Cisco

Exam Questions 200-201

Understanding Cisco Cybersecurity Operations Fundamentals

NEW QUESTION 1
Which two elements are assets in the role of attribution in an investigation? (Choose two.)

A. context
B. session
C. laptop
D. firewall logs
E. threat actor

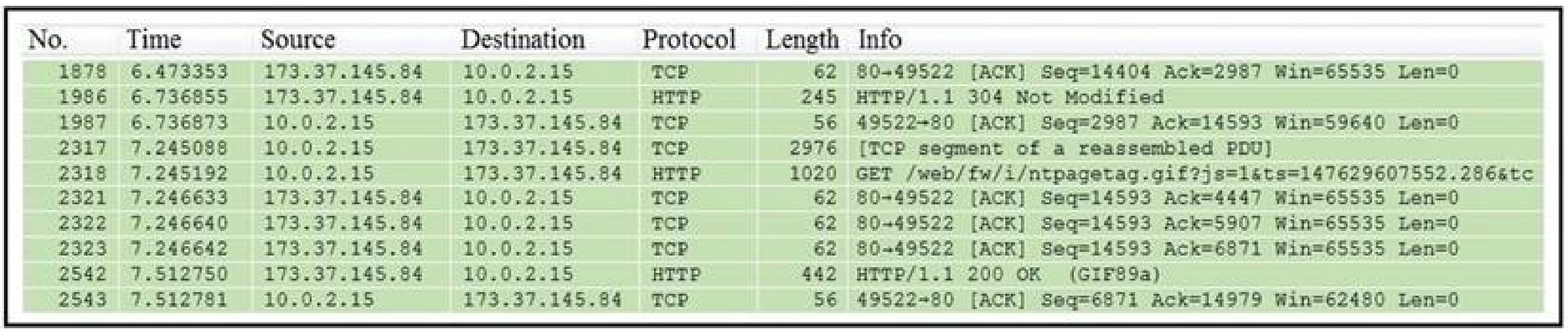
Answer: AE

NEW QUESTION 2
What is a benefit of agent-based protection when compared to agentless protection?

A. It lowers maintenance costs
B. It provides a centralized platform
C. It collects and detects all traffic locally
D. It manages numerous devices simultaneously

Answer: B

NEW QUESTION 3
Refer to the exhibit.



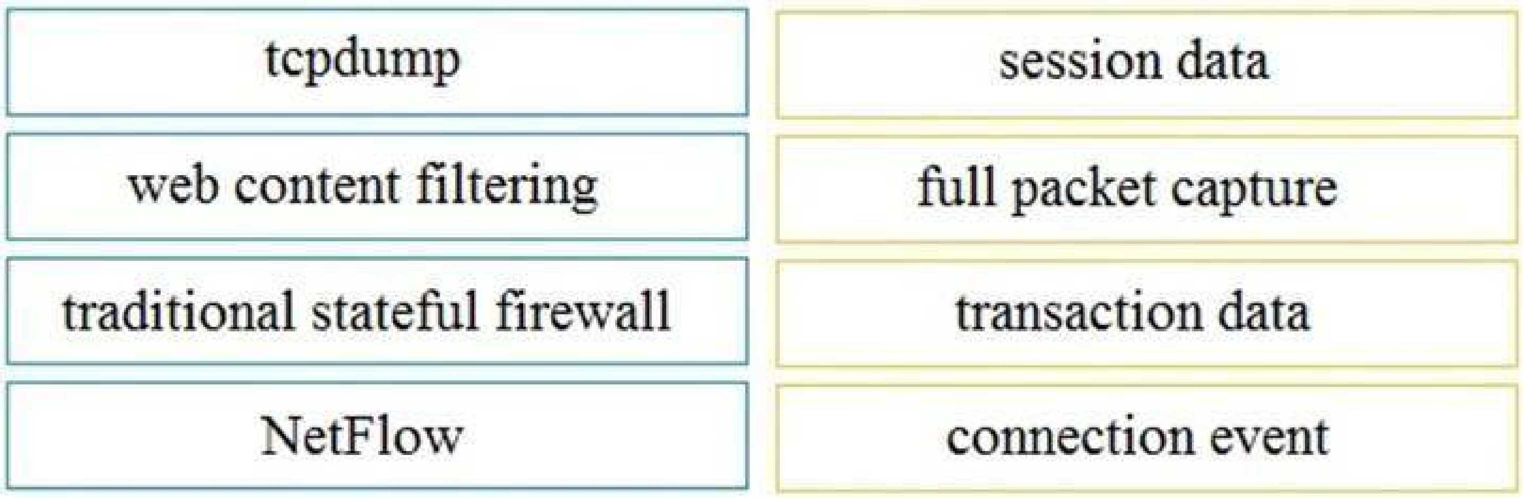
No.	Time	Source	Destination	Protocol	Length	Info
1878	6.473353	173.37.145.84	10.0.2.15	TCP	62	80→49522 [ACK] Seq=14404 Ack=2987 Win=65535 Len=0
1986	6.736855	173.37.145.84	10.0.2.15	HTTP	245	HTTP/1.1 304 Not Modified
1987	6.736873	10.0.2.15	173.37.145.84	TCP	56	49522→80 [ACK] Seq=2987 Ack=14593 Win=59640 Len=0
2317	7.245088	10.0.2.15	173.37.145.84	TCP	2976	[TCP segment of a reassembled PDU]
2318	7.245192	10.0.2.15	173.37.145.84	HTTP	1020	GET /web/fw/i/ntpagetag.gif?js=1&ts=147629607552.286&tc
2321	7.246633	173.37.145.84	10.0.2.15	TCP	62	80→49522 [ACK] Seq=14593 Ack=4447 Win=65535 Len=0
2322	7.246640	173.37.145.84	10.0.2.15	TCP	62	80→49522 [ACK] Seq=14593 Ack=5907 Win=65535 Len=0
2323	7.246642	173.37.145.84	10.0.2.15	TCP	62	80→49522 [ACK] Seq=14593 Ack=6871 Win=65535 Len=0
2542	7.512750	173.37.145.84	10.0.2.15	HTTP	442	HTTP/1.1 200 OK (GIF89a)
2543	7.512781	10.0.2.15	173.37.145.84	TCP	56	49522→80 [ACK] Seq=6871 Ack=14979 Win=62480 Len=0

Which packet contains a file that is extractable within Wireshark?

A. 2317
B. 1986
C. 2318
D. 2542

Answer: D

NEW QUESTION 4
Drag and drop the technology on the left onto the data type the technology provides on the right.



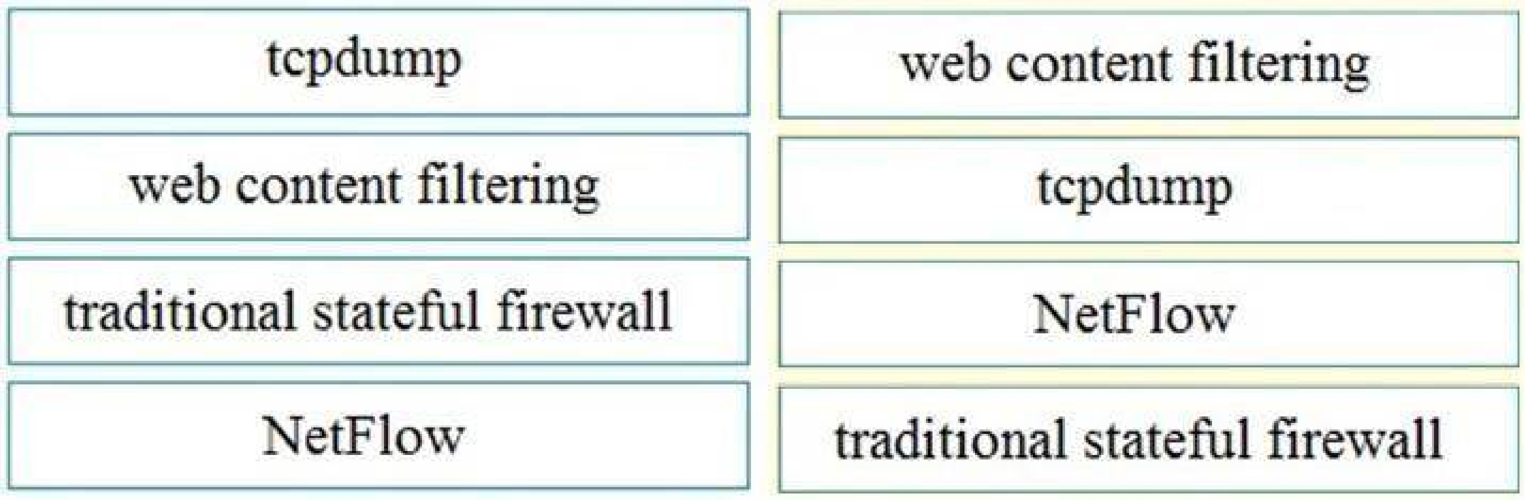
tcpdump
web content filtering
traditional stateful firewall
NetFlow

session data
full packet capture
transaction data
connection event

A. Mastered
B. Not Mastered

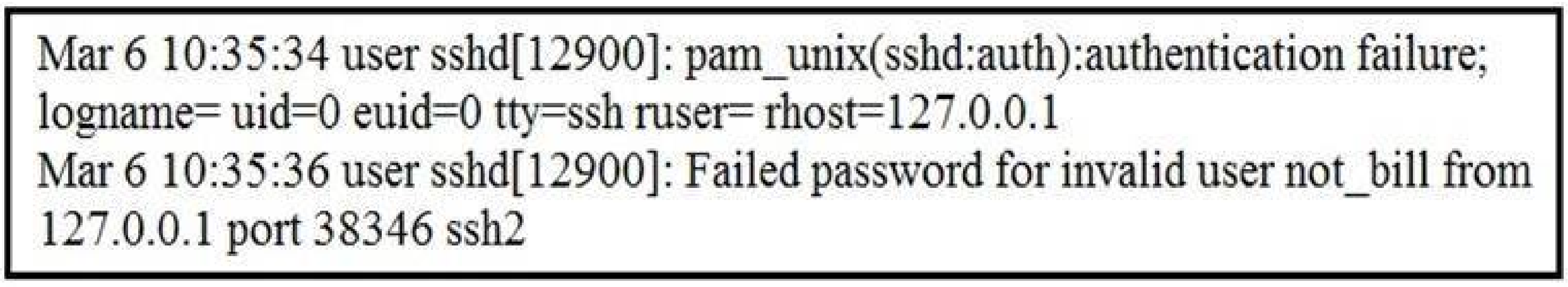
Answer: A

Explanation:



tcpdump	web content filtering
web content filtering	tcpdump
traditional stateful firewall	NetFlow
NetFlow	traditional stateful firewall

NEW QUESTION 5
Refer to the exhibit.



```
Mar 6 10:35:34 user sshd[12900]: pam_unix(sshd:auth):authentication failure;
logname= uid=0 euid=0 tty=ssh ruser= rhost=127.0.0.1
Mar 6 10:35:36 user sshd[12900]: Failed password for invalid user not_bill from
127.0.0.1 port 38346 ssh2
```

In which Linux log file is this output found?

A. /var/log/authorization.log
B. /var/log/dmesg
C. var/log/var.log
D. /var/log/auth.log

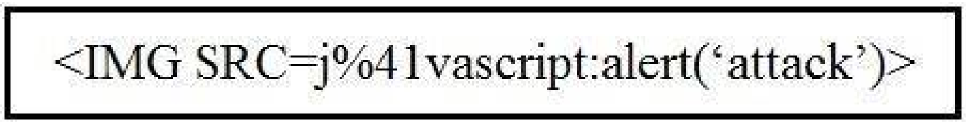
Answer: D

NEW QUESTION 6
Which piece of information is needed for attribution in an investigation?

