



METADATA

— FORENSICS —

Patrick Eller
Metadata Forensics, LLC
1108 E Main St
Richmond, VA 23219

Introduction and Qualifications

1. I have been asked by the law firm Birnberg Peirce who represent Julian Assange, to provide a report giving my opinion on relevant aspects of the indictment in which he faces a number of charges under the US Espionage Act 1917 and under the Computer Fraud and Abuse Act.
2. I am the President and CEO of Metadata Forensics, LLC at 1108 East Main Street, Richmond, Virginia. The work of Metadata Forensics provides digital investigation and forensic examination in both civil and criminal cases. I am also an Adjunct Professor for the University of Maryland Global Campus, (UMGC) and Champlain College Burlington Vermont, VT in the field of digital forensics, teaching undergraduate and graduate level programs. I have also previously served as a Digital Forensic Expert Witness instructor for the Intermediate Trial Advocacy Course and Special Victims Counsel Course located at the US Army Judge Advocate General Law School, Charlottesville Virginia.
3. I served for 20 years in the US Army during which time I held positions in the role of criminal investigator and supervisor of investigations relating to digital evidence in particular. From 2012 until 2019 I was the Command Digital Forensic Examiner and was responsible for all administrative, inspection and oversight functions within a digital forensic program which included more than 80 digital forensic examiners at US Army Criminal Investigation Command headquarters, Quantico Virginia VA.
4. I have read Part 19 of the Criminal Procedure Rules relating to Expert Evidence and believe that my advice is compliant with the rules.

Instructions

5. I have been provided by Mr. Assange's legal team with copies of the indictments and directed to the transcripts of the court martial proceedings against Private Manning (available via the Internet) and have been provided with further information from lawyers representing Mr. Assange which I have followed up myself with direct enquiries from one of the providers of that information.
6. I have been asked to consider the allegations in the indictment. I note that the claim made by the US prosecutors, contained within their affidavits alleges first that Mr. Assange and Private Manning reached an illegal agreement during March 2010 in which Assange agreed to assist Manning in cracking a password stored on US Department of Defense (DoD) computers connected to the classified secret internet protocol router network (SIPRNet). Manning who had access to the computers in connection with her duties as an intelligence analyst, was using the computers to download classified records to transmit to WikiLeaks. Second, that cracking the password would have allowed Manning to log on to the computers under a username that did not belong to her and that such a measure would have made it more difficult for investigators to determine the source of the disclosures. Third, relying upon a number of chats surrounding the claimed agreement to substantiate this theory, the prosecution refers to a discussion concerning release of information and specifically the provision by Manning of a partial hash value asking if

Assange knew how to assist in cracking it.

7. I was asked at the beginning of December 2019 by lawyers acting for Mr. Assange to conduct a review of available evidence relevant to these assertions and to consider the validity of the prosecution's claims within the extradition request. I was contacted by Michael Mori, a US Attorney, involved in carrying out investigations on behalf of Mr. Assange jointly with his UK legal team and agreed to provide advice on the issues about which I was consulted, including the legal teams understanding of the technical evidence in Manning's court martial.
8. In due course I was made aware by Mr. Mori that his UK legal team had received convincing information that suggested the claims made by the prosecution for the interpretation of the Manning "chat" were not reliable and that Manning and others in the unit in which she was working in Iraq, made regular and wide use of avoidance of the administrator restrictions said to have been the subject of avoidance in the indictment. His lawyers were informed, I understood, that it was very well known that the purposes for such avoidance included introducing into computers the means of access to leisure material such as movies, or to research other areas of interest or short cut restrictions in the course of normal work. The ownership and administration of the computers was conducted by civilian contractors and not the military unit using them.
9. In a preliminary review of the court martial transcripts I could observe that a sizable amount of such obviously unauthorized material of the above kinds was found on the computers in the T-SCIF.
10. Mr. Mori informed me that he had been able to trace and speak to a member of Manning's unit at the time who had been willing to meet him and with whom Mr. Mori conducted an extended discussion. Mr. Mori whilst in discussion in person with that individual, together with a colleague, asked me if there were particular areas it would be of assistance to me to have clarified and/or confirmed. In consequence I was able to speak to that individual at some length. He outlined and confirmed much of the background of which I had already been able to see as a result of my ongoing review of the computer evidence of the court martial transcripts. He described Manning's reputation in the unit as the go-to person for technical help, including for installing programs. He was aware of her "hash cracking" conversations with others at the time. He was entirely aware of the activities of members of the unit, in the utilizing classified access for the purpose of viewing movies and games.
11. In broad terms, before turning to a detailed analysis of the corroborative evidence I can say that in my review of the court martial transcripts, I found strong support for the proposition that the interpretation placed by the prosecution on the conversation with Manning and Assange could not be reliably or safely construed to be for the purpose of obtaining anonymity for Manning so that classified information could be extracted without personal anonymity being compromised.
12. In this report I refer to a number of aspects. Firstly, I explain technical issues in relation to the "hash cracking" evidence and make a number of comments upon the validity of the assertion that the purpose of the chat was for Manning to download documents anonymously.

13. I am familiar with all of the systems and technical references referred to in the prosecution's summary. I believe a number of the technical assertions are stated with a lack of understanding of how these systems work. As I will explain in further detail separately.
14. I then provide an analysis of the testimonies during Manning's court martial which detail the work and computer security practices in the T-SCIF. In particular, key points that arise that are demonstrated by the court martial testimonies about computer usage in that section:
 - Soldiers regularly put unauthorized files and programs on computers in the T-SCIF.
 - Other Soldiers cracked the administrator password in order to install programs.
 - Manning's colleagues viewed her as a technical expert (a view enjoyed by Manning).
 - Manning's colleagues regularly asked her to install programs on their computers.
 - Further forensic analysis is impossible due to the destruction of evidence.
15. In all aspects of my analysis, I point to the available court martial documents which provide the foundation for my opinion.
16. I have been asked within this report to formulate the technical propositions in as easily understandable a way as possible.

