Forensic Network Analysis Tools: Strengths, Weaknesses, and Future Needs

By

Eoghan Casey

Presented At

The Digital Forensic Research Conference

DFRWS 2003 USA  Cleveland, OH (Aug 6th - 8th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

http://dfrws.org
Forensic Network Analysis Tools

Strengths, Weaknesses, and Future Needs

Eoghan Casey
- Author, Digital Evidence and Computer Crime
- Editor, Handbook of Computer Crime Investigation
- Technical Director, Knowledge Solutions
- eco@corpus-delicti.com
The Basics

- Hardware and configuration
- Read-only
- Security
- Integrity
  - Existing tools do not calculate MD5
    - Do it yourself after collection
- Documenting losses
  - Existing tools to not log all losses
- Document system status & performance
- Logging examiner actions
  - Not currently => rely examiner’s notes
Hardware

- CatOS Switched Port Analyzer (SPAN)
  - Only copies valid Ethernet packets
  - Not all error information duplicated
  - Low priority of SPAN may increase losses
- Physical tap
  - Copy signals without removing layers
  - May split Tx and Rx (reassembly required)
- Platform
  - Testing but no published data
  - \(< 200 \text{ Mb/sec} => \) Linux
  - \(> 200 \text{ Mb/sec} => \) FreeBSD
  - Kernel customization
HW (Vendor v Homemade)

- Commercial
  - More costly but uniform expertise
  - Vendor can testify about HW & OS config
  - Vendor responsible for problems

- Homemade
  - Less expensive but variable expertise
  - You can testify about HW & OS config
  - You are responsible for problems
Read Only

- No network response
  - Including ARP replies
- No network queries
  - Use internal DNS resolution
- No downloads from Internet
  - Don’t insert content from the Web when reconstructing Web pages
Security

- Secure OS configuration
  - Patches
  - Do not overuse root/Administrator account
- Secure remote access
  - SSH
  - SSL
- Secure programming
  - Prevent buffer overflows
  - Prevent crashes (and resulting data loss)
Data Loss

NIC:
% /sbin/ifconfig
eth0 Link encap:Ethernet HWaddr 00:B0:D0:F3:CB:B5
inet addr:128.36.232.10 Bcast:128.36.232.255
Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:19877480 errors:0 dropped:0 overruns:128 frame:0
TX packets:7327676 errors:0 dropped:0 overruns:0 carrier:1
collisions:442837 txqueuelen:100
Interrupt:23 Base address:0xec80

Kernel:
# tcpdump -X host 192.168.12.5
tcpdump: listening on xl0
.....[data displayed on screen]...
^C
29451 packets received by filter
4227 packets dropped by kernel

- Losses at the switch
  - show inter
- Bug or misrepresentation in application

Figure from Eoghan Casey's “Error, Uncertainty, and Loss” article in International Journal of Digital Evidence (Vol. 1, Iss. 2)
Overview of Tools

- Tcpdump (www.tcpdump.org)
  
  - de facto standard file format (.dmp)
- Ethereal (www.ethereal.com)
- Review (www.net.ohio-state.edu/software/)
- IRIS (www.eye.com)
- InfiniStream (www.networkassociates.com)
- NetIntercept (www.sandstorm.net)
- NetDetector (www.niksun.com)
- NFR Security (www.nfrsecurity.com)
- NetWitness (www.forensicexplorers.com)
- SilentRunner (www.silentrunner.com)
- DCS1000 w/ CoolMiner/Packeteer (FBI)
Overview of Tool Features

- **Tcpdump** (multiple platforms, free)
  - Limited examination capabilities
- **Ethereal** (multiple platforms, free)
  - Basic examination capabilities
- **IRIS** (Windows, $)
  - Basic examination capabilities
- **NetWitness** (Windows, IIS, MSSQL, $)
  - Basic examination capabilities
  - Security concerns relating to ISS and MSSQL
- **InfiniStream** (Linux collector, Win console, $)
  - Tcpdump import but not export (.cap export)
  - Good examination capabilities (Sniffer-based)
Overview of Tool Features