A. proxy logs showing the source RFC 1918 IP addresses
B. RDP allowed from the Internet
C. known threat actor behavior
D. 802.1x RADIUS authentication pass arid fail logs

Answer: C

NEW QUESTION 7
Refer to the exhibit.



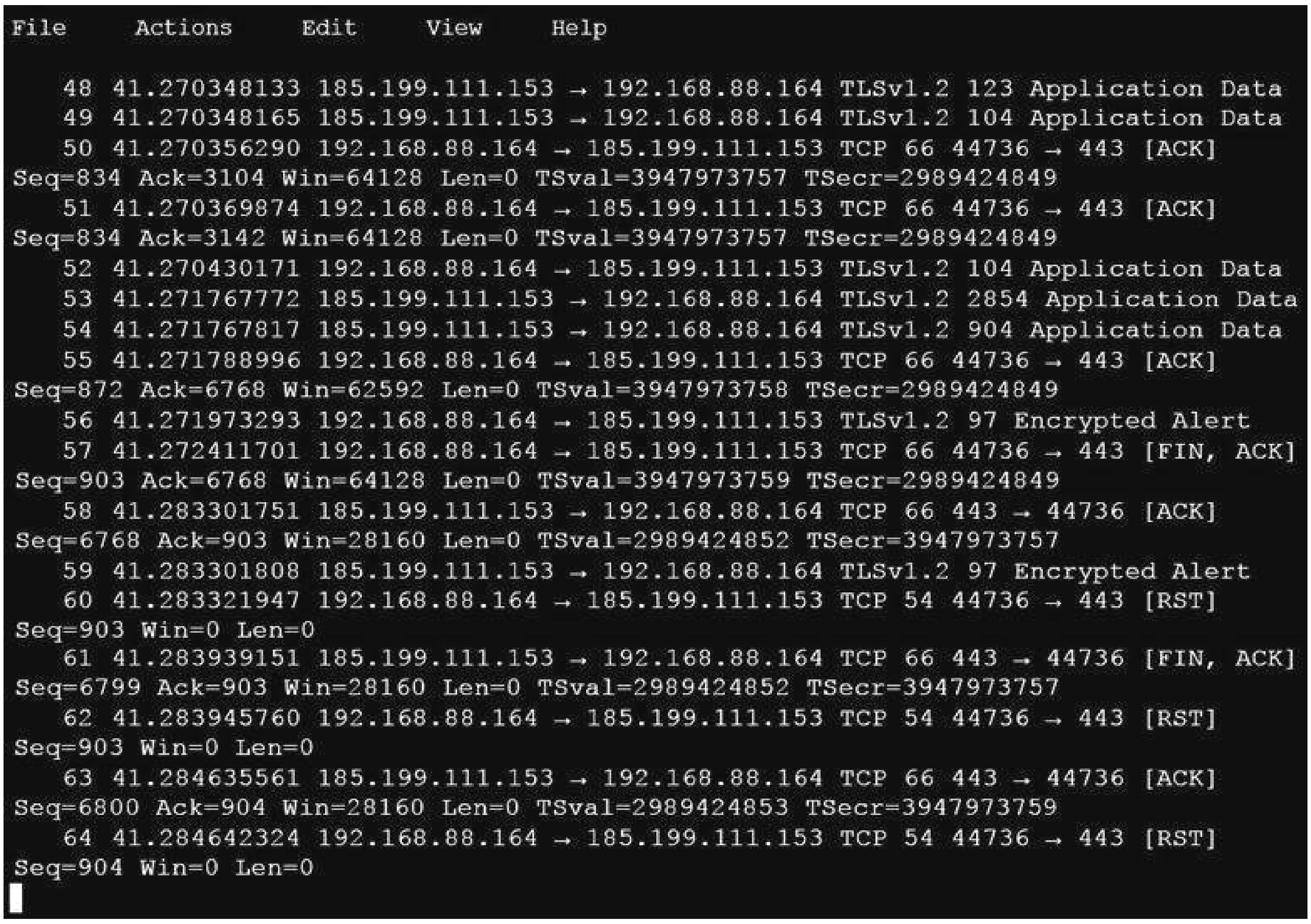
```
<IMG SRC=j%41vascript:alert('attack')>
```

Which kind of attack method is depicted in this string?

A. cross-site scripting
B. man-in-the-middle
C. SQL injection
D. denial of service

Answer: A

NEW QUESTION 8
An analyst is investigating a host in the network that appears to be communicating to a command and control server on the Internet. After collecting this packet capture the analyst cannot determine the technique and payload used for the communication.



```
    48 41.270348133 185.199.111.153 → 192.168.88.164 TLSv1.2 123 Application Data
    49 41.270348165 185.199.111.153 → 192.168.88.164 TLSv1.2 104 Application Data
    50 41.270356290 192.168.88.164 → 185.199.111.153 TCP 66 44736 → 443 [ACK]
Seq=834 Ack=3104 Win=64128 Len=0 TSval=3947973757 TSecr=2989424849
    51 41.270369874 192.168.88.164 → 185.199.111.153 TCP 66 44736 → 443 [ACK]
Seq=834 Ack=3142 Win=64128 Len=0 TSval=3947973757 TSecr=2989424849
    52 41.270430171 192.168.88.164 → 185.199.111.153 TLSv1.2 104 Application Data
    53 41.271767772 185.199.111.153 → 192.168.88.164 TLSv1.2 2854 Application Data
    54 41.271767817 185.199.111.153 → 192.168.88.164 TLSv1.2 904 Application Data
    55 41.271788996 192.168.88.164 → 185.199.111.153 TCP 66 44736 → 443 [ACK]
Seq=872 Ack=6768 Win=62592 Len=0 TSval=3947973758 TSecr=2989424849
    56 41.271973293 192.168.88.164 → 185.199.111.153 TLSv1.2 97 Encrypted Alert
    57 41.272411701 192.168.88.164 → 185.199.111.153 TCP 66 44736 → 443 [FIN, ACK]
Seq=903 Ack=6768 Win=64128 Len=0 TSval=3947973759 TSecr=2989424849
    58 41.283301751 185.199.111.153 → 192.168.88.164 TCP 66 443 → 44736 [ACK]
Seq=6768 Ack=903 Win=28160 Len=0 TSval=2989424852 TSecr=3947973757
    59 41.283301808 185.199.111.153 → 192.168.88.164 TLSv1.2 97 Encrypted Alert
    60 41.283321947 192.168.88.164 → 185.199.111.153 TCP 54 44736 → 443 [RST]
Seq=903 Win=0 Len=0
    61 41.283939151 185.199.111.153 → 192.168.88.164 TCP 66 443 → 44736 [FIN, ACK]
Seq=6799 Ack=903 Win=28160 Len=0 TSval=2989424852 TSecr=3947973757
    62 41.283945760 192.168.88.164 → 185.199.111.153 TCP 54 44736 → 443 [RST]
Seq=903 Win=0 Len=0
    63 41.284635561 185.199.111.153 → 192.168.88.164 TCP 66 443 → 44736 [ACK]
Seq=6800 Ack=904 Win=28160 Len=0 TSval=2989424853 TSecr=3947973759
    64 41.284642324 192.168.88.164 → 185.199.111.153 TCP 54 44736 → 443 [RST]
Seq=904 Win=0 Len=0
```

Which obfuscation technique is the attacker using?

A. Base64 encoding
B. transport layer security encryption
C. SHA-256 hashing
D. ROT13 encryption

Answer: B

NEW QUESTION 9
What specific type of analysis is assigning values to the scenario to see expected outcomes?

A. deterministic
B. exploratory
C. probabilistic
D. descriptive

Answer: A

NEW QUESTION 10
What is the practice of giving an employee access to only the resources needed to accomplish their job?

A. principle of least privilege
B. organizational separation
C. separation of duties
D. need to know principle

Answer: A

NEW QUESTION 10
What should a security analyst consider when comparing inline traffic interrogation with traffic tapping to determine which approach to use in the network?

A. Tapping interrogation replicates signals to a separate port for analyzing traffic
B. Tapping interrogations detect and block malicious traffic
C. Inline interrogation enables viewing a copy of traffic to ensure traffic is in compliance with security policies
D. Inline interrogation detects malicious traffic but does not block the traffic

Answer: A

NEW QUESTION 14
Which evasion technique is a function of ransomware?

A. extended sleep calls
B. encryption
C. resource exhaustion

D. encoding

Answer: B

NEW QUESTION 15
Which metric in CVSS indicates an attack that takes a destination bank account number and replaces it with a different bank account number?

A. integrity
B. confidentiality
C. availability
D. scope

Answer: A

NEW QUESTION 18
Which step in the incident response process researches an attacking host through logs in a SIEM?

A. detection and analysis
B. preparation
C. eradication
D. containment

Answer: A

NEW QUESTION 20
One of the objectives of information security is to protect the CIA of information and systems. What does CIA mean in this context?

A. confidentiality, identity, and authorization
B. confidentiality, integrity, and authorization
C. confidentiality, identity, and availability
D. confidentiality, integrity, and availability

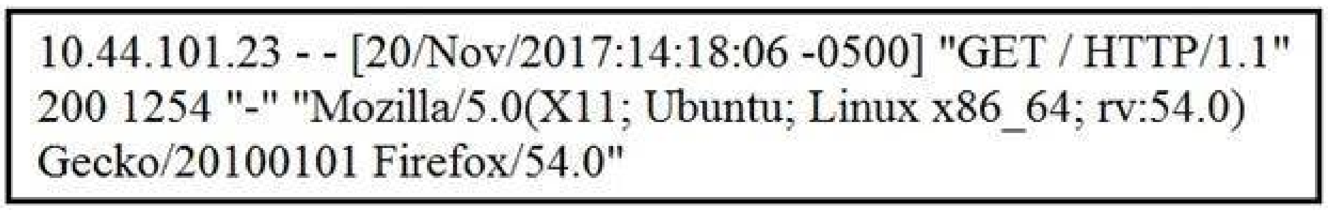
Answer: D

NEW QUESTION 22
A security specialist notices 100 HTTP GET and POST requests for multiple pages on the web servers. The agent in the requests contains PHP code that, if executed, creates and writes to a new PHP file on the webserver. Which event category is described?

A. reconnaissance
B. action on objectives
C. installation
D. exploitation

Answer: C

NEW QUESTION 24
Refer to the exhibit.



```
10.44.101.23 - - [20/Nov/2017:14:18:06 -0500] "GET / HTTP/1.1"
200 1254 "-" "Mozilla/5.0(X11; Ubuntu; Linux x86_64; rv:54.0)
Gecko/20100101 Firefox/54.0"
```

What does the message indicate?

A. an access attempt was made from the Mosaic web browser
B. a successful access attempt was made to retrieve the password file
C. a successful access attempt was made to retrieve the root of the website
D. a denied access attempt was made to retrieve the password file

Answer: C

NEW QUESTION 25
Which event artifact is used to identity HTTP GET requests for a specific file?

A. destination IP address
B. TCP ACK
C. HTTP status code
D. URI

Answer: D

NEW QUESTION 29
What is the virtual address space for a Windows process?

A. physical location of an object in memory
B. set of pages that reside in the physical memory
C. system-level memory protection feature built into the operating system
D. set of virtual memory addresses that can be used

Answer: D

NEW QUESTION 33
What do the Security Intelligence Events within the FMC allow an administrator to do?

A. See if a host is connecting to a known-bad domain.
B. Check for host-to-server traffic within your network.
C. View any malicious files that a host has downloaded.
D. Verify host-to-host traffic within your network.

Answer: A

NEW QUESTION 36
What makes HTTPS traffic difficult to monitor?

A. SSL interception
B. packet header size
C. signature detection time
D. encryption

Answer: D

NEW QUESTION 41
A security expert is working on a copy of the evidence, an ISO file that is saved in CDFS format. Which type of evidence is this file?

