JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Intro to Cyber Incident Response

CYBER INCIDENT RESPONSE

What does this section cover?

- Phases of an incident response
- Creating an incident response team
- How to classify an incident
- Analyzing network events
- Detecting network probes and attacks

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

What does this section cover?

- Investigating issues on a host/server
- Investigating service and applications
- Building a basic forensic toolkit
- Capabilities of different forensic tools
- How to conduct a forensic investigation

What is Cyber Incident Response?

- Actions taken in response to a security incident or event
- An organized approach to understanding the incident, mitigating its negative effects, planning the recovery, and investigating the root cause

Bottom Line…

- We will discuss the high-level concepts of how to develop a cyber incident response program and how the incident response team should operate during a cyber incident, including the basics of digital forensics and its associated toolsets

JASON DION

TRAINING THE CYBER SECURITY WORKFORCE

Security Incidents

CYBER INCIDENT RESPONSE

Cyber Incidents Will Happen

- No matter what your organization does to prevent a cyber incident… eventually one will happen to you

- How will you respond?

- How will you react?

- How will you recover?

You Must Plan Your Response

- Plan in advance your response
- Allows you to have a coordinated and methodical response
- Prior planning minimizes the damage and decreases your response time

Security Events and Incidents

- Event
  - Any observable occurrence in a system or network
- Adverse Event
  - Any event that has negative consequences
- Incidents
  - An imminent threat of violation, or a violation itself, of a security policy, acceptable use policy, or standard security practice

Security Events and Incidents

Not every event is an incident,

but every incident contains

at least one event

Computer Security Incident Response Team (CSIRT)

Team of professionals responsible for handling a security incident within an organization by using a standardized procedures

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Incident Response Teams

CYBER INCIDENT RESPONSE

Creating the Team

- Members are permanent or temporary
- Core team is cybersecurity professionals with incident response experience
- Temporary members brought in for specific cases (like a DB Admin for SQL)
- Smaller organizations have CSIRT as a collateral role in addition to their day job

What does management do?

- Active role in an incident response
- Ensure team has funding, resources, and expertise needed to conduct incident response
- Make critical business decisions
- Communicate with legal or news media
- Communicate with key stakeholders

So, who is on the CSIRT?

- Leader is a skilled Incident Responder
- Subject matter experts
- IT support staff
- Legal counsel
- Human resource staff
- Public relations and marketing staff

Can you outsource the CSIRT?

- Retaining a third-party gives you instant capability without daily resourcing
- Can be very expensive
- Ensure your organization is comfortable with the third-party’s guaranteed response time
- Agree upon the scope of work to be performed

Scope of Control for a CSIRT

- What would trigger activation of CSIRT?
- Who authorizes the activation?
- Do they respond for all parts of the organization, or just specific ones?
- Can CSIRT talk to law enforcement?
- Can CSIRT talk to the media?
- How would CSIRT escalate an issue?

Testing the Teams

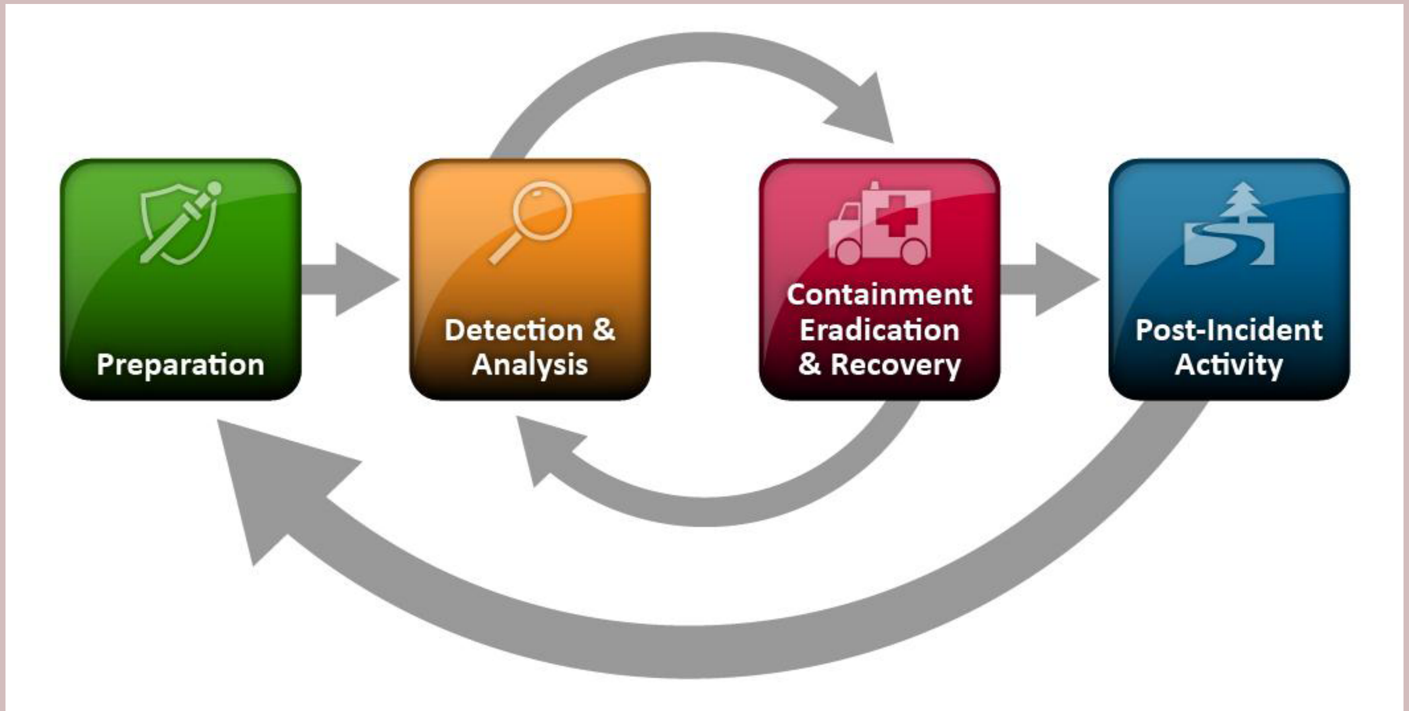
- Plans without testing are ineffective
- You must ensure the teams are trained and ready for an incident response
- Testing allows a walkthrough of the policy, procedures, and playbooks
- Can be combined with a penetration test to simulate a real attacker

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Incident Response Phases

CYBER INCIDENT RESPONSE

Incident Response Phases



This process is not linear…it is cyclical

NIST SP 800-61
(Computer Security Incident Handling Guide)

Preparation

- Takes preparation to build a well-prepared CSIRT
- Requires proper policy foundation within the organization
- Preparation includes building proper cyber defenses in the organization
- Also, includes identifying/training personnel and building response kits

Preparation: Toolkits

- Digital forensic workstations
- Forensic software
- Packet capture devices
- Spare servers/network gear
- Backup devices
- Blank removable media
- Collection, analysis, & reporting laptops
- Portable printers
- Office supplies
- Evidence collection materials

Detection and Analysis

- Hardest to standardize
- Tools help in detection, but it takes a trained analyst to understand all the details during analysis
- When detection occurs, analysts shift to validation mode, then into analysis
- Primarily passive activities designed to uncover and analyze incident

Detection and Analysis: Event Indicators

- Alerts
  - IDS/IPS, SIEM, Anti-virus, or other software alerts
- Logs
  - From operating systems, services, applications, network devices, and network flows
- Publically Available Information
  - News, media, and other open-source information
- People
  - Suspicious activity reported by users or admins

Detection and Analysis: Best Practices for Analysis

- Profile networks/systems
- Understand the baseline
- Create good logging policies
- Conduct event correlation
- Synchronize network & system clocks
- Maintain organization knowledge base
- Capture network traffic ASAP in incident
- Filter information to reduce confusion
- Know when to bring in outside help

Containment, Eradication, and Recovery

- Focuses on stopping the spread of the incident, remove it from the network, and recovering from it

- Phase focuses on active detection and removal of the incident

Containment, Eradication, and Recovery (5 Steps)

1. Pick containment strategy
2. Use strategy to limit the damage incident causes
3. Gather evidence needed for potential future legal actions
4. Identify attacking system or attacker
5. Remove effects of incident and recover normal business operations

Post-Incident Activities

- CSIRT isn’t done once the incident is contained and eradicated, they still need to conduct:
  - Event reconstruction
  - Lessons learned
  - Evidence retention

Post-Incident Activities: Event Reconstruction

- Recreate a timeline of the incident
- Identify the root cause of the intrusion and/or incident
- Conduct consultations with system administrators and management

Post-Incident Activities: Lessons Learned

- Utilizes the timeline to aid improvement of procedures and tools used by CSIRT
- Group discussion to determine how the incident was handled, and how it could have been handled better.
- Lessons learned must be fed into the ITSM processes in order to follow-on actions to be taken

Post-Incident Activities: Lessons Learned

- What happened and when?
- How did staff perform?
- Were procedures followed?
- Were procedures adequate?
- What should have been done differently?
- Was information shared effectively?
- How could we detect incident sooner?
- What new tools or resources does the organization need?

Post-Incident Activities: Evidence Retention

- Large quantities of evidence have been collected

- What do we do with it all?
- CSIRT must identify internal/external retention requirements

If legal actions will be conducted, consult an attorney before deleting anything!

Post-Incident Activities:
Evidence Retention Timelines

- US Government Agencies must retain all incident handling items for **3 years** due to legal requirements

- Most organizations maintain records for **2 years**, unless otherwise required by regulatory requirements

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Policy & Procedures

CYBER INCIDENT RESPONSE

Incident Response Policy

- Foundation of the organization’s Incident Response program
- Guides efforts at a high-level
- Provides authority for response efforts
- Approved by CEO or CIO
- Should be fairly timeless

Contents of the Policy

- Statement of management commitment
- Purpose
- Objectives
- Scope of policy
- Definitional terms
- Roles, responsibilities, and authority
- Incident prioritization scheme
- Measures of performance for CSIRT
- Reporting requirements
- Contact information

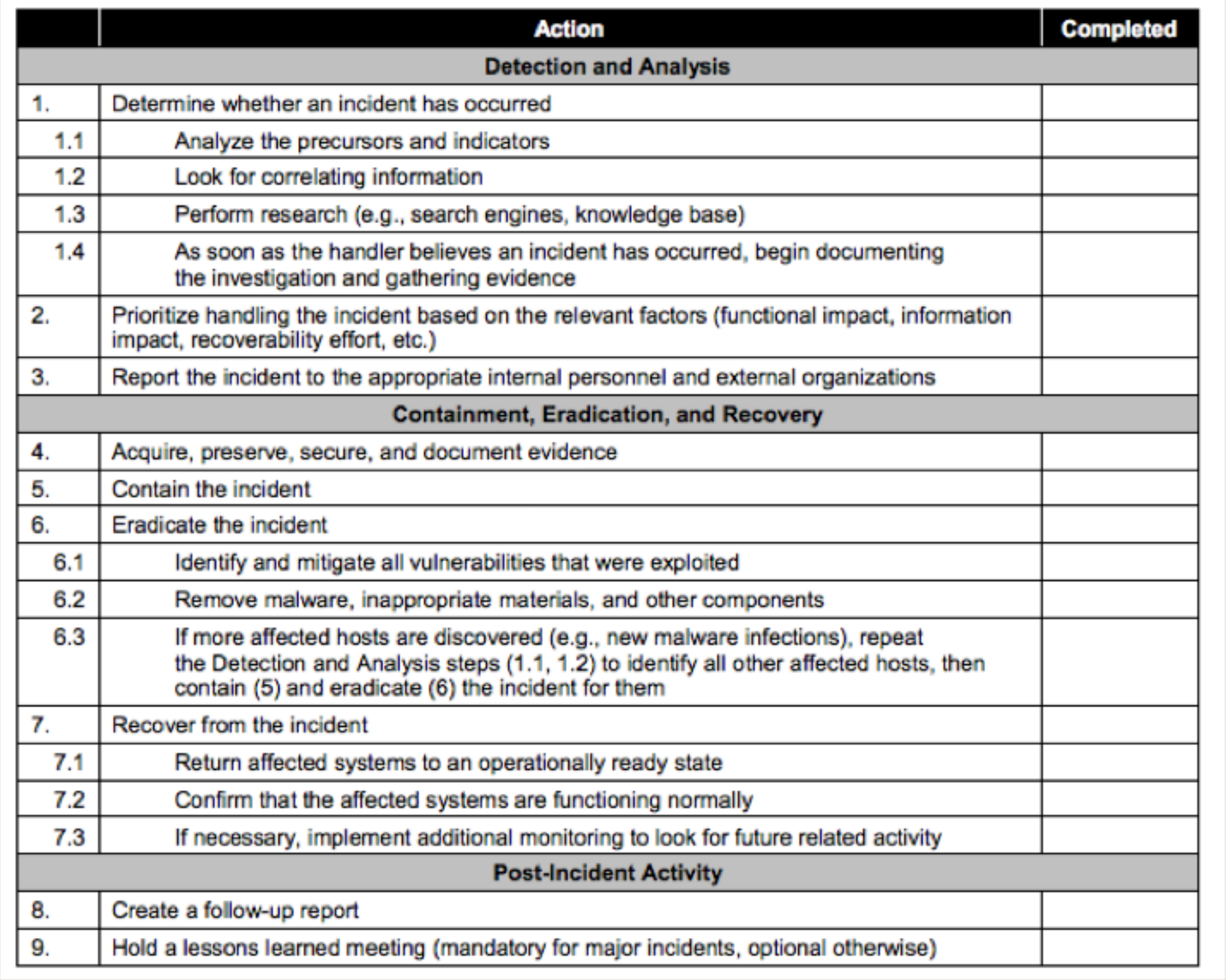
Incident Response Procedures

- Detailed information
- Step-by-step guidelines
- Not a replacement for CSIRT's professional judgement and expertise
- Often developed as a specific *playbook*

What is a Playbook?

- Describes a response to a high severity type of incident, such as:
  - Data breach of financial information
  - Data breach of personally identifiable information
  - Phishing attack against customers
  - Web server defacements
  - Loss of corporate laptop
  - Intrusion into the corporate network
  - Windows Golden Ticket reset

Incident Response Checklist



	Action	Completed
	Detection and Analysis	
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.	Report the incident to the appropriate internal personnel and external organizations	
	Containment, Eradication, and Recovery	
4.	Acquire, preserve, secure, and document evidence	
5.	Contain the incident	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
	Post-Incident Activity	
8.	Create a follow-up report	
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	

NIST SP 800-61

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

JASON DION

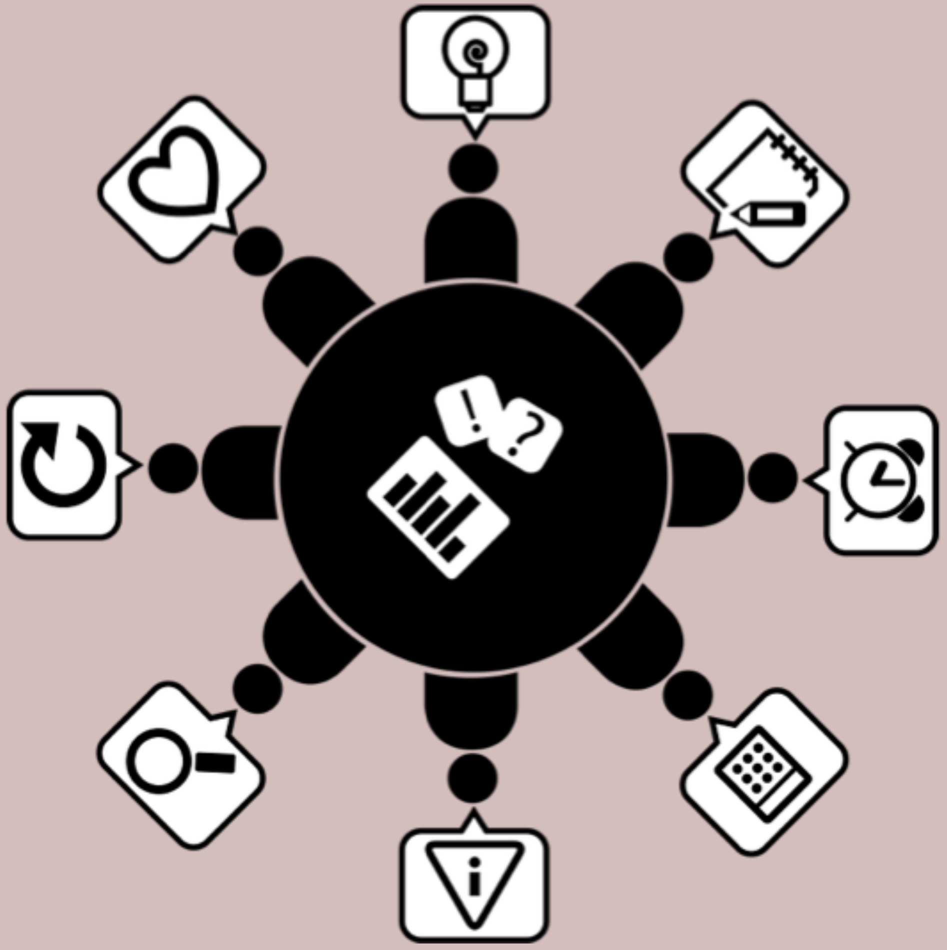
TRAINING THE CYBER SECURITY WORKFORCE

Communication and Info Sharing

CYBER INCIDENT RESPONSE

Communication and Info Sharing

- During an incident, how will your communicate and share information?



Internal Communication

- How will the CSIRT communicate amongst themselves and to leadership?

- How will management communicate to the other employees?

Internal Communication

- Incident response plan dictates how you will communicate during an incident
- Use an out-of-band communication

External Communication

- When will you communicate with outside people like law enforcement, media, shareholders, and others?

- Your incident response plan should state when…

JASON DION

TRAINING THE CYBER SECURITY WORKFORCE

External Communication

- Law Enforcement
  - If incident involves criminal acts (ask attorney first)
- Information Sharing Partners
  - Do you want to share indications of your incident?
- Vendors
  - Can provide patches and support during incident
- Other organizations affected
  - Do you have evidence others were targeted?
- Media or General Public
  - May be mandatory depending on type of incident
  - Do you volunteer the information to the media?

Incident Classification

CYBER INCIDENT RESPONSE

Incident Classification

- All incidents should be classified by their threat and severity
- Allows comparison of current incident with past and future ones
- Aids in personnel’s understanding of the incident being worked on

Classifying Threats

- External or Removable Media
  - Attack executed by removable media or peripheral
- Attrition
  - Attack employing brute-force to compromise, deny, or degrade services, systems, or networks
- Web
  - Attack executed from web-based application or site
- Email
  - Attack executed from email or attachment

Classifying Threats

- Impersonation
  - Attack that replaces something benign with something malicious (spoofing, SQL inject, etc)
- Improper Usage
  - Violation of organization’s AUP (P2P program)
- Loss or Theft of Equipment
  - Computing device or media is lost or stolen
- Unknown
  - Attack that comes from an unknown origin

Classifying Threats

- Other
  - Attack that comes from a known origin, but doesn’t fit into the other categories
- Advanced Persistent Threat (APT)
  - Not a category under NIST, but prevalent today
  - Often funded by nation stations, organized crime, or other sources
  - Highly skilled and sophisticated attackers
  - Often takes advantage of zero-day vulnerabilities

Classifying Severity: Scope of Impact

- Degree of impairment that an incident causes an organization and the effort to recover from the incident
- Functional impact
  - Degree of impairment to an organization
- Economic impact
  - Amount of financial loss to an organization
- Recoverability impact
  - Amount of time lost by an organization

Classifying Severity: Scope of Impact

- Functional impact
  - Degree of impairment to an organization

Category	Definition
None	None; No effect to the organization’s ability to provide all services to all users
Low	Minimal effect; the organization can still provide all critical services to all users but has lost efficiency
Medium	Organization has lost the ability to provide a critical service to a subset of system users
High	Organization is no longer able to provide some critical services to any users

NIST 800-61(Table 3-2)

Classifying Severity: Scope of Impact

- Economic impact
  - Amount of financial loss to an organization

Category	Definition
None	None; No financial loss experienced by the organization
Low	Minimal effect; the organization expects to experience a loss of $25,000 or less
Medium	Organization expects to experience a loss of $25,000 to $999,999
High	Organization expects to experience a loss of $1,000,000 or more

Not covered by NIST 800-61

Classifying Severity: Scope of Impact

- Recoverability impact
  - Amount of time lost by an organization

Category	Definition
Regular	Time to recovery is predictable with existing resources
Supplemented	Time to recovery is predictable with additional resources
Extended	Time to recovery is unpredictable; additional resources and outside help are needed
Not Recoverable	Recovery from the incident is not possible (such as sensitive data exfiltrated and posted publically); launch investigation

NIST 800-61 (Table 3-4)

Classifying Severity: Types of Data

- The type of data involved in the incident also affects the classification of severity

- Information impact
  - Degree of information compromise during incident

Classifying Severity: Types of Data

- Information impact (Government)
  - Degree of information compromise during incident

Category	Definition
None	No information was exfiltrated, changed, deleted, or otherwise compromised
Privacy Breach	Sensitive PII of taxpayers, employees, beneficiaries, etc was access or exfiltrated
Proprietary Breach	Unclassified proprietary information, such as protected critical infrastructure information was accessed or exfiltrated
Integrity Loss	Sensitive or proprietary information was changed or deleted

