



Network Traffic Exploration Application

Presented By Grant Vandenberghe

Grant.Vandenberghe@drdc-rddc.gc.ca

(613) 991-6464



Defence Research and
Development Canada

Recherche et développement
pour la défense Canada

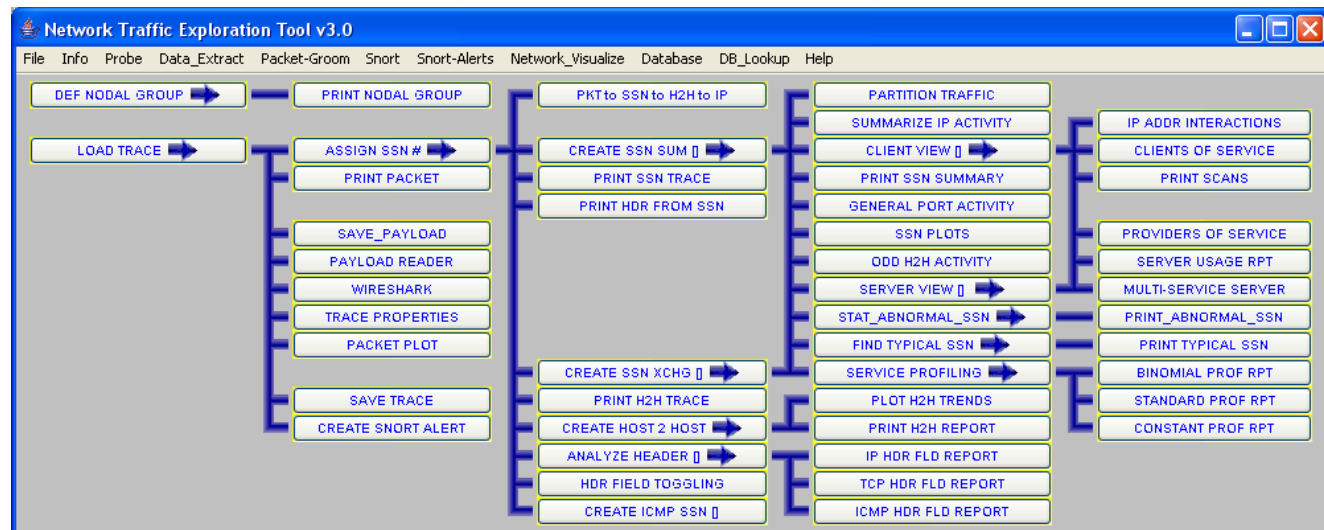
Canada¹



Introducing the NTE

The Network Traffic Exploration (NTE) application allows the user to explore network traces and prototype new detection algorithms.

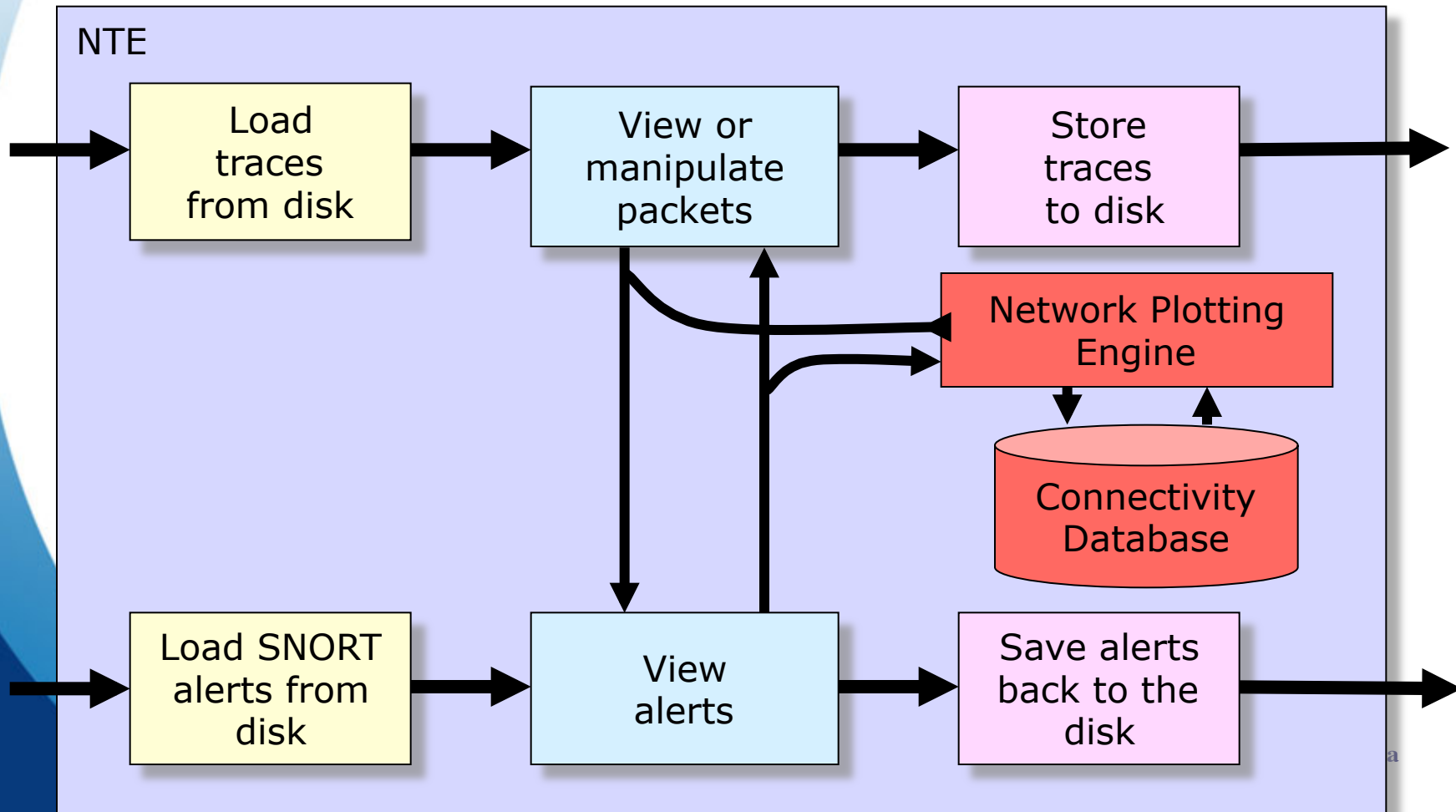
The NTE is useful for security analysts because of its varied and flexible presentation capabilities.





