Amat Victoria Curam

Deep 6 Security

Acta Non Verba

Network Threat Hunting

Analysis: Part 2 of 3

http://www.deep6cyber.com

Network Threat Hunting

- Visibility
- **Analysis**
- Success

ng the correct type
and the Show Bench"—
rly Retriever Club).
elected to carefully consider
dard of Points as drawn un
mmittee met in March 1933
ation, the standard that ap-
nd approved by a Genera
lub is most fortunate
d Ashburton
DESCRIPTION AND STANDARD OF POINTS

Intro

Michael Meason – Deep 6 Security, LLC

- Areas of Influence
  - Telecommunications Engineering
  - Network Engineering
  - Cyber Security Operations

- Letters
  - BS in CIS, MS in Telecomm., CISSP, CSFI-DCOE, NSTISSI 4011,4015, CNSSI 4012-4016, Certified Cyber Intel Tradecraft Professional

- Others
  - Husband/Father, KG5DQA, Aviation

- Handle
  - SigmetXray

Intro

Trae Norman – Deep 6 Security, LLC

- Areas of Influence
  - Information Technology Administration and Engineering
  - Information Security

- Letters
  - CISSP, CEH, GCIA, GNFA, MCITP, MCSA, MCTS, BS in CIS

- Others
  - Husband/Father, Hobbyist Programmer

- Handle
  - SH

- **KSA**
- Networks
- Operating Systems
- Protocol Examples
- Now What?

Knowledge, Skills, and Abilities

- Skills
- Foundational Knowledge

Skills

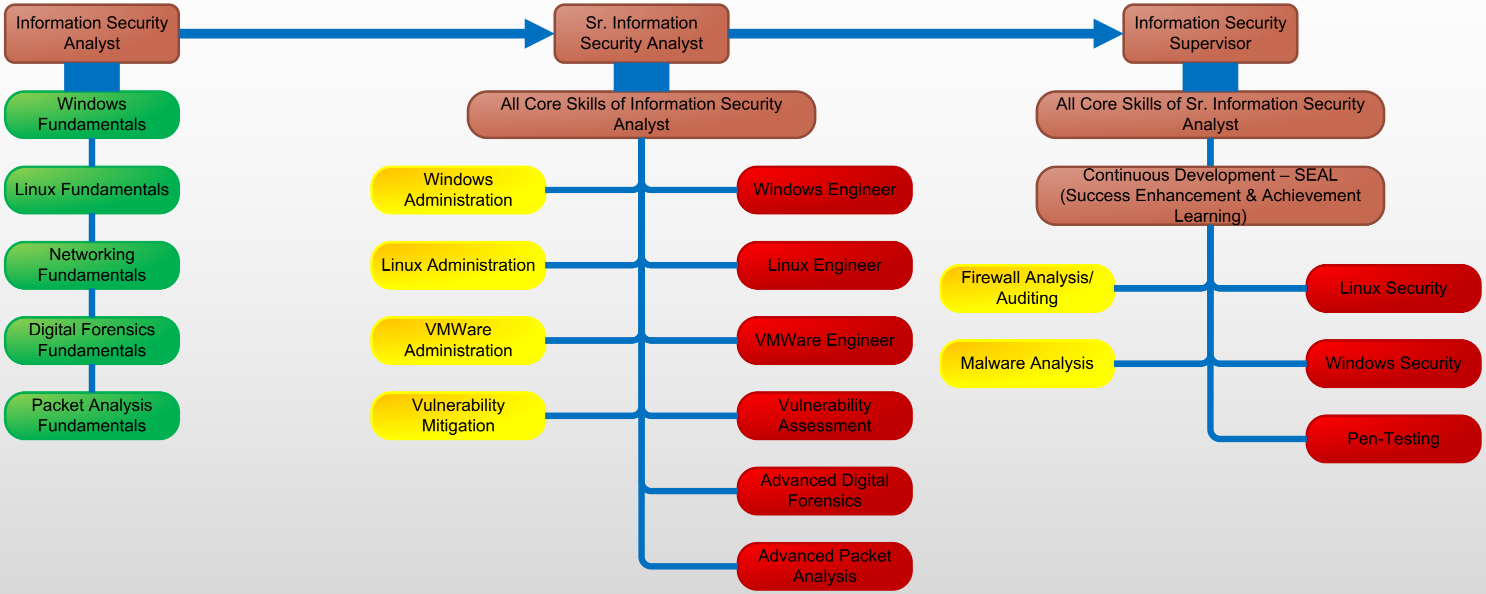
- Telecom
- Digital Forensics
- Networking
- Virtual Administrator
- SAN Administrator
- Domain Administrator
- etc.…

- Cross Training
- OTJ Training
- Professional Training

"The half-life of security knowledge is about 18 months."

Foundational Training

Information Security Training Paths



Information Security Analyst

Windows Fundamentals

Linux Fundamentals

Networking Fundamentals

Digital Forensics Fundamentals

Packet Analysis Fundamentals

Sr. Information Security Analyst

All Core Skills of Information Security Analyst

Windows Administration

Linux Administration

VMWare Administration

Vulnerability Mitigation

Windows Engineer

Linux Engineer

VMWare Engineer

Vulnerability Assessment

Advanced Digital Forensics

Advanced Packet Analysis

Information Security Supervisor

All Core Skills of Sr. Information Security Analyst

Continuous Development – SEAL (Success Enhancement & Achievement Learning)

Firewall Analysis/ Auditing

Malware Analysis

Linux Security

Windows Security

Pen-Testing

- KSA
- **Networks**
- Operating Systems
- Protocol Examples
- Now What?

Types of Networks

Size:

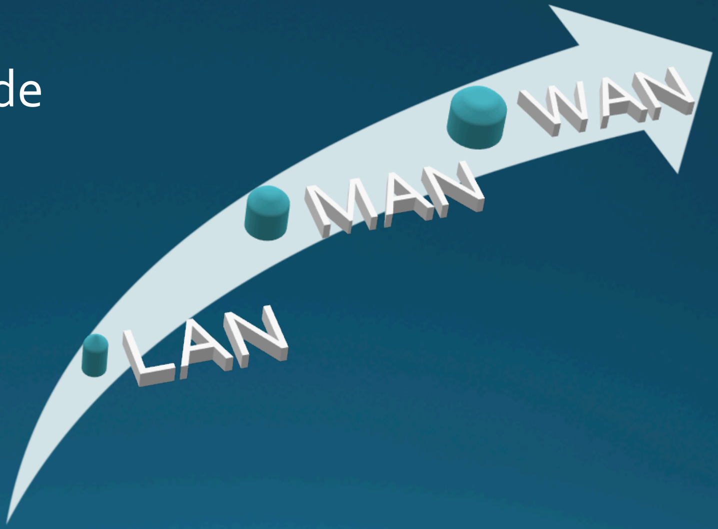
- PAN – Personal Area Network
- LAN – Local Area Network
- MAN – Metropolitan Area Network
- WAN – Wide Area Network

Function:

- SAN – Storage Area Network
- VPN – Virtual Private Network

LAN – Local Area Network
MAN – Metropolitan Area Network
WAN – Wide Area Network

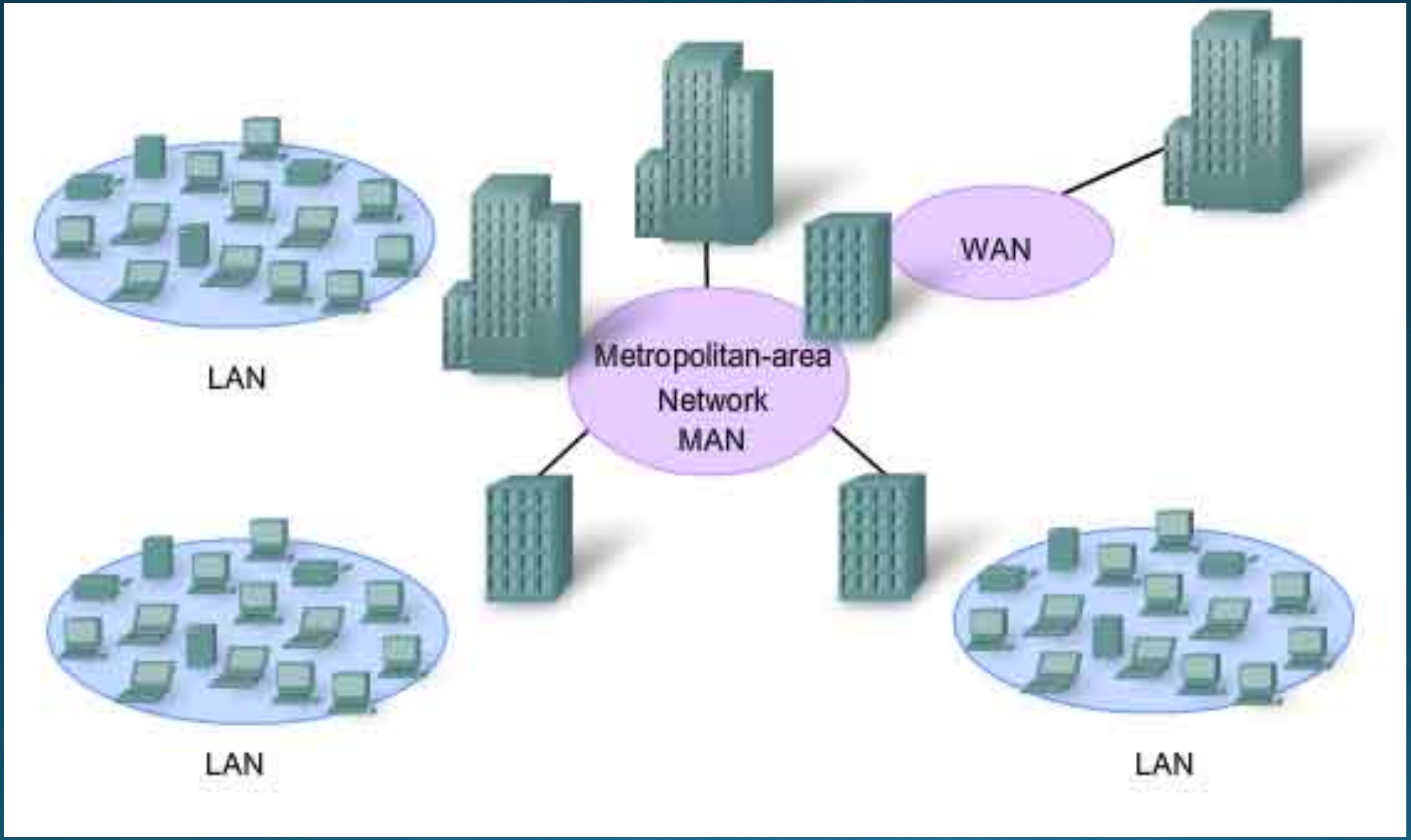
- Area of Effect:
  - LAN – Building/Campus
  - MAN – City wide
  - WAN – Greater than city wide