NIST 800-61 (Table 3-3)

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Classifying Severity: Types of Data

- Information impact (Private Company)
  - Degree of information compromise during incident

Category	Definition
None	No information was exfiltrated, changed, deleted, or otherwise compromised
Regulated Information Breach	Information regulated by an external compliance obligation was accessed or exfiltrated (GLBA, SOX, HIPAA, etc)
Intellectual Proprietary Breach	Sensitive proprietary information was accessed or exfiltrated
Confidential Proprietary Breach	Corporate confidential information was accessed or exfiltrated
Integrity Loss	Sensitive or proprietary information was changed or deleted

Not covered by NIST 800-61

Network Event Monitoring

CYBER INCIDENT RESPONSE

Network Event Monitoring

- Network event analysis is a common task for cybersecurity analysts
- Gather, correlate, and analyze data from different systems/sensors on network
- Used to detect or prevent incidents

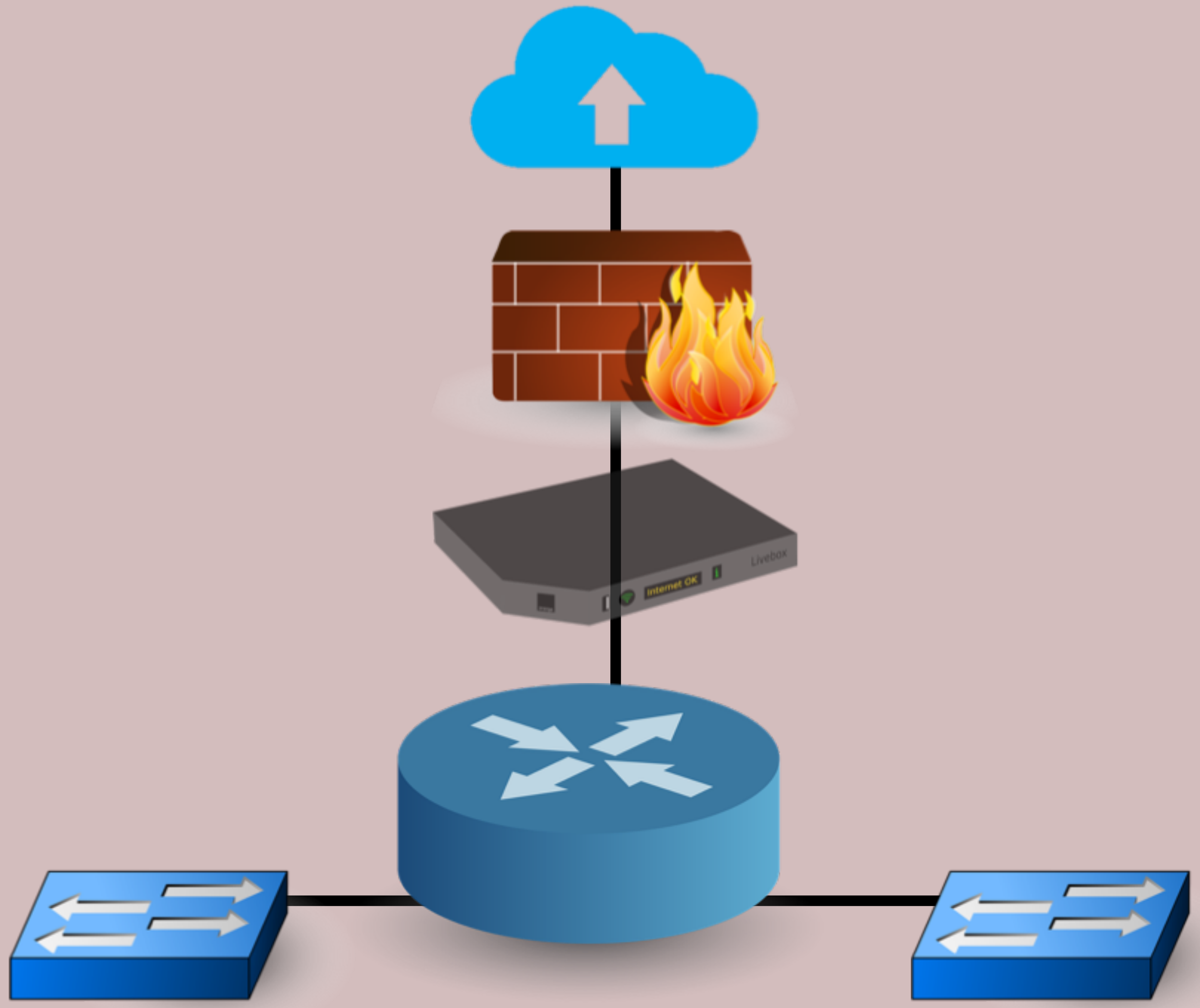
Router-based Monitoring

- Provides data flow on the network and information on the status of the device
- Relies on capturing the data about the traffic passing through a router
- Called *network flows*

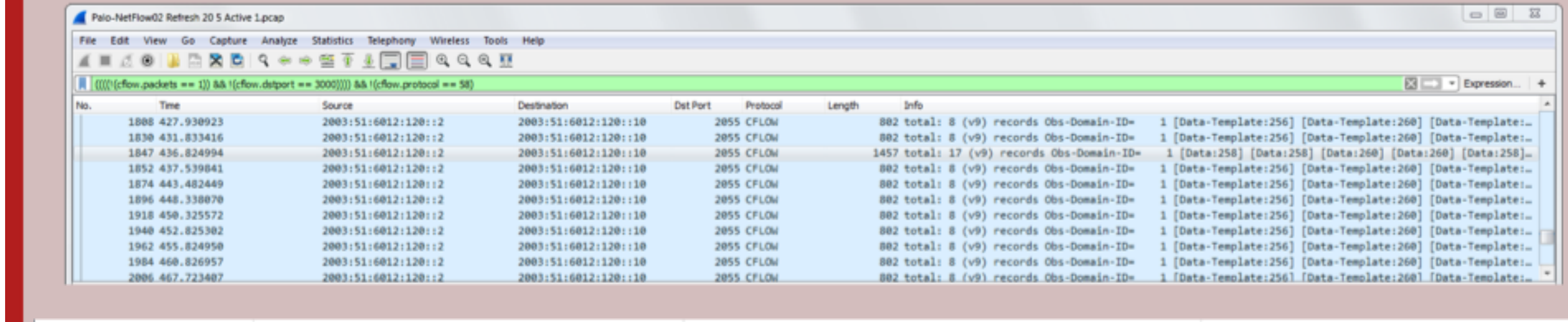
Network Flows

- Netflow, sFlow, J-Flow, …
  - All are standards for monitoring traffic flows
  - Count information about the traffic at the interface
  - Samples traffic (1:100, 1:1000, etc)
- RMON
  - Operates at layers 1, 2, 3, 4 of the OSI model
  - Operates as client/server model with probes
  - Provides statistics, history, alarms, and events to a Management Information Base (MIB)
- SNMP (Simple Network Management)
  - Collects information about routers/switches
  - Information is about the devices themselves, not the traffic crossing those devices

Network Flows

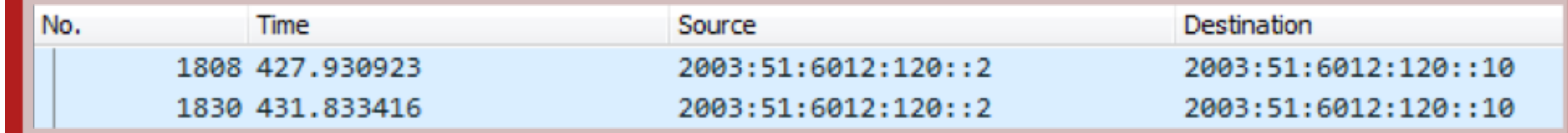


Example Network Flows

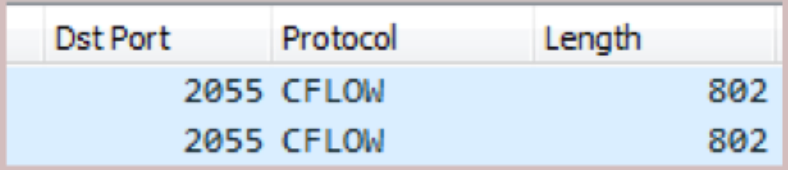


```
((((!(cflow.packets == 1)) && !(cflow.dstport == 3000)))) && !(cflow.protocol == 58)
```

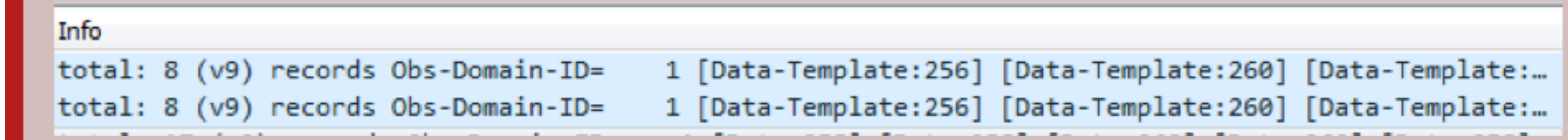
```
No.     Time        Source                  Destination              Dst Port Protocol  Length Info
   1808 427.930923  2003:51:6012:120::2     2003:51:6012:120::10     2055 CFLOW        802 total: 8 (v9) records Obs-Domain-ID=    1 [Data-Template:256] [Data-Template:260] [Data-Template:…
   1830 431.833416  2003:51:6012:120::2     2003:51:6012:120::10     2055 CFLOW        802 total: 8 (v9) records Obs-Domain-ID=    1 [Data-Template:256] [Data-Template:260] [Data-Template:…
   1847 436.824994  2003:51:6012:120::2     2003:51:6012:120::10     2055 CFLOW       1457 total: 17 (v9) records Obs-Domain-ID=    1 [Data:258] [Data:258] [Data:260] [Data:260] [Data:258]…
   1852 437.539841  2003:51:6012:120::2     2003:51:6012:120::10     2055 CFLOW        802 total: 8 (v9) records Obs-Domain-ID=    1 [Data-Template:256] [Data-Template:260] [Data-Template:…
   1874 443.482449  2003:51:6012:120::2     2003:51:6012:120::10     2055 CFLOW        802 total: 8 (v9) records Obs-Domain-ID=    1 [Data-Template:256] [Data-Template:260] [Data-Template:…
   1896 448.338070  2003:51:6012:120::2     2003:51:6012:120::10     2055 CFLOW        802 total: 8 (v9) records Obs-Domain-ID=    1 [Data-Template:256] [Data-Template:260] [Data-Template:…
   1918 450.325572  2003:51:6012:120::2     2003:51:6012:120::10     2055 CFLOW        802 total: 8 (v9) records Obs-Domain-ID=    1 [Data-Template:256] [Data-Template:260] [Data-Template:…
   1940 452.825302  2003:51:6012:120::2     2003:51:6012:120::10     2055 CFLOW        802 total: 8 (v9) records Obs-Domain-ID=    1 [Data-Template:256] [Data-Template:260] [Data-Template:…
   1962 455.824950  2003:51:6012:120::2     2003:51:6012:120::10     2055 CFLOW        802 total: 8 (v9) records Obs-Domain-ID=    1 [Data-Template:256] [Data-Template:260] [Data-Template:…
   1984 460.826957  2003:51:6012:120::2     2003:51:6012:120::10     2055 CFLOW        802 total: 8 (v9) records Obs-Domain-ID=    1 [Data-Template:256] [Data-Template:260] [Data-Template:…
   2006 467.723407  2003:51:6012:120::2     2003:51:6012:120::10     2055 CFLOW        802 total: 8 (v9) records Obs-Domain-ID=    1 [Data-Template:256] [Data-Template:260] [Data-Template:…
```



No.	Time	Source	Destination
1808	427.930923	2003:51:6012:120::2	2003:51:6012:120::10
1830	431.833416	2003:51:6012:120::2	2003:51:6012:120::10



Dst Port	Protocol	Length
2055	CFLOW	802
2055	CFLOW	802

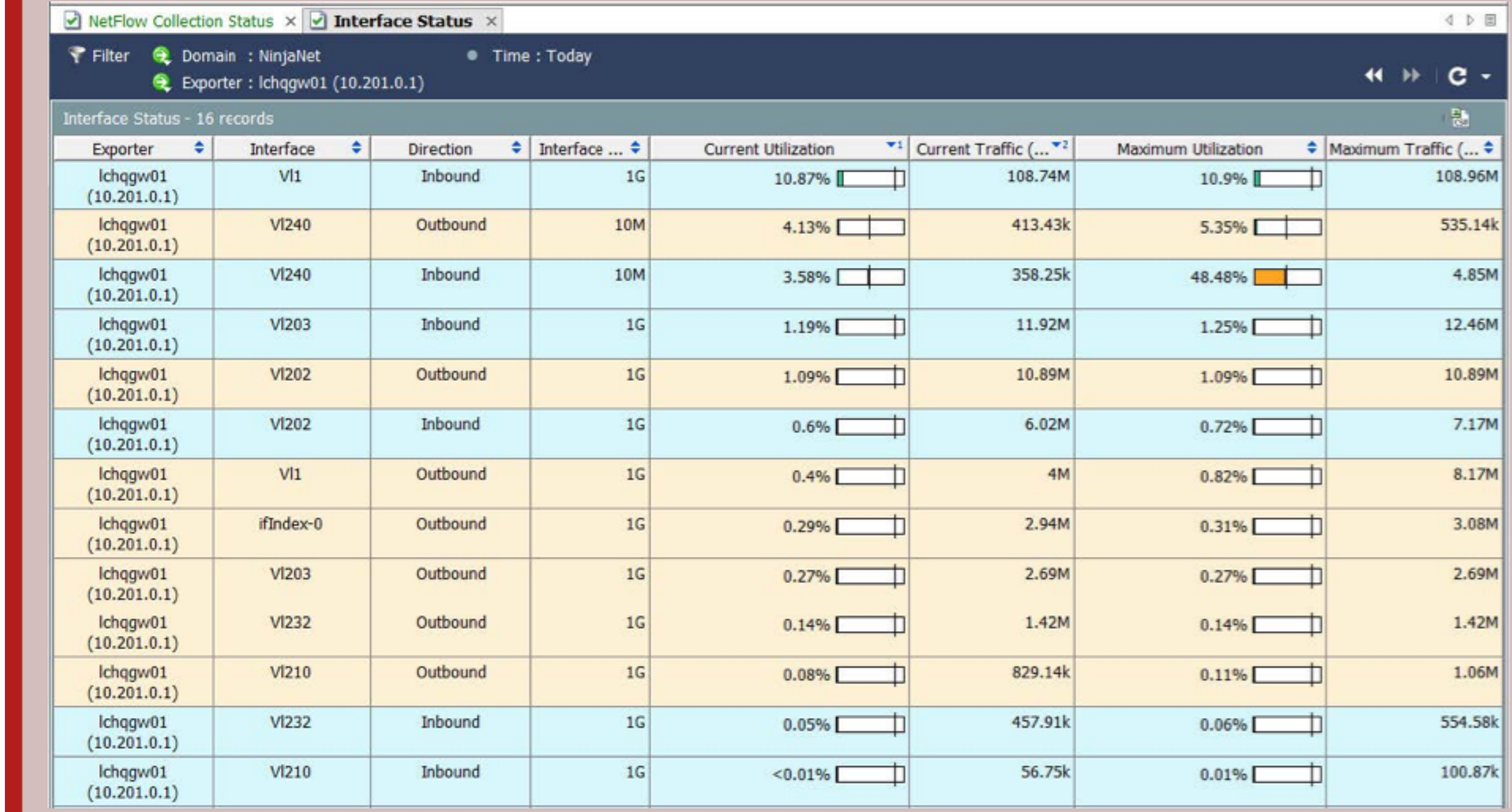


```
Info
total: 8 (v9) records Obs-Domain-ID=    1 [Data-Template:256] [Data-Template:260] [Data-Template:…
total: 8 (v9) records Obs-Domain-ID=    1 [Data-Template:256] [Data-Template:260] [Data-Template:…
```

JASON DION

TRAINING THE CYBER SECURITY WORKFORCE

Example Network Flows



Domain : NinjaNet

Time : Today

Exporter : lchqgw01 (10.201.0.1)

Interface Status - 16 records

Exporter	Interface	Direction	Interface ...	Current Utilization	Current Traffic (...	Maximum Utilization	Maximum Traffic (...
lchqgw01 (10.201.0.1)	Vl1	Inbound	1G	10.87%	108.74M	10.9%	108.96M
lchqgw01 (10.201.0.1)	Vl240	Outbound	10M	4.13%	413.43k	5.35%	535.14k
lchqgw01 (10.201.0.1)	Vl240	Inbound	10M	3.58%	358.25k	48.48%	4.85M
lchqgw01 (10.201.0.1)	Vl203	Inbound	1G	1.19%	11.92M	1.25%	12.46M
lchqgw01 (10.201.0.1)	Vl202	Outbound	1G	1.09%	10.89M	1.09%	10.89M
lchqgw01 (10.201.0.1)	Vl202	Inbound	1G	0.6%	6.02M	0.72%	7.17M
lchqgw01 (10.201.0.1)	Vl1	Outbound	1G	0.4%	4M	0.82%	8.17M
lchqgw01 (10.201.0.1)	ifIndex-0	Outbound	1G	0.29%	2.94M	0.31%	3.08M
lchqgw01 (10.201.0.1)	Vl203	Outbound	1G	0.27%	2.69M	0.27%	2.69M
lchqgw01 (10.201.0.1)	Vl232	Outbound	1G	0.14%	1.42M	0.14%	1.42M
lchqgw01 (10.201.0.1)	Vl210	Outbound	1G	0.08%	829.14k	0.11%	1.06M
lchqgw01 (10.201.0.1)	Vl232	Inbound	1G	0.05%	457.91k	0.06%	554.58k
lchqgw01 (10.201.0.1)	Vl210	Inbound	1G	<0.01%	56.75k	0.01%	100.87k

JASON DION

TRAINING THE CYBER SECURITY WORKFORCE

SNMP v3

- Simple Network Management Protocol
- Adds encryptions, authentication, and user capabilities to SNMP traffic
- SNMP v1 and SNMP v2 are considered obsolete and a security risk

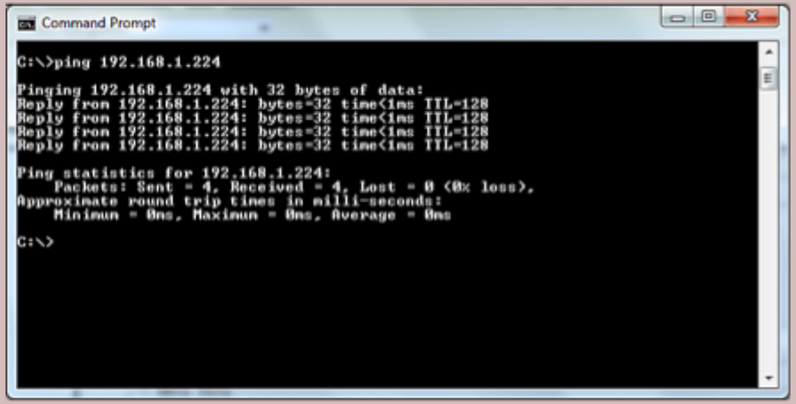
Active Monitoring

- Request is sent to a remote system and data is collected from the end point
- Data contains information about:
  - Availability
  - Routes
  - Packet delays
  - Packet loss
  - Bandwidth

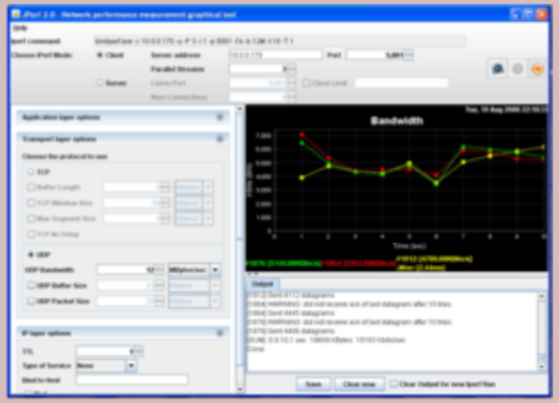
Active Monitoring (Examples)

- Ping
  - Data acquired by using ICMP on remote system
  - Basic up and down information and latency only

