

Exam Code: 1T6-511

Exam Name: Network Analysis & Troubleshooting

Vendor: Network General Corp

Version: DEMO

Part: A

1: To save a trace file as a compressed file from the Sniffer you must use the extension:

- A.CAP
- B.zip
- C.enc
- D.caz

Correct Answers: D

2: This is a screen from the Decode Summary window.

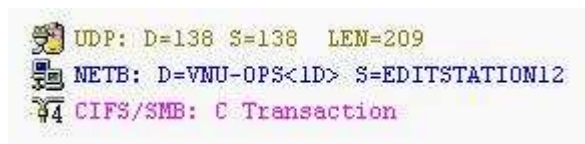
Source Address	Dest Address	Summary
001111195130	Broadcast	ARP: C PA=[192.168.0.26] PRO=IP
Dell 3BF149	001111195130	ARP: R PA=[192.168.0.26] HA=Dell 3BF149 PRO=IP
Cisco 32D494	Bridge_Group_Addr	BPDU: S: Pri=8000 Port=8022 Root: Pri=8000 Addr=00B06432D480 Cost=0
[192.168.0.1]	[192.168.0.26]	ICMP: Echo
[192.168.0.26]	[192.168.0.1]	ICMP: Echo reply
[192.168.0.1]	[192.168.0.26]	ICMP: Echo
[192.168.0.26]	[192.168.0.1]	ICMP: Echo reply

Which of the following statements is true for this capture?

- A.192.168.0.1 initiated a ping
- B.192.168.0.26 initiated a ping
- C.192.168.0.26 has a MAC address of 001111195130
- D.192.168.0.1 should not repeat the ICMP: Echo

Correct Answers: A

3: This is the Detail window for this question.



Which of the following statements is true for this Decode Detail window?

- A.One of the UDP ports should be ephemeral
- B.UDP is the Station layer protocol
- C.NETB is the Connection layer protocol
- D.UDP is the Transport layer protocol

Correct Answers: D

4: When troubleshooting a slow application, which of the following could be indicators of an application-specific problem?

- A.Commands with timely responses
- B.Large or full-size frames
- C.Long Delta times before each client request
- D.None of the above

Correct Answers: D

5: This is the Decode Hex window for this question.

```

00000000: 00 11 11 19 51 30 00 10 a4 b8 90 f5 08 00 45 00 ....Q0..x,08..E.
00000010: 00 64 bf a2 40 00 80 06 8b c2 c0 a8 00 02 42 62 .d;<@.€.<AA"..Bb
00000020: ac 22 3b b5 05 2e b7 8b 67 c7 46 94 2e 08 50 18 -";p...<gCF"..P.
00000030: 44 70 5b 3d 00 00 3b 30 20 4c 4f 47 49 4e 20 74 Dp[=...;0 LOGIN t
00000040: 65 63 68 73 75 70 70 74 32 20 71 77 65 72 74 79 echsuppt2 qwerty
00000050: 20 31 37 34 30 20 31 20 31 35 35 37 37 32 20 71 1740 1 155772 q
00000060: 77 65 72 74 79 62 61 62 65 20 64 69 6e 67 64 6f wertybabe dingdo
00000070: 6e 67 ng

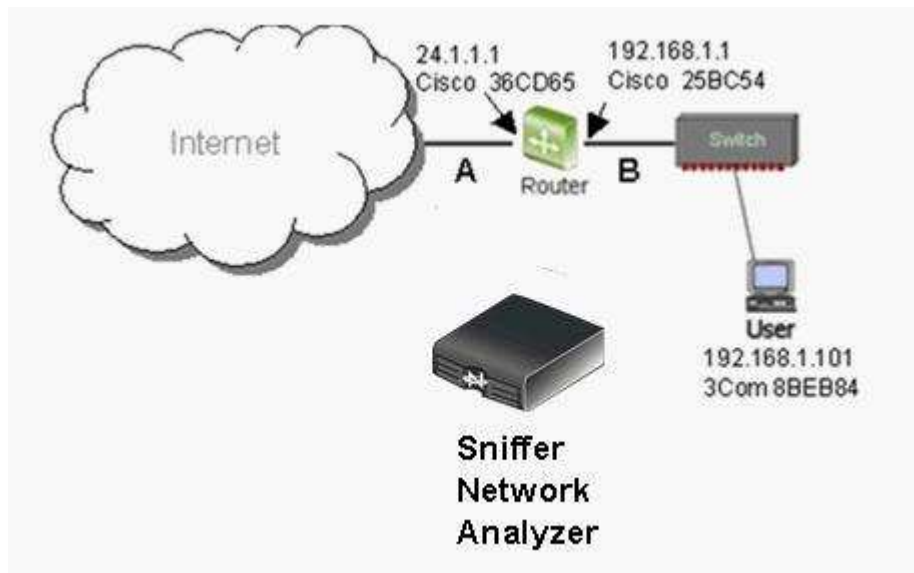
```

