Lesson 9
Computer Forensics

CASE STUDY

All things were made through him, and without him was not any thing made that was made (John 1:3).

Terms to Know

Ad clicking – hackers display advertisements that may entice the user to click on an ad and open malware.

Keylogging – hackers record the user's keystrokes to decipher passwords, etc.

Phishing – an email disguised as professional in which the user is requested to provide passwords, address, telephone number, etc.

Ransomware – hackers access computer files and lock the user out, often demanding ransom to regain access.

Screenshot managing – hackers access the user's screen and take screenshots of passwords, etc.

Webcam managing – hackers hijack the user's webcam in hopes of watching the user's keystrokes for passwords, conversations, and other data.

Application – refers to individual authorization within a single application or service.

Computer network – a group of computers, using similar protocols, that are connected to one another for the purpose of communicating data electronically.

Endpoint – the breaking down of a network into individual systems.

Firewall – prevents unauthorized access to specific devices, such as hardware or software, and protects from people trying to get into the computer system. Based upon a set of security rules, a firewall will either allow traffic to access or block information on a computer or network.

Virtual Private Network (VPN) – a type of network security that, when used to connect to the internet, encrypts your request and masks your location.

Case Study

Teacher: Review the case study and discuss it with your student. Be sure to address any notes the student took, as well as sensitive or difficult topics you want to talk through with your student. The topic of this case is a computer worm.

Student: Review the case study. You can use this page to take notes on anything from the case that you have questions or concerns about. Discuss your thoughts with your teacher.

Notes

Multiple Choice

Circle the best answer from the choices below.

1. What is computer forensics also known as?
   a. Cybercrime
   b. Cyber sleuthing
   c. Internet investigation
   d. Online crime analysis
   e. None of the above

2. Just as a computer requires a(n) _____, creation requires a(n) _____.
   a. Inventor, Designer
   b. Designer, Author
   c. Programmer, Creator
   d. Programmer, Inventor
   e. Inventor, Creator

3. What two symbols does binary code use?
   a. *Laghu* and *guru*
   b. 0's and 1's
   c. Light and heavy
   d. + and –
   e. All of the above
   f. None of the above

Matching

Mark the letter in front of the best answer.

a. Charles Babbage b. Ada Lovelace c. Pingala d. Gottfried Leibniz

1. _____ Developed a binary numeral system using light (*laghu*) and heavy (*guru*)
2. _____ Formalized binary logic in the 1700s
3. _____ Considered the father of computers
4. _____ The first computer programmer

Short Answer

Respond to the following questions in complete sentences.

1. Give two examples of technology in the Bible and their scriptural reference.

   a. _____

   _____

   _____

   b. _____

   _____

   _____

2. What are algorithms? What do they serve as?

   a. _____

   _____

   _____

   b. _____

   _____

   _____

3. What two early computing machines did Charles Babbage invent and in what years?

   a. _____

   _____

   _____

   b. _____

   _____

   _____

Multiple Choice

Circle the best answer from the choices below.

1. What are the three main components every computer consists of?
   a. Control bus, Microsoft Word, and hard drive
   b. CPU, RAM, and control bus
   c. Hard drive, RAM, and control bus
   d. RAM, CPU, and internet browser
   e. Internet browser, NIC, and CPU
   f. None of the above

2. What term is associated with erasing data on computer systems? (There is more than one answer.)
   a. Wiping (deep formatting)
   b. Smudging
   c. Dusting
   d. Erasing
   e. Shredding
   f. Reformatting
   g. Reprogramming

3. Traces of data that remain on a system is called:
   a. Dark data
   b. Residual data
   c. Lost data
   d. Invisible data
   e. Chalkboard data

Abbreviations

Write out the full title of each abbreviation below.

1. CPU: _____
2. RAM: _____
3. NIC: _____
4. OS: _____

Short Answer

Respond to the following questions in complete sentences.

