UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS AMERICA, INC.,

Petitioner,

v.

UNILOC LUXEMBOURG S.A.,
Patent Owner.

Case IPR2017-01801
United States Patent No. 8,995,433

DECLARATION OF WILLIAM C. EASTTOM II

TABLE OF CONTENTS

I, Chuck Easttom, hereby declare as follows:

I. INTRODUCTION

1. My name is William Charles Easttom II ("Chuck Easttom"). Uniloc Luxembourg S.A. ("Uniloc" or the "Patent Owner") retained me to provide my expert opinions regarding United States Patent No. 8,995,433 (the "'433 Patent").

2. From 2003 to 2013, I taught professional development courses to IT professionals in programming (C, Java, C++, and C#), web development (HTML, JavaScript, CSS, and .net), networking, and network security at Collin College, McKinney, TX. From 2000 to 2003, I was Department Chair for Computer Information Systems at Remington College, in Garland, TX. I have been a software engineer at Alegis Corporation Systems Group and a programmer at Boeing Aerospace Operations.

3. The Patent Owner asked me to study Claims 1-5, 7-12, 14-17, 25, and 26 (the "challenged claims") of the '433 Patent ("EX1001") to determine whether a person having ordinary skill in the technical art most pertinent to the art of the challenged claims at the time of the priority date for the '433 Patent (hereafter a "PHOSITA") would have considered those claim obvious in light of the asserted references considered as a whole.

4. I reviewed the ’433 Patent, its prosecution file wrapper, the state of the art at the time the application was filed, the references asserted by Samsung, Samsung’s Petition IPR2017-1801 (“Petition”), the Declaration of Dr. Haas (EX1002) in support of the Petition, the references relied upon in the Petition (including *Zydney* and *Griffin*) and the Declaration of Dr. Val DiEuliis from IPR2017-01428 in support of the Patent Owner. IPR2017-01428 also involved a challenge to the ’433 Patent based on *Zydney*. I also determined the scope and content of the prior art, ascertained the differences between the challenged claims of the ’433 Patent and the prior art, and determined the level of ordinary skill in the art most pertinent to the claimed technology. All the opinions I express here are my own.

5. Based on the above, and my familiarity with those having ordinary skill in the art at the time the application was filed, and my decades of experience in the field of computer science including communications systems, I concluded that none of the challenged claims would have been obvious in light of the arguments and references relied upon in the Petition.

6. The Patent Owner compensates me at my standard consulting rate of $300 per hour. Patent Owner also reimburses my reasonable expenses necessary to this work. I have no financial interest in Patent Owner, and my

compensation is not contingent upon the results of my study or the substance of my opinions.

II. MY BACKGROUND AND QUALIFICATIONS

7. I have worked in the computer industry for over 25 years. During that time, I have had extensive experience with network communications systems. I hold 42 industry certifications, which include certifications in network communications. I have authored 24 computer science books, several of those deal with network communications topics. I am a named inventor on thirteen United States patents:

- ✓ United States Patent No. 9,755,887, entitled "Managing a Network Element Operating on a Network", issued Sep. 5, 2017, assigned to Open Invention Network LLC.
- ✓ United States Patent No. 9,754,108, entitled "Method and Apparatus of Performing Data Executable Integrity Verification", issued Sep. 5, 2017, assigned to Open Invention Network LLC.
- ✓ United States Patent No. 9,753,957, entitled "System and Method for Document Tracking", issued Sep. 5, 2017, assigned to Open Invention Network LLC.

- ✓ United States Patent No. 9,686,227, entitled “Domain Name Service Based Remote Programming Objects”, issued Jun. 20, 2017, assigned to Open Invention Network LLC.
- ✓ United States Patent No. 9,619,656, entitled “Method and Apparatus of Performing Distributed Steganography of a Data Message”, issued Apr. 11, 2017, assigned to Open Invention Network LLC.
- ✓ United States Patent No. 9,405,907, entitled “Method and Apparatus of Performing Data Executable Integrity Verification”, issued Aug. 2, 2016, assigned to Open Invention Network LLC.
- ✓ United States Patent No. 9,313,167, entitled “Domain Name Service Based Remote Programming Objects”, issued Apr. 12, 2016, assigned to Open Invention Network LLC.
- ✓ United States Patent No. 8,984,639, entitled “Method and Apparatus of Performing Data Executable Integrity Verification”, issued Mar. 17, 2015, assigned to Open Invention Network LLC.

- ✓ United States Patent No. 8,825,845, entitled "Managing a Network Element Operating on a Network", issued Sep. 2, 2014, assigned to Open Invention Network LLC.
- ✓ United States Patent No. 8,825,810, entitled "Domain Name Service Based Remote Programming Objects", issued Sep. 2, 2014, assigned to Open Invention Network LLC.
- ✓ United States Patent No. 8,819,827, entitled "Method and Apparatus of Performing Data Executable Integrity Verification", issued Aug. 26, 2014, assigned to Open Invention Network LLC.
- ✓ United States Patent No. 8,713,067, entitled "Stable File System", issued Apr. 29, 2014, assigned to Open Invention Network LLC.
- ✓ United States Patent No. 8,527,779, entitled "Method and Apparatus of Performing Distributed Steganography of a Data Message", issued Sep. 3, 2013, assigned to Open Invention Network LLC.

8. I am also a member of the Association of Computing Machinery (ACM) and the Institute of Electrical and Electronics Engineers (IEEE). I am also a member of the ACM Distinguished Speakers program and on the

advisory board for the cybersecurity program at Embry Riddle University. I attach my curriculum vitae hereto as Appendix A, which includes a more detailed description of my professional qualifications, a list of publications, teaching, and professional activities.

III. LEGAL STANDARDS USED IN MY ANALYSIS

9. I am not an attorney. I have, however, worked closely with counsel, including patent counsel, in over 40 litigations where I have become informed of and relied on certain recurring legal principles related to the validity of patents. I rely on counsel for the law and rely on my learning in reaching the opinions I set forth in this Declaration.

A. I am Familiar with the Legal Concept of Obviousness.

10. I understand that a claim in a patent can be invalidated for being "obvious" if the differences between the subject matter of the claims and the asserted prior art are such that that subject matter as a whole would have been obvious to a PHOSITA at the time the claimed inventions were conceived (i.e., the priority date for the '433 Patent). I understand that every determination on obviousness requires a review of the scope and content of the asserted references, analysis of the differences between those references and the patent claims at issue, and the level of ordinary skill in the pertinent art at the time the inventions were conceived.

11. I have been informed that if a single limitation of a claim is absent from the cited art, the claim cannot be considered obvious.

12. I understand that it is improper to combine references where the references teach away from the proposed combination. I understand also that the following factors are among those relevant in considering whether a reference teaches away:

- whether a PHOSITA, upon reading the reference would be led in a direction divergent from the path that was taken by the applicant;
- whether the reference criticizes, discredits, or otherwise discourages investigation into the claimed invention;
- whether a proposed combination would produce an inoperative result;
- whether a proposed combination or modification would render the teachings of a reference unsatisfactory for its intended purpose; and
- whether a proposed combination would change the basic principles under which a reference was designed to operate.

13. I understand that the level of ordinary skill in the art is important in every obviousness analysis because that is the prism or lens through which the USPTO Board views the patent claims. Evaluating the claimed invention

through the eyes of the PHOSITA prevents factfinders from using either their own insight or hindsight, to gauge obviousness or nonobviousness. The factfinder must view the claims from the standpoint of a PHOSITA at the time just prior to the invention being made, rather than looking back from the claims as issued and using that claim as a blueprint to the claimed invention. A PHOSITA working in the art at the time of the invention cannot be assumed to be able to predict future developments in the art that in hindsight might appear to have been predictable.

B. Priority Date of the ’433 Patent

14. U.S. Patent No. 8,995,433 (“’433” or “EX1001”), titled System and method for instant VoIP messaging, was issued on Mar. 31, 2015. The application 14/224,125, by inventor Michael J. Rojas, was filed on Mar. 24, 2014 and claims priority to, *inter alia*, U.S. Patent Application No. 10/740,040 filed on Dec. 18, 2003. For purposes of this declaration, I have assumed the priority date for the ’433 Patent is Dec. 18, 2003. EX1001 (cover page).

C. The Person Having Ordinary Skill in the Technical Art (PHOSITA)

15. I understand that a PHOSITA is a hypothetical person who is presumed to have ordinary skill in the art as of the time of invention. I understand that factors that may be considered in determining the level of

ordinary skill in the art may include: (a) the type of problems encountered in the art; (b) prior solutions to those problems; (c) the rapidity with which innovations are made in the field at the time; (d) the sophistication of the technology; and (e) the education and skill level of workers active in the field at the time of the invention.

16. The Patent Owner asked me to provide my opinion as to the qualifications of a PHOSITA to which the challenged claims of the ’433 Patent pertained as of 2003. In my opinion, a PHOSITA would be someone with a baccalaureate degree related to computer technology and 2 years of experience with network communications technology, or 4 years of experience without a baccalaureate degree.

D. Broadest Reasonable Interpretation (“BRI”)

17. I understand that the terms in Claims 1-5, 7-12, 14-17, 25, and 26 of the ’433 Patent are to be given their broadest reasonable interpretation (“BRI”) in light of the specification of the ’433 Patent as understood by a PHOSITA at the time of the priority date for the ’433 Patent. I used this understanding throughout my analysis.

IV. THE TECHNOLOGY CLAIMED IN CLAIMS 1-5, 7-12, 14-17, 25, AND 26 OF THE ’433 PATENT

18. The ’433 Patent “relates to Internet telephony (IP telephony). More particularly, the inventions are directed to systems and methods for

enabling local and global instant VoIP messaging over an IP network, such as the Internet, with PSTN support." *Id.* at 1:19-23.

19. The '433 Patent provides the historical context by describing how "[traditional] telephony was based on a public switched telephone network (i.e., "PSTN"). EX1001 at 1:25-35. This is the well-known telephone system that has served the world for well over a century.

20. The '433 Patent explains "An alternative to the PSTN is Voice over Internet Protocol (i.e., "VoIP"), also known as IP telephony or Internet telephony. *Id.* at 1:36-38. The patent elaborates as follows:

> In the IP telephony, a VoIP terminal device is connected to a packet-switched network (e.g., Internet) and voice communication from the VoIP terminal device is digitized, packetized and transmitted over the packet-switched network to a destination VoIP terminal device, which reconstructs the packets and audibly plays, stores or otherwise processes the transmission. The VoIP terminal device may be a VoIP telephone or a general-purpose personal computer (PC) enabled for IP telephony. More specifically, the PC is programmed with the software and equipped with audio input/output devices (e.g., a combination of microphone and speaker or a headset) to serve as a VoIP terminal device. The PC so enabled and equipped will herein be referred to as a VoIP terminal device or a VoIP softphone.

(*Id.* at 1:38-51) (underlining added.)

21. After explaining how VoIP and instant text messaging were nascent arts, inventor Mr. Rojas explained the motivation for his invention as follows:

> However, notwithstanding the foregoing advances in the VoIP/PSTN voice communication and voice/text messaging, there is still a need in the art for providing a system and method for providing instant VoIP messaging over an IP network. More particularly, there is a need in the art for providing local and global instant voice messaging over VoIP with PSTN support.

(*Id.* at 2:48-54) (underlining added.)

22. Fig. 2 from the '433 Patent, reproduced below is "an exemplary illustration of a local instant voice messaging (IVM) system 200 according to the present invention. The instant voice messaging system 200 comprises a local IVM server 202 that "provides the core functionality for enabling instant voice messaging with PSTN support according to the present invention." *Id.* at 6:54-59 (emphasis added).

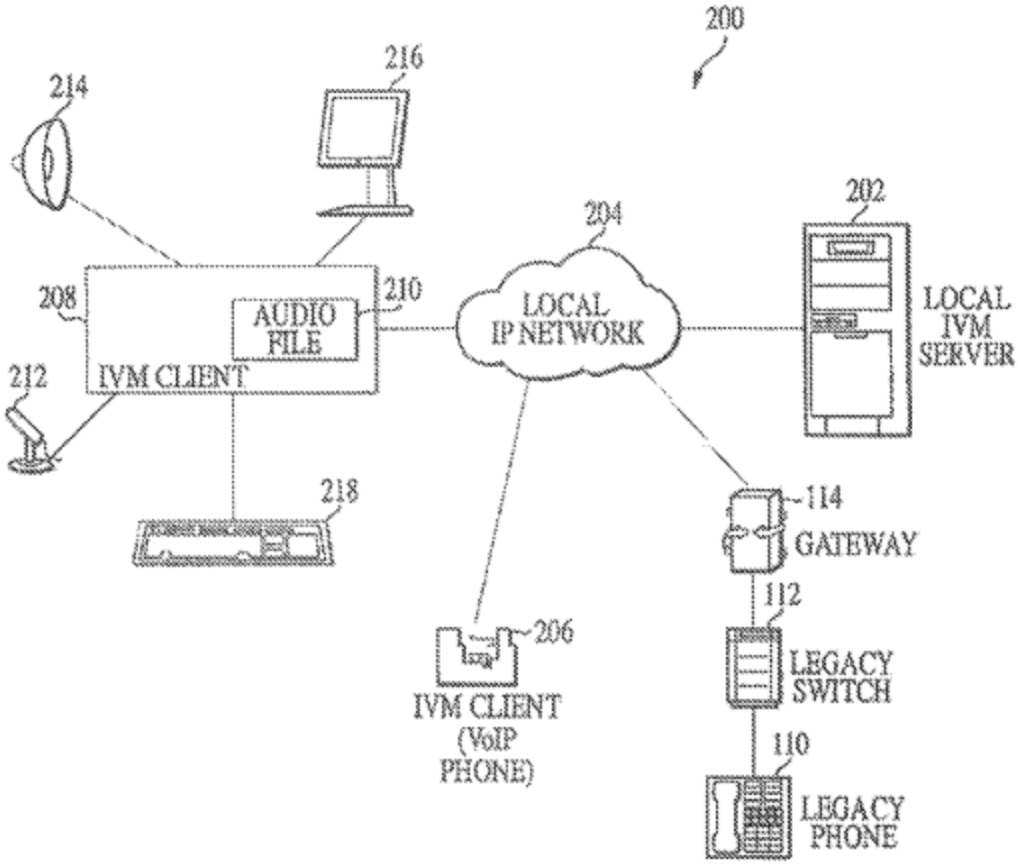

FIG. 2

Fig. 2 of the ’433 Patent: System Diagram of the Instant Voice Messaging System (IVM)

23. The local IVM server 202 “is enabled to provide instant voice messaging to one or more IVM clients 206 and 208, as well support instant voice messaging for PSTN legacy telephones 110.” *Id.* at 6:62-65. The local IP network 204, a packet-switched network, connects the IVM server 202 to clients 208 (viz., a computer system), VoIP Phone 206, and legacy telephone 110 (e.g., a land-line phone). Clients incorporate devices such as

microphones, which enable a person's voice to be recorded, and speakers to allow voice messages to be heard by the users. *Id.* at 7:9-26.

