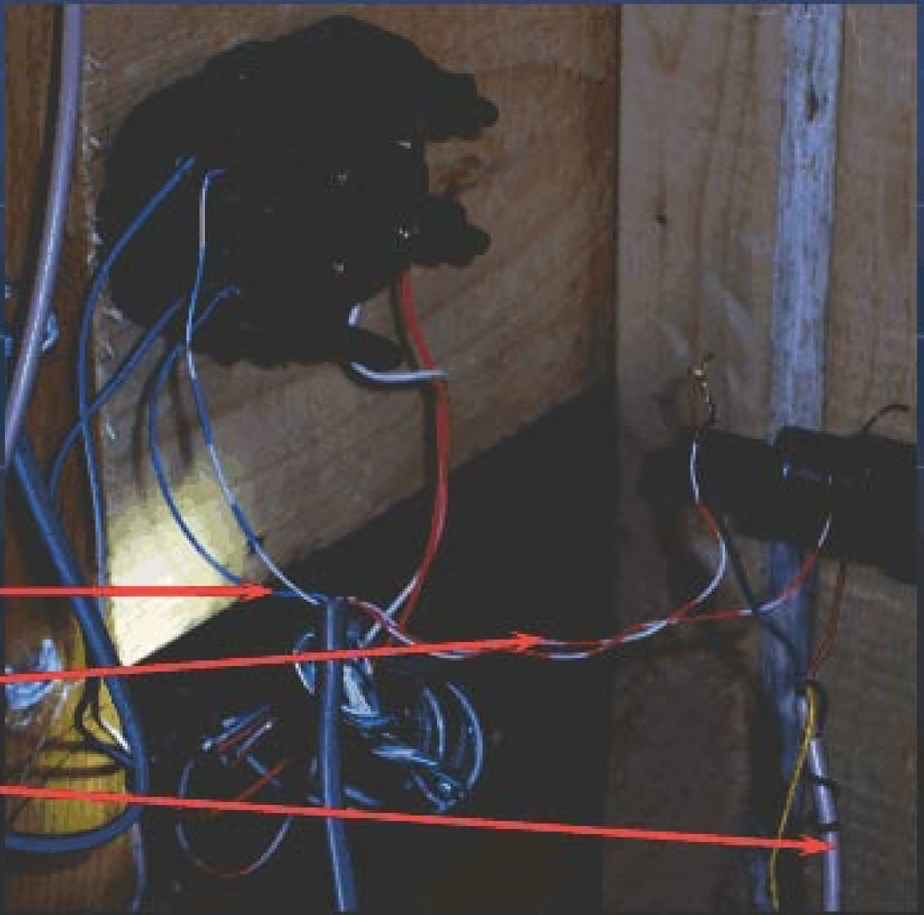
   Can You See it?



Amateur Wiretapping?

Twisted Connections

1. 2nd Pair Exploit
2. Microphone
3. Patch Cable
4. Tape Recorder
5. RS Job
   - BL-WH - OK
   - OR-WH – Bad
   - Grey – to SPY



Amateur Wiretapping?

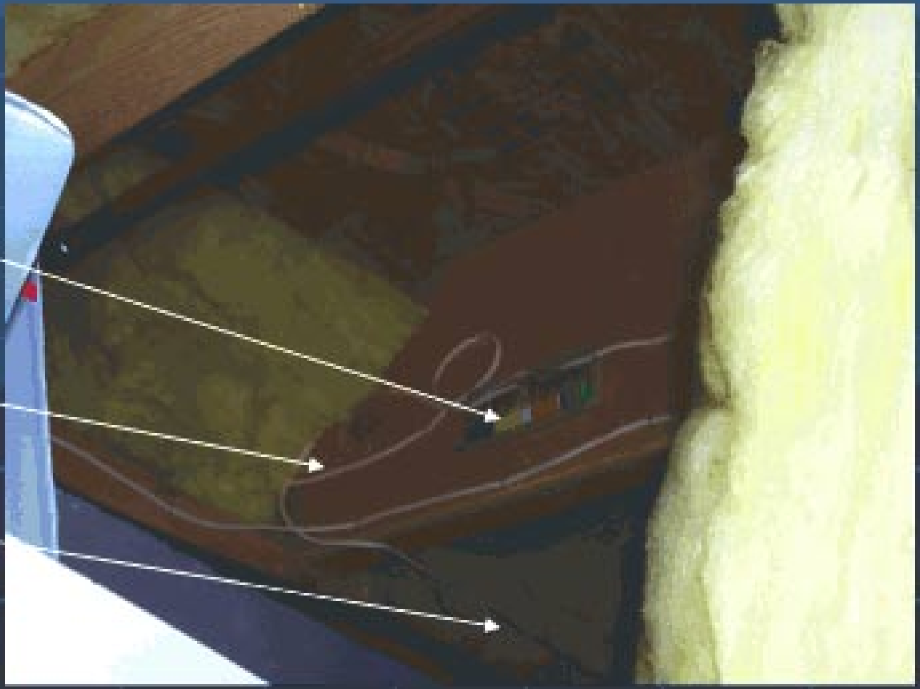
Junction Block

Patch Cable

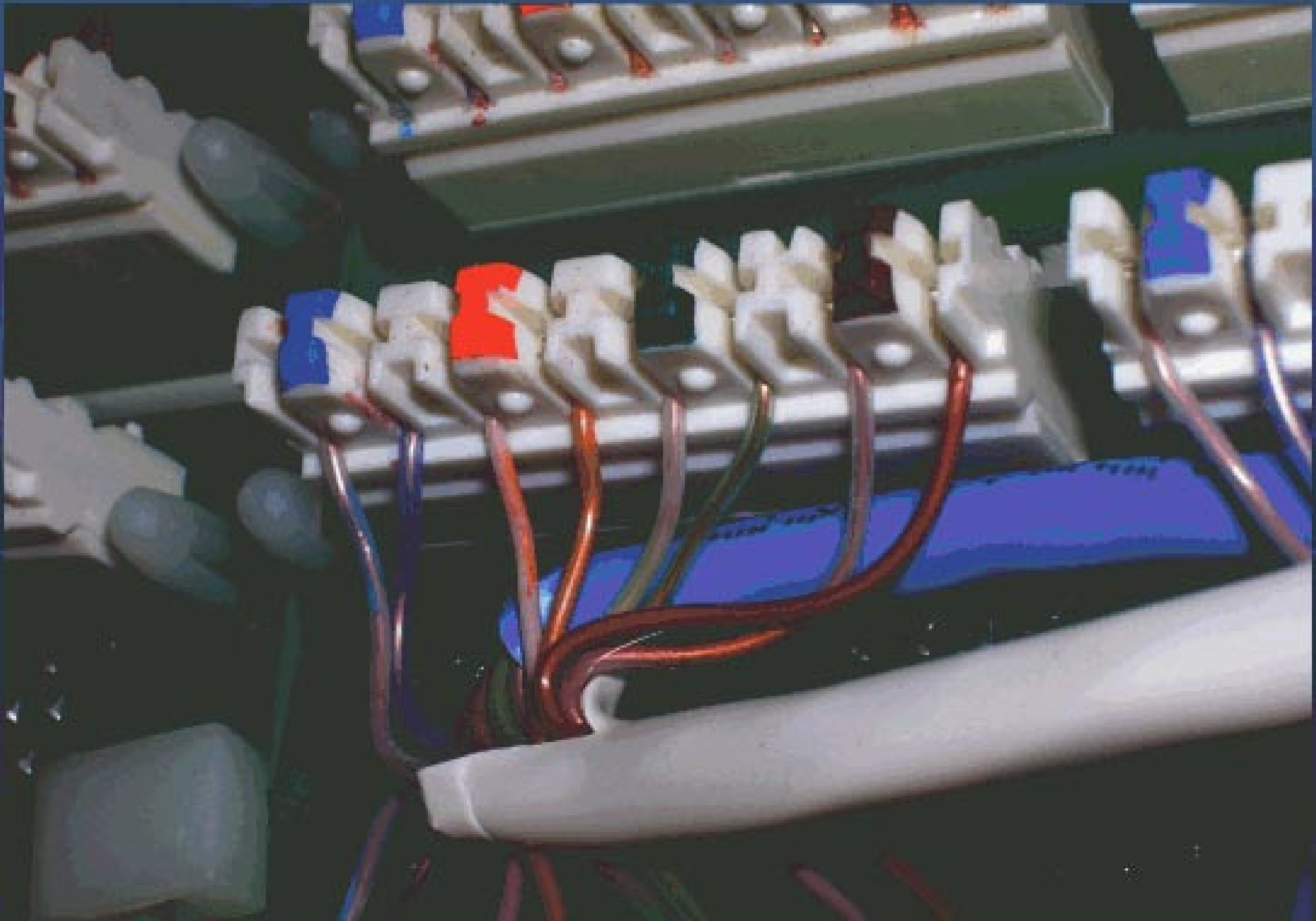
To Tape Recorder

All Radio Shack Parts

Hidden Under
Fiberglass Insulation



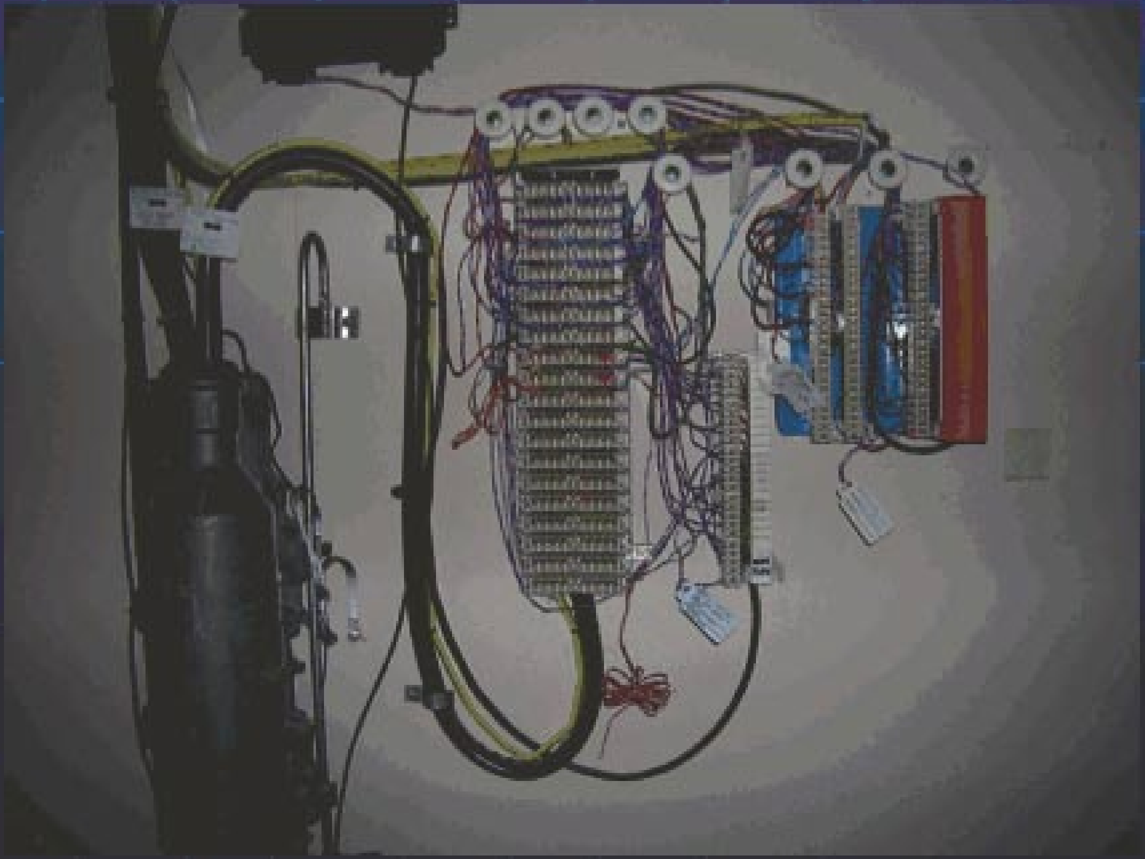
In-House Wiring Panels



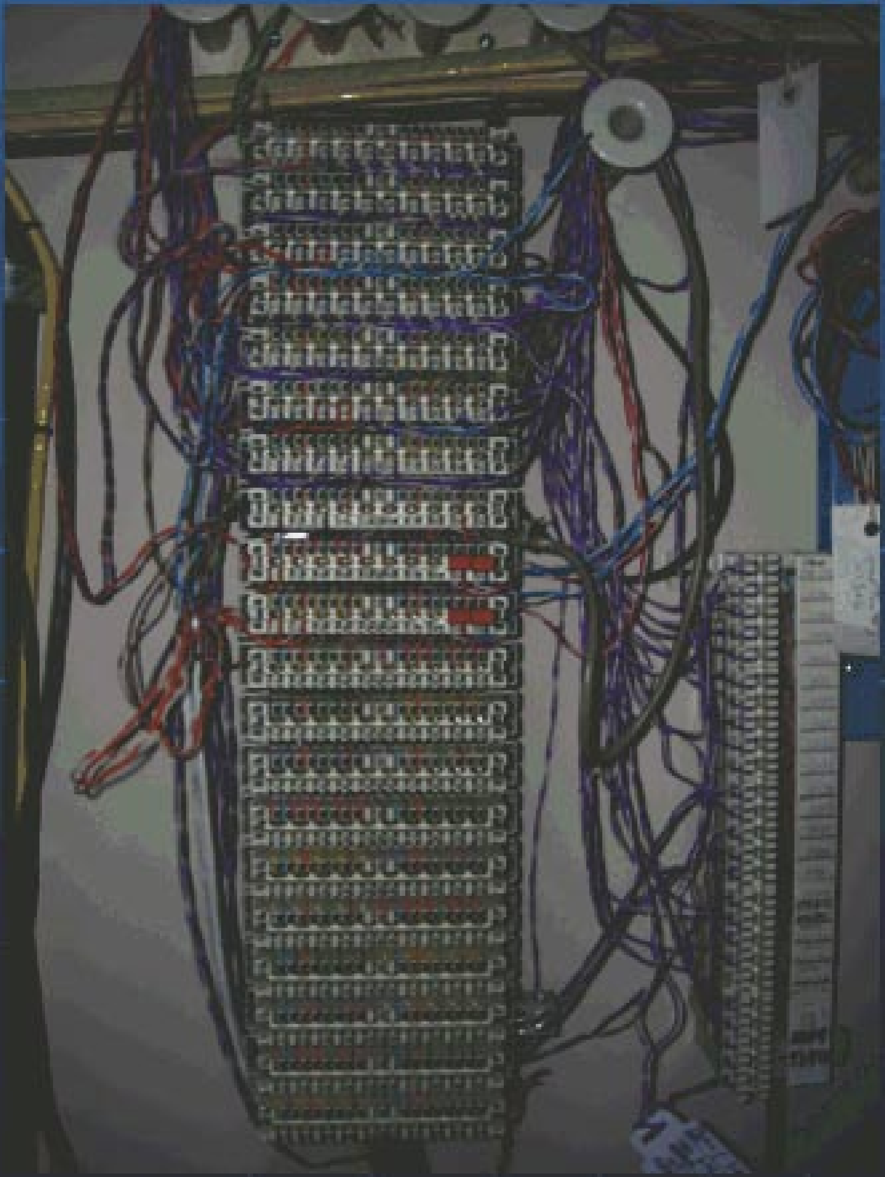
Common Phone Closet

Typical Defense Contractor Site

- Extra Wires?
- Transmitters?
- Recorders?
- Bridges?
- Taps?
- Slaves?



Closer Look

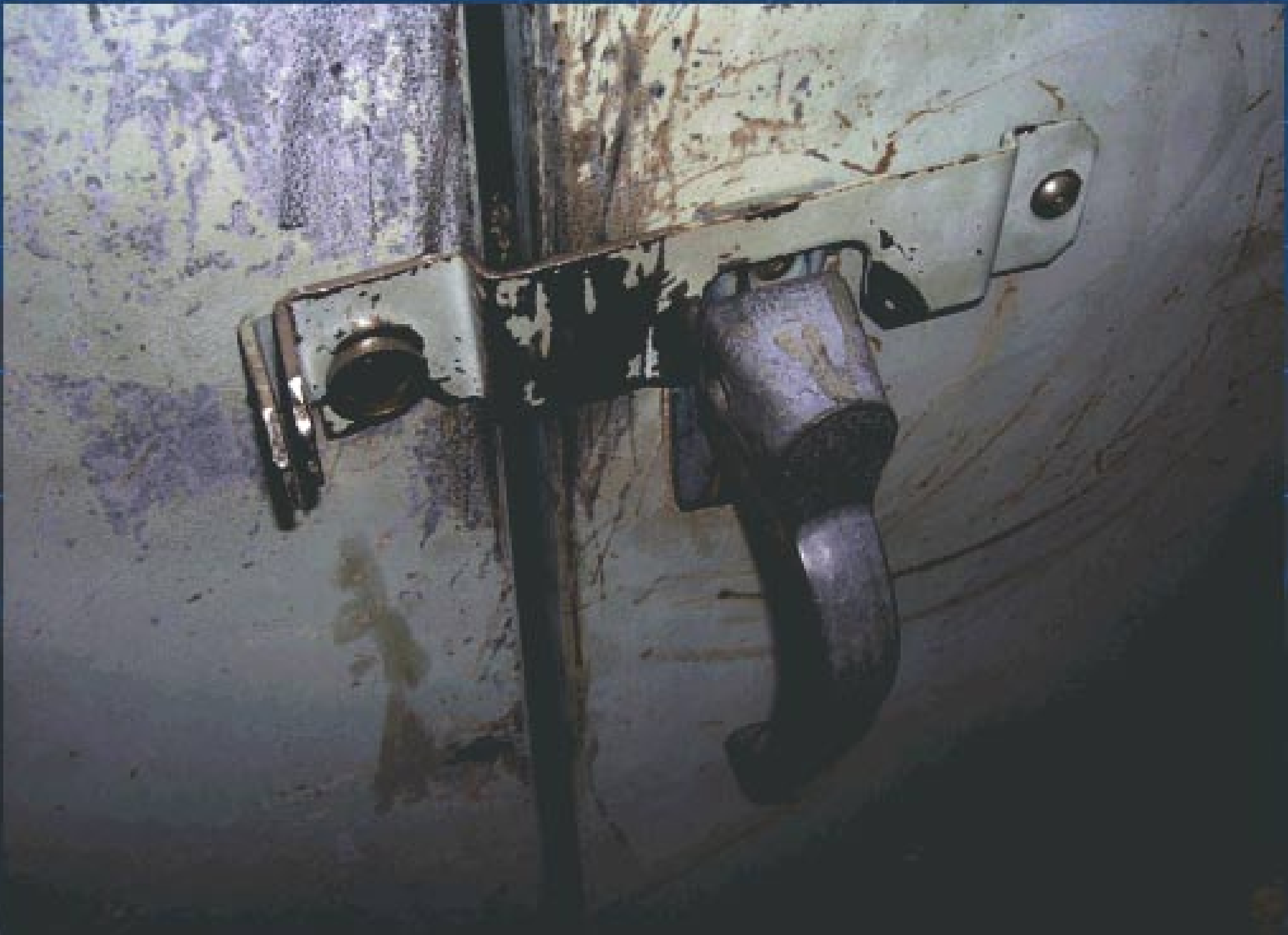


1. Things are not at all as they should be.
2. Can you see the issue?
3. Only an extensive technical audit will find what is there, if anything.

Hint:
Left Side of 110, 9th Row, 3rd pair
Silver Box Behind 110, Gray Cable

This Leads to Mischief

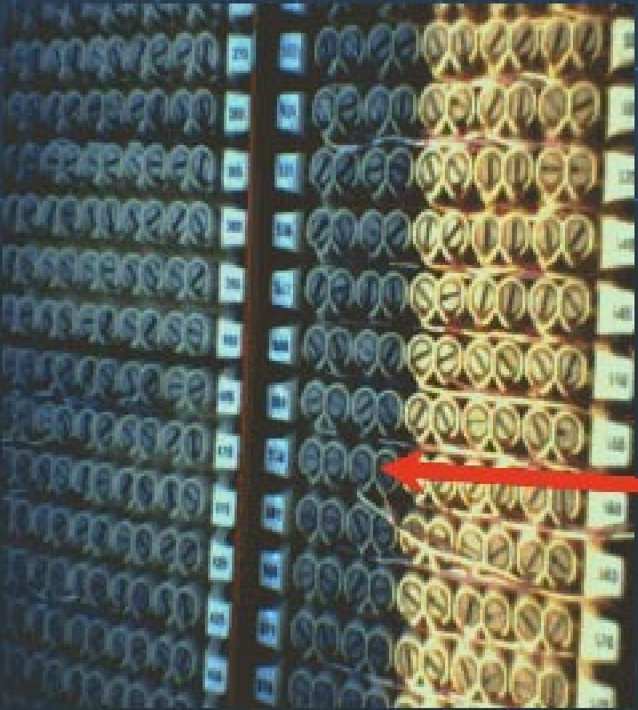
Where is the Lock?



(in)Secure Cross Connection

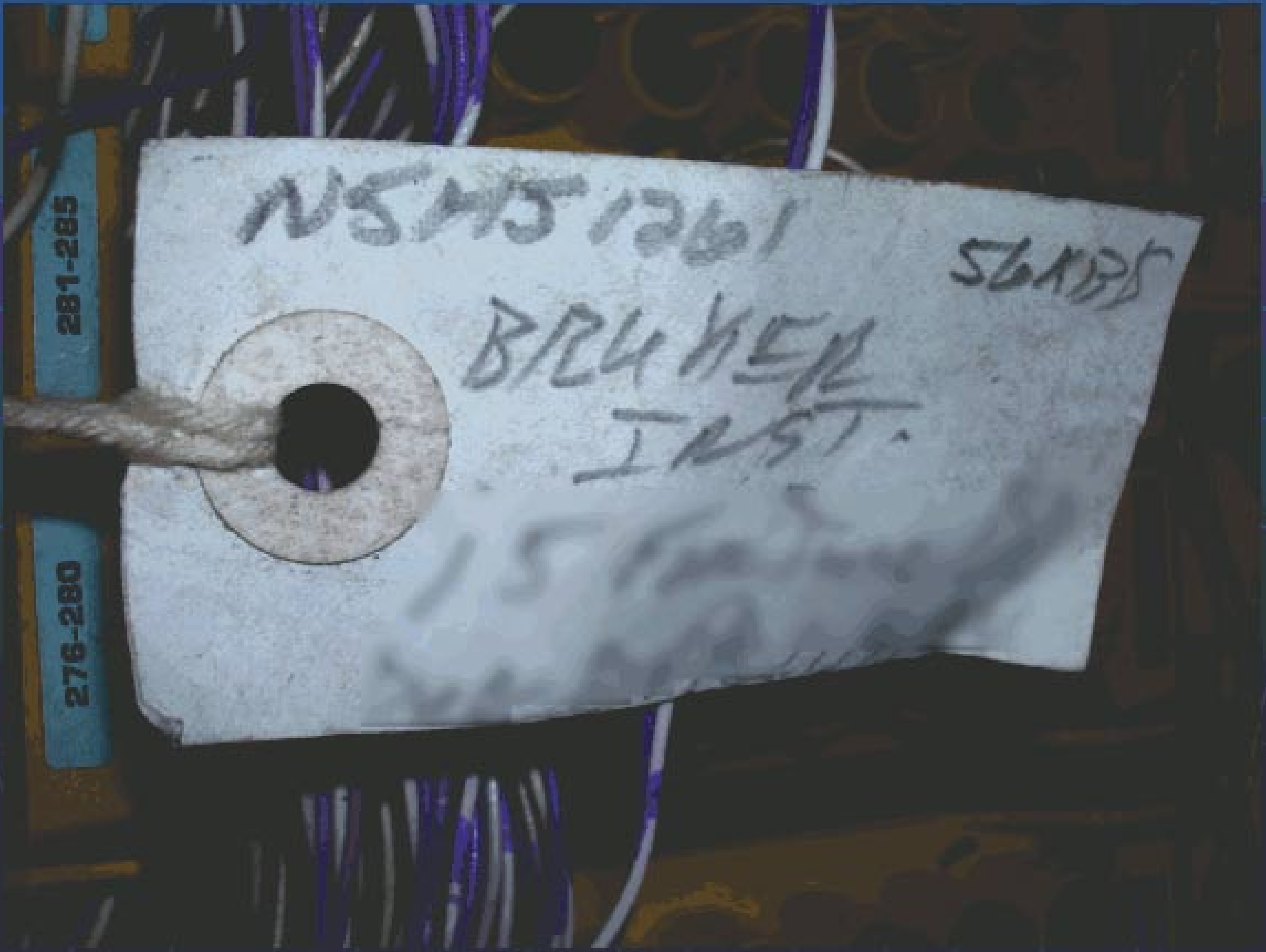
- Rarely Locked
- Cables Often Labeled
- Pairs Often Labeled
- Lots of Extra Space
- Remote from Target
- Easy Access
- Professional Target

Pair 557, Where Are You?

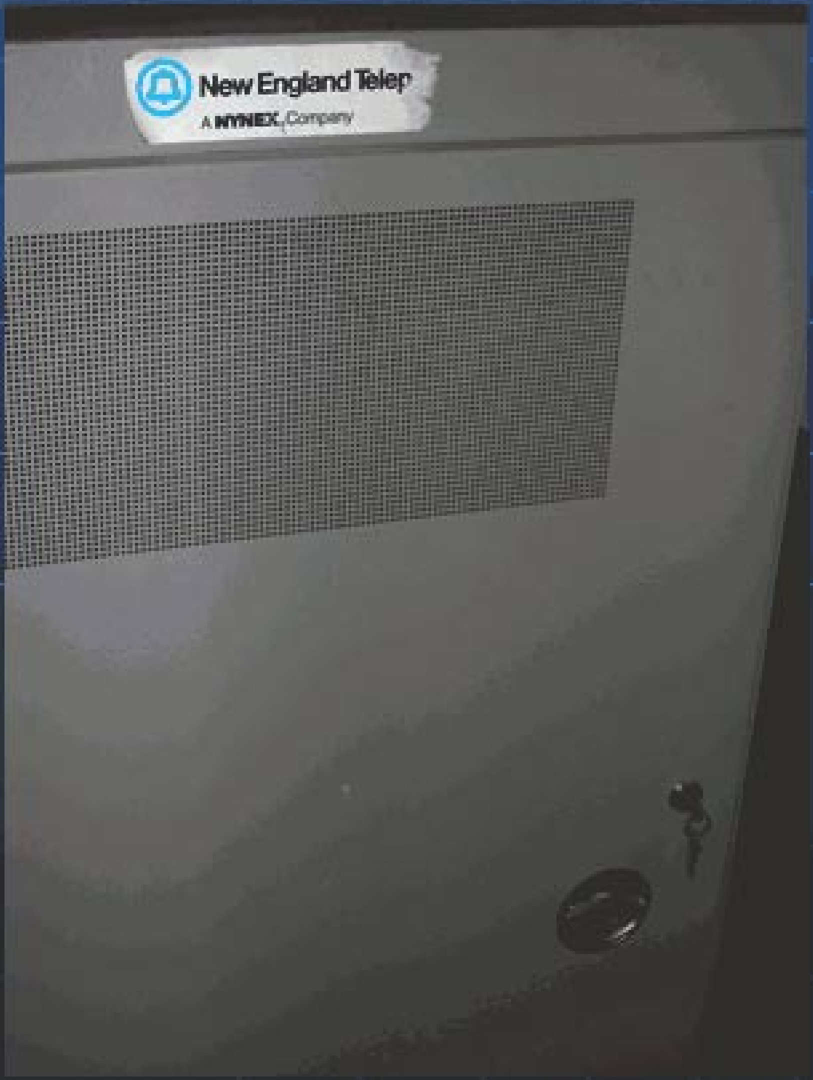


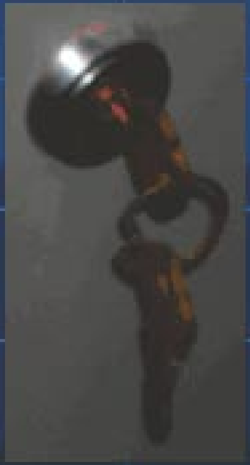
Tapped
Pair 557

Even Easier When Tagged



Better Yet is When They Leave the Keys in the Mux Cabinet Lock





Keys to the Kingdom
Equals Full Mux Access

More Keys To The Kingdom

- Nice that the phone company left the key to the mux on top the rack.