1. Define hardware and software and provide two examples of each.

   a. _____

   _____

   b. _____

   _____

2. Provide an example of how the operating system allows the application software to talk to the hardware other than the one given in the lesson.

   _____

   _____

   _____

   _____

   _____

3. What is format?

   _____

   _____

   _____

   _____

   _____

4. What records data on the hard drive when it is formatted?

   _____

   _____

   _____

   _____

   _____

Read from page 104 to the heading "Security" on page 106.

Multiple Choice

Circle the best answer from the choices below.

1. In what year did Tim Berners-Lee introduce the world to the internet?
   a. 1961
   b. 1970
   c. 1991
   d. 1992
   e. None of the above

2. What is the primary challenge for a computer forensic investigator regarding email correspondence?
   a. The lack of cache
   b. The lack of encryption
   c. The lack of sender/receiver identification
   d. All of the above
   e. None of the above

3. Servers are described as virtual filing cabinets. What important functions do servers provide?
   a. Storage
   b. Collaboration
   c. Information delivery
   d. Electronic surveillance
   e. All of the above
   f. None of the above

Fill-in-the-Blank

Fill in the blanks with the correct answer.

1. A(n) _____ address is an address that points to a location on the internet.
2. _____ history is a record of the website addresses that the computer has recently visited and any data associated with the websites.
3. _____ is temporary storage that retains information about browser history, frequently visited sites, and search terms.

Short Answer

Respond to the following questions in complete sentences.

1. What are cookies, as related to the internet? Provide an example.

2. A computer forensic investigator will conduct a thorough examination of all activity on the computer. In what areas will the investigator search?

3. Why is it never wise to insert a USB drive from an unknown source into a personal computer?

Multiple Choice

Circle the best answer from the choices below.

1. What do firewalls do?
   a. Prevent unauthorized access to specific devices
   b. Protect from people trying to get into the computer system
   c. Allow traffic to access or block information on a computer or network
   d. All of the above
   e. None of the above

2. For a computer forensic investigator to search for information related to a case on a computer, what steps apply? (There is more than one answer.)
   a. Obtain a search warrant for the computer
   b. Obtain a search warrant for the individual files
   c. Immediately download all files onto the investigator's personal computer for analysis
   d. No chain of custody is required, the search warrant covers this requirement
   e. Secure the computer from unauthorized access
   f. No search warrant is needed

Matching

Mark the letter in front of the best answer.

a. Ransomware	b. Screenshot managing	c. Ad clicking
d. Keylogging	e. Phishing	f. Webcam managing

1. _____ Hackers access the user's screen and take screenshots of passwords, etc.
2. _____ Hackers display advertisements that may entice the user to click on an ad and open malware
3. _____ Hackers access computer files and lock the user out, often demanding ransom to regain access
4. _____ An email disguised as professional in which the user is requested to provide passwords, address, telephone number, etc.
5. _____ Hackers hijack the user's webcam in hopes of watching the user's keystrokes for passwords, conversations, and other data
6. _____ Hackers record the user's keystrokes to decipher passwords, etc.

Short Answer

Respond to the following questions in complete sentences.

