WHO IS HERE TODAY?

CESI Tradecraft

CLANDESTINE ELECTRONIC SURVEILLANCE / INTERCEPT

TSCM

TECHNICAL SURVEILLANCE COUNTERMEASURES

Level of Defensive Effort Increases Depending Upon Risk and Demands Regarding Security

WRONG!

Lose Preconceived Notions

Make NO Assumptions along these lines of reasoning

All Threats Below plus Foreign Industrial Espionage
Foreign Competitors Nation States

All Threats Below, plus Terrorist, Vengeful Grudge Carrier, Coworker Vying for Promotion

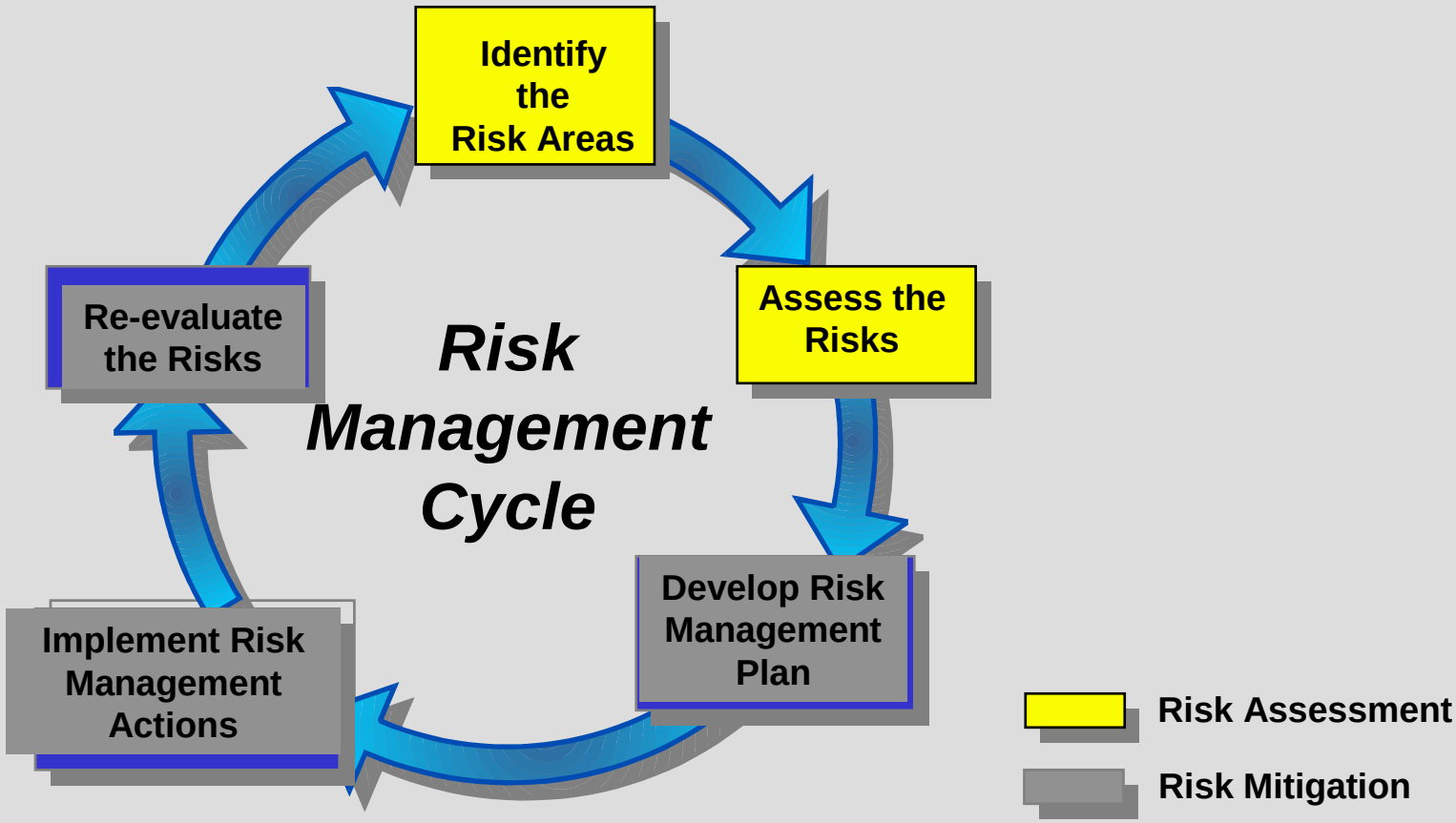
All Below, plus Competitor Intelligence Agent
Insider / Shareholder Activities, Labor Disputes

Jealous Spouse / Lover, Ex-Adversaries
Stalker, Extortionists – perhaps business related,
Kidnappers, Prurient interest

- What is RISK MANAGEMENT?
  - The process concerned with identification, measurement, control and minimization of security risks in information systems to a level commensurate with the value of the assets protected.

(Definition from National Information Systems Security (INFOSEC) Glossary, NSTISSI No. 4009, Aug. 1997)

- Introduction to Risk Management



"Lesson 5, Risk Management", Operational Information Systems Security Trainee Guide (National Cryptologic School)

FIRST ORDER: IDENTIFYING ASSETS

You know what needs to be kept “Close to the Vest”

BUT MUCH WILL NOT BE SO APPARENT

Defining Value Defines the (potential) Adversary

Defining the Adversary (motives) defines the Victim

- CSEI as a Prelude to Cyber-Based Attack – Reconnaissance
- Define Value in Terms of Worth to Opposition
- MONEY has Value and, to some, is worth stealing
  - “look” of a commonly used document
- Social Calendar
- Sabotage as Motive
- Revenge as Motive
- “Cover” Unrelated Crimes Alert of Suspicion
- Prurient Interest

*

- RISK

  - The likelihood that a particular threat using a specific attack, will exploit a particular vulnerability of a system that results in an undesirable consequence.

threat

(Definition from National Information Systems Security (INFOSEC) Glossary, NSTISSI No. 4009, Aug. 1997)

- THREAT

-Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or the denial of service.

(Definition from National Information Systems Security (INFOSEC) Glossary, NSTISSI No. 4009, Aug. 1997)

- THREAT QUESTION:

-Should you consider the ***vias*** of information and interface to be part of an information system?

