VERIFYING COMPUTER USAGE WITH INTERNET INFRASTRUCTURE

"Trust no one"

SUMMARY

Since Federal regulation of interstate commerce is firmly established, and since the Internet is also a subject of Federal regulation and since virtually every computing device including phones can connect to the Internet I suggest seizing computer hardware is neither effective nor efficient. Instead, law enforcement should only serve a warrant, make two read-only copies, let the owner choose one copy to keep and depart. In the event that the computer hardware in question is already being backed up by a commercial service it is not even necessary to go to where the subject computer hardware is: one need only provide one readable and read-only copy to the law enforcement agency and to the subject.

The Advantages

1. Prosecution and defense have exactly equal resources at a point in time. There is virtually no discovery.
2. No purported evidence can be altered, interpreted, lost, deleted during handling, sold to third parties … Law enforcement should have been making a read-only copy in any case.
3. The defending party has access to information and processing – it would be difficult to contact an attorney, much less assist in defense, without a computer or phone, thumb drives, second hard drives ...

During 1944 German intelligence felt that certain messages were invasion indicators that ordered local resistance groups to perform sabotage. But a Verlaine poem did not indicate where between Bergen Norway and Barcelona Spain (perhaps 2400 miles of coastline) the invasion would be. It is now SEVEN months after the January 6th attack – evidence that legislative colleagues and members of their staffs were aware of the possibility of the attack being carried out is surely degrading and proof that a file existed then and contains what law enforcement claims ...

If Congressman DeSaulnier or some colleagues wanted to do a 21st century investigation of the laptop computer purported to belong to Hunter Biden there are several pieces of useful information:

/1/ If Hunter Biden purchased the laptop from a vendor such as Best Buy there would be transmission of the laptop's identification by Best Buy to the manufacturer for warranty purposes.

/2/ If the laptop uses the Windows operating system Hunter Biden would likely have registered with Microsoft. That means that the seller of the operating system knows a great deal about the version of the operating system software as well as the hardware that software is running on. There is a similar situation with Apple computers and with Chrome books from Google.

/3/ If the laptop uses the Microsoft Office software Hunter Biden would likely have registered with Microsoft. Again, that means that the seller of the software system knows a great deal about the version of the software, the operating system and the hardware that software is running on.

/4/ It would typically be the case virtually every seller of software or hardware would capture configuration information either at installation time or whenever updates took place. For example, if Windows Update changes the contents of files on your computer Microsoft is informed that the changes were applied. Were you also using Microsoft Office Microsoft would also be informed that Office software is now running on an updated version of Windows. Another possibility is that Hunter Biden prefers a browser such as Chrome or Firefox – in which case there would be an install and updates.

/5/ Information about a computer includes (with real examples)

/a/ the domain = Gateway (Hunter Biden's home network)
/b/ the user ID = Peter
/c/ the computer name = GATEWAY
/d/ Operating System = Microsoft Windows 7 Build 7601
Service Pack 1 32 bit
Microsoft Windows 7 Home Premium
Version = 6.1.7601

/e/ processor ID = BFEBFBFF0001067A. This is NOT unique

/f/ MAC address(es) = 00:26:2D:1F:10:58/20:41:53:59:4E:FF
/g/ Internet address(es) = fe80::d459:a504:4728:cb07%11
20:41:53:59:4E:FF
/h/ Not all hard disk manufacturers conform, but it is sometimes possible to obtain the maker, model and serial number for the laptop's hard disk drive. Usually, even if there is serious damage, it is always possible to determine the capacity of the drive as well as the amount of remaining free space. I am not clear on exactly what damage was to be repaired, nor why Hunter Biden did not use a government-approved repair facility.