A. CD data copy prepared in Windows
B. CD data copy prepared in Mac-based system
C. CD data copy prepared in Linux system
D. CD data copy prepared in Android-based system

Answer: A

NEW QUESTION 46
A malicious file has been identified in a sandbox analysis tool.
Which piece of information is needed to search for additional downloads of this file by other hosts?

A. file type
B. file size
C. file name
D. file hash value

Answer: D

NEW QUESTION 49
An offline audit log contains the source IP address of a session suspected to have exploited a vulnerability resulting in system compromise.
Which kind of evidence is this IP address?

A. best evidence
B. corroborative evidence
C. indirect evidence
D. forensic evidence

Answer: B

NEW QUESTION 52
What is an example of social engineering attacks?

A. receiving an unexpected email from an unknown person with an uncharacteristic attachment from someone in the same company
B. receiving an email from human resources requesting a visit to their secure website to update contact information
C. sending a verbal request to an administrator who knows how to change an account password
D. receiving an invitation to the department’s weekly WebEx meeting

Answer: B

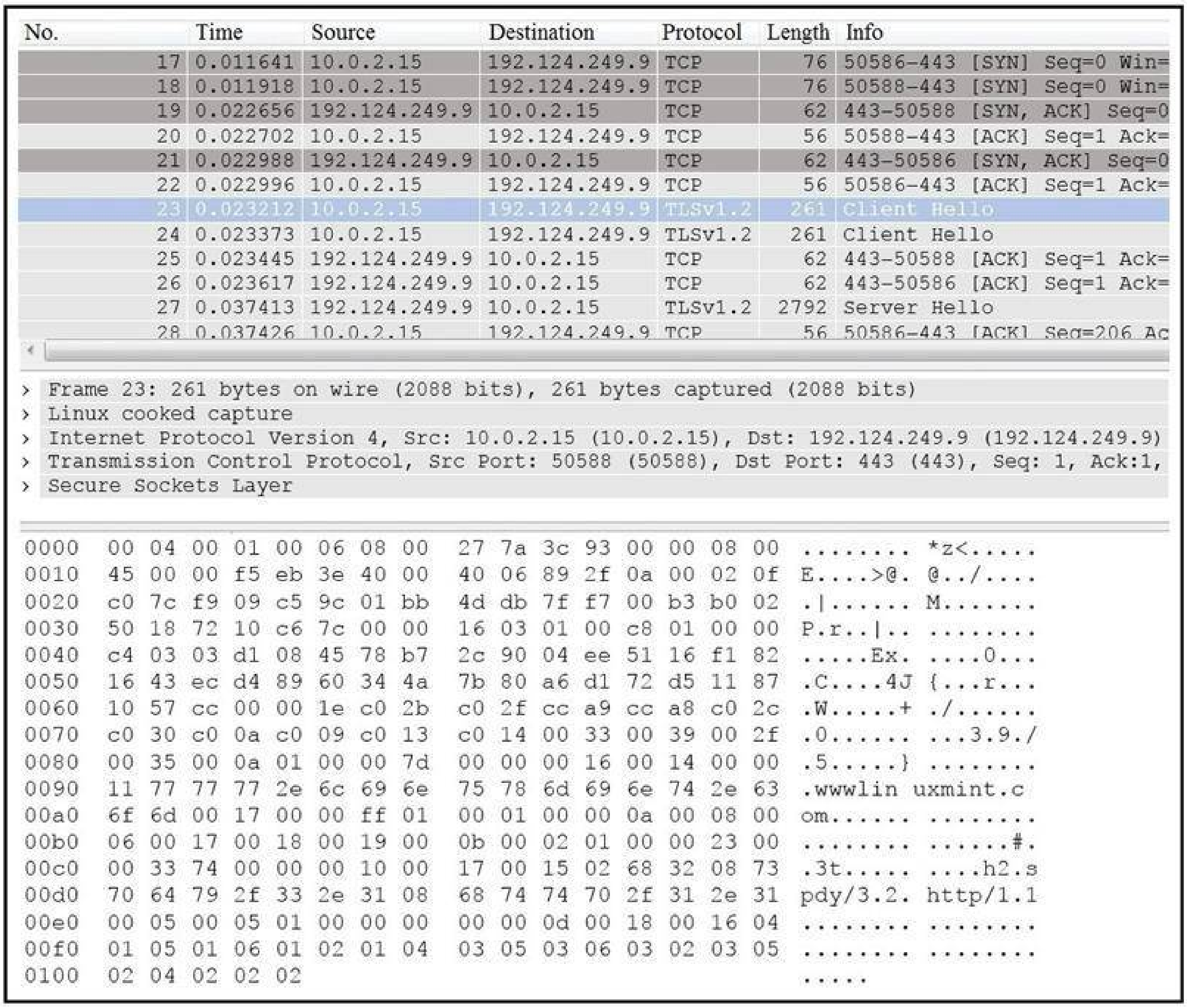
NEW QUESTION 54
Which event artifact is used to identify HTTP GET requests for a specific file?

A. destination IP address
B. URI
C. HTTP status code

D. TCP ACK

Answer: B

NEW QUESTION 56
Refer to the exhibit.

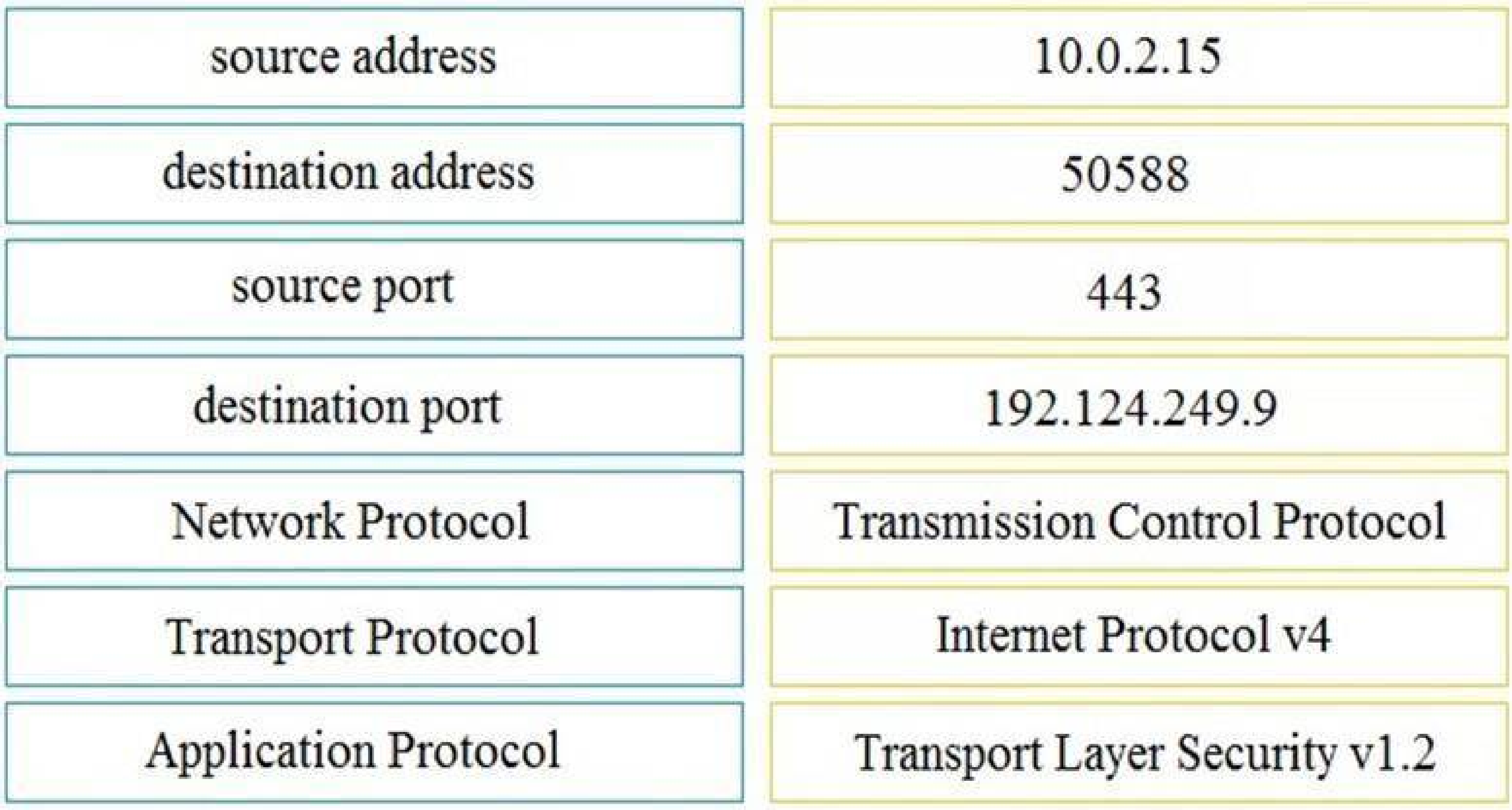


```
No.   Time      Source         Destination    Protocol Length Info
   17 0.011641  10.0.2.15      192.124.249.9  TCP        76   50586-443 [SYN] Seq=0 Win=
   18 0.011918  10.0.2.15      192.124.249.9  TCP        76   50588-443 [SYN] Seq=0 Win=
   19 0.022656  192.124.249.9  10.0.2.15      TCP        62   443-50588 [SYN, ACK] Seq=0
   20 0.022702  10.0.2.15      192.124.249.9  TCP        56   50588-443 [ACK] Seq=1 Ack=
   21 0.022988  192.124.249.9  10.0.2.15      TCP        62   443-50586 [SYN, ACK] Seq=0
   22 0.022996  10.0.2.15      192.124.249.9  TCP        56   50586-443 [ACK] Seq=1 Ack=
   23 0.023212  10.0.2.15      192.124.249.9  TLSv1.2   261   Client Hello
   24 0.023373  10.0.2.15      192.124.249.9  TLSv1.2   261   Client Hello
   25 0.023445  192.124.249.9  10.0.2.15      TCP        62   443-50588 [ACK] Seq=1 Ack=
   26 0.023617  192.124.249.9  10.0.2.15      TCP        62   443-50586 [ACK] Seq=1 Ack=
   27 0.037413  192.124.249.9  10.0.2.15      TLSv1.2  2792   Server Hello
   28 0.037426  10.0.2.15      192.124.249.9  TCP        56   50586-443 [ACK] Seq=206 Ac
```

```
> Frame 23: 261 bytes on wire (2088 bits), 261 bytes captured (2088 bits)
> Linux cooked capture
> Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 192.124.249.9 (192.124.249.9)
> Transmission Control Protocol, Src Port: 50588 (50588), Dst Port: 443 (443), Seq: 1, Ack:1,
> Secure Sockets Layer
```

```
0000  00 04 00 01 00 06 08 00  27 7a 3c 93 00 00 08 00  ........ *z<.....
0010  45 00 00 f5 eb 3e 40 00  40 06 89 2f 0a 00 02 0f  E....>@. @../....
0020  c0 7c f9 09 c5 9c 01 bb  4d db 7f f7 00 b3 b0 02  .|...... M.......
0030  50 18 72 10 c6 7c 00 00  16 03 01 00 c8 01 00 00  P.r..|.. ........
0040  c4 03 03 d1 08 45 78 b7  2c 90 04 ee 51 16 f1 82  .....Ex. ....Q...
0050  16 43 ec d4 89 60 34 4a  7b 80 a6 d1 72 d5 11 87  .C....4J {...r...
0060  10 57 cc 00 00 1e c0 2b  c0 2f cc a9 cc a8 c0 2c  .W.....+ ./......
0070  c0 30 c0 0a c0 09 c0 13  c0 14 00 33 00 39 00 2f  .0...... ...3.9./
0080  00 35 00 0a 01 00 00 7d  00 00 00 16 00 14 00 00  .5.....} ........
0090  11 77 77 77 2e 6c 69 6e  75 78 6d 69 6e 74 2e 63  .wwwlin uxmint.c
00a0  6f 6d 00 17 00 00 ff 01  00 01 00 00 0a 00 08 00  om...... ........
00b0  06 00 17 00 18 00 19 00  0b 00 02 01 00 00 23 00  ........ ......#.
00c0  00 33 74 00 00 00 10 00  17 00 15 02 68 32 08 73  .3t..... ....h2.s
00d0  70 64 79 2f 33 2e 31 08  68 74 74 70 2f 31 2e 31  pdy/3.2. http/1.1
00e0  00 05 00 05 01 00 00 00  00 00 0d 00 18 00 16 04  ........ ........
00f0  01 05 01 06 01 02 01 04  03 05 03 06 03 02 03 05  ........ ........
0100  02 04 02 02 02                                    .....
```

Drag and drop the element name from the left onto the correct piece of the PCAP file on the right.