NTE Architecture

The NTE is a MATLAB application has been developed on top of an open library of packet analysis functions.

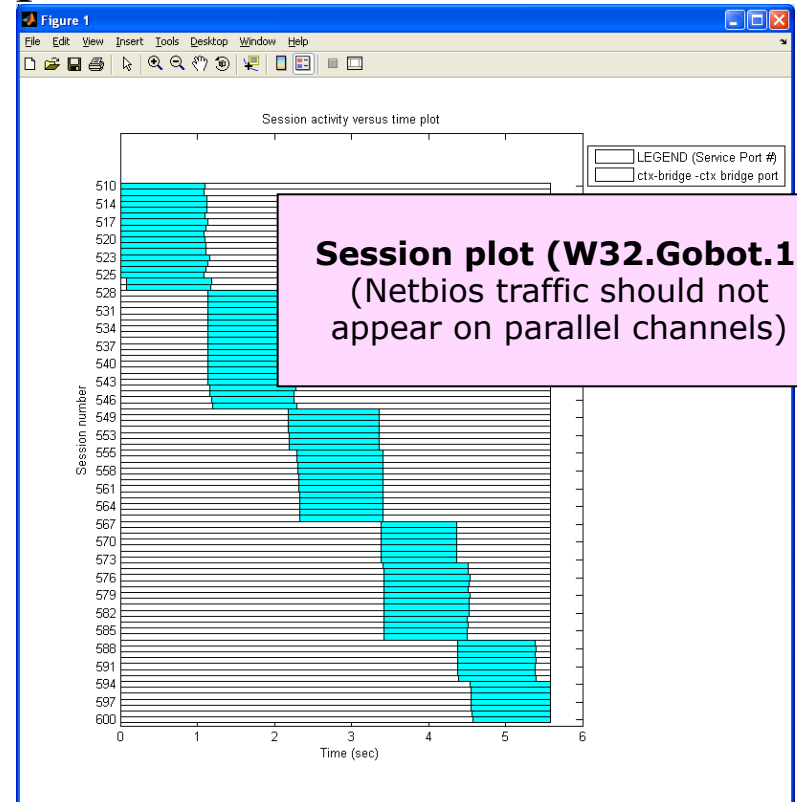
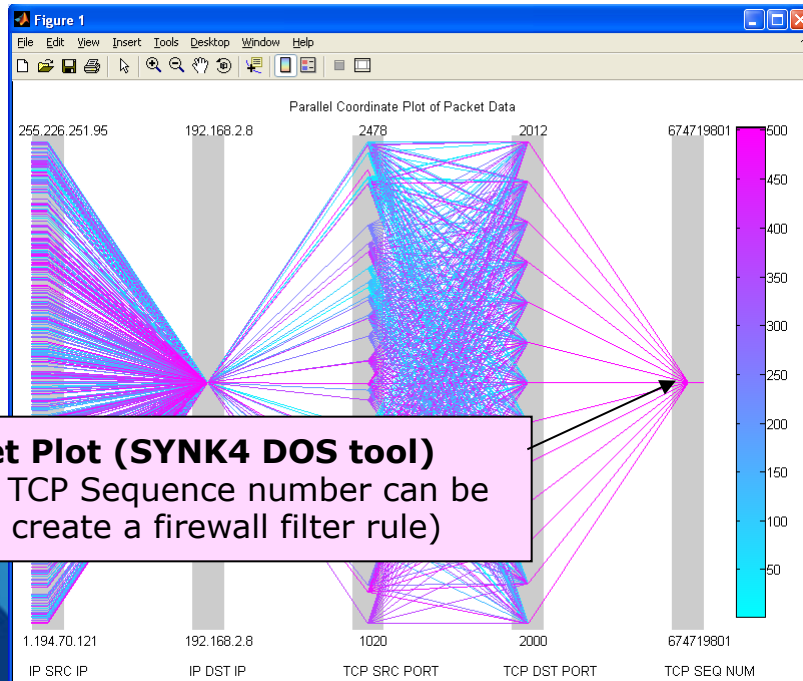




Loading and Viewing Packets

One or more traces can be loaded into the NTE and the packets can be selectively viewed .

The user can explore the data from both a packet, session or host-to-host perspective

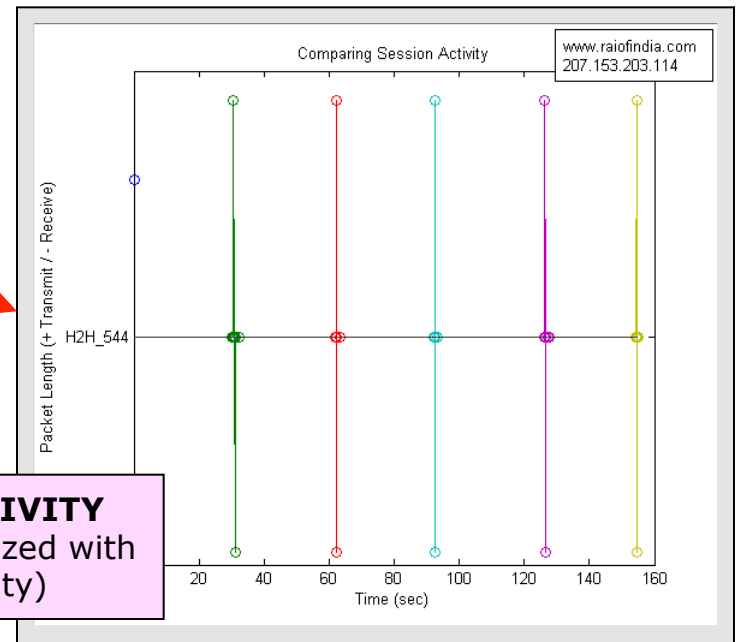
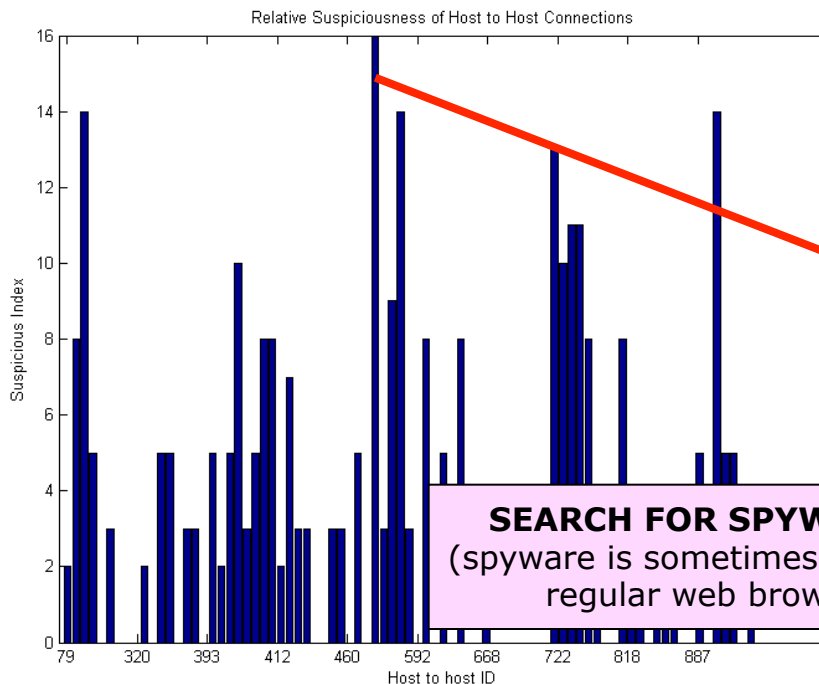




