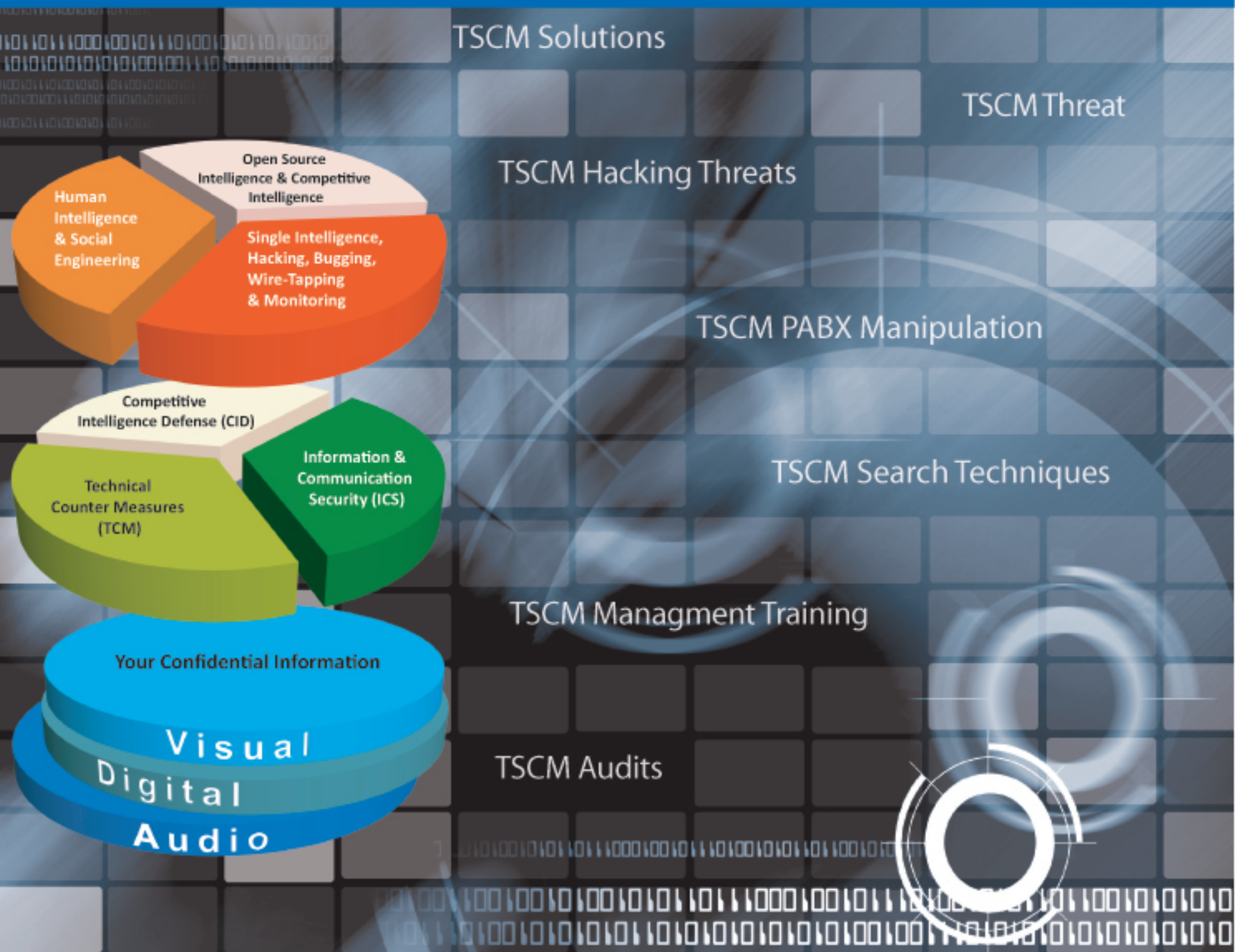


# TSCM

## Government Technical Surveillance Counter Measure Solutions



# TSCM

## Government Technical Surveillance Counter Measure Solutions

PRESENTED TO  
CUSTOMER NAME

The Country Flag



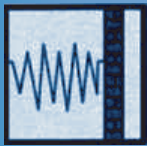
Version 7

# TSCM INDEX



- 1 - Introduction
- 2 - The Threat
- 3 - Recommendations
- 4 - Training Course Overview
- 5 - Training Course Syllabuses
- 6 - Recommended Products
- 7 - Technical Data Sheets
- 8 - IP/PABX Manipulation
- 9 - Commercial Quotations
- 10 - Terms & Conditions
- 11 - Contact Details
- 12 - Elaman Catalogs Overview

# TSCM INDEX



1 - Introduction

2 - The Threat

3 - Recommendations

4 - Training Course Overview

5 - Training Course Syllabuses

6 - Recommended Products

7 - Technical Data Sheets

8 - IP/PABX Manipulation

9 - Commercial Quotations

10 - Terms & Conditions

11 - Contact Details

12 - Elaman Catalogs Overview



## Introduction

## TSCM Intro

The following information is a guideline to various espionage threats; the recommendations on how to start up a TSCM Team linked to Training Courses for all different user levels, and recommendations for products that have proven their reliability & competence, and which are used by various government sweep teams around the world.

The search efficiency of a sweep team is of paramount importance. Government statistics show that the manpower used in a TSCM sweep is divided according to the following percentages:

Physical Search	35%
Cable Measurement	30%
Radio Frequency Measurement	10%
ISDN Phone System Checks	10%
Anti Hacking Manipulation	15%

One of the many misconceptions is that most inexperienced personnel presume the biggest espionage threat is from wireless bugs. However, this is NOT the case: cable and software manipulation are the most common targets for intelligence-gathering operators.

The key to creating a successful Sweep Team is not simply buying all the top equipment on the market, but rather using a systematic, logical, and efficient approach:

1- Identify the Threat of Surveillance Equipment
2- Set Up and Manage a TSCM Team
3- Implement Technical and Management Training
4- Review the range of sweep products
5- Set up a TSCM workshop
6- Repeat the above skills
7- Establish an IT network test procedure
8- PABX administration training.

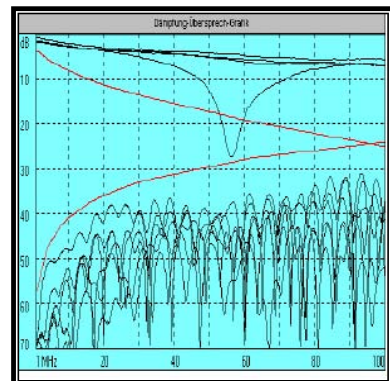
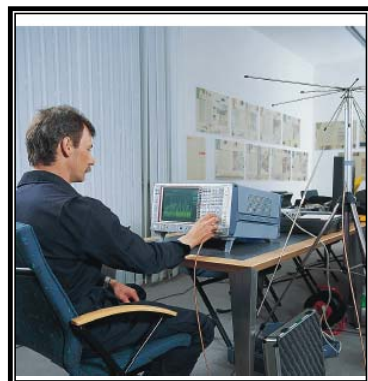
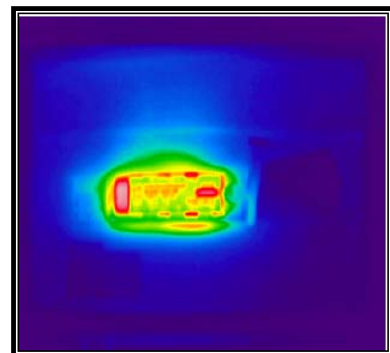
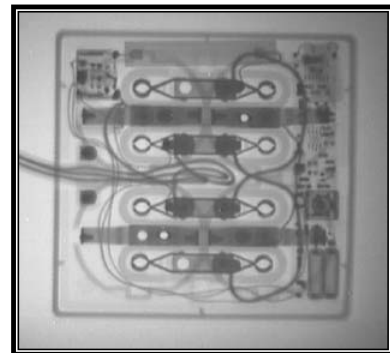
## Introduction

## TSCM Intro

At our TSCM workshop facilities in Germany we can introduce you to the above detailed program. During a 1- to 2-day seminar we can show you the tactics of our sweep teams and the equipment used in sweep operations (an investment well over one million Euros). The follow-up training programs, which last 2-3 weeks, are given by the most advanced and renowned TSCM sweep engineers in different fields. We can also carry out an audit of your available sweep team and provide technical operational training on any equipment you already have.

If you require any further assistance please do not hesitate to contact us.

### TSCM SWEEP



## Strategic Security Overview

## Overview

Within today's global environment, strategically sensitive information has the potential to damage or destroy your interests both domestically and abroad.

Leaked or illegally obtained information, while of great value to the beneficiary, can damage the strategic interests of the organization from where it was obtained, if acted upon effectively by a competitor or opportunist. Although this represents a serious breach of security in the short term, what is potentially damaging in the long term, is the loss of initiative including the resultant loss of confidence in that organization as a "safe and secure pair of hands".

*It is not uncommon for espionage to be an ongoing, undetected and a draining aspect of business life*

Whilst individuals condoning and conducting such information gathering are engaging in highly illegal and dangerous activity, the tangible benefits of doing so often outweigh the risks; as such activity is seldom detected if not effectively monitored. It is not uncommon for espionage to be an ongoing, undetected and a draining aspect of daily life.

*Most countries can expect attacks from espionage specialists*

It is a National responsibility to undertake reasonable, realistic and practical precautions to deter or counteract unscrupulous parties. To reduce exposure to this invisible, yet tangible threat, is an act of due diligence.

Most countries may reasonably expect to receive the attention of Espionage or Surveillance specialists operating on behalf of their clients. These will range from competitors to opportunists to foreign governments, all looking to further their own ends.

### How is sensitive information obtained?

There are two main methods:

The first method is via a human resource, preferably a person already in a key position within the target organization. Whilst the recruitment or placement of a live asset is the preferable option, it is also the most time consuming, complex and expensive. Typically, recruitment agents (or "handlers") will meet the identified target already in place, either directly or through a third party. The handler will proceed to profile the target individual for areas of strength, weakness, preferences etc ("face time") and form an assessment. This assessment will range from psychological to financial. Should the assessment be favorable, the handler will then probe areas of personal weakness with a view to expanding them, whilst at the same time, encouraging areas of empathy, thereby placing him/her in the position of an increasingly close confidant. The objective is to cement a relationship that will ripen for exploitation. This technique is often referred to as "hooking".

## Strategic Security Overview

## Overview

The second method is a leap forward in sophistication, which is electronic surveillance. The placement of listening devices in key areas such as offices, boardrooms, telephone lines and homes can reveal a wealth of information. Not only is this about tangible business plans and the practice of any organization, but also, the quality of the dynamics and relationships within those organizations. Clearly, any “hooking” operation may well begin with electronic surveillance. Whilst it is time consuming to transcribe and analyze the recordings, this is a quick, clean and easy way to access and analyze proprietary information.

Equally valid, although it excludes the human context, is accessing databases through “hacking”. Hacking may be used either to gather information or sabotage electronic systems by inserting logic bombs, viruses etc. Most organizations contact the outside world via telephone lines and can be contacted in return. Electronic “gatekeeper” and “firewall” systems are now considered standard amongst most organizations as this form of access violation usually surfaces and consequently the threat becomes tangible, understood and counteracted.

For an insignificant fee, when compared to the potential gain, it is not difficult to find an agent who will arrange to have listening devices installed. These agents will range from private security companies (often former government employees) to telephone engineers to private investigators. This type of surveillance goes on day in and out with highly sophisticated equipment, light legal penalties, and instigators normally two or three parties removed from the scene. Consequently, from the point of view of the predator, there are strong motives, ample means and a very good chance of not being caught.

***This is a dilemma faced by many and consequently it is more difficult to defend against this form of attack than to instigate it.***

If someone is stealing your laptops, you know; however, if someone is analyzing the strategy and fabric of your organization you may not truly know, even if you may suspect. In short, how do you know if you are losing strategically sensitive information through an invisible medium? This is a dilemma faced by many. Consequently, it is considerably more difficult to defend against this form of threat than to instigate it.

### How do I know or find out if I am a target?

Assume that you are. As already discussed you may be targeted in different ways. It would be a major undertaking to constantly monitor and investigate all methodologies, and probably only warranted in exceptional circumstances. However, it would be safe to say that if you are being targeted, you have been or are almost certainly being bugged. Consequently, a sweep of sensitive areas and phone lines would be the most efficient, cost effective and appropriate way forward.

A sweep, which many view as a standard service, alongside office cleaning and fire/access system maintenance, can be conducted at any time, either at night, during a sensitive in-house or off-site meeting in cars or even airplanes. This provides either immediate reassurance or tangible evidence of espionage activity.



## Strategic Security Overview

## Overview

### What do I do if I am being bugged?

First, tell no one. Assemble a trusted TSCM management team.

A variety of options are available, which may include running a disinformation campaign or surveillance operation, further investigation, removing the device or apprehending/investigating the technician/employee suspected of placing the device.

The business activities and climate at that time, combined with the quality of the device, (which gives an indication of the sophistication and funding behind the hostile party), are likely to dictate the appropriate course of action.



# TSCM INDEX



1 - Introduction

2 - The Threat

3 - Recommendations

4 - Training Course Overview

5 - Training Course Syllabuses

6 - Recommended Products

7 - Technical Data Sheets

8 - IP/PABX Manipulation

9 - Commercial Quotations

10 - Terms & Conditions

11 - Contact Details

12 - Elaman Catalogs Overview

# THE THREAT

<b>Technical Trends</b>	<b>1-18</b>
<b>Communication Monitoring</b>	<b>19-23</b>
<b>Wire Tapping</b>	<b>23-26</b>
<b>TSCM Sweeps</b>	<b>27-40</b>
<b>Software Manipulations</b>	<b>41-49</b>
<b>ISP Manipulations</b>	<b>49-54</b>

TRENDS AND TYPICAL RISKS  
FACING A TSCM TEAM

# State-of-the-art technologies of technical espionage and counter-measures

Speaker: Franz-Josef Schauka,  
former captain and team-leader TSCM  
of the German Military Intelligence (MAD)

## Overview

### Room monitoring

- Miniaturizing
- Camouflage
- Technical trends

### Telecommunication monitoring

- Interception and wire tapping
- Software manipulations (PBX course only)

### Countermeasures

- Risk analysis and Prevention
- TSCM Sweeps

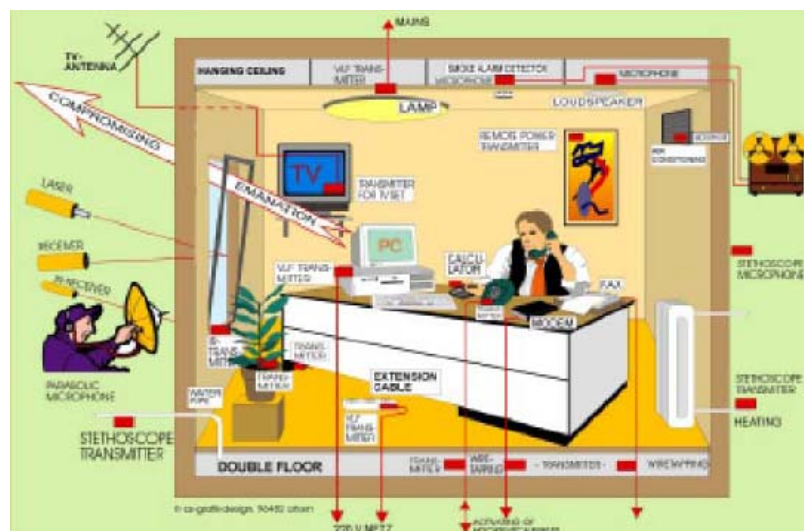
### Demonstrations



## The Threat

### 1- Room Monitoring

### Room Monitoring



## The Threat

### Room Monitoring

#### ▪ Methods

- Using miniaturized bugs
- Using highly sophisticated unconventional camouflage
- Using high-end transmission technologies
- Manipulation of existing devices

### Miniaturizing

#### ▪ Surface Mounted Devices (SMD-parts)

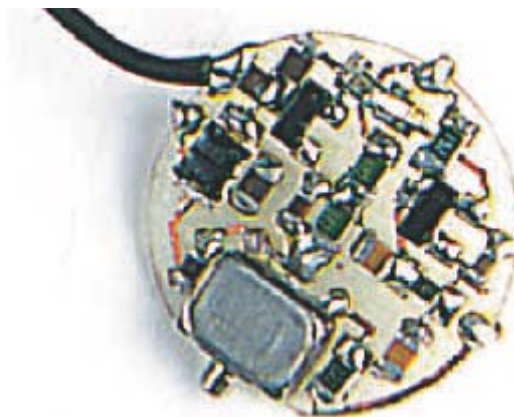
- Consequences of using of SMD-parts
- Industrial manufacturing of circuit plates by machines  
large number of bugs
- Low cost, high integrated components

## The Threat

### Miniaturizing



### Miniaturizing



## The Threat

### Miniaturizing



### Camouflage

- In or as harmless items
  - Walls, wall panels, hollows, (e.g. hanging ceilings, double floors, built-in furniture)
  - Solid-seeming material (e.g. wood, metal)
  - Insignificant objects (e.g. pasteboard, door-stop)
  - Decorations (e.g. paintings, flowers)



## The Threat

### Camouflage



### Camouflage

#### ■ As articles of daily use

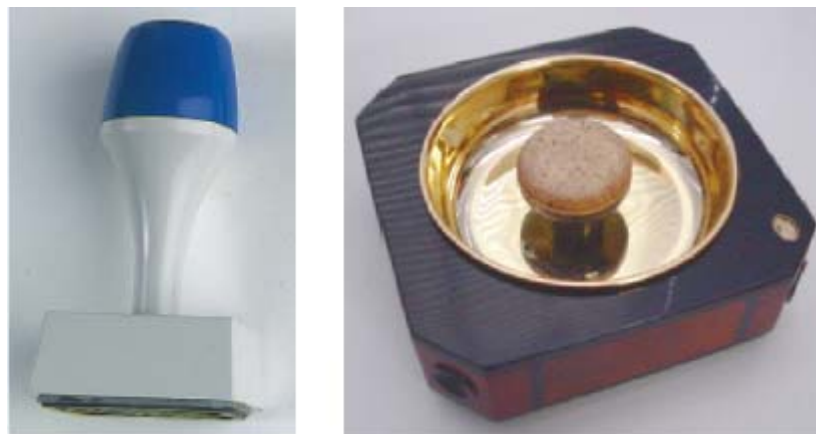
- Desk-items (e.g. stamp, paper clip box, mouse pad, ashtray)
- Writing utensils (e.g. pen, high-lighter)
- Personal Items (e.g. Mobile, gas-lighter, clothes!)

## The Threat

### Camouflage



### Camouflage

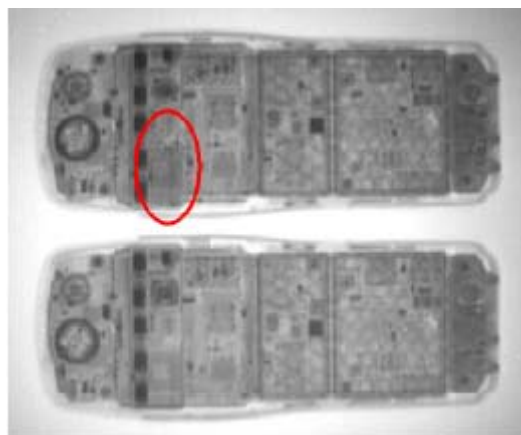


## The Threat

### Camouflage

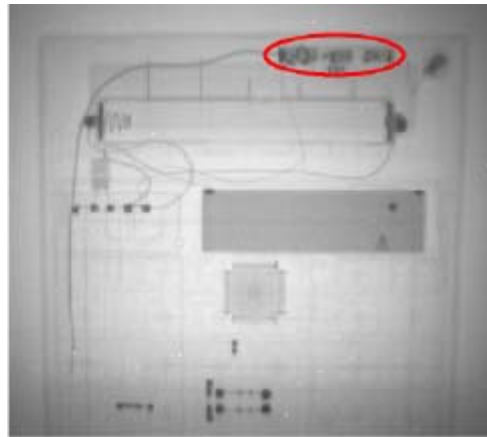


### Camouflage



## The Threat

### Camouflage



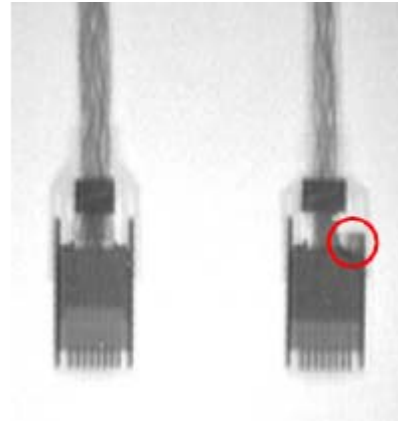
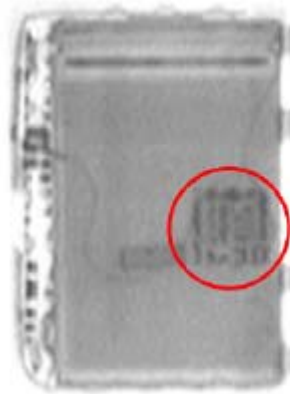
### Camouflage

#### ■ In electrical devices

- Mobile phone accumulators and chargers, telephone and mains adapter and plugs, light switches
- Motion and smoke detectors, air conditioning control systems
- Desk items (e.g. calculators, desk lamps, radios)
- Communication systems (e.g. fax machines, Pc Cameras).

## The Threat

### Camouflage

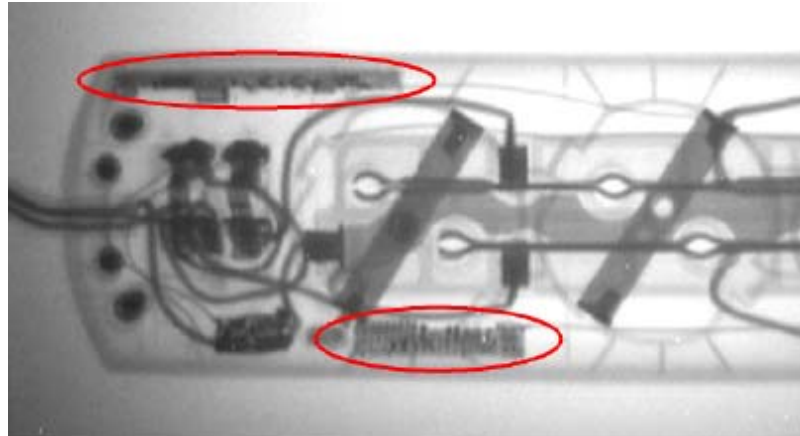


### Camouflage

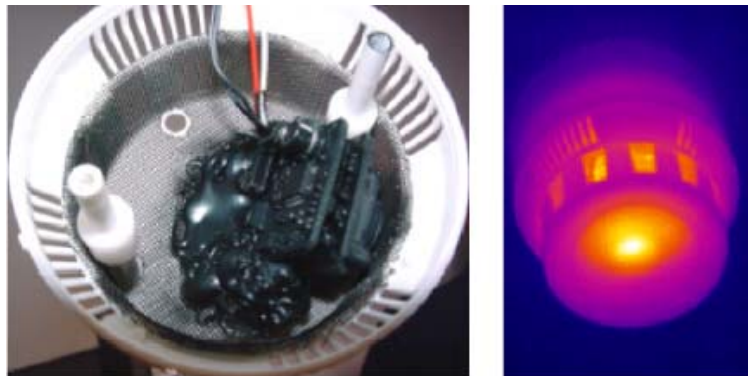


## The Threat

### Camouflage



### Camouflage



## The Threat

### Technical Trends

- **Sophisticated technologies of control**
  - Voice control (VOX) is standard today
  - Radio control of all parameters (e.g. ON-OFF, power and frequency)
  - Remote power ON-OFF (“passive bugs”)
  - Control by timer or sensors

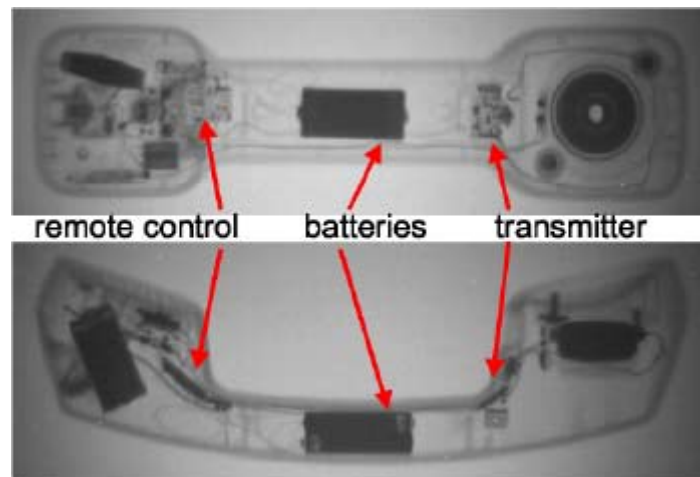
### Technical Trends





## The Threat

### Technical Trends



### Technical Trends

- **State-of-the-art methods of transmission**
  - Using high-end standard procedures and protocols (GSM, DECT, Bluetooth, W-LAN)
  - Misuse of highly available ISM and LPD standard components (e.g. walkie-talkies and telemetry transmitters)
  - Misuse of high-end methods of wired transmissions (e.g. fiber-optics, ISDN and LAN wiring)

## The Threat

### Technical Trends



### Technical Trends

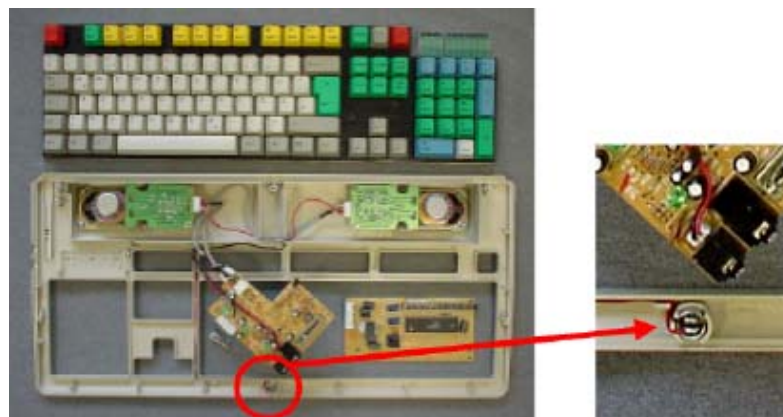


## The Threat

### Technical Trends

- **Manipulation instead of installation**
  - Misuse of existing systems (e.g. phone systems, PCs, intercoms and loudspeaker systems)
  - Modification of common electric devices (e.g. telephones, office machines and multimedia systems)

### Technical Trends



## The Threat

### Technical Trends



### Technical Trends

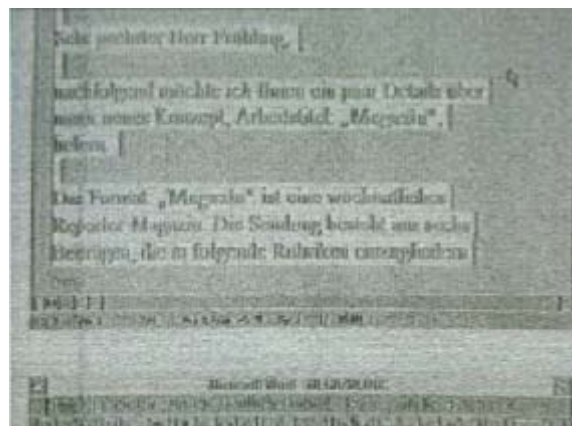


## The Threat

### Technical Trends

- **Receiving of unintended emanations**
  - **Reproducing of compromising emanations of PC components (e.g. graphic board, monitor, printer, keyboard)**
  - **ATTENTION: The emanation of TFT flat screens is stronger than the emanations of visual display units with conventional tubes!**

### Technical Trends



## The Threat

### Telecommunication Monitoring

- Risks from international calls
  - Monitoring of microwave-transmissions
  - Monitoring of the communication satellites
  - Monitoring of national and international telephone-wires (incl. sea-cable and fiber optic wires)

### Telecommunication Monitoring

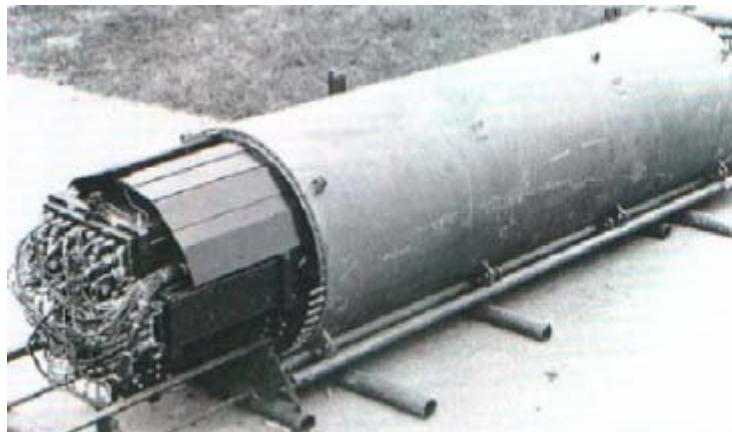


## The Threat

### Telecommunication Monitoring



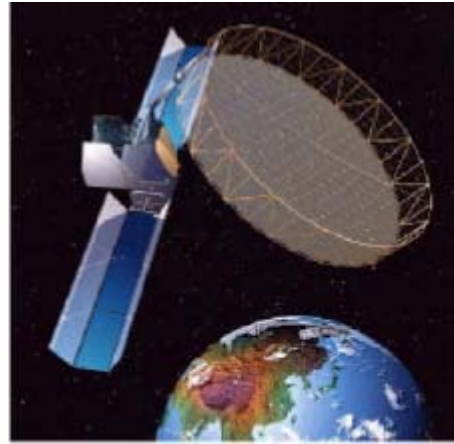
### Telecommunication Monitoring





## The Threat

### Telecommunication Monitoring



### Telecommunication Monitoring



## The Threat

### Telecommunication Monitoring



### Wireless Transmissions



## The Threat

### Wireless Transmissions



### Wire Tapping

#### ■ Sources of danger

- Public networks (PSTN)
- PBXs and distribution boxes
- All telephone wires
- Telephone plugs and adapters
- Telecommunication devices (telephones, fax and answering machines, modems)

## The Threat

### Wire Tapping



### Wire Tapping



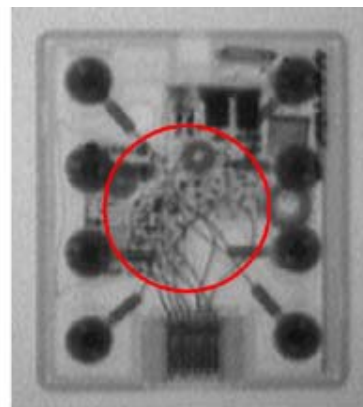


## The Threat

### Telephone Bugs

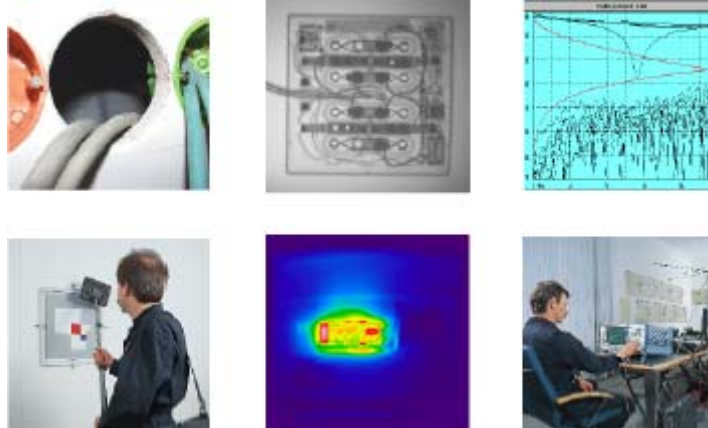


### Telephone Bugs



## The Threat

### TSCM Sweeps



### TSCM Sweeps

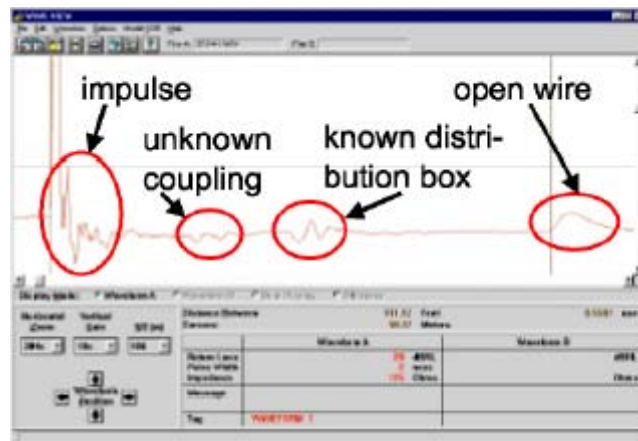
#### ■ Physical search

- Manual opening of all hollows (screwdriver)
- Visual inspection (mirrors, lights)
- X-ray inspection of all items
- Using optical endoscopes and video endoscopes for inaccessible hollows

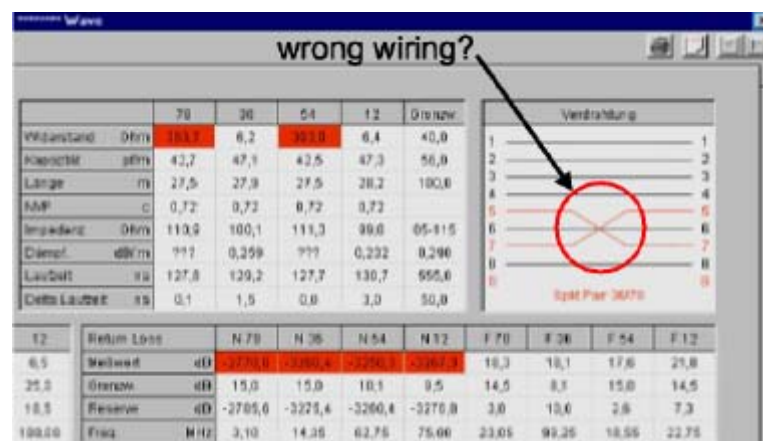


## The Threat

### TSCM Sweeps



### TSCM Sweep



## TSCM Sweeps

- ISDN phone system checks
  - Checking the configuration of the features
  - Checking for warning-tones
  - Checking the remote access
  - Checking for default users and passwords
  - Checking Log files

## TSCM Sweep

```

Command: list hist
list history

                                HISTORY
Date of Loaded Translation: 12:00 am Sat Aug 19, 2000
Date  Time Port      Login Actn  Object  Qualifier
11/01 15:28 NET      sciboz add    station 1100
11/01 15:22 NET      sciboz cha    station 1700
11/01 15:17 NET      tis
11/01 15:03 NET      sciboz cha    vector  117
11/01 15:00 NET      sciboz dup    station 1999
11/01 15:00 NET      sciboz add    dup-stn 6599
11/01 15:00 NET      sciboz rem    station 6559
11/01 15:00 NET      sciboz dup    station 1996
11/01 15:00 NET      sciboz add    dup-stn 5588
11/01 14:59 NET      sciboz dup    station 1997
      press CANCEL to quit -- press NEXT PAGE to continue
  
```

### 2- Typical Risks

### Typical Risks

- **Weak points of the construction**
  - **Placing the distribution boxes in cleaning rooms**
  - **Placing the PBX in critical rooms on the ground floor (direct to public areas)**

## The Threat

### Typical Risks



### Typical Risks

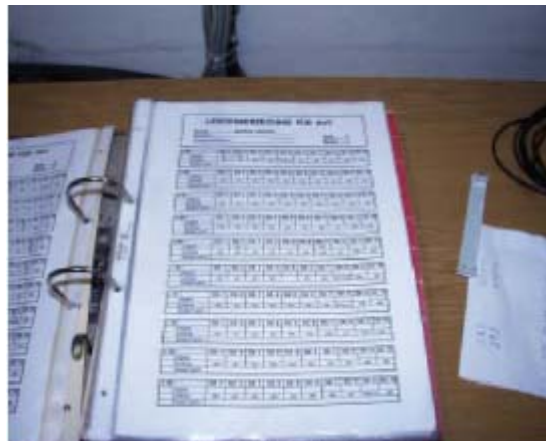


## The Threat

### Typical Risks

- **Organizational mistakes**
  - **Missing documentation about the telecommunication wiring**
  - **Storing the documentation with names, room and extension numbers in the distribution boxes**

### Typical Risks



## The Threat

### Typical Risks



### Typical Risks

- **Organizational mistakes**
  - **Uncontrolled access to ISDN test-equipment of the service staff**
  - **Using the memory of fax machines without periodical checking the stored numbers**

## The Threat

### Typical Risks

- Measurement and Test Equipment



### Typical Risks





## The Threat

### Typical Risks

- **Organizational mistakes**
  - **Outsourcing of all services in the telecommunication (e.g. wiring, installation, administration, service)**
  - **Missing possibility to check the outsourced service**

### Typical Risks

- **Technical weak points**
  - **Technical rooms and distribution boxes are not consequently locked (e.g. using standard locks like RITTAL 3524 or DIRAK 1333)**
  - **Common use of the distribution boxes for telecommunication, data network, access control, intrusion- and fire-alarm systems**

## The Threat

### Typical Risks



### Typical Risks



## The Threat

### Typical Risks

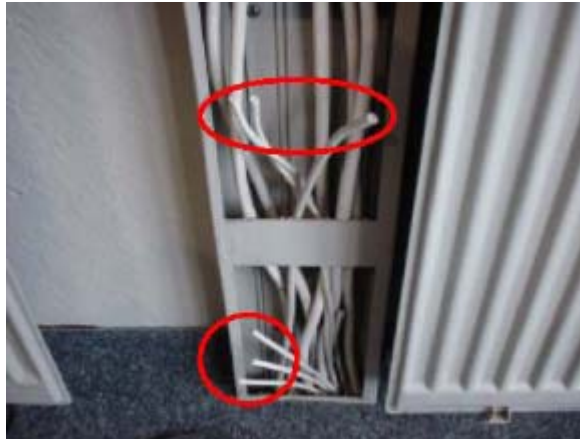


### Typical Risks



## The Threat

### Typical Risks



### Typical Risks

#### ■ Technical weak points

- **Outsized new wiring (surplus cable or wires)**
- **Unnecessary Patches in case of structured wiring (e.g. CAT-5)**
- **Missing encryption systems for critical telecommunication transmissions (voice, fax and data)**

## The Threat

### Typical Risks



### Typical Risks

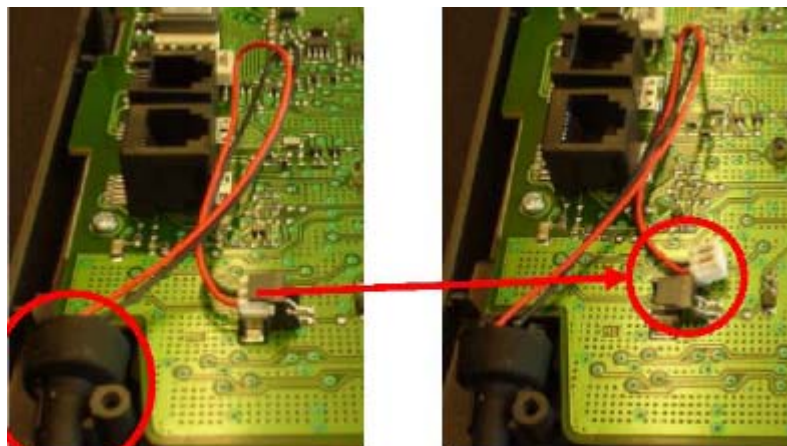


## The Threat

### Typical Risks

- **Technical weak points**
  - Digital phones with hands-free-answer-back in critical rooms (e.g. of board members)
  - Telephones (as well as analog) in conference rooms
  - Using cordless phones (especially of former generation which can easily be monitored)

### Typical Risks



### 3- Software Manipulations

#### Software Manipulations

- **Reasons for possible manipulations**
  - **Manufacturers are ignoring the security risks of their ISDN systems (some install “backdoors”)**
  - **Administrators have no awareness of existing security risks (e.g. by using remote access)**
  - **Users of ISDN systems permanently ask for new technical features, without thinking about risks**
  - **Software manipulations by specific attacks (by “methods of hackers”)**

## Software Manipulations

```
DIS-PASSW;
H500: AMO PASSW STARTED
```

```
PASSWORD | CLASS
-----+-----
HICOM    | 5
```

```
|UID| NAME | AUTHORIZATIONS | STATUS | OPTIONS | RE- | LOCK- | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
|-----+-----+-----+-----+-----+-----+-----+
| 1 | ROOT | .....XXXXXXXXX | | | | | | | | | | | | | | | | | |
| 2 | LROOT | ..X..XXXXXXXXX | INIT. | X X X X X X | 99 | 0 |
| | | | | | | | | | | | | | | | | | |
```

## Software Manipulations

### ■ Kind of manipulations

- Manipulation and misuse of regular features (e.g. hands-free answer back or "virtual" conferencing)
- Activation of hidden features (e.g. witness function, service observing or "lawful" interception)
- Adding new self-created features (own programs) to the PBX



## Software Manipulations

- Misuse of regular features

```

display cor 1                                     Page 1 of 3
                CLASS OF RESTRICTION
                COR Number: 1
                COR Description: INTERNATIONAL
                FRI: 6                               APLT? n
                Can Be Service Observed? y           Calling Party Restriction: none
                Can Be A Service Observer? y         Called Party Restriction: none
                Time of Day Chart: 1                 Forced Entry of Account Codes? n
                Priority Queuing? n                   Direct Agent Calling? n
  
```

## Software Manipulations

- Misuse of regular features

```

display system-parameters features               Page 8 of 9
                FEATURE-RELATED SYSTEM PARAMETERS
SERVICE OBSERVING
Service Observing: Warning Tone? n or Conference Tone? n
display system-parameters features
  
```

## The Threat

### Software Manipulations

Kuerzel	Bezeichnung	Zeitlage
wt	Wahlton	003
ft	Freiton	001
ewt	Externer Wahlton	002
bt	Besetztton	000
swt	Sonderwahlton	006
at	Aufschalteton	004
qt	Quittungston	005
ht	Hinweiston	011
awt	Abweiston	000
akt	Anklopfen	008
amt	Aufmerksamkeitston	007
dt	Datenton	-01
bw	Bitte Warten	012
wta	Amtswahlton	002
as	Anrufschutz	011
lte	Leitungston Export	001
akq	Anklopf-Quittungston	004
nv	Nachricht vorhanden	-01
rfwt	Rueckfragewahlton	003
lwa	Nachwahlaufforderung	000

### Software Manipulations

#### Export Features

MOEGLICHE WERTE :

- AMTFANG
- LEDSIGN
- VMSIWV
- RELCON
- RERING
- AUTOV
- NOTAUF
- NOTTR

(CHINA LM)

(CHINA LM)

(CHINA LM)

## The Threat

### Software Manipulations

EINHEIT	GE- KAUFT	VER- WENDET	FREI
BETRIEBSSOFTWARE V3.0 PLUS	544	524	20
TELEFONIEREN PLUS	432	432	0
KEY 300	0	0	0
AMT / NETWORKING	32	32	0
ATM NETWORKING 1.0	60	60	0
ATM NETWORKING 2.0	0	0	0
ATM INTERWORKING 1.0	0	0	0
CORDLESS E	0	0	0
MULTIRATE SWITCHING	0	0	0
PNE	0	0	0
VOICE COMPRESSION	0	0	0
FLEXROUTING SUPERVISOR	0	0	0
FLEXROUTING AGENT	0	0	0
TELEWORKING	0	0	0
AMT / NETWORKING KOMFORT	NEIN	NEIN	
ACL-ANSCHALTUNG VON SIEMENS-SPRACHANWENDUNGEN	NEIN		
HICOM CORDLESS ES	NEIN		
<b>LAWFUL INTERCEPTION</b>	NEIN		
CDR-E SAMPLER	NEIN	NEIN	

### Software Manipulations

- Lawful Interception

LEISTUNGSMERKMALE IN DEN PAKETEN	GE- KAUFT	VER- WENDET	FREI
<b>UEBERWACHUNG GEMAESS GESETZL. VORGABEN V1.0</b>	NEIN		
EINHEIT : ANZAHL AN SYSTEMEN			
LEISTUNGSMERKMAL			
ERMUEGLICHT FUER ABGEGRENZTE KUNDENSEGMENTE DIE EINSCHALTUNG VON UEBERWACHUNGSMASSNAHMEN GEMAESS FERNMELDEUEBERWACHUNGSVERORDNUNG			

### Software Manipulations

- **Implementing of Own Scripts**

```

01
02 goto      step 10 if ani          in      table 10
03 goto      step 7  if unconditionally
04 goto      step 10 if time-of-day is fri 17:30 to mon 08:00
05 goto      step 10 if time-of-day is all 18:00 to all 06:00
06
07 wait-time 15 secs hearing music
08
09
10 route-to  number 71700          with cov n if unconditionally

```

### Software Manipulations

- **In videoconfere**

- 

- 

- **ncing systems**

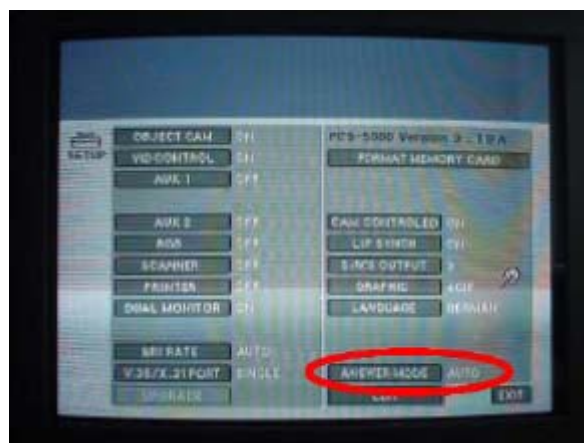
- **Activating of the “auto answer mode” is the most common mistake (Reason: The system must be usable for board members)**
- **Often no ringing tone is configured**
- **Most effective method of protection is a mains switch for**

## The Threat

### Software Manipulations



### Software Manipulations



## The Threat

### Software Manipulations

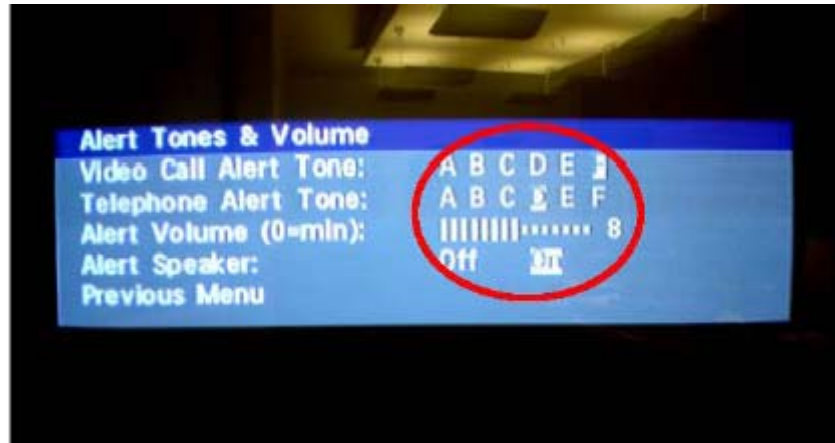


### Software Manipulations



## The Threat

### Software Manipulations



### 4- WAN-LAN Access

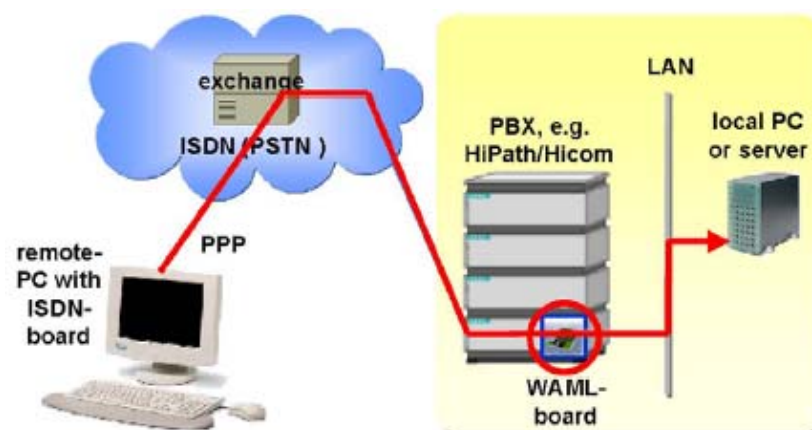
## The Threat

### WAN-LAN Access

#### ■ Problems

- Continuous fast increasing fusion between telecommunication and IT
- Internal "remote" Administration of the own PBX by LAN)
- Increasing IP-telephony
- LAN-access possible in case of wrong configuration

### WAN-LAN Access





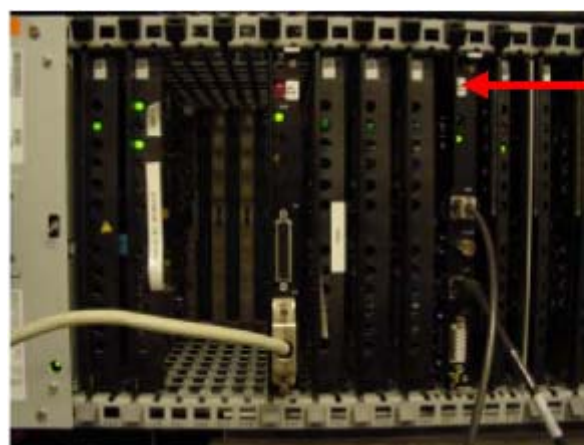
## The Threat

### WAN-LAN Access

- Authentication by the calling party no.

