— The DataBus —

Monthly Newsletter of

The Dayton Microcompter Association

Volume XI (New Series) Nº 11 (November 2021)

Dave SCHWAB:

Raspberry Pi Zero 2 W

—Contents—

SAVE A TREE (or at least a branch)! If you prefer to print your DATABUS rather than read it directly from a monitor, don't print page 19 unless you need to become a member or renew your membership.

Post Office Box 4005
Dayton, Ohio 45401
(937) 777-DMA1
(777-3621)

Visit us at:
DMA1.org

Your 2021/22 Officers:

President
Gary Coy
Vice-President
Edwin Davidson
Secretary
Glady Campion
Treasurer
Pat Flynn
Officers need not be Trustees.

Trustees:

Glady Campion
Edwin Davidson
Patrick Flynn
Peter Hess
Chester Howes
Ken Phelps
Dave Schwab
Ed Skuya
Gary Turner

Webmasters:

Mark Camden
& Brent Kerlin

Webmaster Emeritus:
Dave Lundy, †4/13/20

Established in 1976, DMA is a group of Dayton-area professionals and enthusiasts in the field of computing and digital information technology. General Membership Meetings are usually held on the last Tuesday of each month. DMA has a number of Special Interest Groups (SIGs) in areas ranging from digital investing and genealogy to the Linux operating system. Each SIG meets according to its own schedule. DMA is a member of the Association of Personal Computer Users' Groups (APCUG) and the Affiliated Societies' Council (ASC). Click on any of the logos—including our own (top left)—to go to that organization's Web site.

Submissions ...

The DataBus welcomes compliments, complaints, suggestions, and especially articles. We can accept articles in ASCII, or as attachments in plain text, Microsoft Word, Open or Libre Office Writer, or, yes, even in WordStar (a word-processing program that goes back to about 1980!). Send articles to:

Editor@DMA1.org

All articles are subject to editing for spelling, grammar, usage, and space. Retain a copy of your work, as The DataBus cannot be responsible for loss. When articles are of roughly equal quality and importance, those by paid-up DMA members receive preference.

November Meeting: 7 P.M., Tuesday, the 30TH
No Driving—No Parking—No Charge*

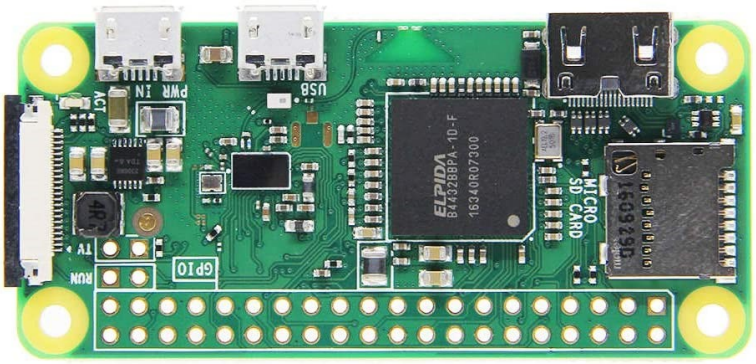
* This is a "hybrid" meeting: via Zoom, but also in person. Come at 6 P.M. if you wish to join us in person for dinner at T. J. Chump's Restaurant in suburban Huber Heights, next door to the Meijer's Supermarket. Click *here* for a map. The restaurant has free parking. It is also accessible via RTA bus routes 18 and 19, but there is a short walk from the bus stop in the Meijer's department store parking lot to the restaurant.

Dave SCHWAB: *Raspberry Pi Zero 2 W*

If you come in person, join us at 6 P.M. for dinner.
The Main Meeting starts at 7 P.M. via Zoom.

Raspberry Pi Zero 2 W

Presented by **DAVE SCHWAB**



JUST AS SMALL — FIVE TIMES AS FAST. There are three versions of Raspberry Pi Zero. The original appeared in 2015 at the amazing price of $5. In 2017, the Pi Zero W added Wi-Fi and Bluetooth and cost only $10. The very latest, the Pi Zero 2 W has been given a major upgrade with a quad-core ARM processor. This model is well worth the $15 and stores can't keep them in stock. [EDITOR'S NOTE: A quick check on the Internet shows that vendors are price-gouging by charging considerably more than the list price quoted in this article.]

Dave Schwab will explain the details on this little screamer. He'll run through the specifications and talk about how easy it is to program one of them. Dave is a long-time member of DMA, past presenter, current Trustee, and has had plenty of experience with all varieties of Raspberry Pi.