24. A PHOSITA would have understood, upon studying the totality of the '433 Patent, and specifically the written descriptions above and elsewhere in the '433 Patent, that "clients" in the '433 Patent are devices, such as computers and telephones, and not the people who use the devices. *See e.g.*, *Id.* at 9:31-32. The patent expresses this in the following exemplary passages:

> The IVM client 208 is a general-purpose programmable computer equipped with a network interface (not shown), such as an Ethernet card, to provide connectivity to the network 204.

Id. at 12:13-16 (underlining added.)

> The user operates the IVM client 208 by using the input device 218 to indicate a selection of one or more IVM recipients from the list.

Id. at 8:5-8; also 8:60-62 (underlining added.)

> The one or more recipients are enabled to display an indication that the instant voice message has been received and audibly play the instant voice message to an associated user.

Id. at 8:33-36 (underlining added.)

25. The exemplary passages above demonstrate that the user is not the client, which is a device, but rather an entity (e.g., person, another device,

software) that interfaces with and operates the client device using input and output devices.

26. The first passage above explicitly discloses that the client is a computer. The second passage explicitly discloses that the "user" operates the client.

27. Finally, the third passage explains that "recipients are enabled to ... "audibly play the instant voice message to an associated user." *Id.* This exemplary statement explains that a "recipient" is not the "user." A PHOSITA would have understood, after studying the totality of the '433 Patent, that "recipients" are client devices, not people.

28. Regarding the operation of at least one embodiment, the '433 Patent explains "the IVM client (VoIP telephone) 208 is connected over the network 204 to the IVM server 202, which as aforementioned enables instant voice messaging functionality over the network 204." *Id.* at 8:53-56. The operations proceed generally, according to an exemplary embodiment, as follows:

- The client displays a list, provided and stored by the server, of one or more IVM recipients. *Id.* at 8:56-58.
- "The user operates the IVM client 206 by using a keypad on the VoIP telephone 206 to indicate a selection of one or more IVM recipients from the list." *Id.* at 8:60-62.

- The client transmits the selection of the recipient(s) to the server. *Id.* at 8:62-63.
- The client begins recording audio and the user speaks into a microphone or headset or telephone handset of the client. *Id.* at 8:62-9:1.
- The client records the user's speech into an audio file, which may be stored in a storage device (e.g., memory, magnetic disk). *Id.* at 9:1-4; see also *Id.* at 8:11-15.
- The client transmits the recorded audio file (i.e., instant voice message) to the server via the network. *Id.* at 9:6-8; see also *Id.* at 8:25-26.
- The server transmits the instant voice message (that is, the audio file) to the recipient(s) who are currently connected to the network. *Id.* at 9:16-25. If a recipient is not currently connected to the network, the server temporarily saves the instant voice message and delivers it to the IVM client when the IVM client connects to the local IVM server. *Id.*

29. The '433 Patent also teaches "when an instant voice message is to be transmitted to the one or more IVM recipients, one or more documents may be attached to the instant voice message to be stored or displayed by the one or more selected IVM recipients." *Id.* at 12:32-36. Regarding attachments, the '433 Patent teaches:

> The user may also open any file attachments and move or save the files to a separate location on the client using a drag-and-drop process.

Id. at 13:9-12.

> The attachment of one or more files is enabled conventionally via a methodology such as "drag-and-drop" and the like, which invokes the document handler 306 to make the appropriate linkages to the one or more files and flags the messaging system 320 that the instant voice message also has the attached one or more files.

Id. at 13:35-40.

30. In my opinion, a PHOSITA would have understood that the Mr. Rojas refers to files, such as documents, spreadsheets, pictures, and so forth, as entities separate from the audio file itself, and that the term "attachment" should be interpreted as other files or information that are sent with a message. For example, a text message may contain a picture attachment, which is a separate file that is distinct from the actual text in the message.

31. I copy here, for the convenience of the Board, Claims 1, 6, and 9, which are in independent format:

> 1. A system comprising:
>
> an instant voice messaging application including a client platform system for generating an instant voice message and a messaging system for transmitting the instant voice message over a packet-switched network via a network interface;
>
> wherein the instant voice messaging application displays a list of one or more potential recipients for the instant voice message;

wherein the instant voice messaging application includes a message database storing the instant voice message, wherein the instant voice message is represented by a database record including a unique identifier; and

wherein the instant voice messaging application includes a file manager system performing at least one of storing, deleting and retrieving the instant voice messages from the message database in response to a user request.

EX1001, 23: 65 - 24:15.

6. A system comprising:

an instant voice messaging application including a client platform system for generating an instant voice message and a messaging system for transmitting the instant voice message over a packet-switched network via a network interface;

wherein the instant voice messaging application displays a list of one or more potential recipients for the instant voice message;

wherein the instant voice messaging application includes a file manager system performing at least one of storing, deleting and retrieving the instant voice messages from a message database in response to a user request; and

wherein the instant voice messaging application includes a compression/decompression system for compressing the instant voice messages to be transmitted over the packet-switched network and decompressing the instant voice messages received over the packet-switched network.

EX1001, 24:33-51.

9. A system, comprising:

an instant voice messaging application comprising:

a client platform system for generating an instant voice message;

a messaging system for transmitting the instant voice message over a packet-switched network, and wherein the instant voice message application attaches one or more files to the instant voice message.

EX1001, 24:60-67.

V. *GRIFFIN* IS DIRECTED TO USER INTERFACES.

32. *Griffin* is a patent directed to user interfaces. *Griffin* is not as Petitioner asserts "a system for exchanging speech (i.e., voice) chat messages in real time between wireless mobile terminals….". Pet. p. 9. Rather, *Griffin* is a user interface patent for "displaying and interacting with speech and text group chat threads." *Griffin*, 1:62–65.

33. *Griffin* does not teach real time communication. Petitioner argues that *Griffin* supports transmission in real time, but neither Petitioner nor *Griffin* describe communication of speech in real time. Real-time communication requires both the capability for transmission in real time as well as the capability for receipt in real time. Petitioner does not account for when the recipient using the *Griffin* system actually receives messages. To the contrary, as I explain below, the speech Petitioner argues is transmitted in real time is quite likely not received in real time even when the target user is

already using their device, because a specific chat history window required for speech message receipt is not being displayed at the device (even in the unlikely event that the chat history window was being displayed, there are still several other reasons why a PHOSITA would not combine *Griffin* with *Zydney*). Petitioner does not show that *Griffin* supports real-time communication of speech.

34. The only mention of "real-time" in *Griffin* is in the general Technical Field: "a novel technique of managing the display of a plurality of real-time speech and text conversations (e.g., chat threads) on limited display areas." *Griffin*, 1:9–11.

35. In my opinion, *Griffin* contradicts Petitioner's argument that *Griffin* discloses an "instant voice message." *Griffin* teaches a system that has no knowledge of, or interest in, and no way to know whether a recipient is positioned to hear a message. *Griffin* is interested only in whether a terminal is configured to be able to receive a message at some point in the future.

36. Petitioner relies on the feature in *Griffin* of "presence status" to argue that *Griffin* "includes terminals 100 that are presented with information regarding the availability of other terminals 100 for messaging and facilitates the real-time (i.e., immediate) transmission of speech chat messages between available terminals." EX1002, ¶83. Nowhere, however, does Petitioner

reference *Griffin*'s failure to deliver a message even when the terminal is "Available," which I further explain below.

37. *Griffin* discloses instantaneous text messages, but *Griffin* does not disclose instant voice messages. Every passage of *Griffin* that Petitioner relies on is directed explicitly toward text messaging. Petitioner does not point to any part of *Griffin* that describes instant voice messaging. All Petitioner says is that *Griffin* is "consistent with" passages in the '433 Patent. In my opinion, Petitioner does not explain how or why Petitioner believes that *Griffin* discloses an "instant voice message."

38. In my opinion, Petitioner relies on an understanding of "push-to-talk" that is relevant today (i.e., 2017), but was not relevant in 2002. Pet. at pp. 10, 16, 35, 61. In 2002, when *Griffin* filed his application, a PHOSITA would have understood "push-to-talk" as technology that enables a mobile device to operate as a half-duplex radio similar to a walkie-talkie. When *Griffin* was filed, "push-to-talk" was used by radio operators, for instance, in the Citizens Band. Every mention of push-to-talk in *Griffin* refers to that half-duplex, radio-based communication method. No PHOSITA would equate such a method with the claimed "instant voice message."

39. But even if "push-to-talk" could be stretched to cover an "instant voice message," the communication in *Griffin* did not take place "over a

packet-switched network." In 2003, all such communication was made over circuit-switched networks.

40. The system in *Griffin* has no knowledge of, or interest in, and has no way to know whether a device is ready and able to "hear" a message. In *Griffin*, the message to be sent from the server complex 204 is prepared based on the technical ability of a terminal to receive the message at some arbitrary point in the future. The message is only delivered if the user has the "chat history display" visible on the user interface. *Griffin*, 11:48-67.

VI. THE VOICE CONTAINERS OF *ZYDNEY* ARE NOT AUDIO FILES.

41. *Zydney* "relates to the field of packet communications, and more particularly to voice packet communication systems." EX1006 at 1:4-5.3 (referring to *Zydney* by page and line numbers).

42. *Zydney* explains "[the] present invention is a system and method for voice exchange and voice distribution utilizing a voice container." EX1006 at 1:19-20 (underlining added). Moreover, "voice containers can be stored, transcoded and routed to the appropriate recipients instantaneously or stored for later delivery." *Id.* at 1:21-2 (emphasis added). *Zydney* defines "voice container" as "a container object that contains no methods but contains voice data or voice data and voice data properties." *Id.* at 12:6-8. A PHOSITA would have understood that this definition means *Zydney*'s voice container is

a data construct (viz., an "object") used in object-oriented programming languages, such as Java or C++, to hold other data constructs, such as data values and other objects, but performs no functions (methods). Dr. Val DiEuliis has an apt analogy. He testified in IPR2017-01257 (which challenged a patent related to the '433 Patent based on *Zydney*) that a container object is like a box, it holds things but it is not the things it holds. For example, if a box contains paper clips, the actual box itself is not a paper clip.

43. *Zydney* teaches "the originator digitally records messages for one or more recipients using a microphone-equipped device and the software agent. The software agent compresses the voice and stores the file temporarily on the PC if the voice will be delivered as an entire message." *Id.* at 16:1-4 (emphasis added). A PHOSITA would have understood that *Zydney* may temporarily store the audio data in a file, which is another type of data structure and which may even be stored on a magnetic disk drive or other medium.

44. Before the voice data is sent to a recipient, it is placed in the voice container and the container is sent. *Zydney* explains this process:

> The present invention system and method for voice exchange and voice distribution 20 allows a software agent 22 with a user interface in conjunction with a central server 24 to send, receive and store messages using voice containers illustrated by

> transmission line 26 in a pack and send mode of operation to another software agent 28. A pack and send mode of operation is one in which the message is first acquired, compressed and then stored in a voice container 26 which is then sent to its destination(s).

Id. at 10:20-11:3 (underlining added.)

45. The passage above explains that *Zydney*'s voice message is the audio data; however, it is stored in a voice container, which is a type of data structure, distinct from a file.

46. After the voice container is received by a recipient, "voice files can be played and recorded using voice container enabled devices." *Id.* at 21:14-16. Thus, *Zydney* teaches that a recipient must have a device that is able to process voice containers in order to audibly play back the voice data.

47. *Zydney*'s voice container contains additional components besides the "voice data or voice data and voice data properties." Fig. 3 and its accompanying text explain that communications and application oriented information is included, such as an originator's code, recipients' codes, originating time, delivery time(s), number of plays, voice container source, voice container reuse restrictions, delivery priority, session values and number, and more. *Id.* at 23:1-12.

48. *Zydney* explains that files, such as multi-media files, may be attached to a voice container. *Id.* at 19:2-5. *Zydney* states "[for] example, the voice container may have digitized greeting cards appended to them to present a personalized greeting." *Id. Zydney* explains that various industry standards, such as Multipurpose Internet Mail Extension (MIME) format, may be used to format the voice container so that attachments may be associated with it. *Id.* at 19:6-20:9.

49. *Zydney* discloses two ways to send a voice message: (a) pack and send; and (b) intercom. First, the "pack and send" method "is one in which the message is first acquired, compressed and then stored in a voice container 26 which is then sent to its destination(s)." *Id.* at 11:1-3; *see also* Pet. at 48 and EX1002 at ¶¶ 79-81. *Zydney* also allows for storing the voice container, either locally or at the server, if the recipient is not available. EX1003 at 2:3-6. Second, *Zydney* explains that, if a recipient is online, the originator can begin a real-time "intercom" call which simulates a telephone call or a voice instant messaging session, which allows for an interruptible conversation." EX1006 at 15:8-10.

