Introduction to Network Security Monitoring

INFO-6081 – Monitoring & Incident Response

FANSHAWE

Learning Outcomes

- What is Network Security Monitoring?
- Computer Incident Response Team
- Detecting Intrusions vs Preventing Intrusions
- Why Does NSM Work?
- NSM Deployment
- Legal Considerations
- NSM Data Types
- NSM Drawbacks

Enterprise Security Considerations

There are only two types of companies: those that know they’ve been compromised, and those that don’t know.

Dmitri Alperovitch, 2011

There are only two types of companies: companies that have been hacked and will be hacked again.

Robert Mueller, 2012

What is Network Security Monitoring?

- Network Security Monitoring (NSM) is a practice of collection, analysis and escalation of indicators of compromise
- NSM is used to find intruders on the network, detect the actions taken by the intruders, and respond to the compromise
- Network Security Monitoring began as an informal discipline with the creation of the Network Security Monitor in 1988

Computer Incident Response Team

- In modern society, many organizations are under constant attack by potential intruders
- As such, incident response should be a continuous business process
    - In reality, it is often an ad-hoc process, or a task designated to IT or system administrators
- The team responsible to counter such threats is the Computer Incident Response Team (CIRTs)
    - A CIRT may be one or more individuals whose duties include detecting and responding to threats

Benefits of a CIRT

- Having a formal Computer Incident Response Team benefits the organization in the following ways:
  - CIRTs collect detailed network logs and captures
  - CIRTs analyze this data to find compromised assets (laptops, servers, accounts)
  - CIRTs work with equipment owners to contain the compromised assets
  - CIRTs use NSM data for damage assessment, assessing the cost and cause of the incident

Does NSM Prevent Intrusions?

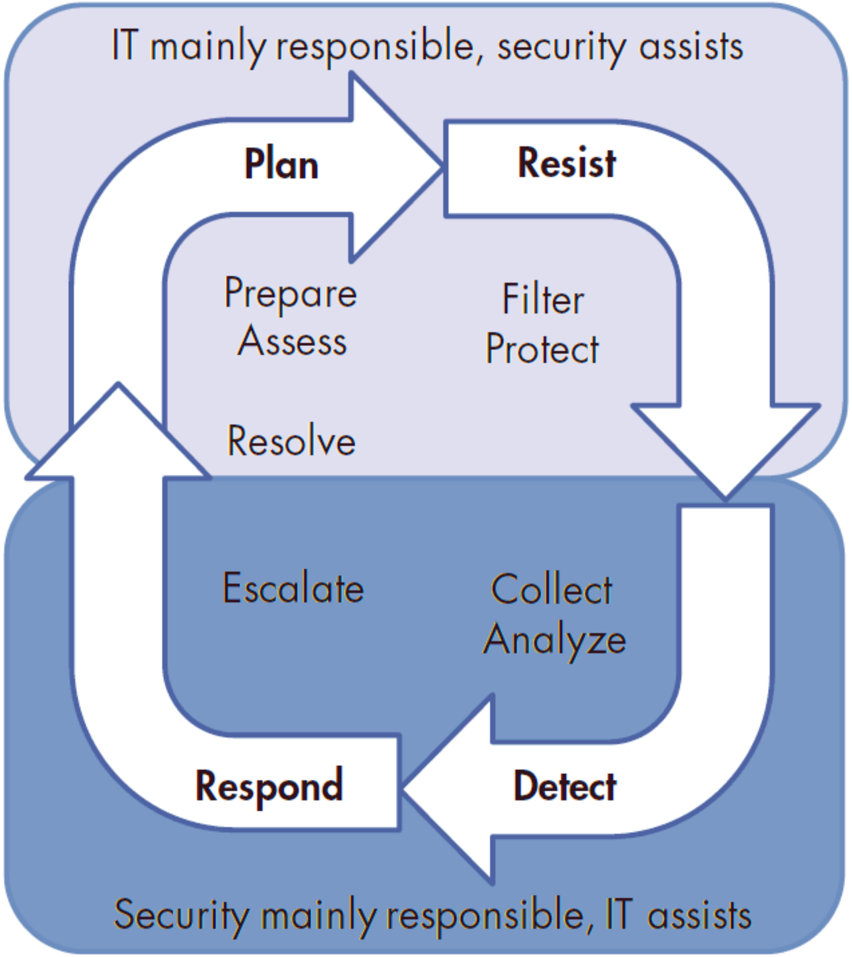
- NSM does not prevent network intrusions, as prevention eventually fails (breaches are inevitable)
- The goals of NSM are not to prevent intruders from breaching your defenses, but to prevent intruders from attaining their objectives
- Intruders can rarely complete their attack in a matter of minutes or hours, so they seek to gain persistence in target networks and have been known to stay active for years at a time

Does NSM Prevent Intrusions?

- Less advanced intrusions may achieve their goals in a number of hours or days
- Within the period, from initial unauthorized access to ultimate mission accomplishment, the CIRT can detect, respond to, and contain intruders to prevent them from completing their objective

Detecting Intrusions vs Preventing Intrusions

- If we can detect an intrusion, why can't we prevent them?
  - The systems and processes designed to protect us aren't perfect
  - Prevention can block known attacks, but performs poorly against new threats
  - Adversaries are often persistent, and use multiple tactics to compromise a system


IT mainly responsible, security assists
Plan
Resist
Prepare
Assess
Filter
Protect
Resolve
Escalate
Collect
Analyze
Respond
Detect
Security mainly responsible, IT assists

Case Study: The Importance of Time

One real-world example shows the importance of time when defending against an intruder. In November 2012, the governor of South Carolina published the public version of a Mandiant incident response report.*

Mandiant is a security company that specializes in services and software for incident detection and response. The governor hired Mandiant to assist her state with this case. Earlier that year, an attacker compromised a database operated by the state’s Department of Revenue (DoR). The report provided details on the incident, but the following abbreviated timeline helps emphasize the importance of time. This case is based exclusively upon the details in the public Mandiant report.

Case Study: The Importance of Time

August 13, 2012

- An intruder sends a malicious (phishing) email message to multiple DoR employees.
  - At least one employee clicks a link in the message, unwittingly executing malware and becoming compromised in the process.
- Available evidence indicates that the malware stole the user’s username and password.

Case Study: The Importance of Time

August 27, 2012

- The attacker logs in to a Citrix remote access service using stolen DoR user credentials.
- The attacker uses the Citrix portal to log in to the user’s workstation, and then leverages the user’s access rights to access other DoR systems and databases.

Case Study: The Importance of Time

August 29 – September 11, 2012

- The attacker interacts with a variety of DoR systems, including domain controllers, web servers, and user systems.
- He obtains passwords for all Windows user accounts and installs malicious software on many systems.
- Crucially, he manages to access a server housing DoR payment maintenance information.

Case Study: The Importance of Time

September 12, 2012

- The attacker copies database backup files to a staging directory.

Case Study: The Importance of Time

September 13 and 14, 2012

- The attacker compresses the database backup files into 14 (of the 15 total) encrypted 7-Zip archives.
- The attacker then moves the 7-Zip archives from the database server to another server and sends the data to a system on the Internet.
- Finally, the attacker deletes the backup files and 7-Zip archives.

Case Study: The Importance of Time

September 15, 2012

- The attacker interacts with 10 systems using a compromised account and performs reconnaissance.

Case Study: The Importance of Time

September 16 – October 16, 2012

- There is no evidence of attacker activity, but on October 10, 2012, a law-enforcement agency contacts the DoR with evidence that the personally identifiable information (PII) of three individuals has been stolen.
- The DoR reviews the data and determines that it would have been stored within its databases.
- On October 12, 2012, the DoR contracts with Mandiant for assistance with incident response.

Case Study: The Importance of Time

October 17, 2012

- The attacker checks connectivity to a server using the backdoor installed on September 1, 2012.
- There is no evidence of additional activity.

Case Study: The Importance of Time

October 19 and 20, 2012

- The DoR attempts to remedy the attack based on recommendations from Mandiant.
- The goal of remediation is to remove the attacker’s access and to detect any new evidence of compromise.

Case Study: The Importance of Time

October 21 – November 20, 2012

- There is no evidence of malicious activity following remediation.
- The DoR publishes the Mandiant report on this incident.

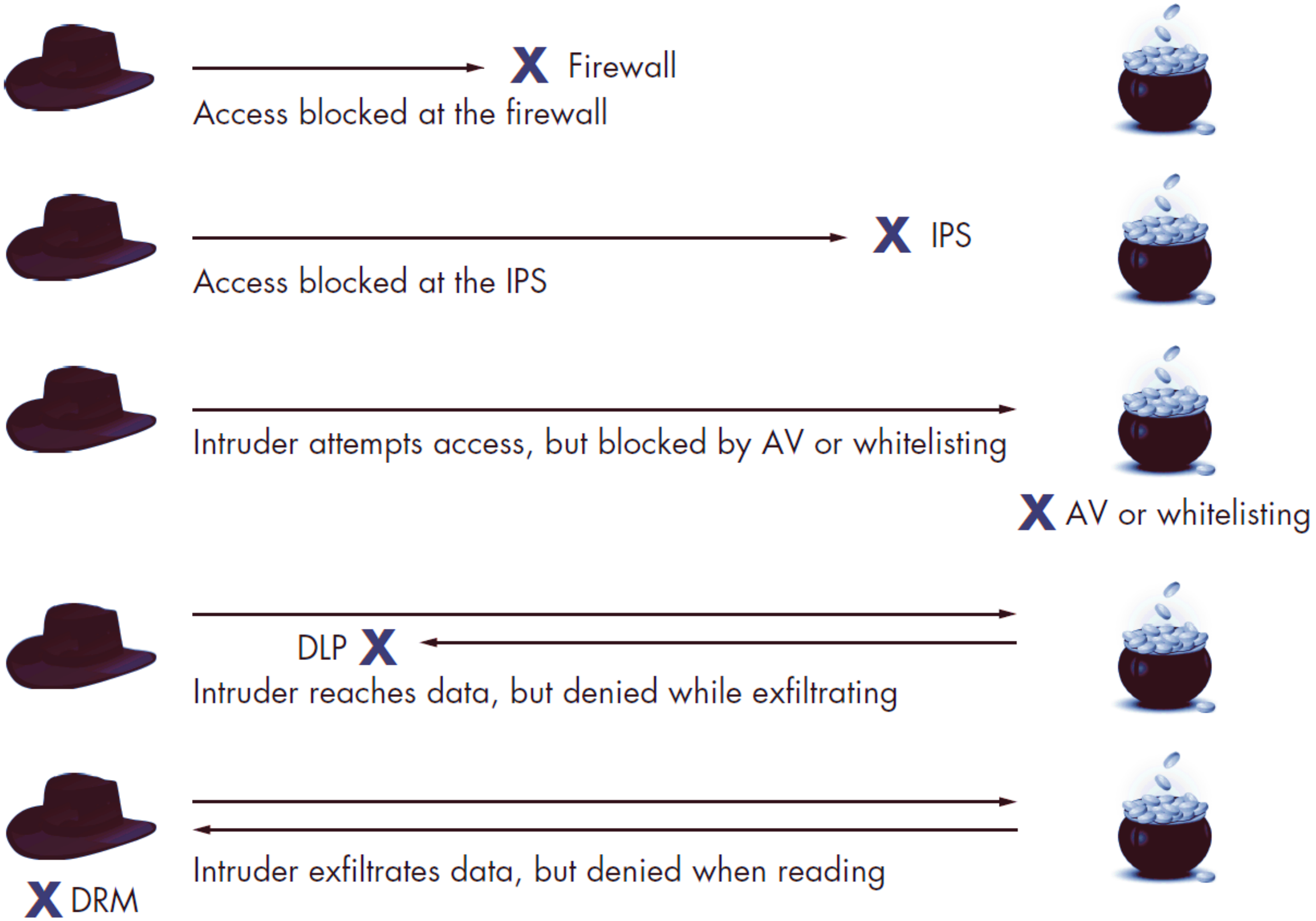
NSM vs Continuous Monitoring

- Continuous monitoring (CM) describes processes and technologies used to detect complicate and risk auditing shortfalls
  - CM is vulnerability-centric, focusing on configuration and software weaknesses
- NSM describes processes and technologies used to detect intrusion into the network
  - NSM is threat-centric, focusing on adversaries and incidence-of-compromise

NSM Role in the Overall Security Plan

- NSM is only one component of a security plan
- Other components include Firewalls, Intrusion Detection and Prevention systems, Antivirus, Access Controls, Data Loss Prevention and Digital Rights Management
- All of these components provide a control measure that is designed to drop, block or filter undesired actions at various stages of an attack
- NSM is a strategy backed by tactics that focus on visibility, not control
- NSM can add visibility when other network controls fail

NSM Role in the Overall Security Plan



X Firewall

Access blocked at the firewall

X IPS

Access blocked at the IPS

Intruder attempts access, but blocked by AV or whitelisting

X AV or whitelisting

DLP X

Intruder reaches data, but denied while exfiltrating

Intruder exfiltrates data, but denied when reading

X DRM

Why Does NSM Work?

- NSM provides the ability to detect, respond to and contain intruders even when they evade control measures that block, filter and deny malicious activity
- Network operators must achieve perfect defense in order to keep out intruders
  - If an intruder finds and exploits a vulnerability in a system, they may be able to compromise large portions of the system
- The goals of an intruder include compromising a network, establish persistence mechanisms, and remaining in the system, undetected, free to gather information at will

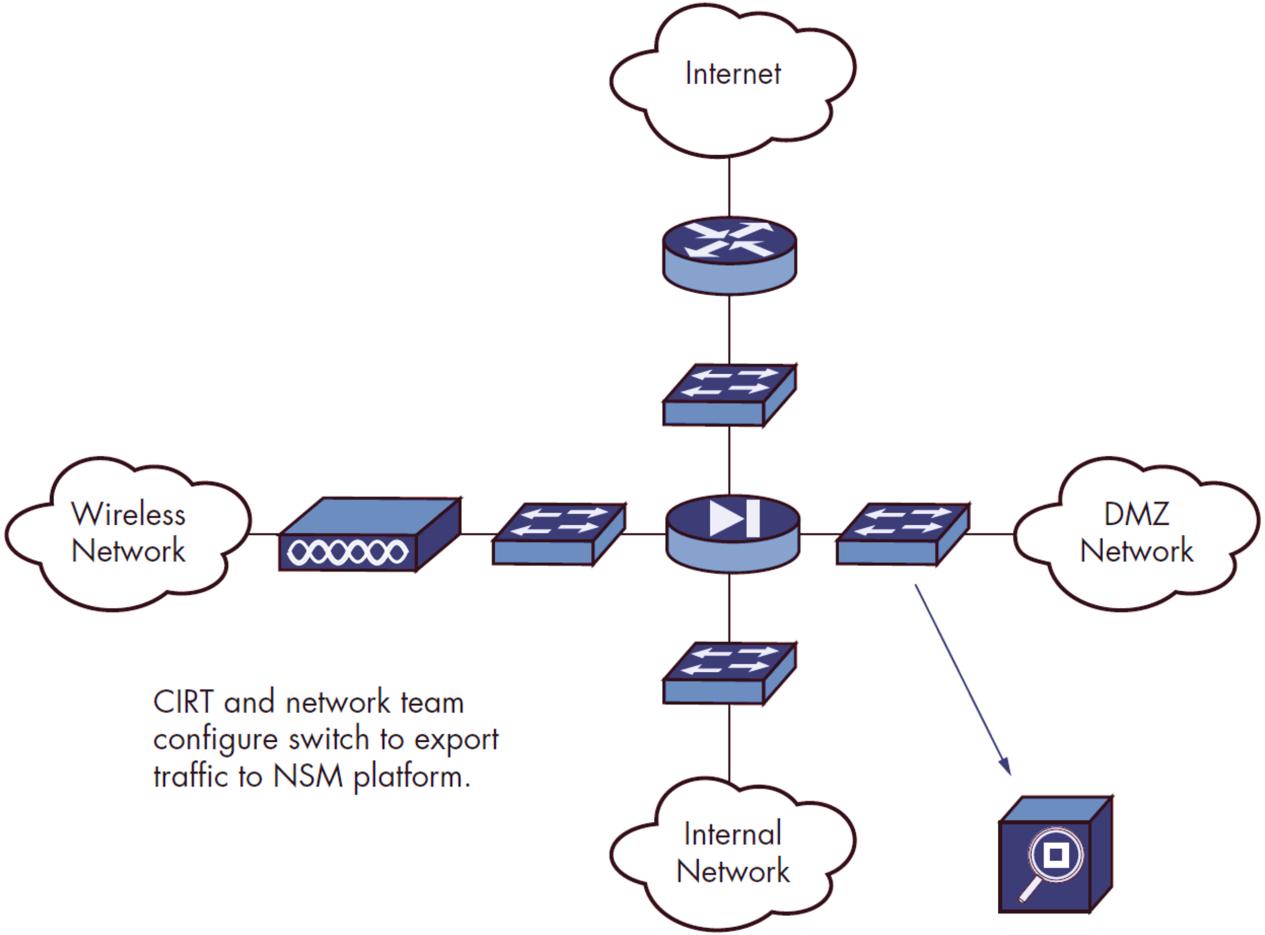
Why Does NSM Work?