Inspired? Here is a list of projects built with a Pi Zero that could be improved with the Zero 2:

https://hackaday.io/projects?tag=raspberry pi

Our meeting starts at 7 P.M. DMA members will receive an invitation by e-mail for Zoom. Others may request an invitation using …

http://www.dma1.org/contact-us/

Or … join us in person at T.J. CHUMP'S, 7050 Executive Blvd, Huber Heights, OH. Click *here* for a map. (Free parking) Chump's restaurant is also accessible via public transit: RTA Bus Lines #18 and 19. Click *here* for the Route 18 weekday schedule (be sure it's the *weekday,* not the Saturday or Sunday schedule), and *here* for the Route 19 schedule (same comment as for Route 18). A short walk across the parking lot of Meijer's department store is necessary.

… TDB

Minutes are normally published almost two months late, because the Minutes for, say, the October Board meeting must be approved by the Trustees at the *following month's* meeting — in this case, early November. The corrected and approved October Minutes would thus appear in the October DATABUS (this issue), published toward the end of the month.

Trustees' meetings are on the *first Monday of each month,* except when that day is a legal holiday, for example: Labor Day in September. During the epidemic, Trustees began meeting via ZOOM. This was so successful that they have decided to continue the practice indefinitely. Meetings begin at 7 P.M. and are open to all DMA members. Request ZOOM credentials (that's a fancy way of saying "an invitation") from Treasurer GLADY CAMPION at the November General Membership meeting.

DMA Board of Trustees

MINUTES – Meeting of Monday, October 4, 2021

CALL TO ORDER

The meeting was called to order at 7:05 P.M. by Peter Hess, via ZOOM.

Trustees present: Glady Campion, Gary Coy, Edwin Davidson, Peter Hess, Chester Howes, Ken Phelps, Dave Schwab, Ed Skuya, and Gary Turner. Guests: Pat Flynn, Mark Camden.

OFFICERS' REPORTS

President – Ken Phelps

No report

Vice President – Peter Hess

Peter informed the board of a free online seminar on October 12 by Network for Good.

The planned speaker for our September meeting cancelled at the last minute. Edwin Davidson stepped in with information on Free and Open Source Software (FOSS).

Secretary – Glady Campion

Glady presented Minutes for the September board meeting. Edwin Davidson moved the Minutes be accepted. Ed Skuya seconded and the motion passed with Glady abstaining.

Treasurer – Pat Flynn

Pat presented a report for September.

—Notice—

Because of confidentiality concerns (for example, hackers could readily discover in what financial institutions DMA holds its assets), Treasurer's Reports are published. However, account balances are available to DMA members on request.

COMMITTEE REPORTS

Audit – Glady Campion

In progress

Fundraising – Peter Hess

Peter has asked the membership for a volunteer to do a Web survey, but no one has come forward yet.

Marketing – Peter Hess, Edwin Davidson, Pat Flynn, Debra McFall

Catherine Devlin has asked to join the Marketing Committee.

Peter sends out over 35 press releases each month.

(Continued on page 5)

(October Minutes—Continued from page 4)

Membership – Glady Campion

As of the end of September, we had 50 Regular, 4 Associate, 0 Student, and 5 Life members for a total of 59. Attendance was 27, including 17 who attended in person at TJ Chumps.

Prizes: Mike Stock chose the WD Elements SE 1TB external hard drive. Gary Coy picked up the Cooler Master MM711 gamer mouse. Eric Ottoson snagged the Sony WH-CH510 wireless headphones. Kathleen Kannik grabbed the Tenda 5-port gigabit switch.

Net Admin Team – Ken Phelps, Gary Turner, Pat Flynn, Brent Kerlin, Mark Camden

Mark e-mailed the Trustees a report by Wordfence on the security of our website, reporting no threats. He updated the list of Trustees on the Web site and added the DMA Bylaws as a PDF document.

Programs – Peter Hess

Thanks to Edwin Davidson for talking about Free and Open Source Software.

October – Gary Coy and Ken Phelps will put together a presentation on Windows 11 and Cybersecurity.

Peter continues to work on bringing in speakers from MetroNet and Generac.

Other suggested topics: Ransomware, Deep Fakes, Streaming video, Car hacking, Chromebooks, Bitcoin and Block chain, InitiativeQ.com, Data.ohio.gov, and converting laptops to Chromebooks.

Publications – Martin Arbagi

The September DataBus issue was posted to the Web site. Martin submitted the DataBus for the APCUG newsletter contest.

UNFINISHED BUSINESS

Wright State Archives – Martin Arbagi, Glady Campion

Still in progress

Next Board Meeting

The next Board Meeting will be 7:00 p.m. on Monday, November 1, 2021. We will continue to use Zoom.