If you were going to create a Data Pattern filter on LOGIN it would be helpful to know that the letter is at offset _____.

- A.38
- B.39
- C.3A
- D.3B

Correct Answers: B

6: This is the network map.

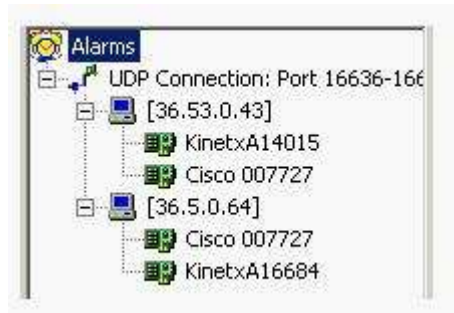


If a Sniffer Network Analyzer captured a frame at point A going from User to a server somewhere on the Internet, that frame would contain: (Choose all that apply.)

- A. An IP destination address of 24.1.1.1
- B. An IP destination address of the server
- C. A DLC destination address of Cisco 36CD65
- D. A DLC source address of Cisco 36CD65
- E. An IP source address of 192.168.1.101

Correct Answers: B D E

7: This is a screen from the Expert Objects detail.



Which of the following statements are true for this Object detail screen? (Choose all that apply.)

- A.This is the detail for a Duplicate IP Address alarm
- B.This is the detail for a Local Routing alarm
- C.KinetxA14015 is a robable Prouter
- D.This is the detail for a Window Exceeded alarm
- E.This is a connectionless Conversation

Correct Answers: B E

8: The only frame type that contains a DLC Ethertype field is:

- A.Novell Law frame
- B.Ethernet version two
- C.802.3 frame
- D.802.3 with SNAP

Correct Answers: B

9: Which of the following protocols are summarized when the Expert Overview pane and Station layer are selected?

- A.ARP, Ethernet, Cisco CDP
- B.ICMP, IP, IPX
- C.TCP, UDP
- D.NetBIOS, SMB

Correct Answers: B

10: Which of the following best describes the function of the Transport layer of the OSI Reference Model?

- A.Packet framing
- B.Reports upper-layer errors
- C.Connection management
- D.Manages user sessions

Correct Answers: C

11: OSI layer 4 is concerned with _____.

- A.ACKs and flow control working correctly
- B.Routing or frame delivery
- C.Connections working correctly
- D.Physical problems

Correct Answers: A

12: The OSI Transport layer corresponds to the Expert _____ layer.

- A.Data Link
- B.Connection
- C.Session
- D.Network

Correct Answers: B

13: Which of the following resources in the Sniffer is useful in identifying the endpoints in conversations in a captured trace?

- A.Expert DLC Layer Summary
- B.Pattern Match filter
- C.Matrix
- D.All of the above

Correct Answers: C

14: A sound troubleshooting methodology includes as part of the process a focus on finding imbalances or errors.

- A.TRUE
- B.FALSE

Correct Answers: A

15: Which of the following is recommended as part of the troubleshooting methodology?

- A.Use the Expert and Summary window first
- B.Use the Detail window first
- C.Use a top-down approach
- D.Use the Hex window first

Correct Answers: A

16: The interframe spacing in Fast Ethernet is _____.

- A.9.6 milliseconds
- B.96.0 nanoseconds
- C..96 microseconds
- D..96 milliseconds

Correct Answers: C

17: This is the Summary window for this question.