- If an organization that makes visibility a priority, it can be extremely hostile to persistent intruders
- With the right tools, data and skills, the CIRT can detect an intrusion and disrupt the intruder before they achieve their goals

NSM Deployment

- NSM starts at the network (with some variations including host-based agents), and collects network traffic information
- To be successful, you need to understand network architecture and protocols to determine the optimal placement of NSM sensors
  - The CIRT will often collaborate with the network team to determine this
- In the following scenario, an NSM sensor has been placed between the demilitarized zone (DMZ) for optimal visibility

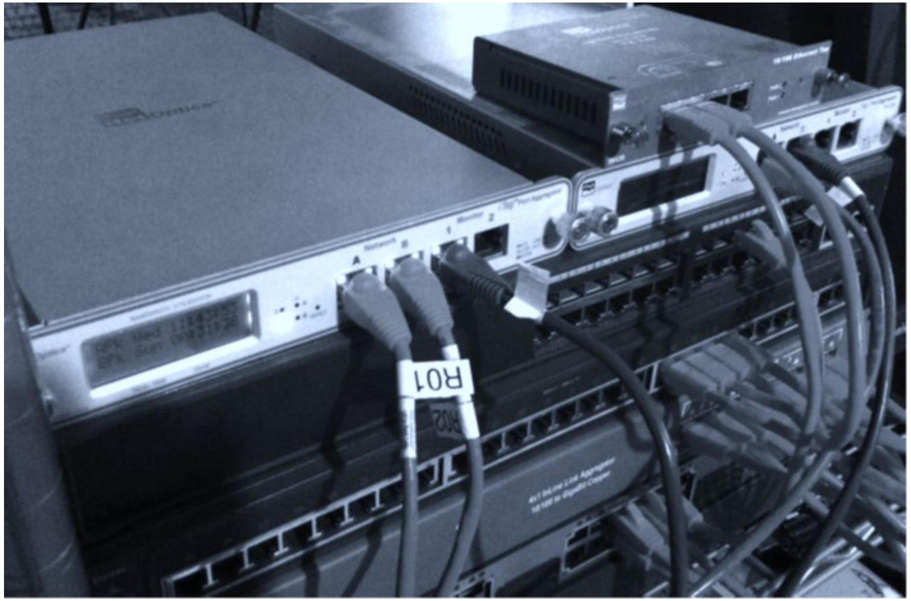
NSM Deployment



CIRT and network team configure switch to export traffic to NSM platform.

NSM Deployment

- Similar to the requirements of an intrusion detection system (IDS), NSM sensors require a copy of network traffic to operate
  - This can be achieved by means of port mirroring on a network switch, or by use of a hardware tap



When NSM Won’t Work

- Regardless of how many sensors are placed on the network, NSM will not work well if it doesn’t have visibility of the traffic that you care about
- Traffic that is encrypted cannot be inspected (by standard methods), so it is now desirable for intruders to encrypt all communications
- As wireless networks also use encryption, it is often only possible to monitor traffic at the egress edge of a wireless network
  - Any communications directly between wireless hosts is not observed

When NSM Won't Work

- Similarly, NSM does not generally operate on cellular traffic, as the network is outside the bounds of the technical and legal mandate for most organizations
- In cloud environments, NSM faces unique challenges as the service provider owns the network infrastructure and will usually not provide access to customers

Legal Considerations

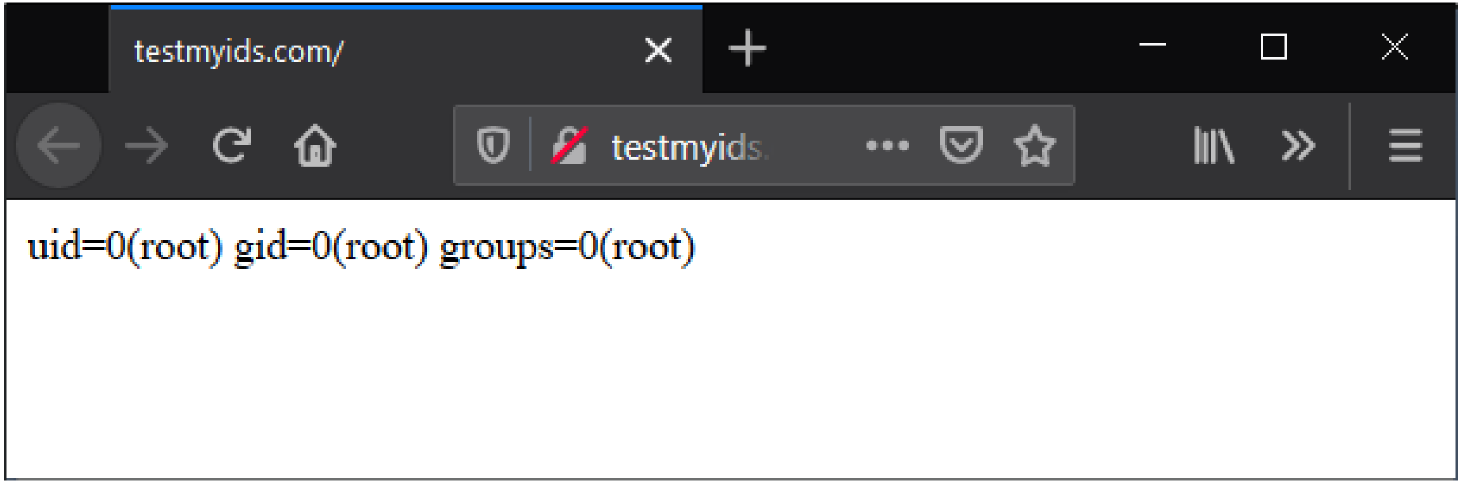
- As laws change based on location, it is advised that the legality of NSM is assessed for every region that the organization will operate in
- In most situations, monitoring is permitted, provided that the involved parties are aware that monitoring is in place and provide consent
- It is important that users are prompted when connecting to the network with a message indicating that monitoring is in place and that they have no expectation of privacy while accessing network resources

Protecting User Privacy

- As it is important to protect user privacy, NSM operations should focus on the intruder, and not on monitoring authorized users
- The CIRT are focused with external threats, forensic teams are focused on internal threats
  - The work of the CIRT and forensic investigators should remain separate unless you have been directed to provide logs to the investigator
- If the two groups are not clearly defined, users are less likely to trust the CIRT and may by less cooperative when an intrusion occurs

Sample NSM Test

- In this example, we use the Firefox web browser to visit http://www.testmyids.com/, which is used to test some types of security equipment
- The page returns what looks like the output of a Unix user ID (id) command run by an account with user ID (UID) 0, such as a root user



```
uid=0(root) gid=0(root) groups=0(root)
```

Sample NSM Test

- On the network, the Firefox web browser and the http://www.testmyids.com/ web server together generate three sets of data relevant to the NSM approach:
  - The browser generates a Domain Name System (DNS) request for http://www.testmyids.com/, and receives a reply from a DNS server
  - The browser requests the web page, and the web server replies
  - The web browser requests a Favorite icon from the web server, and the web server replies.

NSM Data Types

- NSM data may include the following:
  - Full content
  - Extracted content
  - Session data
  - Transaction data
  - Statistical data
  - Metadata
  - Alert data

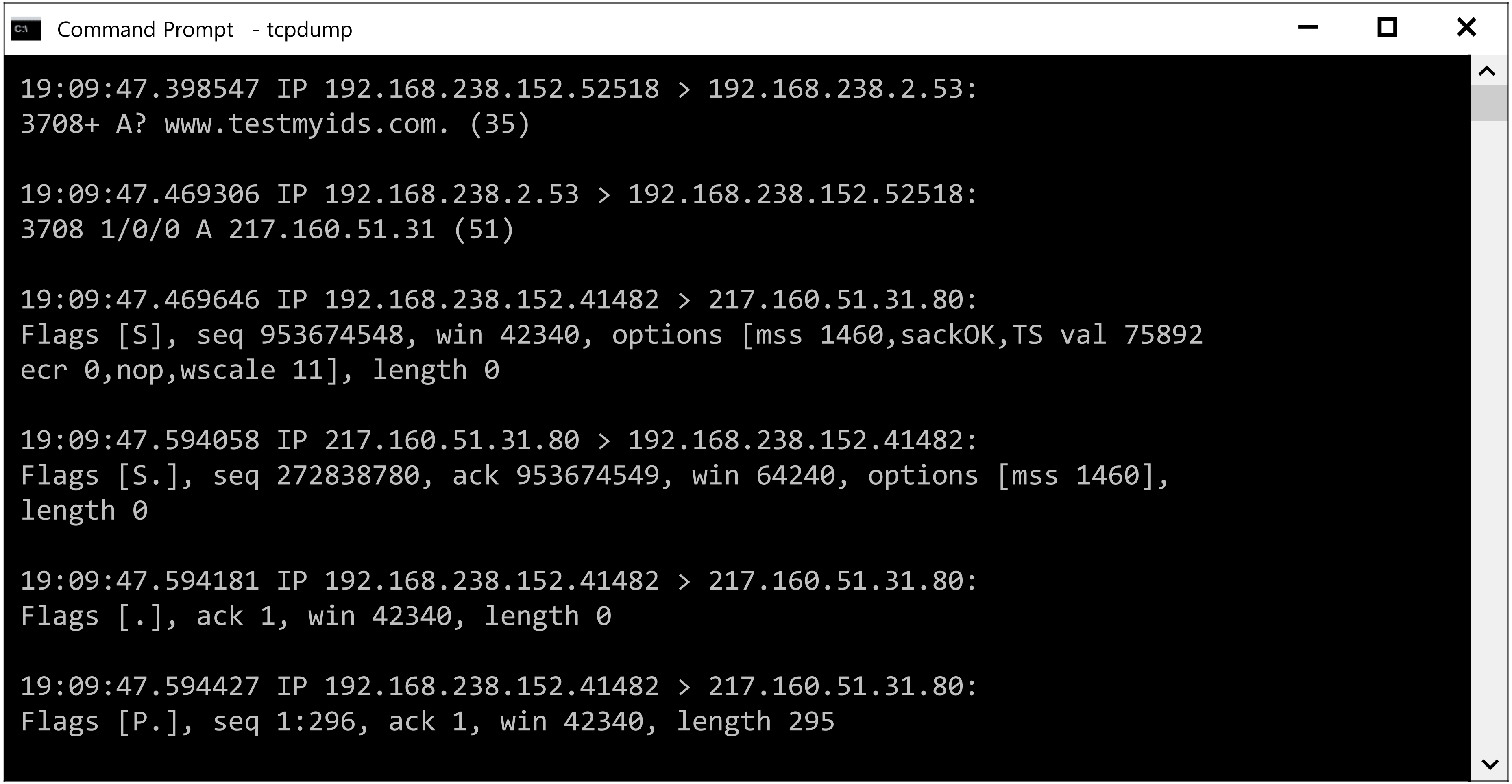
Full Content Data

- When we collect full content data, all the network information that is passed to the NSM sensor is saved
- When analysists work with full content data, the data is generally reviewed in two stages
  - Reviewing a summary of the data, represented by traffic headers
  - Inspecting individual packets

Reviewing a Data Summary

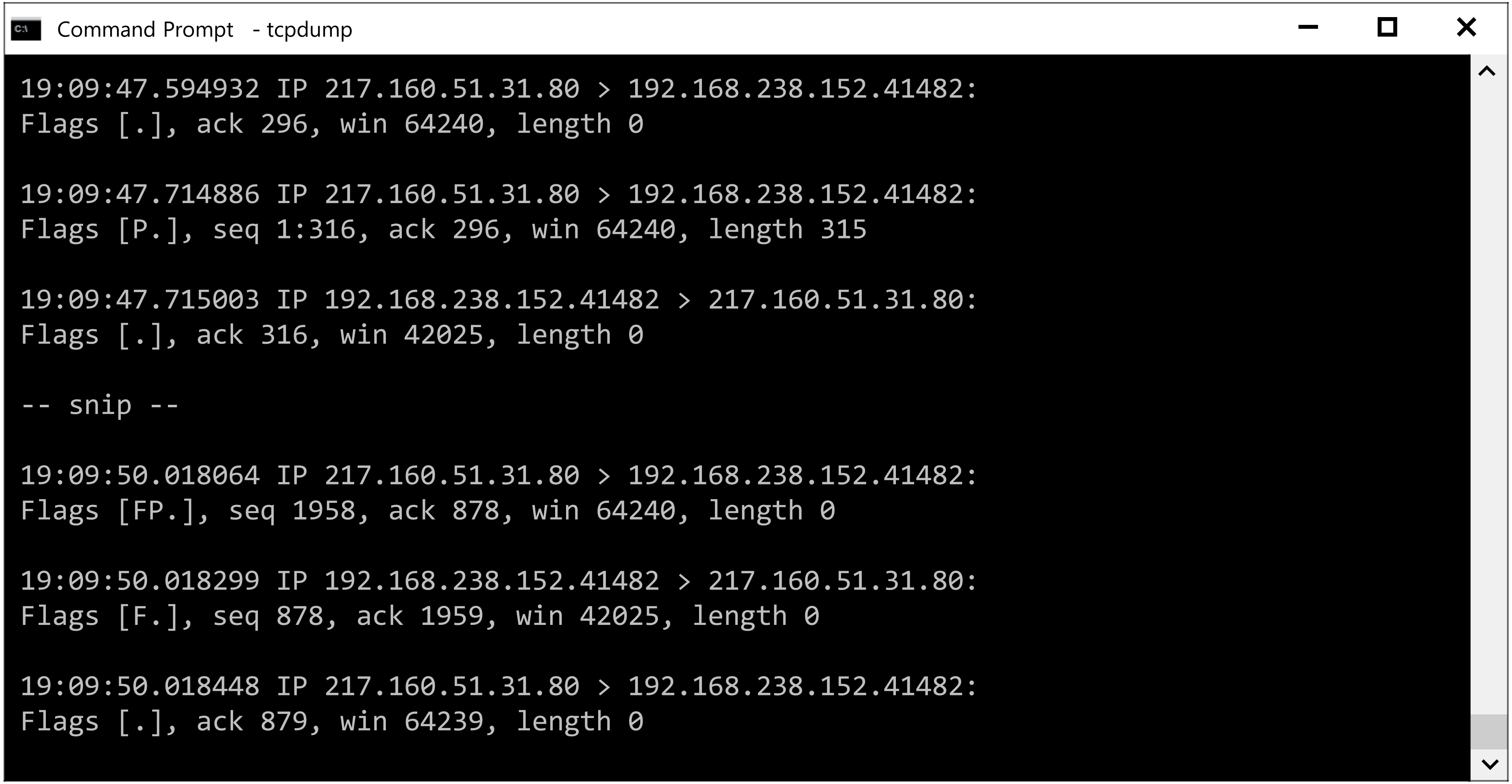
- The example displays the output of using the Tcpdump tool while browsing http://testmyids.com/, displaying header information

Reviewing a Data Summary



```
19:09:47.398547 IP 192.168.238.152.52518 > 192.168.238.2.53:
3708+ A? www.testmyids.com. (35)

19:09:47.469306 IP 192.168.238.2.53 > 192.168.238.152.52518:
3708 1/0/0 A 217.160.51.31 (51)

19:09:47.469646 IP 192.168.238.152.41482 > 217.160.51.31.80:
Flags [S], seq 953674548, win 42340, options [mss 1460,sackOK,TS val 75892
ecr 0,nop,wscale 11], length 0

19:09:47.594058 IP 217.160.51.31.80 > 192.168.238.152.41482:
Flags [S.], seq 272838780, ack 953674549, win 64240, options [mss 1460],
length 0

19:09:47.594181 IP 192.168.238.152.41482 > 217.160.51.31.80:
Flags [.], ack 1, win 42340, length 0

19:09:47.594427 IP 192.168.238.152.41482 > 217.160.51.31.80:
Flags [P.], seq 1:296, ack 1, win 42340, length 295
```