- iPerf
  - Measures maximum bandwidth of a given network
  - Remote testing of a link
  - Useful to determine a baseline of the network



```
C:\>ping 192.168.1.224

Pinging 192.168.1.224 with 32 bytes of data:
Reply from 192.168.1.224: bytes=32 time<1ms TTL=128
Reply from 192.168.1.224: bytes=32 time<1ms TTL=128
Reply from 192.168.1.224: bytes=32 time<1ms TTL=128
Reply from 192.168.1.224: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.224:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```


JPerf 2.0 - Network performance measurement graphical tool
Client
Server
Application layer options
Transport layer options
TCP
UDP
IP layer options
Bandwidth
Time (sec)
Output
Save
Clear now
Clear Output for new Iperf Run

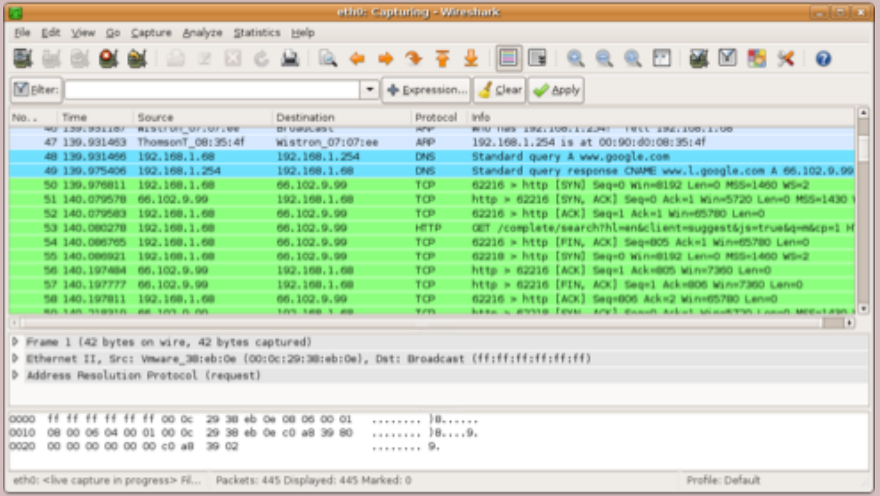
```
[1912] Sent 4112 datagrams
[1864] WARNING: did not receive ack of last datagram after 10 tries.
[1864] Sent 4445 datagrams
[1876] WARNING: did not receive ack of last datagram after 10 tries.
[1876] Sent 4426 datagrams
[SUM] 0.0-10.1 sec 18609 KBytes 15103 Kbits/sec
Done.
```

Passive Monitoring

- Uses a network tap to copy all traffic between two devices

- Useful for after-the-fact analysis

- Detailed information about:
  - Rate of traffic
  - Protocols used
  - Content


eth0: Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Clear
Apply

```
No. .  Time        Source              Destination         Protocol  Info
   47 139.931463  ThomsonT_08:35:4f   Wistron_07:07:ee    ARP       192.168.1.254 is at 00:90:d0:08:35:4f
   48 139.931466  192.168.1.68        192.168.1.254       DNS       Standard query A www.google.com
   49 139.975406  192.168.1.254       192.168.1.68        DNS       Standard query response CNAME www.l.google.com A 66.102.9.99
   50 139.976811  192.168.1.68        66.102.9.99         TCP       62216 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
   51 140.079578  66.102.9.99         192.168.1.68        TCP       http > 62216 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430
   52 140.079583  192.168.1.68        66.102.9.99         TCP       62216 > http [ACK] Seq=1 Ack=1 Win=65780 Len=0
   53 140.080278  192.168.1.68        66.102.9.99         HTTP      GET /complete/search?hl=en&client=suggest&js=true&q=m&cp=1 H
   54 140.086765  192.168.1.68        66.102.9.99         TCP       62216 > http [FIN, ACK] Seq=805 Ack=1 Win=65780 Len=0
   55 140.086921  192.168.1.68        66.102.9.99         TCP       62218 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
   56 140.197484  66.102.9.99         192.168.1.68        TCP       http > 62216 [ACK] Seq=1 Ack=805 Win=7360 Len=0
   57 140.197777  66.102.9.99         192.168.1.68        TCP       http > 62216 [FIN, ACK] Seq=1 Ack=806 Win=7360 Len=0
   58 140.197811  192.168.1.68        66.102.9.99         TCP       62216 > http [ACK] Seq=806 Ack=2 Win=65780 Len=0

▷ Frame 1 (42 bytes on wire, 42 bytes captured)
▷ Ethernet II, Src: Vmware_38:eb:0e (00:0c:29:38:eb:0e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▷ Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 00 0c  29 38 eb 0e 08 06 00 01   ........ )8......
0010  08 00 06 04 00 01 00 0c  29 38 eb 0e c0 a8 39 80   ........ )8....9.
0020  00 00 00 00 00 00 c0 a8  39 02                     ........ 9.

eth0: <live capture in progress> Fil...   Packets: 445 Displayed: 445 Marked: 0   Profile: Default
```

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Network Monitoring Tools

CYBER INCIDENT RESPONSE

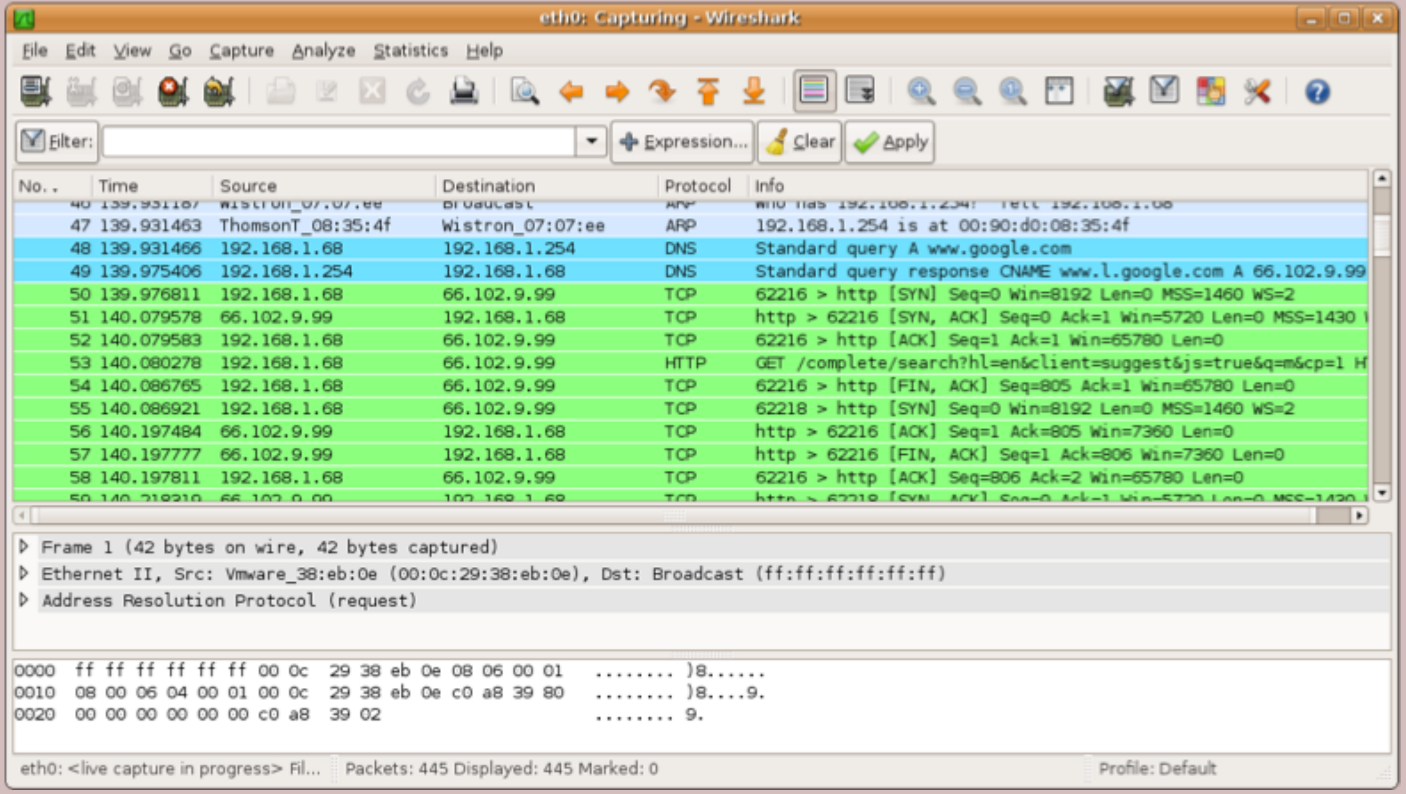
Network Monitoring Tools

- Many network monitoring tools are available for different use cases
- Combination of network data is more powerful than a single piece of data
- Different tools can analyze data in different ways, as well

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Wireshark

- Passive monitoring and packet capture
- Used for packet analysis


eth0: Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression...
Clear
Apply

```
No. .  Time        Source           Destination      Protocol  Info
   46 139.931187  Wistron_07:07:ee Broadcast        ARP       Who has 192.168.1.254?  Tell 192.168.1.68
   47 139.931463  ThomsonT_08:35:4f Wistron_07:07:ee ARP      192.168.1.254 is at 00:90:d0:08:35:4f
   48 139.931466  192.168.1.68     192.168.1.254    DNS       Standard query A www.google.com
   49 139.975406  192.168.1.254    192.168.1.68     DNS       Standard query response CNAME www.l.google.com A 66.102.9.99
   50 139.976811  192.168.1.68     66.102.9.99      TCP       62216 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
   51 140.079578  66.102.9.99      192.168.1.68     TCP       http > 62216 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 
   52 140.079583  192.168.1.68     66.102.9.99      TCP       62216 > http [ACK] Seq=1 Ack=1 Win=65780 Len=0
   53 140.080278  192.168.1.68     66.102.9.99      HTTP      GET /complete/search?hl=en&client=suggest&js=true&q=m&cp=1 H
   54 140.086765  192.168.1.68     66.102.9.99      TCP       62216 > http [FIN, ACK] Seq=805 Ack=1 Win=65780 Len=0
   55 140.086921  192.168.1.68     66.102.9.99      TCP       62218 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
   56 140.197484  66.102.9.99      192.168.1.68     TCP       http > 62216 [ACK] Seq=1 Ack=805 Win=7360 Len=0
   57 140.197777  66.102.9.99      192.168.1.68     TCP       http > 62216 [FIN, ACK] Seq=1 Ack=806 Win=7360 Len=0
   58 140.197811  192.168.1.68     66.102.9.99      TCP       62216 > http [ACK] Seq=806 Ack=2 Win=65780 Len=0
   59 140.218319  66.102.9.99      192.168.1.68     TCP       http > 62218 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 
```

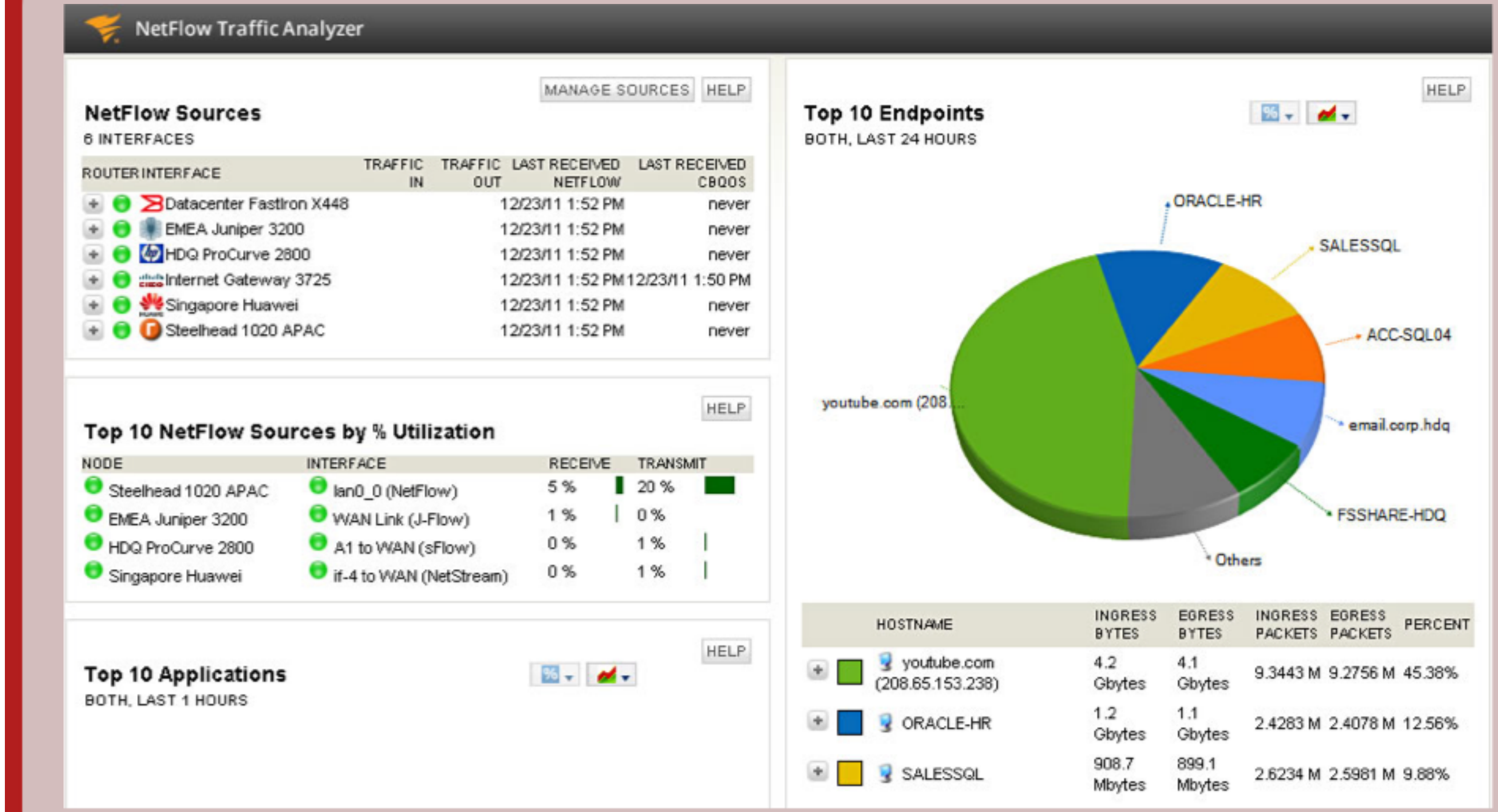
```
▷ Frame 1 (42 bytes on wire, 42 bytes captured)
▷ Ethernet II, Src: Vmware_38:eb:0e (00:0c:29:38:eb:0e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▷ Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff 00 0c  29 38 eb 0e 08 06 00 01   ........ )8......
0010  08 00 06 04 00 01 00 0c  29 38 eb 0e c0 a8 39 80   ........ )8....9.
0020  00 00 00 00 00 00 c0 a8  39 02                     ........ 9.
```