ISDN REMOTE TERMINAL TABLE						
IP-ADDRESS	SHORT HOLD TIME	B-CHANNELS FOR CHANNEL BUNDLING	BITRATE ON B-CHANNEL	CALL BACK	STATION NUMBER	USAGE
192.168.XXX.XXX	30	1	64KBIT	N	007121XXXXXXX	IN OUT
192.168.XXX.XXX	30	1	64KBIT	N	497121XXXXXXX	IN
					007121XXXXXXX	IN OUT
					497121XXXXXXX	IN

### WAN-LAN Access



## The Threat

### WAN-LAN Access



### WAN-LAN Access

- Connection between 3 networks

NETWORK INTERFACE TABLE			
INTERFACE NAME	IP-ADDRESS	IP-NETMASK	MTU
ATLLAN	192.168.XXX.XXX	255.255.255.000	1500
EXTLAN1	010.000.XXX.XXX	255.000.000.000	1500
ISDN1	192.168.XXX.XXX	255.255.255.000	1500

## The Threat

### WAN-LAN Access

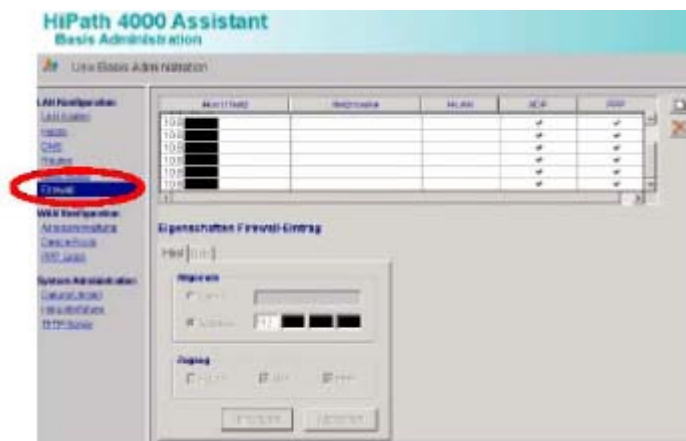
- Unused Firewall

```

GLOBAL PARAMETERS
-----
WAML STATION NUMBER: XXXX
SYSTEM TYPE:          HICOM          NUMBER OF B-CHANNELS: 2
BYTERATE:             100 KB/SEC.    PACKAGE RATE:          1000 PER SEC.
CALL RETRIES:         3              CALL PAUSE:            5 SEC.
HIGH WATER MARK:     90 %           ADD CHANNEL TIMER:     40 SEC.
LOW WATER MARK:      65 %           SUB CHANNEL TIMER:     30 SEC.
TRACE-LEVEL:         3              FIREWALL:              NONE
LAN HW-INTERFACE:    WESTERN        ACTIVE FLAGS:         ATENUM  EXTLAN1 ISDN
ADP ACCESS VIA ISDN INTERFACES: ROUTE
ADP ACCESS VIA EXTERNAL LAN INTERFACES: ROUTE

H01  THERE ARE NO DATA CONFIGURED IN TABLE 'FIRELIP'
H01  THERE ARE NO DATA CONFIGURED IN TABLE 'FIREMAC'
    
```

### WAN-LAN Access



## The Threat

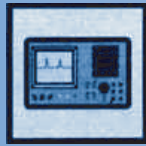
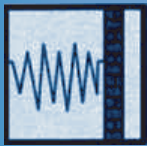
**Communication can be Secure!**



**Thank for your Time**

**Elaman GmbH**

# TSCM INDEX



1 - Introduction

2 - The Threat

3 - Recommendations

4 - Training Course Overview

5 - Training Course Syllabuses

6 - Recommended Products

7 - Technical Data Sheets

8 - IP/PABX Manipulation

9 - Commercial Quotations

10 - Terms & Conditions

11 - Contact Details

12 - Elaman Catalogs Overview

## RECOMMENDATIONS FOR A GOVERNMENT SWEEP TEAM

We recommend the following steps be taken to set up, equip and manage a government Sweep Team. The recommendations were made after close cooperation with the German Government.

### 1. Recommendations

#### Recommendations for future development of skills and equipment

- Teach the basic TSCM skills or repeat TSCM skills already learned
- Coordination within the Sweep Teams
- Start a small workshop for the counter-teams
- Set into place management pre-planning protocols and reporting methods
- Emphasize cable measurement and security
- Set into place assessment protocols of areas to be swept
- PABX Manipulation & anti-hacking protocols

### 2. Equipment

For a more successful team and sweep results, additional equipment, especially for the physical search and cable measurement, is needed.

### 3. Aim of the Sweep Team

- To make all rooms for Government meetings free of surveillance systems
- To make sure the system and search procedures detect and render harmless surveillance products such as:
  - - Audio bugs; all frequencies and modulations
  - - Video cameras and transmitters
  - - Microphones; wired analog and fiber optic
  - - All cable based surveillance equipment
  - - Telephone, e-mail and fax monitoring systems
  - - All surveillance equipment installed in shredders, walls etc.
  - - GSM phones used as surveillance phones
  - - PABX manipulation
  - - IP hacking

## Recommendations

## Sweep

### TRAINING PACKAGE

The most important part of a successful Sweep Team is the initial training and management set up. We offer below a complete management set up including operational, technical and management training. We will make available specialist sweep engineers and managers to teach the use of equipment and how to set up a Sweep Team.

#### 4. Training

Schedule		Duration
<b>Stage 1-</b>	-Training in Europe at our TSCM Laboratory on how to manage and organize a Sweep Team including training on all technical threats and solutions	2 Weeks
<b>Stage 2-</b>	-Training in the threat of PABX-ISP manipulation and how to test and protect yourself against such attacks	2 Weeks
<b>Stage 3-</b>	-Proposals for equipment based on turnkey product selection	2 Weeks
<b><u>After Purchasing Equipment</u></b>		
<b>Stage 4-</b>	-Operational Training on the equipment in Germany (acceptance)	2 Weeks
	-Advanced training focusing on cables (Germany)	1 week
	-Repetition of theory, background and updating technologies -PABX administration training	2 weeks
<b>Stage 5-</b>	-Training in end-user country - A	2 Weeks
	-Training on equipment and usage taking into consideration the end-user's conditions	
	-Review of management and coordination techniques	
<b>Stage 6-</b>	-Training in end-user country - B	
	-Follow-up training on products and search techniques within 6 months from the last training and again 12 months	1 Week
	-Focusing on the warranty of the products	

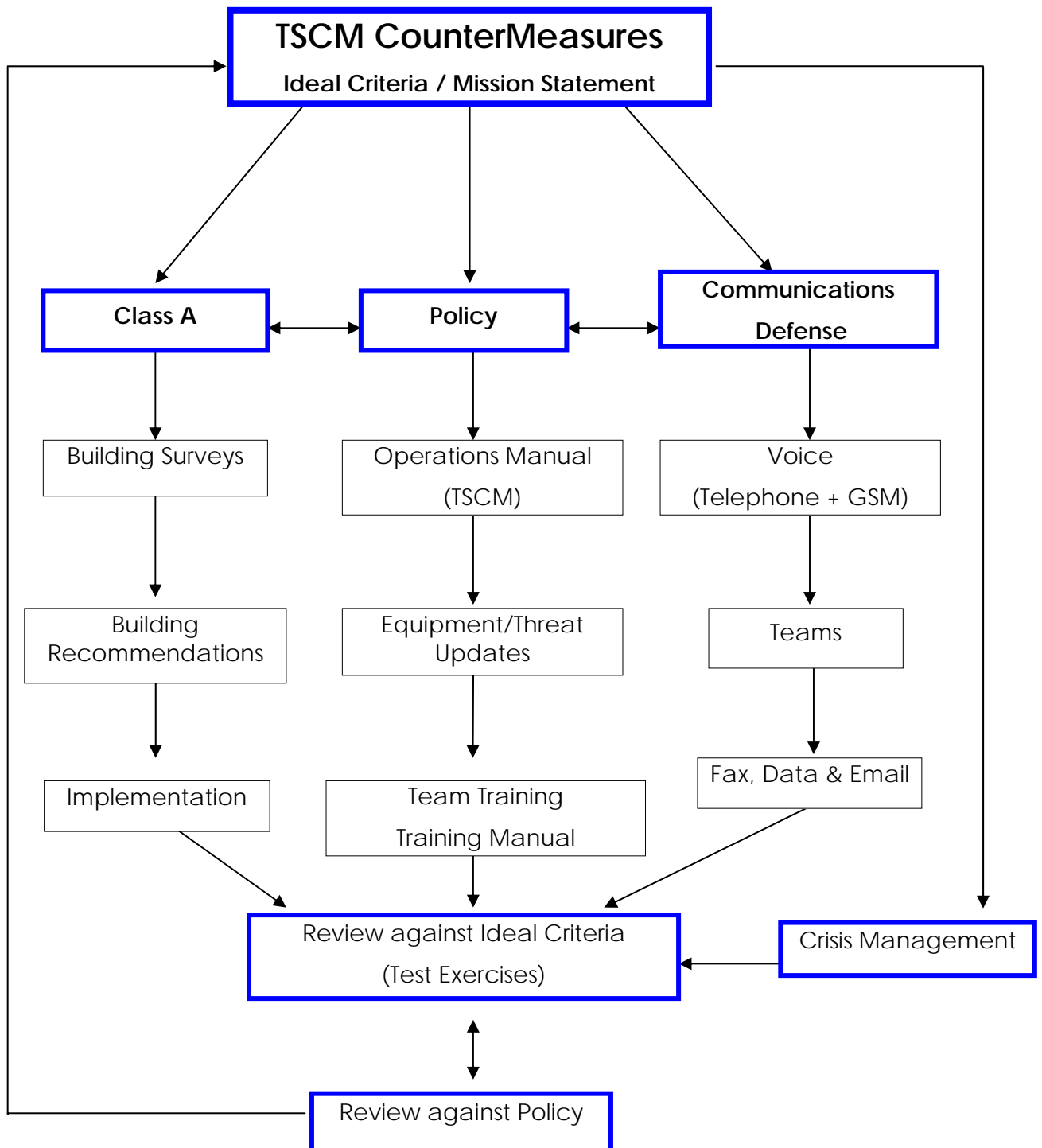
#### 5. Management

- Establish planning documentation and protocols
- Establish equipment check list
- Establish service and test checks
- Establish sweep area profile
- Establish transportation and storage system
- Establish regular update of new technologies
- Have good selection of training courses, both technical and operational
- Establish your own sweep workshop

# Recommendations

# Sweep

DIAGRAM 1

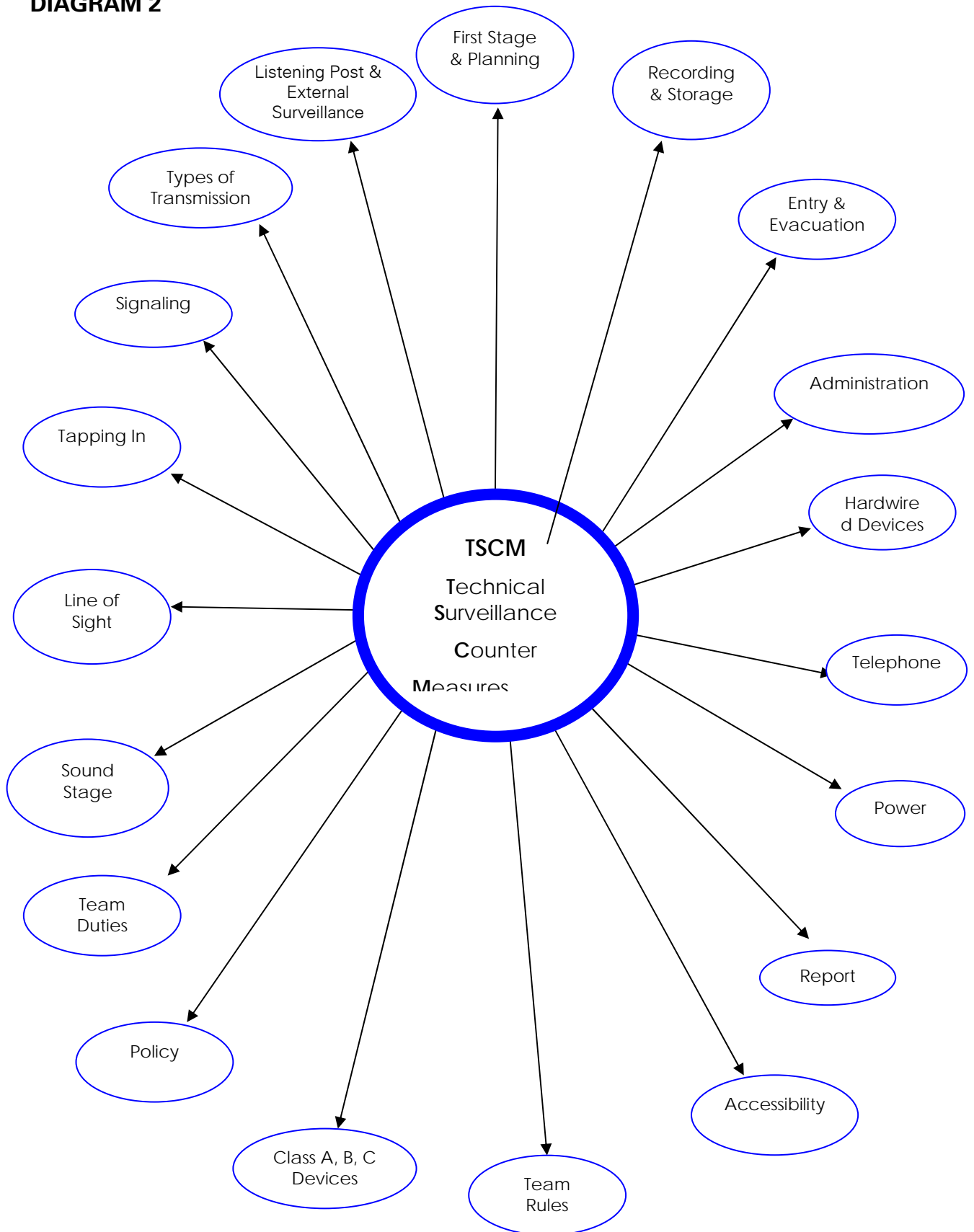




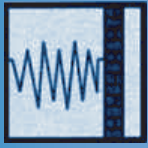
# Recommendations

# Sweep

DIAGRAM 2



# TSCM INDEX



1 - Introduction

2 - The Threat

3 - Recommendations

4 - Training Course Overview

5 - Training Course Syllabuses

6 - Recommended Products

7 - Technical Data Sheets

8 - IP/PABX Manipulation

9 - Commercial Quotations

10 - Terms & Conditions

11 - Contact Details

12 - Elaman Catalogs Overview

## TSCM Course List

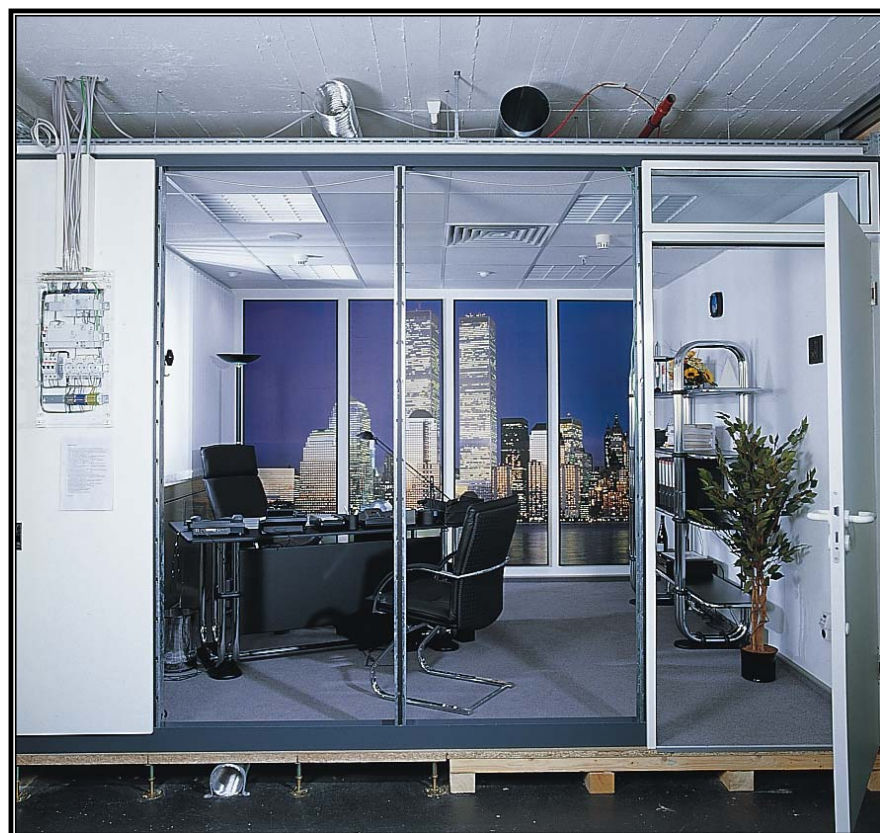
## Training

<b>TSCM Training COURSE overview</b>				
<b>Course No.</b>	<b>Course name</b>	<b>Duration</b>	<b>Location</b>	<b>Number of students</b>
8000	TSCM Search and Technical Course	2 weeks	Germany	6 students
8001	TSCM Advanced Cable Course	2 weeks	Germany	6 students
8002	TSCM Senior Management Course	1 week	Germany	4 students
8003	TSCM Technical Threat Course	1 week	Germany	6 students
8004	TSCM Product Training Course	2 weeks	Germany	6 students
8005	PBX Manipulation Course	1 week	Germany	6 students
8006	PBX Advanced Manipulation Course	1 week	Germany	8 students
8007	PBX Senior Engineer Course	2 weeks	Germany	6 students
8008	Anti-Hacking Course	1 week	Germany	6 students
8009	ISP Manipulation Advanced Course	2 weeks	Germany	6 students
8010	TSCM Threat Assessment	1 week	customer	6 students
8011	TSCM Sweep Team Review	1 week	customer	No limit
8012	TSCM Equipment Audit	1 week	customer	No limit
8013	TSCM Product Training Course	2 weeks	customer	No limit
8014	PBX-ISP Penetration Assessment	1 week	customer	6 students
8015	PBX Turnkey Service Support	1 year	Varies	individual
8016	TSCM Sweeping of Cars	1 week	Germany	4 students
8017	Computer Forensics	1 week	Germany	4 students
8018	TSCM IT Course	1 week	Germany	4 students

**Example of a TSCM Course Offer**

**Course Offer**

## **PROPOSAL FOR A 2-WEEK TSCM COURSE**



**TSCM TEST ROOM**

**LOCATION: TRAINING INSTITUTE AND END-USER LOCATIONS**

## Example of a TSCM Course Offer

## Course Offer

### TSCM TRAINING COURSE

**Duration:** 2 Weeks

**Qualifications:** On the successful completion of the course, all students will receive a certificate including an individual assessment.

**Student Group:** The course has been designed for Government Security Agencies responsible for managing and carrying out Technical Surveillance sweeps. The technical level of the course is tailored to each individual group. Specific threats concerning the students can be incorporated into the course. The training is designed for 6 people.

**Aim:** To up date and manage a Sweep Team with an introduction to all forms of technical espionage; the art of carrying out a sweep, including search and location in friendly and unfriendly environments incorporating documentation and reporting techniques.

**Language:** The course is conducted in English.

**Objectives:** At the end of the course students will be able to demonstrate an understanding of:

- The threat of technical espionage
- Set up and manage a Sweep Team
- Practical training
- Physical search
- Reporting and Documentation
- Pre-Sweep equipment selection

**Location:** German (students should fly to Nuremburg Airport)

**Basic Training Package includes:**

- All teaching, practical and course work in Germany
- Course notes in hard copy and CD-ROM
- Individual student assessment
- Recommendations for future development of skills and equipment
- Designed for 6 persons

**Rate:**

Hotel accommodation - includes three daily meals, laundry, daily rate for 6 persons

**Payment Terms:** 50% on confirmation  
25% on commencement  
25% on completion

## Example of a TSCM Training Institute

## Training

### LOCATION: TRAINING INSTITUTE AND END-USER LOCATIONS



**Training office**



**TSCM TEST ROOM**



**Training room**



**Ceiling training office**



## Example of a TSCM Training Institute

## Training



Lab 1-TSCM Planning



Lab 2-TSCM Equipments

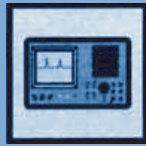
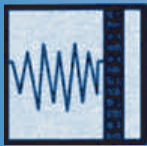


Lab 3-Pabx Manipulation



Lab sitting area

# TSCM INDEX



1 - Introduction

2 - The Threat

3 - Recommendations

4 - Training Course Overview

5 - Training Course Syllabuses

6 - Recommended Products

7 - Technical Data Sheets

8 - IP/PABX Manipulation

9 - Commercial Quotations

10 - Terms & Conditions

11 - Contact Details

12 - Elaman Catalogs Overview



# TSCM Search and Technical Course

# Model 8000

COURSE NO. 8000: TSCM SEARCH AND TECHNICAL COURSE (TSCM LAB EUROPE)					
	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY
<b>TOPICS 1ST WEEK</b>	<p><b>Introduction:</b></p> <ul style="list-style-type: none"> <li>Greeting</li> <li>Presentation of the company and syllabus</li> </ul> <p><b>The threat (1):</b></p> <ul style="list-style-type: none"> <li>Latest technologies</li> <li>Latest methods of wired and wireless transmissions</li> <li>Camouflage of bugs</li> <li>Demonstrations of sophisticated bugs</li> </ul>	<p><b>The threat (2):</b></p> <ul style="list-style-type: none"> <li>Telecommunication monitoring in PSTN</li> <li>In house wiretaps</li> <li>Monitoring of wireless transmissions</li> </ul> <p><b>Counter-measures:</b></p> <ul style="list-style-type: none"> <li>The prevention of bugging</li> <li>Bug-proof rooms</li> <li>Methods of TSCM</li> <li>Overview equipment</li> <li>Demonstrations</li> </ul>	<p><b>Practical training (1):</b></p> <p>Cable measurement:</p> <ul style="list-style-type: none"> <li>Overview: Methods of cable measurement</li> <li>Basics and limits of Time-Domain-Reflectometer (TDR)</li> <li>NF- and VLF-Detection</li> <li>Demonstrations</li> <li>Practical exercises by the students</li> </ul>	<p><b>Practical training (2):</b></p> <p>Cable measurement:</p> <ul style="list-style-type: none"> <li>Detection of unknown wires</li> <li>Using a LAN-Tester</li> <li>Oscilloscope</li> <li>Multimeters</li> <li>Other equipment for cable measurement</li> <li>Demonstrations</li> <li>Practical exercises by the students</li> <li>Repetition of cable measurement</li> </ul>	<p><b>Practical training (3):</b></p> <p>The physical search:</p> <ul style="list-style-type: none"> <li>Using NLJDs</li> <li>IR-Thermalvision</li> <li>Demonstrations and practical exercises</li> </ul> <p><b>The threat (3):</b></p> <ul style="list-style-type: none"> <li>Telecommunication and room monitoring by software attacks against ISDN PBXs</li> <li>Demonstrations</li> </ul>

# TSCM Search and Technical Course

# Model 8000

COURSE NO. 8000: TSCM SEARCH AND TECHNICAL COURSE (TSCM LAB EUROPE)					
	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY
<b>TOPICS 2ND WEEK</b>	<p><b>Practical training (4):</b> The physical search:</p> <ul style="list-style-type: none"> <li>• The visual inspection of rooms and technically devices</li> <li>• Endoscopes and Video-Endoscopes</li> <li>• X-ray inspection by different systems</li> <li>• Metal-Detection</li> <li>• Demonstrations and practical exercises</li> <li>• Other equipment</li> </ul>	<p><b>Practical training (5):</b> RF-Detection:</p> <ul style="list-style-type: none"> <li>• IR-Detection</li> <li>• Field strength- /Near-field-measurement</li> <li>• Sonic-Labeling and Silent Sound Correlation</li> <li>• Difference-Spectrum-Analysis</li> <li>• Demonstrations and practical exercises</li> <li>• Preparing for sweep</li> </ul>	<p><b>Practical exercise (1):</b></p> <ul style="list-style-type: none"> <li>• Complete sweep of the bugged training-room by the participants (using full equipment)</li> <li>• Support by experienced instructors</li> </ul> <p><b>Discussion:</b></p> <ul style="list-style-type: none"> <li>• Questions</li> <li>• Evaluation of the search results</li> </ul>	<p><b>Practical exercise (2):</b></p> <ul style="list-style-type: none"> <li>• Complete sweep of a bugged conference-room by the participants (using reduced equipment)</li> <li>• Support by experienced instructors</li> </ul> <p><b>Discussion:</b></p> <ul style="list-style-type: none"> <li>• Questions</li> <li>• Evaluation of the search results</li> </ul>	<p><b>Practical exercise (3):</b></p> <ul style="list-style-type: none"> <li>• Complete sweep of a bugged hotel room by the participants (using minimum equipment)</li> <li>• Support by experienced instructors</li> </ul> <p><b>Summary:</b></p> <ul style="list-style-type: none"> <li>• Questions/results</li> <li>• Final discussion about the course</li> </ul>

# TSCM Advanced Cable Course

# Model 8001

COURSE NO. 8001: TSCM ADVANCED CABLE COURSE (AT COBURG/GERMANY)					
	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY
<b>TOPICS 1ST WEEK</b>	<p><b>Introduction:</b></p> <ul style="list-style-type: none"> <li>Greeting</li> <li>Presentation of the company and syllabus</li> </ul> <p><b>The threat (1):</b></p> <ul style="list-style-type: none"> <li>State-of-the-art technologies of wired transmissions</li> <li>Camouflage of bugs</li> <li>Demonstrations of sophisticated bugs</li> </ul>	<p><b>The threat (2):</b></p> <ul style="list-style-type: none"> <li>Overview telecommunication monitoring today</li> <li>Hard- and Software attacks</li> </ul> <p><b>Countermeasures:</b></p> <ul style="list-style-type: none"> <li>The prevention of wire tapping</li> <li>Bug-proof rooms</li> <li>Overview cable measurement</li> <li>Demonstrations</li> </ul>	<p><b>Practical training (1):</b></p> <p>RF detection for cable surveys:</p> <ul style="list-style-type: none"> <li>Field strength-/and Near field-measurement</li> <li>Sonic-Labeling and Silent Sound Correlation</li> <li>Difference-Spectrum-Analysis</li> <li>Demonstrations</li> <li>Practical exercises by the students</li> </ul>	<p><b>Practical training (2):</b></p> <p>The physical search for cable surveys:</p> <ul style="list-style-type: none"> <li>Using NLJDs</li> <li>Endoscopes and Video-Endoscopes</li> <li>X-ray inspection by different systems</li> <li>Other equipment</li> <li>Demonstrations</li> <li>Practical exercises by the students</li> </ul>	<p><b>Practical exercise (1):</b></p> <ul style="list-style-type: none"> <li>Physical check of bugged and tapped telecommunication facilities, telephone sets, adapters, plugs, and other accessories by the students</li> <li>Support by an experienced instructor</li> </ul> <p><b>Discussion:</b></p> <ul style="list-style-type: none"> <li>Questions/results</li> </ul>

# TSCM Advanced Cable Course

# Model 8001

COURSE NO. 8001: TSCM ADVANCED CABLE COURSE (AT COBURG/GERMANY)					
	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY
TOPICS 2ND WEEK	<p><b>Practical training (3):</b> Cable measurement:</p> <ul style="list-style-type: none"> <li>• The inductive Detection of unknown wires</li> <li>• NF- and VLF-Detection</li> <li>• Multi meters</li> <li>• Oscilloscopes</li> <li>• Demonstrations</li> <li>• Practical exercises by the students</li> </ul>	<p><b>Practical training (4):</b> Cable measurement:</p> <ul style="list-style-type: none"> <li>• Time-Domain-Reflectometer (TDR) as the main method:               <ul style="list-style-type: none"> <li>- Physical basics</li> <li>- Advantages and disadvantages</li> <li>- Limits of this technology</li> </ul> </li> <li>• Demonstrations</li> <li>• Practical exercises by the students</li> </ul>	<p><b>Practical training (5):</b> Cable measurement:</p> <ul style="list-style-type: none"> <li>• Using a LAN-Tester in structured networks (e.g. CAT5)</li> <li>• Demonstrations</li> <li>• Other equipment for cable measurement</li> <li>• Demonstrations</li> <li>• Practical exercises by the students</li> <li>• Preparing for the exercises next day</li> </ul>	<p><b>Practical exercise (2):</b></p> <ul style="list-style-type: none"> <li>• Cable sweep of tapped in-house wiring by the students</li> <li>• Support by an experienced instructor</li> </ul> <p><b>Discussion:</b></p> <ul style="list-style-type: none"> <li>• Questions/results</li> <li>• Preparing for the exercises next day</li> </ul>	<p><b>Practical exercise (3):</b></p> <ul style="list-style-type: none"> <li>• Cable sweep of unknown tapped wiring between buildings by the students</li> <li>• Support by an experienced instructor</li> </ul> <p><b>Summary:</b></p> <ul style="list-style-type: none"> <li>• Questions/results</li> <li>• Final discussion about the course</li> </ul>

# TSCM Senior Management Course

# Model 8002

COURSE NO. 8002: TSCM SENIOR MANAGEMENT COURSE (TSCM LAB EUROPE)					
	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY
TOPICS	<p><b>Introduction:</b></p> <ul style="list-style-type: none"> <li>Greeting</li> <li>Presentation of the company and syllabus</li> </ul> <p><b>Countermeasures:</b></p> <ul style="list-style-type: none"> <li>The prevention of bugging</li> <li>Bug-proof rooms</li> <li>Methods of TSCM</li> <li>Overview of equipment</li> <li>Demonstrations</li> </ul>	<p><b>Management (1):</b></p> <p>TSCM for Supervisors:</p> <ul style="list-style-type: none"> <li>Typical tasks of a sweep team</li> <li>How to set up a sweep team</li> <li>The personnel requirements</li> <li>The technical requirements</li> <li>Managing a sweep team</li> </ul> <p><b>Discussion:</b></p> <ul style="list-style-type: none"> <li>Questions</li> </ul>	<p><b>Management (2):</b></p> <p>TSCM for Supervisors:</p> <ul style="list-style-type: none"> <li>Why and how to carry out location checks</li> <li>Known, unknown, own and strange buildings</li> <li>Organizational aids:               <ul style="list-style-type: none"> <li>Checklists</li> <li>Software</li> </ul> </li> <li>Domestic and foreign logistics</li> </ul> <p><b>Discussion:</b></p> <ul style="list-style-type: none"> <li>Questions</li> </ul>	<p><b>Management (3):</b></p> <p>TSCM for Supervisors:</p> <ul style="list-style-type: none"> <li>Preparing a sweep</li> <li>How to carry out sweeps abroad</li> <li>Improvised sweeps</li> <li>The supervision of a sweep</li> <li>Reporting and documentation               <ul style="list-style-type: none"> <li>Photos</li> <li>Written reports</li> <li>Databases</li> </ul> </li> </ul> <p><b>Discussion:</b></p> <ul style="list-style-type: none"> <li>Questions</li> </ul>	<p><b>Practical exercise:</b></p> <ul style="list-style-type: none"> <li>Supervision of a sweep by the students (sweep carried out by the organizer's sweep team)</li> <li>Support by experienced instructors</li> </ul> <p><b>Summary:</b></p> <ul style="list-style-type: none"> <li>Questions/results</li> <li>Final discussion about the course</li> </ul>

# TSCM Product Training Course

# Model 8004

COURSE NO. 8004: TSCM PRODUCT TRAINING COURSE (TSCM LAB EUROPE)					
	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY
<b>TOPICS 1ST WEEK</b>	<p><b>Introduction:</b></p> <ul style="list-style-type: none"> <li>Greeting</li> <li>Presentation of the company and syllabus</li> </ul> <p><b>Repetition:</b></p> <ul style="list-style-type: none"> <li>Latest methods of wired and wireless transmissions</li> <li>Camouflage of bugs</li> <li>Methods of TSCM</li> <li>Overview equipment</li> <li>Demonstrations</li> </ul>	<p><b>Product training (1):</b></p> <p>Detection of active wireless transmissions:</p> <ul style="list-style-type: none"> <li>IR-Detection</li> <li>Field strength-measurement</li> <li>Near field-measurement</li> <li>Frequency-Counters and other Receivers</li> <li>Practical exercises by the students</li> </ul>	<p><b>Product training (2):</b></p> <p>Detection of active wireless transmissions:</p> <ul style="list-style-type: none"> <li>Sonic-Labeling</li> <li>Silent Sound Correlation</li> <li>Spectrum-Analysis</li> <li>Difference-Spectrum-Analysis</li> <li>Practical exercises by the students</li> <li>Repetition of RF-measurement</li> </ul>	<p><b>Product training (3):</b></p> <p>The physical search:</p> <ul style="list-style-type: none"> <li>Using NLJDs</li> <li>(Dis-)advantages of different types</li> <li>Metal-Detection by different systems</li> <li>IR-Thermal vision for TSCM (active and passive)</li> <li>Practical exercises by the students</li> </ul>	<p><b>Product training (4):</b></p> <p>The physical search:</p> <ul style="list-style-type: none"> <li>The visual inspection of rooms and technical devices</li> <li>Endoscopes and Video-Endoscopes</li> <li>X-ray inspection by different systems</li> <li>Other equipment</li> <li>Practical exercises by the students</li> <li>Repetition of the physical search</li> </ul>

# TSCM Product Training Course

**Model 8004**

COURSE NO. 8004: TSCM PRODUCT TRAINING COURSE (TSCM LAB EUROPE)					
	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY
<b>TOPICS 2ND WEEK</b>	<p><b>Product training (5):</b> Cable measurement:</p> <ul style="list-style-type: none"> <li>• The inductive Detection of unknown wires</li> <li>• NF- and VLF-Detection</li> <li>• Multimeters</li> <li>• Oscilloscopes</li> <li>• Practical exercises by the students</li> </ul>	<p><b>Product training (6):</b> Cable measurement:</p> <ul style="list-style-type: none"> <li>• Time-Domain-Reflectometer (TDR) as the main method:               <ul style="list-style-type: none"> <li>- Physical basics</li> <li>- Advantages and disadvantages</li> <li>- Limitations of this technology</li> </ul> </li> <li>• Practical exercises by the students</li> </ul>	<p><b>Product training (7):</b> Cable measurement:</p> <ul style="list-style-type: none"> <li>• Using a LAN-Tester in structured networks (e.g. CAT5)</li> <li>• Demonstrations</li> <li>• Other equipment for cable measurement</li> <li>• Practical exercises by the students</li> <li>• Preparing for the sweeps next days</li> </ul>	<p><b>Practical exercise (1):</b></p> <ul style="list-style-type: none"> <li>• Sweep of the bugged training-room by the students (using full equipment)</li> <li>• Support by an experienced instructor</li> </ul> <p><b>Discussion:</b></p> <ul style="list-style-type: none"> <li>• Questions</li> <li>• Evaluation of the search results</li> </ul>	<p><b>Practical exercise (2):</b></p> <ul style="list-style-type: none"> <li>• Sweep of a bugged hotel room by the students</li> <li>• Support by an experienced instructor</li> </ul> <p><b>Summary:</b></p> <ul style="list-style-type: none"> <li>• Questions</li> <li>• Evaluation of the search results</li> <li>• Final discussion about the course</li> </ul>

# PBX Manipulation Course

# Model 8005

COURSE NO. 8005: PBX MANIPULATION COURSE (TSCM LAB EUROPE)					
	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY
TOPICS	<p><b>Introduction:</b></p> <ul style="list-style-type: none"> <li>Greeting</li> <li>Presentation of the company and syllabus</li> </ul> <p><b>The threat (1):</b> Software attacks against ISDN PBXs:</p> <ul style="list-style-type: none"> <li>Telecommunication and room monitoring by software</li> <li>Hacking of PBX remote-access-ports</li> <li>Typical mistakes in configuration</li> </ul>	<p><b>Practical training (1):</b> Software attacks against ISDN PBXs demonstrated on different types:</p> <ul style="list-style-type: none"> <li>War-dialling and Live-Hacking</li> <li>Manipulation of PBX features for telecommunication and room monitoring</li> <li>Interception of VoIP</li> <li>WAN-LAN-access</li> <li>Demonstrations</li> <li>Practical exercises by the students</li> </ul>	<p><b>The threat (2):</b></p> <ul style="list-style-type: none"> <li>In-house Wiretaps</li> <li>The bugging of extensions and telecommunication equipment</li> <li>Demonstrations</li> </ul> <p><b>Practical training (2):</b> Cable measurement:</p> <ul style="list-style-type: none"> <li>Overview: Methods of cable measurement</li> <li>Demonstrations</li> <li>Practical exercises by the students</li> </ul>	<p><b>Practical training (3):</b> Cable measurement:</p> <ul style="list-style-type: none"> <li>Detection of unknown wires</li> <li>NF- and VLF-Detection</li> <li>Basics and limits of Time-Domain-Reflectometer (TDR)</li> <li>Using a LAN-Tester</li> <li>Other equipment for cable measurement</li> <li>Demonstrations</li> <li>Practical exercises by the Students</li> </ul>	<p><b>The threat (3):</b></p> <ul style="list-style-type: none"> <li>Telecommunication monitoring in PSTN</li> <li>Monitoring of wireless transmissions</li> <li>Demonstrations</li> </ul> <p><b>Countermeasures</b></p> <ul style="list-style-type: none"> <li>Software Audits and the protection of PBXs and wiring</li> </ul> <p><b>Summary:</b></p> <ul style="list-style-type: none"> <li>Questions</li> <li>Final discussion about the course</li> </ul>



# PBX Advanced Manipulation Course

# Model 8006

COURSE NO. 8006: PBX ADVANCED MANIPULATION COURSE (TSCM LAB EUROPE)					
	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY
TOPICS	<p><b>Introduction:</b></p> <ul style="list-style-type: none"> <li>Greeting</li> <li>Presentation: Company and syllabus</li> </ul> <p><b>The threat:</b> Software attacks against ISDN and VoIP PBXs:</p> <ul style="list-style-type: none"> <li>Monitoring by software</li> <li>Hacking of PBX remote-access-ports</li> <li>Typical mistakes in configuration</li> </ul>	<p><b>Practical training (1):</b> PBX manipulations of SIEMENS Hi path 4000: Demonstrations and practical exercises:</p> <ul style="list-style-type: none"> <li>Basics</li> <li>War-dialling and Live-Hacking</li> <li>Manipulation of PBX features for Monitoring</li> <li>WAN-LAN-access</li> <li>Countermeasures and Software Audits</li> </ul>	<p><b>Practical training (2):</b> PBX manipulations of NORTEL Meridian 1: Demonstrations and practical exercises:</p> <ul style="list-style-type: none"> <li>Basics</li> <li>The difficulty of NORTEL-Hacking</li> <li>Manipulation of PBX features for Monitoring</li> <li>WAN-LAN-access</li> <li>Countermeasures and Software Audits</li> </ul>	<p><b>Practical training (3):</b> PBX manipulations of ALCATEL Omni PCX 4400: Demonstrations and practical exercises:</p> <ul style="list-style-type: none"> <li>Basics</li> <li>War-dialling and Live-Hacking</li> <li>Manipulation of PBX features for Monitoring</li> <li>WAN-LAN-access</li> <li>Countermeasures and Software Audits</li> </ul>	<p><b>Practical training (4):</b> PBX manipulations of ERICSSON MD110: Demonstrations and practical exercises:</p> <ul style="list-style-type: none"> <li>Basics</li> <li>The difficulty of ERICSSON-Hacking</li> <li>Manipulation of PBX features for Monitoring</li> <li>WAN-LAN-access</li> <li>Countermeasures and Software Audits</li> <li>Questions</li> <li>Final discussion about the course</li> </ul>

# PBX Senior Engineer Course

# Model 8007

COURSE NO. 8007: PBX SENIOR ENGINEER COURSE (TSCM LAB EUROPE)					
	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY
TOPICS 1ST WEEK	<p><b>Introduction:</b></p> <ul style="list-style-type: none"> <li>Greeting</li> <li>Presentation: Company and syllabus</li> </ul> <p><b>The threat (1):</b> Software attacks against ISDN and VoIP PBXs:</p> <ul style="list-style-type: none"> <li>Monitoring by software</li> <li>Hacking of PBX remote-access-ports</li> <li>Typical mistakes in configuration</li> </ul>	<p><b>Practical training (1):</b> PBX manipulations of SIEMENS Hi path 4000: Demonstrations and practical exercises:</p> <ul style="list-style-type: none"> <li>Basics</li> <li>War-dialling and Live-Hacking</li> <li>Manipulation of PBX features for Monitoring</li> <li>WAN-LAN-access</li> <li>Countermeasures and Software Audits</li> </ul>	<p><b>Practical training (2):</b> PBX manipulations of NORTEL Meridian 1: Demonstrations and practical exercises:</p> <ul style="list-style-type: none"> <li>Basics</li> <li>The difficulty of NORTEL-Hacking</li> <li>Manipulation of PBX features for Monitoring</li> <li>WAN-LAN-access</li> <li>Countermeasures and Software Audits</li> </ul>	<p><b>Practical training (3):</b> PBX manipulations of ALCATEL Omni PCX 4400: Demonstrations and practical exercises:</p> <ul style="list-style-type: none"> <li>Basics</li> <li>War-dialling and Live-Hacking</li> <li>Manipulation of PBX features for Monitoring</li> <li>WAN-LAN-access</li> <li>Countermeasures and Software Audits</li> </ul>	<p><b>Practical training (4):</b> PBX manipulations of ERICSSON MD110: Demonstrations and practical exercises:</p> <ul style="list-style-type: none"> <li>Basics</li> <li>The difficulty of ERICSSON-Hacking</li> <li>Manipulation of PBX features for Monitoring</li> <li>WAN-LAN-access</li> <li>Countermeasures and Software Audits</li> </ul>

# PBX Senior Engineer Course

# Model 8007

COURSE NO. 8007: PBX SENIOR ENGINEER COURSE (TSCM LAB EUROPE)					
	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY
<b>TOPICS 2ND WEEK</b>	<p><b>Practical training (5):</b> Additional practical exercises by the students:</p> <ul style="list-style-type: none"> <li>• War-dialling and Live-Hacking</li> <li>• Interception of VoIP</li> <li>• The protection of PBXs</li> </ul> <p><b>Discussion:</b></p> <ul style="list-style-type: none"> <li>• Questions</li> <li>• Repetition</li> </ul>	<p><b>Practical training (6):</b> Additional practical exercises by the students:</p> <ul style="list-style-type: none"> <li>• Manipulation of PBX features for Monitoring on SIEMENS, ERICSSON, ALCATEL and NORTEL platforms</li> </ul> <p><b>Discussion:</b></p> <ul style="list-style-type: none"> <li>• Questions</li> <li>• Repetition</li> </ul>	<p><b>The threat (2):</b></p> <ul style="list-style-type: none"> <li>• In-house Wiretaps</li> <li>• The bugging of extensions and telecommunication equipment</li> <li>• Demonstrations</li> </ul> <p><b>Practical training (7):</b> Cable measurement:</p> <ul style="list-style-type: none"> <li>• Overview: Methods of cable measurement</li> </ul>	<p><b>Practical training (8):</b> Cable measurement:</p> <ul style="list-style-type: none"> <li>• Basics and limits of Time-Domain-Reflectometer (TDR)</li> <li>• NF- and VLF-Detection</li> <li>• Oscilloscope</li> <li>• Multimeters</li> <li>• Demonstrations</li> <li>• Practical exercises by the students</li> </ul>	<p><b>Practical training (9):</b> Cable measurement:</p> <ul style="list-style-type: none"> <li>• Detection of unknown wires</li> <li>• Using a LAN-Tester</li> <li>• Other equipment for cable measurement</li> <li>• Demonstrations and practical exercises</li> </ul> <p><b>Summary:</b></p> <ul style="list-style-type: none"> <li>• Questions</li> <li>• Final discussion about the course</li> </ul>

# Anti-Hacking Course

# Model 8008

COURSE NO. 8008: ANTI-HACKING COURSE (TSCM LAB EUROPE)					
	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY
<b>Topics</b>	<p><b>Introduction:</b></p> <ul style="list-style-type: none"> <li>Greeting</li> <li>Presentation: Company and syllabus</li> </ul> <p><b>The threat (1):</b></p> <p>Hacking for Administrators</p> <ul style="list-style-type: none"> <li>Hacking tools</li> <li>Virus construction sets and Trojans</li> <li>Port-scanning</li> <li>Buffer Overflows</li> <li>URL attacks</li> <li>Path climbing</li> <li>Browser attacks</li> <li>Demonstrations</li> </ul>	<p><b>The threat (2):</b></p> <p>Hacking for Administrators</p> <ul style="list-style-type: none"> <li>Man-in-the-Middle attacks (encryption)</li> <li>Firewall Hacking</li> <li>Advanced scanning techniques</li> <li>Scanning tools</li> <li>Boot attacks</li> <li>DoS and DDoS</li> <li>Password-Cracking</li> <li>Attacks against Web-Applications</li> <li>Social engineering</li> <li>Demonstrations and practical exercises</li> </ul>	<p><b>Practical training (1):</b></p> <p>LAN and Internet-Live-Hacking:</p> <ul style="list-style-type: none"> <li>LAN-Sniffing</li> <li>Firewall "Piercing"</li> <li>DNS Spoofing</li> <li>DoS attack</li> <li>Boot attack demo</li> <li>Penetration testing</li> <li>Security tools</li> <li>Demonstrations</li> <li>Practical exercises by the students</li> </ul>	<p><b>Practical training (2):</b></p> <p>WLAN-Hacking:</p> <ul style="list-style-type: none"> <li>Basics of WLAN technology</li> <li>WLAN Implementing</li> <li>WLAN Hacking tools</li> <li>WLAN Sniffing</li> <li>Penetration testing</li> <li>DoS against WLAN</li> <li>WLAN Security</li> <li>Demonstrations</li> <li>Practical exercises by the students</li> <li>Common War Driving (live test)</li> </ul>	<p><b>Practical training (3):</b></p> <p>IT-Forensic:</p> <ul style="list-style-type: none"> <li>LAN-Analysis</li> <li>Basics of File Systems</li> <li>Preparing Images, e.g. from HDD, RAM</li> <li>Securing of fleeting evidence</li> <li>Recovery of deleted evidence</li> <li>Demonstrations</li> </ul> <p><b>Summary:</b></p> <ul style="list-style-type: none"> <li>Questions/results</li> <li>Final discussion about the course</li> </ul>

# Anti-Hacking Course

# Model 8008

COURSE NO. 8008: ANTI-HACKING COURSE (TSCM LAB EUROPE)						
	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	
TOPICS 2ND WEEK	<p><b>Practical training (5):</b> Additional practical exercises by the students:</p> <ul style="list-style-type: none"> <li>• War-dialling and Live-Hacking</li> <li>• Interception of VoIP</li> <li>• The protection of PBXs</li> </ul> <p><b>Discussion:</b></p> <ul style="list-style-type: none"> <li>• Questions</li> <li>• Repetition</li> </ul>	<p><b>Practical training (6):</b> Additional practical exercises by the students:</p> <ul style="list-style-type: none"> <li>• Manipulation of PBX features for Monitoring on SIEMENS, ERICSSON, ALCATEL and NORTEL platforms</li> </ul> <p><b>Discussion:</b></p> <ul style="list-style-type: none"> <li>• Questions</li> <li>• Repetition</li> </ul>	<p><b>The threat (2):</b></p> <ul style="list-style-type: none"> <li>• In-house Wiretaps</li> <li>• The bugging of extensions and telecommunication equipment</li> <li>• Demonstrations</li> </ul> <p><b>Practical training (7):</b> Cable measurement:</p> <ul style="list-style-type: none"> <li>• Overview: Methods of cable measurement</li> </ul>	<p><b>Practical training (8):</b> Cable measurement:</p> <ul style="list-style-type: none"> <li>• Basics and limits of Time-Domain-Reflectometer (TDR)</li> <li>• NF- and VLF-Detection</li> <li>• Oscilloscope</li> <li>• Multimeters</li> <li>• Demonstrations</li> <li>• Practical exercises by the students</li> </ul>	<p><b>Practical training (9):</b> Cable measurement:</p> <ul style="list-style-type: none"> <li>• Detection of unknown wires</li> <li>• Using a LAN-Tester</li> <li>• Other equipment for cable measurement</li> <li>• Demonstrations and practical exercises</li> </ul> <p><b>Summary:</b></p> <ul style="list-style-type: none"> <li>• Questions</li> <li>• Final discussion about the course</li> </ul>	