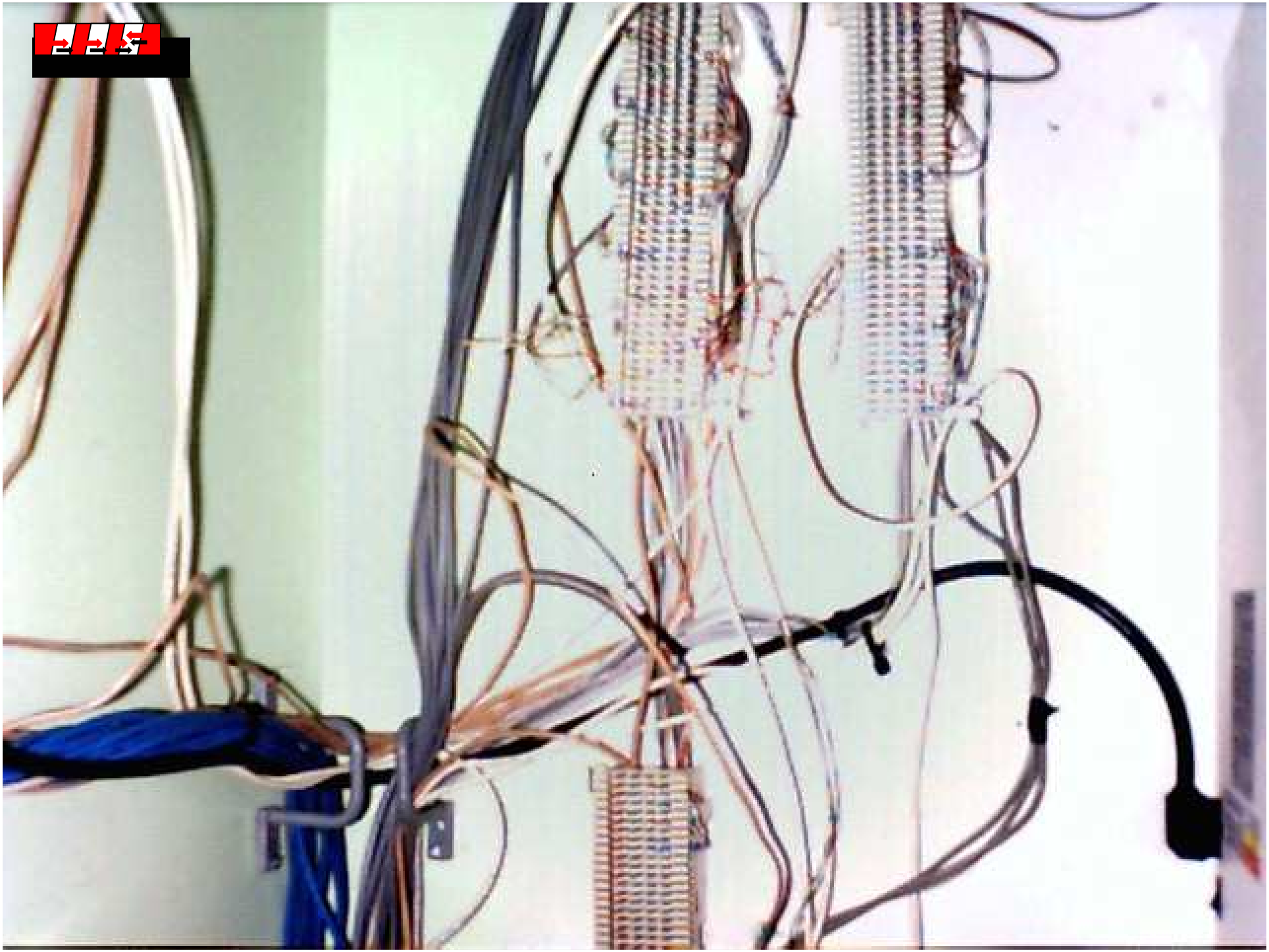
-Computer operator input/output devices

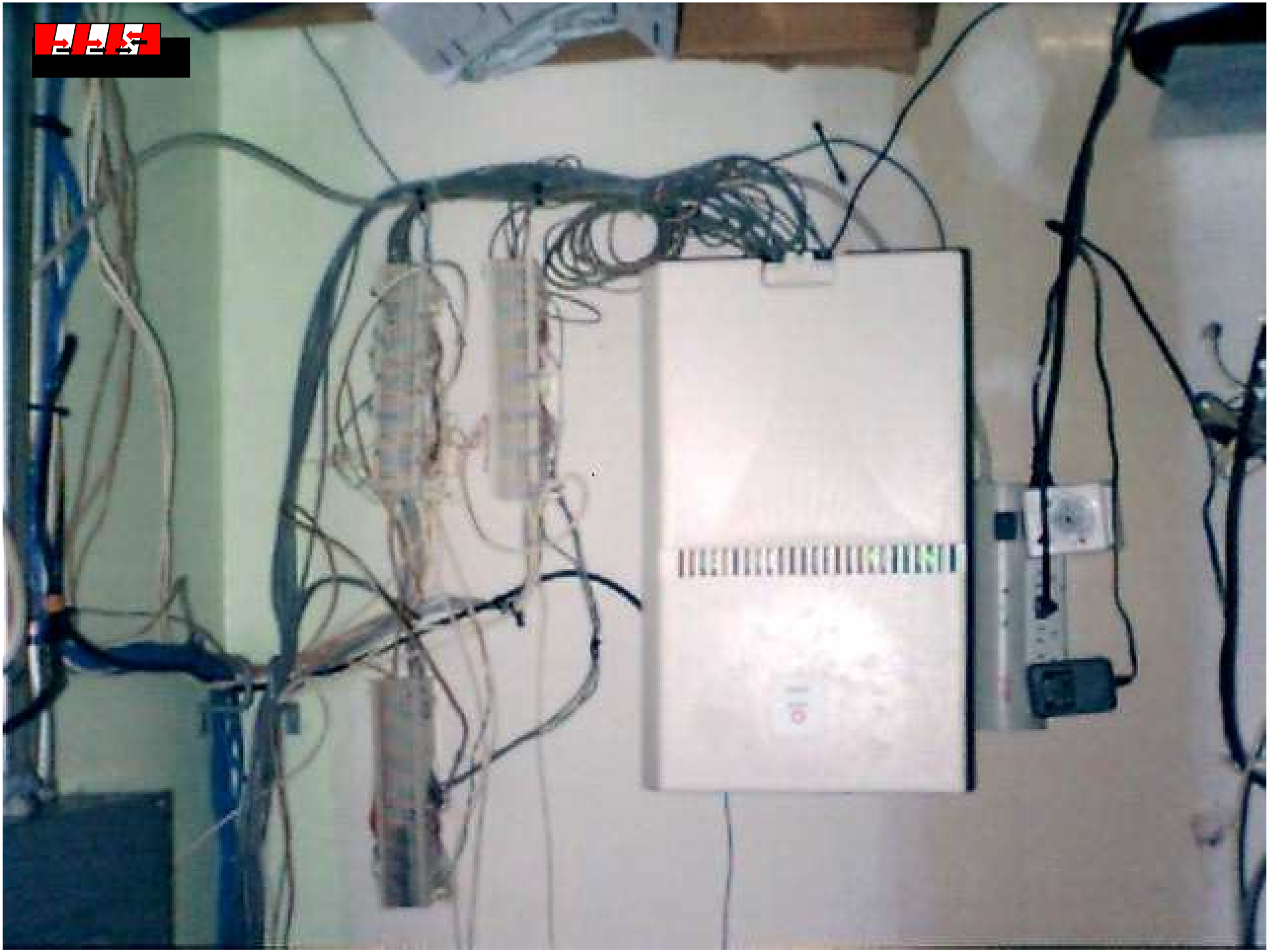
-LAN cabling

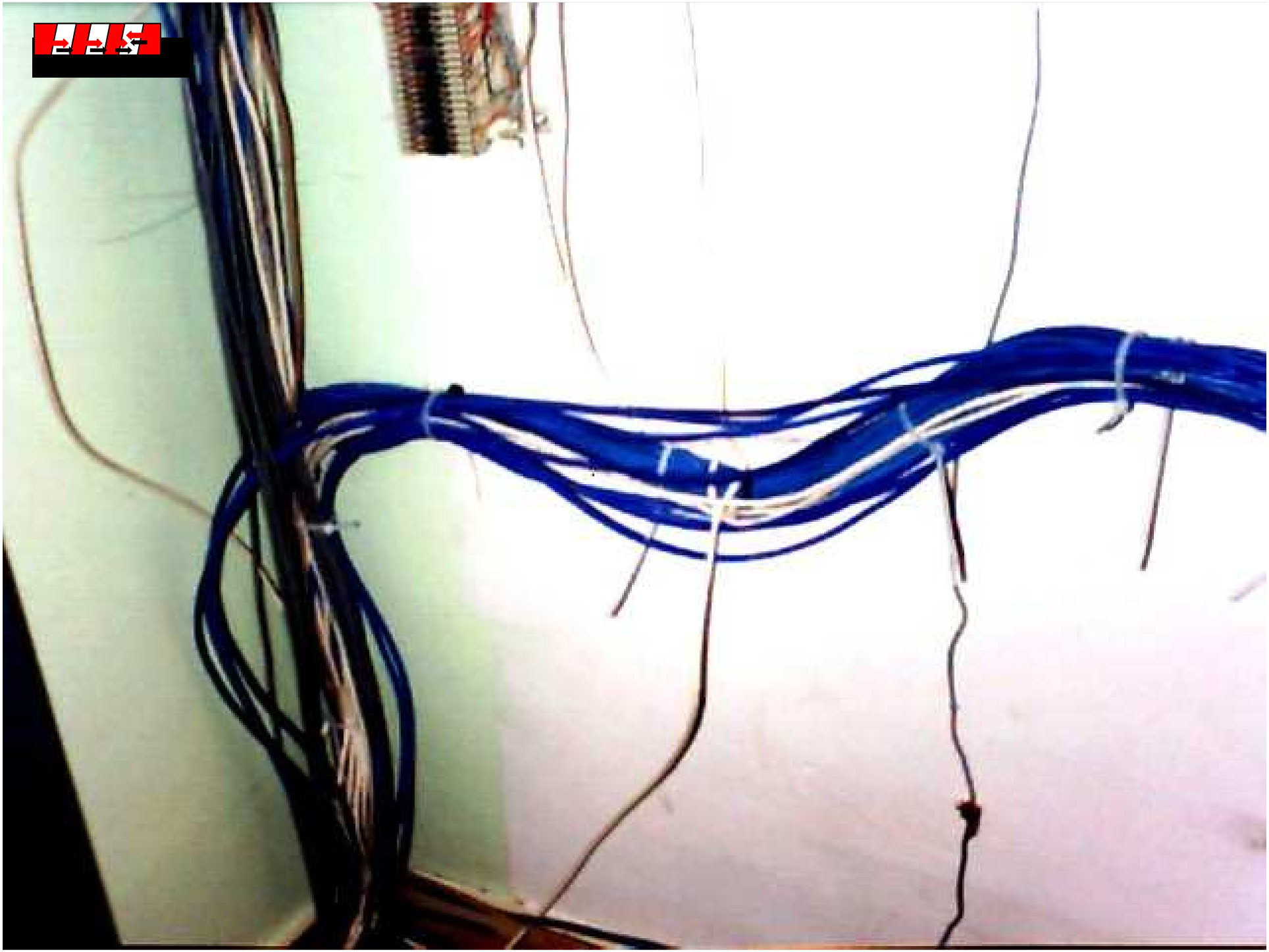
-Telecom (POTS, T1, CLEC over broadband, Optical Fiber)

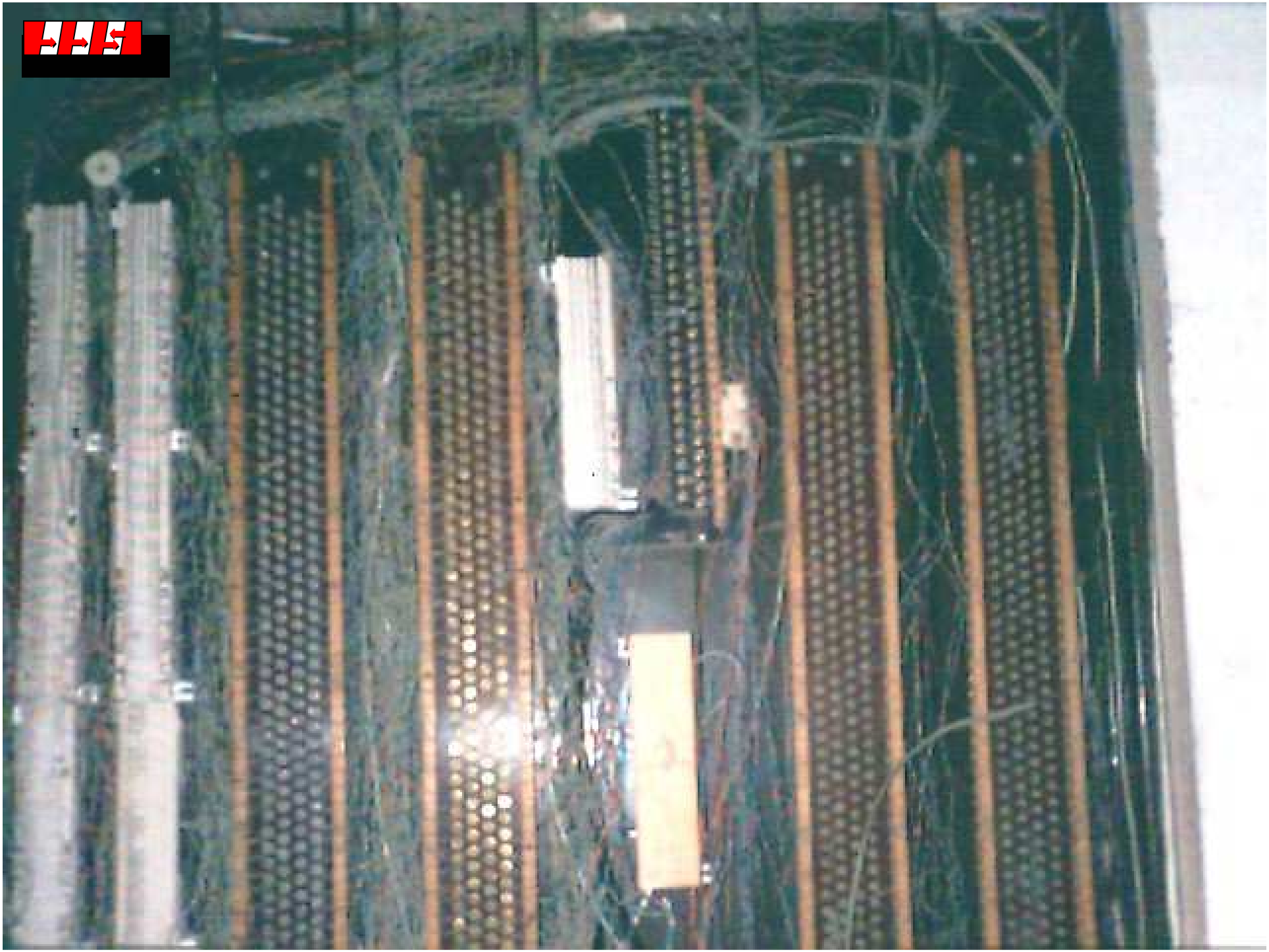
-Miscellaneous (Photocopiers, Teleconference Wiring)

