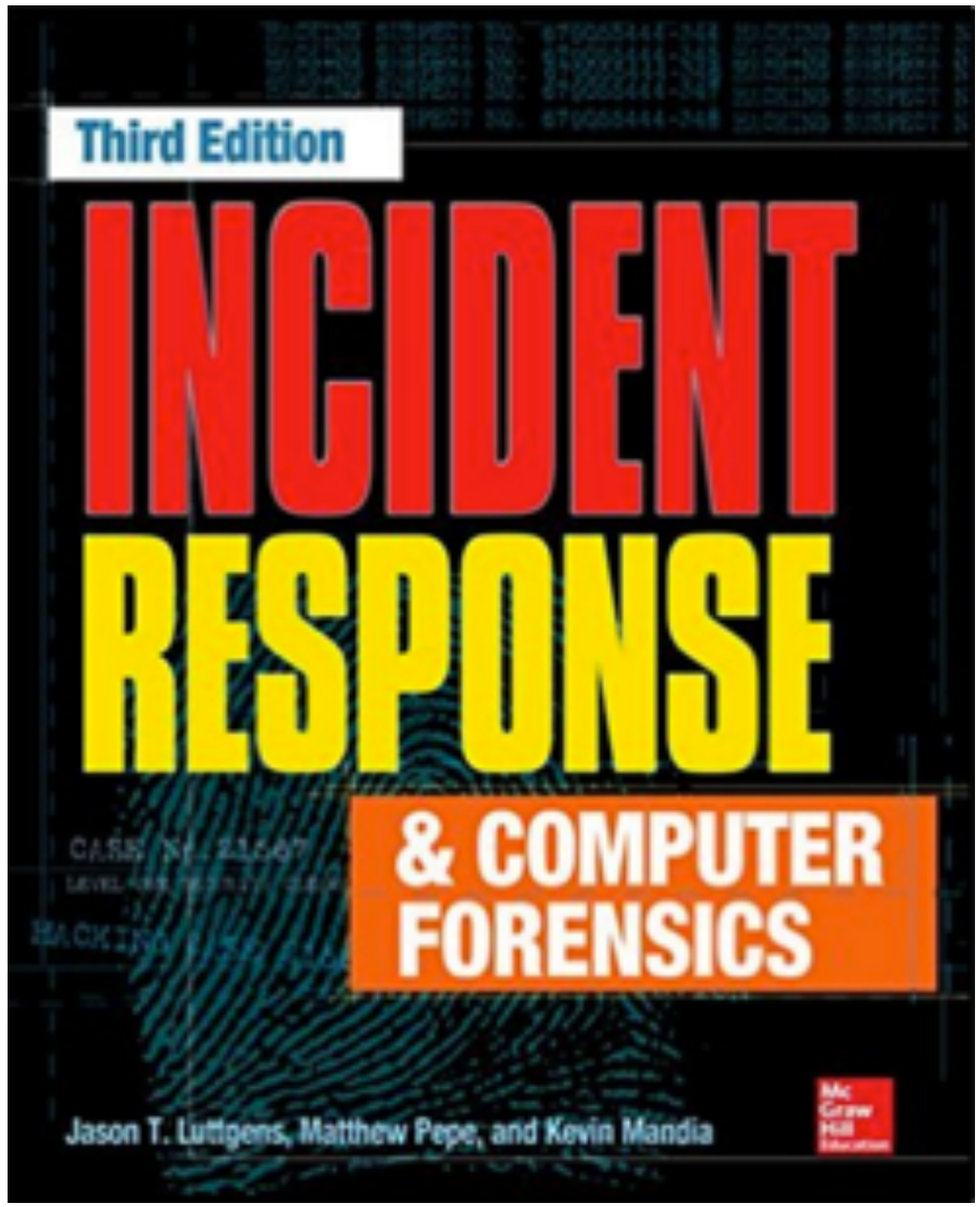
CNIT 152: Incident Response



9 Network Evidence

Updated 10-7-21

The Case for Network Monitoring

- **Confirm or dispel suspicions surrounding an alleged computer security incident**
- **Accumulate additional evidence and indicators**
- **Verify the scope of a compromise**
- **Identify additional parties involved**
- **Generate a timeline of events occurring on the network**