Evaluating A Situation

The NTE includes functions to help determine if a set of packets are “suspicious”. Among these are:

- Heuristic Analysis
- Statistical Analysis
- Signature-Based



SEARCH FOR SPYWARE ACTIVITY
(spyware is sometimes characterized with regular web browsing activity)

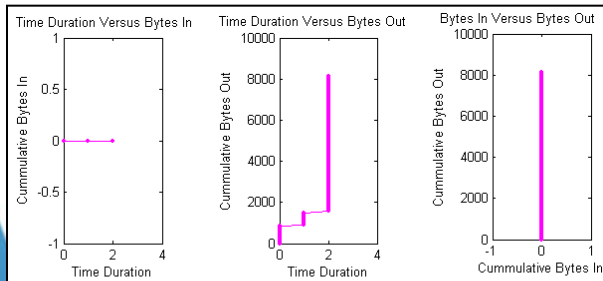


Automating Analysis and Recording An Investigation

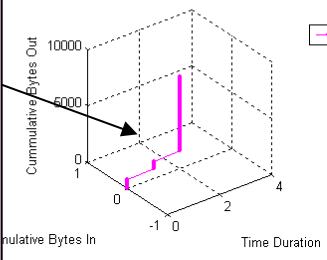
Some events are true while others are false alarms.

The NTE has the ability to create a script on the fly to detect an attack or filter a false alarm.

The script's capability can be used to log the steps taken in performing an investigation.



```
% Load the PCAP trace array
%
[PKT_DATA, IP_OPT, TCP_OPT, PAYLOAD]=load_pcap_file_plus_ev('C:\DATA \good_bad_2.dmp', ...
    'TRACE_NUMBER', '1', 'BPF', 'ip');
%
% Assign session id numbers and host-2-host id numbers to the trace array
PKT_IDX=assign_session_number(PKT_DATA, PAYLOAD);
%
% Create the host to host array
%
[H2H_SUM, H2H_LIST]=create_h2h_array(PKT_DATA, PKT_IDX);
%
% Print a summary of the host to host connections
% [the filter embedded this is the print function also detects the HTTP tunnel].
%
[SSN_NUM, H2H_NUM]=print_host_to_host_details(H2H_SUM, H2H_LIST, 'ALL', 5, ...
    'TTL_PKTS=1&SERV_PORT=80&PROTOCOL=6');
%
% Convert host to host connections back to packets
%
[PKT_REF_NUM]=find_pkt_from_h2h(PKT_IDX, H2H_NUM);
```



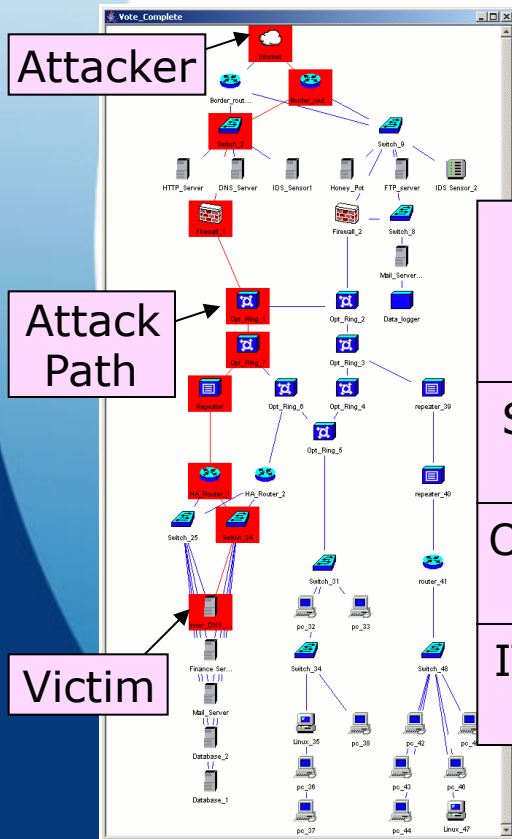
Typical http activity has a U shaped profile

This out-of-band HTTP tunnel can be detected by the adjacent script



Relating This Small Event To The Bigger Picture

Packet events and exchanges can be overlaid onto network diagrams.