Protocols:

- Ethernet
- ATM
- FDDI

LAN, MAN, and WAN Continued…



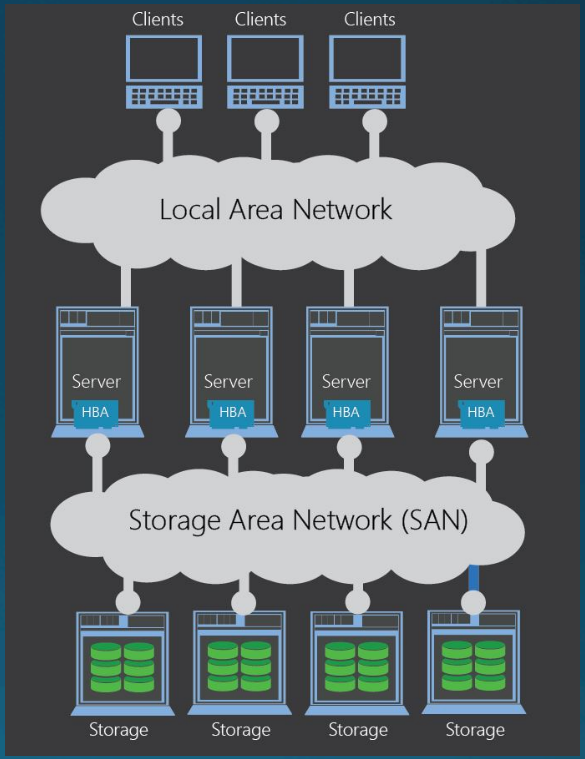
Network Functions

SAN – Storage Area Network

Protocols: iSCSI, FCP

VPN – Virtual Private Network

Encrypted network tunnel across public infrastructure.

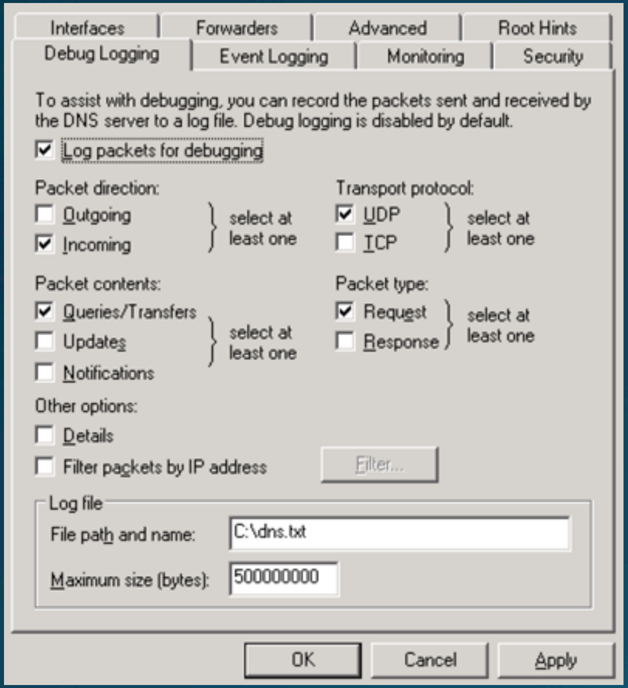


- KSA
- Networks
- **Operating Systems**
- Protocol Examples
- Now What?

Windows

- Some event logs to look for in security:
  - 5152, 5156, 5158
- Review hardware registered and any USB devices for PAN connectivity and Wireless access
- Review network information for dual homes configurations
- DNS analytics, audit events, and logs
- DHCP lease review

DNS Logging



To assist with debugging, you can record the packets sent and received by the DNS server to a log file. Debug logging is disabled by default.

☑ Log packets for debugging

Packet direction:
- ☐ Outgoing
- ☑ Incoming

} select at least one

Transport protocol:
- ☑ UDP
- ☐ TCP

} select at least one

Packet contents:
- ☑ Queries/Transfers
- ☐ Updates
- ☐ Notifications

} select at least one

Packet type:
- ☑ Request
- ☐ Response

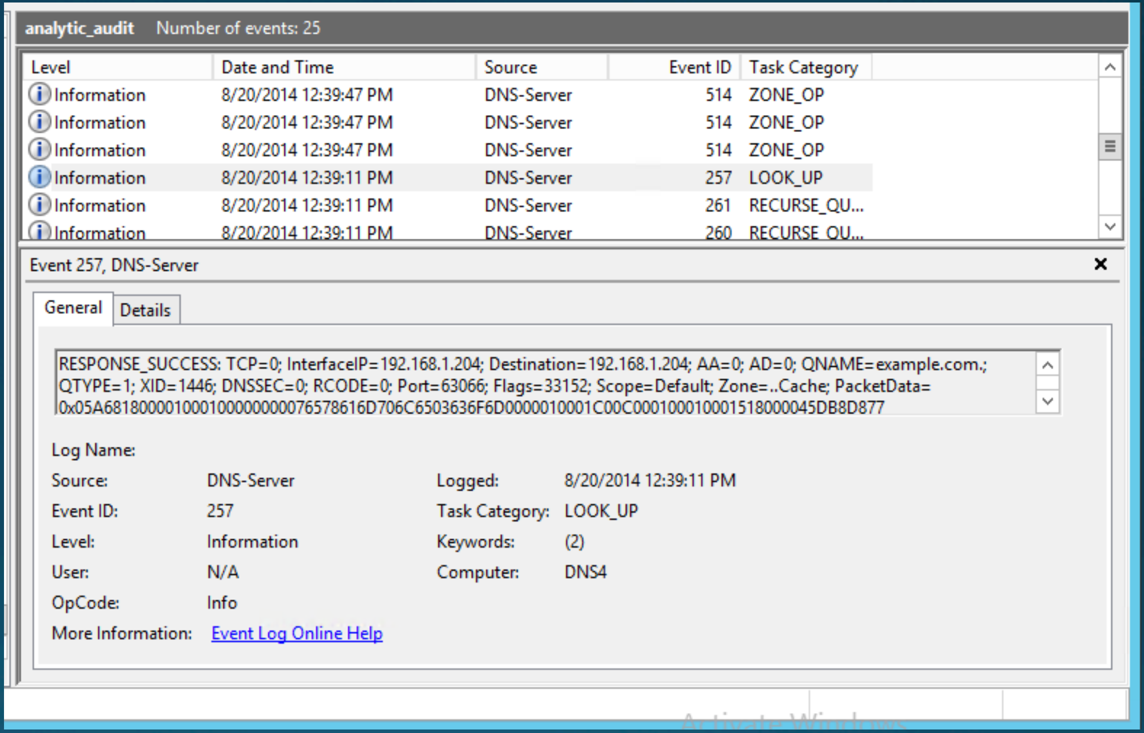
} select at least one

Other options:
- ☐ Details
- ☐ Filter packets by IP address

Log file

File path and name: C:\dns.txt

Maximum size (bytes): 500000000



analytic_audit Number of events: 25

Level	Date and Time	Source	Event ID	Task Category
Information	8/20/2014 12:39:47 PM	DNS-Server	514	ZONE_OP
Information	8/20/2014 12:39:47 PM	DNS-Server	514	ZONE_OP
Information	8/20/2014 12:39:47 PM	DNS-Server	514	ZONE_OP
Information	8/20/2014 12:39:11 PM	DNS-Server	257	LOOK_UP
Information	8/20/2014 12:39:11 PM	DNS-Server	261	RECURSE_QU...
Information	8/20/2014 12:39:11 PM	DNS-Server	260	RECURSE_QU...