Types of Network Monitoring

Types of Network Monitoring

1. **Event-based alerts**
2. **Packet captures**
3. **Session information**
4. **High-level statistics**

Types of Network Monitoring

1. Event-based alerts

- **Snort, Suricata, SourceFire, RSA NetWitness**
- **Require rule sets**
- **Provides real-time notification**

Types of Network Monitoring

2. Full Packet Captures

- **Can reconstruct everything sent on the network**
- **Helps to identify scope of data theft**
- **Capture actions done with interactive shells**
- **Closely monitor malware communicating with remote sites**

Types of Network Monitoring

3. Session information

- **Header logging**
- **Can identify connections and addresses**
- **Cannot reconstruct data transmitted**

Types of Network Monitoring

4. High-level statistics

- **Showing type and number of packets**
- **Can reveal suspicious patterns, such as abnormally high volumes of traffic**

Event-Based Alert Monitoring

- **Most common type**
- **Based on rules or thresholds**
- **Events are generated by Network Intrusion Detection Systems (NIDS)**
  - **Or by software that monitors traffic patterns and flows**
- **Standard tools: Snort and Suricata**

Indicators (or Signatures)

- **Matched against traffic observed by the network sensor**
- **Simple indicators**
  - **Such as IP address + port**
  - **"Cheap" (small load on sensor)**
- **Complex indicators**
  - **Session reconstruction or string matching**
  - **Can burden the sensor so much it drops packets**

Example Snort Rule

- **This rule detects SSH Brute Force attacks**
  - **Depth: how many bytes of packet to read**
  - **Links Ch 9a, 9b**

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 22
(msg:"INDICATOR-SCAN SSH
brute force login attempt";
flow:to_server,established; content:"SSH-";
depth:4; detection_filter:track by_src, count 5,
seconds 60;
metadata:service ssh; classtype:misc-activity;
sid:19559; rev:5;)
```

alert_fast

- **Put this in Snort configuration file**
  - `output alert_fast alerts.txt`
- **Simplest output module for Snort**
- **Puts text into a file**

Detect Fake SSL Certificate