Proposed Response To Attack

Secondary Effects

Operational Impact

IT Services Impact

COURSE OF ACTION FEATURE

IMPACT ASSESSMENT

| SERVICE_ID | SERVICE_PLANE | TOTAL IMPORTANCE | QTY NODES AFFECTED |
|------------------------------|---------------|------------------|--------------------|
| DNS External network service | | 200 | 5 |

Network Plotter

This section displays three windows from a network analysis tool. The top window, 'Impact Assessment', shows a network view with nodes like Internet, Border_rout..., DBell_ZONE, DNS_Server, HTTP_Server, FTP_server, RING, HA_Router_1, HA_Router_2, OFFICE1, router_41, OFFICE2, Switch_25, Switch_24, Inner_DNS, Finance Ser..., Database_1, Database_2, and Mail_Server. The middle window, 'IMPACT ASSESSMENT', shows a table with one row: 'DNS External network service' with a total importance of 200 and 5 affected nodes. The bottom window, 'Network Plotter', shows a detailed view of affected nodes: Inner_DNS, Finance Ser..., pc_36, Linux_35, Database_1, FTP_server, Honey_Pot, and HTTP_Server.



DEMONSTRATION

Starting Premise

You are handed a trace containing suspicious traffic.

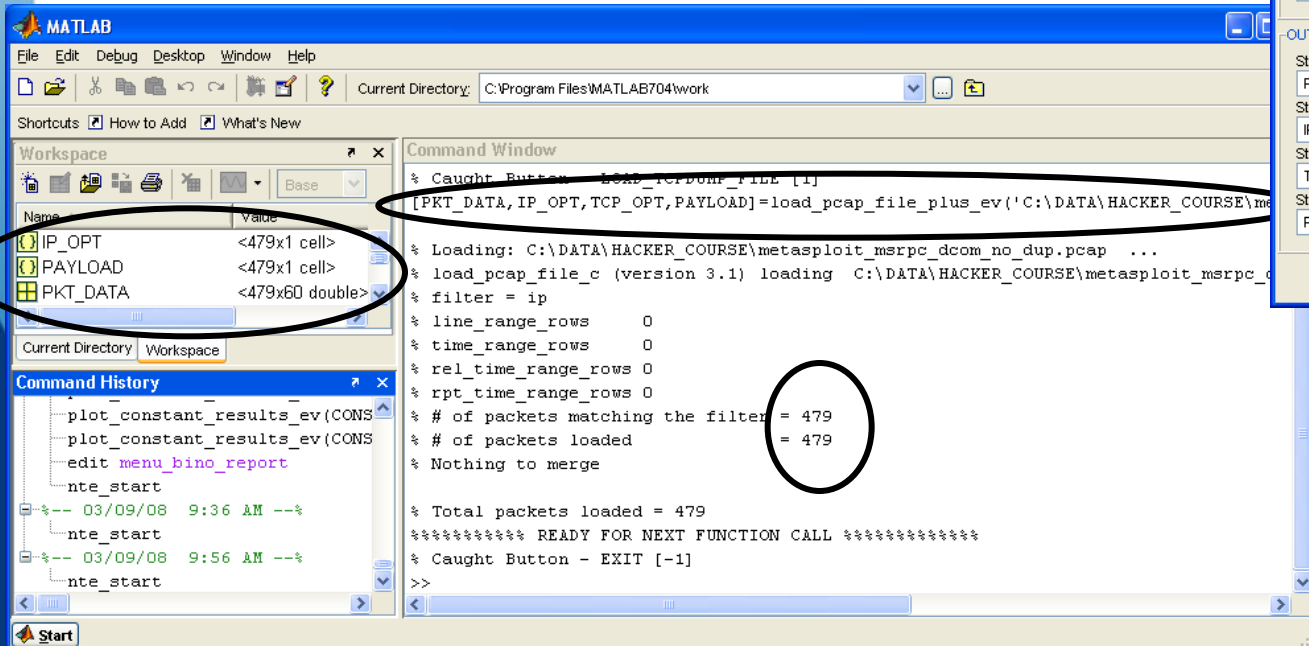
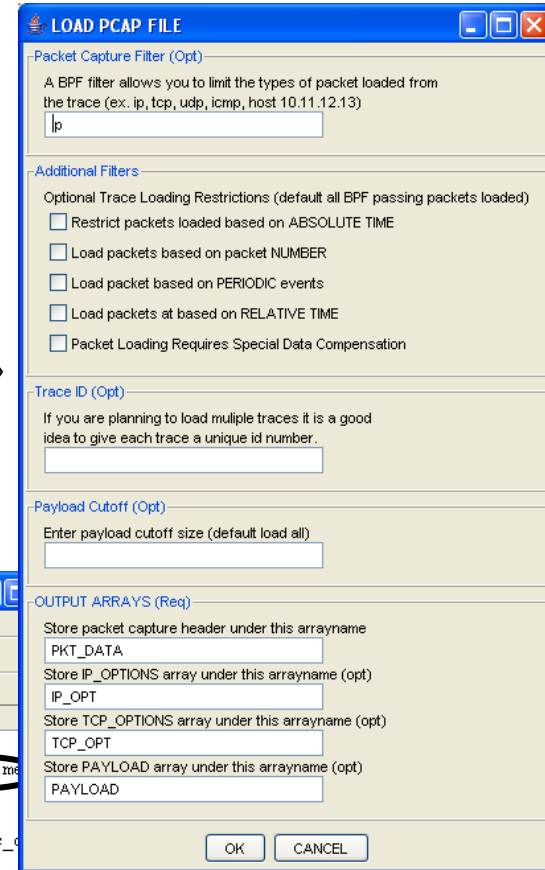
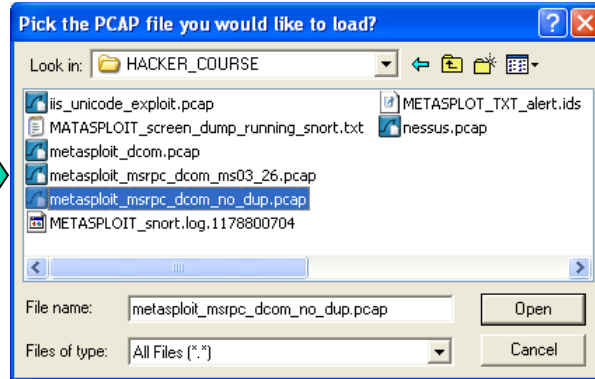
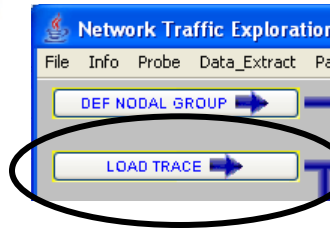