```
eth0: <live capture in progress> Fil...   Packets: 445 Displayed: 445 Marked: 0   Profile: Default
```

SolarWinds: NetFlow Traffic Analyzer

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE



NetFlow Traffic Analyzer

NetFlow Sources

6 INTERFACES

MANAGE SOURCES HELP

ROUTER INTERFACE	TRAFFIC IN	TRAFFIC OUT	LAST RECEIVED NETFLOW	LAST RECEIVED CBQOS
Datacenter FastIron X448			12/23/11 1:52 PM	never
EMEA Juniper 3200			12/23/11 1:52 PM	never
HDQ ProCurve 2800			12/23/11 1:52 PM	never
Internet Gateway 3725			12/23/11 1:52 PM	12/23/11 1:50 PM
Singapore Huawei			12/23/11 1:52 PM	never
Steelhead 1020 APAC			12/23/11 1:52 PM	never

Top 10 NetFlow Sources by % Utilization

HELP

NODE	INTERFACE	RECEIVE	TRANSMIT
Steelhead 1020 APAC	lan0_0 (NetFlow)	5 %	20 %
EMEA Juniper 3200	WAN Link (J-Flow)	1 %	0 %
HDQ ProCurve 2800	A1 to WAN (sFlow)	0 %	1 %
Singapore Huawei	if-4 to WAN (NetStream)	0 %	1 %

Top 10 Applications

BOTH, LAST 1 HOURS

HELP

Top 10 Endpoints

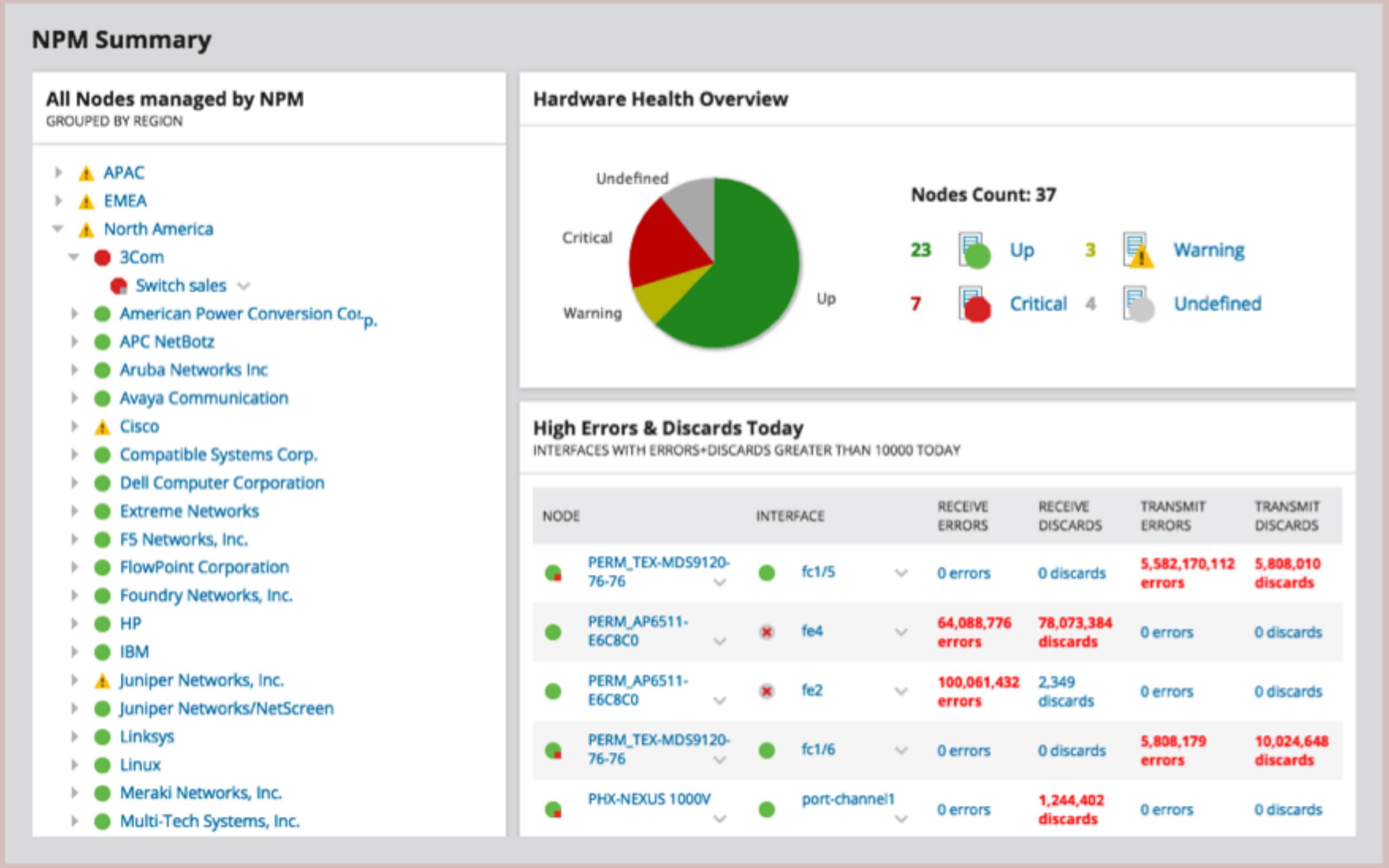
BOTH, LAST 24 HOURS

HELP

HOSTNAME	INGRESS BYTES	EGRESS BYTES	INGRESS PACKETS	EGRESS PACKETS	PERCENT
🟩 youtube.com (208.65.153.238)	4.2 Gbytes	4.1 Gbytes	9.3443 M	9.2756 M	45.38%
🟦 ORACLE-HR	1.2 Gbytes	1.1 Gbytes	2.4283 M	2.4078 M	12.56%
🟨 SALESSQL	908.7 Mbytes	899.1 Mbytes	2.6234 M	2.5981 M	9.88%

http://demo.solarwinds.com

SolarWinds:
Network Performance Monitor



NPM Summary

All Nodes managed by NPM
GROUPED BY REGION

- ▸ ⚠ APAC
- ▸ ⚠ EMEA
- ▾ ⚠ North America
  - ▾ ● 3Com
    - ● Switch sales ⌄
  - ▸ ● American Power Conversion Corp.
  - ▸ ● APC NetBotz
  - ▸ ● Aruba Networks Inc
  - ▸ ● Avaya Communication
  - ▸ ⚠ Cisco
  - ▸ ● Compatible Systems Corp.
  - ▸ ● Dell Computer Corporation
  - ▸ ● Extreme Networks
  - ▸ ● F5 Networks, Inc.
  - ▸ ● FlowPoint Corporation
  - ▸ ● Foundry Networks, Inc.
  - ▸ ● HP
  - ▸ ● IBM
  - ▸ ⚠ Juniper Networks, Inc.
  - ▸ ● Juniper Networks/NetScreen
  - ▸ ● Linksys
  - ▸ ● Linux
  - ▸ ● Meraki Networks, Inc.
  - ▸ ● Multi-Tech Systems, Inc.

Hardware Health Overview

Nodes Count: 37

23	Up	3	Warning
7	Critical	4	Undefined

High Errors & Discards Today
INTERFACES WITH ERRORS+DISCARDS GREATER THAN 10000 TODAY

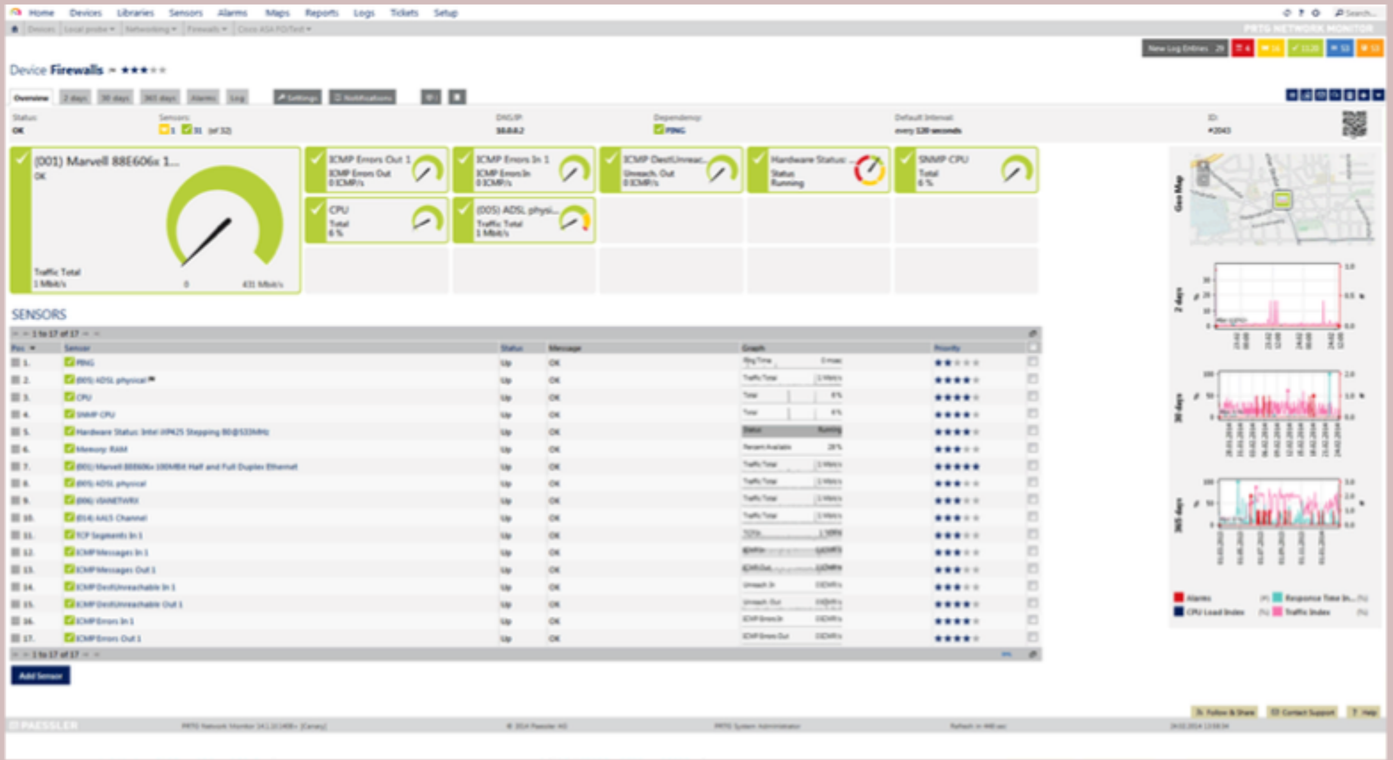
NODE	INTERFACE	RECEIVE ERRORS	RECEIVE DISCARDS	TRANSMIT ERRORS	TRANSMIT DISCARDS
● PERM_TEX-MDS9120-76-76 ⌄	● fc1/5 ⌄	0 errors	0 discards	5,582,170,112 errors	5,808,010 discards
● PERM_AP6511-E6C8C0 ⌄	✖ fe4 ⌄	64,088,776 errors	78,073,384 discards	0 errors	0 discards
● PERM_AP6511-E6C8C0 ⌄	✖ fe2 ⌄	100,061,432 errors	2,349 discards	0 errors	0 discards
● PERM_TEX-MDS9120-76-76 ⌄	● fc1/6 ⌄	0 errors	0 discards	5,808,179 errors	10,024,648 discards
● PHX-NEXUS 1000V ⌄	● port-channel1 ⌄	0 errors	1,244,402 discards	0 errors	0 discards

http://demo.solarwinds.com

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

PRTG

- Paessler Router Traffic Grapher
- Server monitoring, network monitoring, and bandwidth monitoring

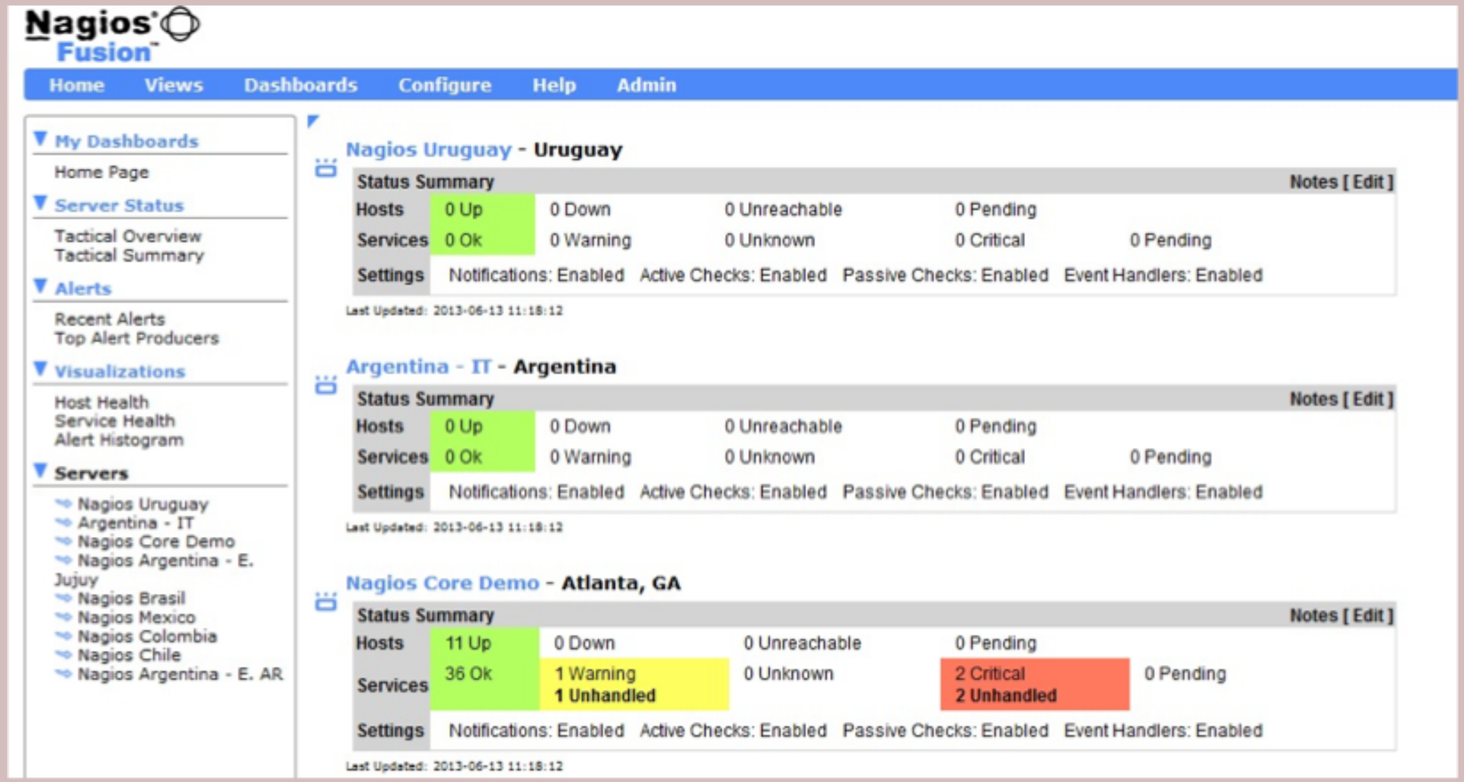


PRTG

- Packet sniffing
  - Monitors packet headers to determine traffic type
- Flows
  - Collects information about connections
- SNMP
  - Network devices report about events through traps
- WMI (Windows Management Instrumentation)
  - Management data of the operating system using scripts or application access

Nagios

- Network and system log monitoring tool
- Provides GUI for system, services, and monitoring capabilities



Nagios Uruguay - Uruguay

Status Summary					Notes [Edit]
Hosts	0 Up	0 Down	0 Unreachable	0 Pending	
Services	0 Ok	0 Warning	0 Unknown	0 Critical	0 Pending
Settings	Notifications: Enabled	Active Checks: Enabled	Passive Checks: Enabled	Event Handlers: Enabled	

Last Updated: 2013-06-13 11:18:12

Argentina - IT - Argentina

Status Summary					Notes [Edit]
Hosts	0 Up	0 Down	0 Unreachable	0 Pending	
Services	0 Ok	0 Warning	0 Unknown	0 Critical	0 Pending
Settings	Notifications: Enabled	Active Checks: Enabled	Passive Checks: Enabled	Event Handlers: Enabled	

Last Updated: 2013-06-13 11:18:12

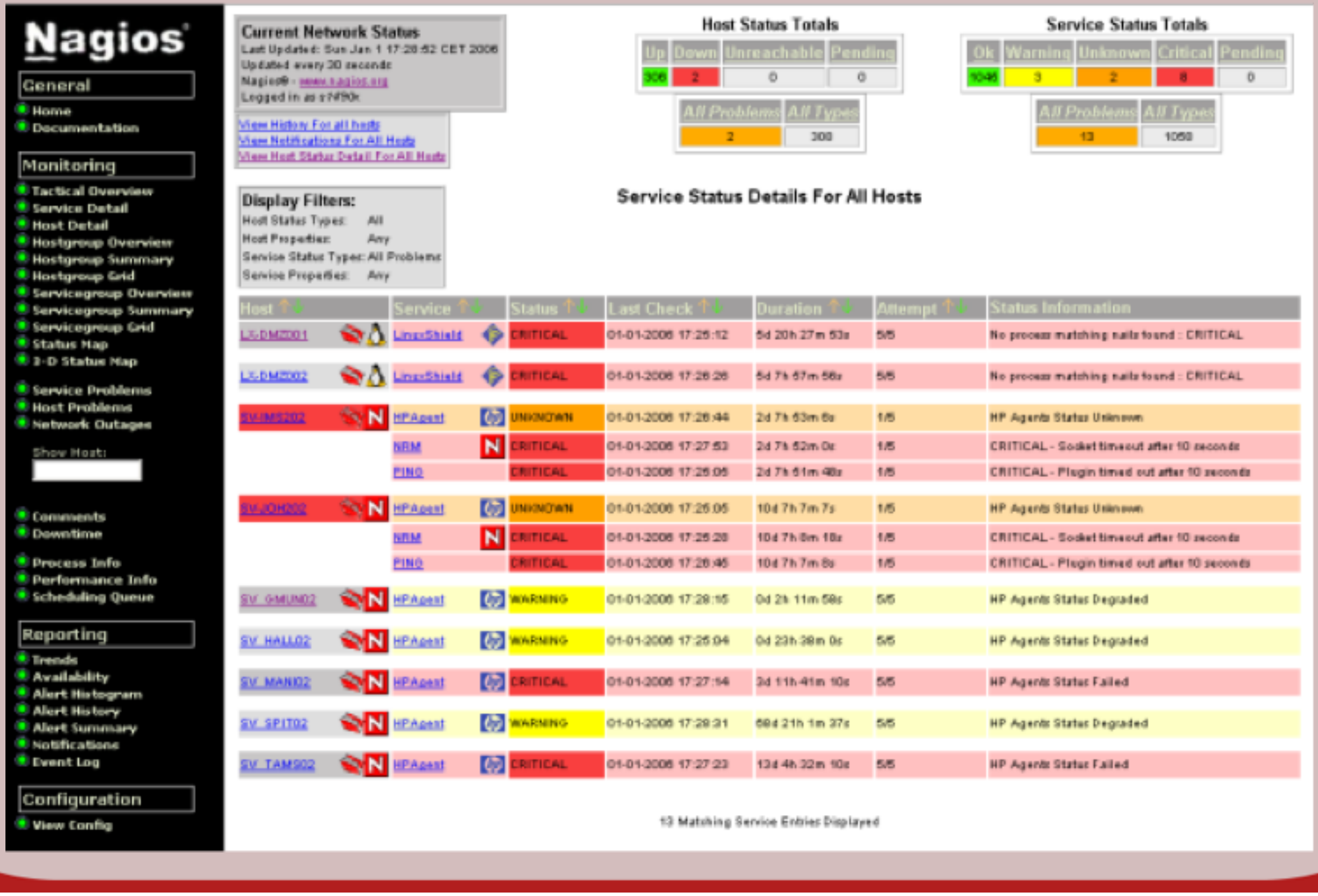
Nagios Core Demo - Atlanta, GA

Status Summary					Notes [Edit]
Hosts	11 Up	0 Down	0 Unreachable	0 Pending	
Services	36 Ok	1 Warning **1 Unhandled**	0 Unknown	2 Critical **2 Unhandled**	0 Pending
Settings	Notifications: Enabled	Active Checks: Enabled	Passive Checks: Enabled	Event Handlers: Enabled	

Last Updated: 2013-06-13 11:18:12

Nagios

- “Critical” in Nagios isn’t based on CVE’s, but by thresholds you set during config



Current Network Status
Last Updated: Sun Jan 1 17:28:52 CET 2006
Updated every 30 seconds
Nagios® - www.nagios.org
Logged in as s7490x

View History For all hosts
View Notifications For All Hosts
View Host Status Detail For All Hosts

Host Status Totals

Up	Down	Unreachable	Pending
306	2	0	0

All Problems	All Types
2	308

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
1046	3	2	8	0

All Problems	All Types
13	1059

Display Filters:
Host Status Types: All
Host Properties: Any
Service Status Types: All Problems
Service Properties: Any

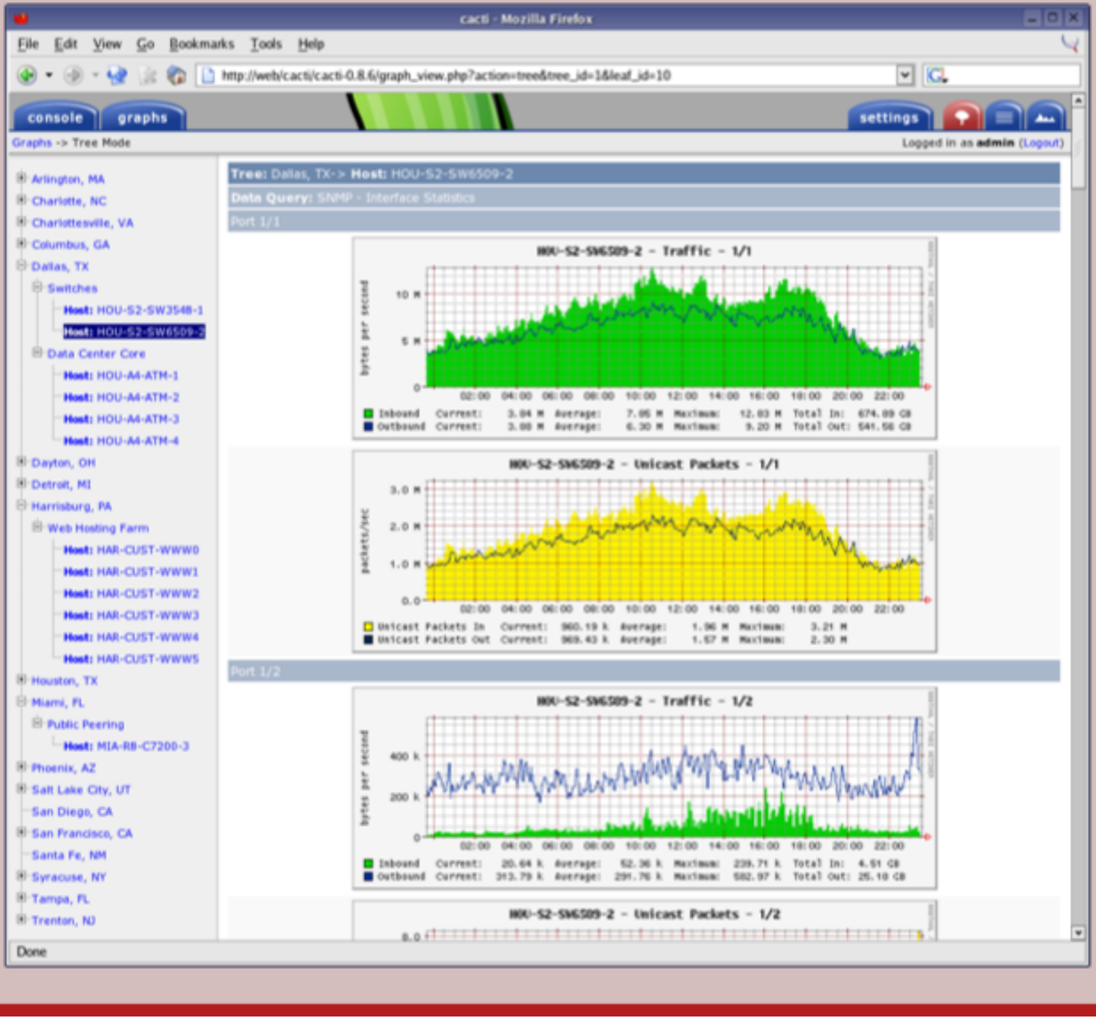
Service Status Details For All Hosts

Host	Service	Status	Last Check	Duration	Attempt	Status Information
LX-DMZ001	LinuxShield	CRITICAL	01-01-2006 17:25:12	5d 20h 27m 53s	5/5	No process matching nails found : CRITICAL
LX-DMZ002	LinuxShield	CRITICAL	01-01-2006 17:26:26	5d 7h 57m 56s	5/5	No process matching nails found : CRITICAL
SV-IMS202	HPAgent	UNKNOWN	01-01-2006 17:26:44	2d 7h 53m 6s	1/5	HP Agents Status Unknown
	NRM	CRITICAL	01-01-2006 17:27:53	2d 7h 52m 0s	1/5	CRITICAL - Socket timeout after 10 seconds
	PING	CRITICAL	01-01-2006 17:25:05	2d 7h 51m 48s	1/5	CRITICAL - Plugin timed out after 10 seconds
SV-JOH202	HPAgent	UNKNOWN	01-01-2006 17:25:05	10d 7h 7m 7s	1/5	HP Agents Status Unknown
	NRM	CRITICAL	01-01-2006 17:25:28	10d 7h 8m 18s	1/5	CRITICAL - Socket timeout after 10 seconds
	PING	CRITICAL	01-01-2006 17:26:46	10d 7h 7m 8s	1/5	CRITICAL - Plugin timed out after 10 seconds
SV_GMUN02	HPAgent	WARNING	01-01-2006 17:28:15	0d 2h 11m 58s	5/5	HP Agents Status Degraded
SV_HALL02	HPAgent	WARNING	01-01-2006 17:25:04	0d 23h 38m 0s	5/5	HP Agents Status Degraded
SV_MANI02	HPAgent	CRITICAL	01-01-2006 17:27:14	3d 11h 41m 10s	5/5	HP Agents Status Failed
SV_SPIT02	HPAgent	WARNING	01-01-2006 17:28:31	68d 21h 1m 37s	5/5	HP Agents Status Degraded
SV_TAMS02	HPAgent	CRITICAL	01-01-2006 17:27:23	13d 4h 32m 10s	5/5	HP Agents Status Failed

13 Matching Service Entries Displayed

Catci

- Uses SNMP polling of network devices for status information and shows a GUI


cacti - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://web/cacti/cacti-0.8.6/graph_view.php?action=tree&tree_id=1&leaf_id=10
console
graphs
settings
Graphs -> Tree Mode
Logged in as admin (Logout)
Arlington, MA
Charlotte, NC
Charlottesville, VA
Columbus, GA
Dallas, TX
Switches
Host: HOU-S2-SW3548-1
Host: HOU-S2-SW6509-2
Data Center Core
Host: HOU-A4-ATM-1
Host: HOU-A4-ATM-2
Host: HOU-A4-ATM-3
Host: HOU-A4-ATM-4
Dayton, OH
Detroit, MI
Harrisburg, PA
Web Hosting Farm
Host: HAR-CUST-WWW0
Host: HAR-CUST-WWW1
Host: HAR-CUST-WWW2
Host: HAR-CUST-WWW3
Host: HAR-CUST-WWW4
Host: HAR-CUST-WWW5
Houston, TX
Miami, FL
Public Peering
Host: MIA-RB-C7200-3
Phoenix, AZ
Salt Lake City, UT
San Diego, CA
San Francisco, CA
Santa Fe, NM
Syracuse, NY
Tampa, FL
Trenton, NJ
Tree: Dallas, TX-> Host: HOU-S2-SW6509-2
Data Query: SNMP - Interface Statistics
Port 1/1
HOU-S2-SW6509-2 - Traffic - 1/1
bytes per second
Inbound Current: 3.04 M Average: 7.05 M Maximum: 12.03 M Total In: 674.09 GB
Outbound Current: 3.08 M Average: 6.30 M Maximum: 9.20 M Total Out: 541.56 GB
HOU-S2-SW6509-2 - Unicast Packets - 1/1
packets/sec
Unicast Packets In Current: 960.19 k Average: 1.96 M Maximum: 3.21 M