```
alert tcp $EXTERNAL_NET 443 -> $HOME_NET any (msg:"ET TROJAN FAKE AOL SSL
Cert APT1"; flow:established,from_server; content:"|7c a2 74 d0 fb c3 d1 54 b3 d1 a3 00 62
e3 7e f6|"; content:"|55 04 03|"; content:"|0c|mail.aol.com"; distance:1; within:13;
reference:url,www.mandiant.com/apt1; classtype:trojan-activity; sid:2016469; rev:3;
metadata:attack_target Client_Endpoint, deployment Perimeter, tag SSL_Malicious_Cert,
signature_severity Major, created_at 2013_02_21, updated_at 2016_07_01;)
```

- **Detects a specific fake certificate used by the APT 1 group identified by Mandiant in 2003**
- **Written by Emerging Threats**
- **Matches serial number and Issuer string**
  - **Link Ch 9h**

Header and Full Packet Logging

- **Two distinct purposes**
  - **To help IR team generate signatures, monitor activity, or identify stolen data**
  - **Collect evidence for an administrative or legal matter**
- **Consider whether to treat packet captures as evidence and generate a chain of custody**

Thoroughness

- **IDS systems can retain the full session that generated an alert**
- **But for targeted collection against specific subjects, use tcpdump or Wireshark**

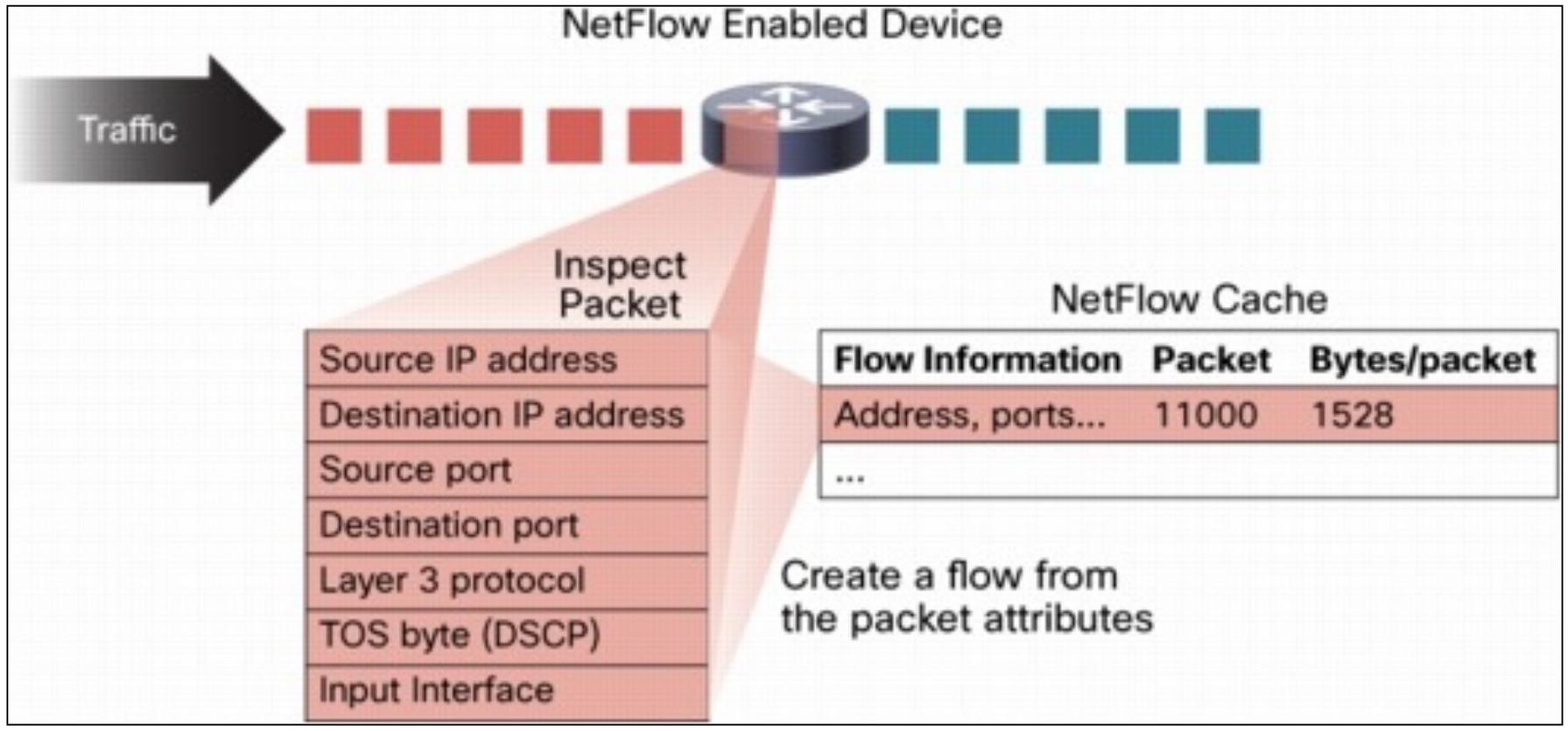
tcpdump

- **Complete packet capture of an HTTP request**
- **Limiting capture to 64 bytes captures only the headers (called "trap and trace" by law enforcement)**