Allegations in the indictment of Julian Assange

17. I have been provided with the initial and superseding indictments against Assange, their supporting affidavits and the 'jabber' chat log. In those documents, the United States Government alleges that Assange conspired with Chelsea Manning in violation of the Computer Fraud and Abuse Act contrary to paragraphs 1030(a)(1) (obtaining information by unauthorized computer access) and 1030(a)(2) (computer espionage) of Title 18, US Code Section 371.
18. It is alleged that the conspiracy began in January 2010, and that "the primary purpose of the conspiracy was to facilitate Manning's acquisition and transmission of classified information related to the national defense of the United States so that WikiLeaks could publicly disseminate the information on its website". Specifically, the initial indictment contains the following assertions (emphasis added):

*"The portion of the password Manning gave to Assange to crack was stored as a "hash value" in a computer file that was **accessible only by users with administrative-level privileges**, and used special software, namely a Linux operating system, to access the computer file and obtain the portion of the password provided to Assange" (paragraph 9)*

“Cracking the password would have allowed Manning to log onto the computers under a username that did not belong to her. Such a measure would have made it more difficult for investigators to identify Manning as the source of disclosures of classified information” (paragraph 10)

19. The indictment states that the Jabber chat logs form part of the basis of the 'overt act' in service of the conspiracy. Both the initial and the superseding indictment state the following under the heading 'manners and means of the conspiracy':

- i. *“It was part of the conspiracy that Assange and Manning used the "Jabber" online chat service to collaborate on the acquisition and dissemination of the classified records, and to enter into the agreement to crack the password hash stored on United States Department of Defense computers connected to the Secret Internet Protocol Network.*
- ii. *It was part of the conspiracy that Assange and Manning took measures to conceal Manning as the source of the disclosure of classified records to WikiLeaks, including by removing usernames from the disclosed information and deleting chat logs between Assange and Manning.*
- iii. *It was part of the conspiracy that Assange encouraged Manning to provide information and records from departments and agencies of the United States.*
- iv. *It was part of the conspiracy that Assange and Manning used a special folder on a cloud drop box of WikiLeaks to transmit classified records containing information related to the national defense of the United States.”*

20. The superseding indictment also alleges that the overt acts in furtherance of the conspiracy include, but are not limited to:

- i. *On or about March 2 2010, Manning copied a Linux operating system to a CD, to allow Manning to access a United States Department of Defense computer file that was accessible only to users with administrative-level privileges.*
- ii. *On or about March 8 2010, Manning provided Assange with part of a password hash stored on United States Department of Defense computers connected to the Secret Internet Protocol Network.*
- iii. *On or about March 10 2010, Assange requested more information from Manning related to the password hash. Assange indicated that he had been trying to crack the password hash by stating that he had "no luck so far".*

21. In her affidavit, Megan Brown, a Special Agent with the FBI, states that “the conspirators took elaborate measures to conceal their communications, mask their identities, and destroy any trace of their conduct, using, for example, encryption and anonymization techniques, and erasing and wiping data”. In describing how probable cause has been established, Megan Brown makes the following conclusion:

*“Cracking the password would have allowed Manning to **log onto the computers under a username that did not belong to her.** Such a deceptive measure would have made it **more difficult for investigators to determine the source of the illegal disclosures**”*

22. This refers to the password hash which Manning sent, which was for an “ftp user” account on one of the computers which Manning used. (paragraph 96, affidavit of Megan Brown)

Technical analysis of the password hashing allegation

Manning’s access and seeking anonymity

23. Upon reading the indictment, it became clear that the technical explanation of the password hashing allegations is deficient in a number of ways which cast doubt upon the assertion that the purpose of the Jabber chat was for Manning to be able to download documents anonymously.
24. As a preliminary point, the timeline of events shows that this Jabber chat which allegedly took place between Manning and Assange occurred after Manning had already downloaded the 10 Reykjavik 13 cable, the Guantanamo Detainee Assessment Briefs, the Iraq War Reports (CIDNE-I) and the Afghanistan War Reports (CIDNE-A). Downloading the CIDNE documents were something she had to do routinely in the course of work, as offline backups were needed in the event that there were SIPRNet connectivity issues.
25. The only set of documents named in the indictment that Manning sent after the alleged password cracking attempt were the State Department Cables. Manning had authorized access to these documents (access and authorization will be discussed in more detail later in this report), and had must have indeed accessed the Cables from her usual account on the SIPRNet computers in order to download and submit the 10 Reykjavik 13 cable to WikiLeaks in February 2010.
26. Prior to any detailed technical analysis, the indictment’s assertion that Manning hoped to gain anonymity or was trying to access information that she did not already have authorization to access is a weak one, as she already had authorized access which she used to download the above datasets. It is unclear to me that any anonymity would have been gained by cracking the password hash to gain access to the ftpuser account. I will return to this in more detail later in this report.

Inaccuracies in the description of the password hash

27. In the superseding indictment, the US Government correctly state that both the SAM and system file are needed to crack the password hash. However, they misunderstand what exactly Manning is alleged to have sent Assange.

28. In my view, this inaccuracy casts doubt on the extent to which, in investigating the alleged conspiracy between Manning and Assange, the US have fully assessed the technical evidence available to them in order to gain an understanding of computer usage in the T-SCIF which I believe is highly relevant to a proper explanation of events.

Hash functions

29. By way of background, a hash function takes data as input and changes it to generate a fixed-size, relatively unique identifier for the data called a hash value. Hash functions are deterministic, irreversible, one-way functions, usually written in hexadecimal (a numbering system that uses 16 characters).

30. Hash functions are used to authenticate in this case users and passwords on a computer. Rather than storing the password itself on the computer, the computer checks the output of the hash function, the password hash, which is saved on the computer. When a user tries to login, the password that they input is hashed using the same hash function as the original password. Then it is compared to the hash value that was generated from the original password and stored on the computer. If these two hash values are the same, then the computer determines that the user must have entered the same password as when they first set it and allows them to login to the account.

31. The US government has made a technical mistake in explaining this situation since Manning's trial. The criminal complaint against Assange states:

"As additional security, the computer does not store the full hash value in one location. Instead, the hash value for that username is broken into two parts. One part is stored in the Security Accounts Manager (SAM) database as the SAM registry file. The SAM file in a Windows operating system keeps usernames and parts of the hash value associated with the username. The other part of the hash is stored in the "system file." To obtain the full hash value associated with the password, one needs the parts from the SAM file and the system file." (paragraph 82, affidavit of Megan Brown)

32. This is not correct. The password hash itself is not broken up and split between the SAM

file and system file. It is stored in full in the SAM file, but encrypted with a key (which is not part of the hash) generated from data in the SAM file and system file. The hashes themselves are not split into halves or stored in the system file, they are stored in the SAM file. The SAM file alone, however, is not sufficient to crack the password hashes.