No.	Status	Source Address	Dest Address	Summary
29	[A]	[10.10.10.100]	[10.10.10.97]	TCP: D=80 S=4123 SYN SEQ=20653579 LEN=0 WIN=65535
30	[B]	[10.10.10.97]	[10.10.10.100]	TCP: D=4123 S=80 SYN ACK=20653580 SEQ=139386105 LEN=0 WIN=4128
31	[A]	[10.10.10.100]	[10.10.10.97]	TCP: D=80 S=4123 ACK=139386106 WIN=65535
32	[A]	[10.10.10.100]	[10.10.10.97]	HTTP: C Port=4123 GET /exec/show/device/portinfo/CR HTTP/1.1
33	[B]	[10.10.10.97]	[10.10.10.100]	HTTP: R Port=4123 HTTP/1.0 Status=Unauthorized
34	[A]	[10.10.10.100]	[10.10.10.97]	TCP: D=80 S=4123 FIN ACK=139386444 SEQ=20653754 LEN=0 WIN=65197
35	[A]	[10.10.10.100]	[10.10.10.97]	TCP: D=80 S=4124 SYN SEQ=20653603 LEN=0 WIN=65535
36	[B]	[10.10.10.97]	[10.10.10.100]	TCP: D=4123 S=80 ACK=20653755 WIN=3954
37	[B]	[10.10.10.97]	[10.10.10.100]	TCP: D=4124 S=80 SYN ACK=20653604 SEQ=3744768563 LEN=0 WIN=4128
38	[A]	[10.10.10.100]	[10.10.10.97]	TCP: D=80 S=4124 ACK=3744768564 WIN=65535
39	[A]	[10.10.10.100]	[10.10.10.97]	HTTP: C Port=4124 GET /exec/show/device/portinfo/CR HTTP/1.1
40	[B]	[10.10.10.97]	[10.10.10.100]	TCP: D=4123 S=80 FIN ACK=20653755 SEQ=139386444 LEN=0 WIN=3954
41	[A]	[10.10.10.100]	[10.10.10.97]	TCP: D=80 S=4123 ACK=139386445 WIN=65197
42	[B]	[10.10.10.97]	[10.10.10.100]	TCP: D=4124 S=80 ACK=20653825 WIN=3907

Which frames are part of the session close process in this example? (Choose all that apply.)

A.34

B.36

C.38

D.40

E.41

Correct Answers: A B D E

18: In the Sniffer Expert interface, the Service layer objects relate to which layer of the OSI reference model?

A.Application layer

B.Presentation layer

C.Session layer

D.Transport layer

Correct Answers: A

19: This is the Summary window for this question.

No.	Status	Source Address	Dest Address	Summary	Delta Time
28		[192.168.0.1]	[192.168.0.26]	Telnet: C PORT=3043 IAC Won't Echo	0.000.413
29		[192.168.0.26]	[192.168.0.1]	Telnet: R PORT=3043 login:	0.000.246
30		[192.168.0.1]	[192.168.0.26]	Telnet: C PORT=3043 IAC Do Echo	0.000.061
31		[192.168.0.26]	[192.168.0.1]	TCP: D=3043 S=23 ACK=3877413358 WIN=	0.037.679
32		[192.168.0.1]	[192.168.0.26]	Telnet: C PORT=3043 u	1.226.999
33		[192.168.0.26]	[192.168.0.1]	TCP: D=3043 S=23 ACK=3877413359 WIN=	0.000.262
34		[192.168.0.26]	[192.168.0.1]	Telnet: R PORT=3043 u	0.000.279
35		[192.168.0.1]	[192.168.0.26]	Telnet: C PORT=3043 s	0.093.591
36		[192.168.0.26]	[192.168.0.1]	Telnet: R PORT=3043 s	0.000.434
37		[192.168.0.1]	[192.168.0.26]	Telnet: C PORT=3043 e	0.090.477
38		[192.168.0.26]	[192.168.0.1]	Telnet: R PORT=3043 e	0.000.532
39		[192.168.0.1]	[192.168.0.26]	Telnet: C PORT=3043 r	0.060.970
40		[192.168.0.26]	[192.168.0.1]	Telnet: R PORT=3043 r	0.000.432
41		[192.168.0.1]	[192.168.0.26]	TCP: D=23 S=3043 ACK=15813354 WIN=17	0.116.841
42		[192.168.0.1]	[192.168.0.26]	Telnet: C PORT=3043 2	0.725.625
43		[192.168.0.26]	[192.168.0.1]	Telnet: R PORT=3043 2	0.000.517
44		[192.168.0.1]	[192.168.0.26]	TCP: D=23 S=3043 ACK=15813355 WIN=17	0.179.068
45		[192.168.0.1]	[192.168.0.26]	Telnet: C PORT=3043 <OD>	1.439.456
46		[192.168.0.26]	[192.168.0.1]	Telnet: R PORT=3043 <OD0A>	0.000.529
47		[192.168.0.1]	[192.168.0.26]	TCP: D=23 S=3043 ACK=15813357 WIN=17	0.169.318
48		[192.168.0.26]	[192.168.0.1]	Telnet: R PORT=3043 Password:	0.000.268
49		[192.168.0.1]	[192.168.0.26]	TCP: D=23 S=3043 ACK=15813367 WIN=17	0.200.892
50		[192.168.0.1]	[192.168.0.26]	Telnet: C PORT=3043 p	1.061.153