Event 257, DNS-Server

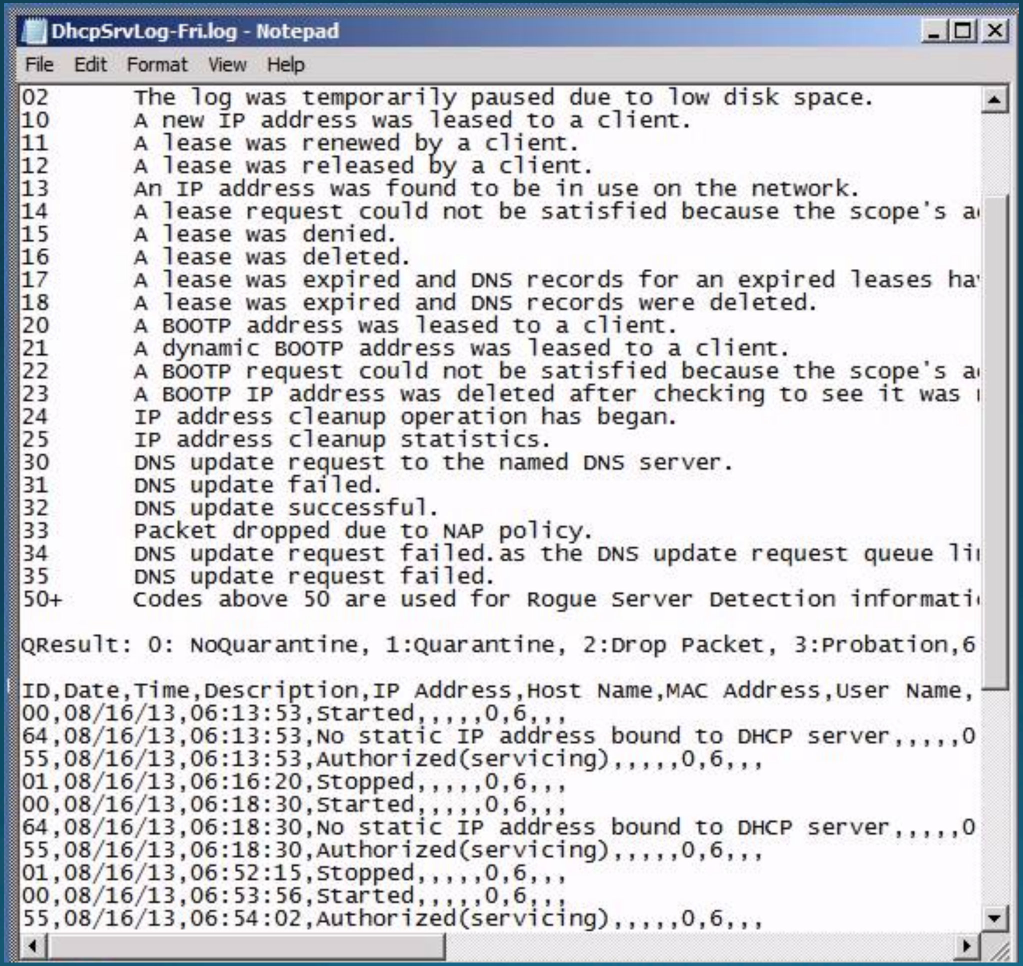
```
RESPONSE_SUCCESS: TCP=0; InterfaceIP=192.168.1.204; Destination=192.168.1.204; AA=0; AD=0; QNAME=example.com.;
QTYPE=1; XID=1446; DNSSEC=0; RCODE=0; Port=63066; Flags=33152; Scope=Default; Zone=..Cache; PacketData=
0x05A681800001000100000000076578616D706C6503636F6D0000010001C00C000100010001518000045DB8D877
```

Log Name:			
Source:	DNS-Server	Logged:	8/20/2014 12:39:11 PM
Event ID:	257	Task Category:	LOOK_UP
Level:	Information	Keywords:	(2)
User:	N/A	Computer:	DNS4
OpCode:	Info		
More Information:	Event Log Online Help		

```
1/7/2016 11:51:29 AM 0428 PACKET  0000003003F7DD00 UDP Snd 172.16.160.97   fb03 R Q [8081   DR  NOERROR] A     (4)time(7)windows(3)com(0)
1/7/2016 11:51:29 AM 0428 PACKET  00000030018B4BA0 UDP Rcv 172.16.160.97   d273   Q [0001   D   NOERROR] A     (5)ctldl(13)windowsupdate(3)com(0)
1/7/2016 11:51:29 AM 0428 PACKET  0000003003F7DD00 UDP Snd 8.8.8.8         0e9e   Q [0001   D   NOERROR] A     (5)ctldl(13)windowsupdate(3)com(0)
```

http://www.deep6cyber.com

DHCP Logging Information

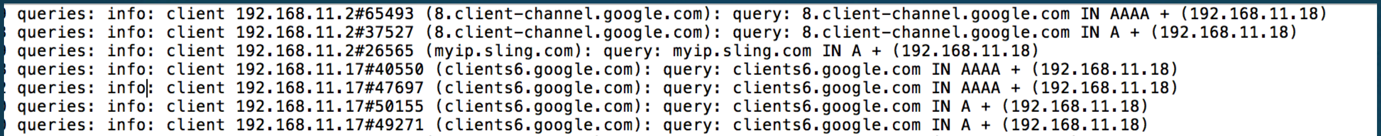


```
02      The log was temporarily paused due to low disk space.
10      A new IP address was leased to a client.
11      A lease was renewed by a client.
12      A lease was released by a client.
13      An IP address was found to be in use on the network.
14      A lease request could not be satisfied because the scope's a
15      A lease was denied.
16      A lease was deleted.
17      A lease was expired and DNS records for an expired leases ha
18      A lease was expired and DNS records were deleted.
20      A BOOTP address was leased to a client.
21      A dynamic BOOTP address was leased to a client.
22      A BOOTP request could not be satisfied because the scope's a
23      A BOOTP IP address was deleted after checking to see it was 
24      IP address cleanup operation has began.
25      IP address cleanup statistics.
30      DNS update request to the named DNS server.
31      DNS update failed.
32      DNS update successful.
33      Packet dropped due to NAP policy.
34      DNS update request failed.as the DNS update request queue li
35      DNS update request failed.
50+     Codes above 50 are used for Rogue Server Detection informati

QResult: 0: NoQuarantine, 1:Quarantine, 2:Drop Packet, 3:Probation,6

ID,Date,Time,Description,IP Address,Host Name,MAC Address,User Name,
00,08/16/13,06:13:53,Started,,,,,0,6,,,
64,08/16/13,06:13:53,No static IP address bound to DHCP server,,,,,0
55,08/16/13,06:13:53,Authorized(servicing),,,,,0,6,,,
01,08/16/13,06:16:20,Stopped,,,,,0,6,,,
00,08/16/13,06:18:30,Started,,,,,0,6,,,
64,08/16/13,06:18:30,No static IP address bound to DHCP server,,,,,0
55,08/16/13,06:18:30,Authorized(servicing),,,,,0,6,,,
01,08/16/13,06:52:15,Stopped,,,,,0,6,,,
00,08/16/13,06:53:56,Started,,,,,0,6,,,
55,08/16/13,06:54:02,Authorized(servicing),,,,,0,6,,,
```

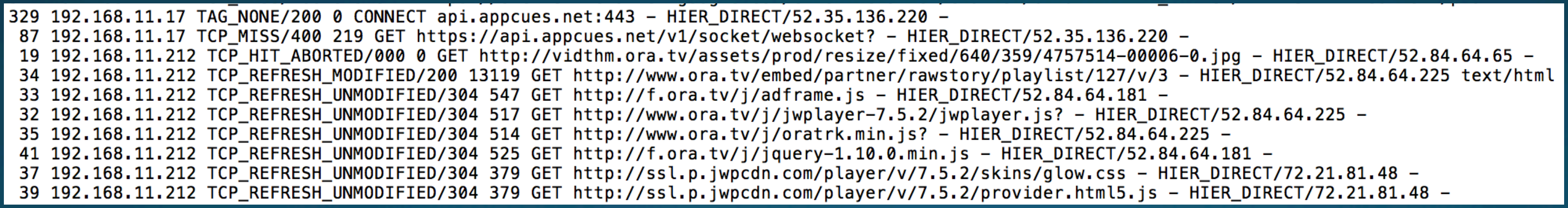
Linux

- Review hardware registered and any USB devices for PAN connectivity and Wireless access
- Review network information for dual homed configurations
- Common log file location - /var/log/
- iptables logs (configurable)
- Bind DNS logs
- Squid Proxy