33. This is because the password hashes stored in the SAM file are encrypted with the SAM lock tool (SYSKEY). So while the SAM file contains the full hashes, it only contains the encrypted versions of the password hashes and is thus useless alone. The encryption key needs to be retrieved in order to decrypt the password hashes stored in the SAM file. Retrieving this key requires portions of both the System file and SAM file.

34. Manning only retrieved the encrypted hash value from the SAM file. She did not have the System file or the portions of the SAM file that are required to reconstruct the decryption key for the hash. This decryption step is necessary before the hash can be cracked and it is a separate process from cracking the hash by guessing different password values with rainbow tables. At the time, it would not have been possible to crack an encrypted password hash such as the one Manning obtained.

35. Encryption of the password (or the password hash) is not mentioned at all in the criminal complaint or indictment, aside from stating that “the creation of the hash value is a form of encryption for storing the password”. This is different from the encryption of the hash value with a symmetric key. Therefore, the description of the password as being split between the SAM and system files is inaccurate in both the initial and superseding indictment, and means that what Manning sent was insufficient to be able to crack the password in the way that the government have described.

Manning’s Alleged Actions

36. I have reviewed the Manning court martial documents in order to build a background timeline to the alleged conspiracy in the indictment.
 - i. Manning reinstalled the operating system on her personal computer on January 25, 2010 (Exhibit 1, p. 111). Then, on January 31, 2010, Manning erased the free space on her MacBook Pro (Exhibit 2, p.10976, Exhibit 4). The technical effect of this would have been to overwrite any deleted files so that they very likely could not be recovered later. She was on leave in the United States during this time period.
 - ii. On February 1, 2010, Manning burned two operating systems (.iso files called “lflivecd-x86-6.3-r2145-nosrc.iso” and “systemrescuecd-x86-1.3.5.iso”) to CDs using her MacBook Pro (Exhibit 3, p.8532, Exhibit 4).
 - iii. On February 11, Manning once again cleared the free space on her MacBook Pro (Exhibit 4), once again overwriting any deleted files.

- iv. On March 2, 2010, Manning created a Linux CD using the .iso file “systemrescuecd-x86-1.3.5.iso” (Exhibit 3 p.8533, Exhibit 4). Version 1.4.0 of SystemRescueCD was released on March 1, 2010¹, but Manning was still using version 1.3.5.
- v. Manning started a SIPRNet computer from this Linux CD (Exhibit 3, p.8529 - 8539).
- vi. There were two main SIPRNet computers that Manning had access to, which are referred to as IP1 and IP2 in Assange’s indictment or .22 and .40 in Manning’s trial. The .22 computer was an Alienware computer with the IP address 22.225.41.22 (Exhibit 5). The .40 computer was a Dell computer with the IP address 22.225.41.40 (Exhibit 5). Both computers were running Windows (Exhibit 6, p.1). Manning probably started the .22 computer from the live CD because the string she sent matches a portion of the hex dump of the SAM file from that computer (Exhibit 3, p.8534).
- vii. After starting the SIPRNet computer with the Linux CD, Manning would have needed to mount the Windows partition. This would have enabled her to view all files on the Windows OS, even those associated with other users or locked by the operating system when Windows was running.
- viii. To obtain the string of text later sent over jabber, Manning would then need to navigate to the SAM file at Windows/system32/config/SAM and take a dump of the file (allowing her to view it in hexadecimal).
- ix. Manning then attempted to determine the location of the password hash for “ftuser” in the hex dump of the SAM file. The value that she copied is shown in the screenshot of the hex dump of the SAM file below (Exhibit 7).

```

01 02 00 00 00 00 00 05 20 00 00 00 20 02 00 00 66 00 74 00 70 00 | .....f-t-p-
00 65 00 72 00 01 00 FF | u.s.e.r...f.t.p.u.s.e.r...yyyyyyyyyyyyyy
01 00 80 C1 10 49 FA EB F4 41 D5 24 FB 3C 4C D5 35 1C 01 00 01 00 | yyyyyy#ú<.....|Å Iue&A&ú<L05
00 01 00 01 00 01 00 01 00 F8 FF FF FF E0 2C 00 00 F0 FF FF FF B8 | ylí| |)QÁ|yx|N>.....syyya, .syyy,

```

- x. As explained earlier, this hexadecimal string is not enough to crack the password even if it is the correct portion of the SAM file. The decryption key for the hash would also need to be obtained, which requires data from other portions of the SAM file and the System file (which Manning did not have).
- xi. On March 8, 2010 according to the Jabber chat log, Manning asked Assange if he was “any good at lm hash cracking?” He replied “we have rainbow tables for lm”. In response to this, Manning sent the hexadecimal string that she found in the SAM file and Assange said that he “passed it on to our lm guy”.

¹ <https://distrowatch.com/index.php?distribution=systemrescue>

dawgnetwork@jabber.ccc.de	Nobody	2010-03-08 15:55:28	any good at lm hash cracking?
pressassociation@jabber.ccc.de	Nathaniel Frank	2010-03-08 16:00:29	yes
pressassociation@jabber.ccc.de	Nathaniel Frank	2010-03-08 16:00:44	donations; not sure.
pressassociation@jabber.ccc.de	Nathaniel Frank	2010-03-08 16:00:55	something in order of .5M
pressassociation@jabber.ccc.de	Nathaniel Frank	2010-03-08 16:01:30	but we lost our CC processor, so this is making matters somewhat painful.
pressassociation@jabber.ccc.de	Nathaniel Frank	2010-03-08 16:02:23	we have rainbow tables for lm
dawgnetwork@jabber.ccc.de	Nobody	2010-03-08 16:04:14	80c11049faebf441d524fb3c4cd5351c
dawgnetwork@jabber.ccc.de	Nobody	2010-03-08 16:05:07	i think its lm + lmnt
dawgnetwork@jabber.ccc.de	Nobody	2010-03-08 16:05:38	anyway...
dawgnetwork@jabber.ccc.de	Nobody	2010-03-08 16:06:08	need sleep >yawn>
dawgnetwork@jabber.ccc.de	Nobody	2010-03-08 16:09:06	not even sure if thats the hash... i had to hexdump a SAM file, since i dont have the system file...
pressassociation@jabber.ccc.de	Nathaniel Frank	2010-03-08 16:10:06	what makes you think it's lm?
pressassociation@jabber.ccc.de	Nathaniel Frank	2010-03-08 16:10:19	its from a SAM?
dawgnetwork@jabber.ccc.de	Nobody	2010-03-08 16:10:24	yeah
pressassociation@jabber.ccc.de	Nathaniel Frank	2010-03-08 16:11:26	passed it onto our lm guy
dawgnetwork@jabber.ccc.de	Nobody	2010-03-08 16:11:40	thx