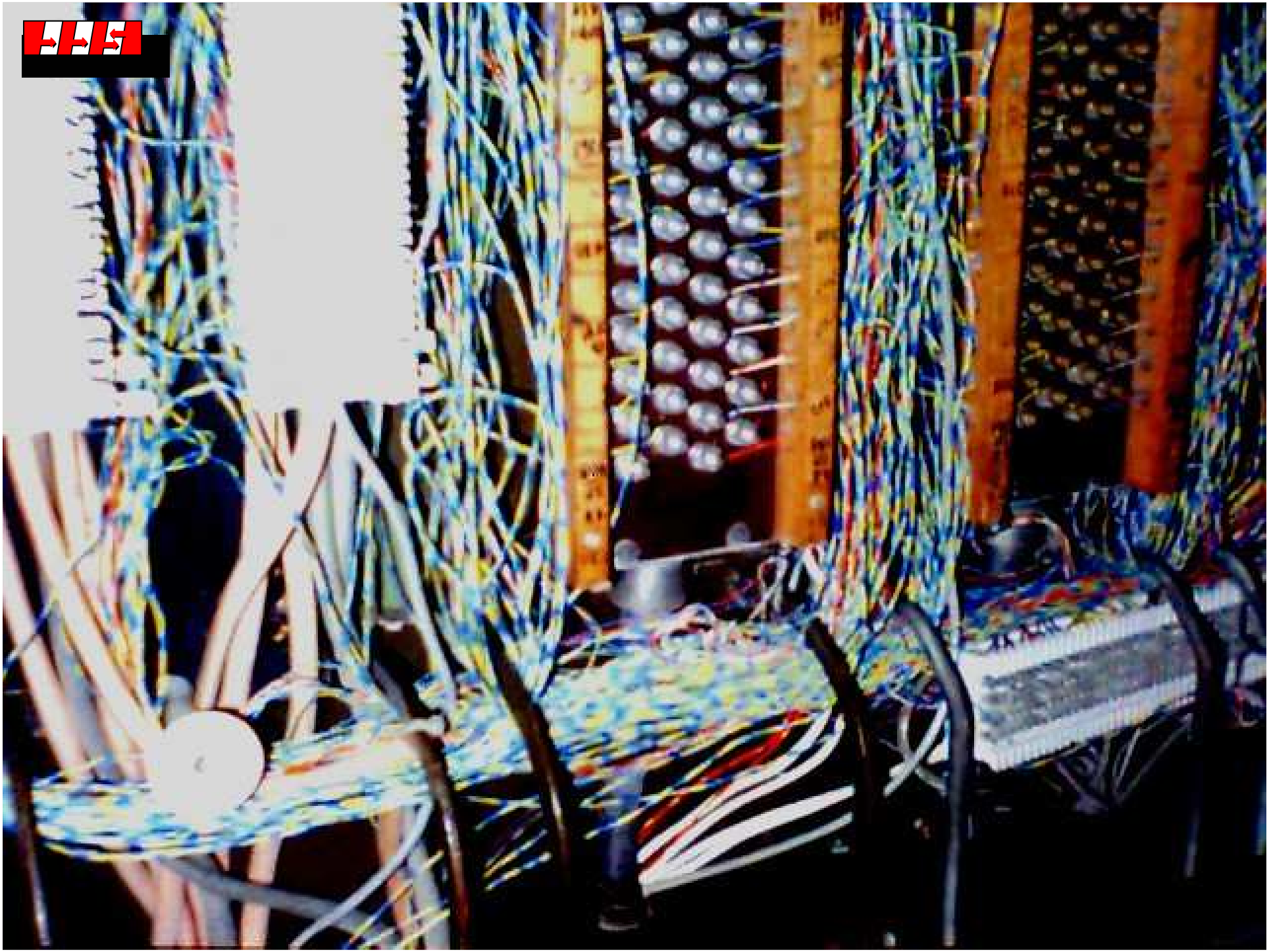
-Air

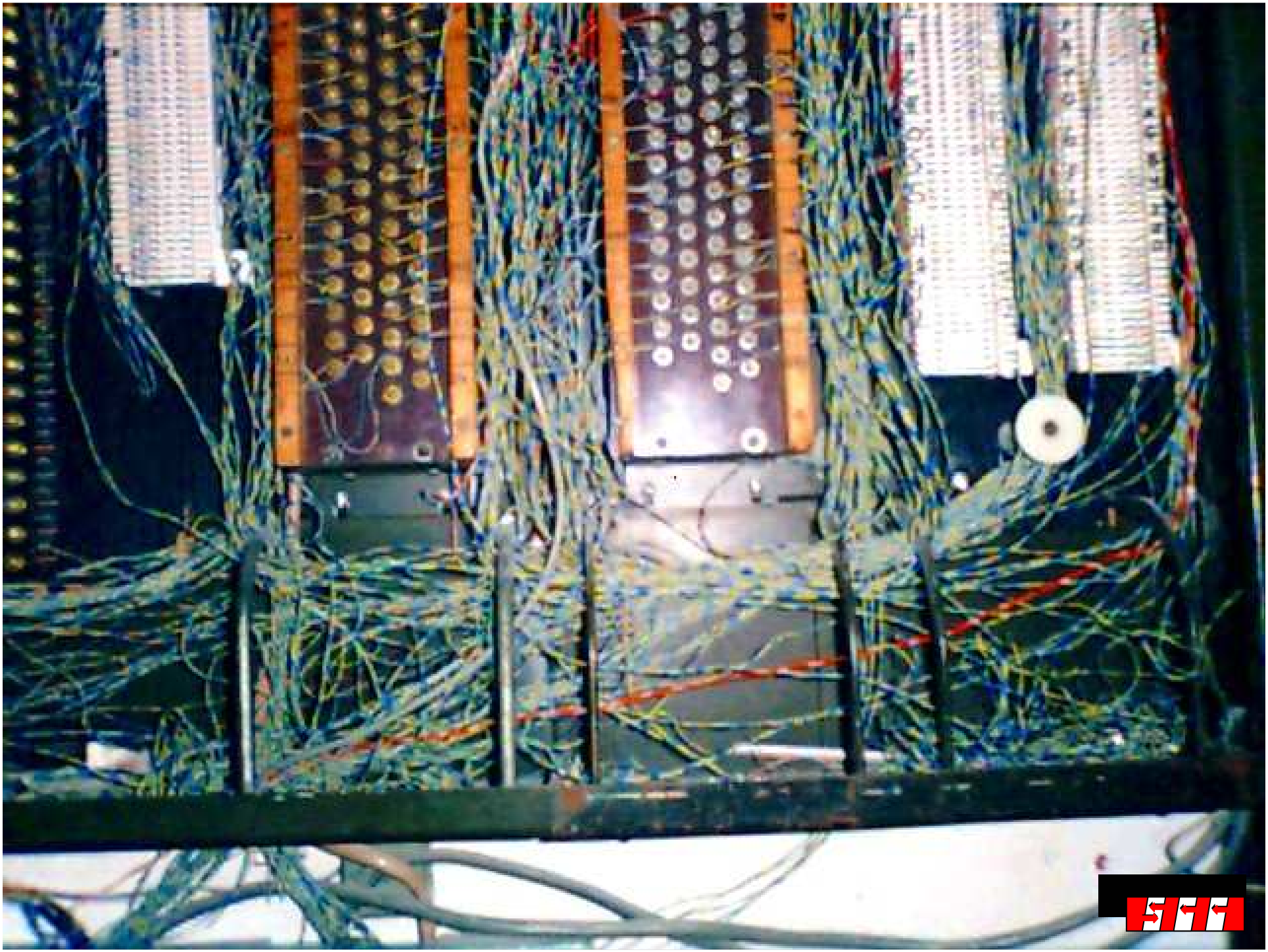


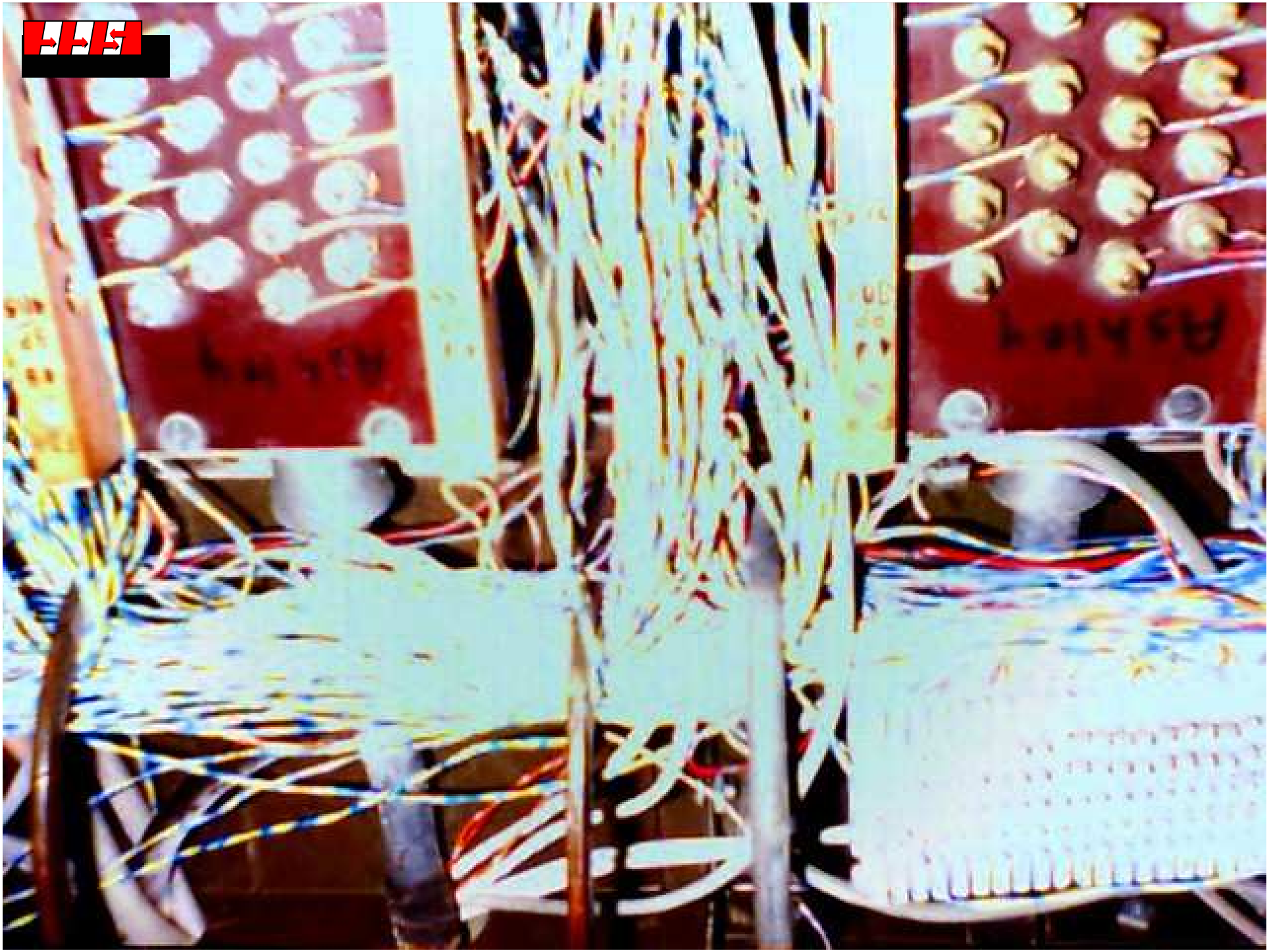




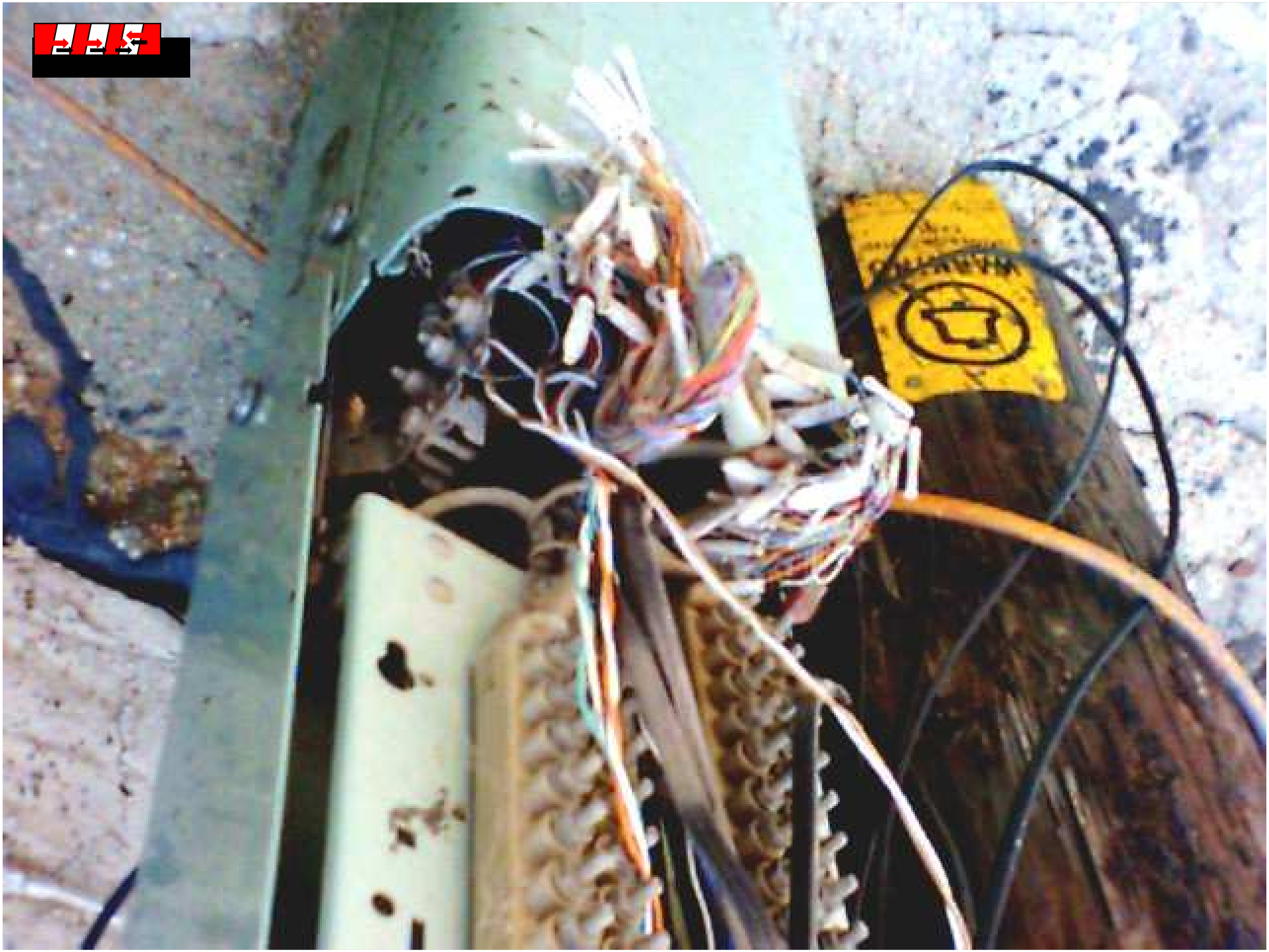


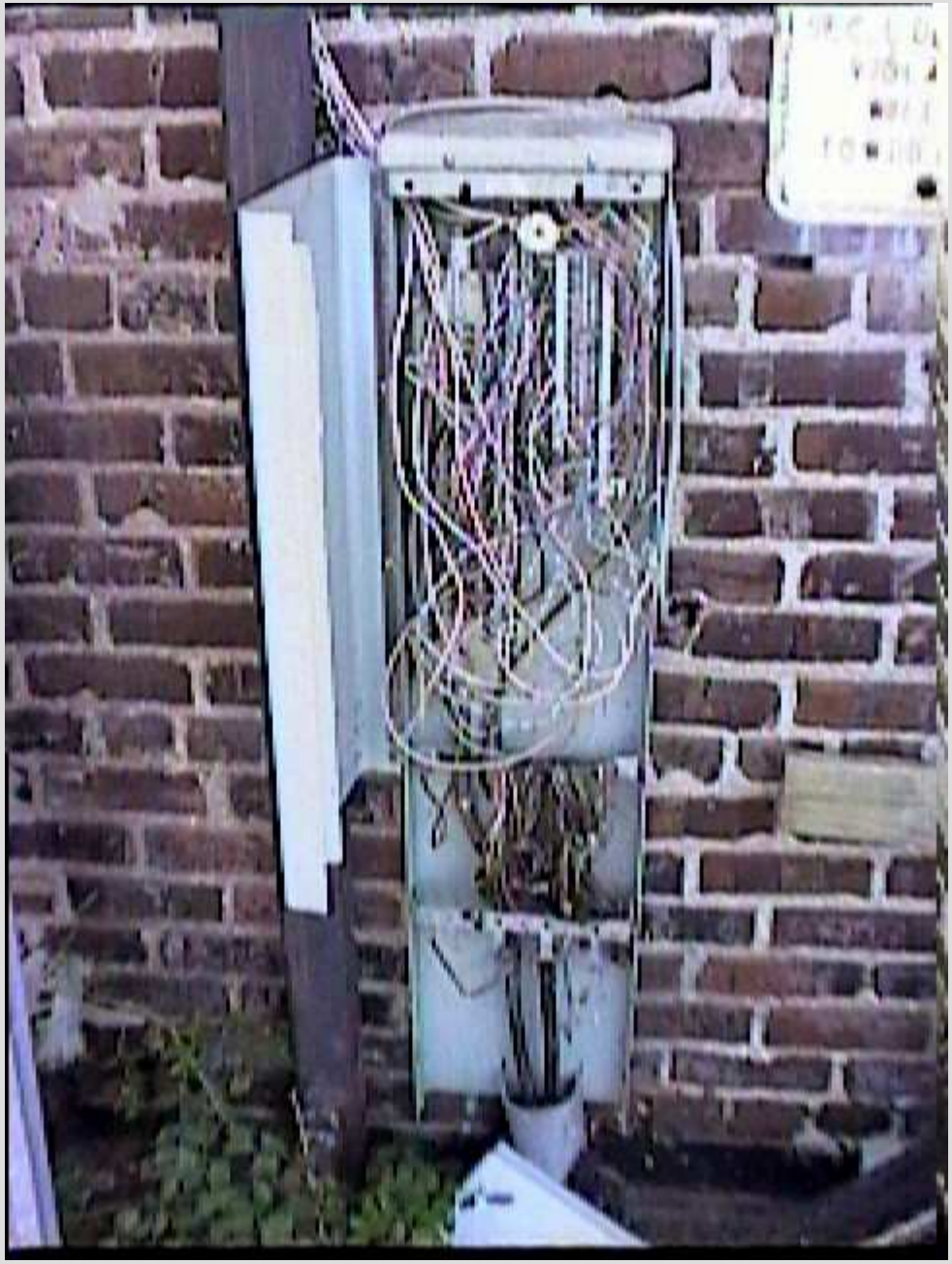






T.H. Gee
Sharp





Outdoor “B” Box

One of the “Fingers” of TELCO Distribution System