50. The method of generating the voice message is the same regardless of whether the message delivery method is "pack-and-send' or "intercom." The "pack and send" method "is one in which the message is first

acquired, compressed and then stored in a voice container 26 which is then sent to its destination(s).” *Id.* at 11:1-3. Thus, the method of generating the voice message is: (1) acquire the message (e.g., using a microphone); (2) compress the audio data; (3) store the audio data in a voice container; and (4) send the voice container to its destination.

51. Likewise, when the “intercom mode” is used to deliver the voice message, the audio data is placed in a voice container and the voice container is sent to the destination. *Zydney* teaches “[once] the delivery mode [intercom or pack-and-send] has been selected, the originator digitally records messages for one or more recipients using a microphone-equipped device and the software agent.” *Id.* at 17:1-3. Thus, the data is acquired using the same method regardless of whether the recipients are online or offline because they are acquired the same way regardless of whether the pack-and-send or the intercom mode of delivery is selected. In the pack-and send mode, the complete voice message (that is, the voice data) is stored in a voice container and sent to the destination. For the “intercom” mode, *Zydney* teaches:

> If the real time "intercom" mode has been invoked, a small portion of the digitized voice is stored to account for the requirements of the Internet protocols for retransmission and then transmitted before the entire conversation has been completed. Based on status information received from the central

> server, the agent then decides on whether to transport the voice containers to a central file system and/or sends it directly to another software agent using the IP address previously stored in the software agent.

EX1006 at 16:4-10 (underlining added.)

VII. GRIFFIN CANNOT BE COMBINED WITH *ZYDNEY*

52. In my opinion *Griffin* cannot be combined with the system described by *Zydney*. Petitioner does not explain how such a combination could be done, and in my opinion, it could not be achieved. Petitioner proposes several grounds for combining *Griffin* and *Zydney*, but none addresses the fundamental incompatibility that while *Griffin* is indifferent to a recipient's immediate availability, *Zydney* requires instant communication. Thus, Petitioner's proposal relies on a misunderstanding. Petitioner appears to believe that *Griffin* and *Zydney* are operating from the same definition of the "connectivity status." That is wrong. "Connectivity status." in *Griffin* and *Zydney* mean entirely different things. *Zydney* requires status to include "the core states of whether the recipient is online or offline." EX1006, p. 14. *Griffin* doesn't know whether a recipient is actually online. *Griffin* and *Zydney* could not be combined and a PHOSITA would not be motivated to combine them.

53. Petitioner's combination of *Griffin* and *Zydney* is inoperable for text-only buddies. If *Zydney*'s concept of available/unavailable was inserted

in place of the status 702 in *Griffin*, then a text-only buddy such as JaneT (in FIG. 7 of *Griffin*) would be considered available for instant voice messaging simply by virtue of having an Internet connection (e.g., that enables communication with the server complex 204). However, JaneT does not have the ability to receive and/or play speech messages (which is why she was designated "TextOnly" in the first place). A PHOSITA would realize that this would lead to erroneous behavior, because JaneT should not be considered available for instant voice messaging. Petitioner has not even acknowledged this problem, let alone explained how to deal with it. A PHOSITA would avoid such erroneous behavior, and would therefore not combine *Griffin* and *Zydney* in the manner Petitioner has.

54. In addition, attempting to combine the system of *Zydney* in the system described by *Griffin* would frustrate the purpose of *Zydney* to deliver messages instantaneously, because *Griffin* is indifferent to whether the receiving terminal can receive a message at the instant it was sent, and *Griffin* intentionally delays delivery of messages even if the recipient is otherwise available (as that term is understood by *Zydney*), just because the recipient does not have the chat history display active.

55. Furthermore, *Griffin* and *Zydney* have opposite principles of operation. *Griffin* is a server-based messaging paradigm in which technical

feasibility of communicating a message to a recipient terminal is determined at the server complex 204 rather than at the mobile terminal 100 and in which only the messages vetted by the server complex 204 are subsequently communicated by the server complex 204. The server complex 204 of *Griffin* sends, rather than stores, all outbound chat messages 400 it receives that are technically capable of being received by the receiving terminals 100 (subject to later queuing after receipt at a targeted recipient terminal). In contrast, *Zydney* is so concerned with instantaneous delivery of its voice container that it bypasses its Central Server entirely if at all possible, such as when P2P communication is possible between sender and receiver. Petitioner's suggested combination would require *Griffin* to be substantially changed before its principle of operation could be compatible with *Zydney*.

56. *Griffin* makes available only the most recent message. *Griffin* states: "In a current implementation, the most recently received speech message (or at least that portion that will fit in available memory) [is] queued at the receiving terminal." *Griffin*, 11:50–53. A PHOSITA would understand this to mean that only the most recently received speech message (or portion thereof) is queued at the receiving terminal, so any previous speech messages (including those that were sent before the user switched or opened to the "chat history display") would be lost.

57. Because *Griffin* enlists a server complex 204 that determines message-delivery feasibility and only sends messages determined to be feasible, the server complex 204 conditionally queues messages. *Griffin* thus would not gain any advantage or derive benefit from *Zydney*'s P2P direct communication paradigm.

58. In my opinion, Petitioner is just speculating when suggesting that *Griffin* would benefit from *Zydney*'s "status information received [by sending devices] from the central server" (*see Zydney*, 16:7-10 and ¶ bridging pp. 14-15) for accomplishing *Zydney*'s P2P communication. *Griffin* already has the above discussed presence status 702 indicator, which may contain content such as "Available" and "Off." *Griffin*, Fig. 7.

59. Petitioner proposes several grounds for combining *Griffin* and *Zydney*, but the ability of *Zydney* to provide the sending device with P2P communication feasibility information does not benefit the system of *Griffin*. Petitioner's proposal for importing *Zydney*'s P2P "status information" into *Griffin's* server-based system does not appear to benefit *Griffin*. To the extent even possible, such P2P "status information" of *Zydney* configured for use at *Zydney*'s sending device, if hypothetically imported into *Griffin* and if configurable for use at *Griffin*'s server complex 204, would appear to overlap with *Griffin*'s existing technology (while introducing erroneous behavior for

text-only buddies and due to dropped messages, as I explain herein). That is, rather than enhancing *Griffin*'s presence status 702 server-based paradigm, such a hypothetical combination would *introduce redundancy* into *Griffin*'s existing server complex 204 in which an "Off" status and conditional storage of messages are already provided, and Petitioner does not appear to assert otherwise.

VIII. PETITIONER'S RELIANCE ON CLARK IS MISPLACED.

60. Petitioner admits that neither *Griffin* nor *Clark* discloses the claimed "file manager system." EX1002, ¶129; Pet. at 26-27. Petitioner also admits that Petitioner's proposed combination itself would have to be yet further modified before it could disclose the claims "file manager system." Ex. 1002, ¶¶132-138; Pet. at 27-28; EX1002, ¶129.

61. In the *Griffin* system, the sender does not store a copy of messages sent. In order to have a copy of a sent message, the sender must copy the message to herself, in other words, the sender has to also be the recipient, or the message is gone and cannot be stored or retrieved. EX1005, 10:30-33, 43-51.

62. *Clark* teaches away from the proposed combination. *Clark* explains that "MessageSummary table 52" is separate and distinct from the message data itself. EX1007, Fig. 5A. *Clark* describes the desirability of

making it easier to link the MessageSummary table 52 to data messages that are in an external storage. *Clark* also explains why the message data should be separate from the MessageSummary table 52, because doing so increases processing performance. *Id.* at 16:54-58.

63. Petitioner cites various passages from *Clark* (EX1007) allegedly supporting the position that *Clark* adds, deletes, and retrieves messages from *Clark*'s "message store 23" in response to user requests to do so. Pet. at 28. But Petitioner cites passages describing requests passed from one component of *Clark*'s system 20 (e.g., the message client 27) to another component of *Clark*'s system 20 (e.g., the message store server 23), where neither of the components is what Petitioner alleges is the claimed message database (i.e., Petitioner refers to the message store 23). *Clark* does not add, delete, or retrieve messages from message store 23.

64. The '433 Patent specifies: "The file manager accesses a message database 310, in which both the received and recorded instant voice messages are represented as database records, each record comprising a message identifier and the instant voice message." EX1001, 12:36–40 (emphasis added).

65. The Petition admits that *Griffin* lacks this element. Pet., p. 21. *Clark* also lacks this element. The Petition primarily cites to Fig. 5A of *Clark*

and its associated description as allegedly disclosing the claimed database record. *Id.* at 22–26. In particular, the Petition asserts that the "message store 23" of *Clark* discloses the claimed message database and that "StoreMessageID," which is included in a "MessageSummary table 52," discloses the claimed unique identifier. *Id.* at 48. However, FIG. 5A of *Clark* shows the "MessageSummary table 52" as being outside the "message store 23." EX1007, FIG. 5A. Further, the "MessageSummary table 52" does not include any message data at all. *Clark* explicates the contents of MessageSummary table 52:

> The actual contents of the MessageSummary will vary depending upon the . . . implementation, but in a currently preferred embodiment . . . MessageSummary table 52 includes the following fields:

MessageId	A non-zero value that uniquely identifies a row in MessageSummary table 52.
FolderExcludeList	(Array of [FolderId + FolderDateTime]) - Identifies the Folders from which shortcuts, that would normally be created by automatic rules, should be removed.
IsUnread	Indicates whether the message is in an unread state.
IsCorresp	Indicates whether the message is correspondence from or to a recognized correspondent. The logic to set this value is described below.
MessageDateTime	The date and time to be displayed to the user when listing messages in a folder. For unsent messages this contains the creation date/time, for received messages this contains the receive date/time, and for sent message this contains the send date/time.
DisplayNames	The sender or recipient names to be displayed to the user when listing messages in a folder. For received messages this contains the sender's name, and for sent or unsent messages this contains is the names of the primary recipients.
Subject	The subject of the message.

EX1007, 17:1–24.

66. In *Clark*, the message data is included in a "Message table 54" that is separate from the MessageSummary table 52, as shown in Fig. 5A. Further, in Fig. 5A of *Clark*, the MessageSummary table and the Message table are in separate data stores (the catalog database 28 and the message store 23, respectively). And the Petition notes that the catalog database 28 and the message store 23 of *Clark* can be combined, as in Fig. 5B. Pet., p. 22. However, none of the tables shown in Fig. 5B of *Clark* includes a

"StoreMessageID," which is the only item of *Clark* that the Petition has asserted as disclosing the claimed unique identifier. Pet. 22–26.

67. There would be no motivation to combine *Griffin* with *Clark* in the manner as the Petition proposes for two separate reasons. First, both *Griffin* and *Clark* lack this element, as the Petition admits and as described above. In other words, neither *Griffin* nor *Clark* has a requisite component of the proposed combination.

68. Second, *Clark* teaches away from the proposed combination, and therefore there could have been no motivation to combine. *Clark* explains that "MessageSummary table 52" is separate and distinct from the message data itself. EX1007, FIG. 5A. Indeed, *Clark* describes the desirability of making it easier to link the MessageSummary table 52 to data messages that are in an external storage. Id. at 16:54–58. *Clark* also explains that keeping MessageSummary table 52 separate and distinct from the message data is desirable because doing so enhances processing performance. Processing performance is enhanced because a row of the MessageSummary table 52 is small, due to the row not containing the actual message data. EX1007, 16:58–63. *Clark* explains why the message data should be separate from the MessageSummary table 52:

> A first reason for implementing a MessageSummary table that is distinct from Message table 54 is that having a separate Message

> Summary table 52 facilitates linking to messages in an external message store 23. A second reason is to enhance processing performance-a MessageSummary record (i.e. a row in MessageSummary table 52) is typically much smaller than its related message record (i.e. a row in Message table 54) and it is consequently much faster to read MessageSummary records than it is to read Message records.
> EX1007, 16:54–63.

69. Because *Clark* teaches away from including the message data in the same database record as the unique identifier, there would not have been any motivation to combine *Clark* with *Griffin*.

70. The claim language at issue expressly requires a message database at the sending device. This was confirmed by the Board in its Decision to Institute IPR2017-00225, a related IPR, in which the Board stated "we agree with Patent Owner that the instant voice message application and the recited message database, by the plain reading of the claim language, is directed to the application at the client." Decision to Institute Inter Partes Review, IPR2017-00225, May 25, 2017 at 18-19 (citations omitted.)

71. The purpose of *Clark*'s database is the organization and storage of messages so that users can control when they are added, deleted, or otherwise handled. See EX1008.

IX. CONCLUSION

72. For the reasons set forth herein, Claims 1-3 of the ’433 Patent are not rendered obvious in light of the references and testimony cited by Petitioner.

73. I understand that, in signing this Declaration, the Declaration will be used as evidence in an *inter partes* review before the Patent Trial and Appeal Board concerning the validity of the ’433 Patent. I understand that I may be subject to cross-examination in the proceeding. I will appear for such cross-examination during the time allotted for cross-examination and at a time and location convenient for myself and the parties.

74. I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Dated Tuesday, November 7, 2017

William C. Easttom II

APPENDIX A

Appendix A: Curriculum Vitae of William. C. Easttom II (Chuck Easttom)

Contents

Education

University Degrees

- B.A. Southeastern Oklahoma State University. Major Communications with Minors in Chemistry and Psychology. Extensive coursework in science (chemistry, physics, and biology) as well as neuroscience (neurobiology of memory, cognitive science, etc.). Also, additional coursework in computer science including programming and database courses.
- M.Ed. Southeastern Oklahoma State University. Coursework included technology related courses such as digital video editing, multimedia presentations, and computer graphics. A statistics course was also part of the coursework.