- xii. Later that day, at 10:28 pm, Manning searched for “rainbow tables” on SIPRNet (Exhibit 2, p.10998).
- xiii. On March 10, 2010, Assange asked “any more hints about this lm hash?” and said “no luck so far”. Manning did not seem to reply.

pressassociation@jabber.ccc.de	Nxxxxxxx Fxxxx	2010-03-10 23:30:54	any more hints about this lm hash?
pressassociation@jabber.ccc.de	Nxxxxxxx Fxxxx	2010-03-10 23:31:03	no luck so far

Accessing data anonymously

- 37. As part of her work as an intelligence analyst with top secret clearance, Manning already had legitimate access to all of the databases from which she downloaded data. Logging into another local user account would **not** have provided her with more access than she already possessed or even anonymous access to these databases.
- 38. From the evidence available at the Manning court martial and from my own military background and experience, I consider that the databases available to Manning had three different ways of controlling and tracking access:
 - A) Databases were accessible to anyone with a SIPRNet connection
- 39. Firstly, many databases were accessible to anyone with a SIPRNet connection. These databases did not require any additional log in information or account-based access control. Access was not controlled with accounts. In particular, the databases referenced in counts 3, 7, 10, and 13 (Net Centric Diplomacy, for the cables) and counts 2, 6, 9, and 12 (for the Detainee Assessment Briefs) were databases that anyone with SIPRNet access could use without any further authentication or login at that time.

40. During Manning's court martial, Captain Steven Lim (one of her supervisors) testified about the Net Centric Diplomacy database and explained that he had given the link to his analysts to use in their work. He noted that the Net Centric Diplomacy database did not require accounts or any other login information:

"Q. Did the diplomatic cables and the Net-Centric Diplomacy Database, did it have some sort of password that you had to enter in order ----

A. It did not, no, sir.

Q. Okay. Was it available to anybody who had SIPRNET access?

A. Yes, it was." (Exhibit 18, p.9885-9887)

41. The Detainee Assessment Briefs also did not require any login information to access. During Manning's court martial, Jeffrey Motes stated that the Detainee Assessment Briefs were stored in a few locations, including Intellipedia (Exhibit 8, p.8734). It was also explained during the court martial that Intellipedia is on Intelink (Exhibit 9, p.7948-9). Intelink logs presented as evidence in Manning's court martial show that she accessed the Detainee Assessment Briefs via Intelink (Exhibit 10, Exhibit 11). These logs also indicate that no username, password, or specific account was needed to download the data. This is in line with testimony from Manning's court martial, which explained that users did not need accounts to access most databases on Intelink:

"At the time, users were not required to have Intelink passport accounts to use most Intelink services, including the SIPRNET Internet search and browsing." (Exhibit 9, p.7956)

42. The government allegation that there was an attempt to gain anonymity is greatly undermined by the tracking system which identified users. Databases like the Net Centric Diplomacy database and Intelink could be accessed from any account on the computer, including local user accounts (Exhibit 12, p.8910-8914). But the account on the computer that the user logged into was not used in any way to identify the user to the database. Instead, access was tracked using IP addresses.
43. Internet Protocol (IP) addresses are identifiers for computers on a network that help the network determine how to send data to the correct computer. IP addresses are often used by websites to track which users access what data when. During Manning's trial, the meaning of IP addresses in Intelink logs was explained:

"The "22.225.41.40" is the IP address. This indicates that a computer with that IP address made the request for information. Essentially, it provides an electronic location for the user using Intelink." (Exhibit 5)

44. IP addresses are entirely distinct from the local user accounts on the computer. The username or other details about the account the user is using on the local computer are not sent to any website or online database at any point. This means even if Manning was in fact logged into the ftpuser account rather than her own normal account, this would have no effect on tracking because databases like Net Centric Diplomacy or Intelink would not receive information about what account she was using on the computer. These databases would only be able to track her using her IP address.

45. Manning's two SIPRNet computers were referred to by their IP addresses throughout the court martial: 22.225.41.22 and 22.225.41.40 (or the .22 and .40 computers for short) (Exhibit 5) and are the addresses which identified Manning as accessing the data. Merely logging into a different local user account on the computer (such as ftpuser) would not anonymize Manning at all because the IP address of the computer would remain the same regardless of what user account is in use. Importantly, IP addresses were relied upon as evidence of the user (being Manning) throughout the court martial. For example, Intelink search logs for the IP addresses used by Manning's computers were cited as evidence of Manning's interest in WikiLeaks:

"Intelink is a SIPRNET search engine, very similar to Google, in fact, powered by Google. The logs collected in this case by CID agents, are linked to the .22 and .40 addresses and those logs span the length of PFC Manning's deployment, so approximately 1 November to the end of May 2010 -- 1 November 2009 to the end of May 2010. The evidence will show that those computers searched for WikiLeaks more than 100 times on the SIPRNET." (Exhibit 14, p.7413)

46. Similarly, Intelink logs for the IP address 22.225.41.22 were used as evidence that Manning had downloaded the Detainee Assessment Briefs (Exhibit 10, Exhibit 11). During Manning's trial, it was explained that Intelink only could track users by IP address:

"At that time we did not track users by log-in identifiers. Instead, we tracked usage by IP address."(Exhibit 9, p.7952)

47. The Net Centric Diplomacy database (from which Manning downloaded the diplomatic cables) also tracked users by their IP addresses:

"The NCD server logs track the Internet Protocol (IP) address of a user requesting our resources, as well as the time and date that request was made, whether the user retrieved the resource or not, and the metadata associated with that connection."(Exhibit 16)

48. There are two notable points to consider with the access to Net Centric Diplomacy database: first that the database did not require a password, just the link and second that the cables in the database were considered relatively non-sensitive and many people had access, likely anyone with access to SIPRNet and the link. There are other cables with different captions that are not available on SIPRNet.