# TSCM Sweep Team Review

# Model 8011

COURSE NO. 8011: TSCM SWEEP TEAM REVIEW (END USER COUNTRY)					
	SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY
<b>TOPICS</b>	<p><b>Introduction:</b></p> <ul style="list-style-type: none"> <li>• Visiting the customer's facilities</li> <li>• Checking the existing TSCM equipment</li> </ul> <p><b>Repetition</b></p> <p><b>Countermeasures:</b></p> <ul style="list-style-type: none"> <li>• The prevention</li> <li>• Methods of TSCM</li> <li>• Overview equipment</li> <li>• Preparing for the sweep next day</li> </ul>	<p><b>Practical exercise (1):</b></p> <ul style="list-style-type: none"> <li>• Sweep of a bugged hotel room by the students</li> <li>• Support by an experienced instructor</li> </ul> <p><b>Discussion:</b></p> <ul style="list-style-type: none"> <li>• Questions</li> <li>• Evaluation of the search results</li> <li>• Preparing for the sweep next day</li> </ul>	<p><b>Practical exercise (2):</b></p> <ul style="list-style-type: none"> <li>• Sweep of a bugged conference room by the students</li> <li>• Support by an experienced instructor</li> </ul> <p><b>Discussion:</b></p> <ul style="list-style-type: none"> <li>• Questions</li> <li>• Evaluation of the search results</li> <li>• Preparing for the sweep next day</li> </ul>	<p><b>Practical exercise (3):</b></p> <ul style="list-style-type: none"> <li>• Sweep of a bugged office by the students</li> <li>• Support by an experienced instructor</li> </ul> <p><b>Discussion:</b></p> <ul style="list-style-type: none"> <li>• Questions</li> <li>• Evaluation of the search results</li> <li>• Preparing for the sweep next day</li> </ul>	<p><b>Practical exercise (4):</b></p> <ul style="list-style-type: none"> <li>• Sweep of a bugged living room by the students</li> <li>• Support by an experienced instructor</li> </ul> <p><b>Summary:</b></p> <ul style="list-style-type: none"> <li>• Questions</li> <li>• Evaluation of the search results</li> <li>• Final discussion about the course</li> </ul>

# TSCM Sweep Team Review

# Model 8011

COURSE NO. 8011: TSCM SWEEP TEAM REVIEW (END USER COUNTRY)					
	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY
<b>TOPICS 2ND WEEK</b>	<p><b>Practical training (5):</b> Additional practical exercises by the students:</p> <ul style="list-style-type: none"> <li>• War-dialling and Live-Hacking</li> <li>• Interception of VoIP</li> <li>• The protection of PBXs</li> </ul> <p><b>Discussion:</b></p> <ul style="list-style-type: none"> <li>• Questions</li> <li>• Repetition</li> </ul>	<p><b>Practical training (6):</b> Additional practical exercises by the students:</p> <ul style="list-style-type: none"> <li>• Manipulation of PBX features for Monitoring on SIEMENS, ERICSSON, ALCATEL and NORTEL platforms</li> </ul> <p><b>Discussion:</b></p> <ul style="list-style-type: none"> <li>• Questions</li> <li>• Repetition</li> </ul>	<p><b>The threat (2):</b></p> <ul style="list-style-type: none"> <li>• In-house Wiretaps</li> <li>• The bugging of extensions and telecommunication equipment</li> <li>• Demonstrations</li> </ul> <p><b>Practical training (7):</b> Cable measurement:</p> <ul style="list-style-type: none"> <li>• Overview: Methods of cable measurement</li> </ul>	<p><b>Practical training (8):</b> Cable measurement:</p> <ul style="list-style-type: none"> <li>• Basics and limits of Time-Domain-Reflectometer (TDR)</li> <li>• NF- and VLF-Detection</li> <li>• Oscilloscope</li> <li>• Multimeters</li> <li>• Demonstrations</li> <li>• Practical exercises by the students</li> </ul>	<p><b>Practical training (9):</b> Cable measurement:</p> <ul style="list-style-type: none"> <li>• Detection of unknown wires</li> <li>• Using a LAN-Tester</li> <li>• Other equipment for cable measurement</li> <li>• Demonstrations and practical exercises</li> </ul> <p><b>Summary:</b></p> <ul style="list-style-type: none"> <li>• Questions</li> <li>• Final discussion about the course</li> </ul>

# TSCM Equipment Audit

# Model 8012

COURSE NO. 8012: TSCM EQUIPMENT AUDIT (END USER COUNTRY)					
	SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY
<b>TOPICS</b>	<p><b>Introduction:</b></p> <ul style="list-style-type: none"> <li>• Visiting the customer’s facilities</li> <li>• Checking the existing TSCM equipment</li> </ul> <p><b>Repetition: The threat (1):</b></p> <ul style="list-style-type: none"> <li>• Latest technologies of technical espionage</li> <li>• Latest methods of wired and wireless transmissions</li> <li>• Camouflage of bugs</li> </ul>	<p><b>Repetition: The threat (2):</b></p> <ul style="list-style-type: none"> <li>• Telecommunication monitoring in PSTN</li> <li>• In-house Wiretaps</li> <li>• Monitoring of wireless transmissions</li> </ul> <p><b>Repetition: Countermeasures:</b></p> <ul style="list-style-type: none"> <li>• The prevention of bugging</li> <li>• Bug-proof rooms</li> <li>• Methods of TSCM</li> <li>• Overview equipment</li> </ul> <p><b>Discussion:</b></p> <ul style="list-style-type: none"> <li>• Questions</li> </ul>	<p><b>Practical training (1):</b></p> <p>Cable measurement with the customer’s equipment:</p> <ul style="list-style-type: none"> <li>• Detection of unknown wires</li> <li>• NF- and VLF-Detection</li> <li>• Basics and limits of Time-Domain-Reflectometer (TDR)</li> <li>• Using a LAN-Tester</li> <li>• Other equipment for cable measurement</li> <li>• Demonstrations</li> <li>• Practical exercises by the Students</li> </ul>	<p><b>Practical training (2):</b></p> <p>The physical search with the customer’s equipment:</p> <ul style="list-style-type: none"> <li>• Visual inspection of rooms and technical equipment</li> <li>• Using optical Endoscopes and other optical aids</li> <li>• X-ray inspection</li> <li>• Using the NLJD</li> <li>• Metal-Detection</li> <li>• Other equipment for physical search</li> <li>• Demonstrations</li> <li>• Practical exercises by the Students</li> </ul>	<p><b>Practical training (3):</b></p> <p>RF-Detection with the customer’s equipment:</p> <ul style="list-style-type: none"> <li>• IR-Detection</li> <li>• Field strength- /Near-field-measurement</li> <li>• Sonic-Labeling and Silent Sound Correlation</li> <li>• Spectrum-Analysis</li> <li>• Other equipment for RF-measurement</li> <li>• Practical exercises by the Students</li> </ul> <p><b>Summary:</b></p> <ul style="list-style-type: none"> <li>• Final discussion about the course</li> </ul>



# TSCM Equipment Audit

# Model 8012

COURSE NO. 8012: TSCM EQUIPMENT AUDIT (END USER COUNTRY)					
	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY
<b>TOPICS 2ND WEEK</b>	<p><b>Practical training (5):</b> Additional practical exercises by the students:</p> <ul style="list-style-type: none"> <li>• War-dialling and Live-Hacking</li> <li>• Interception of VoIP</li> <li>• The protection of PBXs</li> </ul> <p><b>Discussion:</b></p> <ul style="list-style-type: none"> <li>• Questions</li> <li>• Repetition</li> </ul>	<p><b>Practical training (6):</b> Additional practical exercises by the students:</p> <ul style="list-style-type: none"> <li>• Manipulation of PBX features for Monitoring on SIEMENS, ERICSSON, ALCATEL and NORTEL platforms</li> </ul> <p><b>Discussion:</b></p> <ul style="list-style-type: none"> <li>• Questions</li> <li>• Repetition</li> </ul>	<p><b>The threat (2):</b></p> <ul style="list-style-type: none"> <li>• In-house Wiretaps</li> <li>• The bugging of extensions and telecommunication equipment</li> <li>• Demonstrations</li> </ul> <p><b>Practical training (7):</b> Cable measurement:</p> <ul style="list-style-type: none"> <li>• Overview: Methods of cable measurement</li> </ul>	<p><b>Practical training (8):</b> Cable measurement:</p> <ul style="list-style-type: none"> <li>• Basics and limits of Time-Domain-Reflectometer (TDR)</li> <li>• NF- and VLF-Detection</li> <li>• Oscilloscope</li> <li>• Multimeters</li> <li>• Demonstrations</li> <li>• Practical exercises by the students</li> </ul>	<p><b>Practical training (9):</b> Cable measurement:</p> <ul style="list-style-type: none"> <li>• Detection of unknown wires</li> <li>• Using a LAN-Tester</li> <li>• Other equipment for cable measurement</li> <li>• Demonstrations and practical exercises</li> </ul> <p><b>Summary:</b></p> <ul style="list-style-type: none"> <li>• Questions</li> <li>• Final discussion about the course</li> </ul>

# TSCM Product Training Course

# Model 8013

COURSE NO. 8013: TSCM PRODUCT TRAINING COURSE (END USER COUNTRY)					
	SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY
<b>1ST WEEK (INSTRUCTOR 1)</b>	<p><b>Introduction:</b></p> <ul style="list-style-type: none"> <li>• Visiting the customer's facilities</li> <li>• Checking the existing equipment for RF- and cable measurement</li> </ul> <p><b>Product training (1):</b></p> <ul style="list-style-type: none"> <li>• Overview: Cable measurement</li> <li>• Practical exercises</li> </ul>	<p><b>Product training (2):</b></p> <p>Cable measurement with the customer's equipment:</p> <ul style="list-style-type: none"> <li>• NF- and VLF-Detection</li> <li>• Detection of unknown wires</li> <li>• Basics and limits of Time-Domain-Reflectometer (TDR)</li> <li>• Practical exercises</li> </ul>	<p><b>Product training (3):</b></p> <p>Cable measurement with the customer's equipment:</p> <ul style="list-style-type: none"> <li>• Oscilloscope</li> <li>• Multimeters</li> <li>• Using a LAN-Tester</li> <li>• Other equipment for cable measurement</li> <li>• Practical exercises</li> <li>• Repetition of cable measurement</li> </ul>	<p><b>Product training (4):</b></p> <p>Detection of active wireless transmissions:</p> <ul style="list-style-type: none"> <li>• IR-Detection</li> <li>• Field strength-measurement</li> <li>• Near field-measurement</li> <li>• Frequency-Counters and other Receivers</li> <li>• Practical exercises</li> </ul>	<p><b>Product training (5):</b></p> <p>Detection of active wireless transmissions:</p> <ul style="list-style-type: none"> <li>• Sonic-Labeling</li> <li>• Silent Sound Correlation</li> <li>• Spectrum-Analysis</li> <li>• Difference-Spectrum-Analysis</li> <li>• Practical exercises</li> <li>• Repetition of RF-measurement</li> </ul>

# TSCM Product Training Course

# Model 8013

COURSE NO. 8013: TSCM PRODUCT TRAINING COURSE (END USER COUNTRY)					
	SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY
2ND WEEK (INSTRUCTOR 2)	<p><b>Introduction:</b></p> <ul style="list-style-type: none"> <li>• Visiting the customers facilities</li> <li>• Checking the existing equipment for physical search</li> </ul> <p><b>Product training (6):</b> The physical search measurement with the customer's equipment:</p> <ul style="list-style-type: none"> <li>• Using NLJDs</li> <li>• (Dis-)advantages of different types</li> <li>• Practical exercises</li> </ul>	<p><b>Product training (7):</b> The physical search:</p> <ul style="list-style-type: none"> <li>• Metal-Detection</li> <li>• IR-Thermal vision</li> <li>• Visual inspection</li> <li>• Endoscopes and Video-Endoscopes</li> <li>• X-ray inspection by different systems</li> <li>• Other equipment</li> <li>• Practical exercises</li> <li>• Repetition of physical search</li> <li>• Preparing for sweep the next day</li> </ul>	<p><b>Practical exercise (1):</b></p> <ul style="list-style-type: none"> <li>• Sweep of a bugged office by the students (using full equipment)</li> <li>• Support by an experienced instructor</li> </ul> <p><b>Discussion:</b></p> <ul style="list-style-type: none"> <li>• Questions</li> <li>• Evaluation of the search results</li> <li>• Preparing for the sweep next day</li> </ul>	<p><b>Practical exercise (2):</b></p> <ul style="list-style-type: none"> <li>• Sweep of a bugged conference room by the students (using reduced equipment)</li> <li>• Support by an experienced instructor</li> </ul> <p><b>Discussion:</b></p> <ul style="list-style-type: none"> <li>• Questions</li> <li>• Evaluation of the search results</li> <li>• Preparing for the sweep next day</li> </ul>	<p><b>Practical exercise (3):</b></p> <ul style="list-style-type: none"> <li>• Sweep of a bugged hotel room by the students</li> <li>• Support by an experienced instructor</li> </ul> <p><b>Summary:</b></p> <ul style="list-style-type: none"> <li>• Questions</li> <li>• Evaluation of the search results</li> <li>• Final discussion about the course</li> </ul>

# PBX-ISP Penetration Assessment

# Model 8014

COURSE NO. 8014: PBX-ISP PENETRATION ASSESSMENT (END USER COUNTRY)					
	SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY
<b>Topics</b>	<p><b>Introduction:</b></p> <ul style="list-style-type: none"> <li>• Visiting the customer's facilities</li> <li>• Checking the existing PBX equipment</li> </ul> <p><b>The threat (1):</b></p> <p>ISDN PBXs:</p> <ul style="list-style-type: none"> <li>• Telecommunication and room monitoring by software</li> <li>• Hacking of PBX remote-access-ports</li> <li>• Typical mistakes in configuration</li> <li>• Manipulation of PBX features</li> <li>• Interception of VoIP</li> <li>• WAN-LAN-access</li> <li>• The protection of PBXs</li> </ul>	<p><b>The threat (2):</b></p> <p>Hacking for Administrators:</p> <ul style="list-style-type: none"> <li>• Hacking tools</li> <li>• Virus construction sets and Trojans</li> <li>• Port-scanning</li> <li>• Buffer Overflows</li> <li>• URL attacks</li> <li>• Path climbing</li> <li>• Browser attacks</li> <li>• Demonstrations</li> <li>• Practical exercises by the students</li> </ul>	<p><b>The threat (3):</b></p> <p>Hacking for Administrators:</p> <ul style="list-style-type: none"> <li>• Man-in-the-Middle attacks (encryption)</li> <li>• Firewall Hacking</li> <li>• Scanning tools</li> <li>• Boot attacks</li> <li>• DoS and DDoS</li> <li>• Password-Cracking</li> <li>• Attacks against Web-Applications</li> <li>• Social engineering</li> <li>• Demonstrations</li> <li>• Practical exercises by the students</li> </ul>	<p><b>Practical training (1):</b></p> <p>LAN and Internet-Live-Hacking:</p> <ul style="list-style-type: none"> <li>• LAN-Sniffing</li> <li>• Firewall "Piercing"</li> <li>• DNS Spoofing</li> <li>• DoS attack</li> <li>• Boot attack demo</li> <li>• Penetration testing</li> <li>• Security tools</li> <li>• Demonstrations</li> <li>• Practical exercises by the students</li> </ul>	<p><b>Practical training (2):</b></p> <p>WLAN-Hacking:</p> <ul style="list-style-type: none"> <li>• Basics of WLAN</li> <li>• WLAN Implementing</li> <li>• WLAN Hacking tools</li> <li>• WLAN Sniffing</li> <li>• Penetration testing</li> <li>• DoS against WLAN</li> <li>• WLAN Security</li> <li>• Demonstrations</li> <li>• Practical exercises by the students</li> <li>• Common War Driving (live test)</li> </ul> <p><b>Summary:</b></p> <ul style="list-style-type: none"> <li>• Questions</li> <li>• Final discussion about the course</li> </ul>

# TSCM Sweeping of Cars for Professionals

Model 8016

COURSE NO. 8016: TSCM SWEEPING OF CARS FOR PROFESSIONALS (TSCM LAB EUROPE)					
	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY
TOPICS	<p><b>Introduction:</b></p> <ul style="list-style-type: none"> <li>Greeting</li> <li>Presentation of the company and syllabus</li> </ul> <p><b>Countermeasures:</b></p> <ul style="list-style-type: none"> <li>Basic knowledge of automotive electronics</li> <li>Communication technology in cars</li> <li>Hiding places and hollows in and under cars</li> <li>Considering bullet-proof cars</li> <li>Overview equipment for sweeping of cars</li> <li>Preparing for the car sweep next day</li> </ul>	<p><b>Practical exercise (1):</b></p> <p>Sweep of a bugged luxury car (e.g. Mercedes S-Class, BMW 7-series or AUDI A8) by the students:</p> <ul style="list-style-type: none"> <li>Briefing and technical instructions by an experienced mechanic</li> <li>Disassembling the interior</li> <li>Physical check of interior and cabin</li> <li>Support by an experienced instructor and mechanic</li> </ul> <p><b>Discussion:</b></p> <ul style="list-style-type: none"> <li>Questions</li> <li>Results of the day</li> </ul>	<p><b>Practical exercise (2):</b></p> <p>Sweep of a bugged luxury car by the students (part 2):</p> <ul style="list-style-type: none"> <li>Near field measurement</li> <li>Difference-Spectrum-Analysis</li> <li>X-ray inspection by different systems</li> <li>Disassembling the dashboard</li> <li>Measurement of Electronic Components</li> <li>Support by an experienced instructor and mechanic</li> </ul> <p><b>Discussion:</b></p> <ul style="list-style-type: none"> <li>Questions</li> <li>Results of the day</li> </ul>	<p><b>Practical exercise (3):</b></p> <p>Sweep of a bugged car by the students (part 3):</p> <ul style="list-style-type: none"> <li>Physical search in engine compartment and boot</li> <li>Reassembling of parts</li> <li>Visual inspection of the underside</li> <li>Using mirrors, Endoscopes and Video-Endoscopes</li> <li>Using NLJDs</li> <li>Support by an experienced instructor and mechanic</li> </ul> <p><b>Discussion:</b></p> <ul style="list-style-type: none"> <li>Questions</li> <li>Results of the day</li> </ul>	<p><b>Practical exercise (4):</b></p> <p>Sweep of a bugged car by the students (part 4):</p> <ul style="list-style-type: none"> <li>Final checks and measurements</li> <li>Final reassembling of parts</li> <li>Test run</li> <li>Documentation and Reporting</li> <li>Support by an experienced instructor and mechanic</li> </ul> <p><b>Summary:</b></p> <ul style="list-style-type: none"> <li>Questions</li> <li>Evaluation of the search results</li> <li>Final discussion about the course</li> </ul>

# Computer Forensics

# Model 8017

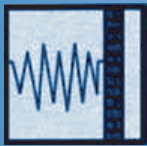
COURSE NO. 8017: COMPUTER FORENSICS					
	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY
<b>Topics</b>	<p><b>Introduction:</b></p> <ul style="list-style-type: none"> <li>Greeting</li> <li>Presentation of the company and syllabus</li> </ul> <p><b>Introduction:</b></p> <ul style="list-style-type: none"> <li>Computer Forensics and Investigations</li> <li>Forensic Office and Laboratory</li> <li>Forensic process</li> <li>Current Computer Forensics Tools</li> </ul>	<p><b>Forensic basics :</b></p> <ul style="list-style-type: none"> <li>Processing Crime and Incident Scenes</li> <li>Digital Evidence Controls</li> <li>Microsoft Windows Systems</li> <li>Unix Systems</li> <li>Boot Processes and File Systems</li> <li>Preparing sterile examination media</li> <li>Data Acquisition</li> <li>Write Blocker</li> </ul> <p><b>Discussion:</b></p> <ul style="list-style-type: none"> <li>Questions</li> <li>Results of the day</li> </ul>	<p><b>Forensic analysis I:</b></p> <ul style="list-style-type: none"> <li>File forensics</li> <li>E-Mail Investigations</li> <li>Investigating data streams</li> <li>File storage dates and times</li> <li>File deletion/recovery</li> <li>Recovering Internet Usage Data</li> <li>Recovering: Swap Files/Temporary Files/Cache Files</li> </ul> <p><b>Discussion:</b></p> <ul style="list-style-type: none"> <li>Questions</li> <li>Results of the day</li> </ul>	<p><b>Forensics Analysis II:</b></p> <ul style="list-style-type: none"> <li>Tool usage</li> <li>Encase Forensic Edition,</li> <li>X-Ways Forensic</li> <li>Forensic Toolkit (FTK),</li> <li>Linux tools</li> <li>Linux forensic suites</li> <li>Sysinternals tools</li> <li>Case Study</li> </ul> <p><b>Discussion:</b></p> <ul style="list-style-type: none"> <li>Questions</li> <li>Results of the day</li> </ul>	<p><b>Mobile Forensics:</b></p> <ul style="list-style-type: none"> <li>Hardware tools</li> <li>Software tools</li> <li>Recovering deleted data from SIM card</li> <li>Recovering deleted data from a cell phone</li> <li>PDA Computer Forensics</li> </ul> <p><b>Summary:</b></p> <ul style="list-style-type: none"> <li>Questions</li> <li>Final discussion about the course</li> </ul>

# TSCM IT Course

# Model 8018

COURSE NO. 8018: TSCM IT COURSE					
	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY
Topics	<p><b>Introduction</b></p> <p><b>FinFisher Attacks</b></p> <ul style="list-style-type: none"> <li>• FinFisher 1</li> <li>• FinFisher 2</li> <li>• FinFisher 3</li> </ul> <p><b>Trojan Horses</b></p> <ul style="list-style-type: none"> <li>• Features</li> <li>• Detection</li> <li>• Prevention</li> </ul>	<p><b>Information Gathering</b></p> <ul style="list-style-type: none"> <li>• Search Engines</li> <li>•</li> <li>• Networks               <ul style="list-style-type: none"> <li>• Mapping</li> <li>• Scanning</li> <li>• Enumeration</li> <li>• Sniffing</li> <li>• Redirection</li> </ul> </li> <li>•</li> <li>• Countermeasure</li> <li>• Model 7543               <ul style="list-style-type: none"> <li>• LAN/WLAN Analyzer</li> </ul> </li> </ul>	<p><b>Attacking</b></p> <ul style="list-style-type: none"> <li>• Passwords</li> <li>• Bypass</li> <li>• Default</li> <li>• Brute force</li> <li>• Cracking</li> <li>• Software Security               <ul style="list-style-type: none"> <li>• Attacks</li> <li>• Verification</li> <li>• Prevention</li> </ul> </li> </ul>	<p><b>Attacking</b></p> <ul style="list-style-type: none"> <li>• Wireless               <ul style="list-style-type: none"> <li>• WLAN</li> <li>• Bluetooth</li> <li>• Keyboards</li> </ul> </li> <li>• Voice-over-IP</li> <li>• Audio Sniffing</li> <li>• Protocol Attacks</li> <li>• Countermeasure</li> <li>• Model 7540               <ul style="list-style-type: none"> <li>• WiFi Detector</li> </ul> </li> </ul>	<p><b>Cryptography</b></p> <ul style="list-style-type: none"> <li>• File Systems</li> <li>• Communication</li> <li>• SSL</li> <li>• Policies               <ul style="list-style-type: none"> <li>• Notebooks</li> <li>• External Networks</li> <li>• Internal Networks</li> <li>• Hardware</li> </ul> </li> </ul>

# TSCM INDEX



1 - Introduction

2 - The Threat

3 - Recommendations

4 - Training Course Overview

5 - Training Course Syllabuses

6 - Recommended Products

7 - Technical Data Sheets

8 - IP/PABX Manipulation

9 - Commercial Quotations

10 - Terms & Conditions

11 - Contact Details

12 - Elaman Catalogs Overview



## Typical Technical Sweep Operation

## Sweep Pics



Telephone Junction Box



Turnkey TSCM System



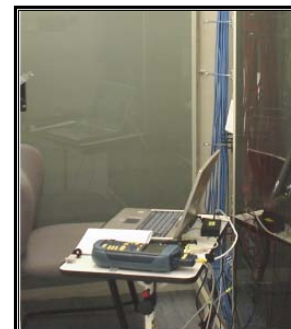
Analyzing Antennas



Visually Checking Underfloor Ducts



Passive Wall Sweep



LAN Tester



X-Raying Wall Ceiling Cables



Cable Measurement

## Product Description

## Products

<b>Ref.</b>	<b>Qty</b>	<b>Model</b>	<b>Description</b>
1	1	7501	NLJD Non Linear Junction Detector
1b		7501-2	Advanced Non Linear Junction Detector
2	1	7502-1	TSCM Search Tool Kit
3	1	7502-2	Advanced /Telecomms Search Tool Kit
4	1	7504	Portable X-Ray System
4b	1	7504 option	Advanced Flat Screen X-Ray Imager
5	1	7505	Thermal - Wall Scanner
5b	1	7505-2	Thermal Imaging for Surveillance Applications
6	1	7506	Locator
7	1	7507-01	Optical System to Detect Cameras, Lens (Room Version)
8	1	7508	Advanced Scan Detector System
9	1	7509	TDR Multi Channel Cable Detector
10	1	7510	Digital Advanced Hand Held Oscilloscope
11	1	7511	Detection Receiver
12	1	7513	Wall Depth Measurement System
13	1	7514-2	video remote probe inspection
14	1	7515	Marking Kit-Covert Stickers Illuminator
15	1	7516	Optical Search Toolkit
16	1	7517-01	Video and Audio RF Detection System
17	1	7517-02	Advanced Video & Audio RF Detection System
18	1	7518 oscor	OMNI SPECTRAL CORRELATOR
19	1	7518 option	Omni Spectral Correlator
20	1	3521	High Power GSM Jamming System
21	1	3522	Room Jammer
22	1	3525	Computer Screening Jammer
23	1	3526	Anti-Laser-Microphone Noise Jammer
24	1	3527	Advanced Counter Surveillance Jammer
25	1	7519	FSH Portable Spectrum Analyzer
26	1	7520	Bug Detector
27	1	7521	EB200-High Speed Frequency Scanner 3 GHz with DF

## Product Description

## Products

28	1	7522	Digital Scout Frequency Detector
29	1	7523	Advanced Cable Tracing System
30	1	7525	X-ray for Screening VIP Presents
31	1	7527	Encryption Product - GSM Encryption Phones
32	1	7530	Ultra Scan50b
33	1	7539	3D image enhancer
34	1	7540	Wireless Network detector
35	1	7541	Telephone Line analyzer Detector
36	1	7542	Secure document scanner
37	1	7543	LAN/WLAN Checking System
38	1	7544	TSCM Search Video Pole Camera
39	1	7545	Video Wireless Detection
40	1	7546	Cable Amplifier System
41	1	7547	Flat Panel X-ray system
42	1	4014	GSM Detection System
43	1	1013	Night Vision kit
44	1	2001	Door Opening kit

## Recommended Product Description

## Sweep List

### Special Sweep List Government Approved

#### For in-country sweep teams, including portable cases and vehicles

This equipment is installed in portable casing, which can easily be moved from place to place

#### 1.1. Model 7501 - 4th Generation NLJD Electronic Circuitry Detector (PASSIVE)

The Non Linear Junction Detector (NLJD) is used in the initial physical search phase of a sweep. Its unique use allows an operative to quickly and effectively scan a location for concealed electronic components. The Model 7501 is a versatile third harmonic NLJD which detects, analyzes and pin-points the location of suspect electronic devices, whether they are switched on or off.



#### 1.1.2 Model 7501-2 - Advanced NLJD (PASSIVE)

The unit provides the capability to detect hidden electronic devices, regardless of whether the device is radiating, hard wired, or even turned on at all! Its unique design means that it is lightweight, completely portable and folds away into a small case.



#### 1.2. Model 7502-1 - Search Tools and Test Equipment (SEARCH)

This tool kit is usually used with a Non-linear Junction Detector (NLJD) and provides tools that are uniquely suited for use with an NLJD. The tool kit comes in a leather tool bag.



#### Model 7502-2 - Advanced/Telecoms Search Tool kit (SEARCH)

Designed as a TSCM team toolkit that includes all the necessary tools needed to carry out a thorough physical and cable search. Containing the basic toolset required for telephone sweeps, such as a digital multimeter, butt set and structured cabling tools; it compliments more advanced cable tools such as the Line Amplifier or CPM700. All the electro mechanical tools in this set have been put together to provide a wide range of aids for completing a full physical search, such as work lights, mirrors, opening tools and even a drill to allow use of borescopes or videoscopes.







#### 1.3. Model 7504 - Portable X-Ray System Software Viewing System (OPTICAL SEARCH)

This unit can see through objects to check on electronic circuitry/tape recorders/transmitters and microphones/cameras, hidden in secret areas. It is also used to compare electrical devices for any changes on PCB boards. This mobile x-ray generator comes with a PC and a camera to detect any bugs hidden in gifts presented to VIPs.



## Recommended Product Description




## Sweep List

<p><b>Model 7504 Option - Advanced Flat Screen X-Ray Imager</b></p> <p>A flat panel x-ray imager offering high resolution images in the most confined spaces from different orientations and with even greater coverage (25 x 33 cm). Specifically designed for security and law enforcement professionals it is flatter, safer, stronger and less expensive than many other fragile flat panel units. It is available as a complete x-ray system or a single flat panel upgrade.</p>	
<p><b>1.4. Model 7505 - Optical Wall Scanning System, NATO Approved</b> <b>(SEARCH)</b></p> <p>The physical inspection of a target location is the most time consuming part of a sweep. All surfaces and objects must be inspected. The Model 7505 was developed to perform a quick and thorough search to locate concealed eavesdropping devices. A concealed device will emit a heat signature easily spotted by a thermal inspection system.</p>	
<p><b>1.4.2 Model 7505-2 – Thermal Imaging for Surveillance Applications</b> <b>(SEARCH)</b></p> <p>The Unit is a flexible, easy to use, handheld thermal imager, which is suitable for all law enforcement operations, including surveillance, TSCM, police, firearms teams and others. It has a large clear display, a 150+ m image range, image storage to SD card, and temperature measurement that is ideal for hydroponics. It can detect people in total darkness and allows covert distance surveillance offering high resolution images of 160x120 pixels and an auto hotspot tracker that is useful for highlighting people.</p>	
<p><b>1.5. Model 7506 - Locator – Locates &amp; Detects Transmitters</b> <b>(RF LOCATION)</b></p> <p>This portable hand-held unit is used to pinpoint the exact location of a detected transmitter and can locate both analog and digital transmitters.</p>	
<p><b>1.6. Model 7507-01 - Video Camera and Lens Detector</b> <b>(OPTICAL SEARCH)</b></p> <p>This hand-held system will detect cameras/lenses covertly installed in rooms and conference places. (Room version)</p>	
<p><b>1.7. Model 7508 - Building Sweep System with Dual Antenna/Software</b> <b>(ACTIVE RF)</b></p> <p>The Advanced Scan Detector System, Model 7508, is uniquely different from all other RF Detection Systems. It is an advanced system which uses spectrum analyzer with the latest software technologies to provide accurate results. It uses a twin antenna system, placing one antenna outside of the target location and one inside. Using the software it is able to show all suspicious transmissions which are stronger in the target location than outside. This is a strong indicator of a transmitting eavesdropping device.</p>	




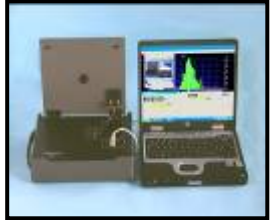




## Recommended Product Description

## Sweep List

<p><b>1.8. Model 7509 - Multi-Channel Wired Analyzer (CABLES)</b></p> <p>The unit is one of the most valuable TSCM test instruments available. This equipment is capable of detecting many wiretap methods that are undetectable by conventional telephone analyzers, meters or other instrumentation. The unit is designed to reveal all wire irregularities by displaying the characteristic signatures and distances to each wire irregularity. Without a TDR, the presence and location of all wire irregularities cannot be pinpointed, and therefore will not be physically inspected.</p>	
<p><b>1.9. Model 7510 Digital Advanced Handheld Oscilloscope (CABLES)</b></p> <p>The digital oscilloscope is useful for measuring all the basic measurements in electronic equipment and for establishing modifications that could have been caused by manipulation or integration of surveillance equipment.</p>	
<p><b>1.10. Model 7511 - Detection Receiver (RF ACTIVE/IR)</b></p> <p>One of the first tools to be used during a physical search should be the Broadband RF Detector. This versatile unit can indicate the location of a transmission source, whether hidden in phone, room or body transmitters, remote control signals, computer bugs, fax or telex transmitters, video transmitters, pulsed tracking transmitters, spread spectrum, and even wide band frequency hopping or 'burst' transmitters. This is a multi use tool which covers a wide range of tasks from basic physical searches to cable verification.</p>	
<p><b>1.11. Model 7513 - Through-The-Wall Display System (SEARCH)</b></p> <p>This unit measures the depth of a wall and shows objects, such as microphone cables, transmitters or cameras on a in-built display. This can be used in conjunction with a Non Linear Junction Detector.</p>	
<p><b>1.12. Model 7514□2 - Video Probe Remote Visual Inspection (SEARCH)</b></p> <p>A remote visual video boreoscope power tool for improving inspection productivity. The base is a portable workstation for inspection data management, plus a light source and storage reel for the probe. It has a high resolution LCD screen and powerful computing platform for data management and worldwide connectivity. Probes come in size from 3.2 mm up to 8.4 mm in diameter.</p>	
<p><b>1.13. Model 7515 - Secret Marking Kit Seals and Light Source (SEARCH)</b></p> <p>After carrying out a room search special equipment is used to mark the searched area. A check of the room can be made later to see if anything has been tampered with, for example, after a sweep all electrical sockets are secretly marked so if an intruder tries to connect a bug it can be detected.</p>	

## Recommended Product Description

## Sweep List

<p><b>1.14. Model 7516 - Optical Search System Set (SEARCH)</b></p> <p>The Optical Search Toolkit is the budget alternative accessory kit to enable a thorough and effective physical search. For use in validating information provided with other equipment, such as the NLJD, the Optical Search Toolkit is ideal for searching hard to reach and inaccessible areas.</p>	
<p><b>1.15. Model 7517-01 - Audio-Video Transmission Decoder Detector Analyzer (ACTIVE RF)</b></p> <p>The unit analyzes, detects and decodes audio/video RF transmission and displays its results on an in-built monitor. It also scans telephone and mains cables. This unit can detect infrared. The frequency coverage is up to 3000 MHz. A NATO-approved antenna system enables covert scanning to take place.</p>	
<p><b>1.16. Model 7517-02 - Advance A/V Transmission Decoder Detector Analyzer (ACTIVE RF)</b></p> <p>This unit can sweep an entire building from one location. This model is the next-level model 7517-01 with a frequency range of 10 KHz-6 GHz.</p>	
<p><b>1.17. Model 7518 Oscan - Omni Spectral Correlator</b></p> <p>A phased locked super heterodyne spectrum analyzer, designed specifically for counter surveillance that automatically selects antenna inputs. Frequency spans can be programmed with single button control for rapid recall and automatic searching. Patented fold-out antenna panel automatically selects the proper antenna. Enhanced trace analysis provides ability to compare target sweep area traces to friendly traces, to quickly identify evidence of transmitters in target sweep area.</p> <p><b>Model 7518 option - Microwave Downconverter</b></p> <p>The OSCOR Microwave Downconverter option (MDC-2100) features an array of high gain directional antennas. It can function in sweep, analyze and correlation modes and includes a tripod. The MDC-2100 can be used in a stationary position sitting on the provided tripod or it can be moved around to provide a thorough sweep of the area. For proper operation, the MDC-2100 should be located at least three feet away from the OSCOR.</p>	 
<p><b>1.18. Model 3521 - GSM Hi-Power Jamming System (JAMMING)</b></p> <p>This portable GSM jamming system can jam and protect meetings and conferences with its 25-watt output. The system is also available in CDMA frequencies upon request. Other optional extras include output power up to 120-watt to protect complete areas.</p>	

## Recommended Product Description


## Sweep List

<p><b>1.19. Model 3525 - Computer Screening Jammer - Defender (JAMMING)</b></p> <p>The Defender will jam the frequencies emitted from a monitor/computer/keyboard that can be monitored by hi-tech interception equipment, without interfering with the operation of your computer.</p>	
<p><b>1.20. Model 3526 - Laser Jamming System (JAMMING)</b></p> <p>This unit jams laser and audio signals in a room. Sensors are attached to windows and can stop any laser system from working.</p>	
<p><b>1.21. Model 3527 - Jamming System 20-2400 MHz (JAMMING)</b></p> <p>This Jammer will protect against wireless RF video and audio bugs. It is portable and easy to use and covers a wide band. It has a white noise tone generator adding extra security.</p>	
<p><b>1.22. Model 7519 - FSH Spectrum Analyzer (RF ACTIVE)</b></p> <p>This Hand-held Spectrum Analyzer enables quick and effective RF measurement of rooms and signal analysis. It displays all analog and digital signals. The FSH is available in 2 models: 100 - 3 GHz or 100 - 6 GHz. The 6 GHz is particularly interesting for detecting 5.8 GHz video signals.</p>	
<p><b>1.23. Model 7520 - Covert Bug Detector (Detection)</b></p> <p>Powerful, sensitive and adjustable cigarette box size bug detector, which detects active transmitters and bugging devices close by. Its discrete vibrating alarm allows it to be body-worn. Powerful rechargeable batteries guarantee long operating time.</p>	
<p><b>1.24. EB200 - High Speed Frequency Scanner with DF (RF ACTIVE)</b></p> <p>The EB200 with its digital scan mode enables band frequencies of up to 3 GHz to be scanned in milliseconds enabling short burst transmitters, remote control transmissions, etc. to be immediately detected and located.</p>	
<p><b>1.25. Model 7522 - Digital Scout Frequency Detector (RF ACTIVE)</b></p> <p>This hand-held unit provides an immediate frequency fix of possible transmissions in a closed area. With an add-on receiver the audio of the captured signal can be heard.</p>	
<p><b>1.26. Model 7523 - Cable Tracking System (CABLES)</b></p> <p>With cable measurement taking up to 30 percent of a sweep effort, tools that provide important information effectively and quickly are needed. The Advanced Cable Tracing System is designed to aid in locating all cables coming from the target location. Capable of tracing cables buried as deep as 2 meters, this system excels in ensuring all potentially dangerous cables are found.</p>	



## Recommended Product Description

## Sweep List

<p><b>1.27. Model 7525 - X-ray System for VIP Gifts, Presents, etc (SEARCH)</b>          As a security precaution all received gifts should be x-rayed for any possible surveillance equipment – remember the gift the Russians gave to the Americans?</p>	
<p><b>1.28. ROHDE &amp; SCHWARZ GSM Encryption (VOICE PROTECTION)</b>          GSM Encryption is used to secure the communication of the VIP/sweep team members. The system is compatible with desktop telephones and secures what is sent over the network. This is also available for e-mail security.</p>	
<p><b>1.29. Model 7530 - X-ray Unit (SEARCH)</b>          As a security precaution this product would be used for checking VIP gifts and objects such as bags, telephone phones, etc. to locate any bugging equipment.</p>	
<p><b>1.30. Model 7539 - 3D Image Enhancer (SEARCH)</b>          The 3D Image Enhancer is a mobile system that converts 2d x-ray images into 3d images. It can be quickly and easily set up and its user friendly interface means no extra training is required. It can convert conventional films and storage foils.</p>	
<p><b>1.31. Model 7540 - Wireless Network Detector (Detection)</b>          A professional Wireless Network Detection and Visualization tool that detects and stores all the important information about your wireless network environment automatically to an SQL Database, and visualizes your WLAN infrastructure on your own imported maps.</p>	
<p><b>1.32. Model 7541 - Telephone Line Analyzer (Detection)</b>          Second to the physical search, cable and wiring checks are the most time consuming and technical. To ensure an effective and thorough cable check, there are over 10 checks for each cable, requiring a skilled operative and careful documentation. The Telephone Line Analyzer provides a complete integrated suite of tools to analyze, inspect, and test digital telephone lines (and other wiring) for taps and other eavesdropping devices.</p>	
<p><b>1.33. Model 7542 - Secure Document Scanner (Detection)</b>          An innovative overall concept for handling important and confidential documents that uses a newly developed security-paper, which acts as a magnetic storage medium. It uses a special read-write device that connects to a PC or laptop. The digital document-certificates are administered through a Trust Center. This scanner offers state-of-the-art technical solutions for document protection that are beyond comparison, especially developed for high security demands.</p>	



## Recommended Product Description

## Sweep List

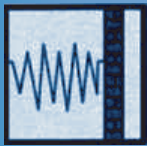
<p><b>1.34. Model 7543 - LAN/WLAN Checking System (Detection)</b></p> <p>The LAN checking system has come a long way since just checking structured cabling. The threat of an IT related attack has heightened bringing with it the need to check IT systems. The LAN/WLAN Checking System is capable of performing checks on structured cabling and any data present on the line. Its semi automated checks provide clear information presented in a printable report.</p>	
<p><b>1.35. Model 7544 - Video Pole Camera (SEARCH)</b></p> <p>Sometime during a physical inspection it is not be possible to have the means or time to inspect all hard to reach areas. The Video Pole Camera was developed with the aim of providing an accurate search of the target location. With its hi-resolution camera and screen and 6-foot reach it is possible to get into areas a search mirror kit cannot. Inspect drop ceilings, behind immovable objects, around corners, or other difficult to reach areas, even in dark situations with the Video Pole Camera.</p>	
<p><b>1.36. Model 7545 - Video Wireless Detection (Detection)</b></p> <p>A fast scanning receiver that detects wireless video cameras. A 2.5" TFT color LCD displays what the hidden camera is looking at. A smaller LCM displays the frequency and signal it is locked on to. It can scan all available video frequencies in 15 seconds and detect signals as far away as 500 feet.</p>	
<p><b>1.37. Model 7546 - Cable Amplifier System (Detection)</b></p> <p>The Cable Amplifier System is a high gain audio amplifier used to detect and identify certain types of surveillance devices attached to building wiring, such as telephone wiring, LAN and server systems, AC power, alarm wires, etc. It provides flexible features and has proven to be very useful in many situations. This amplifier is quite useful for checking telephone lines and other wiring for hostile microphones, testing for hook switch audio leakage, and detection of eavesdropping devices that are sensitive to bias voltages or currents.</p>	
<p><b>1.38. Model 7547 - Flat Panel X-ray System</b></p> <p>The unit is a state-of-the art digital mobile flat panel X-ray system manufactured in Western Europe. The flat image converter enables many different applications in the fields of security and non-destructive-testing. For EOD use the Notebook provides a save operation by 100 m cable or remote control. The high resolution of 127 <math>\mu</math>m allows the identification of even the smallest details on X-ray images with more than 16,000 grey levels.</p>	
<p><b>1.39. Model 4014 - GSM Detection System (Detection)</b></p> <p>This system was developed as a counter-measure to detect active GSM monitoring systems that create bogus sites. It is a GSM receiver, which constantly scans the GSM control channels of all networks (dual band) looking for changes in the overhead parameters transmitted by the genuine network. The GSM Detection System is able to recognize bogus cell sites that are attempting to mimic a legitimate site for its own purposes. Used for protection in embassies or high level meetings.</p>	

## Recommended Product Description

## Sweep List

<p><b>1.40. Model 1013 - Night Vision Viewer (IR &amp; FIBER OPTIC SEARCH)</b></p> <p>Usually used in surveillance operations. Night Vision Viewer has a dual role in a TSCM team in the search for fiber optic microphones, laser and IR rays that are almost impossible to detect with standard sweep equipment.</p>	
<p><b>1.41. Model 2001 - Lock-Picking for Entry into Closed Areas (SEARCH)</b></p> <p>When carrying out a sweep there may be occasions when it is impossible to gain access because the door is locked or the telephone is enclosed in a box. Therefore, every sweep kit should include a lock-picking set.</p>	

# TSCM INDEX



1 - Introduction

2 - The Threat

3 - Recommendations

4 - Training Course Overview

5 - Training Course Syllabuses

6 - Recommended Products

7 - Technical Data Sheets

8 - IP/PABX Manipulation

9 - Commercial Quotations

10 - Terms & Conditions

11 - Contact Details

12 - Elaman Catalogs Overview

## Product Description

## Products

<b>Ref.</b>	<b>Qty</b>	<b>Model</b>	<b>Description</b>
1	1	7501	NLJD Non Linear Junction Detector
1b		7501-2	Advanced Non Linear Junction Detector
2	1	7502-1	TSCM Search Tool Kit
3	1	7502-2	Advanced /Telecomms Search Tool Kit
4	1	7504	Portable X-Ray System
4b	1	7504 option	Advanced Flat Screen X-Ray Imager
5	1	7505	Thermal - Wall Scanner
5b	1	7505-2	Thermal Imaging for Surveillance Applications
6	1	7506	Locator
7	1	7507-01	Optical System to Detect Cameras, Lens (Room Version)
8	1	7508	Advanced Scan Detector System
9	1	7509	TDR Multi Channel Cable Detector
10	1	7510	Digital Advanced Hand Held Oscilloscope
11	1	7511	Detection Receiver
12	1	7513	Wall Depth Measurement System
13	1	7514-2	video remote probe inspection
14	1	7515	Marking Kit-Covert Stickers Illuminator
15	1	7516	Optical Search Toolkit
16	1	7517-01	Video and Audio RF Detection System
17	1	7517-02	Advanced Video & Audio RF Detection System
18	1	7518 oscore	OMNI SPECTRAL CORRELATOR
19	1	7518 option	Omni Spectral Correlator
20	1	3521	High Power GSM Jamming System
21	1	3522	Room Jammer
22	1	3525	Computer Screening Jammer
23	1	3526	Anti-Laser-Microphone Noise Jammer
24	1	3527	Advanced Counter Surveillance Jammer
25	1	7519	FSH Portable Spectrum Analyzer
26	1	7520	Bug Detector
27	1	7521	EB200-High Speed Frequency Scanner 3 GHz with DF

## Product Description

## Products

28	1	7522	Digital Scout Frequency Detector
29	1	7523	Advanced Cable Tracing System
30	1	7525	X-ray for Screening VIP Presents
31	1	7527	Encryption Product - GSM Encryption Phones
32	1	7530	Ultra Scan50b
33	1	7539	3D image enhancer
34	1	7540	Wireless Network detector
35	1	7541	Telephone Line analyzer Detector
36	1	7542	Secure document scanner
37	1	7543	LAN/WLAN Checking System
38	1	7544	TSCM Search Video Pole Camera
39	1	7545	Video Wireless Detection
40	1	7546	Cable Amplifier System
41	1	7547	Flat Panel X-ray system
42	1	4014	GSM Detection System
43	1	1013	Night Vision kit
44	1	2001	Door Opening kit

# NLJD Non-Linear Junction Detector

# Model 7501

**Non Linear Junction Detectors (NLJD) are used in the initial physical search phase of a sweep. Its unique use allows an operative to quickly and effectively scan a location for concealed electronic components.**

The Model 7501 is a versatile third harmonic non-linear junction detector which detects, analyzes and pin-points the location of suspect electronic devices, whether they are switched on or off.



## TECHNICAL FEATURES

- Channel selectable; four operating frequencies to ensure potential interfering signals are avoided, (FCC 915MHz, EU 869MHz and classic 888MHz; Available in one unit for universal operation). The four spot frequencies are customer selectable
- High Power Transmission to rapidly search a large area with greater penetration; adjustable power control 2mW to 1Watt (2Watt optional)
- Constant power transmission, as opposed to pulsed operation. (Continuous transmission reduces risk of missing a threat from inadvertent rapid movement of antenna head)
- Unique 4-way thumb control conveniently placed on display screen for most commonly used functions
- Ergonomic sweep head with increased sensitivity reduces search time, 6dBi gain
- Circularly polarized antenna improves reliability, and reduces risk of missing a threat due to incorrect antenna polarization
- Quick fit removable smart battery housed inside control module; provides over 2-hrs operation.
- Minimum set-up time; extension Lengths 52-208 cm.
- Robust, lightweight aluminum, fiberglass and carbon design; operational weight only 2kg; in transit case 5.6kg.