- M.B.A. Northcentral University Emphasis in Applied Computer Science. Extensive course work in graduate computer science including graduate courses in: C++ programming, C# programming, Computer Graphics, Web Programming, Network communication, Complex Database Management Systems, and Artificial Intelligence. Approximately 30 graduate hours of graduate computer science courses. Additionally, a doctoral level statistics course was included. A semester research project in medical software was also part of the curriculum. I also took several research courses beyond the requirements for the degree.
- Doctor of Science (In progress) Capitol Technology University. Majoring in cybersecurity, dissertation topic is a study of post quantum computing asymmetric cryptographic algorithms.

Industry Certifications

The following is a list of computer industry certifications I have earned.

Hardware and Networking Related Certifications

1. CompTIA (Computer Technology Industry Associations) A+ Certified
2. CompTIA Network + Certified
3. CompTIA Server+ Certified
4. CompTIA I-Net+ Certified

Operating System Related Certifications

5. CompTIA Linux + Certified
6. Microsoft Certified Professional (MCP) – Windows Server 2000 Professional Certification Number: A527-9546
7. Microsoft Certified Systems Administrator (MCSA) Windows Server 2000 Certification Number: A527-9556
8. Microsoft Certified Systems Engineer (MCSE) Windows Server 2000 Certification Number: A527-9552
9. Microsoft Certified Technology Specialist (MCTS) Windows Server 2008 Active Directory Microsoft Certification ID: 1483483
10. Microsoft Certified Technology Specialist (MCTS) Windows 7 Microsoft Certification ID: 1483483
11. Microsoft Certified IT Professional (MCITP) Windows 7 Microsoft Certification ID: 1483483
12. Microsoft Certified Solutions Associate Windows 7 Microsoft Certification ID: 1483483
13. National Computer Science Academy Windows 8 Certification Certificate #: 4787829

Programming and Web Development Related Certifications

14. Microsoft Certified Professional (MCP) – Visual Basic 6.0 Desktop Applications Microsoft Certification ID: 1483483
15. Microsoft Certified Professional (MCP) – Visual Basic 6.0 Distributed Applications Microsoft Certification ID: 1483483
16. Microsoft Certified Application Developer (MCAD) - C# Microsoft Certification ID: 1483483
17. Microsoft Certified Trainer (MCT 2005-2012) Microsoft Certification ID: 1483483
18. Microsoft Certified Technology Specialist (MCTS) Visual Studio 2010 Windows Application Microsoft Certification ID: 1483483
19. Microsoft Certified Technology Specialist (MCTS) Visual Studio 2010 Data Access Microsoft Certification ID: 1483483
20. National Computer Science Academy HTML 5.0 Certification Certificate #: 4788000.
21. National Computer Science Academy ASP.Net Certification Certificate #: 4788342
22. Certified Internet Webmaster (CIW) Associate CIW0163791

Database Related Certifications

23. Microsoft Certified Database Administrator (MCDBA) SQL Server 2000 Microsoft Certification ID: 1483483
24. Microsoft Certified Technology Specialist (MCTS) Implementing SQL Server 2008 Microsoft Certification ID: 1483483
25. Microsoft Certified IT Professional (MCITP) SQL Server Administration Microsoft Certification ID: 1483483

Security and Forensics Related Certifications

26. CIW Certified Security Analyst CIW0163791
27. EC Council Certified Ethical Hacker v5 (CEH) ECC942445
28. EC Council Certified Hacking Forensics Investigator v4 (CHFI) ECC945708
29. EC Council Certified Security Administrator (ECSA) ECC947248
30. EC Council Certified Encryption Specialist (ECES)
31. EC Council Certified Instructor
32. CISSP – Certified Information Systems Professional #387731
33. ISSAP – Certified Information Systems Architect #387731
34. CCFP – Certified Cyber Forensics Professional #387731
35. Certified Criminal Investigator (CCI)

36. Forensic Examination of CCTV Digital VTR Surveillance Recording Equipment
37. Oxygen Phone Forensics Certified
38. Access Data Certified Examiner (ACE) 2014-2017
39. OSForensics Certified Examiner (OSFCE)
40. Certified Forensic Consultant (CFC)

Software Certifications

41. National Computer Science Academy Microsoft Word 2013 Certification Certificate #: 5078016
42. National Computer Science Academy Microsoft Word 2000 Certification Certificate #: 5078187

Licenses

Texas State Licensed Private Investigator. Registration Number 827827. Associated with Allegiant Investigations & Security License Number: A18596

Publications

Books

1. Easttom, C. (2003). Moving from Windows to Linux. Newton Center, MA: Charles River Learning. 1st Edition, Charles River Media.
2. Easttom, C., Hoff, B. (2006). Moving from Windows to Linux, 2nd Ed. Newton Center, MA: Charles River Learning. 1st Edition, Charles River Media.
3. Easttom, C. (2003). Programming Fundamentals in C++. Newton Center, MA: Charles River Learning. 1st Edition, Charles River Media.
4. Easttom C. (2002). JFC and Swing with JBuilder 8.0. Plano, Texas: WordWare Publishing.
5. Easttom, C. (2002). JBuilder 7.0 EJB Programming. Plano, Texas: WordWare Publishing.
6. Easttom, C. (2001). Beginning JavaScript, 1st Edition. Plano, Texas: WordWare Publishing.
7. Easttom, C. (2002). Beginning VB.Net. Plano, Texas: WordWare Publishing.
8. Easttom, C. (2001). Advanced JavaScript, 2nd Edition. Plano, Texas: WordWare Publishing.
9. Easttom, C. (2005). Introduction to Computer Security. New York City, New York: Pearson Press.
10. Easttom, C. (2006). Network Defense and Countermeasures. New York City, New York: Pearson Press.

11. Easttom, C. (2005). Advanced JavaScript, 3rd Edition. Plano, Texas: WordWare Publishing.

12. Easttom, C., Taylor, J. (2010). Computer Crime, Investigation, and the Law. Boston, Massachusetts: Cengage Learning.

13. Easttom, C. (2013). Essential Linux Administration: A Comprehensive Guide for Beginners. Boston, Massachusetts: Cengage Learning.

14. Easttom, C. (2011). Introduction to Computer Security, 2nd Edition. New York City, New York: Pearson Press.

15. Easttom, C. (2012). Network Defense and Countermeasures, 2nd Edition. New York City, New York: Pearson Press.

16. Easttom, C. (2013). System Forensics, Investigation, and Response, 2nd Edition. Burlington Massachusetts: Jones & Bartlett.

17. Easttom, C. (2014). CCFP Certified Cyber Forensics Professional All-in-One Exam Guide. New York City, New York: McGraw-Hill Publishing.

18. Easttom, C., Dulaney, E. (2015). CompTIA Security+ Study Guide: SY0-401. Hoboken, New Jersey: Sybex Press.

19. Easttom, C. (2015). Modern Cryptography: Applied Mathematics for Encryption and Information Security. New York City, New York: McGraw-Hill Publishing.

20. Easttom, C. (2016). Computer Security Fundamentals, 3rd Edition. New York City, New York: Pearson Press.

21. Easttom, C. (2017). System Forensics, Investigation, and Response, 3rd Edition. Burlington Massachusetts: Jones & Bartlett.

22. Easttom, C., Dulaney, E. (2017). CompTIA Security+ Study Guide: SY0-501. Hoboken, New Jersey: Sybex Press.

23. Easttom, C. (2018). Penetration Testing Fundamentals: A Hands On Guide to Reliable Security Audits. New York City, New York: Pearson Press. Writing complete, will be published in early 2018.

24. Easttom, C., Christy, R. (2017). CompTIA Security+ Review Guide: SY0-501. Hoboken, New Jersey: Sybex Press.

25. Easttom, C., Roberts, R. (2018). Networking Fundamentals, 3rd Edition. Goodheart-Wilcox Publishing. Writing complete, will be published in early 2018

.

Papers, presentations, & articles.

1. Easttom, C. (2010). RSA and its Challenges. EC Council White Paper.
2. Easttom, C. (2010). Finding Large Prime Numbers. EC Council White Paper
3. Easttom, C. (2010). A Method for Finding Large Prime Numbers. Haking Magazine. Hands-On Cryptography Issue.

4. Easttom, C. (2014). A method for finding large prime numbers. Open Source Article published by Academia.edu 2014.
5. Easttom, C. (2011). The RSA Algorithm - The ups and Downs. CryptoMagazine.
6. Easttom, C. (2011). Feistel Ciphers - An Overview. Presentation at Cast Security Conference. Washington, D.C.
7. Easttom, C. (2011). Steganography- History and Modern Applications. Presentation at Takedown Security Conference.
8. Easttom, C. (2012). Problems with RSA. Presentation at Takedown Security Conference – Dallas, TX.
9. Easttom, C. (2013). Cryptanalysis. Presentation at Takedown Security Conference. Huntsville, Alabama.
10. Easttom, C. (2014). An Overview of Cryptographic S-Boxes used in Block Ciphers. Research Gate. DOI RG.2.2.14084.94088.
11. Easttom, C. (2014). Cryptographic Backdoors. Presentation at ISC2 Security Congress. Atlanta, Georgia.
12. Easttom, C. (2014). Cryptographic Backdoors. Presentation at University of Texas Dallas ACM Chapter Conference.
13. Easttom, C. (2014). Windows Registry Forensics. Research Gate. DOI RG.2.2.29603.86561
14. Easttom, C. (2014). Artificial Intelligence, Fuzzy Logic, Neural Networks and Fuzzy Neural Networks and their impact on Electronic Medical Records. Academia.edu.
15. Easttom, C. (2014). A Basic Overview of Electro-Magnetic Interference. Academia.edu.
16. Easttom, C. (2014). An Overview of Targeted Malware. Academia.edu.
17. Easttom C. (2014). An Introduction to Mobile Forensics. Academia.edu.
18. Easttom, C. (2015). Cryptographic Backdoors. Academia.edu.
19. Easttom, C. (2015). The History of Computer Crime in America. Academia.edu.
20. Easttom, C. (2015). Spyware Techniques. Academia.edu.
21. Easttom, C. (2015). Recovering Deleted Files from NTFS. Academia.edu.
22. Easttom, C. (2015). Multi-dimensional analysis of cyber-forensic evidence. Academia.edu.
23. Easttom, C. (2016). Spyware coding techniques. Journal of Information Security Science & Digital Forensics (HJISSDF), 1 (1)
24. Easttom, C. (2016). Cryptographic Backdoors – an overview. Journal of Information Security Science & Digital Forensics (HJISSDF), 1 (1)
25. Easttom, C. (2016). A Look at Spyware Techniques. 2600 Magazine, *33*(3). Autumn issue 2016.
26. Easttom, C. (2016). Multi-Dimensional Analysis of Digital Forensic Evidence. Forensic Examiner Journal, *25* (4).

27. Easttom, C. (2016). Applying Graph Theory to Evidence Evaluation. Research Gate DOI: RG.2.2.23391.0528
28. Easttom, C. (2017). An Overview of Pseudo Random Number Generators. Research Gate. DOI: RG.2.2.13941.58087
29. Easttom, C. (2017). A Model for Penetration Testing. Research Gate. DOI: RG.2.2.36221.15844
30. Easttom, C. (2017). The RSA Algorithm Explored. International Journal of Innovative Research in Information Security. (IJIRIS). 4(1).
31. Easttom, C. (2017). Utilizing Graph Theory to Model Forensic Examination. International Journal of Innovative Research in Information Security (IJIRIS), 4(2).
32. Easttom, C. (2017). Applying Graph Theory to Modeling Investigations. IOSR Journal of Mathematics (IOSR-JM) 13,2 PP 47-51. doi:10.9790/5728-130205475
33. Easttom, C. (2017). Enhancing SQL Injection with Stored Procedures. 2600 Magazine. 34(3).
34. Easttom, C. (2017). An Overview of Key Exchange Protocols. IOSR Journal of Mathematics (IOSR-JM). 13(4). DOI: 10.9790/5728-1304021618

Patents

U.S. Patent No. 8,527,779 B1 Method and apparatus of performing distributed steganography of a data message

U.S. Patent No. 8,713,067 Stable File System

U.S. Patent No. 8,819,827 B1 Method and apparatus of performing data executable integrity verification

U.S. Patent No. 8,825,845 B1 Managing a network element operating on a network

U.S. Patent No. 8,825,810 B1 Domain name service based remote programming objects

U.S. Patent 8,984,639 Method and apparatus of performing data executable integrity verification

U.S. Patent No. 9,405,907 Method and apparatus of performing data executable integrity verification (a continuation patent of '639)

US Patent No. 9,313,167 Domain name service based remote programming objects

US Patent No. 9,619,656 Method and apparatus of performing distributed steganography of a data message (continuation patent of 8,527,779 B1)

US Patent No. 9,686,227 Domain Name Service based remote programming objects (continuation patent of U.S. Pat. No. 9,313,167)

US Patent No. 9,755,887 Managing a network element operating on a network

US Patent No. 9,754,108 Method and apparatus of performing data executable integrity verification

US Patent No. 9,753,957 System and method for document tracking

Standards and Certification Creation

1. Member of the advisory board for Embry Riddle University cyber security program within the Homeland Security degree program.
1. Created the course and certification test for Certified OSForensics Examiner (OSFCE). OSForensics is a forensic software tool used to analyze computers.
2. Reviewer for scientific papers submitted to IEEE Security & Privacy.
3. Editorial board member for the year 2016 for *Journal of Information Security Science & Digital Forensics.* This is an international peer reviewed information security journal.
4. Editorial board for the year 2016 member for *The Forensic Examiner*. This is a peer reviewed forensic journal.
5. Subject matter expert for the Computer Technology Industry Association (CompTIA) Server + exam creation team. I was part of the team that helped create the CompTIA Server+ certification test.
6. Subject matter expert for the Computer Technology Industry Association (CompTIA) Linux+ exam review team. I was part of the team that helped create the CompTIA Linux+ certification test.
7. Subject matter expert for the Computer Technology Industry Association (CompTIA) Security+ exam Job Task Analysis team. I was part of the team that helped create the CompTIA Security+ certification test.
8. Subject matter expert for the Computer Technology Industry Association (CompTIA) Certified Technical Trainer exam revision team.