49. Manning described how she got access to the cables in her statement during the pretrial:

"I first became aware of the diplomatic cables during my training period in AIT. I later learned about the Department of State or DoS Net-centric Diplomacy NCD portal from the 2/10 Brigade Combat Team S2, Captain Steven Lim. Captain Lim sent a section wide email to the other analysts and officers in late December 2009 containing the SIPRnet link to the portal along with the instructions to look at the cables contained within them and to incorporate them into our work product."(Exhibit 17)

50. She also described the classification and distribution of the cables:

“In particular, I wanted to know how each cable was published on SIPRnet via the Net Centric Diplomacy. As part of my open source research, I found a document published by the Department of State on its official website.

The document provided guidance on caption markings for individual cables and handling instructions for their distribution. I quickly learned the caption markings clearly detailed the sensitivity level of the Department of State cables. For example, NODIS or No Distribution was used for messages at the highest sensitivity and were only distributed to the authorized recipients.

The SIPDIS or SIPRnet distribution caption was applied only to recording of other information messages that were deemed appropriate for a release for a wide number of individuals. According to the Department of State guidance for a cable to have the SIPDIS caption, it could not include other captions that were intended to limit distribution.

The SIPDIS caption was only for information that could only be shared with anyone with access to SIPRnet. I was aware that thousands of military personnel, DoD, Department of State, and other civilian agencies had easy access to the tables. The fact that the SIPDIS caption was only for wide distribution made sense to me, given that the vast majority of the Net Centric Diplomacy Cables were not classified.”

(Exhibit 17)

An exhibit in Manning’s trial confirms her description of the cable classification scheme and provides additional information on the distribution restrictions on the diplomatic cables (Exhibit 16).

B) Accounts were separate from the user accounts on the computer

51. Secondly, some SIPRNet websites and databases did require accounts in order to gain access, but these accounts were separate from the user accounts on the computer. In these cases, users needed to create online accounts specific to the website or set of websites. The details about these accounts (including the password hashes used to authenticate the user) would have been stored on the server for the website, not on the laptop that Manning was using.

52. This configuration is the same as when someone creates an account on a website on the normal internet and then can access the website from any device using the same username and password. The same user may also have a username and password that they use to login to their laptop, but this has nothing to do with accounts that they may have on external websites.

C) Access to Active Directory was controlled with domain accounts

53. Thirdly, access to data on Active Directory would have been controlled with domain accounts. On Windows, it is important to distinguish between two types of accounts that

users can use to log into the computer: domain accounts and local accounts. Domain accounts can be used to share data on the network with other users. Domain user accounts are part of a domain and can access data that other members of the domain share on it. They can also access any other domains with which their domain has configured a trust relationship. SIPRNet typically used Active Directory domains to control access to a variety of data. This form of access control was explained during Manning's court martial:

“Q. Okay. Let's talk about access controls on the SIPRNET, all right?”

A. Sure, sir.

Q. Other than information that might be password protected, were there any access controls on the SIPRNET that you're aware of?”

A. I'm not sure what you mean, sir.

Q. If I had SIPRNET access, like I was a person who had the clearance, had a computer hooked up to the SIPRNET, was there any limitation on what I could go see on the SIPRNET?”

A. Yes, sir.

Q. And what was that limitation?”

A. You -- there are probably hundreds, if not thousands, of locations on SIPRNET that you would not be able to go to.

Q. Because of why?”

A. Being a member of the 2nd Brigade, 10th Mountain, you had -- your authorizations were based on being a member of my domain. As a member of my domain, you could not go to the, you know, M&D north sites or their shared drive or their SharePoint portal and access anything because I did not have a trust relationship configured in my active directory and their active directory that allowed us to share information in that sort of manner. You could not go to Afghanistan site shared drive or any location and pull information unless we had a trust established. Or if they had that alternate distance site configured in such a manner that you did not require verification of your authenticity.

Q. Okay, so I want to break it down just -- if I'm understanding you right, I could go on -- on a SIPRNET computer on your domain, I could go to any place that you had a trust relationship with?”

A. Inside my domain you could go to any -- you can go to SharePoint portal, you could go to any of the -- you can go to the T-drive, you can go to any of the -- the locations we had that were available to general users. We had some locations that were completely restricted to administrators that no one had rights to but myself, my NCO, my warrants, and a few other guys. But as a general user, you could go to anywhere within my brigade that was not specifically prohibited.

Q. And ----

A. Outside of the domain -- outside of the brigade, we'll say, you could not go to 1st Brigade, 3rd ID; you could not type in their address in the URL bar, bring up their site and access any information unless they specifically configured their systems to allow visitors. If you allow visitors, then anyone can have access to what you give visitors access to. And that goes for every other unit on SIPRNET in the world. However, my brigade, because we work closely with certain units, we had a trust established, which means I trust all of their users, meet the requirements, they trust all my users -- that's the general term. The trust is actually the connection that's -- that allows anyone in their domain access to mine and allows anyone in mine access

to the FAR domain. And we had established -- trust established with several of the other brigades in the M&DB area and with multinational brigade. And -- because we had Corps level assets on my network that I managed with MNFI.” (Exhibit 8, p.8668-8673)

54. Local accounts are specific to the individual computer and do not grant access to additional data on the network. Users logged into a local account can store data on the specific computer and access websites normally, but would not be able to access data via active directory because their account is not part of an active directory domain. This limitation of local accounts was also discussed during Manning’s court martial:

“If I plug into the network but I log in locally. So I'm not part of the domain, I just log in with a local user account, I can still print; I can still visit Web sites; I can still run programs on my machine. I may not be able to do domain-specific services, such as access restricted areas of SharePoint or access e-mail if I -- if I'm on a machine that's not part of the domain or if I'm logged in locally and I try to open up my e-mail it's -- I'm going to get a prompt for what we call "domain credentials." It's then going to ask for a domain user, domain password, which if I don't have I'm not going to get into the e-mail.” (Exhibit 12, p.8910-8914)

55. The ftpuser account was a local account (Exhibit 2, p.10999). Therefore, a person logged into the ftpuser account would not have been able to access data on the active directory domain if configured properly. This means that the ftpuser account would have been useless for accessing data available via Active Directory anonymously because it would not have been able to access data via Active Directory. It may have still been possible to access online databases with other forms of access control, such as Net Centric Diplomacy or the Open Source Center. But in this case, access would have still been identifiable regardless of the account used on the computer because users would have been tracked with IP addresses or database-specific accounts (as explained above).