```
11:28:46.581258 IP kali.55743 > 159.203.238.50.http: Flags [P.], seq 1:377, ack 1, win 29200,
length 376
        0x0000:  4500 01a0 b6bd 4000 4006 4708 ac10 0184  E.....@.@.G.....
        0x0010:  9fcb ee32 d9bf 0050 82f4 b80e 9b03 4121  ...2...P......A!
        0x0020:  5018 7210 3d25 0000 4745 5420 2f20 4854  P.r.=%..GET./.HT
        0x0030:  5450 2f31 2e31 0d0a 486f 7374 3a20 6174  TP/1.1..Host:.at
        0x0040:  7461 636b 6469 7265 6374 2e73 616d 7363  tackdirect.samsc
        0x0050:  6c61 7373 2e69 6e66 6f0d 0a55 7365 722d  lass.info..User-
        0x0060:  4167 656e 743a 204d 6f7a 696c 6c61 2f35  Agent:.Mozilla/5
```

Statistical Monitoring

- **Cisco NetFlow**
- **Number of packets & bytes in each "flow" (session)**



Statistical Monitoring

Commercial visualization products available from Fluke, HP, Solarwinds, and IBM

Link Ch 9c

flow-tools and argus

- **Open-source**
- **Convert pcap file (from tcpdump) to Argus format**
- **Graph all packets > 68 bytes from server1 by port number**