Linux BIND DNS/Squid Proxy Logging



```
queries: info: client 192.168.11.2#65493 (8.client-channel.google.com): query: 8.client-channel.google.com IN AAAA + (192.168.11.18)
queries: info: client 192.168.11.2#37527 (8.client-channel.google.com): query: 8.client-channel.google.com IN A + (192.168.11.18)
queries: info: client 192.168.11.2#26565 (myip.sling.com): query: myip.sling.com IN A + (192.168.11.18)
queries: info: client 192.168.11.17#40550 (clients6.google.com): query: clients6.google.com IN AAAA + (192.168.11.18)
queries: info: client 192.168.11.17#47697 (clients6.google.com): query: clients6.google.com IN AAAA + (192.168.11.18)
queries: info: client 192.168.11.17#50155 (clients6.google.com): query: clients6.google.com IN A + (192.168.11.18)
queries: info: client 192.168.11.17#49271 (clients6.google.com): query: clients6.google.com IN A + (192.168.11.18)
```



```
329 192.168.11.17 TAG_NONE/200 0 CONNECT api.appcues.net:443 - HIER_DIRECT/52.35.136.220 -
 87 192.168.11.17 TCP_MISS/400 219 GET https://api.appcues.net/v1/socket/websocket? - HIER_DIRECT/52.35.136.220 -
 19 192.168.11.212 TCP_HIT_ABORTED/000 0 GET http://vidthm.ora.tv/assets/prod/resize/fixed/640/359/4757514-00006-0.jpg - HIER_DIRECT/52.84.64.65 -
 34 192.168.11.212 TCP_REFRESH_MODIFIED/200 13119 GET http://www.ora.tv/embed/partner/rawstory/playlist/127/v/3 - HIER_DIRECT/52.84.64.225 text/html
 33 192.168.11.212 TCP_REFRESH_UNMODIFIED/304 547 GET http://f.ora.tv/j/adframe.js - HIER_DIRECT/52.84.64.181 -
 32 192.168.11.212 TCP_REFRESH_UNMODIFIED/304 517 GET http://www.ora.tv/j/jwplayer-7.5.2/jwplayer.js? - HIER_DIRECT/52.84.64.225 -
 35 192.168.11.212 TCP_REFRESH_UNMODIFIED/304 514 GET http://www.ora.tv/j/oratrk.min.js? - HIER_DIRECT/52.84.64.225 -
 41 192.168.11.212 TCP_REFRESH_UNMODIFIED/304 525 GET http://f.ora.tv/j/jquery-1.10.0.min.js - HIER_DIRECT/52.84.64.181 -
 37 192.168.11.212 TCP_REFRESH_UNMODIFIED/304 379 GET http://ssl.p.jwpcdn.com/player/v/7.5.2/skins/glow.css - HIER_DIRECT/72.21.81.48 -
 39 192.168.11.212 TCP_REFRESH_UNMODIFIED/304 379 GET http://ssl.p.jwpcdn.com/player/v/7.5.2/provider.html5.js - HIER_DIRECT/72.21.81.48 -
```

Parsing Tools Examples

Windows

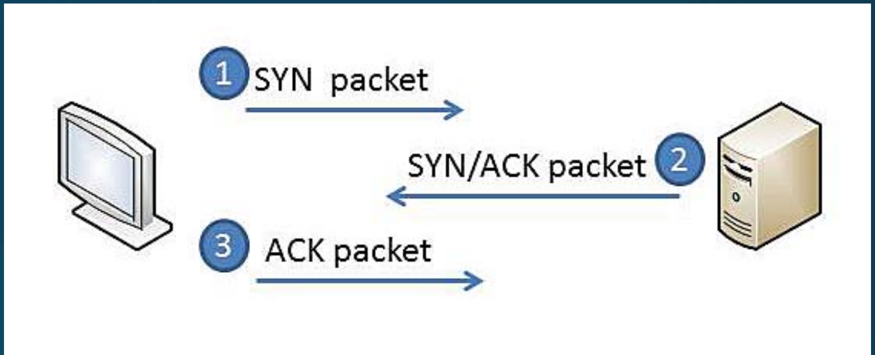
- Sawmill
- Splunk
- ZedLan
- Powershell and other builtin commands

Linux

- Sawmill
- Splunk
- Bind Log Analyzer
- awk and other built-in commands

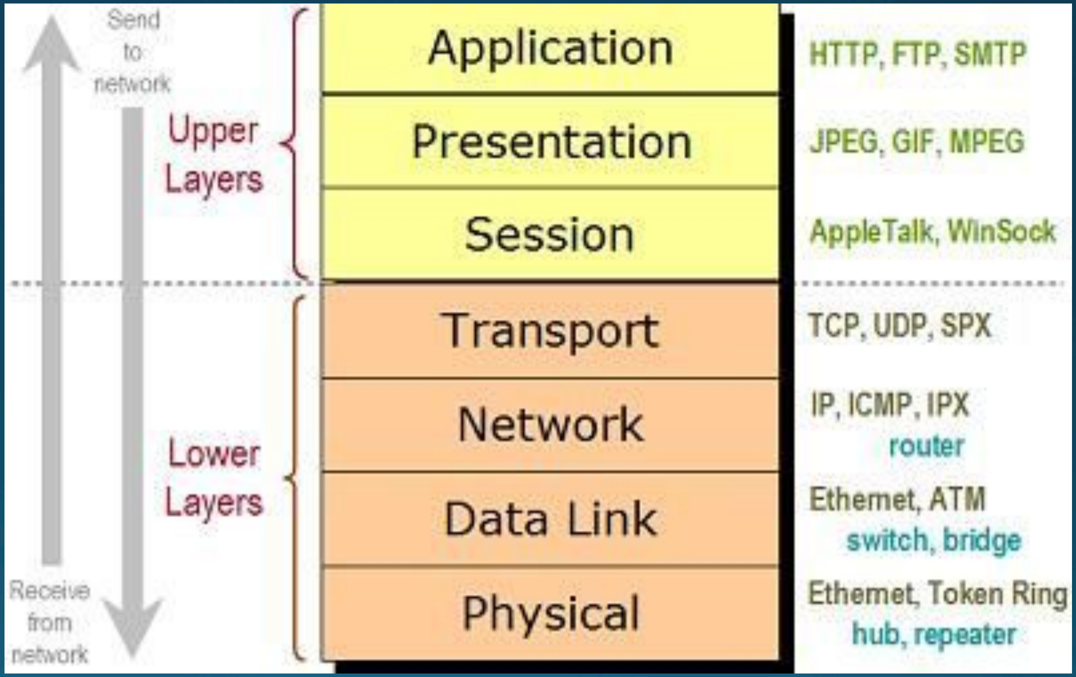
- Benefits of parsing tools
- Other options

- KSA
- Operating Systems
- **Protocol Examples**
- Now What?



Protocol Examples

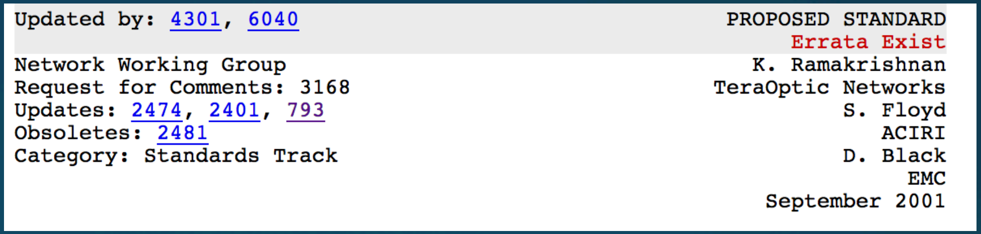
- Request for Comments
- IPv4/6
- TCP
- ICMP
- NTP
- TCP DNP3
- MOPRC



Application	HTTP, FTP, SMTP
Presentation	JPEG, GIF, MPEG
Session	AppleTalk, WinSock
Transport	TCP, UDP, SPX
Network	IP, ICMP, IPX router
Data Link	Ethernet, ATM switch, bridge
Physical	Ethernet, Token Ring hub, repeater

Request For Comments (RFC)

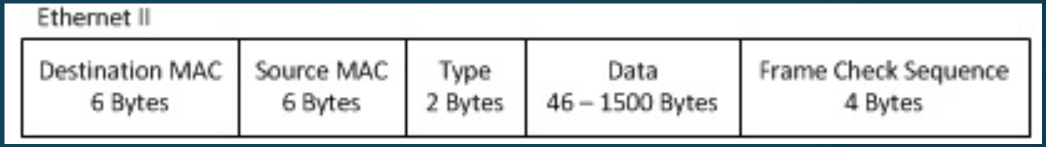
- Contain technical and organizational notes about the Internet
- Published from the Internet Engineering Task Force (IETF) and the Internet Society (ISOC)
- https://www.ietf.org



```
Updated by: 4301, 6040                                  PROPOSED STANDARD
                                                             Errata Exist
Network Working Group                                     K. Ramakrishnan
Request for Comments: 3168                             TeraOptic Networks
Updates: 2474, 2401, 793                                         S. Floyd
Obsoletes: 2481                                                     ACIRI
Category: Standards Track                                        D. Black
                                                                      EMC
                                                           September 2001
```

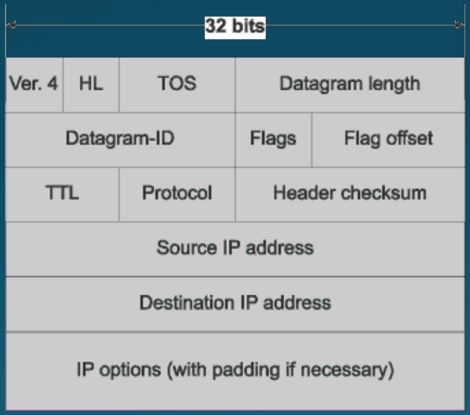
IPv4 and IPv6 Header

- Ethernet Frame Header Type field
- Fields consolidated in IPv6
- Extension Headers (EH) IPv6