## NLJD Non-Linear Junction Detector

Model 7501

### THE MODEL 7501 MAY BE USED TO IDENTIFY:

- Active or Live Bugs
- Inactive Bugs
- Turned On Bugs
- Turned Off Bugs
- Burned Out Bugs
- Dead Bugs
- Covert or Concealed Video Cameras
- Microwave Transmitters
- Remote Control or Remote Powered Bugs
- Resonant Cavity Devices
- Concealed Cellular, PCs, and GSM Telephones
- Electronic Timers for Hidden Bombs
- Wireless Microphones
- Hidden Tape Recorders (even broken ones)
- Covert Eavesdropping Devices



### EQUIPMENT CONTENTS:

- Control Module
- Display Module
- Antenna Head
- Battery Charger
- 2 Re-chargeable NiMH Batteries
- Earphones
- 36 cm Extension Tube
- Transit Case

### TECHNICAL DATA:

TRANSMITTER	
Frequency range	Four spot frequencies in the range of 869-916 MHz. (dependent on country of use)
Power output	Adjustable 2mW to 1W ERP (2 W optional)
Filtering	10 section filter



## NLJD Non-Linear Junction Detector

## Model 7501

Output connector	50 ohm double screened co-ax socket
<b>RECEIVER (RX1)</b>	
Frequency range	1738 - 1832 MHz (transmitter selection controls receiver frequencies)
Sensitivity	Detection at -130 dBm.
Filtering	6 section filter
Input connector	50 ohm double screened co-ax socket
<b>RECEIVER (RX2)</b>	
Frequency range	2607-2748 MHz (transmitter selection controls receiver frequencies)
Sensitivity	Detection at -130 dBm.
Filtering	6 section filter
Input connector	50 ohm double screened co-ax socket
<b>DISPLAYS</b>	
	Target response/comparison Transmitter output power Battery level, mode selection (RX1 and RX2) Frequency selection, signal strength (R1 and R2)
<b>CONTROLS</b>	
	4 way thumb control selects range and receiver selection Volume up and down, frequency select and ON/OFF
<b>ANTENNA</b>	
Frequency coverage	860-920 MHz, 1720-1840 MHz and 2580-2760 MHz.
Gain	6 dbi.
Polarization	RHC Right hand circular
<b>CHARGER</b>	
Input voltage	100-240 VAC.
Charging current	1200mA/auto trickle charge
Charge time	Up to 1.5 hours
Type	Microprocessor controlled, short circuit and timer
<b>BATTERY</b>	
Type	Nickel metal hydride - smart battery
Voltage	10.8V DC/1700 mAh.
Test	Built in battery level indicator
Run time	2 hours - normal operation

## Advanced Non-Linear Junction Detector

## Model 7501-2

Non Linear Junction Detectors are used in the initial physical search phase of a sweep. Its unique use allows an operative to quickly and effectively scan a location for concealed electronic components.

The Model 7501-2 provides the means to detect hidden electronic devices, regardless of whether the device is radiating, hard wired, or even turned on at all! Its unique design means that it is lightweight and completely portable as it folds away into its small case.



### TECHNICAL FEATURES

- Minimum set-up time, no cables or bulky transceiver units to carry
- Lightweight, balanced ergonomic design for ease of use
- High transmit power for rapidly searching a large area
- Circularly polarized antenna reduces search time and improves reliability
- Dual harmonic with discrimination algorithms minimizes false alarms
- Standard type camcorder battery with long use time and quick charge function
- Wireless headphones and graphic display for simultaneous audio & visual information
- 2nd and 3rd harmonic operation includes advanced algorithms for minimizing false alarms as well as listening capability for each harmonic
- Dynamic power control for locating threats; automatic or manual control (10 mwatt to 1 watt)
- Synthesized transceiver provides frequency stability and agility to automatically search for clean operating frequencies (frequency range 902-928 MHz for US models and 850 MHz to 1,000 MHz for export models)
- Circular, polarized antenna removes risk of missing a threat due to incorrect antenna polarization



## Advanced Non-Linear Junction Detector

Model 7501-2

### THE ORION MAY BE USED TO IDENTIFY:

- Active or Live Bugs
- Inactive Bugs
- Turned On Bugs
- Turned Off Bugs
- Burned Out Bugs
- Dead Bugs
- Covert or Concealed Video Cameras
- Microwave Transmitters
- Remote Control or Remote Powered Bugs
- Resonant Cavity Devices
- Concealed Cellular, PCs, and GSM Telephones
- Electronic Timers for Hidden Bombs
- Wireless Microphones
- Hidden Tape Recorders (even broken ones)
- Covert Eavesdropping Devices



### TECHNICAL DATA

#### TRANSMITTER

Frequency Bands: 880 - 1005 MHz using 200 kHz steps. USA versions: 902.2 - 927.8 MHz. Foreign models are adjustable between 880 and 1005 MHz. The unit is actually usable down to 850 MHz, but there is 1-2 dB of loss in receiver sensitivity due to filter roll-off of the second harmonic.

Peak Power: 1.4 Watts (effective radiated power including antenna gain and all system losses).

Power Control: 30 dB range in 2 dB steps; Pulsed to limit average output power to FCC max.

#### RECEIVER

Frequency Bands: Second (1700-2010 MHz) or third (2550-3015 MHz) harmonic of transmit fundamental frequency.

Sensitivity: -130 dBm for both Harmonics.

Gain Control: The gain of the unit is enhanced using software integration. Various modes of operation have different integration algorithms for maximum performance. The gain is controlled by setting the level of integration using the SET key.

Receiver IF BW: 3 kHz

**Unit Operational Weight:** 3.4 lbs (1.54 kg)

**Antenna Polarization:** Circular for both transmit and receive functions.

## Advanced Non-Linear Junction Detector

## Model 7501-2

### INFRARED HEADPHONES

- Headphones can be plugged directly into main unit or plugged into the Infrared Receiver
- Plugging headphones into the main Unit turns off the IR transmit function on the main unit
- Plugging headphones into the IR Audio Receiver automatically turns on the IR Audio Receiver
- Volume control is adjusted via the main Unit

### BATTERY SPECIFICATIONS

- Externally rechargeable standard type battery
- 7.2 VDC camcorder style NiCad
- Run time 1 hour on full charge when operating at full power. Normal usage should result in run time hours

### BATTERY CHARGER

- Dual battery charger with automatic operation
- Charging time is approximately 45 minutes to 1 hour depending on battery vendor
- Sequentially charges both batteries

### LED INDICATORS:

- Flashing LED - charge pending (applies to the situation when two batteries are simultaneously placed in the charger)
- Bright LED - fast charging
- Dark LED - No battery or charge complete

### OPTIONAL

Model 7501-3 – High power non-linear junction detector

## TSCM Search Tool Kits

## 7502 series

### MODEL 7502-1: SEARCH TOOL KIT

Once the NLJD has located a potential threat there are ways to verify the status of the potential threat. All tools required to aid in the classification of the potential threat are included within the NLJD toolkit.

The TSCM Search Toolkit contains selected tools for verifying the existence of threatening electronic surveillance devices. This toolkit, which comes in leather tool bag, is uniquely suited for use with a Non-Linear Junction Detector.

### EQUIPMENT CONTENTS

- Borescope with built-in light and right-angled viewer for inspecting inside walls, furniture, etc...
- Wire tracing system to trace miscellaneous cables
- Fluke multi-meter for testing miscellaneous cables and electronic devices
- Combination stud finder and metal detector for non-destructive evaluation
- Hammer to evaluate the stability of a junction under physical vibration
- Ultraviolet light and marking pen
- Multi-purpose geared screwdriver. Provides screwdriver function as well as small drill for use with borescope
- Miscellaneous tools: pliers, wire cutters, leatherman (multi-purpose tool), inspection mirrors, measuring tape, flashlight, drill bits for walls, etc



## TSCM Search Tool Kits

## 7502 series

### MODEL 7502-2: ADVANCED/TELECOMS SEARCH TOOL KIT

Designed as a TSCM team toolkit, this model has all the necessary tools needed to carry out a thorough physical and cable search. Containing the basic toolset required for telephone sweeps, such as a Digital Multimeter, Butt Set and structured cabling tools, it compliments more advanced cable tools, such as the Line Amplifier or CPM700. All the electro mechanical tools in this set have been put together to provide a wide range of aids for completing a full physical search, such as work lights, mirrors, opening tools and even a drill to allow use of borescopes or videoscopes.

The Advanced Search Toolkit includes the recommended TS30™ DataSafe® Lineman's Test Set, Fluke 177 backlit true-rms DMM with extended capacitance range and DeWalt DW980k-2 Heavy-Duty Cordless 3/8" Drill/Driver Kit with extended run-time batteries. The versatile kit is designed for contractors who demand the highest quality and most complete tool assortment. Use the Advanced Search Toolkit to service and install voice and data circuits, phone switches, datacom networks, computers, telephone packets and virtually anything integrating voice and data. Wrap and unwrap wire terminals, trace and troubleshoot wires, punch 110 and 66 blocks plus pull wires through conduit.

The name-brand tool selection includes Cementex 1000-V screwdriver and channel lock pliers, Klein cushion-grip screwdrivers and nut-drivers, a Fluke voltage detector, fluorescent work light with extension cord, leather gloves, stapler and staples for RG-59 and RG-6 coax, plus more.

Our robust black polyethylene case features reinforced construction, extra-large corners, steel spring-loaded handles and quarter-turn latches. This is the only hard case kit with a built-in DMM pouch. The 35.6-pound SPC21-96 is 17.75" x 14.5" x 9" (inside dimensions). Empty 082X471 case also may be ordered separately.





## Portable X-ray System

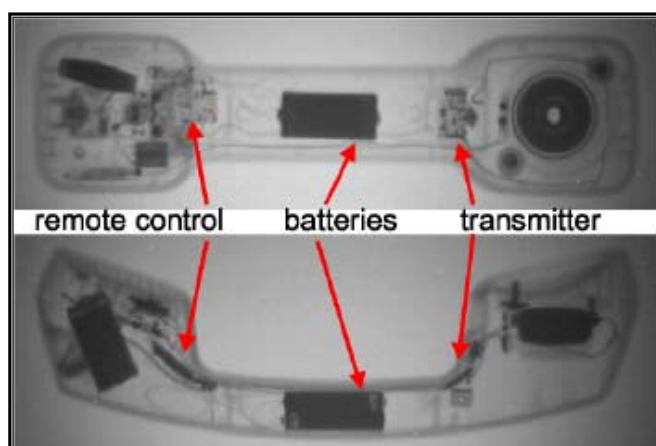
## Model 7504

One of the biggest threats in TSCM is the miniaturization of technology allowing very small eavesdropping devices to be well concealed. It is imperative all items which cannot be cleared safe with the naked-eye be passed through the Portable X-Ray System.

The digital X-ray system allows an operative so see inside any item allowing a non destructive detailed physical inspection.

The digital X-ray system is easily set up and deployed in minutes by one person and can be configured to suit different environments.

It comes with a choice of x-ray sources, adjustable exposure settings, different size ICUs and has both wireless and ROV capabilities.



### FEATURES

- search and examine suspicious objects on the spot
- portable, easy to set up and use in 2 minutes
- image analysis includes zoom, reverse black and white, pseudo-color, pseudo 3D and measure, show gradients, rotation, distance, contrast enhancement and more
- image print and email
- archive in excess of 32,000 images on PC or CD
- annotation tools
- full database management tools

### X-RAY STANDARD CONFIGURATION:

- Lightweight X-Ray Generator
- Laptop PC
- Image Capture Unit (ICU)
- Transportation Case
- 50 Meter Cable Drum and Optional Wireless Control
- Spare Generator Battery
- Battery Charger
- Instruction Manual



## Portable X-ray System

Model 7504

### MODEL 7504 IMAGE CAPTURE UNIT (ICU)

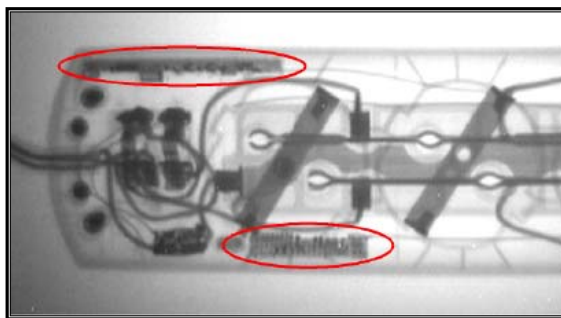


Standard Image Area	8 X 10" (20.32 X 25.40 cm) Optional: 10 x 13" custom sizes available
Camera Type	High Performance CCD
Horizontal Resolution	625 TV lines
Video Signal/Noise	Better than 40 dB

### X-RAY GENERATOR



Option 2	XR200: 2 kg with battery 150kV maximum energy
	Penetration: 15 mm steel
	5.5 kg with battery



X-ray view of a remote control plug transmitter



Keyboard connector with concealed logger



X-ray view of calculator and pen with inbuilt transmitter



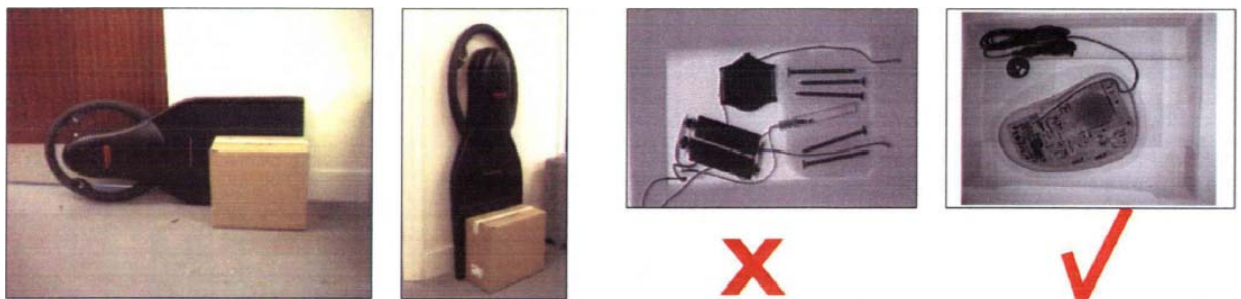
## Advanced Flat Screen X-ray Imager

## 7504 option

The Model 7504 option – more coverage, more rugged and more reliable than the rest!

Model 7504 option is an innovative flat panel x-ray imager from us. The unique flat panel design gives high resolution images, in the most confined spaces, from different orientations and with even greater coverage (25 x 33 cm).

Model 7504 option was specifically designed for security and law enforcement professionals and is flatter, safer, stronger and less expensive than many other fragile flat panel units. It utilizes all the features of the Model 7504 image processing software to produce high resolution x-ray images. It is available as a complete x-ray system or a single flat panel upgrade.



Some great reasons why to invert or to upgrade your old conventional x-ray unit to Model 7504 wedge

- High Resolution Images Utilizes Elaman's powerful imaging software
- Flatter Substantially slimmer than conventional units
- Safer No re-approach to suspect objects
- Stronger No mirrors, and fewer fragile components
- Faster High quality images straight to pc. No reapproach, no scanning, no developing required
- 50% more coverage 25 x 33 cm (10 x 13"). Complete x-ray system fits in a single case
- More rugged in the field Specifically designed for Police and EOD operations
- Less expensive No film, no consumables, fewer fragile components
- More versatile Tri-directional. Use upright or slide in from either side

The Model 7504 option is available as a complete flat panel x-ray solution and/or as an upgrade to Golden portable x-ray systems currently using:

- Costly Polaroid Film or Image Processors
- Conventional CCD imaging Boxes

The Model 7504 option integrates with Elaman's imaging software to produce high resolution x-ray images.

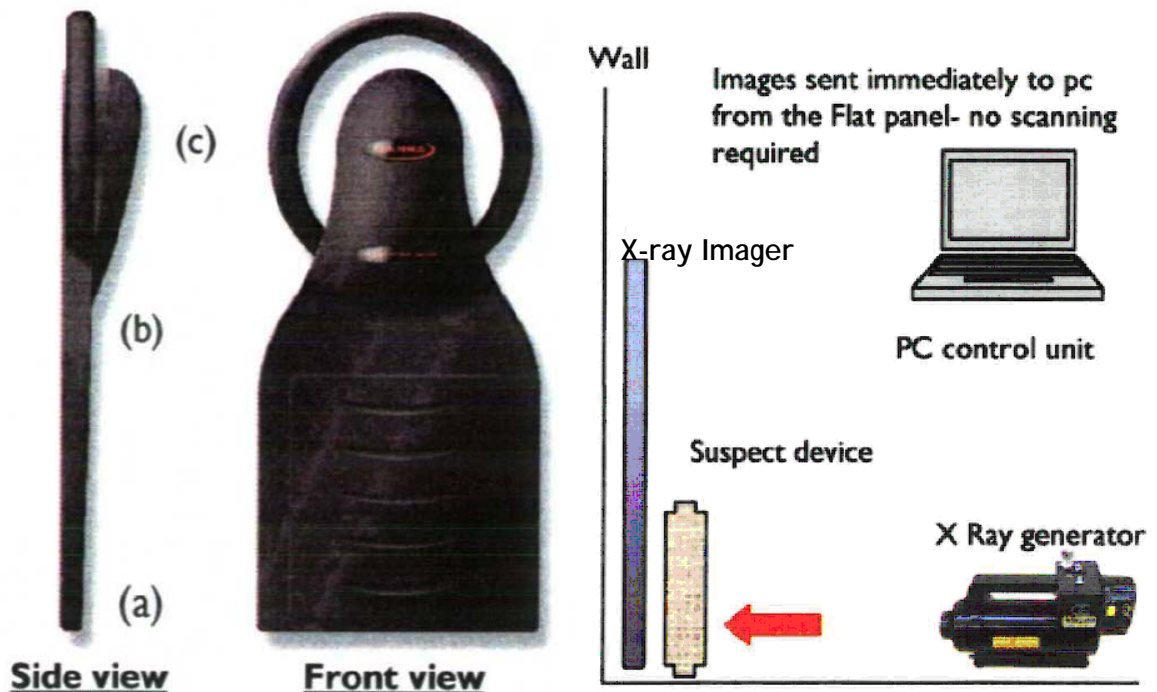
## Advanced Flat Screen X-ray Imager

7504 option

### DIMENSIONS:

Imaging Areas:	25.4 x 33 cm (10" x 13")
(a) Depth (bottom):	2.9 cm (1.1")
(b) Depth top of panel:	3.7 cm (1.45")
(c) Depth at domed area (above screening area):	11.4 cm (4.4")
Width:	34.4 cm (13.5")
Height:	93.2 cm (36.6")

Please note all dimensions are approximate



## Thermal Wall Scanner

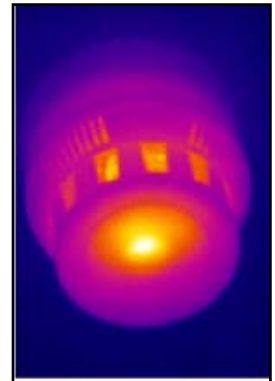
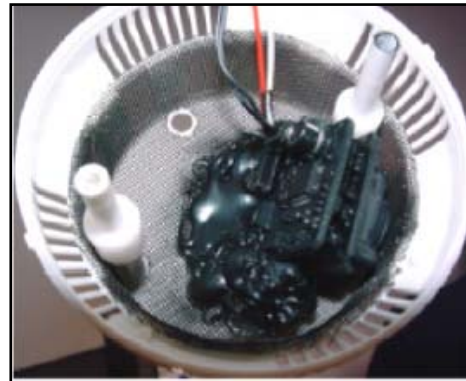
## Model 7505

A physical inspection of a target location is the most time consuming part of a sweep. All surfaces and objects must be inspected. In order to perform a quick and thorough search the Model 7505 has been developed to help locate concealed eavesdropping devices. A concealed device will emit a heat signature easily spotted by the Thermal Inspection System.

The Model 7505 is an ultra-compact infrared CCD camera, which provides advanced and superb image quality, while offering portability and exceptional cost performance. Because it is very small and lightweight, the optional battery-powered camera can be used in very narrow and difficult to reach places. Furthermore, it allows imaging while walking. The system comes with a number of options, e.g. an LCD-display which can be removed from the camera itself and a memory card slot for file storage.

Visual Image

Thermal Image

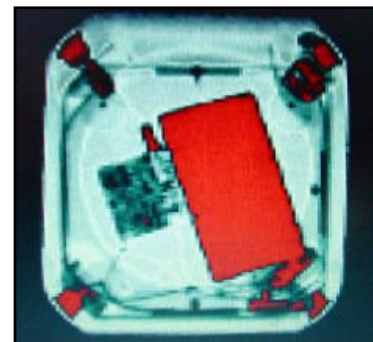
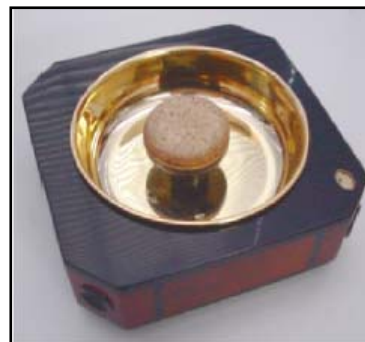


Video Camera

### USAGE

The Model 7505 detects "Hotspots" quickly and reliably. "Hotspots" are very small warm areas generated by bugging surveillance equipment used for eavesdropping, often placed in walls, ceilings or furniture.

Any change in the heat structure of objects can be detected by using the Model 7505.



Ashtray

Ashtray Transmitter

### FEATURES

- Ultra compact IR-camera kit system
- Various accessories
- Digital zoom function with flexible optical objective performance
- File-storage inside the camera using the optional PCMCIA drive
- Camera protection against environment influences by using an optional suitable cover
- RS-232 online control with command software
- TFT color LCD-display with 256 true-color display-integrated control buttons, optional cable extension
- Integrated long-life sterling cryocooler with whispering run
- Digital interfacing corresponding with the PCMCIA, PCI and DRVURBS PC-connection



## Thermal Wall Scanner

## Model 7505

### SPECIFICATIONS

Measuring range	Range 1	Đ20 to 100j C	Đ40 to 120j C
	Range 2	0 to 250j C	0 to 500j C
	Range 3 (option)	100 to 800j C	200 to 2000j C
	Range 4 (option)	200 to 2000j C	Ñ
Resolution	0.06j C (at 30j C 60Hz) — range 1		
Accuracy	±2j C or ±2% of reading		
Spectral range	8 to 14µm		
Focusing range	30 cm to infinity		
Field of view	21.7j (H) x 16.4j (V)		
Frame time	60 frames /sec		
Thermal image pixels	320 (H) x 240 (V) pixels		
A/D resolution	14 bits		
Measuring functions	Run/Freeze		
Interval measurement	Recording on memory card : 2 to 3600 sec interval Trigger function		
Emissive correction	0.10 to 1.00 (at 0.01 step)		
Storage device	Compact flash memory card for:		
	Thermal image in S IT or BMP file format		
	Visible image in S IT or JP E G file format		
Movie recording	Real-time memory : 1664 images (max. 60Hz)		
Video signal output	NTS C/PAL composite video signal, S -video		
Interface	IE E E 1394, R S -232C		
Operating temp/humidity	Đ15 to 50j C, 90% R H or les s (not condensed)		
Storage temp./humidity	Đ40 to 70j C, 90% R H or les s (not condensed)		
Power supply	AC adaptor : 100V to 240V, DC 7.2V (nominal)		
Power consumption	Approx. 6W (typ)		
Shock and vibration	294m/sec <sup>2</sup> (IE C60068-2-27), 29.4m/sec <sup>2</sup> (IE C60068-2-6)		
Environmental protection	IP 54 (IE C60529)		
Dimensions	Approx. 108 (W) x 113 (H) x 189 (D) mm (excluding projection)		
Weight	Approx. 1.3kg (excluding battery and LCD)		
	Approx. 1.6kg (including battery and LCD)		
Standard accessories	AC adaptor, battery pack (2pcs ), battery charger, compact flash memory card, grid belt, neck s trap, lens cap		

## Thermal Imaging for Surveillance Applications Model 7505-2

### HANDHELD IMAGER FOR LAW ENFORCEMENT

Traditionally, thermal imaging is used by law enforcement helicopters and specialist teams.

The Model 7502-2 has been identified as a cost effective solution for all law enforcement operations and has been well received by various Police Forces worldwide after trials within TSU, Firearms and other teams.

- Surveillance
- TSCM Operations
- Recently used vehicle detection



### THE IMAGER UNIT

**An innovative handheld thermal imager that offers outstanding imaging performance, together with flexibility and ease of use at minimal cost.**

This handheld unit delivers affordable thermal night vision for many practical law enforcement uses.

### Technical details

- Large clear display
- Simple operation
- Weighs just .75kg
- Lowest cost high definition imager on the market
- 150+ m image range
- Image storage to SD card
- Temperature measurement ideal for hydroponics
- 160 \* 120 image

### Proven Technology

The technology within this small unit has been used in industrial and commercial applications for over a decade.

### Range of options and accessories

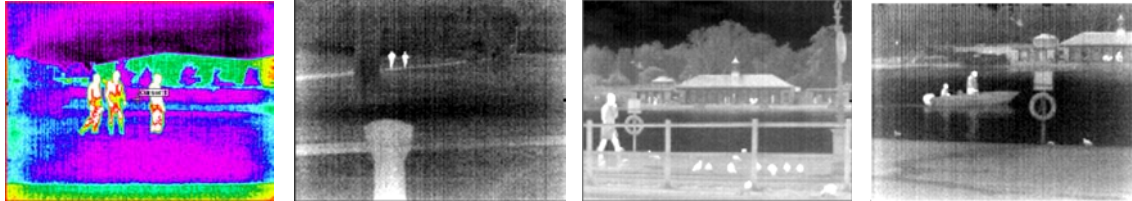
- Car and desk chargers
- Unit with higher image updating speed (35 frames/second)
- Unit with twice the image range (250+ m)





## Thermal Imaging for Surveillance Applications Model 7505-2

### SURVEILLANCE APPLICATIONS



#### Detects people in total darkness and allows covert distance surveillance

- Covert Surveillance
- Monitoring of arrivals and departures
- Monitoring of open areas
- Safer parks initiatives

In darkness, thermal imaging gives the ability to “see” in zero light conditions proving valuable in many situations.

Surveillance features include

- High resolution 160x120 pixel image
- Large clear screen
- Auto hotspot tracker – useful for highlighting people
- Selectable color palettes
- Digital x2 zoom
- Optional screen shade to prevent light emission/reflection image storage to SD card

#### An important tool for “sweeping” buildings

For non-alerting bug detection, the unit provides measurement of surface temperatures and visible indication of irregularities.

Where a listening device/bug is working, it may alter the temperature of the adjacent material/wall.

- This temperature difference will be shown as a “hot spot”

During a house search, the unit can be used at arm’s length to scan cupboards, difficult to reach places, lofts and hatches, etc.

- A picture is taken first, then unit is withdrawn so the image can be looked at before the officer enters the confined space

Firearms teams have successfully been using this unit during recent exercises and operations.

### SCOPE OF DELIVERY

#### The unit comes with

- Camera and rechargeable battery
- Wrist strap
- Carry case
- Charger
- Software on CD
- SD Memory card/SD memory card reader

## Locator

## Model 7506

### LOCATOR RADIO MICROPHONE DETECTOR

#### THE RF NEAR FIELD COMPONENT

The Model 7506 was developed for counter electronic surveillance. Its primary requirement was to be able to covertly detect clandestine Radio Microphones that could effectively be used by both non-experienced and experienced counter measure personnel. Its performance therefore had to be independent of the local RF environment, a domain where many previous instruments failed.

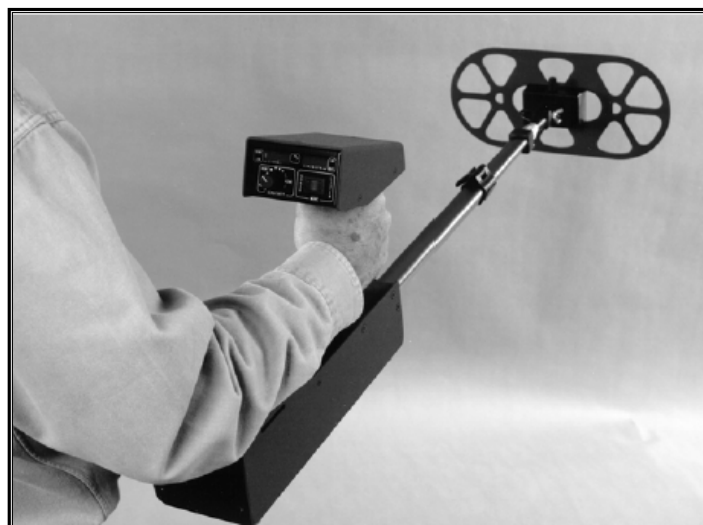
The result is Model 7506, which is a differential broadband "H" field detection system, has the following specifications:

#### TECHNICAL

Frequency Range	25 MHz - 4 GHz and beyond
Detection capabilities	All types of Radio Microphone including "Smart" bugs, such as frequency hopping and spread spectrum.
Audible Warning	SONAR or Listen (demodulation) modes, via closed headphones.
Visual Warning	Field strength with direction finding read out

#### PHYSICAL

Hand held with an antenna system mounted on a telescopic boom. The antenna head is detachable for easy storage in a custom foam-lined case. It is supplied with high quality closed headphones.



## Optical System to Detect Cameras, Lenses Model 7507-01

The Model 7507-01 camera detector is a small device, which enables you to quickly and effectively detect hidden cameras.

When sweeping the designated premises (study, living room, office etc.) with the device, keep in mind that a pin-hole camera is always aimed at a certain zone, a bed, a table etc., where it is easier to observe people. Stay in these zones when sweeping the room with the device.

Cameras may be fixed not only to the walls or ceiling, but into the interior of some objects like clocks, lamps, fire and safety sensors, files for documents, sockets, switches etc.

Several cameras may be installed, that is why after detection of one camera, continue to sweep the room with the device in different directions.

The best operating distance when sweeping a room is 2-4 m.

When sweeping surfaces and objects with the device, gently move the observation zone up and down.

When inspecting an area with reflecting surfaces (mirrors, polished furniture etc.), always position yourself so that there is no direct reflection between you and the mirrored surface. This will stop the direct back-reflection of laser emission and light in the eye-piece.



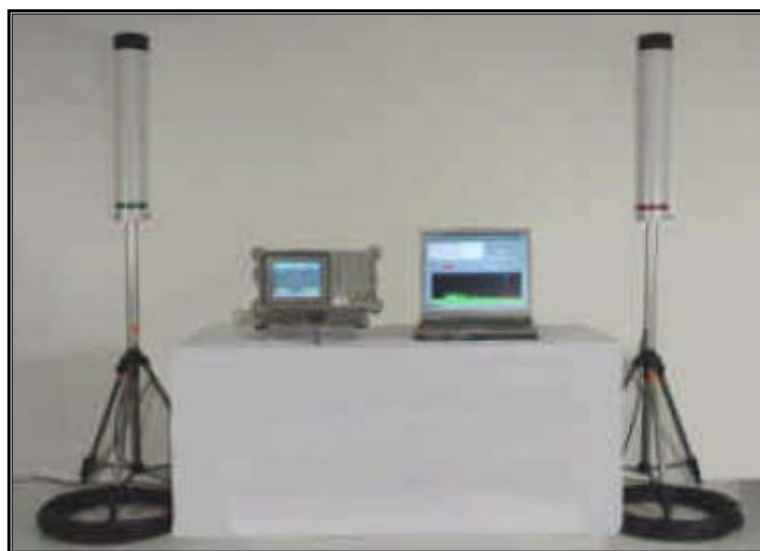


## Advanced Scan Detector System

## Model 7508

### DESCRIPTION

The Advanced Scan Detector System, Model 7508, is uniquely different from all other RF Detection Systems. It is an advanced system which uses spectrum analyzer with the latest software technologies to provide accurate results. It uses a twin antenna system, placing one antenna outside the target location and one inside. Using the software it is able to show all suspicious transmissions which are stronger in the target location than outside. This is a strong indicator of a transmitting eavesdropping device.



### USAGE

Today's advanced bugs can use digital-burst transmission, including low power, making it extremely difficult to detect with standard spectrum analyzers. The Model 7508 compares the RF activities inside a danger area with the spectrum outside. By using the software options there is an "online" possibility to detect all kinds of newer RF bugs, also "low power devices", burst- or spread spectrum-transmissions.

### FEATURES

- Measurements possible between 9 kHz and 26.5 GHz
- Switchable increase of input power
- Inputs and outputs for video signals with BNC connectors
- 6" TFT-Display
- Smallest spectrum analyzer of its kind
- Practical shoulder belt
- Rubber protections
- Optional differential spectrum analyzing software with additional antenna and switching hardware
- The differential software up the 7508 enables 24-hour detection and location of any transmitter's radio surveillance earphone

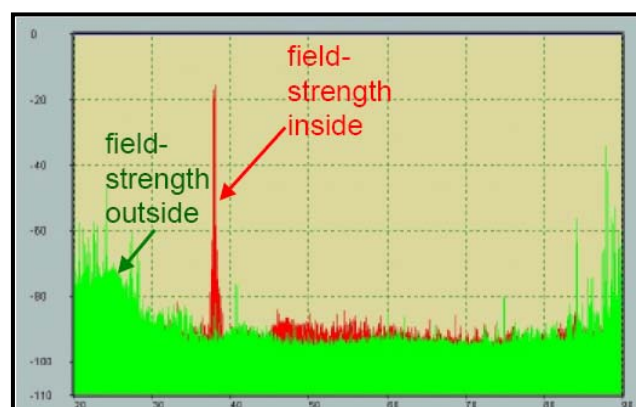
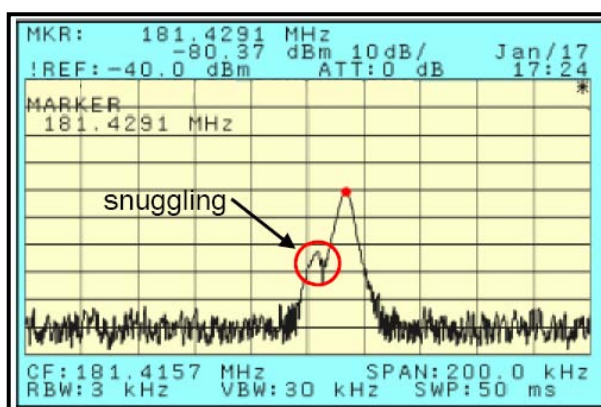
# Advanced Scan Detector System

# Model 7508

## TECHNICAL DATA

Basic Unit	
Frequency range:	9 kHz to 26.5 GHz
Resolution bandwidths:	1 kHz to 3 MHz
	5 MHz in Function ZS
Phase noise:	-100 dBc/Hz to zu 3 GHz
Noise floor down to:	-145 dBm at 100 Hz RBW
Tracking generator:	2.2 GHz
Output level:	-31 to 0 dBm in 1 dB S.
Input level:	+ 27 dBm
Storage media:	2 PCMCIA-Slots
Power:	- 230 V Netzteil
	- Akku-Pack (max. 1,5 h)
	- 12 V DC

OPTIONS	
with Option 26:	100 Hz und 300 Hz
with switched-on pre amplifier with a gain of >25dB	
with Option 74:	2.7 GHz



## TDR Multi-Channel Cable Detector

## Model 7509

The TDR is one of the most valuable TSCM test instruments available. This equipment is capable of detecting many wiretap methods that are undetectable by conventional telephone analyzers, meters or other instrumentation.

The TDR is designed to reveal all wire irregularities (impedance mismatches) by displaying the characteristic signatures and distances to each wire irregularity. Without a TDR, the presence and location of all wire irregularities cannot be pinpointed, and therefore will not be physically inspected. This can also establish possible previous wiretap activity, or modifications intended for future use. Since many wiretap operations are fairly short-lived, this information can be extremely important. Without a TDR, the TSCM technician would be unable to detect hidden parallel bridge taps, split/resplit inductive wiretaps, mini-taps or other forms of clandestine telephone line modifications.

### USAGE

The TDR can quickly, safely and reliably locate the following cable defaults:

- Inductive line tap
- Capacitive line tap
- Split/resplit
- Disconnections
- Illegal wire tapping
- Short circuits
- Alteration of impedance
- Change of pairs
- Return loss
- Intermitting faults



### FEATURES

- Tests both twisted pair and coaxial cables
- Superior fault location in any industry and any application
- Sub-nanosecond pulse width in coaxial mode locates small, often unsuspected, faults that are close together
- RANGE-PLUS simplifies keypad operation by combining a specific pulse width, vertical gain, and cable length
- Live waveform testing
- Intermittent Fault Detection (IFD) mode detects and displays intermittent faults and allows the operator to manipulate and reposition the waveform without affecting the IFD function
- Noise filters eliminate unwanted waveform noise
- Rugged, weatherproof packaging
- Portable, compact, lightweight

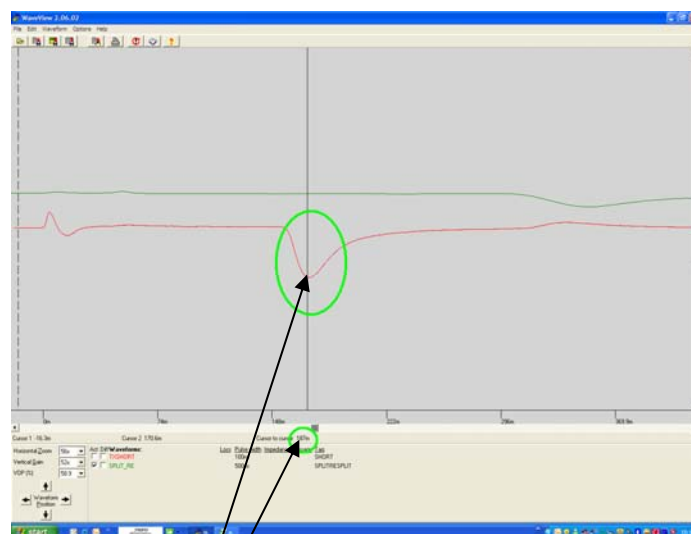
### TECHNICAL DATA

Measurement range:	10 m to 19.4 Km
Pulse width symmetrical:	2ns, 25ns, 100ns, 1ms, 6ms
Pulse width coaxial:	0.9, 5, 25, 100, 500 ns
Precision, symmetrical:	+/- 0.15m + 0.01 % v. MW

## TDR Multi-Channel Cable Detector

## Model 7509

Precision, coaxial:	+/- 0.03m + 0.01 % v. MW
Max. resolution:	0.1 m at v/2
Handling:	One function per button
v/2 adapting:	m/ms from 48 to 148
Adapting:	various
Waveform storage, standard:	8 waveforms
Waveform storage, optional:	32 waveforms
Input protection:	400 volts (AC + DC) from DC to 400 Hz and decreases to 10 volts at 1 MHz
Serial I/O port:	RS-232
Display:	320 x 240 dot matrix liquid crystal display (LCD) with CFL backlighting
Power source:	internal, rechargeable 7.2 nickel metal hydride
Charging source:	external 12 VAC, 1.3 A
Operating time:	>6 h continuous without backlight
Operating temperature:	32 dF (0°C) to 122 dF (50°C)
Typical temperature:	5 dF (-15°C) to 140 dF (60°C)
Storage temperature:	-4 dF (-20°C) to 140 dF (60°C)
Humidity:	95 % max. relative humidity non condensing
Dimensions (W x D x H):	9.75 in x 5 in x 10.5 in/247.6 mm x 127 mm x 267 mm
Weight:	6 lb (2.7 kg)



Eavesdropping device located and distance

## Digital Advanced Handheld Oscilloscope

## Model 7510

### DESCRIPTION

The Model 7510 includes a multifunctional measurement system with oscilloscope and millimeter facilities. Furthermore, it has a built-in paperless writer. The rechargeable NiMH-battery packs guarantee a usage of 4 hours (AC-independent) work and are able to be recharged within 4 hours. With its several automatic power saving possibilities, the Model 7510 can last all day.

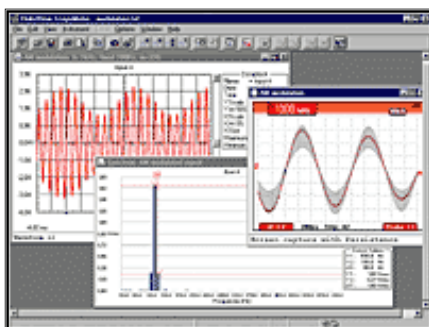
### USAGE

The Model 7510 is an important tool to handle all the different basic measurements for

- TC (Telecommunication networks)
- DC (Data communication networks)
- ACS (Access control systems)
- FDS (Fire detection systems)
- IDS (Intrusion detection systems)
- EIB (European installation bus)
- BBTv (Broadband television)

### FEATURES

- Dual input, available with 60, 100 or 200 MHz bandwidth
- Up to 2.5 GS/s real-time sampling per input
- mAs current-over-time measurement
- Connect-and-View™ automatic triggering, a full range of manual trigger modes plus external triggering
- 30,500 points per input record length using Scope Record™ mode
- Automatic capture and replay of 100 screens
- 24 automatic waveform measurements
- Cursor, zoom and real-time clock
- Four hour rechargeable NiMH battery pack
- 1,000V CAT II and 600V CAT III safety certified
- Up to 1,000V independently floating isolated inputs
- Includes a 5,000 count true-rms multi meter and a Trend Plot™ paperless recorder



The software helps you get more out of your scope meter by

- **Documenting:** transfer screens, waveforms and measurement data from the scope meter to your PC for printing, or to import data to other programs
- **Archiving:** Store and retrieve waveforms with text annotations and create your own library for easy reference and comparison
- **Analysis:** gather valuable measurement data and enable cursor measurements to reveal relationships and conditions

# Digital Advanced Handheld Oscilloscope

# Model 7510

## TECHNICAL DATA

Bandwidth	Fluke 199C, 199B: 200 MHz
Max. real time sample rate	2.5 GS/s
Display	144 mm Full Color LCD
Digital Persistence	Yes, Gives analog oscilloscope like waveform decay (user selectable)
FFT Analysis	Frequency spectrum analysis using mathematical function Fast Fourier Transform (FFT)
Envelope mode	Yes
Waveform Compare	Visual Reference and Automatic Pass/Fail testing
Max. record length in Scope mode:	3000 points per input channel
in Scope Record mode:	27,000 points per input or more (5 ms/div to 2 min/div.)
Number of inputs	2 plus external / DMM input, all isolated from each other and from ground
Number of digitizers	2
Independently floating isolated inputs	Up to 1000 V between inputs, references and ground
Glitch capture	Up to 3 ns using Pulse Width triggering; 50 ns peak detect at 5 ms/div. to 1 min/div.
Time base range in Scope mode	5 ns/div to 2 min/div
Trigger types	Connect-and-View <sup>®</sup> , Free Run, Single Shot, Edge, Delay, Video Frame, Video line, Selectable pulse width and External
Advanced Trigger Types	N-Cycle Trigger. Delay Trigger by N events Dual Slope Trigger. Trigger on both rising and falling edges of waveform
Scope Measurements	7 cursors measurements, 30 automatic measurements

## Digital Advanced Handheld Oscilloscope

## Model 7510

Cursor-limited Automatic Measurements	Vrms or Wavg automatic measurement within cursor defined time limits
Scope-Record Trigger modes	Start on Trigger, Stop on Trigger
Capture last 100 screens	Automatic, with Replay capability
Dual input Trend Plot	Yes, with Cursors and Zoom
Memory for screens and set-ups	10 screens with set-up 5 more memories are made available upon registration of the Scope Meter
Memory for recordings	Two, each can store 100 scope screens, a Scope Record or a Trend Plot
True RMS multi meter	5000 counts, Volts, Amps, Ohms, Continuity, Diode, Temp
Battery (installed)	4 hr Ni-MH BP190
Line power	Adapter / battery-charger included
Size	25.6 x 16.9 x 6.4 cm (10.1 x 6.7 x 2.5 inch)
Weight	2 kg
PC and Printer interface	Using optional Optically Isolated RS232 adapter/cable



## Detection Receiver

## Model 7511

One of the first tools to be used during a physical search should be the Detection Receiver. This versatile unit can indicate the location of a transmission source, whether hidden in phone, room or body transmitters, remote control signals, computer bugs, fax or telex transmitters, video transmitters, pulsed tracking transmitters, spread spectrum, and even wide band frequency hopping or 'burst' transmitters. This is a multi use tool which covers a wide range of tasks from basic physical searches to cable verification.

### BROADBAND DETECTOR ADVANTAGES

**Portable Sweep Kit** - provides everything needed to perform a professional sweep; fits inside a standard briefcase.

**Multi-Functional Utility** - Comes with probes to detect RF transmitters (audio and video), carrier current transmitters, and telephone bugs. Probes are also available to detect for infrared transmitters, tape recorders, and acoustic leakage.

**Wideband Coverage** - From 200Hz to over 3GHz with no holes or gaps.

**Monitor Mode** - After a sweep, the alarm monitor (silent or audible alert) guards against new devices brought in or remote control activation of surveillance devices.

**Auxiliary Audio Input** - Allows user to listen to telephones or lines for "hotmikes," hookswitch by-pass and "infinity" bugs. Unknown wires and cables can be tested for wired microphones.



### TECHNICAL SPECIFICATIONS

#### R.F. PROBE:

- **Gain:** 20dB nominal frequency
- **Response:** 50kHz-2GHz  $\pm 3$ dB 3GHz-10dB
- **Sensitivity:** -62dBm (1 segment) -85dBm M.D.L.

#### VLF PROBE:

- **Frequency Response:** 15kHz-1MHz-3dB
- **MAX input voltage:** 300 VAC 50-60Hz
- **Isolation:** 1500 VAC 60Hz
- **Sensitivity:** -38dBm (1 segment) -60 M.D.L.



## Detection Receiver

## Model 7511

### AUDIO AMPLIFIER:

- **Input Impedance:** 50K Ohm balanced
- **Input Range:** 1.7 $\mu$ V-10V (135dB) AGC
- **Dynamic Range:** 100dB (high and low gain)
- **Frequency Response:** 100Hz- 15kHz $\pm$ 3dB (filtered) 500Hz-24dB/octave, 2.5kHz-18dB/octave
- **Headphone Output:** 5Vp-p 220  $\Omega$
- **Record Out:** 25 mVp-p nominal with AGC

### DISPLAY:

- **LCD Bargraph:** 18 segment with pulsing single segment trip point
- **50dB Dynamic Range** (1 segment High Gain to MAX Low Gain)
- **Alert Output:** 2.8kHz tone or silent red LED at 2Hz
- **Remote Output:** N.O. contact (300mA 25V MAX)

### BATTERY:

- **8 ea. MN1500** AA Alkaline - Life 10-16 hrs
- (Optional) 8 ea. 550mAh NiCad - life 3-5 hrs per charge
- **Low Battery Indicator:** approx. 10% remaining power

### AC ADAPTER/CHARGER:

- **Input:** 95-130VAC 50-60Hz, or 200-275VAC 50-60Hz
- **Output:** 12VDC with 500mA NiCad Recharge Time: 8-10 hrs

### CPM-700 UNIT:

- **Size:** 9 1/8 x 6 1/8 x 1 3/4 in, 23.2 x 15.6 x 4.4 cm
- **Weight:** 39 oz, 1.1 kg

### CARRY CASE WITH ALL STANDARD ITEMS:

- **Size:** 16 3/8 x 11 1/4 x 3 in, 41.6 x 28.6 x 7.6cm
- **Weight:** 7 lbs, 3.18 kg

## Wall Depth Measurement System

## Model 7513

### DESCRIPTION

The Model 7513 is a metal detector using a visual display to control iron inlays inside walls, floors or ceilings. The results of this easy-to-handle positioning and measurement system are based on electromagnetic effects which are shown on an LCD Screen.

### USAGE

Model 7513 is used to produce visual information of length, width, depth, position and quality of iron inlays in concrete and other ferromagnetic metals inside closed materials. This metal detector allows for a speedy visual search for hidden bugs inside buildings



### FEATURES

- Easy analysis of iron material inside walls, floors or ceilings by using a visual display
- Zoom function
- Measurement information of the depth
- Picture processing possible by:
  - Import in Word
  - Output to an external printer
- Less height of the probe
- Delivery in a strong tool case with accessories

### TECHNICAL DATA

Speed of measurement:	0.5 m/s
Max. depth:	180 mm
Amplifying of width:	between 6 to 36 mm
Max. sphere of measurement at one run through:	600 mm x 600 mm
Working temperature:	between -10°C to +50°C
Size of probe:	230mm x 133mm x 140mm
Size of monitor:	270mm x 195mm x 80mm
Max. sphere of measurement without download:	15m <sup>2</sup>

## TSCM Video Remote Probe Inspection

## Model 7514-2

### PRODUCTIVITY TOOL

For TSCM search operational comes a revolutionary new video borescope – the Video Probe Remote Visual Inspection System – a power tool for improving tscm inspection productivity.

### FEATURES

- Extra-bright, high-resolution LCD screen and high-output illumination deliver sharp, clear images
- Dual-purpose shipping and operating case
- Lightweight wireless remote control (optional)
- Powerful computing platform for data management and worldwide connectivity



### QUICKCHANGE™ PROBES

With its interchangeable QuickChange probes, the Video Probe Remote Visual Inspection system quickly reconfigures probe diameter and length for maximum productivity.