```
argus -mAJRU 512  -r serverFarm_1.pcap -w serverFarm_1.pcap.arg3
```

```
ragraph dbytes dport -M 1s -fill -stack -r serverFarm_1.pcap.arg3 - tcp and
   dst bytes gt 68 host server1
```

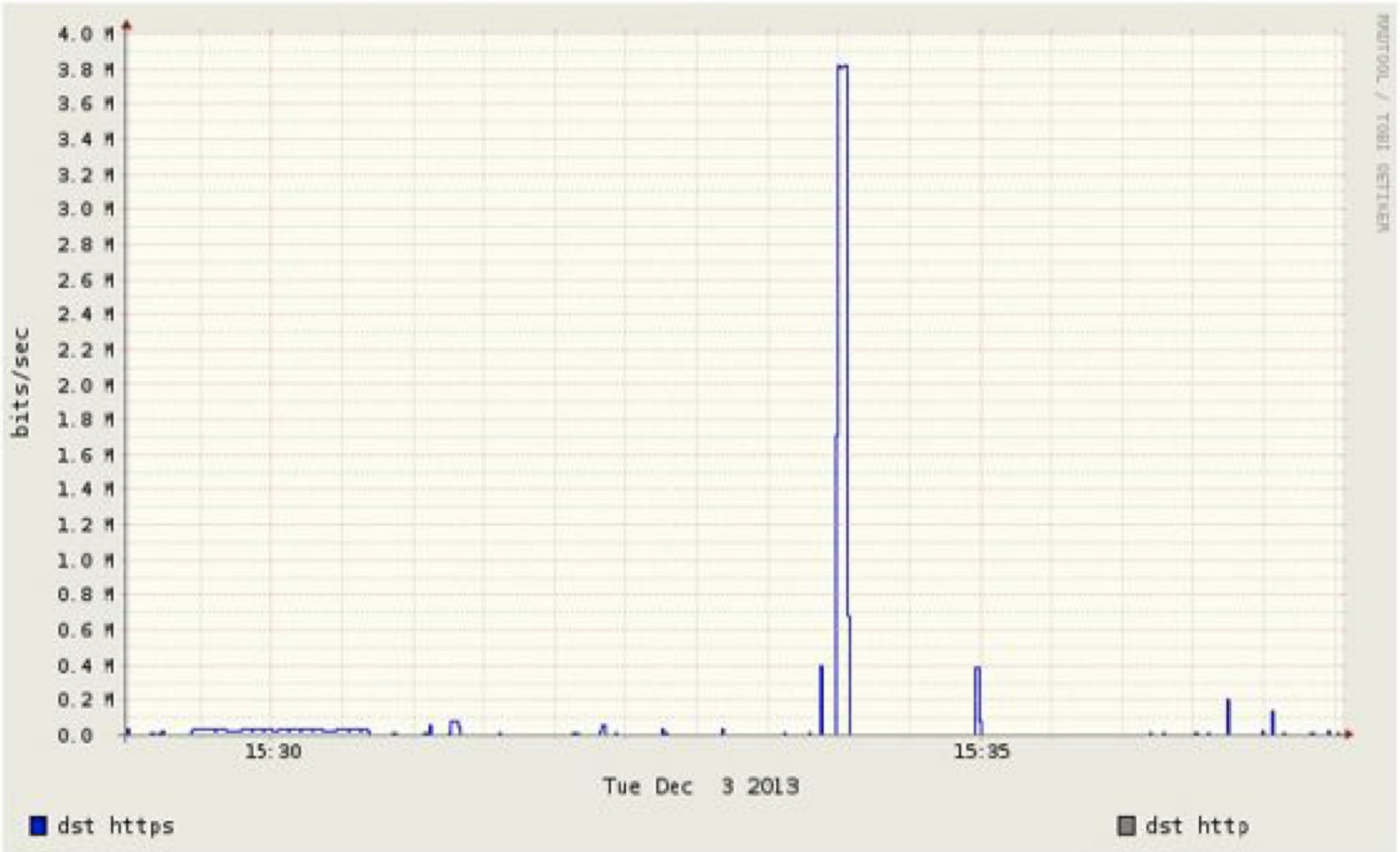


Figure 9-1. Unexpected server traffic

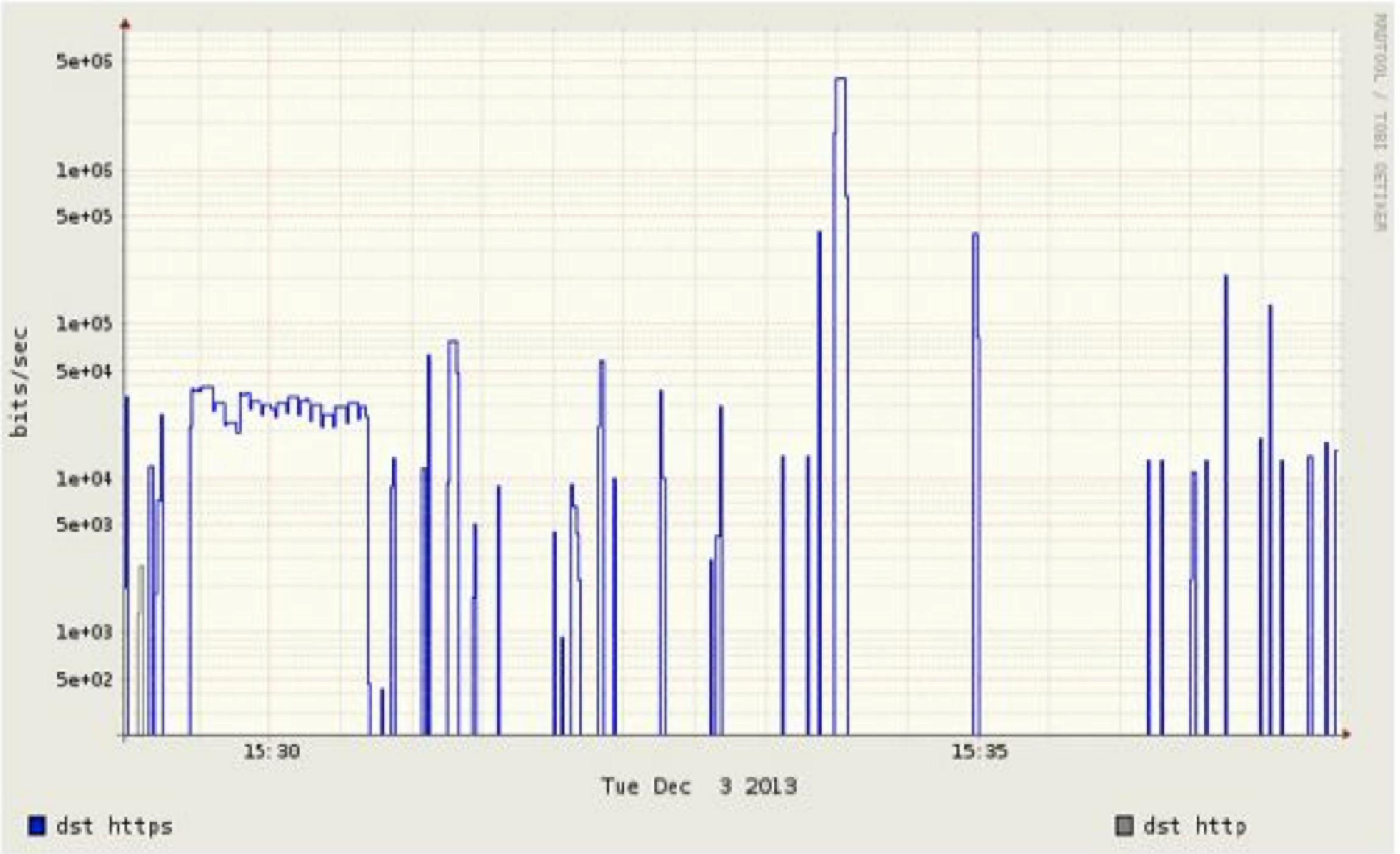


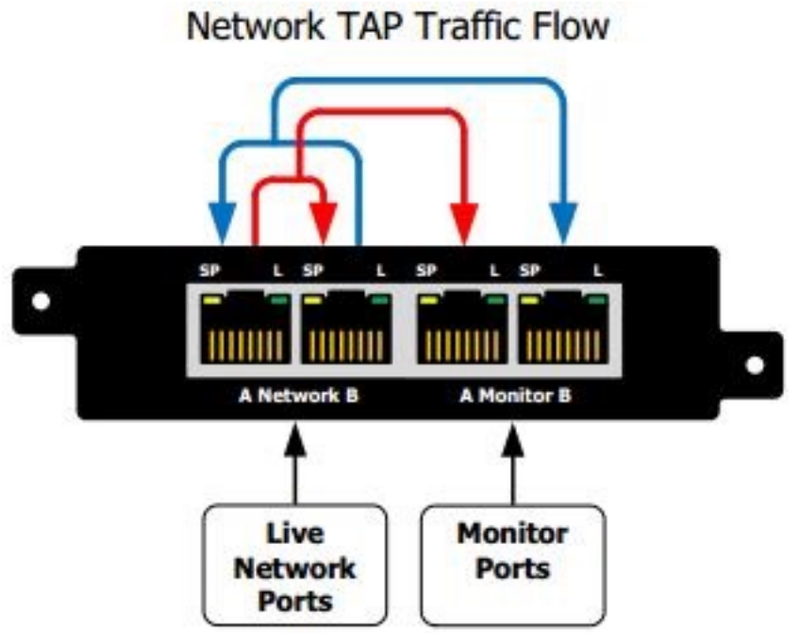
Figure 9-2. Unexpected server traffic—log scale

9a

Setting Up a Network Monitoring System

Simple Method

- **Deploy laptops or 1U servers with hardware network taps**
- **Snort + tcpdump works**
- **Best if you are setting up monitoring after an incident is detected--fast & easy**



IDS Limitations

- **IDS platforms cannot reliably perform both intrusion detection and network surveillance simultaneously**
- **If you set an IDS to capture full-content, its effectiveness as a sensor will diminish**

Effective Network Surveillance

- **Define your goals for performing the network surveillance.**
- **Ensure that you have the proper legal standing to perform the monitoring activity.**
- **Acquire and implement the proper hardware and software.**
- **Ensure the security of the platform, both electronically and physically.**
- **Ensure the appropriate placement of the monitor on the network.**
- **Evaluate the data captured by your network monitor to ensure you meet the goals you defined.**

Hardware

- **Difficult to collect and store every packet traversing high-speed links**
- **Recommended:**
  - **1U servers from large manufacturers**
  - **Linux-based network monitoring distributions**
  - **Linux now outperforms FreeBSD**
  - **For best performance, use NTOP's PF_RING network socket, not the default AF_PACKET interface**