Ethernet II

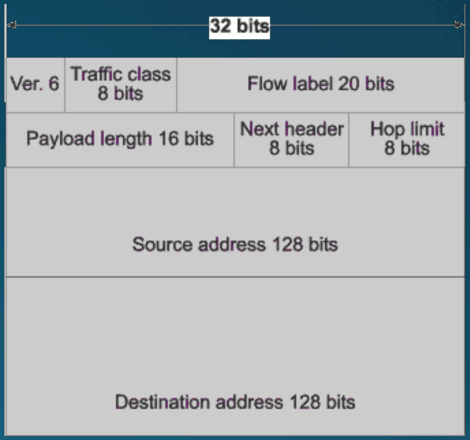
Destination MAC 6 Bytes	Source MAC 6 Bytes	Type 2 Bytes	Data 46 – 1500 Bytes	Frame Check Sequence 4 Bytes



32 bits

Ver. 4	HL	TOS	Datagram length	
Datagram-ID			Flags	Flag offset
TTL		Protocol	Header checksum	
Source IP address				
Destination IP address				
IP options (with padding if necessary)				

IPv4 header



32 bits

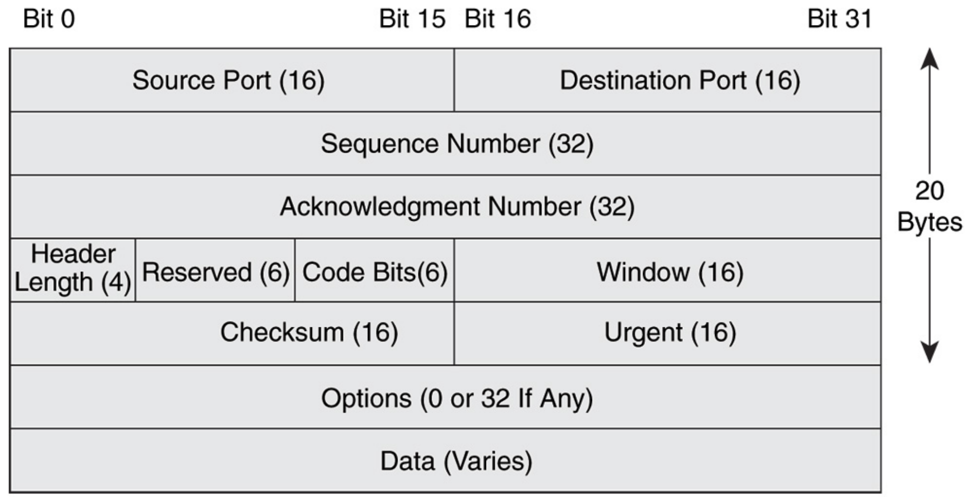
Ver. 6	Traffic class 8 bits	Flow label 20 bits	
Payload length 16 bits		Next header 8 bits	Hop limit 8 bits
Source address 128 bits			
Destination address 128 bits			

IPv6 header

http://www.deep6cyber.com

TCP Header

- RFC 6040
- 3-way handshake
- Error control
- Ordered transfer



Bit 0 Bit 15 Bit 16 Bit 31

Source Port (16) | Destination Port (16)

Sequence Number (32)

Acknowledgment Number (32)

Header Length (4) | Reserved (6) | Code Bits(6) | Window (16)

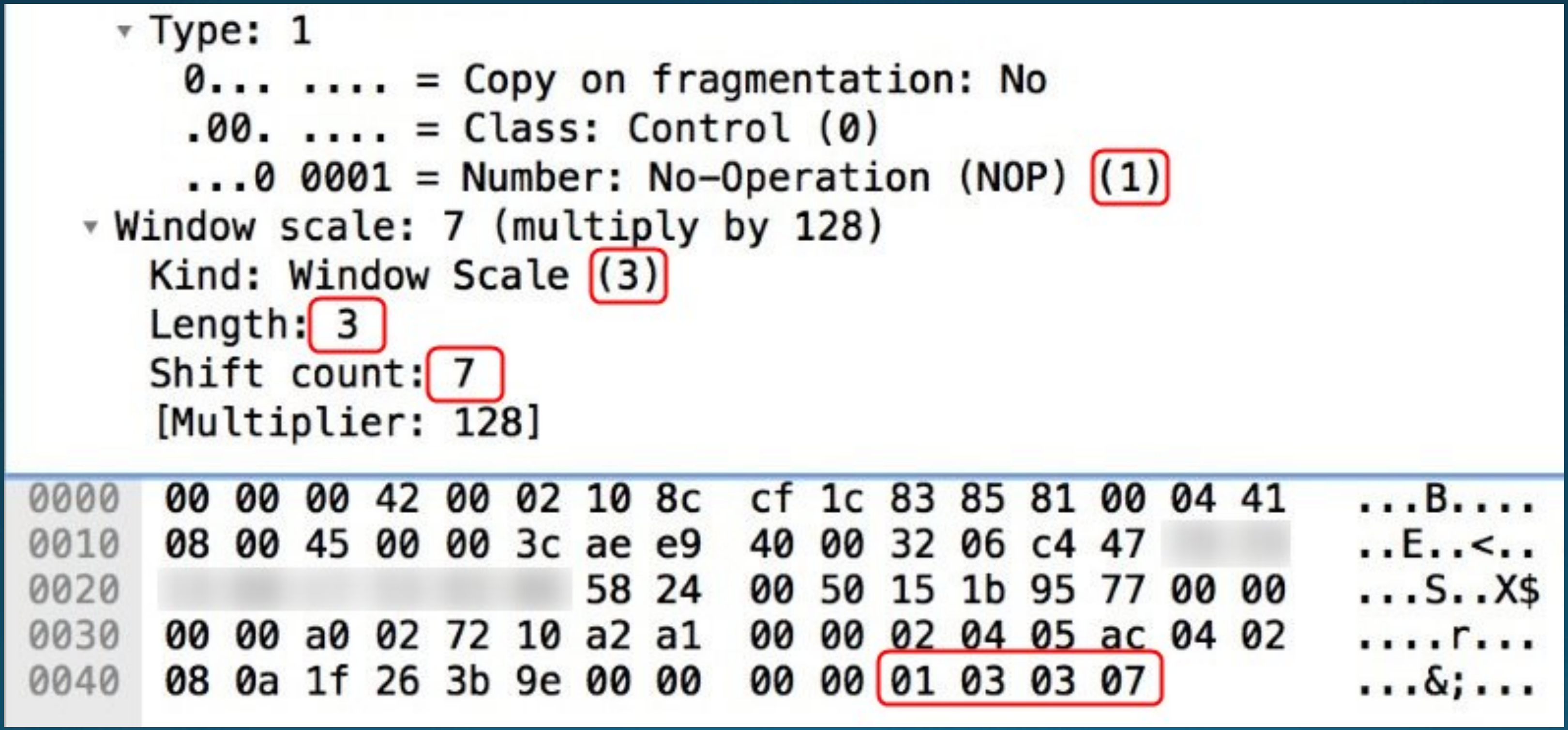
Checksum (16) | Urgent (16)

Options (0 or 32 If Any)

Data (Varies)

20 Bytes

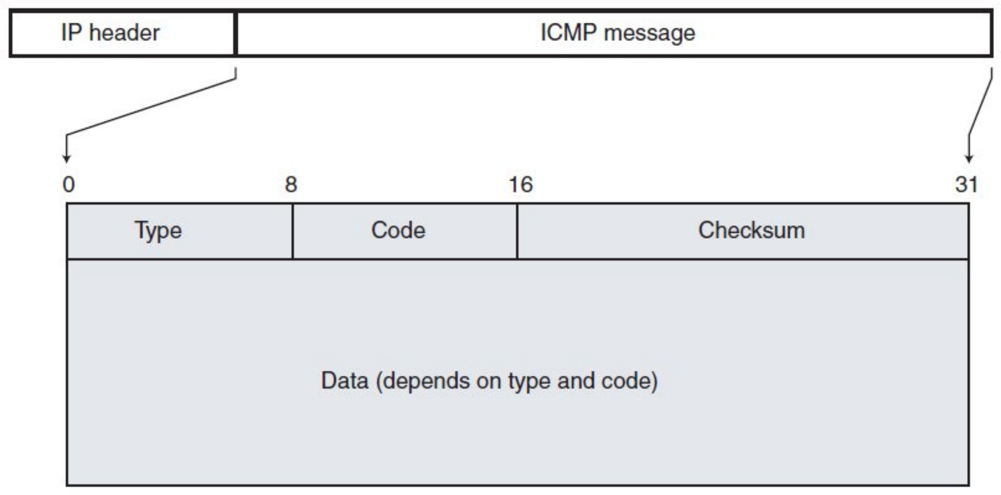
TCP Example



```
  ▾ Type: 1
      0... .... = Copy on fragmentation: No
      .00. .... = Class: Control (0)
      ...0 0001 = Number: No-Operation (NOP) (1)
▾ Window scale: 7 (multiply by 128)
    Kind: Window Scale (3)
    Length: 3
    Shift count: 7
    [Multiplier: 128]

0000  00 00 00 42 00 02 10 8c  cf 1c 83 85 81 00 04 41   ...B....
0010  08 00 45 00 00 3c ae e9  40 00 32 06 c4 47 [redacted]   ..E..<..
0020  [redacted]       58 24  00 50 15 1b 95 77 00 00   ...S..X$
0030  00 00 a0 02 72 10 a2 a1  00 00 02 04 05 ac 04 02   ....r...
0040  08 0a 1f 26 3b 9e 00 00  00 00 01 03 03 07         ...&;...
```