Unicast Packets Out Current: 969.43 k Average: 1.57 M Maximum: 2.30 M
Port 1/2
HOU-S2-SW6509-2 - Traffic - 1/2
bytes per second
Inbound Current: 20.64 k Average: 52.36 k Maximum: 239.71 k Total In: 4.51 GB
Outbound Current: 313.79 k Average: 291.76 k Maximum: 582.97 k Total Out: 25.18 GB
HOU-S2-SW6509-2 - Unicast Packets - 1/2
02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00 20:00 22:00
Done

Detecting Network Events

CYBER INCIDENT RESPONSE

Detecting Network Events

- Cybersecurity analysts should be able to determine an incident based on events

- Analysis of logs and other data are key to understanding if an event will become an incident

- Types of Network Events:
  - Beaconing
  - Unusual bandwidth consumption
  - Link and connection failures
  - Unexpected traffic

Beaconing

- Beaconing or a heartbeat sends a signal to a Command and Control system due to a botnet or malware infection

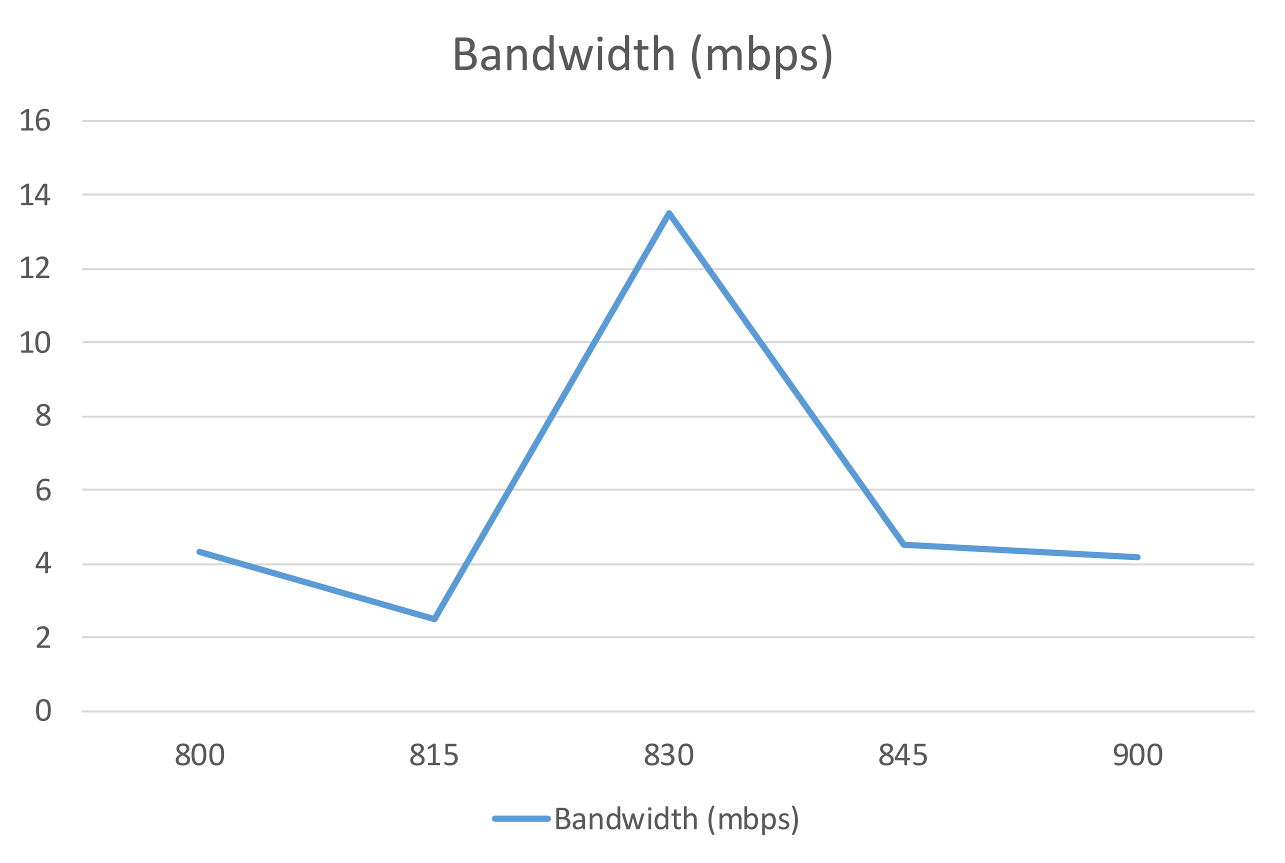
- Usually sent over HTTP or HTTPS

- Can be difficult to detect

- Generally occurs at a certain frequency or pattern

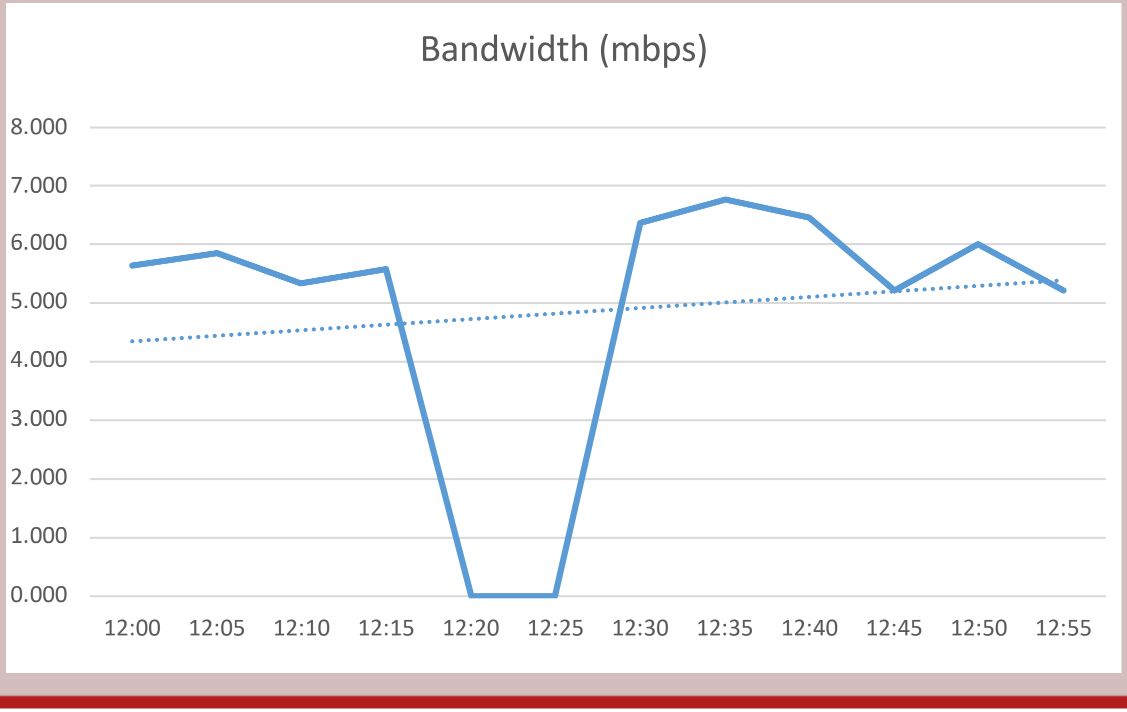
Unusual Bandwidth Consumption

- Unusual bandwidth consumption could cause service issues or can be a sign of larger trouble



Link and Connection Failures

- Generally occur due to a hardware, firmware, or software issues
- Could be as simple as a bad module, broken cable, or unplugged connector



Unexpected Traffic

- Detected by IDS/IPS, traffic monitoring systems, or by manual observation
- Understanding your baseline is important
- Not all unexpected traffic is malicious, but it should be investigated/understood
- Could be unusual based on type of traffic, end point location, or amount

Detecting Unexpected Traffic

- Baselines or Anomaly-based
  - Monitoring system alarm based on traffic that is outside the normal baseline
- Heuristics or Behavior-based
  - Uses signatures and defined rules to detect
- Protocol Analysis
  - Seeks to detect protocols where they aren't expected, like VPNs or IPv6 tunnels

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Network Probes and Attacks

CYBER INCIDENT RESPONSE

Network Probes and Attacks

- Much of your incident handling will involved network probes and attacks

- Network probes are usually part of reconnaissance efforts and are easy to detect (like a port scan)

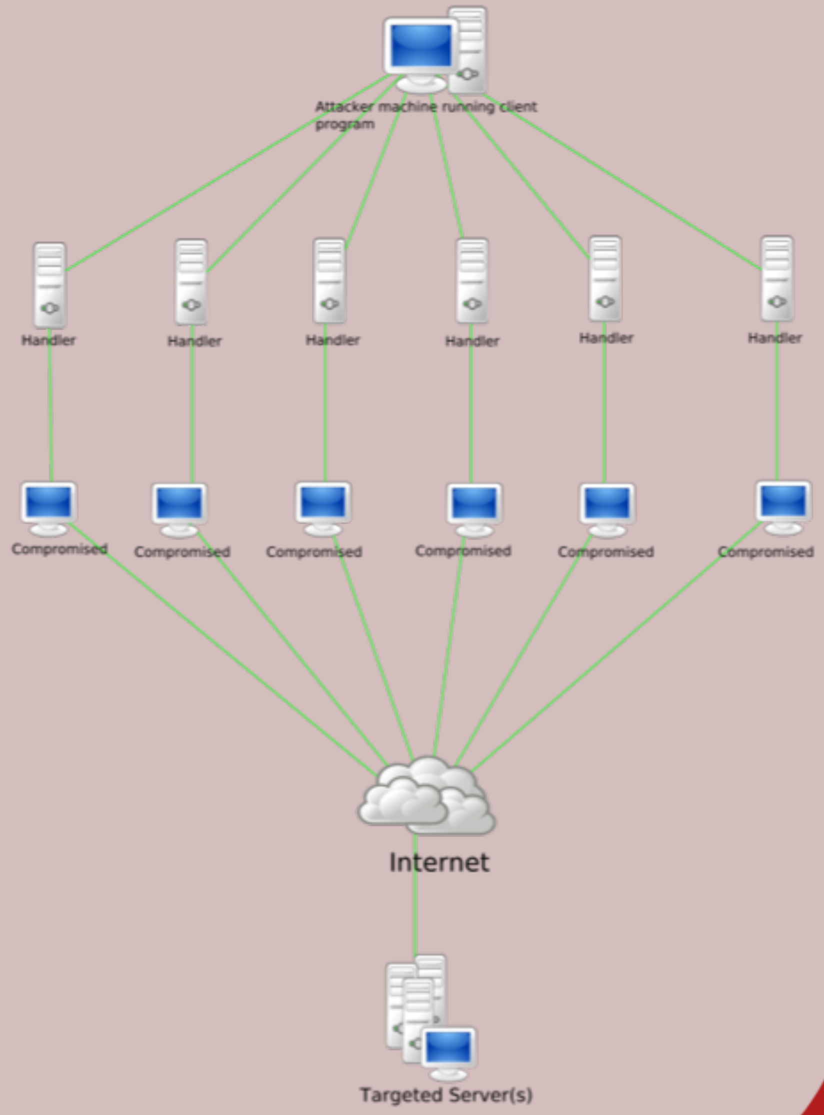
Denial of Service (DoS)

- Detection:
  - Attacks on a given network, system, or service from a single source
  - Attempts to overwhelm system or network
- Prevention:
  - Block the attacker using your firewall or IPS

Distributed Denial of Service (DDoS)

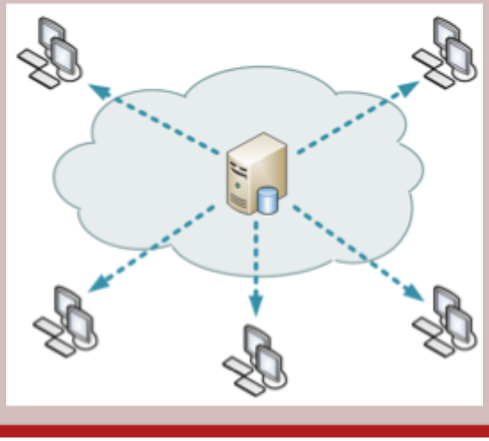
- Attacks on a given network, system, or service from simultaneous multiple sources

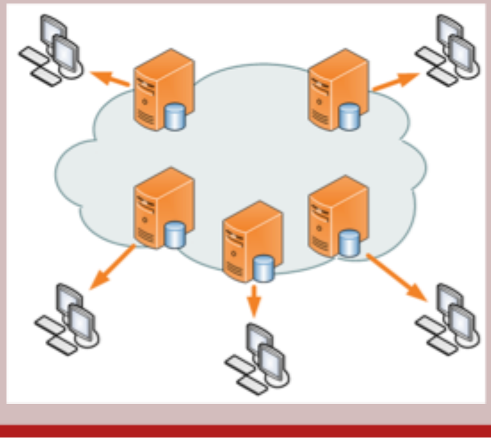
- Attempts to overwhelm system or network



Distributed Denial of Service (DDoS)

- Detection:
  - Traffic coming from known botnet IPs
  - Monitoring your traffic and usage patterns
- Prevention:
  - Network designed with distributed network of endpoints (like Akamai)
  - Ensure your networks can scale upwards





Detecting Rogue Devices

- MAC Address Validation
  - Ensure all devices are “Known Devices”
  - Check device MAC against vendor codes
- Scan the Network to identify devices
- Conduct physical site inspections
- Analyze traffic for irregular behavior

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Rogue Wired Devices

- Usually occurs when an employee or attacker connects a wired device
  - Adds a switch or hub to the network

- Network Access Control and Port Security can prevent this occurring

Rogue Wireless Devices

- Can be detected by conducting wireless surveys and mapping the area
- Often used as an Evil Twin to trick users to connect to them and steal information

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Server and Host Events

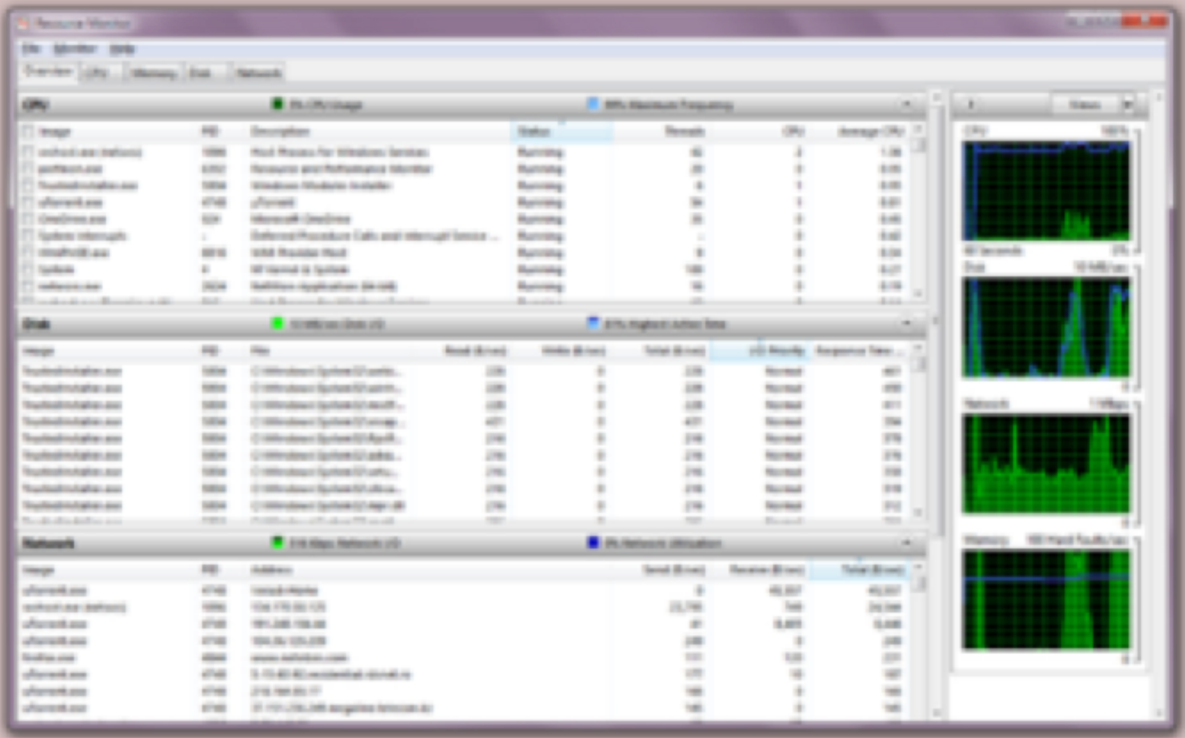
CYBER INCIDENT RESPONSE

System Monitoring

- Processor (CPU), Memory, and Drives
- CPU attacks usually occur as DoS
- Memory is monitored by the OS based on given thresholds
    - Memory leaks occur when programs don’t release memory after being terminated
    - Eventually, all memory can be used up
    - System restarted to release the memory

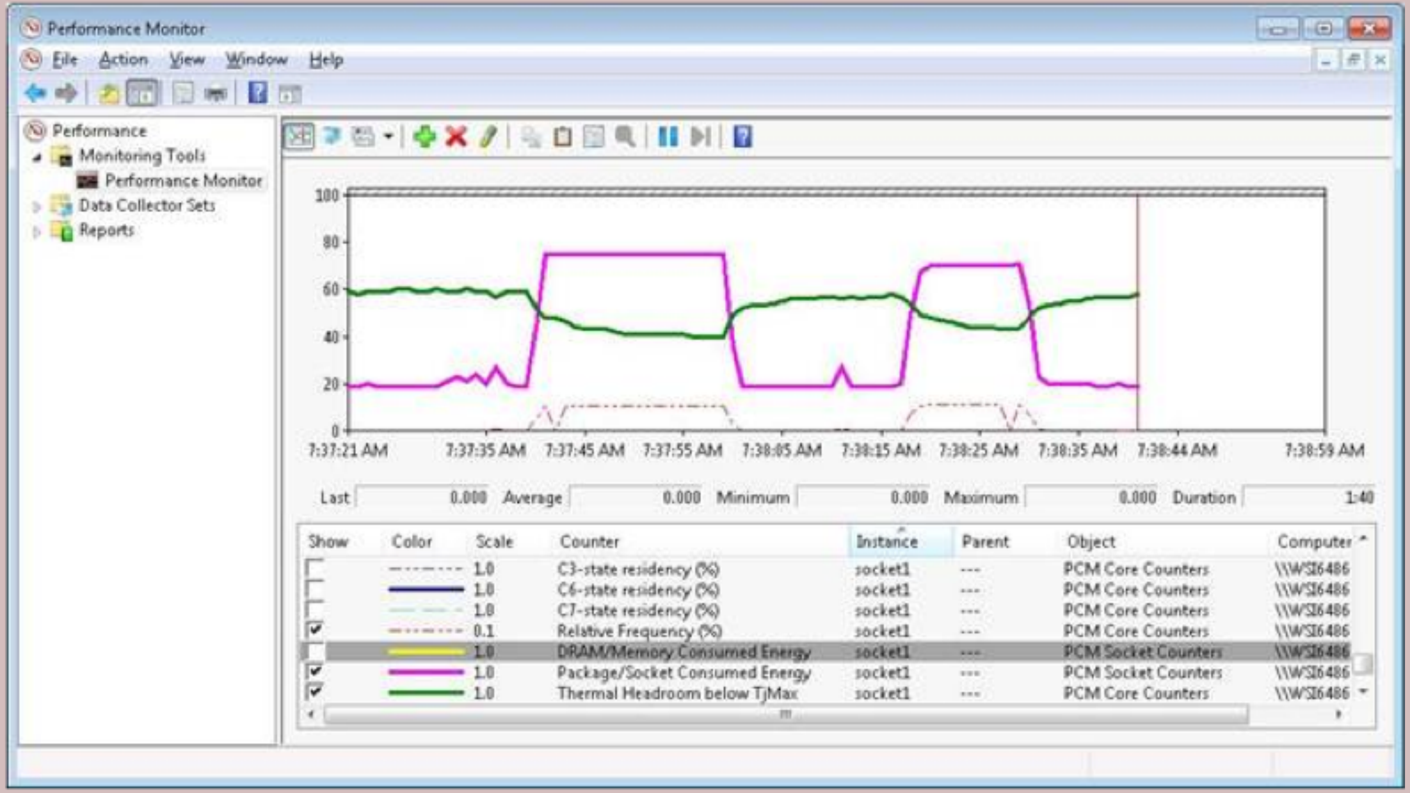
System Monitoring Tools: Windows

- Resource Monitor (or resmon)
  - Built-in Windows tool for monitoring
  - CPU, Memory, Disk, and Network Utilization



System Monitoring Tools: Windows

- Performance Monitor (or perfmon)
  - Built-in Windows tool for monitoring
  - Supports collection from remote systems



Last 0.000 Average 0.000 Minimum 0.000 Maximum 0.000 Duration 1:40

Show	Color	Scale	Counter	Instance	Parent	Object	Computer
□	-·-·-	1.0	C3-state residency (%)	socket1	---	PCM Core Counters	\\WSI6486
□	▬	1.0	C6-state residency (%)	socket1	---	PCM Core Counters	\\WSI6486
□	- - -	1.0	C7-state residency (%)	socket1	---	PCM Core Counters	\\WSI6486
☑	-·-·-	0.1	Relative Frequency (%)	socket1	---	PCM Core Counters	\\WSI6486
□	▬	1.0	DRAM/Memory Consumed Energy	socket1	---	PCM Socket Counters	\\WSI6486
☑	▬	1.0	Package/Socket Consumed Energy	socket1	---	PCM Socket Counters	\\WSI6486
☑	▬	1.0	Thermal Headroom below TjMax	socket1	---	PCM Core Counters	\\WSI6486

System Monitoring Tools: Linux

- ps
  - CPU and memory utilization, process info
- top
  - Like ps, but also provides sorting by top usage
- df
  - Report of disk usage
- w
  - Accounts logged on, who ran process

Malware and Unsupported Software

- Use centralized management tools to conduct installs and inventory
- Antivirus and antimalware tools
- Conduct blacklisting of software/files
- Application whitelisting

Unauthorized Access, Changes, and Privileges

- Users and permissions are complex with the number of systems in use

- Central Management tools (SIM/SIEM) can correlate logs for analysis
  - Authentication logs
  - User creation logs
  - System logs
  - Application logs
  - Security event logs

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Service and Application Events

CYBER INCIDENT RESPONSE

Service/Application Events

- Services and Applications should be monitored per good ITSM processes
  - Are they up/down?
  - Are they responding properly?
  - Are they functioning properly?
  - Are they conducting transactions properly?
  - Are they logging properly?

Service Anomalies

- Non-security issues:
  - Authentication errors
  - Permission issues
  - Services don’t start on boot up
  - Service failures

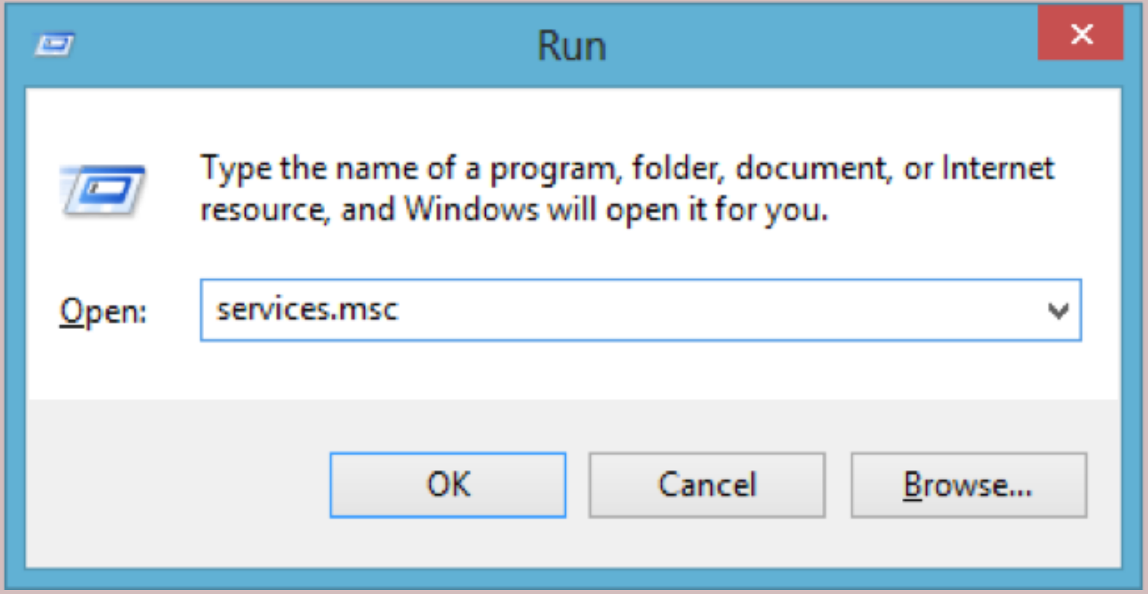
- Investigate the issue to ensure it is not security related

- Use antivirus, antimalware, file integrity checking, and whitelisting to verify

Checking Service Status

- Windows:
  - services.msc (GUI) or sc (command line)

- Linux:
  - service –status-all (command line)

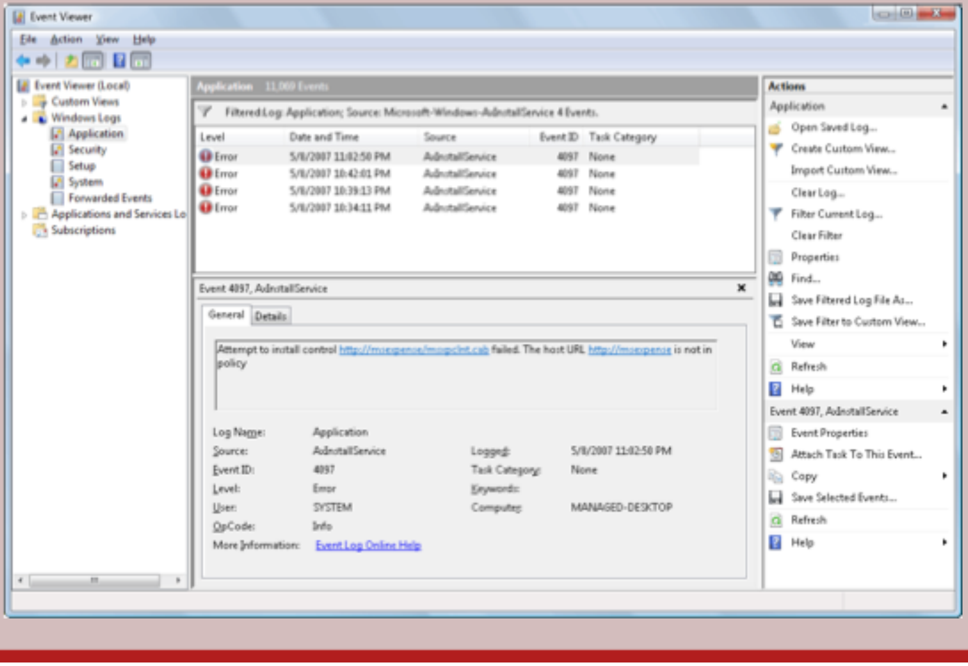


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: services.msc

Service/Application Logs

- Windows:
  - Use Windows Event Viewer to view Application Logs
- Linux:
  - Log to the /var/log directory
  - Use tail to view the end of the log files



Filtered Log: Application; Source: Microsoft-Windows-AdnstallService 4 Events.

Level	Date and Time	Source	Event ID	Task Category
Error	5/8/2007 11:02:50 PM	AdnstallService	4097	None
Error	5/8/2007 10:42:01 PM	AdnstallService	4097	None
Error	5/8/2007 10:39:13 PM	AdnstallService	4097	None
Error	5/8/2007 10:34:11 PM	AdnstallService	4097	None

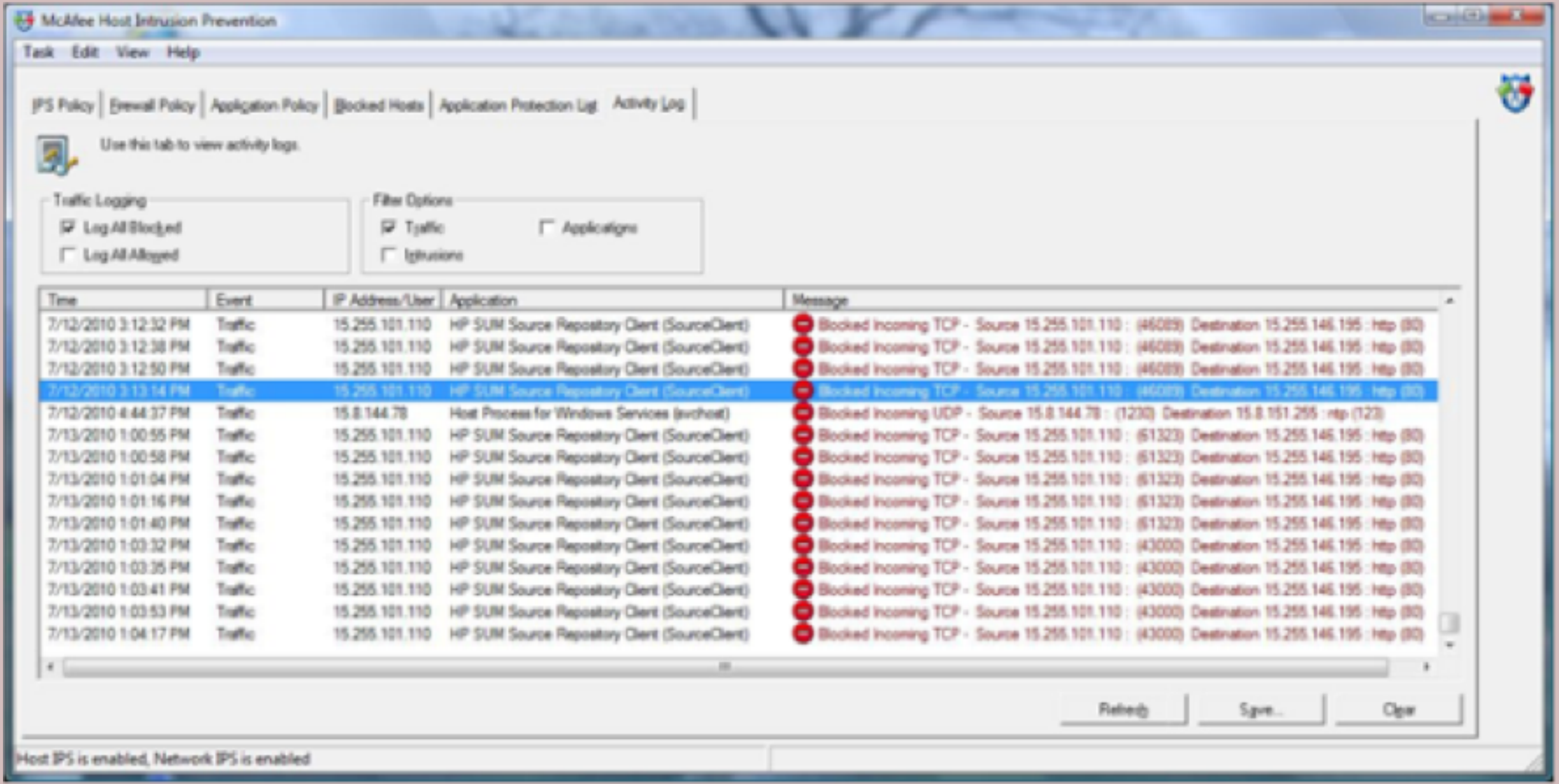
Event 4097, AdnstallService

Attempt to install control http://msexpense/msopclnt.cab failed. The host URL http://msexpense is not in policy

Log Name:	Application		
Source:	AdnstallService	Logged:	5/8/2007 11:02:50 PM
