Digital Investigation (2005) 2, 247-253

Digital Investigation

Case study: A failure success' clothing

Erin E. Kenneally [a,*], **Andrea Monti** [b]
[a] *San Diego Supercomputer Center" Alchemy, Inc., USA*
[b] *University of Chieti, Italy*

Table of Contents

Surveying the scene

The headlines read familiar: 'Hacker Successfully Nabbed for Virus Writing'. Current news features are fertile with accounts of digital miscreants, so the recent guilty verdict of an Italian worm author is relatively indistinguishable amidst the growing list of digital justice victories. What's more, the Defendant admitted malware (as labeled by the prosecutor) authorship and dissemination from the start, there was no cat-and-mouse chase with the Italian police, and the code was relatively impotent. Fodder for CSI this is not. This case is, however, remarkable for what it does not say: procedurally, how NOT to conduct a digital investigation, and substantively, what are the underlying lessons it offers forensic practitioners and society in general?

Legal precedent in the field of digital investigations/digital evidence admissibility is burgeoning, resulting in digital forensic practices that are guided by industry standards developed from a mix of conjectural empiricism and anecdotal abstraction. In other words, our techniques are informed by what we think will be admissible and/or reliable based on how courts have ruled on other types of digital investigations or by analogizing to rulings on traditional evidence. In the absence of precedent, questions concerning "will

* Corresponding author. University of California San Diego, Pacific Institute for Computer security, San Supercomputer Center, 9500 Gilman Dr., La Jolla, CA 92093-0505, USA. Tel.: +1 858 534 5000.
E-mail addresses: erin@sdsc.edu (E.E. Kenneally), amonti@unich.it (A. Monti).
1742-2876/$. see front matter © 2005 Published by Elsevier Ltd.
doi: 10.1016/j.diin.2005_10.002

the X evidence be admitted or carry weight if I do loom for digital investigators, and we are left with inefficient avoidance of risk.

On one level, this case highlights how investigators and courts can be less than arduous in their scrutiny of various forensic procedures resulting in eVidentiary deficiencies that, under evolved forensic standards, should have rendered much of the digital evidence unreliable at best and inadmissible at worst. Here the court apparently ignored many blatant forensic mistakes and interpreted the law questionably. So, courts do not always get it right, fair enough, but what is the implication for future, similar cases if courts choose to apply and interpret the law with less rigor than novel cases deserve?

On a deeper level, the significance of this case on the horizon of 21 st century jurisprudence is that offers of proof (i.e. establishing the actus reus and mens rea elements of a crime) in the digital realm present new challenges. How do we infer intent from the action of automated programs act on our behalf? How do we infer consent from the actions of computers and programs who are a proxy for some human actor? The just resolution of these types of questions demands that sound forensic procedures be maintained lest it becomes more difficult to create precedent that correctly blueprints for consistent resolutions of like issues dressed in new clothing.

Specifically, this case raises issues about how we infer 'unauthorization' and 'dangerousness' from the architecture and interaction with an automated worm program. This is because Italian penal law does not forbid the creation of a self-replicating code as such, but rather, prohibits the spread of any "dangerous" program capable of damaging an information system. Therefore, proving that the code was executed without the consent of the user, whether the virus acted differently than what the user expected, and whether or not the worm was capable of causing damage (disclosing confidential user data/information) become issues of first impression.

As the line demarking "dangerous" and "destructive" can be more nebulous in the digital realm, the arguments on either side become more credible, and the competition for truth turns on more certain procedural factors. If we permit laziness in the application of forensic procedures, we either focus attention away from the substantive interpretation of laws applied to novel controversies, or preclude tackling substantive interpretation because of muddied procedural waters.

Just the facts, ma'am

In March 2001, the Vierika worm was released into the wild and brought to the attention of the Italian law enforcement, Guardia di finanza (GdF) the "fiscal and economic" police. Upon notification by an anti-virus manufacturer,1 the website containing the page infected with the main worm code was shut down in a few hours by the free hosting ISP in Italy. Police obtained account ownership and transaction records from the ISP, which allowed them to obtain a search warrant for Gabriele Canazza, a 30-year-old programmer from Bologna. During the execution of the warrant the GdF asked Mr. Canazza to disclose Vierika, to which he voluntarily made available the worm's source code. Ca-

---

[1] 1 F-Secure Virus Definitions: Vierika, available at <http://www.f-secure.com/v-desks/vierika.shtrnl>.

nazza was then charged with computer trespass (sect. 615 ter codice penale). While Canazza was present, authorities accessed his PC and burned three CDs containing copies of the Vierika source code, leaving one copy with the Defendant. Furthermore, in the presence of his original attorney, Canazza released a statement claiming full authorship of the Vierika code while denying that his "essay", or proof of concept, was a violation of the law.