- **Review (Unix, free)**
  - Good examination capabilities

- **NetIntercept (FreeBSD, $)**
  - Designed with evidentiary issues in mind
  - Excellent examination capabilities
    - Feature rich but still user-friendly
    - Decrypt SSH and SSL if key are available
  - Basic analysis capabilities

- **NetDetector (FreeBSD, $)**
  - Excellent examination capabilities
  - Graphic analysis features (Xpert)
  - Integrated IDS capabilities (Snort)
Overview of Tool Features

- **NFR Security ($)**
  - Custom analysis using N-code
  - OpenBSD collector, Windows admin console, Solaris/Linux mgmt server & Oracle database

- **SilentRunner (Windows, $)**
  - Powerful visual & analysis capabilities

- **DCS1000 (Windows, available to LE)**
  - Unique filtering with law enforcement in mind (e.g., RADIUS, e-mail pen register)
  - Not clear how robust (complexity of RADIUS and capturing content in e-mail header)
Examples

Key points
- Collection: capture all content versus filtering
- Documentation: poor across the board
- Examination: recover, classify, decode, reduce, search
- Analysis: individualize, evaluate source, advanced recovery, reconstruct, visualize, present
Collection

- Tcpdump
  - 68 byte default
- Ethereal
  - 65535 bytes default snap length
- Others
  - 68 < snap length < 65535 bytes
<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Origin IP Address</th>
<th>User Name</th>
<th>Activity Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mon Jul 14 23:21 01 EDT 2003</td>
<td>10.70.0.2</td>
<td>admin</td>
<td>logged in</td>
</tr>
<tr>
<td>Mon Jul 14 23:22 13 EDT 2003</td>
<td>10.70.0.2</td>
<td>admin</td>
<td>Deleted ALL events from the log</td>
</tr>
<tr>
<td>Tue Jul 14 02:13 EDT 2003</td>
<td>10.70.0.2</td>
<td>admin</td>
<td>Reconstructed data at 08/19/2003 22:18:03</td>
</tr>
<tr>
<td>Tue Jul 14 02:13 EDT 2003</td>
<td>10.70.0.2</td>
<td>admin</td>
<td>added/edited alarm 1</td>
</tr>
<tr>
<td>Tue Jul 14 02:13 EDT 2003</td>
<td>10.70.0.2</td>
<td>admin</td>
<td>added/edited alarm 2</td>
</tr>
<tr>
<td>Tue Jul 14 02:13 EDT 2003</td>
<td>10.70.0.2</td>
<td>admin</td>
<td>added/edited alarm 3</td>
</tr>
<tr>
<td>Tue Jul 14 02:13 EDT 2003</td>
<td>10.70.0.2</td>
<td>admin</td>
<td>logged in</td>
</tr>
<tr>
<td>Tue Jul 14 02:13 EDT 2003</td>
<td>10.70.0.2</td>
<td>admin</td>
<td>logged out</td>
</tr>
<tr>
<td>Tue Jul 14 02:13 EDT 2003</td>
<td>10.70.0.2</td>
<td>admin</td>
<td>Reconstructed data at 08/19/2003 22:18:03</td>
</tr>
<tr>
<td>Thu Jul 14 02:13 EDT 2003</td>
<td>10.70.0.2</td>
<td>admin</td>
<td>Data Imported from alarac.mj.nikun.com in voip001нем-1 Egyptians</td>
</tr>
</tbody>
</table>
External MD5 Calculations
Filtering During Collection

- BPF/Ethereal filtering syntax
  - IP address, port, etc.
- MAC address
- Custom NFR Security filters (using N-code)
- DCS1000
  - RADIUS
  - DHCP
- Filtering on protocol is risky
  - Pen register for e-mail (DCS1000)
  - If necessary, be very careful
  - Ideally use a specialized tool for this purpose
Examination: Protocol Decode

