UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT

SUMMARY ORDER

Rulings by summary order do not have precedential effect. Citation to a summary order filed on or after January 1, 2007, is permitted and is governed by Federal Rule of Appellate Procedure 32.1 and this Court's Local Rule 32.1.1. When citing a summary order in a document filed with this Court, a party must cite either the Federal Appendix or an electronic database (with the notation "summary order"). A party citing a summary order must serve a copy of it on any party not represented by counsel.

At a stated term of the United States Court of Appeals for the Second Circuit, held at the Thurgood Marshall United States Courthouse, 40 Foley Square, in the City of New York, on the 2nd day of July, two thousand eighteen.

PRESENT: JOSÉ A. CABRANES,
GERARD E. LYNCH,
SUSAN L. CARNEY,
Circuit Judges.

UNITED STATES OF AMERICA,

Appellee,

v. 17-2479

FABIO GASPERINI,

Defendant-Appellant.

FOR APPELLEE: SARITHA KOMATIREDDY, Assistant United States Attorney, (David C. James, Assistant United States Attorney, *on the brief*), *for* Richard P. Donoghue, United States Attorney, Eastern District of New York, New York, NY.

FOR DEFENDANT-APPELLANT: SIMONE BERTOLLINI (Paul F. O'Reilly, *on the brief*), Law Offices of Simone Bertollini, New York, NY.

Appeal from a judgment of the United States District Court for the Eastern District of New York (Nicholas G. Garaufis, *Judge*).

UPON DUE CONSIDERATION WHEREOF, IT IS HEREBY ORDERED, ADJUDGED, AND DECREED that the judgment of the District Court filed August 11, 2017, be and hereby is **AFFIRMED**.

Fabio Gasperini appeals from a judgment convicting him, after a jury trial, of one count of misdemeanor computer intrusion under 18 U.S.C. § 1030(a)(2). The District Court sentenced him to the statutory maximum term of principally 12 months' imprisonment and a $100,000 fine, as well as ordering him to forfeit his "botnet" and related infrastructure. We assume the parties' familiarity with the underlying facts, the procedural history of the case, and the issues on appeal, which are explained in greater detail in an accompanying opinion of the Court.

In addition to the arguments addressed in that opinion, Gasperini also argues that: (1) the indictment did not provide him sufficient notice of the lesser included offense on which he was ultimately convicted; (2) there was insufficient evidence that he unlawfully gained access to any protected computer; (3) the District Court lacked jurisdiction, because the offense was committed abroad; (4) the District Court made several erroneous evidentiary rulings, including improperly allowing insufficiently authenticated hard drives to be introduced, and improperly allowing impeachment of the defense witness; and (5) his sentence was substantively unreasonable. We consider these claims *seriatim*.

1. Notice of Lesser-Included Offense

Gasperini argues that the indictment – which charged him with violating the aggravated, felony version of § 1030 – did not provide him with sufficient notice that he could be convicted of the lesser-included, misdemeanor version of the offense, which does not require proof of a fraudulent or commercial purpose. Rule 31(c)(1) of the Federal Rules of Criminal Procedure specifically permits a defendant to be found guilty of "an offense necessarily included in the offense charged." Two of our sister circuits have held that this rule in itself provides notice to a defendant that he may be convicted of a lesser included offense regardless of whether the lesser included offense is specifically pleaded. *See*, *e.g.*, *United States v. McGill*, 964 F.2d 222, 240 (3d Cir. 1992); *United States v. Brewster*, 506 F.2d 62, 74 (D.C. Cir. 1974). We need not decide here, however, whether that is correct as to every possible application, since, in this case, the government explicitly referenced, in the indictment and in a pre-trial filing, the lesser included offense of misdemeanor computer intrusion. Gasperini was thus on clear notice that the lesser offense was in play.

2. Sufficiency of the Evidence

Gasperini argues that there was insufficient evidence that he accessed a QNAP computer in the United States. That argument is premised on a citation to the testimony of two government

expert witnesses suggesting that the relevant ports on the American QNAP machines that they examined were closed, such that they could not be entered and affected by Gasperini's malware. But Gasperini ignores later testimony that the ports were initially found closed because the experts were connecting to the ports incorrectly. Once the mistake was corrected, the ports were in fact determined to have been open, and thus exposed to Gasperini's malware. At most, then, the issue presented a question of credibility and the weighing of conflicting evidence for the jury, not a question of insufficient evidence.

Nor is there merit to Gasperini's contention that the government failed to prove that he had obtained information from the computers. At a minimum, there was evidence that Gasperini's intrusion provided him with information about the username and password files stored on the computers, allowing a reasonable jury to conclude that Gasperini had obtained information from those computers. *See Jackson v. Virginia*, 443 U.S. 307, 319 (1979) ("[T]he relevant question is whether, after viewing the evidence in the light most favorable to the prosecution, any rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt.").