The Vierika worm itself is categorized as one of the mass mailer variety and is written in Visual Basic script. The first part of the worm arrives via an MS Outlook message as an attachment. The subject of the e-mail reads, "Vierika is here" and the message attachment is file named "vierika. JPG.vbs". When the attachment is run, the script changes the security zone settings of Internet Explorer and alters the user's browser home page to an Italy-based Web page. The next time the Internet Explorer browser is started, the browser connects to that Italian web page containing the second part of the worm ("Vindex.html"), which displays the message "THE MATRIX IS CONTROL" . This part of the worm code executes directly from that site by capitalizing on the previously changed security zone settings. This script code is the main part of the worm and it takes the first part of the worm (c:\Vierika.JPG.vbs) and spreads it using MS Outlook to every address listed in the address book. [2]

Canazza was formally tried on the basic crime of illegal trespass aggravated by the charge of disseminating a program aimed at damaging or interrupting the operations of a computer system. [3]

Under Italian law, the legal elements for trespass include:

a) Willingly accessing a system without authorization
b) by defeating security measures
c) or abusing a legitimate access credential

The legal elements for the aggravated charge of damage to computers include:

a) willingly writing (or spreading) a computer program

---

[2] See, Anatomy of a Worm: Handling the Vierika Case, Stefano Zanero, Politecnico Milano, Dip. di Elettronica e Informazione, available at <www.nonloso.net> see also, <http://www.zdnet.co.uk/news/2001/12/ns-2·1943.html>.

[3] Art. 615 Ter CP; Art. 615-Quinquies CPo Italian Penal Code Article 615.3: unauthorized access into a computer or telecommunication systems: anyone who enters unauthorized into a computer or telecommunication system protected by security measures, or remains in it against the expressed or implied will of the one who has the right to exclude him, shall be sentenced to imprisonment not exceeding three years. Italian Penal Code, Article 615.5: spreading of programs aimed at damaging or interrupting a computer system: "Anyone who spreads, transmits or delivers to computer program, whether written by himself or by someone else, aimed at or having the effect of damaging to computer or telecommunication system, the programs or given contained in or pertaining to it, or interrupting in full or in part or disrupting its operation is punished with the imprisonment for to term of up to two years and to aim of up to It. L. 20.000.000", available at <http://www.ladysharrow.ndirect. co.uk/library/lawslitalian_law.htm>.

b) whose aim or effect is to provoke damage to a computer program or information, or alter the way a system works.

Trial the competition for truth

Prosecution case
During the "capo di imputazione" (Cdl)4 Canazza was accused of:

- authoring the Vierika code;
- sending Vierika to the Italian ISP;
- infecting some 900 user PCs by way of sending it through the ISP;
- illegally trespassing the above mentioned 900 PCs;
- stealing confidential information (especially e-mail addresses); and,
- damaging the PC's working conditions.

The prosecution's position was that the trespass and damages elements were met by virtue of Vierika's self·propagation activity which constituted theft of users' PC computing power, overcharging the ISP's network bandwidth (denial of service argument); and exposure of infected computers to third party infiltration by lowering IE's security zone settings. The prosecutor put forth evidence of the worm code and its workings, log files from the ISP linking the infected site ownership to Canazza. At no time did the prosecutor offer any specific evidence of these damages.

Defense strategy and forensic assessment

Dissecting the law and the code
The defense countered that the required elements of the charges were not proven. Specifically, the prosecution did not offer evidence that the source code recovered from Canazza's computer was the same that was spread across the network and allegedly infected and damaged some 900 users.

