



INVESTIGATIONS, SECURITY, &
COUNTERMEASURES

www.kimmonsinv.com

Texas State License # C04124

713-532-5881

TSCM and DEBUGGING CASE STUDIES

TSCM, Technical Surveillance Counter Measures and Debugging Case Study #1:

1 THE CLIENT & REQUIREMENTS

We were contacted by a major energy firm with worldwide operations and an employee who brought possible corporate espionage to the attention of top level management. The client minimized involvement of upper management in working with us because the employee indicated upper level misconduct.

The indications were that critical and proprietary information was getting out to a single competitor employing past members of our client's management. The suspected person was an Executive Vice President, so this was a sensitive and covert countermeasures and debugging operation. Sensitive and highly valuable seismic information was getting out of the company. This included surveys, and geological and seismic studies that help energy companies to locate areas with oil and gas deposits justifying a full scale drilling operation.

The client wanted Kimmons Investigation Services, Inc. to pinpoint how information was leaking and leverage our investigative skills in getting to the root of all spying and determining the extent of the damage and all people involved. Unlike many TSCM, Technical Surveillance Countermeasures, companies, Kimmons Investigations employs trained investigators, many previously employed by the government or police forces. This allows us to not only discover and dismantle covert surveillance, but also to investigate those involved and discover other possible threats through that investigation.

2 WHERE WE SWEEPED FOR BUGS

We concentrated on the executive offices of not only the suspected person, but also all other top level management personnel. This isn't necessarily due to a suspicion that others were involved. We must determine everywhere the suspected spy may have located bugs and covert surveillance gear to monitor communications and steal vital information.

3 WHAT WE USED — EQUIPMENT

Oscor Spectrum Analyzer



This highly sophisticated analyzer is quite expensive, and many TSCM companies simply do not expend the funds to employ it. The problem is that it's one of the most effective tools available to scan spaces for radio frequency and other bugs based on their emissions and transmissions.

Using this tool, we are able to ascertain that device(s) exist, and sometimes their exact location. However, just knowing they're present, we can employ another highly effective tool to zero in on their precise locations.

Non Linear Junction Detector

A Non-Linear Junction Detector detects the presence of electronics, regardless of whether the electronic target is radiating, hard wired, or even turned off.

The ORION 2.4 locates hidden electronics in walls, floors, ceilings, fixtures, furniture, or containers. An antenna-mounted line-of-sight display lets the operator focus on the target while sweeping. The NEW ORION 2.4 transmits at 2.4GHz frequency for detecting small electronics such as SIM cards and cell phones.



4 WHAT WE FOUND — SWEEP & INVESTIGATION

In our sweep of the executive offices, we found a phone tap on the CEO's phone. This tap enabled the covert recording of any or all conversations the CEO had over the phone. We pinpointed the location of the bug and eliminated it. Most TSCM companies would be done at this point, leaving further investigation of the suspected party up to others or law enforcement.

Kimmons Investigation Services, Inc. is a full service TSCM and private investigations company. We moved forward at the request of the client with interviews of the VP as to why he was engaged in these activities and where the information was being delivered. It seems that he was funneling information to another new company formed by ex-employees of the client. They were paying handsomely for the information, but there was more.

This Executive VP, other than the money motive, was focused on helping to build up the competitor company and leaving to run it at some point in the near future. This operation was well-planned and executed covertly. Small mistakes led to another employee's suspicions, and this employee started the ball rolling with a tip to management.

If you have concerns about leaks of proprietary information in your organization, call or email us immediately for a private consultation to determine how we can help.

TSCM, Technical Surveillance Counter Measures and Debugging Case Study #2 Executive Summary:

Dear [REDACTED]:

Enclosed is a copy of our Report of Technical Surveillance Countermeasures Survey (TSCM) covering our activities on your behalf on [REDACTED] at [REDACTED], Houston, Texas 77056. If you require further discussion on any of the presented material, please feel free to contact me at any time.

Thank you for your confidence in our services

Sincerely,

KIMMONS INVESTIGATIVE SERVICES, INC

REPORT OF EAVESDROPPING COUNTERMEASURES SURVEY

On Friday, January 25, 2013, a requested Eavesdropping Countermeasure Survey (TSCM) was conducted on the residence located at [REDACTED], Houston, Texas 77056. The survey was accomplished by a team of Investigators/Technicians from **KIMMONS INVESTIGATIVE SERVICES, INC., Houston, Texas.**

SCOPE AND FINDINGS

TELEPHONES

Scope: No telephone instruments were tested.