/6/ I do not know if Hunter Biden, either on his own initiative, or because his father worked for the United States government, employed what is called a masking service. Here, if one is e-publishing on social media, adding web pages or files via FTP (file transfer protocol software) or using email one pays the masking service a modest fee. When you, for example, send an email it contains the user and domain name of the intended recipient: peterfzoll would be the user name and yahoo.com would be the domain name. What is also sent with an email is the sender's user name and domain (tara.kopp would be the user and mail.house.gov would be the domain) AND your MAC address, your Internet address and other

information such as what browser you used. What a masking service does is modify your email's metadata so your user name, domain, MAC address, IP address and so on are hidden. Companies such as ProtonMail, Mailbox.org, Zoho, Posteo and Private Mail substitute their information so the receiving party cannot readily discover who the sender (you) are, nor where you sent the message from. Were you (or Hunter Biden) using ProtonMail, for example, to send me an email when I to reply the email goes not directly to you, but rather to ProtonMail. ProtonMail exchanges out their information for yours and sends the email along. Unless the recipient is very clever, there is no indication that there was any masking. Even if the recipient knows that masking was done it is very difficult to trace anything to ProtonMail, let alone beyond that to the actual sender.

/7/ With a modest amount of diligence any investigative agency such as the FBI should long ago have built a searchable chronology of information (presumably a database) that would resemble a spreadsheet with columns for

/a/ information type – email send; email receive; Facebook message; tweet; software download ...
/b/ date and time
/c/ sender (user and domain)
/d/ receiver (user and domain)
/e/ MAC address
/f/ internet address
/g/ hard disk status
/h/ operating system version
/i/ application software version (for a download)
/j/ processor ID
/k/ keywords
/l/ the actual text, images and so on
/m/ verified

/8/ Note that it is hardly unusual for someone to use multiple emails but the hardware would stay the same

/9/ Also note that the internet address might change as the user moved from home to Amtrak to the office … but the hardware would stay the same.

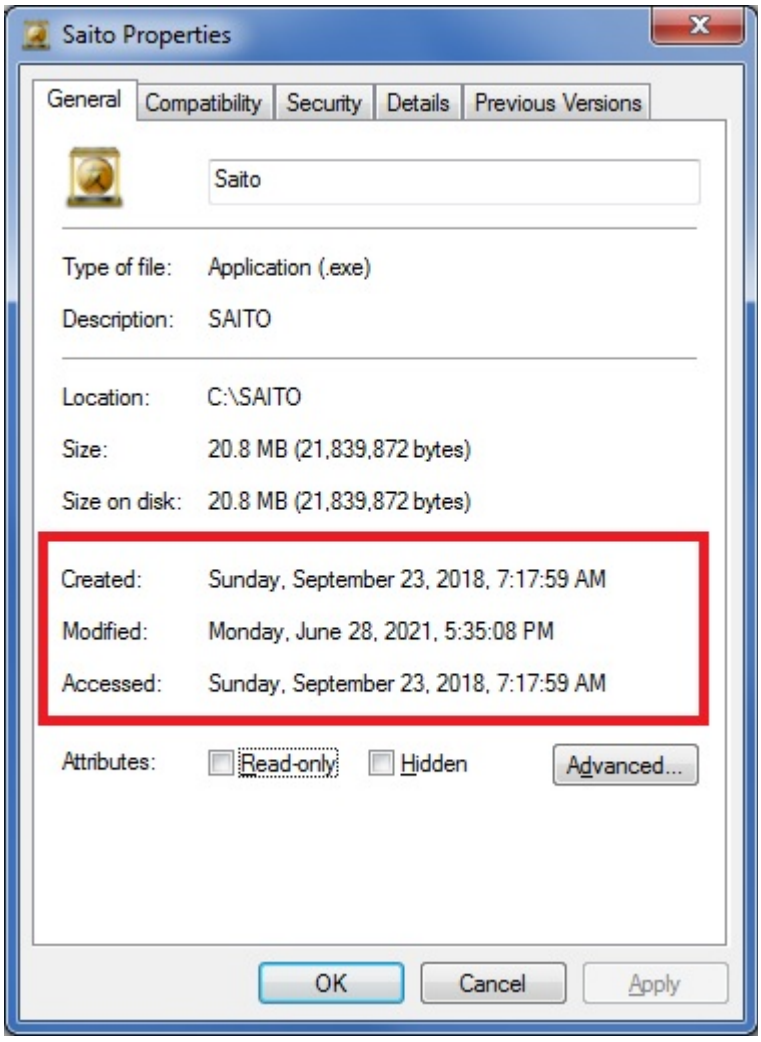
/10/ Unless Hunter Biden suddenly went dark after purportedly dropping off his laptop for repairs, he would have had at least one other computer. It would useful to determine how many computers were active and when and where he utilized them.