Reviewing a Data Summary



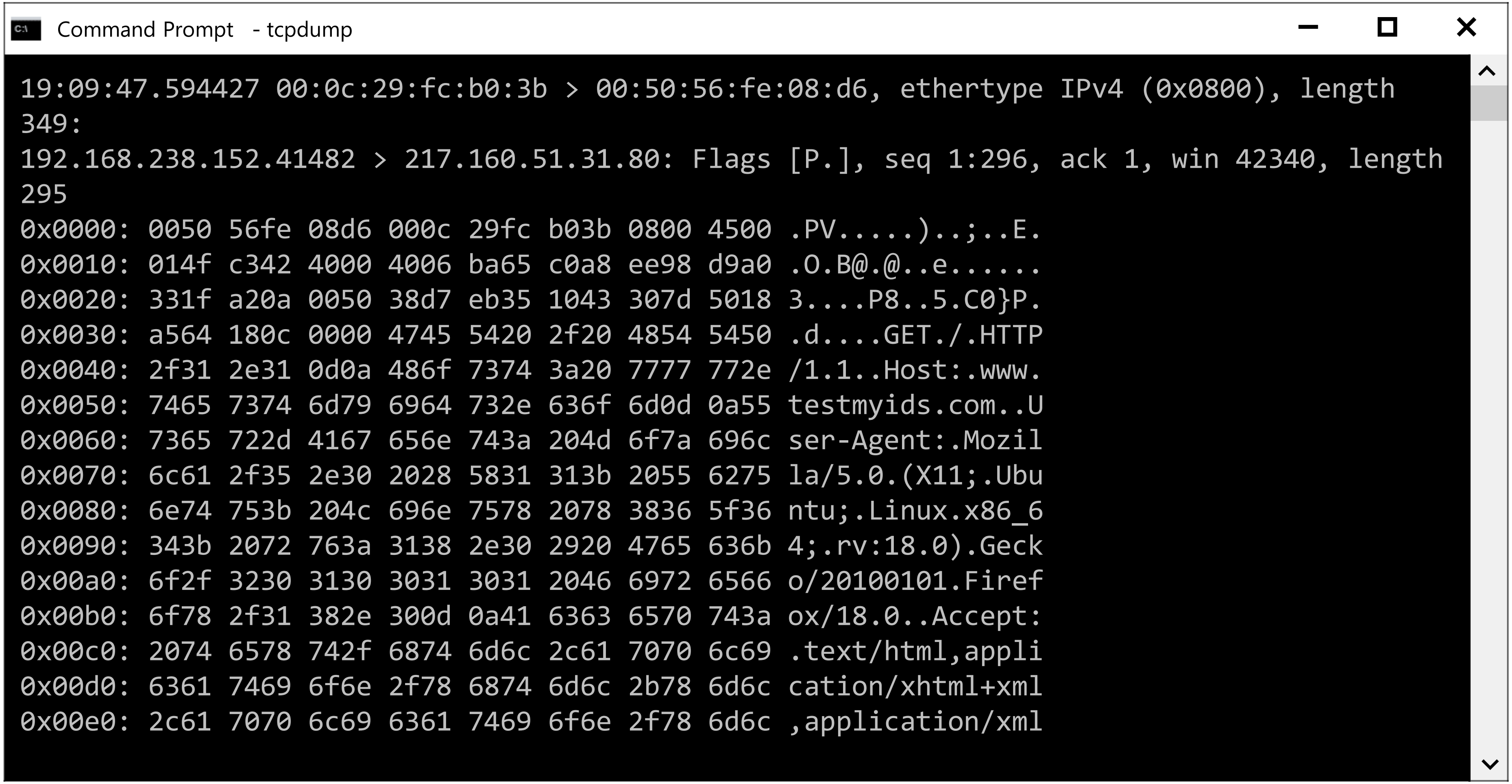
```
19:09:47.594932 IP 217.160.51.31.80 > 192.168.238.152.41482:
Flags [.], ack 296, win 64240, length 0

19:09:47.714886 IP 217.160.51.31.80 > 192.168.238.152.41482:
Flags [P.], seq 1:316, ack 296, win 64240, length 315

19:09:47.715003 IP 192.168.238.152.41482 > 217.160.51.31.80:
Flags [.], ack 316, win 42025, length 0

-- snip --

19:09:50.018064 IP 217.160.51.31.80 > 192.168.238.152.41482:
Flags [FP.], seq 1958, ack 878, win 64240, length 0

19:09:50.018299 IP 192.168.238.152.41482 > 217.160.51.31.80:
Flags [F.], seq 878, ack 1959, win 42025, length 0

19:09:50.018448 IP 217.160.51.31.80 > 192.168.238.152.41482:
Flags [.], ack 879, win 64239, length 0
```

Full Content Data

Inspecting Packets

- After reviewing the summary data, analysists select one or more packets for deeper inspection
- The example shows the shows the same headers as seen in the sixth packet from the previous example, but with the layer 2 header listed first
- The headers are now followed by payloads, displayed in both hexadecimal and converted to ASCII

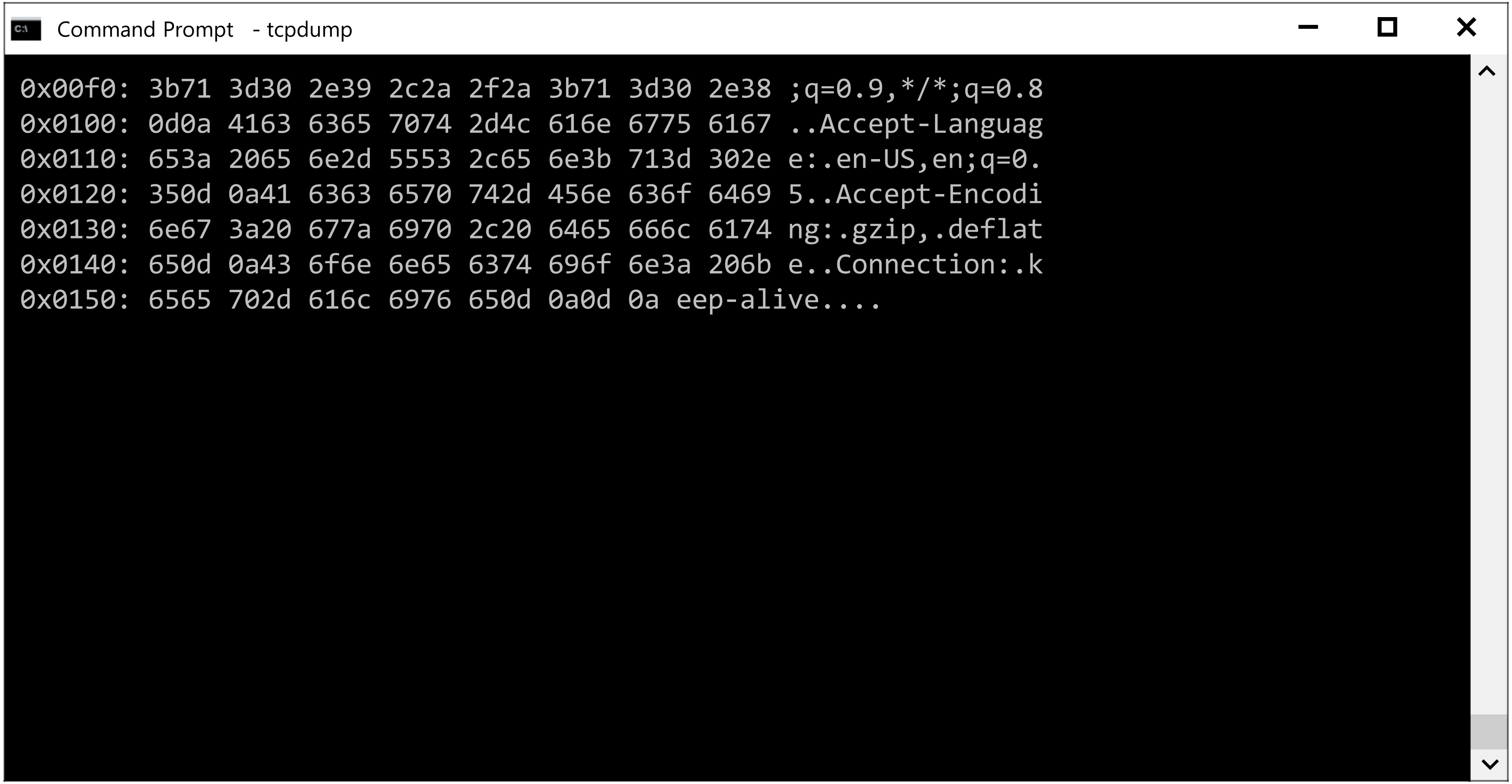
Inspecting Packets



Command Prompt - tcpdump

```
19:09:47.594427 00:0c:29:fc:b0:3b > 00:50:56:fe:08:d6, ethertype IPv4 (0x0800), length
349:
192.168.238.152.41482 > 217.160.51.31.80: Flags [P.], seq 1:296, ack 1, win 42340, length
295
0x0000:  0050 56fe 08d6 000c 29fc b03b 0800 4500 .PV.....)..;..E.
0x0010:  014f c342 4000 4006 ba65 c0a8 ee98 d9a0 .O.B@.@..e......
0x0020:  331f a20a 0050 38d7 eb35 1043 307d 5018 3....P8..5.C0}P.
0x0030:  a564 180c 0000 4745 5420 2f20 4854 5450 .d....GET./.HTTP
0x0040:  2f31 2e31 0d0a 486f 7374 3a20 7777 772e /1.1..Host:.www.
0x0050:  7465 7374 6d79 6964 732e 636f 6d0d 0a55 testmyids.com..U
0x0060:  7365 722d 4167 656e 743a 204d 6f7a 696c ser-Agent:.Mozil
0x0070:  6c61 2f35 2e30 2028 5831 313b 2055 6275 la/5.0.(X11;.Ubu
0x0080:  6e74 753b 204c 696e 7578 2078 3836 5f36 ntu;.Linux.x86_6
0x0090:  343b 2072 763a 3138 2e30 2920 4765 636b 4;.rv:18.0).Geck
0x00a0:  6f2f 3230 3130 3031 3031 2046 6972 6566 o/20100101.Firef
0x00b0:  6f78 2f31 382e 300d 0a41 6363 6570 743a ox/18.0..Accept:
0x00c0:  2074 6578 742f 6874 6d6c 2c61 7070 6c69 .text/html,appli
0x00d0:  6361 7469 6f6e 2f78 6874 6d6c 2b78 6d6c cation/xhtml+xml
0x00e0:  2c61 7070 6c69 6361 7469 6f6e 2f78 6d6c ,application/xml
```

Inspecting Packets



```
0x00f0: 3b71 3d30 2e39 2c2a 2f2a 3b71 3d30 2e38 ;q=0.9,*/*;q=0.8
0x0100: 0d0a 4163 6365 7074 2d4c 616e 6775 6167 ..Accept-Languag
0x0110: 653a 2065 6e2d 5553 2c65 6e3b 713d 302e e:.en-US,en;q=0.
0x0120: 350d 0a41 6363 6570 742d 456e 636f 6469 5..Accept-Encodi
0x0130: 6e67 3a20 677a 6970 2c20 6465 666c 6174 ng:.gzip,.deflat
0x0140: 650d 0a43 6f6e 6e65 6374 696f 6e3a 206b e..Connection:.k
0x0150: 6565 702d 616c 6976 650d 0a0d 0a eep-alive....
```

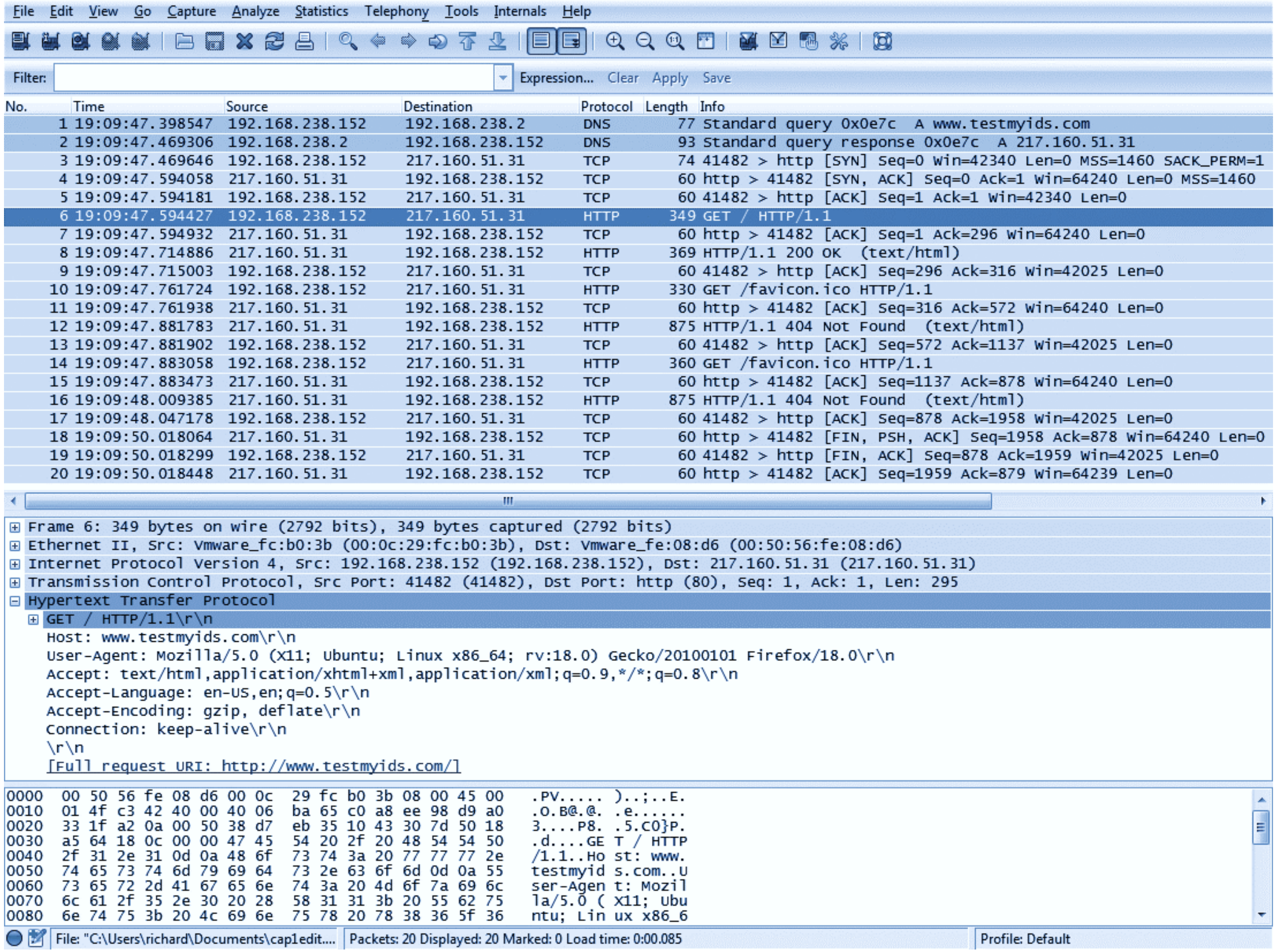
Full Content Data

- This view provides much more information than the header did
- You see full header information including MAC
- addresses, IP addresses, IP protocol, etc., but also the higher-level content sent by the web browser
- You can read the GET request, the user agent, some Hypertext Transfer Protocol (HTTP) headers (Accept, Accept-Language, Accept-Encoding, etc.

Using Graphical Tools to View Traffic

- Graphical tools like Wireshark can also be used to view full content traffic
- The following screenshot shows the same packet from the previous example
- Full content data provides the most flexible options for traffic analysis

Using Graphical Tools to View Traffic



```
No.  Time             Source           Destination      Protocol Length Info
   1 19:09:47.398547  192.168.238.152  192.168.238.2    DNS        77 Standard query 0x0e7c  A www.testmyids.com
   2 19:09:47.469306  192.168.238.2    192.168.238.152  DNS        93 Standard query response 0x0e7c  A 217.160.51.31
   3 19:09:47.469646  192.168.238.152  217.160.51.31    TCP        74 41482 > http [SYN] Seq=0 Win=42340 Len=0 MSS=1460 SACK_PERM=1
   4 19:09:47.594058  217.160.51.31    192.168.238.152  TCP        60 http > 41482 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
   5 19:09:47.594181  192.168.238.152  217.160.51.31    TCP        60 41482 > http [ACK] Seq=1 Ack=1 Win=42340 Len=0
   6 19:09:47.594427  192.168.238.152  217.160.51.31    HTTP      349 GET / HTTP/1.1
   7 19:09:47.594932  217.160.51.31    192.168.238.152  TCP        60 http > 41482 [ACK] Seq=1 Ack=296 Win=64240 Len=0
   8 19:09:47.714886  217.160.51.31    192.168.238.152  HTTP      369 HTTP/1.1 200 OK  (text/html)
   9 19:09:47.715003  192.168.238.152  217.160.51.31    TCP        60 41482 > http [ACK] Seq=296 Ack=316 Win=42025 Len=0
  10 19:09:47.761724  192.168.238.152  217.160.51.31    HTTP      330 GET /favicon.ico HTTP/1.1
  11 19:09:47.761938  217.160.51.31    192.168.238.152  TCP        60 http > 41482 [ACK] Seq=316 Ack=572 Win=64240 Len=0
  12 19:09:47.881783  217.160.51.31    192.168.238.152  HTTP      875 HTTP/1.1 404 Not Found  (text/html)
  13 19:09:47.881902  192.168.238.152  217.160.51.31    TCP        60 41482 > http [ACK] Seq=572 Ack=1137 Win=42025 Len=0
  14 19:09:47.883058  192.168.238.152  217.160.51.31    HTTP      360 GET /favicon.ico HTTP/1.1
  15 19:09:47.883473  217.160.51.31    192.168.238.152  TCP        60 http > 41482 [ACK] Seq=1137 Ack=878 Win=64240 Len=0
  16 19:09:48.009385  217.160.51.31    192.168.238.152  HTTP      875 HTTP/1.1 404 Not Found  (text/html)
  17 19:09:48.047178  192.168.238.152  217.160.51.31    TCP        60 41482 > http [ACK] Seq=878 Ack=1958 Win=42025 Len=0
  18 19:09:50.018064  217.160.51.31    192.168.238.152  TCP        60 http > 41482 [FIN, PSH, ACK] Seq=1958 Ack=878 Win=64240 Len=0
  19 19:09:50.018299  192.168.238.152  217.160.51.31    TCP        60 41482 > http [FIN, ACK] Seq=878 Ack=1959 Win=42025 Len=0
  20 19:09:50.018448  217.160.51.31    192.168.238.152  TCP        60 http > 41482 [ACK] Seq=1959 Ack=879 Win=64239 Len=0
```

```
⊞ Frame 6: 349 bytes on wire (2792 bits), 349 bytes captured (2792 bits)
⊞ Ethernet II, Src: Vmware_fc:b0:3b (00:0c:29:fc:b0:3b), Dst: Vmware_fe:08:d6 (00:50:56:fe:08:d6)
⊞ Internet Protocol Version 4, Src: 192.168.238.152 (192.168.238.152), Dst: 217.160.51.31 (217.160.51.31)
⊞ Transmission Control Protocol, Src Port: 41482 (41482), Dst Port: http (80), Seq: 1, Ack: 1, Len: 295
⊟ Hypertext Transfer Protocol
  ⊞ GET / HTTP/1.1\r\n
    Host: www.testmyids.com\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:18.0) Gecko/20100101 Firefox/18.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://www.testmyids.com/]
```