Event ID:	4097	Task Category:	None
Level:	Error	Keywords:	
User:	SYSTEM	Computer:	MANAGED-DESKTOP
OpCode:	Info		
More Information:	Event Log Online Help		

Service/Application Behavior

- Create and understand a baseline
- Log/alert on anything outside of baseline



Use this tab to view activity logs.

Traffic Logging
☑ Log All Blocked
□ Log All Allowed

Filter Options
☑ Traffic
□ Applications
□ Intrusions

Time	Event	IP Address/User	Application	Message
7/12/2010 3:12:32 PM	Traffic	15.255.101.110	HP SUM Source Repository Client (SourceClient)	Blocked Incoming TCP - Source 15.255.101.110 : (46089) Destination 15.255.146.195 : http (80)
7/12/2010 3:12:38 PM	Traffic	15.255.101.110	HP SUM Source Repository Client (SourceClient)	Blocked Incoming TCP - Source 15.255.101.110 : (46089) Destination 15.255.146.195 : http (80)
7/12/2010 3:12:50 PM	Traffic	15.255.101.110	HP SUM Source Repository Client (SourceClient)	Blocked Incoming TCP - Source 15.255.101.110 : (46089) Destination 15.255.146.195 : http (80)
7/12/2010 3:13:14 PM	Traffic	15.255.101.110	HP SUM Source Repository Client (SourceClient)	Blocked Incoming TCP - Source 15.255.101.110 : (46089) Destination 15.255.146.195 : http (80)
7/12/2010 4:44:37 PM	Traffic	15.8.144.78	Host Process for Windows Services (svchost)	Blocked Incoming UDP - Source 15.8.144.78 : (1230) Destination 15.8.151.255 : ntp (123)
7/13/2010 1:00:55 PM	Traffic	15.255.101.110	HP SUM Source Repository Client (SourceClient)	Blocked Incoming TCP - Source 15.255.101.110 : (61323) Destination 15.255.146.195 : http (80)
7/13/2010 1:00:58 PM	Traffic	15.255.101.110	HP SUM Source Repository Client (SourceClient)	Blocked Incoming TCP - Source 15.255.101.110 : (61323) Destination 15.255.146.195 : http (80)
7/13/2010 1:01:04 PM	Traffic	15.255.101.110	HP SUM Source Repository Client (SourceClient)	Blocked Incoming TCP - Source 15.255.101.110 : (61323) Destination 15.255.146.195 : http (80)
7/13/2010 1:01:16 PM	Traffic	15.255.101.110	HP SUM Source Repository Client (SourceClient)	Blocked Incoming TCP - Source 15.255.101.110 : (61323) Destination 15.255.146.195 : http (80)
7/13/2010 1:01:40 PM	Traffic	15.255.101.110	HP SUM Source Repository Client (SourceClient)	Blocked Incoming TCP - Source 15.255.101.110 : (61323) Destination 15.255.146.195 : http (80)
7/13/2010 1:03:32 PM	Traffic	15.255.101.110	HP SUM Source Repository Client (SourceClient)	Blocked Incoming TCP - Source 15.255.101.110 : (43000) Destination 15.255.146.195 : http (80)
7/13/2010 1:03:35 PM	Traffic	15.255.101.110	HP SUM Source Repository Client (SourceClient)	Blocked Incoming TCP - Source 15.255.101.110 : (43000) Destination 15.255.146.195 : http (80)
7/13/2010 1:03:41 PM	Traffic	15.255.101.110	HP SUM Source Repository Client (SourceClient)	Blocked Incoming TCP - Source 15.255.101.110 : (43000) Destination 15.255.146.195 : http (80)
7/13/2010 1:03:53 PM	Traffic	15.255.101.110	HP SUM Source Repository Client (SourceClient)	Blocked Incoming TCP - Source 15.255.101.110 : (43000) Destination 15.255.146.195 : http (80)
7/13/2010 1:04:17 PM	Traffic	15.255.101.110	HP SUM Source Repository Client (SourceClient)	Blocked Incoming TCP - Source 15.255.101.110 : (43000) Destination 15.255.146.195 : http (80)

Host IPS is enabled, Network IPS is enabled

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

CompTIA CySA+

Service/Application Attacks

- Anomalous Activity
  - Doesn’t match the typical behavior
  - Investigate the activity and solve
- New Accounts
  - Were they authorized?
  - Do they have excessive permissions?
- Unexpected Output
  - Improper output or garbage output
  - User and admin training imperative to determining the root cause

Service/Application Attacks

- Unexpected outbound communication
  - Why is the application sending out data?
  - Detect with network monitoring
- Service Interruption
  - Simple issue or a DDoS?
  - Monitoring tools can help determine reason
- Memory Overflows
  - Causes OS errors and crashes
  - Monitoring for them is hard
  - Detecting after a crash is easier

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Digital Forensics

CYBER INCIDENT RESPONSE

Digital Forensics

- Forensics are used to determine any changes, activities, or actions that have occurred on a host or server
- Allows incident responders to determine what occurred by putting together various pieces of information
- Similar techniques are used by incident response teams and law enforcement

Documentation in Digital Forensics

- Documentation is one of the most important steps in digital forensics
- Everything you do needs to be repeatable by a third-party investigator
- Chain of Custody is imperative for use in law enforcement

Forensics Toolkits

- Consist of specialized software and hardware to conduct imaging of hard disks and follow-on analysis

- Mobile devices require additional specialized tool kits

Forensic Toolkit Components

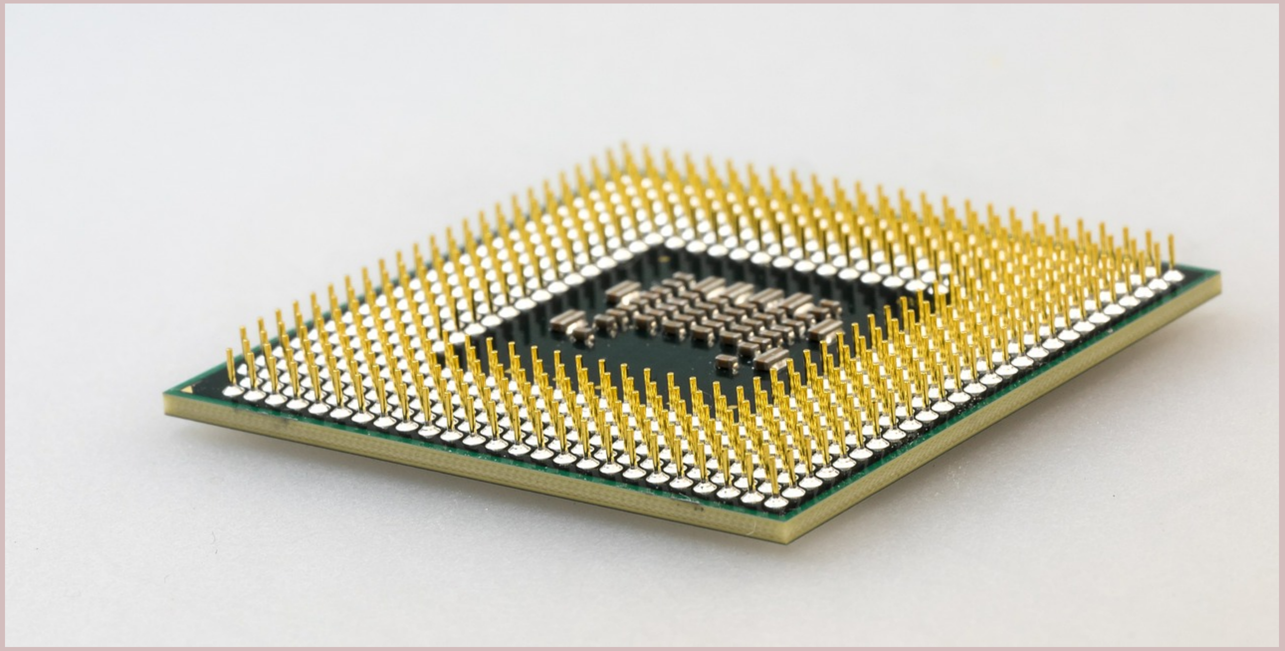
CYBER INCIDENT RESPONSE

Forensic Toolkit

- Contain a wide variety of software and hardware needed to conduct collection and analysis of data in the field
- Toolkits vary widely in cost and capability

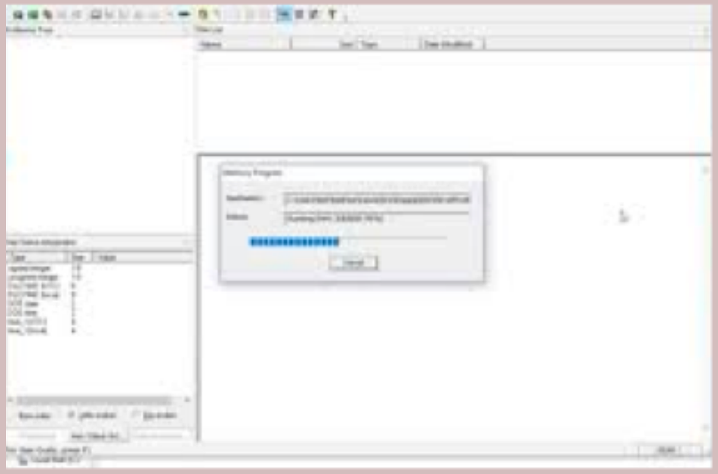
Digital Forensic Workstation

- Conducts data capture and analysis
  - Multicore CPU
  - Maximum RAM
  - Large, fast storage



Forensic Investigation Software

- Capture and analyze forensic images
- Document and track investigations
  - Forensic Toolkit (FTK)
  - EnCase
  - SANS Investigative Forensic Kit (SIFT)
  - The Sleuth Kit (TSK)



Write Blocker

- Ensures hard drives being imaged cannot be written to or its data changed
  - Hardware variants
  - Software variants

- Ensures integrity of the captured disk

Forensic Drive Duplicator

- Designed to copy hard drives without changing the original
- Dedicated device that copies drive and hashes the disk image

Wiped Drives and Removable Media

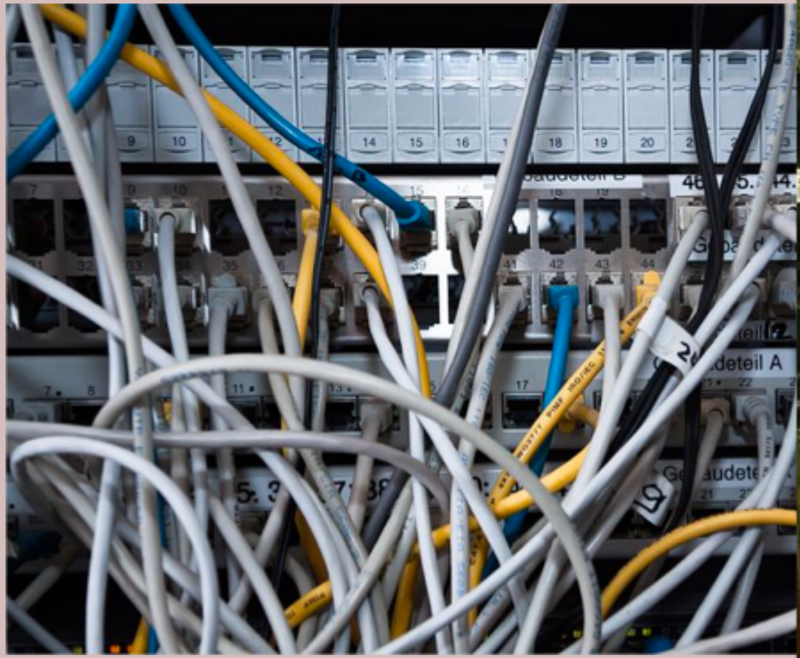
- Clean hard drives that are ready to receive disk images on
- Drives are prepared using a drive wipe before use in the field

Cables and Drive Adapters

- Be ready to copy/collect any type of media you come across while in the field

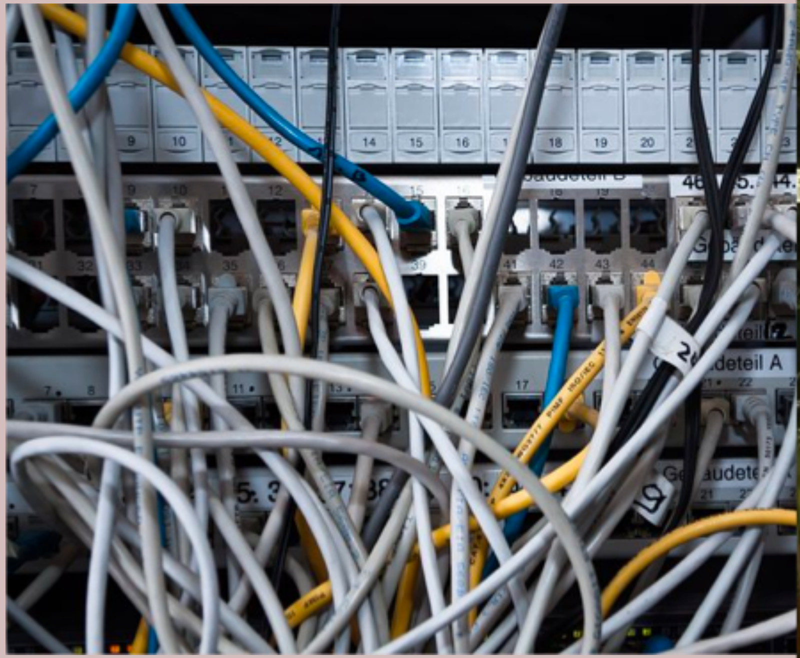
Digital Camera

- Used to photograph system layout, system configurations, drive labels, how a machine is cabled, etc.



Label Maker and Labels

- Label cables, components, and other items collected while in the field



Documentation and Checklists

- Chain of Custody forms, incident response forms and plan, and more

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Mobile Forensic Toolkits

CYBER INCIDENT RESPONSE

Mobile Forensic Toolkits

- Mobile devices have different operating systems and security issues
- Capturing data from mobile devices can be more difficult and needs special tools

Tools to Access the SIM Card

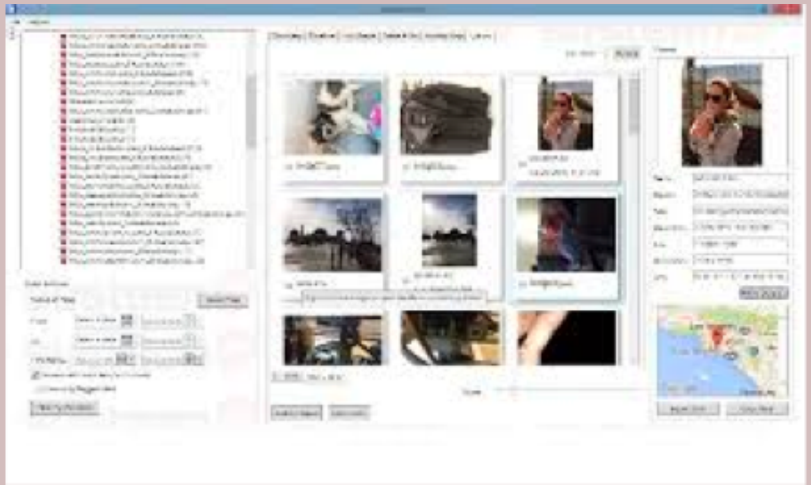
- Different phones require small screwdrivers or a push pin-style tool

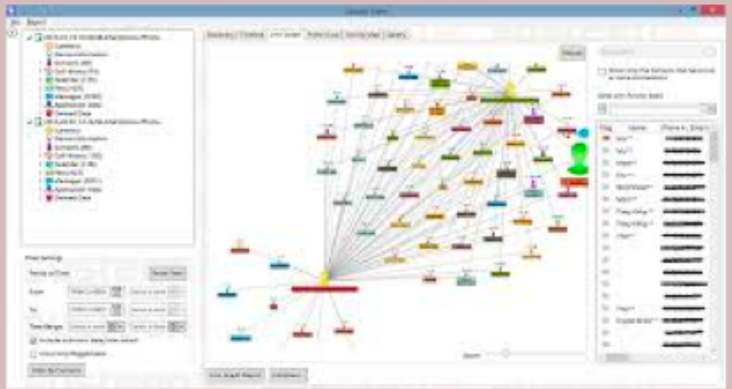
Connection Cables

- Lightning cables or 30-pin for Apple
- USB Micro, Mini, or USB-C for Android

Mobile Forensic Software

- Specialized software for accessing mobile devices





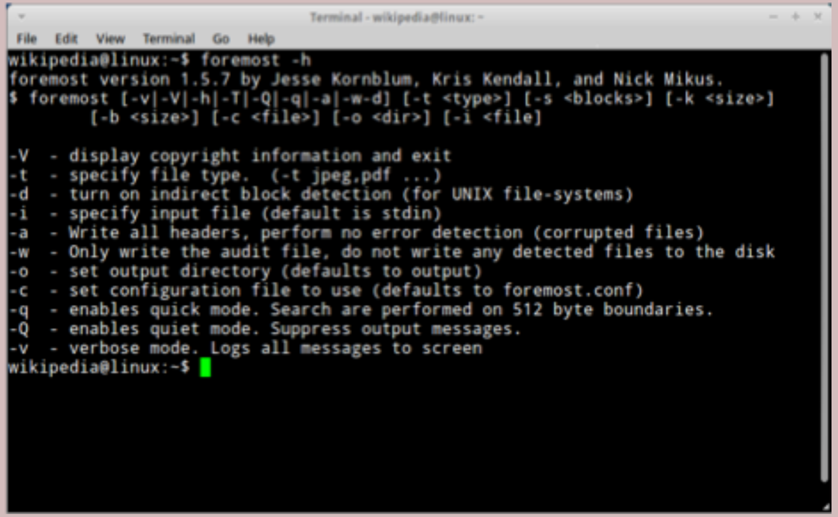
JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Forensic Software

CYBER INCIDENT RESPONSE

Forensic Software

- Commercial and Open-Source for:
  - Imaging
  - Analysis
  - Hashing and validation
  - Process and memory dumps
  - Password cracking
  - Log viewer



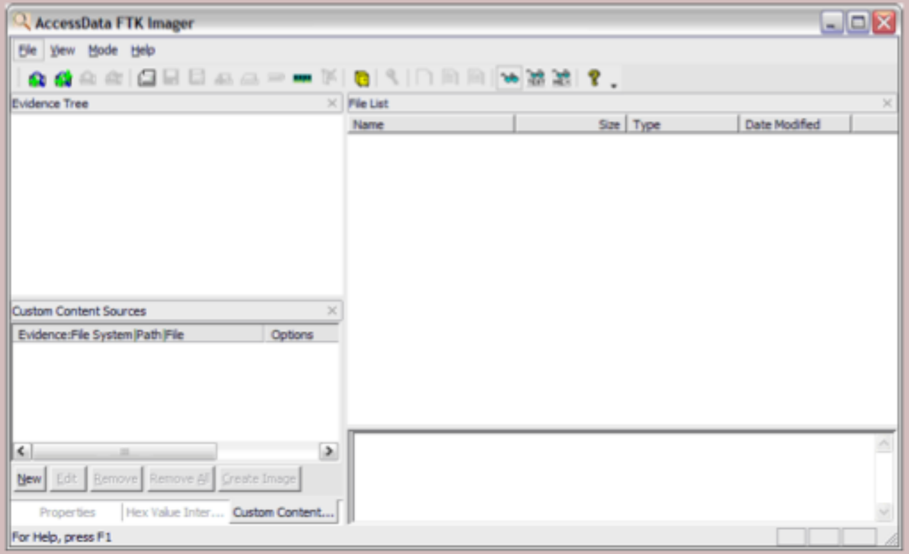
```
wikipedia@linux:~$ foremost -h
foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus.
$ foremost [-v|-V|-h|-T|-Q|-q|-a|-w-d] [-t <type>] [-s <blocks>] [-k <size>]
        [-b <size>] [-c <file>] [-o <dir>] [-i <file]