Recall that Canazza never disputed his authorship or transmission of the Vierika software. Canazza fully admitted to writing the code and putting it out on the Internet. He did not, however, confess to illegal trespass (art. 615-Ter CP) or having written a program that caused damage (sect. 615-Quinquies CPl. So, in addition to challenges based on lack of evidence, the defense argued that trespass by Canazza was impossible because the Vierika code did not allow remote control of an infected computer, thereby negating the mental intent ("willingly accessing") element. It was not a Trojan program, a dialer or a phishing tool, which in effect meant that it never communicated e-mail addresses or any other information with a master controller to send or receive information. The defense argued that since Vierika was not structured to communicate back to a master computer, it cannot be claimed that Canazza performed the intentional access.

Second, Canazza disputed that Vierika was a "virus", by virtue of the legal definition: 'a computer program whose aim or effect is to provoke damage to a computer program or

---

[4] Roughly, the list of facts committed by the Defendant "crossed" with the laws that have been infringed.

information, or alter the way a system works'. To this effect, the defense offered up technical testimony disputing that Vierika was dangerous or that it was aimed at damaging software, data or systems. Specifically, the defense countered that Vierika was a harmless worm.

To reiterate, the dispute centered around whether Canazza wrote and disseminated code that intentionally accessed another's system without authorization by subverting security measures, and was intended to cause damage. Canazza claimed his Vierika code was not a virus, but rather, an "essay" or "proof of concept" that was not intended to provoke any damage. The defense argument, therefore, was that the mental element of the crime was not present and he was not in violation of the law. The defense attempted to fortify its claim that Canazza lacked the willingness to cause damage by putting forth evidence from which one could deduce Vierika was not designed to cause damage. To counter the network bandwidth damages claim, evidence was put forth showing that Vierika's spreading capacity was weak. Regarding the alleged damages resulting from the lowered security zones, defense experts cast doubt as to whether lowering the zones actually exposed the infected PCs to unauthorized access by third parties. Vierika, it was argued, did not try to lower security measures any more than what common and prevalent personal firewall or antivirus programs do.

In terms of countering the potential dangerousness claim, the defense technical experts concluded that Vierika could not have caused significant harm to the Internet infrastructure, as alleged by the prosecution. This was based on the following findings: the Italian law enforcement wrongly calculated the real population that could be potentially affected by the worm-susceptible population as being the "totality of the computers being sold today". On the contrary, the worm used functions specific to only certain users on machines running Windows platform, with the Outlook (not including Outlook Express) application installed.

As for the trespass charge, the defense disputed that the security zones should be considered a "security measure", rather than the marketing verbiage put forth by Microsoft. In other words, the zones should be considered a custom configuration that are part of the user browsing preferences which are just different ways of using the software. The IE "security" zones do not meet the law's definition of "security measure" "some thing that allows safe code to interact with the system, excluding the malware to provoke harm" since they are completely blind to the nature of the code being executed on the machine (i.e. if the level is heightened to its maximum, no remote code -useful or harmful -can be run on the machine). [5]

Turning to whether the code execution was done without the user's consent, the opinion proffered was that there is one act by which a user grants consent to the execution of a program in a Windows-based platform-by invoking it or double-clicking it. Vierika did not usurp this principle, but maintained the purported authorization paradigm since it did not use a vulnerability to launch itself without user intervention.

---

[5] See Zanero.

In addressing a closely related point of debate, it could reasonably be argued that Vierika tricked, enticed or otherwise created false expectations as to its content (i.e. that it would not violate security restrictions) so as to negate the inference of user consent in clicking on the attachment. The assertion is that the users' expectations of the program's function depend upon explicit indicators such as content description, the software or file icon, the file name, etc. Other mechanisms for securing advanced knowledge of what code written and compiled by others will do is to engage in low level analysis of the code, such as relying on assurances of the program author in source code or manually inspect the code (e.g. disassembling and debugging), both nontrivial tasks that average computer users cannot be reasonably expected to perform. However, Vierika did not employ a deceptive or error-inducing icon or name, nor did the conjoined e-mail attempt to social engineer the user into running the viral code. The message clearly stated, "Vierika is here", and the attachment visibly appeared as a VBS shell script.