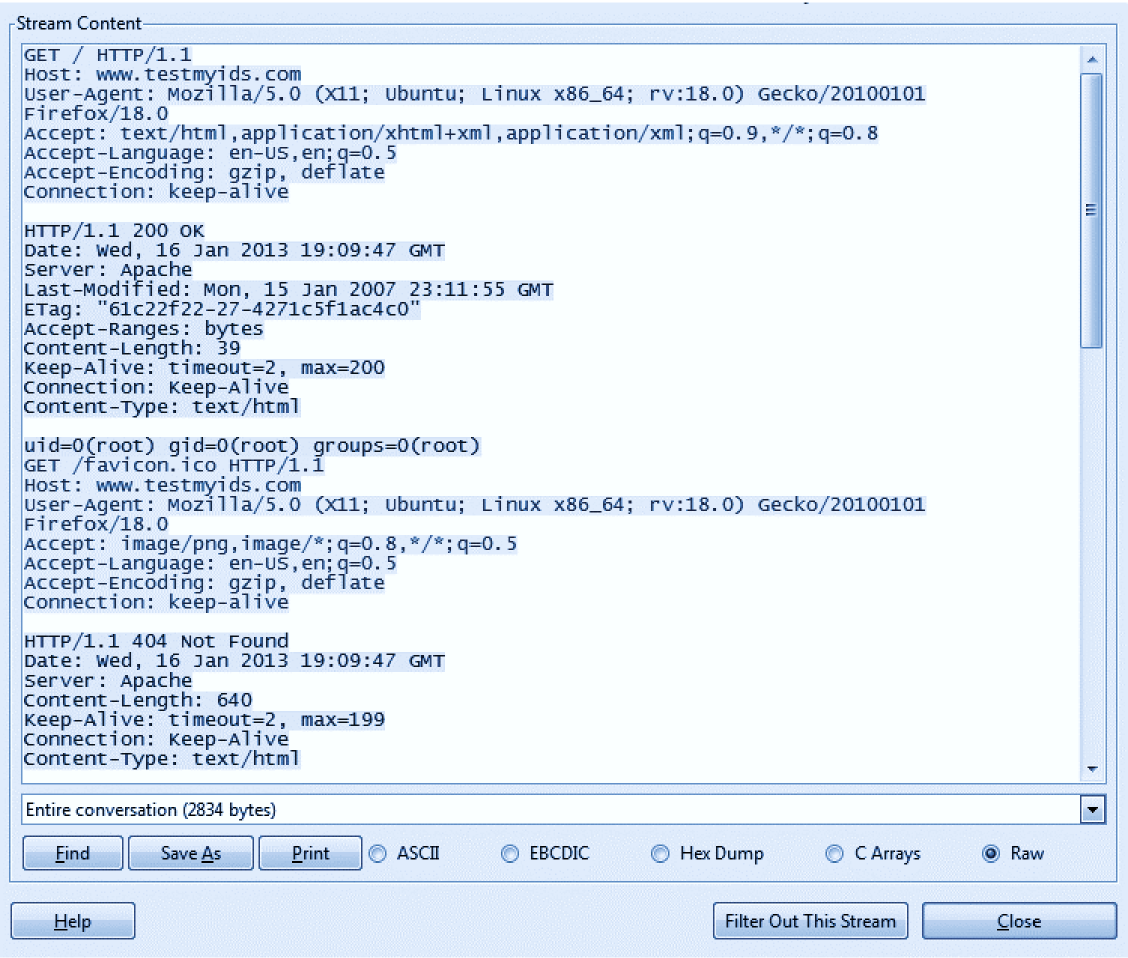
```
0000  00 50 56 fe 08 d6 00 0c  29 fc b0 3b 08 00 45 00   .PV..... )..;..E.
0010  01 4f c3 42 40 00 40 06  ba 65 c0 a8 ee 98 d9 a0   .O.B@.@. .e......
0020  33 1f a2 0a 00 50 38 d7  eb 35 10 43 30 7d 50 18   3....P8. .5.C0}P.
0030  a5 64 18 0c 00 00 47 45  54 20 2f 20 48 54 54 50   .d....GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 77 77 77 2e   /1.1..Ho st: www.
0050  74 65 73 74 6d 79 69 64  73 2e 63 6f 6d 0d 0a 55   testmyid s.com..U
0060  73 65 72 2d 41 67 65 6e  74 3a 20 4d 6f 7a 69 6c   ser-Agen t: Mozil
0070  6c 61 2f 35 2e 30 20 28  58 31 31 3b 20 55 62 75   la/5.0 ( X11; Ubu
0080  6e 74 75 3b 20 4c 69 6e  75 78 20 78 38 36 5f 36   ntu; Lin ux x86_6
```

File: "C:\Users\richard\Documents\cap1edit.... Packets: 20 Displayed: 20 Marked: 0 Load time: 0:00.085 Profile: Default

Extracted Content Data

- Extracted Content refers to high-level data streams, such as files, images, and media
- Unlike full content data, the transferred data itself is the focus of the investigation
- This type of data review could uncover malware an attacker transferred into the network
- The following example shows the content sent from the web browser to the web server and from the web server back to the web browser

Extracted Content Data



Stream Content

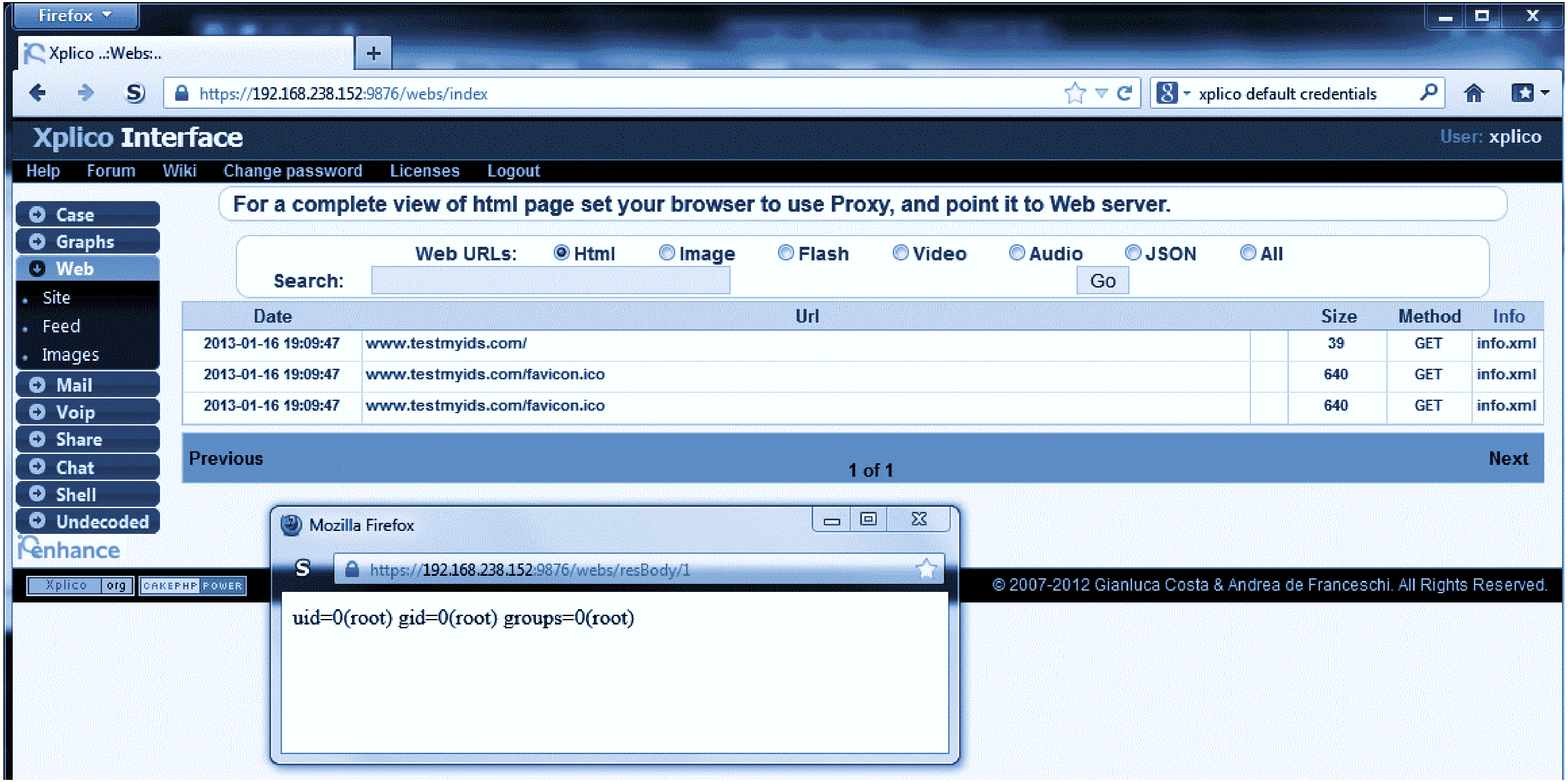
```
GET / HTTP/1.1
Host: www.testmyids.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:18.0) Gecko/20100101
Firefox/18.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive

HTTP/1.1 200 OK
Date: Wed, 16 Jan 2013 19:09:47 GMT
Server: Apache
Last-Modified: Mon, 15 Jan 2007 23:11:55 GMT
ETag: "61c22f22-27-4271c5f1ac4c0"
Accept-Ranges: bytes
Content-Length: 39
Keep-Alive: timeout=2, max=200
Connection: Keep-Alive
Content-Type: text/html

uid=0(root) gid=0(root) groups=0(root)
GET /favicon.ico HTTP/1.1
Host: www.testmyids.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:18.0) Gecko/20100101
Firefox/18.0
Accept: image/png,image/*;q=0.8,*/*;q=0.5
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive

HTTP/1.1 404 Not Found
Date: Wed, 16 Jan 2013 19:09:47 GMT
Server: Apache
Content-Length: 640
Keep-Alive: timeout=2, max=199
Connection: Keep-Alive
Content-Type: text/html
```

Entire conversation (2834 bytes)

Extracted Content Data

- CIRTs can analyze extracted content for suspicious or malicious data
- Intruders may have injected links to malicious websites into websites trusted by users in an effort misdirect them
- In addition to viewing web browsing activities as logs or data streams, it can be helpful to view a reconstruction of a web browsing session
- Xplico can rebuild a web page whose content was captured in network form

Extracted Content Data



For a complete view of html page set your browser to use Proxy, and point it to Web server.

Web URLs: ● Html ○ Image ○ Flash ○ Video ○ Audio ○ JSON ○ All

Search: Go

Date	Url	Size	Method	Info
2013-01-16 19:09:47	www.testmyids.com/	39	GET	info.xml
2013-01-16 19:09:47	www.testmyids.com/favicon.ico	640	GET	info.xml
2013-01-16 19:09:47	www.testmyids.com/favicon.ico	640	GET	info.xml

Previous 1 of 1 Next

© 2007-2012 Gianluca Costa & Andrea de Franceschi. All Rights Reserved.

```
uid=0(root) gid=0(root) groups=0(root)
```

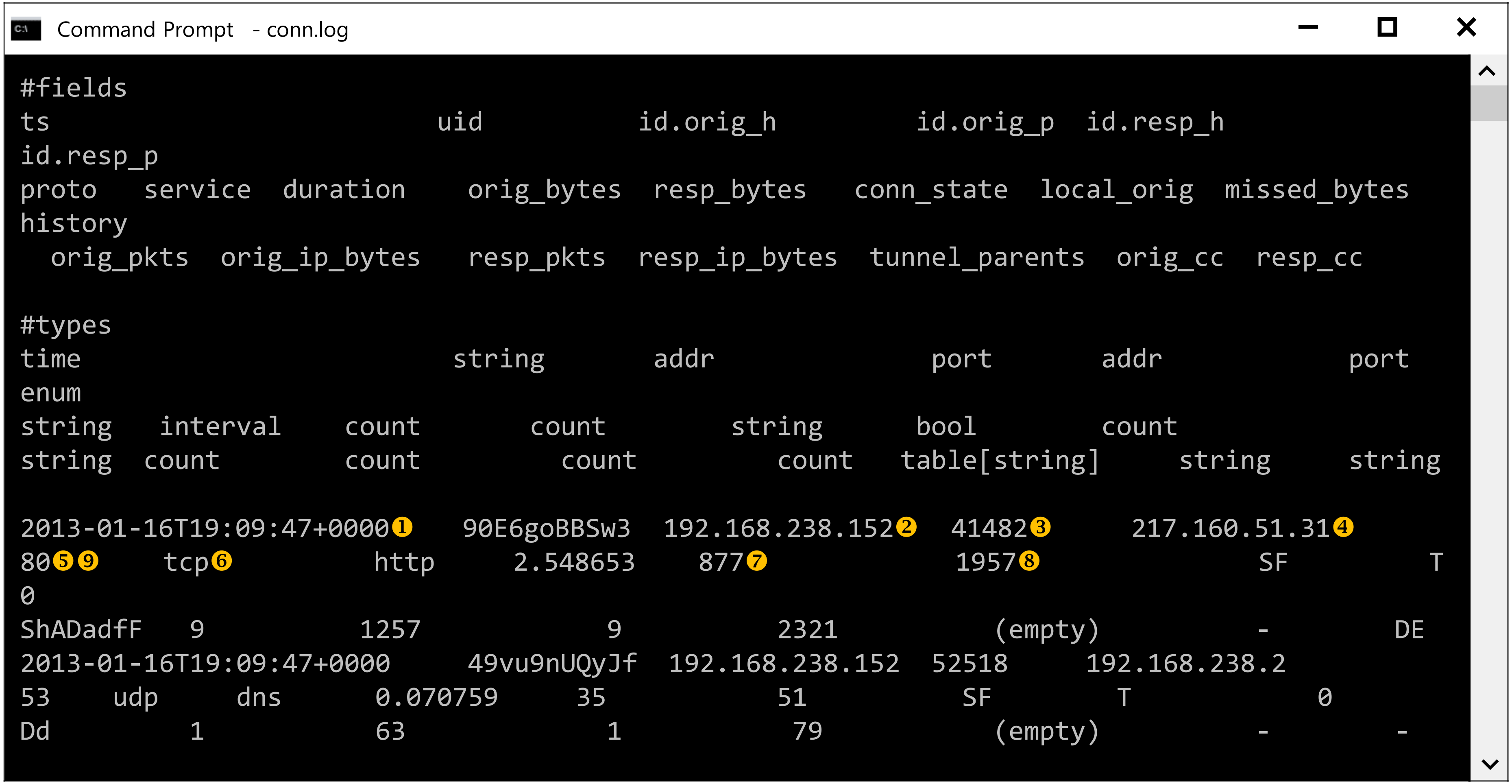
Extracted Content Data

- CIRTs extract content from network traffic in order to use the data as an input for another analytical tool
- NSM tools can extract executable binaries and submit them to antivirus engines for analysis
- The samples could also be reverse engineered, or “detonated” in a sandbox environment for additional examination

Session Data

- Session data is a record of the conversation between two network nodes
- A tool like Bro can generate logs based on its inspection of network traffic
- The example displays an excerpt from the Bro *conn.log* related to the Full Content Data example

Session Data



```
#fields
ts                         uid          id.orig_h          id.orig_p  id.resp_h
id.resp_p
proto   service  duration    orig_bytes  resp_bytes   conn_state  local_orig  missed_bytes
history
  orig_pkts  orig_ip_bytes   resp_pkts  resp_ip_bytes  tunnel_parents  orig_cc  resp_cc

#types
time                        string       addr                port       addr              port
enum
string   interval     count        count        string      bool        count
string  count         count         count         count   table[string]     string      string

2013-01-16T19:09:47+0000❶   90E6goBBSw3  192.168.238.152❷  41482❸     217.160.51.31❹
80❺❾     tcp❻            http     2.548653    877❼               1957❽               SF         T
0
ShADadfF   9          1257            9          2321          (empty)          -        DE
2013-01-16T19:09:47+0000     49vu9nUQyJf  192.168.238.152  52518     192.168.238.2
53     udp     dns      0.070759     35           51           SF         T            0
Dd           1          63            1           79           (empty)          -        -
```