1. What are the six categories that human cybercrime falls into?

   a. _____

   b. _____

   c. _____

   d. _____

   e. _____

   f. _____

2. What are AF tools?

   _____

   _____

   _____

   _____

   _____

   _____

3. What are the four goals of AF tools?

   a. _____

   b. _____

   c. _____

   d. _____

4. What does a conviction in a criminal computer forensic investigation result in? What about in a civil court case?

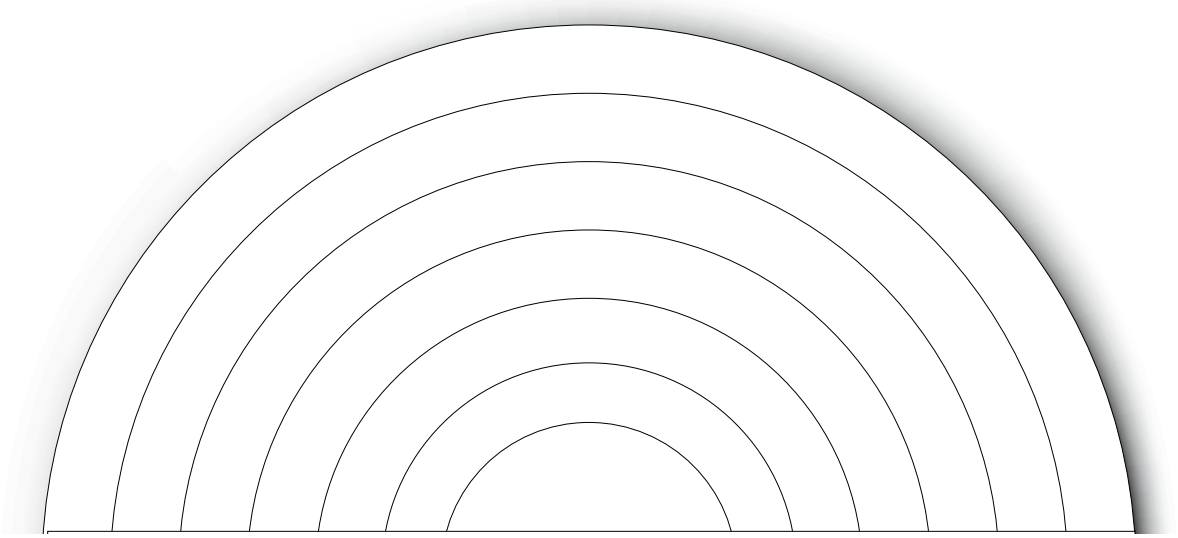
   a. _____

   _____

   b. _____

   _____

1. Label the seven layers of cybersecurity on the diagram below.



2. Explain why humans are identified as the number one key to protection of information.

_____

_____

_____

_____

_____

3. Fill in the chart below of the basic differences between hardware and software.

	Hardware	Software
Types		
Function		
Examples		
Nature		

Take time to study Lessons 5–9 for the Unit 3 Test.

Encoding and Decoding Data

Note: Cyber criminals use many ways to reach your data. They use simple to complex approaches to find and translate that data to something meaningful and potentially use it against you.

Encoding is a process of converting readable text data from one form to another form. Decoding is reverting the form back to its original text data. While encoding and decoding are similar to encryption and decryption, their intent is different. While encryption and decryption are used to obfuscate or hide the data from the user, encoding and decoding are used for data transmissions, compression, and storage, and are easily translatable. For this exercise, the student will decode a series of messages from binary to ASCII (and ultimately to characters). Interpret the results and come to a conclusion. Then the student will create an encoded message.

Note: Never send sensitive data in email, text, and social media. This includes date of birth and social security numbers. While many social media and financial banks claim that they are safe, there is always a flaw in security.

Terminology

The following is a brief terminology list to help you with the exercise:

- Bit – a 0 or 1 value.
- Byte – a sequence of zeros or ones with the length of eight bits.
- Register – the storage width of the byte's representation. For our examples, we are using 7-byte-width registers with padding to separate the bytes.
- Padding – used for clarity of byte representation and is not required.

```
01001101 01101001 01100011 01101000 01100001 01100101 01101100
```

Exercise – Decoding

Convert the following encoded binary messages to ASCII using the Simple Binary ASCII Table Reference on page 129.

Note: Cyber criminals are able to decipher many messages that they are able to capture. Sometimes they can use that information against you.