Before an Incident

- **If your organization plans ahead**
- **Commercial solutions combine Snort-style alerting with storage**

Intrusion detection and prevention system (IDPS): Cisco

Intrusion detection and prevention systems (IDPS) monitor systems by signature or anomaly-based intrusion behavior. IDPS has threat detection, smart alerting, and automatic blocking capabilities.

Cisco Next-Gen IPS (NGIPS)

Cisco's acquisition of Sourcefire in 2013 brought to the networking giant the Firepower Next-Generation Intrusion Prevention System (NGIPS). With NGIPS, Cisco promises to stop more threats, increase malware detection rates, and provide threat insights to enable security automation. The ability to configure over 4,000 commercial applications and vendor support for configuring custom applications points to the granular control network administrators can have over traffic between segments. Cisco sits in our top IDPS products as well as our top BAS solutions.

Runner up: Trend Micro TippingPoint TPS

Our second listing of multinational cybersecurity firm Trend Micro is their IDPS line of solutions, the TippingPoint Threat Protection System (TPS) family. Trend Micro boasts that TippingPoint goes beyond next-gen IPS in offering threat protection, dynamic scalability, deep inspection, and flexible deployment. TippingPoint features that stand out include on-box SSL inspection, enterprise vulnerability remediation (eVR), and asymmetric traffic inspection. Trend Micro currently offers TippingPoint TPS in four models fit for organizations of varying sizes.

- From 2021 https://www.esecurityplanet.com/products/best-network-security-tools/

Security Onion