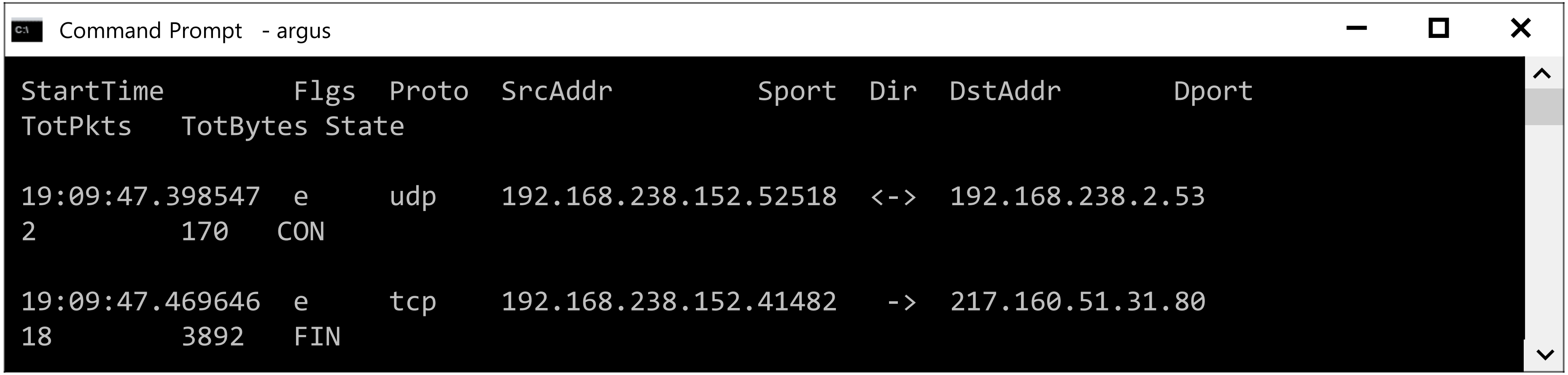
Session Data

- Session data collapses much of the detail into core elements:
  1) Timestamp
  2) Source IP Address
  3) Source Port
  4) Destination IP Address
  5) Destination Port
  6) Protocol
  7) Application bytes sent by the source
  8) Application bytes sent by the destination

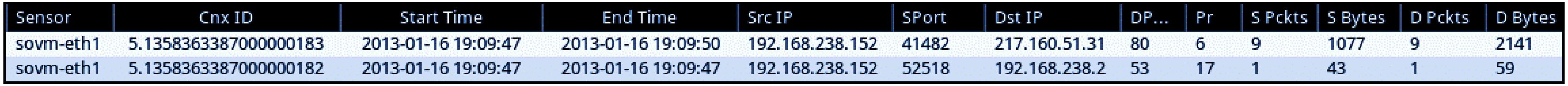
Session Data

- Session data requires much less hard drive space than full content data
- Both may be generated, with an extended retention period applied to session data
- The following examples show session data generated by the Argus and Siguil tools
- Session data is focused on the “call details” of network activity, such as who spoke, when, how, and the amount of information exchanged by each party

Session Data



```
StartTime          Flgs  Proto  SrcAddr             Sport  Dir  DstAddr        Dport
TotPkts    TotBytes State

19:09:47.398547  e     udp    192.168.238.152.52518  <->  192.168.238.2.53
2          170    CON

19:09:47.469646  e     tcp    192.168.238.152.41482   ->  217.160.51.31.80
18         3892    FIN
```

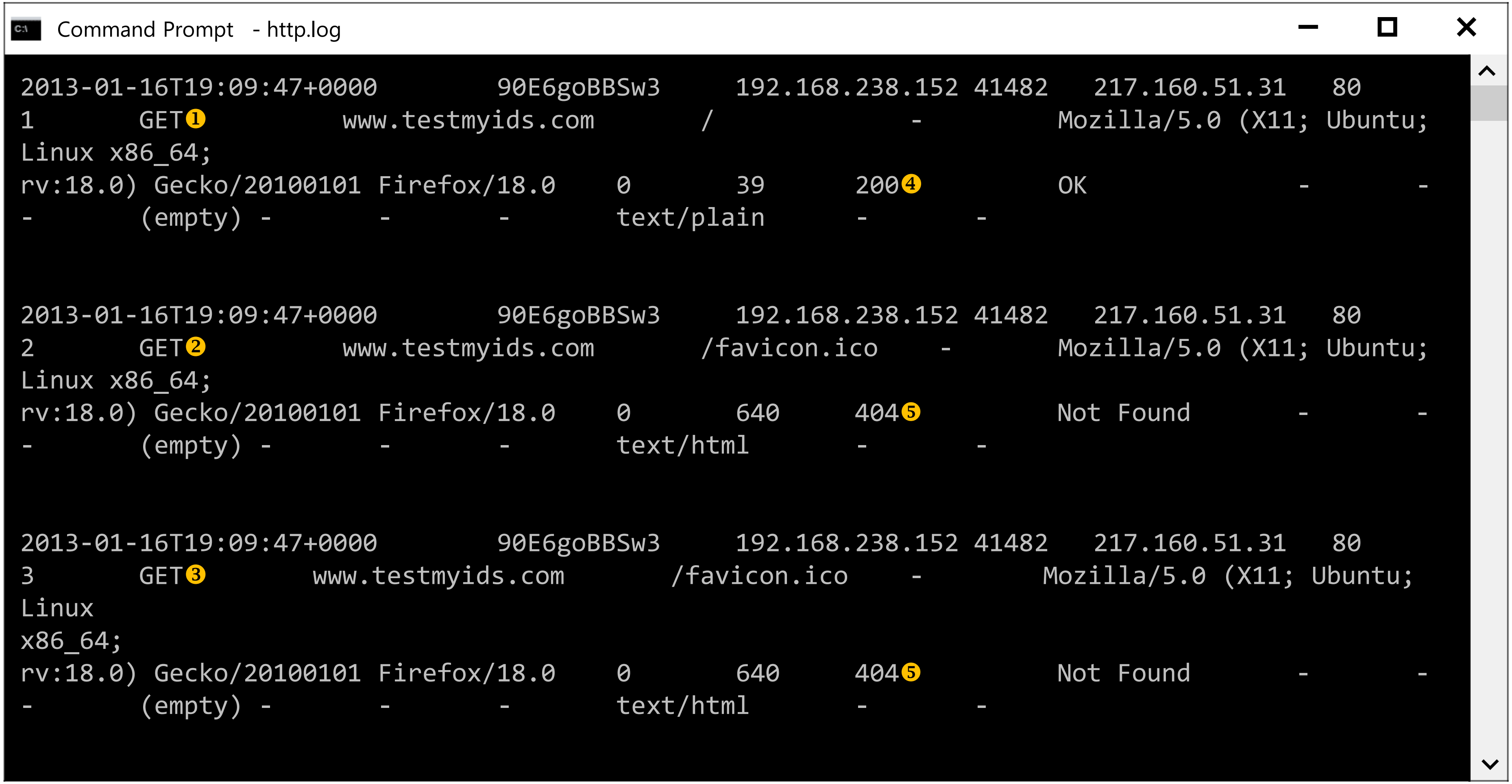


Sensor	Cnx ID	Start Time	End Time	Src IP	SPort	Dst IP	DP...	Pr	S Pckts	S Bytes	D Pckts	D Bytes
sovm-eth1	5.1358363387000000183	2013-01-16 19:09:47	2013-01-16 19:09:50	192.168.238.152	41482	217.160.51.31	80	6	9	1077	9	2141
sovm-eth1	5.1358363387000000182	2013-01-16 19:09:47	2013-01-16 19:09:47	192.168.238.152	52518	192.168.238.2	53	17	1	43	1	59

Transaction Data

- Transaction data focuses on understanding the requests and replies exchanged between two network devices
- The example reviews an *http.log* generated by Bro detailing the request and reply between a web browser and a web server

Transaction Data

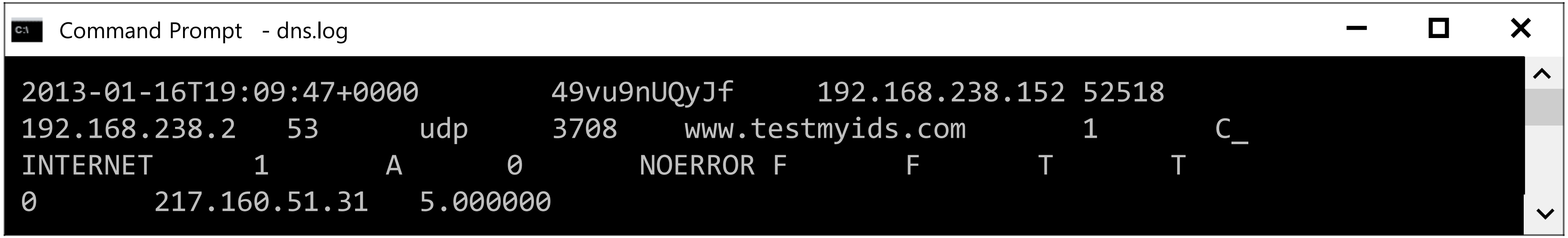


```
2013-01-16T19:09:47+0000        90E6goBBSw3     192.168.238.152 41482   217.160.51.31   80
1       GET❶            www.testmyids.com       /               -               Mozilla/5.0 (X11; Ubuntu;
Linux x86_64;
rv:18.0) Gecko/20100101 Firefox/18.0    0       39      200❹            OK              -       -
-       (empty) -       -       -       text/plain      -       -


2013-01-16T19:09:47+0000        90E6goBBSw3     192.168.238.152 41482   217.160.51.31   80
2       GET❷            www.testmyids.com       /favicon.ico    -       Mozilla/5.0 (X11; Ubuntu;
Linux x86_64;
rv:18.0) Gecko/20100101 Firefox/18.0    0       640     404❺            Not Found       -       -
-       (empty) -       -       -       text/html       -       -


2013-01-16T19:09:47+0000        90E6goBBSw3     192.168.238.152 41482   217.160.51.31   80
3       GET❸          www.testmyids.com       /favicon.ico    -       Mozilla/5.0 (X11; Ubuntu;
Linux
x86_64;
rv:18.0) Gecko/20100101 Firefox/18.0    0       640     404❺            Not Found       -       -
-       (empty) -       -       -       text/html       -       -
```

Transaction Data

- The records show:
  1) The web browser’s GET request for the web root /
  2) One request for a *favicon.ico* file
  3) A second request for a *favicon.ico* file
  4) A 200 OK for the web root GET request
  5) Two 404 Not Found responses for the favicon.ico file
- The output provides enough information to understand the communication between the web browser and the web server, but not as much detail as the full content data
- The following example reviews a DNS request and reply

Transaction Data



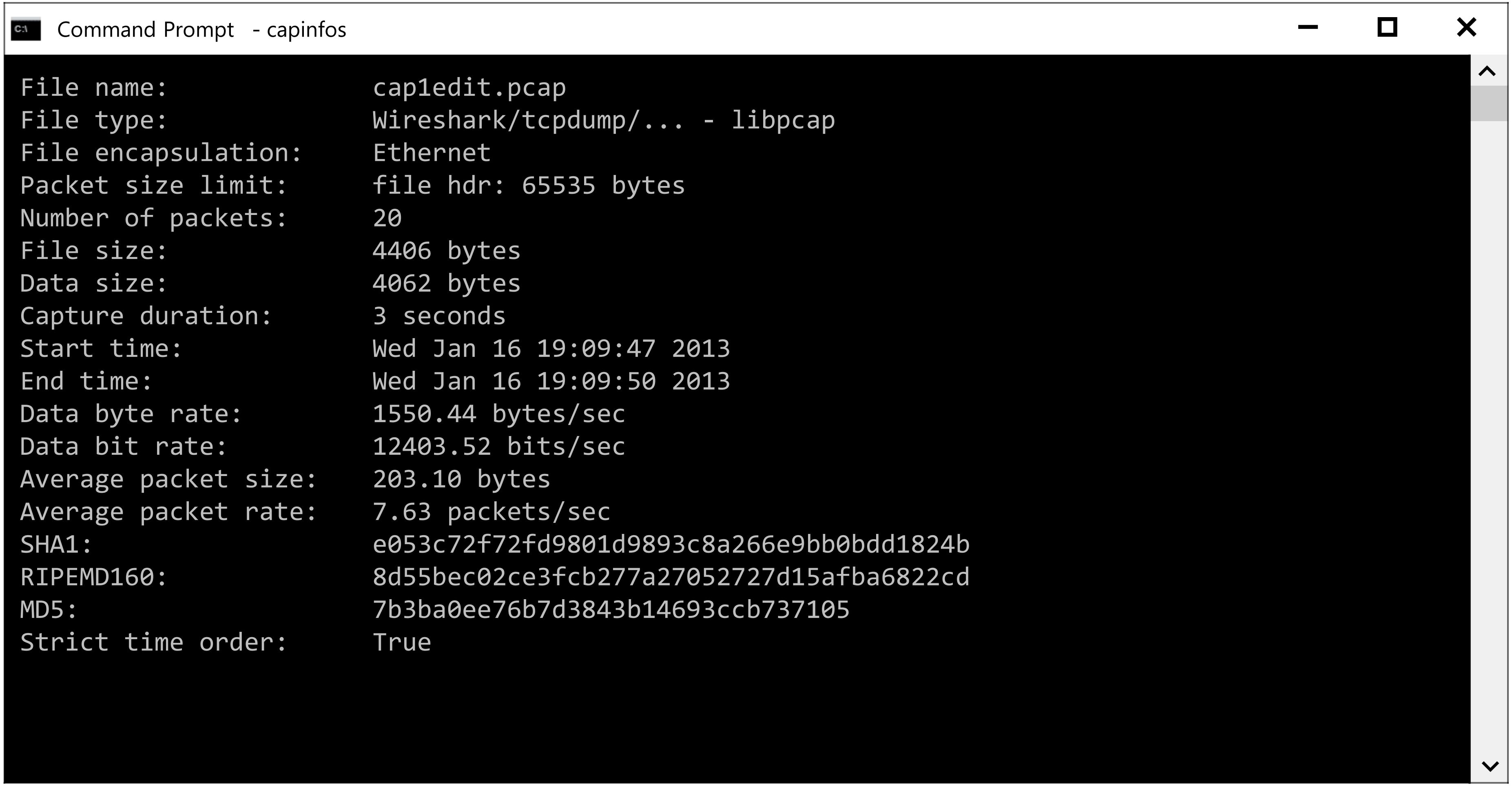
```
2013-01-16T19:09:47+0000        49vu9nUQyJf     192.168.238.152 52518
192.168.238.2   53      udp     3708    www.testmyids.com       1       C_
INTERNET      1       A      0       NOERROR F       F       T       T
0       217.160.51.31   5.000000
```

- Bro and other tools can render transaction data as long as the software understands the protocol being inspected

Statistical Data

- Statistical data describes the traffic resulting from various aspects of an activity
- This could be data related to network log files, or reports derived form analyzing network traffic
- The following example displays the output of the Capinfos tool that is package with Wireshark
- Key aspects of the capture are displayed, such as the number of bytes in the trace (file size), the amount of actual network data (data size), start and end times, etc.