List of DMA accounts – Glady Campion

Glady is continuing work on a list of all accounts currently held by DMA.

Summer Picnic – Glady Campion

Our picnic was held Saturday, August 28, at Shellabarger Park in Riverside. There were 32 people who attended. Glady submitted a list of items purchased as door prizes for the picnic.

Gary Coy moved that Glady be reimbursed for the $1219.55 spent on door prizes. Dave Schwab seconded and the motion passed with Glady abstaining.

Holiday Party – Glady Campion

Glady expressed concern about an indoor event with what will likely be another wave of infections (the so-called o [omicron] mutation) during winter months. After some discussion, the Trustees agreed to postpone the party another year.

Use of the DMA Zoom Account – Peter Hess

Peter asked for a motion on the use of the DMA Zoom account for groups not part of DMA. Currently Mark Camden uses it for Dayton WordPress training sessions. Edwin Davidson wants to use it for a writers group that meets on 3rd Tuesdays.

Dave Schwab moved that the DMA Zoom account may be used for educational events, free of charge, (1) if the use is approved by the DMA officers, (2) if the event does not interfere with one previously scheduled by DMA or a special interest group, (3) if the use is in the spirit

(Continued on page 7)

Have a business card? Are you a DMA member?

Any paid–up member of the Dayton Microcomputer Association is entitled to a *free* business card–sized advertisement in The DataBus. Send a good–quality image (600 dpi or better) to Editor@DMA1.org, or give your business card to **Martin Arbagi,** the Editor, at any DMA meeting. We can embed a link to your Web site (if you have one) within the image of your card. Under weird IRS regulations, your Web site may not include discount coupons for DMA members, although discount offers may be included in the advertisement *itself.*

☺ Help DMA by using Amazon's Smile program! ☺

Amazon, the Internet's largest retailer (if you haven't noticed, Amazon isn't just for books any more!) has a "Smile" feature whereby Amazon donates a percentage of almost any purchase you make to a selected nonprofit organization. There is *no* extra cost to you. Click *here* to learn more or *here* to go directly to the sign-up page. Be sure to put DMA down as the beneficiary of your purchases.

(OCTOBER MINUTES—Continued from page 5)

of the DMA mission, and (4) if the person using the account is a current member of DMA. Gary Coy seconded, and the motion passed.

NEW BUSINESS

Election of Officers – Peter Hess

Congratulations to ...

President: Gary COY; Secretary: Pat FLYNN;

Vice-president: Edwin DAVIDSON; Treasurer: Glady CAMPION

VOLUNTEER OF THE MONTH/QUARTER/YEAR

Ed Skuya was nominated as Volunteer of the Month for working the ZOOM connection for DMA meetings at TJ Chumps every month. He uses his laptop to connect with the ZOOM session and provides audio and video for all those attending in person.

ADJOURNMENT

Gary Coy moved to adjourn at 9:31 P.M. Dave Schwab seconded and the motion passed.

Respectfully Submitted,

Glady Campion,

... Secretary

The Officers & Trustees of The Dayton Microcomputer Association extend their Best Wishes for an enjoyable 2021 Holiday Season.

… But see the bottom of page 17.

Patronize Our Member–Advertisers!

Have you heard....?

Compiled from various sources

October, 2021

Facebook Name Change

At the company's annual Connect conference this Thursday, Mark Zuckerberg reportedly plans to discuss the renaming of Facebook to reflect its focus on building the metaverse, according to an unnamed knowledgeable source. The company aims to be known for more than social media. The rebranding will likely involve the formation of an umbrella company to oversee Facebook along with Instagram, WhatsApp, Oculus, and its many other acquisitions.

… Cnet, TheVerge

Android apps on Windows 11

Microsoft is currently allowing Windows 11 testers to try out Android apps. A preview version of the Windows Subsystem for Android is currently available to some beta testers of Windows 11, those who have Intel, AMD, or Qualcomm processors. The Android apps will run side by side with Windows apps. Microsoft built a subsystem in Windows 11 to enable Android app support. It includes the Linux kernel and an Android OS based on the Android Open Source Project (AOSP) version 11. Microsoft is currently enabling Android apps only in the Beta Channel of Windows 11, with plans to bring the preview to Dev Channel users "down the road."

… TheVerge

3D Videos with just a Phone Camera

A 3D image of a person inserted into a video game or as a visual effect in a movie is usually constructed with an intricate process known as "volumetric capture", involving dozens of cameras in a professional studio. But an Irish startup called Vologrames has made the process available to anyone with an iPhone and their free app Volu. First launched on the App Store in September, it will soon be available on Android. It's the first content creation app capable of turning standard mobile video into augmented reality. The phone camera captures video from one angle and the app uses artificial intelligence to add the 3D shape and texture in areas that the camera does not see.