9. Created the EC Council Certified Encryption Specialist course and certification test. Then revised the course and certification in 2017.
10. Created the EC Council CAST Advanced Encryption course.
11. Worked on the Job Task Analysis Team for the Certified Ethical Hacker v8 test.

Professional Awards and Memberships

1. Distinguished Speaker of the ACM (2017 to 2020)
2. Member of the International Association of Cryptological Research (IACR)
3. Member of the ACM (Association of Computing Machinery)
4. Member of the ACM Special Interest Group on Artificial Intelligence
5. Member of the ACM Special Interest Group on Security, Audit and Control
6. Member of the IEEE (Institute of Electronics and Electrical Engineers)
7. Member of the IEEE Computing group
8. Associate Member of the American Academy of Forensic Sciences (2015 to 2018)
9. Member of InfraGard (FBI-Civilian group for cyber security)
10. 1992-1993 National Deans List
11. Who's Who in American Colleges and Universities 1998
12. Marquis Who's Who in America
13. Marquis Who's Who in Education
14. Marquis Who's Who in Science and Engineering

Speaking Engagements

1. Mid-Cities PC Users Group September 19, 2003. The topic was computer security in general.
2. The Harvard Computer Society April 5, 2004. The topic was computer security.
3. The ACM Chapter of Columbia University November 15, 2005. The topic was computer viruses.
4. DeVry/Keller University in Dallas December 2009 Commencement Speaker.
5. Public presentation on computer crime in McKinney Texas in July 2008.
6. Southern Methodist University Computer Science and Engineering Colloquium September 2010. The topic was organized computer crime and computer terrorism. I was an invited speaker.
7. Takedowncon security conference in Dallas Texas, May 2011. The topic was steganography. I was an invited speaker.
8. An Overview of Modern Cryptography, May 5, 2011 Webinar
9. CAST Conference in Washington D.C. August 2011. The topic was Cryptography: Feistel Ciphers. The audience was primarily Department of Defense personnel and contractors. I was an invited speaker.

10. Digital Certificates: An Expert View, January 12, 2012 Webinar
11. Takedown security conference in Dallas Texas, May 2012. The topic was RSA cryptography. I was an invited speaker.
12. Problems with RSA, November 4, 2012 Webinar
13. Takedowncon security conference in Huntsville Alabama, July 15, 2013. The topic was cryptanalysis. The audience was primarily Department of Defense personnel and contractors. I was an invited speaker.
14. September 25-26, I conducted a 2-day master class in hacking techniques, in Singapore for Clariden Global. I was an invited speaker.
15. March 2014, I conducted a presentation for the University of Texas ACM chapter. The topics where distributed steganography and cryptographic backdoors.
16. May 26-27, 2014. I conducted a 2-day workshop in software testing in Singapore for Clariden Global. I was an invited speaker.
17. June 2014, I conducted a public talk on computer crime and internet safety in Melissa Texas, sponsored by the Melissa Police Department.
18. October 1, 2014 presentation of a talk on cryptographic backdoors at the ISC2 Security Conference in Atlanta Georgia.
19. October 5, 2014 presentation of a talk on cryptographic backdoors at the Hakon convention in Indore, India. I was an invited speaker.
20. October 17, 2014 U.S. Secret Service, North Texas Electronic Crimes (N-TEC) Task Force presenting a talk on the history and current state of computer crime. I was an invited speaker.
21. November 7, 2014 North Texas Crime Commission-Healthcare Cyber Security Symposium presenting a talk on health care breaches. I was an invited speaker.
22. January 27, 2015: Collin County Sheriff's Academy Alumni Association. "Cybercrime and online predators".
23. April 14, 2015 Brighttalk webinar “What you don’t know about Cryptography and how it can hurt you”.
24. May 4, 2015 North Texas Crime Commission-Healthcare Cyber Security Symposium presenting a talk on the causes and remediation of health care breaches. I was an invited speaker.
25. May 12, 2015 SecureWorld Houston “What you don’t know about Cryptography and how it can hurt you”.
26. August 20, 2015. Southwest Financial Crimes Forum “7 biggest mistakes of incident response.” I was an invited speaker.
27. September 30, 2015 ISC2 Security Congress “Cryptanalysis for Forensics”.
28. October 3, 2015. Conducted a 1-day workshop in Malware at Hakon India. I was an invited speaker.
29. October 4, 2015. Hakon India Indore India. 2015 “Cyberwar and Terrorism”.
30. November 4, 2015 iSMG Fraud Summit in Dallas Texas “Business Email Masquerading: How Hackers Are Fooling Employees to Commit Fraud”. I was an invited speaker.
31. November 5, 2015 SWACHA Electronic Payments Summit in Irving Texas “Emerging Trends in Cyber Crime”. I was an invited speaker.

32. May 25, 2016 “Improving Professional Standards in Cyber Forensics” Keynote speaker for Association of Digital Forensics Security and Law. I was an invited speaker.
33. June 22, 2016 the topic was “Cyber Security Issues Facing Business” Texas Security Bank Business Institute meeting. I was an invited speaker.
34. August 4, 2016 “Steganography: The in’s and Out’s” DefCon 24, Las Vegas.
35. September 12, 2016 USMCOC Third North American Sustainable Economic Development Summit Cyber Security, Information Technology & Innovation Panel. I was an invited speaker.
36. September 13, 2016 Tarleton State University CyberSecurity Summit at the George W. Bush Institute. The topic was "A template for incident response". I was an invited speaker.
37. September 28, 2016 Secure World Dallas. A presentation on "Analyzing Forensic Evidence -Applications of graph theory to forensic analysis”.
38. October 2, 2016 Hakon India (Indore India). A presentation on “The Dark Web Markets – Implications for Law Enforcement and Counter Terrorism”. I was an invited speaker.
39. October 18-19, 2016 Jordan Cyber Security & Forensics Forum (JCSFF-2016) Presenting two presentations. The topics were “Zero Day Exploits” and “How to forensically analyze Zero Day Exploits”. I was an invited speaker.
40. December 1-2. I conducted a 2-day advanced workshop on cyber-threat intelligence in Singapore for Clariden Global. I was an invited speaker.
41. January 17, 2017 the 2nd International Congress of the International Association of Law and Forensic Science (IALFS), in Cairo Egypt January 17, 18, 19. The topics were “Improving Digital Forensics” and “Applying Graph Theory to Model Forensic Examinations”. I was an invited speaker.
42. February 11, 2017. North Texas Cyber Security Association bi monthly meeting. Speaking on Dark Web Markets and their impact for law enforcement and intelligence agencies. Plano Texas Collin College Courtyard Campus.
43. February 17, 2017. American Academy of Forensic Sciences 69th Annual Meeting. Speaking on a novel approach JTAG phone forensics.
44. March 3, 2017. University of North Texas. A presentation on Applying Graph Theory to Analyzing Digital Evidence.
45. May 24, 2017. Enfuse 2017 conference in Las Vegas. A presentation on Applying Graph Theory to Analyzing Digital Evidence.
46. July 27, 2017. Defcon 25 2017 conference in Las Vegas. A presentation entitled “Windows: The Undiscovered Country” on undocumented features of Windows and SQL Server that can be used for hacking and penetration testing.
47. September 25, 2017 ISC2 Security Congress in Austin Texas. A presentation on" Applying Graph Theory to Analyzing Digital Evidence".
48. September 27 and 28, 2017. Secure Jordan conference in Amman. I presented two talks. The first is "An overview of current challenges in phone forensics". The second is " How to address dark web markets".
49. October 18-19 SecureWorld Dallas 2017. A presentation on "Cryptography, what you don't know and how it can hurt you".

Litigation Support Experience

I have worked for both plaintiffs and defendants in computer science related cases. These cases include software copyright, trademark infringement, patent cases, and computer crime related cases. In patent cases I have opined on both infringement and validity issues. I have also testified as to the valuation of computer software.

1. 2004-2005 AVG v. Microsoft, consulting for the firm of McKool Smith on behalf of the plaintiff AVG. This was a patent infringement case involving six patents. I was the testifying expert for one patent (the '286 patent) and a consulting expert for the others. This case involved software analysis for several hundred gigabytes of software source code as well as preparation of claim charts.
2. 2006 Harrison v. Comtech Solutions Worldwide Inc., consulting for the firm of Winthrop & Weinstine on behalf of Comtech Solutions. This was a software copyright infringement case. I was a consulting expert for this case.
3. 2006 The Weidt Group v. Cold Spring Granite Company, consulting for the firm of Winthrop & Weinstine on behalf of The Weidt Group. This was a software copyright infringement case. I was a consulting expert for this case.
4. 2008 Countryman v. NextMedia Inc., consulting for the firm Siebman, Reynolds, Burg, & Phillips on behalf of the plaintiff, Countryman. This case involved an alleged breach of network security. I was a testifying expert, the case settled before trial.
5. 2008-2009 Virnetx v. Microsoft, consulting for firm of McDermott, Will, and Emery on behalf of the plaintiff Virnetx. This was a patent infringement case. This case involved software analysis for several hundred gigabytes of software source code. I was a consulting expert for this case. The case went to trial in 2010.
6. 2010 SSL Services LLC v. Citrix Systems Inc., consulting for the firm of Dickstein and Shapiro LLC on behalf of the plaintiff SSL Services. This was a patent infringement case. I was a consulting expert for this case. Case No. 2-08-cv-158 (E.D. Tex.)
7. 2009-2012 Uniloc v. multiple defendants, consulting for the firm of Ethridge Law Group on behalf of Uniloc. This was a patent infringement case. I consulted and performed the analysis of over 100 potential defendants, determining if the products in question infringed. This involved analyzing the software utilizing standard network forensics techniques as well as reviewing source code. The case also required me to prepare over 100 claim charts. Case numbers including: No. 6:14-cv-00415 (E.D. Tex.) (ArcSoft, Inc.), No. 6:14-cv-00420 (E.D. Tex.) (Canon U.S.A., Inc.), No. 6:14-cv-00424 (E.D. Tex.) (Embarcadero Technologies, Inc.).
8. 2011-2012 Virnetx v. Cisco et. al.; Virnetx v Mitel, et. al., consulting for the firm of McKool Smith on behalf of Virnetx. This was a patent infringement case. I was a consulting expert for this case. This case involved software analysis for over 20 gigabytes of software source code for various Cisco

products. I also worked on the related Alcatel case and reviewed source code for those products as well. Case No. 6:10-cv-00417 (E.D. Tex.)

9. 2011 Parallel Networks v. Abercrombie & Fitch, multiple defendants and multiple law firms on behalf of approximately 80 defendants. This was a patent infringement case. Most of the defendant's I was working on behalf of, won summary judgement Case No. 6:10-cv-00111 (E.D. Tex.).
10. 2011 Nuance v. Vlingo, consulting for the firm of Hays, Bostic, & Cronnin, on behalf of Vlingo. This was a patent infringement case. I was a consulting expert for this case that involved extensive source code review. Case No. 1:09-cv-11414 (D. Mass.).
11. 2011 Eolis v. Adobe Systems Inc., et al., Consulting for the firm of Locke, Lord, Bissel, and Liddell on behalf of defendant Citibank. This was a patent infringement case. I was a consulting expert for this case. Case No. 6:09-cv-00446 (E.D. Tex.).
12. 2012 Smartphone case v. Apple on behalf of the firm of Hayes, Bostic, and Cronin on behalf of Smartphone. This was a patent infringement case. I was a consulting expert for this case. As part of my work on this case I reviewed Apple iOS source code. Case No. 6:13-cv-00196 (E.D. Tex.).
13. 2012 Smartphone case v. Android (HTC and Sony) on behalf of the firm of Nelson, Bumgardner, and Castro on behalf of Smartphone. This was a patent infringement case. I was a consulting expert for this case. As part of my work on this case I reviewed source code for several Android based phones. Case No. 6:10-cv-00580 (E.D. Tex.).
14. 2012-2013 Market One Models v. Tekcenture. For the plaintiff. This was a software copyright infringement case. This case also involved valuation of software and intellectual property. I was a testifying expert in this case. The case settled during trial. Dallas County CAUSE NO. CC-10-05682-A.
15. 2012-2013 Allstate v. Nationwide consulting for the firm Banner & Whitcoff, on behalf of AllState. This was a patent infringement case; I was a consulting expert for this case. My work on this case involved software source code review for insurance applications. The case settled before trial. Case No. 1:12-cv-03609 (N.D. Ill.).
16. 2012 Unified Messaging Solutions LLC v. Facebook Inc., Google inc., Intuit, etc. consulting for the firm of Nelson, Bumgardner, and Castro on behalf of Unified Messaging Solutions LLC. This was a patent infringement case. I was a consulting expert for this case. This case involved extensive software source code analysis. Cases No. 6:11-cv-00120 (E.D. Tex.) (Facebook), No. 6:12-cv-00085 (E.D. Tex.) (Intuit), No. 6:11-cv-00464 (E.D. Tex.) (Google).
17. 2012- 2013 DN Lookup Technologies v. Charter Communications et. al. Consulting for the firm of Lee, Jorgensen, Pyle & Kewalraman on behalf of DN Lookup Technologies. This was a patent infringement case. I was a consulting expert for this case. Case No. 1:11-cv-01177 (D. Del.).
18. 2013 Droplets v. Amazon, et al Consulting for the firm of Wilson, Sonsini, Goodrich, & Rosati on behalf of the defendants E-Trade, Charles Schwab, Ameritrade, and ScottTrade. This was a patent infringement case. I was a

consulting expert for this case. The case settled before trial. Case No. 3:12-cv-03733 (N.D. Cal.).