Statistical Data

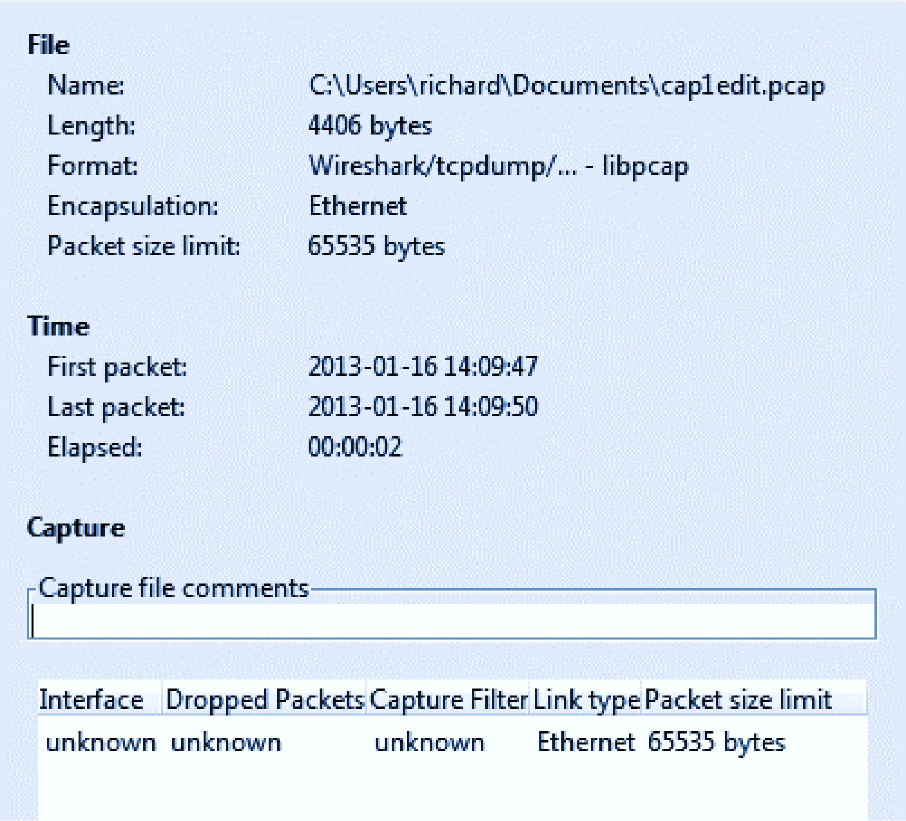


```
File name:              cap1edit.pcap
File type:              Wireshark/tcpdump/... - libpcap
File encapsulation:     Ethernet
Packet size limit:      file hdr: 65535 bytes
Number of packets:      20
File size:              4406 bytes
Data size:              4062 bytes
Capture duration:       3 seconds
Start time:             Wed Jan 16 19:09:47 2013
End time:               Wed Jan 16 19:09:50 2013
Data byte rate:         1550.44 bytes/sec
Data bit rate:          12403.52 bits/sec
Average packet size:    203.10 bytes
Average packet rate:    7.63 packets/sec
SHA1:                   e053c72f72fd9801d9893c8a266e9bb0bdd1824b
RIPEMD160:              8d55bec02ce3fcb277a27052727d15afba6822cd
MD5:                    7b3ba0ee76b7d3843b14693ccb737105
Strict time order:      True
```

Statistical Data

- Wireshark provides several ways to view various forms of statistical data
- The first example is a simple description of the captured traffic
- The information displayed is similar to that of the Capinfos utility, but generated from the GUI
- The second example displays protocol distribution statistics, providing traffic broken down by type
- Analysisists use this information to identify anomalies that could indicate an attack

Statistical Data



File

Name:	C:\Users\richard\Documents\cap1edit.pcap
Length:	4406 bytes
Format:	Wireshark/tcpdump/... - libpcap
Encapsulation:	Ethernet
Packet size limit:	65535 bytes

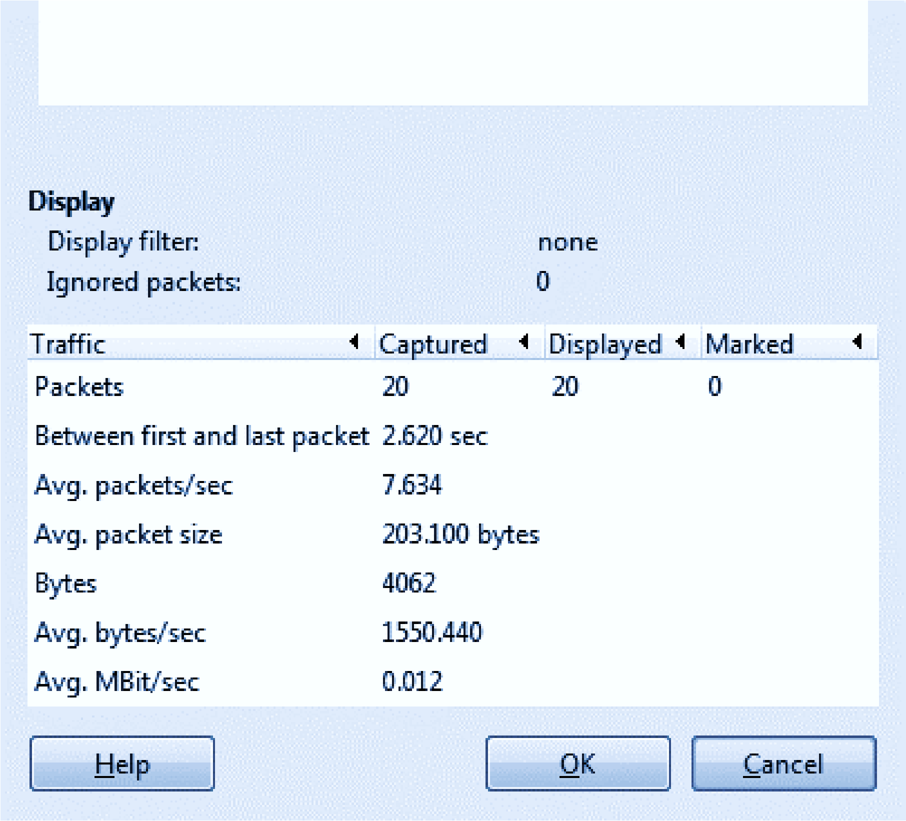
Time

First packet:	2013-01-16 14:09:47
Last packet:	2013-01-16 14:09:50
Elapsed:	00:00:02

Capture

Capture file comments

Interface	Dropped Packets	Capture Filter	Link type	Packet size limit
unknown	unknown	unknown	Ethernet	65535 bytes

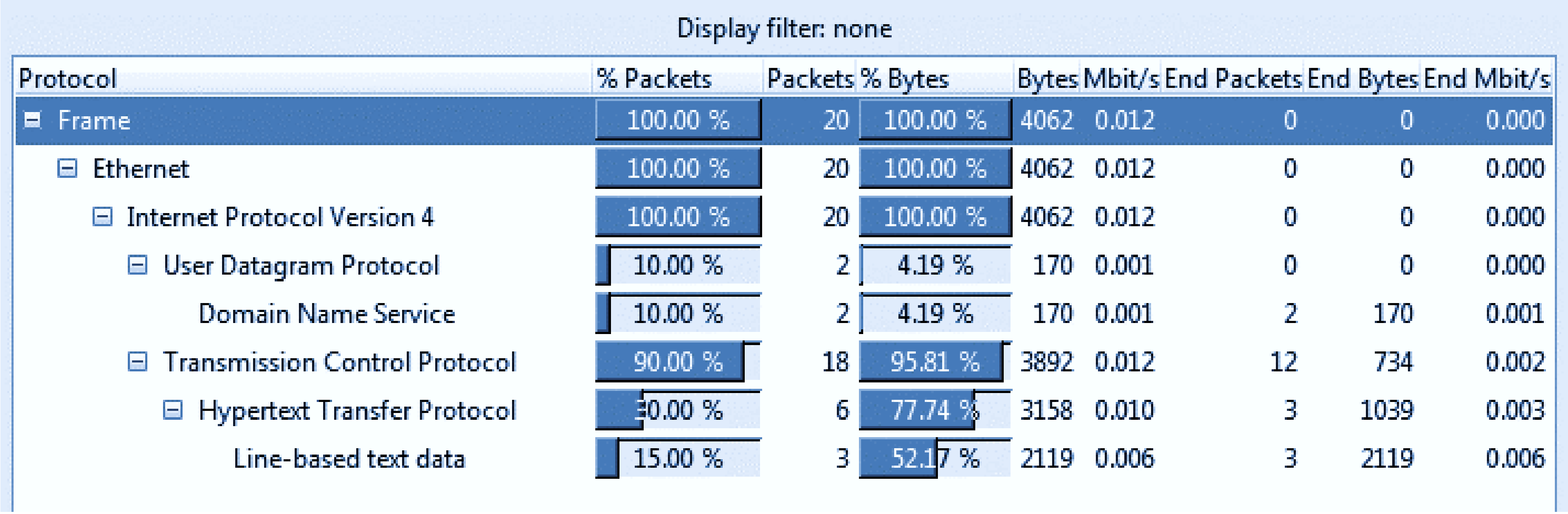


Display

Display filter:	none
Ignored packets:	0

Traffic	Captured	Displayed	Marked
Packets	20	20	0
Between first and last packet	2.620 sec		
Avg. packets/sec	7.634		
Avg. packet size	203.100 bytes		
Bytes	4062		
Avg. bytes/sec	1550.440		
Avg. MBit/sec	0.012		

Statistical Data

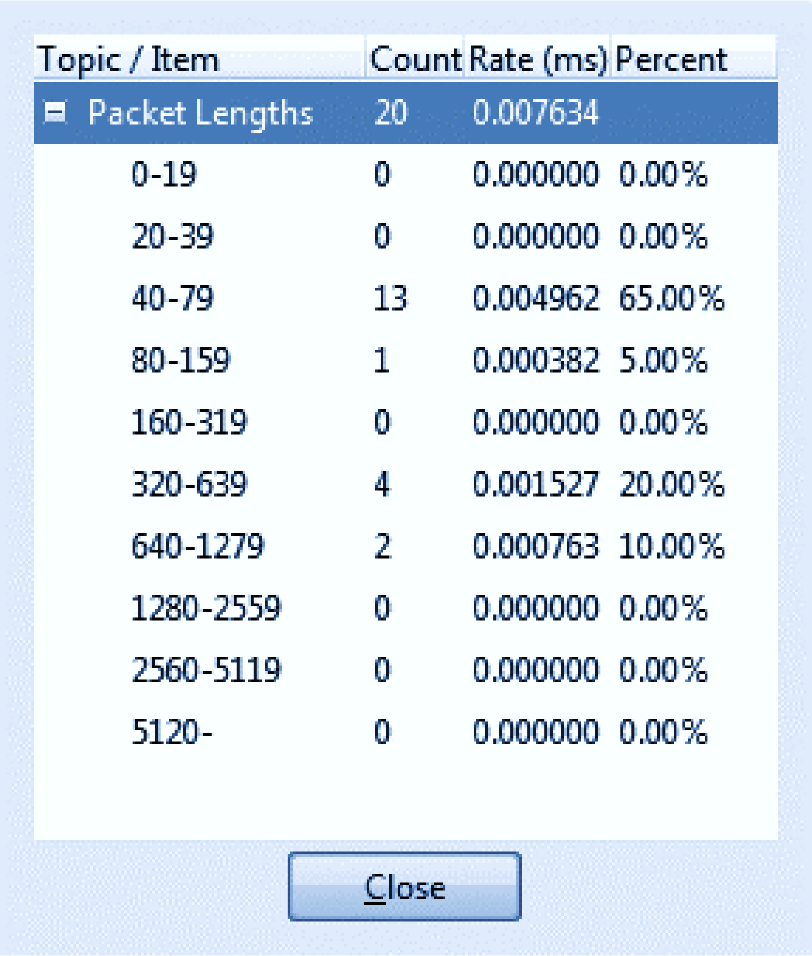


Display filter: none

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
⊟ Frame	100.00 %	20	100.00 %	4062	0.012	0	0	0.000
⊟ Ethernet	100.00 %	20	100.00 %	4062	0.012	0	0	0.000
⊟ Internet Protocol Version 4	100.00 %	20	100.00 %	4062	0.012	0	0	0.000
⊟ User Datagram Protocol	10.00 %	2	4.19 %	170	0.001	0	0	0.000
Domain Name Service	10.00 %	2	4.19 %	170	0.001	2	170	0.001
⊟ Transmission Control Protocol	90.00 %	18	95.81 %	3892	0.012	12	734	0.002
⊟ Hypertext Transfer Protocol	30.00 %	6	77.74 %	3158	0.010	3	1039	0.003
Line-based text data	15.00 %	3	52.17 %	2119	0.006	3	2119	0.006

Statistical Data

- Wireshark can also generate packet length statistics, which are useful to indicate abnormal traffic patterns
- During a distributed denial-of-service attack (DDoS), an attacker could generate millions of packets of a specific length to bombard a target

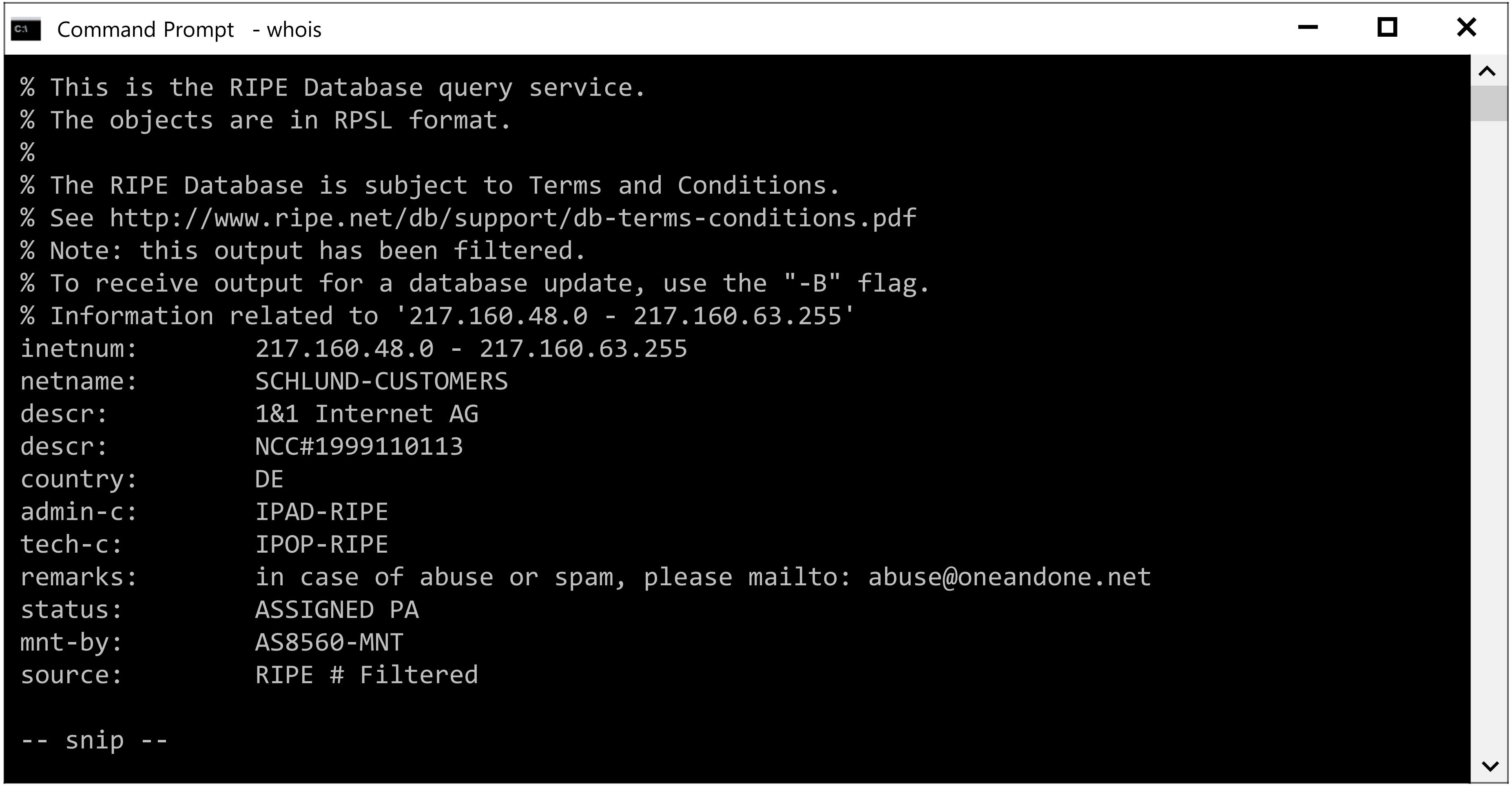


Topic / Item	Count	Rate (ms)	Percent
⊟ Packet Lengths	20	0.007634	
0-19	0	0.000000	0.00%
20-39	0	0.000000	0.00%
40-79	13	0.004962	65.00%
80-159	1	0.000382	5.00%
160-319	0	0.000000	0.00%
320-639	4	0.001527	20.00%
640-1279	2	0.000763	10.00%
1280-2559	0	0.000000	0.00%
2560-5119	0	0.000000	0.00%
5120-	0	0.000000	0.00%

Metadata

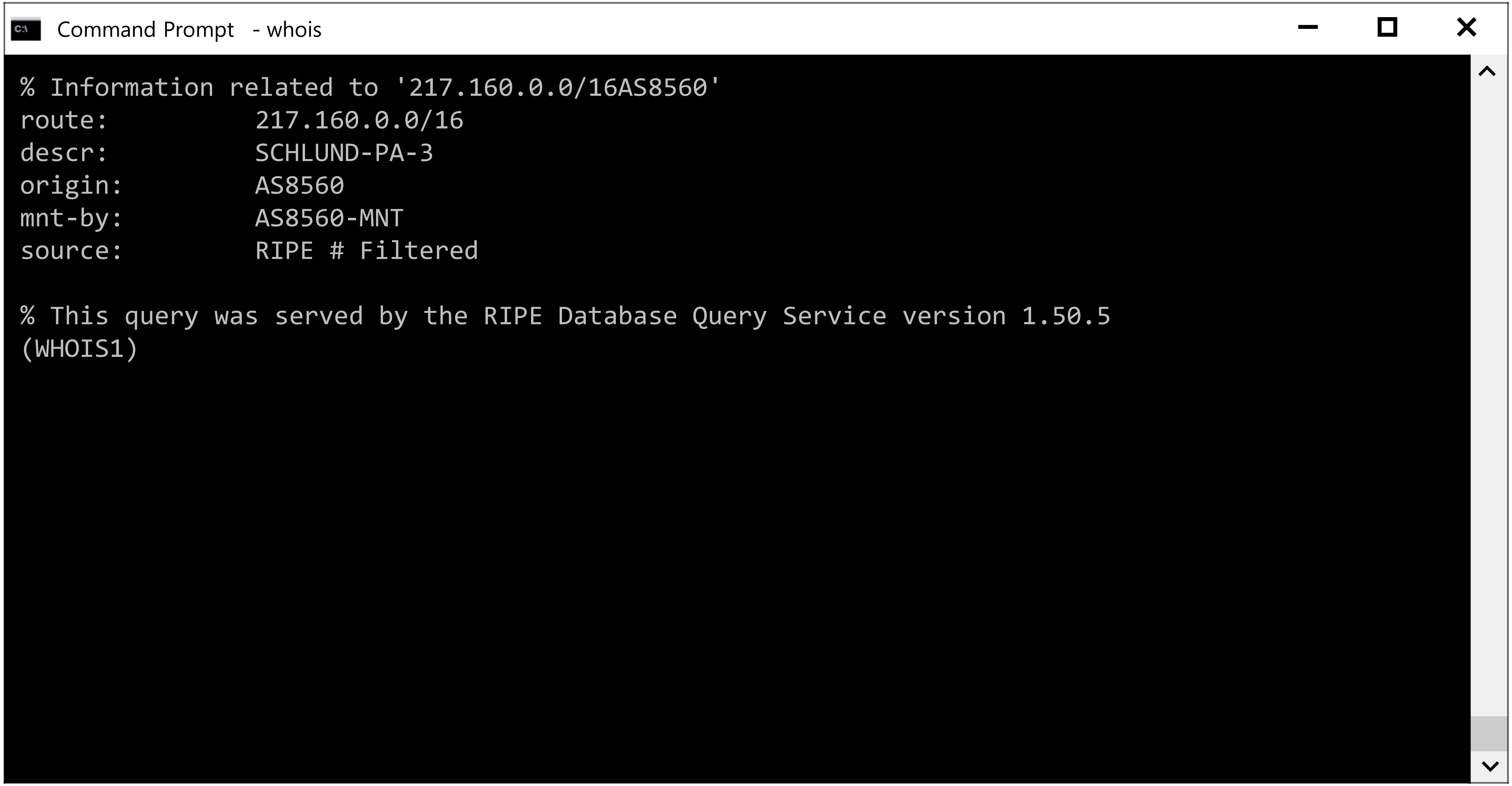
- Metadata is “data about data”
- To generate metadata, we extract key elements from network activity, then leverage an external tool to understand it
- In the examples, we have seen IP addresses recurring throughout, we could question:
  - Who owns these addresses?
  - Where are the hosts located?
  - Does their presence indicate an potential intrusion?
- In the following examples, we inspect an IP address with a WHOIS query, followed by a domain lookup with WHOIS