- **Free Linux distribution, with kernel patches installed (securityonion.net)**
- **Includes analysis tools**

DNS Long Tail Analysis

hostname	Count ▾
jdtcjdyqjyousia.com	1
www.whatsmyipaddress.com	1
lifeinsidedetroit.com	1
etgibmyhmbzjoyut1.com	1
www.getmyip.org	1
checkip.dyndns.org	1
qwe.mvdunalterableairreport.net	1
zcjipitikrhabk.com	1
xxrdwspble4u.com	1
adstairs.ro	1
freeways.in	1
analytics.shareaholic.com	1

Deploying the Network Sensor

- **Where are the network egress points?**
- **Does the network use specific routes to control internal traffic? External traffic?**
- **Are “choke points” available at suborganization or administrative boundaries?**
- **How is endpoint traffic encapsulated when it arrives at firewalls or “choke points”? Is VLAN trunking in use, for example?**
- **Where are network address translation devices in use? Web proxies?**

Major Network Changes

- **May facilitate network surveillance**
  - **Ex: route all company locations through a single Internet connection with MPLS (Multiprotocol Label Switching), not a separate ISP for each office**

Secure Sensor Deployment

- **Place network sensor in a locked room, to maintain chain of custody**
- **Patch the OS, keep it up to date**
- **Protect it from unauthorized access**
- **Document everything**
- **Review logs**
- **Use Tripwire to ensure integrity of OS**

Evaluating Your Network Monitor

- **Is it receiving the traffic you want to monitor?**
- **Is the hardware responsive enough to achieve your goals?**
- **Create signatures to detect test traffic and test your monitor**
  - **Such as a nonexistent URL**
- **Performance metrics in logs will tell you if the sensor is dropping packets**