/11/ Likewise, normal prudence would suggest that user files or possibly the entire computer should be backed up presumably by Hunter Biden or, in some cases, by a commercial service. If such backups still exist and can be read they would serve as a useful basis for determining which files were changed in the course of the repairs. How much of a backup (if any at all) was made by the repair shop is not known to me.

/12/ Depending on what repairs were done one could expect to see an installation of Windows; Windows updates, perhaps some application downloads; and some testing of internet access. It would be routine to determine which user files (documents, pictures …) were updated after being dropped off for repairs and discard these as they would not be the responsibility of the owner. Some care would have to be taken to verify that the system clock was not distorted – by setting the clock to the past one can, with some effort, construct events that did not really happen at that time.

/13/ If there are user files thought to be incriminating it is trivial but required that their metadata be checked. An investigating agency would

have to preserve a backup image for legal purposes – files that were even just accessed are usually inadmissible as evidence. Of particular interest would be doing a right button mouse click (or software equivalent) on a file of interest



In the above example, the date created would have to be after the time Hunter Biden purchased the machine and before the machine was dropped off for repair. Those same limits would also apply to the modified and accessed dates.

/14/ Unfortunately, spoofing is a somewhat popular indoor sport among

those with less morals than a snapping turtle. This involves intentional alteration of the MAC address, the user and domain. It can be thought of as masking oneself usually to make multiple login attempts. Sometimes the Internet address is also manipulated to prevent backtracing. Suppose, for example, an evildoer wanted to rather tediously guess your email password in order to login as you. An alert systems administrator would likely notice lots of login failures and block access by the implicated domain, user, MAC address, computer and Internet address. It is very rare that anyone counter-attacks spoofers.

/15/ Even if a hostile party cannot login to your computer or your email it is possible to gain some information using what is often called sniffing. If the domain and user or MAC address or computer are known the Internet addresses used in sending and receiving can be used to determine a physical location. Even if a Vice-President or Congressperson is very diligent about security seemingly innocent communication by aides or reporters can provide location information. Note that this disclosure of location might not be an act of commission (sending an email, for instance, back to one's editor at the New York Times, paying a bill or sending in an expense report) but could as easily be an act of omission: Windows Update might launch without considering whether the target laptop is in Boston or Bosnia.

Summing up

/A/ Even at some distance in time it should be possible to clearly establish and verify whether Hunter Biden bought the laptop in question as well as when, where and how (credit card, cash …)

/B/ There should also be clear patterns of activity. If , for example, it appears that the laptop was used to pay bills the associated vendor would have to have a matching electronic record. It is not sufficient to assert that

a PG&E bill was paid using the laptop – one must verify this with a corresponding entry from PG&E. A tactic favored here by evildoers is to post a payment of a trivial amount to P&E and allow it to process. Then the payment is canceled BUT the evildoer now knows that account at PG&E that the payment went to is valid and so is the credit card or bank account.

/C/ Similarly, it is insufficient to assert that Hunter Biden sent or received an email, downloaded a file, re-tweeted or whatever. This has to be verified by an offsetting activity by the other correspondent as well as by the owner of whatever connection was used. If it was asserted that Hunter Biden sent an email to his father from Minsk, for example, there would have to be an offsetting activity on his father's email account with an appropriate Minsk Internet address as well as five records from the Starbucks in Minsk: /1/ the router in Starbucks granted a login request by the laptop /2/ the router in Starbucks received the email from the laptop /3/ the router in Starbucks successfully transmitted the email /4/ the router in Starbucks received notice that the transmission was received /5/ the router in Starbucks eventually logged Hunter Biden off. Some effort would be spent to verify that the router at the Starbucks actually was operating the day before and the day after and appears to have spent a more or less normal day with lots of traffic from other users on the day in question.

/D/ I certainly cannot speak to whether Hunter Biden met with Kazakh oligarchs at a posh restaurant in Georgetown or not. It is something of a mystery how the New York Post could still be publishing revelations two years after the laptop was seized. I would like to think that the FBI would have completed a forensic investigation in hours (at worst a very small number of days) and filed charges or not. If an agency like the FBI is taking any longer than that there is a real problem so the Oversight Committee should ask when a problem was detected, what were the methods, how long did they take and what was the result.