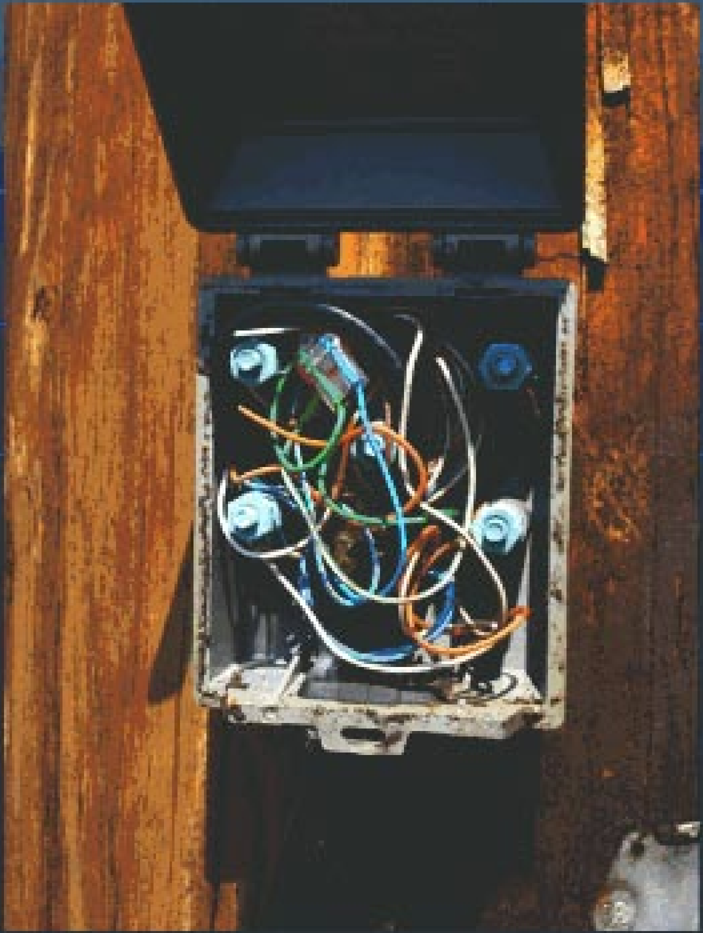
Fiber Optic Demarcation

- Fiber is Easy to Tap
- Higher Bandwidth
- More Intelligence
- Harder to Detect
- Illusion of Security

Fiber Optic Multiplexing

Local Transmission

- Terminal

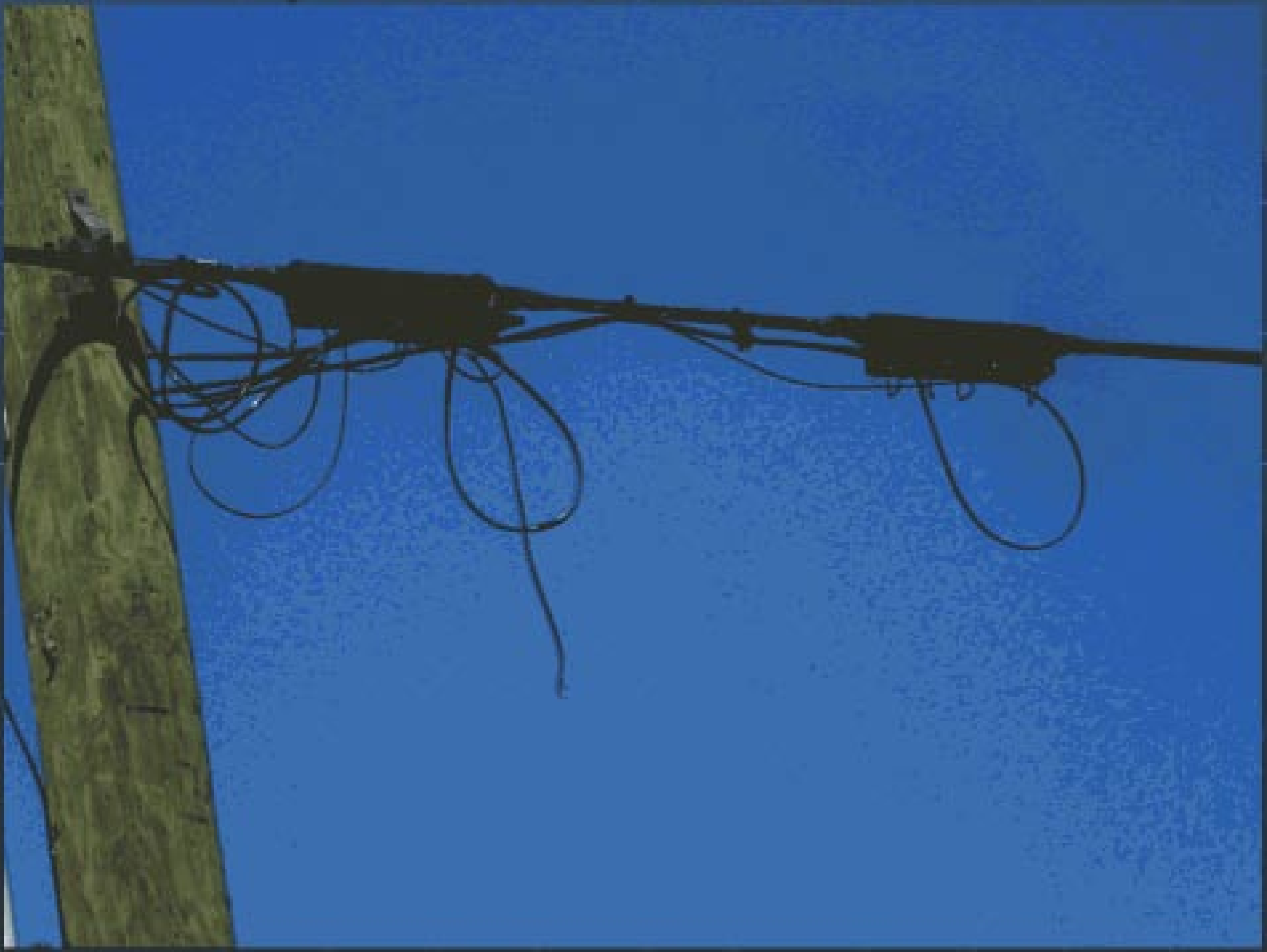


Local Transmission

- Pedestal

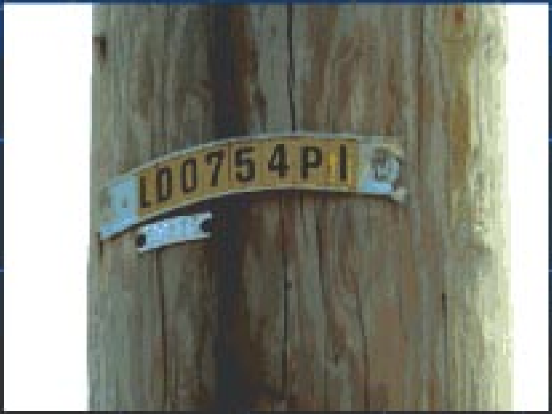
Local Transmission

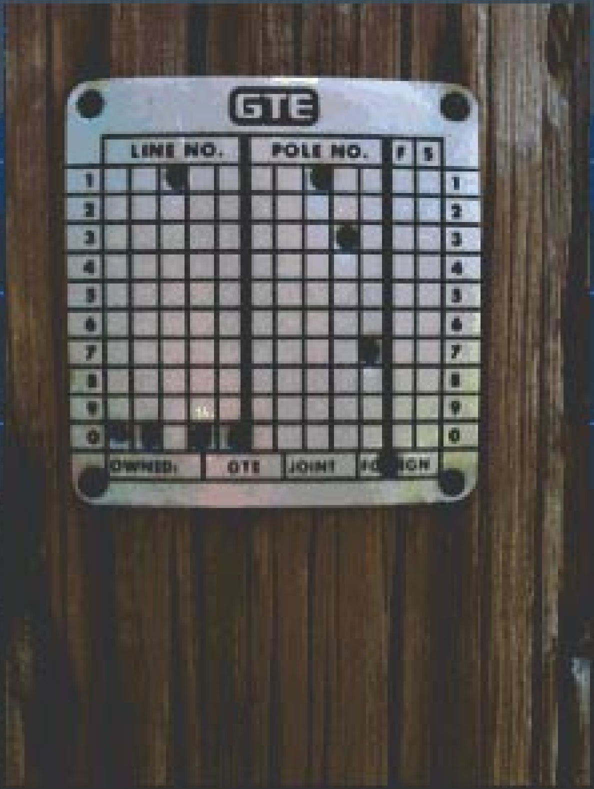
- Boot/Easy Access Point



Local Transmission

- Pole Walk

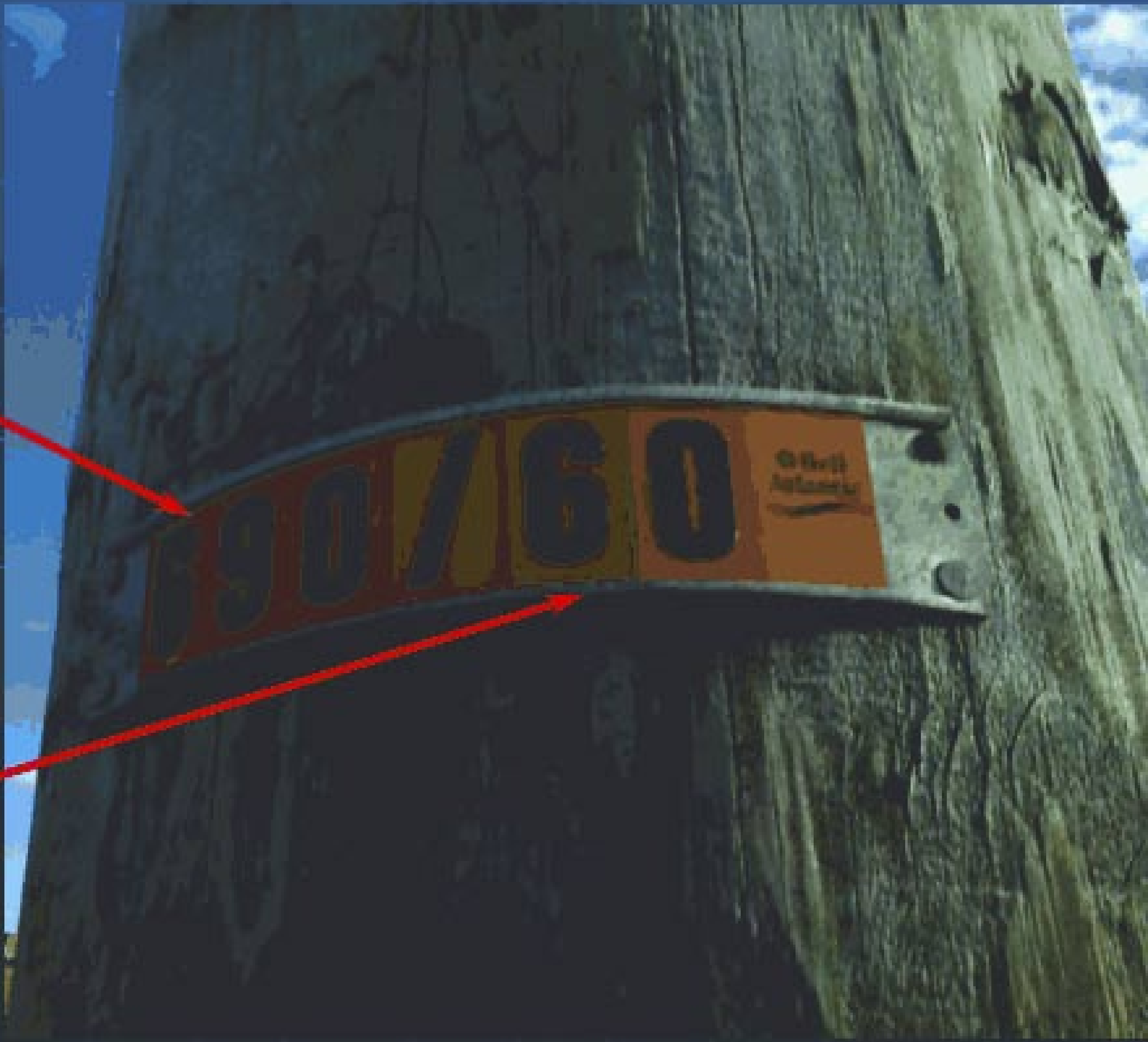




Local Transmission

Pole Address

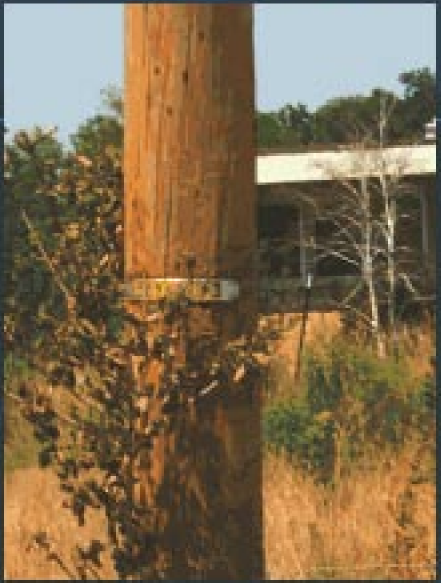
- Line Number
- Pole Number



Local Transmission

Pole Inventory
Line # 754

- Pole #1 – 173 ft down line
- Pole #2 – 461 ft down line
- Pole #3 – 759 ft down line



Local Transmission

Pole Inventory

Line # 754

- Pole #4 – 1045 ft down line
- Pole #5 – 1321 ft down line
- Pole #6 – 1610 ft down line
- Pole #7 – 1897 ft down line

- Continue for another 15,000 feet, or 50 poles to Central Office

Local Transmission

Pole Inventory

1. What Cables are Present
2. What Terminals or Boots Are Present
3. Service Cables Present?
    - Distance from Pole to Demark Point
4. Spoor?
5. Tool Marks?
6. Tape Recorders?
7. Document what you find

Local Transmission

Pole Inventory

- Lay Pole Inventory Findings onto 100:1 Civil Engineering Maps
- Use During Future TDR and FDR Studies
- Try to Use a Professional GIS Applications (ARC, X-Map, etc)

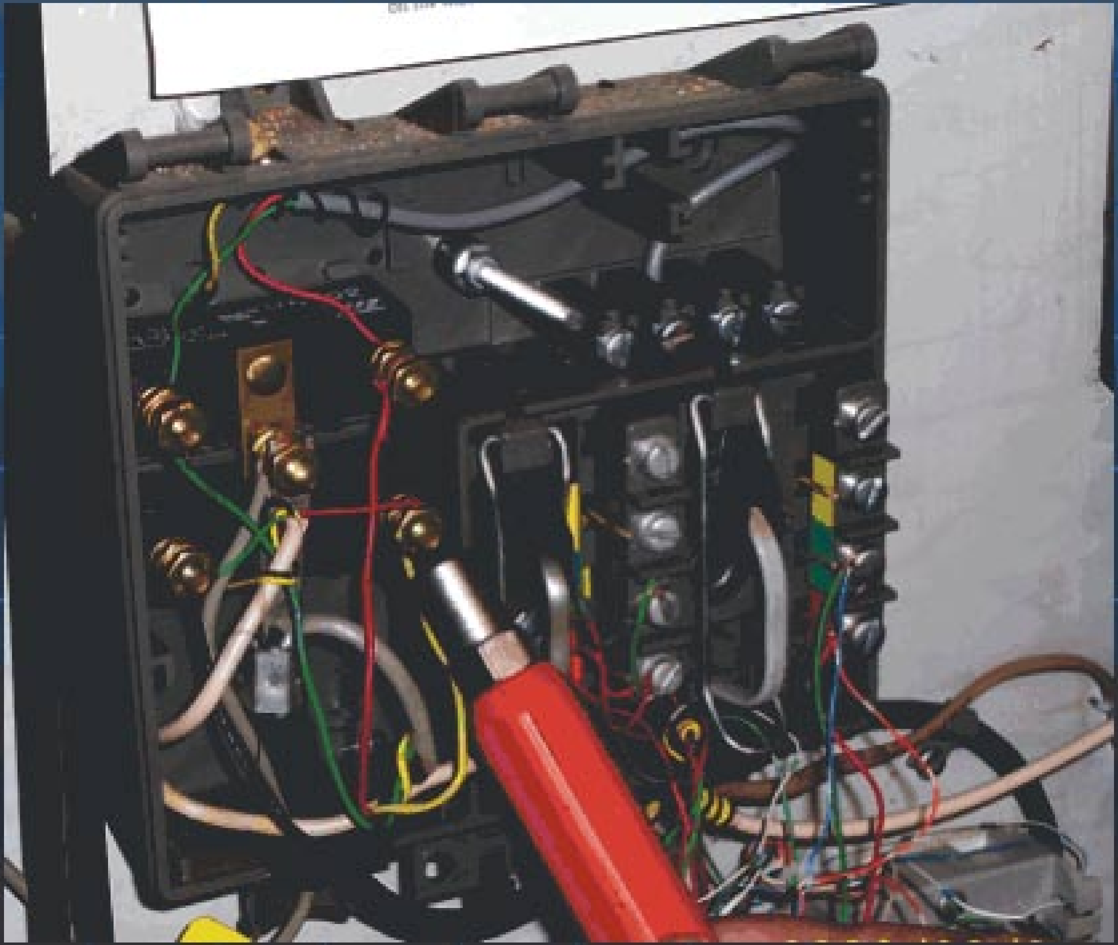
Demarcation or NID

- Looks Harmless, but it’s not…

Network Interface Risk

Common Place to Find a Spies Bugs and Wiretaps

What is Wrong Here?



Instrument

Vulnerabilities

1. Speaker or Microphone Exploit
2. Installation of Foreign Device
3. Hookswitch Manipulation
4. Software/Firmware Exploits
5. Normal Operation Exploits
6. Moderate Protection, Easy to Subvert

Cordless Phone

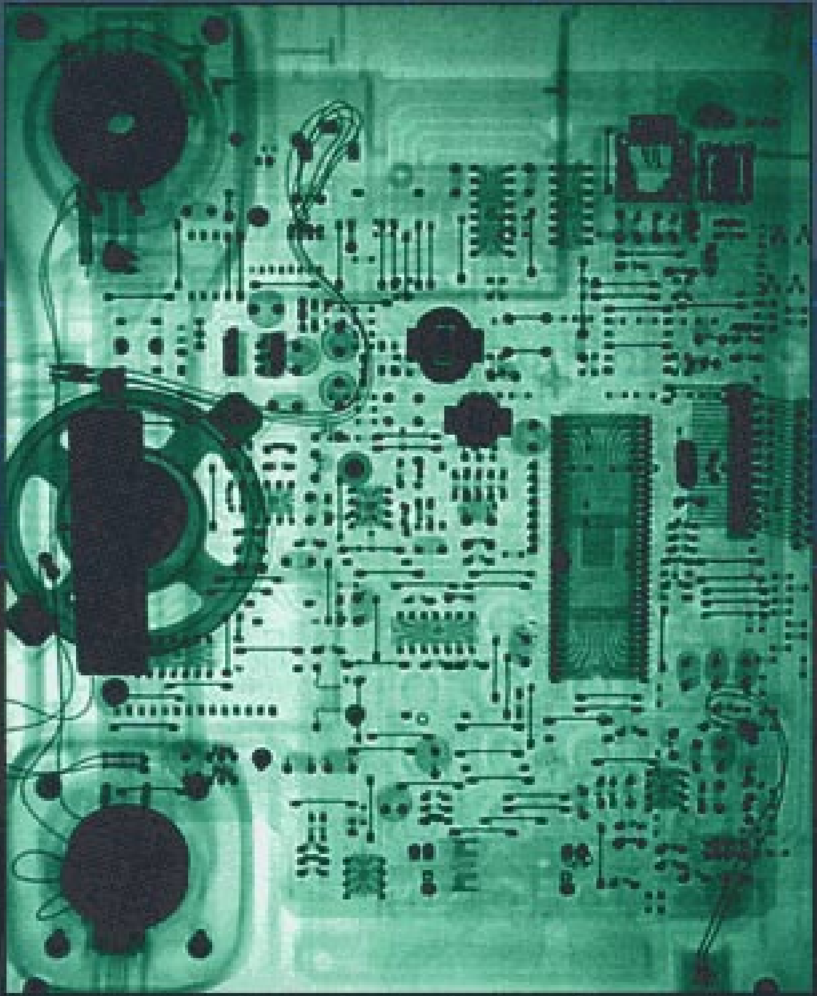
1. Costs Under $20
2. Zero Security
3. 4 Primary Bands
4. RS Scanners
5. Really Bad News
6. Self Bugging
7. Clueless User

Exploited Mitel Phone

- Capacitor Only
- Spare Pair
- Microphone Tap

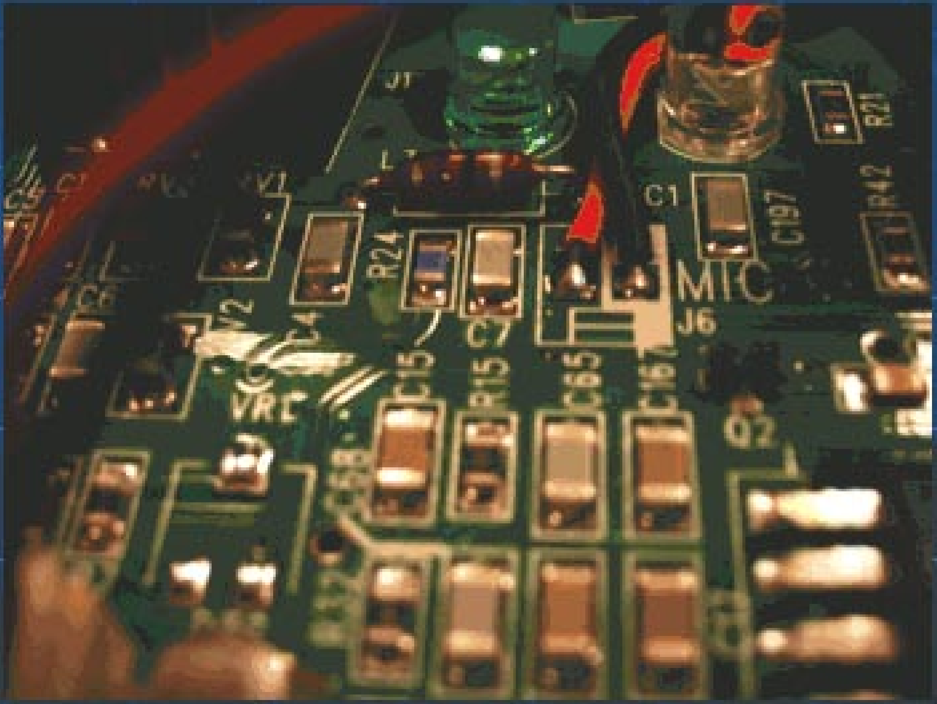
Hostile Device Added

- Device and Clips
- X-Ray of Phone
- Physical Inspection



Modified Speaker Phone

- SMT Diode Pulled
- Capacitor Added
- Audio Bridged
- Hostilely Induced



Local Distribution

Vulnerabilities

1. Station Cables
2. Wall Plates
3. Raw Wiring (in walls and ceilings)
4. Cross Connection Points (IDF/MDF)
5. Normally Not Protected or Supervised
6. IDF/MDF May Be on IDS, Usually Not

IDF Rats Nests

Local Switch

Vulnerabilities

1. Cross Connections Points in MDF
2. Switch Input/Output Ports
3. Switch/PCM Backplane
4. Parallel Channels
5. Switch Software/Firmware Exploits
6. May, or May Not Be Protected

Demarcation/Network Interface

Vulnerabilities

1. Ripe for Exploitation
2. Poorly Protected
3. Generally Accessible
4. Target Specific
5. Significant Choke Point

Local Transmission Network

Vulnerabilities

1. Post Demarcation/NID
2. Before Switch at Central Office
3. Easy to Isolate Single Subscriber
4. Open Terminals and Boots
5. Not Protected, Wide Open

Switching at Central Office

Vulnerabilities

1. Central Office
2. Used to Be Huge Buildings
3. Modern Small Scale Switching
4. Post 9-11 Logo Removals
5. High Value OVERT Choke Point
   - CALEA and .gov targeting
6. Usually Highly Protected, Alarmed, etc

Transmission Network

Vulnerabilities

1. Between Central Offices
2. Mostly Single Mode Fiber Optics
3. Accessible Pubic Pathways
4. Usually Well Marked
5. High Value COVERT Choke Points
6. Cable Vaults on Alarms (sometimes)
7. “Supervised” Against Breakage
8. No Security

Telephonic Integration

- Voice over IP
  - Cable Modems “Fools Phone”
  - Other Broadband Services
  - One Jack to Do Everything
- ISDN (fading out over VOIP)
- Fiber Optic Internet Service
- EVDO (Wireless Broadband)
- Other Wireless Services

The Realistic Threat

- RF Device
- Hard Exploit/Modifications
- Hard Wired Recorder
- Wireless Intercept
- Software Manipulation
- Other Methods

Essential Defensive Tasks

- Conductor Inventory
- Pathway Mapping
- Known Electronic Metrics
  - Re-Testing Against Metric
  - Open Testing
- Physical Inspections
- Repeat

Auditing Telephone Instruments

- What Kind of Phones
- "Soft Under-Belly"
- What Should It Normally Do
  - Is It a Risk?
  - Is It a Threat?
  - Hostile Manipulation?

Feature, Hazard, or Risk?

Wire Path Audit Tools

- Proper Ladder is Key
- Flashlight
- Note Book
- Smart Tone Sets
- Labor Intensive

Auditing Wiring

- What Wire is in the Walls?
- What Wire is in the Ceiling?
- Wall Plates?
- Termination Points
- Junction Points/Punch Blocks

Auditing Wiring

- Conductor Maps (on paper)
  - Signal Pathways
  - Pair Combinations
  - Industry Standard Pin-Outs
  - Color Codes?

  - Conductor Length (metrics)
    - Fractions of an Inch Accuracy

  - Non Linear Junction Conductor Combinations

Auditing Transmission Paths

- Map Out Every
  - Cable
  - Conductor
  - Wire
  - Fortuitous Pathway

  - Location Mapping Accuracy Must Be To Within Fractions of an Inch

Auditing Switching Systems

- What is the Default Generic?
  - Actual Translation?
  - What is Different?
  - Is it Safe?
  - Repeat Bi-Weekly or Monthly

- Always Reduce to hardcopy
- Excel is One of the Best Tools for Auditing PBX Translations

Auditing Instruments

- Tampering with Actual Instrument
- Tampering with:
  - Uncontrolled Accessories
    - Handsets, Cords Cables
    - Power Supplies
    - Low Bandwidth (300 Hz) Filter Bypass
    - Proximity to RF Emitters
      - Nextel vs STU-III Exploit

Auditing Instruments

- Basic Electronic Analysis
- Actual Audit and Visual Inspection
- Intense Physical Inspection
- Extended Technical Analysis
  - 750+ measurements on a single phone
  - Almost 200 printed pages per phone

Penetrations, Hacks, and Attacks.

- Common Manipulations
  - AVAYA, NorTel, etc
- Raw Hacking/Manipulations
  - Usually Targets Switch
- Naked Attacks
  - Digital "BLIP" Box

- Appropriate Counter Measures

VOIP Attacks

- Extremely High Risk
  - Rarely Use Mechanical Hook Switch
  - Open Microphone Exploit Common
  - Firmware Can Be Remotely Modified
  - Extremely Insecure
  - Network Provides a Serious Choke Point

VOIP Attacks

- Multiple Packages to Monitor VOIP
  - Cain-Abel
  - Wireshark
  - Many Others
  - New Software Coming Out Every Month
  - Plug-and-Play Function

Reasonable VOIP Audit Efforts

- Inventory VOIP NW Connections
- Install True Switch
  - Limit Number of Users per Switch
  - Watch the Port Statistics
  - Ensure VOIP Mechanical Hookswitch
  - Monitor VOIP backbone “off hours”
  - Use In-Line Analyzers on Suspect Lines

Reasonable VOIP Audit Efforts

- Wireshark and similar simple software based sniffers are an Eavesdroppers Friend

- But, simple sniffers can also be used to track down weak security or phones passing VOIP room audio.