Alternative methods of gaining access to another account

56. If Manning merely wanted to login to an account other than her own, she would have been able to do so without cracking any passwords or hacking anything. This is because she already had easy access to the accounts of other soldiers in the T-SCIF.
57. During an interview of one of the supervisors of the T-SCIF that Manning was working in during that time period, it was stated that it was common for some Soldiers not to log out of the computers and permit other analysts to use the laptop without logging in. Each user of a laptop could set the time limit when the laptop would automatically lock the screen and require the user to re-login. As 8 to 10 analysts including Manning were sharing the 4 secret laptops, some of the analysts were getting on and off the laptops without logging out as to a means to accomplish tasks quickly during a shift. This statement above shows Manning could have already accessed documents using account other than her own to try to hide the downloading of documents.
58. Additionally, using the account of another Soldier in the T-SCIF would have been of limited utility in accessing data anonymously because it still would have been possible to narrow down the suspects in any data breaches to the small group of soldiers in the T-

SCIF using the user tracking mechanisms described in the previous sections.

There is no indication that Manning was trying to access data anonymously

59. On the basis of an analysis of the technical setup in the T-SCIF, I do not consider that the allegation that Manning was trying to access data anonymously is tenable. Before the password cracking discussion on March 8, 2010, Manning had already downloaded and leaked hundreds of thousands of documents using her normal account on her normal SIPRNet computers, including the CIDNE-I and CIDNE-A SigActs (the Iraq and Afghan War Logs), the Rules of Engagement and Collateral Murder video, and the Detainee Assessment Briefs (Exhibit 17). I have not seen any evidence that Manning attempted to download these documents anonymously. There is also no indication that Manning was trying to crack the ftpuser account password in order to download data anonymously. She also does not mention the password cracking incident in her guilty plea, despite explaining other events related to her leaks in great detail, including how, when, and why she downloaded and leaked documents (Exhibit 17).
60. As explained earlier, the ftpuser account would also not have granted Manning anonymous access to any data. This includes the Net Centric Diplomacy database because that database tracked user access with IP addresses (Exhibit 16). This is notable because the 251,287 diplomatic cables from the Net Centric Diplomacy database were the main set documents that Manning leaked to WikiLeaks after the March 8, 2010 password cracking conversation (Exhibit 17), and the only set of documents downloaded after this point that is mentioned in the indictment of Assange. Yet, cracking the ftpuser password would have been useless in obtaining anonymous access to this data.
61. The technical impossibility of using the ftpuser account to download data anonymously combined with Manning's past behavior of downloading hundreds of thousands of documents from her own account indicate that it is highly unlikely that Manning's attempt to crack the ftpuser password had anything to do with leaking documents. I do not see any benefit that Manning would gain in terms of accessing data or obscuring her identity.

Re password cracking agreement

62. I do not proffer a view as to whether it can be considered that there was such an agreement, recognizing that this may be an argument to be appropriately made by Mr. Assange's legal team. I list below a number of factors that may be relevant to such an argument.
63. The Jabber chat referenced earlier doesn't state the hash came from a Government Computer. Manning did not claim that she was trying to crack the hash in order to access data anonymously. In fact, basic technical knowledge or research would have shown that a local user account would not have given Manning any additional or more anonymous access to data on a network than what she already possessed (as explained earlier in this report).
64. While she may have been able to use a local user account to access data on the local

computer, it seems clear from my research that Manning could clearly already access all data on the local computer by booting a Linux CD and reading the files without the access controls imposed by the Windows operating system, as she did to access the SAM file. This was a level of access that Manning obtained independently, before the March 8, 2010 jabber chat and without any evidence of anyone instructing or assisting her in this process.

65. Basic technical knowledge or research would have also shown that Manning did not have a decrypted password hash that could be used to crack the password. She only had the encrypted hash from the SAM file and not the key to decrypt it that could be derived from the system file. This encrypted hash was useless to obtain access to anything. There are far easier, more reasonable ways to obtain the decrypted password hash, yet the other party of the chat did not advise Manning of this or otherwise instruct Manning on how to obtain the decrypted password hash.

Computer Usage in the T-SCIF

66. In reviewing the testimonies during Manning's court martial, and in discussing computer usage in the T-SCIF with the witness, crucial points have arisen which I consider to be relevant considerations in the investigation of Manning's actions. In particular:
- Soldiers put unauthorized files and programs on computers in the T-SCIF
 - Manning's colleagues viewed her as a technical expert
 - Manning's colleagues regularly asked her to install programs on their computers
 - Other soldiers cracked the administrator password in order to install programs
 - Issues with computers were fixed by reimaging

Soldiers put unauthorized files and programs on computers in the T-SCIF

67. While the soldiers in the T-SCIF were primarily conducting intelligence analysis based on classified information, they also sometimes took breaks during their 12 hour long shifts in order to watch movies, listen to music, play games, or go to the gym (Exhibit 19, p.252-3, Exhibit 18, p.9934-7). These practices lead to lax security.
68. Watching movies and playing games meant that there were as a result unclassified, unauthorized files and programs on computers dedicated to sensitive, classified work. Movies, music, games, and programs were put on the T-Drive, stored on computer desktops, or loaded onto the computers via CD (Exhibit 19, p.252-3). Several of Manning's former colleagues testified about these breaches of security practices during her court martial. Some of these testimonies were summarized as follows:

"Captain Steve Lim: Soldiers listened to music and watched movies on their computers and saved music, movies and games, unauthorized software.