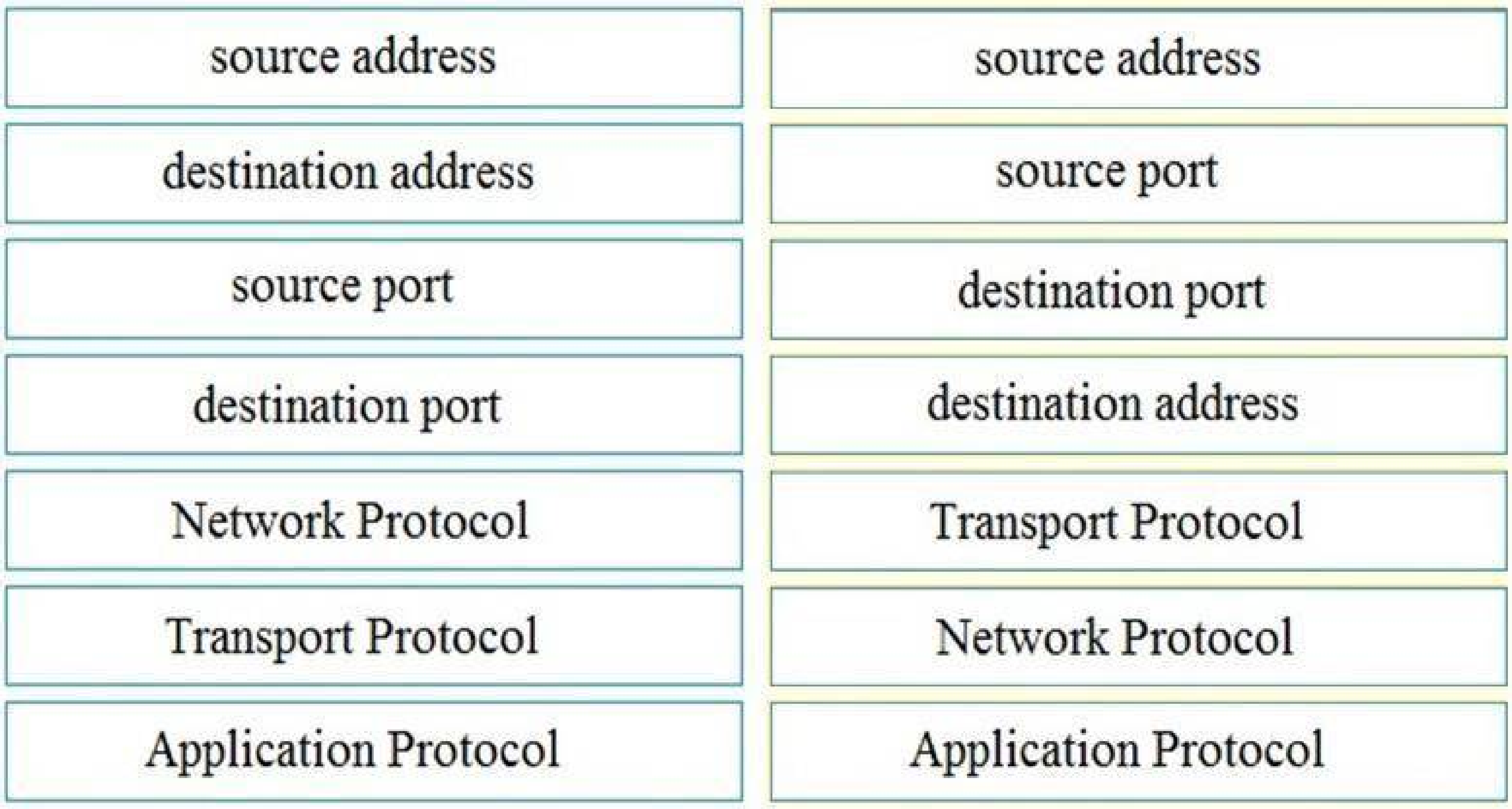


source address	10.0.2.15
destination address	50588
source port	443
destination port	192.124.249.9
Network Protocol	Transmission Control Protocol
Transport Protocol	Internet Protocol v4
Application Protocol	Transport Layer Security v1.2

A. Mastered
B. Not Mastered

Answer: A

Explanation:



source address	source address
destination address	source port
source port	destination port
destination port	destination address
Network Protocol	Transport Protocol
Transport Protocol	Network Protocol
Application Protocol	Application Protocol

NEW QUESTION 59
How is attacking a vulnerability categorized?

A. action on objectives
B. delivery
C. exploitation
D. installation

Answer: C

NEW QUESTION 60
An analyst is exploring the functionality of different operating systems.
What is a feature of Windows Management Instrumentation that must be considered when deciding on an operating system?

A. queries Linux devices that have Microsoft Services for Linux installed
B. deploys Windows Operating Systems in an automated fashion
C. is an efficient tool for working with Active Directory
D. has a Common Information Model, which describes installed hardware and software

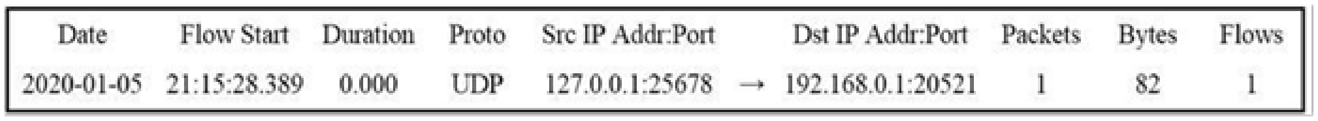
Answer: D

NEW QUESTION 64
At which layer is deep packet inspection investigated on a firewall?

A. internet
B. transport
C. application
D. data link

Answer: C

NEW QUESTION 68
Refer to the exhibit.



Date	Flow Start	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Packets	Bytes	Flows
2020-01-05	21:15:28.389	0.000	UDP	127.0.0.1:25678	→	192.168.0.1:20521	1	82	1

Which type of log is displayed?

A. proxy
B. NetFlow
C. IDS
D. sys

Answer: B

NEW QUESTION 70
Which two elements are used for profiling a network? (Choose two.)

A. session duration

B. total throughput
C. running processes
D. listening ports
E. OS fingerprint

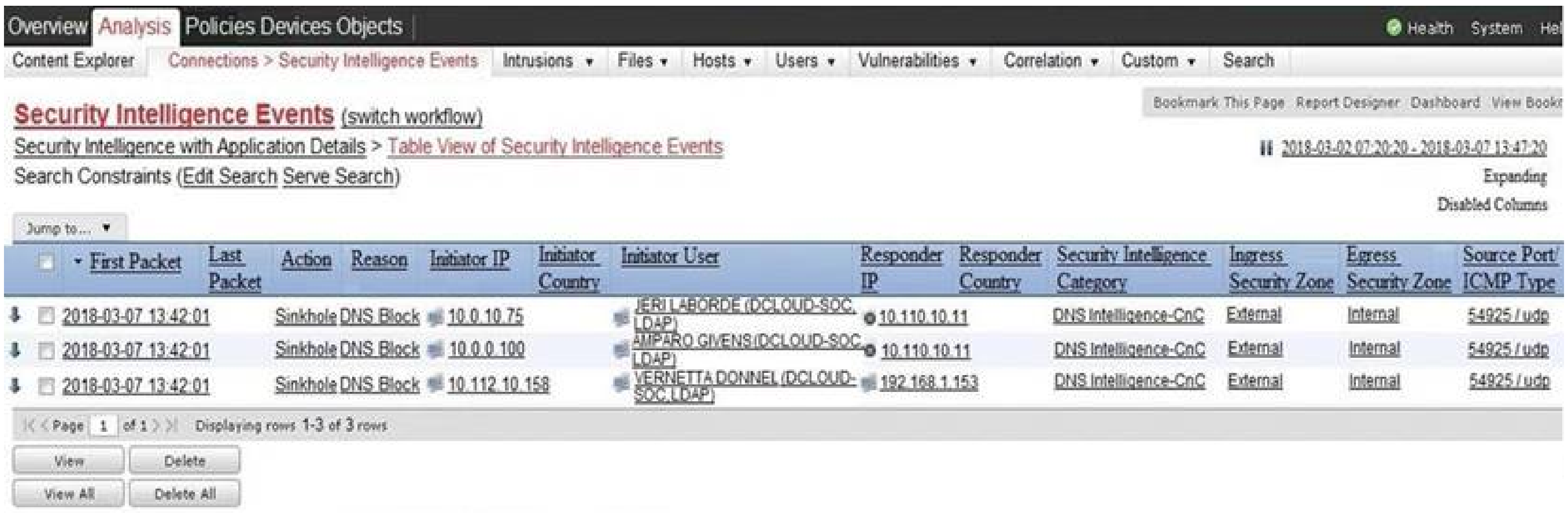
Answer: DE

NEW QUESTION 74
How is NetFlow different than traffic mirroring?

A. NetFlow collects metadata and traffic mirroring clones data
B. Traffic mirroring impacts switch performance and NetFlow does not
C. Traffic mirroring costs less to operate than NetFlow
D. NetFlow generates more data than traffic mirroring

Answer: A

NEW QUESTION 77
Refer to the exhibit.



Security Intelligence Events (switch workflow)
Security Intelligence with Application Details > Table View of Security Intelligence Events
Search Constraints (Edit Search Serve Search)

2018-03-02 07:20:20 - 2018-03-07 13:47:20
Expanding
Disabled Columns

		First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Initiator User	Responder IP	Responder Country	Security Intelligence Category	Ingress Security Zone	Egress Security Zone	Source Port/ ICMP Type
⬇	□	2018-03-07 13:42:01		Sinkhole	DNS Block	10.0.10.75		JERI LABORDE (DCLOUD-SOC, LDAP)	10.110.10.11		DNS Intelligence-CnC	External	Internal	54925 / udp
⬇	□	2018-03-07 13:42:01		Sinkhole	DNS Block	10.0.0.100		AMPARO GIVENS(DCLOUD-SOC, LDAP)	10.110.10.11		DNS Intelligence-CnC	External	Internal	54925 / udp
⬇	□	2018-03-07 13:42:01		Sinkhole	DNS Block	10.112.10.158		VERNETTA DONNEL (DCLOUD-SOC, LDAP)	192.168.1.153		DNS Intelligence-CnC	External	Internal	54925 / udp

|< < Page 1 of 1 > >| Displaying rows 1-3 of 3 rows

Which two elements in the table are parts of the 5-tuple? (Choose two.)

A. First Packet
B. Initiator User
C. Ingress Security Zone
D. Source Port
E. Initiator IP

Answer: DE

NEW QUESTION 82
......