19. 2013 Andrews v. Medical Excesses LLC. Consulting for the firm of Maynard, Cooper & Gale on behalf of the defendant. This was a liability case involving a breach of network security. The case settled before trial. Case No. 2:11-cv-1074 (M.D. Ala.).
20. 2013 Macro Niche Software, Inc. and Michael j. Ruthemeyer v. 4 Imaging Solutions, L.L.C., Protech Leaded Eyewear, Inc. And Imaging Solutions of Australia consulting for the firm of Kevin R. Michaels, P.C on behalf of the plaintiff. This was a software copyright infringement case. This case also involved valuation of software and intellectual property. I was a testifying expert in this case. The case settled before trial. Case No. 4:12-cv-2292 (S.D. Tex.).
21. 2013 Geotag v. Frontier Communications et al. Consulting for the firm of Reese, Gordon, & Marketos on behalf of the plaintiff. This was a patent infringement case involving multiple defendants. I was a testifying expert in this case. The case involved extensive source code and product analysis. The cases settled before trial. Case No. 2:10-cv-00265 (E.D. Tex.).
22. 2013-2014 Geotag v. Starbucks et al. Consulting for the firm of Reese, Gordon, & Marketos on behalf of the plaintiff. This was a patent infringement case involving multiple defendants. I was a testifying expert in this case. The case involved extensive source code and product analysis. The cases settled before trial. Case No. 2:10-cv-00572 (E.D. Tex.).
23. 2013-2014 Geotag v. AT&T et al. Consulting for the firm of Malouf & Nockels LLP and the Winstead law firm, on behalf of the plaintiff. This was a patent infringement case. I was a testifying expert in this case. The case involved extensive source code and product analysis. The case settled before trial. Case No. 3:13-cv-00169 (N.D. Tex.).
24. 2013 MCNE, Inc. and David Todd McGee v Amarone Partners LLC, et. al. District Court of Dallas County. Consulting for the firm of Howie Law PC on behalf of the defendant. This was a software copyright infringement case. I was a testifying expert in this case, but the case settled before trial. Case Dallas County, Texas DC-11-03860.
25. 2013 PiNet v. J.P. Morgan Chase. Consulting for the firm of Puziniak Law Office on behalf of the plaintiff. This was a patent infringement case. I was a testifying expert on invalidity issues. The case settled before trial. Case 1:12-cv-00282 (D. Del.).
26. 2014 Pragmatus Telecom LLC v Volkswagen Group of America. Working for the defendant on behalf of the firm Locke Lord LLP. I was a consulting expert. The case settled before trial. Case 1:12-cv-01559 (D. Del.).
27. 2014 API Technical Services LLC vs Anthony Francis et. al. working for the defendant on behalf of the Wade Law Firm. I was a testifying expert in this case, the case settled before trial. Case 4:13-cv-627 (E.D. Tex.).
28. 2014 Ameranth, Inc. v. Genesis Gaming Solutions, Inc., for the defendant Genesis Gaming Solutions. This was a patent infringement case. I was a

testifying expert in this case, the case settled before trial. This case was in the Central District of California. Case 8:13-cv-00720 (C.D. Cal.).

29. 2014 Ameranth, INC v. ITCS INC., for the defendant ITCS. This was a patent infringement case. I was a testifying expert in this case, the settled before trial. This case was in the Central District of California SA 8:13-00720 AG. Case 8:13-cv-00720 (C.D. Cal.).
30. 2014 Neomedia Inc. vs Dunkin Brands Inc. Civil Action No.: 13-cv-02351-RM-BNB. I was retained by the firm of Nutter law on behalf of the defendant Dunkin Brands Inc. The case settled before trial. Case 1:13-cv-02351 (D. Colo.).
31. Neomedia v Marriot Intl. Inc Civil Action No. 14-cv-001752-KLM. I was retained by the firm of Ballard Spahr LLP for the defendant. The case settled before trial. Case 1:13-cv-001752 (D. Colo.).
32. 2014 Federal Trade Commission vs Boost Software Inc. for the defendant. Case 14-cv-81397 (S.D. Fla.). The case settled.
33. 2014 Federal Trade Commission vs PC Cleaner Pro Inc. for the defendant. Case 14-cv-81395 (S.D. Fla.). The case settled.
34. 2015 E AutoXchange LLC vs Academy, LLC. I am working on behalf of the defendant for the law firm of Wolfe & Wyman LLP. This was a software copyright infringement case. Case 1:14-cv-01278. The case settled.
35. 2015 Attorney General of Florida v ASAP Tech Help LLC, Working for the firm of Lubell & Rosen for the defendant. This case settled before trial. Case 2015 CA002751XXXXMB. Case concluded.
36. 2015 SNA1 S.p.A. v Barcrest Group Ltd. For the firm of Winget, Spadafora, & Schwartzberg on behalf of Illinois Insurance Company. I was a consulting expert. The case settled.
37. 2015 Suncoast Post-Tension LTD vs Peter Scoppa, et. al. US District Court Houston. For the firm of Macdonald Devin P.C., on behalf of the defendant. Case No. 4:13-cv-03125. Case concluded.
38. 2015-2017 Walmart Stores Inc. v. Cuker Interactive LLC. for the Henry Law Firm on behalf of Cuker Interactive LLC. Software trade secrets is the underlying matter in the case. Case has concluded.
39. 2015 United States of America vs. Anastasio N. Laoutaris. District Court for the Northern District of Texas, Dallas Division case no 3:13-CR-00386-B. Working for the firm of Law Office of John R. Teakell on behalf of the defendant. This was a criminal case involving alleged violation of 18 U.S.C. 1030 (a)(5)(A) and (c)(4)(B)(i). Case concluded.
40. 2016 VPN Multicast Technologies LLC vs AT&T Corp., Civil Action No.: 3:15-cv-02943-M. Patent infringement case. For the firm of The Simon Law Firm on behalf of the plaintiff. This case settled.
41. 2015-2016 Bradium Technologies vs Microsoft Cause 35:27 Patent infringement case. For the firm of Kenyon & Kenyon LLP on behalf of the plaintiff.
42. 2016 United States v Michael Thomas. Eastern District of Texas Sherman Division Case No 4:13CR227. For the firm of Tor Ekeland, P.C. on behalf of the defense. Case concluded.

43. 2016 Motio Inc. VS. BSP Software LLC, Brightstar. United States District Court for the Northern District of Texas Dallas Division Civil Action No. 3:16-cv-00331-O. For the firm of Walsh Law on behalf of the plaintiff. The case settled.
44. 2016-2017 Sanders et. al. v. Knight et. al. For the firm of Bradley, Murchison, Kelley, and Shea.
45. 2016 – 2017 Thomas Sisoian v. IBM. United States District Court for the Western District of Texas Austin Division Case No. 1-14-CV-565-SS. For the firm of DiNovo Price Ellwanger & Hardy LLP on behalf of the plaintiff.
46. 2016 – 2017 Evicam International, Inc. v. Enforcement Video, LLC, d/b/a WatchGuard Video. US District Court for the Eastern District of Texas, Sherman Division Case No. 4:15-cv-00105-ALM. For the firm of Reese, Gorden, and Marketos on behalf of the defendant WatchGuard Video on the topic of patent invalidity. Case has concluded.
47. 2016 – 2017 Uniloc USA v Cisco Systems Inc. Civil Action No. 6:15-cv-1175. Eastern District of Texas Tyler Division. Working for the firm of Prince Lobel, on behalf of the plaintiff.
48. 2016 – 2017 Uniloc USA v Facebook Inc. Civil Action No. 6:15-cv-223. Eastern District of Texas Tyler Division. Working for the firm of Prince Lobel, on behalf of the plaintiff.
49. 2016 – 2017 Uniloc USA v Huawei Enterprises Inc. Civil Action No. 6:15-cv-0099. Eastern District of Texas Tyler Division. Working for the firm of Prince Lobel, on behalf of the plaintiff. This case has settled.
50. 2016 – 2017 Uniloc USA v Unify Inc. Civil Action No. 6:16-cv-101. Eastern District of Texas Tyler Division. Working for the firm of Prince Lobel, on behalf of the plaintiff. This case has settled.

Testifying Experience

1. I testified at trial regarding patent invalidity on July 13th and July 14th, 2017 in the case of Evicam International, Inc. v. Enforcement Video, LLC, d/b/a WatchGuard Video.
2. My deposition was taken on June 27th in the case of Thomas Sisoian v. IBM. United States District Court for the Western District of Texas Austin Division Case No. 1-14-CV-565-SS.
3. My deposition was taken on June 17th in the case of Evicam International, Inc. v. Enforcement Video, LLC, d/b/a WatchGuard Video, on the issues of patent invalidity.
4. I testified at trial April 17 and 18, 2017 in the case of Walmart Stores Inc. v. Cuker Interactive LLC. July 12, 2016. Case No. 5:14-CV-5262
5. I testified at a hearing regarding multiple motions in the case of Walmart Stores Inc. v. Cuker Interactive LLC. December 12, 2016. Case No. 5:14-CV-5262
6. My deposition was taken in the case of Walmart Stores Inc. v. Cuker Interactive LLC. July 12, 2016. Case No. 5:14-CV-5262

7. I testified in the trial of United States v Michael Thomas June 7, 2016.
8. My deposition was taken in the case of Federal Trade Commission and State of Florida v Inbound Call Experts, LLC, et. al. Case No. 14-81395-CIV-Marra/Matthewman US District Court Southern District of Florida
9. I testified in the trial of Suncoast Post-Tension LTD vs Peter Scoppa, et. al. October 9, 2015.
10. I testified in the trial of United States of America vs. Anastasio N. Laoutaris, September 25, 2015 and September 28, 2015.
11. My deposition was taken in the Suncoast Post-Tension LTD vs Peter Scoppa, et. al. case August 27, 2015.
12. My deposition was taken in the Attorney General of Florida v ASAP Tech Help LLC case May 22, 2015.
13. I testified at a non-jury trial/hearing in the Federal Trade Commission vs PC Cleaner Pro Inc. case December 17, 2014.
14. I testified at a non-jury trial/hearing in the Federal Trade Commission vs Boost Software Inc. case November 24, 2014.
15. My deposition was taken in the Neomedia Inc. vs Dunkin Brands Inc. case relating to patent indefiniteness/invalidity issues on November 13, 2014
16. My deposition was taken in the Geotag v AT&T case relating to validity issues on July 9, 2014.
17. My deposition was taken in the Geotag v AT&T case relating to infringement issues on June 11, 2014.
18. My deposition was taken in the Geotag v. Starbucks et. al. case relating to invalidity issues in regard to the defendants Dominos and Darden May 15 2014
19. My deposition was taken in the Geotag v. Starbucks et. al. case relating to infringement issues in regard to the defendant Darden May 14 2014
20. My deposition was taken in the Geotag v. Frontier Communications et. al. case relating to infringement issues in regard to the defendants Gander Mountain and Abercrombie and Fitch 24 January 2014.
21. My deposition was taken in the Geotag v. Frontier Communications et. al. case relating to infringement issues in regard to the defendants Trane and Genesco 23 January 2014.
22. My deposition was taken in the Geotag v. Frontier Communications et. al. case relating to infringement issues in regard to the defendants Cinemark, Spencer's Gifts, and Regis Corp. on 22 January 2014.
23. My deposition was taken in the Geotag v. Frontier Communications et. al. case relating to infringement issues in regard to the defendants Walmart, Nike, and Advanced auto on 21 January 2014.
24. My deposition was taken in the PiNet v. J.P. Morgan Chase case relating to invalidity in January 2014.

25. My deposition was taken in the Geotag v. Frontier Communications et. al. case relating to infringement issues in regard to the defendants in Judge Gilstrap's court in December 2013.
26. My deposition was taken in the Geotag v. Frontier Communications et. al. case relating to alleged invalidity issues in regard to the defendants in Judge Gilstrap's court in December 2013.
27. My deposition was taken in the Microsoft v. Geotag case in regard to Google in December 2013.
28. I testified at an evidentiary hearing in the matter of Macroniche Software Inc. v 4 Imaging Solutions LLC, et. al. Southern District of Texas Houston Division.
29. I testified at the trial of Market One v. Tekcenture case in the Dallas County Courts in February 2013.
30. My deposition was taken in the Geotag v. Frontier Communications case in regard to the defendant Yellow Pages in September 2013.
31. My deposition was taken in the Market One v. Tekcenture case in December 2012.
32. My deposition was taken in 2011 in Eolas Tech. Inc. v. Adobe Systems, Inc., et al., Civil Action No. 6:09-cv-446 (E.D. Tex.) (On behalf of defendant, Citibank).