- **Tcpdump** has limited decode capabilities
- **Ethereal**
  - More decodes but assumes default behavior
  - “Decode As” feature
- **InfiniStream/Sniffer**
  - Several decodes including some VoIP
- **NetDetector**
  - Understands protocols including some VoIP
- **NetIntercept**
  - Understands protocols including some VoIP
  - More powerful stream reconstruction
  - Flags anomalies (like file sig mismatch)
  - Flags missing SEQ #’s in TCP session
Review: X Session Decode

Server

Client
Review: X Session Replay

- Step-by-step session replay
- Pauses before redrawing screen

Figure from Steve Romig's "Incident Response Tools" chapter in Handbook of Computer Crime Investigation
Examination: Data Reduction

- GUI versus command syntax
  - Review: session summary & browsing
  - NetIntercept: Forensics tab
Examination: Data Reduction

- SilentRunner: 3-D Visualization
- NFR Security: Query interface
Examination: Visualization

- Traffic charts
- Top Talkers
- Top Pairs
Examination: Visualization

- SilentRunner
  - 3-D display of traffic helps focus on interesting activities

- General purpose visualization tools
  - Clustering and other techniques for visually representing data to help examiners identify useful items in large datasets
Search and Recovery

- **Ethereal**
  - Miss keyword split between two packets
  - Export Web page & view in browser (bad)
  - File extraction requires expertise & tools

- **NetIntercept**
  - Performs search on reconstructed data
  - Sandbox for viewing Web pages
  - Does not execute code in Web pages
  - Automated file extraction

- **NetDetector**
  - GUI & regular expression on command line
  - Sandbox for viewing Web pages

- **NFR Security database query customization**

- **SilentRunner**
  - N-gram Analysis
Ethereal: Search

Frame 3900 (538 on wire, 538 captured)
- Ethernet II
  - Destination: 00:30:ab:1d:cd:ef (DELTA_1d:cd:ef)
  - Source: 00:00:82:8a:c4:6b (ACER_8a:c4:6b)
  - Type: IP (0x0800)
- Internet Protocol, Src Addr: 192.168.0.5 (192.168.0.5), Dst Addr: sealfd.seal.hotmail.msn.com (20)
- Transmission Control Protocol, Src Port: 32942 (32942), Dst Port: http (80), Seq: 1433552153, Ack: 5735469088
- Hypertext Transfer Protocol
NetIntercept: Search
NetDetector: Search (GUI)
NetIntercept: Image Extraction
Ethereal: Web Page
NetIntercept: Web Page
Figure from Eoghan Casey’s “Digital Evidence and Computer Crime”, 2nd edition

NetIntercept: Search/Recover
Analysis

- Temporal views
  - Timelines
  - Histograms/charts
- Relational analysis
  - Thicker lines for higher traffic
  - N-gram analysis
- SilentRunner
  - 3-D visualization can be useful for analysis
  - Develop baseline of network activities for comparison
  - Visually represents anomalies and other noteworthy events
Analysis: NetIntercept
Analysis: NetDetector (Snort)
NetDetector (Snort cont.)

![NetDetector Interface]

### NIKSUN Event Viewer

#### Time Frame

<table>
<thead>
<tr>
<th>Start</th>
<th>Relative</th>
<th>End</th>
<th>Relative</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dec 16 2002 13:38:11</td>
<td></td>
<td>now</td>
<td></td>
</tr>
</tbody>
</table>

#### Alarm Filter

- All Severities
- All Event Types
- Name/Sig ID
- Source IP Addr
- All Links

#### Options

- Deletions...
- Options...