NEW QUESTION 1
Which two elements are assets in the role of attribution in an investigation? (Choose two.)

A. context
B. session
C. laptop
D. firewall logs
E. threat actor

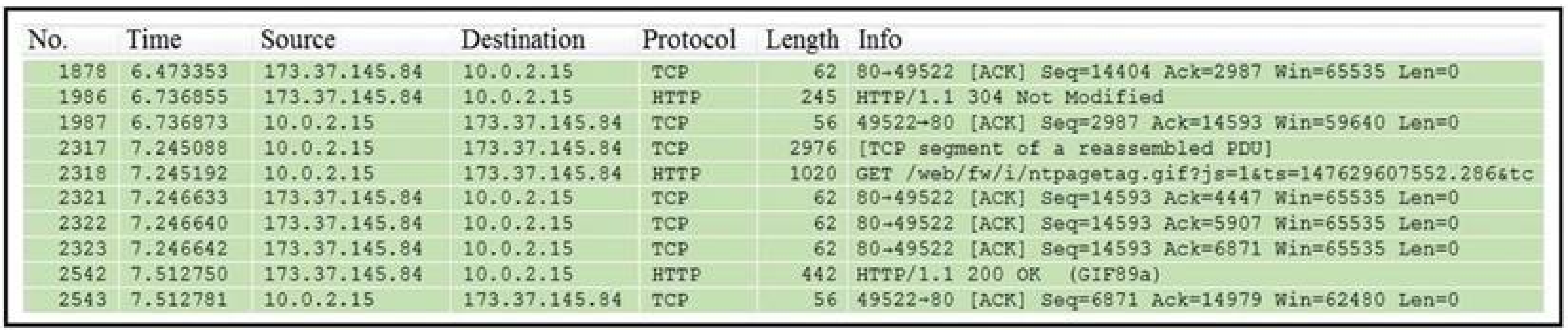
Answer: AE

NEW QUESTION 2
What is a benefit of agent-based protection when compared to agentless protection?

A. It lowers maintenance costs
B. It provides a centralized platform
C. It collects and detects all traffic locally
D. It manages numerous devices simultaneously

Answer: B

NEW QUESTION 3
Refer to the exhibit.



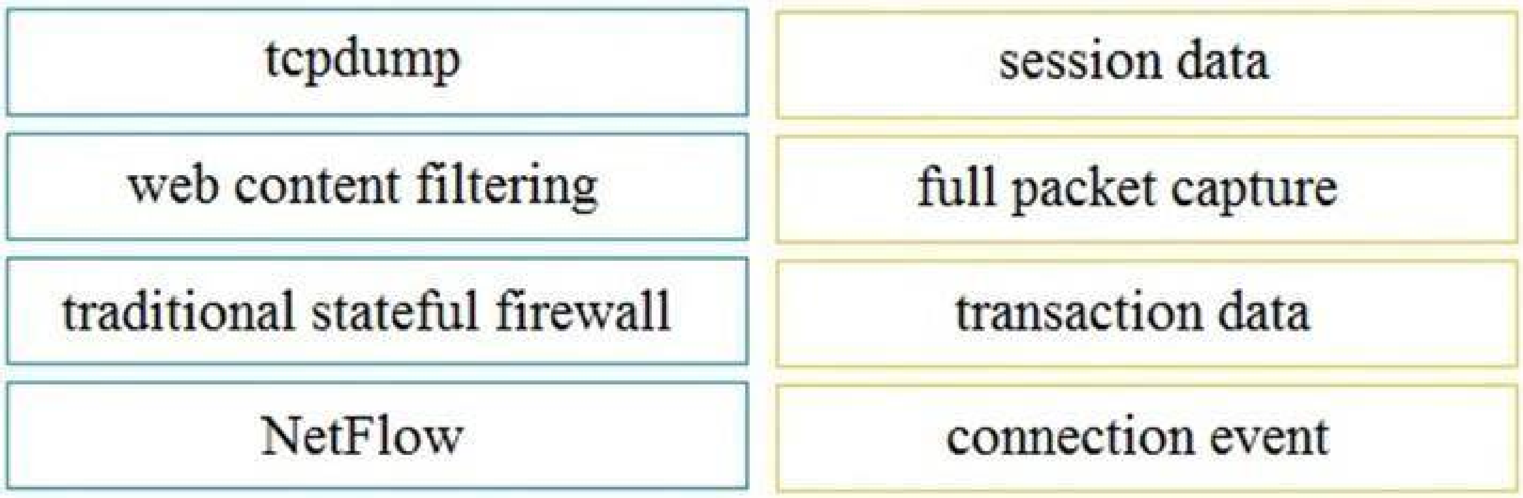
No.	Time	Source	Destination	Protocol	Length	Info
1878	6.473353	173.37.145.84	10.0.2.15	TCP	62	80→49522 [ACK] Seq=14404 Ack=2987 Win=65535 Len=0
1986	6.736855	173.37.145.84	10.0.2.15	HTTP	245	HTTP/1.1 304 Not Modified
1987	6.736873	10.0.2.15	173.37.145.84	TCP	56	49522→80 [ACK] Seq=2987 Ack=14593 Win=59640 Len=0
2317	7.245088	10.0.2.15	173.37.145.84	TCP	2976	[TCP segment of a reassembled PDU]
2318	7.245192	10.0.2.15	173.37.145.84	HTTP	1020	GET /web/fw/i/ntpagetag.gif?js=1&ts=147629607552.286&tc
2321	7.246633	173.37.145.84	10.0.2.15	TCP	62	80→49522 [ACK] Seq=14593 Ack=4447 Win=65535 Len=0
2322	7.246640	173.37.145.84	10.0.2.15	TCP	62	80→49522 [ACK] Seq=14593 Ack=5907 Win=65535 Len=0
2323	7.246642	173.37.145.84	10.0.2.15	TCP	62	80→49522 [ACK] Seq=14593 Ack=6871 Win=65535 Len=0
2542	7.512750	173.37.145.84	10.0.2.15	HTTP	442	HTTP/1.1 200 OK (GIF89a)
2543	7.512781	10.0.2.15	173.37.145.84	TCP	56	49522→80 [ACK] Seq=6871 Ack=14979 Win=62480 Len=0

Which packet contains a file that is extractable within Wireshark?

A. 2317
B. 1986
C. 2318
D. 2542

Answer: D

NEW QUESTION 4
Drag and drop the technology on the left onto the data type the technology provides on the right.



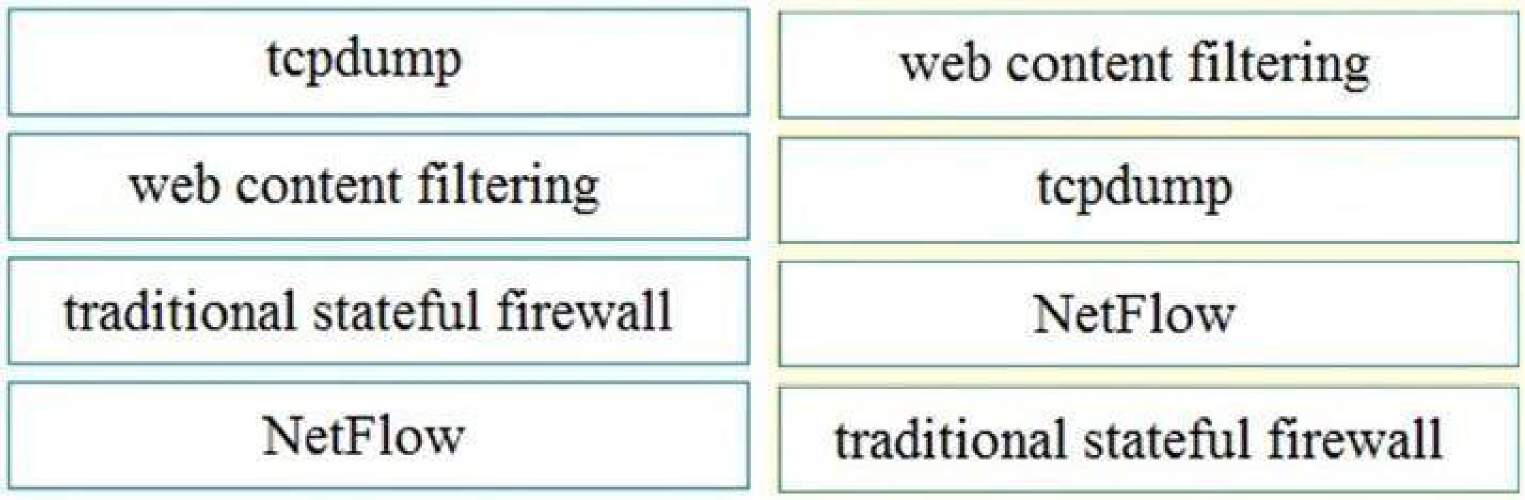
tcpdump
web content filtering
traditional stateful firewall
NetFlow

session data
full packet capture
transaction data
connection event

A. Mastered
B. Not Mastered

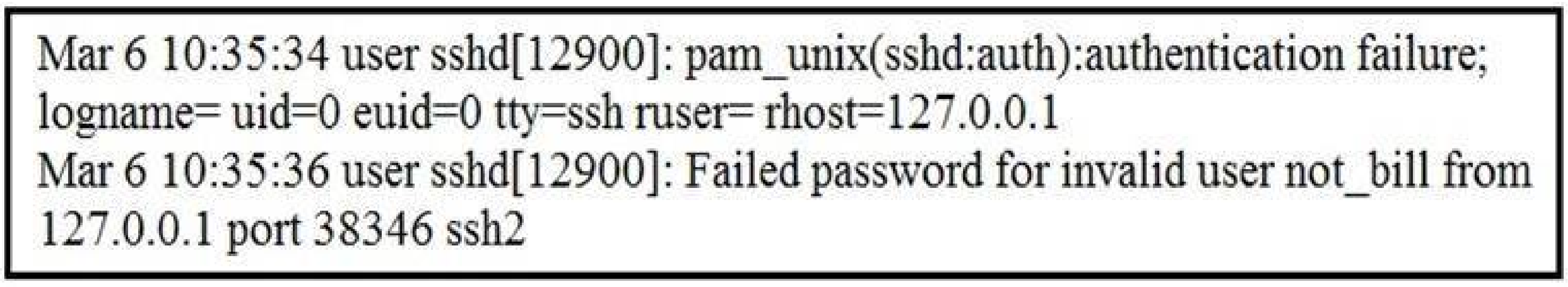
Answer: A

Explanation:



tcpdump	web content filtering
web content filtering	tcpdump
traditional stateful firewall	NetFlow
NetFlow	traditional stateful firewall

NEW QUESTION 5
Refer to the exhibit.



```
Mar 6 10:35:34 user sshd[12900]: pam_unix(sshd:auth):authentication failure;
logname= uid=0 euid=0 tty=ssh ruser= rhost=127.0.0.1
Mar 6 10:35:36 user sshd[12900]: Failed password for invalid user not_bill from
127.0.0.1 port 38346 ssh2
```

In which Linux log file is this output found?

A. /var/log/authorization.log
B. /var/log/dmesg
C. var/log/var.log
D. /var/log/auth.log

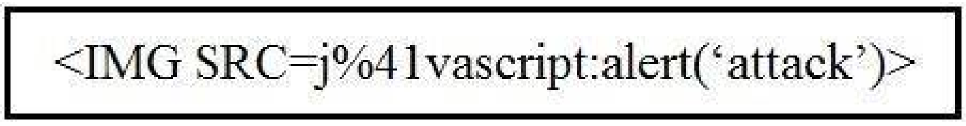
Answer: D

NEW QUESTION 6
Which piece of information is needed for attribution in an investigation?