Findings: NA

RADIO FREQUENCY ANALYSIS

Scope: A Radio Frequency Spectrum Analysis was conducted between the frequencies of 20 KHz and 3 GHz for detection of clandestine transmitters. An REI OSCOR 5000-E, REI CPM-700, and other associated equipment was utilized.

Findings: No active radio frequency eavesdropping transmitter signals were observed.

CARRIER CURRENT TRANSMISSION

Scope: A search for carrier current transmission was conducted on all phases of the power lines in the target area.

Findings: No discrepancies were noted.

PHYSICAL INSPECTION

Scope: A detailed physical search was performed in the target area to include inspection of interiors, surfaces, furniture, ventilation ducts, pictures and artifacts.

Findings: No discrepancies were noted.

INFRARED TRANSMISSIONS

Scope: A search for infrared transmissions was conducted in the target area.

Findings: No active infrared eavesdropping transmission signals were observed.

WIRELESS CAMERA DETECTOR / LOCATOR

Scope: A search for wireless cameras was conducted in the target area. A WVS1000 (900-2520MHz) was utilized.

Finding: No active wireless cameras were detected in the target area.

LIMITATION

Technical countermeasures surveys of the type conducted indicate the status of the area inspected at the time of the conclusion of the survey. Admission to the searched area of unauthorized personnel by employees / cleaning crews or failure to maintain continuous and effective control of the searched area, allowing repairs or alterations to or within the searched area without the supervision of responsible personnel, or the introduction of new furnishings into the searched area prior to the completion of a thorough inspection of such furnishings will nullify the security afforded by this survey.

TSCM, Technical Surveillance Counter Measures and Debugging Debugging Case Study #3:

I received a call from a professional woman going through a divorce. She and her husband, also a business professional, had adjacent offices, and she was concerned that he might be spying on her to gain an edge in the divorce.

He was a psychologist, and she had a professional head-hunting business. She felt that their offices right next door to each other could make it easy for her husband to place a listening device or other eavesdropping to “gather dirt” on her. Of course, there was no dirt to gather (well, maybe not), but she wanted us to do some checking for bugs.

One day when her husband wasn’t in his office, I and one of my technicians made a trip to her office and unpacked our gear to do some detecting. The first thing that jumped out was that both offices shared the same telephone equipment room.

All of the business telephone lines converged into one phone box in that telephone room. This is normally a red flag in any multiple office building, as it’s too easy to tap phone lines when you can do it where the surveilled party never goes. Often, they don’t even know the room exists.

We started checking each phone line and it didn’t take long to find a problem. Hidden in the ceiling of the telephone room and connected to one of the phone lines was a tape recorder!

These type of setups are easy and cheap, so they're often used by non-professionals to record phone conversations. They simply run down to Radio Shack and buy an "activator" for \$25-\$30. The activator device is connected to the phone line and the recorder.

Its name comes from the "activation" of the recorder when someone opens the circuit and begins to use any phone on that extension. The phone receiver is picked up, and the recorder is started. It stops recording when the phone is hung up.

We were feeling pretty good, as our equipment had proved itself, and we were about to make our client happy and solve her eavesdropping problem ... or so we thought.

I proudly escorted our client into the phone room and showed her the device. I told her we hadn't checked the lines yet to see which one of her lines her soon-to-be ex-husband had tapped, but we'd get right on it. My happy moment was dimming because she seemed surprised and nervous.

I asked her what was wrong, as we were about to solve her eavesdropping problem. You can't make this stuff up. She told us that she had that device placed and tapped into her husband's office phone!

Inadvertently, my client had placed me and my firm in a precarious position. In the state of Texas, recording a phone conversation is legal only if one party to the conversation is aware that it is being recorded. Both need not know. But, in this case, every conversation between her husband and anyone except her was being illegally recorded. Neither party was aware of the tap, a felony in Texas!

This took some thought, as I now knew about a felony crime committed by my client. The proper approach would be to call the police and turn her in for the crime. Of course, it's not great client relations to send them to jail, and you rarely get paid when you do.

Could it get any worse? YEP! I asked her who had installed the device. It turned out to be another PI, an ex-police officer and a personal friend of mine. He operated a one-man business, but I never knew him to cross legal lines like this.

I couldn't bring myself to turn both my client and my friend into the police. I was pretty rough with her in telling her that if she had any sense she wouldn't do anything like this again. I took the equipment with me, leaving no bugs in the offices.

It's no wonder that she was suspicious that her husband would spy on her. It was in her nature. As I said, divorce cases aren't usually much fun, but they sure can be interesting!

INVESTIGATIONS, SECURITY, & COUNTERMEASURES

www.kimmonsinv.com

Texas State License # C04124

713-532-5881