### Summary

<table>
<thead>
<tr>
<th>Severity</th>
<th>Time Stamp</th>
<th>Link</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Warning</td>
<td>Mon Jul 28 06:23:59 EDT 2003</td>
<td>ind4.niksun.com/s0</td>
<td>Host Flood detected to destination 10.0.0.126, hosts counted: 6</td>
</tr>
<tr>
<td>Info..</td>
<td>Mon Jul 28 06:23:44 EDT 2003</td>
<td>ind4.niksun.com/s0</td>
<td>Link utilization exceeded to 0.0338%</td>
</tr>
<tr>
<td>Severe</td>
<td>Mon Jul 28 06:23:11 EDT 2003</td>
<td>ind4.niksun.com/s0</td>
<td>Cisco IDS [200] [Net Sweep Exp] detected from 10.10.0.0 to 10.0.0.126</td>
</tr>
<tr>
<td>Critical</td>
<td>Mon Jul 28 06:23:11 EDT 2003</td>
<td>ind4.niksun.com/s0</td>
<td>Link utilization exceeded to 1.4652%</td>
</tr>
<tr>
<td>Warning</td>
<td>Mon Jul 28 06:22:19 EDT 2003</td>
<td>ind4.niksun.com/s0</td>
<td>Link utilization exceeded to 1.5193%</td>
</tr>
<tr>
<td>Info..</td>
<td>Mon Jul 28 06:21:51 EDT 2003</td>
<td>ind4.niksun.com/s0</td>
<td>Link utilization exceeded to 0.3326%</td>
</tr>
<tr>
<td>Info..</td>
<td>Mon Jul 28 06:21:50 EDT 2003</td>
<td>ind4.niksun.com/s0</td>
<td>Link utilization exceeded to 0.3327%</td>
</tr>
<tr>
<td>Warning</td>
<td>Mon Jul 28 06:21:44 EDT 2003</td>
<td>ind4.niksun.com/s0</td>
<td>Host Flood detected to destination 10.0.0.126, hosts counted: 4</td>
</tr>
<tr>
<td>Info..</td>
<td>Mon Jul 28 06:21:43 EDT 2003</td>
<td>ind4.niksun.com/s0</td>
<td>Link utilization exceeded to 0.3330%</td>
</tr>
<tr>
<td>Info..</td>
<td>Mon Jul 28 06:21:28 EDT 2003</td>
<td>ind4.niksun.com/s0</td>
<td>Link utilization exceeded to 0.3329%</td>
</tr>
<tr>
<td>Severe</td>
<td>Mon Jul 28 06:21:11 EDT 2003</td>
<td>ind4.niksun.com/s0</td>
<td>Invalid IP address, source 64.200.148.28 and destination 10.0.0.126</td>
</tr>
</tbody>
</table>

Displaying 1-100 of 2096 records.
Visualization & Data mining

- Visualization techniques
  - Clustering and other techniques for visually representing data to help examiners identify noteworthy patterns and items in large datasets

- Data mining
  - Finding patterns, associations, links
  - Recognizing patterns of behavior
Reporting

- Bookmarks
- Default reports
  - Inventory hosts, accounts, nicknames files, etc.
  - Top talkers
- Alerts

Figure from Steve Romig’s “Incident Response Tools” chapter in Handbook of Computer Crime Investigation
### Web Pages

<table>
<thead>
<tr>
<th>Connection Size</th>
<th>File Name</th>
<th>Host</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>/o1i-bin/linkdirector/signup?_lang=En</td>
<td>help.msn.com</td>
</tr>
<tr>
<td>31</td>
<td>/en_us/frameset.asp?Topic=REGTyr20Passport BrandID= Filter= H_VE</td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>/en_us/helpwindow.asp?Topic=REG20Passport BrandID= Filter= H_VE</td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>/en_usf_tbar.asp?UNI=PPx25.ini_H ITSF ile=ppx25.its51 H_VER=1.5b1</td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>/data/en_usidata/ppx25.its51%conte H_APP=Microsoft+%2ENET+Pass xmlite=</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>/o1i-bin/login</td>
<td>loginnet.passport.com</td>
</tr>
<tr>
<td>184</td>
<td>/logoat.png?_lang=EN lc=1033 id=2 r</td>
<td></td>
</tr>
</tbody>
</table>