Professional Experience

From:	2005
To:	Present
Organization:	Chuck Easttom Consulting
Title:	Computer Scientist/Consultant

As an independent consultant, I have developed 2 electronic medical records software solutions, several small financial and web based applications, microcontroller programming, and consulted with various companies on networking and security issues. My consulting work has included security audits, penetration tests, and forensic analysis. I have also done corporate training and college teaching in a wide range of topics including network administration, network security, web development (HTML, JavaScript, CSS, ASP, ASP.Net etc.), programming (C, C++, C#, Java, VB, etc.) and database operations (MS SQL Server, MySQL, PostGres, Microsoft Access, Oracle, etc.). I also developed the advanced cryptography course for the EC- Council. I developed training courses for various companies such as SkillSoft and SimpliLearn in topics such as NoSQL, MongoDB, VMWare cloud, Information Systems Auditing, CSSLP certification prep, CISA certification prep, and others. I frequently consult with various companies on computer security, cryptography, forensics, and related issues. My consulting activities have included a variety of government agencies including U.S. and Foreign governments. Some of my training courses are through my own training

company CEC-LLC, which is approved by the U.S. Department of Homeland Security National Initiative for Cyber Security Careers and Studies (NICCS) https://niccs.us-cert.gov/training/search/cec-security-llc

From: 2003
To: 2013
Organization: Collin College (Professional Development Department)
Title: Adjunct Instructor (Part Time)

I taught professional development courses to IT professionals in programming (C, Java, C++, and C#), web development (HTML, JavaScript, CSS, and .net), networking, and network security. I have also designed and taught computer security courses for the college. These courses include:

- CompTIA Security+ Certification Prep.
- CISSP Certification Prep
- Hacking & Penetration Testing
- Computer Forensics
- Network Administration

From: 2003
To: 2005
Organization: Great American Insurance Company- Professional Liability Division
Title: Systems Director
Summary: In this position I oversaw all application development including complex insurance Windows applications, web development including extensive online systems, database administration with SQL Server, network administration on a Windows based network, and network security for a division of an insurance company. This role combined management with hands on work in all of these areas. I was first hired as Systems Manager, then after 12 months promoted to Systems Director. While in this role I oversaw and participated in the development of a web portal to allow customers to apply for insurance, renew policies, and check status. I personally developed an extensive reporting application. I also oversaw and participated in a complete re-writing of the underwriting application used by our underwriters. Development was primarily using .Net with Microsoft SQL Server as a backend.

From: 2000
To: 2003
Organization: Remington College
Title: Department Chair for Computer Information Systems department
Summary: I was initially hired as an instructor but was later promoted to department chair. I taught a variety of computer science courses and managed the Computer Information Systems department. I taught courses in programming, systems analysis, web development (HTML, JavaScript, Java Applets, and .Net), e-

commerce, and information security.

From:	1999
To:	2000
Organization:	Digital Speech Systems Inc.
Title:	Senior Software Engineer
Summary:	I began at digital speech as a software engineer and was later promoted to senior software engineer. My duties included developing voicemail and related software as well as mentoring new programmers. The programming work included work on voicemail server software, unified messaging software, and related applications. I worked extensively with C, Visual C++, SQL Server, and Visual Basic.

From:	1998
To:	1999
Organization:	Southeastern Oklahoma State University
Title:	Director of Academic Computing
Summary:	I began as the Director of Educational Technology for the School of Arts and Letters but then took over the management of the entire universities information systems when I was promoted to the Director of Academic Computing for Southeastern Oklahoma State University. In this position I managed all technical support for the campus as well as overseeing all network administration, network security, and web development.

From:	1996
To:	1998
Organization:	Alegis Corporation Systems Group
Title:	Software Engineer
Summary:	I began as a programmer/analyst and was later promoted to Software Engineer. I worked developing Windows based financial and collections applications for companies such as Boatman's Bank of St. Louis, Chrysler Financial, and Western Union. I worked extensively with C, C++, and Visual Basic (Versions 4.0 and 5.0). I also developed and oversaw the website or the company using HTML, JavaScript, and Cascading Style Sheets.

From:	1995
To:	1996
Organization:	Boeing Aerospace Operations
Title:	Contract Programmer/Analyst
Summary:	I worked as part of a team developing a Windows application to manage the maintenance and engineering tasks for the NATO AWACS. I worked with C, C++ and Visual Basic (starting with version 3.0) as well as Microsoft SQL

Server.

From: 1991
To: 1995
Organization: Worked various technical support and computer related jobs while attending college. From late 1993 to 1995 a great deal of time was spent developing websites with HTML (1.0), JavaScript (beginning with its release in late 1995). Among the websites I created were websites for: a computer store, two martial arts studios, a quarter horse ranch, and a university chess club. During that same time period I worked extensively with some of the early browsers such as Mosaic and Netscape (late 1994). Prior to 1992, in 1991 to 1993 I worked building and repairing PC's.

From: 1987
To: 1991
Organization: United States Army
HHC 5/21 Infantry Battalion
7th Light Infantry Division
Title: Highest rank E-4
Summary: Awards received – Army Service Ribbon, National defense medal, marksman badge with grenade component. Honorable discharge.

Continuing Professional Education

I am always interested in updating and expanding my education, and therefore participate in seminars, webinars, online courses, continuing education/professional development training, etc. In some cases, I retake introductory or intermediate courses as a refresher. Here is an exemplary list of such courses.

- Paul Deitel, Teaching Strategies for Visual C# 2008 from Pearson Publishing – 2010.
- Design and Analysis of Algorithms from Massachusetts Institute of Technology – 2012.
- Parallel Computing from Massachusetts Institute of Technology – 2013.
- Microsoft Technet - Windows 7 Feature Overview – 2011.
- Programming Methodology from Stanford University Center for Professional Development – 2012.
- Perl fundamentals from the Association of Computing Machinery 2012.
- Key Issues in Distributed Systems from Stanford University Center for Professional Development – 2013.
- Introduction to HTML5 and CSS3 from the Association of Computing Machinery – 2013.
- Software Program Control Flow Fundamentals from the Association of Computing Machinery – 2013.

- Harvard Extension School CS 50 Intensive Introduction to Computer Science. This was an intensive coverage of C, PHP, MySQL, Algorithms, and Data Structures. I took this course as a refresher – 2014.
- The Fundamentals of Conducting an Internal Investigation from Guidance Software (webinar) – 2015
- Carnegie Mellon University Software Engineering Institute - Trends and New Directions in Software Architecture (webinar)- 2015
- Analyzing Evidence from Mobile Devices, Including Hidden and Deleted Data. Oxygen Forensics (webinar) – 2015

- Technical Debt in Large Systems: Understanding the Cost of Software Complexity. Massachusetts Institute of Technology (webinar) – 2015
- Current Trends in Computer Security. Stanford University (webinar) – 2015
- Windows FE and Live Forensic Triage (webinar) Forensic Magazine. – 2015
- American College of Forensic Examiners course - Forensic Examination of CCTV Digital VTR Surveillance Recording Equipment. 2015
- American College of Forensic Examiners course - Developmental and Motivational Factors of Transnational Terrorists. 2015
- American College of Forensic Examiners course - Psychological Profiles of Terrorists. 2015
- Oxygen Forensics Trainer Certification Course – 2015
- Access Data FTK Online training course – 2015
- American College of Forensic Examiners course - Digital Forensics in the 21st Century – 2016
- Specialized Forensic Photography and Diagramming – June 2017

References to my work

The following sections are provided as examples of the impact my work in computer science has had in the field.

Media References

My computer science expertise has been sought out by reporters including:

- CNN Money interviewed me regarding alleged unbreakable cryptography http://money.cnn.com/2011/09/02/technology/unhackable_code/
- CBS SmartPlanet interviewed me regarding NSA and cryptography http://www.smartplanet.com/blog/bulletin/nsa-proof-products-protective-or-a-profit-motive/
- "NSA proof products: protective or a profit motive?" also appeared on ZDNet
- E-Books directory lists my “Moving from Windows to Linux” book as one of the top 10 Linux books http://www.e-booksdirectory.com/linux/top10.html.
- Lawrence Journal World interviewed me for a hacking story that was published August 6, 2006. The article was entitled "Hackers infiltrate Web site".

- GoCertify.com Author Interview "Author Interview: CCFP Certified Cyber Forensics Professional All-in-One Exam Guide" January 2015
- ISMG interviewed me regarding the JP Morgan Chase Breach of 2015 http://www.bankinfosecurity.com/interviews/what-jpmorgan-chase-breach-teaches-us-i-2982
- CIO Magazine (Nov 14, 2016) in the article "12 steps to lower your espionage risk" references my book Computer Security Fundamentals 3rd Edition
- Forensic Focus Magazine (June 2017) interviewed me regarding my work in applying graph theory to digital forensics.

References to publications

My books and articles have been referenced by numerous computer scientists, including being referenced in several Ph.D. dissertations and Master's Thesis'. A few of those references are included here:

Dissertations and Thesis citing my work

1. An assessment of user response to phishing attacks: the effects of fear and self-confidence by Deanna House, Ph.D. Dissertation in Information Systems, University of Texas Arlington.
2. Assessment of Users' Information Security Behavior in Smartphone Networks- Ph. D dissertation of Mohammadjafar Esmaeili Eastern Michigan University.
3. A cryptographically-based operating system security model that protects against privileged attackers. By Christian Pain Ph.D. Dissertation Murdoch University School of Information Technology
4. Assessing and Mitigating Information Security Risk in Saudi Arabia. Ph.D. dissertation of Abdulaziz Saad Alarifi. University of Wollongong
5. Reference Model Based High Fidelity Simulation Modeling for Manufacturing Systems by Hansoo Kim Ph.D. Dissertation, School of Industrial and Systems Engineering Georgia Institute of Technology.
6. Leadership Styles and Information Security in Small Businesses: An Empirical Investigation by Debasis Bhattachary, Ph.D. Dissertation, University of Phoenix.
7. The adoption of business-to-business systems by small and medium enterprises in Amman and the perceptions of its influence on performance and efficiency by Anals A. AlBakry, Ph.D. Dissertation, University of Southern Queensland.
8. Models, Services and Security in Modern Online Social Networks, Ph.D. dissertation of Alessio Bonti Deakin University, Australia.
9. Design of a Forensic Overlay Model for Application Development Linlin Ke, Master's Thesis, College of Engineering, University of Canterbury.
10. Forensic Analysis of Linux Physical Memory: Extraction and Resumption of Running Processes. ED Mougoue, Master's Thesis, James Madison University.

11. Motivations behind Software Piracy: From the viewpoint of Computer Ethics Theories. Bethelhem Tadele, Master's Thesis University of Oulu (Scandinavia).
12. Securing CAN Bus Communication: An Analysis of Cryptographic Approaches by Jennifer Ann Bruton. Master's Thesis National University of Ireland, Galway.
13. Guidelines for the Adaptation of the TETRA Educational Programme at Nelson Mandela Metropolitan University to Address Human Behavioural Issues. Master's thesis of Nico Pieter Fouché.
14. A DDoS Security Control Framework. Post graduate thesis of Lars Drost.
15. The Value of the Automated Fingerprint Identification System as A Technique in The Identification of Suspects. Madimetja Edward Mokwele, Master's Thesis University of South Africa.
16. Securing CAN Bus Communication: An Analysis of Cryptographic Approaches by Jennifer Ann Bruton. Master's Thesis M.Sc. in Software Engineering. National University of Ireland
17. Radical Reddits: into the Minds of Online Radicalized Communities. Utrecht University. Master's Thesis. Verhaar, P.
18. Encryption, storage technology and security of data at rest. Alkorbi, Mohammed. Master's Thesis, Unitec Institute of Technology.
19. Proactive Forensic Support for Android Devices. Karthik Rao. Master's Thesis: Master of Technology in Cyber Security. Amrita School of Engineering
20. The Value of The Automated Fingerprint Identification System as A Technique in The Identification of Suspects. Adimetja Edward Mokwel. Master of Technology Thesis University of South Africa.

Papers citing my work

1. Hackers, spies, and stolen secrets: protecting law firms from data theft by Alan W. Ezekiel. Harvard Journal of Law & Technology Volume 26, Number 2 Spring 2013Taming the diversity of information assurance & security - Journal of Computing Sciences in Colleges Volume 23, Issue 4 (April 2008) J. Paul Myers, Sandra Riela.
2. Adding information assurance to the curriculum - Journal of Computing Sciences in Colleges Volume 22, Issue 2 (December 2006) Richard Weiss.
3. Effect of Windows XP Firewall on Network Issues in Informing Science and Information Technology Volume 4, 2007 *Al-Rawi (King Faisal University Saudi Arabia), Lansari (Zayed University UAE)*.
4. Ahssan, M., Abdulkareem, I. (2017). A Proposed Non Feistel Block Cipher Algorithm. *The 1st International Conference on Information Technology*.
5. Assessing Risks of Policies to Patch Software Vulnerabilities Radianti, Sveen, and Gonzalez.
6. A study of efficient avoidance in the event of DNS (domain name system) failure - Proceedings of the 8thConference on 8th WSEAS International Conference on Automation and Information - Volume 8 Lin, Hwang, Lin.
7. Embracing the Diversity of Information Assurance & Security - Myers

8. A study of efficient avoidance in the event of DNS (domain name system) failure -Yang, Hyon, and Hankyu.
9. Social and Organizational Aspects of Information Security Management - K. Michael.
10. The Problems and Policy Alternatives for Cyber Security in the Networking Age by Lee Ki Shik.
11. Securing Small Business: - The Role of Information Technology Policy. Batten and Castleman.
12. The Impact of Virtual Private Network (VPN) on a Company's Network. Powell, J.M.
13. Thinking Globally: Incorporating an International Component in Information Security Curricula. Kiswani and Al-Bakari.
14. Security, ethics and electronic commerce systems: cybercrime and the need for information sharing security White and Long.
15. The Expanded Risk Horizon of Accounting Networks Utilizing Wireless Technology - David R. Fordham -AIS Educator Journal Volume: 4 Issue: 1 2009.
16. Researches on the IPv6 Network safeguard linked system - Ma Yue, Lian Hong, and Zhang Xiao Feng- Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference 2010.
17. Migration from Microsoft to Linux on Servers and Desktops. –Kumar.
18. Decision making process in migration from Microsoft to Linux –Kumar.
19. Automatic Generation of Intelligent JavaScript Programs for Handling Input Forms in HTML Documents Suzuki and Tokuda Dept. of Comp. Science, Tokyo Inst. of Tech.
20. Influence of copyrights over the relationships in elearning Ivan Pogarcic, Marko Pogarcic, Matej Pogarcic Polytechnic of Rijeka, University of Rijeka, Faculty of Law, University of Ljubljana.
21. Using Whois Based Geolocation and Google Maps API for support cybercrime investigations, Asmir Butkovic et. al.
22. Odyssey of Data Security with A New Perception. Ankita & Lavisha
23. Cyber Law: Approach to Prevent Cyber Crime. M Verma, SA Hussain, SS Kushwah.
24. The Internet-EDI Systems Adoption by Enterprises in Jordan: Descriptive Analysis of Adoption, Strategies and Benefits by Anas Al Bakri International Journal of Internet and Distributed Systems.
25. Encryption Protocol using some Pieces of Message as Key by S. Prakancharoen - International Journal of Applied Computer Technology.
26. A Patient Privacy Protection Scheme for Medical Information System by by Lu, Wu, Liu, Chen, and Guo. Journal of Medical Systems October 2013.
27. A study of information security awareness and practices in Saudi Arabia by Alarifi, A.; SISAT, Univ. of Wollongong, Wollongong, NSW, Australia. doi: 10.1109/ICCITechnol.2012.6285845.
28. Secure login by using One-time Password authentication based on MD5 Hash encrypted SMS by Sediyono, E.; Satya Wacana Christian Univ.,