Metadata



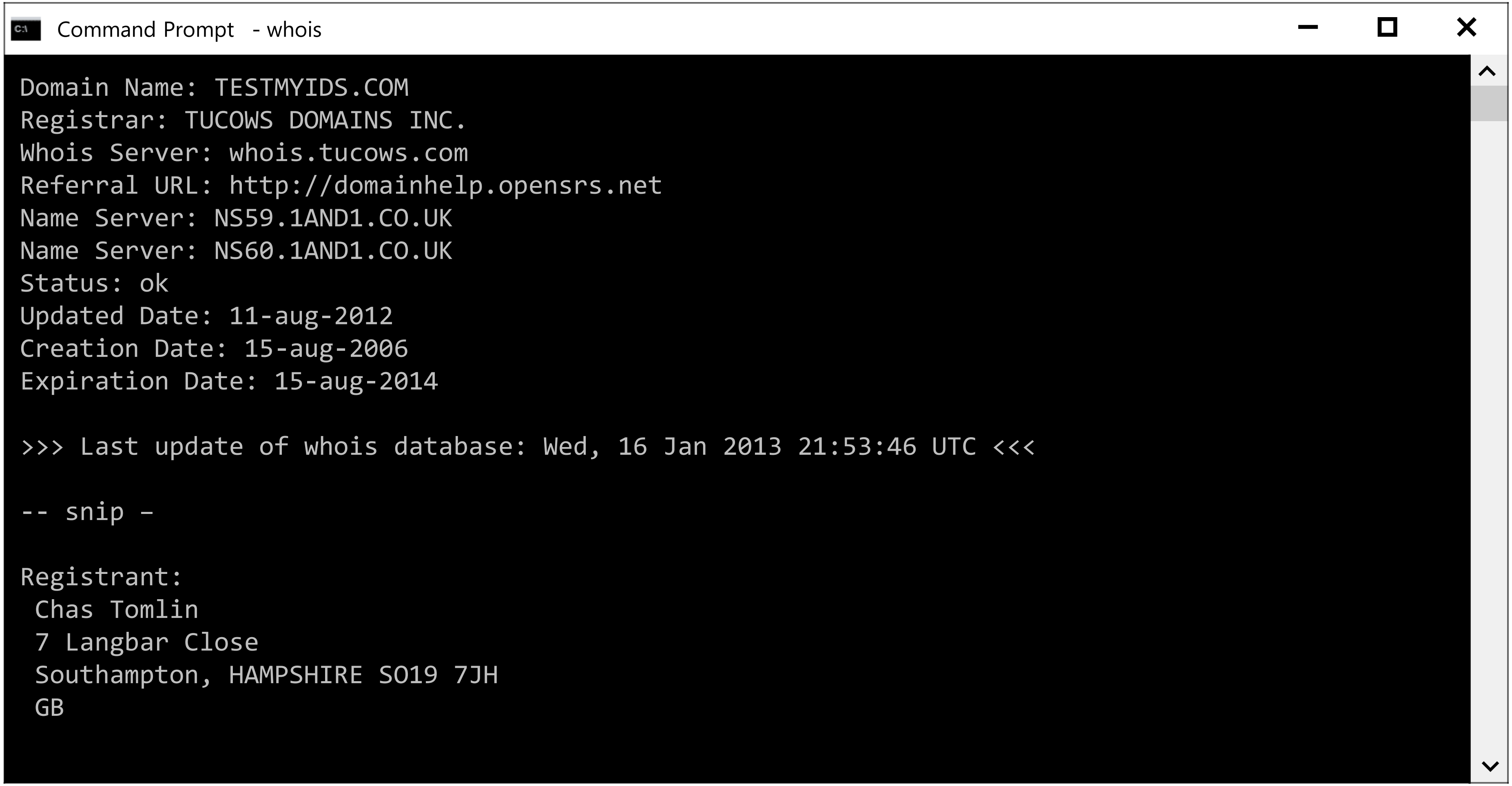
```
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf
% Note: this output has been filtered.
% To receive output for a database update, use the "-B" flag.
% Information related to '217.160.48.0 - 217.160.63.255'
inetnum:        217.160.48.0 - 217.160.63.255
netname:        SCHLUND-CUSTOMERS
descr:          1&1 Internet AG
descr:          NCC#1999110113
country:        DE
admin-c:        IPAD-RIPE
tech-c:         IPOP-RIPE
remarks:        in case of abuse or spam, please mailto: abuse@oneandone.net
status:         ASSIGNED PA
mnt-by:         AS8560-MNT
source:         RIPE # Filtered

-- snip --
```

Metadata



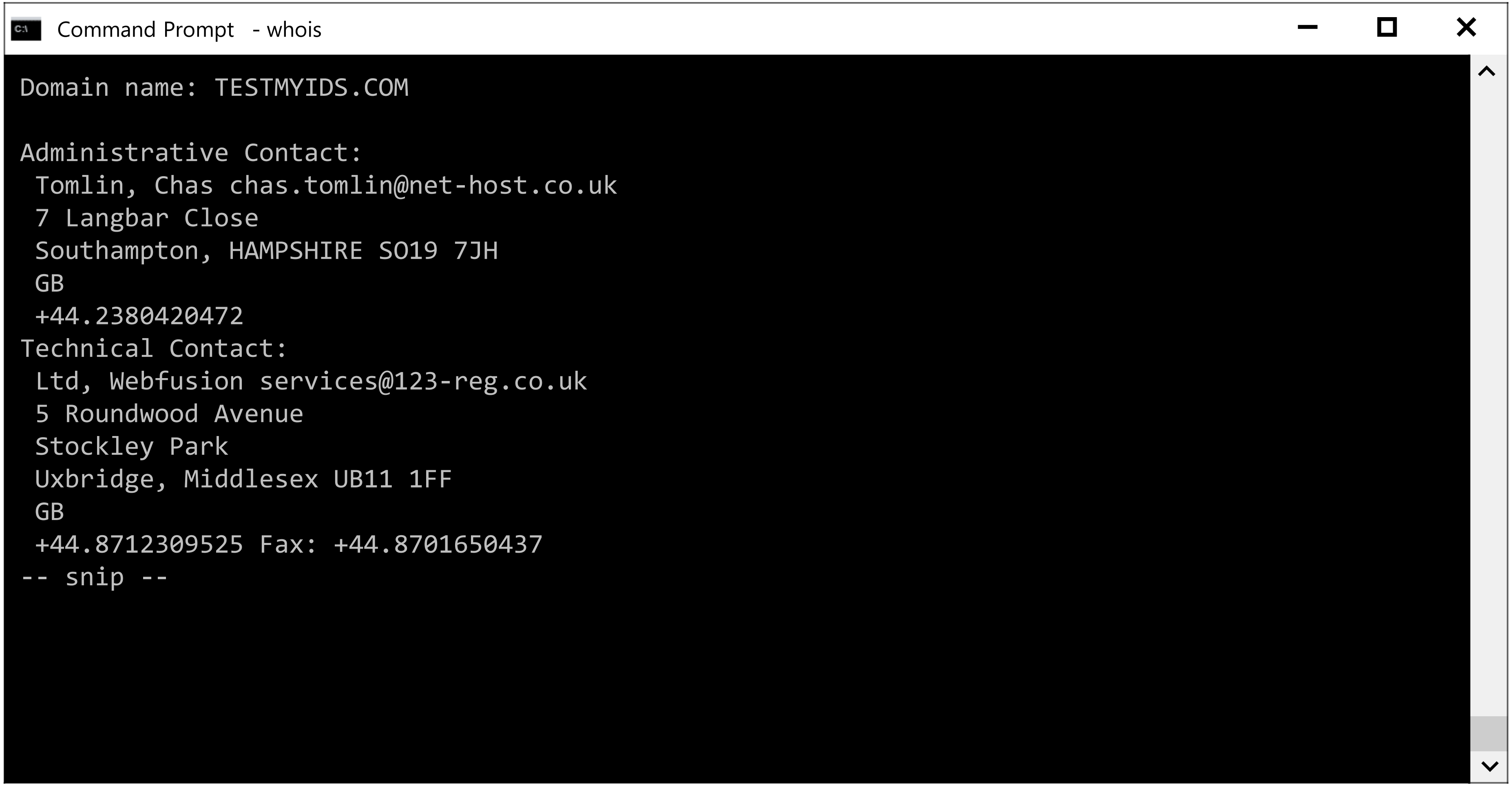
```
% Information related to '217.160.0.0/16AS8560'
route:          217.160.0.0/16
descr:          SCHLUND-PA-3
origin:         AS8560
mnt-by:         AS8560-MNT
source:         RIPE # Filtered

% This query was served by the RIPE Database Query Service version 1.50.5
(WHOIS1)
```

Metadata



```
Domain Name: TESTMYIDS.COM
Registrar: TUCOWS DOMAINS INC.
Whois Server: whois.tucows.com
Referral URL: http://domainhelp.opensrs.net
Name Server: NS59.1AND1.CO.UK
Name Server: NS60.1AND1.CO.UK
Status: ok
Updated Date: 11-aug-2012
Creation Date: 15-aug-2006
Expiration Date: 15-aug-2014

>>> Last update of whois database: Wed, 16 Jan 2013 21:53:46 UTC <<<

-- snip –

Registrant:
 Chas Tomlin
 7 Langbar Close
 Southampton, HAMPSHIRE SO19 7JH
 GB
```

Metadata

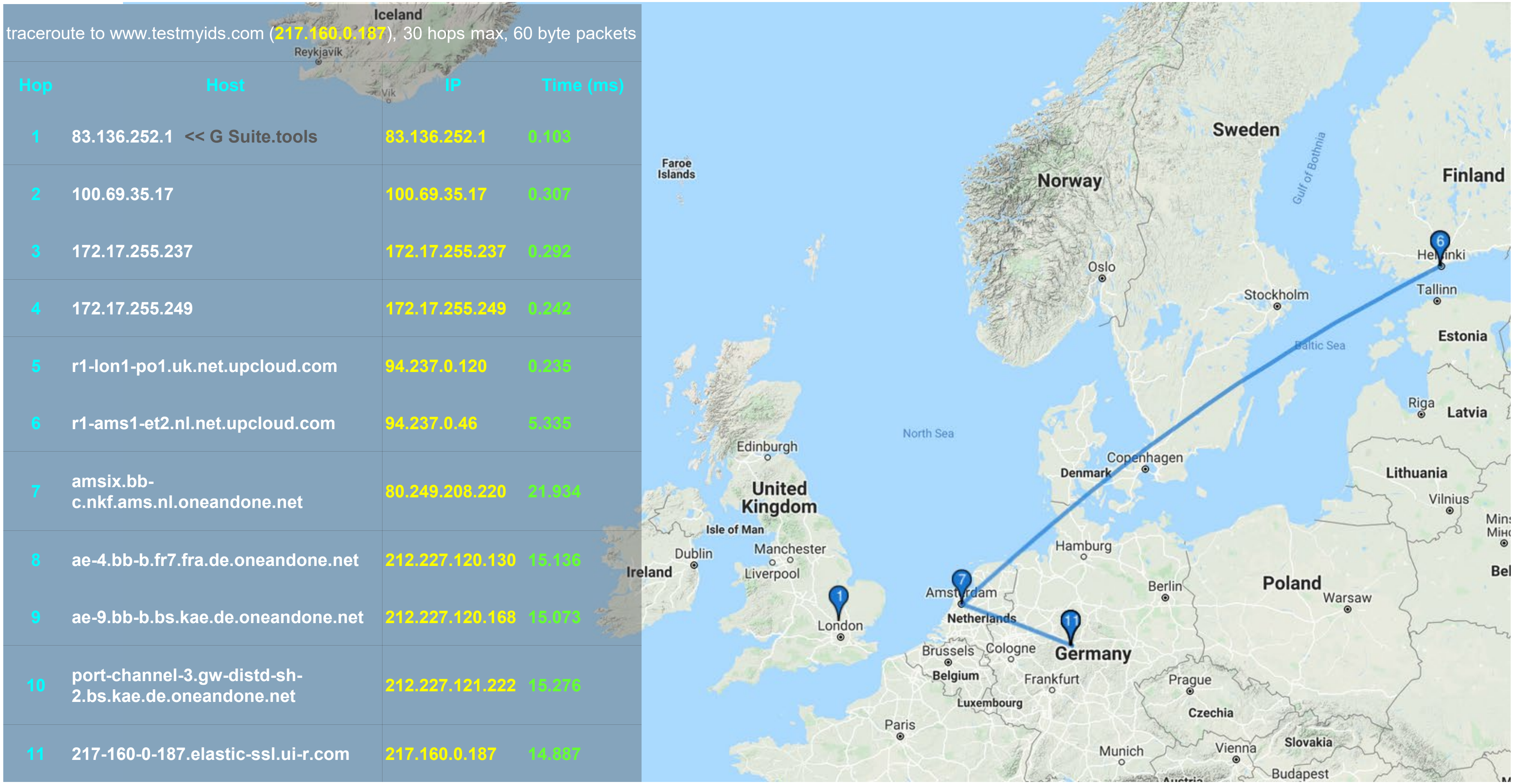


```
Domain name: TESTMYIDS.COM

Administrative Contact:
 Tomlin, Chas chas.tomlin@net-host.co.uk
 7 Langbar Close
 Southampton, HAMPSHIRE SO19 7JH
 GB
 +44.2380420472
Technical Contact:
 Ltd, Webfusion services@123-reg.co.uk
 5 Roundwood Avenue
 Stockley Park
 Uxbridge, Middlesex UB11 1FF
 GB
 +44.8712309525 Fax: +44.8701650437
-- snip --
```

Metadata

- The domain testmyids.com is registered to a user in the England
- We may also analyze the routing information to see how www.testmyids.com connects to the internet
- In the following example, we use G Suite.tools (https://gsuite.tools) to show a route summary of the path from the G Suite.tools server to the testmyids.com server