Commonplace in Both Commercial and Residential Areas

Capacity of 500 Single Subscriber Loops

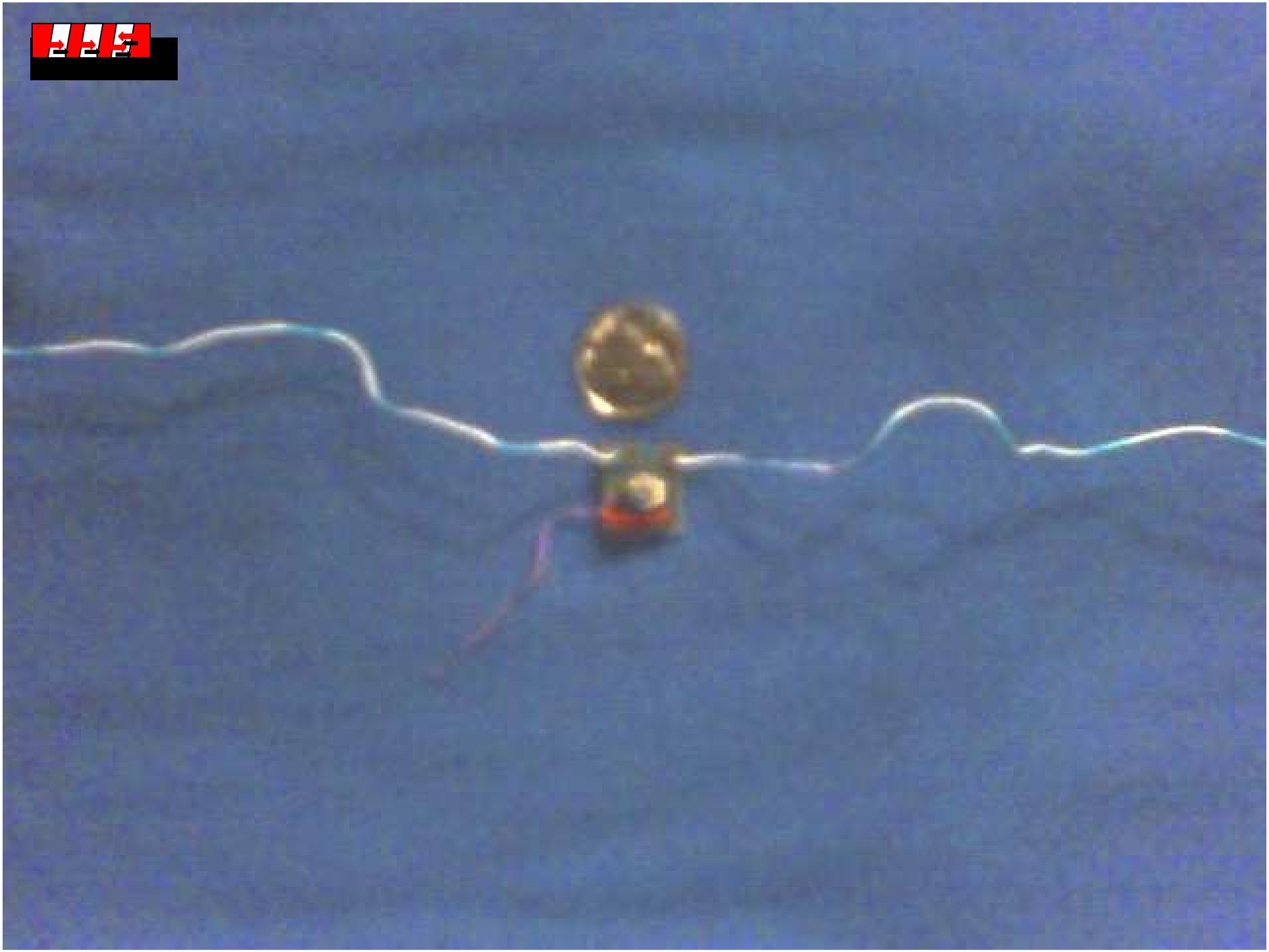
Common Appearance

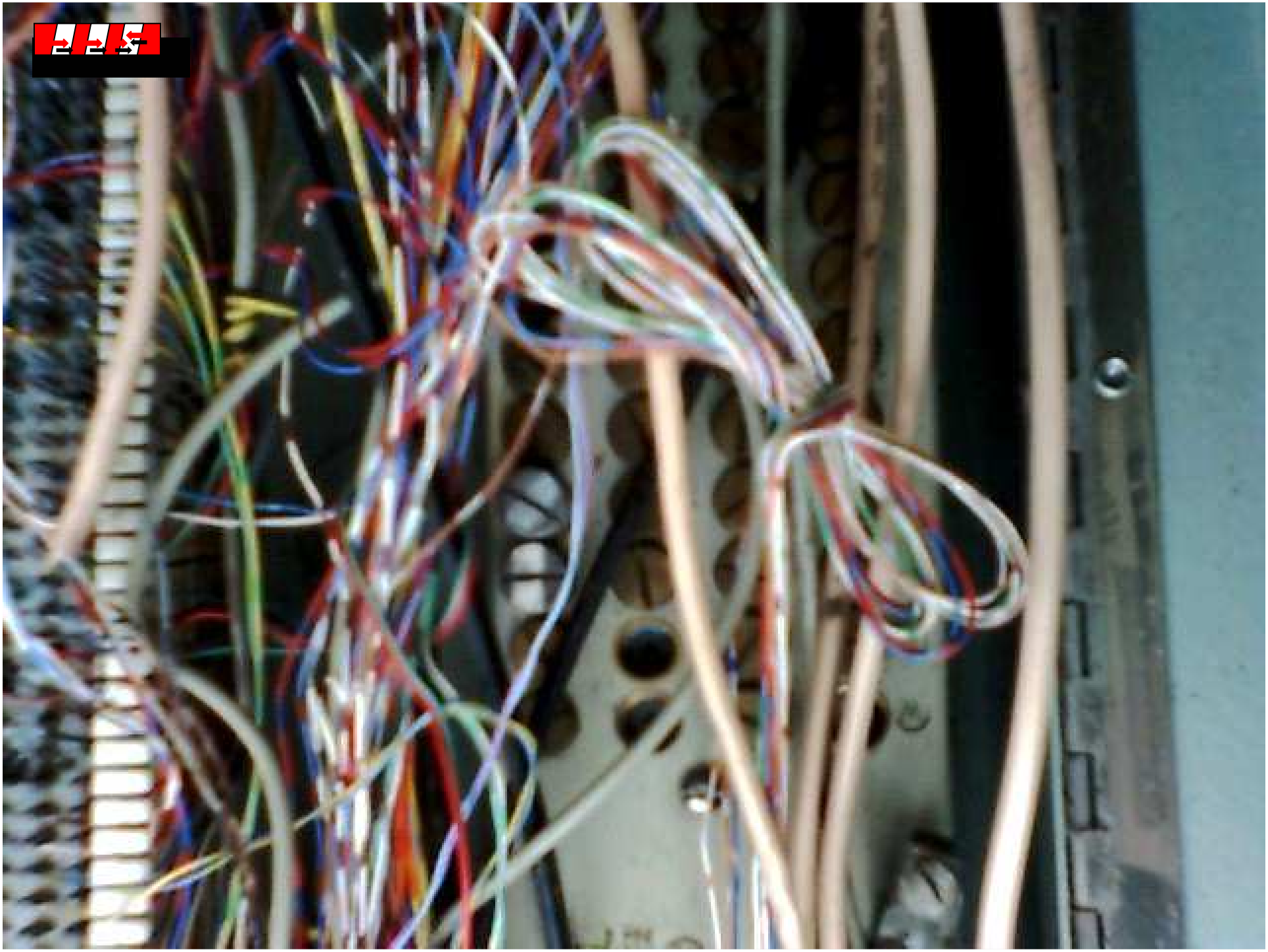
Close up view which highlights a few of many plastic splice connectors