- Use with caution, and do not eavesdrop

Reasonable VOIP Audit Efforts

Packet Sniffers for VOIP Leakage

1. At the instrument
2. At the switch
3. On the Backbone
4. Both sides of the firewall or router
5. At the Multiplexers
6. Just before it hits fiber (at DS level)
7. Where the signals leave the building

Reasonable VOIP Audit Efforts

Packet Sniffers for VOIP Leakage

1. Purpose built hardware and instruments (avoid computers)
2. Take care not to disrupt traffic
3. Do not broadcast an address yourself
4. ***RX only, do not TX***

Reasonable VOIP Audit Efforts

Packet Sniffers for VOIP Leakage

1. Watch for split pairs
2. Inductive Coupling?
3. Unused VOIP pairs?
4. Room audio on unused pairs?

Mechanisms to Detect and Defeat VOIP Attacks and Exploits

- Detection
  - Unregistered IP Address on VOIP NW
  - Non-VOIP Asset on VOIP Network
  - Hub, not Switch Being Used
  - Machine Being Used On Backbone
    - Classic Man-in-the-Middle Exploit
  - Suspect Data Traffic on an Unused VOIP Phone Line or Conductor

Mechanisms to Detect and Defeat VOIP Attacks and Exploits

- Visual Detection **– Use the Eyes Alone**
  - Visual Inspection of Instrument
    - Is the speakerphone option active?
    - Cisco or Avaya Firmware Exploits?
  - Visual Inspection of Switch
    - Data traffic on switch port…
    - When not actually on a voice call

Methods to Secure VOIP Systems

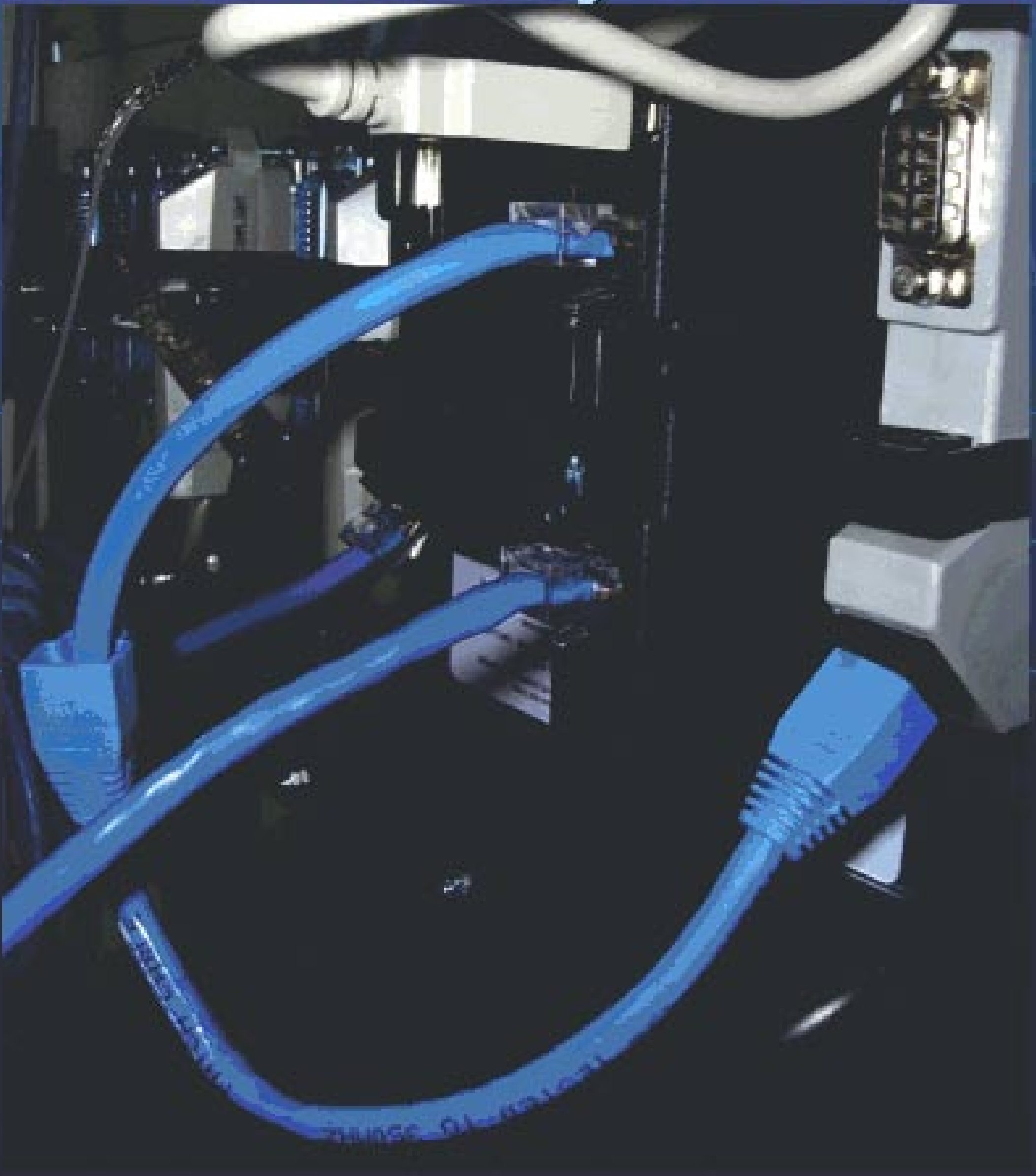
- Utilize Smart Switches, with Stats

- Keep VOIP Terminals on Dedicated Networks, Routers, and Gateways

- Keep VOIP off of Main Network
  - Do Not Integrate into Primary Data Networks

- Lockdown Instrument Firmware
  - Disallow Firmware Updates over the Network

Methods to Secure VOIP Systems



- Keep the VOIP Gateway Admin Port off the fscking Internet

- Lazy Systems Administrators Make Really Bad Security People

  User Name = root
  Account PW = root

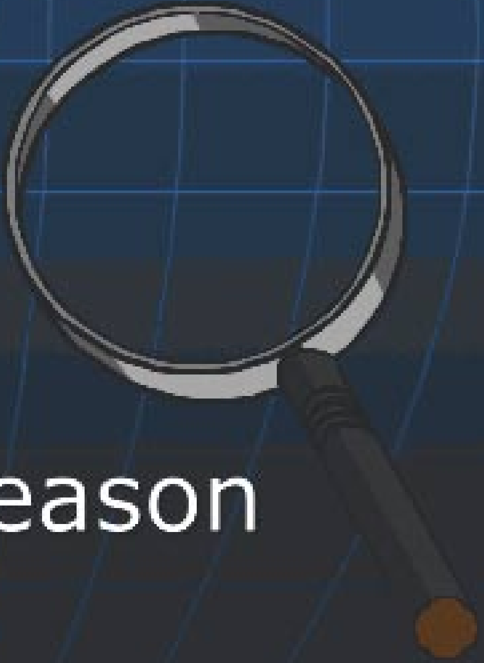
Please Use The Professionals

- Highly Specialized Skills
- Laboratory Test Gear
- Long, Tedious Tests
- Hundreds of Test Forms
- Takes Hours Per Phone
  - A Full Exam
    - 8-12 Hours Per Phone
  - Cursory Testing
    - Four Hours Per Phone

TSCM

Technical Surveillance Counter Measures

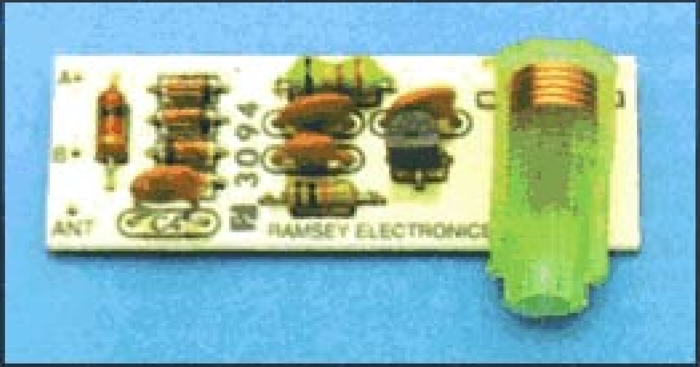
- Inspection by a technician or engineer of a physical item or place
- Highly Technically Trained
- Vast Equipment Required
- Specialized Protocols



Scientific Voice of Reason

Illicit Eavesdropping

In the United States over six million dollars worth of surveillance devices are sold each day - This number is very conservative



Defenses Against the Dark Arts

- Map Out All Wires Present
- Fully Remove Any Unused Wires
  - Optionally, pull at least 30 feet back
  - Remove all unneeded wall plates
- Certify and Seal Wires to Be Used

Defenses Against the Dark Arts

- TSCM Services on Wires Before Live Usage
- Do Not Have Excessive Wires
  - Do we REALLY need that wire?
  - Never over-wire a sensitive area
  - Wire Cutters are your friend

MINIMIZE – MINIMIZE - MINIMIZE

Defenses Against the Dark Arts

- Isolate VOIP and Non VOIP Networks
- Sterilize and Seal Instruments
- In-Line Analysis on Backbone
    - Watch for Traffic Patterns
    - Log all packet headers
    - DAILY or Weekly Auditing

Defenses Against the Dark Arts

- Know the Insides all Instruments
- Know the Exploitable Points
- Learn About Hook Switches

Defenses Against the Dark Arts

- Inspect all IDF/MDF Wiring Blocks
- Add IDF/MDF to Alarm/IDS Systems
- Video Coverage on all IDF/MDF

Defenses Against the Dark Arts

- Inspect the Demarcation Point
- Inspection the Local Terminals
- TDR Mapping of all:
  - Copper Appearance Points
  - Bending or Binding of Cable
  - Above Ground and Below Ground Sites

Defenses Against the Dark Arts

- Pole Walk
  - Map Out All Telephone Poles Back to CO
  - Inventory Position of all Boots
  - Can Involve Miles of Documenting Poles
  - Should Match with TDR Shots

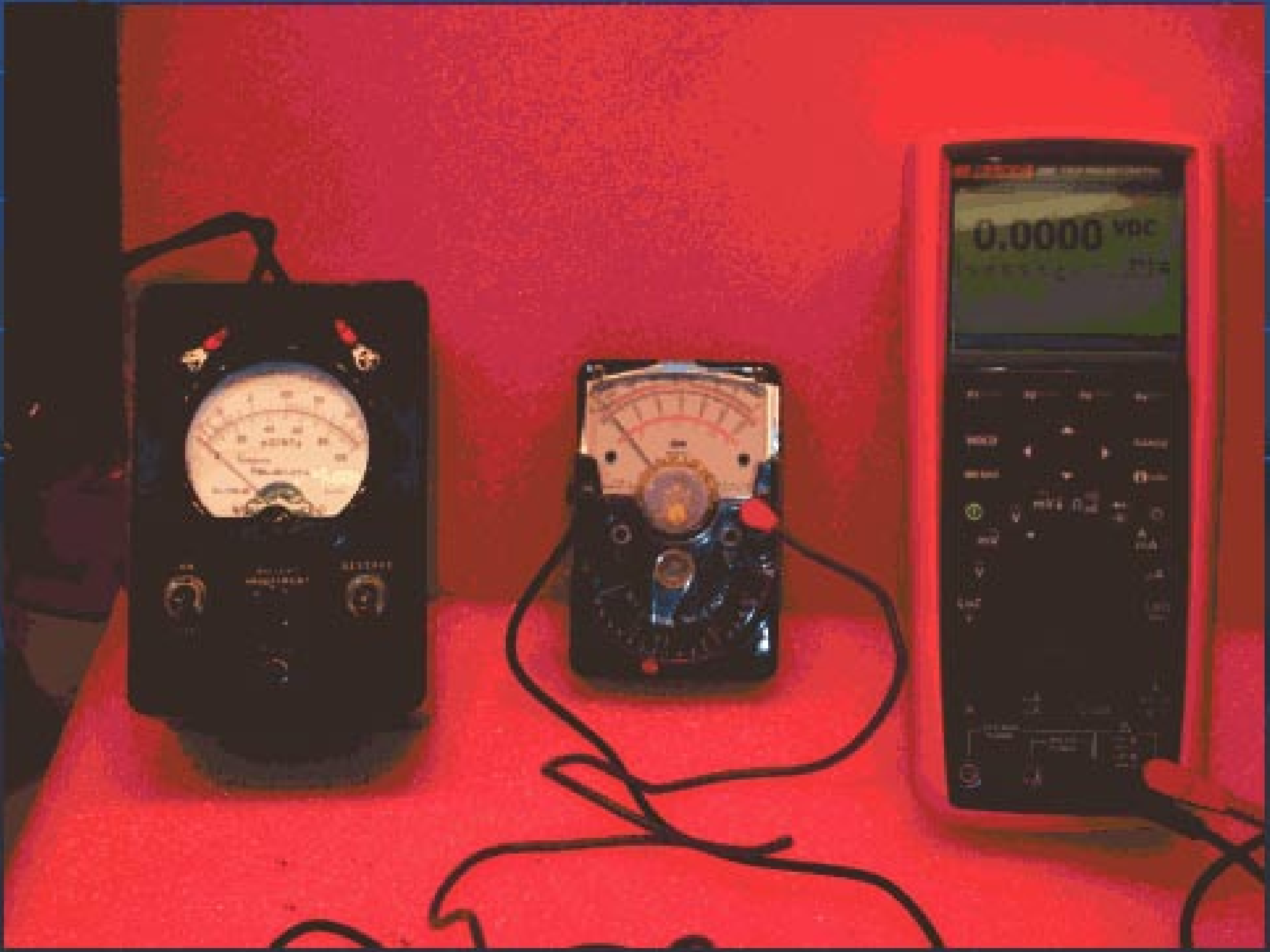
Basic Instrument and Line Tests

- Lets Chat About Bug Sweeping Tools and Test Equipment For a Bit.

- But We Will Focus Mostly on Equipment that You Can Find in Almost Any Electronics Shop, Classroom, or Labs.

Basic Instrument and Line Tests

- Simple Multi-Meters



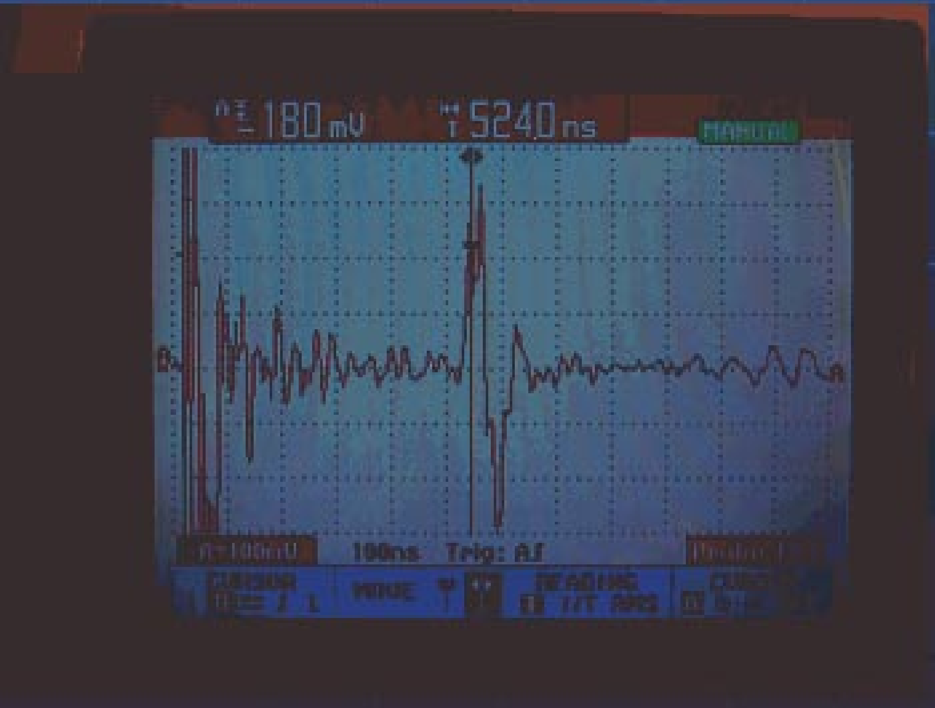
Basic Instrument and Line Tests

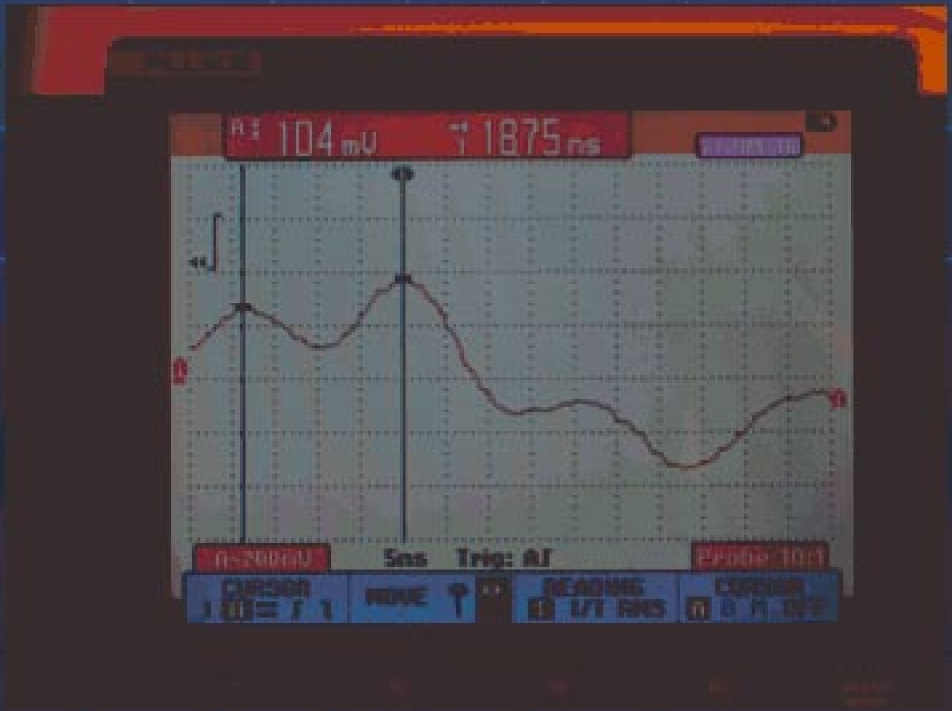
- Oscilloscope
  - Critical as TDR
  - Spectrum Analysis
  - Waveforms
  - Invaluable

Basic Instrument and Line Tests

Scope Used as Precision TDR

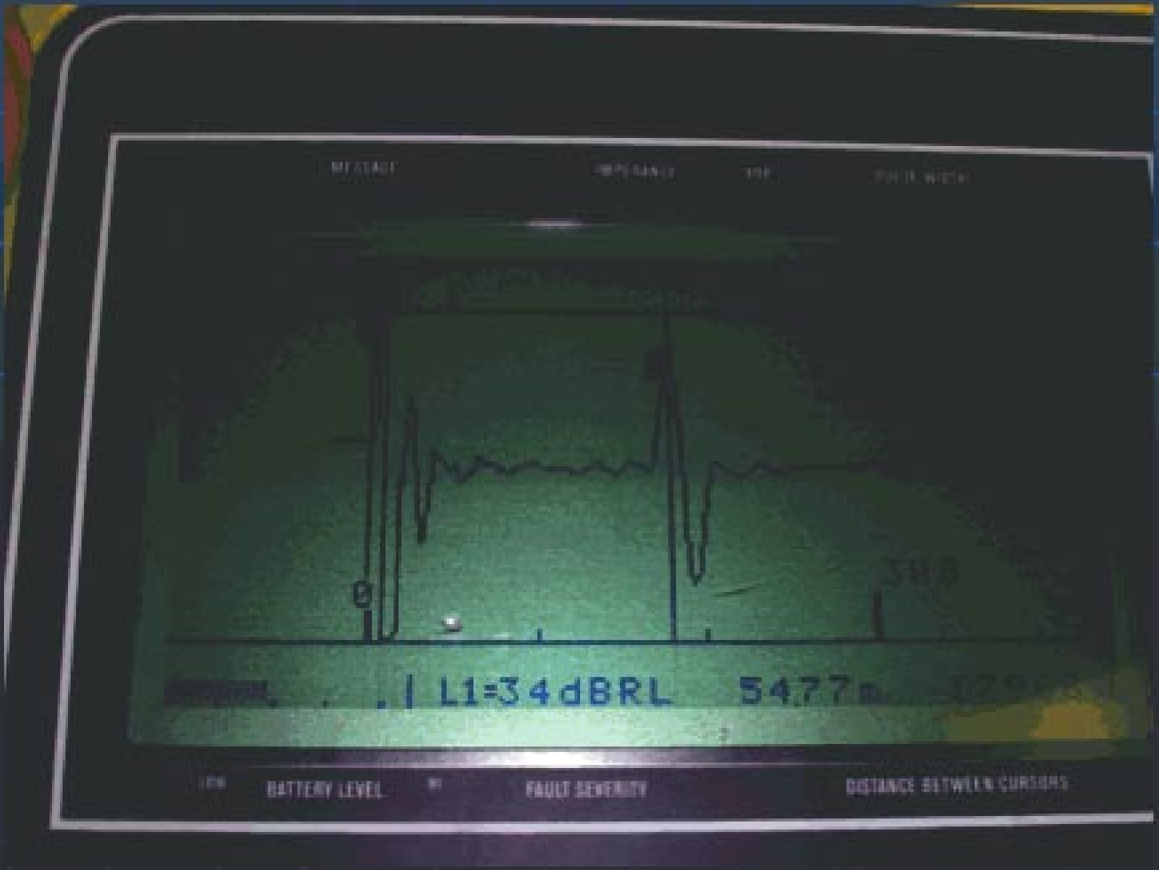
Provides Distance to Fault or Anomaly





Basic Instrument and Line Tests

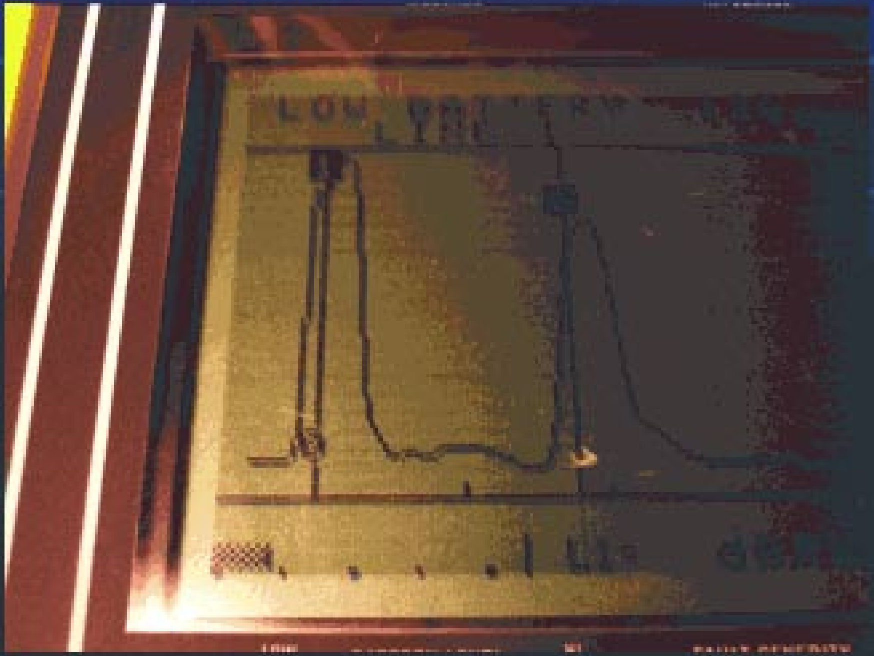
- Commercial TDR
- Inaccurate
- Easy to Use
- Lacks Detail

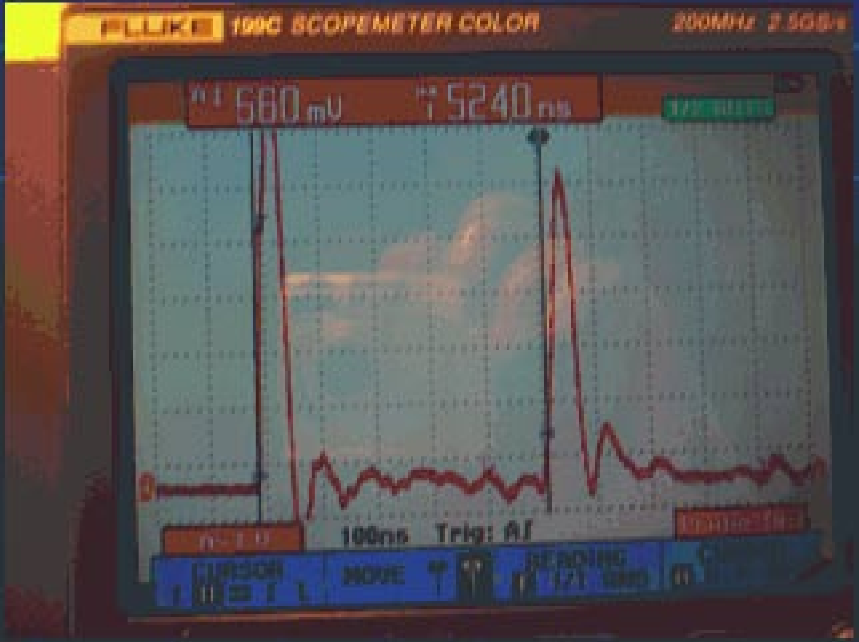


Basic Instrument and Line Tests

- TDR Display vs. O’scope TDR Display

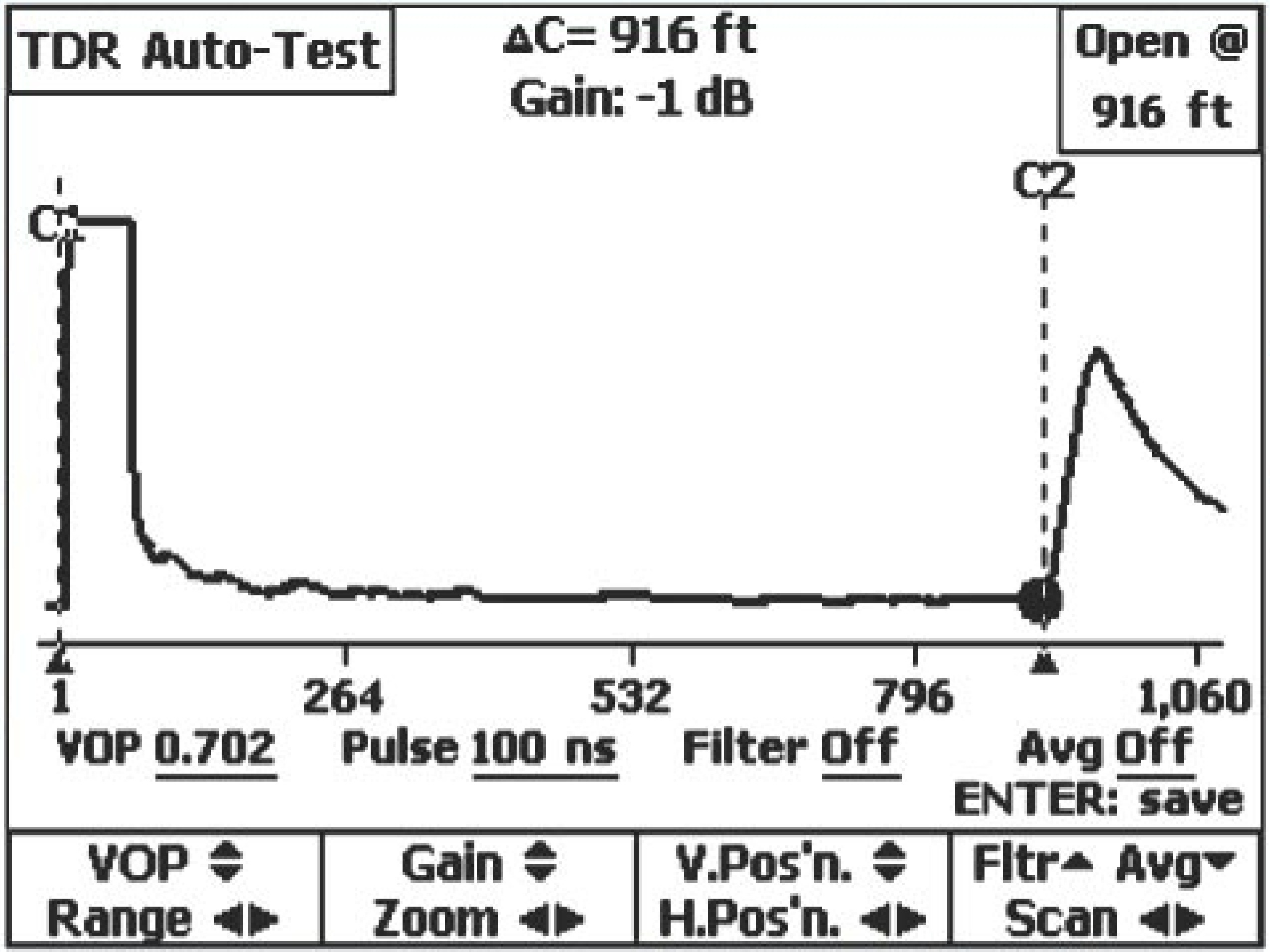
The O’scope is usually better then the TDR