Examine this capture closely. Which statement is true?

A.This appears to be a normal Telnet session

- B.Telnet is a session layer protocol
- C.The delta times in frames 32, 45, and 50 would warrant investigation
- D.None of the above

Correct Answers: A

20: This is the Summary window for this question.

No.	S	Source Address	Dest Address	Summary	Delta Time
28		[192.168.0.1]	[192.168.0.26]	Telnet: C PORT=3043 IAC Won't Echo	0.000.413
29		[192.168.0.26]	[192.168.0.1]	Telnet: R PORT=3043 login:	0.000.246
30		[192.168.0.1]	[192.168.0.26]	Telnet: C PORT=3043 IAC Do Echo	0.000.061
31		[192.168.0.26]	[192.168.0.1]	TCP: D=3043 S=23 ACK=3877413358 WIN=	0.037.679
32		[192.168.0.1]	[192.168.0.26]	Telnet: C PORT=3043 u	1.226.999
33		[192.168.0.26]	[192.168.0.1]	TCP: D=3043 S=23 ACK=3877413359 WIN=	0.000.262
34		[192.168.0.26]	[192.168.0.1]	Telnet: R PORT=3043 u	0.000.279
35		[192.168.0.1]	[192.168.0.26]	Telnet: C PORT=3043 s	0.093.591
36		[192.168.0.26]	[192.168.0.1]	Telnet: R PORT=3043 s	0.000.434
37		[192.168.0.1]	[192.168.0.26]	Telnet: C PORT=3043 e	0.090.477
38		[192.168.0.26]	[192.168.0.1]	Telnet: R PORT=3043 e	0.000.532
39		[192.168.0.1]	[192.168.0.26]	Telnet: C PORT=3043 r	0.060.970
40		[192.168.0.26]	[192.168.0.1]	Telnet: R PORT=3043 r	0.000.432
41		[192.168.0.1]	[192.168.0.26]	TCP: D=23 S=3043 ACK=15813354 WIN=17	0.116.841
42		[192.168.0.1]	[192.168.0.26]	Telnet: C PORT=3043 2	0.725.625
43		[192.168.0.26]	[192.168.0.1]	Telnet: R PORT=3043 2	0.000.517
44		[192.168.0.1]	[192.168.0.26]	TCP: D=23 S=3043 ACK=15813355 WIN=17	0.179.068
45		[192.168.0.1]	[192.168.0.26]	Telnet: C PORT=3043 <OD>	1.439.456
46		[192.168.0.26]	[192.168.0.1]	Telnet: R PORT=3043 <OD0A>	0.000.529
47		[192.168.0.1]	[192.168.0.26]	TCP: D=23 S=3043 ACK=15813357 WIN=17	0.169.318
48		[192.168.0.26]	[192.168.0.1]	Telnet: R PORT=3043 Password:	0.000.268
49		[192.168.0.1]	[192.168.0.26]	TCP: D=23 S=3043 ACK=15813367 WIN=17	0.200.892
50		[192.168.0.1]	[192.168.0.26]	Telnet: C PORT=3043 p	1.061.153

Examine this capture closely. Expert display is disabled. Which statement is true?

- A.Telnet is a session layer protocol
- B.The user at 192.168.0.1 would complain of slow response
- C.The delta times in frames 32, 45, and 50 would warrant investigation
- D.None of the above

Correct Answers: D