Captain Casey Fulton: Soldiers saved music, games and computers to their computers. She added mIRC Chat and Google Earth to her computer.

Mr. Jason Milliman: Soldiers added unauthorized games and music to their computers and was aware that Soldiers were adding unauthorized software to their computers although he did not believe the practice is common.

Captain Thomas Cherepko: he saw unauthorized music, movies, games and unauthorized programs improperly stored on the drive. He advised his immediate supervisor and the Brigade Executive Officer concerning the presence of unauthorized media on the T-drive, nothing was done.

Ms. Jihrleah Showman: She and everyone else in the unit viewed mIRC chat as mission essential and everyone put it on their computers." (Exhibit 19, p.252-3)

69. Soldiers also testified that they did not just put files on the T-Drive, but actually installed or tried to install programs (Exhibit 19, p.252-3, Exhibit 9, p.8028-8042). Sometimes these programs were required for work purposes, including programs that were not officially approved but were viewed as "mission essential" (such as mIRC chat) (Exhibit 19, p.252-3).
70. Officially, Jason Milliman, a contractor based out of FOB Hammer, was supposed to install programs on the DCGS-A computers. During Manning's court martial, Milliman testified that only he and one other person had administrator access on the DCGS-A computers (Exhibit 8, p.8691-8695). But even Milliman could not simply decide to install a program. For each new program, or even a new version of an approved program, there was a lengthy approval process (Exhibit 8, p.8701-5). Programs that were assessed and authorized would then obtain a "certificate of networkiness" and could then be installed on the computers (Exhibit 8, 8642-8643).
71. This process was too time consuming and cumbersome, so soldiers would try to find alternate ways of running or installing programs instead of asking Milliman to install them from the start. For example, Joshua Ehresman testified during Manning's court martial that he initially tried to install a media player without asking Milliman for help:

"Q. You wanted to have a media viewer from a CD and you put that into your computer.

A. Yes, ma'am.

Q. And you put a shortcut on the desktop to use that?

A. No. I would just go straight to the CD, ma'am. I have a shortcut to the CD player.

Q. You had a shortcut to the CD player?

A. Yes, ma'am.

Q. Then why did you go to Mr. Milliman at all about using that CD?

A. If the CD got scratched or you lost it or something, you didn't have access to that computer or to that program no more. So I wanted to put stuff on my computer. Anything I wanted to put on it that was not already on a DCGS I had to go through Mr. Milliman.

Q. So this media viewer, did you actually run it from the CD or did Mr. Milliman put it on your computer?

A. I ran it from a CD for a little while until Mr. Milliman said it was okay to put it on and he eventually put it on for me.

Q. I thought I heard you testify earlier that you had tried to use it from the CD and

you needed administrative rights?

A. Yes. That's -- I initially tried to put on it myself.

Q. On the computer?

A. Yes, ma'am.

Q. If you weren't supposed to add things to the computer then why did you do that?

A. Because we -- I did not know at that time that the DCGS was not our property and that's why we're not allowed to put those that on the DCGS because they were not our, 2-10, property. I assumed they were ours from home, which they were not." (Exhibit 13, p.9848-9850)

72. The above examples of evidence from the Manning court martial indicate that unauthorized use of computers was commonplace.

Other soldiers cracked the administrator password in order to install programs

73. There is evidence in the court martial transcript that shows that there were other occasions where soldiers cracked the administrator password in order to install programs. Jason Milliman, the contractor in charge of administering the DCGS-A laptops at Forward Operating Base Hammer, testified during Manning's court martial that it was a common occurrence for soldiers to try to crack the administrative password to install programs:

"Q. Now based upon your experience, you did have situations where in the past you had military members trying to crack the password to the DCGS-A computer?

A. When there's a RIP/TOA, it was a common occurrence that ---

Q. And I'm sorry -- just to stop you there. The RIP/TOA was just when two units were swapping out?

A. When they would overlap -- yes. That when the 82nd would leave and 2/10 would come in, it's called a RIP/TOA; Relief In Place and Transition of Authority. So when the new unit coming in would bring in their DCGS-A computers, the standard philosophy, I guess, or belief of the unit is they're our machines, we have full rights, you can't have administrator privileges. So there was a special letter signed by somebody saying that only the DCGS-A FSEs had administrative privileges not the unit S-6s. So in the very beginning there was friction, but we got it ironed out. So there were a couple of occasions where they would crack my password, remove the administrator account, and we would battle that out." (Exhibit 8, p.8707)

74. During Manning's court martial, Milliman also recounted a specific incident where soldiers cracked his password in order to install a program and then deleted his administrator account:

"Q. Now, you did report an incident that involved XP Lite, correct? Another executable ----

MJ: XP?

CDC[MR. COOMBS]: XP Lite.

MJ: Lie or Lite?

CDC[MR. COOMBS]: Lite. L-I-T-E, ma'am.

A. That name sounds familiar. I'm not sure -- I mentioned a program to prosecuting attorneys that -- I didn't remember what the name was, but there was some program

they liked that would condense PowerPoint programs. If that's that program, then I remember it. But I don't remember a name specifically.

Q. All right. And do you remember ever going essentially to the S-6 because they added that program to the DCGS-A machine over your authorization?

A. There was a program -- I think I mentioned this earlier that they had cracked my password in order to install. It may have been that software, but I don't recall what the name of the software was.

Q. And when you took that to the S-6, what happened after you said, hey, you cracked my password, you added this program, what happened after that?

A. I had to reimage the machine because one of things one of the steps they took was to delete the administrator account from the machine, which is a required account for me to do my job, so I had to reimage the machine, which reinstalled the administrator account, and put those back the way they were before S-6 got a hold of it." (Exhibit 14, p.10571-10572

Manning's colleagues viewed her as a technical expert

75. It is clear from the evidence in her court martial that Manning's colleagues viewed her as the most technically proficient soldier in her unit. This was because she frequently helped others solve computer problems and also regularly bragged about her technical skills. For example, Showman testified during Manning's court martial that Manning indicated that she could get around passwords for some websites that her unit needed to access:

"He indicated -- not necessarily the computers we were working on, but the portals that we had to access when we first arrived. We were having issues getting access to some division portals. He indicated to me that their passwords were not complicated and he can always get through them." (Exhibit 15, p.7754)

76. It does not sound like Manning necessarily cracked or circumvented the password in this situation, but merely bragged that she was able to do so. Showman notes that the passwords in question here were for online portals, not user accounts on the computers.
77. Manning also tried to discuss technical topics and projects with her colleagues. During Manning's court martial, David Sadtler testified that Manning once proposed starting some sort of hash cracking business. Specifically, Manning wanted to generate rainbow tables and sell them:

"Q. During your conversations with PFC Manning, did you ever have a conversation about setting up a hash table software?