Probes come in 3.9 mm, 6.1 mm, and 8.4 mm diameters. The 6.1 mm probes are built for increased durability with:

- Titanium camera head that is 8 times stronger than older designs
- Laser-welded bending neck seam which strengthens a critical joint
- A double tungsten braid insertion tube for added crush resistance



### SYSTEM

The base unit is a portable workstation for inspection data management, as well as a light source and storage reel for the probe. The unit features:

- 512 MB (standard) up to 4 GB (optional) internal CompactFlash® card
- 3 USB 2.0 ports
- 10/100 Ethernet port for PC with optional Internet connection
- Optional battery/UPS pack in one- or two-hour capacities
- Two PC card slots that accept memory and communication cards
- User configurable NTSC/PAL video format selection



# TSCM Video Remote Probe Inspection

# Model 7514-2

## TECHNICAL SPECIFICATIONS

<b>OPERATING ENVIRONMENT</b>		
<b>System Operating Temp:</b>	<b>Operating</b>	-4° to 115°F (-20° to 46°C) LCD requires warm-up period below 32°F (0°C)
<b>Tip Operating Temp:</b>		-13° to 176°F (-25° to 80°C) Reduced articulation below 32°F (0°C)
<b>Storage Temperature:</b>		-13° to 140°F (-25° to 60°C)
<b>Relative Humidity:</b>		95% max, non condensing
<b>Waterproof:</b>		Insertion tubes are watertight to 1 bar (14.5 psig, 10.2 m [33.5 ft.] of H2O)
<b>Hazardous Environments:</b>		Not rated for use in hazardous environments
<b>SYSTEM</b>		
<b>Case Dimensions:</b>		
<b>Standard:</b>		54.6 x 49.5 x 32.0 cm (21.5 x 19.5 x 12.6 in.)
<b>Tall:</b>		54.6 x 60.9 x 32.0 cm (21.5 x 24 x 12.6 in.)
<b>Weight:</b>		
<b>In Case:</b>		21.8 kg (48 lbs.)
<b>Without Case:</b>		10.9 kg (24 lbs.)
<b>QUICKCHANGE™ PROBES</b>		
<b>6.1 mm (0.242 in.) and 8.4 mm (0.331 in.) Diameter Probes</b>		
<b>Image Sensor:</b>		1/6" Color SUPER HAD CCD®
<b>Pixel Count:</b>		440,000 pixels
<b>Temperature Sensor:</b>		Integrated Temperature Warning System
<b>Camera Housing:</b>		Titanium
<b>Articulation:</b>		360° All-Way®
<b>Tip Optics:</b>		Double threaded attachment
<b>3.9 mm (0.154 in.) Diameter Probes</b>		
<b>Image Sensor:</b>		1/10" Color, SUPER HAD CCD
<b>Pixel Count:</b>		290,000 pixels
<b>Camera Housing:</b>		Titanium
<b>Articulation:</b>		360° All-Way
<b>Tip Optics:</b>		Double threaded attachment
<b>HANDSET</b>		
<b>Dimensions:</b>		39 x 18 x 13 cm (15.4 x 7.1 x 5.1 in.)
<b>Weight:</b>		1.81 kg (3.98 lbs.)

## TSCM Video Remote Probe Inspection

## Model 7514-2

<b>Construction:</b>	Polycarbonate housing with integrated elastomer bumpers
<b>LCD:</b>	16.3 cm (6.4 in.) diagonal, 16 x 9 aspect ratio, 800 x 480 pixels, wide VGA
<b>LCD Brightness:</b>	380 nits (cd/m <sup>2</sup> )
<b>Power Tube:</b>	2.4 m (8 ft.) long
<b>User Controls:</b>	Joystick and complete button function set
<b>Microphone:</b>	Built-in microphone for audio annotation located on the top center of the handset
<b>BASE UNIT</b>	
<b>Dimensions:</b>	44 x 22 x 35 cm (17.3 x 8.7 x 13.8 in.)
<b>Weight:</b>	7.21 kg (15.90 lbs.)
<b>Construction:</b>	Aluminum chassis with polyurethane bumpers
<b>System CPU:</b>	Intel Pentium® M
<b>Video Processors:</b>	Multiple digital signal processors
<b>Brightness Control:</b>	Automatic and variable, adjustable auto gain and exposure
<b>System Memory:</b>	Internal CompactFlash® card, 512 MB (standard) to 4 GB (optional)
<b>Lamp Type:</b>	75W High Intensity Discharge (HID)
<b>Lamp Output:</b>	4300 Lumens
<b>Lamp Life:</b>	1000 hour median
<b>Keyboard Input:</b>	USB keyboard with built-in trackball
<b>Video Outputs:</b>	Switchable NTSC/PAL S-Video, Standard 15-pin PC video connector
<b>Video Input:</b>	Auto detecting NTSC/PAL S-Video
<b>USB:</b>	Three external USB 2.0 ports
<b>Ethernet:</b>	Integrated 10/100 Ethernet port
<b>PCMCIA:</b>	Two 32-bit PC card slots
<b>AC Input:</b>	AC Nominal input: 100 to 240 V, 50 to 60 Hz; 115 V, 400 Hz; 275 W max
<b>AC Output:</b>	100 W max; IEC320-2-2 Type F connector
<b>AC Fuse:</b>	6.3A, 250V, fast acting
<b>DC Input:</b>	11 to 15 VDC; nominal 12 VDC; 150 W max
<b>DC Fuse:</b>	20A, 600 VDC, fast acting
<b>Audio Connectors:</b>	<b>Output</b> Built-in front panel speaker, 3.5 mm stereo line level out, 2V RMS max, 3.5 mm stereo headphone

## TSCM Video Remote Probe Inspection

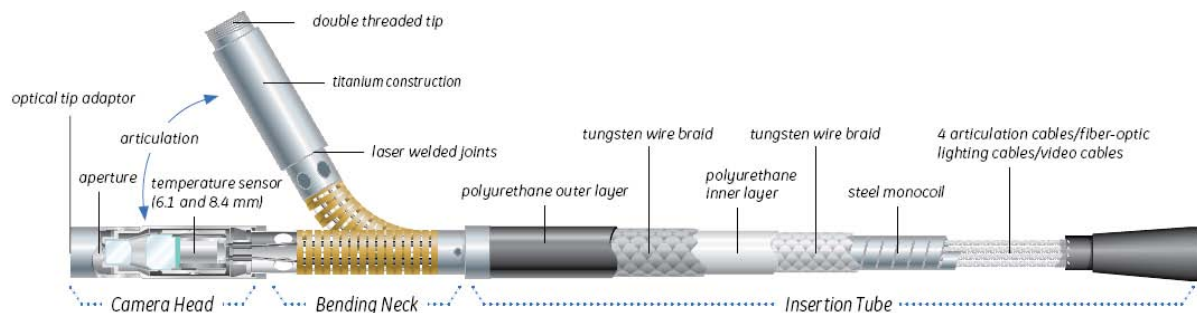
**Model 7514-2**

<b>Audio Input Connector:</b>	3.5 mm microphone
-------------------------------	-------------------

### TIP ARTICULATION

Length	Straight Tube
4.5 m and less	Up/Down – 150° min, Left/Right – 150° min
6.0 m	Up/Down – 130° min, Left/Right – 130° min
8.0 m	Up/Down – 120° min, Left/Right – 120° min
9.6 m	Up/Down – 90° min, Left/Right – 90° min

### INSERTION TUBE



### TECHNICAL SPECIFICATIONS

#### SOFTWARE

<b>Operating System:</b>	Multitasking with desktop software options
<b>User Interface:</b>	Drop-down menu driven operation, joystick, and keypad
<b>File Manager:</b>	File and folder creation, naming, copying and deleting
<b>Audio Data:</b>	PC compatible, 15 second files (WAV or MP3 format). PCM audio with MPEG2 video recordings
<b>Image Controls:</b>	Adjustable brightness, 1/10,000 sec to 12 sec exposure. Left/Right invert for side-view tip correction. Freeze frame, live/still Inverse+ enhancement, side-by-side split screen
<b>Digital Zoom:</b>	1X to 3X – Continuous and 5-level stepped
<b>User Available Memory:</b>	100 MB internal, user-supplied external
<b>Annotation:</b>	Text and arrow overlays and custom logos
<b>Articulation Controls:</b>	360° All-Way® steering, Steer-and-Stay™, Home
<b>Lamp Control:</b>	On/Off, menu-controlled
<b>Software Updates:</b>	Field upgradeable via removable media
<b>Temperature Warning:</b>	Integrated camera and base unit temperature warning systems
<b>DVD writing:</b>	DVD+R, DVD-R, still images, audio clips, MPEG2 video and PCM audio real-time recording

# TSCM Video Remote Probe Inspection

# Model 7514-2

## MEASUREMENT

Supported Measurement Features

Feature	ShadowProbe®	StereoProbe®	Comparison
Length/Distance	■	■	■
Depth	■	■	
Point-to-Line	■	■	■
Non-perpendicular Length	■	■	
Area	■	■	■
Multi-Segment Length	■	■	■
Circle Gauge	■		■
3x Zoom Windows	■	■	■
5 Measurements per Image	■	■	■

## OPTICAL TIPS

Tip View (DOV)	Tip Color	Field of View (FOV)*	Depth of Field (DOF)	3.9 mm Optical Tip Part #	6.1 mm Optical Tip Part #	8.4 mm Optical Tip Part #
<b>Standard Tips</b>						
FORWARD	NONE	☒	80°	6-80 mm (0.24-3.15 in.)	PXT480FG	
FORWARD	NONE	☒	50°	50 mm (1.97 in.)-infinity		XLG3T6150FF
FORWARD	WHITE	○	50°	12-200 mm (0.47-7.87 in.)		XLG3T6150FG
FORWARD	BLACK	●	120°	5-120 mm (0.20-4.72 in.)		XLG3T61120FG
FORWARD	NONE	☒	40°	250 mm (9.84 in.)-infinity		XLG3T8440FF**
FORWARD	YELLOW	●	20°	500 mm (19.68 in.)-infinity		XLG3T8420FF
FORWARD	GOLD	●	80°	25-500 mm (0.98-19.68 in.)		XLG3T8480FG
FORWARD	BLACK	●	120°	5-200 mm (0.20-7.87 in.)		XLG3T84120FN
SIDE	BROWN	●	80°	4-80 mm (0.16-3.15 in.)	PXT480SG	
SIDE	BROWN	●	50°	45 mm (1.77 in.)-infinity		XLG3T6150SF
SIDE	GREEN	●	50°	9-160 mm (0.35-6.30 in.)		XLG3T6150SG
SIDE	BLUE	●	120°	4-100 mm (0.16-3.94 in.)		XLG3T61120SG
SIDE	RED	●	80°	1-20 mm (0.04-0.79 in.)		XLG3T6180SN
SIDE	BROWN	●	40°	250 mm (9.84 in.)-infinity		XLG3T8440SF**
SIDE	GREEN	●	80°	25-500 mm (0.98-19.68 in.)		XLG3T8480SG
SIDE	BLUE	●	120°	4-200 mm (0.16-7.87 in.)		XLG3T84120SN
<b>ShadowProbe® Measurement Tips</b>						
FORWARD	WHITE	○	50°	12-30 mm (0.47-1.18 in.)		XLG3TM6150FG
SIDE	BLUE	●	50°	7-24 mm (0.28-0.94 in.)		XLG3TM6150SG
<b>StereoProbe® Measurement Tips</b>						
FORWARD	BLACK	●	60°/60°	4-80 mm (0.16-3.15 in.)		XLG3TM616060FG
FORWARD	BLACK	●	50°/50°	5-45 mm (0.20-1.77 in.)	PXTM45050FG	
FORWARD	BLACK	●	60°/60°	4-50 mm (0.16-1.97 in.)		XLG3TM846060FG
SIDE	BLUE	●	50°/50°	2-50 mm (0.08-1.97 in.)		XLG3TM615050SG
SIDE	BLUE	●	50°/50°	4-45 mm (0.16-1.77 in.)	PXTM45050SG	
SIDE	BLUE	●	60°/60°	4-50 mm (0.16-1.97 in.)		XLG3TM846060SG

\*FOV is specified diagonally.

\*\*Indicates tips with maximum brightness.

## Marking Kit – Covert Stickers Illuminator

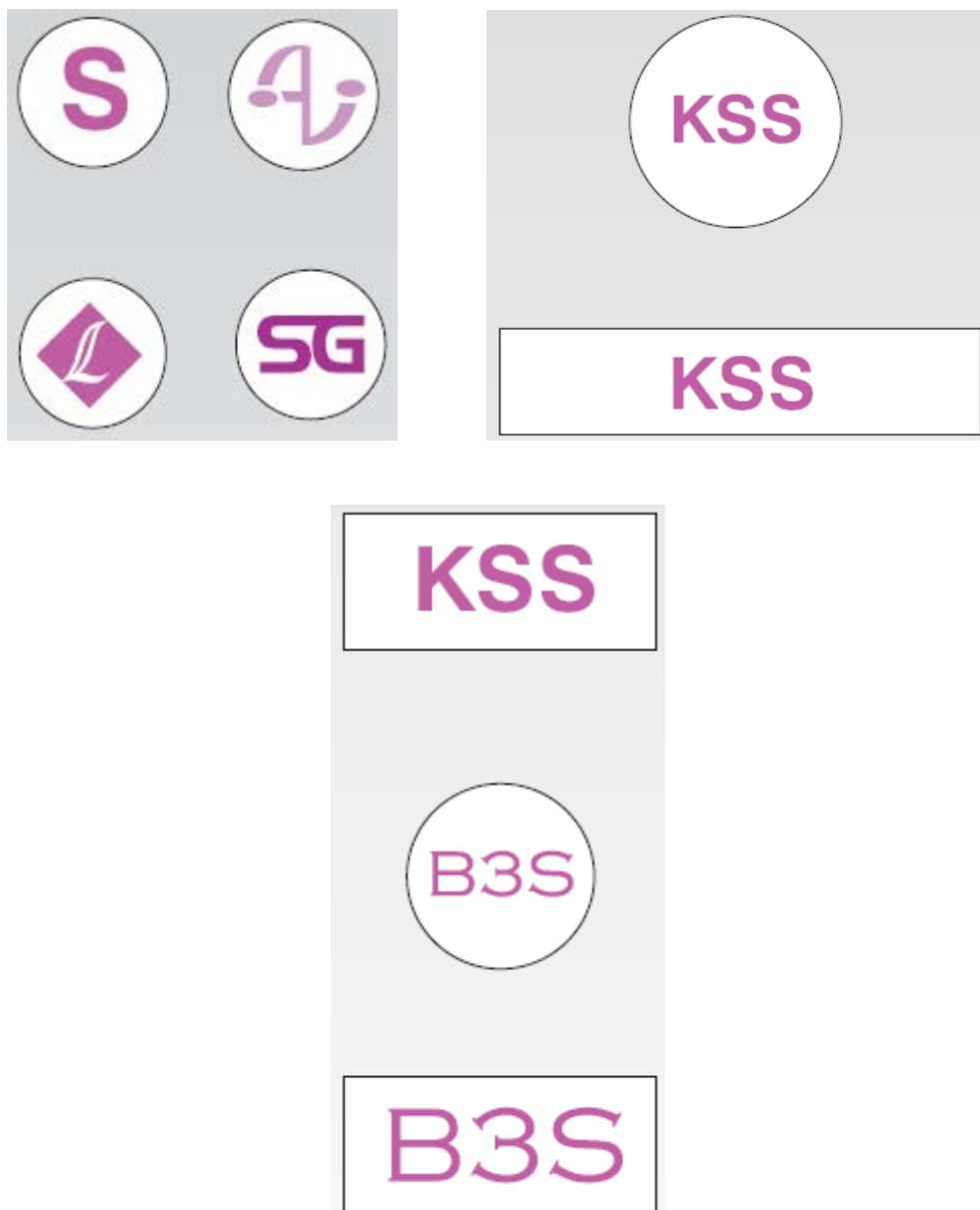
Model 7515

A thin gauge ultra destruct acetate with similar tamper evident properties to the type C vinyl.

This is a cleat material, suitable for covert application and has a permanent acrylic based adhesive for use on any smooth, non porous surface especially glass and most forms of plastic

Invariably printed with UV (invisible) test or design which can be detected by using a UV light source

### SAMPLE LAYOUTS





## Optical Search Kit

## Model 7516

The Optical Search Toolkit is the budget alternative accessory kit to enable a thorough and effective physical search. For use in validating information provided with other equipment, such as the NLJD, the Optical Search Toolkit is ideal for searching hard to reach and inaccessible areas.



The kit includes a side viewing endoscope for searching inaccessible areas (for example, wall cavities, crawl spaces, ventilation ducts, behind dashboards) through a gap of 10mm (0.4 in) in diameter. A 10W halogen lamp on the tip of the endoscope provides bright illumination and enables inspections to be made over distances of up to 1.5m (5ft). Power for the endoscope is supplied from a secondary power socket in the fluorescent handlamp included in the kit.

Search mirror equipment includes a long telescopic arm that extends to 1500mm (59in.) for inspecting inaccessible areas in buildings, and a short fixed length model which is ideal for room searches. Both can be fitted with the range of interchangeable mirrors supplied.

The kit also contains a fluorescent handlamp to provide a wide area working light and two right angle flashlights with belt clips.

A selection of miniature mirrors and light probes and illuminated magnifiers are included to assist in the internal inspection of hard to reach areas. Mirror sizes range from 4.5 to 64mm in diameter.



# Optical Search Kit

# Model 7516

## SPECIFICATIONS

Kit contents	Inventory & Specifications
Flash light	Right angle 2 C-cell (2 per kit)
Handlamp	Fluorescent, 12 W, socket for endoscope
Endoscope	10w lamp, 9.65mm (0.38in) diameter, 350mm (13.8in), side viewing (90° to shaft)
Mirror arm with flashlight	500mm (19.7 in), 45° mirror angle, 2 D-cell
Mirror arm	Telescopic, 1500mm (59in) open, 390mm (15.3in) closed
Mirror	140mm (5.5in) diameter, glass, convex, 127g (4.48oz) (3 per kit)
Mirror	64mm (2.5in) diameter, glass, plano, 32g (1.12oz) (2 per Kit)
Mirror	64x114mm (2.5x4.5 in), glass, plano, 68g (2.4oz) (1 per kit)
Battery Handle	2C-cell (2 per kit)
The following light probe fit the battery handle	
Lamp holder	Converts battery handle to torch
Magnifier	x8 with lamp
Light probe	2mm 0.08in) diameter, 150mm (5.9 in) length
Mirror sleeve	4.5mm (0.18in) diameter, mirror, fits light probe LP2/150
Light probe	3mm (0.12in) diameter, 50mm (1.97in) length
Mirror sleeve	9.5mm (0.37in) diameter, mirror, fits light probe LP3/50
Light probe	3mm (0.12in) diameter, 200mm (7.9in) length
Mirror sleeve	9.5mm (0.37in) diameter, mirror, fits light probe LP3/200
Light probe	8mm (0.3in) diameter, 254mm (10in) length, right angled, rigid
Light probe	14mm (0.55in) diameter, 380mm (14.96in) length, straight, rigid
Light probe	14mm (0.55in) diameter, 380mm (14.96in) length, flex and stay
Light probe	14mm (0.55in) diameter, 380mm (14.96in) length, safety, acrylic
Clip-on mirrors and accessories to fit 14mm diameter light probes	
Extension	380mm (14.96in) length, straight
Extension	380mm (14.96in) length, angled
Mirror	64mm (2.5in) diameter, adjustable ball & socket joint
Mirror	380mm (1.5in) diameter, adjustable ball & socket joint
Recovery magnet	

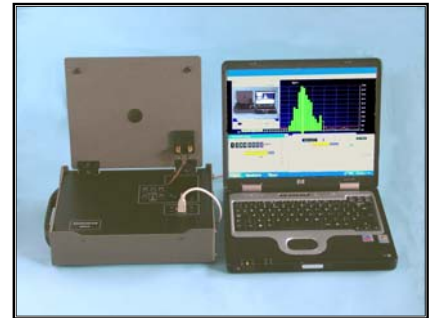
## Video & Audio RF Detection System

Model 7517-01

### SPECTRUM

#### The RF Intermediate Field Component

This is a portable system for radio frequency surveillance analysis. As an Intermediate Field Counter Measure it can monitor an area of several rooms at a time. It is easily programmable, with results stored for repeated and future appraisal, with a full A4 report printout of text and graphical display in line or bar. A novice user with a modest background in radio scanning can have the unit operational in 30 minutes to produce a fully documented predetermined scan.



#### **This is NOT to be confused with Near Field, one room at a time equipment**

This is rapid deployment spectrum analysis, with additional Spectrum Analyzer functions. It can readily identify clandestine transmissions including Spread Spectrum devices, and display video transmission, "picture in picture" display.

### SYSTEM COMPONENTS

- Fully self-contained unit, battery/mains operation
- Windows Software professionally designed for Electronic Counter Measures

### OPERATING FEATURES

The Video Capture system allows the operator to establish the type of video transmission. The actual video image is displayed, picture in picture, on the Laptop screen, and can be stored, saved and replayed.

Mains and Line monitoring for cable/telephone line.

### SOFTWARE FACILITIES INCLUDE:

- Automatically saves each scan; once every scan, or once every hour, for an unattended operation
- Routinely compares files for additions and omissions
- Possible Threat mode for continuous unattended operation, with alarm
- Manual tune mode
- Spectrum analyzer mode

### SPECIFICATIONS

- Frequency Range 10 KHz to 3.0GHz
- Internal rechargeable battery
- High Speed Scanning
- Video interpretation and display
- Mains and line/cable monitoring
- A4 print out
- "Possible Threat" warning features
- Auto save for unattended RF spectrum time profiling



## Advanced Video & Audio RF Detection System Model 7517-02

### SPECTRUM



**The Advanced RF Far Field Component**

This is a portable system for radio frequency surveillance analysis. As a Far Field Counter Measure it can monitor a large area of many rooms or can target one at a time. It is easily programmable, with results stored for repeated and future appraisal, with a full A4 report printout of text and graphical display in line or bar. A novice user with a modest background in radio scanning can have the unit operational in 30 minutes to produce a fully documented predetermined scan.

**This is NOT to be confused with Near Field, one room at a time equipment.**

This is a professional, highly disciplined spectrum analysis, with additional Spectrum Analyzer functions. It can readily identify clandestine transmissions including Spread Spectrum devices, and display video transmissions.

### SYSTEM COMPONENTS

- The Model 7517-02 Super Wide Band Active Antenna
- The Model 7517-02 receiver unit, now with extended frequency range to 6 GHz, and includes antenna switching and video analysis
- ECM Windows software professionally designed for Electronic Counter Measures
- HF super compact antenna
- VLF Mains/telephone line/cable interface
- Rugged transport case

### OPERATING FEATURES

The Video Capture system allows the operator to establish the type of video transmission, AM, FM or inverted FM with switchable de-emphasis. The actual video image is displayed on the laptop, "picture in picture", and can be stored and replayed.

Mains monitoring, software controlled, allowing L - N, L - E, N - E and auxiliary earth monitoring.

Line monitoring for cable/telephone line.

## **Advanced Video & Audio RF Detection System Model 7517-02**

### **SOFTWARE FACILITIES INCLUDE:**

- Full remote control of antenna switching, video interpretation and display
- Task scheduler for automatic sequence and save of scans. This is ideal for an unattended monitoring exercise
- In built data base for display of frequency band allocation
- Routinely compares files for additions and omissions
- Possible Threat Mode for continuous unattended operation, with alarm
- Manual tune Mode
- Spectrum Analyzer Mode

### **SPECIFICATIONS**

- Frequency Range 10 KHz to 6 GHz
- High Speed Scanning
- Video interpretation and "picture in picture" display
- Advanced mains and line/cable monitoring
- A4 print out
- "Possible Threat" warning features
- Option for remote control
- Vehicle installation option with covert antennas

### **FURTHER SYSTEM DETAILS**

There are three primary components: The Receiver, the Antenna, and the Software. The system is housed in a single, very rugged, transport case.

#### **THE RECEIVER**

This is an upgrade from the previous system, and can be seen, bottom left, of the picture overleaf. It has an extended frequency range to 6 GHz. In addition, video is displayed on the Laptop screen, and can be saved and replayed at a later date. There is the option of a second video monitor if required.

#### **THE ANTENNA**

This is the Model 7517-02, an active version of our long standing Model 7517-01, and has an extremely wide frequency response, equating to a dipole from 25 MHz to 9 GHz.

It has a beam width of 120 degrees, front and back, circularly polarized.

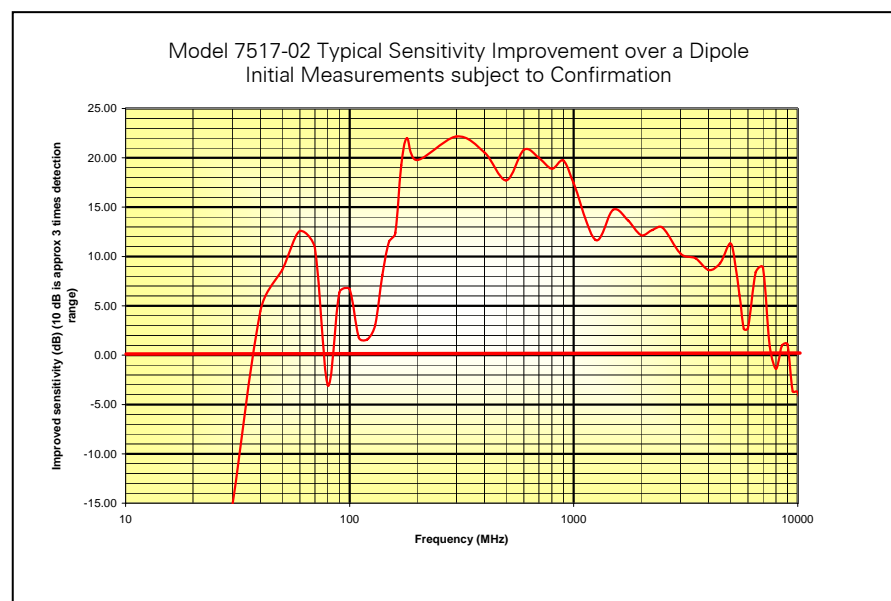
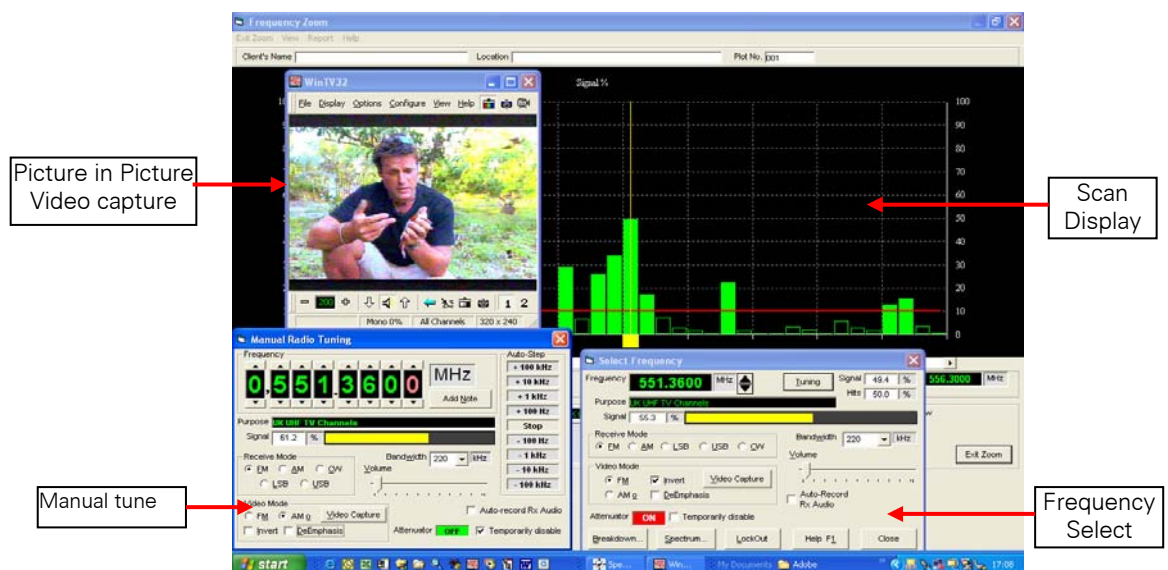
# Advanced Video & Audio RF Detection System Model 7517-02

## THE SOFTWARE

The software is subject to ongoing development and now includes a Database to identify and display the type of transmission intercepted. Personalized notes can be added to the data.

A Task Scheduler is provided to help group personally configured scans to be automatically run and saved.

Audio can be saved to the Laptop in the form of a "wav" file.



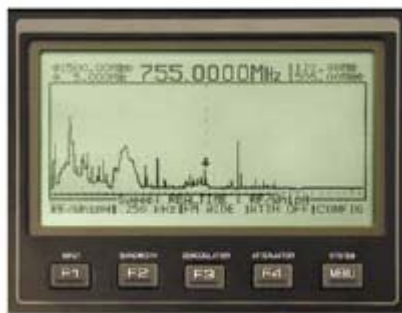


## Omni Spectral Correlator

## Model 7518 OSC

### HIGH-SENSITIVITY SPECTRUM ANALYZER

1. Phased Locked Super Heterodyne Spectrum Analyzer
2. Frequency Range: 10kHz To 3ghz (10kHz To 21ghz With Optional Microwave Down Converter)
3. Automatically Selected Antenna Inputs
4. Sweeping If Bandwidths: 250kHz, 15kHz, And 6kHz
5. Frequency Spans Can Be Programmed With Single Button Control For Rapid Recall And Automatic Searching



The OSCOR provides user-friendly controls and a high-quality digital graphic display.

The OSCOR is one of the few Spectrum Analyzers designed specifically for countersurveillance.

### BUILT-IN SUITE OF DEMODULATORS

#### AUDIO DEMODULATORS

1. FM wideband
2. FM narrowband
3. AM wideband
4. AM narrowband
5. Sub-carrier
6. Single Sideband
- 7.

#### VIDEO FORMATS

1. NTSC, PAL, SECAM
2. AM or FM demodulation
3. + or - synchronization pulse
- 4.

#### IF BANDWIDTHS

1. Audio: 250kHz, 15kHz, and 6kHz
2. Video: 10MHz

### PATENTED THREAT LOCATING SYSTEM

The Patented Threat Locating System uses sonic ranging and triangulation to locate the transmitter microphone.

*This patented system can only be used if an audio signal can be demodulated with the OSCOR.*



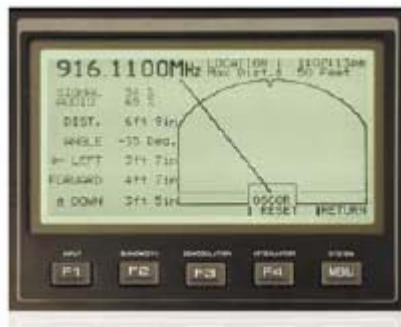
Built-in suite of demodulators and audio oscilloscope view of signals.



Monitor displays video signals for protection against covert video transmitters.

## Omni Spectral Correlator

## Model 7518 OSC



To locate a digitally demodulated transmitter, the OSCOR RF locator probe is utilized.

### BUILT-IN ANTENNA ARRAY

1. ACTIVE WHIP ANTENNA: 0.5-1505MHz frequency coverage.
2. DISCONE ANTENNA: 1500-3000MHz frequency coverage.
3. LOOP ANTENNA: 10-500kHz frequency coverage.
4. INFRARED DETECTOR: 360°; wavelengths of 850-1070nm and modulation from 10kHz-5MHz.
5. STATUS INDICATORS: Display the selected antenna.
6. AC VLF: (not shown in picture) The AC power cord serves as a probe for testing for carrier current type transmitters.
7. BUILT-IN 20dB PRE-AMP: Improves receiver sensitivity.



Patented fold-out antenna panel automatically selects the proper antenna. Pre-amp provides maximum sensitivity for the proper input. No unreliable cable connections or mismatched antenna inputs.

### AUTOMATIC SEARCHING, SIGNAL DETECTION, SPECTRUM TRACE ACQUISITION, AND STORAGE

1. "LOAD FRIENDLY" mode stores outside ambient signals and traces prior to performing a sweep.
2. TARGET SWEEP AREA SIGNALS are easily differentiated from ambient environment "Friendly Signals" and "Friendly Trace."
3. ALL SIGNALS are dated, classified, and stored for later retrieval and automatic tuning.
4. SIGNAL AND TRACE DATABASES can be stored for later comparison and analysis to determine if any new signals have been introduced into the environment.



## Omni Spectral Correlator

## Model 7518 OSC



The OSCOR provides an automatic solution to rapidly logging and classifying the signals of your environment.

Quick Reference Guide provides a single chart that completely defines the programming process.

### TRACE ANALYSIS FOR RAPID DETECTION OF SOPHISTICATED TRANSMITTERS

1. OPTIMIZED SWEEP TIME FOR FAST ANALYSIS: less than 5 seconds to complete one 1.5GHz pass.
2. FRIENDLY SPECTRUM TRACE provides reference trace for comparisons against sweep location trace.
3. PEAK TRACE MINUS FRIENDLY TRACE quickly shows evidence of analog and digital transmitters including frequency hopping and burst/packet transmitters.
4. TRACES CAN BE COMPARED for RF mapping of transmission sources within a building.
5. DETAILED TRACE DATA IS STORED using 120,000 data points across the Whip High, Discone, and MDC antennas.

Enhanced Trace Analysis provides ability to compare target sweep area traces to friendly traces, to quickly identify evidence of transmitters in the target sweep area (including frequency hopping and burst/packet transmitters). Trace and signal data can be further analyzed or stored on a computer via USB interface, for future comparisons or RF mapping.



### AUTOMATIC THREAT CLASSIFICATION

1. AUTOMATICALLY ANALYZES SIGNALS using a patented sound pattern correlator.
2. CORRELATOR PROCESS is integrated over time to ensure accurate correlation.
3. SIGNAL THREAT LEVEL ESTABLISHED ON A SCALE FROM 1 TO 5 is based on the integrated correlation value.
4. DIGITAL SIGNALS or signals that cannot be demodulated or correlated are flagged based on RSSI increase from Friendly reference.

## Omni Spectral Correlator

## Model 7518 OSC



For signals that are readily demodulated, the OSCOR easily classifies threatening signals. Signals that are not readily demodulated are flagged for manual inspection.

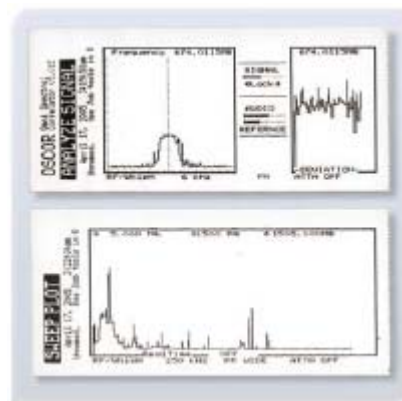
The patented OSCOR correlator provides signal classification by correlating the demodulated audio of a received signal to the ambient environment.

### BUILT-IN PRINTER FOR RAPID HARDCOPIES

Printouts can be generated of:

1. Frequency Spectrum
2. Oscilloscope View
3. Correlation Results
4. Signal Database Listings
5. Frequency Span Listings
6. Threat Location Information
7. System Configuration

The OSCOR's built-in thermal printer provides a user-friendly "What You See is What You Get" method of generating printouts of important sweep data.



The built in printer allows you to make quick printouts of suspicious signals, or complete spectrum traces.

### PC INTERFACE AND REMOTE CONTROL OF THE OSCOR

The OSCOR PC interface software provides enhanced analysis capabilities as well as the ability to create permanent *signal* databases and *trace* profiles of sweep environments for RF mapping and future comparisons. The software also provides professional report and graph capabilities.

## Omni Spectral Correlator

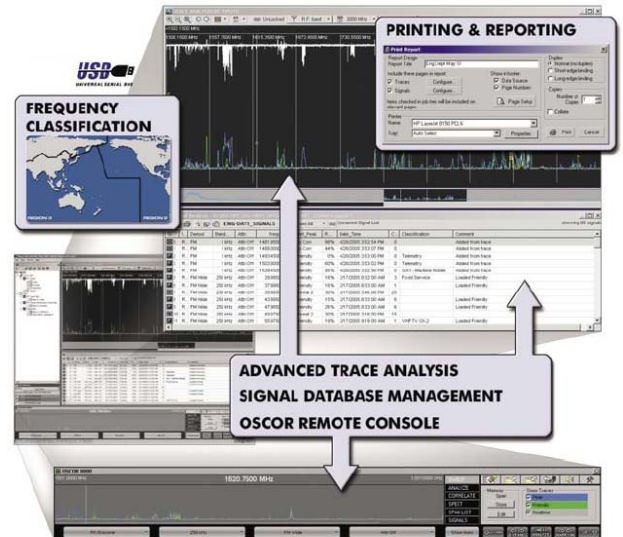
## Model 7518 OSC

### Software ADVANTAGES:

1. STORE, UPLOAD, AND DOWNLOAD signal and trace info.
2. PROGRAM THE OSCOR for automatic operation.
3. IMPROVED CONFIGURABLE USER INTERFACE.
4. SIGNAL CLASSIFICATION using international frequency allocations.
5. CUSTOMIZABLE REPORTS and frequency spectrum graphs.
6. COMPARE AND ANALYZE historical signal and trace data to easily identify new signals detected in the sweep environment.
7. HIGH RESOLUTION FULL-COLOR GRAPHICAL DISPLAY.

### Software BENEFITS:

1. REMOTE CONTROL OF OSCOR from PC computer.
2. RAPID THREAT INDICATION using detailed comparison of stored RF spectrum traces.
3. QUICKLY IDENTIFY SOPHISTICATED TRANSMITTERS (frequency hopping & burst/packet) using peak difference traces analysis.



## OSCOR ADVANTAGES

- Digital Spectrum Analyzer: Designed Specifically For Counter surveillance
- Automatically Switched Antenna Array: With Built-In Pre-Amps
- Automatic Programmability: Continuously Scans, Stores Signals And Traces, And Detects Threat Signals
- Enhanced Trace Analysis: Detects Sophisticated Devices Such As Frequency Hopping And Burst/Package Transmitters
- Signal Database: Provides Storage And Recall Of Detected Signals And Spectrum Traces
- Opc Software: Remote Control Capability And Ability To Store Signal And Trace Profiles For Future Comparison And Rf Mapping
- Audio Analysis Mode: Provides Suite Of Demodulators
- Video Demodulator And Monitor: Provides Viewing Of Covert Video Transmitters
- Acoustic Correlator: Classifies Threatening Signals
- Built-In Printer: Provides Hardcopy Of Signal Analysis Information
- Multiple Threat Locating Systems: Patented Sonar Threat Locating System And Rf Locator Probe
- Complete Package Of Sweep Equipment: Folds Into A Durable Attache-Style Case

## Omni Spectral Correlator

## Model 7518 OSC



The OSCOR is the only available security product that provides all of the above features in a single portable package.

### TECHNICAL SPECS

#### RF SYSTEM

Receiver:	Quad Conversion Super Heterodyne phase locked Spectrum Analyzer
Frequency Coverage:	10kHz - 3GHz
Tuning Resolution:	100Hz
Sensitivity:	0.8 $\mu$ V typical with 15kHz bandwidth (+15dBm Max)
Demodulators:	AM, FM Wide, FM Narrow, FM SC, SSB/CW
IF Bandwidths:	250kHz, 15kHz, 6kHz
Attenuators:	0, -20dB at Active Whip, Discone, and VLF-MF input
Dynamic Range:	90dB
Subcarrier Tuning Range:	15-250kHz
Antenna Types:	
Balanced Loop:	10-500kHz
Active Whip:	500kHz-1500MHz
Discone:	1500-3000MHz
Infrared Detector:	10kHz-5MHz, 850-1070nm
AC Carrier Current:	10kHz-5MHz (balanced across power line)

## Omni Spectral Correlator

## Model 7518 OSC

### AUDIO SYSTEM

Frequency Response:	50Hz-15kHz
Voiceband Filter:	300-3000Hz; 18dB/octave roll off
AGC Dynamic Range:	60dB
Output Power:	3W at 4 $\Omega$
Headphone Output:	0-2V rms
Remote Contact:	Normally open (200mA/32V max)
Balanced Auxiliary Input:	0.5V rms nominal @ 600 $\Omega$
Reference Audio Input:	1mV-1V rms @ 3.9k $\Omega$
Sonic Correlator:	50Hz-15kHz (frequency independent)
Audio Alarm:	3-level programmable 2-tone ringer
Squelch:	Automatic digital or manual control over full display range
Headphones:	Low acoustic leakage, 16 $\Omega$ output limited to 105dBA

### VIDEO SYSTEM

IF Bandwidth:	10MHz
Independent Control of Formats	
Protocols:	NTSC, PAL, SECAM
Demodulators:	AM or FM
Synchronization Pulse:	+ or -

### SYSTEM INTERFACE

Backlit Display:	128 x 256 Segment Graphics Supertwist LCD
Built-in Printer:	192 dpi graphics on 2-inch-wide thermal paper
Rotary Tuning Dial:	128 Pulse/Rev with variable count ratio
USB Interface to PC	
Removable Program Key for firmware updates	

### POWER SYSTEM

AC Input:	105-130VAC/210-260VAC, 50-60Hz, 24W
External DC Input:	12-18VDC, 1A max
Internal Battery:	12V, 2.9Ah 3-hour operation per charge typical

### MECHANICAL

Size (HxWxD):	6.25 in x 18.5 in x 14.5 in (15.9 cm x 47 cm x 36.8 cm)
Weight:	29 lbs (13.2 kg)



## Omni Spectral Correlator

## 7518 Option

The Microwave Down-converter products provide increased frequency coverage for detecting illegal surveillance devices with the OSCOR.

- MDC-900 Frequency Range: 3–9GHz (Band 1 Only)
- MDC-2100 Frequency Range: 3–21GHz (Band 1, 2, & 3)

### TECHNICAL ADVANCEMENTS

- Direct frequency control and band selection with OSCOR
- Integrated High Gain Log Periodic Antennas
- Tripod provides stability for MDC antennas

### TECHNICAL SPECIFICATIONS

#### MODES & FREQUENCY RANGES:

Frequency Range: 3–21GHz

Conversion output Frequency: 5–3005MHz

#### MODES OF OPERATION:

Band 1: 3–9GHz

Band 2: 9–15GHz

Band 3: 15–21GHz

All Bands: 3–21GHz

#### ANTENNA GAIN:

Band 1: 6.1dB

Band 2: 5.3dB

Band 3: 8.4dB

#### MDS (MINIMUM DETECTABLE SIGNAL)

(Includes sensitivity, antenna gain, and filtering losses)

Band 1: -122.1dBm

Band 2: -122.3dBm

Band 3: -124.4dBm

#### MECHANICAL:

Input Power: 200 milliamps at 12V

Weight: 1.1 lb (.5 kg)

Dim: 11.4 in x 3.1 in x 1.4 in  
(29 cm x 8 cm x 3.5 cm)

#### TRIPOD:

Weight: .77 lb (.35 kg)

Dim: 8.75 in x 2.5 in x 1.5 in  
(22.2 cm x 6.4 cm x 3.8 cm)

Usage Height: 5.5 in (14 cm)



The MDC shown in operation with the OSCOR.



## High Power GSM Jamming System

## Model 3521

### MODEL 3521 - PORTABLE HIGH-POWER-JAMMER – 25 WATTS

The Model 3521 is an RF Jammer designed to paralyze the 2 way full duplex RF links between mobile phones and the local cellular cells.

#### GSM 900/1800 MHZ

##### FREQUENCY RANGE:

900 - 970 MHz: Channel 1

1820-1920 MHz: Channel 2

Optional Version: CDMA

##### INPUT-POWER:

RF Output Power: 25 Watts

Omni directional Antenna

Optional Version: 120 Watts

##### MODULATION:

Duplex Sweep

(Special Digital-Modulation)

##### POWER SUPPLY:

90-240 VAC

50-80 Hz/3 A

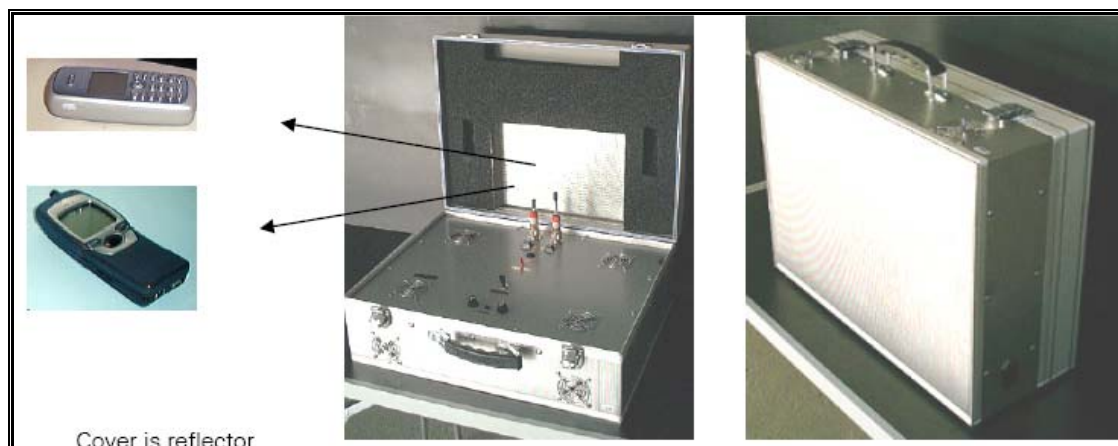
Extern DC: 24 v - (use from car battery)

##### MAXIMUM CONTROL PANEL (JAMMER DISTANCE):

Can reach long distance of more than a KM depending on the type of antennas and topography of the areas

**DIMENSIONS:** 49 x 36 x 18 cm

**WEIGHT:** 30 Kg



## Room Jammer

## Model 3522

### MODEL 3522 TECHNICAL MANUAL

The Model 3522 Jammer is based on our long standing technological leadership and its proven jamming technology. We have widely used product base attests to our determination to provide high end, quality products to customers around the world.

### SPECIFICATIONS

#### FREQUENCY RANGE

GSM double Band

890-1920 MHz

#### OUTPUT-POWER

890-970 MHz: 1.5W

1820-1920 MHz: 1.5W

#### MODULATION

Special-Digital Sweep

#### INPUT DC:

24-26V automatic/1.3A

(DC-Box 95-240VCA)

#### MAXIMUM CONTROL PANEL (JAMMER DISTANCE)

900Mhz: 14-20m

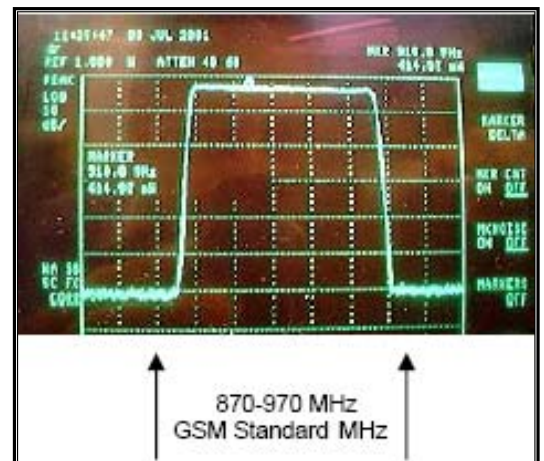
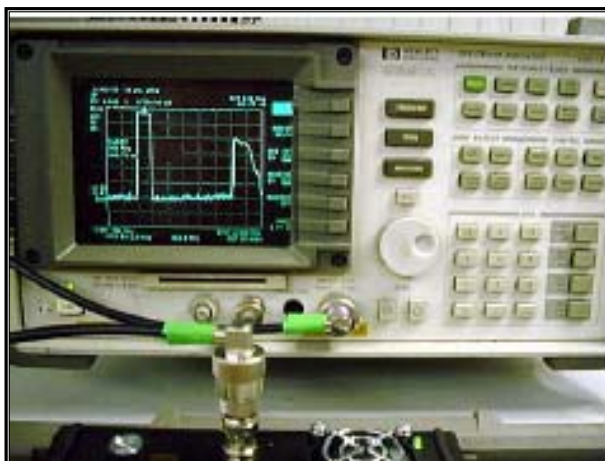
1800MHz 12-20m

(max. 400 sq m in rooms)

#### 2 ANTENNAS/SMA CONNECTOR

**DIMENSIONS:** 110 x 170 x 64 mm

**WEIGHT:** 550 g



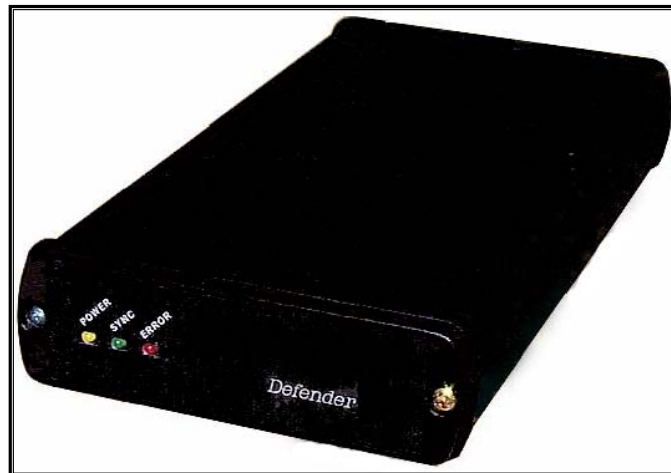


## Computer Screening Jammer

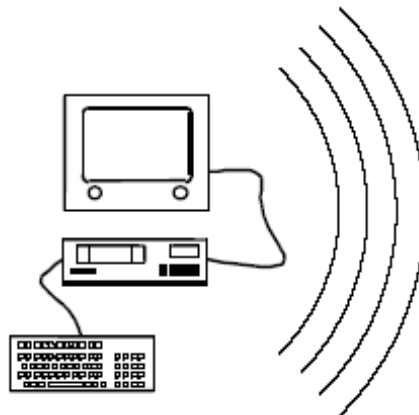
Model 3525

### COMPUTER SECURITY EQUIPMENT - DATA DEFENDER

#### GENERAL DESCRIPTION



The compromising electro-magnetic radiation, which is emitted when working with computers, makes it possible for unauthorized reproduction of the monitor picture and the siphoning off of



data.