Basic Instrument and Line Tests

- CopperPro 990 Line Analyzer TDR/FDR



TDR Auto-Test

ΔC= 916 ft

Gain: -1 dB

Open @ 916 ft

VOP 0.702 Pulse 100 ns Filter Off Avg Off

ENTER: save

Basic Instrument and Line Tests

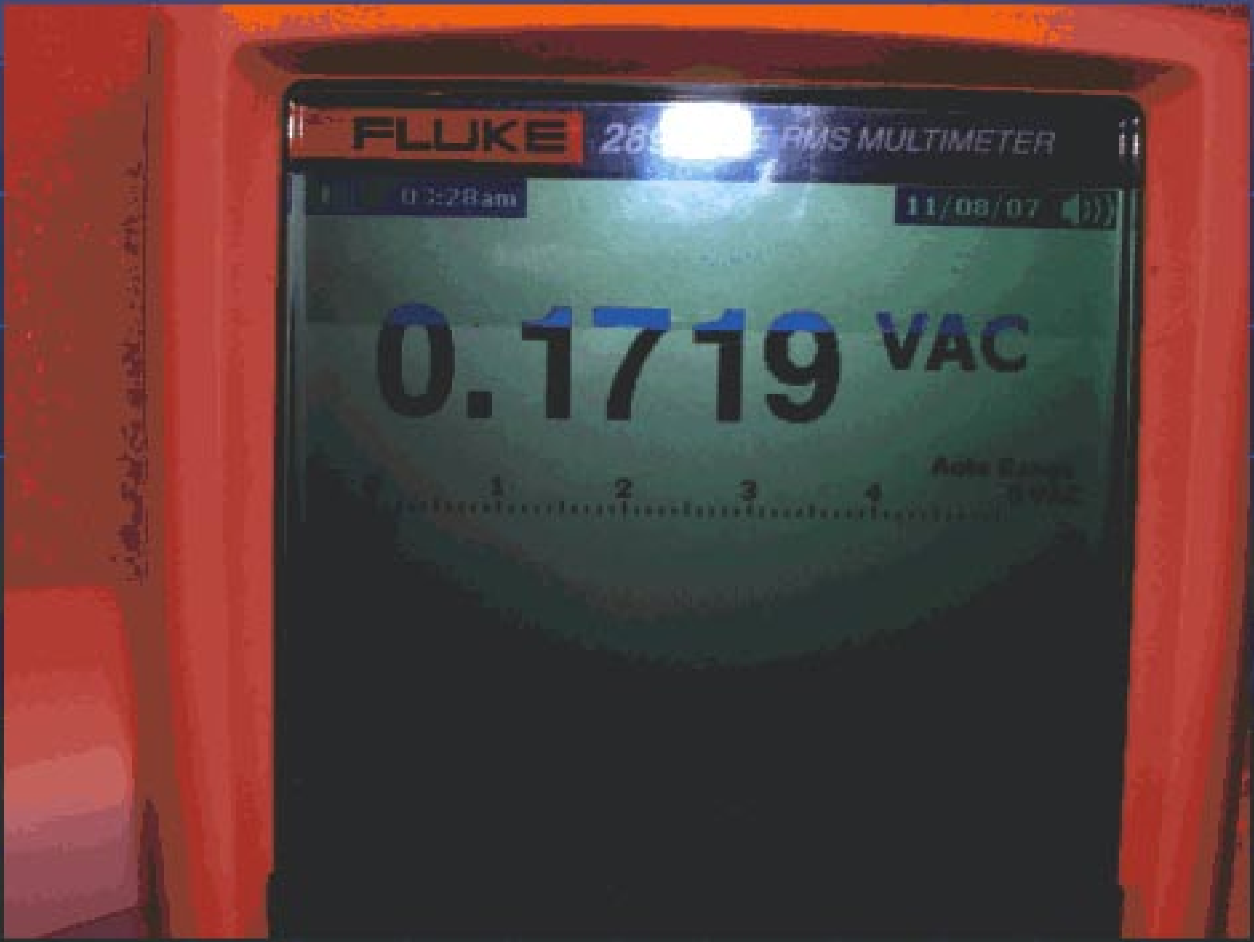
On Hook DC Voltage -49.32 VDC

Basic Instrument and Line Tests

Off Hook DC Voltage -7.68 bias volts

Basic Instrument and Line Tests

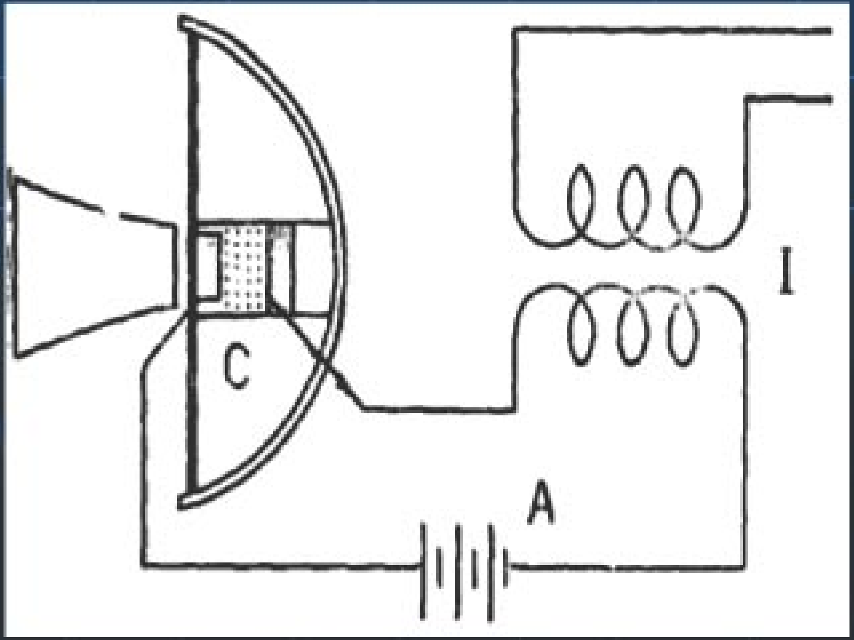
Off Hook AC Voltage - Raw Audio



Basic Instrument and Line Tests

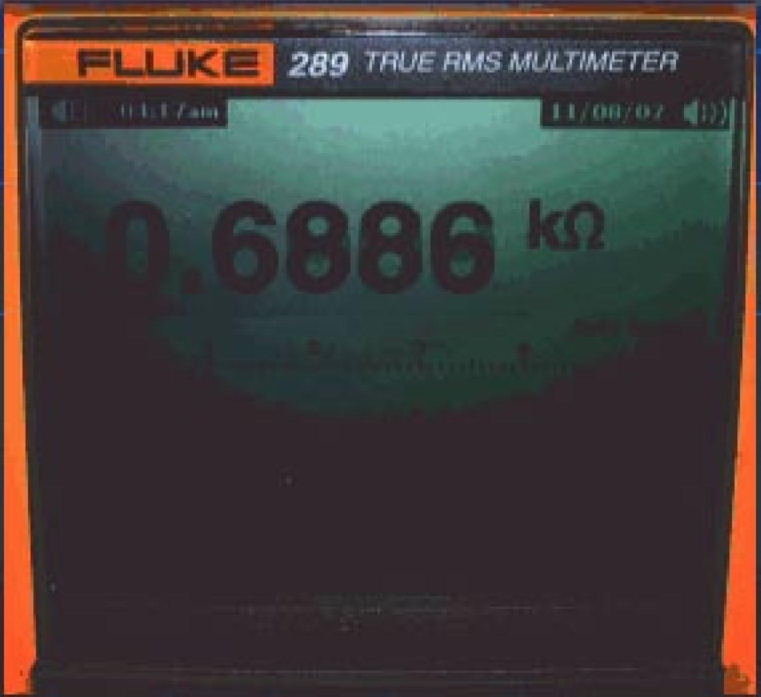
Resistance of Phone Microphone Alone

- Carbon Fiber Microphone/Transmitter
- Microphone is a Variable Resistor



Basic Instrument and Line Tests

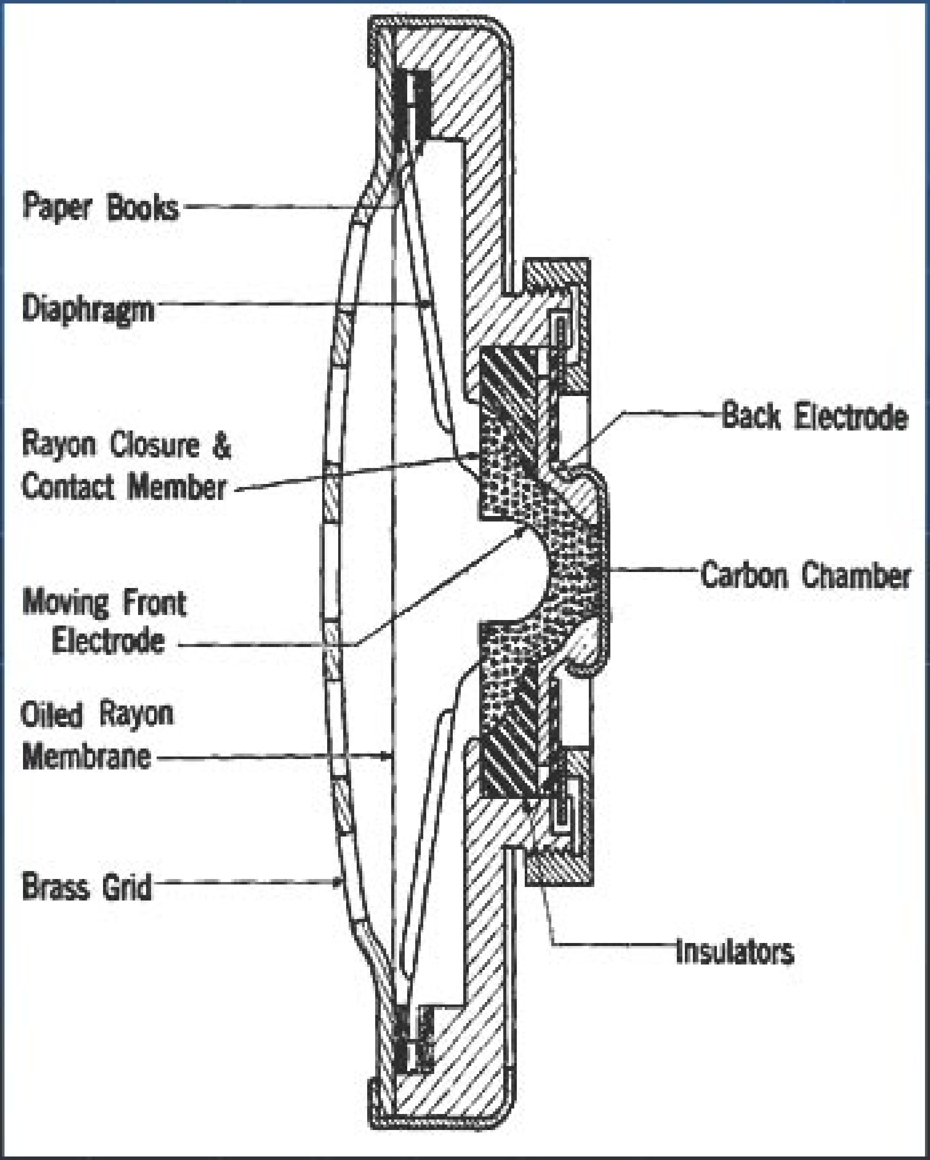
CF Microphone



Basic Instrument and Line Tests

CF Microphone

- One of the most dangerous bugs
- Just hook up an amplifier with .3 to 1 volt of bias and listen in.

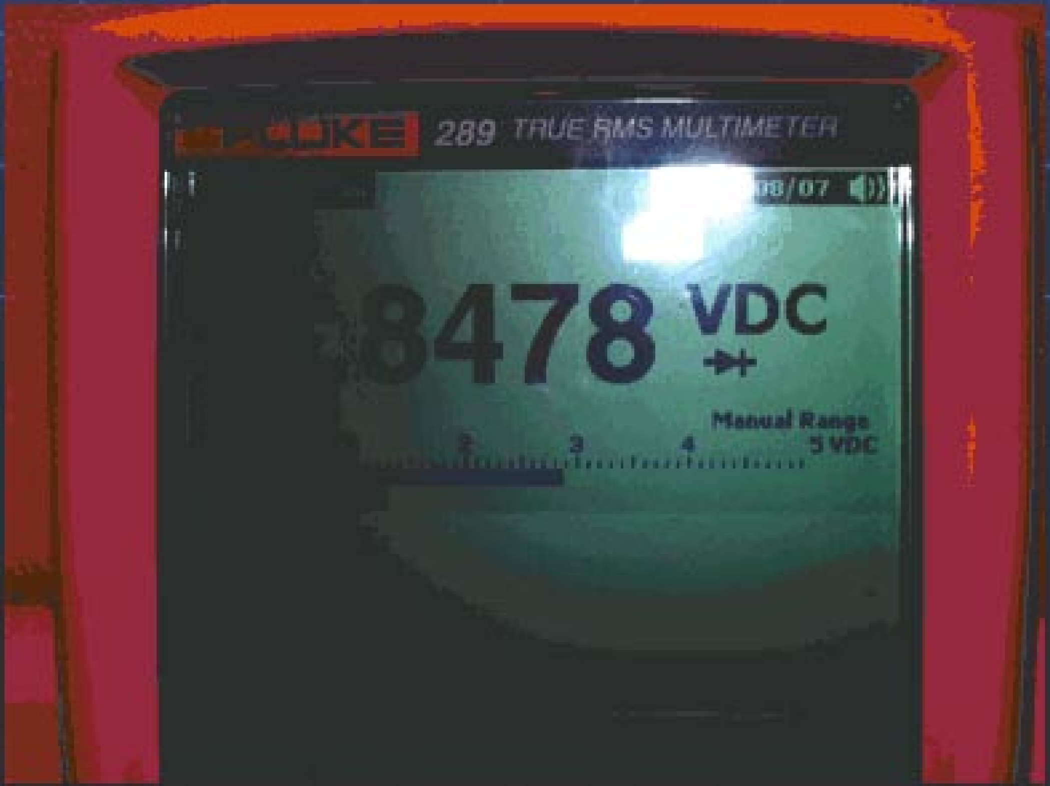


Basic Instrument and Line Tests

Diode Break Down Tests

- We Have a Bug
- Bias Voltage
- “Invisible Bug”

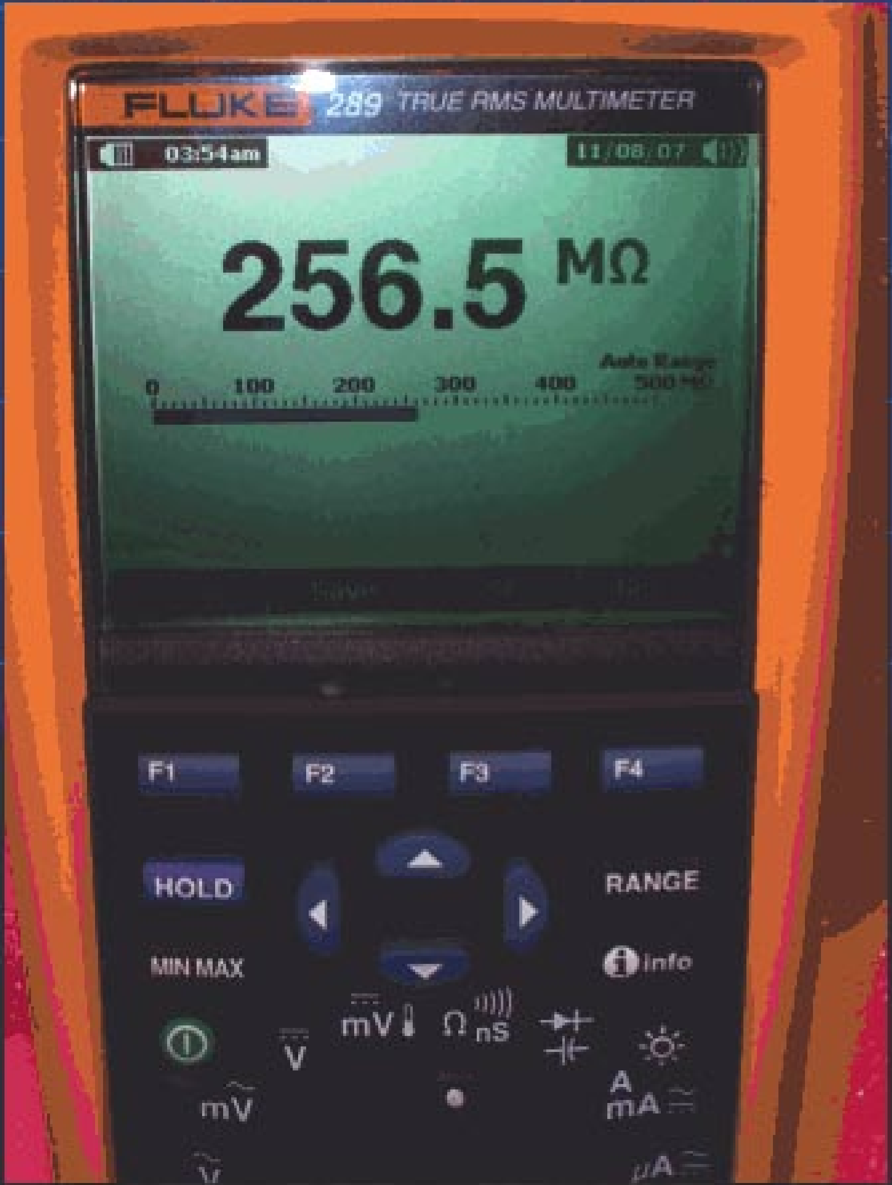
NLJ Pings also Works Well



Basic Instrument and Line Tests

Insulation
Breakdown Test

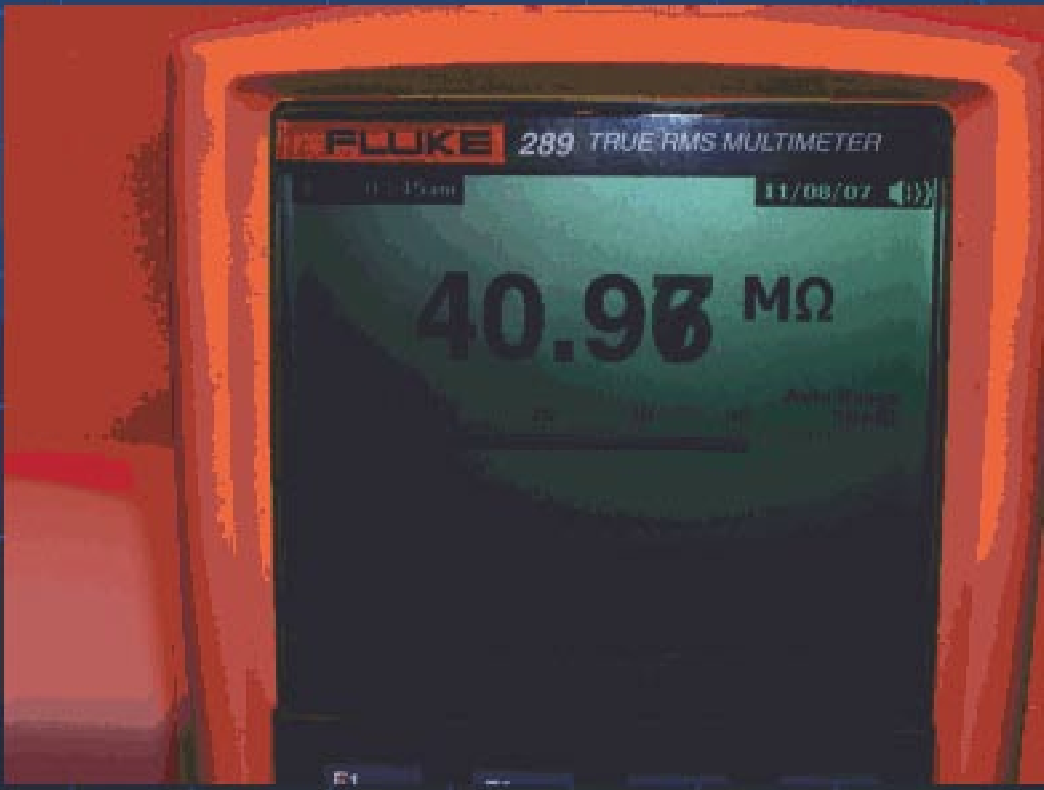
Normal Response



Basic Instrument and Line Tests

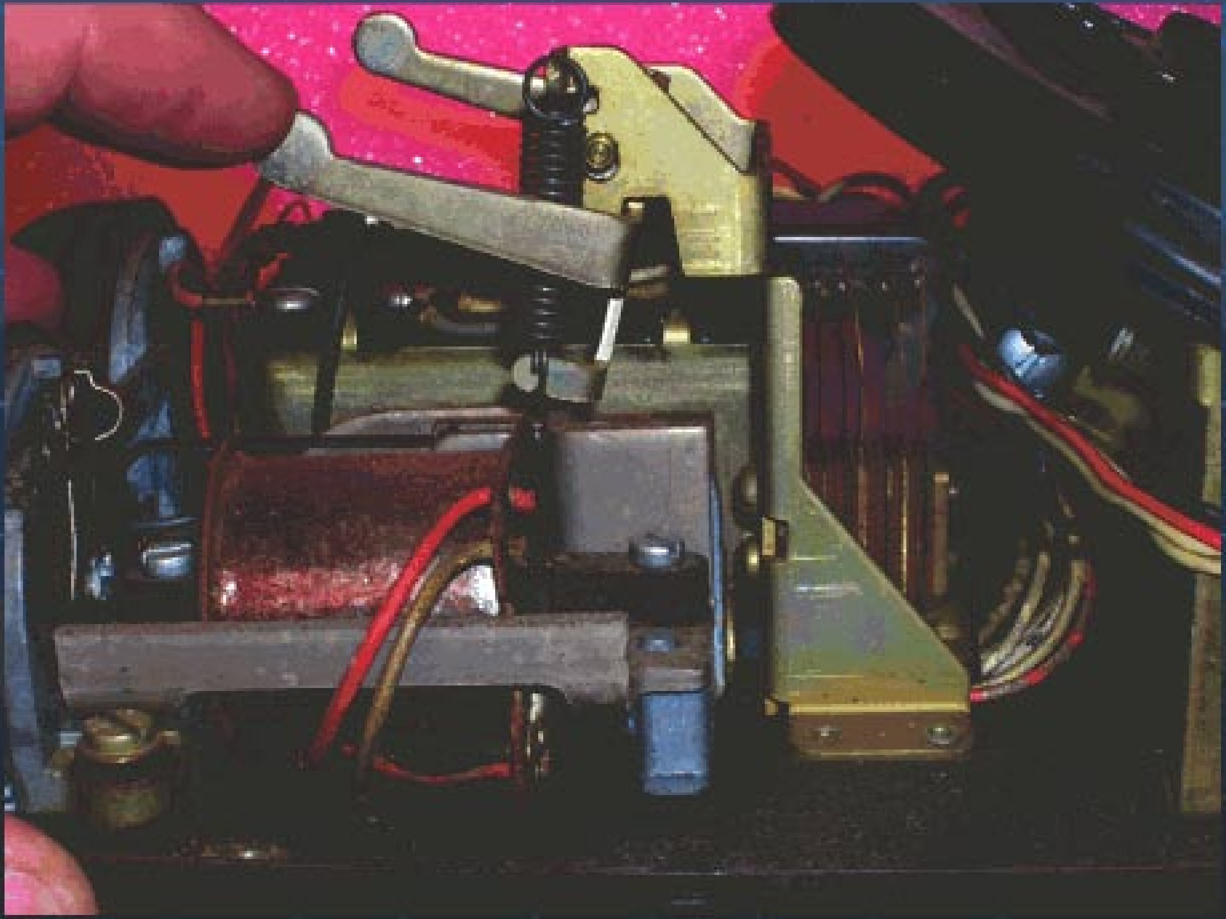
Insulation Breakdown Test

Bugged Response



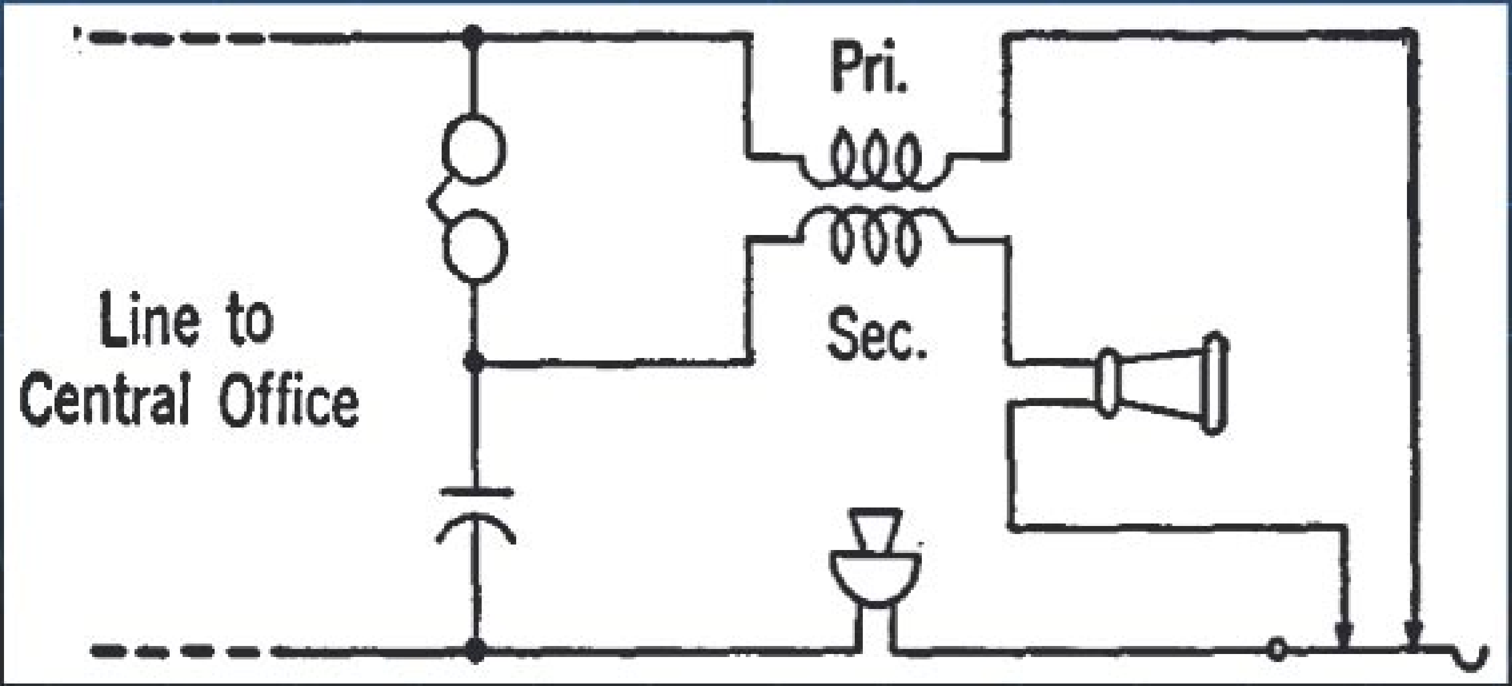
Instrument Hook Switch

- Hook Switch on Right Third of Picture, Under Dial.



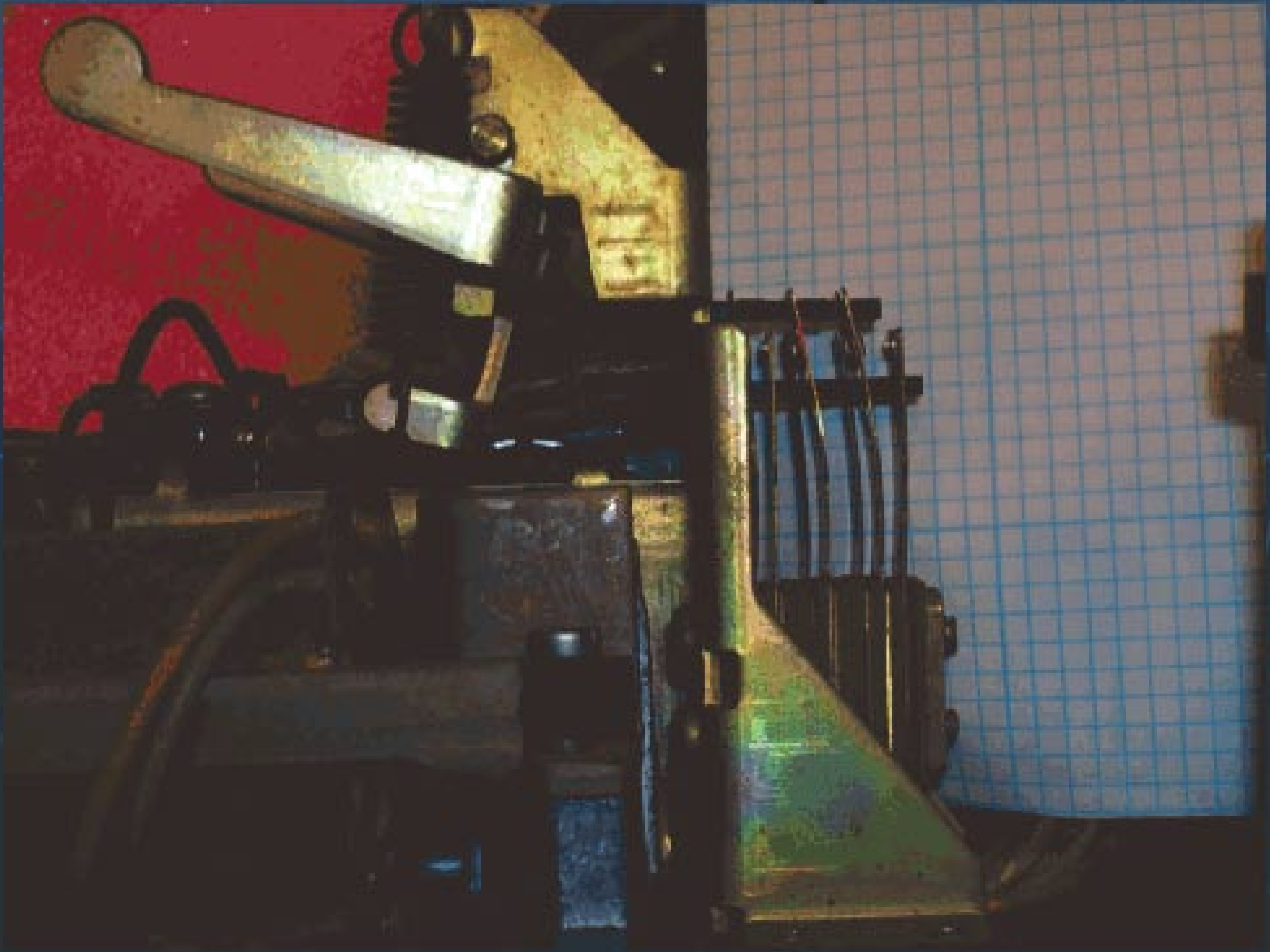
Instrument Hook Switch

- Essential Phone Circuit
  - Eavesdropper adds a Capacitor to Bridge Switch



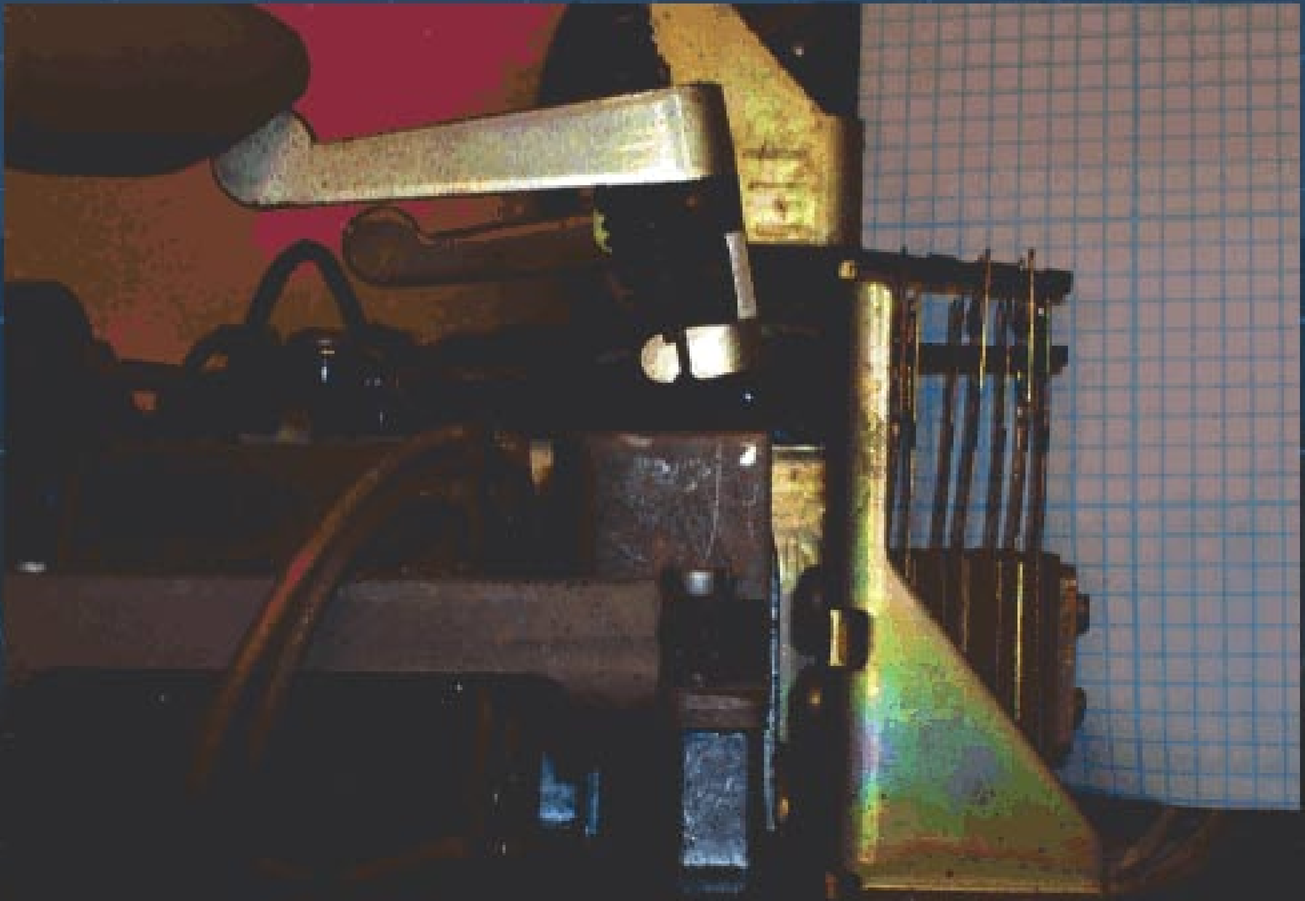
Instrument Hook Switch

Hook Switch Release (Audio Flows)



Instrument Hook Switch

- Hook Switch Depressed (Audio Should Stop)



Tools and Test Equipment

- For Hardcore Technical Folks Only

Tools and Test Equipment

Very Simple, Basic Tools…

Can Find Very Sophisticated Wiretaps and Bugs

Tools and Test Equipment

- Current Leakage Test Jig
- Line Imbalance Test
- Finds Many Parasitic Line Powered Devices
- Requires
  - Two Resistors
  - Three Alligator Clips
  - One Digital Voltmeter
  - Pencil and Paper

- Keep It Simply Simple

Wiretap Detection Documentation

- Before we can take measurements we need to collect some base level data.