In addressing the issue of whether Vierika was capable of disclosing confidential user data, defense technical experts opined that Vierika did not tamper with the host machines any more than was necessary to activate its self-propagation function. The prosecution's claim was that the mass mailing behavior of Vierika constituted disclosure of private data by virtue of using Windows Address Book to initiate self-propagation. The counter argument was that "disclosure" requires at least one unauthorized subject to have access to data on the system. As such, Vierika could not be considered a subject, because it used information present on the host but did not relay it to third parties. Each e-mail was addressed to a single recipient.so Vierika did not bring about disclosure of confidential data.

As far as data protection is concerned, it was argued that Vierika did not adversely affect or violate the classical confidentiality/ integrity/availability principles of information security.

Procedural defense
To counter the forensic evidence presented by the prosecution, the defense-appointed academic forensic expert opined that the 'forensic acquisition of information from the ISP and the enforcement of the search warrant at Canazza's home was contrary to all the international acknowledged forensics standards. For example, the extent of law enforcement's collection in executing the search warrant consisted of booting the suspect's computer and burning logical copies of the source code.

Another defense point was -without implying that what has been given the Court was the actual Vierika code -to ask for a court-appointed-expert source code review and opine on the "dangerousness" of the Vierika program.

Outcome and lessons learned
On July 21, 2005 the Bologna Court found Canazza guilty of both trespass and authoring a virus. The case is currently under appeal, and Canazza faces a 6-month imprisonment sentence and a stiff fine.

One purpose of this case study was to highlight how investigating and prosecuting crimes involving digital activity can raise challenging issues of proof for which sound forensic procedures can help resolve. As with the Vierika trial, there was a strong tendency to view the forensic issues as mere technicalities that were not afforded the proper importance in deciding whether the elements of the crimes were proven beyond a reasonable doubt by the Prosecution.

"Prosecutors want to win especially when a guilty defendant tries to get off because of some governmental misconduct -a "technicality". In such cases, the law demands acquittal. ... Prosecutors ... often seek convictions in cases based on illegally obtained evidence. In such cases the prosecutors are not seeking justice. They, like the defendant who wants an acquittal, are seeking only one thing: to win". [6]

This short excerpt from a renowned Harvard Law Professor and civil right advocate clearly reinforces the question, one that could be considered a species of the Fruit of the Poisonous Tree doctrine. [7] Does the lack of forensic soundness render evidence inadmissible, and poison all subsequent evidence gathered by law enforcement as a result?

Neither Italy nor the U.S. has a clear rule that imposes the mandatory adoption of forensic techniques as a prerequisite for evidence admissibility. While the requirement to prove "authenticity" is a hallmark of U.S. evidence law, it leaves open to interpretation and application "how" that is to be done. While there are reams of cases establishing admissibility and reliability standard for physical evidence, precedent in the realm of digital evidence is only beginning to evolve and decisions are made on a case-by-case basis. The Canazza case is but one of a litany of cases that reveal a frightening trend of paying little heed to the importance of proper forensic procedure in resolving crimes that rely on digital evidence. [8]

---

[6] A. Dershowitz The Best Defense, p. 11-12 Vintage Books (1983).

[7] The Italian Legal system does not have, or at least enforces very lightly, the "poisoned fruit doctrine" in relationship to the mistaken collected evidences.

8 In a still pending trial for a bank-webslte-cracking case (Criminal Court of Milan, Case n. 12424/01, Justice Dr. Milanesi) defense and public prosecutor are debating hardly about the admissibility in court of a police-made cd-rom allegedly containing logfiles and other evidences, of which nobody ever heard after two years of public hearing and now "re·emerged" after one of the investigators mentioned this cd-rom under cross-examination. Apart from the statement that the concerned cd-rom is a copy of what the police had on its servers, and that those files were given to the police from the targeted bank IT-security counselor, the defense attorney was not provided with even the slightest element to evaluate the merit of this so-called "evidence".On the contrary, the Criminal Court of Civitavecchia (Rome) decision n.1277/04, in a child pornography case where the defendant was acquitted, acknowledged the importance of a court-appointed expert revision of the investigative claims: "since the agents didn't adopt adequate measures to guarantee the identity between the exchanged files .. the Court counselor correctly remarked that that have been found in the above mentioned directory cannot be identified - technically speaking - as the very same sent the defendant from the police, being possible to label it just as file of identical content".