There are various possibilities available to protect against from an unauthorized attack on the compromising electro-magnetic emissions:

#### 1. **Tempest Computer**

In this case a modified computer emits no compromising radiation. Because so few are manufactured, these devices are very expensive. Also, their compatibility with other systems is often restricted.

#### 2. **Shielded Rooms**

This form of protection has the advantage that standard PC systems can be used. The disadvantage of this form of protection is its high cost. In addition flexible use of the computer is not possible.

## Computer Screening Jammer

## Model 3525

### 3. Protection Device

A protection device works by superimposing jamming signals and is suitable for any PC that is connected to a monitor via an external line. The computer can be used "bug proofed" in any position.

### PROTECTION DEVICE DEFENDER

In contrast to other versions of protection devices that generate broad band noise that is superimposed on the video signal, the Defender detects only the computer system's pixel frequency information, and sends out a narrow band noise on this frequency. The pixel frequency depends on the computer system being used and is between 20 and 80 MHz and has the highest amplitude in this range.

A microprocessor controlled spectrum analyzer searches for the pixel frequency. The pixel frequency you are interested in is scanned and the voltages of the single frequencies are assessed and saved. Furthermore, the frequency of the horizontal synchronization line is obtained and the possible pixel frequencies are calculated.

A noise generator is clocked at the output of the protection device at the determined frequency. This type of noise generator is a narrow band and can always be switched automatically to the last found frequency.

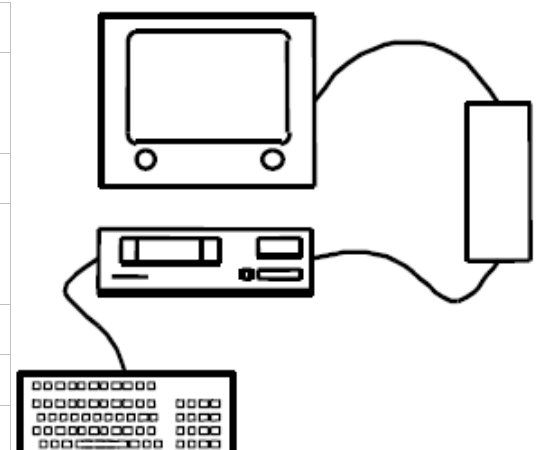
### USE OF THE PROTECTION DEVICE DEFENDER

The Defender is suitable for any computer that is connected to a monitor via an external line.

The connection of the Defender is effected by the installation of the VGA cable from the graphic card to the monitor via the protection device.

### TECHNICAL DATA

Scanning Frequency:	20 - 80 MHz
Connections:	VGA-Input (SubD 15-pin) VGA-Input (SubD 15-pin)
Indicators:	Power LED Sync. LED Error LED
Power Supply:	5 V DC (via mains power pack)
Power Consumption:	Approx. 700 mA
Dimensions :	110 x 35 x 185 mm
Weight:	500 g



## Anti-Laser Microphone Noise Jammer

## Model 3526

### AUDIO JAMMING NOISEBATH SYSTEM

The security of the patented NOISEBATH system is based upon the following six principles:

- Maximizing complexity and coverage by ambient mixing of target's voice with masking sounds
- Reducing the effectiveness of acoustic pick-up devices
- Making computer filtering difficult by the design of the masking source material
- Hindering listening by human transcribers with psycho-acoustic elements which create fatigue
- Reducing the value of any information recovered with meaningless sequences of words in the masking material
- Reducing the credibility of any derived information with deliberately deceptive masking material



Playing NOISEBATH masking source material through the speakers of a properly configured system creates a "bath" of noise around the target, which mixes with the actual voices or equipment sounds. This hinders the exploitation of the target's acoustics.



NOISEBATH is compatible with the STU III and other Secure Telephones. The masking sounds have negligible impact on the remote secure phone user. The masking level can be adjusted by remote control.

There is up to a 25db reduction in sound level within the protection zone from the sound level outside the protection zone.

### ACOUSTIC MASKING MATERIAL

The acoustic masking source material is produced according to a specialized NOISEBATH formula and can be recorded on compact discs or generated in real time. Masking source material is a combination of varying pink noise, synthetic speech, actual speech and psycho-acoustic elements configured to minimize disruption to those being protected and maximize disruption to electronic audio surveillance systems and human listeners.

Masking can also consist of specialized equipment sounds to mask intelligence bearing acoustics such as from computer keyboards.

Masking source material is available in different languages, regional accents, dialects, or even for a particular person or persons. Mixtures of voice types are also available.

Regional Editions are produced from actual voices and synthetic vocal sounds within a language or dialect selected by the customer such as American English Military Operations, Regional American Dialects Political & Legislative Subjects, Regional German Dialects, South American Spanish, Gulf Arabic, and Specialized Vocabularies of Various Intelligence and Law Enforcement Operations.



## Advanced Counter Surveillance Jammer

## Model 3527

### MODEL 3527 TECHNICAL MANUAL

The Model 3527 Jammer is based on our long standing technological leadership and its proven jamming technology. We have widely installed product base attests to our determination to provide high-end, quality products to customers around the world.

The Model 3527 will protect room conversation against wireless bugs by Jamming the frequency modulation of the bugs.

### SPECIFICATIONS

#### FREQUENCY RANGE:

- 5 channels
- HF 20 - 80MHz
- VHF 80 - 200MHz
- UHF 200 - 500MHz
- SHF 500 - 1000MHz
- SHFII 1800- 2000MHz

#### POWER-OUTPUT:

- 45-50 W sum of all channels

#### MODULATION:

- Double-Digital-Sweep

#### POWER-SUPPLY:

- 220-240 V

#### 5 ANTENNAS:

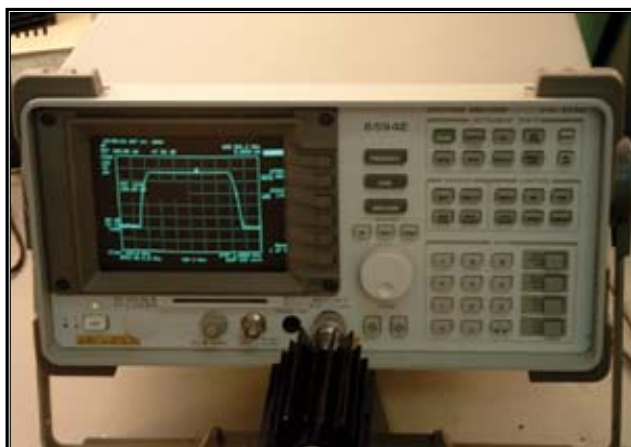
- 50 ohm N-Connector

#### JAMMING DISTANCE:

- 200 m

#### DIMENSIONS: 460 x 520 x 280 mm

#### WEIGHT: Approximately 19 kg



## FSH Portable Spectrum Analyzer

Model 7519

### DESCRIPTION

The FSH Series (2, 3 or 6 GHz) spectrum analyzers are compact, battery-powered tools that provide RF measurement for TSCM based signal analysis/monitoring. In addition, the FSH3 spectrum analyzer includes a color display that reduces errors by enhancing the visibility of critical signal details. The powerful software package with signal comparison evaluation provides excellent functionality and compares previously scanned measurement.

### APPLICATIONS

- TSCM Nearfield Analysis
- Cable installation and maintenance
- Verifies production line equipment
- General field use for communications installation and maintenance
- Field wireless equipment installation and maintenance. Outdoor antenna characteristics measurements.



### FEATURES & BENEFITS

- Portable handheld spectrum analyzer; Small and light enough to be perfect for handheld applications
- Superior RF Characteristics - fast, accurate, precision instrument for its price
- Color display enhances usability and visibility; 100 kHz to 3 GHz frequency range; covers all major communication standard transmission frequencies
- RMS detector for correct digital signal analysis
- Over 4-hour battery life; extremely portable for field use
- Built-in preamplifier; improve sensitivity by 15 dB; improved instrument sensitivity to detect more low level signals
- Selectable output power for the tracking generator; 0 dBm; test devices with higher power ratings without additional external equipment; additional narrower resolution bandwidths down to 100 Hz; improved performance measuring narrow bandwidth signals



## FSH Portable Spectrum Analyzer

## Model 7519

### CHARACTERISITICS

	<b>FSH 3</b>	<b>FSH 6</b>
Frequency Range	100KHz to 3 GHz	100KHz to 6 GHz
Resolution Bandwidth	1KHz(100 Hz) to 1MHz	10Hz to 1 GHz
Video Bandwidth	10 Hz to 1 MHz	10 Hz to 1 MHz
Displayed Avg. Noise Level	Typ. -116 (-125*) dBm (1 kHz) -	135 dBm
T.O.I.	15 dBm typ.	15 dBm typ.
SSB Phase Noise	<-100dBc (Hz) at 100 kHz carrier offset	<-100dBc (Hz) at 100 kHz carrier offset
Detectors	Sample, peak, auto peak, RMS	Sample, peak, auto peak, RMS
Total Measurement Uncertainty	1.5 dB	1.5 dB
Reference Level	-80dBm to +20 dBm	-80dBm to +20 dBm
Dimensions W x H x D (mm)	170x120x270	170x120x270
Weight	2.5 kg	2.5 kg



## Covert RF Bug Detector up to 6 GHz

## Model 7520

### DESCRIPTION

This compact Bug Detector is the latest generation of high sensitive broadband Radiofrequency-Detectors and is the size of a cigarette packet. It detects active miniaturized transmitters within a distance of some meters and is excellent to use as an additional instrument when looking for bugging devices.

The sensitivity of the Bug Detector is adjustable to allow the precise allocation of active transmitters nearby. The signaling can either be acoustic or visual with an LED bargraph. With a discrete vibration alarm this device can also be body-worn. By using the Bug Detector's earphone, signals of common modulations can be demodulated. The rechargeable battery guarantees long operating time.

### FEATURES

#### ADVANTAGES:

- The Bug Detector is highly miniaturized and discrete
- It's more sensitive than most large near-field receivers (so called. „Bug Finders“)
- The frequency range covers all common RF-standards, like GSM, UMTS, DECT, Bluetooth & WLAN
- Detects active sound, video & data transmissions
- The vibration alarm allows hidden body-worn use
- Excellent cost/performance ratio

**Important notice: An RF-Receiver cannot replace a physical search!**

#### INCLUDED:

- Receiver with changeable broadband antenna
- Earphone & mini-charger (AC adapter)
- Shock protected transport case & user manual

**Change without notice!**

### TECHNICAL DATA

Frequency range:	10 MHz to > 6 GHz
Receiver sensitivity:	-46 dBm at 10 MHz -58 dBm at 900 MHz -58 dBm at 2300 MHz -32 dBm at 5000 MHz
Audio-output:	1 W / 8 Ω
Demodulation:	AM, ASK, FSK, (FM)
Power supply:	AC adapter 100 - 240 V Charging at 4,2 V/650 mA Lithium Batt. 3,7 V/2000 mAh
Current consumption:	30/300 mA (without/with vibration)
Battery life:	> 10 hours
Size:	85 x 55 x 18 mm (Receiver)
Antenna:	70 mm broad-band antenna
Weight:	110 g (Receiver)/450 g (Set)







## Miniport Receiver EB200

Portable monitoring from 10 kHz to 3 GHz

- Ergonomic design for on-body operation
- Continuous frequency range 10 kHz to 3 GHz
- Detection of unlicensed transmitters
- Location of close-range to medium-range targets with the aid of Handheld Directional Antenna HE200
- Digital IF section with 12 bandwidths (150 Hz to 150 kHz)
- Fast, accurate level indication across 110 dB dynamic range
- Scanning modes
  - Frequency scanning
  - Memory scanning
- Frequency spectrum (option)
- IF panorama display (option)
- Remote-controllable via RS232 CPPP or LAN (Ethernet 10Base-T)



**ROHDE & SCHWARZ**

## Brief description

Miniport Receiver EB200 with Active Directional Antenna HE200 is a portable unit for radiomonitoring in the wide frequency range from 10 kHz to 3 GHz. Whether used for monitoring

In case of power supply interruption, all the data is stored. Operation can thus be resumed immediately after the power supply is restored.

- Location of close-range to medium-range targets with the aid of Hand-held Directional Antenna HE200
- Detection of undesired emissions including pulsed emissions
- Detection of unlicensed transmitters communicating illegally or interfering with licensed transmission



emissions, detecting interference or locating mini-transmitters irrespective of their position, EB200 offers features unrivalled in its class. The favourably priced and compact receiver with LAN interface may also be used in computer-based stationary systems.

The EB200 is characterized by high input sensitivity and frequency setting accuracy throughout the frequency range from 10 kHz to 3 GHz.

Its small dimensions and low weight as well as a sturdy, pickup-proof die-cast aluminium housing with well-protected integrated operating elements make the EB200 ideal for use in places which cannot be reached with a vehicle. Its low power consumption permits battery operation typically of four hours. The EB200 battery pack is easily accessible and can be exchanged quickly.

EB200 fulfils the following tasks:

- Monitoring of given frequencies, eg storage of 1 to 1000 frequencies, squelch setting, constant monitoring of one frequency or cyclical scanning of several frequencies
- Searching in a frequency range with freely selectable start and stop frequency and step widths of 1 kHz to 9.999 MHz

- Protection against tapping by detecting miniature spy transmitters (bugs)
- Monitoring of one's own radio exercises in a service band
- Monitoring of selected transmissions
- Remote-controlled operation via modem and PC in coverage measurement and monitoring systems

EB200 and HE200: ergonomic design for on-body operation



## Specifications

<b>Frequency range</b> Frequency setting via keypad or rollkey	10 kHz to 3 GHz	AF output, balanced Loudspeaker output Headphones output Output log. signal level	600 Ω, 0 dBm 8 Ω, 500 mW via volume control 0 V to +4.5 V
Frequency accuracy Aging Synthesizer setting time Oscillator phase noise	1 kHz, 100 Hz, 10 Hz, 1 Hz or in selectable increments ≤±1.5×10 <sup>-6</sup> (-10°C to +55°C) ≤±0.5×10 <sup>-6</sup> /year ≤3 ms ≤-100 dBc/Hz at 10 kHz offset	<b>BITE</b>	monitoring of test signals by means of loop test
<b>Antenna input</b>	N socket, 50 Ω, VSWR ≤3; SMA con- nector for rackmounting at rear panel	<b>Data interface</b> Option	RS232 C PPP LAN (Ethernet 10Base-T)
Oscillator reradiation RF attenuation Input selection 100 kHz to 20 MHz 20 MHz to 1.5 GHz 1.5 GHz to 3 GHz	≤-107 dBm 30 dB, man. or autom., switchable highpass/lowpass tracking preselection highpass/lowpass	<b>General data</b> Operating temperature range Rated temperature range Storage temperature range Humidity Shock	-10°C to +55°C 0°C to +50°C -40°C to +70°C max. 95%, cyclic test 25/55°C to DIN IEC 68-2-27 (MIL-STD-810D, MIL-T-28800D), 40 g, shock spectrum 45 Hz to 2 kHz to DIN IEC 68-2-6 (MIL-T-28800D), 5 Hz to 55 Hz, 0.15 mm amplitude to DIN IEC 68-2-36, 10 Hz to 500 Hz, 1.9 g (rms)
<b>Interference rejection, nonlinearities</b> Image frequency rejection IF rejection 2nd order intercept point 3rd order intercept point Internal spurious signals	≥70 dB, typ. 80 dB ≥70 dB, typ. 80 dB typ. 40 dBm typ. 2 dBm ≤-107 dBm	Vibration (sinewave)  Vibration (noise)  Electromagnetic compatibility (EMC)	(MIL-STD-810D, MIL-T-28800D), 40 g, shock spectrum 45 Hz to 2 kHz to DIN IEC 68-2-6 (MIL-T-28800D), 5 Hz to 55 Hz, 0.15 mm amplitude to DIN IEC 68-2-36, 10 Hz to 500 Hz, 1.9 g (rms)
<b>Sensitivity</b> Overall noise figure (including AF section) 20 MHz to 650 MHz 650 MHz to 1500 MHz 1500 MHz to 2700 MHz 2700 MHz to 3000 MHz Signal-to-noise ratio	≤14 dB, typ. 12 dB ≤15.5 dB ≤14 dB, typ. 12 dB ≤15 dB, typ. 13 dB measurement with telephone filter to CCITT	Power supply  Dimensions (W x H x D)  Weight (without battery pack) Battery pack	EN50081/82-1,82-2, MIL-STD-461, CE03; RE02 and RS03 battery pack (typ. 6 h operation) or DC 10 V to 30 V (max. 22 W) 210 mm x 88 mm x 270 mm ½ 19" x 2 HU 4 kg 1.5 kg
AM, bandwidth 6 kHz, f <sub>mod</sub> = 1 kHz, m = 0.5 20 MHz to 2700 MHz, V = 1 μV 2.7 GHz to 3 GHz, V = 1.3 μV FM, bandwidth 15 kHz, f <sub>mod</sub> = 1 kHz, deviation = 5 kHz 20 MHz to 2700 MHz, V = 1 μV 2.7 GHz to 3 GHz, V = 1.3 μV	≥10 dB ≥10 dB ≥25 dB ≥25 dB	<b>Directional antennas HE200/HE200HF</b>	
<b>Demodulation</b> IF bandwidths	AM, FM, USB, LSB, CW 12 (150/300/600 Hz/1.5/2.4/6/ 9/15/30/50/120/150 kHz)	Frequency range Antenna modules  20 MHz to 200 MHz 200 MHz to 500 MHz 500 MHz to 3000 MHz Option 0.01 MHz to 20 MHz Polarization  Loop antenna 0.01 MHz to 20 MHz	0.01 MHz to 3000 MHz 20 MHz to 3000 MHz, with 3 plug-in antennas loaded loop antenna loaded loop antenna log-periodic antenna
IF bandwidths for level and deviation indication	15 (150 Hz to 1 MHz) only with IF Panoramic Unit EB200SU signal-controlled, can be set from -10 dBμV to +100 dBμV	Option 0.01 MHz to 20 MHz Polarization	loop antenna vertical for all antenna modules, hori- zontal polarization by turning the lon- gitudinal antenna axis by 90°
Squelch	AGC, MGC 80 dB 110 dB	Loop antenna 0.01 MHz to 20 MHz	direction finding for horizontally polar- ized signals not possible because of circular vertical pattern of system
Gain control IF control RF + IF control AFC	digital retuning for signals unstable in frequency	Nominal impedance SWR RF output Gain Antenna factor Field-strength sensitivity Linearity of amplifier	50 Ω <2.5 typ. 1 m cable with N connector for typical values see page 7 for typical values see page 7 for typical values see page 7 IP3, typ. 19 dBm (battery voltage 6 V, 25°C)
Deviation indication Signal level indication	graphical with tuning label graphical as level line or numerical from -10 dBμV to +100 dBμV, acoustic indication by level tone	Current drain	55 mA in active mode 0 mA in passive mode
IF panorama display (option SU)	internal module, ranges 25, 50, 100, 200, 500, 1000 kHz	Power supply Dimensions (W x H x D)	in handle, 4 x 1.5 V mignon cell R6 470 mm x 360 mm x 180 mm (in transport case)
<b>Scan characteristics</b> Automatic memory scan	1000 definable memory locations to each of which a complete data set can be allocated	<b>General data</b> Operating temperature range Rated temperature range	-30°C to +60°C active/passive mode -10°C to +50°C active mode -30°C to +60°C passive mode
Frequency scan	START/STOP/STEP definition with receiving data set	Storage temperature range Vibration resistance	-30°C to +60°C random 10 Hz to 300 Hz: 0.01 g <sup>2</sup> /Hz, 300 Hz to 500 Hz: 0.003 g <sup>2</sup> /Hz, every 30 minutes in 3 orthogonal axes; acceleration approx. 1.9 g rms max. 40 g, crossover frequency 45 Hz in 3 orthogonal axes
<b>Inputs/outputs</b> Digital IF output	serial data (clock, data, frame) up to 256 kbps: 2 x 16 bit	Shock resistance	
Bidirectional reference frequency connectors in out I/Q output (digital) IF 10.7 MHz, wideband	10 MHz, BNC 0.1 V to 1 V; R <sub>i</sub> = 500 Ω 0 dBm, R <sub>o</sub> = 50 Ω AF signal, 2 x 16 bit ±5 MHz uncontrolled for external panoramic display	Weights: Supply and display unit with adapters and compass RF modules 20 MHz to 200 MHz 200 MHz to 500 MHz 500 MHz to 3000 MHz 0.01 MHz to 20 MHz	0.5 kg 0.65 kg 0.55 kg 0.3 kg 0.45 kg 0.4 kg

## Digital Scout Frequency Detector

## Model 7522

### DESCRIPTION

The Model 7522 Digital Scout RF frequency detector/field strength meter is a near field measurement instrument that captures digital, as well as analog signals, from 10MHz -2.6GHz. Until now, the only signals that frequency counters could lock onto were analog signals. In addition to locking onto digital and analog signals, the Model 7522 has a calibrated signal strength measurement from -45dBm to -5dBm.

### USAGE

One can use the Model 7522 in all places where unknown near field RF-signals must be captured, localized and examined regarding their frequencies.

The Model 7522 is capable of detecting many different types of digital modulations that have a minimum pulse width of 500mS; signals such as TDMA, GSM, APCO 25, ON/OFF Keying, TETRA and more.

The Model 7522 is not capable of counting signals such as Spread Spectrum, CDMA and PCS.

### FEATURES

- 10MHz - 2.6GHz frequency range
- 5-6 hour battery operation
- 2x16 alphanumeric LCD with EL backlight
- Signal Strength reading displayed in dBm and barograph –
- 45dBm to -5dBm
- +/- 5dBm signal strength accuracy
- Download memory to a PC using the optional Optolinx interface
- Reaction Tune analog signals with ICOM IC R10, R7000, R7100, R8500 and R9000. AOR AR8000 and AR8200. Optoelectronics Optocom, OS456/Lite, OS535 and R11.BC245XLT and BC780 (SmartLink cable required)
- 1000 memories with 65,000 hits per memory
- Captures both Digital (Minimum 500mS RF pulse required) and analog signals
- Beeper and Vibrator alert
- Super Sensitive, down to 700uV in some bands

### TECHNICAL DATA

Frequency Range:	10MHz to 2.6GHz
Resolution:	1KHz and 100Hz
Frequency Accuracy:	1ppm
Signal Strength:	-45dBm to -5dBm
Signal Accuracy:	+/- 5dBm
Display:	2x16 alphanumeric LCD with EL backlight
Power:	9 VDC, 150mA using model AC90 wall Plug adapter.
Size (H x W x D):	5.25'' x 3'' x 1.5''
Weight:	12 oz



## Advanced Cable Tracing System

## Model 7523

With cable measurement taking up to 30 percent of a sweep effort, tools that provide important information effectively and quickly are needed. The Advanced Cable Tracing System is designed to aid in locating all cables coming from the target location. Capable of tracing cables buried as deep as 2 meters, this system excels in ensuring all potentially dangerous cables are found.





## X-Ray for Screening VIP Presents

## Model 7525

A slim-line, large capacity color mail and parcel scanner

You can't always predict what will arrive in the mail but you can protect yourself against nasty surprises. X-ray scanners see inside your mail and provide on the spot confirmation of unusual or unexpected packages.

- Large inspection chamber accepts postal trays, parcels and briefcases.
- Slim-line design
- Quick and easy to use
- Uses a simple mouse control
- Latest color technology
- Freestanding with front loading door
- Scans VIP presents & suspected bugs



### REASSURANCE FOR YOUR STAFF

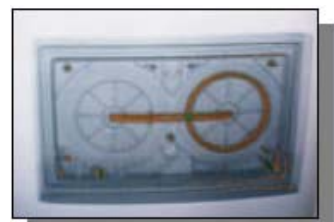
The Model 7525 cabinet X-ray scanner provides on the spot verification of unusual packages giving reassurance to all staff handling mail.

### COMPACT AND EASY TO USE

The Model 7525 is designed for easy use by non-technical staff. Combines a large inspection chamber with a slim-line cabinet allowing you to examine volume mail, large parcels and briefcases in areas where space is at a premium.

### RAPID SCREENING

Items are placed in the front loading inspection chamber and a single button action produces a clear image of the contents in seconds.



### IMAGE ENHANCEMENT COLORSCAN MODEL

- Automatic Image Enhancement
- Negative or inverse image option
- 8 x zoom
- 2 color options for highlighting medium and high density
- objects

# X-Ray for Screening VIP Presents

# Model 7525

## BASIC B/W MODEL (BLACK AND WHITE)

- Simple black and white image

## HEALTH AND SAFETY

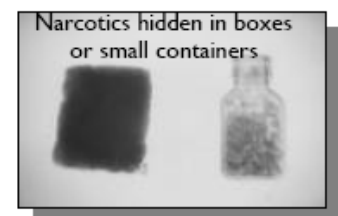
The X-ray scanners use very low level X-rays and conform to all published international Electrical Safety and Radiation Standards and are issued with a certified Radiation Safety and Test report.

## X-RAY IMAGE RECOGNITION

Basic Operator Training and X-ray image recognition charts can be provided.

## SERVICING AND SUPPORT

Full maintenance and back-up support is available. Due to the nature of its design the Model 7525 has no conveyor or electrical moving parts that might require expensive servicing.



## TECHNICAL SPECIFICATIONS

Physical Specifications	
Height:	162.5 cm (65")
Width:	42.8 cm (17")
Depth:	61 cm (24")
Net Weight:	170kg (330lbs)
Image Area:	
Depth:	41 cm (16")
Width:	34 cm (13.6")

Inspection Chamber	
Height:	53.5 cm (21")
Width:	42 cm (17")
Depth:	56 cm (22")
Door Opening:	
Height:	53.5 cm (21")
Width:	34 cm (13.6")
Power requirements	110V, 230V, 50/60 Hz
Shipment specifications	112 (w) x 77 (d) x 150 (h) cm
	Weight: 250kgs





## TopSec GSM

The mobile phone for your confidential calls

- ◆ High security level
- ◆ Top-quality speech encoding for end-to-end voice communication
- ◆ Invariably reliable speech quality
- ◆ Simple handling
- ◆ Recommended by the German Information Security Agency

## TopSec GSM: mobile and confidential

The fast transfer of information and instant decisions, particularly at higher levels of management are more important than ever. Therefore, it must also be possible to exchange confidential information over mobile phones. In the GSM transmission mode, data is only encrypted between mobile phone and base station. Beyond that, the call is routed via radio relay or fixed networks without any protection. In some countries even the minimum security requirements for mobile communication are not met.

The TopSec GSM has been developed so that confidential information can be exchanged reliably and without any risk of eavesdropping.

## The "top secret" mobile phone meets highest demands

The basis of the TopSec GSM is the renowned Siemens dualband mobile phone S 35i. The core, however, is the

crypto module. Due to its size of only 32 mm x 34 mm it has been completely integrated into the S 35i. The TopSec GSM cannot be distinguished from a normal Siemens S 35i mobile phone.

In addition to the encryption function, the TopSec GSM offers all advantages of a latest-generation mobile phone:

- ◆ Excellent speech quality
- ◆ Simple operation
- ◆ Voice dialling
- ◆ Compact size
- ◆ Low weight
- ◆ Internet access via WAP browser
- ◆ Soft modem and
- ◆ IR interface for mobile data transfer

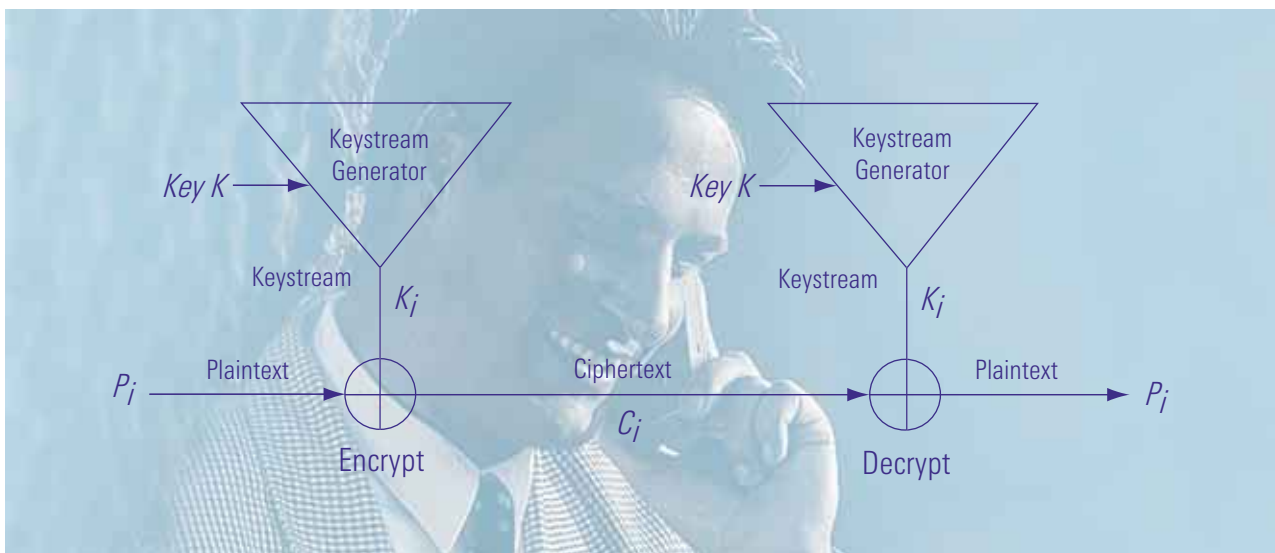
Encrypted speech is transmitted on the transparent GSM data channel. Through the use of the GSM half-rate vocoder, excellent speech quality is ensured even in the encrypted mode. To attain top security, two algorithms are combined; an asymmetrical algorithm with a 1024-bit key for key agreement and a symmetrical algorithm with a 128-bit key for voice encryption.

As is the case with the TopSec ISDN encryption devices for voice and data communication, the TopSec GSM is recommended by the German Information Security Agency, confirming the high security standard.

## Security in mobile radio networks and on the ISDN landline network

The TopSec GSM is suitable for encrypted end-to-end voice communication in the GSM frequency ranges of 900 MHz and 1800 MHz. A confidential discussion can be carried on between two TopSec GSM mobile phones without any risk.

Encrypted calls from the TopSec GSM can also be made to the landline network: the only prerequisite is that the called ISDN station must be protected by a TopSec 703+ of the TopSec product family.



## Absolute confidentiality at a single keystroke

Dial the number of the desired subscriber and briefly press the crypto softkey below the display to switch to the crypto mode.

"Crypto" is indicated in the display to confirm the encryption mode as well as a 4-digit control code (see figure). In the case of closed subscriber groups, automatic authentication is performed by a public key procedure.

Thus you can be sure that your communication is encrypted and that nobody can eavesdrop your call.



In the crypto mode, your TopSec GSM phone and the called TopSec station automatically agree on a new 128-bit key for each call. The 128-bit key is randomly determined out of  $10^{38}$  possibilities and erased after the call is terminated.

This method is one of the essential security features offered by TopSec GSM.

Crypto mode indicated in the display



Size of crypto module

## Specifications

Frequency range GSM class 4 (2 W) GSM class 1 (1 W)	880 MHz to 960 MHz 1710 MHz to 1880 MHz
Voice transmission (GSM half-rate vocoder)	normal operation, encrypted transmission
Operating voltage	3.6 V
Current drain	max. 400 mA
Operating temperature	0°C to 45°C
Standby time	up to 220 hours
Talk time	up to 6 hours

Size	118 mm × 46 mm × 21 mm
Weight	105 g

## Ordering information

TopSec GSM	3531.6527
------------	-----------

## Ultra Scan50b X-ray Unit

## Model 7530

Ultra Scan50b is the subsequent upgrade of Ultra Scan50a. With over 3000 installations worldwide Ultra Scan50b is an extremely successful compact X-ray inspection system.

A modular designed tabletop system; Ultra Scan50b is flexible, extendable and therefore can be used for different applications.

Due to state-of-the-art X-ray-, sensor- and computer-technologies this system offers functionalities, which in the past were reserved solely for aviation security purposes.

Ultra Scan50b permits configurations with operator training, TIP- and image management functionalities.

Being one of the most space saving X-ray inspection systems available, Ultra Scan50b is ideal for use in mailrooms, entrance halls, correctional and judicial facilities, schools and many other security sensitive areas, where contact-free inspection of pouches, bags, letters or packages is required.

Ultra Scan50b –increased security thanks to advanced technology.



### FEATURE HIGHLIGHTS

- Compact desktop solution for mobile and stationary applications
- New X-ray generator plus new sensor technology for high performance

### OPTIONAL

- HI-TIP: Threat Image Projection
- Xtrain: Operator training system
- IMS: Electronic image storage and archive
- Xport: Image export in TIF- or JPEG format incl. automatic transmission to PC via Ethernet

### TECHNICAL DATA HI-SCAN 5030SI

General Specifications	
Tunnel dimensions	532 (B) x 330 (H) [mm] , 21" (B) x 13" (H)
Max. object size	530 (B) x 320 (H) [mm] , 20.9" (B) x 12.6" (H)
Conveyor height	approx. 190 mm (7.4")
Conveyor speed at mains frequency 50 Hz/60 Hz	approx. 0.18 / 0.22 [m/s]
Max. conveyor load (evenly distributed)	60 kg (132 lbs)
Resolution (wire detectability)	Standard: 38 AWG (0.13 mm) typical: 39 AWG (0.10 mm)
Penetration (steel)	Standard: 10 mm, typical: 12 mm
X-ray dose (typical)	HI-MAT: 1.6 µSv (0.16 mrem)
Film safety	Guaranteed even for high speed films up to ISO 1600 (33 DIN)
Duty cycle	100%, no warm-up procedure required

## Ultra Scan50b X-ray Unit

## Model 7530

<b>X-ray Generator</b>	
Anode voltage	100 kV cp
cooling	hermetically sealed oil bath
Beam direction	diagonal
<b>Image Generating System</b>	
X-ray converter	L-shaped detector line, high resolution
Grey levels stored	4096
Image presentation	S/W, color
Digital video memory	1280 x 1024 / 24 bit
Image evaluation functions	B/W, HIGH, LOW, NEG; incl. Option HI-MAT, additionally VARI-MAT, O2, OS electronic zoom: stepless enlargement up to 16-times
Monitor	17" color monitor, low radiation according to MPR II und TCO 99 standards other monitors on request
<b>Additional Features</b>	
Features	Luggage counter, user-id number, display of operating mode, REVIEW-feature to recall previously visible image areas, zoom overview, free programmable keys
Options	HI-TIP, HI-SPOT, SEN, Xport, IMS (Image Management System)
<b>Installation Data</b>	
X-ray leakage	meets all applicable laws and regulations with respect to X-ray emitting devices
CE-labeling	in compliance with 98/37/EWG, 72/23/EWG, 89/336/EWG
Sound pressure level	< 56 dB(A)
Operating-/storage temperature	0° - 40°C/-20°C - +60°C
Humidity	10% - 90% (non-condensing)
Power supply	standard: 230 VAC or 110 VAC +10% / -15% 50 Hz / 60 Hz ± 3 Hz
Power consumption	approx. 0,3 kVA
Protection class system/keyboard	IP 20 / IP 43
Dimensions	1200 (L)2 x 705 (B) x 726 (H) [mm] 47.3" (L)2 x 27.7" (B) x 28,6" (H)
Weight	approx. 160 kg, approx. 352 lbs
Mechanical construction	Steel construction with aluminum panels standard color(s): RAL 9006 (white aluminum)/stainless steel

## 3D image Enhancer

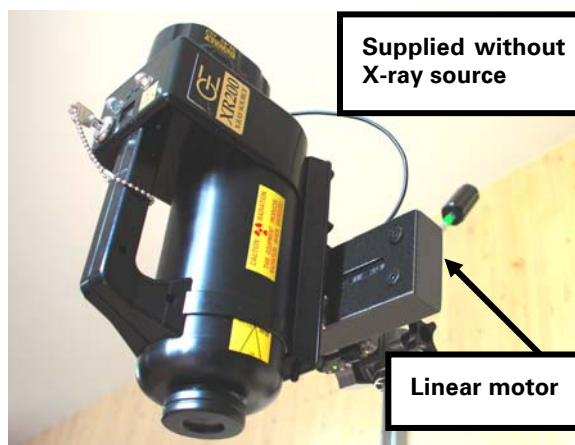
## Model 7539

### DESCRIPTION

The 3D Image Enhancer is a brand-new system for upgrading mobile X-ray units, from 2D into 3D visualizing of X-ray images. The stereoscopic view provides more information about the checked items to the user. Typical applications are EOD, NDT, TSCM and all others, where more security is necessary.

The 3D Image Enhancer is set up very quickly and is easy to handle with an intuitive user interface, which needs no additional training. The software steers a linear motor to move the X-ray source automatically into the right shot positions to provide the required images.

All common types of X-ray image media can be used, even conventional films and storage foils, if they need to be scanned later on. The digital 2D images, coming from a scanner or an image converter, can be individually enhanced and processed into a 3D visualization by the 3D Image Enhancer. In the 3D viewing mode zoom, detail, pan, tilt and rotation of the stereoscopic image is changeable by mouse control.



**Illustration**



**3D Visualization**

### FEATURES

#### ADVANTAGES:

- 3D viewing without red/green or polarized glasses
- Lightweight & easy to use system for intuitive operation
- Adaptable to numerous mobile X-ray units
- All common X-ray images can be processed into 3D (e.g. scans from X-ray films & storage foils, images from analog & digital image converters)
- Import function for JPG, TIF and EPS formats
- Image enhancement, e.g. brightness, contrast, filters, sharpness, bump map, gamma corr. with preview in 2D



## 3D image Enhancer

## Model 7539

### INCLUDED IN DELIVERY:

- 3D Image Enhancer Software for X-ray source motion control, image processing & 3D visualization (single license)
- High end 3D Laptop with mouse
- Linear motor for motion of X-ray source
- Controller for linear motor
- Power supply 100 – 240 V and rechargeable battery
- Cable set 10 m (50 m option available)
- Tripod for linear motor and X-ray source
- Waterproof, shock protected transport case
- Supplied without X-ray source & image converter!

### TECHNICAL DATA

Processing time:	About 10 - 30 s per 3D image
Max image size:	2000 x 2000 pixels
Processor:	Intel® Pentium® 4, 2.8 GHz
Operating System:	Windows® XP Professional
RAM/HDD/Optical Drive:	512 MB DDR SDRAM/60 GB/DVD-R/-RW/RAM (max 8x)
Video Controller:	NVIDIA® GeForce™ 4 440 Go
VRAM:	64 MB DDR video memory
Monitor:	LCD 15" 3D-XGA / 1024 x 768
I/O Ports:	USB 2.0, PCMCIA II, 100 Base-TX, 56 kbps Modem, IEEE1394, SD- & CF-Card, Memory Stick™
Environment:	10 to 35°C / 20 to 80% humidity
Case size:	62 x 50 x 22 cm
Total weight:	15 kg (including case)



# Wireless Network Detector

# Model 7540

## DESCRIPTION

The professional Wireless Network Detector and visualization tool detects and stores all the important information about your Wireless Network Environment automatically to an SQL Database and visualizes your WLAN infrastructure on your own imported maps. The information stored in the Database contains extensive information, such as the Type of Encryption, GPS-Coordinates, and Channels etc. The equipment also provides the possibility to find out the exact location of an unknown Wireless Access Point with the directional Helix-Antenna and the included PDA Device.

With the Wireless Network Detector you are able to see if unauthorized Access Points within your Organization are present.

## FEATURES

- Database-Support to store the information
- Visualize the Access Points on your own maps
- Automated WLAN Visualizing
- PDA solution to locate the Access Points
- Dual Boot (Windows & Linux)
- Sirf III GPS included
- 12V Power Adapters included
- 512 MB Flash Memory included
- Ultra-portable High End Notebook

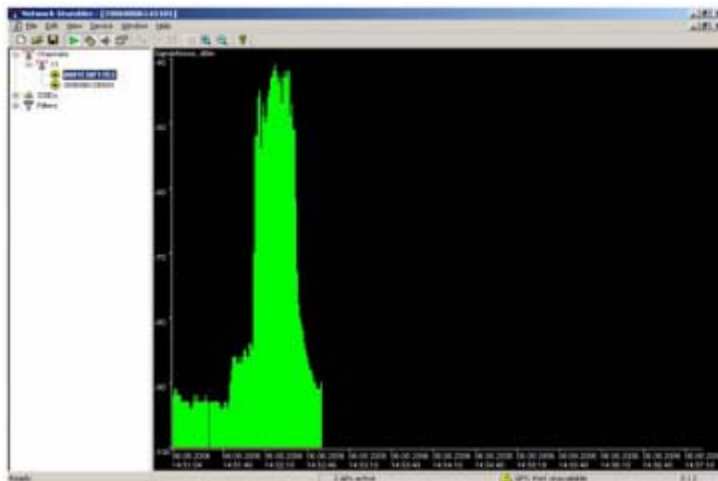
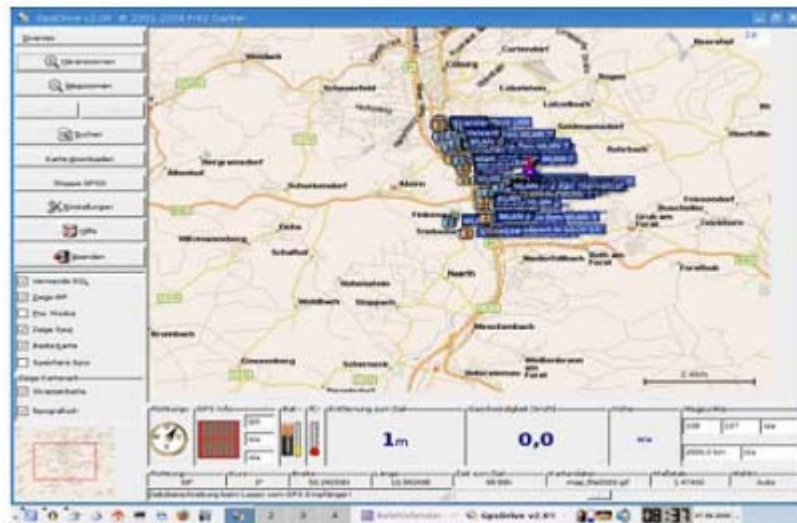
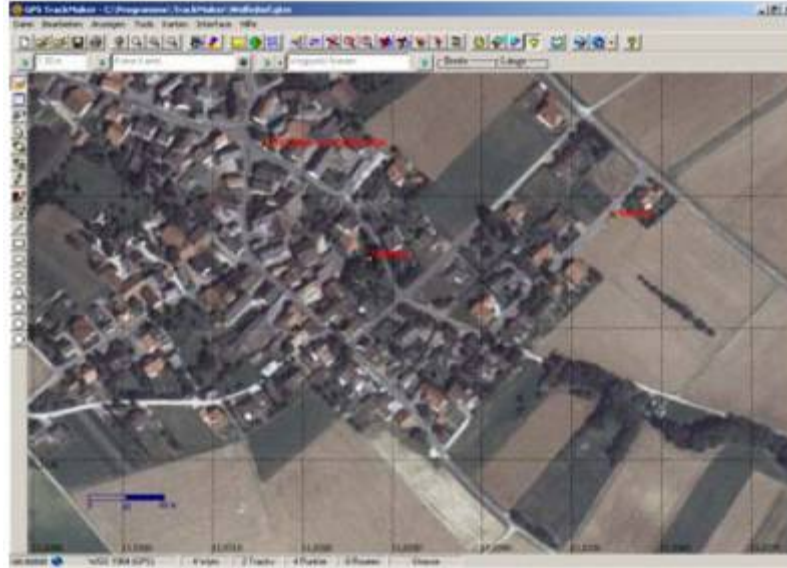


## TECHNICAL DATA

Notebook	IBM Tablet Notebook X41
OS	Linux/Windows® XP Tablet
RAM	512 MB
Hard disk	60 GB
I/O Ports	USB 2.0, PCMCIA II, 100 Base-TX, 56 kbps Modem, IEEE1394, SD-Card, Bluetooth
GPS-Receiver	Sirf III - NMEA
PDA	Sharp Zaurus C-1000
OS	Linux
ROM	128 MB
Case Size:	100 x 40 x 15 cm
Weight:	5,0 kg
WLAN type	802.11 a,b,g

# Wireless Network Detector ILLUSTRATIONS

Model 7540








## Wireless Network Detector

## Model 7540

### WLAN DETECTION AND CONTROL SYSTEM

The WLAN Detection and Control system is designed for TSCM professionals who need to know exactly what 802.11 RF traffic is present, in and around their target location. By using the supplied portable equipment, an operative can survey the target area and map all the RF information onto satellite imagery. By looking at the details provided by the system, it is possible to identify unauthorized 802.11 devices. With the unique traffic control system it is possible to interfere with the unauthorized devices, rendering them useless.

As well as the overt mapping system, it also comes supplied with a covert detections system. The body worn PDA and antenna allows an operator to use the device without being obvious. All the data is then transferred onto the main unit to map all information onto the satellite imagery.

<p>WINDOWS BASED LAPTOP CONTROL SYSTEM WITH DUAL 802.11 b/g</p>	
<p>OMNIDIRECTIONAL VEHICLE ANTENNA</p>	
<p>DIRECTIONAL HANDHELD ANTENNA</p>	
<p>GPS RECEIVER</p>	
<p>WINDOWS BASED PDA COVERT SYSTEM WITH DUAL 802.11 b/g</p>	

## Telephone Line Analyzer Detector

## Model 7541

Second to the physical search, cable and wiring checks are the most time consuming and technical. To ensure an effective and thorough cable check, there are over 10 checks for each cable, requiring a skilled operative and careful documentation.

The Telephone Line Analyzer provides a complete integrated suite of tools to analyze, inspect, and test digital telephone lines (and other wiring) for taps and other eavesdropping devices.



### TECHNICAL FEATURES

- Combines multiple testing capabilities into a single piece of equipment
- Automatic internal pair switching matrix performs tests on all pair combinations
- Quickly performs common test functions including:
  - Multimeter tests (voltage, current, resistance, capacitance)
  - RF Broadband Detector (up to 8GHz)
  - Spectrum Analyzer (up to 85MHz)
  - High Gain Audio Amplifier
  - Bias Generator +80 VDC
  - Audio Oscilloscope with active input (20Hz to 20KHz)
- Digital Demodulation to confirm that the telephone line is not passing audio
- Frequency Domain Reflectometer (FDR) to check for taps on the line
- Line Non-Linear Junction Detector (NLJD) Functionality to detect electronics connected to a line
- NLJD Line Trace Probe for tracing wires and locating electronics



# Telephone Line Analyzer Detector

# Model 7541

## Digital Demodulation

Includes digital decoding capabilities for approximately 80 percent of the world's digital phone systems. Demodulation CODECS are upgradeable as new phone systems become available.

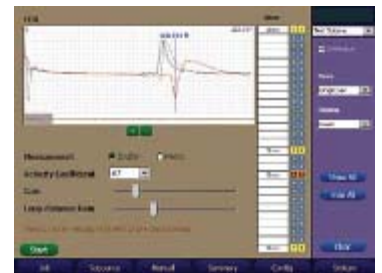
Digital Demodulation confirms that a line on a digital phone system is not passing audio when it should not.



## Frequency Domain Reflectometer (FDR)

Similar to a TDR (Time Domain Reflectometer) but based on a different technical approach, the Model 7541's FDR can "shoot" a line for impedance anomalies indicating a tap on the wire.

The FDR also has the ability to plot multiple FDR traces on the same display for comparison of multiple pairs or historical comparison.



## Non-Linear Junction Detection (NLJD) on a Line

The Model 7541 includes an NLJD test to detect electronics connected to an isolated line.

This is one of the most powerful tests for quickly determining whether or not there are additional electronics attached to a wire.

The example to the right indicates a parallel tap on pair 4:5.

Because of the coupling in balanced pairs, any combination with either a 4 or 5 indicates some electronic content, but the electronics are clearly detected on pair 4:5.



## Digital Multimeter Tests

The Model 7541 includes basic multimeter tests, such as Voltage, Current, Capacitance, and Resistance.