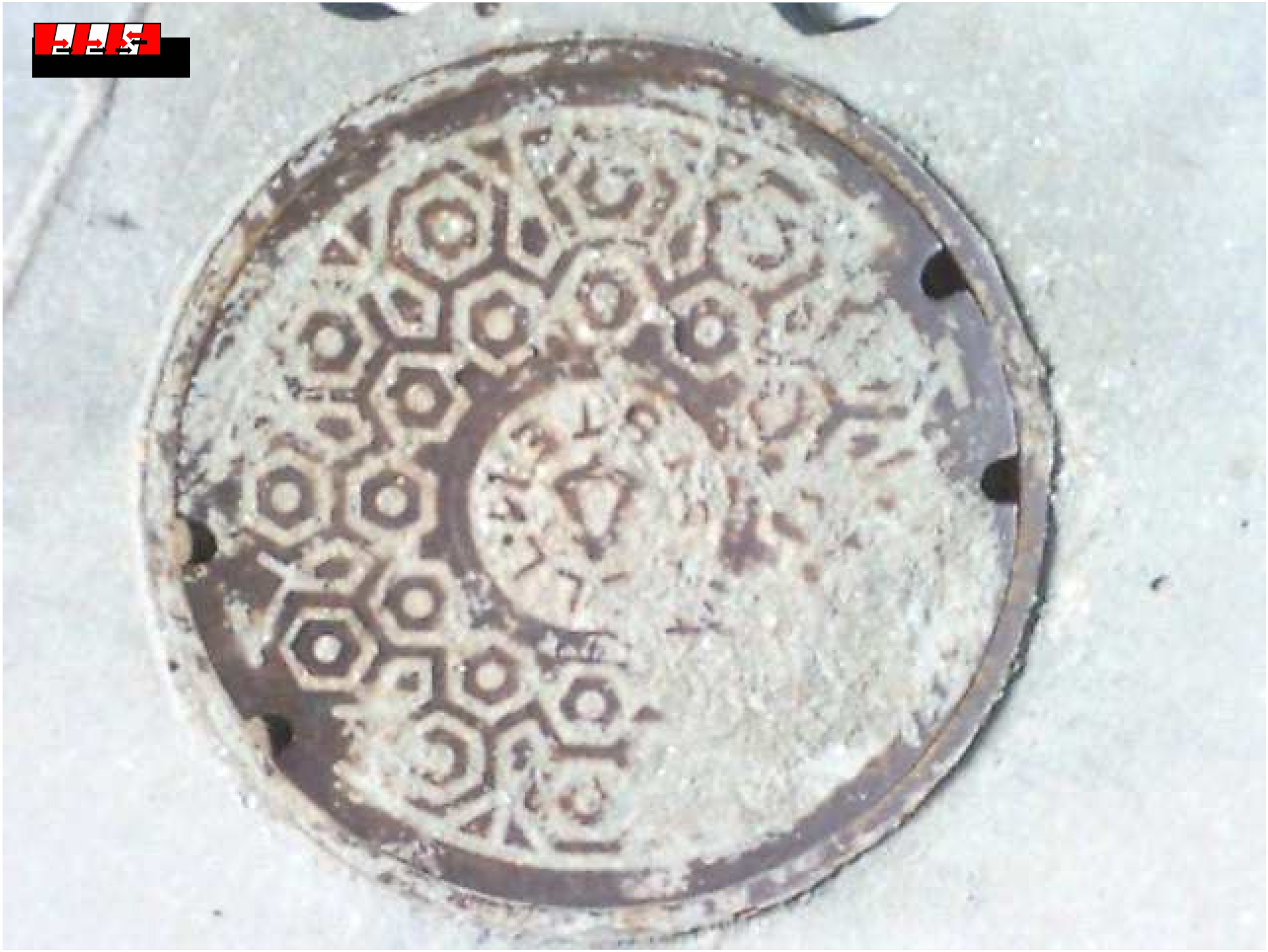
Wiretap devices are easily hidden -

RF Transmitters are disguised within Standard Splice Connector

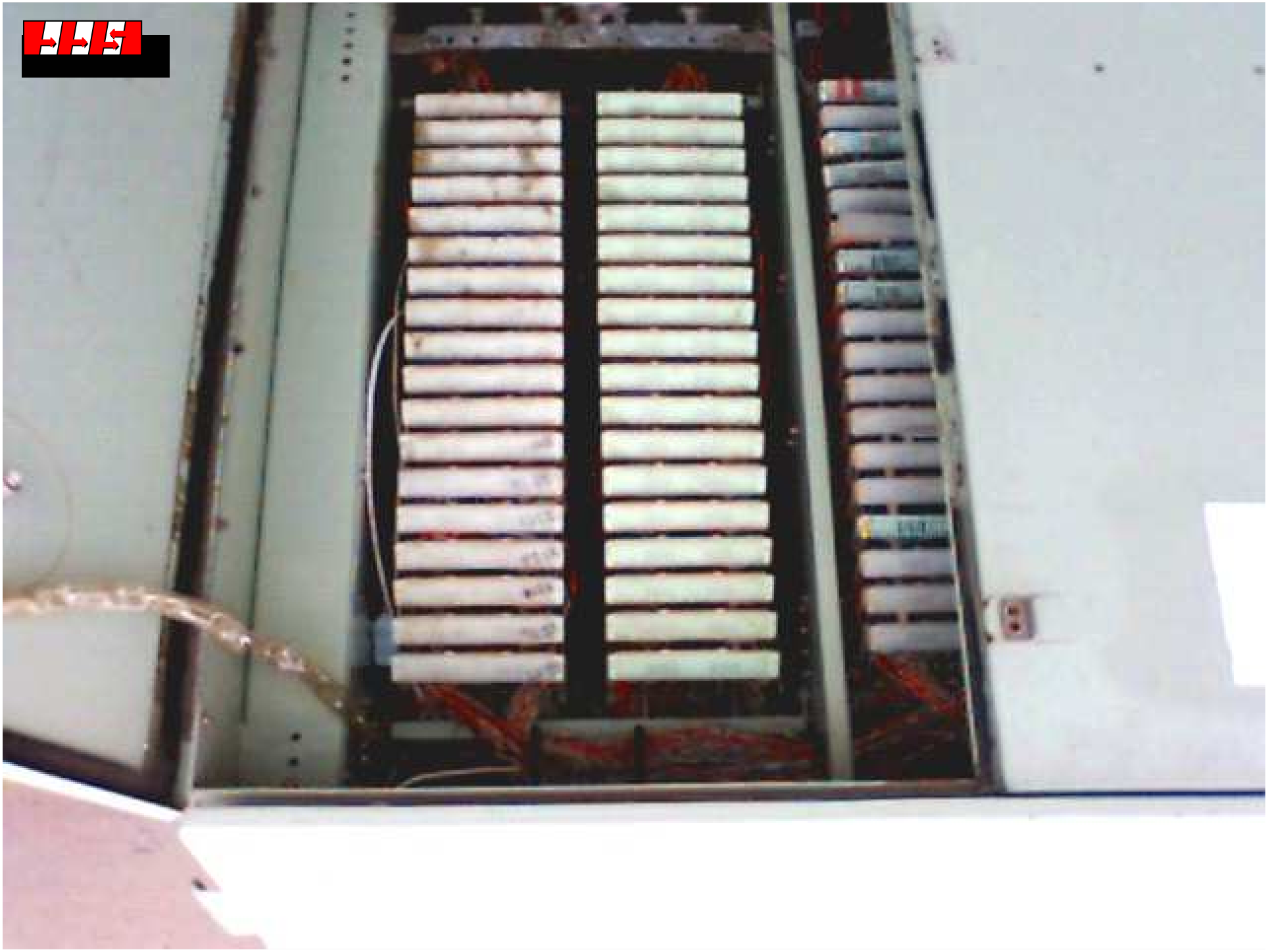
UR and/or UG CONNECTORS

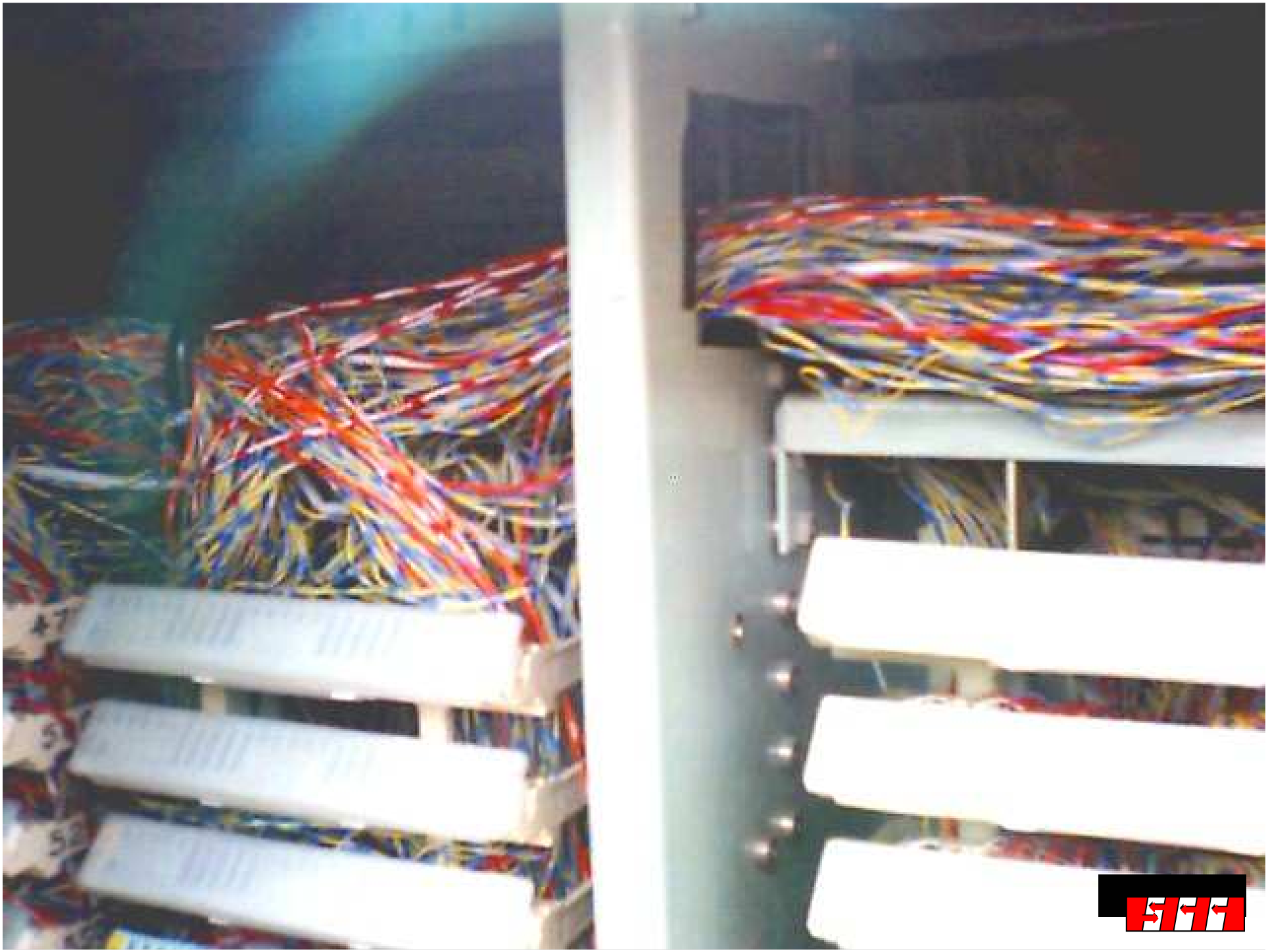


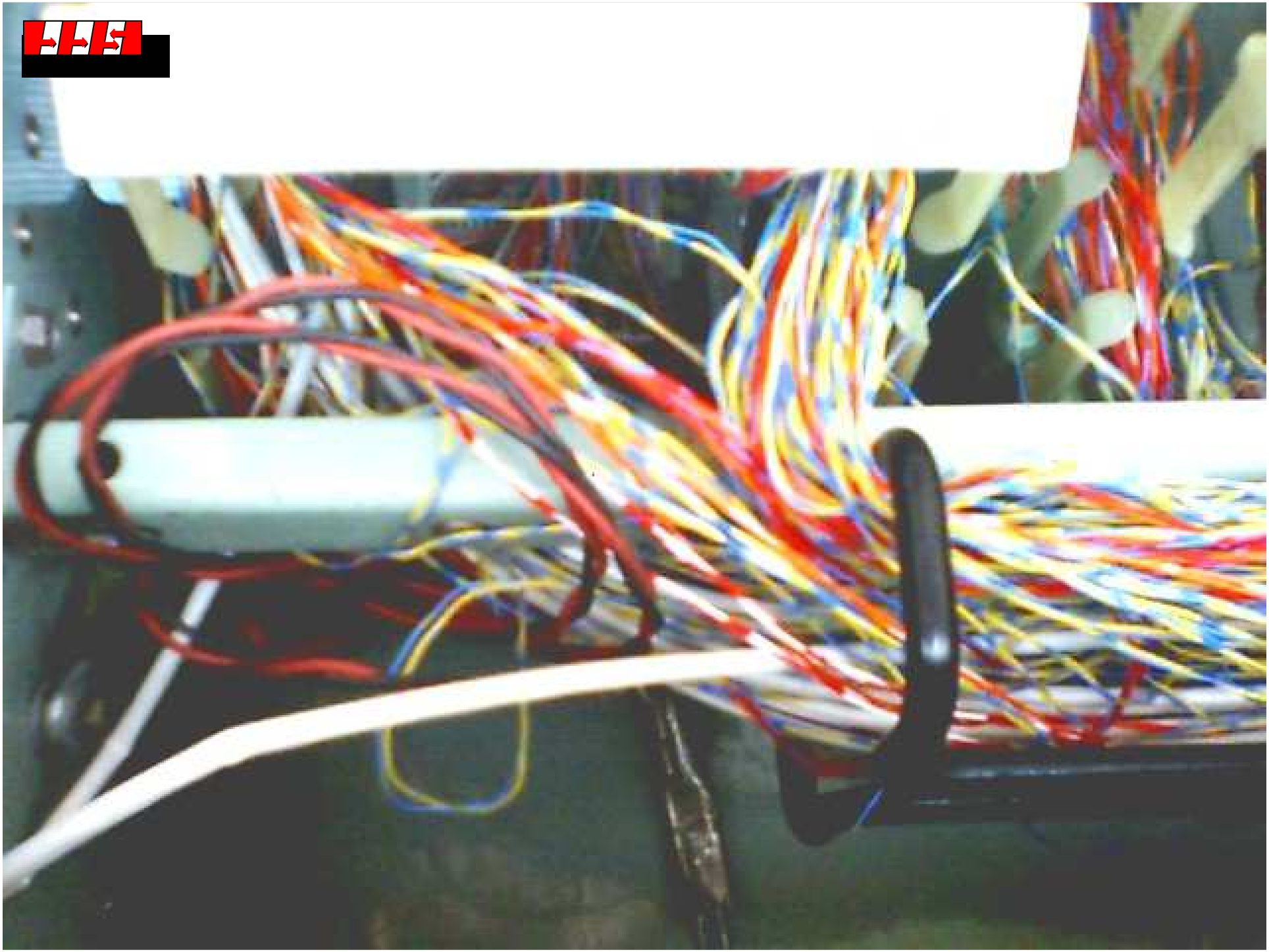




WEST SNOHO
COMMUNICA







Parallel Telephone XMTR

But so far, these examples are only analog (POTS) and ethernet (LAN)…

WE USE T-1, So HA HA HA!

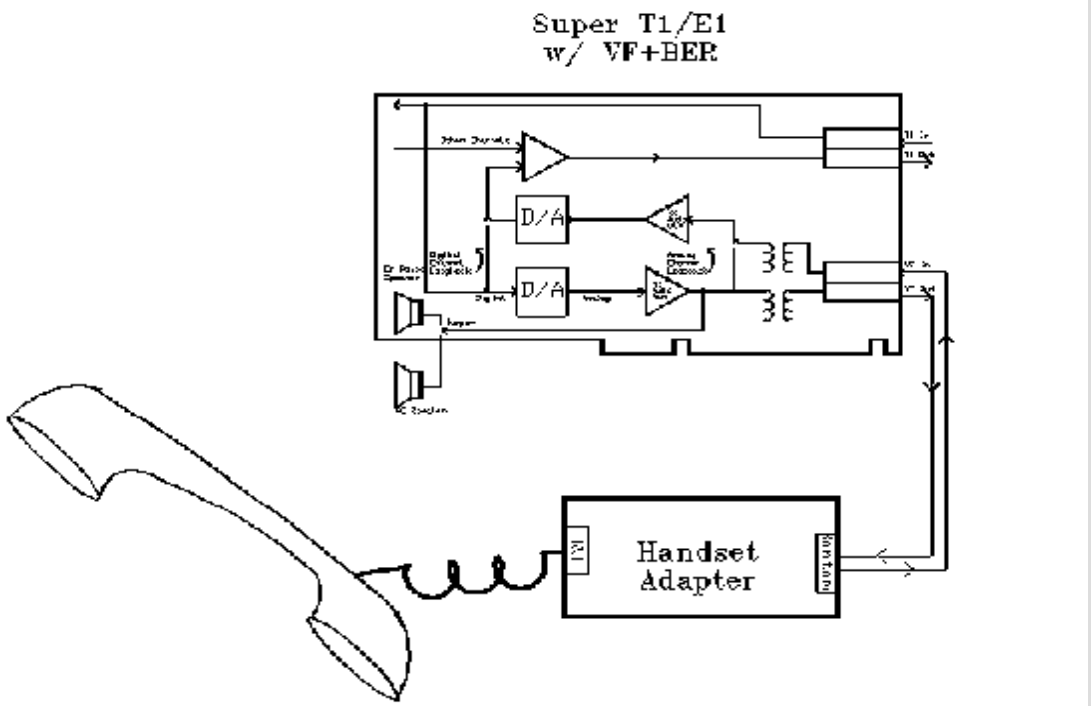
HOW ABOUT THAT?

Eh, Dougy Boy?

You so rudely ask


KFAW-418
A, 1-75
FH 202, 176-200
A, 101-175
FA02, 276-400
A, 201-275
FH 202, 176-200
A, 301-375
FH 202, 376-400
A, 401-418


Telephone Handset Adapter for T1, E1, T3
from GL Communications, Inc.



Voice input and <u>output</u> to/from T1/E1 timeslots

Voice record and playback capability in conjunction with direct-to-disk software

Calling capability on *any timeslot*

Drop and insert capability

Tekelec Protocol Analyzer

Allows you to passively monitor data on a data line without affecting the traffic – interpret the traffic.

