IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF DELAWARE

UNITED STATES OF AMERICA,	:	
	:	
Plaintiff,	:	
	:	**Cr. A. No. 10-112-LPS**
v.	:	
	:	
XIANG LI,	:	
	:	
Defendant.	:	

GOVERNMENT'S STATEMENT OF FACTS

Had this matter gone to trial, the United States would have proved the following beyond a reasonable doubt through witnesses, testimony, and other competent and admissible evidence:

Between April 2008 and June 2011, Defendant Xiang Li operated an online business through which he engaged in the unauthorized reproduction and distribution of copyrighted software via the Internet. The copyrighted software sold by Defendant was "cracked," meaning that the digital license files and access control features created to prevent unauthorized access to the copyrighted software had been disabled or circumvented.

Defendant unlawfully distributed these copyrighted works – commonly referred to as "cracked" or "pirated" software – by selling them on websites with the domain names www.crack99.com, www.cad100.net, and www.dongle-crack-download.com ("the Websites"). *See* Demonstrative Chart at 1 (Exhibit 1). Defendant's Websites advertised over two thousand different "cracked" software products for sale at a fraction of their retail prices. The advertised software, most of which was created and copyrighted by companies based in the United States, is used in numerous applications, including defense, engineering, manufacturing, space exploration, aerospace simulation and design, mathematics, storm water management, explosive

simulation, and manufacturing plant design. The prices listed for these software products on Defendant's Websites ranged from $20 to $1,200. The actual retail value of these products ranged from several hundred dollars to over three million dollars.

Between April 2008 and June 2011, Defendant engaged in over 500 transactions through which he distributed approximately 550 different copyrighted software titles to at least 325 purchasers located in at least 28 states and over 60 foreign countries. *See* Ex. 1, at 2-3. These software products were owned by approximately 200 different manufacturers. More than one-third of these purchases were made by individuals within the United States, including small business owners, government contractors, students, inventors, and engineers.

In February 2008, Defendant registered the domain names for www.crack99.com, www.cad100.net, and www.dongle-crack-download.com ("the Websites"), listing himself as the registrant and operator of the Websites, which he controlled from Chengdu, China. Also in February 2008, Defendant created the Google email account china9981@gmail.com, which he used to facilitate the sale and transfer of pirated software to website customers.

Defendant received the funds generated from the unauthorized sale of the copyrighted works. *See* Ex. 1, at 1. Defendant collected monies sent by customers through such remitters as Western Union and MoneyGram as payment for cracked software. Defendant also established a bank account at Bank of China into which some of the proceeds from the sales of copyrighted software were deposited. Furthermore, Defendant distributed illicit funds to others for their work in furtherance of the criminal conduct.

Based on very limited transactional data the United States was able to obtain from certain U.S.-based payment remitters, Defendant obtained proceeds in excess of $60,000 from the sale of pirated software. This figure does not include any payments that Defendant received from

foreign-based payment processors. This amount represents a fraction of the retail value of these products, which the United States calculates as totaling at least $100 million.

Search warrants conducted on the contents of Defendant's gmail account captured over 25,000 e-mails transmitted between February 2008 and June 2011. These emails were transmitted between Defendant and hundreds of customers seeking to purchase pirated software products advertised on Defendant's websites. During this time period, Defendant used this gmail account to conduct well over 500 illegal software sales to customers located throughout the world. *See* Ex. 1, at 3. During most of these illegal transactions, Defendant used his gmail account to transmit copies of the pirated software products to his paying customers via compressed electronic files or hyperlinks to download servers located in the United States and elsewhere. *See* Ex. 1, at 1.

Defendant acknowledged his involvement in this unlawful software piracy conspiracy throughout his emails with customers. In a January 14, 2009 email exchange, for instance, a customer asked Defendant why he was reluctant to mail the customer a copy of the cracked software. Defendant answered this customer's question by stating, "Because the end of the strict customs checks. This is contraband." In another email exchange with a customer on or about February 2, 2009, Defendant stated: "I am not a crack production engineers (my job is to collect)[.] This is an international organization created to crack declassified document[s]." During a May 2009 email with a customer, Defendant stated, "I need to use your money to seek the help of experts to cracker master I earn 10% of the profits." In a November 2008 email exchange with another customer, Defendant stated that he would charge $1000 to obtain a cracked version of a particular software program. When the customer wrote, "Yes ok tell me who do this," Defendant replied: "Experts crack, Chinese people Sorry can not reveal more."