The automatic switching matrix allows the user to quickly measure and display results for all pair combinations, easily identifying any anomalies.



## TECHNICAL SPECIFICATIONS

### CONTROL SYSTEM

- Primary Computer: 32bit RISC processor, 520MHz
- Internal Memory: 64MB SDRAM (OS), 64MB Flash
- External Memory: Compact Flash to 2GB

### DIGITAL I/O

- Network: 10/100 Ethernet Controller
- USB: USB Host (B type) for connection to PC; USB Device (A type) supports external keyboard, mouse, and "thumb" drive use

# Telephone Line Analyzer Detector

Model 7541

## ANALOG I/O

Headphone Output: 3.5mm Mono connector  
Microphone Input: 3.5mm Mono input

## USER INTERFACE

Hard Keys: 6 Soft menu keys, 5 button quadrant navigation and other dedicated keys

Encoder: High-resolution optical encoder

Integrated touch screen with stylus

Test Inputs:

Dual MOD8: Supports 2, 4, 6, & 8 wire modular phone jacks

Banana Type: Standard sleeved sockets: Ring, Tip, and Earth

SMB RF Input: RF/Antenna connection to 8 GHz broadband detector

Expansion Port: Supports communication & measurement for use with future accessories

## RF SYSTEM

Spectrum Analyzer:

Dual conversion, super-heterodyne receiver

Frequency Range: 10kHz to 85MHz

Sweep Time: 2 Seconds

Step Size: 1kHz

Bandwidth: 18kHz

Sensitivity: -100dBm

Broadband Detector:

RF SMB Input: 100kHz to 8GHz

Balanced Line Test: 100kHz to 600MHz

Sensitivity: -65dBm

## DIGITAL MULTIMETER

Range: Quick response auto-ranging, 500msec sample rate

AC/DC Volts: 0 to 400VDC, 0 to 250VAC

Resistance: 0 to 40 MegOhm

Capacitance: 4nF to 400µF

## BIAS GENERATOR

Optically Isolated, Direct Digital Control: High voltage DAC

Output Ceiling: + - 80 VDC

Modulation: Sine, ramp, triangle sawtooth, & square waves up to 300hz.

## AUDIO

Optically Isolated: Wideband audio path optically isolates user from connection

Bandwidth: 10MHz at nominal gain of 60dB

Gain: Up to 80dB total system gain (voice band)

AGC: Digitally controlled automatic gain

Filter: Analog voice band filter (300Hz to 3kHz)

## Telephone Line Analyzer Detector

**Model 7541**

### POWER SYSTEM

External Input: 9 - 15VDC @ 3A

Universal Power Supply: 100-240VAC, 50-60Hz

Removable Battery: Rechargeable Lithium ion, 4-6 hours of run time

### MECHANICAL

Dimensions: 9.5in x 12in x 2in (24.1cm x 30.5cm x 5.0cm)

Unit Weight with Battery: 6 lbs (2.7 kg)

Case Dimensions: 6.25in x 14.9in x 18.5in (15.9cm x 37.8cm x 47.0cm)

Case Weight (Including Model 7541 and accessories): 11.5 lbs (5.2 kg)

Operating Temperature: 0°C to +50°C





## Secure Document Scanner

## Model 7542

The cutting-edge Model 7542 Secure Document Scanner is an overall concept for an extremely safe and high standard of handling important and confidential paper documents. The major components are a completely new developed security-paper that acts as a magnetic storage medium, as well as a special read-write device with a PC or Laptop connection.



Model 7542 media is writeable and printable using standard methods (Laser, Inkjet, Offset etc.). The magnetic memory is either invisibly paper-integrated, laminated, or can be glued on afterwards. Encrypted data of any kind, like digital certificates or information concerning the origin and authenticity of the document, can, from now on, be stored.



The digital document-certificates are administrated through a Trustcenter. All memory-data is compared with the deposited data after authentication via an encrypted connection. The Model 7542 offers state-of-the-art technical solutions for document-protection beyond comparison, especially developed for high security-demands.

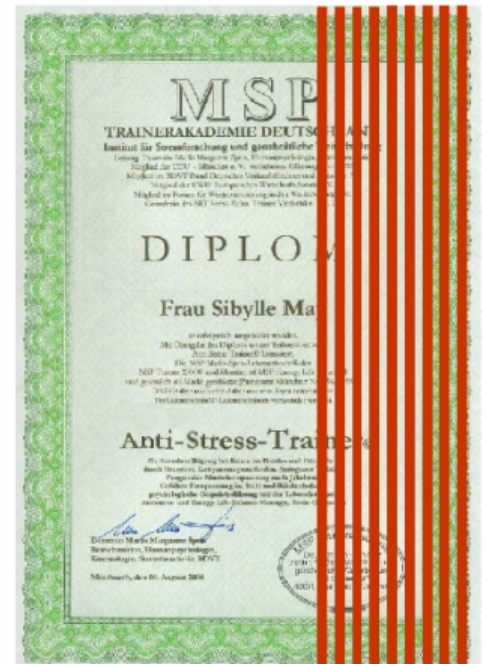
### FEATURES

#### ADVANTAGES:

- Unrivalled proof of document-identity
- Offers invisible protection
- Several paper-grades and formats are available
- Suitable for already existing documents, independent of format
- Manipulation-proof solution through digital certificates
- Encrypted certificate-comparison through a Trustcenter
- A certification is scheduled

#### INCLUDED:

- The Model 7542 starter set with one read-write device
- Single-licence software for Trustcenter-accessibility
- 500 sheets DIN A4, 160 g/m<sup>2</sup>, with internal memory
- 500 sheets DIN A4, 90 g/m<sup>2</sup>, with laminated memory
- Optional individual processing-stations available
- Additional biometrical user ID possible



## LAN/WLAN checking system

## Model 7543

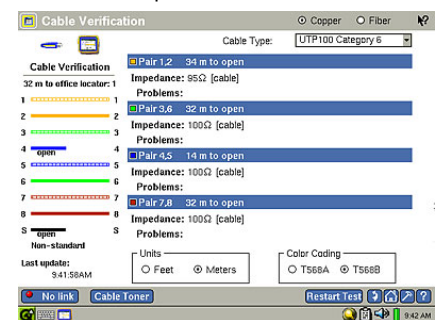
The LAN checking system has come a long way since just checking structured cabling. The threat of an IT related attack has heightened bringing with it the need to check IT systems. The LAN/WLAN Checking System is capable of performing checks on structured cabling and any data present on the line. Its semi automated checks provide clear information presented in a printable report.

**Fully Automated** - The LAN Checking System provides an instant view of the state of the network with its information-rich Autotest Results main screen and tri-color LEDs. Multiples tests run concurrently, speeding problem discovery. Selecting any individual test displays overview information on the left side preview pane; Select Details for in-depth test information.



**Cable Checker** - Verify the characteristics of UTP and STP copper cabling: length, impedance, shorts, opens and wire mismatches showing taps, bridges and tampering on the cable and the distance to the tap.

**Signal Verification** - Test 802.3af Power over Ethernet (PoE) links. The LAN Checking System can emulate an 802.3af powered device to solicit and measure voltage on each pin showing illegal power activity on the cable.



**Discover unauthorized devices** - Discover up to 1,000 devices and extract switch and VLAN information showing if unauthorized devices are present.

**Discover unauthorized traffic** - View your network's traffic statistics, including protocol mix, top senders, top broadcasters, and error sources. Identify and locate bandwidth hogs and isolate them from the network if necessary. Analyze performance trends with baseline data reports. Analyze traffic showing attacks and unauthorized protocols.

**Discover unauthorized wireless devices** - Wireless security is a top concern, and wireless security policies are difficult to enforce. Use Wireless LAN Checking System to perform periodic audits of the wireless environment. Wireless LAN Checking System automatically discovers rogue access points, unauthorized wireless bridges, mobile clients and ad-hoc networks, enabling quick response and resolution.

**Locate Rogue Wireless AP** - An unauthorized "rogue" access point can compromise network security by exposing the company's network to the outside world. Use the wireless LAN Checking System "Security Scan" feature to identify rogue APs and "Locate" to hunt them down

## LAN/WLAN checking system

## Model 7543

**Survey RF Site** - Use the Wireless LAN Checking System to capture baseline RF coverage data immediately after the wireless infrastructure is installed and compare historical data to periodic survey data over time. Use this information to make minor adjustments to wireless access points, transmit power, relocate access points, minimizing RF leakage or show external sources of RF.

**Cable Locating** – The breakthrough IntelliTone digital signaling works with the IntelliTone Pro Probe to locate voice, data, and coax video cabling through up to two feet of sheetrock, Isolating all electromagnetic and radio frequency interference in digital mode. Featuring IntelliTone cable mapping; after tracing, use the Tone Probe to verify wiremap.

### Specifications

<b>RFC 2544 Testing Option (option for LAN/Pro models)</b>	
Compatible remote device	EtherScope, EtherScope Series II Network Assistant
Tests	Throughput, Latency, Frame Loss
Frame content	All 0s, all 1s, alternating 1s and 0s, Pseudo Random Bit Sequence (PRBS), Incrementing Byte
Frame size	64, 128, 256, 512, 1024, 1280, 1518, sweep of all sizes
Application port	User defined
Rate (bps)	Up to 1000 M (using an EtherScope as a remote device)
802.1Q settings	VLAN Id, priority
IP TOS settings	IP Precedence/TOS parameter, DiffServe Code Point
Throughput settings	Duration, maximum rate, measurement accuracy
Latency settings	Duration, rate, iterations
Frame loss settings	Duration, rate, step size
Results format	Tabular, graphical, xml-based report
<b>Internetwork Throughput Option (included with RFC 2544/ITO Option)</b>	
Compatible remote device	OptiView v4 Integrated Network Analyzer, EtherScope, EtherScope Series II Network Assistant, OneTouch Series II
Frame content	All 0s, all 1s, alternating 1s and 0s, Pseudo Random Bit Sequence (PRBS)

## LAN/WLAN checking system

## Model 7543

Frame size	64, 128, 256, 512, 1024, 1280, 1518, sweep of all sizes
Rate (bps)	672 to 1000 M (using an EtherScope as a remote device)
Duration(s)	1 to 64,800 (18hr)
Results	Frames sent, received, rate and percent loss for both upstream and downstream directions
Results format	Tabular, graphical, xml-based report
<b>Traffic generator (included with RFC 2544/ITO Option)</b>	
Traffic type	Broadcast, multicast or unicast
Frame type	Benign Ethernet, Benign LLC, NetBEUI, Benign IP, IP/ICMP Echo, IP/UDP Echo, IP/UDP Discard, IP/UDP Chargen, IP/UDP NFS, IP/UDP NetBIOS
Frame size	64, 128, 256, 512, 1024, 1280, 1518
Rate	Utilization (%): >0 – 100, Frames/second: 1 – 1488095
Duration	Seconds: 1 – continuous, Frames: 1 – continuous
<b>Wireless LAN Adapter Card (WLAN/Pro models)</b>	
Specification compliance	IEEE 802.11a, 11b, 11g
Certifications	FCC part 15, Telec, CTICK, ETSI, EN301893, EN60950 Interoperability WECA Compliant
Interface	32-bit Cardbus
Outdoor operating range	Up to 515 m (1690 ft)
Indoor operating range	Up to 85 m (279 ft)
Data rate	802.11a: up to 54 Mbps, 802.11b: up to 11 Mbps, 802.11g: up to 54 Mbps
Output power	18 dBm peak power
Infrastructure mode	BSS
External antenna connector jack	Hirose MS-147

## LAN/WLAN checking system

## Model 7543

### Wireless LAN Directional Antenna (WLAN/Pro models)

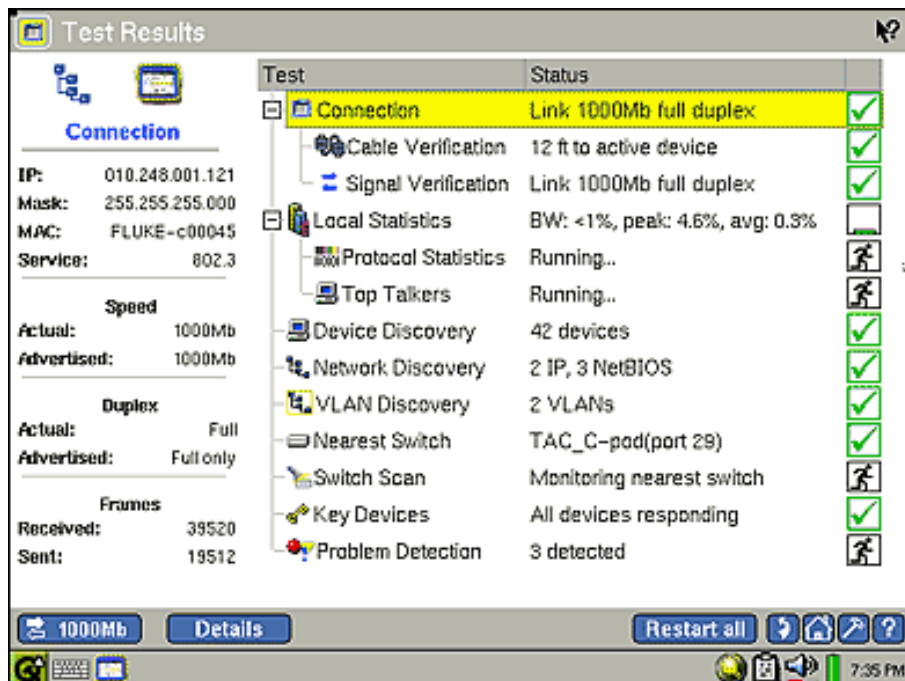
Frequency range	2.4 – 2.5 and 4.9 - 5.9 GHz
Minimum gain	5.0 dBi in the 2.4 GHz band and 7.0 dBi in the 5 GHz band
External antenna connector plug	Hirose MS-147

### Fiber Optic Transceiver (option for LAN/Pro models)

Ethernet rate	1000 Mbps
Type	Small Form-factor Pluggable (SFP)
Connector	Duplex LC

### Security

Authentication types	LAN: 802.1X, WLAN: 802.1X, 802.11i, WEP, WPA, WPA2
EAP types	TLS, GTC, MD5, MS-CHAP-V , LEAP, PEAP-GTC, PEAP-MD5, PEAP-MS-CHAP-V , PEAP-TLS, TTLS-PAP, TTLS-CHAP, TTLS-MS-CHAP, TTLS-MS-CHAP-V , TTLS-EAP-MD5, TTLS-EAP-GTC, TTLS-EAP-MS-CHAP-V , TTLS- EAP-TLS



The screenshot displays a 'Test Results' window with a tree view of tests and their statuses. The 'Connection' test is highlighted in yellow and shows a status of 'Link 1000Mb full duplex' with a green checkmark. Other tests include Cable Verification, Signal Verification, Local Statistics, Protocol Statistics, Top Talkers, Device Discovery, Network Discovery, VLAN Discovery, Nearest Switch, Switch Scan, Key Devices, and Problem Detection, all with various statuses and icons.

Test	Status
Connection	Link 1000Mb full duplex
Cable Verification	12 ft to active device
Signal Verification	Link 1000Mb full duplex
Local Statistics	BW: <1%, peak: 4.6%, avg: 0.3%
Protocol Statistics	Running..
Top Talkers	Running..
Device Discovery	42 devices
Network Discovery	2 IP, 3 NetBIOS
VLAN Discovery	2 VLANs
Nearest Switch	TAC_C-pod(port 29)
Switch Scan	Monitoring nearest switch
Key Devices	All devices responding
Problem Detection	3 detected

Additional information shown in the interface includes:

- Connection:** IP: 010.248.001.121, Mask: 255.255.255.000, MAC: FLUKE-c00045, Service: 802.3
- Speed:** Actual: 1000Mb, Advertised: 1000Mb
- Duplex:** Actual: Full, Advertised: Full only
- Frames:** Received: 39520, Sent: 19512

## TSCM Search Video Pole Camera

## Model 7544

Sometime during a physical inspection it is not be possible to have the means or time to inspect all hard to reach areas. The Video Pole Camera was developed with the aim of providing an accurate search of the target location. With its hi-resolution camera and screen and 6-foot reach it is possible to get into areas that a search mirror kit cannot. Inspect drop ceilings, behind immovable objects, around corners, or other difficult to reach areas, even in dark situations with the Video Pole Camera.

- **Cable Basket Runs**
- **False Ceilings**
- **False Floors**
- **Behind, under and over heavy immovable objects**

Inspect drop ceilings, behind immovable objects, around corners, or other difficult to reach areas, even in dark situations with the Video Pole Camera.

### FEATURES

The Video Pole Camera provides a small, self contained, easy to use pole camera inspection system. The 24-inch pole extends to over 6 feet without changing configuration, giving the average user over 10 feet of reach.

White LED illumination for color inspection in dark areas (i.e. drop ceilings)

IR LED illuminated black and white camera head available for covert or tactical applications

Large 6.4 inch (16 cm) diagonal, high resolution display, enhanced brightness, color monitor

No external cables, ready-to-use out of the case

Collapsible pole, removable camera head, monitor, and batteries fit into a case slightly larger than a standard briefcase

Extremely portable, lightweight, and easy to use





## TSCM Search Video Pole Camera

Model 7544

### TECHNICAL SPECIFICATIONS:

#### STANDARD COLOR CAMERA HEAD

Signal Format:	NTSC
Horizontal Resolution:	More than 380 Lines
Sensitivity:	0.5 Lux / F1.2, 1.0 Lux / F2.0 (AGC ON)
Illumination:	4 White LEDs with variable brightness control



#### OPTIONAL IR ILLUMINATED BLACK & WHITE CAMERA HEAD

Signal Format:	NTSC
Horizontal Resolution:	420 Lines
Sensitivity:	0.0003 Lux / F1.2, 1.0 Lux / F2.0 (AGC ON)
Illumination:	8 Infrared LEDs with variable brightness control



#### COLOR LCD DISPLAY

Size:	6.4 inch (16 cm) diagonal
Brightness:	300 nits
Viewing Angles:	+/- 50° horizontal, +/- 40° vertical
Display Controls:	color saturation, contrast, and brightness
Camera Head Controls:	variable illumination



#### RECHARGEABLE POWER SUPPLY

Charger and two Ni-MH Battery Packs included

Average Run-Time:	2.0 Hours
Average Charge-time:	1.8 Hours

#### MECHANICAL

Collapsed Length (incl. Camera Head):	24.5 inches (62 cm)
Extended Length (incl. Camera Head):	6.5 feet (200 cm)
Weight:	3.6 lbs (1.6 kg)
Case Size:	18.5x6 x14.5 inches 47x15.3x36.8 cm
Case Weight, Pole Camera, Accessories:	11.0 lbs (5.0kg)



**Inspect hard to reach and inaccessible areas with the portable, quick-to-deploy Video Pole Camera.**





## Video Wireless Detection

## Model 7545

The Video Wireless Detection unit is a fast scanning receiver that detects wireless video cameras from 900MHz-2.52GHz for quick effective detection of wireless video signals during TSCM search operations.

With a 2.5" TFT color LCD the Video Wireless Detection unit shows you what the hidden camera is looking at. A separate smaller LCM displays the frequency and the signal strength of the signal the Video Wireless Detection unit locked on to. The Video Wireless Detection unit quickly scans, in about 15 seconds, all the available video frequencies used.

The Video Sweeper works with a full range of video protocols including NTSC, PAL, CCIR or EIA systems. The Video Sweeper has both an automatic and manual scan mode and an alarm may be activated for an audible alert when a camera is detected.

The Video Wireless Detection unit can detect some signals from as far away as 500 feet. The detection distance depends upon the power output of the transmitter and the sensitivity level selected on the unit. The Video Wireless Detection unit has 5 separate receive sensitivity settings ranging from -20dBm to -60dBm.

### FEATURES

- Frequency Range 900MHz to 2.52GHz
- Detects NTSC, PAL, CCIR, EIA systems
- Signal strength indicator
- 5 selectable receive sensitivity settings
- Audible beeper alert
- Detection distance up to 500 feet
- 2.5" TFT color LCD display
- Scans frequency range in 15 seconds
- Includes AC adapter, two antennas and case
- Operates on 4 AA batteries
- Automatic or manual scan
- LCM displays frequency and signal strength
- Audio and Video output jacks for external use
- Size: 4.75"H x 2.75"W x 1.5"D



### TECHNICAL SPECIFICATIONS

<b>Frequency Range</b>	900MHz-2.52GHz
<b>Sensitivity</b>	-20dBm to -60dBm
<b>Display</b>	2.5 TFT color display with LCM display for frequency
<b>Video Protocols</b>	Detects NTSC, PAL, CCIR and EIA systems
<b>Scan Speed</b>	Scans entire frequency range in 15 seconds
<b>Size</b>	4.57"H x 2.75"W x 1.5"D
<b>Weight</b>	12 oz.
<b>Battery</b>	Internal 4 AA alkaline, NiCD, NiMH batteries (not included)
<b>Operating Time</b>	2 hours
<b>Power</b>	5vdc, 2amp 110-240v center positive adapter included.
<b>External Connection</b>	3.5mm mono Alarm and Video output

## Cable Amplifier System

## Model 7546

**One of the essential tools used within a cable sweep is the Cable Amplifier System. It is necessary to use an amplifier to detect hardwired microphones, insert voltage into a line to power a hidden microphone and to record the voltage present on the line.**

**The Cable Amplifier System** is a high gain audio amplifier used to detect and identify certain types of surveillance devices attached to building wiring, such as telephone wiring, LAN and server systems, AC Power, and Alarm wire, etc.



It is designed to provide flexible features and has proven to be very useful in many situations. This amplifier is quite useful for checking telephone lines and other wiring for hostile microphones, testing for hook switch audio leakage, and detection of eavesdropping devices that are sensitive to bias voltages or currents

### TECHNICAL FEATURES

- This multifunctional amplifier has a built in AC/DC digital voltmeter, selectable audio filters, and an extremely wide dynamic range
- Balanced and unbalanced high impedance inputs provide connectivity to a variety of suspect wiring
- The CMA100 also provides a bias voltage adjustable between -15V and +15V DC that is used to activate possible devices that are voltage or current sensitive. The bias generator is compatible with most types of line conditions
- All of these functions employ a sophisticated automatic gain control circuit that is superior to most audio amplifiers

### SPECIFICATIONS

Input Impedance:	50k balanced
Common Mode Rejection:	>75 dB
Maximum Usable Input:	10V p-p
Preamp Auto Attenuator:	0 to -20 dB ( with overload warning LED )
Automatic Gain Control:	-20 to +120 dB ( includes preamp auto attenuator )
Manual Gain Control:	0, 25, 50, 75, 100 dB
Headphone Gain Control:	0 to 15 dB
Maximum System Gain:	115 dB manual mode, 120 dB in Auto Mode
Frequency Response:	100 Hz to 15 kHz
High Pass Filter:	300 Hz to 20 kHz
Low Pass Filter:	100 Hz to 3 kHz

## Cable Amplifier System

**Model 7546**

Band Pass Filter:	300 Hz to 3 kHz
Headphone Audio Output	
Line-Out Audio Output:	600
Bias Control:	0 to +/-15V DC, 5mA max (over current protected, input impedance is reduced to 3k ohms when bias is active)
Digital Voltmeter:	3.5 Digit, auto zero, auto polarity, +/-199.9V AC/DC
Power On/Low Battery LED ( LED off @ 6.0V )	
Maximum Input voltage:	250V AC/DC
Leakage Resistance to Case:	>10M
Size:	7.3"(184.4mm) x 2.75"(69.8mm) x 1.75"(44.5mm)
Weight:	12.1 oz (343g)



# Flat Panel X-Ray System

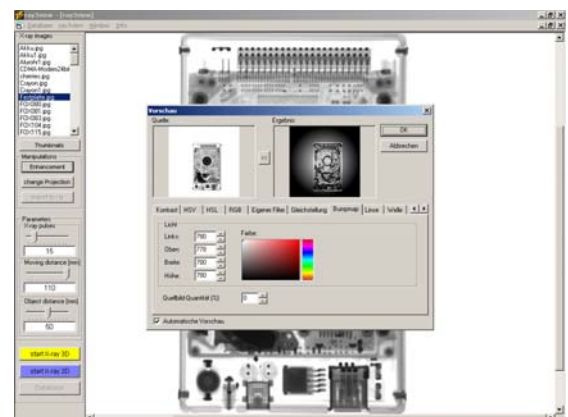
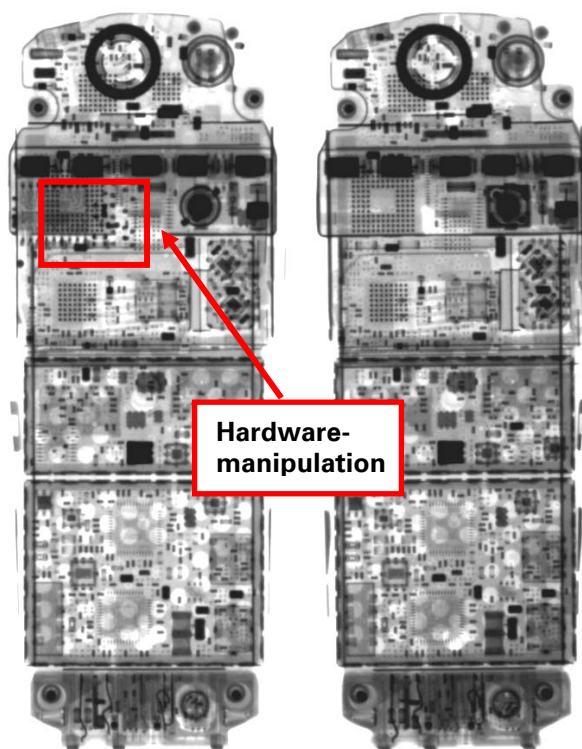
# Model 7547

## DESCRIPTION

The unit is a state-of-the-art digital mobile flat panel X-ray system manufactured in Western Europe. The flat image converter enables many different applications in the fields of security and non-destructive-testing. For EOD use the Notebook provides a save operation by 100 m cable or remote control. The high resolution of 127  $\mu$ m allows the identification of even the smallest details on X-ray images with more than 16,000 grey levels.

With its battery operation, its extensive image enhancement software with integrated database and most of all its optional visualisation of 3D x-ray images the unit is an unique inspection device. Our continuous updates always provide you the latest software versions and our help desk will support you with any necessary technical advice.

## ILLUSTRATIONS



# Flat Panel X-Ray System

**Model 7547**

## FEATURES

### ADVANTAGES:

- Adaptable to numerous industrial X-ray units
- Image enhancement, e.g. brightness, contrast, filters, sharpness, bump map, gamma correction
- Helpdesk & free software updates
- Optional upgrade for 3D X-ray image-visualisation

### INCLUDED IN DELIVERY:

- High-resolution, digital flat panel detector
- Image processing & control software (single license)
- **FlashScan** control unit & high performance Notebook
- Power supply 100 – 240 V & rechargeable battery
- Cable set 10 & 50 m; user manual
- Waterproof, shock protected transport case
- **Supplied without X-ray source!**

## TECHNICAL DATA

<b>Notebook:</b>	State-of-the-art, 15" XGA TFT, > 1,5 GHz, > 40 GB HDD, DVD
<b>Type of detector:</b>	THALES FlashScan 35 Fast amorphous silicon TFT-Panel
<b>Processing time</b>	< 2 s per image
<b>Imaging area:</b>	400 x 280 mm
<b>Image size (Pixel):</b>	3200 x 2240 (1 mm <sup>2</sup> ~ 64 Pixel)
<b>Resolution:</b>	127 $\mu$ m (~4 lp/mm)
<b>Digital output:</b>	14 bit (> 16,000 grey levels)
<b>Required X-ray source:</b>	30 – 160 kV (e.g. Golden Engineering XR-150 or XR-200)
<b>Battery operation:</b>	> 2 hrs. (dep. on No of images)
<b>Dimensions:</b>	50 x 36 x 4,6 cm (converter)      62 x 50 x 35 cm (carrying case)
<b>Total weight:</b>	Approx. 40 kg (excl. X-ray source)

## GSM Detection System

## Model 4014

### OVERVIEW

The GSM Tracer is a system developed as a counter-measure to bogus GSM base stations. In general, the use of advanced encryption in the GSM system means that mobile calls are relatively secure. Off-air interception of calls is very difficult. An alternative method is to use a bogus base station and force a mobile to use this in unencrypted mode. Such a system can also be used to determine the IMSI (IMSI grabbing) to enable interception at the switch.



This is of particular concern where cell phones are likely to be used for sensitive communications or in the vicinity of an area thought likely to be subject to espionage. At particular risks are:

- Senior Officials
- Government Buildings
- Embassies
- High Profile Personnel

By monitoring transmissions from legitimate base stations the GSM Tracer is able to build up a picture of the network environment and use this to recognize suspicious transmissions from bogus base stations. Key features of the system are:

- All Networks continually scanned and monitored
- Compact, portable, easy set up, and configured
- Display of Encryption type and detection of any changes
- Programmable alarms for various changes in status

### GSM TRACER

The GSM Tracer system is a GSM receiver, which constantly scans the GSM control channels of all networks (dual band). It looks for changes in the overhead parameters transmitted by the genuine network. The GSM receiver will be looking for LAC changes, lack of paging, 'call set-ups' without encryption, changes in power, switching encryption off/on etc. The Display shows all of the current channels detected, network operator, encryption used, hopping used, and amount or absence of pages transmitted.

### BOGUS CELL DETECTION

By being aware of the transmitted system information on the control channels of legitimate cell sites within the area, the GSM Tracer is able to recognize bogus cell sites that are attempting to mimic a legitimate site for its own purposes. Once the GSM receiver has latched onto these bogus cell transmissions, it then decodes the transmissions, giving the user information such as target IMSI.

The GSM receiver has the ability to perform its own scans based on neighbor lists read from the overhead of the genuine cells.



## **GSM Detection System**

## **Model 4014**

In a mobile environment, when the bogus cell's target passes through the genuine cells, these signal strengths (from the targets perspective) will increase, then decrease, as the target passes close by, and then away from the relevant cell sites. In the case where a bogus cell is following a target in a vehicle, the transmission will remain roughly constant. This situation can be identified by the GSM Tracer system.

The GSM Tracer is small, portable, and 12V DC powered. It is equally suited for office or in vehicle installations.

### **ALARM GENERATION**

The GSM Tracer's alarm can be set to trigger on a number of parameters. For example, it could be used to indicate when the local cell operators have turned off the encryption and/or frequency hopping. This could indicate that they intend to use direction-finding equipment. It can also trigger when a channel changes its LAC, which implies a bogus cell is forcing a location up-date from mobiles in the target area.

### **LOGGING OF SURROUNDING MOBILES**

The GSM Tracer can survey an area from a mobile platform, such as a car. The logs will be the signal strength of surrounding Cells as seen by the GSM Tracer with position information from an attached GPS receiver. When the GSM Tracer is later located at its stationary position it can decode measurement reports from mobiles in the immediate area. These measurement reports can be matched with the survey logs giving the position of the mobiles. The mobiles will be identified by their TMSI. The survey results are stored in such a way as to be able to be read by mapping programs.

### **FLUSHING OF TMSI'S**

The GSM Tracer can be connected to a serially controlled GSM mobile. This mobile is commanded to send a silent text to a target mobile in the area. The GSM Tracer will see the page and can deduce the TMSI associated with the target number.

### **USER INTERFACE**

The GSM Tracer is available with an embedded single board computer. Connection of a screen, keyboard and mouse will be needed to set up the alarm parameters. Alternatively the GSM Tracer can be driven directly from an attached laptop PC via the USB port. The operating system used is Windows XP, which has the facility for 'Remote Desktop', where via a VPN connection, the operation of the GSM Tracer can be controlled from a remote PC.

### **DECODE CALLS**

The GSM Tracer is a dual receiver capable of frequency hopping and following unencrypted calls, displaying text messages and recording audio. There is an option to enable the Hound dog to decode A5/2 encryption "off air"



## GSM Detection System

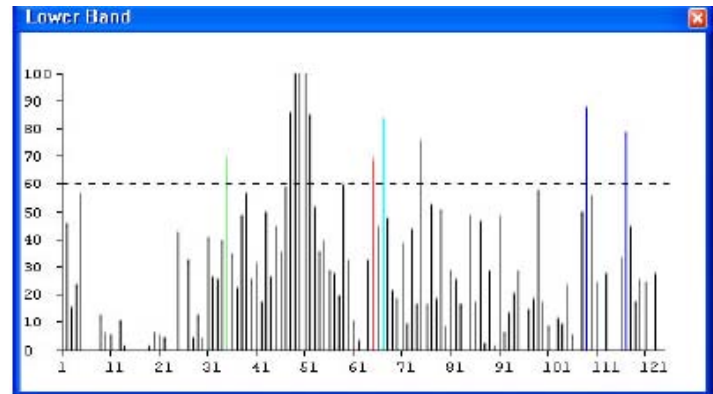
## Model 4014

### GSM TRACER FEATURES

The GSM Tracer system will constantly scan the GSM control channels of all networks (dual band). The following describes some of the features of the GSM Tracer software:

#### THE CHANNEL SCAN WINDOW

The Channel Scan windows display the power levels detected for each of the channels in the bands being scanned as a bar chart. Colors are used to highlight channels of interest.



The horizontal axis is the ARFCN of the channels. The vertical axis is the power level of the channel at this location.

The colors of the bars indicate different information:

- Black – Channels that are not broadcast channels
- Dark blue – Broadcast channels with no cell information
- Light blue – Broadcast channels with cell information, but unknown security
- Green – A channel ciphered with A5/1
- Red – A channel ciphered with A5/2 or not ciphered



A summary of information about a channel can be obtained by moving the mouse pointer over it. Clicking on a channel will display more detailed information in the Channel Properties window.

#### THE CHANNEL LIST WINDOW

The Channel List window contains a list of all the broadcast channels that GSM Tracer has discovered, while it has been scanning, and any information it has gained from these channels.

There are ten values for each channel in the list:

- ARFCN – The assigned channel number
- Network – The name of the network operating the cell serviced by this channel
- MNC – The Mobile Network Code of the network operator (useful if GSM Tracer does not know the name of the operator)
- Power Level – The last power level detected for this channel
- Ciphering – The type of ciphering being used (unknown, A5/1, A5/2 or none)
- Last Active – The last time the channel was detected sending broadcast information
- Empty Paging – The percentage of empty paging messages seen on the channel
- Channel Type – The type of channel being used (IV, V, or VI)
- Hopping – If the channel uses hopping for dedicated channels
- Individual Settings – If there are individual settings for alerts about this channel

# GSM Detection System

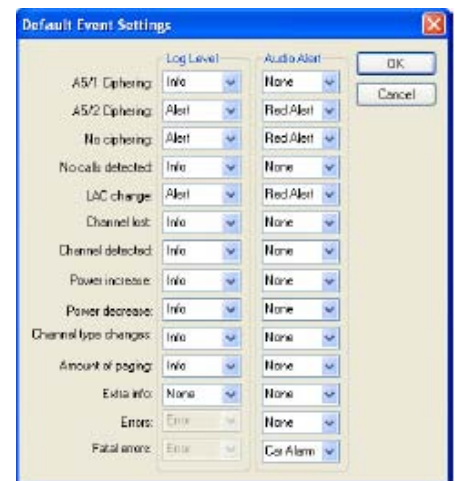
# Model 4014

ARPCN	Network	MNC	Power Level	Ciphering	Last Active	Empty Paging	Channel Type	Hopping	Individual Settings
36	02	10	70	A5/L	2004/11/05 13:18:01	35%	DV	Yes	Yes
65	Vodafone	15	70	A5/L	2004/11/05 13:16:30	49%	DV	Yes	Yes
67	Vodafone	15	85	None	2004/11/05 13:16:52	36%	DV	Yes	No
109	02	10	88	A5/L	2004/11/05 13:17:12	37%	DV	Yes	Yes
117	02	10	70	Unknown	2004/11/05 13:17:16		DV		Yes

## ALERTS

There are a number of events that will trigger the GSM Tracer alerts, all of the parameters can be set, and the corresponding reporting can be selected.

- A5/1 Ciphering
- A5/2 Ciphering
- No ciphering
- LAC changes
- No calls detected
- Channel lost
- Channel detected
- Power increase
- Power decrease
- Channel type changes
- Amount of paging
- Extra info
- Error
- Fatal

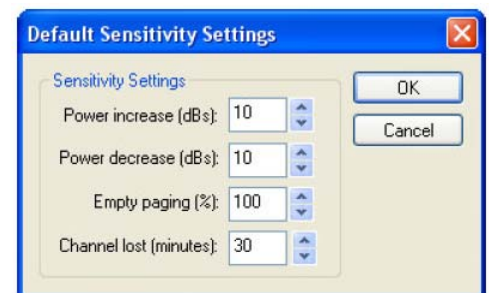


Default Event Settings dialog box showing Log Level and Audio Alert settings for various events.

Event	Log Level	Audio Alert
A5/1 Ciphering	Info	None
A5/2 Ciphering	Alert	Red Alert
No ciphering	Alert	Red Alert
No calls detected	Info	None
LAC change	Alert	Red Alert
Channel lost	Info	None
Channel detected	Info	None
Power increase	Info	None
Power decrease	Info	None
Channel type changes	Info	None
Amount of paging	Info	None
Extra info	None	None
Error	Error	None
Fatal error	Error	Cell Alarm

On the left side of the dialog there is a list of all the events that can occur while GSM Tracer is scanning. For each of the events there are two selection boxes. The left hand box sets the log level of the event, this will display the event in the 'Alert' or 'Info' display.

For change in Power levels, levels in Empty paging, and the time a Channel is lost, there is a further screen to set the levels of the Alert trigger.



Default Sensitivity Settings dialog box showing Sensitivity Settings for various events.

Event	Sensitivity Setting
Power increase (dBs)	10
Power decrease (dBs)	10
Empty paging (%)	100
Channel lost (minutes)	30

## DISPLAY WINDOW

- Window
  - Channel List – Displays the Channel List window
  - Lower Band – Displays the Channel Scan window for the 900 or 850 band
  - Upper Band – Displays the Channel Scan window for the 1800 or 1900 band
  - Channel Properties – Displays the Channel Properties window
  - Alerts – Displays the Alert Log window
  - Errors – Displays the Error Log window
  - Information – Displays the Information Log window

## Night Vision Viewer

## Model 1013

The Model 1013 Night Vision Viewer Unit is used for TSCM purposes to detect large laser monitoring systems (890NM) and fiber optical microphones.

The Model 1013 is designed to offer the largest selection of cameras available for the user. If your application calls for video surveillance (Sony, Canon, Panasonic, etc.), you can order the required adapter pairs.

If you also need to record using an SLR or digital camera, (Canon, Nikon or Minolta), just order the adapters for these cameras and switch back and forth.



Central Intensifier Unit with Monocular Viewer

The heart of the modular night vision is the CIU (Central Intensifier Unit), an electro-optical device with electronic communication that ensures proper interface between the camera and the lens.

A variety of Gen II, Gen III, and Gen IV XD-4 Central Intensifier Units allow you to tailor a system in terms of resolution, sensitivity, spectral response, gain, output brightness and budget.

Dark, moonlit or starlit nights can easily be recorded and imaged as bright, high-resolution scenes by the camera's daylight sensor or film. The Model 1013 extends the camera's usable light range without the drawbacks of slower shutter speeds or time integration.

As new cameras and technologies are introduced, new camera and lens adapters will be developed for the Model 1013, ensuring that your night vision system will never become obsolete! After you choose the adapter pairs (depending on the camera or camcorder you are using) you must choose the Central Intensifier Unit suited for your applications.



## Covert Door Opening Equipment

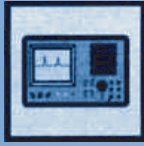
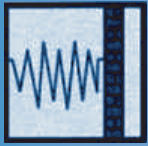
## Model 2001

### THE KIT CONSISTS OF:

1. 1 "Sputnik"
2. 1 "Tubular"
3. 1 Multi-Lock Pick Set
4. 1 E-Pick Professional Set "New Generation"
5. 1 Door Opening Set"
6. 1 Dental Pick Set
7. 1 Falle Lock Picks
8. 1 Pin Tumbler Decoder
9. 1 Hobbsche Hooks (Set of 4 different sizes)
10. 1 Cross Pick
11. 1 Matador Pick Set
12. 1 Duplicate Key Set
13. 1 Multi-pick Set
14. 1 Multifräße
15. 1 Lock-force "Professional Set"
16. 1 Tension Set (25 pieces)
17. 1 Milwaukee Mobil Reloader
18. 1 Accu-Light
19. 1 Replacement Lights (2 Pieces)
20. 1 Accu-Driller Lock-Tor
21. 1 Replacement Accu
22. 1 Kitbor Chubb Lever Set
23. 1 Jiggler Set (3 different Sets)
24. 1 Circle Manipulation Spiral-Needles (4 diff. pieces)
25. 1 Circle Manipulation Spiral-Needles small (2 pieces)
26. 1 Door Rod
27. 1 Window Opener
28. 1 European Percussion Spring System
29. 1 Door Panel Manipulation Hook
30. 1 Door Manipulation Card incl. 2 diff. Holders
31. 1 Manipulation Set for Lever Locks (13 Diff. Sizes)
  - A: Length: 75mm Shaft: 45mm (10 Pieces)
  - B: Length: 90 mm Shaft: 60mm (16 Pieces)
  - D: Length: 90 mm Shaft: 60mm (20 Pieces)
  - F: Length: 90 mm Shaft: 60mm (24 Pieces)
  - G: Length: 90 mm Shaft: 60mm (24 Pieces)
  - H: Length: 90 mm Shaft: 60mm (24 Pieces)
  - J: Length: 100 mm Shaft: 80mm (12 Pieces)
  - K: Length: 100 mm Shaft: 80mm (12 Pieces)
  - L: Length: 100 mm Shaft: 80mm (12 Pieces)
  - M: Length: 100mm Shaft: 80mm (24 Pieces)
  - N: Length: 150mm Shaft: 120mm (24 Pieces)
  - O: Length: 110mm Shaft: 80mm (15 Pieces)
  - P: Length: 150mm Shaft: 120mm (12 Pieces)



# TSCM INDEX



1 - Introduction

2 - The Threat

3 - Recommendations

4 - Training Course Overview

5 - Training Course Syllabuses

6 - Recommended Products

7 - Technical Data Sheets

8 - IP/PABX Manipulation

9 - Commercial Quotations

10 - Terms & Conditions

11 - Contact Details

12 - Elaman Catalogs Overview

## IT/Computer Threat

## IT Threat

**For every action there is an equal and opposite reaction. The same is true for IT/Infrastructure Security. For every security measure employed, soon enough there will a method TO break through it.**

With the advancements in digitization and technology more and more communications systems are becoming digitized and computerized. Analog telephone systems are migrating to ISDN. ISDN is migrating to Voice over IP. Wired networks are migrating to wireless networks. One of the obvious threats from this is interconnectivity. A reason and advantage for digitization and computerization is interconnectivity – multiple systems being able to speak to each other across great distances. The telephone system in Germany is connected to the telephone system and administration system in Canada. Although useful for the company employing the system, it is just as useful for the eavesdropper, who is able to attack the system from anywhere in the world and at any time.

Although countermeasures and attacks are constantly over taking each other there is still the need to employ security. Countermeasures are still going to be effective as a deterrent and an obstacle for the attacker. Slowing down the attack or simply making it too much effort can prevent a successful attack.

One of the best countermeasures is knowledge. Educating users and operators to employ their own security, use the system safely, and have the ability to recognize the signs of an attack are a large proportion of IT TSCM.

Following are just some of the attacks employed that all users should be aware of:

Time Bomb	Dictionary Scan
Logic Bomb	Digital Snooping
Rabbit	Shoulder Surfing
Bacterium	Dumpster Diving
Spoofing	Browsing
Masquerade	Spamming
Sequential Scan	Tunneling
Software Malfunction	Equipment Malfunction
Back Door	

### Information Security

A large amount of information is readily available for an attacker to use to carry out attacks. By being able to recognize areas of weakness users can proactively be more secure with information, thus reduce the opportunities for a potential attacker. The examples below show information found on the internet that would be useful to an attacker. It is quite easy, without knowledge, to inadvertently publish secure information on the internet.



## IT/Computer Threat

## IT Threat

```

Whois Server Version 2.1 at whois.tmaginic.net

Database contains ONLY .COM, .NET, .TV, .CC domains.

Owner Contact:
  Gottfried Lanz
  AVM
  Schulhausstrasse 2 1
  Oberwil-Lieli, 8966, CH

Punycode Name:  data-alliance.com
Unicode Name:   data-alliance.com

Admin Contact
  Gottfried Lanz
  AVM
  ****@a-v-m.ch
  Schulhausstrasse 2 1
  Oberwil-Lieli, 8966, CH
  phone: +49.566412056

Technical Contact
  Gottfried Lanz
  AVM
  ****@a-v-m.ch
  Schulhausstrasse 2 1
  Oberwil-Lieli, 8966, CH
  phone: +49.566412056

Zone Contact
  Gottfried Lanz
  AVM
  ****@a-v-m.ch
  Schulhausstrasse 2 1
  Oberwil-Lieli, 8966, CH
  phone: +49.566412056

Record expires on: 2008-04-06 16:34:08

Domain servers in listed order:

  ns1.sedoparking.com 217.160.95.94
  ns2.sedoparking.com 217.160.141.42
  
```

## Index of /etc/passwd

Name	Last modified	Size	Description
 <a href="#">Parent Directory</a>	31-Jul-2003 12:36	-	
 <a href="#">AT-admin.cgi</a>	31-Jul-2003 12:55	2k	
 <a href="#">Count.cgi</a>	31-Jul-2003 12:55	3k	
 <a href="#">CrazyWWWBoard.cgi</a>	31-Jul-2003 12:55	3k	
 <a href="#">Search.pl</a>	31-Jul-2003 12:55	9k	
 <a href="#">WSFTP.LOG</a>	31-Jul-2003 12:55	309k	
 <a href="#">YaBB.pl</a>	31-Jul-2003 12:55	5k	
 <a href="#">vti_inf.html</a>	31-Jul-2003 13:06	1k	
 <a href="#">access.log</a>	31-Jul-2003 12:55	141k	
 <a href="#">accounts.txt</a>	31-Jul-2003 12:55	22k	
 <a href="#">admin.db</a>	31-Jul-2003 12:55	51k	
 <a href="#">administrators.pwd</a>	31-Jul-2003 12:55	1k	
 <a href="#">administrators.pwd.i...&gt;</a>	31-Jul-2003 12:55	2k	
 <a href="#">adpassword.txt</a>	31-Jul-2003 13:07	1k	
 <a href="#">ad.cgi</a>	31-Jul-2003 13:07	2k	
 <a href="#">amadmin.pl</a>	31-Jul-2003 12:55	8k	
 <a href="#">auctionweaver.pl</a>	31-Jul-2003 13:10	9k	
 <a href="#">auth_user_file.txt</a>	31-Jul-2003 13:10	3k	
 <a href="#">authors.pwd</a>	31-Jul-2003 12:55	1k	
 <a href="#">authors.pwd.index</a>	31-Jul-2003 12:55	1k	
 <a href="#">backup</a>	15-Jul-2003 08:33	940k	
 <a href="#">bash_history</a>	31-Jul-2003 12:55	12k	
 <a href="#">bb-hist.sh</a>	31-Jul-2003 12:55	2k	
 <a href="#">bbs_forum.cgi</a>	31-Jul-2003 12:55	6k	

### Hardware Security

It is a common belief that all potential attacks are based around remote access and networks. This is far from the truth and some of the most lethal attacks are committed at the computer. Generally, computer hardware and configurations are very secure and provide ease of use for the user. This is a huge area of weakness in what could be a very security conscious system. Giving an attacker 30 seconds of access to a computer can result in masses of secure information being gained without the user's knowledge. This would also be the ideal time in which to prime the machine for future, more lethal attacks

By knowing how these attacks take place it is possible to introduce preventative action and secure all areas of potential weakness.