X.25, PSH, SNA, ASYNC, BSC, DPNSS, and more

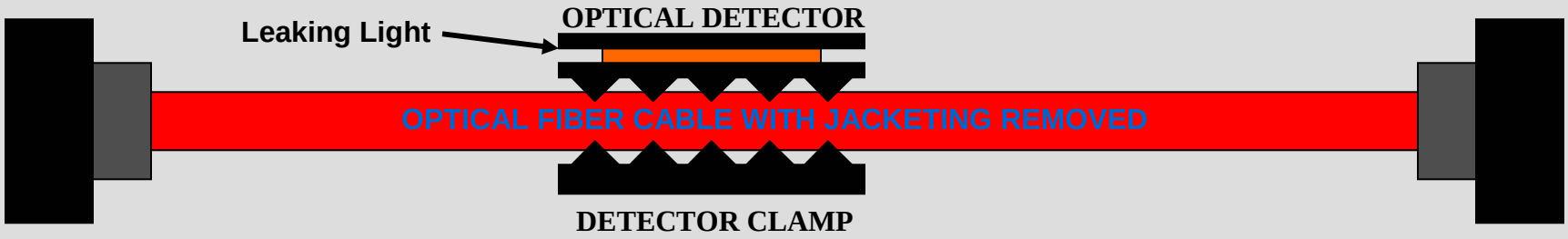
Allows you to insert/extract voice frequency signals to/from selected channels. Allows voice path or intercept capabilities.

ISDN (PRI & BRI),

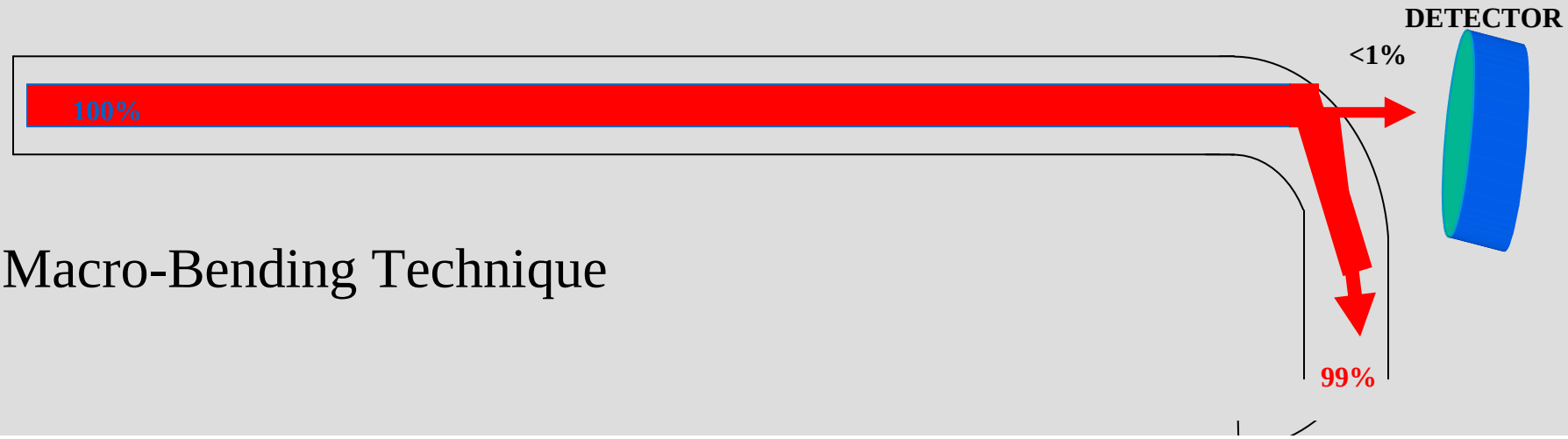
Monitor these International Protocols

SS #7, DASS 2, DMI mode 2, V.120, DDCMP, X.21, more

OPTICAL FIBER?



Bleeding of Light by clamp-induced Micro-Bending



Macro-Bending Technique

Optical Fiber Identifier

Detector Type	**InGaAs**
Spectral Range	**820 to 1600 nm**
Specified Wavelength	**1310, 1550 nm**
Insertion Loss	**0.2 dB @ 1310 nm**
Tone Detection	**2000Hz**
Fiber Type	**Jacketed Ribbon**
Power	**9 VDC**
Size	**8.5”H x 1.5”W x 1.1”D**

For non-invasive Discrimination of Signals in Fiber Optic Cables Without Disrupting Service

Low induction bend loss

Indicates direction and signal

Fiber Optic Clip-on Coupler

- THREAT QUESTION RESTATED

-In other words…

From an ISS Viewpoint…

Some information assets are deemed worthy of your strongest security efforts while residing on servers in the ***"at rest"*** state…

Why is that **same valuable information** afforded **NO protection** when it is ***"in motion"***?

*

- RISK

likelihood

The likelihood that a particular threat using a specific attack, will exploit a particular vulnerability of a system that results in an undesirable consequence.

(Definition from National Information Systems Security (INFOSEC) Glossary, NSTISSI No. 4009, Aug. 1997)

- Definition of Likelihood
  - LIKELIHOOD of the threat occurring is the estimation of the probability that a threat will succeed in achieving an undesirable event.

(Definition from National Information Systems Security (INFOSEC) Glossary, NSTISSI No. 4009, Aug. 1997)

- Considerations in Assessing the Likelihood of Threat

  – Presence of threats
  – Tenacity of threats
  – Strengths of threats
  – Effectiveness of safeguards

(Definition from National Information Systems Security (INFOSEC) Glossary, NSTISSI No. 4009, Aug. 1997)

*

- RISK

  - The likelihood that a particular threat using a specific attack, will exploit a particular vulnerability of a system that results in an undesirable consequence.

attack

(Definition from National Information Systems Security (INFOSEC) Glossary, NSTISSI No. 4009, Aug. 1997)

- ATTACK
  - An attempt to gain unauthorized access to an information system's services, resources, or information, or the attempt to compromise an information system's integrity, availability, or confidentiality, as applicable.

(Definition from National Information Systems Security (INFOSEC) Glossary, NSTISSI No. 4009, Aug. 1997)

ASSESSING AN ***INTERCEPT*** ATTACK

Intercept Threat Assessment is MORE than identifying assets and profiling the assumed potential Attacker's Motives. That only supplies the ***WHO*** and the ***WHY***.

Nearly ALL Commercial Enterprise (even SUPER Multinationals) will require a Legitimate Outside TSCM Consultant to provide the ***Technological WHAT*** and ***HOW***. Only this will complete the Threat Assessment process and help these organizations decide for themselves.

*

- RISK

vulnerability

The likelihood that a particular threat using a specific attack will exploit a particular vulnerability of a system that results in an undesirable consequence.

(Definition from National Information Systems Security (INFOSEC) Glossary, NSTISSI No. 4009, Aug. 1997)

- VULNERABILITY

-Weakness in an information system, cryptographic system, or other components (e.g... , system security procedures, hardware design, internal controls) that could be exploited by a threat.

(Definition from National Information Systems Security (INFOSEC) Glossary, NSTISSI No. 4009, Aug. 1997)

- Vulnerability Examples (Infinite)
  - Easy, total access to VIAS
  - Misconception & Myth
  - No Awareness Training to combat Soc Eng’g
  - Awaiting Overt Signs of Previous Covert Action
    - Too late… IF EVER
    - THINK ASSURANCE…NOT DETECTION
    - **I can Bug Anyone’s Office**

*

- RISK

  - The likelihood that a particular threat using a specific attack will exploit a particular vulnerability of a system that results in an undesirable consequence.

consequence

(Definition from National Information Systems Security (INFOSEC) Glossary, NSTISSI No. 4009, Aug. 1997)

- CONSEQUENCE
  - A consequence is that which logically or naturally follows an action or condition.

(Definition from National Information Systems Security (INFOSEC) Glossary, NSTISSI No. 4009, Aug. 1997)

- RISK ASSESSMENT

  -A process of analyzing THREATS to and VULNERABILITIES of an information system and the POTENTIAL IMPACT the loss of information or capabilities of a system would have. The resulting analysis is used as a basis for identifying appropriate and cost-effective counter-measures.

(Definition from National Information Systems Security (INFOSEC) Glossary, NSTISSI No. 4009, Aug. 1997)

- Benefits of Risk Assessment
  - Increased awareness
  - Assets, vulnerabilities, and controls
  - Improved basis for decisions
  - Justification of expenditures

"Lesson 5, Risk Management", Operational Information Systems Security Trainee Guide (National Cryptologic School)

- Risk Assessment Process
  - Identify assets
  - Determine vulnerabilities
  - Estimate likelihood of exploitation
  - Compute expected loss

"Lesson 5, Risk Management", Operational Information Systems Security Trainee Guide (National Cryptologic School)

- Properties of Value Analysis

  -Confidentiality
  -Integrity
  -Availability
  -Non-repudiation

"Lesson 5, Risk Management", Operational Information Systems Security Trainee Guide (National Cryptologic School)

- Primary Risk Calculation Methodologies

Quantitative

&

Qualitative

"Lesson 5, Risk Management", Operational Information Systems Security Trainee Guide (National Cryptologic School)

- Threat and Vulnerability Revisited

  The capability or intention to exploit, or any circumstance or event with the potential to cause harm such as a hacker.

  A weakness in a system that can be exploited.

“Lesson 5, Risk Management”, Operational Information Systems Security Trainee Guide (National Cryptologic School)

- Likelihood
  - The Likelihood of a successful attack is the probability that an adversary would succeed in carrying out an attack.

“Lesson 5, Risk Management”, Operational Information Systems Security Trainee Guide (National Cryptologic School)

- Factors influencing an attack
  - Level of threat
  - Vulnerabilities
  - Countermeasures applied

“Lesson 5, Risk Management”, Operational Information Systems Security Trainee Guide (National Cryptologic School)

- Determine Level of Threat
  - Criteria for evaluating the level of threat:
    - History
    - Capability
    - Intention or motivation

"Lesson 5, Risk Management", Operational Information Systems Security Trainee Guide (National Cryptologic School)

Applied to Threat of Technical Intercept

- Determine Level of Threat
  - Criteria for evaluati… …hreat:
    - History: **UN…**
    - Capabi… **…ouse capability to estimate**
    - I… …tion: **Dedicated, definitely not casual**
      ***IF* specifically targeted**

History: UNKNOWN

The Purpose and Meaning of Clandestine

How many *spies* does it take…

…to change a light bulb?

The Purpose and Meaning of Clandestine

WHAT LIGHT BULB?

Omaha World-Herald May 15, 1999 -by John W. Allman, WORLD-HERALD STAFF WRITER

Phone Threats Lead Police to Dead Ends

Flowers, a computer warning and a bomb threat.

Omaha police are trying to unravel a series of mysterious events surrounding theats received at the department's headquarters Thursday night and Friday morning.

A phone call to the department's front counter information line at 11:45 p.m. Thursday said a bomb was inside the building.

Police searched, but did not find any suspicious devices. They then tracked the initial call through caller identification and 911 records to a house in northwest Omaha near 148th and California Streets.

When they arrived at the house, however, the real mystery began, said Officer Don Savage, a police spokesman.

A man at the house told police he was expecting them because of a message he had received about 5 p.m. on his home computer that said police would be coming to his house later that night.

The man also said his mother had received 24 pink roses earlier in the day from a florist. A note was attached to the roses that said "CLOPS, you're my buddy."

The man told police that CLOPS is his computer name.

Police took the man downtown to report his story. While the man was downtown, Savage said, the department received four other phone calls from the same phone line. Each time, the caller either spoke and made various threats or just kept the line open.

The last call was received at 2:30 a.m. Friday, Savage said.

Some computer users can "spoof" a person's electronic mail address to send e-mail under a different name, but that technology does not apply to phone lines, said Bob Lamphier, manager of Nebraska public policy for U S West Communications.

"The only way we know it can be done is somebody's making a physical connection," said Lamphier, who spoke to U S West phone and computer security experts Friday.

Such connections can be made several ways: accessing the phone line from inside the residence; tapping into it outdoors; or accessing the line from within the phone company's network.

It takes "a huge amount of sophistication" and expensive equipment to access a phone line in any other way, Lamphier said.

Police did not arrest the man whose phone line was used during the calls, Savage said.

An investigation is continuing.

Gone In An Instant

Omaha World-Herald - May 23, 2004

- **BY VIRGIL LARSON** WORLD-HERALD STAFF WRITER

Travis and Annette Taylor lost nearly $10,000 in their Ameritrade brokerage account last year…

…Ameritrade suggested in a letter to the couple that they may have been careless about protecting their username and password and that somebody else used them to get into their account. The company said it was not at fault and wouldn't reimburse the Taylors.

…The Taylors say that they have always protected ID information and that they've tested their computer and found no sign of tampering by which the IDs might have been stolen. They question why Ameritrade doesn't electronically track down the computer that was used to commit the fraud.

…"Ameritrade systems were not compromised," Jared Hanson, an Ameritrade regulatory analyst, wrote in a Nov. 14 letter to the Taylors. "It appears" the Taylors' ID and password were "shared or stolen," the letter said. "It is also possible your personal computer may have been accessed and the information stolen."

…Travis Taylor said he uses a regular phone-line dial-up connection, not one that is "always on" like high-speed connections. And he was not a day-trader who spent hours at a time connected to the Internet with his account open.

…He said he installed a firewall last July, never used another computer to connect to his Ameritrade account and didn't give out the username and password. "Even my wife didn't know the password," he said.

…ran a "search and destroy" software on the computer to test the suggestion it had been accessed. "There was nothing in there indicating anybody had been in my computer," Travis Taylor said.

TV Executive Charged with Spying on Fox FX Network

Fri Jul 30, 2004 07:45 PM ET

LOS ANGELES (Reuters) - A former television executive was charged on Friday with wiretapping staff meetings at Fox's FX cable network after the company fired him and he went to work at competing networks, prosecutors said.

Randolph Steve Webster, 38, is accused of wiretapping a conference room via telephone at FX between July 31, 2001 and Jan. 20, 2004, prosecutors said.

Webster surrendered on Friday, and was charged with one count of felony wiretapping. If convicted, he faces up to three years in prison.

Webster served as vice president of publicity at FX starting in 1999 but was fired in July of 2001. He went on to work at Sony Pictures, helping to plan the Game Show Network, then took a post at Universal Television Group in 2002, prosecutors said.