Starting the NTE

The image shows a MATLAB window with the Command Window open, displaying the command `>> nte_start`. A green arrow points from this command to the Network Traffic Exploration Tool v3.0 interface, which is a graphical user interface for network analysis. The interface includes a menu bar (File, Info, Probe, Data_Extract, Packet-Groom, Snort, Snort-Alerts, Network_Visualize, Base, DR, Help) and a main workspace with various tool buttons. The buttons are organized into several columns and rows, including options like 'DEF NODAL GROUP', 'LOAD TRACE', 'PRINT NODAL GROUP', 'ASSIGN SSN #', 'PRINT PACKET', 'SAVE_PAYLOAD', 'PAYLOAD READER', 'WIRESHARK', 'TRACE PROPERTIES', 'PLOT IP VS TIME', 'PKT XCHG DIAGRAM', 'SAVE TRACE', 'CREATE SNORT ALERT', 'PRINT SSN TRACE', 'CREATE SSN XCHG', 'PRINT H2H TRACE', 'CREATE HOST 2 HOST', 'ANALYZE HEADER', 'HDR FIELD TO 3GLING', 'CREATE ICMP SSN', 'PARTITION TRAFFIC', 'SUMMARIZE IP ACTIVITY', 'CLIENT VIEW', 'PRINT SSN SUMMARY', 'GENERAL PORT ACTIVITY', 'SSN PLOTS', 'ODD H2H ACTIVITY', 'SERVER VIEW', 'STAT_ABNORMAL_SSN', 'FIND TYPICAL_SSN', 'SERVICE PROFILING', 'PLOT H2H TRENDS', 'PRINT H2H REPORT', 'IP HDR FLD REPORT', 'TCP HDR FLD REPORT', 'ICMP HDR FLD REPORT', 'IP ADDR INTERACTIONS', 'CLIENTS OF SERVICE', 'PRINT SCANS', 'PROVIDERS OF SERVICE', 'SERVER USAGE RPT', 'MULTI-SERVICE SERVER', 'PRINT_ABNORMAL_SSN', 'PRINT TYPICAL_SSN', 'BINOMIAL PROF RPT', 'STANDARD PROF RPT', and 'CONSTANT PROF RPT'.



Load Packets Associated with Alert



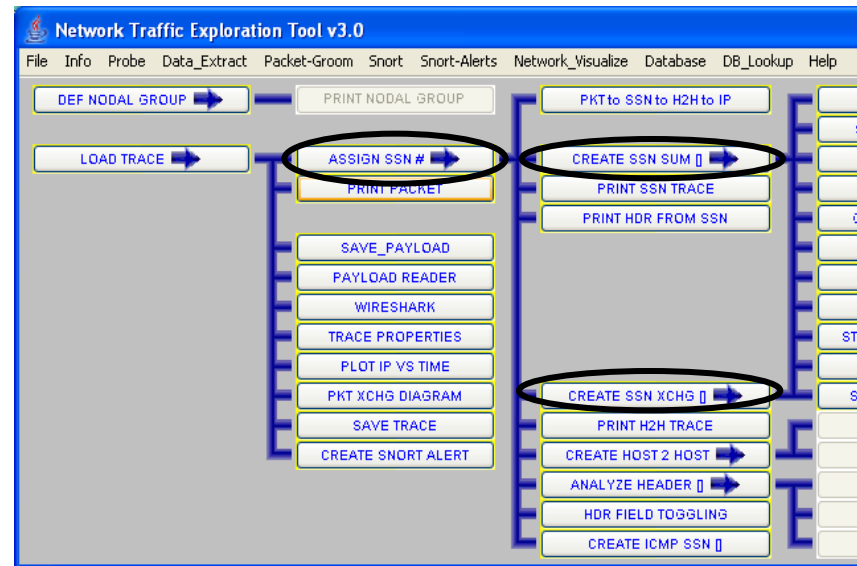


Steps Not Shown

Assign Session Number To Each Packet In Trace

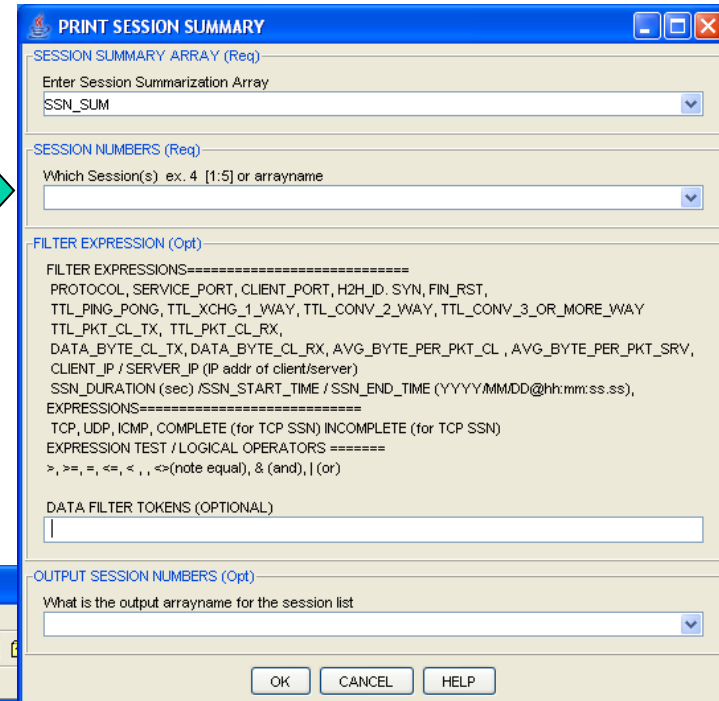
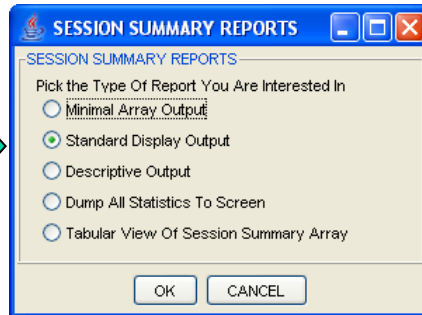
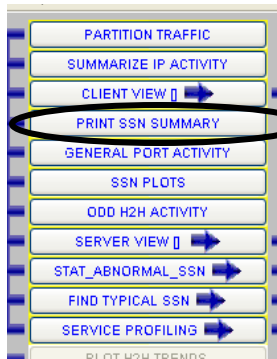
Summarize each session using 90 different statistical measurements