## IT/Computer Threat

## IT Threat

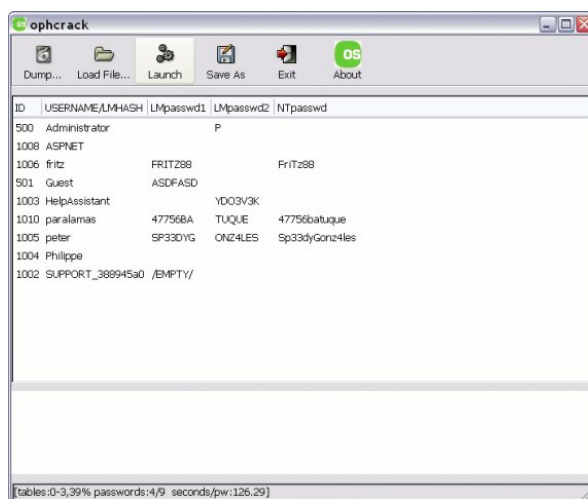
### Keyloggers



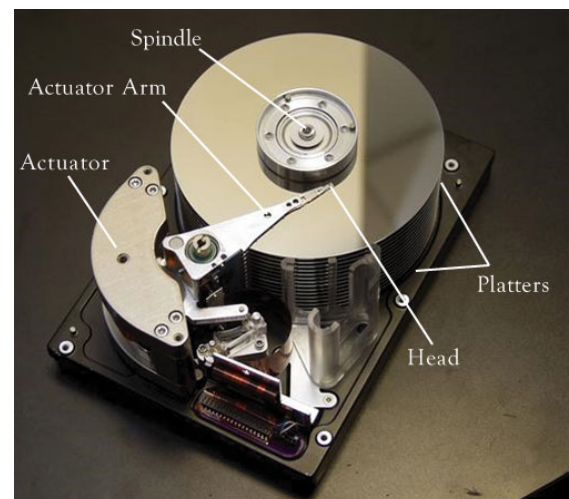
### USB Attack



### Password Cracking



### System Destruction



### Network Security

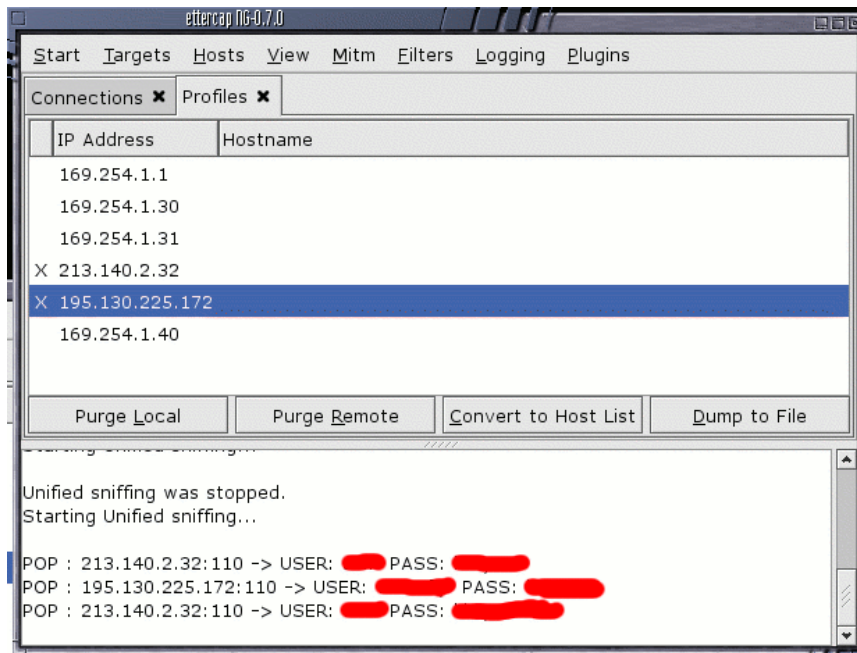
By the very nature of networks, fluid communication, they are generally an ideal target for potential attacks. With access to a mass of devices from one entry point, an attacker has the potential to gain information from many different sources.

#### Sniffing

An attacker is able sit on a network without the need to show his presence of actively attacking specific machines. Just by simply sitting on the network and watching the information passed around, it is possible to extract secure data and information for possible future attacks

## IT/Computer Threat

## IT Threat



### VoIP Attacks

Voice over Internet Protocol is becoming very popular due to the ease of mass installation and low cost. It is a very effective means of communication but also a potential hole in secure system. By sitting on the network, or leaving a small device monitoring the network, an eavesdropper is able to record all conversations as well as extract usernames and passwords. By being able to identify this weakness it is possible to provide measures to ensure a system is safeguarded.

```

sipcrack 0.1 ( majomu | www.remote-exploit.org )
-----
* reading and parsing dump file...
* found accounts:

num  server      client      user  algorithm  hash / password
1    192.168.19.81 192.168.19.120 500   plain      12345
2    192.168.19.81 192.168.19.120 500   plain      34after12
3    192.168.19.81 192.168.19.120 500   md5        d3bc10e4f2c9c275fe7da2f20f17600f
4    192.168.19.81 192.168.19.120 500   md5        e9827d8cda285252d5ce87ad8e3c64ca
5    192.168.19.81 192.168.19.120 500   md5        6524e36591b0dd77efa87cede26b4af3

* select which entry to crack (1 - 5): 3

* generating static md5 hash...1a24e68fa4904bd8ce0b7a2b37fffab2
* starting bruteforce against user '500' (md5 hash: 'd3bc10e4f2c9c275fe7da2f20f17600f')
* loaded wordlist: 'big-wordlist.txt'
* tried 8462686 passwords in 13 seconds
* found password: 'alb2c3'
* updating 'logins-sip.txt'...done
  
```

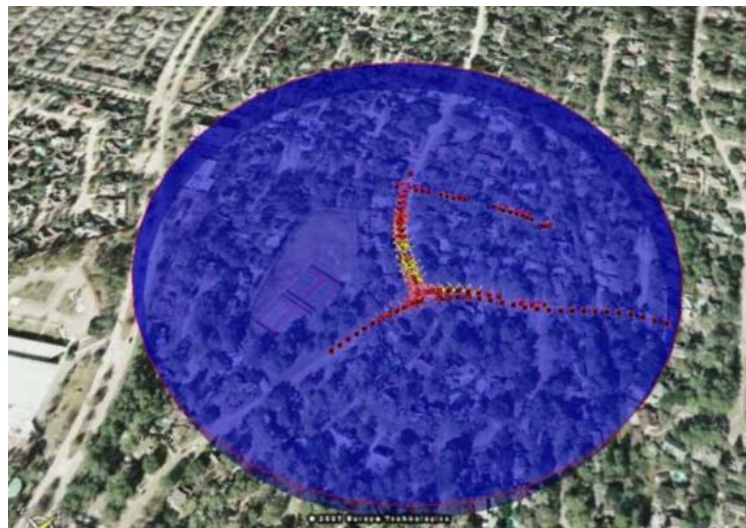
## IT/Computer Threat

## IT Threat

### Wireless Security

802.11 networks are now replacing the conventional structured cabling networks due to the ease of installation and cost effectiveness. By providing a wireless network, blanket covering an area, there are several security implications involved.

It is not always possible to prevent the network leaking out into the public domain. By not knowing where the network presence is, it is not possible to know whether it is possible for an attacker to be able to access the network from the public domain.



802.11 security poses one of the largest threats for IT. There are several security methods, some more secure than others. Without knowledge it is very easy to inadvertently use an insecure method. With wireless security being able to be broken within 10 minutes it is possible for an eavesdropper to have a presence on what you believe is a secure network.

```

C:\WINDOWS\system32\cmd.exe - aircrack.exe -x -0 checkpassword.ivs
aircrack 2.3
[00:00:02] Tested 2 keys (got 270169 IVs)
KB  depth  byte(vote)
0  0/ 1  63( 61) A2( 12) 08( 12) 39(  6) FB(  5) 74(  5)
1  0/ 1  68( 95) B2( 15) 3B( 13) 8A(  5) 44(  5) 0A(  5)
2  0/ 1  65( 43) F7(  8) 37(  8) 1D(  7) 6A(  5) 40(  3)
3  0/ 1  63( 98) B1( 15) 19( 12) CC(  5) BA(  5) 35(  5)
4  0/ 1  6B( 58) 6C( 12) FE( 12) 4F(  9) 02(  9) CB(  3)
5  0/ 1  70( 76) F8( 12) DE(  8) 8B(  6) 17(  5) 58(  5)
6  0/ 1  61( 75) C3( 15) 6E( 12) 9E( 10) 63( 10) 77(  8)
7  0/ 2  73( 34) 15( 26) 3D( 10) 72(  9) A7(  8) 9A(  6)
8  0/ 1  73( 87) E1( 15) B5( 12) B3( 10) DE( 10) E0( 10)
9  0/ 1  77( 99) 9B( 13) 36( 13) 0A( 12) 5D( 11) F6( 10)
10 0/ 4  6F( 22) 82( 13) F2( 13) 49( 13) DE( 10) 1A( 10)
11 0/ 1  72( 154) A9( 16) FB( 15) 73( 12) 5A( 11) C5( 10)
12 0/ 2  64( 30) BF( 25) DC( 10) 48( 10) 00( 10) 43( 10)

KEY FOUND! [ 63:68:65:63:6B:70:61:73:73:77:6F:72:64 ] (checkpassword)
Press Ctrl-C to exit.
  
```

## IT TSCM Course

## IT Course

### IT TSCM COURSE

The IT TSCM course is intended to provide participants with the necessary knowledge to help install countermeasures and proactive procedures within an IT Environment.

With a mixture of theory and hands-on practice the participants will be shown the common attacks in IT and, if possible, how to safeguard against them.

By the end of the course the participants will be able to:

- Identify sources of threats
- Identify threats
- Identify potential areas of weakness
- Recognize a threat/potential threat and provide countermeasures
- Perform 802.11 site surveys
- Perform cable and traffic analysis
- Structure security policies
- Perform basic penetration testing

Windows Password Cracking

Email Sniffing

Password Sniffing

Wireless Cracking

Website Defacement

Information Scavenging

Voice Over IP Interception

Physical Attacks

Network Attacks

Bluetooth Hacking

Mobile Phone Hacking

Methods in proactive protection and penetration testing will be taught, including User Authentication Methods, Encryption, Hardware Protection as well as practical hands-on deployment of the systems.

The latter part of the course is aimed at TSCM Products being used effectively in the field of IT

# IP/PABX Manipulation Software

# Training

## RECOMMENDED SOFTWARE

### INTRODUCTION

<u>Ref.</u>	<u>Model</u>	<u>Description</u>
1	Model 4011-01	Advance War Dialing Software
2	Model 4011-02	NetIntercept S200 Appliance
3	Model 4011-03	AccessData© Password Recovery Toolkit™
4	Model 4011-04	AccessData® Distributed Network Attack®
5	Model 4011-05	AccessData® Registry Viewer™
6	Model 4011-06	AccessData® Forensic Toolkit®
7	Model 4011-07	AccessData® Ultimate Toolkit™

As Internet gateway controls tighten, hackers are returning to an easier, often forgotten route into the network unsecured, back-door modems.

### OBJECTIVES

To identify any unauthorized modems connected to corporate systems that provide a route into the network by an attacker. To attempt to break-in through any modem or RAS server undetected. This is achieved by using software to dial through the company's telephone PBX range. Once systems are identified, attempts are made to breach the underlying OS and to attempt default account password logins.

### DESCRIPTION

While it is vital to secure your Internet perimeter, it's equally important to secure potential back-door routes into your network. Unauthorized or poorly configured modems connected to your systems could give an attacker direct access to your internal network.

In our experience modems are found on between 1% to 4% of corporate telephone lines. So for a DDI range of 1,000 numbers, we expect to see between 10 and 40 modems.

Routinely detecting the presence of unauthorized modems by a physical walk-through of office space and manual telephone dialing is impractical for most organizations.

War-dialing service is designed to solve this problem. Our service aims to train personnel to locate unauthorized modems and identify the type of system connected.

From here you can attempt to gain access to the corporate network through this point or simply flag up the modem to the client for investigation and remove it if necessary.





## Software Description

4011-01

### MODEL 4011-01 - ADVANCE WAR DIALING SOFTWARE

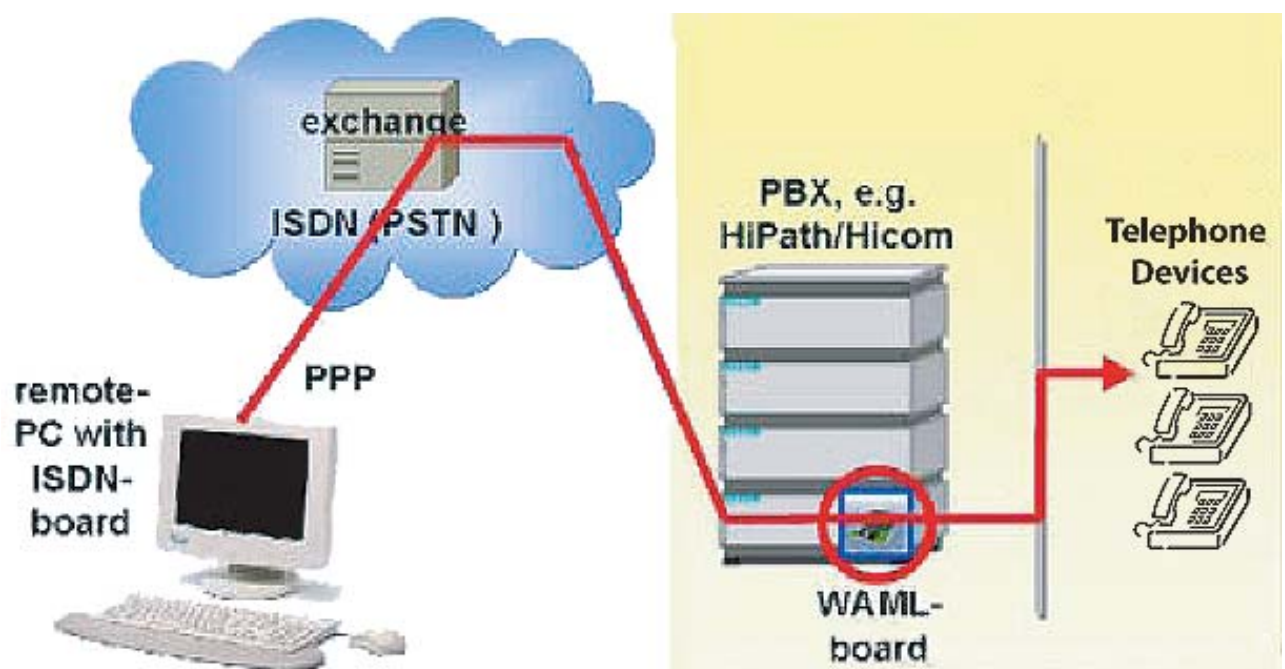
GASCAN is an on ISDN-based Dialer that uses the War dialer principle to call phone numbers. The call results are analyzed to identify the remote devices.

GASCAN allows you to:

- Perform security audits to identify vulnerabilities of external PSTN entry points like Modems, Fax, PCs, Router, Remote Access Systems, any ISDN application and Unified Messaging Systems
- Automate the revision of your PBX configuration and devices
- Check the implementation of your outsourced PBX and telecommunication infrastructure
- Document your telecommunication infrastructure for your facility management
- Optimize your telecommunication infrastructure
- Simulate heavy load for quality checks of your services and products

### SPECIAL FEATURES

- Least Cost Routing
- Support for using PBX switching technology
- Hides caller ID
- A remote control is possible by using Remote Access capabilities of the operating system
- One PCI or PCMCIA GASCAN adapter is included, that supports one ISDN BRI line with two b-channels.





## Software Description

4011-02

### MODEL 4011-02 – NETINTERCEPT S200 APPLIANCE

Capture, Analyze and Discover the Network Traffic Driving Your Business.

Detailed Information about the system can be found in the separate document

The S200 appliance running NetIntercept 3.0.2 includes

- 1 Intel P4 2.4 GHz CPU
- 1GB DDR266 MHz SDRAM
- 1 10/100 MB Ethernet Network Interface
- 1 10/100 MB Ethernet Network Interface Card
- 250GB SATA/150 7200 RPM drive, 8MB Cache
- 200GB usable by NetIntercept
- 2U Rack mount Case
- 52x24x52 CDRW

This position includes one year of software support and updates.

Due to the sensitive nature of this software we require an end user with his contact data due to export legislation, license and support issues.

### OVERVIEW



Most network monitoring tools cannot provide all the information that security professionals, IT managers, network administrators, auditors, software developers, and analysts need to know. The only way to richly and completely know how your network is being used is to capture the data packets and analyze them in detail.

Network consultants know the value of this information, even when it comes with a high manpower cost. They will run a packet Sniffer like TCPdump to capture raw network traffic into disk files, and then inspect the data with programs like strings. This yields only a brief and confusing glimpse into traffic data – and it is manually intensive and massively time-consuming. NETINTERCEPT (NI) is a network monitoring and analysis system.

## Software Description

4011-02

NETINTERCEPT is delivered as a complete system, with hardware and software pre-installed, ready to be placed in a machine room or NOC and plugged into the network at the firewall border.

To use NETINTERCEPT, an IT manager simply connects the system; no configuration is required to monitor and analyze traffic from the system's console. Unlike Intrusion Detection Systems (IDSs), it doesn't actively look at traffic and report events in real-time. Instead, it records all traffic on the hard drive, writing over the oldest information when the storage limit is reached. Thus, traffic from the last several hours, days, or weeks (depending on the size of your NETINTERCEPT configuration and average bandwidth) is available for study. Traffic is selected via the user interface, and then analyzed in batch mode. A typical user would begin a batch analysis:

- After noticing a traffic peak
- Because an event was logged by a network management system
- After receiving an alarm from an IDS, or
- As a core part of any overall security monitoring strategy

After an analysis, all network traffic in the selected interval becomes available to system administrators through an easy-to-use graphical user interface (GUI) and printed reports. NETINTERCEPT can be used either sparingly (an occasional half-hour to review recent alerts), or continuously (as part of a full-scale effort to optimize network infrastructure, monitor network usage, or study an attempted break-in). NETINTERCEPT lets users:

- Study an external break-in attempt
- Monitor correspondence and watch for confidential data being sent outwards
- Display the contents of a remote login or a web session
- Be aware of unusual or potentially troublesome traffic on the network
- Reconcile the relationships between hostnames and IP addresses in network traffic
- Use the GUI to interactively view traffic categorized or sorted by dozens of attributes, such as time of day, username, client and server machine identities, or session size
- Select connections of interest by criteria, such as keywords found in e-mail header fields, Ethernet addresses, TCP or UDP port numbers, file names, and Web Uniform Resource Identifiers (URLs)

### HOW NETINTERCEPT WORKS

NETINTERCEPT is designed to work in three major steps:

#### 1. Capture Network Traffic

- Packets are automatically captured from a 10/100/1000 BaseT LAN or compatible packet monitoring port on a high-speed switch
- Packets are stored on NETINTERCEPT's hard disk in TCPdump-format files. As new data is captured, it replaces older data on a first-in, first-out basis

## Software Description

4011-02

### 2. Analyze Network Traffic

- The user selects a time interval of interest, and the system protects data from that interval from being overwritten by new data
- Packets from the time interval are reassembled into individual data streams (sequences of related packets) and saved to disk
- Each data stream is passed through the NETINTERCEPT analysis engine, which attempts to recognize the protocols and content using a hierarchical set of parse modules. The parsing process allows NETINTERCEPT to detect spoofing by interpreting the content of data streams, rather than making a guess based solely on packet headers and port numbers
- NETINTERCEPT extracts search criteria so the user can readily find specific network transactions. The parse results and analysis conclusions are stored in a database

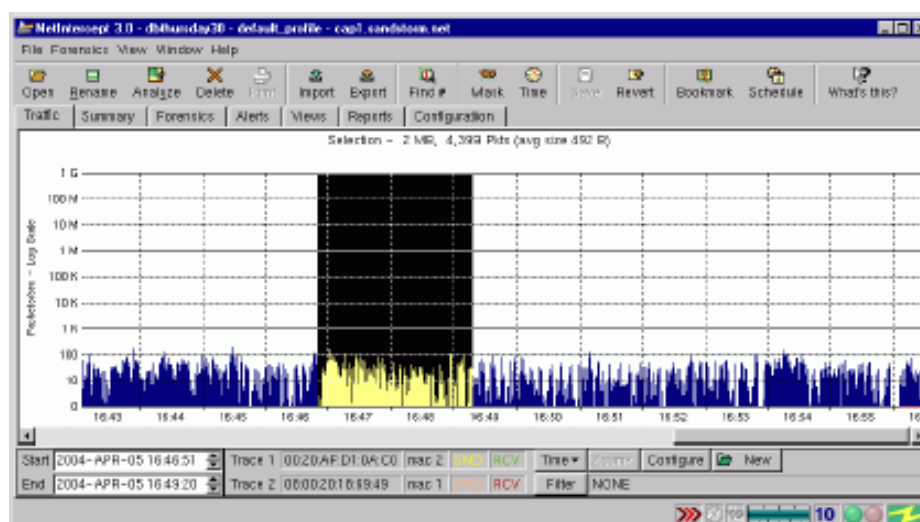
### 3. Data Discovery

- Users can browse interactively through NETINTERCEPT's results database using the GUI
- Users can instruct NETINTERCEPT to generate a variety of detailed reports from the current database

## CAPTURING NETWORK TRAFFIC

NETINTERCEPT captures network traffic using a modified UNIX kernel and a standard Ethernet interface card placed in intercept mode. The capture subsystem runs continuously, regardless of whether the GUI is active. Tests by Sandstorm have demonstrated a 99.9% capture rate on a fully-loaded 100Base-T network, and 99.99% capture rate on a lightly-loaded network.

Long term archival storage of captured data in NETINTERCEPT is accomplished by storing the raw dump files. The archived dump file can be written directly to a removable media device attached to the NETINTERCEPT machine, or transferred over the network to other machines for archiving. Because the file format is compatible with the Unix TCPdump utility, dump files captured by NETINTERCEPT can be transferred to other computers and analyzed with other tools, if desired.



## Software Description

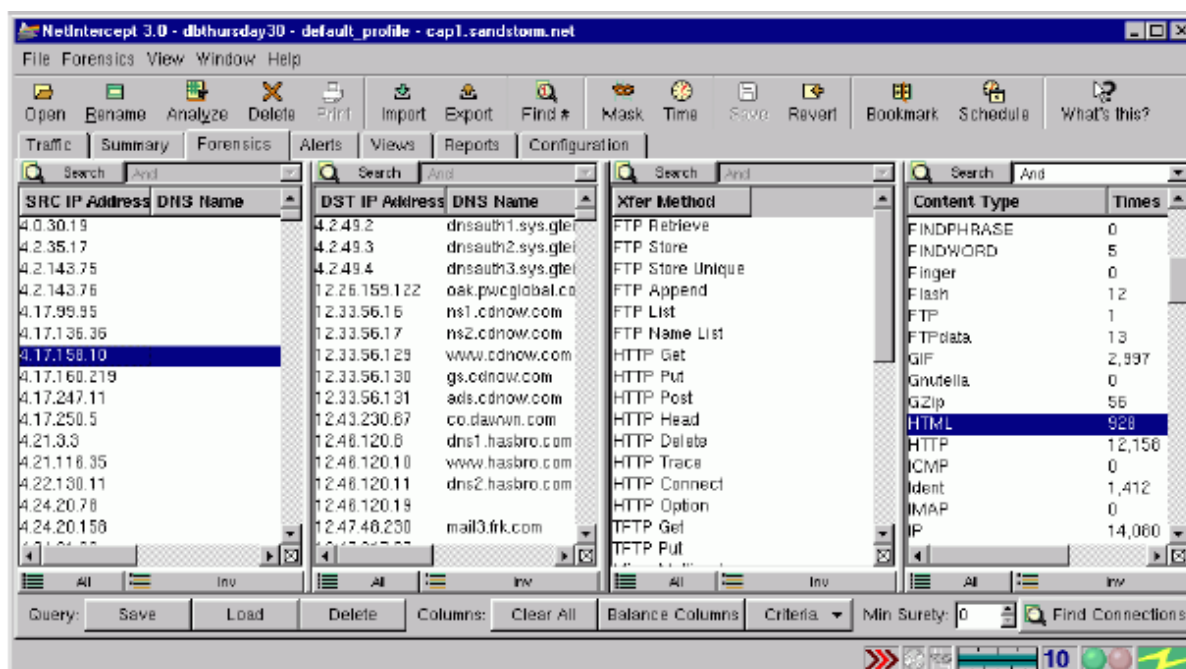
4011-02

### ANALYZING NETWORK TRAFFIC

NETINTERCEPT performs stream reconstruction on demand. When the user selects a range of captured network traffic to analyze, NETINTERCEPT assembles those packets into multiple streams. NETINTERCEPT can identify over 85 types of data streams, including FTP, HTML, telnet, e-mail with attachments, Microsoft documents (including Word, Excel, and PowerPoint), and nested data such as images or documents inside TAR files. Because the parser uses a nested hierarchy of modules – each specialized to parse a type of data – the architecture is very clean and easily extensible. The reconstructed TCP and UDP streams are then presented to the NETINTERCEPT analysis subsystem for identification.

The analysis modules are arranged in a tree structure. Each module specializes in a particular protocol, and may pass portions of the data stream both to child modules for lower-level analysis and back to parent modules in the case of compressed, packaged, or encrypted content. Modules that find data useful as search criteria or for statistical purposes extract and store that information in an SQL database.

File-like objects (web pages, e-mail attachments, etc.) encountered can also be stored. A pointer to the object and a unique code generated from an MD5 hash of the object are stored in the NETINTERCEPT SQL database, while the object itself is stored to the hard disk. By storing pointers, NETINTERCEPT saves each unique object only once, thereby saving disk space.



### BROWSING AND DISCOVERING

NETINTERCEPT stores a permanent record of all data traffic and the conclusions of its analysis, with links to supporting information. The NETINTERCEPT GUI displays information stored in this results database. The GUI can be used either via the system console, or remotely over a secure, encrypted X Windows connection to a display elsewhere.

## Software Description

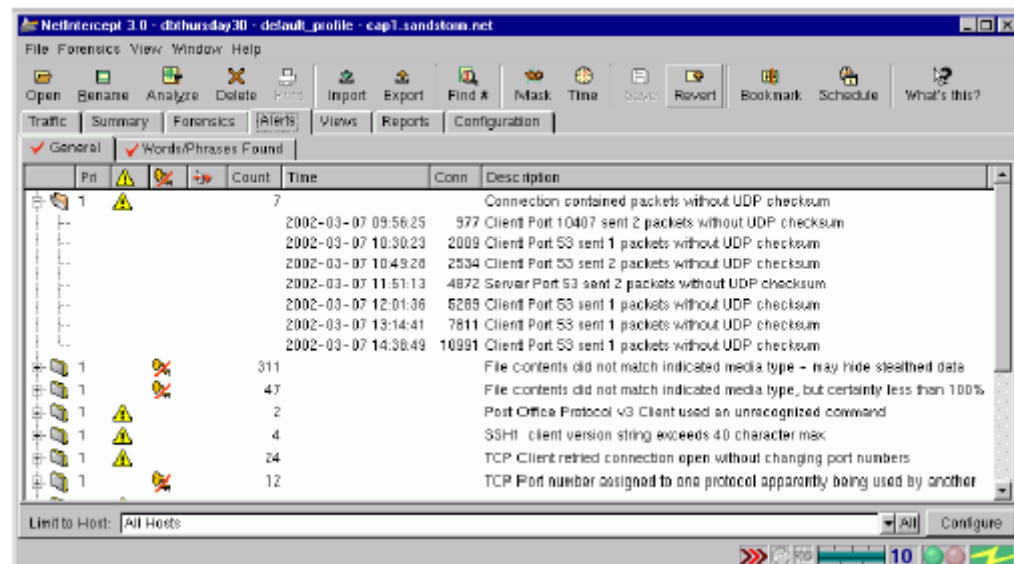
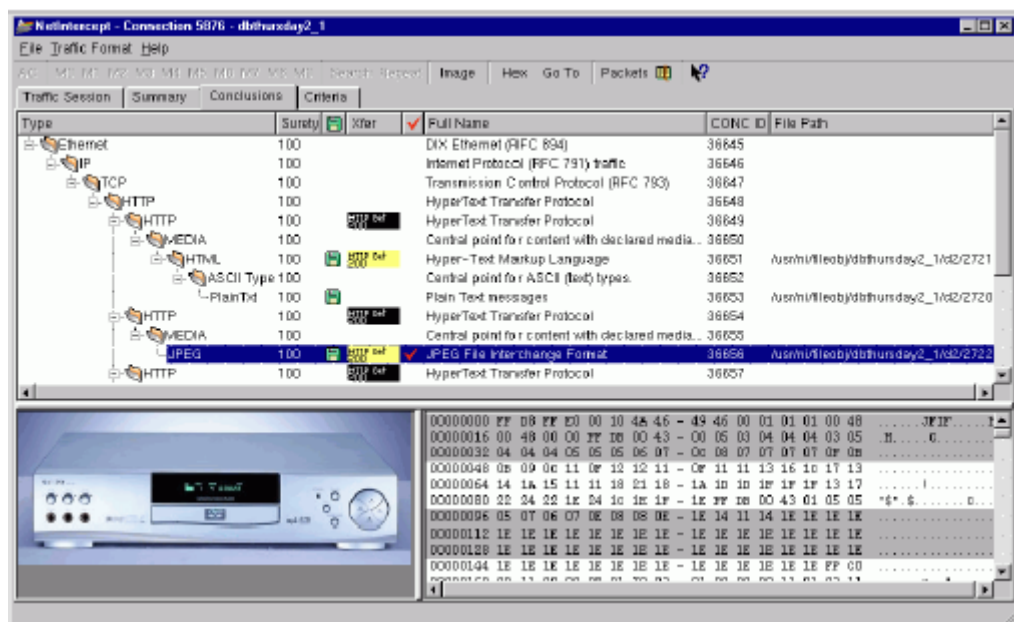
4011-02

- **Main Window.** This window contains tabs to allow the user to view summary information from the overall packet stream, then drill down for detail on the connection session
  - **Traffic Tab.** Shows an interactive display of network traffic volume over time
  - **Summary Tab.** Shows a big-picture overview and summary statistics for the current database
  - **Forensics Tab.** Allows selection (from lists of criteria such as content type or username) of network connections for deeper analysis in the Connection Examination window (described below)

## Software Description

4011-02

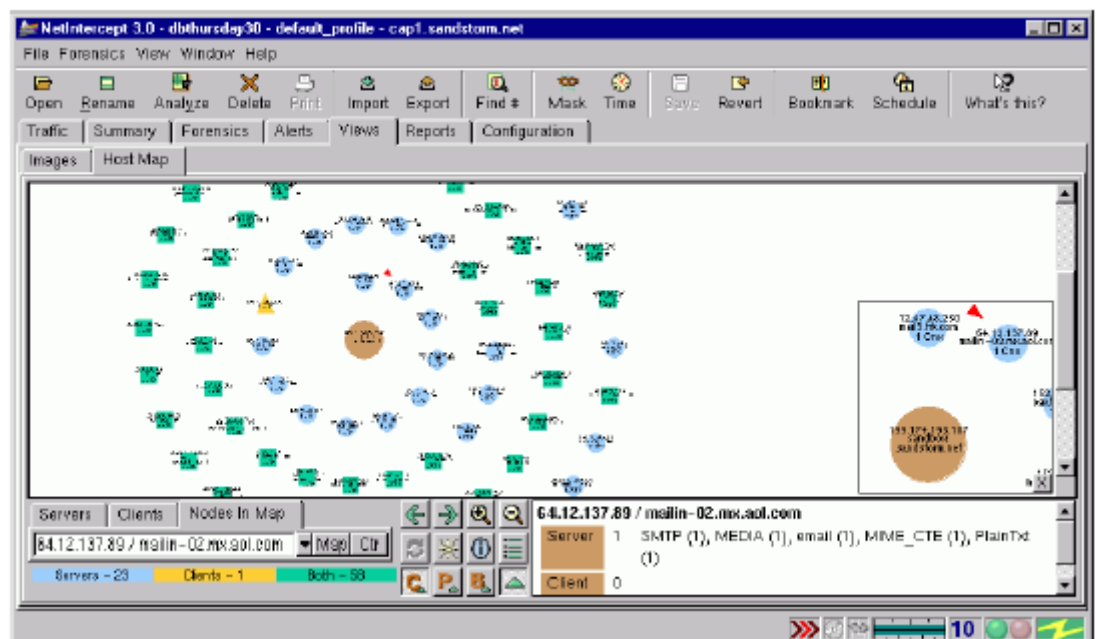
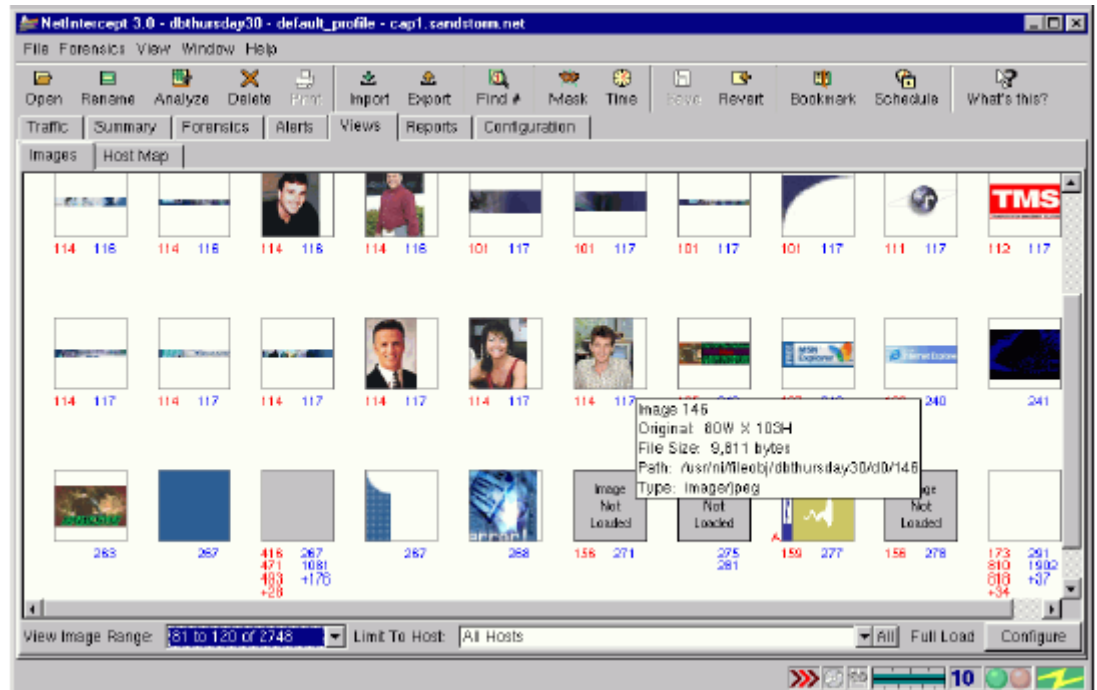
- **Alerts Tab.** Lists unusual or suspicious activities NETINTERCEPT has discovered, including attacks, security violations, and network errors.



- **Views Tab.** Displays thumbnails of all graphic images discovered in the packet stream. Allows browsing of host-to-host connections. Displays web pages reconstructed from network traffic

## Software Description

4011-02



- **Configuration Tab.** Controls data capture and analysis settings and defaults
- **Connection Examination Window.** Detailed information on a particular network connection
- **Traffic Session Tab.** Displays the actual data stream (and optionally packet headers) from the selected network connection
- **Summary Tab.** Displays traffic summary of the selected connection including search criteria values found
- **Conclusions Tab.** Contains results of NETINTERCEPT's content analysis and access to any file data elements found



## Software Description

4011-02

- **Criteria Tab.** Exposes Forensic search criteria that selected this network connection

Other windows of interest include Packet View, Web View, Image View, and Report View.

NETINTERCEPT also includes a variety of convenient and easy-to-use reports that users can generate in plain text or HTML format, or display through the NETINTERCEPT GUI. Each report is created from a template, which can be edited by the user to produce customized reports for specific applications. Report types supported in NETINTERCEPT include:

- **Traffic Reports.** Provide details of network traffic volume among machines on the monitored network
- **Content Reports.** Provide descriptions of content (such as web pages or email) that was part of your network traffic
- **Network Description Reports.** Provide summary information about your network
- **Focus Reports.** Show network traffic for a specific user, hostname, or IP address
- **Security and Protocol Hygiene Reports.** Show breaches in network security or network traffic anomalies

### **RUNNING NETINTERCEPT AUTOMATICALLY**

NETINTERCEPT contains scripting components to automatically save, parse, export, delete and report on traffic from the monitored network. These components can be assembled into shell scripts and scheduled to run on a timetable appropriate to the volume of traffic being monitored.

### **SSH AND SSL DECRYPTION**

NETINTERCEPT offers the capability to decrypt SSH sessions to and from systems that have been modified to support this activity using an asymmetric encryption key escrow mechanism. One copy of NI is capable of decrypting traffic from any number of SSH hosts so modified (provided that the traffic appears on the monitored network). This capability works with both SSH-1 and SSH-2 sessions. NETINTERCEPT also offers the capability to decrypt SSL sessions to and from SSL servers you control. This is accomplished by importing the server's private keys into NETINTERCEPT. One copy of NI is capable of decrypting traffic from any number of machines running correctly configured SSL servers (provided that traffic appears on the monitored network). This capability works with all versions of SSL up to 3.1 (TLS 1).

### **PRIVACY PROTECTION**

For more than twenty years, network monitoring tools have made it possible to covertly monitor data moving between computers over a network. NETINTERCEPT's ability to parse and understand data types is a valuable protector of individual privacy because it allows network managers to surgically examine data on a crowded network without accidentally viewing information that is unrelated to an investigation.

Specifically, NETINTERCEPT has the following privacy-protection features:

- Collects and graphically display network utilization, without analyzing the content of the traffic
- Selects suspicious or unusual traffic for display by hostname, protocol, or username, without viewing others' data

## Software Description

4011-02

- Views captured images without associated username information, unless desired
- Specifies what types of data will be analyzed in the traffic or stored in the permanent database
- Password-controlled access to the NETINTERCEPT hardware, software, and data
- Audit logging of all triggered analysis activities

### NETINTERCEPT CONFIGURATIONS

S series	For DMZs and simple analysis purposes	Captures up to 95 Megabits/second burst rate
		Parses up to 5 Megabits/second sustained average data rate
		Single P4 CPU
		Up to 95 GB data storage, 1 GB RAM
		(2)10/100 Ethernet interfaces for monitoring and control
		Standard 2U rack size
DR series	For extended performance	Increased capture and analysis rate with
		4 way RAID controller and Dual Intel XEON CPUs
		Up to 300 GB data storage, 1 GB RAM
		(2)10/100/1000 Ethernet interfaces for monitoring and control
		4U rack size
DRG series	For backbones and advanced requirements	Captures up to 300 Megabits/second burst rate
		Completely parses up to 10 Megabits/second sustained average
		data rate
		8 way RAID controller and Dual Intel XEON CPUs
		Up to 770 GB data storage, 3 GB RAM
		(2)10/100/1000 Ethernet interfaces for monitoring and control
		4U rack size

## Software Description

4011-03

### **MODEL 4011-03 - ACCESSDATA® PASSWORD RECOVERY TOOLKIT™ (PRTK™)**

The Password Recovery Toolkit is perfect for law enforcement and corporate security professionals. If you need access to locked files or if your users have simply locked themselves out of their files, the PRTK can get you back in.

#### **SECURITY RISK ASSESSMENT TOOL**

Many people use the same password to gain access to different programs and network login areas. This could be one of the weakest links in your organization's security profile! Some password protection schemes are easy to crack, while others are virtually impossible. But what if the same password is used for both programs? By gaining access to the weakest one you have gained access to the strongest one without the need to crack both.

#### **FEATURES**

- Enables password management
- Analyzes files and their passwords with an optional report file
- Recovers all types of passwords regardless of password length
- Analyzes multiple files at one time
- Recovers multilingual passwords
- Prevents unauthorized use with a personal security code
- Free technical support between 8:00 A.M. to 5:00 P.M. MST

## Software Description

4011-03

### PASSWORD RECOVERY MODULES

AccessData has a wide variety of individual password breaking modules that can help you recover lost passwords for almost every product in the industry.

#### Individual Password Breaker Modules

MS Access	Mail (MS)	QuickBooks
ACT!	MS Money	Quicken
Ami Pro	MYOB	WinRAR
Approach	My Personal check	Scheduler+
ARJ	Writer	Symphony
Ascend	Norton Secret Stuff	Versa Check
Backup	Organizer	MS Word
Best Crypt	MS Outlook	WordPerfect
Bullet Proof FTP	Palm	Word Pro
Cute FTP	Paradox	Adobe PDF
Data Perfect	PGP Disk File 4.0	Win95/Win98 PWL Files
dBase	PGP Secret Key Ring	IE Content Advisor
Encrypt Magic Fldr	Pro Write	W E_FTP
Excel	Project (MS)	Netscape Mail
FoxBASE	WinZip & Generic	Source Safe
File Maker Pro	Zippers	PC-Encrypt
Lotus 1-2-3	Q&A	
	Quattro Pro	

## Software Description

4011-04

### **MODEL 4011-04 - ACCESSDATA® DISTRIBUTED NETWORK ATTACK® (DNA®)**

#### **PUTTING IDLE TIME TO WORK**

Guaranteed recovery of lost passwords for MS Office 97/2000 products including Word and Excel; now includes Adobe Acrobat (PDF) file decryption! DNA puts idle time to work.

Distributed Network Attack, or DNA, is a new approach to recovering password protected files. In the past, recoveries have been limited to the processing power of one machine. DNA uses the power of machines across the network or across the world to decrypt passwords.

The DNA Server is installed in a central location where machines running DNA Client can access it over the network. DNA Manager coordinates the attack, assigning small portions of the key search to machines distributed throughout the network. DNA Client will run in the background, only taking unused processor time.

#### **FEATURES**

- Easy to read Statistics and Graphs
- Add user dictionaries
- Optimization for password attacks for specific languages
- Customize user dictionaries
- Stealth client installation functionality
- Automatic Client update when updating the DNA Server
- Control what clients work on certain jobs

#### **SUPPORTED FILE FORMATS**

##### **Recovers and Decrypts**

- ARJ
- MS Word and Excel (97 & 2000)
- PDF 1.4 and below

##### **Recovers a Password**

- Office XP
- PGP Disk 4, 5, 6
- Pkzip
- RAR up to version 2.9 of WinRAR-WinZip

## Software Description

4011-05

### MODEL 4011- 05 - ACCESSDATA® REGISTRY VIEWER™

The Access Data Registry Viewer gives you the ability to view independent Windows registry files. Using the Registry Viewer provides access to the “Protected Storage System Provider” key, which contains e-mail and Internet passwords and settings. Easily generate reports containing valuable data from Registry keys of interest. The Registry Viewer includes a USB or parallel dongle to restrict unauthorized use.

#### FEATURES

##### Access and Decrypt Protected Storage Data

- AutoComplete “form” data from Google, Yahoo, and more
- Internet Explorer account login names and passwords
- Outlook and Outlook Express account information including servers, users, and passwords

##### View Independent Registry Files

- Access User.dat, NTUser.dat, Sam, System, Security, Software, and Default files
- Opens all versions of Windows Registry files
- View files individually without reconstructing the full Registry

##### Report Generation

- HTML reporting capabilities
- Easily integrates with Forensic Toolkit case reports

##### Integrates with AccessData’s Forensic Tools

- Seamlessly load Registry files directly from the Forensic Toolkit into the Registry Viewer
- Generate password lists for use with Password Recovery Toolkit
- Access Data® Forensic Toolkit®

The Access Data Forensic Toolkit® (FTK™) offers law enforcement and corporate security professionals the ability to perform complete and thorough computer forensic examinations. The FTK features powerful file filtering and search functionality. FTK's customizable filters allow you to sort through thousands of files to quickly find the evidence you need. FTK is recognized as the leading forensic tool to perform e-mail analysis.

##### Easy to Use

- View over 270 different file formats with Stelent's Outside in Viewer Technology
- FTK Explorer allows you to quickly navigate through acquired images
- Generate audit logs and case reports
- Compatible with the Password Recovery Toolkit™ and Distributed Network Attack®.

## Software Description

4011-05

### Advanced Searching

- Full text indexing powered by dtSearch® yields instant text search results
- Advanced searches for JPEG images and Internet text
- Locates binary patterns using Live Search
- Automatically recovers deleted files and partitions
- Targets key files quickly by creating custom file filters.

### Supported File & Acquisition Formats

- File formats include: NTFS, NTFS compressed, FAT 12/16/32, and Linux ext2 & ext3.
- Image formats include: Encase, SMART, Snapback, Safe back (up to but not including v.3), and Linux DD.

### E-mail & Zip File Analysis

- Supports: Outlook, Outlook Express, AOL, Netscape, Yahoo, EarthLink, Eudora, Hotmail, and MSN e-mail.
- Views, searches, prints, and exports e-mail messages and attachments.
- Recovers deleted and partially deleted e-mail.
- Automatically extracts data from PKZIP, WinZip, WinRAR, GZIP, and TAR compressed files.

### Known File Filter™ (KFFTM)

- Identifies and flags standard operating system and program files.
- Identifies and flags known child pornography and other potential evidence files
- Includes hash datasets from NIST and Hash keeper
- Coming soon! Create your own custom hash sets.

### Registry Viewer™

- Accesses and decrypts protected storage data
- Views independent registry files
- Reports generation
- Integrates with Access Data's forensic Tools
- Access Data© One Year Subscription Features
- Constant access to cutting edge technology.
- No hassle with individual upgrades.
- Web-updates for the Forensic Toolkit



# TSCM INDEX



1 - Introduction

2 - The Threat

3 - Recommendations

4 - Training Course Overview

5 - Training Course Syllabuses

6 - Recommended Products

7 - Technical Data Sheets

8 - IP/PABX Manipulation

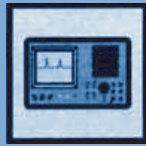
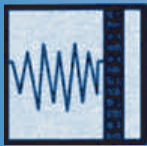
9 - Commercial Quotations

10 - Terms & Conditions

11 - Contact Details

12 - Elaman Catalogs Overview

# TSCM INDEX



1 - Introduction

2 - The Threat

3 - Recommendations

4 - Training Course Overview

5 - Training Course Syllabuses

6 - Recommended Products

7 - Technical Data Sheets

8 - IP/PABX Manipulation

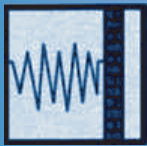
9 - Commercial Quotations

10 - Terms & Conditions

11 - Contact Details

12 - Elaman Catalogs Overview

# TSCM INDEX



1 - Introduction

2 - The Threat

3 - Recommendations

4 - Training Course Overview

5 - Training Course Syllabuses

6 - Recommended Products

7 - Technical Data Sheets

8 - IP/PABX Manipulation

9 - Commercial Quotations

10 - Terms & Conditions

11 - Contact Details

12 - Elaman Catalogs Overview

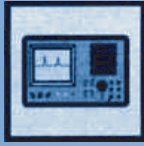
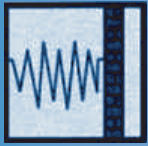


If you would like further Information about ELAMAN,  
or would like to discuss a specific requirement or project, please contact us at:

**Elaman GmbH**  
**German Security Solutions**  
**Seitzstr. 23**  
**80538 Munich**  
**Germany**

**Tel: +49-89-24 20 91 80**  
**Fax: +49-89-24 20 91 81**  
**info@elaman.de**  
**www.elaman.de**

# TSCM INDEX



1 - Introduction

2 - The Threat

3 - Recommendations

4 - Training Course Overview

5 - Training Course Syllabuses

6 - Recommended Products

7 - Technical Data Sheets

8 - IP/PABX Manipulation

9 - Commercial Quotations

10 - Terms & Conditions

11 - Contact Details

12 - Elaman Catalogs Overview

# Overview of Elaman Catalogs



## ABOUT US

More than 10 years of experience in communication and security requirements for law enforcement agencies convinced us of the need to establish ELAMAN GmbH in 2004, specializing in security requirements for government and law enforcement authorities worldwide.

ELAMAN GmbH, established in 2004, provides advanced integration systems, international consultancy and strategic technologies in Communications Systems, National Security, and Defense. The highly experienced international managers from different sectors focus to provide the solution to enable our customers to be more than adequately equipped to counter the threat of today and tomorrow.

ELAMAN is a German based company with its headquarters in Munich/Germany. Our aim is to provide comprehensive security products and solutions, technical consultancy and services as well as professional training for our customers in Europe, the Middle East, Far East and Africa.

- Technical Consulting
- Professional Audio & Video Surveillance Products
- VIP Protection & Specialists Detection
- Monitoring- and Tracking Systems, Spectrum Monitoring
- Counter (Anti-) Surveillance
- Specialist Training
- Intelligence Software

ELAMAN is a leader in International marketing and trading, specializing in defense technology, communications and security. Through strategic partnerships with many leading international companies, we provide Law Enforcement Agencies alike with unique technology solutions.

An essential element of our philosophy is the conviction that training and the understanding of products and technology are critical factors and major strengths in assuring successful security solutions.

Our vast experience and services for well known companies, such as Siemens, Alcatel, Ericsson, Rohde & Schwarz, Spectronic, and others, has enabled us to handle even the most challenging and complex requirements and offer solutions that meet the relevant needs of Lawful Enforcement Agencies in the Middle East, Africa and Asia.

Consequently, we have the expertise to offer solutions using state of the art technology and comprehensive functions for flawless operation, training and services.

## CONFIDENT RELATIONSHIP

Confidentiality is essential in the business of security. ELAMAN can guarantee this as a German company and can furthermore be your sole interface with the manufacturers of security products and services. ELAMAN's business approach is to treat our customers as full partners in a relationship which is beneficial to both parties.

This goal outwards to our customer will be represented by:

**Holger Rumscheidt** as Managing Director and **Eugen Fissl** as Consultant and Partner.