… CNN Business

State Department to form New Cyber Office

In order to confront cybersecurity challenges such as ransomware and waning global security, the

(Continued on page 10)

(Digital Whispers/Have You Heard?—Continued from page 9)

State Department plans to create a bureau of cyberspace and digital policy, reporting directly to the Deputy Secretary of State, at least for its first year. The changes are designed to allow better response to state-sponsored intrusions of US government networks, theft of intellectual property, and interference in US elections.

… The Wall Street Journal

MacOS Monterey

This year is the 20th anniversary of Apple's MacOS operating system, and Apple celebrated with the release of MacOS Monterey in late October.

… Cnet

Beethoven's Tenth Symphony

When Ludwig van Beethoven died in 1827, he had started work on a tenth symphony. But due to his poor health, all he left behind were a few musical sketches. Ever since, musicians have wondered what this tenth work might have become. So a group of scientists at a startup called Playform AI spent two years teaching a machine Beethoven's entire body of work and his creative process. A full recording of the newly created tenth symphony was released this month the same day as the world premiere performance was scheduled for Bonn Germany. The effort was launched by Dr. Matthias Roder, director of the Karajan Institute in Salzburg Austria as part of an effort to celebrate the composer's 250th birthday.

… Smithsonian Magazine

A/V Comparatives Releases Latest Effectiveness Tests

Regular readers of The DataBus know **A/V Comparatives** (A/V) as the Austrian outfit that emulates Consumers' Union, the American nonprofit that publishes the popular *Consumer Reports* magazine (CR). CR takes no advertising, deriving its revenues primarily through sales of its publications, contributions, and "nonrestrictive government grants." CR can thus make impartial judgements on various products based on testing in its laboratories. A/V tries to do the same thing with cybersecurity products, though it does accept "sponsorships" (nonrestrictive grants) from private industry as well as from the Austrian government, and contributions from individual donors.

AV Comparatives has released its 2021 scores for selected consumer security programs, that is, those aimed at consumers using their digital devices at home or for personal reasons. It can be found here. Quick summary: Avira (a German company) and Avast (originally a Czech outfit, but recently bought out by the Norton Lifelock Company) scored highest on consumer applications, tying for first place. Tests of "enterprise" products, that is, security programs aimed at businesses rather than individual consumers, can be found here.

… AV Comparatives

Compiled by Glady Campion, except for the last item, which was contributed by Martin Arbagi.

DMA Events for Nov 21 – Dec 25, 2021

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
Nov 21	Nov 22	Nov 23	Nov 24	Nov 25 	Nov 26 **Python Self-Study** Noon, Online See http://d8ndl.org	Nov 27
Nov 28	Nov 29	Nov 30 **MAIN MEETING** 7:00pm Online -AND- TJ Chumps 7050 Executive Blvd Huber Heights	Dec 1	Dec 2 **Genealogy SIG** Restarting 6:30pm Online	Dec 3 **Python Self-Study** Noon, Online See http://d8ndl.org	Dec 4 **Classic Computers** 3:00pm By phone
Dec 5	Dec 6 **DMA Trustees** 7:00pm Online	Dec 7	Dec 8 **Dayton Dynamic Languages** 7:00pm **Innovation Hub** / online http://d8ndl.org	Dec 9 **NASAC** 6:00pm Xenia Library	Dec 10 **Python Self-Study** Noon, Online See http://d8ndl.org	Dec 11
Dec 12	Dec 13	Dec 14 **Investment SIG** 7:00pm Online Investment_sig @dma1.org	Dec 15	Dec 16 **Linux SIG** 7:00pm 348 Russ Eng Wright State Univ. Colonel Glenn Hwy Beavercreek	Dec 17 **Python Self-Study** Noon, Online See http://d8ndl.org	Dec 18 **Classic Computers** 3:00pm By phone
Dec 19	Dec 20 **Apple Dayton** CANCELLED	Dec 21 *Winter Begins* 	Dec 22	Dec 23	Dec 24	Dec 25 *Happy Holidays* 

A Monkey and a Typewriter Make a Hash with Shakespeare and a Soccer Ball *Being* Part 2 of Passwords and Hash

By Arthur Gresham, Editor, UCHUG Drive Light
Under the Computer Hood User Group
www.uchug.org
1editor101 (at) uchug.org

This is a follow up to part 1 *PASS(word) The Beef, the Hash, the Salt for Einstein, and a Dictionary,* which, if you missed it is here:
https://docs.google.com/document/d/1nhni0e-gjnb5yZwcmQv6fdINksdqqDJpFVBgHnknY3k/edit#
[Editor's Note: It's also available in the previous issue (October 2021) of The DataBus, on line as a PDF file at: 2110.pdf (dma1.org)]

This discussion is a follow-up to Part 1: "PASS(word) The Beef, the Hash, the Salt for Einstein, and a Dictionary," in which I introduced the process of hashing passwords and the concept of Salt.