-V  - display copyright information and exit
-t  - specify file type.  (-t jpeg,pdf ...)
-d  - turn on indirect block detection (for UNIX file-systems)
-i  - specify input file (default is stdin)
-a  - Write all headers, perform no error detection (corrupted files)
-w  - Only write the audit file, do not write any detected files to the disk
-o  - set output directory (defaults to output)
-c  - set configuration file to use (defaults to foremost.conf)
-q  - enables quick mode. Search are performed on 512 byte boundaries.
-Q  - enables quiet mode. Suppress output messages.
-v  - verbose mode. Logs all messages to screen
wikipedia@linux:~$ 
```

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Imaging Media and Drives

- Bit by bit copy of a drive, including the slack space and unallocated space

- FTK Imager
- EnCase Imager
- dd



Analysis Software

- Creates timeline of system changes
- Validates file against known good copy
- File system analysis for hidden files, changes, access, and metadata
- Windows Registry analysis
- Log file parsing and analysis

- Examples:
  - Commercial:
    FTK and EnCase
  - Open-source:
    SIFT, CAINE, and Autopsy

Hashing and Validation

- Creates a unique file integrity check of a disk image after creation

- Used as part of chain of custody

- EnCase uses built-in hashing with its .EO1 format

- Should use both MD5 & SHA1/SHA256

Process and Memory Dumps

- State of the Operating System and data in-resident memory at time of collection
- Difficult to collect without changing the contents contained
- Useful to capture decryption keys for full disk encryption
- Hibernation files and crash dumps can also contain some of this data

Process and Memory Dumps

- Tools
  - fmem and LiME (Linux)
  - DumpIt (Windows)
  - Volatility Framework (Windows, Linux, OS X)
  - EnCase
  - FTK

- Memory dumps on system can be found at %SystemRoot%\MEMORY.DMP

- Dumps analyzed with Microsoft's WinDbg

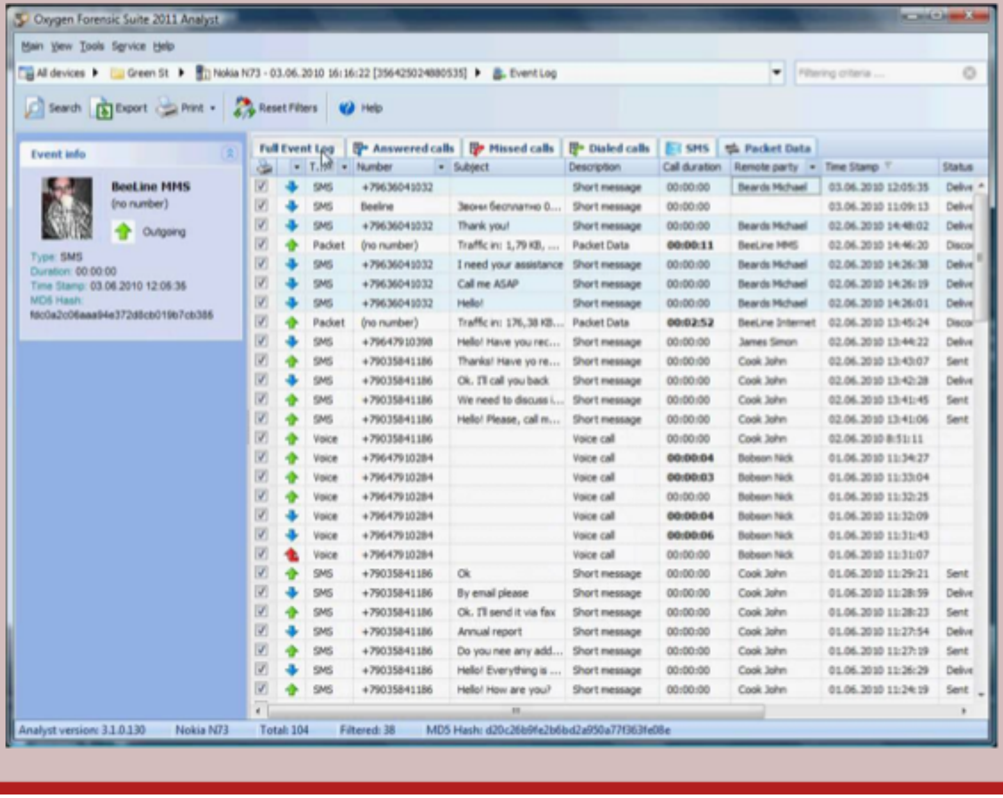
Password Cracking/Recovery

- Encrypted and password protected files required cracking or guessing password
- Hacking tools like John The Ripper and Cain and Able can be used
- DOC, XLS, PPT, and ZIP files have other specialized password cracking tools:
  - Advanced Office Password Breaker
  - ElcomSoft's Distributed Password Recovery
  - Zip2John
  - …numerous others…

Log Viewers

- Used to analyze log files from collected system images

- Can create timelines and visual the data



Oxygen Forensic Suite 2011 Analyst
Main View Tools Service Help
All devices ▸ Green St ▸ Nokia N73 - 03.06.2010 16:16:22 [356425024880535] ▸ Event Log
Filtering criteria ...
Search Export Print Reset Filters Help
Full Event Log
Answered calls
Missed calls
Dialed calls
SMS
Packet Data

Event info

BeeLine MMS
(no number)
Outgoing

Type: SMS
Duration: 00:00:00
Time Stamp: 03.06.2010 12:06:36
MD5 Hash:
fdc0a2c06aaa94e372d8cb019b7cb386

		T...	Number	Subject	Description	Call duration	Remote party	Time Stamp	Status
☑	↓	SMS	+79636041032		Short message	00:00:00	Beards Michael	03.06.2010 12:05:35	Delive
☑	↓	SMS	Beeline	Звони бесплатно 0...	Short message	00:00:00		03.06.2010 11:09:13	Delive
☑	↓	SMS	+79636041032	Thank you!	Short message	00:00:00	Beards Michael	02.06.2010 14:48:02	Delive
☑	↑	Packet	(no number)	Traffic in: 1,79 KB, ...	Packet Data	**00:00:11**	BeeLine MMS	02.06.2010 14:46:20	Disco
☑	↓	SMS	+79636041032	I need your assistance	Short message	00:00:00	Beards Michael	02.06.2010 14:26:38	Delive
☑	↓	SMS	+79636041032	Call me ASAP	Short message	00:00:00	Beards Michael	02.06.2010 14:26:19	Delive
☑	↓	SMS	+79636041032	Hello!	Short message	00:00:00	Beards Michael	02.06.2010 14:26:01	Delive
☑	↑	Packet	(no number)	Traffic in: 176,38 KB...	Packet Data	**00:02:52**	BeeLine Internet	02.06.2010 13:45:24	Disco
☑	↓	SMS	+79647910398	Hello! Have you rec...	Short message	00:00:00	James Simon	02.06.2010 13:44:22	Delive
☑	↑	SMS	+79035841186	Thanks! Have yo re...	Short message	00:00:00	Cook John	02.06.2010 13:43:07	Sent
☑	↓	SMS	+79035841186	Ok. I'll call you back	Short message	00:00:00	Cook John	02.06.2010 13:42:28	Delive
☑	↑	SMS	+79035841186	We need to discuss i...	Short message	00:00:00	Cook John	02.06.2010 13:41:45	Sent
☑	↑	SMS	+79035841186	Hello! Please, call m...	Short message	00:00:00	Cook John	02.06.2010 13:41:06	Sent
☑	↑	Voice	+79035841186		Voice call	00:00:00	Cook John	02.06.2010 8:51:11	
☑	↑	Voice	+79647910284		Voice call	**00:00:04**	Bobson Nick	01.06.2010 11:34:27	
☑	↑	Voice	+79647910284		Voice call	**00:00:03**	Bobson Nick	01.06.2010 11:33:04	
☑	↑	Voice	+79647910284		Voice call	00:00:00	Bobson Nick	01.06.2010 11:32:25	
☑	↓	Voice	+79647910284		Voice call	**00:00:04**	Bobson Nick	01.06.2010 11:32:09	
☑	↓	Voice	+79647910284		Voice call	**00:00:06**	Bobson Nick	01.06.2010 11:31:43	
☑	↑	Voice	+79647910284		Voice call	00:00:00	Bobson Nick	01.06.2010 11:31:07	
☑	↑	SMS	+79035841186	Ok	Short message	00:00:00	Cook John	01.06.2010 11:29:21	Sent
☑	↓	SMS	+79035841186	By email please	Short message	00:00:00	Cook John	01.06.2010 11:28:59	Delive
☑	↑	SMS	+79035841186	Ok. I'll send it via fax	Short message	00:00:00	Cook John	01.06.2010 11:28:23	Sent
☑	↓	SMS	+79035841186	Annual report	Short message	00:00:00	Cook John	01.06.2010 11:27:54	Delive
☑	↑	SMS	+79035841186	Do you nee any add...	Short message	00:00:00	Cook John	01.06.2010 11:27:19	Sent
☑	↓	SMS	+79035841186	Hello! Everything is ...	Short message	00:00:00	Cook John	01.06.2010 11:26:29	Delive
☑	↑	SMS	+79035841186	Hello! How are you?	Short message	00:00:00	Cook John	01.06.2010 11:24:19	Sent

Analyst version: 3.1.0.130 Nokia N73 Total: 104 Filtered: 38 MD5 Hash: d20c26b9fe2b6bd2a950a77f363fe08e

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Training and Certification

CYBER INCIDENT RESPONSE

Importance of Training and Certification

- Full-time forensic personnel should be properly trained and certified
- If not, evidence might not be able to be used in court
- Forensic experts and their credentials are called into question by the defense

Industry Certifications

CCE	Certified Computer Examiner
CFCE	Certified Forensic Computer Examiner
CHFI	Computer Hacking Forensic Investigator
GCFA	GIAC Certified Forensic Analyst
GCFE	GIAC Certified Forensic Examiner
CSFA	Cybersecurity Forensic Analyst
ACE	AccessData Certified Examiner (FTK)
EnCE	EnCase Certified Examiner
DMC	Digital Media Collector
DFE	Digital Forensic Examiner

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

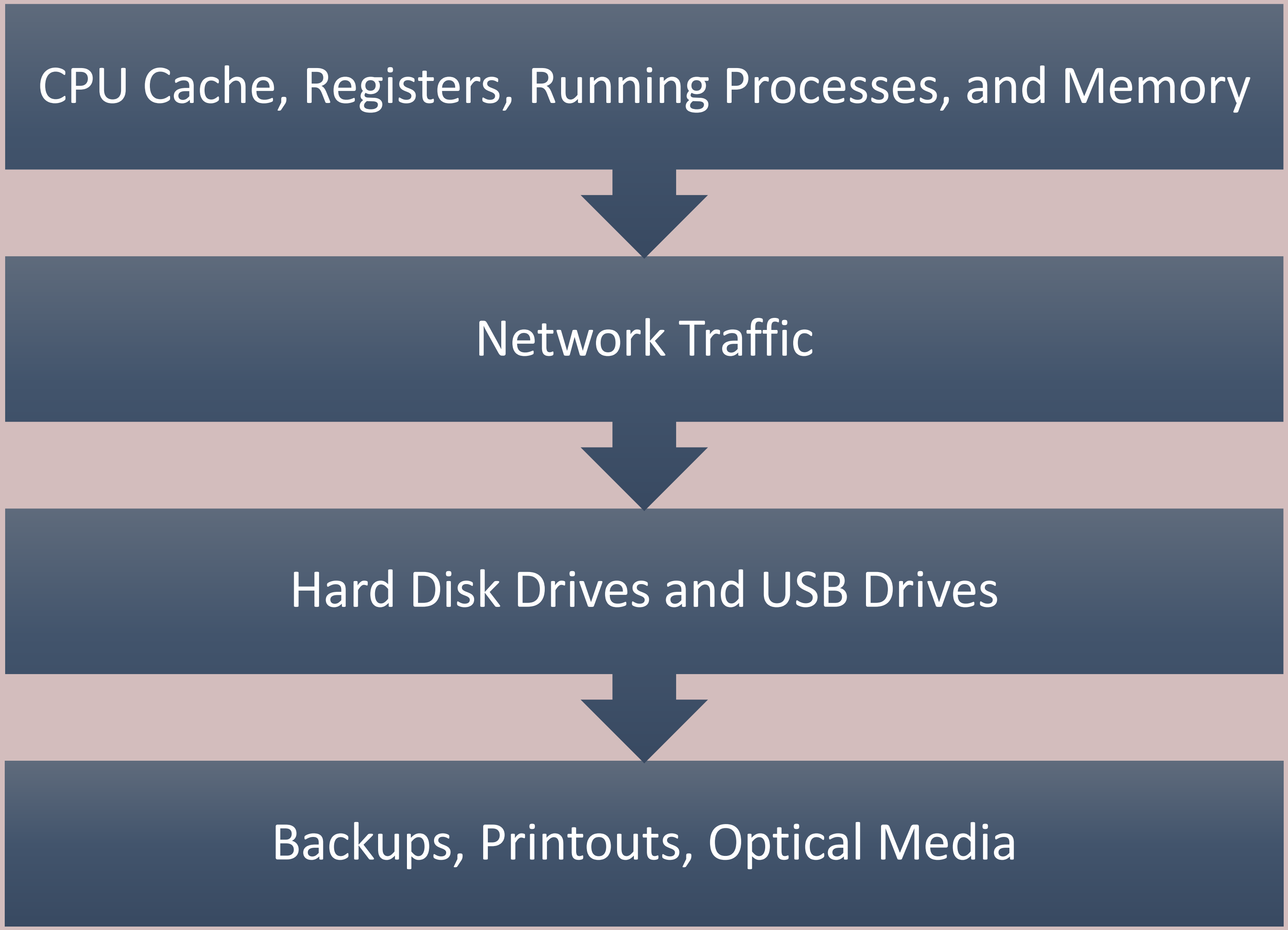
Forensic Investigation Process

CYBER INCIDENT RESPONSE

Forensic Investigation Process

1. Determine what you want to find out
2. Determine location to find that info
3. Document your plan
4. Acquire/preserve the evidence needed
5. Perform initial analysis (log actions)
6. Conduct deeper analysis (log actions)
7. Report on your findings

Order of Volatility (Data Collection Priorities)



CPU Cache, Registers, Running Processes, and Memory

Network Traffic

Hard Disk Drives and USB Drives

Backups, Printouts, Optical Media

What do you do when you find something you don't expect?

- There's always a risk you will find what you didn't want to find…

…Employee breaking the AUP

…Evidence of illegal activities

JASON DION

TRAINING THE CYBER SECURITY WORKFORCE

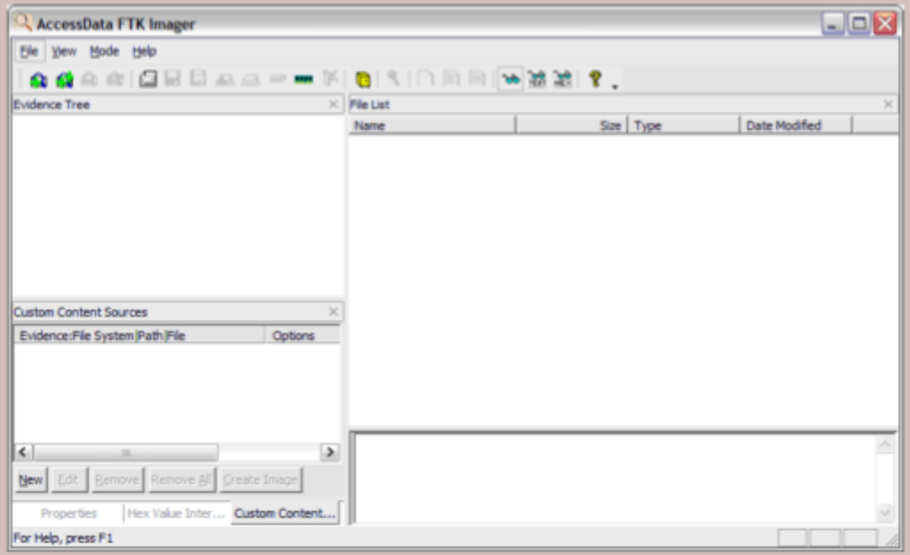
Disk Imaging

CYBER INCIDENT RESPONSE

Imaging Media and Drives

- Bit by bit copy of a drive, including the slack space and unallocated space

- FTK Imager
- EnCase Imager
- dd



dd

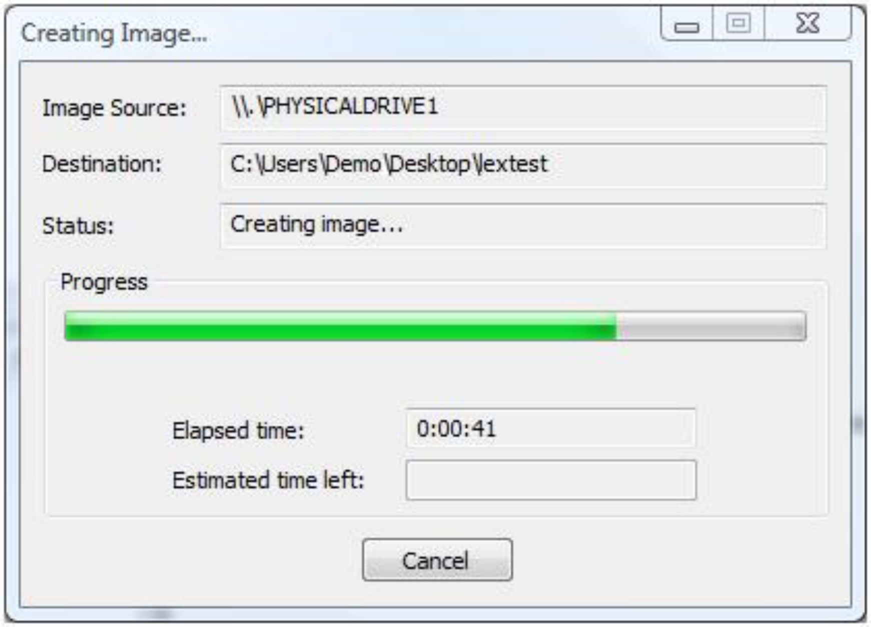
- Standard Linux and UNIX tool

- Can clones drives using bit-by-bit copy