A. proxy logs showing the source RFC 1918 IP addresses
B. RDP allowed from the Internet
C. known threat actor behavior
D. 802.1x RADIUS authentication pass arid fail logs

Answer: C

NEW QUESTION 7
Refer to the exhibit.



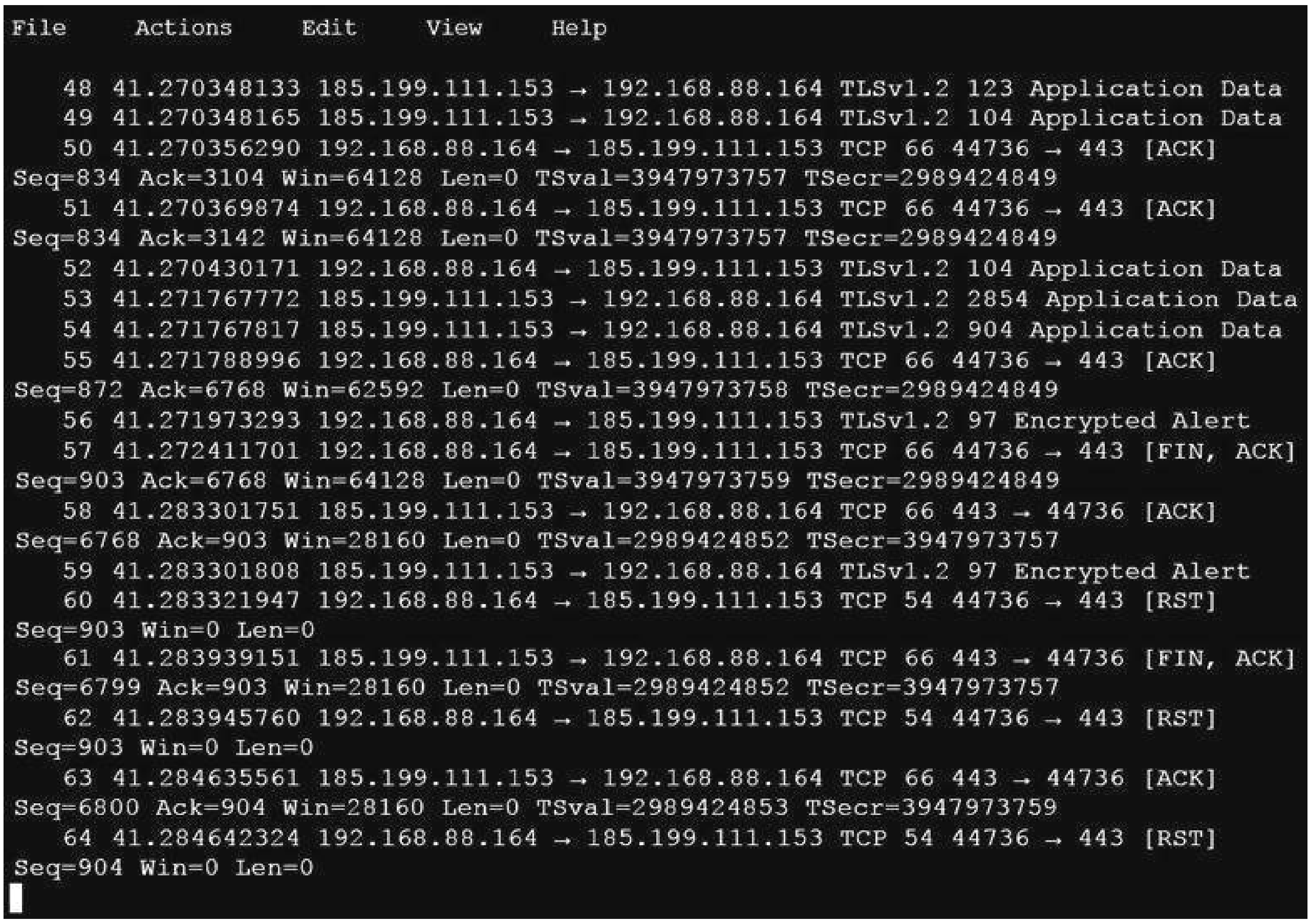
```
<IMG SRC=j%41vascript:alert('attack')>
```

Which kind of attack method is depicted in this string?

A. cross-site scripting
B. man-in-the-middle
C. SQL injection
D. denial of service

Answer: A

NEW QUESTION 8
An analyst is investigating a host in the network that appears to be communicating to a command and control server on the Internet. After collecting this packet capture the analyst cannot determine the technique and payload used for the communication.



```
    48 41.270348133 185.199.111.153 → 192.168.88.164 TLSv1.2 123 Application Data
    49 41.270348165 185.199.111.153 → 192.168.88.164 TLSv1.2 104 Application Data
    50 41.270356290 192.168.88.164 → 185.199.111.153 TCP 66 44736 → 443 [ACK]
Seq=834 Ack=3104 Win=64128 Len=0 TSval=3947973757 TSecr=2989424849
    51 41.270369874 192.168.88.164 → 185.199.111.153 TCP 66 44736 → 443 [ACK]
Seq=834 Ack=3142 Win=64128 Len=0 TSval=3947973757 TSecr=2989424849
    52 41.270430171 192.168.88.164 → 185.199.111.153 TLSv1.2 104 Application Data
    53 41.271767772 185.199.111.153 → 192.168.88.164 TLSv1.2 2854 Application Data
    54 41.271767817 185.199.111.153 → 192.168.88.164 TLSv1.2 904 Application Data
    55 41.271788996 192.168.88.164 → 185.199.111.153 TCP 66 44736 → 443 [ACK]
Seq=872 Ack=6768 Win=62592 Len=0 TSval=3947973758 TSecr=2989424849
    56 41.271973293 192.168.88.164 → 185.199.111.153 TLSv1.2 97 Encrypted Alert
    57 41.272411701 192.168.88.164 → 185.199.111.153 TCP 66 44736 → 443 [FIN, ACK]
Seq=903 Ack=6768 Win=64128 Len=0 TSval=3947973759 TSecr=2989424849
    58 41.283301751 185.199.111.153 → 192.168.88.164 TCP 66 443 → 44736 [ACK]
Seq=6768 Ack=903 Win=28160 Len=0 TSval=2989424852 TSecr=3947973757
    59 41.283301808 185.199.111.153 → 192.168.88.164 TLSv1.2 97 Encrypted Alert
    60 41.283321947 192.168.88.164 → 185.199.111.153 TCP 54 44736 → 443 [RST]
Seq=903 Win=0 Len=0
    61 41.283939151 185.199.111.153 → 192.168.88.164 TCP 66 443 → 44736 [FIN, ACK]
Seq=6799 Ack=903 Win=28160 Len=0 TSval=2989424852 TSecr=3947973757
    62 41.283945760 192.168.88.164 → 185.199.111.153 TCP 54 44736 → 443 [RST]
Seq=903 Win=0 Len=0
    63 41.284635561 185.199.111.153 → 192.168.88.164 TCP 66 443 → 44736 [ACK]
Seq=6800 Ack=904 Win=28160 Len=0 TSval=2989424853 TSecr=3947973759
    64 41.284642324 192.168.88.164 → 185.199.111.153 TCP 54 44736 → 443 [RST]
Seq=904 Win=0 Len=0
```

Which obfuscation technique is the attacker using?

A. Base64 encoding
B. transport layer security encryption
C. SHA-256 hashing
D. ROT13 encryption

Answer: B

NEW QUESTION 9
What specific type of analysis is assigning values to the scenario to see expected outcomes?

A. deterministic
B. exploratory
C. probabilistic
D. descriptive

Answer: A

NEW QUESTION 10
What is the practice of giving an employee access to only the resources needed to accomplish their job?

A. principle of least privilege
B. organizational separation
C. separation of duties
D. need to know principle

Answer: A

NEW QUESTION 10
What should a security analyst consider when comparing inline traffic interrogation with traffic tapping to determine which approach to use in the network?

A. Tapping interrogation replicates signals to a separate port for analyzing traffic
B. Tapping interrogations detect and block malicious traffic
C. Inline interrogation enables viewing a copy of traffic to ensure traffic is in compliance with security policies
D. Inline interrogation detects malicious traffic but does not block the traffic

Answer: A

NEW QUESTION 14
Which evasion technique is a function of ransomware?

A. extended sleep calls
B. encryption
C. resource exhaustion

D. encoding

Answer: B

NEW QUESTION 15
Which metric in CVSS indicates an attack that takes a destination bank account number and replaces it with a different bank account number?

A. integrity
B. confidentiality
C. availability
D. scope

Answer: A

NEW QUESTION 18
Which step in the incident response process researches an attacking host through logs in a SIEM?

A. detection and analysis
B. preparation
C. eradication
D. containment

Answer: A

NEW QUESTION 20
One of the objectives of information security is to protect the CIA of information and systems. What does CIA mean in this context?

A. confidentiality, identity, and authorization
B. confidentiality, integrity, and authorization
C. confidentiality, identity, and availability
D. confidentiality, integrity, and availability

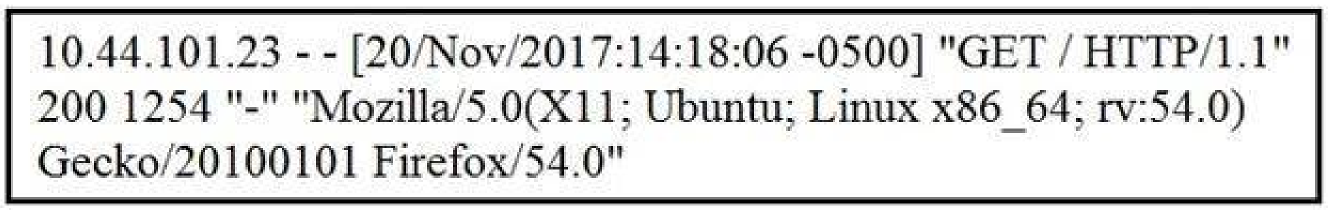
Answer: D

NEW QUESTION 22
A security specialist notices 100 HTTP GET and POST requests for multiple pages on the web servers. The agent in the requests contains PHP code that, if executed, creates and writes to a new PHP file on the webserver. Which event category is described?

A. reconnaissance
B. action on objectives
C. installation
D. exploitation

Answer: C

NEW QUESTION 24
Refer to the exhibit.



```
10.44.101.23 - - [20/Nov/2017:14:18:06 -0500] "GET / HTTP/1.1"
200 1254 "-" "Mozilla/5.0(X11; Ubuntu; Linux x86_64; rv:54.0)
Gecko/20100101 Firefox/54.0"
```

What does the message indicate?

A. an access attempt was made from the Mosaic web browser
B. a successful access attempt was made to retrieve the password file
C. a successful access attempt was made to retrieve the root of the website
D. a denied access attempt was made to retrieve the password file

Answer: C

NEW QUESTION 25
Which event artifact is used to identity HTTP GET requests for a specific file?

A. destination IP address
B. TCP ACK
C. HTTP status code
D. URI

Answer: D

NEW QUESTION 29
What is the virtual address space for a Windows process?

A. physical location of an object in memory
B. set of pages that reside in the physical memory
C. system-level memory protection feature built into the operating system
D. set of virtual memory addresses that can be used

Answer: D

NEW QUESTION 33
What do the Security Intelligence Events within the FMC allow an administrator to do?

A. See if a host is connecting to a known-bad domain.
B. Check for host-to-server traffic within your network.
C. View any malicious files that a host has downloaded.
D. Verify host-to-host traffic within your network.

Answer: A

NEW QUESTION 36
What makes HTTPS traffic difficult to monitor?

A. SSL interception
B. packet header size
C. signature detection time
D. encryption

Answer: D

NEW QUESTION 41
A security expert is working on a copy of the evidence, an ISO file that is saved in CDFS format. Which type of evidence is this file?