A. He had brought me to the side to have what seemed to be a private conversation and he fielded the idea to me that he wanted to generate hash tables on a computer and market that in some fashion.

Q. What are hash tables?

A. Hash tables are mathematical calculations of passwords that are supposed to be in a one-way fashion so that you can't reverse that sequence into the original password, thereby securing that password from release.

Q. And the idea that PFC Manning was talking to you about from what you heard, did you believe that was a marketable idea?

A. It had already been accomplished in the open-source world. Or it was generally already known to exist. So for reimplementing it, it did make sense to me.” (Exhibit 13, p.9854)

78. This conversation suggests that Manning may have been exploring hash cracking due to technical curiosity and potential business opportunities. While she was discussing rainbow tables and password hashes in the jabber chat, she was also discussing the same topics with her colleagues. This, and the other factors previously highlighted, may indicate that the hash cracking topic was unrelated to leaking documents.

Manning’s colleagues regularly asked her to install programs on their computers

79. While Manning may have been interested in password hash cracking for academic or business purposes, learning how to crack passwords would also have been of practical use for her daily work. This was because her colleagues often asked her to install programs, sometimes as part of the unauthorized usage of the computers in the T-SCIF. For example, Madaras, the soldier who shared computers with Manning for several months, testified that Manning helped him setup a chat program:

“Q. So do you recall having PFC Manning set up mIRC chat on your computer?

A. Yes, sir.

Q. And do you recall him doing that for others?

A. Yes, sir.

Q. And mIRC chat, when you did that, it was put on your computer basically as something that you would double click to start on the desktop?

A. Yes, sir.

Q. And you're sure PFC Manning did this and not Mr. Milliman?

A. Yes, sir.

Q. And when PFC Manning did this for you and others, did anyone step in, to your memory, and say, hey, that's not permitted?

A. No, sir.” (Exhibit 9, p.8028)

80. This was a common occurrence, with those in charge of Manning also asking her to install programs for them. For example, Fulton, one of Manning’s direct supervisors, also testified that she asked Manning for help adding programs to her computer (Exhibit 19, p.139-145).
81. During an interview, one of Manning’s other supervisors noted that Private Manning was one of the most technically proficient soldiers in his unit, so he and others would turn to Private Manning when they had computer issues when Mr. Milliman was not working. He stated that he and others would ask Manning to install programs on their laptops when Mr. Milliman was not available or when Mr. Milliman would most likely not approve of the program that they wanted installed on the secret laptops. He said that he did not know how Private Manning accomplished having the programs installed but the programs got installed.
82. While some programs could be run by simply setting up a shortcut on the computer, others required an administrator password to install (Exhibit 8, p.8691-8695). Having the ability to install programs from an administrator account would have helped Manning

fulfill the requests of her colleagues and supervisors to install certain programs.

Fixing Computers by Reimaging

83. Reimaging was one of the main ways problems with laptops were fixed. This process deletes all the data and reloads the operating system with the original settings. In practice, this was most often necessary when soldiers stored too many files on their desktop (Exhibit 8, p.8688-8691).
84. When Milliman reimaged a computer, he would try to copy the data off in order to transfer it back to the computer after it was reimaged. But because each computer was shared between two different people who worked alternating shifts, Milliman had to stay in order to talk to the person who used the same computer on the next shift and ask if they wanted their data backed up too. In order to ensure he was able to talk with people from both shifts, Milliman said that he worked the last part of the day shift and the first part of the night shift (Exhibit 8, p.8712).
85. Milliman also described how he and the other administrators had images that included the most recently authorized versions of the approved, default DCGS programs (Exhibit 8, p.8709).
86. Manning's computer was reimaged on March 1st or 2nd, 2010. During Manning's court martial, it was explained that no copy of the Collateral Murder video was found on Manning's computer before March 2, 2010 because the computer had been reimaged due to having issues and thus there no data from before March 2010 was available (Exhibit 20, p.130).
87. The consequences of reimaging would be that unauthorized files and programs may have been lost. Soldiers would have to go through the same processes again in order to reinstall them. It may be notable that this reimaging took place a few days before the portion of the Jabber chat log in which Manning sent a password hash.
88. A fuller consideration of the technical and contextual elements pertaining to the use of computers in the T-SCIF demonstrates that there were many more potential reasons why Manning would try to crack a password, for example, in order to install programs for her colleagues. Technically, in examining whether this theory is more realistic it is relevant that access to an administrator account would allow Manning to install programs, but would not allow her to download data anonymously. Contextually, that accords with both the historical attempts of soldiers to crack passwords in order to install software and the fact that Manning's colleagues regularly asked for her help installing programs.

Further Considerations

Forensic analysis is impossible due to destruction of evidence

89. Unfortunately, it is impossible to assess this theory with forensic evidence. This is because most of the relevant digital evidence, 10 of the 14 computers from the T-SCIF, were destroyed before their data could be copied (Exhibit 19, p. 313-320). These

computers were destroyed despite requests to preserve them (Exhibit 19, p. 313-320).

90. During Manning’s court martial, her lawyer explained the importance of the preservation of the images of these computers, stating that this data was necessary in order to analyze the programs installed on the computers of other soldiers in the T-SCIF:

“The common practice that he testified would be that people would add later versions that were not authorized; and Captain Casey Fulton testified that my client, at her instruction, added a later version onto her computer. So that one example there would be information that is helpful to the defense. We believe that that is clearly on the ENCASE images and that is why we have asked for them. That is why we asked for them to be preserved and provided.” (Exhibit 19, p.145)

Dated the 10th day of January 2020

Signed _____



Patrick A. Eller
President/CEO
Metadata Forensics, LLC