To be sure, the defense tactic of challenging the "process" before challenging the "results" is not novel. The Supreme Court has held that "[merely raising the possibility of tampering is insufficient to render evidence inadmissible.[9] Commenting on this decision, the U.S. Department of Justice advocates that "[a]bsent specific evidence of tampering, allegations that computer records have been altered go to their weight, not their admissibility. [10] The practical effect is that the defendant bears the burden of proving tampering or unreliability of digital evidence. In order to properly balance the need for efficient resolution of justice, with the rights of defendants to be afforded a presumption of innocence and a fair defense, decisions that convict persons based on evidence obtained via less than arduous forensic procedures must not be endorsed.

Conclusion

To reiterate, the dispute centered around whether Canazza wrote and disseminated code that intentionally accessed another's system without authorization by subverting security measures, and was intended to cause damage. Canazza claimed his Vierika code was not a virus, but rather, an "essay" or "proof of concept" that was not intended to provoke any damage.

Although Mr. Canazza was the first Italian to be indicted after a full trial for alleged virus writing, in a broader perspective he was not alone. Here are a few examples of other indictments for "malware-related" crimes:

- Joseph Louis Popp (maybe the "father" of virus writers) was indicted by an Italian Court in 1993 for racketeering through a Trojan-infected floppy disks mass mailing.
  11Jan de Wit, author of the Anna Kournikova virus, which caused $167,000 (£94.446) in damage, received 150 h community service and subsequently received job offers from IT security firms.
- Spammer Jeremy Jaynes received a 9-year jail sentence by a U.S. court.
- Sasser and Netsky worm author Sven Jaschan was sentenced by a German court to 30 h of community service in response to his codes' infection of millions of computers worldwide at an estimated combined cost of more than $6.25bn (£3.53bn), received a 21-month suspended sentence. .
- Twenty-two-year-old Welsh web designer Simon Vallor was sentenced to two years in prison by Southwark Crown Court for writing the Gokar, Redesi and Admirer viruses, which infected 27,000 PCs ·in 42 countries.
- US-born Jeffrey Lee Parsons, creator of the Blaster B virus, which attacked more than 48,000 computers at an estimated cost of $1.2m (£680,000) was sentenced to 18 months in jail and 100 h community service.

---

[9] United States v. Allen. 106 F.3d 695, 700 (6th Cir. 1997).

[10] Computer Crime and Intellectual Property Section Criminal Division United States Department of Justice Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations Chap. V Sec. B Para 1, available at <http://www.cybercrime.gov/s&smanual2002.htm v. Oct. 25, 2005>.

[11] For an historical finding on early virus writer community development see P. Mungo Approaching Zero Random House; 1st American ed edition (March 16, 1993) ISBN: 0679409386. For the Popp trial "Italian side", A. Monti - S. Chiccarelli Spaghetti hacker Apogeo (1997).

- On Aug. 26, 2005 Carlos Enrique Perez-Melara, author of a spyware program called "Loverspy" was charged with "creating a surreptitious interception device, (i.e., the Loverspy program); sending the program, concealed in an innocuous-appearing electronic greeting card, to victims; advertising the program; advertising the surreptitious use of the program; illegal wiretapping; disclosing illegally intercepted communications; and obtaining unauthorized access to the victim computers. Each count of the 35-count indictment carries a maximum penalty of five years in prison and a maximum fine of $250,000 per count.[12]

If one were to cull a pattern from the patchwork of rulings involving persons accused of writing automated programs, one certain deduction is that courts are struggling with interpreting and applying laws that pttempt to label acceptable behavior in the digital realm. The difficulty lies in translating what society determines to be "good" and "bad" to inform the proper use of technologies that perform actions on our behalf, and the challenge is to focus not on socially undesirable technologies, but socially damaging "uses" of technology. Our collective consciousness in the physical world has little difficulty determining that firing a gun into a crowd is "dangerous" and "destructive", but we are still evolving the analogous digital consciousness. Indeed, launching a worm that renders whole networks unusable is socially detrimental and should not go unpunished.

To be sure, Canazza's "research" claim is not novel, as exemplified in the case of the most infamous virus writer Robert Morris Jr.. Yet, it is not without merit in some circumstances. Most importantly, it highlights the dual nature of virtually all tools and technologies, from the hammer and gun, to viruses and bots: they can be used to accomplish the intentions of their users, both malicious and beneficial.