During a continuing discussion with a friend, while writing Part 1, I finally realized that we were looking at the same things and coming to different conclusions regarding passwords. For example, we debated whether passwords stored as a hash code are really easy to un-encrypt (decode/crack/break/hack) or really hard.

We Both Win

It turns out we are all using the wrong terms. Yes, the hash code for a short password is of little value because it can be determined quickly. He wins. But it is also a fact that a hash code cannot be un-encrypted. I win. I will demonstrate both of these concepts in this article.

The big problem is because several terms are being incorrectly used for the world of hashing and passwords. Let me explain by using very simple examples from our shared experience.

The Gorilla in the Room

You may recall a theoretical discussion when you were in school. Something about a monkey in a room with a typewriter being able to write the works of Shakespeare if he has enough time to randomly peck the keys. This thought experiment is called the **Infinite monkey theorem** (read about it in Wikipedia[1] if you have forgotten how it works).

The strings produced by Hash Algorithms look like something you might think was written by that monkey. We expect that most of what that monkey typed is gibberish. Likewise, the hash for a particular input text (or a picture or an entire operating system, library, or simple password) is an' indicator'. This text appears to be pure gibberish. That is because it does not contain anything actually from the input. The key here is "contain."

The Key is the Container

Let me illustrate that in a different way. You are all familiar with ZIP or RAR, or other compression functions. You have undoubtedly downloaded some program, text, spreadsheet, or audio file, which was sent to you as a compressed file. When you get the file, you "unzip" it into a folder, then read, watch, listen to, or somehow use the contents inside that file. The zip was much smaller than the original contents inside of it. Yet, it contains an EXACT duplicate of the original inputs. If it didn't, you would be very upset. Your program would not run, or

(Continued on page 13)

(HASHED PASSWORDS—Continued from page 12)
your audio would not play, or the words in the text would turneenloiariuwwka08qkj k3lksd fjasdhd rhandnt making you very confused and unhappy. This is a two-way process, In and out.

Hash Algorithms are not a zip of the original input. While the Zip file was easy to unzip because it is designed as a *two*-way process, the Hash is a *one*-way process. You can MAKE a hash, but you can't UN-MAKE it. It does not "contain" any information about the input string; it cannot be cracked. Again, this is a one-way process. What goes in can not come out.

As an extreme example, this week, I installed a new version of Linux on the computer I am typing on right now. The download was a 2 Gigabyte file. Part of the install instructions are to compare the SHA-256 Hash[2] of this download with a given 256-byte check value. The SHA-256 Hash from the authorized site must match your value to ensure that yours is a complete, unaltered download. But the SHA-256 Hash does not contain all of Linux Mint 20.2 Cinnamon and all its files. If it did, I could have just downloaded the Hash, un-made it, and installed it. So, the files aren't contained in the Hash.

Yet if I create the SHA Hash for the string "A" (that is just the letter A), I will still get a 256-byte hash value. And it certainly does not compare to the contents of my Linux download.

This is because a Hash is only what is called an "indicator" value.

The Container has a Key

Let me give you another example and use a couple of other terms that have been misused in this discussion. Perhaps you remember WW II (No, I am not trying to age check you, so put your hearing aids back in your ears and listen up.) During the war, the radio became a vital tool for communications. The allies used it to communicate from London to the generals in the field. But they did not simply use plain words to give instructions. Instead, those instructions were processed with machines that scrambled the letters. The messages were "encrypted." Headquarters used a KEYCODE to garble the text. That text was sent by radio, and anyone with a receiver could get it. But only our side (mostly) had the matching KEYCODE to *un*-encrypt the message.

With our fast, modern-day computers, perhaps we could now DECODE or CRACK those messages (simple cipher codes), but they did not have the means to do it then, so the messages were secure.

But here again, the messages were designed as Two-way messages, containing the plain text going in and coming out with the same exact text when un-encrypted. If it wasn't exact, it would have been of no use in the war effort.

With Hash Algorithms, there is no Container. There is no Key. No Unzipping. No Coding-No De-Coding, No Encryption-No Un-Encryption. Because a Hash is only an "indicator" value.