### Alerts

<table>
<thead>
<tr>
<th>Connection ID</th>
<th>Time</th>
<th>Src IP</th>
<th>Src MAC</th>
<th>Dst IP</th>
<th>Dst MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>199</td>
<td>2003-02-24 16:06:38</td>
<td>192.168.0.5</td>
<td>00:00:E2:8A:C4:6B</td>
<td>207.68.172.245</td>
<td>00:30:AB:1D:CD:EF</td>
</tr>
<tr>
<td>202</td>
<td>2003-02-24 16:06:38</td>
<td>192.168.0.5</td>
<td>00:00:E2:8A:C4:6B</td>
<td>63.150.154.197</td>
<td>00:30:AB:1D:CD:EF</td>
</tr>
<tr>
<td>203</td>
<td>2003-02-24 16:06:38</td>
<td>192.168.0.5</td>
<td>00:00:E2:8A:C4:6B</td>
<td>63.150.154.197</td>
<td>00:30:AB:1D:CD:EF</td>
</tr>
<tr>
<td>204</td>
<td>2003-02-24 16:06:38</td>
<td>192.168.0.5</td>
<td>00:00:E2:8A:C4:6B</td>
<td>152.163.209.77</td>
<td>00:30:AB:1D:CD:EF</td>
</tr>
<tr>
<td>116</td>
<td>2003-02-24 16:06:40</td>
<td>192.168.0.5</td>
<td>00:00:E2:8A:C4:6B</td>
<td>207.68.172.245</td>
<td>00:30:AB:1D:CD:EF</td>
</tr>
<tr>
<td>201</td>
<td>2003-02-24 16:06:40</td>
<td>192.168.0.5</td>
<td>00:00:E2:8A:C4:6B</td>
<td>207.68.172.245</td>
<td>00:30:AB:1D:CD:EF</td>
</tr>
</tbody>
</table>

**Message:** Connection close not captured

**Message:** Media type 'image/gif' requested by GIF, but it didn’t match and PlainTxt did

**Message:** Media type 'text/html' requested by HTML, but it didn’t match and ASCII Type did

**Message:** Media type 'text/html' requested by HTML, but it didn’t match and PlainTxt did

**Message:** Reset out of window

**Message:** Window ignored

This report was generated by NetIntercept® 2.0.
Comparison Summary

- **NetIntercept & NetDetector**
  - Best starting point for examination
  - Useful for most common analysis needs

- **NFR Security**
  - Advanced evidence processing using N-Code, GUI Queries & Perl Query Add-on

- **SilentRunner**
  - 3-D visualization useful in some cases

- **DCS1000**
  - Good effort to filter during collection (e.g., pen register, RADIUS, DHCP)
Summary of Future Needs

- Platform standards to minimize losses
  - Published performance testing
  - Consider security and stability
- Read-only
  - No network responses or queries during collection or examination
- Integrity
  - Not necessarily during collection (after)
- Validate security and data interpretation of tools
- Documentation
  - System status & performance (proper operation)
  - Record primary sources of losses
  - Audit trail of examiner actions
Future Needs (cont.)

- Support tcpdump format import and export
  - Collect using one tool, examine w/ other

- Filtering capabilities during collection
  - DHCP & RADIUS
  - May be safer to use specialize tool for protocol filtering & pen register needs

- Filtering during examination
  - Exclude known files (e.g., logo, safe content)
  - Flag suspicious files (e.g., encrypted files or intellectual property/hacker tools using MD5)
  - Drill down on top host/protocols (e.g., ntop.org)
  - More visualization of data to help filtering
Future Needs (cont.)

- Protocol identification and decode
  - Based on protocol v. variables chars
  - Flag protocol violations, missing SEQ #s
  - More decodes and step-by-step replay

- Text search capabilities
  - Keywords split between multiple packets
  - Grep syntax

- More file extraction capabilities
  - KaZaA fragments from multiple sources

- More analysis capabilities
  - Behavior pattern recognition
  - System profile violations