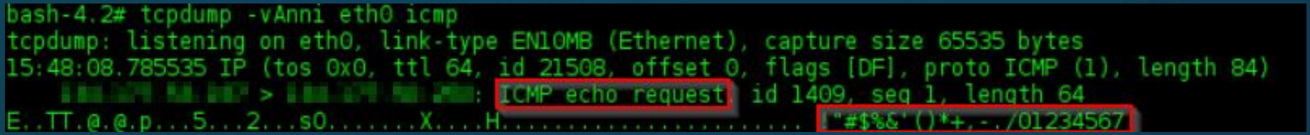
ICMPv4 Header

- RFC 6918
- Types and codes
- 1 byte type and code association
- No standard on Data
- Covert channel



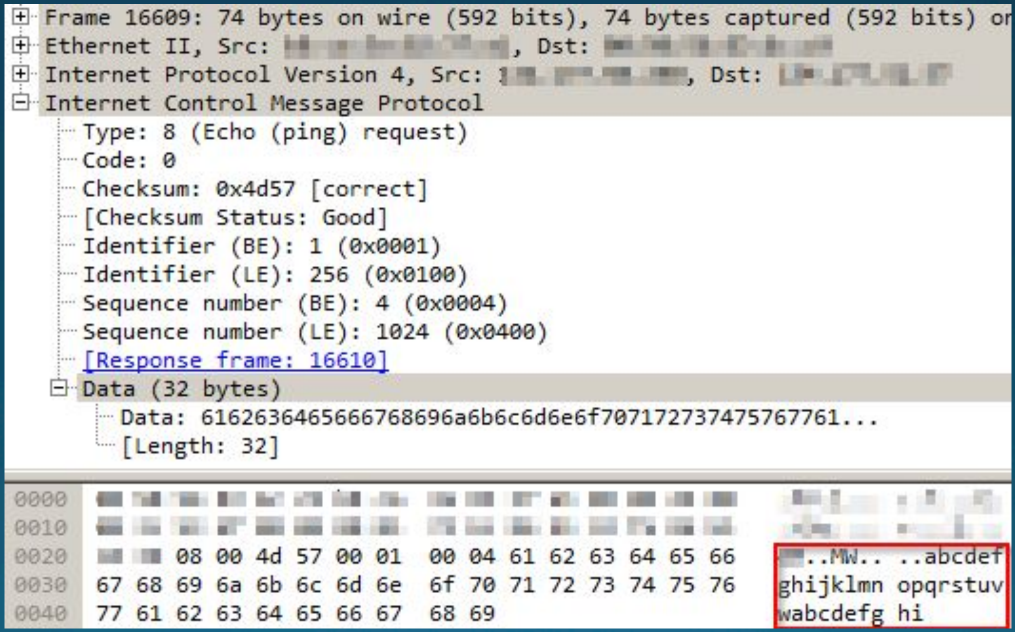
ICMPv4 Example

Linux ICMP



```
bash-4.2# tcpdump -vAnni eth0 icmp
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
15:48:08.785535 IP (tos 0x0, ttl 64, id 21508, offset 0, flags [DF], proto ICMP (1), length 84)
    [redacted] > [redacted]: ICMP echo request, id 1409, seq 1, length 64
E..TT.@.@.p...5...2...sO.......X....H.......................... !"#$%&'()*+,-./01234567
```

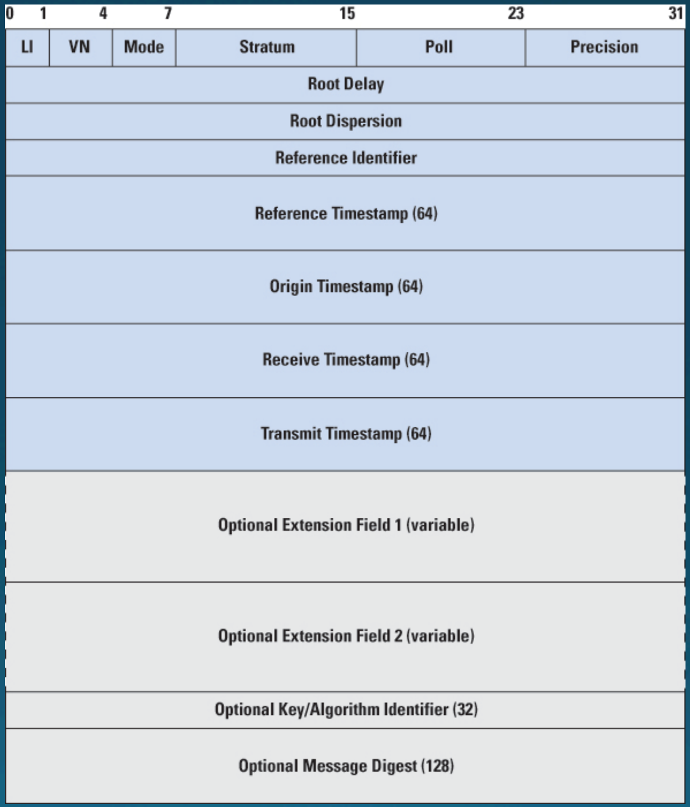
Windows ICMP



```
⊞ Frame 16609: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on
⊞ Ethernet II, Src: [redacted], Dst: [redacted]
⊞ Internet Protocol Version 4, Src: [redacted], Dst: [redacted]
⊟ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d57 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 4 (0x0004)
    Sequence number (LE): 1024 (0x0400)
    [Response frame: 16610]
  ⊟ Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f7071727374757677761...
      [Length: 32]

0000  [redacted]
0010  [redacted]
0020  [redacted] 08 00 4d 57 00 01  00 04 61 62 63 64 65 66   [redacted]..MW.. ..abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

NTP

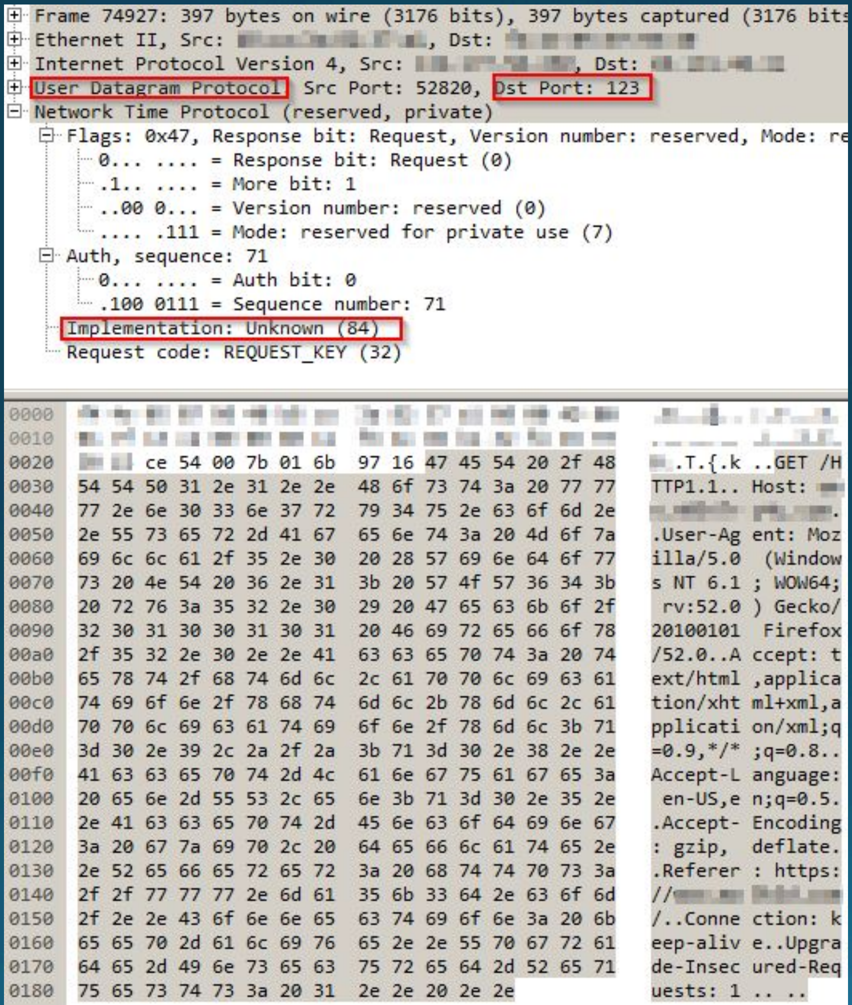
- RFC 5905 (NTPv4)
- NTP is a UDP datagram
- Time synchronization is useful for timeline generation



0 1 4 7 15 23 31

LI	VN	Mode	Stratum	Poll	Precision
Root Delay					
Root Dispersion					
Reference Identifier					
Reference Timestamp (64)					
Origin Timestamp (64)					
Receive Timestamp (64)					
Transmit Timestamp (64)					
Optional Extension Field 1 (variable)					
Optional Extension Field 2 (variable)					
Optional Key/Algorithm Identifier (32)					
Optional Message Digest (128)					

NTP Example

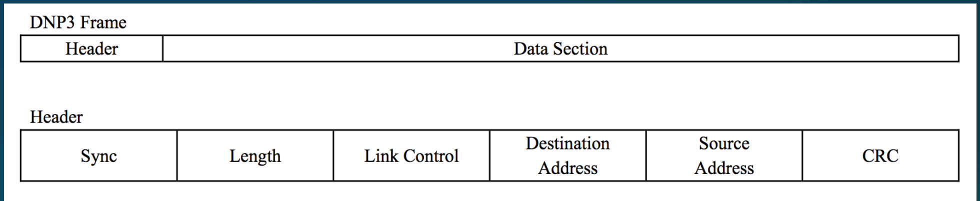