Some of Defendant's biggest customers were Americans who held significant engineering positions with government agencies and government contractors. For instance, Defendant sold and transmitted via the Internet 12 cracked software programs to Cosburn Wedderburn, who was then a NASA electronics engineer, working at NASA's Goddard Space Flight Center, in Greenbelt, Maryland. Between September 2008 and November 2010, Wedderburn exchanged multiple e-mails with Defendant to obtain pirated software programs with an estimated retail value exceeding $1.2 million. These software programs have a broad range of applications including electric engineering, aerospace, telecommunications design and electronic design automation.

Also by way of example, Defendant sold and transmitted via the Internet 10 cracked software programs to Dr. Wronald Best, who held the position of "Chief Scientist" at a Kentucky-based government contractor that services the U.S. and foreign militaries and law enforcement with a variety of applications such as radio transmissions, radar usage, microwave technology, and vacuum tubes used in military helicopters. Between November 2008 and June 2009, Dr. Best exchanged over 260 e-mails with Defendant to obtain 10 pirated software programs from Defendant. The estimated retail value of the 10 pirated software programs Dr. Best received from Defendant exceeds $600,000.

Controlled Purchases of Pirated Software by Law Enforcement Agents

Between January 2010 and June 2011, undercover law enforcement agents made a series of purchases of pirated software advertised on Defendant's Websites. The agents accessed the Websites from computers connected to the Internet from locations in Delaware and Pennsylvania. The agents corresponded by email with Defendant about their purchases, including negotiating price, receiving electronic files containing the pirated software or

hyperlinks that enabled agents to download the pirated software from computer servers located in the United States, and receiving instructions from Defendant on how to install the pirated software. The agents transmitted a series of wire transfers totaling $8,615 from a Western Union location in Delaware to Defendant and a co-conspirator located in Chengdu, China, as payment for the pirated software they purchased.

January 2010 Controlled Purchase of "Satellite Tool Kit 8.0" Software

In January 2010, undercover agents purchased a pirated copy of "Satellite Tool Kit 8.0" ("STK") from Defendant via the Internet. This software product is designed to assist the military, aerospace, and intelligence industries through scenario-based modules that simulate real-world situations, such as missile launches, warfare simulations, and flight trajectories. This software is a product of Analytical Graphics, Inc., which had not authorized Defendant to sell, distribute, or otherwise disseminate its product.

Pursuant to Defendant XIANG LI's email instructions, the undercover law enforcement agent sent a wire transfer in the amount of $1,000 from a Western Union facility located in Claymont, Delaware to Defendant's co-conspirator in Chengdu, China. In response, Defendant transmitted an email to the undercover agent containing three, compressed electronic files. An undercover agent downloaded each of these files, each of which contained operable professional versions of STK, along with the electronic license keys that control access to the software. The STK product sold to the undercover agents by Defendants contained several different modules or scenario functions generally used by the military and intelligence communities, including 3-D warfare scenarios. In total, the STK software sold to the undercover agents has an estimated retail value exceeding $150,000.

February 2010 Controlled Purchase of "Quartus II 9.0" Software

In February 2010, undercover agents purchased a pirated copy of "Quartus II Nios Embedded Suite v9.0," "Quartus II v9.0 FPGA Full Working," and "Quartus II DSP Builder 9.0" from Defendant via the Internet. These software products are used in the design of semi-conductor chips employed in the communications, medical, defense and other industries. This copyrighted software is a product of Altera Corporation, which had not authorized Defendant to sell, distribute, or otherwise disseminate any of these software products.

On February 22, 2010, pursuant to Defendant's email instructions, an undercover agent wired a Western Union payment of $340 to Defendant's co-conspirator in Chengdu, China from a Western Union branch located in Claymont, Delaware. In response, Defendant emailed four compressed electronic files to an undercover agent that contained the four software products ordered by the agents. The estimated total retail value of the Altera software products sold to the undercover agents by Defendants is over $10,000.