Time to make Hash

Time for some fun. I want to program *your* brain. I want *you* to be my Hash Function Computer. You will have only one job. That is to give me an answer to the question I will ask. Trust me, you have the brainpower to do this.

Here is your input text:

I am larger than a softball, smaller than a basketball, I am covered with black and white pentagon shapes, and if you kick me into the net, you will score one point What Am I?

Hint: don't Google it. You will not find the answer ... Just think ...
Don't peek ... Time is Money ... Got your answer?

(Continued on page 14)

(HASHED PASSWORDS—Continued from page 13)

Did you make hash?

If you said "*soccer ball,*" you are right. Those 11 characters are the hash of that input string. I told you this was easy. BUT if I had said to you *"soccer ball"* at the beginning of this article or in a conversation, what is the chance you would have responded with the exact text: "*I am larger than a softball, smaller than a basketball I am covered with black and white pentagon shapes, and if you kick me into the net, you will score one point What Am I?*"

But wait. There are many Hash Algorithms and what you just gave me was the American-11 algorithm. What would you have said if you lived in London?

Sure, I hope you understand in that part of the world, they say *football* instead of soccer. Because that, you see, is the British-8 algorithm, not to be confused with the Spanish-6 algorithm, which would have used *fútbol*. Different algorithms might produce different lengths. Yet, they are all only "indicators" of the *same* exact input. But they do not un-anything any of them. The Hash does not contain the input string. So it can't be cracked.

A Hard Nut to Crack?

In the paragraph titled "We Both Win," I said: **"**the hash code for a short password is of little value because it can be determined quite easily**."**

While a short input text of a hash code may be determined quite easily, note that I did *not* say it could be un-Encrypted or cracked. For this demonstration, I will be using the Art-4 algorithm. Thus, any input string will generate a 4-character hash (cuz my brain is very small).

You will be playing the part of the Internet's bad guys. First, I will show you five input strings (a dictionary of passwords) that have been hashed with the Art4() algorithm. This will represent the bad guys' precomputed Hash Table Dictionary (see part 1 for a description of this).

Input String ART4() hash

AAAAAAAA = aee9
longword = 9546
Password = dc647
Password99 = e6ab
Willam1 = b4b9

(Note all of these passwords have been Pawned[3]. Someone has actually used them!)

Imagine a bank had a Data Breach (someone inside opened an e-mail and clicked on a "Link." You know the rest of the story!) The bank had saved customers' passwords using my algorithm. Their records are in the database, which was stolen from a bank.

I want YOU to see if you can "Crack" any of the bank's data and tell me whose password you "cracked."

Here is a bit of the data breach file:

User Name	Password hash	Balance
Joe	3255	$ 10,100
Mary	7bb4	101,000

(Continued on page 15)

(HASHED PASSWORDS—Continued from page 14)

User Name	Password hash	Balance
Beavis	9546	$ 52.14
Bill	5835	250,000.00

(It takes time, but the lookup yields results — look carefully)

So, did you "Crack" any of the hash values in the bank's data base? Could you try to log in with the password of any of these victims?

It looks like user Bevis may lose his savings. Maybe his *longword* just was not long enough. But did you actually "Decrypt," "Decode," "Crack," "Hack," or "Reverse Engineer" any of the passwords?

No! You simply found a value that matches a known hash (you found it in your Hash Table Dictionary), and you "Guessed" what one of the passwords might be. And you would be exactly correct because, as we learned from Einstein in part 1: "We *expect* to get the same results for a given string every time. To get anything different would be crazy." [EDITOR'S NOTE: It may be well to repeat the observation I made in the first part of this article, published in the October issue of THE DATABUS: There is no evidence that Professor Einstein ever said or wrote this witticism. In any case, anyone who uses a digital device with a touch screen knows that repeating the same action again and again often *does* yield different results!]

By the way, customer Bill, whose root password is William1, will not be in trouble because he salted his password. So, unless you bad guys hash his actual password ("*William1"*) plus his salt (which is "*PlusPepper*") to get an ART4() hash of 5835, you will not be getting into his account.

And because the bank did not SALT the customers' passwords, a plain language hash dictionary leaves many customers vulnerable for this look-up solution.