```
⊞ Frame 74927: 397 bytes on wire (3176 bits), 397 bytes captured (3176 bits
⊞ Ethernet II, Src: [redacted], Dst: [redacted]
⊞ Internet Protocol Version 4, Src: [redacted], Dst: [redacted]
⊞ User Datagram Protocol, Src Port: 52820, Dst Port: 123
⊟ Network Time Protocol (reserved, private)
   ⊟ Flags: 0x47, Response bit: Request, Version number: reserved, Mode: re
        0... .... = Response bit: Request (0)
        .1.. .... = More bit: 1
        ..00 0... = Version number: reserved (0)
        .... .111 = Mode: reserved for private use (7)
   ⊟ Auth, sequence: 71
        0... .... = Auth bit: 0
        .100 0111 = Sequence number: 71
     Implementation: Unknown (84)
     Request code: REQUEST_KEY (32)
```

```
0000  [redacted]                                         [redacted]
0010  [redacted]                                         [redacted]
0020  [redacted] ce 54 00 7b 01 6b  97 16 47 45 54 20 2f 48   [redacted].T.{.k ..GET /H
0030  54 54 50 31 2e 31 2e 2e  48 6f 73 74 3a 20 77 77   TTP1.1.. Host: [redacted]
0040  77 2e 6e 30 33 6e 37 72  79 34 75 2e 63 6f 6d 2e   [redacted].
0050  2e 55 73 65 72 2d 41 67  65 6e 74 3a 20 4d 6f 7a   .User-Ag ent: Moz
0060  69 6c 6c 61 2f 35 2e 30  20 28 57 69 6e 64 6f 77   illa/5.0  (Window
0070  73 20 4e 54 20 36 2e 31  3b 20 57 4f 57 36 34 3b   s NT 6.1 ; WOW64;
0080  20 72 76 3a 35 32 2e 30  29 20 47 65 63 6b 6f 2f    rv:52.0 ) Gecko/
0090  32 30 31 30 30 31 30 31  20 46 69 72 65 66 6f 78   20100101  Firefox
00a0  2f 35 32 2e 30 2e 2e 41  63 63 65 70 74 3a 20 74   /52.0..A ccept: t
00b0  65 78 74 2f 68 74 6d 6c  2c 61 70 70 6c 69 63 61   ext/html ,applica
00c0  74 69 6f 6e 2f 78 68 74  6d 6c 2b 78 6d 6c 2c 61   tion/xht ml+xml,a
00d0  70 70 6c 69 63 61 74 69  6f 6e 2f 78 6d 6c 3b 71   pplicati on/xml;q
00e0  3d 30 2e 39 2c 2a 2f 2a  3b 71 3d 30 2e 38 2e 2e   =0.9,*/* ;q=0.8..
00f0  41 63 63 65 70 74 2d 4c  61 6e 67 75 61 67 65 3a   Accept-L anguage:
0100  20 65 6e 2d 55 53 2c 65  6e 3b 71 3d 30 2e 35 2e    en-US,e n;q=0.5.
0110  2e 41 63 63 65 70 74 2d  45 6e 63 6f 64 69 6e 67   .Accept- Encoding
0120  3a 20 67 7a 69 70 2c 20  64 65 66 6c 61 74 65 2e   : gzip,  deflate.
0130  2e 52 65 66 65 72 65 72  3a 20 68 74 74 70 73 3a   .Referer : https:
0140  2f 2f 77 77 77 2e 6d 61  35 6b 33 64 2e 63 6f 6d   //[redacted]
0150  2f 2e 2e 43 6f 6e 6e 65  63 74 69 6f 6e 3a 20 6b   /..Conne ction: k
0160  65 65 70 2d 61 6c 69 76  65 2e 2e 55 70 67 72 61   eep-aliv e..Upgra
0170  64 65 2d 49 6e 73 65 63  75 72 65 64 2d 52 65 71   de-Insec ured-Req
0180  75 65 73 74 73 3a 20 31  2e 2e 20 2e 2e            uests: 1 .. ..
```

TCP DNP3

- Consists of header and data section
- Header specifies:
  - Frame size
  - Contains data link control information
  - Identifies DNP3 source and destination device addresses
- Data specifies:
  - Data passed down from layers above



DNP3 Frame

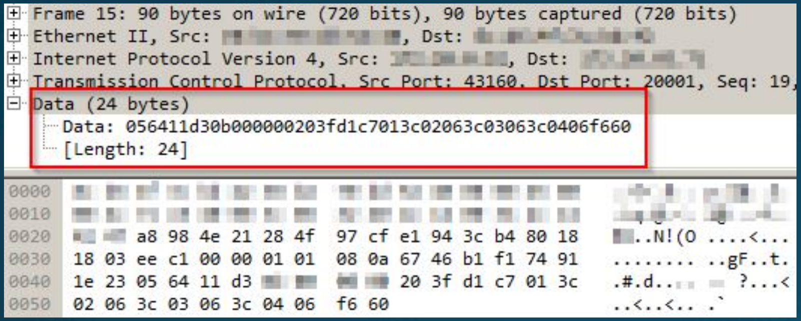
Header	Data Section

Header

Sync	Length	Link Control	Destination Address	Source Address	CRC

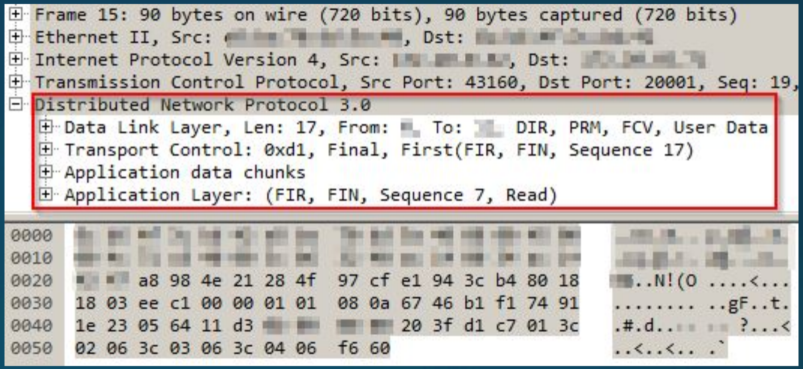
TCP DNP3 Example

DNP3 Raw



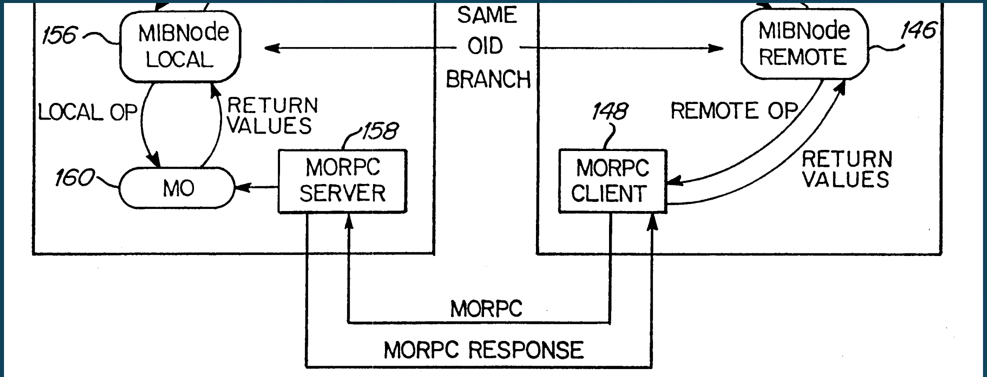
```
⊞ Frame 15: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
⊞ Ethernet II, Src: [redacted], Dst: [redacted]
⊞ Internet Protocol Version 4, Src: [redacted], Dst: [redacted]
⊞ Transmission Control Protocol, Src Port: 43160, Dst Port: 20001, Seq: 19,
⊟ Data (24 bytes)
    Data: 056411d30b000000203fd1c7013c02063c03063c0406f660
    [Length: 24]