March 2010 Controlled Purchase of "HyperSizer" Software

In March 2010, undercover agents purchased pirated copies of "HyperSizer v.5.3.29" and "HyperSizer v.5.3" from Defendant via the Internet. These two software products were designed and produced by Collier Research and Development Corporation, which had not authorized Defendant to sell, distribute, or otherwise disseminate these software products.

On March 18, 2010, pursuant to Defendant's email instructions, an undercover agent wired $200 to Defendant's co-conspirator in Chengdu, China from a Western Union facility in Claymont, Delaware. In response, Defendant emailed a hyperlink that allowed the undercover agent to download operable versions of the HyperSizer software, along with the electronic license keys that control access to the software. The pirated copy of the HyperSizer software

sold to the undercover agent by Defendants had been modified to circumvent the proper functioning of the electronic license keys or files designed to prevent unauthorized access to these products. The HyperSizer software assists in the weight reduction, structural design and stress analysis of the composite materials used in the construction of aircraft and spacecraft. The estimated retail value of the HyperSizer product is approximately $50,000.

November 2010 Controlled Purchase of "Satellite Tool Kit 9.2.1" Software

In November 2010, undercover agents purchased a copy of "Satellite Tool Kit 9.2.1" from Defendant via the Internet. This software product was an updated version of the "Satellite Tool Kit 8.0" software that Defendant sold to the undercover law enforcement agents in January 2010. Analytic Graphics, Inc., the software product manufacturer and copyright holder, had not authorized Defendant to sell, distribute, or otherwise disseminate any of its products.

In an email transmitted on or about November 8, 2010, Defendant stated that the price of the cracked software was "very costly" because of the "development cost." On or about November 12, 2010, pursuant to Defendant's email instructions, an undercover agent wired $2000 to Defendant's co-conspirator in Chengdu, China from a Western Union facility in Claymont, Delaware. In response, Defendant emailed two hyperlinks, resolving to a web server located in Arizona, which allowed the undercover agent to download operable versions of the "Satellite Tool Kit 9.2.1" software, as well as the electronic license key that controls access to the software. The pirated copy of the "Satellite Tool Kit 9.2.1" software sold to the undercover agent by Defendants had been modified to bypass the electronic license keys designed to prevent unauthorized access to these products.

The "Satellite Tool Kit 9.2.1" downloaded by the undercover agent via the hyperlink provided by Defendant was an operable "Professional Edition" of the software, which had been

publicly released by Analytical Graphics, Inc. approximately one month earlier. The estimated retail value of this software was over $240,000.

January 2011 Undercover Purchase of Software and Proprietary Data

Beginning in December 2010, undercover agents engaged in electronic communications with Defendant, during which they discussed a plan in which they would resell copies of pirated software provided by Defendant to small businesses in the United States. On January 4, 2011, an undercover agent transmitted an email to Defendant seeking to purchase copies of fifteen cracked software products. In the email, the undercover agent stated that he and his colleagues planned to resell the software products to small businesses in the United States.

Defendant agreed to supply the requested pirated software products for a total price of $1,467. On January 6, 2011, an undercover agent transmitted a Western Union wire transfer in the amount of $1,467 from Claymont, Delaware to Defendant's co-conspirator in Chengdu, China.

On January 11, 2011, Defendant sent an email to the undercover agent offering to design counterfeit packaging for the fifteen software programs ordered by the undercover agent for an additional price of $1,500. In this same email, Defendant also informed the undercover agent that he had "More pleasant surprises." In particular, Defendant stated that he had approximately twenty gigabytes of valuable internal data from an American software company, which he offered to sell to the undercover agents for an additional $3,000.

On January 11, 2011, an undercover agent transmitted an email to Defendant requesting a sample of the counterfeit design packaging he offered to produce. Defendant sent an email to the undercover agent with an attached image file showing a disc bearing the counterfeit label of an Ansys software product. Defendant stated in this email: "All included CD printing, design, and exquisite box. Color graphic design… Your customers satisfied with your decision."