A. CD data copy prepared in Windows
B. CD data copy prepared in Mac-based system
C. CD data copy prepared in Linux system
D. CD data copy prepared in Android-based system

Answer: A

NEW QUESTION 46
A malicious file has been identified in a sandbox analysis tool.
Which piece of information is needed to search for additional downloads of this file by other hosts?

A. file type
B. file size
C. file name
D. file hash value

Answer: D

NEW QUESTION 49
An offline audit log contains the source IP address of a session suspected to have exploited a vulnerability resulting in system compromise.
Which kind of evidence is this IP address?

A. best evidence
B. corroborative evidence
C. indirect evidence
D. forensic evidence

Answer: B

NEW QUESTION 52
What is an example of social engineering attacks?

A. receiving an unexpected email from an unknown person with an uncharacteristic attachment from someone in the same company
B. receiving an email from human resources requesting a visit to their secure website to update contact information
C. sending a verbal request to an administrator who knows how to change an account password
D. receiving an invitation to the department’s weekly WebEx meeting

Answer: B

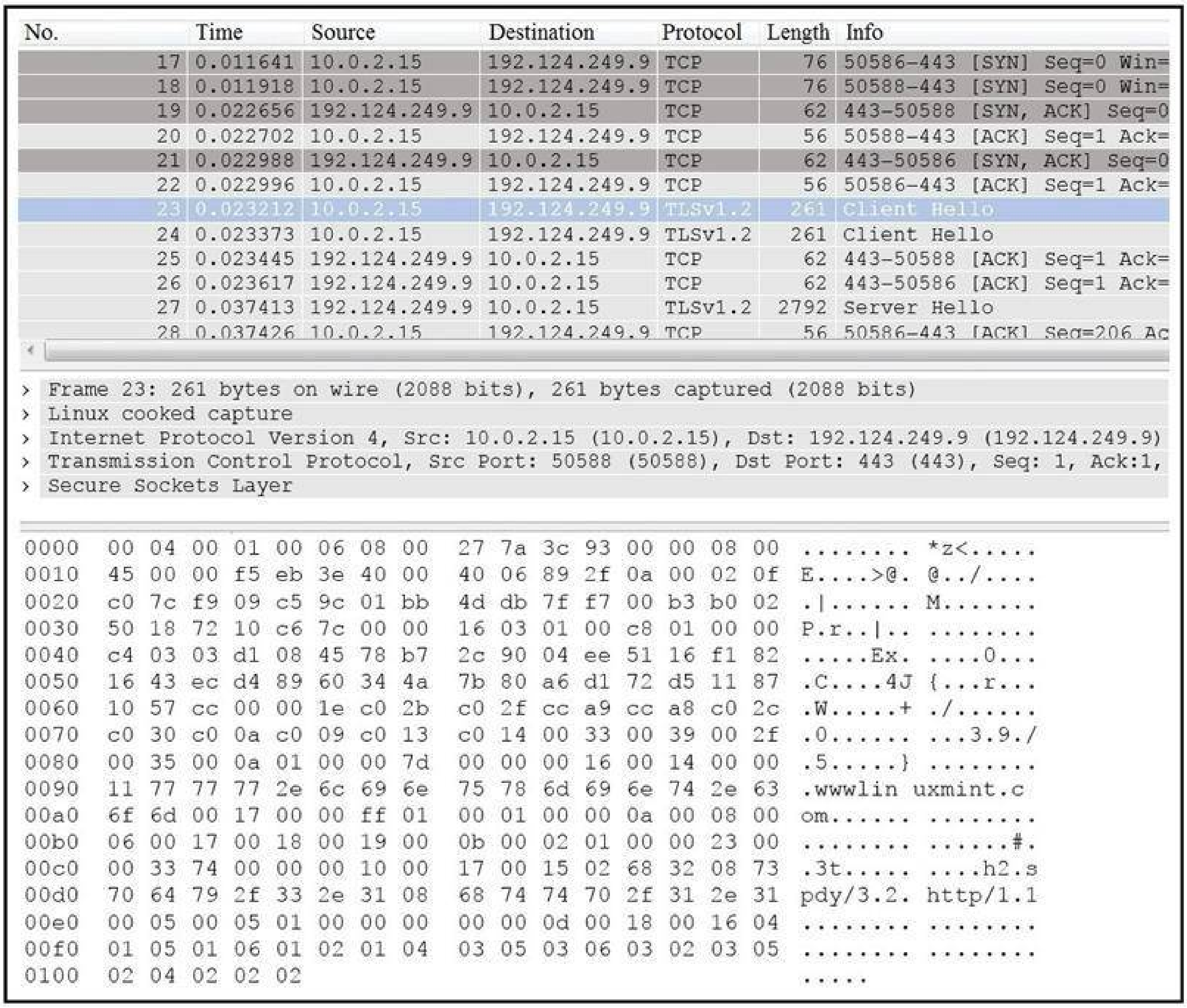
NEW QUESTION 54
Which event artifact is used to identify HTTP GET requests for a specific file?

A. destination IP address
B. URI
C. HTTP status code

D. TCP ACK

Answer: B

NEW QUESTION 56
Refer to the exhibit.

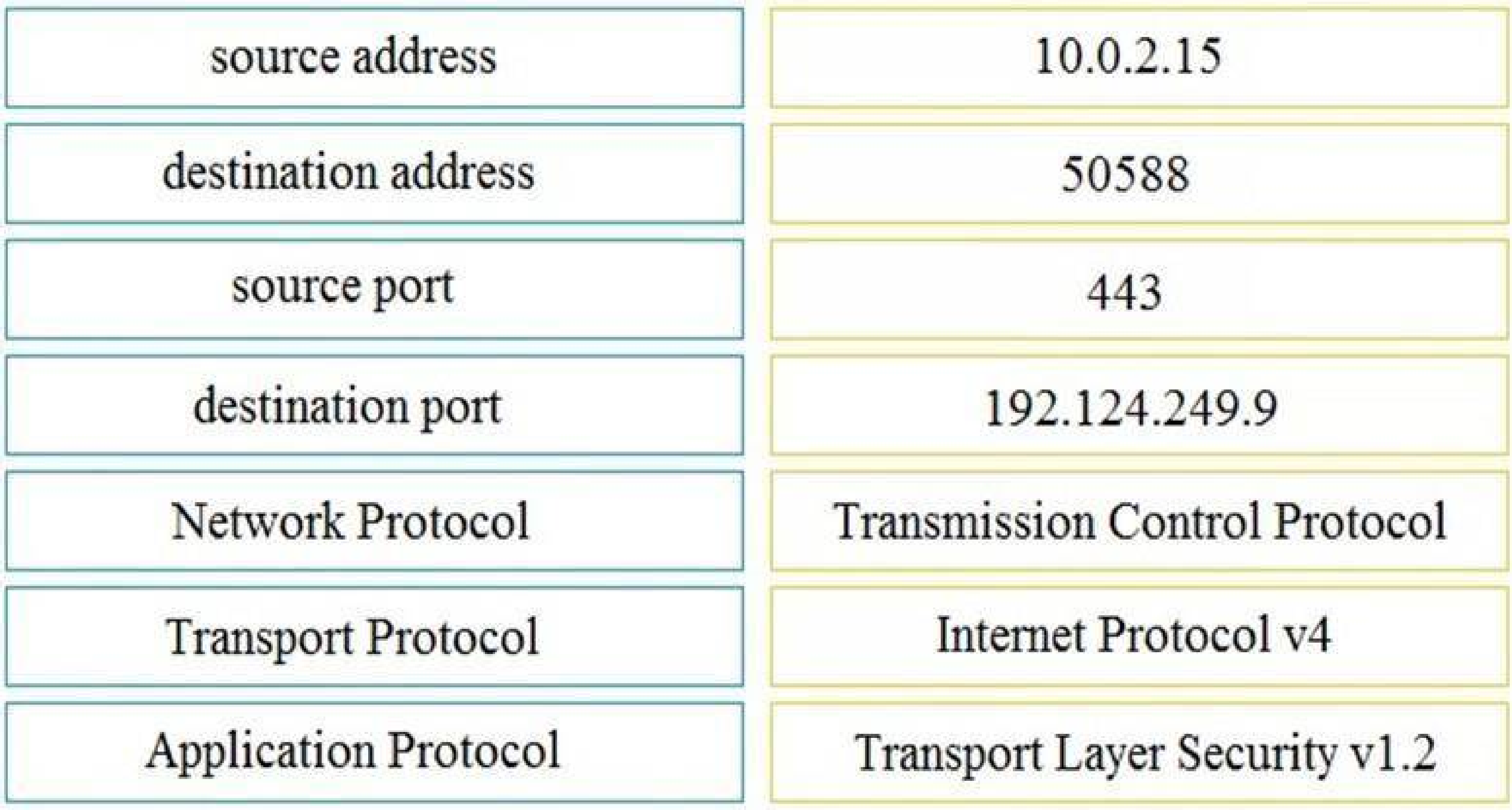


```
No.   Time      Source          Destination     Protocol  Length Info
   17 0.011641  10.0.2.15       192.124.249.9   TCP           76 50586-443 [SYN] Seq=0 Win=
   18 0.011918  10.0.2.15       192.124.249.9   TCP           76 50588-443 [SYN] Seq=0 Win=
   19 0.022656  192.124.249.9   10.0.2.15       TCP           62 443-50588 [SYN, ACK] Seq=0
   20 0.022702  10.0.2.15       192.124.249.9   TCP           56 50588-443 [ACK] Seq=1 Ack=
   21 0.022988  192.124.249.9   10.0.2.15       TCP           62 443-50586 [SYN, ACK] Seq=0
   22 0.022996  10.0.2.15       192.124.249.9   TCP           56 50586-443 [ACK] Seq=1 Ack=
   23 0.023212  10.0.2.15       192.124.249.9   TLSv1.2      261 Client Hello
   24 0.023373  10.0.2.15       192.124.249.9   TLSv1.2      261 Client Hello
   25 0.023445  192.124.249.9   10.0.2.15       TCP           62 443-50588 [ACK] Seq=1 Ack=
   26 0.023617  192.124.249.9   10.0.2.15       TCP           62 443-50586 [ACK] Seq=1 Ack=
   27 0.037413  192.124.249.9   10.0.2.15       TLSv1.2     2792 Server Hello
   28 0.037426  10.0.2.15       192.124.249.9   TCP           56 50586-443 [ACK] Seq=206 Ac

> Frame 23: 261 bytes on wire (2088 bits), 261 bytes captured (2088 bits)
> Linux cooked capture
> Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 192.124.249.9 (192.124.249.9)
> Transmission Control Protocol, Src Port: 50588 (50588), Dst Port: 443 (443), Seq: 1, Ack:1,
> Secure Sockets Layer

0000  00 04 00 01 00 06 08 00  27 7a 3c 93 00 00 08 00  ........ *z<.....
0010  45 00 00 f5 eb 3e 40 00  40 06 89 2f 0a 00 02 0f  E....>@. @../....
0020  c0 7c f9 09 c5 9c 01 bb  4d db 7f f7 00 b3 b0 02  .|...... M.......
0030  50 18 72 10 c6 7c 00 00  16 03 01 00 c8 01 00 00  P.r..|.. ........
0040  c4 03 03 d1 08 45 78 b7  2c 90 04 ee 51 16 f1 82  .....Ex. ....0...
0050  16 43 ec d4 89 60 34 4a  7b 80 a6 d1 72 d5 11 87  .C....4J {...r...
0060  10 57 cc 00 00 1e c0 2b  c0 2f cc a9 cc a8 c0 2c  .W.....+ ./......
0070  c0 30 c0 0a c0 09 c0 13  c0 14 00 33 00 39 00 2f  .0...... ...3.9./
0080  00 35 00 0a 01 00 00 7d  00 00 00 16 00 14 00 00  .5.....} ........
0090  11 77 77 77 2e 6c 69 6e  75 78 6d 69 6e 74 2e 63  .wwwlin uxmint.c
00a0  6f 6d 00 17 00 00 ff 01  00 01 00 00 0a 00 08 00  om...... ........
00b0  06 00 17 00 18 00 19 00  0b 00 02 01 00 00 23 00  ........ ......#.
00c0  00 33 74 00 00 00 10 00  17 00 15 02 68 32 08 73  .3t..... ....h2.s
00d0  70 64 79 2f 33 2e 31 08  68 74 74 70 2f 31 2e 31  pdy/3.2. http/1.1
00e0  00 05 00 05 01 00 00 00  00 00 0d 00 18 00 16 04  ........ ........
00f0  01 05 01 06 01 02 01 04  03 05 03 06 03 02 03 05  ........ ........
0100  02 04 02 02 02                                     .....
```

Drag and drop the element name from the left onto the correct piece of the PCAP file on the right.