District Attorney's spokeswoman Sandi Gibbons would not reveal what Webster purportedly did with the wiretapped data but said Fox went to authorities after its proprietary information was leaked to the public.

Investigators served search warrants at Webster's home and office in February, she said. He is scheduled to be arraigned on Aug. 8.

www.reuters.com/newsArticle.jhtml?type=televisionNews&storyID=5833715

- Criteria for Evaluating the Vulnerability
  - Number of vulnerabilities
  - Nature of vulnerability
  - Countermeasures

"Lesson 5, Risk Management", Operational Information Systems Security Trainee Guide (National Cryptologic School)

- COUNTERMEASURE

  – A countermeasure is an action, device, procedure, or technique used to eliminate or reduce one or more vulnerabilities.

“Lesson 5, Risk Management”, Operational Information Systems Security Trainee Guide (National Cryptologic School)

Examples of Countermeasures

- Procedures:
  - security policies and procedures
  - training
  - personnel transfer
- Hardware:
  - doors, window bars, fences
  - paper shredder
  - alarms, badges
- Manpower:
  - guard force

"Lesson 5, Risk Management", Operational Information Systems Security Trainee Guide (National Cryptologic School)

- CONSEQUENCE

  – A consequence is that which logically or naturally follows an action or condition.

(Definition from National Information Systems Security (INFOSEC) Glossary, NSTISSI No. 4009, Aug. 1997)

- Risk Index

  Risk Index, as defined by the “Yellow Book”, is the disparity between the minimum clearance or authorization of system users and the maximum sensitivity of data processed by a system.

“Lesson 5, Risk Management”, Operational Information Systems Security Trainee Guide (National Cryptologic School)

"…minimum clearance or authorization of system users…"

refers to internal misuse

- Risk Index

Risk Index, as defined by the "Yellow Book", is the disparity between the **minimum clearance** or authorization of system users and the maximum sensitivity of data processed by a system.

"Lesson 5, Risk Management", Operational Information Systems Security Trainee Guide (National Cryptologic School)

"…minimum clearance or authorization of system users…"

refers to internal misuse

- Risk Index

Risk Index, as defined by the "Yellow Book", is the disparity between the **minimum clearance** or authorization of system users and the **maximum sensitivity** of data processed by a system.

"…maximum sensitivity…"

How about PASSWORDS

WHEN WAS THE LAST TIME YOU LOOKED BACK THERE ?

The uncompensated drudgery of Doug Ellsworth

- **Utilizes Flash Memory Modules**
- **Stores max of 2,000,000 keystrokes**
- **Requires NO Software Interface**
- **No Software Needed to Obtain Results**
- **Logs Passwords at BIOS Bootup**

- **Value as a Security Tool ???**
- **Value as a Tool of Evil ???**

Keystroke Logging ***Device***

The uncompensated drudgery of Doug Ellsworth

The uncompensated drudgery of Doug Ellsworth

PART 2

Your Information Assurance Program is Totally Inadequate

Electronic Intercept as a PRELUDE to Cyber Attack?

Do You Know How To Qualify/Select COMPETENT TSCM?

Percentage of your Info/Phys Sec Budget for TSCM Assurance?

Do Professional Technical Intercept Agents Exist?

ILEC Sec Dir admits at Demarc, (Clops, Travis', Webster)

Who Are Technical Intercept Agents?

How Easy to Obtain Effective Devices?

How Easy to Learn Techniques?

Initial Financial Investment Low – Ease of Entry

How Many Intercepts are Detected?

Why So Few?

The Reason Very Few Intercepts Are Detected During A Legitimate, Thorough Survey Is That ***They Do Not Exist…***

…Not At The Time…Not *By The Time*

A Qualified, Legitimate TSCM Survey Is Located, Commissioned, Scheduled and In Process

VICTIM PREDICTABILITY

Information Thieves / Intercept Agents can safely predict:

- People possess little technical or electronic understanding
- People influenced by movies and TV exploits and feel safe
- People see no history of exploits against others - *anywhere*

"If it isn't reported it doesn't happen"

People firmly biased into *denial* of electronic intercept

Information Thieves / CESI Agents can safely predict that *even if denial is overcome* for any reason:

- Too late – short term objective achieved – technique removed

…but even if it isn't too late and ESID removed…

- Targets very often "TIP" their intentions to engage a TSCM effort

…but even if they don't "tip-off"…

- Targets will most often commission an incompetent!! WILL TIP OFF

…but even if competent team is found…

- Targets will limit time-on-site, give wrong info, focus on wrong site

Numbers reveal: odds better than 90% that commissioned TSCM will be incompetent - incapable of detecting intercept.

Information Thieves / Intercept Agents carry on their criminal activities with perceived impunity because if a competent TSCM effort "finds" it:

- Victims RARELY refer incidents to Law Enforcement

…but even if Victim does…

- There's no way to link HIM to the crime – no suspicion

…but even if suspicion is created…

- Mere suspicion is not enough to support criminal charges

…but even if criminal charges are filed…

- No conviction – cannot overcome "beyond a reasonable doubt"

Juries, Judges, LEOs, Prosecutors are people too – same bias.

Assignment:

Obtain specific valuable sensitive secrets of *TARGET* without getting caught. Without becoming "burnt".

Three ways CESI Agent can achieve objective:

1 Cyber-Based Attack – Potentially Very Risky

– risk of discovery (failure) and criminal action

audit trail, "physical" tracking, & (as yet) unknown defenses

Assignment:

Obtain specific valuable sensitive secrets of *TARGET* without getting caught. Without "burning" the assigned mission.

Three ways Criminal Agent can achieve objective:

1 Cyber-Based Attack – Potentially Very Risky

– risk of discovery (failure) and criminal action

audit trail, (as yet) unknown defenses

2 HUMINT – *Extremely* Risky

– also far too Time Consuming and Expensive

Assignment:

Obtain specific valuable sensitive secrets of *TARGET* without getting caught. Without "burning" the assigned mission.

Three ways Criminal Agent can achieve objective:

1 Cyber-Based Attack – Potentially Very Risky

– risk of discovery (failure) and criminal action

audit trail, (as yet) unknown defenses

2 HUMINT – *Extremely* Risky

– also far too Time Consuming and Expensive

3 Electronic Intercept – Safe & Successful & Never Suspected

Assignment:

Obtain specific valuable sensitive secrets of *TARGET* without getting caught. Without "burning" the assigned mission.

Three ways Criminal Agent can achieve objective:

1 Cyber-Based Attack – Potentially Very Risky

– risk of discovery (failure) and criminal action

audit trail, (as yet) unknown defenses

2 HUMINT – *Extremely* Risky

– also far too Time Consuming and Expensive

3 Electronic Intercept – Safe & Successful & Never Suspected

- Residual Risk

  – Portion of risk remaining after security measures have been applied.

(Definition from National Information Systems Security (INFOSEC) Glossary, NSTISSI No. 4009, Aug. 1997)

DON’T RISK A LOT
TO SAVE A LITTLE

The uncompensated drudgery of Doug Ellsworth

COUNTERMEASURES

Alleged TSCM Practitioners are Numerous

- Well-meaning Incompetents
- Con-Artists
- Real TSCM is not an investigative function
- Good for nothing – only CYA value

For Real TSCM Practitioners are Few

- Real TSCM is a narrow technical specialty
- Little economic motivation – extremely slow ROI
- All Regions Need Legitimate Practitioners

COUNTERMEASURES

"Only a Con-Artist or a Fool will claim that a 3-hour 'Sweep' will be adequate for any level of threat"

RESISTORS			CAPACITORS			SEMICONDUCTOR		
27K	1	.02	.001	2	.12	1N4002	1	.08
470K	1	.02	.015	1	.20	2N5210	1	.10
15K	1	.02	220uF	1	.22	2N3904	1	.15
10K	2	.04	10uF	1	.10	KN2222A	2	1.00
1K	1	02	150p	2	.12	MPSH-10	3	.30
12K	1	.02	.01	3	.18	2N4427	1	.15
3.3K	3	.06	.1	2	.20			
47K	2	.04	10p	4	.24	Mic electr	1	1.50
2.2K	1	.02	2.2p	1	.10			
4.7K	2	.04	5p	1	.10	**TOTAL____$ 7.43**		
150	1	.02	22p	1	.06			
220K	1	.02						
120	1	.02	**TRIMMERS**					
10K POT	1	.25	2.8-10p	3	.15			
COILS			6.5-40p	1	1.00			
22 uH	1	.75						
7T #22 5/32” ID	3	0.00						
2T #22 5/32” ID	2	0.00						
3T #22 5/32” ID	1	0.00						

350 mW Subcarrier Bug

Tunable 114-134 MHz

By permission: Winston Arrington, Chicago

RESISTORS		
2.2K	1	.02
100K	1	.02
15K	1	.02
470K	1	.02
10K	1	.02
100K POT	1	.25

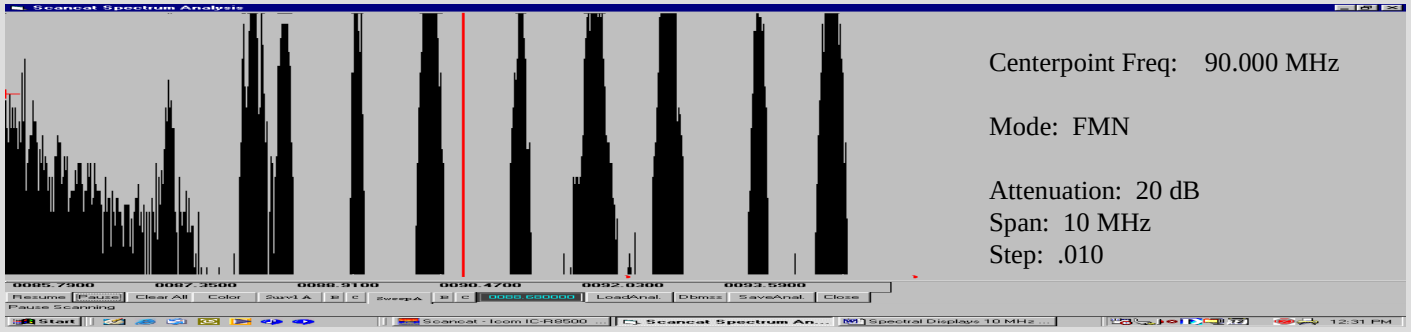
CAPACITORS		
10uF Elec	1	.12
200uF Elec	1	.25
10uF	3	.30
.001	1	.06

SEMICONDUCTORS		
2N3904	3	.45
2N3906	1	.15

TOTAL____$ 1.68

VOX ACTIVATOR

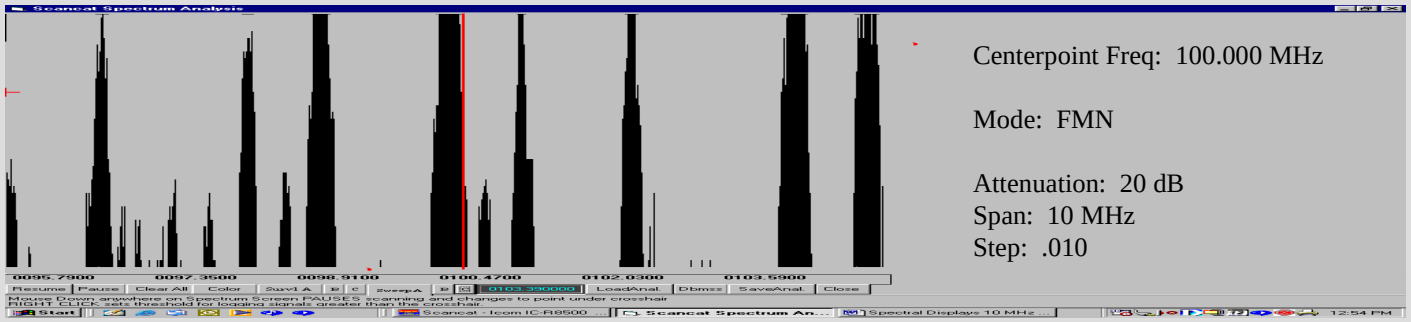
FM COMMERCIAL BROADCAST BAND



Centerpoint Freq: 90.000 MHz

Mode: FMN

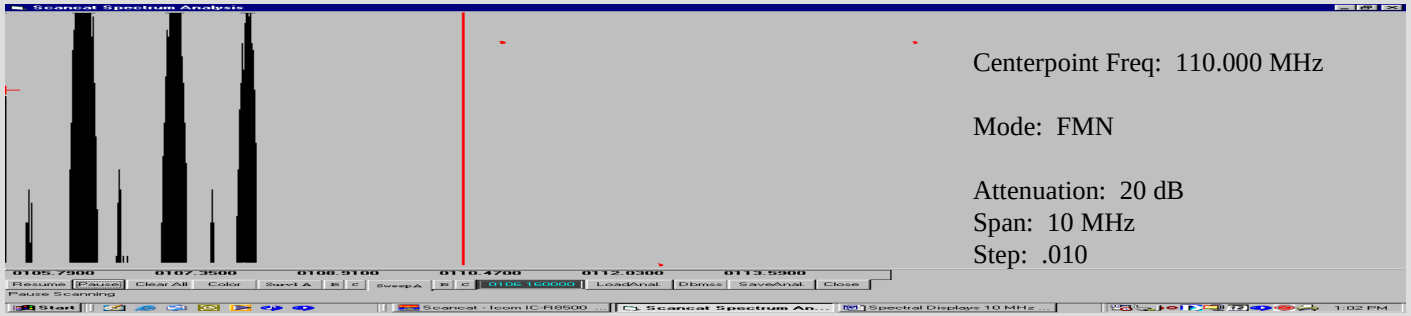
Attenuation: 20 dB
Span: 10 MHz
Step: .010