Do not let that be you. Use Good Passwords, not common short words or expressions that will be found in the dictionary. And when you do enter or change your password, use SALT if it's valuable, SALT it. **... TDB**

References

1 Infinite monkey theorem: click for the Wikipedia article.
https://en.wikipedia.org/wiki/Infinite_monkey_theorem

2 SHA-256 https://www.freeformatter.com/sha256-generator.html#ad-output has a good tutorial.

3 *Pawned Passwords* is a dictionary of 613,584,246 real-world passwords previously exposed in data breaches. This exposure makes them unsuitable for ongoing use as they are at a much greater risk of being used to take over other accounts. Has *your* password already been compromised? https://haveibeenpwned.com/Passwords

Advantages of New Wi-Fi Standards—Geek Free

By Joe Callison, Author, GEEK FREE & FOR~GO (For Geeks Only) blogs;
Convener, Senior Techies SIG
Seniors Computer Club of Greater Kansas City
https://kcsenior.net/
sencommember00 (at) gmail.com

Wi-Fi technology and the routers and Wi-Fi adapters using it have advanced a lot in recent years. It is difficult to explain the nuances of Wi-Fi technology without getting "geeky," so bear with me a little as I attempt to explain some of the terminologies as simply as I can.

The IEEE 802.11 standards for Wi-Fi have used letters to designate each new generation of design, with b, a, g, and n being the most well-known by consumers as the first four generations. The next generation to appear was ac, which was a confusing change in the naming sequence, so it is often referred to simply as Wi-Fi 5 or 5th generation Wi-Fi. The first generation is designed to take full advantage of new technology that was started but not fully implemented in the n or 4th generation. Both take advantage of 2.4GHz and 5GHz frequencies to provide more and faster channels.

Still, the capability of using multiple inputs and multiple outputs (MIMO) to communicate with a device for even faster or more reliable communications was only standardized under Wi-Fi 5. In addition, MIMO could be used electronically to change the antenna beam pattern of the router to focus the signal in the direction of the device it with which was communicating. Wi-Fi 5 standardized the method of communication between the devices and the router to enable interoperability of the router with all brands of Wi-Fi 5 adapters that support this "beamforming" technology instead of proprietary designs that depended on buying matching equipment from one supplier.

To use beamforming technology (which may go by various names by different brands) with multiple devices simultaneously, multi-user MIMO (MU-MIMO) is required, with the number of antennas and radios supported designated as 2×2 or 3×3 or 4×4 for 2, 3, or 4 simultaneous data streams with Wi-Fi 5. Each MU-MIMO data stream can also be multiplexed (divided up) into up to 3 data streams to provide concurrent single data streams to a total of anywhere from 2 to 24 devices depending on the number of MU-MIMO data streams supported by the router. Non-MIMO communications can connect more total devices with the router, but they take turns, one at a time for each frequency, instead of having simultaneous access to the router.

The newest Wi-Fi standards for consumer products are designated with an ax and referred to as Wi-Fi 6 or 6th generation Wi-Fi and support up to 8 simultaneous MU-MIMO data streams. In addition, there is even an enhanced Wi-Fi 6 called Wi-Fi 6E that adds 6GHz frequency antennas and radios for even more and faster channels of communication. For more information on Wi-Fi 4 through 6E, see the following links:

What Is Wi-Fi 6E? | PCMag
WiFi standards explained: WiFi 4 vs WiFi 5 vs WiFi 6 (minim.com)
Buying a new router? Understand these Wi-Fi basics first - CNET

For links to articles on the best routers for 2021, see the following:

(Continued on page 17)

(Wireless Routers—Continued from page 16)

The Best Wireless Routers for 2021 | PCMag
The 8 Best Routers To Flood Your Home With Wi-Fi (popularmechanics.com)

Why might you need a new router? If your current router is several years old; and you are planning to use a 4K or 8K smart television or streaming video device, or you have many different devices using your router at the same time (the average U.S. home has over ten devices that may be in use), or you are concerned about your router security, or if you or your grandkids are gamers or cryptocurrency miners, then you should probably consider buying a new Wi-Fi 6 router.

At this time, there are not many 6GHz devices utilizing 6E, and the routers and adapters can get expensive. Tests on 6E capable routers that are currently available do not show many advantages over Wi-Fi 6. You would probably benefit more from a router with two 5GHz antennas than a router with one 5GHz and one 6GHz. This may change in another year, or two and prices should become more reasonable as more 6E hardware becomes available.

Remember that to take full advantage of these new routers, you will need Wi-Fi adapters that use the same Wi-Fi standards and features, such as MU-MIMO, as the router. Adapters are available for upgrading laptops and desktops to the new standards, but other devices without USB ports that can support Wi-Fi adapters, like phones, are not upgradeable. They will still work fine with the new routers. In addition, your Internet service speed must be high enough to make a meaningful difference in performance with a faster router. You probably will not see much of a speed gain unless you have at least 300Mbps Internet service, but speed alone may not be the reason to replace your old router. **... TDB**

In view of lingering concerns about the COVID epidemic, the Board of Trustees has voted *not* to hold our usual DMA annual Dinner this year.