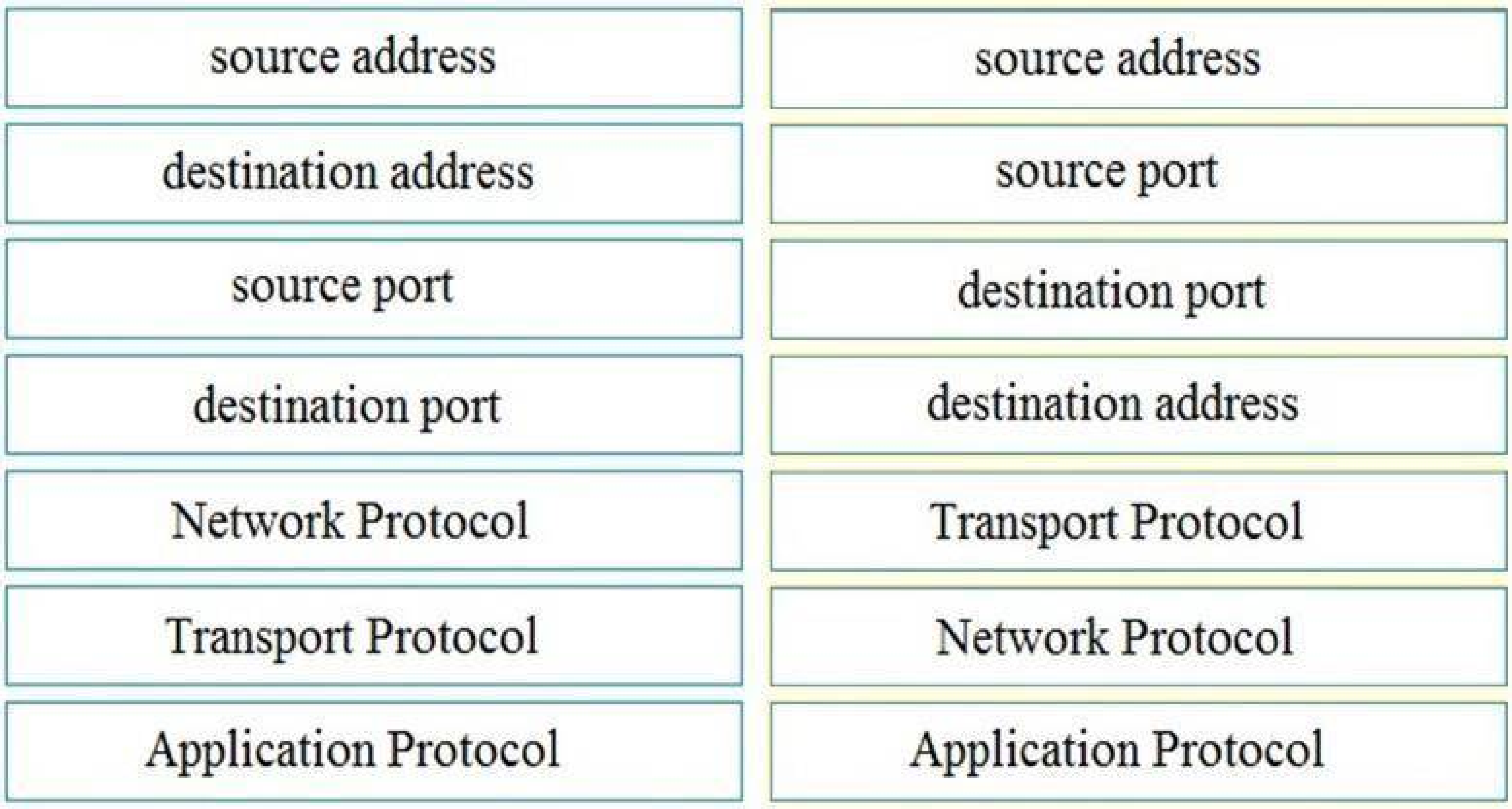


source address	10.0.2.15
destination address	50588
source port	443
destination port	192.124.249.9
Network Protocol	Transmission Control Protocol
Transport Protocol	Internet Protocol v4
Application Protocol	Transport Layer Security v1.2

A. Mastered
B. Not Mastered

Answer: A

Explanation:



source address	source address
destination address	source port
source port	destination port
destination port	destination address
Network Protocol	Transport Protocol
Transport Protocol	Network Protocol
Application Protocol	Application Protocol

NEW QUESTION 59
How is attacking a vulnerability categorized?

A. action on objectives
B. delivery
C. exploitation
D. installation

Answer: C

NEW QUESTION 60
An analyst is exploring the functionality of different operating systems.
What is a feature of Windows Management Instrumentation that must be considered when deciding on an operating system?

A. queries Linux devices that have Microsoft Services for Linux installed
B. deploys Windows Operating Systems in an automated fashion
C. is an efficient tool for working with Active Directory
D. has a Common Information Model, which describes installed hardware and software

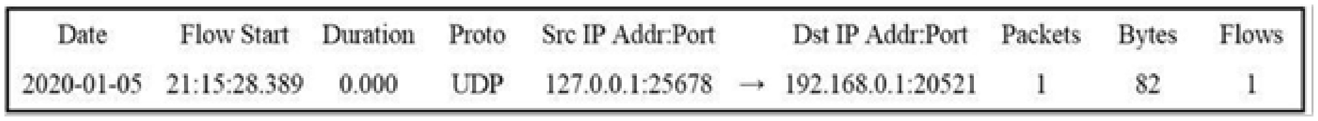
Answer: D

NEW QUESTION 64
At which layer is deep packet inspection investigated on a firewall?

A. internet
B. transport
C. application
D. data link

Answer: C

NEW QUESTION 68
Refer to the exhibit.



```
Date        Flow Start     Duration  Proto  Src IP Addr:Port       Dst IP Addr:Port    Packets  Bytes  Flows
2020-01-05  21:15:28.389   0.000     UDP    127.0.0.1:25678   →   192.168.0.1:20521   1        82     1
```

Which type of log is displayed?

A. proxy
B. NetFlow
C. IDS
D. sys

Answer: B

NEW QUESTION 70
Which two elements are used for profiling a network? (Choose two.)

A. session duration

B. total throughput
C. running processes
D. listening ports
E. OS fingerprint

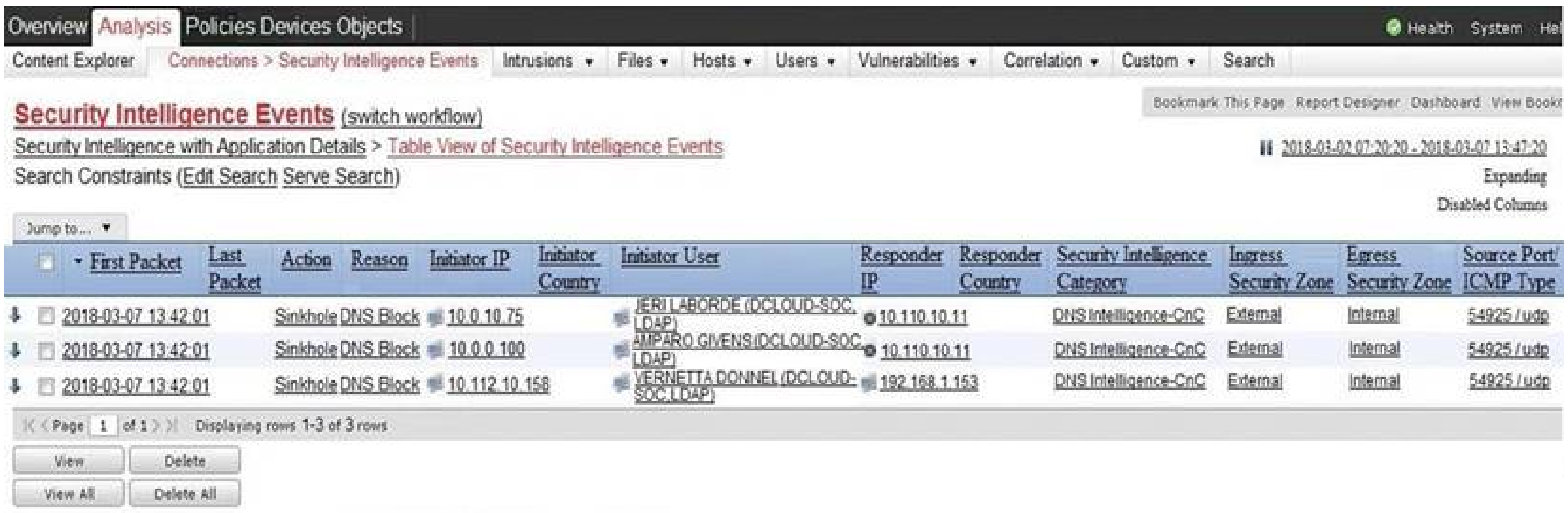
Answer: DE

NEW QUESTION 74
How is NetFlow different than traffic mirroring?

A. NetFlow collects metadata and traffic mirroring clones data
B. Traffic mirroring impacts switch performance and NetFlow does not
C. Traffic mirroring costs less to operate than NetFlow
D. NetFlow generates more data than traffic mirroring

Answer: A

NEW QUESTION 77
Refer to the exhibit.



Security Intelligence Events (switch workflow)
Security Intelligence with Application Details > Table View of Security Intelligence Events
Search Constraints (Edit Search Serve Search)

2018-03-02 07:20:20 - 2018-03-07 13:47:20
Expanding
Disabled Columns

	□	First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Initiator User	Responder IP	Responder Country	Security Intelligence Category	Ingress Security Zone	Egress Security Zone	Source Port/ ICMP Type
⬇	□	2018-03-07 13:42:01		Sinkhole	DNS Block	10.0.10.75		JERI LABORDE (DCLOUD-SOC, LDAP)	10.110.10.11		DNS Intelligence-CnC	External	Internal	54925 / udp
⬇	□	2018-03-07 13:42:01		Sinkhole	DNS Block	10.0.0.100		AMPARO GIVENS (DCLOUD-SOC, LDAP)	10.110.10.11		DNS Intelligence-CnC	External	Internal	54925 / udp
⬇	□	2018-03-07 13:42:01		Sinkhole	DNS Block	10.112.10.158		VERNETTA DONNEL (DCLOUD-SOC, LDAP)	192.168.1.153		DNS Intelligence-CnC	External	Internal	54925 / udp

|< < Page 1 of 1 > >| Displaying rows 1-3 of 3 rows

Which two elements in the table are parts of the 5-tuple? (Choose two.)

A. First Packet
B. Initiator User
C. Ingress Security Zone
D. Source Port
E. Initiator IP

Answer: DE

NEW QUESTION 82
......

Relate Links

100% Pass Your 200-201 Exam with Exambible Prep Materials

https://www.exambible.com/200-201-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/