1.

```
01001101 01101001 01100011 01101000 01100001 01100101 01101100 00100000 01010011 01110100
01100101 01110000 01101000 01101001 01101110 01100111 01101000 01101111 01110101 01110011
01100101 00100000 01101100 01101001 01110110 01100101 01110011 00100000 01101001 01101110
00100000 00110010 00110101 00110110 00110010 00100000 01010111 01100101 01110011 01110100
01101001 01101110 01100111 01100110 01101001 01101100 01101100 00100000 01001100 01101110
00101110 00100000 01000011 01100001 01110010 01110100 01100101 01110010 00101100 00100000
01001101 01010011 00100000 00110010 00110011 00110100 00110101 00110110
```

2.

01001101 01101001 01100011 01101000 01100001 01100101 01101100 00100000 01010011 01110100
01100101 01110000 01101000 01101001 01101110 01100111 01101000 01101111 01110101 01110011
01100101 00100000 01101001 01110011 00100000 01101111 01101110 00100000 01110110 01100001
01100011 01100001 01110100 01101001 01101111 01101110

3.

01001101 01101001 01100011 01101000 01100001 01100101 01101100 00100000 01010011 01110100
01100101 01110000 01101000 01101001 01101110 01100111 01101000 01101111 01110101 01110011
01100101 00100000 01101001 01110011 00100000 01110011 01101001 01101110 01100111 01101100
01100101 00100000 01100001 01101110 01100100 00100000 01101100 01101001 01110110 01100101
01110011 00100000 01100001 01101100 01101111 01101110 01100101

4. What would a cyber criminal be able to ascertain if they are able to obtain and decode these messages?

_____

_____

_____

_____

_____

_____

_____

5. Bonus: Encode the words "Don't be a cyber target" in binary.

_____

_____

_____

_____

_____

_____

_____

Simple Binary ASCII Table Reference

Char	Ascii	Binary	Char	Ascii	Binary	Char	Ascii	Binary
	chr(27)	0100111	F	chr(70)	1000110	c	chr(99)	1100011
*	chr(42)	0101010	G	chr(71)	1000111	d	chr(100)	1100100
+	chr(43)	0101011	H	chr(72)	1001000	e	chr(101)	1100101
,	chr(44)	0101100	I	chr(73)	1001001	f	chr(102)	1100110
-	chr(45)	0101101	J	chr(74)	1001010	g	chr(103)	1100111
.	chr(46)	0101110	K	chr(75)	1001011	h	chr(104)	1101000
/	chr(47)	0101111	L	chr(76)	1001100	i	chr(105)	1101001
0	chr(48)	0110000	M	chr(77)	1001101	j	chr(106)	1101010
1	chr(49)	0110001	N	chr(78)	1001110	k	chr(107)	1101011
2	chr(50)	0110010	O	chr(79)	1001111	l	chr(108)	1101100
3	chr(51)	0110011	P	chr(80)	1010000	m	chr(109)	1101101
4	chr(52)	0110100	Q	chr(81)	1010001	n	chr(110)	1101110
5	chr(53)	0110101	R	chr(82)	1010010	o	chr(111)	1101111
6	chr(54)	0110110	S	chr(83)	1010011	p	chr(112)	1110000
7	chr(55)	0110111	T	chr(84)	1010100	q	chr(113)	1110001
8	chr(56)	0111000	U	chr(85)	1010101	r	chr(114)	1110010
9	chr(57)	0111001	V	chr(86)	1010110	s	chr(115)	1110011
:	chr(58)	0111010	W	chr(87)	1010111	t	chr(116)	1110100
;	chr(59)	0111011	X	chr(88)	1011000	u	chr(117)	1110101
@	chr(64)	1000000	Y	chr(89)	1011001	v	chr(118)	1110110
A	chr(65)	1000001	Z	chr(90)	1011010	w	chr(119)	1110111
B	chr(66)	1000010	`	chr(96)	1100000	x	chr(120)	1111000
C	chr(67)	1000011	a	chr(97)	1100001	y	chr(121)	1111001
D	chr(68)	1000100	b	chr(98)	1100010	z	chr(122)	1111010
E	chr(69)	1000101						