Centerpoint Freq: 100.000 MHz

Mode: FMN

Attenuation: 20 dB
Span: 10 MHz
Step: .010

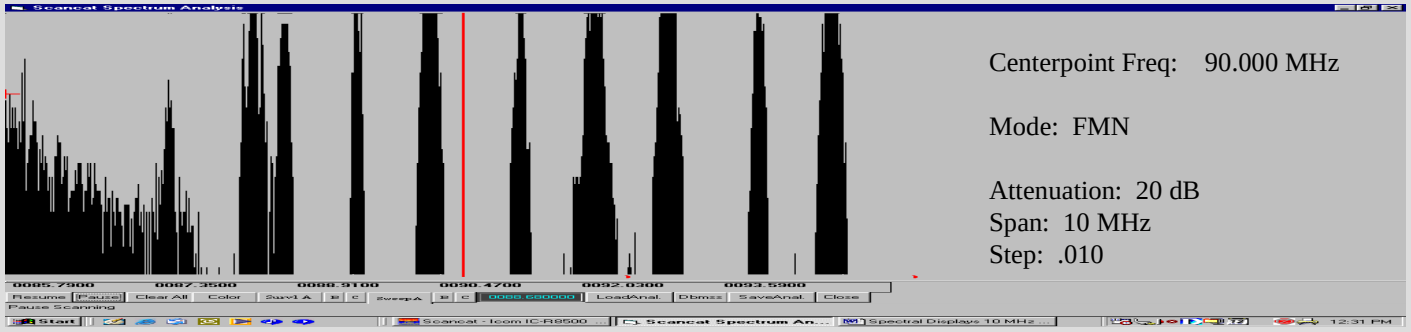


Centerpoint Freq: 110.000 MHz

Mode: FMN

Attenuation: 20 dB
Span: 10 MHz
Step: .010

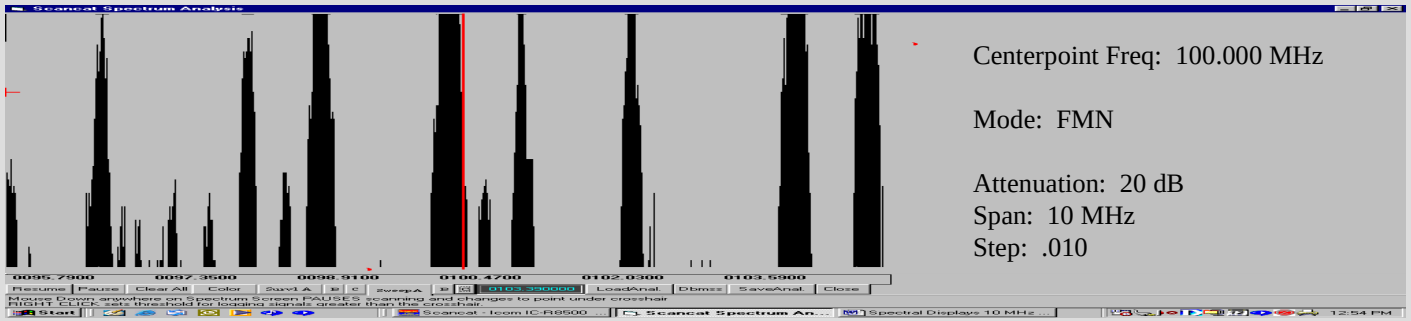
FM COMMERCIAL BROADCAST BAND



Centerpoint Freq: 90.000 MHz

Mode: FMN

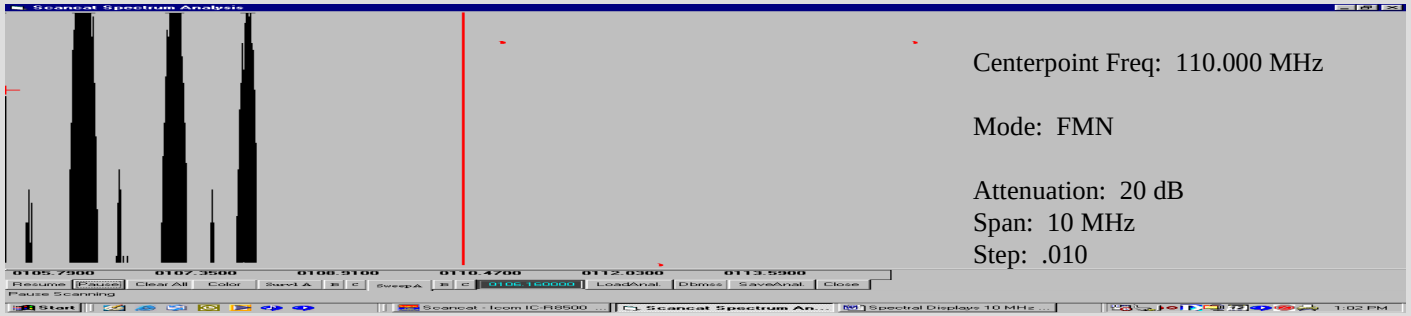
Attenuation: 20 dB
Span: 10 MHz
Step: .010



Centerpoint Freq: 100.000 MHz

Mode: FMN

Attenuation: 20 dB
Span: 10 MHz
Step: .010

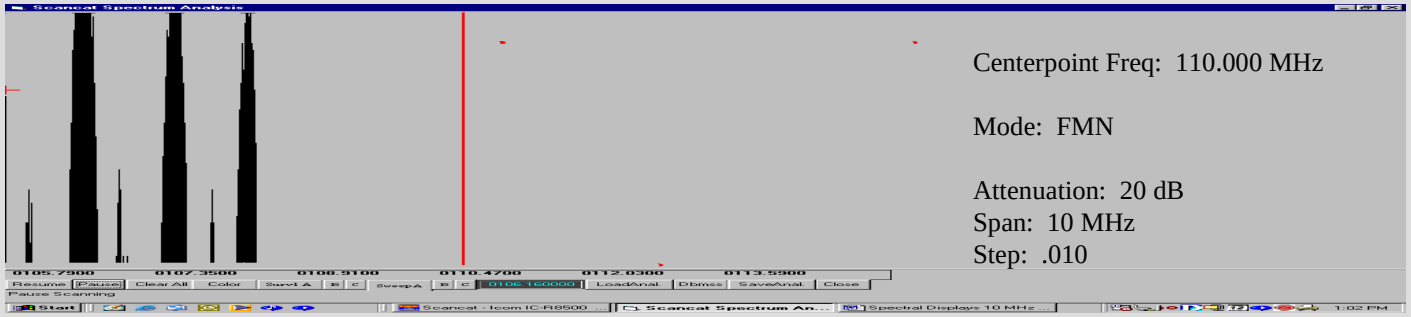


Centerpoint Freq: 110.000 MHz

Mode: FMN

Attenuation: 20 dB
Span: 10 MHz
Step: .010

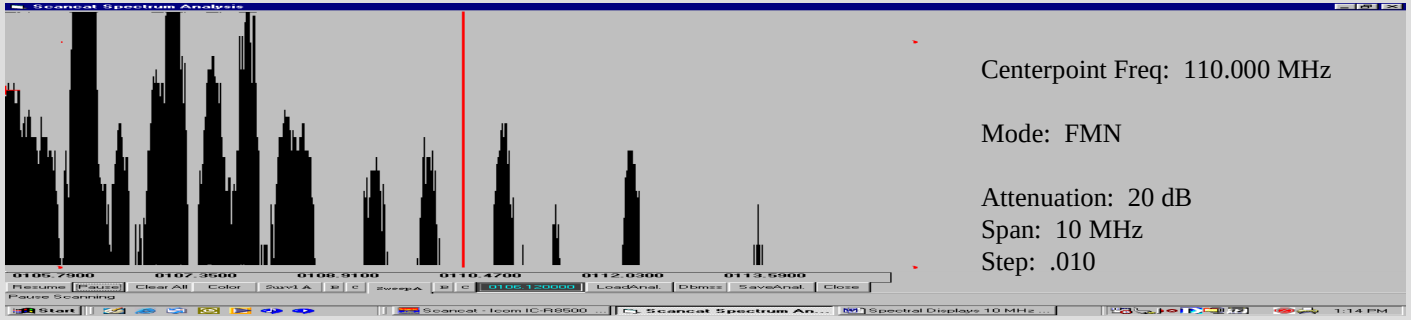
FM COMMERCIAL BROADCAST BAND



Centerpoint Freq: 110.000 MHz

Mode: FMN

Attenuation: 20 dB
Span: 10 MHz
Step: .010



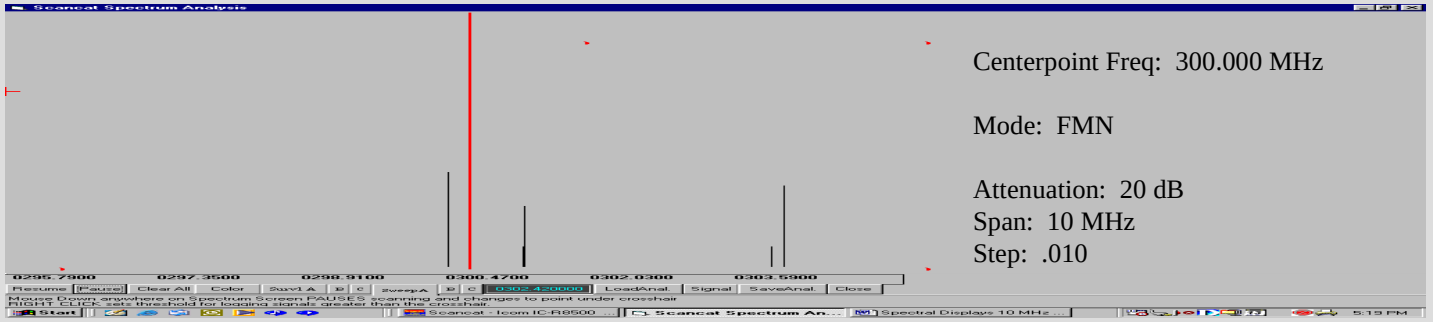
Centerpoint Freq: 110.000 MHz

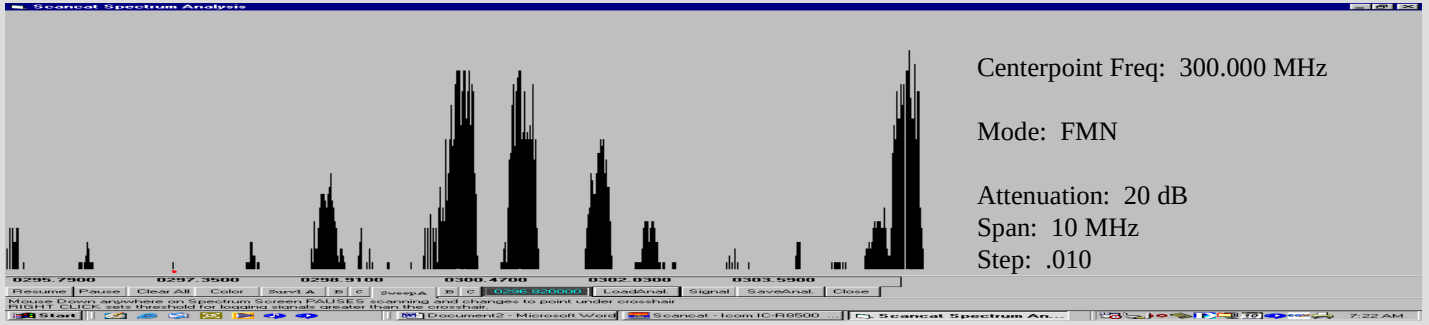
Mode: FMN

Attenuation: 20 dB
Span: 10 MHz
Step: .010

Example of 3rd Harmonic FM Commercial Broadcast Contrasts in Low versus High RF Intensity Locations

“Normal” Intensity RF (control)





High Intensity RF (sweep site)

The uncompensated drudgery of Doug Ellsworth

Qualifying a Countermeasures Provider

No ***LEGITIMATE*** TSCM-er will ***EVER*** divulge the specific identities of ***ANY*** clients

Administer Basic Knowledge Examination

- They've either "been there" or they haven't
- Provided sample questionnaire
  - Perfect score is requirement for consideration

DO NOT accept claims that specialized "TSCM gear" can compensate for basic knowledge examination.

CONCLUSIONS

Regarding Information Assurance:

CESI is a Real Threat / Risk

Threat of CESI Universally Greatly Underestimated

CESI Methods Will Succeed in obtaining a “Take”

CESI Agents Will Not Be Deterred by Serious Felony Criminal Sanctions as Provided by Law

Placement of **CSD/CSP/ESID** Does NOT Require Burglary Risk

INFOSEC Programs Still Inadequate to Cope w/ESI Threat

No Financial Barriers to Entry for New ESI Agents

Serious Financial Barriers to Entry for New TSCMers

CONCLUSIONS
Regarding CESI and Improving Info Assurance:

Don't Try to "Sell" TSCM to Senior Mgt "On Your Own"

Explore Awareness Programs at All Levels of Management

Consider Social Engineering When Pondering CESI Agent Access
– Especially in View of Policy Violations

Consider Hardening Desktops to Keylogging Devices

Consider CESI as a Potential Prelude for Cyber-Attack

Define "Information" Broadly to Include "Intelligence"

Gain Expertise on ESIDs and Methods – or Consult Expert

Do not Overlook *Internal* Threats

Valuable/Secret Info is Not Less Sensitive when "On the Move"

CONCLUSION

doug@enemyofthespy.com

Would like to thank you for attending.

THE FUTURE OF INFORMATION SECURITY AWARENESS IS IN YOUR HANDS!