- Each Type of Element Always Has its of Form of Standardized Layouts for Analysis.

Essential Phone Data

Phone Location
Plate and Jack #
Jack/Plate Height

Phone Manufacturer
Model Number
Serial Number

How Many Buttons?
2, 4, 6, or 8 wire?
Digital or Analog Phone
Inventory/Asset Tag #
FCC Tag/ID?
Date Manuf. Indicated

Color
Type of Phone
Housing Construction
Non Housing Construction

Toolmarks
- "New" Air Holes
- Screws and Covers
- Prymarks/Seals Broken
- Screw Driver Damage

Cords Mangled

Initial Functional Testing

"Naked Ear Only"

- Dial Tone Present
- Hookswitch Flash
- Mute Functional
- Slow Hook Release
- Slow Line Seize
- Cross Talk On Line

Compliance Data

- Ringer Equivalence Number (REN):
- Jack Type on FCC Label:
- FCC Label - Made In:
- Hearing Aid Compatible (HAC)?

Photograph Phone As Found

- Phone Location In Room
- Face of Dial
- Face of LCD Display
- Manuf and SN Plates
- All Tool Marks or Damage
- Mangled or Loose Cables
- Accessories
- Headsets, Earpieces
- Cable Plug to Phone
- Cable Jack in Phone
- Wallplate Markings

Banjo Dance

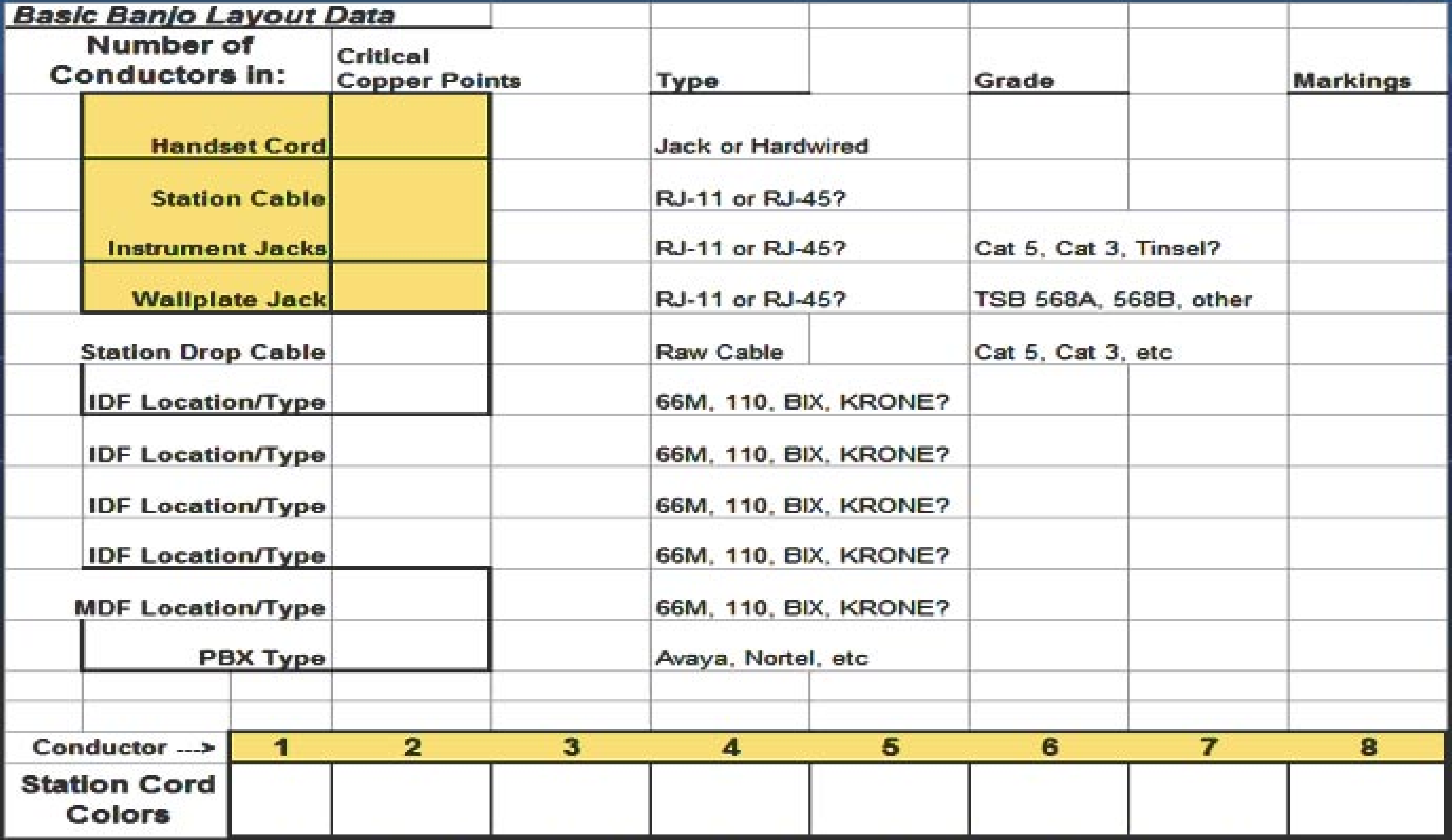
- 16 Pages of Manual or Automated Analysis of Phone, Wiring, and Switch.

- A Banjo Dance is an excellent teaching tool

Banjo Dance

- Minimal Equipment Requirement
  - Digital Volt Meter – Fluke 289
  - Handheld Oscilloscope
  - Pulse Generator
  - Hi-Z Audio Amp w/ Bias Circuit
  - Handheld Spectrum Analyzer
  - NLJD Pinger for Spectrum Analyzer
  - TDR Pinger for Spectrum Analyzer

Basic Banjo Dance Layout



Basic Banjo Layout Data

Number of Conductors in:	Critical Copper Points	Type	Grade	Markings
Handset Cord		Jack or Hardwired		
Station Cable		RJ-11 or RJ-45?		
Instrument Jacks		RJ-11 or RJ-45?	Cat 5, Cat 3, Tinsel?	
Wallplate Jack		RJ-11 or RJ-45?	TSB 568A, 568B, other	
Station Drop Cable		Raw Cable	Cat 5, Cat 3, etc	
IDF Location/Type		66M, 110, BIX, KRONE?		
IDF Location/Type		66M, 110, BIX, KRONE?		
IDF Location/Type		66M, 110, BIX, KRONE?		
IDF Location/Type		66M, 110, BIX, KRONE?		
MDF Location/Type		66M, 110, BIX, KRONE?		
PBX Type		Avaya, Nortel, etc		

Conductor --->	1	2	3	4	5	6	7	8
Station Cord Colors								

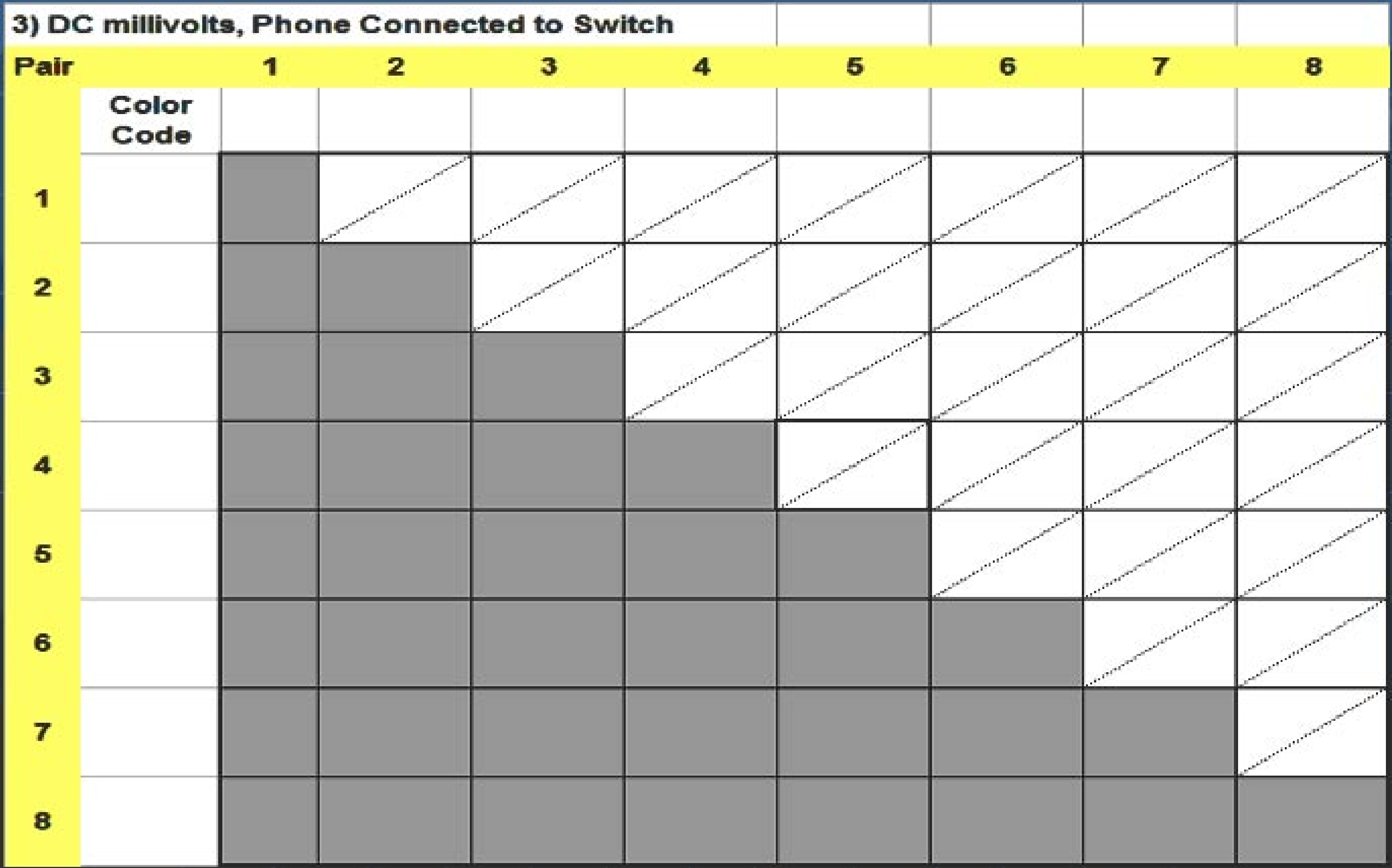
Banjo Dance – DC Volts

1) DC Volts, Phone Connected to Switch									
Pair		1	2	3	4	5	6	7	8
	Color Code								
1		▨							
2		▨	▨						
3		▨	▨	▨					
4		▨	▨	▨	▨				
5		▨	▨	▨	▨	▨			
6		▨	▨	▨	▨	▨	▨		
7		▨	▨	▨	▨	▨	▨	▨	
8		▨	▨	▨	▨	▨	▨	▨	▨

Banjo Dance – AC Volts

2) AC Volts, Phone Connected to Switch									
Pair		1	2	3	4	5	6	7	8
	Color Code								
1		▨							
2		▨	▨						
3		▨	▨	▨					
4		▨	▨	▨	▨				
5		▨	▨	▨	▨	▨			
6		▨	▨	▨	▨	▨	▨		
7		▨	▨	▨	▨	▨	▨	▨	
8		▨	▨	▨	▨	▨	▨	▨	▨

Banjo Dance – DC milliVolts



3) DC millivolts, Phone Connected to Switch

Pair		1	2	3	4	5	6	7	8
	Color Code								
1									
2									
3									
4									
5									
6									
7									
8									

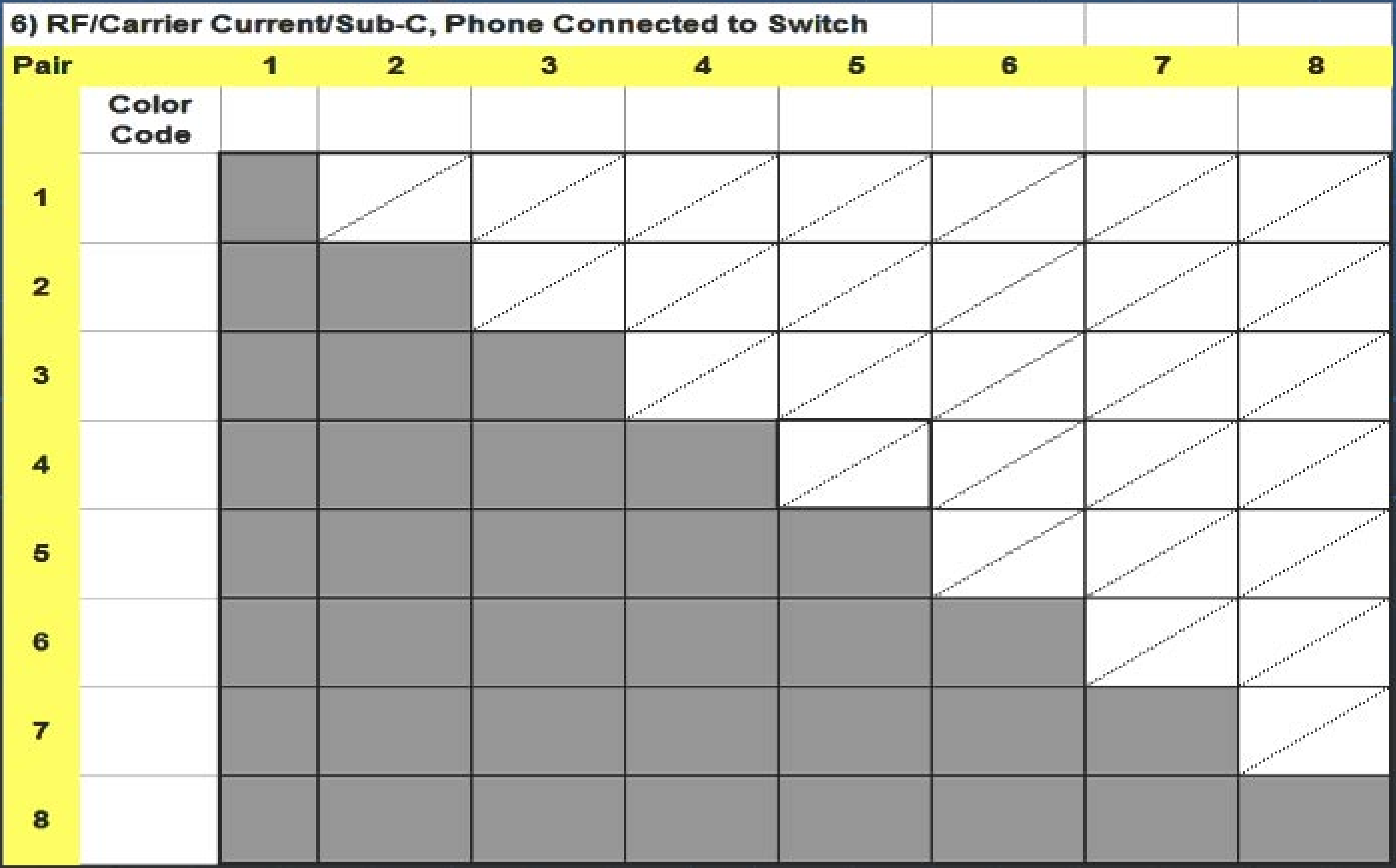
Banjo Dance – AC milliVolts

4) AC millivolts, Phone Connected to Switch									
Pair		1	2	3	4	5	6	7	8
	Color Code								
1									
2									
3									
4									
5									
6									
7									
8									

Banjo Dance – Hi-Z Audio

5) Hi-Z Audio Amplifier, Phone Connected to Switch									
Pair		1	2	3	4	5	6	7	8
	Color Code								
1		▨							
2		▨	▨						
3		▨	▨	▨					
4		▨	▨	▨	▨				
5		▨	▨	▨	▨	▨			
6		▨	▨	▨	▨	▨	▨		
7		▨	▨	▨	▨	▨	▨	▨	
8		▨	▨	▨	▨	▨	▨	▨	▨

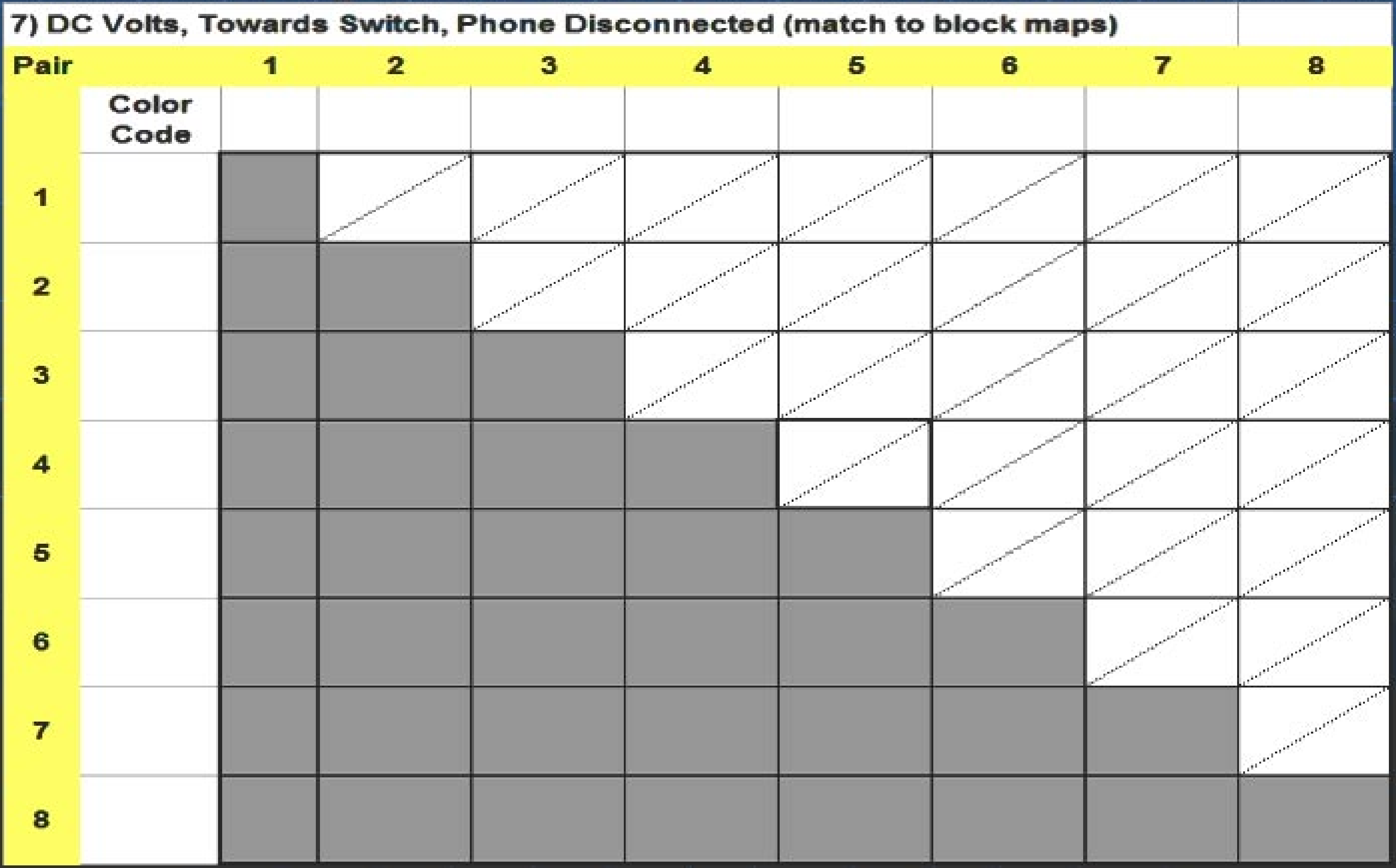
Banjo Dance – RF Carriers



6) RF/Carrier Current/Sub-C, Phone Connected to Switch

Pair		1	2	3	4	5	6	7	8
	Color Code								
1		▨							
2		▨	▨						
3		▨	▨	▨					
4		▨	▨	▨	▨				
5		▨	▨	▨	▨	▨			
6		▨	▨	▨	▨	▨	▨		
7		▨	▨	▨	▨	▨	▨	▨	
8		▨	▨	▨	▨	▨	▨	▨	▨

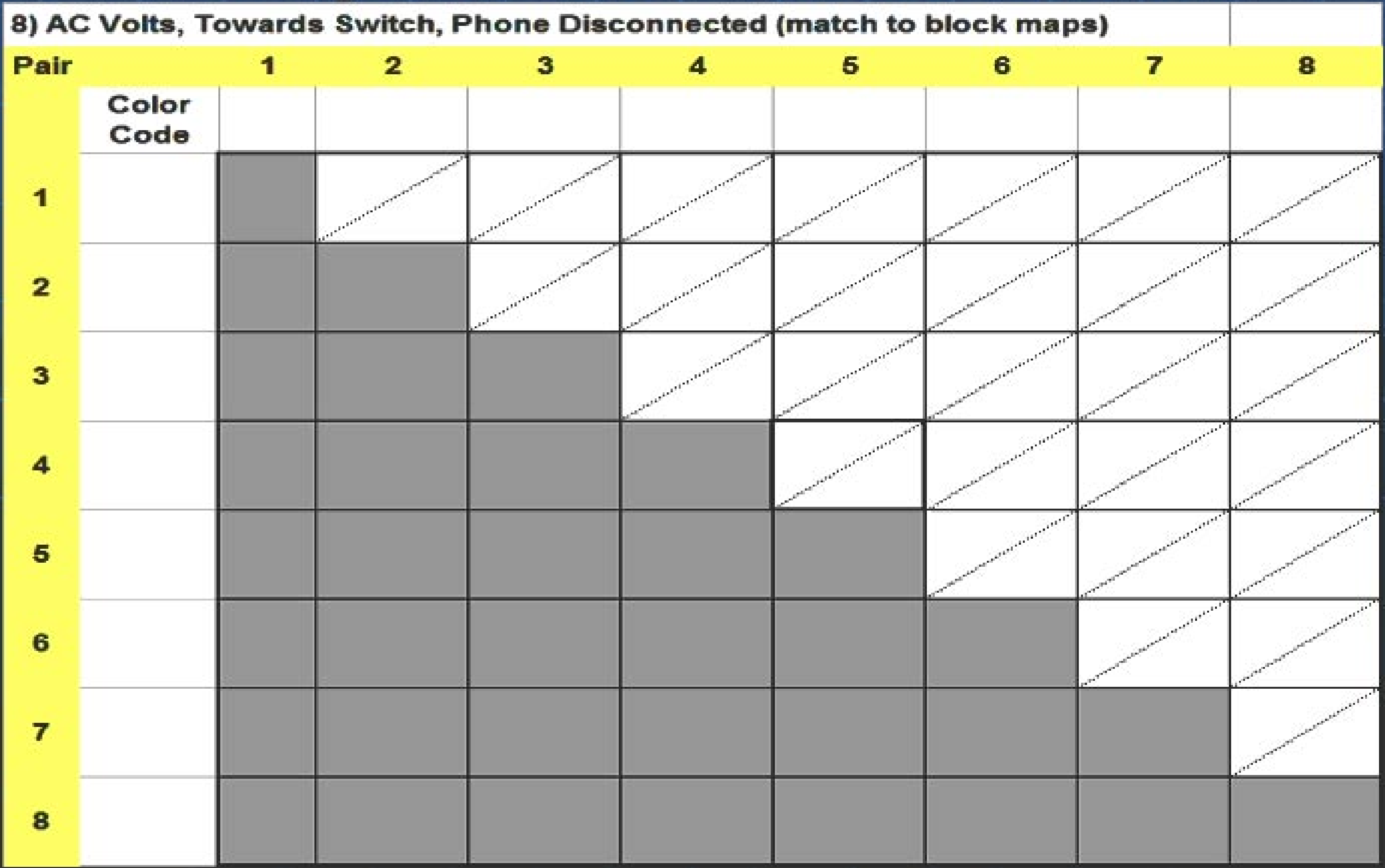
Banjo Dance – DC Volts – to Switch



7) DC Volts, Towards Switch, Phone Disconnected (match to block maps)

Pair		1	2	3	4	5	6	7	8
	Color Code								
1		▨							
2		▨	▨						
3		▨	▨	▨					
4		▨	▨	▨	▨				
5		▨	▨	▨	▨	▨			
6		▨	▨	▨	▨	▨	▨		
7		▨	▨	▨	▨	▨	▨	▨	
8		▨	▨	▨	▨	▨	▨	▨	▨

Banjo Dance – AC Volts – to Switch



8) AC Volts, Towards Switch, Phone Disconnected (match to block maps)

Pair		1	2	3	4	5	6	7	8
	Color Code								
1		▨							
2		▨	▨						
3		▨	▨	▨					
4		▨	▨	▨	▨				
5		▨	▨	▨	▨	▨			
6		▨	▨	▨	▨	▨	▨		
7		▨	▨	▨	▨	▨	▨	▨	
8		▨	▨	▨	▨	▨	▨	▨	▨

Banjo Dance – Oscilloscope

9) Osciliscope Mapping (digital, or RF)									
Pair		1	2	3	4	5	6	7	8
	Color Code								
1		▨							
2		▨	▨						
3		▨	▨	▨					
4		▨	▨	▨	▨				
5		▨	▨	▨	▨	▨			
6		▨	▨	▨	▨	▨	▨		
7		▨	▨	▨	▨	▨	▨	▨	
8		▨	▨	▨	▨	▨	▨	▨	▨

Banjo Dance – AC milliVolts – to Switch

10) AC millivolts, Towards Switch, Phone Disconnected (match to block maps)									
Pair		1	2	3	4	5	6	7	8
	Color Code								
1		▨							
2		▨	▨						
3		▨	▨	▨					
4		▨	▨	▨	▨				
5		▨	▨	▨	▨	▨			
6		▨	▨	▨	▨	▨	▨		
7		▨	▨	▨	▨	▨	▨	▨	
8		▨	▨	▨	▨	▨	▨	▨	▨

Banjo Dance – Ohms/Mega-ohms

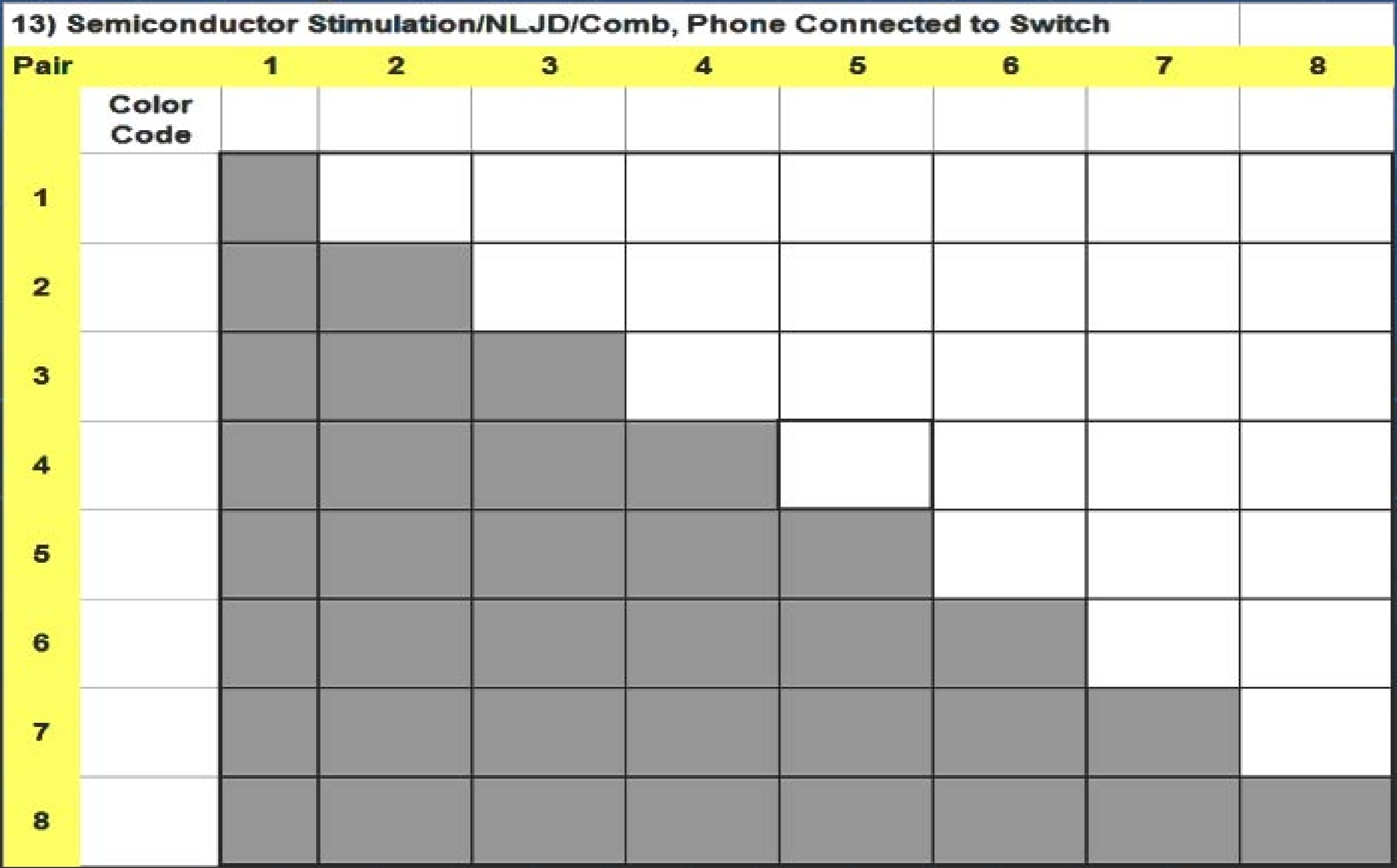
11) Ohms/Mega-ohms - Resistance, Phone Only