Summarize The Session Information Exchange





View Summary Of Trace Session Activity



Command Window Output:

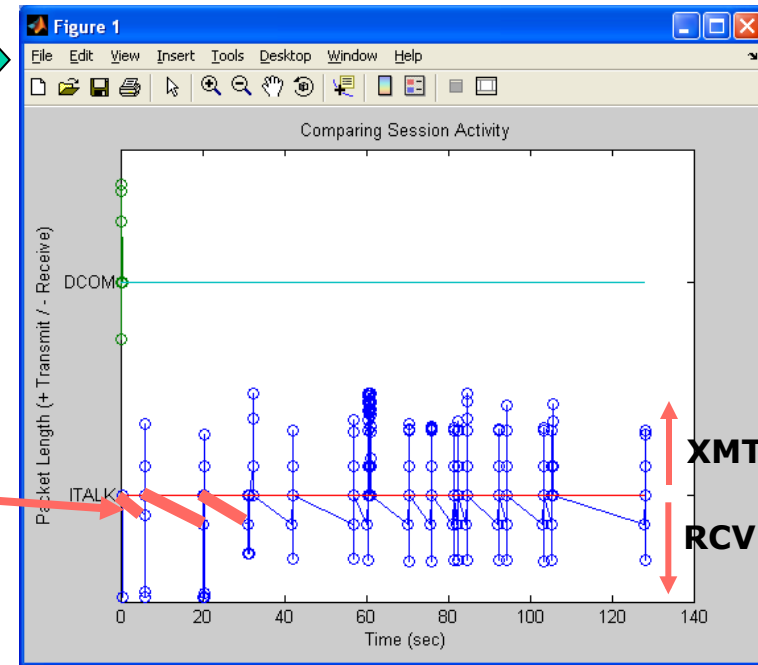
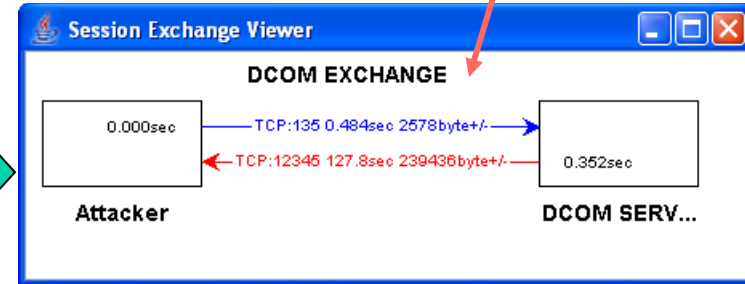
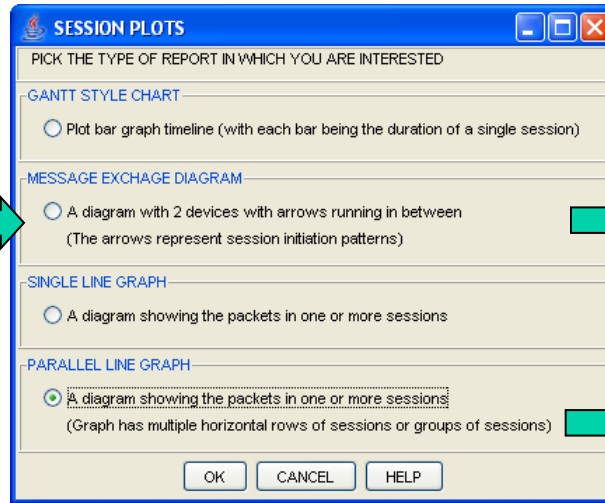
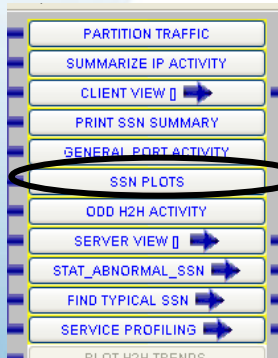
```
***** READY FOR NEXT FUNCTION CALL *****
% Caught Button - PRINT_SESSION_SUMMARY [105]
print_session_summary2_ev(SSN_SUM, 'ALL');
*****
***** Summary Description Of Sessions *****
*****
DATE = 2006/7/5      Total Qty=2
SSN= 1      (TCP ) LEN=1830  PKT=14  +/- DUR=0  COM 192.168.0.30:1384->192.168.0.8
SSN= 2      (TCP ) LEN=220820  PKT=465  +/- DUR=128  INC 192.168.0.8:1041->192.168.0.30
*****
***** READY FOR NEXT FUNCTION CALL *****
% Caught Button - PRINT_SESSION_SUMMARY [105]
% FUNCTION ABORTED
*****
***** READY FOR NEXT FUNCTION CALL *****
```

Annotations in the image:

- A red arrow points from the circled menu item to the dialog boxes.
- A red arrow points from the 'Standard Display Output' radio button to the 'PRINT SESSION SUMMARY' dialog box.
- A red arrow points from the 'PRINT SESSION SUMMARY' dialog box to the MATLAB Command Window.
- Handwritten notes next to the Command Window output: 'epmap / DCOM' next to the first SSN line and 'italk' next to the second SSN line.

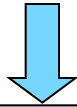


Plot Session Activity





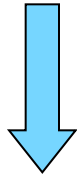
Steps Not Shown



Convert Session #1 Into A List of Packets

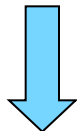


View Packet In Wireshark



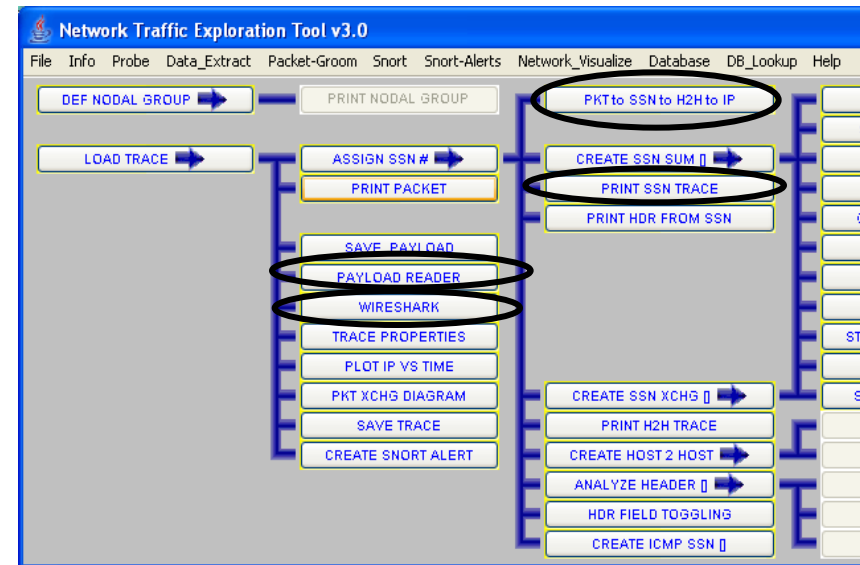
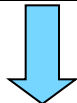
X Wireshark cannot decode the protocol

