

Kestrel Technical Journal

Kestrel TSCM[®] Professional Software

TECH-2016-08-01-001

Technical Research and Standards Group (TRSG)

Paul D Turner, TSS TSI

The Kestrel TSCM[®] Professional Software holds many secrets that oftentimes are only discovered during advanced technical operator certification training conducted in an instructor led classroom environment.

Kestrel has many subtle features that often only reveal themselves to the technical operator by accidental discovery, or as noted above taught during instructor led operator certification training.

One of these little gems is the ability of the Kestrel TSCM[®] Professional Software to automatically predict and select the correct IF bandwidth of the Signal of Interest (SOI) and allow the technical operator to quickly enter the | **DEMODULATION** | process by quickly and effectively selecting | **DEMODULATE** | from a quick select menu structure.

This technique is accomplished when the technical operator first selects one (or perhaps more) Signals of Interest (SOI) manually during the signal analysis and spectrum review process, and works in both an active runtime environment and when viewing a historical Kestrel Project File (KPF) in an active display mode.

Once the technical operator has selected at least one (1) Signal of Interest (SOI) and it is currently displayed on the user-interface, the SOI selected, is placed on the Master Automatic Threat List (ATL), and is flagged on the RF Spectrum Display (RSD) in | **ORANGE** | colour for easy identification as an operator selected / added Signal of Interest (SOI).

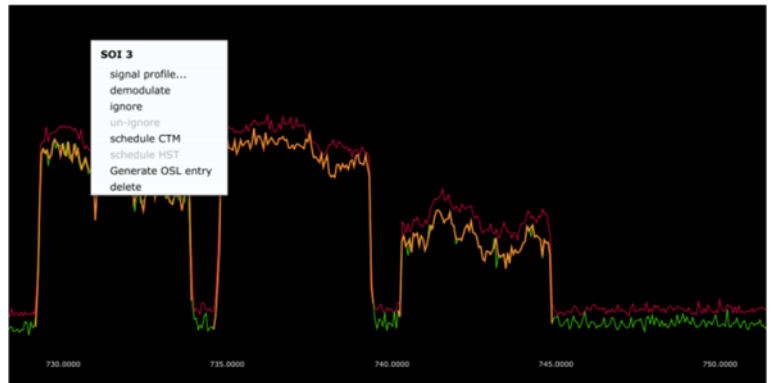
Each SOI selected is independently assigned a unique SOI database ID automatically.

To enter the | **DEMODULATION** | process for any of the signal events flagged by the technical operator as a Signal of Interest (SOI), simply right mouse click on the SOI as displayed.

On the right mouse click pop-up menu the technical operator can directly select the | **DEMODULATE** | menu option |ON | OFF | as required.

Kestrel will immediately enter the | **DEMODULATION** | mode based on the SOI | **CENTRE FREQUENCY** | at the correct | **IF BANDWIDTH** | for the Signal of Interest (SOI) selected.

Consider the following example to better illustrate the technique.



The technical operator has selected three (3) separate signal events during active runtime as Signals of Interest (SOI), and has utilized a right mouse click for the signal event on the left | **SOI 3** | revealing a pop-up menu, with a number of menu options available.

Selecting the | **DEMODULATE** | menu option, results in Kestrel[®] immediately entering the | **DEMODULATION** | process at the correct | **IF BANDWIDTH** | without the necessity of any further operator input.

Once the | **DEMODULATE** | menu option is selected, the | **IF BANDWIDTH** | filter shading will appear for the select Signal of Interest (SOI) and demodulation is immediately active.

Once the technical operator has completed the review and analysis of the selected Signal of Interest (SOI), the demodulation process may be terminated by again accessing the right mouse click menu structure a second time and selecting the | **DEMODULATION OFF** | option.

However, there is one more little gem worthy of discussion that many technical operators might not be aware of, or fully understand.

Kestrel TSCM[®] Professional Software

Managing Tomorrows Threat Model | Today!

Professional Development TSCM Group Inc.

Technical Security Branch (TSB)

The | **IGNORE** | and ultimately | **UN-IGNORE** | menu options that appear on the right click menu structure can be utilized to identify any Signal of Interest (SOI) that has been actively reviewed by the technical operator and determined to be of a friendly nature.

The technical operator can select the | **IGNORE** | menu option, which visually identifies the SOI has having been processed by the technical operator.

The SOI will be flagged on the user-interface and on the Master Automatic Threat List (ATL) for easy identification of | **IGNORED** | signal events.

This technique can be used during the analysis and review process to quickly differentiate between Signals of Interest (SOI) that have been reviewed and those that have not yet been manually reviewed by the technical operator or a technical analyst.

When a Signal of Interest (SOI) is | **IGNORED** | it can be printed as a separate user signal list within the Session Report Generator (SRG).

At any time the technical operator is able to reverse the status by selecting the | **UN-IGNORE** | right click menu option should it later be determined that the SOI requires further technical analysis and review, or perhaps needs to be elevated to a higher threat category based on new information.

“With each new edition of the “Kestrel[®] Technical Journal”, we will reveal yet another essential, need to know feature and any related sub-feature components that bring additional operator-centric functionality, value and convenience to the surface. If you have not yet attended formal Kestrel TSCM[®] Professional Software Technical Operator Certification Training, we strongly recommend that you consider training as an essential and integral component of professional development as a Kestrel[®] Technical Operator”.



Canadian Technical Security Conference (CTSC)

A World of Opportunity – On Both Sides!

It has never been easier for individuals and state players to engage in economic-espionage activities targeting businesses, organizations and governments worldwide. There are many avenues of attack, any one of which has the potential to compromise valuable information. Yet, although annual losses from economic-espionage are immense, many potential targets are largely unaware of the threat - indeed, the victims often have little or no awareness that they have been successfully targeted.

Contrast this situation with the realities facing those tasked with technical security. Even highly trained and experienced technical operators are hard pressed to keep on top of the rapidly evolving threat environment. Up to date knowledge of the actors, their tools and methods, coupled with the specialist expertise needed to identify and pro-actively counter threats, is a necessity. Consequently, it is important for the technical security practitioner to leverage the expertise resident in the Technical Security community of practice through participation in relevant activities such as the annual Canadian Technical Security Conference (CTSC).

The CTSC, now in its 12th year, is a focused technical security event that brings together professional technical operators and others having a range of related interests. This year's conference has a special focus on the threat of economic-espionage with emphasis on the means for combating it. Over a three-day period, participants will acquire relevant theoretical and practical knowledge, including opportunities for hands-on experience with Technical Surveillance Countermeasures (TSCM), a vital, but often over-looked, line of defence for safeguarding information in a technological world.

Participation in activities, such as the Canadian Technical Security Conference (CTSC), positions technical operators and knowledgeable clients to identify potential and actual security compromises and respond appropriately. It just might be an investment that will pay off by helping prevent or limit damage to your organization.

| www.pdtg.ca | www.kestreлтscm.com | www.ctsc-canada.com |

Kestrel TSCM[®] Professional Software is innovative industry leading, disruptive technology, now sold in 25 countries worldwide.