3. Extraterritoriality

Gasperini next argues that the prosecution fails because the Computer Fraud and Abuse Act of 1984 ("CFAA") does not apply extraterritorially, and that the crimes charged in the indictment were an extraterritorial application because the alleged "click fraud" scheme was directed at an Italian company. We note that this argument is properly considered as a challenge to the applicability of the statute of conviction, not to the jurisdiction of the district court, which was premised on the charge that Gasperini committed an "offense[ ] against the law of the United States." 18 U.S.C. § 3231. But however conceptualized, the argument is without merit.

There is a strong argument that § 1030(a)(2) applies extraterritorially. A 1996 amendment to the statute defines a "protected computer" to include any computer "used in interstate *or foreign* commerce or communication," 18 U.S.C. § 1030(e)(2) (emphasis added); *see United States v. Ivanov*, 175 F. Supp.2d 367, 374--75 (D. Conn. 2001) (adopting that argument). But we need not reach that argument here. The offense of which Gasperini was convicted requires no fraud victim, foreign or domestic. Rather, it prohibits unauthorized access to, and obtaining of information from, a computer. The jury had ample evidence to conclude beyond a reasonable doubt that Gasperini accessed, without authorization, nearly 2000 computers in the United States, including 200 within the Eastern District of New York. Whatever may have been true of crimes of which Gasperini was acquitted, the crime of which he was convicted was a domestic application of the statute, which was properly prosecuted even if the statute, or some portions of it, do not apply extraterritorially. The conviction is a domestic offense because the focus of the statute of conviction is gaining access to computers and obtaining information from them, and "[i]f the conduct relevant to the statute's focus occurred in the United States, then the case involves a permissible domestic application even if other conduct occurred abroad." *RJR Nabisco, Inc. v. European Cmty.*, 136 S. Ct. 2090, 2101 (2016).

4. Evidentiary Rulings

In addition to the evidentiary issue discussed in the accompanying opinion, Gasperini challenges two other evidentiary rulings made by the district court during trial. "A district court judge is in the best position to evaluate the admissibility of offered evidence. For that reason, we will overturn a district court's ruling on admissibility only if there is a clear showing that the court abused its discretion or acted arbitrarily or irrationally." *United States v. Valdez*, 16 F.3d 1324, 1332 (2d Cir. 1994). We detect no such abuse of discretion here.

Gasperini objects that copies of the original hard drives seized by Italian officials were not properly authenticated. The district court did not abuse its discretion in concluding that the copies were sufficiently authenticated. This ruling was supported by the testimony of the Italian investigator who had participated in making the copies, and who testified that the accuracy of the copies was validated by matching the "hash values" of the copies and the originals. Matching of hash values is an established method for authenticating digital evidence. *See United States v. Ganias*, 824 F.3d 199, 234–35 (2d Cir. 2016) (*en banc*) (Chin, *J.*, *dissenting*) (discussing authentication by hash values); *see also* Advisory Committee's 2017 Notes on Subd. (14) of Fed. R. Evid. 902 ("Today, data copied from electronic devices, storage media, and electronic files are ordinarily authenticated by 'hash value.' . . . This amendment allows self-authentication by a certification of a qualified person that she checked the hash value of the proffered item and that it was identical to the original.").

Gasperini also argues that the district court erred by permitting the government to impeach his expert witness by questioning him about a misdemeanor conviction that was more than ten years old. Under Rule 609(b)(1) of the Federal Rules of Evidence, such a conviction can only be used for impeachment if its probative value substantially outweighs its prejudicial effect. Whether or not we would have made the same ruling, we conclude that allowing the questions to be asked was not an abuse of discretion, and in any event the limited questioning on the subject, even if error, was harmless in light of the overwhelming evidence of guilt before the jury.

5. Sentencing

Finally, Gasperini complains that his sentence of twelve months in prison was substantively unreasonable. It was not. The district court was well within its discretion to impose the statutory maximum sentence of one year, especially given its finding that the government had in fact proved, by a preponderance of the evidence, that Gasperini had engaged in the fraudulent conduct charged in the counts of the indictment that the jury did not find proven beyond a reasonable doubt. *See United States v.* Yannotti, 541 F.3d 112, 129 (2d Cir. 2008). And even if we discount the evidence of those crimes, the extensive intrusion into thousands of computers, with the attendant costs to computer users and to the manufacturer of the vulnerable machine that were incurred in deleting malware and correcting the vulnerability exploited by Gasperini, amply justified the district court's conclusion that the crime was serious enough to warrant a one-year sentence of imprisonment.

* * *

For the reasons stated above and in the accompanying opinion of the Court, we **AFFIRM** the judgment of the District Court.

FOR THE COURT:
Catherine O'Hagan Wolfe, Clerk