See you next year!

About The Dayton Microcomputer Association, Inc. (DMA)

By Peter Hess, DMA President, 2018-2020

About forty-five years ago, a small group of computer enthusiasts from the Dayton, Ohio area gathered around a kitchen table looking at, and playing with, an early personal computer called the Altair 680 that one of them had purchased. This computer had been featured earlier on the cover of the January 1975 issue of *Popular Electronics* magazine. Paul Allen had shown the selfsame article about the Altair to Bill Gates, and later, they wrote software together for that computer. Still later — and still together — Allen and Gates founded the Microsoft Corporation.

Shortly thereafter, those Dayton-area computer enthusiasts joined together with many others to form The Dayton Microcomputer Association (DMA), now one of the oldest (if not *the* oldest) continuously-operating computer user groups in the world. Typically, computer user groups, and the newer iteration, technology user groups, are volunteer-run operations. The DMA is an all-volunteer led, organized, and run 501(c)(3) non-profit organization.

Now, there are hundreds of computer (or technology) user groups in the world, all of which continue to foster improved communication between technological equipment and software publishers, and users of their products. User groups (both computer and technology) provide an environment where more experienced technology users introduce additional and advanced techniques to novices.

DMA offers both monthly General Membership Meetings, which cover new and innovative topics including a wide range of generic technological topics, and its Special Interest Groups (SIGs) which address concerns about specific technology interests. There are eight different SIGs sponsored by the DMA, covering such topics as the Linux operating system, various programming languages such as Python, the use of technology to investigate genealogy, and digital aids to investing. Neither SIG members nor attendees at DMA General Meetings need be members of the parent organization, though they are encouraged to join so DMA can continue providing its services to the public.

Annual dues for DMA membership, which have not been raised for decades, are $25 for Regular Members, and $12.50 for Family/Associate Members (someone living at the same address as a Regular Member). Nonvoting Student Memberships are *free* to students through age 22. Door prizes at General Meetings, picnics, banquets, and other DMA events, and both product and service discounts are available to all DMA members. **... TDB**

Dayton Microcomputer Association Membership Form

Today's date _____/_____/_____

❒ *NEW* Please credit the DMA member who recruited me: _____

❒ *RENEW* Contact information below is new ❒ Y ❒ N

TYPE OF MEMBERSHIP

❒ *REGULAR*

Name _____ Home / Work (_____) _____-_____

Email _____ Mobile Phone (_____) _____-_____

❒ *ASSOCIATE* Family Associate membership is for a family member living at the same address as a Regular member. Name of Regular member: _____

Name _____ Home / Work (_____) _____-_____

Email _____ Mobile Phone (_____) _____-_____

❒ *STUDENT* Free Student membership is available to those under 22 years of age, enrolled full-time in a program of higher education. Name of School: _____

Name _____ Home / Work (_____) _____-_____

Email _____ Mobile Phone (_____) _____-_____

Home Address _____

City _____ State _____ Zip _____

INTERCHANGE

Skills & interests you might share with DMA _____

What you hope DMA will provide _____

❒ *SHELL ACCOUNT* A shell account on the DMA web server provides file storage, hosting of a personal non-commercial website, @dma1.org email alias (forwarding address), all for a one-time fee of $10. A username must be 8 alpha characters. The usual default is last name and first initial, no caps or punctuation. DMA reserves the right of final decision on all usernames: 1st choice _____ 2nd choice _____

DUES AND FEES

Regular membership	$25.00 x ❒ 1yr ❒ 2yr ❒ 3yr	$_____
Family Associate membership	$12.50 x ❒ 1yr ❒ 2yr ❒ 3yr	$_____
Student membership	FREE	$ 0.00
One-time setup fee for Shell account	$10.00	$_____
Total		$_____

**Note: $10.00 fee will be charged for any returned checks*

Make your check payable to: **Dayton Microcomputer Association, Inc**
Mail check and application to: **PO Box 4005**
Dayton OH 45401-4005

Or use Paypal to send your payment to: **membership@dma1.org**

DMA use only

Member# _____ *Exp* ____/_____ *[ ] Cash [ ] Check#* _____ *[ ] Paypal Proc by* _____

Member# _____ *Exp* ____/_____ *[ ] Cash [ ] Check#* _____ *[ ] Paypal Proc by* _____

Member# _____ *Exp* ____/_____ *[ ] Cash [ ] Check#* _____ *[ ] Paypal Proc by* _____

Revised February 25, 2020