Payload Type Analysis



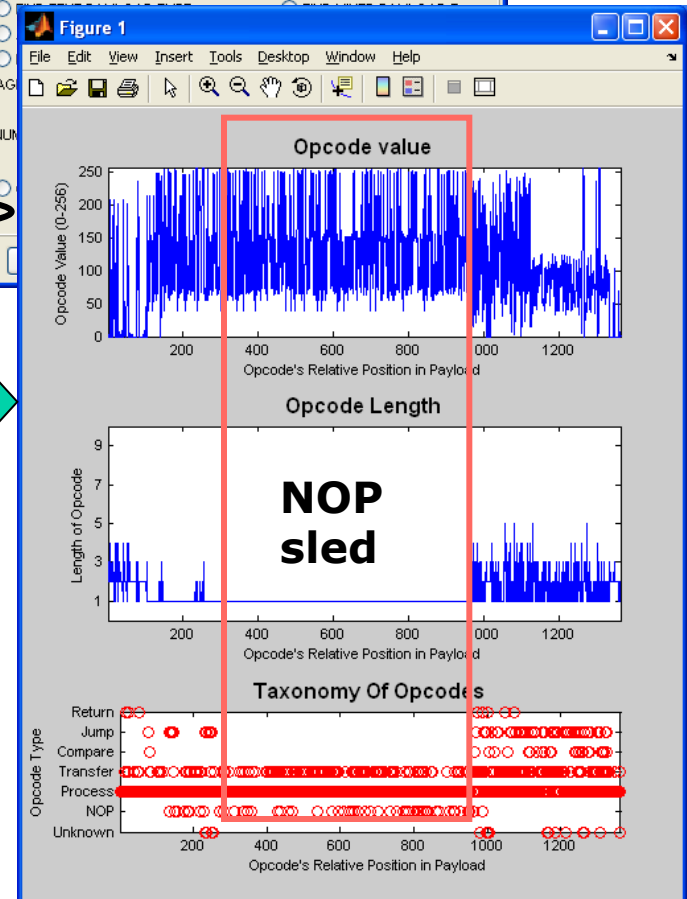
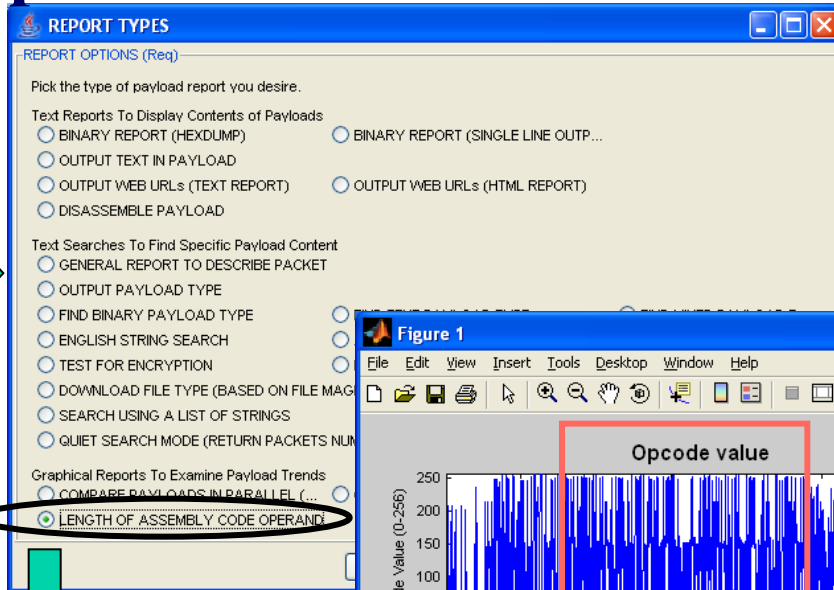
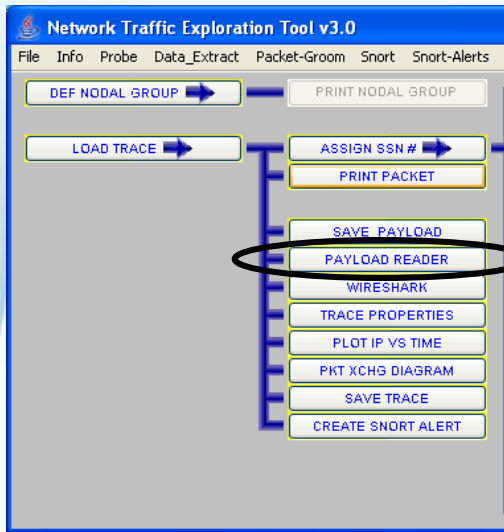
✓ Payload is binary but not random

Isolate All Packets In Session #1 Running From Client To Server





Plot Payload Bytes Based On Machine Language Opcodes





Search For English Strings In Packets

REPORT TYPES

REPORT OPTIONS (Req)

Pick the type of payload report you desire.