Pair		1	2	3	4	5	6	7	8
	Color Code								
1		▨							
2		▨	▨						
3		▨	▨	▨					
4		▨	▨	▨	▨				
5		▨	▨	▨	▨	▨			
6		▨	▨	▨	▨	▨	▨		
7		▨	▨	▨	▨	▨	▨	▨	
8		▨	▨	▨	▨	▨	▨	▨	▨

Banjo Dance – Capacitance, Phone Only

12) uF, nF, pF - Capacitance, Phone Only									
Pair		1	2	3	4	5	6	7	8
	Color Code								
1		▨							
2		▨	▨						
3		▨	▨	▨					
4		▨	▨	▨	▨				
5		▨	▨	▨	▨	▨			
6		▨	▨	▨	▨	▨	▨		
7		▨	▨	▨	▨	▨	▨	▨	
8		▨	▨	▨	▨	▨	▨	▨	▨

Banjo Dance – NLJD Phone & Switch



13) Semiconductor Stimulation/NLJD/Comb, Phone Connected to Switch									
Pair		1	2	3	4	5	6	7	8
	Color Code								
1		▨							
2		▨	▨						
3		▨	▨	▨					
4		▨	▨	▨	▨				
5		▨	▨	▨	▨	▨			
6		▨	▨	▨	▨	▨	▨		
7		▨	▨	▨	▨	▨	▨	▨	
8		▨	▨	▨	▨	▨	▨	▨	▨

Banjo Dance – NLJD Switch Only

14) Semiconductor Stimulation/NLJD/Comb, Switch Only, Phone Disconnected									
Pair		1	2	3	4	5	6	7	8
	Color Code								
1		▨							
2		▨	▨						
3		▨	▨	▨					
4		▨	▨	▨	▨				
5		▨	▨	▨	▨	▨			
6		▨	▨	▨	▨	▨	▨		
7		▨	▨	▨	▨	▨	▨	▨	
8		▨	▨	▨	▨	▨	▨	▨	▨

Banjo Dance – NLJD Phone Only

15) Semiconductor Stimulation/NLJD/Comb, Phone Only, Switch Disconnected									
Pair		1	2	3	4	5	6	7	8
	Color Code								
1		▨							
2		▨	▨						
3		▨	▨	▨					
4		▨	▨	▨	▨				
5		▨	▨	▨	▨	▨			
6		▨	▨	▨	▨	▨	▨		
7		▨	▨	▨	▨	▨	▨	▨	
8		▨	▨	▨	▨	▨	▨	▨	▨

Banjo Dance – TDR/FDR to Switch

16) Time/Frequency Domain Reflectometry, Banjo to Switch, Phone Disconnected

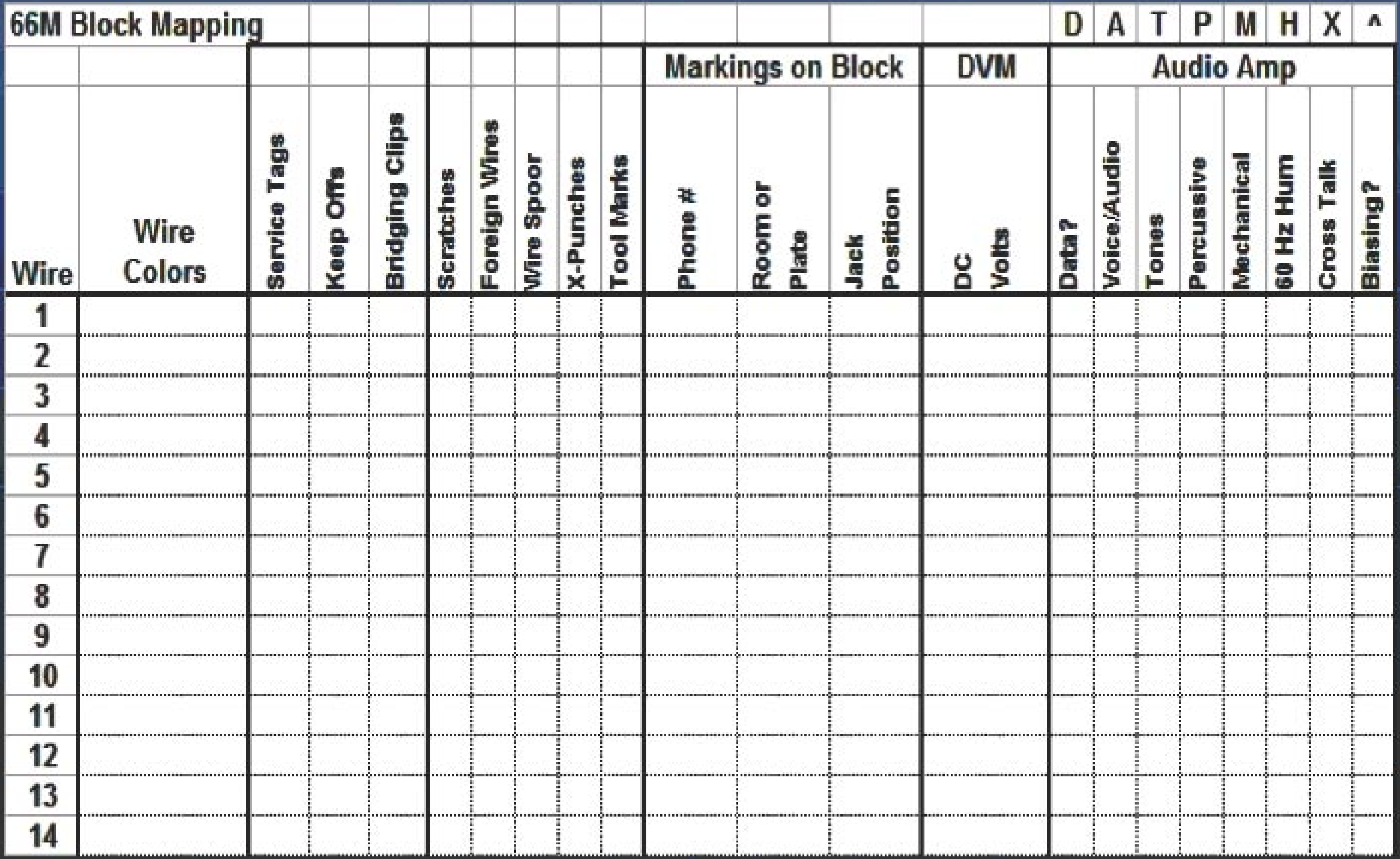
Pair		1	2	3	4	5	6	7	8
	Color Code								
1		▨							
2		▨	▨						
3		▨	▨	▨					
4		▨	▨	▨	▨				
5		▨	▨	▨	▨	▨			
6		▨	▨	▨	▨	▨	▨		
7		▨	▨	▨	▨	▨	▨	▨	
8		▨	▨	▨	▨	▨	▨	▨	▨

Banjo Dance – Results and Summary

Summary of Banjo Dance									
Pair		1	2	3	4	5	6	7	8
	Color Code								
1		▨							
2		▨	▨						
3		▨	▨	▨					
4		▨	▨	▨	▨				
5		▨	▨	▨	▨	▨			
6		▨	▨	▨	▨	▨	▨		
7		▨	▨	▨	▨	▨	▨	▨	
8		▨	▨	▨	▨	▨	▨	▨	▨

66M Block Mapping

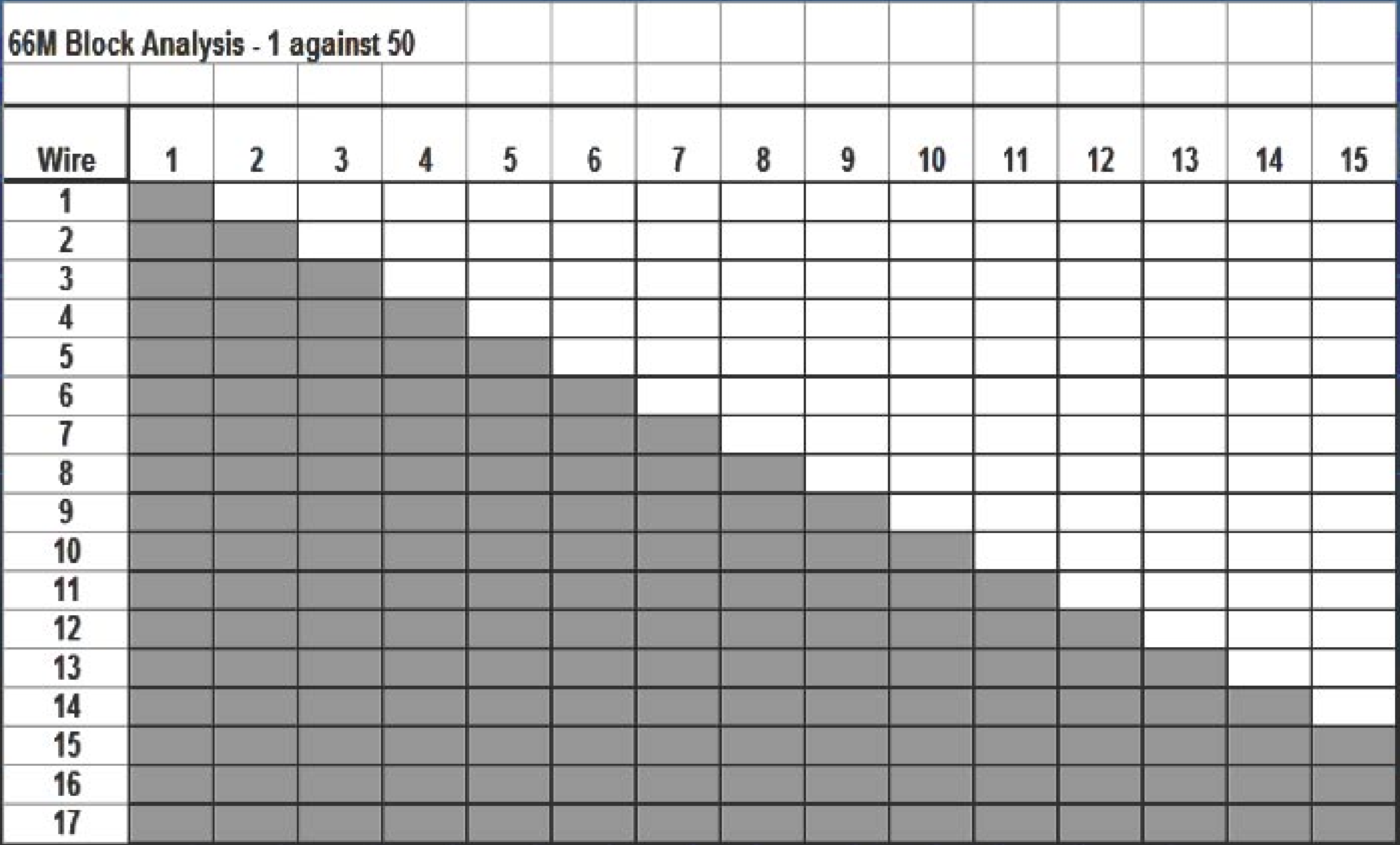
This chart is actually 50 rows long, one 11x17 sheet per block



66M Block Mapping														D	A	T	P	M	H	X	^
										Markings on Block			DVM	Audio Amp							
Wire	Wire Colors	Service Tags	Keep Offs	Bridging Clips	Scratches	Foreign Wires	Wire Spoor	X-Punches	Tool Marks	Phone #	Room or Plate	Jack Position	DC Volts	Data?	Voice/Audio	Tones	Percussive	Mechanical	60 Hz Hum	Cross Talk	Biasing?
1																					
2																					
3																					
4																					
5																					
6																					
7																					
8																					
9																					
10																					
11																					
12																					
13																					
14																					

66M Block Mapping

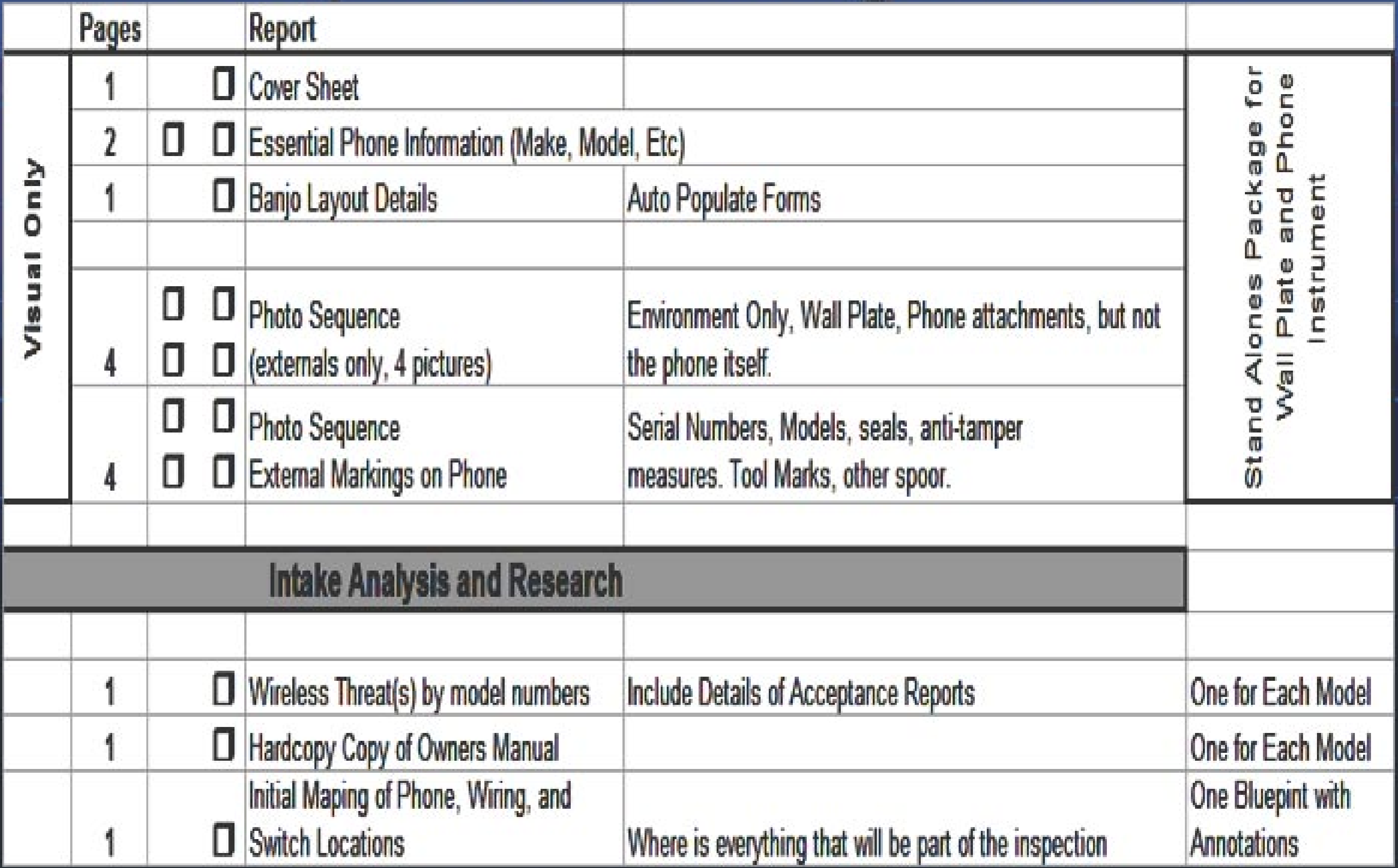
This chart is actually 50 rows long, and 50 columns wide



66M Block Analysis - 1 against 50

Wire	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	▨														
2	▨	▨													
3	▨	▨	▨												
4	▨	▨	▨	▨											
5	▨	▨	▨	▨	▨										
6	▨	▨	▨	▨	▨	▨									
7	▨	▨	▨	▨	▨	▨	▨								
8	▨	▨	▨	▨	▨	▨	▨	▨							
9	▨	▨	▨	▨	▨	▨	▨	▨	▨						
10	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨					
11	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨				
12	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨			
13	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨		
14	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	
15	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
16	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
17	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨

Telephone Tasking Protocol

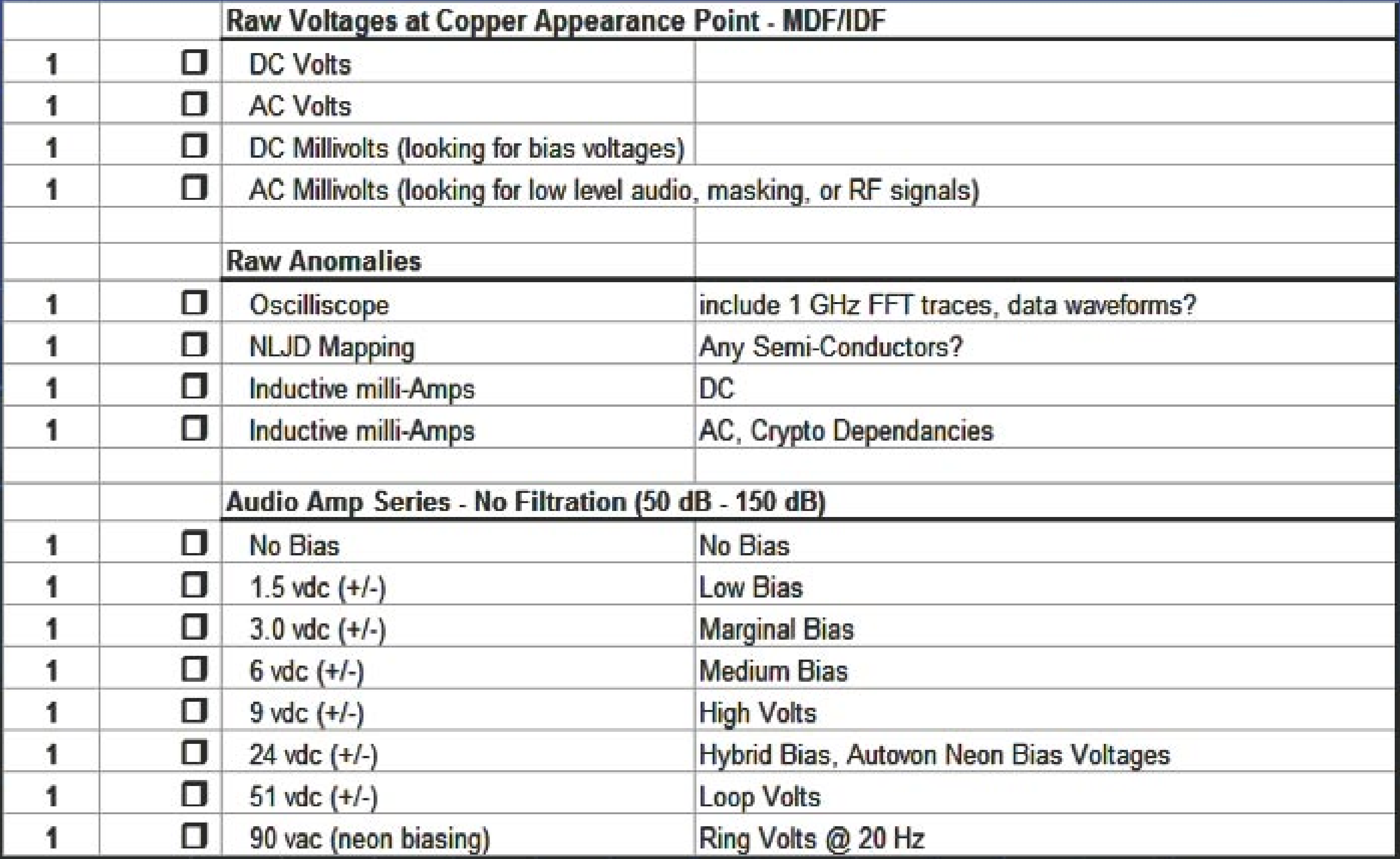


	Pages			Report		
Visual Only	1		□	Cover Sheet		Stand Alones Package for Wall Plate and Phone Instrument
	2	□	□	Essential Phone Information (Make, Model, Etc)		
	1		□	Banjo Layout Details	Auto Populate Forms	
	4	□ □	□ □	Photo Sequence (externals only, 4 pictures)	Environment Only, Wall Plate, Phone attachments, but not the phone itself.	
	4	□ □	□ □	Photo Sequence External Markings on Phone	Serial Numbers, Models, seals, anti-tamper measures. Tool Marks, other spoor.	
Intake Analysis and Research						
	1		□	Wireless Threat(s) by model numbers	Include Details of Acceptance Reports	One for Each Model
	1		□	Hardcopy Copy of Owners Manual		One for Each Model
	1		□	Initial Maping of Phone, Wiring, and Switch Locations	Where is everything that will be part of the inspection	One Bluepint with Annotations

Telephone Tasking Protocol

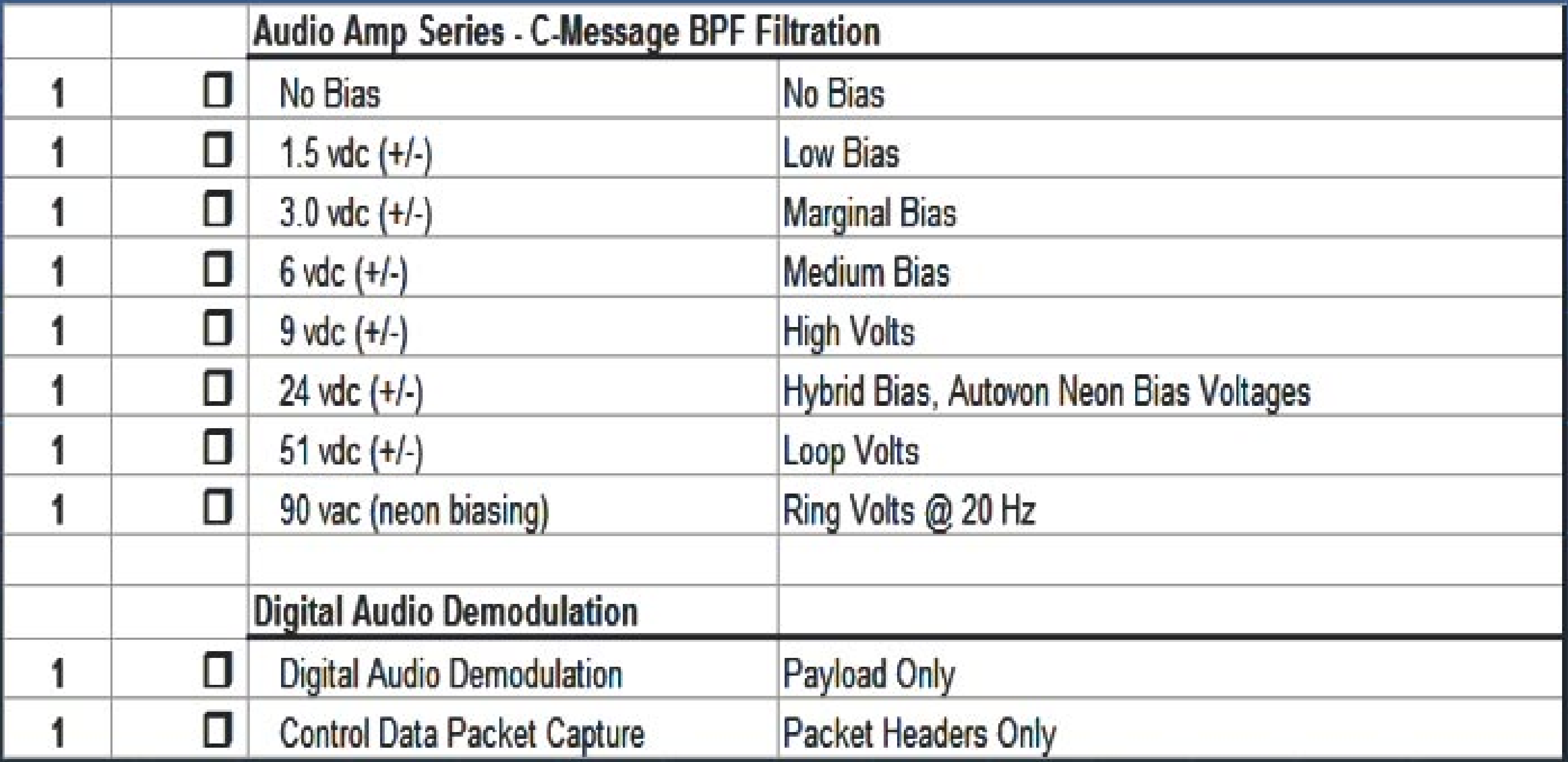
Begin Non-Alerting Sequence
(this is the automated sequence)

Telephone Tasking Protocol



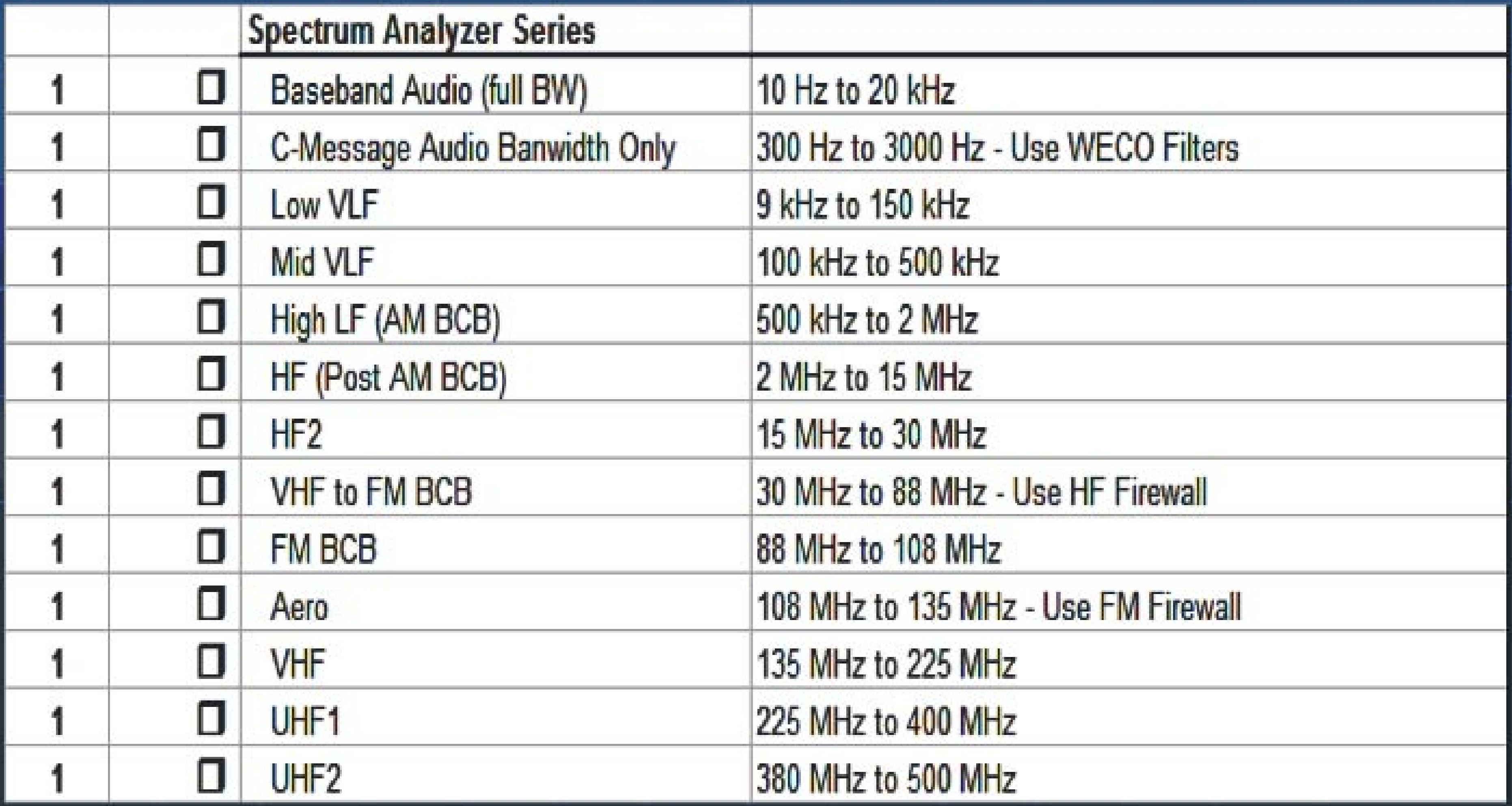
		Raw Voltages at Copper Appearance Point - MDF/IDF	
1	□	DC Volts	
1	□	AC Volts	
1	□	DC Millivolts (looking for bias voltages)	
1	□	AC Millivolts (looking for low level audio, masking, or RF signals)	
		Raw Anomalies	
1	□	Oscilliscope	include 1 GHz FFT traces, data waveforms?
1	□	NLJD Mapping	Any Semi-Conductors?
1	□	Inductive milli-Amps	DC
1	□	Inductive milli-Amps	AC, Crypto Dependancies
		Audio Amp Series - No Filtration (50 dB - 150 dB)	
1	□	No Bias	No Bias
1	□	1.5 vdc (+/-)	Low Bias
1	□	3.0 vdc (+/-)	Marginal Bias
1	□	6 vdc (+/-)	Medium Bias
1	□	9 vdc (+/-)	High Volts
1	□	24 vdc (+/-)	Hybrid Bias, Autovon Neon Bias Voltages
1	□	51 vdc (+/-)	Loop Volts
1	□	90 vac (neon biasing)	Ring Volts @ 20 Hz