0000  [redacted]
0010  [redacted]
0020  [redacted] a8 98 4e 21 28 4f  97 cf e1 94 3c b4 80 18   [redacted]..N!(O ....<...
0030  18 03 ee c1 00 00 01 01  08 0a 67 46 b1 f1 74 91   ........ ..gF..t.
0040  1e 23 05 64 11 d3 [redacted] 20 3f d1 c7 01 3c   .#.d..[redacted] ?...<
0050  02 06 3c 03 06 3c 04 06  f6 60                     ..<..<.. .`
```

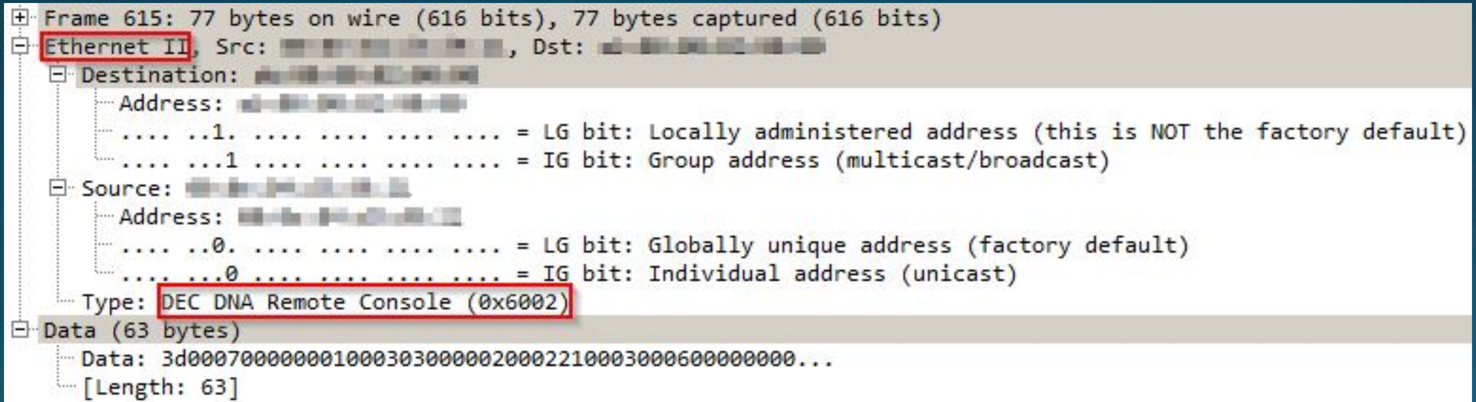
DNP3 Decoded



```
⊞ Frame 15: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
⊞ Ethernet II, Src: [redacted], Dst: [redacted]
⊞ Internet Protocol Version 4, Src: [redacted], Dst: [redacted]
⊞ Transmission Control Protocol, Src Port: 43160, Dst Port: 20001, Seq: 19,
⊟ Distributed Network Protocol 3.0
    ⊞ Data Link Layer, Len: 17, From: [redacted] To: [redacted] DIR, PRM, FCV, User Data
    ⊞ Transport Control: 0xd1, Final, First(FIR, FIN, Sequence 17)
    ⊞ Application data chunks
    ⊞ Application Layer: (FIR, FIN, Sequence 7, Read)

0000  [redacted]
0010  [redacted]
0020  [redacted] a8 98 4e 21 28 4f  97 cf e1 94 3c b4 80 18   [redacted]..N!(O ....<...
0030  18 03 ee c1 00 00 01 01  08 0a 67 46 b1 f1 74 91   ........ ..gF..t.
0040  1e 23 05 64 11 d3 [redacted] 20 3f d1 c7 01 3c   .#.d..[redacted] ?...<
0050  02 06 3c 03 06 3c 04 06  f6 60                     ..<..<.. .`
```

MOPRC Example



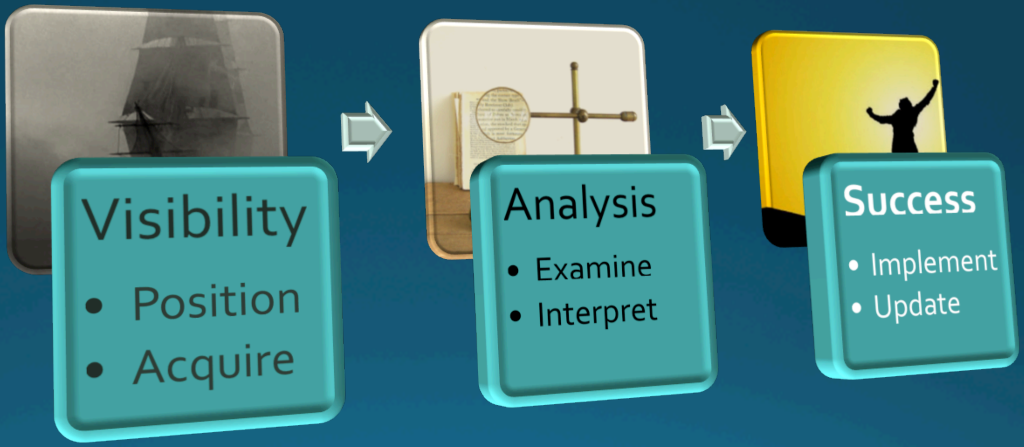


```
⊞ Frame 615: 77 bytes on wire (616 bits), 77 bytes captured (616 bits)
⊟ Ethernet II, Src: [redacted], Dst: [redacted]
   ⊟ Destination: [redacted]
        Address: [redacted]
        .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
        .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
   ⊟ Source: [redacted]
        Address: [redacted]
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
     Type: DEC DNA Remote Console (0x6002)
⊟ Data (63 bytes)
     Data: 3d000700000001000303000002000221000300060000000...
     [Length: 63]
```

- KSA
- Operating Systems
- Protocol Examples
- **Now What?**

Now What?

- A look at potential tools
- Keys for success
- Tips and tricks



Visibility

- Position
- Acquire

Analysis

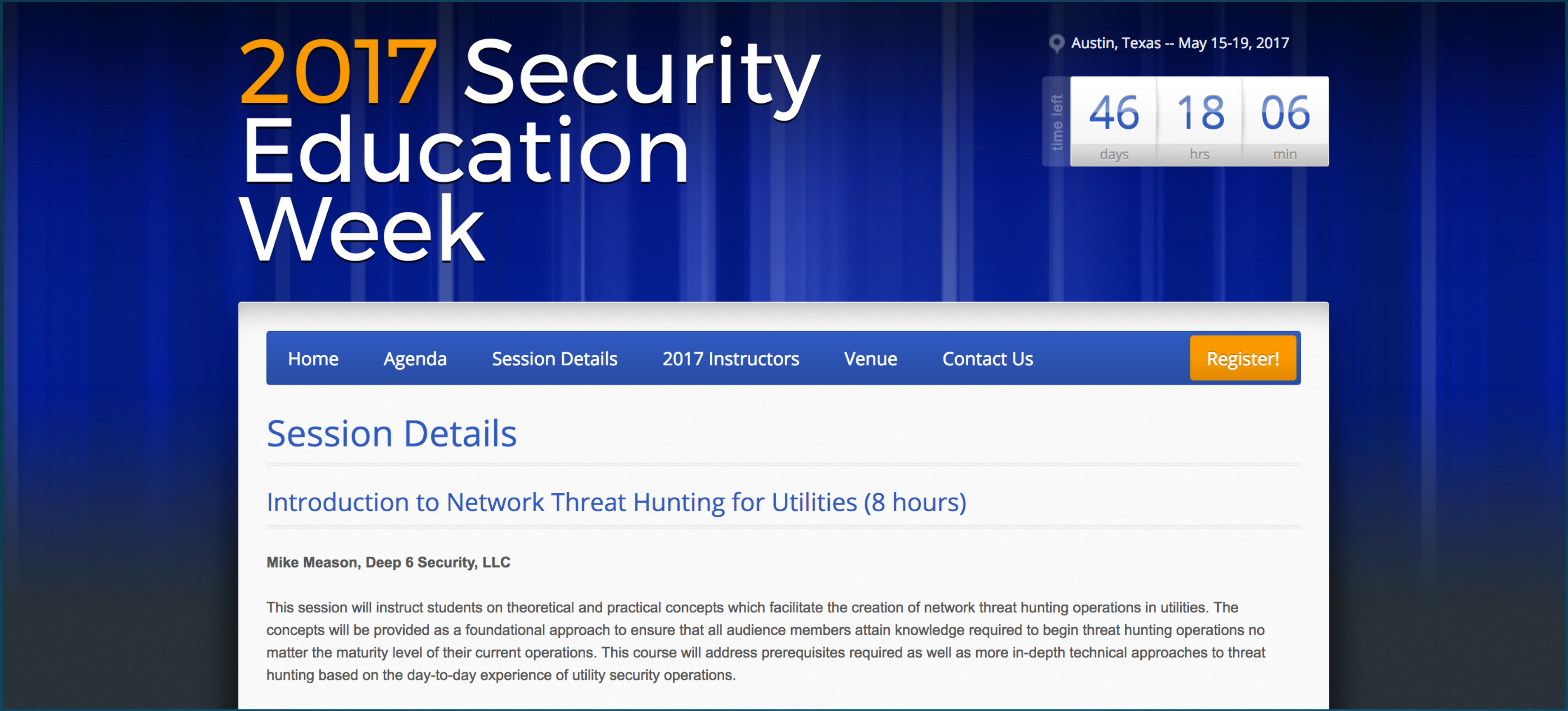
- Examine
- Interpret

Success

- Implement
- Update

ENERGYSEC
SECURING CRITICAL INFRASTRUCTURE

Amat Victoria Curam
Deep 6 Security
Acta Non Verba



2017 Security Education Week

Session Details

Introduction to Network Threat Hunting for Utilities (8 hours)

Mike Meason, Deep 6 Security, LLC

This session will instruct students on theoretical and practical concepts which facilitate the creation of network threat hunting operations in utilities. The concepts will be provided as a foundational approach to ensure that all audience members attain knowledge required to begin threat hunting operations no matter the maturity level of their current operations. This course will address prerequisites required as well as more in-depth technical approaches to threat hunting based on the day-to-day experience of utility security operations.

http://security-education-week.energysec.org/registration/

Questions?

mike@deep6cyber.com

trae@deep6cyber.com

Twitter - @deep6cyber.com