On January 20, 2011, an undercover agent transmitted a Western Union wire transfer in the amount of $4,350 from a location in Claymont, Delaware to Defendant's co-conspirator in Chengdu, China as payment for the design packaging for the previously ordered fifteen software programs and the twenty gigabytes of proprietary data from an American software company.

On February 1, 2011, the undercover agents received a mail package that contained six DVDs. A review of the DVDs revealed that each contained numerous files, including files with titles matching the fifteen software programs the undercover agents had ordered from Defendants. Defendant informed the undercover agents that he would subsequently provide the twenty gigabytes of proprietary data from the American software company.

June 2011 Meeting and Delivery of Software and Proprietary Data in Saipan

Through various email messages and Skype transmissions, Defendant arranged to travel from Chengdu, China to the Island of Saipan in June 2011 to meet with the undercover agents. At the meeting, Defendant was to transfer the pirated software, design packaging and twenty gigabytes of proprietary data paid for by the undercover agent in January 2011. Defendant and the undercover agents also were to discuss their plan for Defendant to transmit pirated software and related counterfeit packaging and labeling to the undercover agents via the Internet, which the undercover agents would assemble and resell to small businesses in the United States.

On June 6, 2011, Defendant traveled by air from China to Saipan to meet with the undercover agents. On June 7, 2011, Defendant met with undercover agents at a hotel in Saipan. During this recorded meeting, Defendant delivered to the undercover agents DVDs containing cracked versions of "Satellite Took Kit" 6.1.3, 8.1, and 9.2.1 software and various add-on software modules, installation programs and cracked license files associated with the software products. *See* Video of Undercover Meeting (Ex. 2). Defendant also delivered multiple

computer disks with counterfeit packaging and product labeling indicating that they contained various software products, including:

a. Ansys 13.0
b. NI Labview
c. Agilent EMPro
d. Ansoft Nexxim
e. Antenna Magus
f. CST Studio Suite
g. Matlab
h. Ansoft Designer
i. Vector Works
j. Hyper Works
k. Pronest
l. Ansoft Maxwell
m. Ansoft HFSS
n. Mastercam
o. Catia V5R20
p. Ansoft Simplorer

Defendant also provided the agents with disks containing approximately twenty gigabytes of proprietary data unlawfully obtained from an American software company.

At the conclusion of the meeting, Defendant was arrested by federal law enforcement agents, and the items that he brought with him to the meeting were seized. During a search of Defendant's hotel room, agents seized various pieces of computer equipment, including digital storage devices and a laptop computer. Defendant was subsequently transported from Saipan to the District of Delaware for prosecution.

Forensic Analysis of Software and Data Obtained During Saipan Meeting

A forensic analysis of the computer equipment and removable digital media seized from Defendant confirmed that it contained pirated copies of the software ordered by the undercover agents, packaging and documentation for such software, and approximately twenty gigabytes of proprietary data obtained from non-public areas of the website and an internal server of an American software company.

In particular, six disks seized from Defendant in Saipan contained an assortment of data obtained from one of the victim company's websites and an internal file transfer protocol site. These files included: the software license server; training and "flash videos" used to teach users how to operate the software; mapping data files including 3-dimensional imagery files; military and civilian aircraft image models; a software module containing data associated with the International Space Station; a complete listing of all of the software modules created by the company, as well as the 3-dimensional graphic images associated with these modules; a high resolution, 3-dimensional imaging program; various training courses under a folder called "Programmers Workshop;" and various other files including PDF and power point files associated with the software.

Counterfeiting Analysis of Software and Data Obtained During Saipan Meeting

As noted above, Defendant brought to the undercover meeting disks that contained the pirated software products ordered and paid for by the undercover agents in January 2011. The manufacturers have confirmed that the materials supplied by Defendant are counterfeit and, in a number of cases, infringe trademarks registered by the manufacturers.

Respectfully submitted,

CHARLES M. OBERLY, III
United States Attorney

By: /s/ David L. Hall
David L. Hall
Assistant United States Attorney

By: /s/ Edward J. McAndrew
Edward J. McAndrew
Assistant United States Attorney

Dated: January 4, 2013