Telephone Tasking Protocol



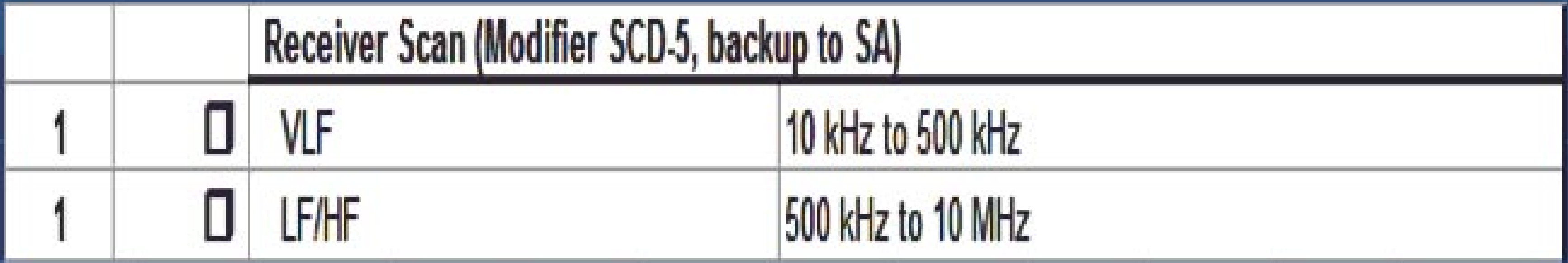
		Audio Amp Series - C-Message BPF Filtration	
1	☐	No Bias	No Bias
1	☐	1.5 vdc (+/-)	Low Bias
1	☐	3.0 vdc (+/-)	Marginal Bias
1	☐	6 vdc (+/-)	Medium Bias
1	☐	9 vdc (+/-)	High Volts
1	☐	24 vdc (+/-)	Hybrid Bias, Autovon Neon Bias Voltages
1	☐	51 vdc (+/-)	Loop Volts
1	☐	90 vac (neon biasing)	Ring Volts @ 20 Hz
		Digital Audio Demodulation	
1	☐	Digital Audio Demodulation	Payload Only
1	☐	Control Data Packet Capture	Packet Headers Only

Telephone Tasking Protocol



		Spectrum Analyzer Series	
1	□	Baseband Audio (full BW)	10 Hz to 20 kHz
1	□	C-Message Audio Banwidth Only	300 Hz to 3000 Hz - Use WECO Filters
1	□	Low VLF	9 kHz to 150 kHz
1	□	Mid VLF	100 kHz to 500 kHz
1	□	High LF (AM BCB)	500 kHz to 2 MHz
1	□	HF (Post AM BCB)	2 MHz to 15 MHz
1	□	HF2	15 MHz to 30 MHz
1	□	VHF to FM BCB	30 MHz to 88 MHz - Use HF Firewall
1	□	FM BCB	88 MHz to 108 MHz
1	□	Aero	108 MHz to 135 MHz - Use FM Firewall
1	□	VHF	135 MHz to 225 MHz
1	□	UHF1	225 MHz to 400 MHz
1	□	UHF2	380 MHz to 500 MHz

Telephone Tasking Protocol

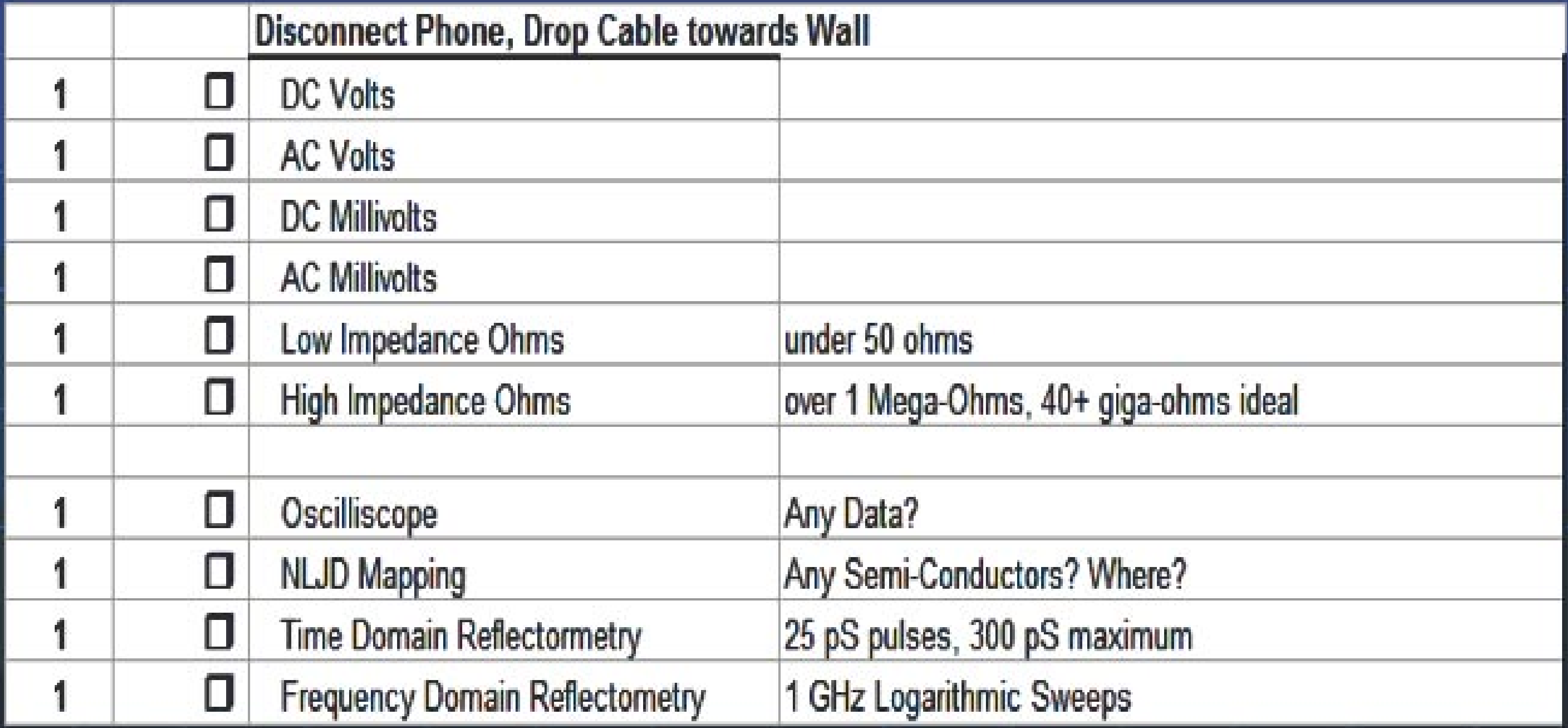


		Receiver Scan (Modifier SCD-5, backup to SA)	
1	□	VLF	10 kHz to 500 kHz
1	□	LF/HF	500 kHz to 10 MHz

Telephone Tasking Protocol

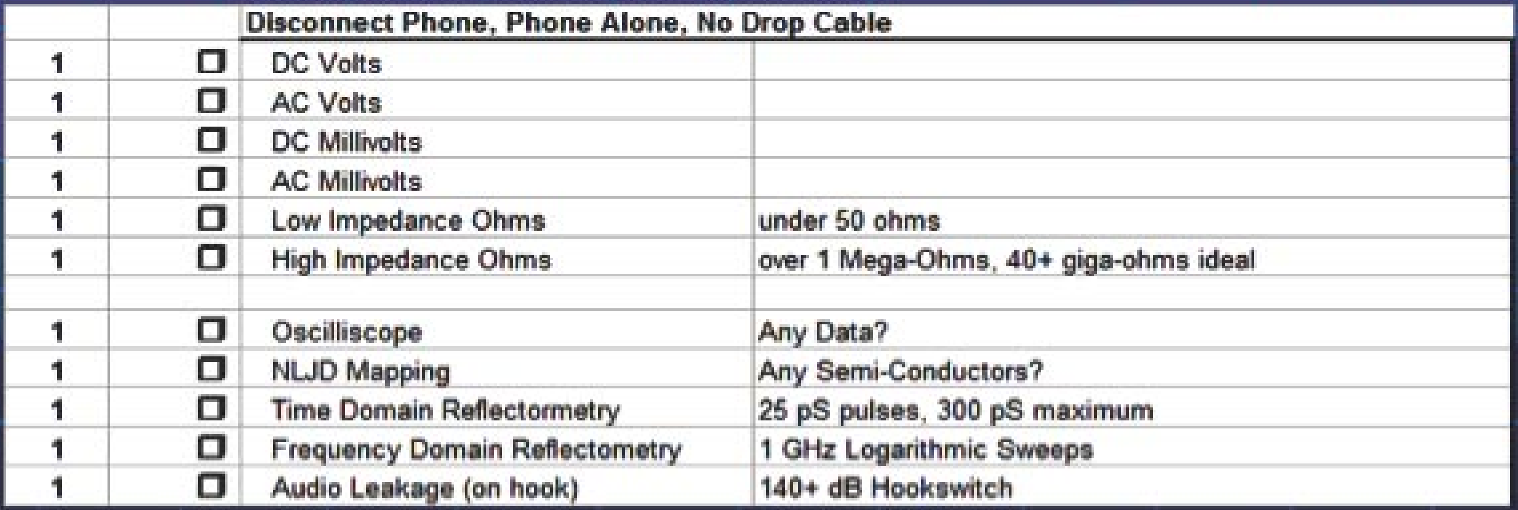
Begin Alerting Sequence

Telephone Tasking Protocol



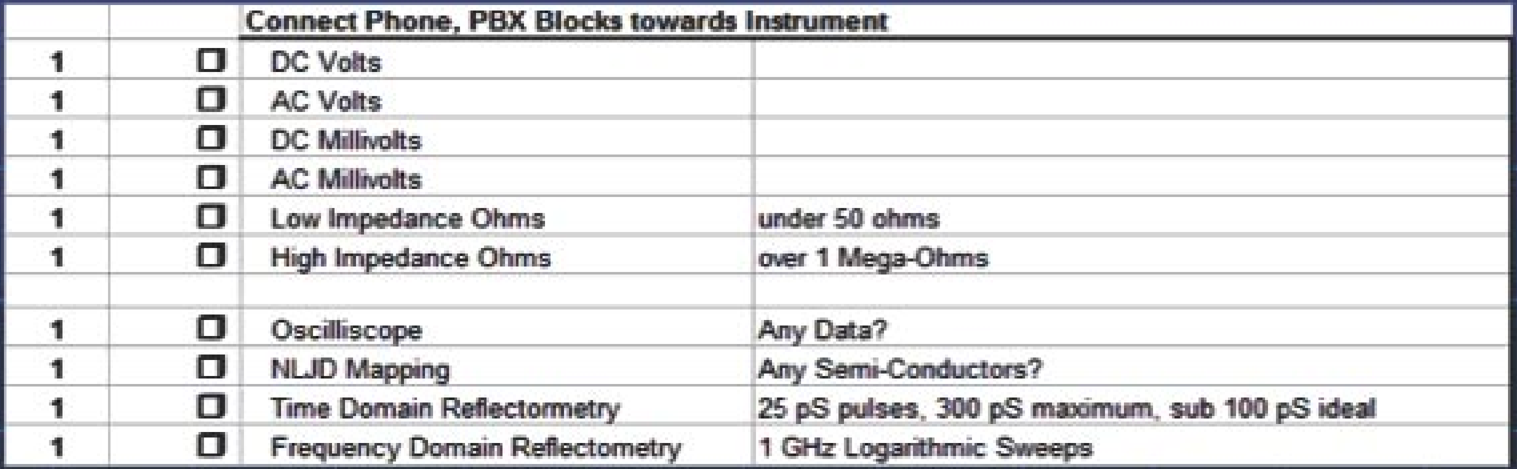
		Disconnect Phone, Drop Cable towards Wall	
1	□	DC Volts	
1	□	AC Volts	
1	□	DC Millivolts	
1	□	AC Millivolts	
1	□	Low Impedance Ohms	under 50 ohms
1	□	High Impedance Ohms	over 1 Mega-Ohms, 40+ giga-ohms ideal
1	□	Oscilliscope	Any Data?
1	□	NLJD Mapping	Any Semi-Conductors? Where?
1	□	Time Domain Reflectormetry	25 pS pulses, 300 pS maximum
1	□	Frequency Domain Reflectometry	1 GHz Logarithmic Sweeps

Telephone Tasking Protocol



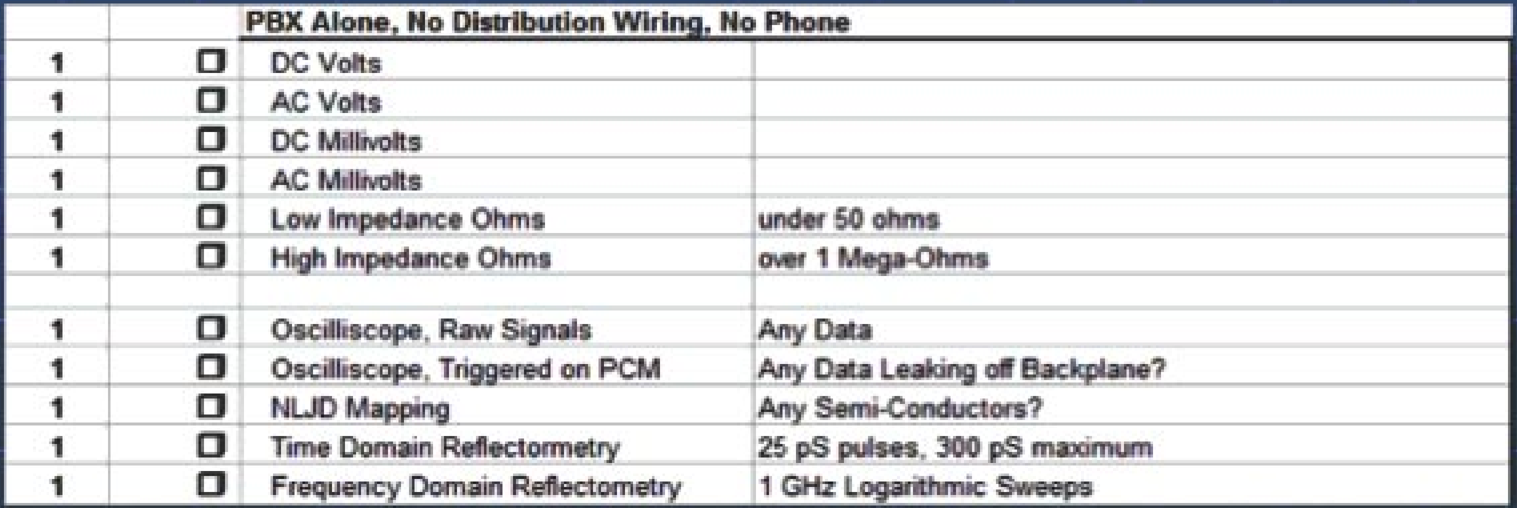
		Disconnect Phone, Phone Alone, No Drop Cable	
1	□	DC Volts	
1	□	AC Volts	
1	□	DC Millivolts	
1	□	AC Millivolts	
1	□	Low Impedance Ohms	under 50 ohms
1	□	High Impedance Ohms	over 1 Mega-Ohms, 40+ giga-ohms ideal
1	□	Oscilliscope	Any Data?
1	□	NLJD Mapping	Any Semi-Conductors?
1	□	Time Domain Reflectormetry	25 pS pulses, 300 pS maximum
1	□	Frequency Domain Reflectometry	1 GHz Logarithmic Sweeps
1	□	Audio Leakage (on hook)	140+ dB Hookswitch

Telephone Tasking Protocol



		Connect Phone, PBX Blocks towards Instrument	
1	□	DC Volts	
1	□	AC Volts	
1	□	DC Millivolts	
1	□	AC Millivolts	
1	□	Low Impedance Ohms	under 50 ohms
1	□	High Impedance Ohms	over 1 Mega-Ohms
1	□	Oscilliscope	Any Data?
1	□	NLJD Mapping	Any Semi-Conductors?
1	□	Time Domain Reflectormetry	25 pS pulses, 300 pS maximum, sub 100 pS ideal
1	□	Frequency Domain Reflectometry	1 GHz Logarithmic Sweeps

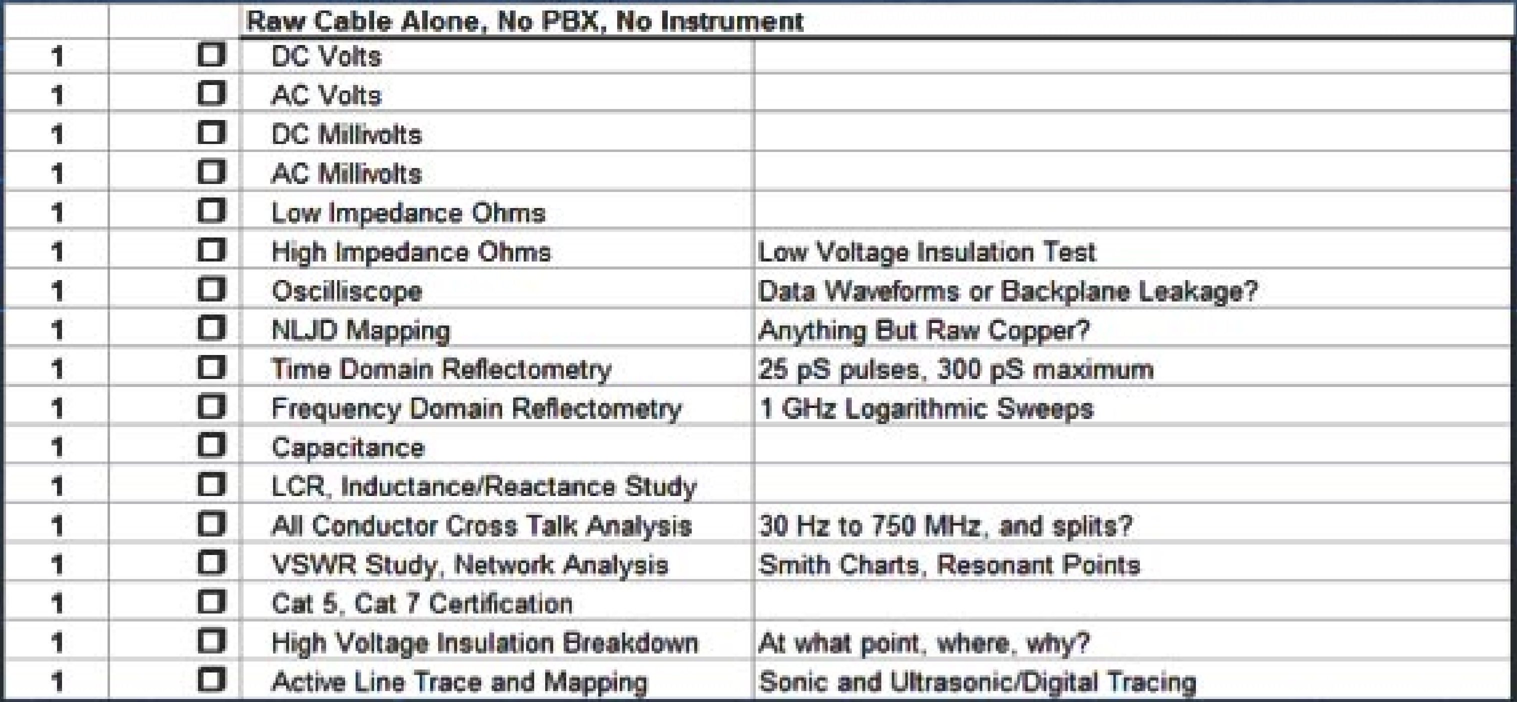
Telephone Tasking Protocol



		PBX Alone, No Distribution Wiring, No Phone	
1	□	DC Volts	
1	□	AC Volts	
1	□	DC Millivolts	
1	□	AC Millivolts	
1	□	Low Impedance Ohms	under 50 ohms
1	□	High Impedance Ohms	over 1 Mega-Ohms
1	□	Oscilliscope, Raw Signals	Any Data
1	□	Oscilliscope, Triggered on PCM	Any Data Leaking off Backplane?
1	□	NLJD Mapping	Any Semi-Conductors?
1	□	Time Domain Reflectormetry	25 pS pulses, 300 pS maximum
1	□	Frequency Domain Reflectometry	1 GHz Logarithmic Sweeps

Telephone Tasking Protocol

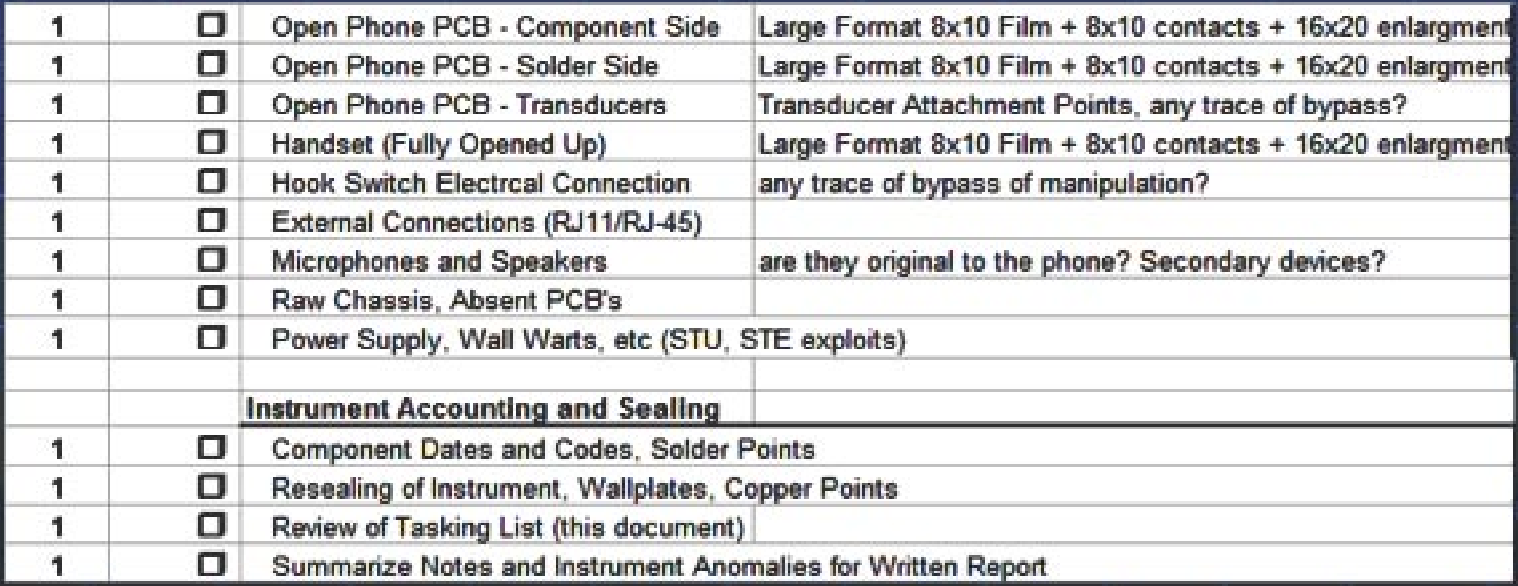
- This Tells Us if Someone Has Tampered With The Raw Wiring or Jacks In Any Way



		Raw Cable Alone, No PBX, No Instrument	
1	□	DC Volts	
1	□	AC Volts	
1	□	DC Millivolts	
1	□	AC Millivolts	
1	□	Low Impedance Ohms	
1	□	High Impedance Ohms	Low Voltage Insulation Test
1	□	Oscilliscope	Data Waveforms or Backplane Leakage?
1	□	NLJD Mapping	Anything But Raw Copper?
1	□	Time Domain Reflectometry	25 pS pulses, 300 pS maximum
1	□	Frequency Domain Reflectometry	1 GHz Logarithmic Sweeps
1	□	Capacitance	
1	□	LCR, Inductance/Reactance Study	
1	□	All Conductor Cross Talk Analysis	30 Hz to 750 MHz, and splits?
1	□	VSWR Study, Network Analysis	Smith Charts, Resonant Points
1	□	Cat 5, Cat 7 Certification	
1	□	High Voltage Insulation Breakdown	At what point, where, why?
1	□	Active Line Trace and Mapping	Sonic and Ultrasonic/Digital Tracing

Telephone Tasking Protocol

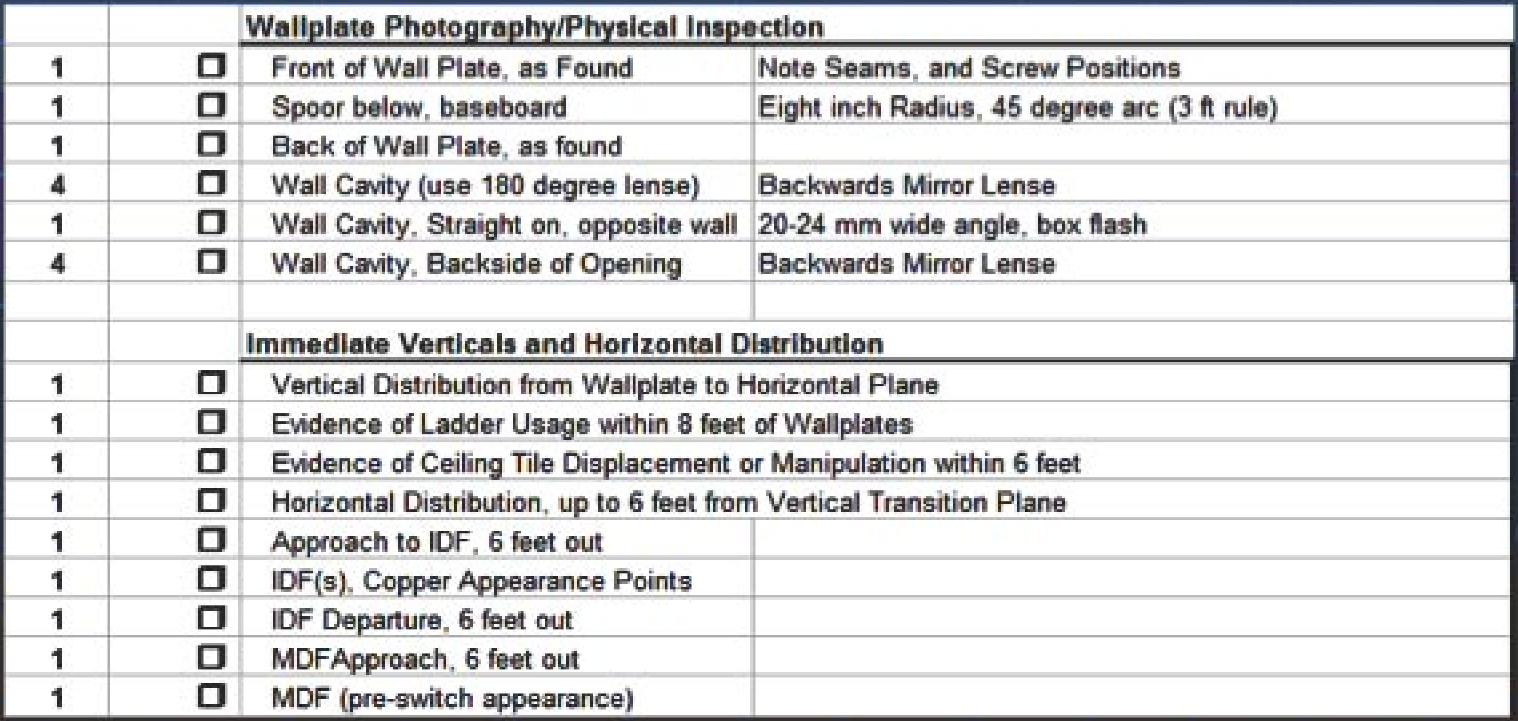
Instrument Physical Inspection



1	□	Open Phone PCB - Component Side	Large Format 8x10 Film + 8x10 contacts + 16x20 enlargment
1	□	Open Phone PCB - Solder Side	Large Format 8x10 Film + 8x10 contacts + 16x20 enlargment
1	□	Open Phone PCB - Transducers	Transducer Attachment Points, any trace of bypass?
1	□	Handset (Fully Opened Up)	Large Format 8x10 Film + 8x10 contacts + 16x20 enlargment
1	□	Hook Switch Electrcal Connection	any trace of bypass of manipulation?
1	□	External Connections (RJ11/RJ-45)	
1	□	Microphones and Speakers	are they original to the phone? Secondary devices?
1	□	Raw Chassis, Absent PCB's	
1	□	Power Supply, Wall Warts, etc (STU, STE exploits)	
		Instrument Accounting and Sealing	
1	□	Component Dates and Codes, Solder Points	
1	□	Resealing of Instrument, Wallplates, Copper Points	
1	□	Review of Tasking List (this document)	
1	□	Summarize Notes and Instrument Anomalies for Written Report	