```
# dd bs-64k if=/dev/disk1/sda1 of=/mnt/usb1/sda1.img
```

FTK Imager

- Commercial product that is free to use
- Documents chain of custody, adds hash, and creates metadata tags for later analysis



Creating Image...

Image Source: \\.\PHYSICALDRIVE1

Destination: C:\Users\Demo\Desktop\extest

Status: Creating image...

Progress

Elapsed time: 0:00:41

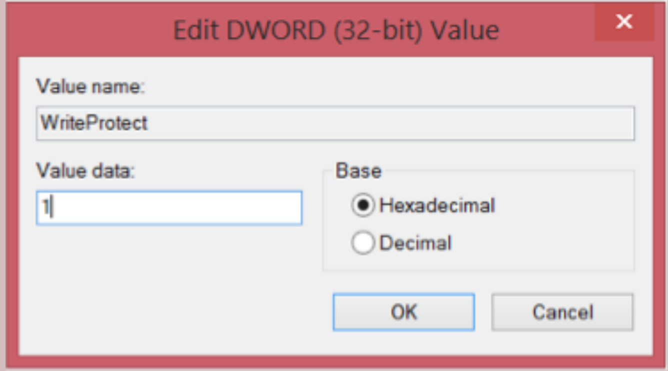
Estimated time left:

Forensic Drive Duplicators

- Very expensive, dedicated devices
- Creates images, hashes, and chain of custody metadata

Write Blockers

- Maintain data integrity on the source disk
- Hardware write blockers should be used for best forensic integrity



Edit DWORD (32-bit) Value

Value name: WriteProtect

Value data: 1

Base: ● Hexadecimal ○ Decimal

Encrypted Drives

- Try to find the password because brute forcing is VERY slow (if possible)

- Capture the computer while logged in to bypass drive encryption when possible

Incident Containment

CYBER INCIDENT RESPONSE

Incident Containment

- Perform this as quickly as possible
- Isolate the issue
- Stop the spread of the incident

Containment Considerations

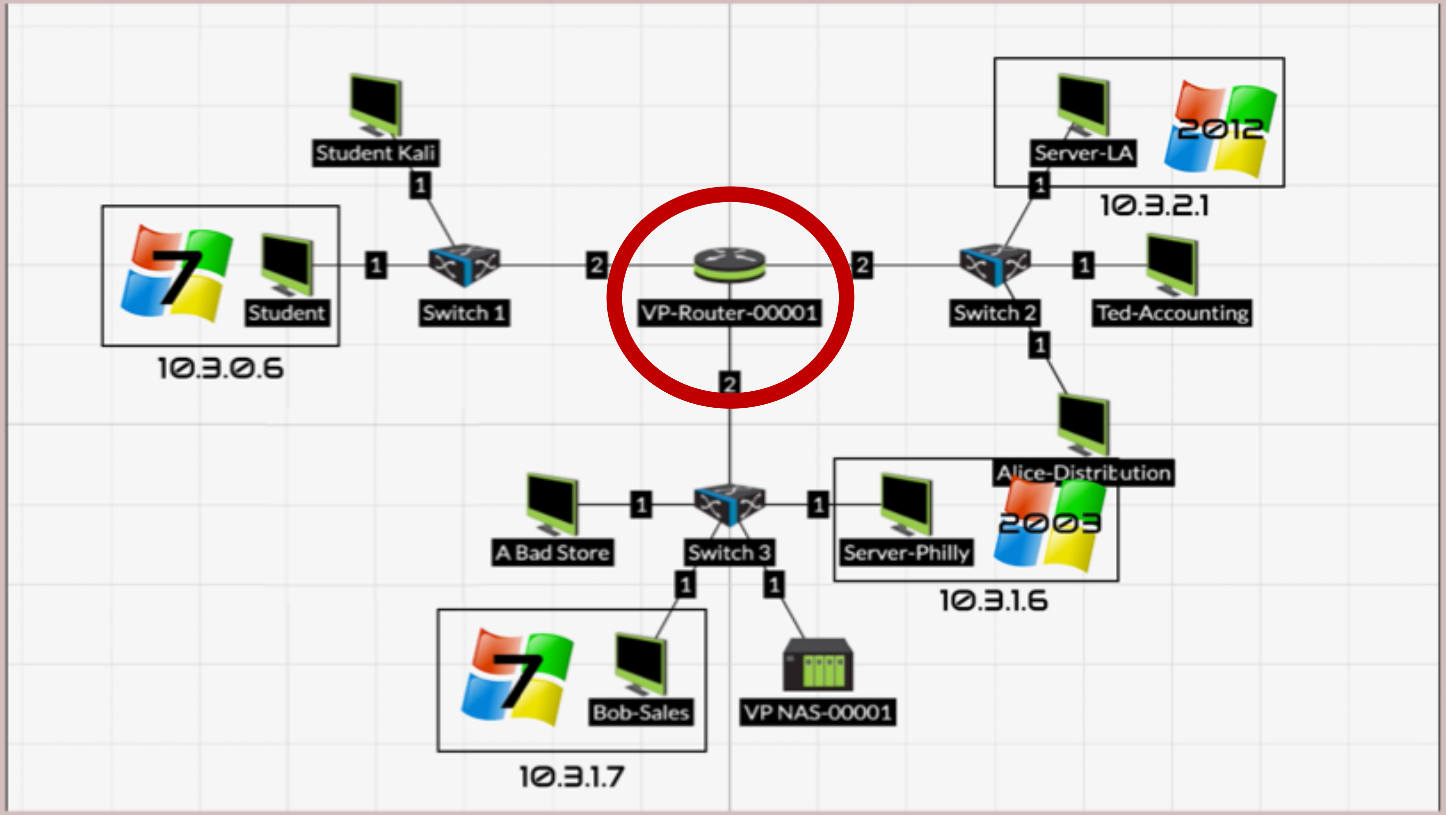
- Containment isn't perfect…
  it is quick and dirty

- Can cause some loss of business functionality

- Coordinate with stakeholders before you take actions

Segmentation

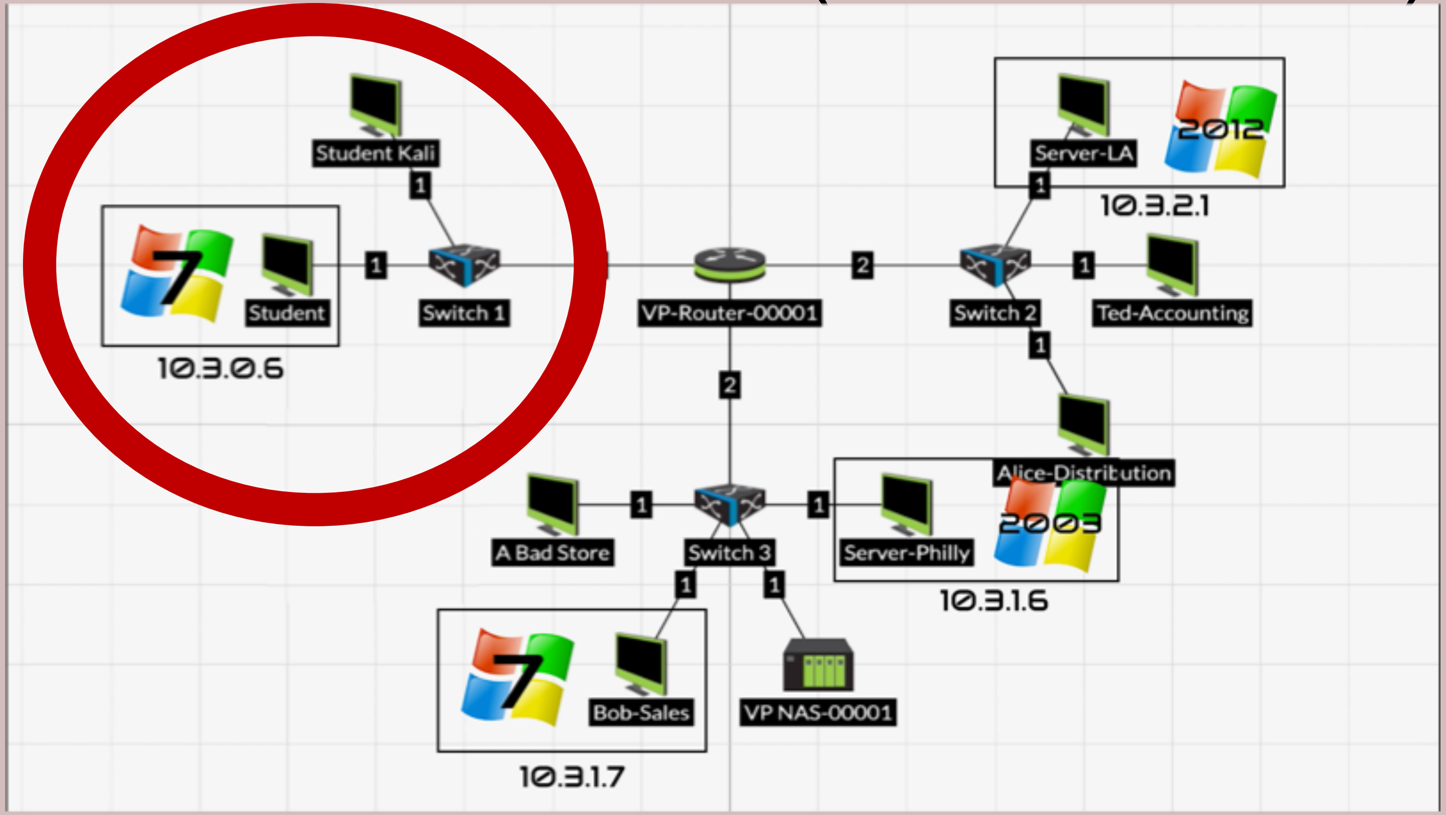
- Proactive strategy to prevent spread from one part of network to another



Isolation or Removal

- Remove a system from your network and directly connect to internet

- Remove the attacker (disconnect PC)



Objective of Containment

- Limit the damage to the organization
- Provide incident handlers an opportunity to collect evidence and repair issue
- Maintain and operate services for your customers to use

Identifying Attackers

- Do you need to identify the attacker?
- Is there a good business reason why?
- Attackers cover their tracks well, and identifying them can take a lot of time and resources, where your goal is simply to minimize business impact…
- Law enforcement has a different viewpoint on this, though…

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Eradication and Recovery

CYBER INCIDENT RESPONSE

Eradication and Recovery

- Remove any artifacts of the incident
- Restore the network to full functionality
- Correct any security deficiencies
- Remove malicious code, sanitize compromised media, and fix any of the affected user accounts

What Recovery is Not…

- Not a rebuilding of the entire network…
- Not a full redesign of the system…
- Not a reason to buy all new equipment…

Reconstruction and Reimaging

- Once an attacker touches your system, consider it compromised
- Reconstruct or reimage the system from a known good backup
- Consider the root cause of the incident so that the system isn't susceptible to the same attack vector again

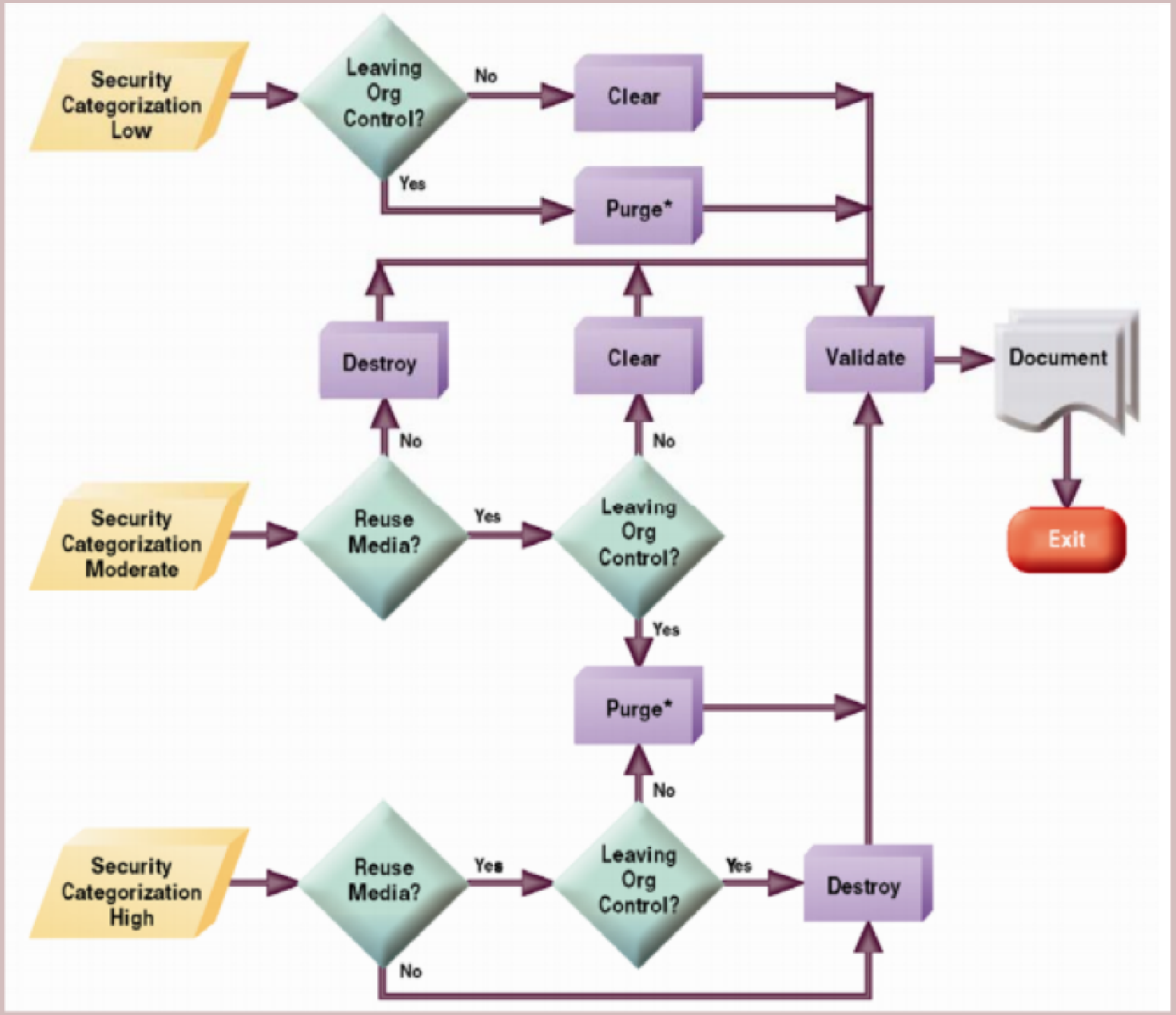
Patching

- Patch any systems that may be vulnerable to the same attack vector
- This is a good time to rescan and patch ALL of your systems…

Sanitization and Disposal

- Clear
  - Logical techniques used to sanitize data (reset to factory state or overwriting a disk with all 0s)
- Purge
  - Physical or logical techniques to make data recovery from a disk infeasible using newest techniques (degaussing or overwrite 0s 35x)
- Destroy
  - Data recovery infeasible and disk drive unusable for storage (melting, incinerating, destroying)

Sanitization and Disposal



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Validation Effort

- Only authorized user accounts exist on each system in the network
- Verify permission assigned to each user
- Verify all systems are logging correctly
- Verify vulnerability scans on all systems are routinely conducted

Finishing the Response

CYBER INCIDENT RESPONSE

Finishing the Response

- Change Management Process

- Lessons-Learned

- Final Report

Change Management Process

- Emergency Change Management Board may have authorized numerous actions during the incident response
- Follow-up to ensure all changes have been documented properly
- Need to ensure that network diagrams and vulnerability scan profiles updated

Lessons-Learned

- Documents the details, the root cause, and the solution to a security incident
- Fact-finding meetings should be conducted as close to the end of an incident response as possible
- Needed changes identified during the lessons-learned process should be fed into the resourcing and Change Management process

Final Report

- Every incident should finish with a compiled written report
- Established organizational “memory”
- Can serve as documentation in case further legal action occurs in the future
- Can identify other deficiencies in the incident response that need to be addressed by management

Final Report Includes…

- Timeline of incident and response events
- Root cause of incident
- Location and description of evidence
- Actions taken to contain, eradicate, and recovery (and the reasoning for them)
- Estimated impact to organization ($,time)
- Post-recovery validation effort results
- Documentation of lessons-learned