Metadata



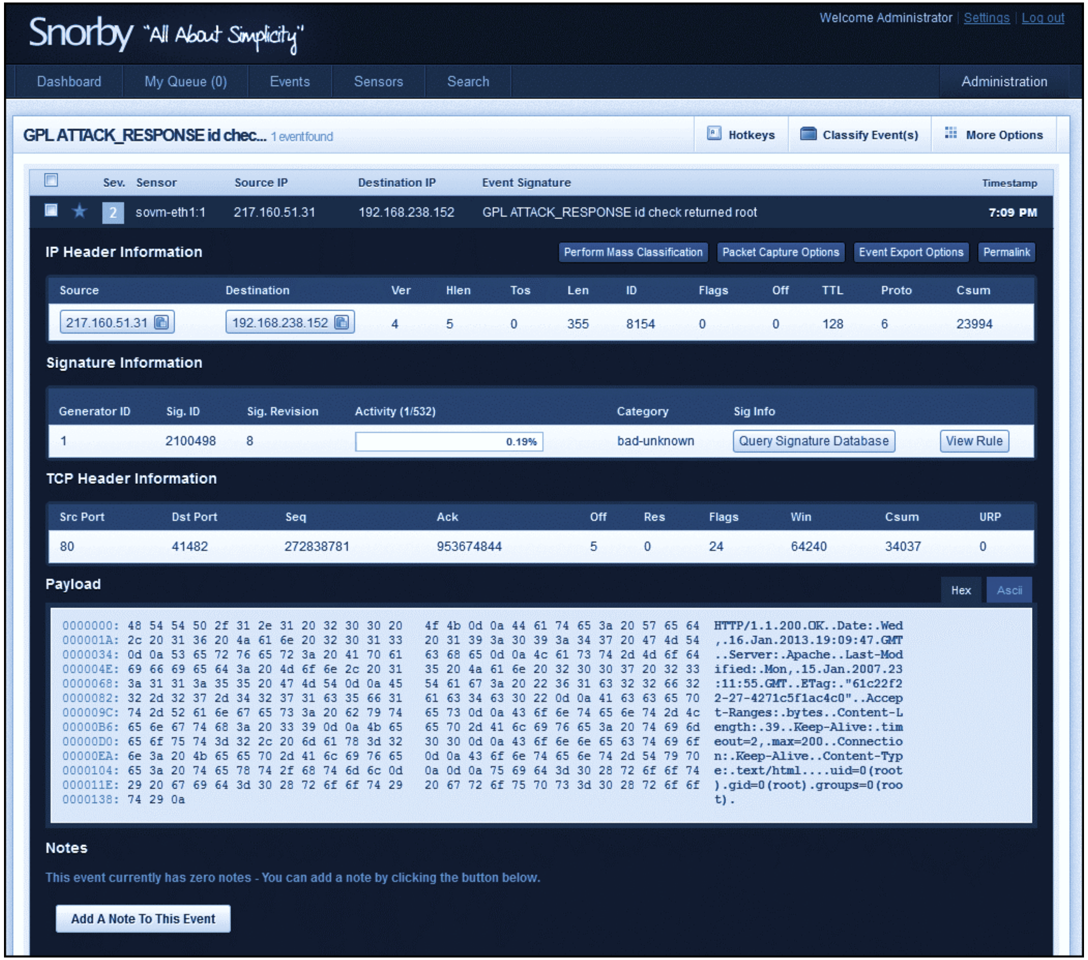
traceroute to www.testmyids.com (217.160.0.187), 30 hops max, 60 byte packets

Hop	Host	IP	Time (ms)
1	83.136.252.1 << G Suite.tools	83.136.252.1	0.103
2	100.69.35.17	100.69.35.17	0.307
3	172.17.255.237	172.17.255.237	0.292
4	172.17.255.249	172.17.255.249	0.242
5	r1-lon1-po1.uk.net.upcloud.com	94.237.0.120	0.235
6	r1-ams1-et2.nl.net.upcloud.com	94.237.0.46	5.335
7	amsix.bb-c.nkf.ams.nl.oneandone.net	80.249.208.220	21.934
8	ae-4.bb-b.fr7.fra.de.oneandone.net	212.227.120.130	15.136
9	ae-9.bb-b.bs.kae.de.oneandone.net	212.227.120.168	15.073
10	port-channel-3.gw-distd-sh-2.bs.kae.de.oneandone.net	212.227.121.222	15.276
11	217-160-0-187.elastic-ssl.ui-r.com	217.160.0.187	14.887

Alert Data

- Alert data reflects whether traffic triggers an alert in an NSM tool
- Intrusion Detection Systems interpret network traffic and create a log when the traffic matches a condition they are programmed to report
- The alerts are based on patterns of bytes, counts of an activity, or other patterns found in the message content
- The following example displays the results of an alert generated by visiting testmyids.com in the Snorby console
  - Snorby is an interface to interpret Snort IDS alerts

Alert Data



GPL ATTACK_RESPONSE id chec... 1 event found

□	Sev.	Sensor	Source IP	Destination IP	Event Signature	Timestamp
□ ★	2	sovm-eth1:1	217.160.51.31	192.168.238.152	GPL ATTACK_RESPONSE id check returned root	7:09 PM

IP Header Information

Source	Destination	Ver	Hlen	Tos	Len	ID	Flags	Off	TTL	Proto	Csum
217.160.51.31	192.168.238.152	4	5	0	355	8154	0	0	128	6	23994

Signature Information

Generator ID	Sig. ID	Sig. Revision	Activity (1/532)	Category	Sig Info	
1	2100498	8	0.19%	bad-unknown	Query Signature Database	View Rule

TCP Header Information

Src Port	Dst Port	Seq	Ack	Off	Res	Flags	Win	Csum	URP
80	41482	272838781	953674844	5	0	24	64240	34037	0

Payload

```
0000000: 48 54 54 50 2f 31 2e 31 20 32 30 30 20   4f 4b 0d 0a 44 61 74 65 3a 20 57 65 64  HTTP/1.1.200.OK..Date:.Wed
000001A: 2c 20 31 36 20 4a 61 6e 20 32 30 31 33   20 31 39 3a 30 39 3a 34 37 20 47 4d 54  ,.16.Jan.2013.19:09:47.GMT
0000034: 0d 0a 53 65 72 76 65 72 3a 20 41 70 61   63 68 65 0d 0a 4c 61 73 74 2d 4d 6f 64  ..Server:.Apache..Last-Mod
000004E: 69 66 69 65 64 3a 20 4d 6f 6e 2c 20 31   35 20 4a 61 6e 20 32 30 30 37 20 32 33  ified:.Mon,.15.Jan.2007.23
0000068: 3a 31 31 3a 35 35 20 47 4d 54 0d 0a 45   54 61 67 3a 20 22 36 31 63 32 32 66 32  :11:55.GMT..ETag:."61c22f2
0000082: 32 2d 32 37 2d 34 32 37 31 63 35 66 31   61 63 34 63 30 22 0d 0a 41 63 63 65 70  2-27-4271c5f1ac4c0"..Accep
000009C: 74 2d 52 61 6e 67 65 73 3a 20 62 79 74   65 73 0d 0a 43 6f 6e 74 65 6e 74 2d 4c  t-Ranges:.bytes..Content-L
00000B6: 65 6e 67 74 68 3a 20 33 39 0d 0a 4b 65   65 70 2d 41 6c 69 76 65 3a 20 74 69 6d  ength:.39..Keep-Alive:.tim
00000D0: 65 6f 75 74 3d 32 2c 20 6d 61 78 3d 32   30 30 0d 0a 43 6f 6e 6e 65 63 74 69 6f  eout=2,.max=200..Connectio
00000EA: 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65   0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70  n:.Keep-Alive..Content-Typ
0000104: 65 3a 20 74 65 78 74 2f 68 74 6d 6c 0d   0a 0d 0a 75 69 64 3d 30 28 72 6f 6f 74  e:.text/html....uid=0(root
000011E: 29 20 67 69 64 3d 30 28 72 6f 6f 74 29   20 67 72 6f 75 70 73 3d 30 28 72 6f 6f  ).gid=0(root).groups=0(roo
0000138: 74 29 0a                                                                          t).
```

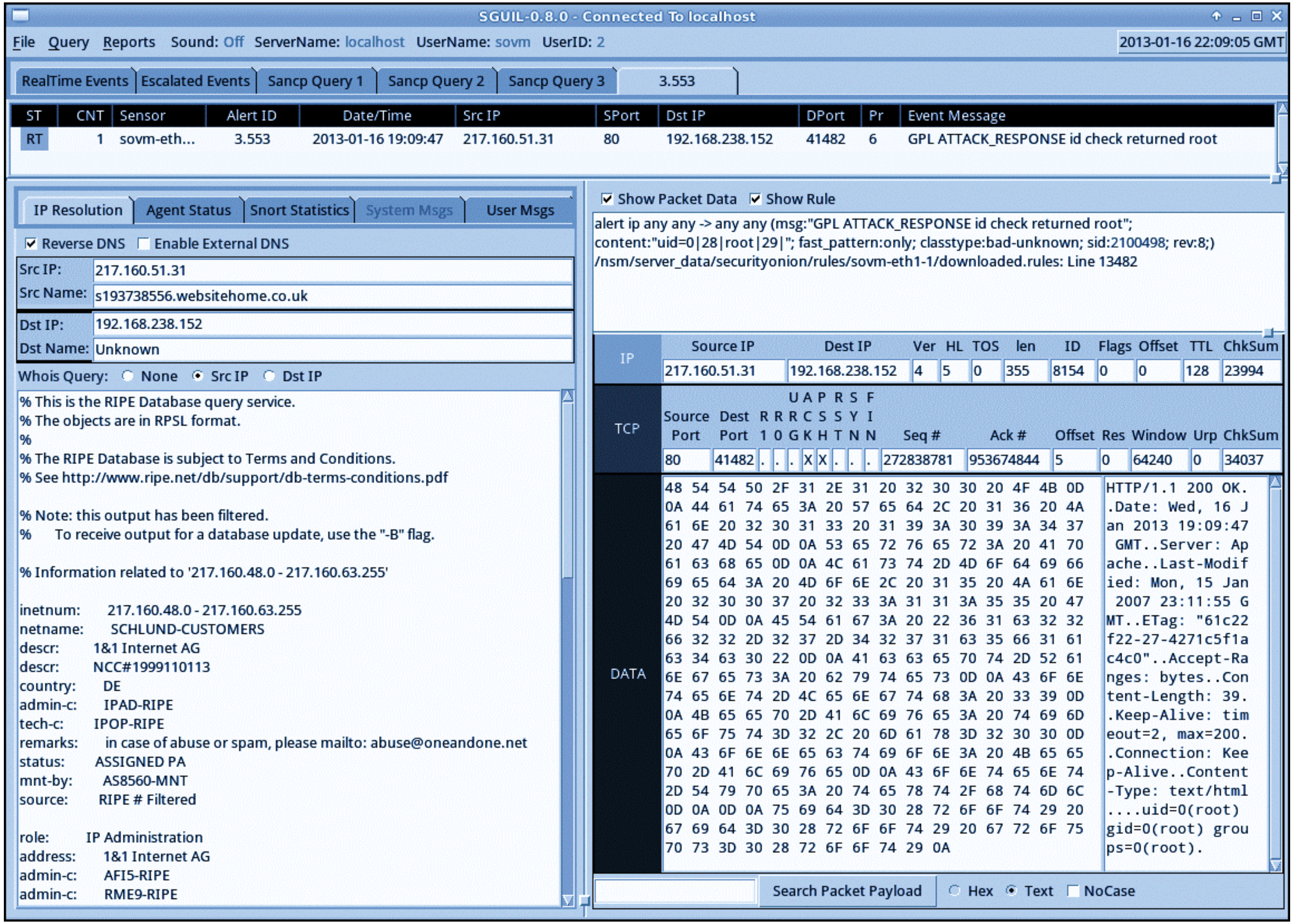
Notes

This event currently has zero notes - You can add a note by clicking the button below.

Alert Data

- In the console, you can see information such as IP addresses related to the connection that triggered the alert
- Snorby allows analysts to search for related data and make incident classifications and management decisions based on alerts
- In the following example, the Sguil console displays much of the same information as Snorby, but Sguil is a “thick client”
- It is up to the analyst to determine if the **GPL ATTACK_RESPONSE id check returned root** alert is suspicious or malicious and begin an investigation

Alert Data



Sound: Off ServerName: localhost UserName: sovm UserID: 2 2013-01-16 22:09:05 GMT

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	sovm-eth...	3.553	2013-01-16 19:09:47	217.160.51.31	80	192.168.238.152	41482	6	GPL ATTACK_RESPONSE id check returned root

☑ Reverse DNS ☐ Enable External DNS

Src IP: 217.160.51.31
Src Name: s193738556.websitehome.co.uk

Dst IP: 192.168.238.152
Dst Name: Unknown

Whois Query: ○ None ● Src IP ○ Dst IP

```
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.
%     To receive output for a database update, use the "-B" flag.

% Information related to '217.160.48.0 - 217.160.63.255'

inetnum:      217.160.48.0 - 217.160.63.255
netname:      SCHLUND-CUSTOMERS
descr:        1&1 Internet AG
descr:        NCC#1999110113
country:      DE
admin-c:      IPAD-RIPE
tech-c:       IPOP-RIPE
remarks:      in case of abuse or spam, please mailto: abuse@oneandone.net
status:       ASSIGNED PA
mnt-by:       AS8560-MNT
source:       RIPE # Filtered

role:         IP Administration
address:      1&1 Internet AG
admin-c:      AFI5-RIPE
admin-c:      RME9-RIPE
```

☑ Show Packet Data ☑ Show Rule

```
alert ip any any -> any any (msg:"GPL ATTACK_RESPONSE id check returned root"; content:"uid=0|28|root|29|"; fast_pattern:only; classtype:bad-unknown; sid:2100498; rev:8;)
/nsm/server_data/securityonion/rules/sovm-eth1-1/downloaded.rules: Line 13482
```

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
	217.160.51.31	192.168.238.152	4	5	0	355	8154	0	0	128	23994

TCP					U	A	P	R	S	F							
	Source	Dest	R	R	R	C	S	S	Y	I							
	Port	Port	1	0	G	K	H	T	N	N	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum
	80	41482	.	.	.	X	X	.	.	.	272838781	953674844	5	0	64240	0	34037

DATA

```
48 54 54 50 2F 31 2E 31 20 32 30 30 20 4F 4B 0D   HTTP/1.1 200 OK.
0A 44 61 74 65 3A 20 57 65 64 2C 20 31 36 20 4A   .Date: Wed, 16 J
61 6E 20 32 30 31 33 20 31 39 3A 30 39 3A 34 37   an 2013 19:09:47
20 47 4D 54 0D 0A 53 65 72 76 65 72 3A 20 41 70    GMT..Server: Ap
61 63 68 65 0D 0A 4C 61 73 74 2D 4D 6F 64 69 66   ache..Last-Modif
69 65 64 3A 20 4D 6F 6E 2C 20 31 35 20 4A 61 6E   ied: Mon, 15 Jan
20 32 30 30 37 20 32 33 3A 31 31 3A 35 35 20 47    2007 23:11:55 G
4D 54 0D 0A 45 54 61 67 3A 20 22 36 31 63 32 32   MT..ETag: "61c22
66 32 32 2D 32 37 2D 34 32 37 31 63 35 66 31 61   f22-27-4271c5f1a
63 34 63 30 22 0D 0A 41 63 63 65 70 74 2D 52 61   c4c0"..Accept-Ra
6E 67 65 73 3A 20 62 79 74 65 73 0D 0A 43 6F 6E   nges: bytes..Con
74 65 6E 74 2D 4C 65 6E 67 74 68 3A 20 33 39 0D   tent-Length: 39.
0A 4B 65 65 70 2D 41 6C 69 76 65 3A 20 74 69 6D   .Keep-Alive: tim
65 6F 75 74 3D 32 2C 20 6D 61 78 3D 32 30 30 0D   eout=2, max=200.
0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 4B 65 65   .Connection: Kee
70 2D 41 6C 69 76 65 0D 0A 43 6F 6E 74 65 6E 74   p-Alive..Content
2D 54 79 70 65 3A 20 74 65 78 74 2F 68 74 6D 6C   -Type: text/html
0D 0A 0D 0A 75 69 64 3D 30 28 72 6F 6F 74 29 20   ....uid=0(root)
67 69 64 3D 30 28 72 6F 6F 74 29 20 67 72 6F 75   gid=0(root) grou
70 73 3D 30 28 72 6F 6F 74 29 0A                  ps=0(root).
```

○ Hex ● Text ☐ NoCase

What’s the Point of All This Data?

- The variety and diversity of NSM data allows CIRTs to identify possible network intrusions and respond accordingly
- NSM data allows for retrospective security analysis (RSA), to apply the newly discovered threat intelligence to previously discovered data in hope of finding intruders who previously evaded detection
- After an attack, the data also for postmortem analysis, which is an examination following incident resolution
  - The purpose of the analysis is often focused on how a future incursion can be avoided

What’s the Point of All This Data?

- Network-centric data should be used to collect, analyze, and escalate as much evidence as your technical, legal, and political constraints allow
- Successful NSM operations collect multiple forms of data, and use that data for both matching activities (IDS) and hunting activities (human review)
- Sophisticated intruders are more likely to evade IDS, so hunting activities are a crucial component of NSM

NSM Drawbacks

- NSM encounters difficulty when faced with one or more of the following situations
  - Encrypted network traffic
  - Network architecture that obscures end-to-end connections with technologies such as network address translation (NAT)
  - Highly-mobile platforms that never use a network segment that is monitored
  - Extreme traffic volumes that could overwhelm the network sensor
  - Privacy concerns that limit access to the traffic required to make NSM effective

Summary

- Network Security Monitoring (NSM) is a practice of collection, analysis and escalation of indicators of compromise with the goal of detecting the actions taken by the intruders, and responding to the compromise
- A Computer Incident Response Team is one or more individuals whose duties include detecting and responding to threats
- NSM is not intended to prevent intrusions, but to detect intrusions that have evaded classic prevention methods

Summary

- Network operators must achieve perfect defense in order to keep out intruders; however, when an intrusion occurs with the right tools, data and skills, the CIRT can detect an intrusion and disrupt the intruder before they achieve their goals
- NSM sensors must be placed on the network in a location that has visibility of the traffic that matters
- Regional laws may limit the amount and type of data that can be collected with NSM, additionally, user privacy should be protected during NSM operations

Summary

- NSM data may include the full content, extracted content, session data, transaction data, statistical data, metadata, and alert data
- NSM encounters difficulty when faced with situations that limit network visibility, such as when traffic is encrypted, or when end-to-end connections are interrupted

References

- Bejtlich, R. (2013). Chapter 1: Network Security Monitoring Rationale. In *The practice of network security monitoring understanding incident detection and response*. San Francisco: No Starch Press.