Salatiga, Indonesia; Santoso, K.I.; Suhartono. doi: 10.1109/ICACCI.2013.6637420.
29. Design and Implementation of a Virtual Calculation Centre (VCC) for Engineering Students, by Alaeddine. Published in International Journal of Online Engineering. 2010, Vol. 6 Issue 1, p18-23.
30. Artificial Intelligence Tool and Electronic Systems Used to Develop Optical Applications, By Tecpoyotl-Torres et. al. Chapter 10 in the book Advances in Lasers and Electro Optics.
31. The entry on 'computer crime and security' in the Encyclopedia of Computer Science and Technology cites my Computer Security Fundamentals textbook.
32. University of British Columbia Law Review "In Plain View R V Jones and the Challenge of Protecting Privacy in an era of computer search"
33. "Researches on the IPv6 Network safeguard linked system" Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on (Volume:7).
34. The Criminalization of Identity Theft under the Saudi Anti-Cybercrime Law 2007 Journal of International Commercial Law and Technology vol 9, no2 by Suhail Almerdas.
35. An Optimized and Secured VPN with Web Service Networking and Communication Engineering vol 6, No2; by A. Balasubramanian, A. Hemanth Kumar, R. Prasanna Venkatesan.
36. Factors Affecting the Implementation of Management Information System In Selected Financial Cooperatives In Nairobi. Published in the International Journal of Social Sciences and Project Planning Management, Vol 1, Issue 2, 2014.
37. A New Classification Scheme for Intrusion Detection Systems by Bilal Beigh published in the International Journal of Computer Network and Information Security vol 6, No. 8, July 2014.
38. Santoso, E. (2014, June). The Role of Biometrics Technology to Support E-Governance in Public and Business Administration. International Scientific Conference "e-governance"
39. Mughal, S. (2014) Counter Measures to Mitigate Cyberstalking Risks: A Value Focused Multiple Criteria Approach.
40. Dragan, A. (2014). Hacking and Computer Crimes Computer Fraud - A Comparative Look at the New Criminal Code and the Criminal Code of the Republic of Moldova. AGORA International Journal of Juridical Sciences No. 1, pp 29-34.
41. Ramakic, A. Bundalao, Z. (2014). Data Protection in Microcomputer Systems and Networks. Acta Tehnica Corviniensis – Bulletin of Engineering (University of Bosnia and Herzegovina)
42. "Preventing Document Leakage through Active Document" by Aaber, Crowder, Fadhel, and Wills. World Congress on Internet Security (WorldCIS-2014).

43. Public Perception vs. the Reality of Bluetooth Security. Janczewski & Wong, International Conference on Information Resources Management (2010).
44. Security, ethics and electronic commerce systems: cybercrime and the need for information sharing security. Kisswani1 & Al-Bakro. International Journal of Liability and Scientific Enquiry. DOI 10.1504/IJLSE.2010.033357.
45. An Overview of Information and Communication Technology (ICT) in Jordan: Review the Literature of Usage, Benefits and Barriers. Al Bakri. International Journal of Internet and Distributed Systems. Vol.1 No.2(2013), Article ID:31349, DOI:10.4236/ijids.2013.12002.
46. Not So Funny Funny-Money: The Threat of North Korean Counterfeiting of U.S. Currency. Corbett. Stevenson University Forensics Journal. Vol 4 2013.
47. Pendekatan Model Ontologi Untuk Merepresentasikan Body of Knowledge Digital Chain of Custody by Prayudi, Luthi, Pratama. Jurnal Cybermaticka. Vol2, No 2 (2014)
48. Digital Chain of Custody: State of the Art. By Prayudi and Sn. International Journal of Computer Applications (0975 – 8887). Volume 114 – No. 5, March 2015.
49. Prayudi, Y., Ashari, A., & Priyambodo, T. K. (2014). Digital Evidence Cabinets: A Proposed Frameworks for Handling Digital Chain of Custody. Int. J. Comput. Appl, 109(9), 30-36.
50. Issac, R. M. (2011, March). Application of Cybernetics in Cyber Criminology. In Proceedings of the UGC Sponsored National Seminar on Cyber Criminology (NSCC~ 2011) at BPC College, Piravom, Kerala, India on (pp. 101-110).
51. Aaber, Z. S., Crowder, R. M., Chang, V., Fadhel, N. F., & Wills, G. B. (2014, December). Towards a Framework for Securing a Document outside an Organisational Firewall. In Cloud Computing Technology and Science (CloudCom), 2014 IEEE 6th International Conference on (pp. 1057-1062). IEEE.
52. Miškovic, V., Milosavljević, M., Adamović, S., & Jevremović, A. Application of Hybrid Incremental Machine Learning Methods to Anomaly Based Intrusion Detection. methods, 5, 6.
53. Graham, C. (2013). Terrorism. com: Classifying Online Islamic Radicalism as a Cybercrime. Journal Article| October, 21(8), 10am.
54. Odion, I. (2015). Data Security in The Cloud Using Serpent Encryption and Distributed Steganography. European Scientific Journal June 2015 edition vol.11, No.18 ISSN: 1857 – 7881 (Print) e - ISSN 1857- 7431.
55. Abdulaziz, A. (2015). Information Assurance Practices in Saudi Arabian Organizations. HCI International 2015, vol 529. DOI: 10.1007/978-3-319-21383-5_106.

56. MITTAL, P., & SINGH, A. A Study of Cyber Crimes & Cyber Laws in India.
57. What Common Law and Common Sense Teach Us About Corporate Cybersecurity. Stephanie Balitzer. University of Michigan Journal of Law Reform. Vol 49 (4), 2016.
58. Using 3-D Virtual Worlds as a Platform for an Experiential Case Study in Information Systems Auditing. By Moscato, Donald R.; Boekman, Diana M. E. Communications of the IIMA Vol. 10, No. 1.
59. Information Security Awareness in Saudi Arabia. Arifi, A., Tootell, H., Hyland, P. CONF-IRM 2012 Proceedings.
60. An Overview of Cloud Systems and Supply Chains in Jordan. Al-Bakri, A. Cloud Systems in Supply Chains. pp 195-213.
61. Dumpster Diving: A Study on Data Recovery and Exploitation. Weaver, R., Cazier, J. Conference: Southeast Institute for Operations Research and the Management Sciences, At Myrtle Beach, South Carolina

Universities using my books

A number of colleges and universities around the world have used, or are using one or more of my books as textbooks. Below is an exemplary sample of some of those universities.

1. Auburn University
2. University of Texas at Dallas
3. University of Dallas
4. University of Oklahoma
5. Arizona Western College
6. Kent State University Ohio
7. California State University, Los Angeles
8. Pennsylvania State University
9. University of Nebraska
10. University of North Dakota
11. Illinois State University
12. University of Southern California
13. Western Illinois University
14. University of South Carolina
15. University of Wyoming
16. Florida State University
17. East Tennessee State University
18. The Citadel
19. University of The Incarnate Word

20. Midwestern State University
21. University of S Carolina-Lancaster
22. Southeast Missouri State University
23. George Mason University
24. Queen's College New York
25. American Military University
26. Columbus State University
27. Texas Christian University
28. Liberty University
29. Illinois Institute of Technology
30. Rochester Institute of Technology
31. California State Los Angeles
32. Wentworth Institute of Technology
33. Western Nevada College
34. Eastern Florida State College
35. Florida State College
36. University of Southern Florida Sarasota
37. University of Alaska at Fairbanks
38. College of So Nevada-Cheyenne
39. College of S Nevada-W Charleston
40. Colorado Mesa University
41. Temple University
42. Calumet College – University of St. Joseph
43. University of Dhaka (Bangladesh)
44. Kurukshetra University (India)
45. Universiti Malaysia Sarawak (Malaysia)
46. Al-Zaytoonah University of Jordan
47. Trinity College of Puerto Rico
48. Technological Institute of the Philippines
49. Nigeria University
50. SRM University Chennai India
51. Louisiana Technical University
52. Brookdale Community College
53. Hagerstown Community College
54. Wake Technical Community College
55. Nashville State Community College

56. Delmar College
57. Southwestern Community College
58. Charter Oak State College
59. Triton College
60. Hartford Community College

In addition to the universities using my books, some of my books have been translated into additional languages including German, Arabic, Korean, and Mandarin.

Training

Since the late 1990's I have been teaching at least on a part-time basis. I have taught courses at colleges, technical schools, corporate training environments, and on site for companies and government agencies. Some of my training courses are through my own training company CEC-LLC, which is approved by the U.S. Department of Homeland Security National Initiative For Cyber Security Careers and Studies (NICCS) https://niccs.us-cert.gov/training/search/cec-security-llc
I have taught courses in the following topics:

1. HTML (including HTML 5 and CSS3)
2. JavaScript (including advanced courses)
3. Java
4. C and C++
5. VB.Net, ASP.Net, and C#
6. Objective C/iPhone programming
7. Microsoft SQL Server
8. Oracle
9. Microsoft Access
10. NoSQL (including MongoDB and CouchDB)
11. Computer Networks (routers, switches, virtualization, SDN, NFV, etc.)
12. Computer Hardware (motherboards, chips, etc.)
13. JTAG techniques for phone forensics
14. Certification preparation courses for the following certifications: CompTIA A+, CompTIA Network+, CompTIA Security+, CISSP, ISSAP, CEH, CISA, CSSLP, ECES, CND, and CHFI.
15. Computer forensics (phone forensics, Windows forensics, general forensic science, etc.)
16. Computer security (principles, IDS/IPS, Honey Pots, policies, DRP/BCP, cyber threat intelligence, etc.)
17. Cryptology (including advanced courses)
18. Math for cryptography including statistics, number theory, combinatorics, abstract algebra, graph theory, and related topics.
19. Windows Server (NT 4.0, Server 2003, Server 2008, Server 2012)
20. Secure programming (including web programming)
21. Linux

22. Hacking and penetration testing
23. Cloud Computing

I have conducted computer security (computer forensics, network security, penetration testing cryptography, etc.) related courses for a variety of government and law enforcement agencies, various law enforcement officers, friendly foreign governments, and a variety of corporations.
I have also created a number of video courses for companies such as Skillsoft on topics such as Secure Programming, MongoDB, NoSQL, Virtualization, Cloud computing, Digital Forensics, and other topics.

Technical Skills

The Following is an exemplary list of technologies. This is not meant to be an exhaustive list, but rather to provide a sample of computer technology areas within which I have expertise. I have experience and/or knowledge with:
Computer Hardware: CPU architecture, motherboard structure, chip programming/testing (using HDLs, SystemVerilog, etc.) and testing, etc.
Programming Languages: C, C++, Assembly, .Net (C#, VB.Net, etc.), Pascal, Python, PHP, Ruby, Perl, Objective C, Java, and SmallTalk.
Software Engineering: Design and testing methodologies. ISO 9000,ISO 15504, also known as Software Process Improvement Capability Determination (SPICE), UML, software complexity measurements, etc.
Web development technologies: HTML, JavaScript, PHP, CSS, ColdFusion, Flash, and Dream Weaver.
Artificial Intelligence: Expert systems, Fuzzy Logic, and AI Programming.
Cryptography: I have extensive knowledge of cryptographic algorithms such as: DES, Blowfish, Twofish, AES, Serpent, RSA, Diffie-Hellman, ElGamal, MQV, ECC, GOST, and others. I also have extensive understanding of cryptographic hashes, message authentication codes, and cryptographic protocols.
Mathematics: Discrete math, number theory, graph theory, and statistics.
Cell Phones: I am experienced with iOS and Android. I have worked with both operating systems extensively including teaching programming for both operating systems, and reviewing source code for both operating systems.
Networking: Network protocols, routers, switches, servers, IPv4, IPv6, Network models and concepts (TCP/IP, OSI, etc.), telecommunications, and network management. Also, very familiar with cloud computing with both theoretical knowledge and hands on experience with VMWare cloud.
Databases: MySQL, SQL Server, DB2, PostGres, Progress, Microsoft SQL Server, MS Access, Oracle, and SQL Anywhere. I have also worked with NoSQL databases including MongoDB and CouchDB.
Computer/Network Security: PCI standards, Common Criteria, penetration testing, computer viruses and other malware, disaster recovery planning, cryptology, firewalls,

IDS, Honey Pots, biometrics, chip security, cyber threat intelligence, and security policies & procedures.

Cyber Forensics: PC forensics, network forensics, cell phone forensics (including JTAG). Experience with a wide range of tools, including but not limited to: Guidance Software Encase, Access Data FTK, Paraben Sim Seizure, Oxygen Forensics, OSForensics, WindowsFE, and various open source tools.

Domains: The domains within which I have practical IT experience include finance & banking, insurance, education, customer management, geographical mapping/tracking, defense department applications, and medical applications.

Soft Skills: I have experience in valuing software and intellectual property as well as IT management related issues.