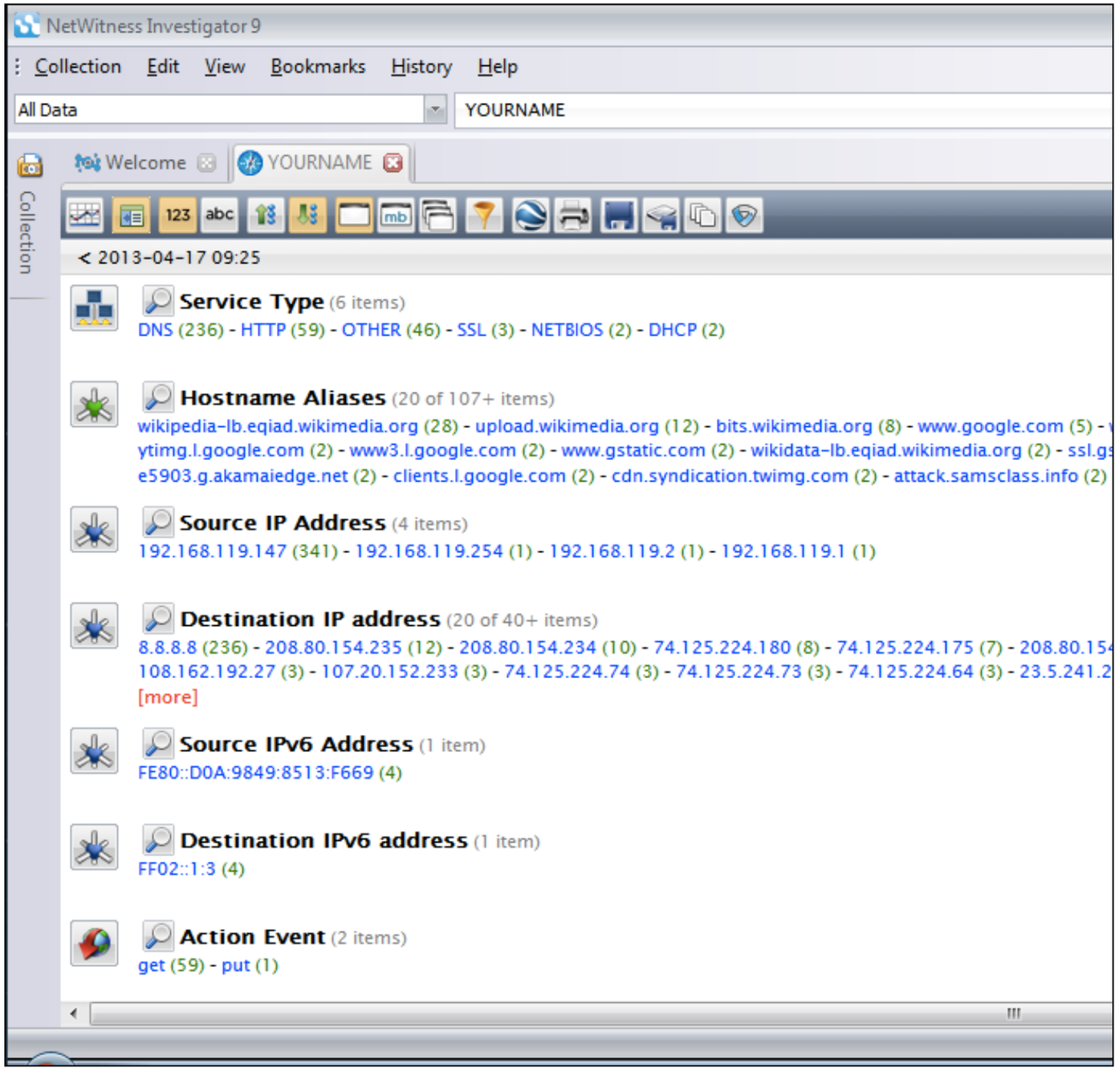
Network Data Analysis

General Principles

- **Wireshark is excellent**
  - **Especially with custom decoders, written in Lua or C**
- **Don't hunt through large packet captures looking for something new**
- **Limit the scope**
- **Use targeted queries that follow your leads and answer investigative questions**

NetWitness Investigator

- **Sorts traffic by protocol**
- **32-bit version seems to be gone**



Collect Logs Generated from Network Events

Examples

- **Routers, firewalls, servers, IDS sensors, and other network devices may maintain logs that record network-based events.**
- **DHCP servers log network access when a system requests an address.**
- **Firewalls allow administrators an extensive amount of granularity when creating audit logs.**

Examples

- **IDS sensors may catch a portion of an attack due to a signature recognition or anomaly detection filter.**
- **Host-based sensors may detect the alteration of a system library or the addition of a file in a sensitive location.**
- **System log files from the primary domain controller several zones away may show a failed authentication during a logon attempt.**

Network-Based Logs

- **Server-based logs are files on the individual systems**
  - **May be altered or deleted by the attacker**
- **Network-based logs may be more reliable**
  - **Especially if network devices are physically and electronically secured**

Log Aggregation

- **Log aggregation is difficult because:**
  - **Logs are in different formats**
  - **Originate from different operating systems**
  - **May require special software to access and read**
  - **May have inaccurate timestamps**

9b