Text Reports To Display Contents of Payloads

- BINARY REPORT (HEXDUMP)
- BINARY REPORT (SINGLE LINE OUTPUT)
- OUTPUT TEXT IN PAYLOAD
- OUTPUT WEB URLS (TEXT REPORT)
- OUTPUT WEB URLS (HTML REPORT)
- DISASSEMBLE PAYLOAD

Text Searches To Find Specific Payload Content

- GENERAL REPORT TO DESCRIBE PACKET
- OUTPUT PAYLOAD TYPE
- FIND BINARY PAYLOAD TYPE
- ENGLISH STRING SEARCH
- TEST FOR ENCRYPTION
- FIND TEXT PAYLOAD TYPE
- ZERO TERMINATED STRING SEARCH
- RECOVER ENCRYPTED PACKETS
- DOWNLOADED FILE TYPE (BASED ON FILE MAGIC)
- FIND MIXED PAYLOAD TYPE
- SEARCH USING A LIST OF STRINGS
- QUIET SEARCH MODE (RETURN PACKETS NUMBERS WITH MINIMAL DATA)

Graphical Reports To Examine Payload Trends

- COMPARE PAYLOADS IN PARALLEL (ASCII N...)
- COMPARE PAYLOADS IN PARALLEL
- LENGTH OF ASSEMBLY CODE OPERAND

PRINT PAYLOAD

INPUT TRACE/PAYLOAD (Req)

Enter the Packet Capture Header Arrayname

PKT_DATA

Enter Payload Arrayname For Trace

PAYLOAD

PACKET RANGE (Opt)

Range of Pkts In Traffic Trace (Default 'ALL') ex. [1:6]

SSN2_PKTS

PRINT DISASSEMBLED RESULT (Req)

- VERBOSE REPORT ON SCREEN
- QUIET REPORT

PACKET OUTPUT (Opt)

Store the packets displayed in the following arrayname

Meterpreter is part of Metasploit

```
PKT= 95 ( 192.168.0.8:1041 -> 192.168.0.30:12345) TCP
-----
core_console_write||
[ == meterpreter server == ]
[ == 00000000 == ]
||
...

```

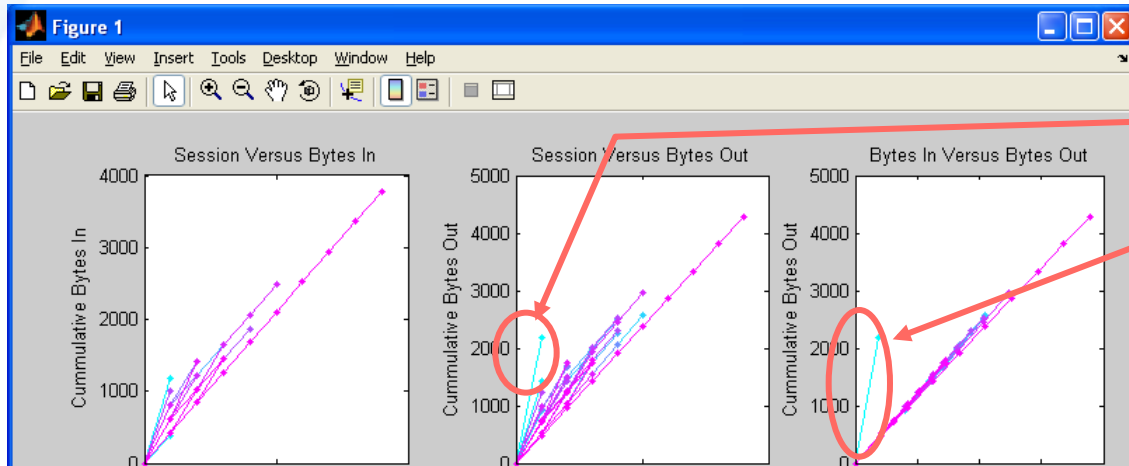
Banner for windows command shell

```
PKT= 178 ( 192.168.0.8:1041 -> 192.168.0.30:12345) TCP
-----
core_channel_write||Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.
C:\WINNT\system32>||

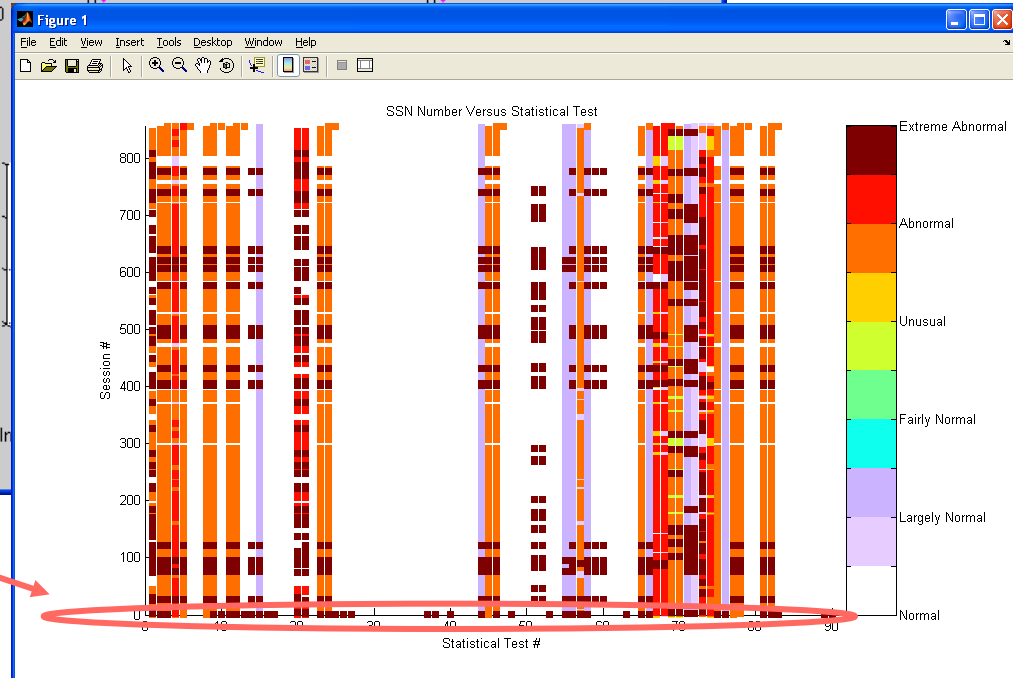
```




Statistical Detection of the Attack



The DCOM
Attack
Session



The attack session deviates significantly from the norm (in 37 different out of 90 tests)



Closing Remarks

Key benefits of NTE

- **Flexible analysis of security events and network based attacks**
- **Broad range of features (300)**
- **Scripting capability**

For more information about the tool you can contact.

Grant.Vandenberghe@drdc-rddc.gc.ca

DEFENCE



DÉFENSE