Telephone Tasking Protocol

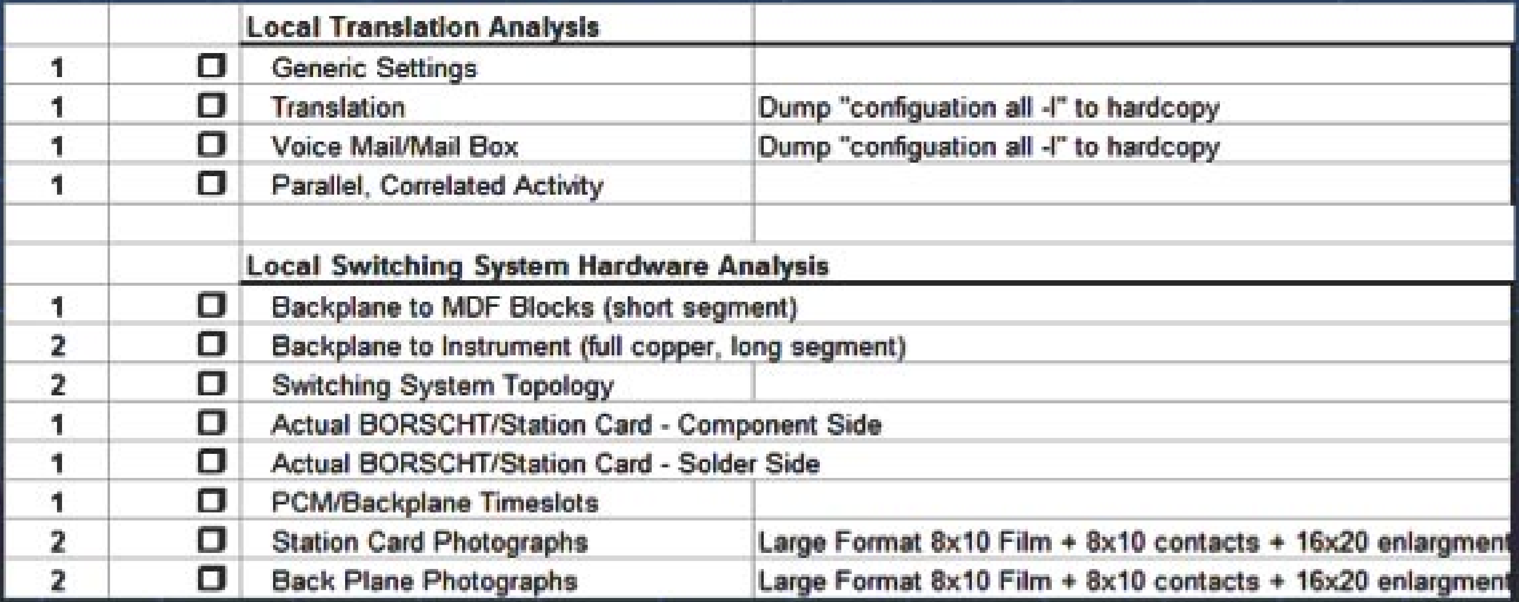
Wall Plate and Cavity Physical Inspections



		Wallplate Photography/Physical Inspection	
1	□	Front of Wall Plate, as Found	Note Seams, and Screw Positions
1	□	Spoor below, baseboard	Eight inch Radius, 45 degree arc (3 ft rule)
1	□	Back of Wall Plate, as found	
4	□	Wall Cavity (use 180 degree lense)	Backwards Mirror Lense
1	□	Wall Cavity, Straight on, opposite wall	20-24 mm wide angle, box flash
4	□	Wall Cavity, Backside of Opening	Backwards Mirror Lense
		Immediate Verticals and Horizontal Distribution	
1	□	Vertical Distribution from Wallplate to Horizontal Plane	
1	□	Evidence of Ladder Usage within 8 feet of Wallplates	
1	□	Evidence of Ceiling Tile Displacement or Manipulation within 6 feet	
1	□	Horizontal Distribution, up to 6 feet from Vertical Transition Plane	
1	□	Approach to IDF, 6 feet out	
1	□	IDF(s), Copper Appearance Points	
1	□	IDF Departure, 6 feet out	
1	□	MDFApproach, 6 feet out	
1	□	MDF (pre-switch appearance)	

Telephone Tasking Protocol

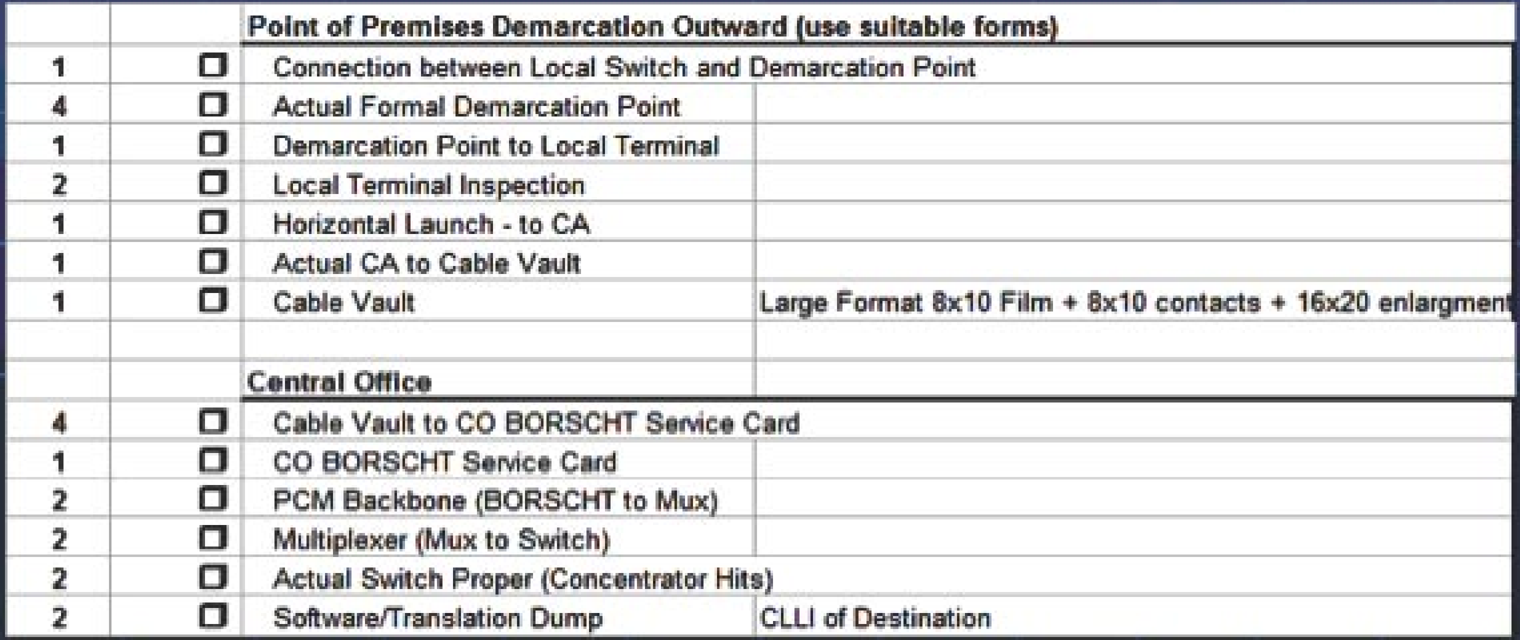
Switching System and Voice Mail Analysis



		Local Translation Analysis	
1	□	Generic Settings	
1	□	Translation	Dump "configuation all -l" to hardcopy
1	□	Voice Mail/Mail Box	Dump "configuation all -l" to hardcopy
1	□	Parallel, Correlated Activity	
		Local Switching System Hardware Analysis	
1	□	Backplane to MDF Blocks (short segment)	
2	□	Backplane to Instrument (full copper, long segment)	
2	□	Switching System Topology	
1	□	Actual BORSCHT/Station Card - Component Side	
1	□	Actual BORSCHT/Station Card - Solder Side	
1	□	PCM/Backplane Timeslots	
2	□	Station Card Photographs	Large Format 8x10 Film + 8x10 contacts + 16x20 enlargment
2	□	Back Plane Photographs	Large Format 8x10 Film + 8x10 contacts + 16x20 enlargment

Telephone Tasking Protocol

Outside Transmission System



		Point of Premises Demarcation Outward (use suitable forms)	
1	□	Connection between Local Switch and Demarcation Point	
4	□	Actual Formal Demarcation Point	
1	□	Demarcation Point to Local Terminal	
2	□	Local Terminal Inspection	
1	□	Horizontal Launch - to CA	
1	□	Actual CA to Cable Vault	
1	□	Cable Vault	Large Format 8x10 Film + 8x10 contacts + 16x20 enlargment
		Central Office	
4	□	Cable Vault to CO BORSCHT Service Card	
1	□	CO BORSCHT Service Card	
2	□	PCM Backbone (BORSCHT to Mux)	
2	□	Multiplexer (Mux to Switch)	
2	□	Actual Switch Proper (Concentrator Hits)	
2	□	Software/Translation Dump	CLLI of Destination

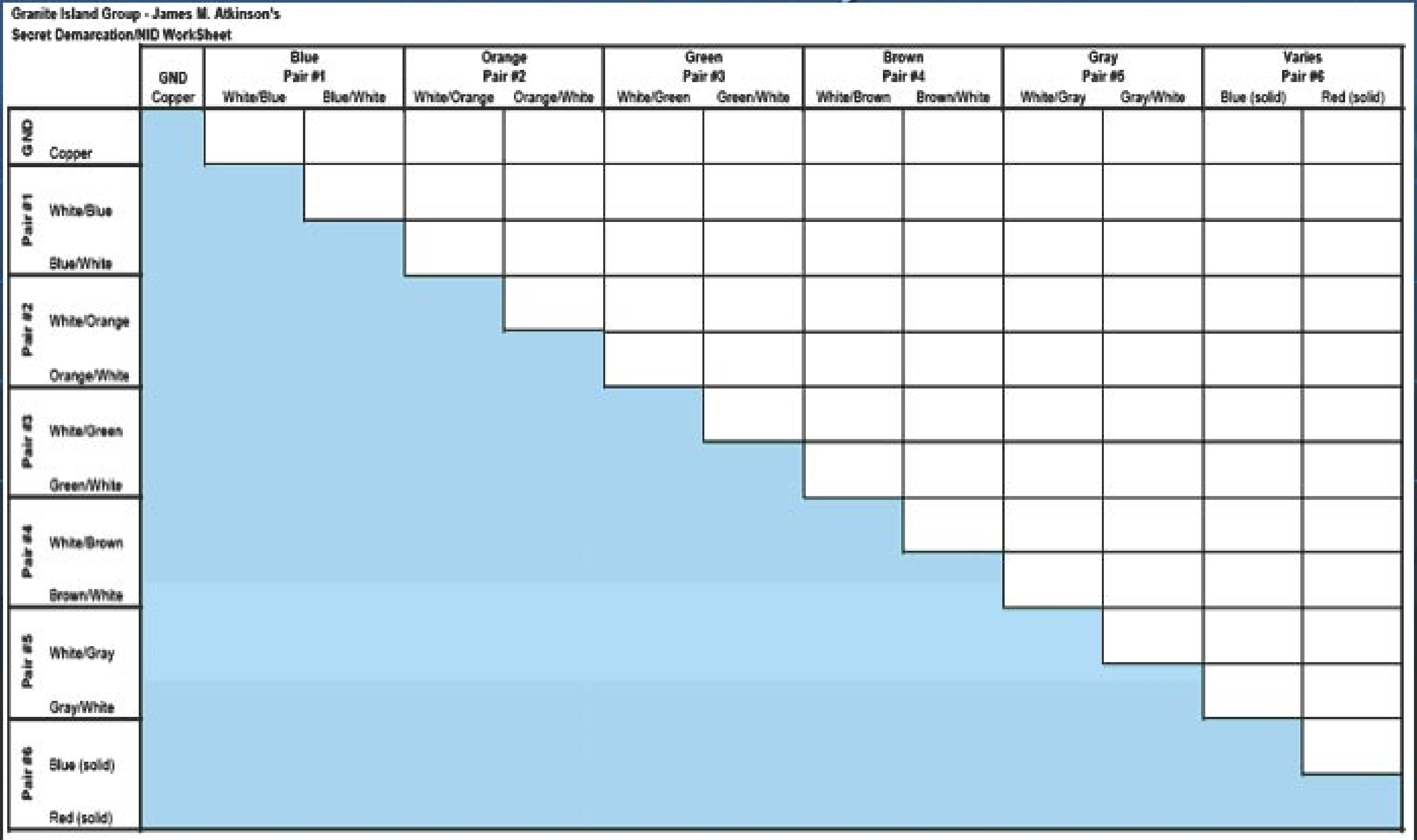
Telephone Tasking Protocol

Results = 168+ Pages on Any Phone

This Analysis is Usually Fully Automated

Residential NID Tests

Same Tests as Banjo Dance

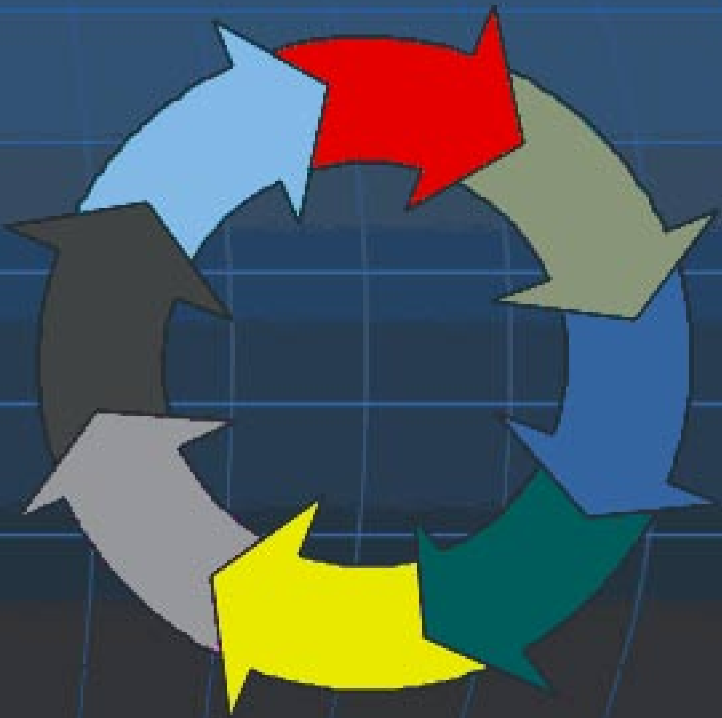


Granite Island Group - James M. Atkinson's
Secret Demarcation/NID WorkSheet

			Blue		Orange		Green		Brown		Gray		Varies	
		GND	Pair #1		Pair #2		Pair #3		Pair #4		Pair #5		Pair #6	
		Copper	White/Blue	Blue/White	White/Orange	Orange/White	White/Green	Green/White	White/Brown	Brown/White	White/Gray	Gray/White	Blue (solid)	Red (solid)
GND	Copper													
Pair #1	White/Blue													
	Blue/White													
Pair #2	White/Orange													
	Orange/White													
Pair #3	White/Green													
	Green/White													
Pair #4	White/Brown													
	Brown/White													
Pair #5	White/Gray													
	Gray/White													
Pair #6	Blue (solid)													
	Red (solid)													

Search Methodology

1. Phone on Desk
2. Station Cable
3. IDF
4. MDF
5. PBX
6. CO Lines
7. Multiplexers
8. Repeat, and Reverse



Caution

We have barely touched on:

1. How a phone can be bugged
2. How phone bugs are found

There are many other methods

You Must Pay Close Attention to Detail

Think about how YOU can find bugs

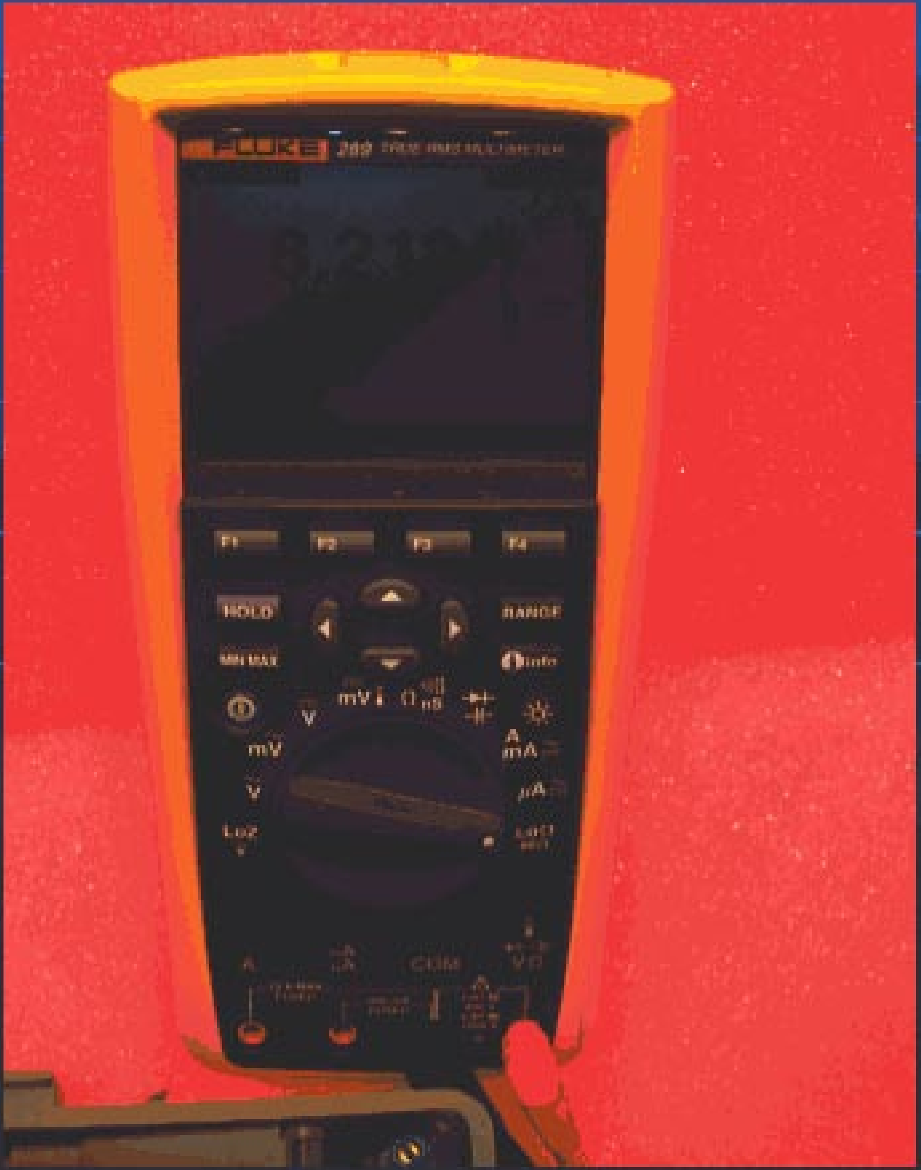
TSCM Mantra

Always Assume that the Phone is Bugged Until You Can Scientifically Prove Otherwise.

Bug/Wiretap Detection Tools

Premium Handheld Digital Volt Meter

Fluke 289



Bug/Wiretap Detection Tools

Premium Handheld Oscilloscope

Fluke 199CS

Bug/Wiretap Detection Tools

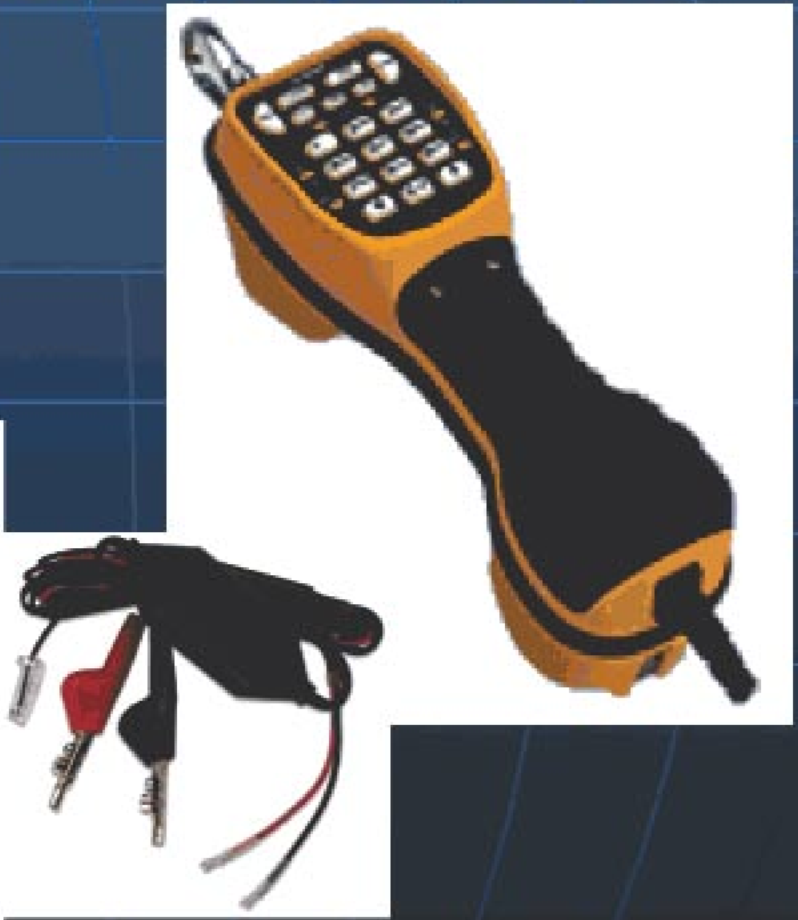
"Brown" Meter

Teledata 40010 & 40011
You need both models

Valuable for Hookswitch
Tests, and leakage test.

Bug/Wiretap Detection Tools

- Premium Craft Sets
- Fluke 44 and TS25
- P-Phone Adapter



Bug/Wiretap Detection Tools

- Tone Tracers

Bug/Wiretap Detection Tools

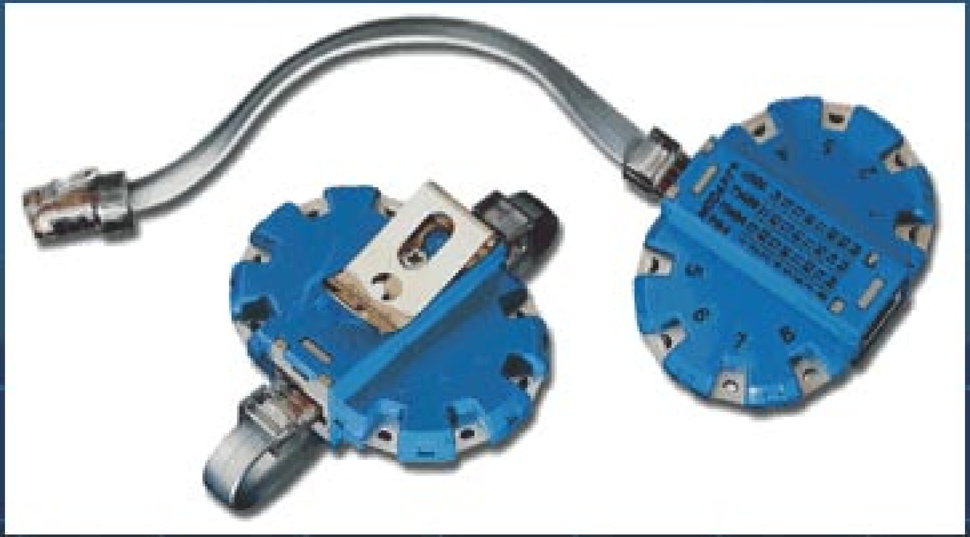
Numeric TDR
(Use with O'Scope)

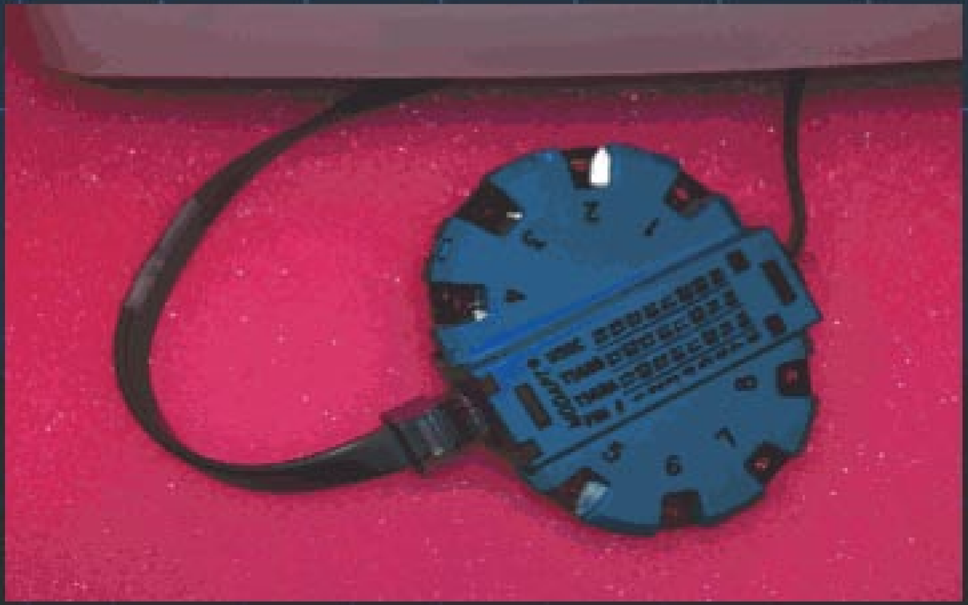
Bug/Wiretap Detection Tools

Wide Selection of Test Adapters

Bug/Wiretap Detection Tools

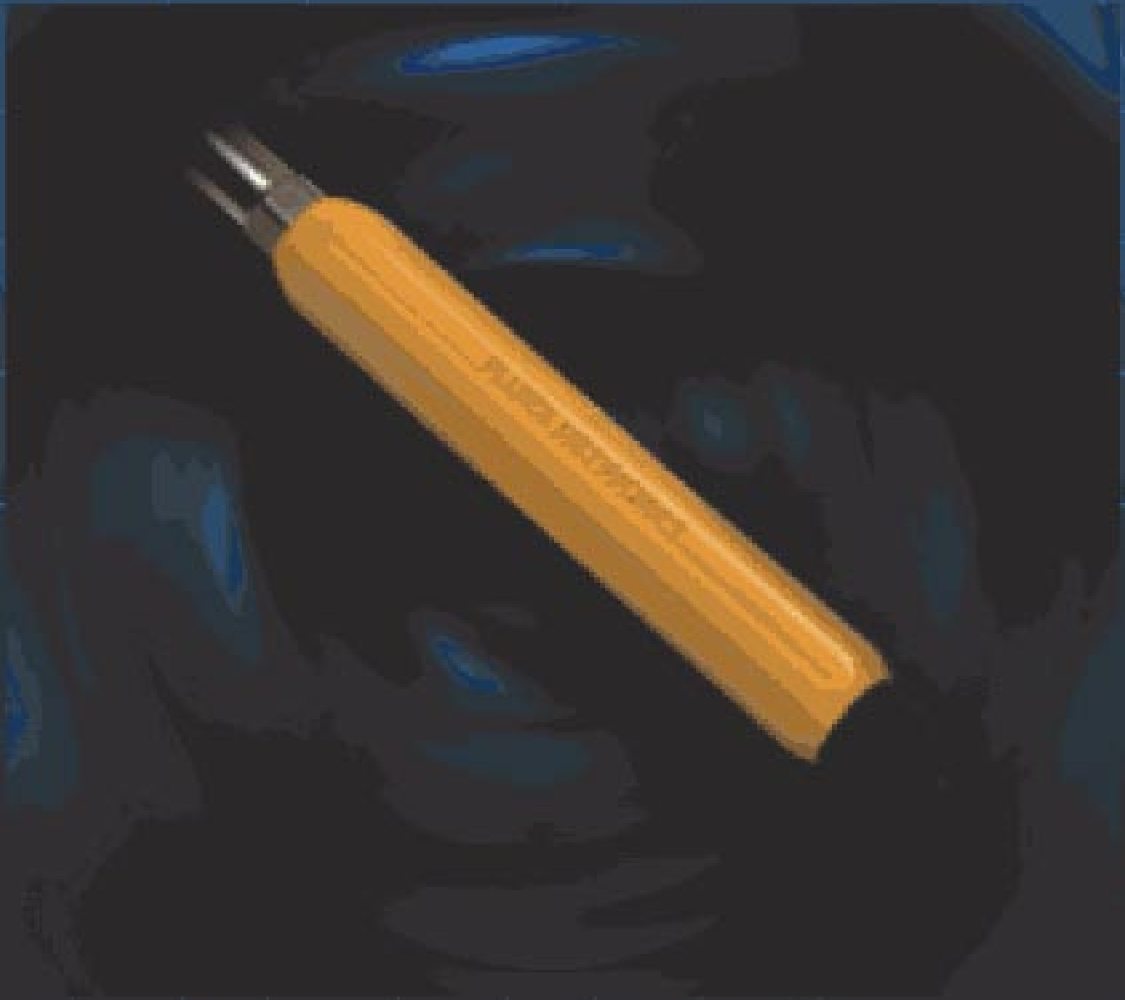
- Banjo





Bug/Wiretap Detection Tools

- Can Wrench



Bug/Wiretap Detection Tools

- Audio Amp with DC Bias Circuit

Bug/Wiretap Detection Tools

- Totally Avoid Spy Shop Toys
- Use Only Laboratory Grade Test Equipment and Procedures
- Take All the Time You Need
- Never Miss the Details, Ever

Bug/Wiretap Detection Tools

A comprehensive test equipment and tool list for finding wiretaps may be found on the following website:

www.tscm.com

The site has over 65,000 printed pages on it regarding TSCM, Bugs Sweeps, and Wiretap Detection

Jim’s Cardinal Rule

Convenience and Privacy are Inversely Proportional™

Questions?

Thank You

Please Keep In Touch

www.tscm.com