So, proving legal elements such as "intent", "consent", “unauthorized", and “dangerous" in the digital realm requires more reliance on multiple streams of corroborating evidence in support. What this means for forensic investigators is that assuring the proper collection, preservation and presentation of the digital artifacts surrounding the "smoking gun" - e.g. the damaging email, the virus code, etc. - is of utmost importance in assuring the just resolution of disputes that hinge on digital evidence.

As the line demarking "dangerous" and "destructive" can be more nebulous in the digital realm, the arguments on either side become more credible, and the competition for truth turns on more certain procedural factors. If we permit laziness in the application of forensic procedures, we either focus attention away from the substantive interpretation of laws applied to novel controversies, or preclude tackling substantive interpretation because of muddied procedural waters.

Critical analysis of the Vierika case holding reveals inferential leaps made by the court that fall short of the rigorous proof that is both required and expected of the criminal justice system. In attempting to establish the physical and mental elements of the crimes charged the court relied primarily on witness testimony, with very little objective presentation of facts. For example, the court took for granted:

---

[12] See, "Creator and Four Users of Loverspy Spyware Program Indicted" avaHable at <http://www.cybercrime.gov/ perezIndict.htm>; (Oct. 24, 2005).

- the forensic soundness of law enforcement
- evidence acquisition and handling;
- the admissibility of ISP's log files
- the necessity of proving some of the actus reus
- elements of the charges -i.e. the actual spreading activity and damage.

Stated differently, factual evidence can be used to prove the actus reus and mens rea elements of a crime by putting it into the context of all facts that form the picture of a past event. Forensically sound techniques ensure that the supporting context is presented objectively, else that baseline context may be skewed and unjust decisions may result.

Erin Kenneally is a licensed attorney who consults, researches, publlshes, and speaks on prevailing and forthcoming issues at the crossroads of information technology and the law. These include evidentiary, procedural, and policy implications related to digital forensics, information security, and privacy technology. She has lectured and helped coordinate training conferences for officers of the court, law enforcement, and industry professionals concerned with digital evidence and information forensics. Ms. Kenneally is a Cyber Forensics Analyst at the San Diego Supercomputer Center and CEO of Elchemy, Inc., a non-profit corporation that conducts applied research and development solutions at the intersection of science and technology, the law and policy. She liaises and holds leadership positions with the Computer and Technology Computer High Tech Task Force (CATCH) and the Global Privacy and Information Quality Working Group, and provides thought leadership to numerous private and government advisory committees and working groups engaged in information technology law issues. Ms. Kenneally holds Juris Doctorate and Master of Forensic Sciences degrees.

Andrea Monti, trial counsel for Gabriele Canazza, is an Italian lawyer. His main field of practice is the Internet and hightech law. He worked for many companies, large and small, national and international. Including software houses, Telco's, Internet Service Providers, International Consulting Firms, Banks. His academic activity is mainly related to the universities of Chieti and Milano. But he gave lectures in several other faculties. Until 2003, Mr. Monti provided -on a regular basis -lectures to law enforcement bodies about computer crime and copyright law. He is a regular columnist for several IT magazine and wrote together with Stefano ChiccareUi the book "Spaghetti Hacker" and with Enrico Zimuel e Corrado Giustozzi, "Segreti, spie, codici cifrati". He translated into Italian Alan Cooper's "The inmates are running the asylum" whit the title "Il disagio tecnologico". Together with Alessia Ambrosini Mr. Monti authored "Trademark online" a survey on the domain-management legal and technical issues. Since 1995 he gave speeches and talks in several national and international conferences including Computer Freedom and Privacy 2000 and 2004 (Toronto and Berkeley), Eurosecurity 2004 (Paris), E-Crime and Computer Evidence Conference 2005 (Montecarlo). He chairs ALCEI Electronic Frontiers Italy (www.alceLit), the Italian digital free-speech advocate NGO. On june 2005 Mr. Monti's blog www.ictlex.net -was appointed by Reporters without Borders of the European "Freedom Blog Award". Any errors or unintentional misrepresentations of this case are the authors' alone and reflect translations of communications about this case between the two authors.